UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE CUENCA

CARRERA DE INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del Título de: Ingeniero de Sistemas

"METODOLOGÍA PARA REALIZAR LA EVALUACIÓN, DETECCIÓN DE RIESGOS, VULNERABILIDADES Y CONTRAMEDIDAS EN EL DISEÑO E IMPLEMENTACION DE LA INFRAESTRUCTURA DE LA RED DE LA EDITORIAL DON BOSCO, MEDIANTE UN TEST DE INTRUSIÓN DE CAJA BLANCA"

AUTORES:

CRISTINA MARIBEL JARAMILLO CASTILLO
JUAN CARLOS RIOFRÍO HERRERA

DIRECTOR:

ING. PABLO LEÓNIDAS GALLEGOS

Cuenca – Ecuador

2015

CERTIFICACIÓN

Yo, Pablo Leónidas Gallegos Segovia, docente de la Universidad Politécnica Salesiana de la carrera de Ingeniería de Sistemas CERTIFICO, haber dirigido y revisado prolijamente cada uno de los capítulos de la Tesis intitulada: "METODOLOGÍA PARA REALIZAR LA EVALUACIÓN, DETECCIÓN DE RIESGOS, VULNERABILIDADES Y CONTRAMEDIDAS EN EL DISEÑO E IMPLEMENTACION DE LA INFRAESTRUCTURA DE LA RED DE LA EDITORIAL DON BOSCO, MEDIANTE UN TEST DE INTRUSIÓN DE CAJA BLANCA", realizado por los estudiantes: Cristina Maribel Jaramillo Castillo y Juan Carlos Riofrío Herrera, y por haber cumplido con todos los requisitos necesarios autorizo su presentación.

Cuenca, 21 de agosto de 2014

Ing. Pablo Gallegos Segovia

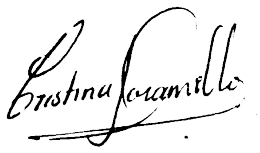
DIRECTOR DE LA TESIS

DECLARATORIA DE RESPONSABILIDAD

Los autores declaramos que los conceptos desarrollados, análisis realizados y las conclusiones del presente trabajo, son de nuestra exclusiva responsabilidad y autorizamos a la Universidad Politécnica Salesiana el uso de la misma con fines académicos.

A través de la presente declaración cedemos los derechos de propiedad intelectual correspondiente a este trabajo a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Cuenca, 4 de febrero de 2015



Cristina Maribel Jaramillo Castillo

C.I. 030235565-6

Juan Carlos Riofrío Herrera

C. I. 1104915937

DEDICATORIA

Con gran cariño y orgullo dedico este trabajo a todas aquellas personas que estuvieron a mi lado y me supieron apoyar para la consecución de esta meta, en especial a:

Mis padres María Teresita Herrera y Máximo Riofrío por su incesable lucha por darme lo mejor, por sus consejos, por todo su apoyo y en general por ser todo para mí.

Mis hermanas y hermanos por su apoyo incondicional y desinteresado, por ser mis amigos, por estar siempre a mi lado y por impulsarme a seguir siempre adelante.

Todos tendiéndome su mano y bríndame su cariño, afecto y confianza.

Juan C. Riofrío

Con todo mi cariño y mi amor dedico todo el esfuerzo y trabajo puesto para la realización de esta tesis a mis padres que con sacrificio y bondad hicieron todo para que yo pudiera lograr mi sueño.

Este trabajo ha sido posible gracias a ellos.

Cristina M. Jaramillo

AGRADECIMIENTO

En esta vida todo tiene un principio y un fin, hoy es el fin de una meta, una meta que parecía muy lejana, pero que con esfuerzo y perseverancia hoy ha culminado, tengo tanto que agradecer pues me siento muy afortunado de poder estar aquí y compartir este momento con seres tan valiosos, es por ello que debo agradecer principalmente a Dios por todas las bendiciones recibidas, a la Virgen del Cisne por guiar mis pasos, a mi familia por el apoyo brindado, por las palabras de aliento, y por estar siempre presentes, inclusive a pesar de la distancia.

También debo dar un agradecimiento especial a mi gran amiga Jessica M. Chicaiza, una persona valiosa que supo brindarme su apoyo para alcanzar esta meta, resaltando las risas y la alegría de preservar una linda amistad.

Agradezco a nuestro director de tesis y amigo Ing. Pablo Gallegos por el apoyo brindado durante esta investigación.

En general a todas las personas especiales que han estado en mi vida mil gracias…..

Juan C. Riofrío

Gracias a Dios por su infinita bondad y amor quien supo darme salud y fuerzas para seguir siempre adelante.

Agradezco a toda mi familia en especial a mis padres y hermanos por su apoyo en los momentos difíciles.

A esas personas importantes en mi vida, que siempre estuvieron listas para brindarme toda su ayuda.

Al Ing. Pablo Gallegos quien nos ha ofrecido sus conocimientos para lograr nuestro objetivo.

A ustedes por siempre mi corazón y mi agradecimiento.

Cristina M. Jaramillo

INTRODUCCIÓN.

Dentro de este proyecto se contempla el desarrollo de una metodología para llevar a cabo un *Penetration test* interno a todos los sistemas e infraestructura de red de la Editorial Don Bosco, en cuya ejecución se realizaran pruebas de penetración que simulan las que se producen durante un ataque, dichas pruebas se plasmaran por medio de la utilización de herramientas de software libre y propietario, teniendo acceso físico a las instalaciones de la empresa e interactuando con el personal en un entorno controlado, con el fin de garantizar que la información es fidedigna y los resultados sean congruentes y certeros.

Sin embargo es limitada la posibilidad de probar toda la gama de técnicas y mecanismos que los crackers o hackers pudieran emplear para vulnerar un sistema informático. A pesar de ello se señalara y demostrara indudablemente la mayor cantidad de vulnerabilidades que posean los sistemas para poder analizarlas y establecer políticas de seguridad, de esta manera preservar la confidencialidad, integridad y disponibilidad de los sistemas de dicha Entidad.

EL punto de partida para el fortalecimiento de la seguridad será conocer la situación real de los sistemas de la empresa que determinará las amenazas, agentes de amenaza, vulnerabilidades así como demostrar los riegos funcionales a las que está expuesto el sistema en su totalidad.

Posteriormente con un análisis de dichas falencias podremos establecer un informe técnico y ejecutivo para los Administrativos de la Empresa, el mismo que contemplara a grandes rasgos una lista detallada de las vulnerabilidades encontradas y verificables. Así como también se suministrara una lista de recomendaciones para que sean aplicadas por los responsables de seguridad en la empresa que entenderán y apreciaran los riesgos potenciales sobre el negocio.

Con esto la Empresa tendrá un panorama claro sobre las vulnerabilidades halladas en los sistemas de información lo cual es imprescindible al momento de aplicar medidas correctivas.

ANTECEDENTES.

La evolución de las redes en la actualidad ha permitido incrementar el flujo de información, permitiendo con ello agilizar procesos, pero esto trae consigo nuevas amenazas y vulnerabilidades. Hoy en día es necesario contar con una red segura, ya que una empresa que no cuente con dicha infraestructura no le será posible garantizar su productividad ni mucho menos su existencia en el mercado.

Tal es el caso de la Editorial Don Bosco, una empresa que comercializa textos y material didáctico de alta calidad, en la cual las actividades y procesos que realizan dependen del uso de sistemas que se relacionan con la información, y por ende dicha empresa está sujeta a riegos que puede impactar de manera económica, comercial, de prestigio y confianza.

En este contexto hay factores a tomar en cuenta, los equipos de cómputo y protocolos de comunicación no disponen de un mecanismo de seguridad por defecto, así mismo el despliegue de la tecnología en la sociedad, pone la capacidad de amenaza en manos de más personas, por esta razón no se puede dejar a un lado y mucho menos dar por hecho que la seguridad de los sistemas de la Editorial Don Bosco se encuentran en óptimas condiciones, ya que actualmente cada vez más empresas reconocen tener incidentes de seguridad en sus organizaciones, lo que demuestra que es importante invertir en su seguridad.

La empresa actualmente está buscando mecanismos que permitan minimizar el riesgo al cual puedan estar expuestos, ya que no existe como tal un proceso a seguir y que con ello garantice o se considere la seguridad de la información al 100%, es así que la implementación de mecanismos de control, como lo son el uso de estándares de seguridad, políticas internas, legislación informática, respaldos, planes de contingencias, esquemas de seguridad perimetral, servicios de seguridad, recomendaciones de instituciones como NIST, SANS, ISO, entre otras, puede ayudar a reducir riesgos.

Hay que garantizar que la información que circula a través de la red de la Editorial don Bosco, así como aquella que es almacenada en un equipo final manejado por un responsable de la empresa sea confiable, integra, disponible y confidencial, ya que de

ello depende que la Empresa cumpla con sus objetivos establecidos. Por otro lado, no es posible garantizar la seguridad global, pero sí es posible disminuir los riegos dentro de la red, esto se logra mediante distintas formas aunque como se mencionó, no necesariamente existe un camino, es decir, se pueden tener distintos esquemas de seguridad de acuerdo con las necesidades propias de la Empresa. Para ello se debe conocer la situación actual y real de los sistemas con el objetivo de mejorar la seguridad y disminuir los riegos mediante un Penetration Test que nos permita analizar todas las deficiencias de los sistemas y de la infraestructura de red con la que cuenta la Editorial Don Bosco.

JUSTIFICACIÓN.

Dado que la inseguridad de los sistemas se da de muchas maneras en nuestro entorno social y en vista de que la información es el factor primordial dentro de los sistemas, las organizaciones buscan tener mayor seguridad en sus esquemas lo que se ve reflejado en una buena imagen y reputación corporativa inclusive evita tener pérdidas económicas así como también de privacidad, integridad y confidencialidad.

El presente proyecto de investigación tiene como finalidad la contribución al fortalecimiento de dicho ámbito tan importante como lo es el campo de seguridad de los sistemas y de la red de la Editorial Don Bosco mediante el establecimiento de políticas de seguridad que responden a tres interrogantes: ¿Contra qué hay que defender a los sistemas? ¿Por qué hay que defenderlos? Y ¿Con qué podemos realizar dicha defensa? Las respuestas están basadas en los resultados de las pruebas de penetración que son un paso previo a los análisis de fallas de seguridad o riesgos para la entidad, enfocadas en comprobar y clasificar vulnerabilidades y el impacto que éstas tengan sobre la organización.

Este estudio deja al descubierto las vulnerabilidades que pudieran ser vistas y explotadas por individuos no autorizados y ajenos a la información como: crackers, hackers, ladrones, ex-empleados, empleados actuales disgustados, competidores, entre otros. Para prever recomendaciones en base a las prioridades de la empresa para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de un evento desfavorable trayendo consigo la disminución de tiempo y esfuerzos requeridos para afrontar situaciones adversas en la organización.

OBJETIVOS.

Objetivo general.

Realizar la evaluación, detección de vulnerabilidades en el diseño e implementación de la infraestructura de la red, para la posterior realización de pruebas de penetración de caja blanca, identificando la mayor cantidad de vulnerabilidades para el desarrollo de posibles soluciones, estableciendo políticas de seguridad acorde a las necesidades de la empresa y mitigar los riesgos de afectación.

Objetivos Específicos.

- Identificar información relevante en la red de la Editorial Don Bosco, implementado herramientas tanto de software libre como propietario para de esta forma evaluar y categorizar cada vulnerabilidad.
- Cumplir con el código de principios éticos y de confidencialidad.
- Realizar un análisis de riesgos que permita priorizar necesidades de seguridad, simulando un ataque real.
- Identificar y proponer soluciones a problemas de seguridad en la red de manera clara y precisa que sirvan como referente para la creación de políticas de seguridad de acuerdo las necesidades de la empresa.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

Capítulo I

1. Fundamentos teóricos.

1.1. Seguridad Informática

Seguridad Informática es un conjunto de herramientas diseñadas para proteger los datos y frustrar a los atacantes informáticos comúnmente llamados *hackers*. El campo de la seguridad informática abarca tanto la seguridad de computadores así como también la de redes y engloba controles físicos, administrativos y automatizados.

Existen diversos tipos de amenazas a la seguridad informática por lo que es necesario conocer los elementos que comprende. La seguridad consta de cuatro elementos básicos:

- **Confidencialidad:** Este elemento expresa el principio de acceso a la información y recursos únicamente por los entes autorizados y mediante los métodos autorizados.
- **Autenticidad:** Este elemento permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser, generalmente esto se logra mediante la utilización de cuentas de usuario y contraseñas de acceso.
- **Integridad:** Se refiere a que la alteración de la información o recursos se realiza únicamente por los entes autorizados y mediante los métodos autorizados.
- **Disponibilidad:** Define el hecho de conservar los recursos y la información, disponibles siempre que sean necesarios.

Por lo tanto un atacante intenta explotar las vulnerabilidades de un sistema o de una red para encontrar debilidades de los cuatro elementos de seguridad. Es así que en la ejecución de un ataque de DoS (Denegación de servicio), se ataca la disponibilidad ya que dicho ataque tiene como objetivo utilizar recursos del sistema y enviar gran cantidad de mensajes para forzar el cierre del mismo, negando así servicios a los usuarios legítimos.

El robo de contraseñas u otros datos que viajan en texto claro a través de redes confiables, es un ataque a la confidencialidad, ya que permite que otra persona que no es el destinatario tenga acceso a los datos. Así también se puede obtener información

confidencial de los dispositivos de almacenamiento tales como discos, portátiles perteneciente a la empresa u organización.

Un ataque que se considera que afecta a la integridad de la información es el *Bit-flipping*, puesto que los datos son alterados en los bits del texto cifrado durante la transmisión, por lo tanto, los administradores del sistema no son capaces de verificar que los datos llegaron como el verdadero remitente pretendía que lleguen.

Por otra parte un ataque de suplantación de MAC ataca la autenticación, ya que permiten que un dispositivo no autorizado se conecte a una red inalámbrica.

Para explotar debilidades de los sistemas informáticos, los atacantes persisten y repiten trucos, sin embargo muchos *hackers* éticos, que forman parte del equipo de seguridad de la organización, detectan estas actividades para adicionar barreras de seguridad en el sistema, sin embargo es difícil lograr un equilibro entre la seguridad y la funcionalidad del sistema para todos los usuarios. Se ha tratado de representar dicho equilibrio con un triángulo como se muestra en la Figura 1-1 en cuyos vértices se encuentran: la seguridad, funcionalidad y facilidad de uso, y se interpreta de tal manera que si la seguridad aumenta, la funcionalidad y la facilidad de uso disminuyen. Ya que demasiadas barreras de seguridad impiden la funcionalidad del sistema y hace que sea difícil de usar para los usuarios. (Graves, 2012)[1]

Figura 1-1 Equilibrio entre funcionalidad, seguridad, y facilidad de uso de un sistema.

[1] Graves, K. (20 de Octubre de 2012). *CEH Certified Ethical Hacker Review Guide.* Obtenido de http://www.it-docs.net/ddata/863.pdf

1.2. Definición de *Penetration Test.*

Penetration test (Test de penetración), es el análisis de la seguridad de redes y sistemas en busca de vulnerabilidades y principalmente consiste en el intento de acceso a varios puntos de dichos sistemas mediante pruebas de penetración que simulan las que se producen durante un ataque malintencionado. Su principal objetivo es introducirse en las instalaciones de una organización y tratar de burlar toda la seguridad que esta pueda tener, para al final recopilar toda la información valiosa y confidencial. (Ramos J. V., 2011).[2]

Además de la definición anteriormente expuesta se dice que es un conjunto de metodologías y técnicas que permiten realizar una evaluación general de las debilidades de los sistemas informáticos ejecutando pruebas de penetración en un entorno empresarial, que no es más que un proceso por medio del cual se somete a un ataque controlado la seguridad de una empresa, buscando identificar las debilidades de sus sistema, antes que un atacante real lo haga, para lo cual es importante recalcar que la seguridad, implica todos aquellos mecanismos, generalmente de prevención y detección, destinados a proteger cualquier recurso de una organización, estos recursos, incluyen el personal, las instalaciones donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, en general hablamos de los activos de la información.

Hay que tomar en cuenta que los sistemas de transmisión de fibra óptica por lo general son más resistentes a la penetración que todos los sistemas electrónicos, puesto que los cables de fibra óptica son difíciles de tocar y el toque se detecta fácilmente porque el descenso de la potencia óptica recibida es muy notable, sobre todo cuando los fotodetectores están operando cerca de su umbral de sensibilidad. (Weik, 2001).[3]

1.3. Necesidad de realizar un *Penetration Test.*

La inseguridad de los sistemas se da de muchas maneras en nuestro entorno y en vista de que la información es el recurso más importante dentro de los sistemas, las empresas

[2] Ramos, J. V. (2011). *CICLO DE VIDA DE UNA PRUEBA DE PENETRACIÓN FÍSICA.* Guatemala: Universidad de San Carlos de Guatemala.

[3] Weik, M. (2001). Computer Science and Communications Dictionary. 978-0-7923-8425-0. doi:10.1007/1-4020-0613-6_13786

se encuentran cada vez más expuestas a ataques informáticos, por lo que las mismas buscan tener mayor seguridad en sus sistemas y como consecuencia una buena imagen y reputación corporativa, inclusive evita tener pérdidas económicas así como también de privacidad, integridad y confidencialidad. Mediante la realización de un *Penetration Test* se contempla esta problemática y consecuentemente se cuida la seguridad de la información ya que los especialistas en esta rama no solo tratan de identificar e informar las debilidades sino que también intentan explotarlas a fin de verificar los niveles de intrusión a los que se expone el sistema de información analizado y por ende se reducen las potenciales vulnerabilidades y su impacto, permitiendo el fortalecimiento de dicho ámbito tan importante como lo es el campo de la seguridad de los sistemas y de la red de las empresas, con el establecimiento de políticas de seguridad que responden a tres interrogantes: ¿Contra qué hay que defender a los sistemas? ¿Por qué hay que defenderlos? Y ¿Con qué podemos realizar dicha defensa? las respuestas están basadas en los resultados de las pruebas de penetración que son un paso previo a los análisis de riesgos para las empresas, enfocadas en comprobar y clasificar vulnerabilidades y el impacto que éstas tengan sobre la organización.

Por último un *Penetration Test* deja al descubierto las vulnerabilidades que pudieran ser vistas y explotadas por individuos no autorizados y ajenos a la información como: *crackers, hackers,* ladrones, ex-empleados, empleados actuales disgustados, competidores, entre otros. Para prever recomendaciones en base a las prioridades de la empresa y así mitigar y eliminar las vulnerabilidades con el fin de reducir el riesgo de ocurrencia de un evento desfavorable trayendo consigo la disminución de tiempo y esfuerzos requeridos para afrontar situaciones adversas en la organización.

Por todo lo dicho anteriormente en necesario realizar un *Penetration* test en las Empresas para:

- Identificar vulnerabilidades conocidas o desconocidas, antes que lo haga un atacante mal intencionado.
- Permitir evaluar cuál es el impacto real de una vulnerabilidad, mediante la realización de pruebas controladas.
- Poner a prueba las políticas existentes de seguridad.
- Estar preparado ante posibles ataques y construir planes de respuesta adecuados.

- Evaluar vulnerabilidades a través de la identificación de debilidades provocadas por una mala configuración de las aplicaciones.
- Analizar y categorizar las debilidades explotables, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad.
- Proveer recomendaciones en base a las prioridades de la organización para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de un evento desfavorable.

1.4. Tipos de *Penetration Test*.

Cuando se realiza un *Penetration Test* es importante considerar uno o más métodos de pruebas de intrusión sobre el sistema, los cuales simulan diferentes situaciones de la realidad. Cada tipo representa un atacante con diferentes niveles de conocimiento sobre la organización objetivo. Estos tipos son los siguientes:

1.4.1. *Penetration Test* de Caja Negra

En este tipo de *Penetration test* el consultor no recibe ningún tipo de información ni acceso autorizado al sistema o red que debe analizar, por lo que esto implica la realización de una evaluación de la seguridad sin conocimientos previos sobre la infraestructura de la red o sobre el sistema que es sometido a prueba. Simula el ataque malicioso desde fuera del perímetro de seguridad de la empresa. Es típicamente el más rápido, sin embargo existe una probabilidad menor de detectar vulnerabilidades ya que simula solamente el mejor de los casos para la organización, lo cual puede generar un falso nivel de confianza al suponer que el atacante no tiene información relevante de la empresa.

1.4.2. *Penetration Test* de Caja Blanca

El consultor tiene acceso a toda la información del sistema o red que debe analizar y la prueba de seguridad se realiza con total conocimiento de la infraestructura de la red, como si se tratase de un administrador de red, por lo que se tiene una probabilidad mayor de detectar vulnerabilidades. En este tipo de pruebas se simula el peor de los casos para la empresa lo cual ofrece un importante nivel de confianza. A diferencia del *Penetration Test* de caja negra este tipo de *test* tiene una duración mayor y se requiere que la persona que realiza las pruebas sea confiable para que pueda recibir todos los detalles de la organización.

1.4.3. Penetration Test de Caja Gris

Comprende cualquier caso intermedio a los anteriores es decir el consultor cuenta solo una parte de la información y realiza pruebas para evaluar la seguridad y otras pruebas internas. Esta tipo de *Penetration Test* examina el grado de acceso de las personas con información privilegiada dentro de la red.

1.5. Personal necesario para un *Penetration Test.*

El equipo que llevará a cabo el *Penetration Test* estará a cargo de diferentes roles y responsabilidades, es importante que el equipo cuente como mínimo con una persona para cada cargo o perfil, recalcando que una misma persona no podrá desempeñar dos cargos a la vez; requiriendo un Gerente de Proyecto y un especialista para las pruebas de vulnerabilidad. A continuación se indican los cargos necesarios para la realización de una prueba de penetración:

- **Operadores.**- Son el personal que participan directamente de las pruebas y no en un papel de apoyo, independientemente de sus especialidades o funciones.
- **Líder del Equipo.-** Tiene la responsabilidad final de entregar la asignación de funciones, administrar el proyecto y a los miembros del equipo, es importante recalcar que este puesto debería ser cíclico puesto que cada especialista puede aportar con una perspectiva distinta, esta rotación debe ser asignada por el coordinador.
- **Coordinador.-** Dirige y asiste los miembros del equipo, asegurándose de que cada uno cumpla con sus roles.
- **Ingeniero Social.-** Debe tener habilidades naturales para el engaño y la manipulación humana, es el encargado de atacar al eslabón más débil de la cadena, es decir el usuario final.
- **Especialista en intrusión de computadoras.-** Este es el *Hacker* ético, se encarga del acceso a las computadoras y redes dentro del *Penetration Test*, siendo su principal objetivo obtener información valiosa y la escala de privilegios del sistema.
- **Especialista en intrusión web.-** Este es el encargado de las inspecciones a páginas web, el cual busca posibles errores o vulnerabilidades mediante el uso

de herramientas automáticas y manuales, que puedan comprometer la seguridad de la empresa.

- **Especialista en redes WLAN. –** Es la persona experta en redes WLAN seguras, el cual dará a conocer el alcance real de la red inalámbrica, fallos en la configuración y vulnerabilidades existentes.

1.6. ¿Quién realiza las pruebas de Penetración?

Las pruebas de penetración pueden ser realizadas por un recurso interno calificado o un tercero calificado, es decir, debe ser experto en sistemas informáticos y estar muy familiarizado con la programación informática, la creación de redes y sistemas operativos. Otro requisito es el conocimiento profundo orientado a plataformas como Windows y Unix. Además debe poseer cualidades como la paciencia, la persistencia y la perseverancia debido a la cantidad de tiempo y el nivel de concentración necesario que requieren para realizar la mayoría de los ataques, comprometer los sistemas y obtener sus resultados.

Si se están utilizando los recursos internos para llevar a cabo pruebas de penetración, esos recursos deben ser *Pentesters* experimentados. Los individuos que realizan pruebas de penetración deben estar separados del ambiente que está siendo testeado. Por ejemplo, el administrador de la seguridad del servidor no debe realizar la prueba de penetración al firewall. (Council, 2008).[4]

La mayoría de encargados de realizar las pruebas de penetración son los *hackers* éticos que con su conocimiento de las áreas de seguridad o relacionadas a ella, están motivados en determinar lo que un atacante malicioso puede ver en el sistema o en la red, hay que recalcar que un *hacker* ético no necesariamente tienen un fuerte control sobre las contramedidas que pueden prevenir los ataques.

1.7. Definición *Ethical Hacking.*

Es explotar las vulnerabilidades existentes en el sistema valiéndose de un *Test* de penetración, que verifica y evalúa la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc.

[4] Council, P. S. (Marzo de 2008). Obtenido de https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/doc/information_supplement_11.3.pdf

con la intención de ganar acceso y mostrar que un sistema es vulnerable, obteniendo información de gran ayuda a las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados.

Siendo el objetivo de un *Ethical hacking* reproducir ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que "Para atrapar a un intruso, primero debes pensar como intruso" (Plata, 2010).[5]

1.8. Clasificación de los *Hackers*.

Antes de iniciar con la clasificación de los *hackers* vamos a definir este término ya que la mayor parte del tiempo se usa la palabra *hacker* de forma errónea debido a que se desconoce el verdadero significado de la misma y la mayoría de personas piensan que los hackers tienen habilidades y conocimientos en computadoras, que pueden romper una contraseña, que saben de programación, en fin, y que eso les permite acceder a información confidencial dentro de cualquier sistema. Pero no todos los *hackers* tienen malas intenciones, algunos se encargan de la seguridad de los sistemas de las organizaciones y otros contribuyen a la seguridad notificando a los fabricantes de software si encuentran algo vulnerable, éstos se conocen como *hackers* éticos, es decir son profesionales de seguridad que realizan pruebas de penetración a una red o sistema en busca de vulnerabilidades utilizando sus conocimientos, habilidades y conjunto de herramientas de *hacking* con fines defensivos y preventivos.

Sin embargo, el término *cracker* describe un *hacker* que utiliza sus habilidades y conjunto de herramientas de *hacking* para fines destructivos u ofensivos, éstos tratan de adentrarse en los sistemas informáticos para causar daño, investigan formas de bloquear protecciones para la propagación de *malware* o para dejar fuera de servicio el sistema o la red (DoS). A veces son pagados para dañar reputaciones corporativas o robar información de tarjetas de crédito, mientras que al mismo tiempo frenan los procesos de negocio comprometiendo la integridad de la organización.

Por lo tanto el *cracker* se distingue del *hacker* ético por sus valores morales, sociales y políticos.

[5] Plata, A. R. (2010). *Ethical Hacking*. Mexico: UNAM-CERT Equipo de Respuesta a Incidentes UNAM.

Por lo expuesto anteriormente los *hackers* pueden ser divididos en tres grupos: *hacker* de sombrero blanco, sombrero negro y sombrero gris.

1.8.1. *Hacker* de Sombrero Blanco

Este término se refiere a los *hackers* éticos quienes utilizan sus habilidades de *hacking* con objetivos defensivos. Por lo general, los *hackers* de sombrero blanco son expertos de seguridad informática que se especializan en realizar pruebas de penetración para localizar debilidades e implementar contramedidas a fin de asegurar los sistemas de información y las redes de datos de las empresas. Cuando estos *hackers* encuentran una vulnerabilidad inmediatamente comunican esta situación al administrador con el propósito de que sea resuelto lo más pronto posible. Algunos son consultores de seguridad, trabajan para alguna compañía en el área de seguridad informática protegiendo los sistemas de los *hackers* de sombrero negro.

1.8.2. *Hacker* de Sombrero Negro

Comúnmente se refiere a los *hackers* maliciosos o *crackers* quienes principalmente motivados por el dinero utilizan sus habilidades con fines ilegales, antimorales o propósitos maliciosos. A diferencia de un hacker de sombrero blanco, el hacker de sombrero negro se aprovecha de las vulnerabilidades con el objetivo de destruir o robar información. Continuamente buscan la forma de entrar o romper la seguridad de los sistemas de las máquinas remotas con intenciones maliciosas mediante alguna vulnerabilidad o error humano. Habiendo ganado acceso no autorizado, los *hackers* de sombrero negro destruyen datos útiles, niegan servicios a usuarios legítimos, causando así muchos problemas.

1.8.3. *Hacker* de Sombrero Gris

Son los que juegan a ser buenos y malos, en otras palabras, tienen ética ambigua es decir pueden trabajar de manera ofensiva o defensiva según la situación ya que tienen los conocimientos de un *hacker* de sombrero negro y los utilizan para penetrar en sistemas y buscar vulnerabilidades para luego ofrecer sus servicios para repararlos bajo contrato. Esta es la línea que divide al *hacker* del *cracker*. Estos *hacker*s advierten y ofrecen la posibilidad de corregir la vulnerabilidad a sus víctimas.

1.9. Tipos de *Ethical Hacking.*

Los hackers éticos pueden utilizar una variedad de métodos para violar la seguridad de una empresa durante un *Penetration Test*. Los métodos más comunes son:

Red remota: representa un *hacker* ético elaborando un ataque a través de Internet, es decir, intenta romper o encontrar una vulnerabilidad desde afuera de las defensas de la red, como vulnerabilidades en el firewall, el proxy o en el router.

Red local: representa a alguien con acceso físico ganando acceso adicional no autorizado utilizando la red local. Para realizar este tipo de ataque el *hacker* ético debe ganar acceso directo a la red local.

Equipo robado: supone el robo de una computadora portátil que es propiedad de un empleado. Información como nombres de usuario, contraseñas, configuraciones de seguridad y tipos de cifrado pueden ser obtenidos al robar una computadora portátil.

Ingeniería Social: intenta comprobar la integridad de los empleados de la organización utilizando el teléfono o a través de una comunicación directa para obtener información que pueda ser útil para cometer un ataque. Los ataques de Ingeniería Social pueden ser utilizados para la obtención de nombres de usuario, contraseñas y otras medidas de seguridad de la empresa.

Entrada física: Es el intento de comprometer las instalaciones físicamente. Una hacker ético que logra el acceso físico a la organización puede plantar virus, troyanos, *rootkits o keyloggers* por hardware directamente sobre los sistemas de la red. (Graves, 2012)[6]

1.10. Procedimientos legales.

1.10.1. Autorización de seguridad.

Cuando se empieza con las pruebas de penetración, los involucrados en el equipo de penetración necesitan tener autorizaciones de seguridad. Las autorizaciones de seguridad dependen de la naturaleza del trabajo que se realizará y la sensibilidad del objetivo. Todas las autorizaciones deberán estar firmadas y debidamente selladas. (Ver anexo 1).

[6] Graves, K. (20 de Octubre de 2012). *CEH Certified Ethical Hacker Review Guide.* Obtenido de http://www.it-docs.net/ddata/863.pdf

Como se había mencionado anteriormente los tipos de *Penetration Test* dependerá de los permisos que se tenga en cuanto a la seguridad por parte de la empresa, si recordamos estos pueden ser:

- **Caja Negra.** El *hacker* ético no cuenta con información del sistema ni de la red que debe analizar.
- **Caja Blanca.** El *hacker* ético tiene acceso a toda la información, incluyendo datos internos, código fuente, tanto del sistema como de la red a analizar.
- **Caja Gris**. Se refiere a un caso intermedio de los dos anteriores, es decir que el *hacker* ético cuenta con un mapa de la red y los segmentos de direcciones relevantes, pero no el código fuente de los aplicativos disponibles, es decir que poseerá información parcial acerca del sistema y de la red.

Debido a la inmediata necesidad de la empresa por proteger sus activos de la información, y de establecer políticas de seguridad acorde a sus necesidades se ha visto necesario realizar un *Penetration Test* tipo caja blanca, el cual nos proporcionará las siguientes ventajas:

- Se tiene mayores probabilidades de detectar vulnerabilidades.
- Simula el peor de los casos para la organización lo cual ofrece un nivel importante de confianza.
- Suele incluir un foco importante en los aplicativos donde usualmente se presentan más problemas. (Guirado, CISA, & CGEIT, 2009)[7]

1.10.2. Investigación de antecedentes.

Antes de permitir la realización de un *Penetration Test*, es importante asegurarse que las personas involucradas en este trabajo sean fiables y que no tengan problemas con la justicia, puesto que podría ser contraproducente para la seguridad de la empresa. Debido a que muchos de los *hackers* éticos están tratando de ingresar al ámbito de la seguridad informática como consultores. Por lo tanto las empresas no tendrían por qué ver favorablemente a alguien que aparece en la puerta con datos confidenciales y

[7] Guirado, A. R., CISA, & CGEIT. (2009). *Penetration Testing - Conceptos generales y situación actual.* ISACA.

ofertas para solucionar las vulnerabilidades de seguridad por un preciso determinado, sino que tendrá que empezar a realizar cierta investigación de antecedentes de los posibles consultores de la seguridad de su empresa.

1.10.3. Legislación para la realización de un *Penetración Test*.

Previo a la realización de un *Penetration Test*, el hacker ético debe estar al tanto de las penalidades que sufre el *hacking* no autorizado en un sistema. Las actividades relacionadas con el *hacking* ético de una red o sistema, deben realizarse mediante un documento legal firmado que le da permiso expreso al *hacker* ético para llevar a cabo las pruebas de penetración en la empresa que es objeto de análisis. Los *hackers* éticos necesitan ser prudentes con sus habilidades de *hacking* y reconocer las consecuencias que implica el mal uso de esos conocimientos ya que si un éste viola las leyes puede ser enjuiciado y sancionado con una pena según la gravedad de la misma.

Ecuador cuenta con La ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, más conocida como Ley 67, publicada en el R.O. / Sup.557 del 17 de Abril del 2002, la misma que tiene un avance muy importante en el sentido de incluir penas que castiguen los ilícitos informáticos, y junto al Código Penal integran normas creadas para la Sociedad de la Información.

Esta ley legisla: conductas ilícitas acceso ilegal a sistemas informáticos, interceptación ilegal de las comunicaciones, daños en los sistemas informáticos, fraude electrónico, fraude en las telecomunicaciones entre otros:

- Art.57 LCEFEMD: Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

- Art.58 LCEFEMD, Conc. Art.202.1 CP: Contra la Información Protegida.- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

- Art.58 últ.inc LCEFEMD, Conc. Art.202.2 CP: Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

- Art.59 LCEFEMD, Conc. Art.262 CP: Destrucción Maliciosa de Documentos.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo.

- Art.60 LCEFEMD, Conc. Art.353.1 CP: Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1. Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2. Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3. Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.

- Art.61 LCEFEMD, Conc. Art.415.1 CP: Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

- Art.61 últ.inc LCEFEMD, Conc. Art.415.1 CP: Destrucción de instalaciones para transmisión de datos.- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.
- Art.62 LCEFEMD, Conc. Art.553.1 CP: Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

- Art.62 últ.inc LCEFEMD, Conc. Art.553.2 CP: Pena.- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento o descifrado de claves secretas o encriptadas;

3. Utilización de tarjetas magnéticas o perforadas;

4. Utilización de controles o instrumentos de apertura a distancia; y,

5. Violación de seguridades electrónicas, informáticas u otras semejantes.

- Art.63 LCEFEMD, Conc. Art.563 inc.2 CP: Estafa.-Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.

- Art.64 LCEFEMD, Conc. Art.606.20 CP: Violación Derecho a la Intimidad.- Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (Espinoza, 2013)[8]

A continuación en la tabla 1-1 se presenta un resumen de los delitos informáticos y sus respectivas sancione de acuerdo a la ley Ecuatoriana.

Tabla 1-1 Delitos Informáticos Contemplados en la ley Ecuatoriana de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Fuente: Reyna, R. Z. (s.f.). Obtenido de http://www.cec.espol.edu.ec/blog/rzambrano/files/2012/08/DELITOS-INFORM%C3%81TICOS-CONTEMPLADOS-EN-LA-LEY-ECUATORIANA.pdf

Art.58 LCEFEMD, Conc. Art.202.1 CP: Contra la Información Protegida	**SANCIÓN CARCELARIA**	**MULTA**
1. Violación de claves o sistemas.	6 meses a 1 año	US$ 500 a US$1.000

[8] Espinoza, A. C. (6 de Marzo de 2013). *El Observatorio.* Obtenido de http://oiprodat.com/2013/03/06/delitos-informaticos-y-comercio-electronico-ecuador/

2. Información obtenida sobre la seguridad nacional, secretos comerciales o industriales.	3 años	US$1.000 a US$1.500
3. Divulgación o utilización fraudulenta de los rubros anteriores.	3 a 6 años	US$2.000 a US$ 10.000
4. Divulgación o utilización por funcionarios a cargo de dicha información.	6 a 9 años	US$2.000 a US$ 10.000
5. Obtención y uso no autorizado de datos personales para cederla o utilizarla.	2 meses a dos años	US$ 1.000 a US$ 2.000
Art.59 LCEFEMD, Conc. Art.262 CP: Destrucción Maliciosa de Documentos Por Funcionarios de Servicio Público.	3 a 6 años	
Art.60 LCEFEMD, Conc. Art.353.1 CP: Falsificación electrónica con ánimo de lucro con perjuicio a terceros y con intensión de :	Serán juzgados a 6 años	
1. Alterar un mensaje de datos		
2. Simulación de mensaje		
3. Suposición de intervención en actos, declaraciones, etc.		
Art.61 LCEFEMD, Conc. Art.415.1 CP: Daños informáticos		
1. Daño doloso se información contenida en un sistema	6 meses a 3 años	US$ 60,oo a US$ 150,oo
2. Realizado por funcionario público o vinculado con la defensa nacional	3 a 6 años	US$ 200 a US$600
3. Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura para la transmisión.	8 meses a 4 años	US$ 200 a US$600
Art.62 LCEFEMD, Conc. Art.553.1 CP: Apropiación ilícita		
1. Uso fraudulento para apropiación de un bien ajeno, etc.	6 meses a 5 años	US$ 500 a US$ 1.000
2. Uso fraudulento mediante la utilización de: inutilización de sistemas de alarma, descubrimiento descifrado de claves secretas, tarjetas magnéticas o carding, controles o instrumentos de apertura a distancia y violación de seguridades electrónicas.	1 a 5 años	US$ 1.000 a US$ 2.000
Art.63 LCEFEMD, Conc. Art.563 inc.2 CP: Estafa.-	1 a 5 años	US$500 a US$ 1.000
Art.64 LCEFEMD, Conc. Art.606.20 CP: Violación Derecho a la Intimidad	2 a 4 días	

1.11. ¿Cómo contratar un *Penetration Test*?

La realización de un *Penetration Test* se encuentra de moda en todo el mundo, hoy existen cientos de empresas o consultores en *Penetration Test* que ofrecen sus

servicios con ética, profesionalidad, metodologías, etc. Pero del lado de la empresa que solicita el servicio para auditar sus sistemas y redes, es decir, la empresa que necesita establecer con certeza que sus sistemas están debidamente protegidos, existen varios aspectos que se deben tener en cuenta una vez seleccionado el consultor para no caer en errores que pudieran llevar a una mala experiencia en cuanto al análisis de la seguridad de sus sistemas.

Por lo general, las empresas u organizaciones solicitantes de servicios de *Penetration Test* deben tener claro los puntos que se deben tratar con el consultor para que la evaluación sea exitosa y que en el proceso no exista fuga de información, malos entendidos o incumplimiento de alguna de las partes.

A continuación se describe lo que la empresa solicitante de un servicio de *Penetration Test* debe conocer.

a) **Como primer punto se selecciona al proveedor del *Penetration Test***

b) Firma de Acuerdo de confidencialidad

Este punto no se debe omitir ya que está relacionado con asuntos legales los cuales deben ser consultados con el abogado de la empresa. Hay que tener en cuenta que la Empresa confiará al consultor datos muy sensibles como usuarios y contraseñas, accesos a entornos de pruebas, así como también, una vez concluido el trabajo, el consultor tendrá en su poder, datos detallados de como explotar posibles vulnerabilidades encontradas, como obtener datos sensibles, como escalar privilegios, etc.

Un Acuerdo de Confidencialidad debe abarcar estos aspectos y solicitar al consultor su absoluta reserva para con los datos otorgados, también debe quedar establecido el futuro de esa información una vez concluido el período de pruebas, que puede ser: almacenamiento seguro, destrucción completa, entre otras.

c) Especificar responsables

Posiblemente tanto la empresa solicitante como la empresa consultora contarán con un número de personas relacionadas con el área de IT. Sin embargo, no es recomendable tratar temas relacionados con el trabajo de *Penetration Test* con más de dos personas de cada parte, igualmente, se debe definir una persona responsable por cada empresa

para una comunicación ordenada y para ser referentes en caso de incidencias las mismas que serán ubicables generalmente mediante teléfono durante el proceso.

d) Definir el alcance del *Penetration Test*

En este punto se establece correctamente lo que se quiere evaluar y hasta qué punto se le permitirá al consultor "explotar" las posibles vulnerabilidades encontradas sin causar un daño a servicios activos, por lo que debe ser acordado entre las dos partes.

En varias ocasiones se suele solicitar servicios de *Penetration Test* sobre sistemas que están en un entorno de pruebas separado de los sistemas en producción, en cuyo caso el cliente no se preocupa por daños o interrupciones, pero también se solicitan en entornos críticos de producción donde una denegación de servicio (D.o.S.) o un ocasional cambio en archivos de configuración pueden incurrir en posibles pérdidas en producción y ganancias.

e) Especificar claramente el entorno a testear

Luego de haber definido el alcance, se tiene que transmitir al consultor de manera clara y comprobada para evitar confusiones. Es muy común que existan equivocaciones tan solo en un número en un rango IP o una letra en una URL, y al equivocar el objetivo, existe la posibilidad de problemas ya que se estarían testeando sistemas que podrían no pertenecer a la propia empresa cliente, generando problemas en la credibilidad del trabajo, pérdida de tiempo y cuestiones de índole legal.

f) Precisar duración del trabajo

El proceso de *Penetration Test* puede generar algunos inconvenientes en los sistemas objetivos, desde caída del rendimiento hasta una involuntaria denegación de servicio. Es por eso que hay que tener en cuenta que tan crítico es el entorno para coordinar con el consultor las ventanas horarias la misma que será respetada, para el proceso de evaluación, evitando los inconvenientes mencionados en horarios pico.

g) Identificación de tráfico

El consultor es el responsable de explicar desde que rangos de IP realizará el Test en caso de que se realice externamente, de manera que el cliente puede identificar claramente de donde provienen los paquetes IP que intentan la manipulación de

aplicaciones, *crawling*, escáneres de puertos , etc. Este punto tiene dos finalidades fundamentales:

- El cliente guarda en los *logs* toda la actividad realizada por el consultor, teniendo así una prueba concreta en caso que éste realice una actividad no autorizada.
- Autorizar los rangos IP declarados por el consultor en posibles sistemas IDS y firewalls que la empresa cliente pueda poseer.

h) Método de intercambio de información

Todo intercambio de datos entre la empresa solicitante y la empresa consultora, tanto la información sensible, como credenciales de acceso de aplicaciones, direcciones IP con sistemas en desarrollo y poco protegidos, etc. Así como también el informe o reporte final, el cual contiene información detallada de posibles vulnerabilidades, pruebas de concepto y pasos para la explotación, debe ser manipulado con especial cuidado entre las personas responsables definidas y mediante canales de comunicación seguros.

Por ejemplo, es altamente recomendable cruzar llaves públicas PGP entre las partes para mantener una comunicación vía email de manera encriptada evitando así que los datos sean legibles por cualquier intermediario. Una opción más avanzada puede ser descarga de archivos vía portal seguro con client-cert SSL, Hardware Tokens, etc o simplemente transferencia de archivos por canales encriptados como SFTP o SCP. (Caire)[9]

1.12. Asignación de responsabilidades en el *Penetration Test.*

Partiendo de los cargos indicados anteriormente, se debe asegurar una correcta asignación de responsabilidades, a continuación en la tabla 1-2 se presenta la asignación de tareas y responsabilidades a cargo de nuestro equipo de trabajo.

[9] Caire, R. (s.f.). *Segurida y Ética*. Obtenido de http://seguridadetica.wordpress.com/2012/05/17/7-consejos-utiles-al-contratar-un-servicio-de-pen-testing/

Tabla 1-2 Asignación de tareas y responsabilidades en el *Penetration Test.*

CARGO	**PERSONA RESPONSABLE**
Operadores	Cristina M. Jaramillo. Juan Carlos Riofrío.
Líeder del Equipo	Cristina M. Jaramillo. Juan Carlos Riofrío.
Coordinador	Ing. Pablo Gallegos.
Ingeniero Social	Juan Carlos Riofrío.
Especialista en intrusión de computadoras	Cristina M. Jaramillo.
Especialista en intrusión web.	Juan Carlos Riofrío.
Especialista en redes WLAN	Cristina M. Jaramillo.

1.13. Etapas que involucran un *Penetration test*

Tenemos seis etapas principales y nascerías para el desarrollo de un Penetration Test que se citan a continuación y que están reflejadas en este trabajo de investigación.

1.13.1. Definición del alcance.

Se trata de delimitar el test de penetración y establecer con la institución reglas y políticas claras sobra hasta que nivel se podrá llegar con las respectivas pruebas.

1.13.1.1. Definicion del Alcance del Alcance del Penetratión Test

En el desarrollo de este documento se contempla la realización de un Penetration test de caja blanca a todos los sistemas e infraestructura de red de la Editorial Don Bosco, en cuya ejecución se realizaran pruebas de penetración que simulan las que se producen durante un ataque, dichas pruebas se plasmaran por medio de la utilización de herramientas de software libre y propietario, teniendo acceso físico a las instalaciones de la empresa e interactuando con el personal en un entorno controlado, con el fin de garantizar que la información sea fidedigna y los resultados sean congruentes y certeros.

Sin embargo es limitada la posibilidad de probar toda la gama de técnicas y mecanismos que los hackers pudieran emplear para vulnerar un sistema informático. A pesar de ello se señalara y demostrara indudablemente la mayor cantidad de vulnerabilidades que posean los sistemas para poder analizarlas y establecer políticas de seguridad y de esta manera preservar la confidencialidad integridad y disponibilidad de los sistemas de dicha Entidad.

EL punto de partida para el fortalecimiento de la seguridad será conocer la situación real de los sistemas de la empresa lo cual nos permitirá verificar en qué grado de cumplimiento se encuentra respecto a la legislación, normativas y estándares internacionales; así como también evaluar el riesgo de fuga de información.

Luego se determinara las amenazas, agentes de amenaza, vulnerabilidades así como demostrar los riegos funcionales a las que está expuesto el sistema en su totalidad.

Posteriormente con un análisis de dichas falencias podremos establecer un informe técnico y ejecutivo para los Administrativos de la Empresa, el mismo que contemplara a grandes rasgos una lista detallada de las vulnerabilidades encontradas y verificables. Así como también se suministrara una lista de recomendaciones para que sean aplicadas por los responsables de seguridad en la empresa que entenderán y apreciaran los riesgos potenciales sobre el negocio.

Con esto la Empresa tendrá un panorama claro sobre las vulnerabilidades halladas en los sistemas de información lo cual es imprescindible al momento de aplicar medidas correctivas.

1.13.2. Definición de metodologías y buenas prácticas a utilizar.

Un Test de Penetración, es un procedimiento metodológico y consecuente en el que se simula un ataque real a una red o sistema, con el propósito de descubrir y subsanar sus problemas de seguridad, a continuación veremos la documentación más recomendada para aprender a realizar correctamente un test de penetración.

1.13.2.1. OSSTMM (Open Source Security Testing Methodology Manual)

Es una metodología aplicable a las pruebas de seguridad que combina estudio y años de experiencia. La metodología en conjunto representa un estándar de referencia en el área de testeo de seguridad.

Es un estándar profesional para el testeo de seguridad en cualquier entorno desde el exterior al interior. Como cualquier estándar profesional, incluye los lineamientos de acción, la ética del pentester profesional, la legislación sobre testeo de seguridad y un conjunto integral de tests.

El objetivo de este manual es crear un método aceptado para ejecutar un test de seguridad minucioso y completo.

No muestra ninguna recomendación a seguir la metodología como si se tratase de un diagrama de flujo. Sin embargo, se presentan una serie de pasos que deben ser vistos varias veces durante la realización de un test exhaustivo. La gráfica de metodología brindada es la manera óptima de llevar a cabo esto, convenientemente de a dos testeadores, aunque cualquier número de testeadores tienen la posibilidad de realizar la metodología en tándem. Lo más importante en esta metodología es que los diferentes tests son evaluados y ejecutados donde sean aplicables, hasta arribar a los resultados esperados dentro de un período de tiempo determinado. Solo así el testeador habrá ejecutado el test en conformidad con el modelo OSSTMM, y por ello, el informe podrá ser considerado mínimamente exhaustivo.

El OSSTMM debe cumplir con las reglas establecidas en las diferentes leyes tanto Internacionales, Federales, Locales, Industriales y Políticas establecidas en la organización.

Cada una de las acciones debe proveer no violar alguna ley, reglamento o política y cada una de las actividades deber ser coordinadas con la organización que requiere la implementación de este tipo de pruebas a su seguridad.

También contempla el cumplimiento de normas y mejores prácticas como las establecidas en el NIST, ISO 27001-27002 e ITIL entre otras. Lo que hace de este manual uno de los más completos en cuanto a la aplicación de pruebas a la seguridad de la información de las organizaciones.

El propósito es brindar una metodología científica al inspeccionar la seguridad en una organización, así como también provee guías para el auditor destinadas a la certificación de dicha organización.

El documento provee una serie de descripciones específicas para el desarrollo de las pruebas de seguridad sobre todos los canales incluyendo aspectos físico, humanos, telecomunicaciones, medios inalámbricos, redes de datos y cualquier otra descripción derivada de una métrica real.

1.13.2.2. OWASP (Open Web Application Security Project)

El Proyecto de seguridad de aplicaciones Web abierta (OWASP) es una comunidad conformada por voluntarios, permite a las organizaciones desarrollar, comprar y mantener aplicaciones que puedan ser confiables. Todas las herramientas OWASP, documentos, foros y capítulos son gratuitas y abiertas a cualquier persona interesada en la mejora de la seguridad de aplicaciones. Aboga por resolver la seguridad de las aplicaciones.

OWASP es un nuevo tipo de organización sin fines de lucro que brinda información imparcial, práctica y rentable sobre seguridad en aplicaciones. Al igual que muchos proyectos de software de código abierto, OWASP produce muchos tipos de materiales en una manera abierta y colaborativa.

OWASP, en particular, se encuentra enfocado en ayudar a las personas a comprender: ¿Qué?, ¿Por qué?, ¿Cuándo?, ¿Dónde? y ¿cómo? Testear sus aplicaciones Web y no sólo proporciona una lista de control simple o prescripción de cuestiones que deben abordarse. El resultado de este proyecto es un marco de pruebas completa, de la que otros puedan construir sus propios programas de pruebas o calificar los procesos de otras personas. La guía de pruebas describe en detalles tanto en el marco de pruebas general y las técnicas necesarias para aplicar el marco en la práctica.

Muchos expertos de la industria y los responsables de la seguridad del software en algunas de las empresas más grandes del mundo están validando el marco de pruebas. Este marco ayuda a las organizaciones a probar sus aplicaciones web con el fin de construir software fiable y seguro, en lugar de simplemente poner de relieve las áreas de debilidad, aunque este último es ciertamente un subproducto de muchos de los guías y listas de control de OWASP.

La guía cubre los siguientes puntos:

- El alcance de las pruebas.
- Los principios de las pruebas con éxito.
- Las técnicas de testeo.
- El Marco de pruebas OWASP y explica sus técnicas y tareas en relación con las diversas fases del ciclo de vida de desarrollo de software.
- Cómo probar las vulnerabilidades específicas (por ejemplo, inyección SQL) por la inspección de código y pruebas de penetración.

En muchas ocasiones, una metodología requiere ser acompañada de documentos que sustenten en pasos prácticos y concretos, parte del contenido de la misma, haciendo de estos una referencia obligada a la hora de realizar un testeo de seguridad.

1.13.2.3. Buenas Prácticas

A continuación se darán a conocer un conjunto de buenas prácticas que se deberán tomar en cuenta a la hora de desarrollar un Penetration Test en empresas.

El pentester deberá cumplir las siguientes premisas de seguridad:

- Determinar en conjunto con el encargado del contrato, cómo se considerará el nivel de riesgo estimado que puede ser: Alto, Medio, Bajo lo cual se utilizará como parámetro para la calificación de las vulnerabilidades.
- No se debe ejecutar simultáneamente más de una herramienta por objetivo de prueba, para minimizar la explotación accidental de vulnerabilidades que generen errores, fallas en los servidores o dispositivos de conexión.
- Una misma prueba se puede ejecutar sobre los Servidores más de una vez pero con distinta herramienta, para propósitos de Comparación y optimización de resultados.
- Registro y documentación de la evidencia y vulnerabilidades identificadas por objetivo de prueba.
- Las pruebas de vulnerabilidad deben ser realizadas con absoluto cuidado para no tener caídas de servidores, ciclos inactivos y otros problemas causados de manera inadvertida por las actividades de escaneo. Para lo cual el pentester

deberá previamente determinar que se requiere para ejecutar la prueba en un ambiente controlado.

- Por ningún motivo se autoriza al pentester a divulgar información que se conozca de la empresa en desarrollo de la ejecución del contrato.
- Garantizar el cumplimiento de la política de Gestión Integrado de la empresa, sus procedimientos, instructivos y manuales.
- El pentester deberá estar directamente vinculado con la ejecución del contrato, de acuerdo con el plan de cargas y trabajo, durante la realización de cada escenario de las pruebas.
- El equipo de trabajo debe contar como mínimo con una persona para cada cargo o perfil del Equipo de Trabajo; una misma persona no podrá desempeñar dos cargos a la vez. Sólo se requiere un Gerente de Proyecto y un especialista para las pruebas de vulnerabilidad.

Serán responsabilidades del Gerente de Proyecto, las siguientes:

- Garantizar el correcto desarrollo de todas las actividades de inicio, ejecución y cierre del proceso de contrato en nombre de la empresa.
- Cumplimiento de principios éticos y de confidencialidad.
- Garantizar la ejecución del plan de cargas y de trabajo del proyecto y mantenerlo actualizado.
- Documentar el plan de ejecución del contrato, de cómo se planeó y como se ejecutó, al igual que las actividades adicionales o modificaciones que fueron necesarias para el logro del desarrollo del contrato.
- Velar por el cumplimiento de la prestación de los servicios contratados con las especificaciones y niveles establecidos en la documentación del contrato.
- Mantener informado al supervisor del contrato de la empresa sobre el estado y avance del proyecto.
- Definir los mecanismos de monitoreo y seguimiento al desarrollo del proyecto.
- Velar por la administración de la calidad y de los riesgos durante la ejecución del proyecto.
- Velar por el cumplimiento de los resultados del proyecto y formular las acciones que permitan lograr el impacto esperado y la continuidad de los servicios.
- Entregar al supervisor del contrato cuando se requiera los entregables que se pacten en desarrollo del proyecto.

- Coordinar el trabajo de cada uno de los miembros del equipo de trabajo que este asignado al proyecto, las actividades que sean necesarias para el logro de los objetivos del proyecto.
- Y las demás que sean necesarias para la cabal y correcta ejecución del objeto del contrato.

Serán responsabilidades del Especialista de las Pruebas de Vulnerabilidad, las siguientes:

- Velar por el cumplimiento de la prestación de los servicios contratados con las especificaciones y niveles establecidos.
- Coordinar todas las actividades y ejecución de la prestación de los servicios con el gerente del equipo de trabajo.
- Mantener informado al supervisor del contrato de la empresa sobre el estado y avance del proyecto.
- Velar por el cumplimiento de los resultados del proyecto y formular las acciones que permitan lograr las metas esperadas.
- Velar por la continuidad de la prestación del servicio de la empresa, cumpliendo las premisas de seguridad.
- Establecer el plan de pruebas de Vulnerabilidad y de intrusión para verificación y aprobación previa por parte de la empresa, para que las mismas sean ejecutadas de manera controlada.
- Entregar toda la información, que sea requerida como parte de los entregables en la forma y contenido solicitado.
- Las actividades tendrán como objetivo la obtención de pruebas del tipo "screen prints" o captura de datos representativos.
- En caso de aparición de algún resultado destructivo o de interrupción o se considere riesgoso y atente contra las premisas de seguridad, la prueba deberá ser interrumpida en forma inmediata, informando la novedad al Gerente del equipo de trabajo y a la empresa para la ejecución de las tareas de recuperación requeridas.

- Las actividades serán reanudadas una vez recibida la indicación formal, tomando las medidas preventivas correspondientes.
- No se realizarán pruebas intrusivas a las vulnerabilidades detectadas, sin evaluar los riesgos correspondientes y previa planeación de la actividad con la empresa.
- Y las demás que sean necesarias para la cabal y correcta ejecución del objeto del contrato. (Cornejo, 2013)[10]

1.13.3. Aplicación de la metodología.

La aplicación de la metodología involucra trabajo de campo el cual requiere de 4 faces importantes.

- **Descubrimiento.** Se trata de entender los riesgos del negocio asociados al uso de activos informáticos para lo cual se realizan investigaciones tratando de recolectar información pública sobre la plataforma tecnológica del cliente, utilizando para ello técnicas pasivas de relevamiento de información.
- **Exploración.** En esta etapa se aplican técnicas no intrusivas para identificar todos los potenciales blancos, que incluye el análisis de protocolos, levamiento de plataforma y barreras de protección, *scanning* telefónico, *scanning* de puertos TCP y UDP, detección remota de servicios y sistemas operativos, análisis de banners y búsqueda de aplicaciones web.
- **Evaluación.** Se basa en el análisis de todos los datos encontrados para la detección y determinación de vulnerabilidades de seguridad informática que afectan a los sistemas evaluados, realizando evaluaciones de seguridad en todos los posibles niveles mediante la ejecución de herramientas de *scanning* de vulnerabilidades, búsquedas en manuales de vulnerabilidades, enumeración de usuarios y datos de configuración.
- **Intrusión.** Se centra principalmente en realizar pruebas de seguridad controladas a las vulnerabilidades propias de los sistemas identificados, utilizando el conocimiento adquirido en etapas previas para identificar alternativas que

[10] Cornejo, S. (Julio de 2013). *highsec.es*. Obtenido de http://highsec.es/2013/07/buenas-practicas-para-realizar-una-auditoria-de-seguridad-a-empresas/

permitan acceder a los sistemas y obtener el control de los mismos teniendo como objetivo la escala de privilegios.

1.13.4. Evaluación de los resultados obtenidos.

En esta etapa se revisarán cada uno de los resultados y se los clasificará según su prioridad de tal forma que se pueda identificar con claridad cuáles de estos representan mayor peligro en cuanto a la seguridad de los activos de la información.

1.13.5. Corrección de los Expuestos detectados (Creación y aplicación de políticas de seguridad).

Una vez que ya se ha determinado cuales son las amenazas potenciales, se indican las posibles soluciones y se crear políticas de seguridad.

1.13.6. Verificación de la corrección (Penetration Test focalizado).

Una vez identificadas las amenazas y creadas las contramedidas conjuntamente con las políticas de seguridad, se realiza un nuevo test de penetración focalizado para verificar que la corrección ha sido correcta y se encuentra funcional.

1.13.7. Creación de Informes.

En esta etapa se procede a realizar un reporte de las vulnerabilidades encontradas y las posibles soluciones para cada una de ellas.

1.14. Estándares usados en un Test de Penetración.

1.14.1. ISO 27001

La norma ISO 27001 fue publicada en octubre de 2005, esencialmente reemplaza la antigua norma BS7799-2. Es la especificación para un SGSI, un Sistema de Gestión de Seguridad de la Información.

El objetivo de la norma es "proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI)". En cuanto a su adopción, esto debería ser una decisión estratégica. Además, "El diseño y la aplicación de la información del sistema de gestión de seguridad de una organización están influenciados por las necesidades de

la organización y los objetivos, requisitos de seguridad, los procesos organizativos utilizados, el tamaño y estructura de la organización".

La versión 2005 de la norma fuertemente empleó el modelo PDCA, Plan-Do-Check-Act para estructurar los procesos. Sin embargo, la última, la versión 2013, pone más énfasis en la medición y evaluación de lo bien que un SGSI de una organización está siendo realizando. Una sección sobre la subcontratación también se añadió a esta versión, y se prestó mayor atención al contexto organizacional de seguridad de la información.

Las secciones del contenido de la norma son:

- Contexto de la Organización
- Información de Liderazgo de Seguridad
- Planificación de un SGSI
- Soporte
- Operación
- Evaluación del Rendimiento
- Mejora
- Anexo A - Lista de los controles y sus objetivos

1.14.2. ISO 17799

ISO / IEC 17799 establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización. Los objetivos descritos proporcionan una guía general sobre los objetivos de gestión de la seguridad de la información. Además contiene las mejores prácticas de los objetivos de control y controles en las siguientes áreas de gestión de seguridad de la información:

- La política de seguridad.
- Organización de la seguridad de la información.
- Gestión de activos.

- Seguridad de Recursos Humanos.
- Seguridad física y ambiental.
- Las comunicaciones y la gestión de las operaciones;
- Control de acceso;
- Sistemas de información de la adquisición, desarrollo y mantenimiento;
- Información de gestión de incidentes de seguridad;
- Gestión de la continuidad del negocio;
- Cumplimiento.

Los objetivos de control y controles en ISO / IEC 17799 están destinados a ser implementado para cumplir con los requisitos identificados por una evaluación de riesgos. ISO / IEC 17799 pretende ser una base común y guía práctica para el desarrollo de estándares de seguridad de la organización y las prácticas eficaces de gestión de la seguridad, y para ayudar a construir la confianza en las actividades interinstitucionales.

CAPÍTULO II

2. Fase de descubrimiento.

Esta fase se centra principalmente en la recopilación de toda la información que sea posible acerca del objetivo, enfocándose esencialmente en la obtención de datos públicamente accesibles, hayan sido publicados a propósito o por desconocimiento, esto implica que no se estará incurriendo en ningún delito y además la víctima no lo detectará.

Esta tarea es llevada a cabo mediante técnicas pasivas de levantamiento de información, para lo cual se puede hacer uso de un sin número de herramientas públicas (motores de búsqueda), envío de simples peticiones HTTP para revelar mensajes de errores y versiones de sistemas, e inclusive se puede recurrir a los perfiles de solicitud de personal para obtener información valiosa acerca de la herramientas usadas por la empresa, recopilando así datos importantes para las pruebas de penetración. (Guerrero, 2012)[11]

2.1 Recolección de la información.

Nuestro objetivo en esta fase será tratar de recopilar información de la organización mediante el uso del *Footprinting*, que es una técnica de recolección de información aplicada sobre los sistemas informáticos y las entidades a las que pertenecen. (Juan Antonio Calles García, 2011)[12] Este proceso se realiza mediante el empleo de diversas técnicas de seguridad informática donde se podría identificar:

- Nombres de dominio
- Bloques de red
- Servicios de red y aplicaciones
- Arquitectura del sistema

[11] Guerrero, E. G. (12 de Enero de 2012). *revista.seguridad*. Recuperado el 16 de Septiembre de 2014, de http://revista.seguridad.unam.mx/numero-12/la-importancia-de-las-pruebas-de-penetraci%C3%B3n-parte-i

[12] Juan Antonio Calles García, P. G. (2011). *La biblia del Footprinting.* Flu Project.

- Sistema de detección de intrusos
- Mecanismos de autenticación
- Acceso a los mecanismos de control
- Direcciones de contacto
- Los números de teléfono
- Direcciones IP.
- Análisis de características de configuración en redes wifi.

Una de las ventajas de realizar el Footprinting es que se utiliza Google u otros navegadores para obtener información. De esta forma podremos determinar la mejor manera de acceder hacia nuestros objetivos sin ser intrusivos y así ganar datos específicos que serán usados como instrumentos para las pruebas en las siguientes fases, este método no sólo acelera el proceso de intrusión mediante el descarte de ciertos conjuntos de herramientas, sino que también reduce la probabilidad de detección y el tiempo del ataque al hacer uso de la herramienta adecuada para el trabajo.

2.1.1. Fuentes de información.

Dentro del proceso de recolección de la información es importante identificar las fuentes de donde se obtendrán dichos datos, para lo cual haremos uso de diferentes herramientas, desde las más simples hasta las más sofisticadas, de tal forma que obtengamos la información suficiente para nuestras pruebas de penetración. A continuación en la tabla 2-1 se detalla una lista de lugares donde podremos obtener datos de importancia (Montero, Técnicas del penetration test, 2005).[13]

[13] Juan Antonio Calles García, P. G. (2011). *La biblia del Footprinting.* Flu Project.

Tabla 2-1 Fuentes de Información

DATOS A OBTENER	**FUENTES DE INFORMACIÓN**					
	GOOGLE	**WHOIS, NMAP**	**DIRECCIÓN TELEFÓNICA**	**WEB DEFACEMENTS**	**NIC**	**INTRANET**
Rangos de direcciones IP asignadas.		X				
Dominios registrados.					X	
DNS a cargo de los dominios.		X			X	
Rangos telefónicos.			X			X
Nombre del personal técnico		X			X	
Cuentas de correo electrónico.	X					
Instituciones, Organizaciones o Compañías vinculadas.	X					
Incidentes de seguridad informática reportados.				X		
Dirección física de la organización.			X			X
Información General	X					X

Una vez que se tiene en claro de dónde obtendremos la información, lo primero que se hace es ir directamente hacia el sitio web de la empresa donde navegaremos por todo el sitio en búsqueda de alguna pista como un enlace olvidado hacia algún sitio que no debería estar, o algo tan común como un simple error que revele el sistema que se usa y su versión.

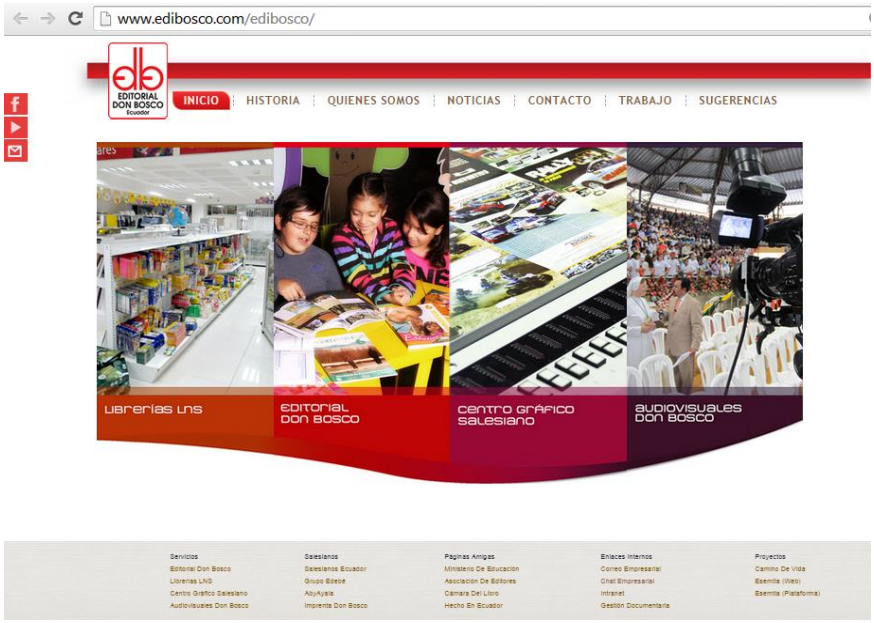


Figura 2-1 Página web de la Editorial Don Bosco.

No siempre con este proceso se garantiza el levantamiento de información de importancia, pero en esta ocasión se pudo encontrar un enlace que nos dirigió hacia la intranet de la empresa.

Figura 2-2 Intranet de la Editorial Don Bosco.

Para obtener un poco más de información se debe realizar una búsqueda avanzada mediante el uso de distintas herramienta, donde una de ellas será *Espiderfoot* que es una aplicación web que contiene diferentes filtros de búsqueda y cuyo propósito es

obtener todo tipo de información acerca del portal web, para lo cual se crea un nuevo escaneo y se marca los filtros que se quieren usar como se muestra a continuación.

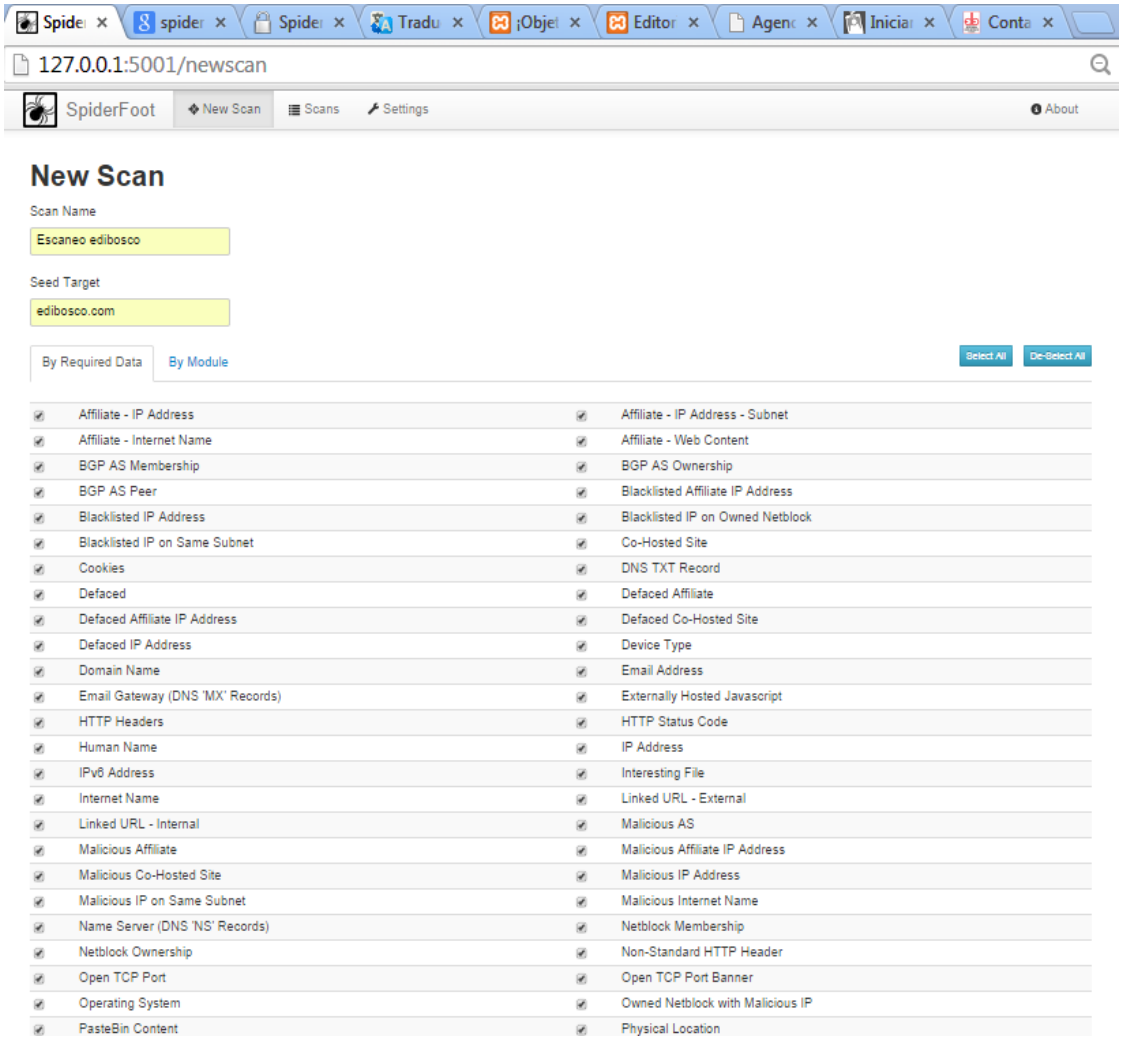


Figura 2-3 Creación de un nuevo escaneo con espiderfoot.

Este escaneo buscara en la web todo tipo de información relacionada al sitio "edibosco.com", y al final nos presentará un resumen indicadnos, dominios, asociación de IP, puertos TCP abiertos, etc.

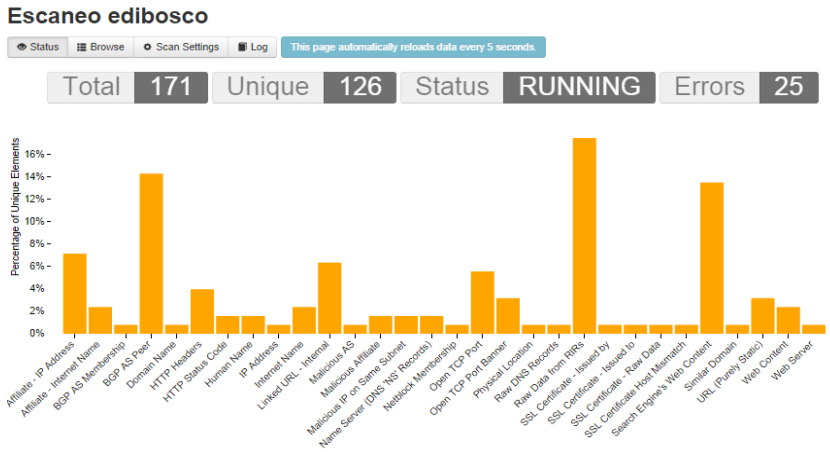


Figura 2-4 Resumen de resultados portal edibosco.com

De este escaneo tenemos los datos más relevantes que se obtuvieron los mismos que se presentan en la tabla 2-2:

Tabla 2-2 Resumen de resultados portal edibosco.com

Nombre de dominio.	edibosco.com
IP de origen de dominio.	108.163.147.39
Locación física	Montreal – Canadá
IP asociadas.	108.163.147.38 - 108.163.147.40 - 108.163.147.41 - 108.163.147.44 - 108.163.147.45 - 108.163.147.46 - 108.163.147.47 - 108.163.147.48
Nombres en internet asociado.	edibosco.com, dad00.xxx.xxx, s403b.panelboxmanager.com, spw00.xxx.xxx
Encaminamiento BGP	108.163.128.0/18
Registros DNS	dad00.xxx.xxx spw00.xxx.xxx
Puertos TCP abiertos	110, 143, 21, 25, 443, 80, 995
Servidor web.	Apache.
ISP	iWeb Technologies Inc.

Es importante identificar aquella información útil y separarla para su posterior utilización, en este caso basados en los resultados anteriores podemos ver que el sitio

web “edibosco.com”, tiene un hosting particular e independiente a de la empresa ubicado en Montreal – Canadá, por lo que se debe tomar en cuenta que la seguridad dependerá del proveedor del hosting, y si se realiza pruebas de penetracoón o no dependerá exclusivamente del el alcance, delimitaciones y restricciones del acuerdo al que se llegó en un principio, por esta razón nos conformaremos con la información anteriormente obtenida y se tratará de buscar información y vulnerabilidades que no afecten las políticas del proveedor de hosting.

Un punto clave dentro de nuestro *Penetration Test*, será la intranet de la empresa, la misma que fue encontrada anteriormente, esta será analizada utilizando las herramientas anteriormente usadas o se podría optar por alguna mejor, donde con la ayuda de Espiderfoot hemos obtenido los siguientes resultados.

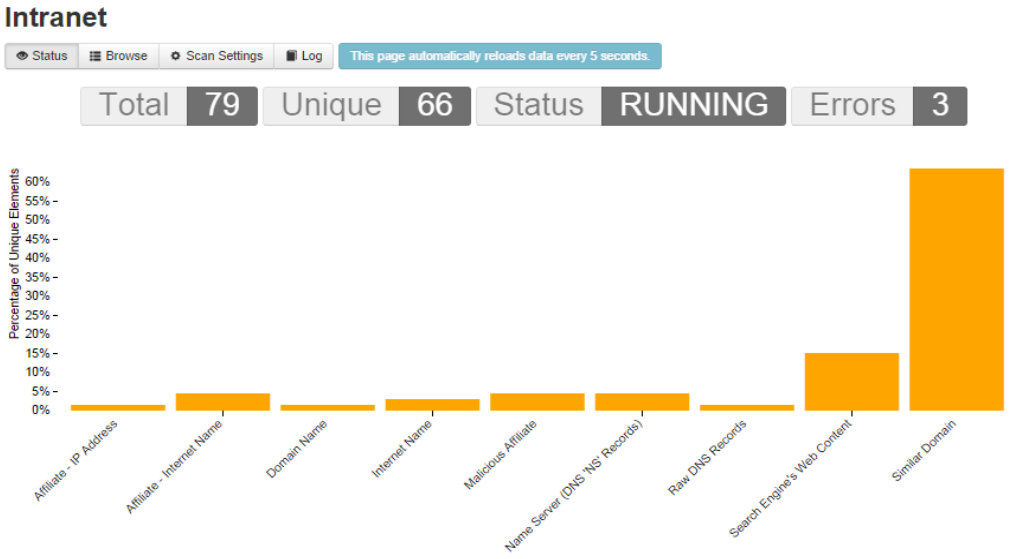


Figura 2-5 Resumen de resultados de la intranet emp.lns.com.ec

De este resumen de resultados tenemos como los datos más relevantes los siguientes.

Tabla 2-3 Resumen de resultados de la intranet emp.lns.com.ec

Nombre de dominio.	Emp.lns.com.ec
IP de origen de dominio.	108.163.147.39
Locación física	Guayaquil – Ecuador
IP asociadas.	192.xxx.xxx.38
Nombres en internet asociado.	Dad00.xxx.xxx, sin00.xxx.xxx, spw00.xxx.xxx
Registros DNS	dad00.xxx.xxx, sin00.xxx.xxx, spw00.xxx.xxx

En este caso la información es muy corta por lo que se debe hacer uso de otras herramientas como el uso de la extensión "IP Address and Domain Information" para Google Chrome la cual nos entregará información más detallada como la localidad, el proveedor, direcciones ip, etc.

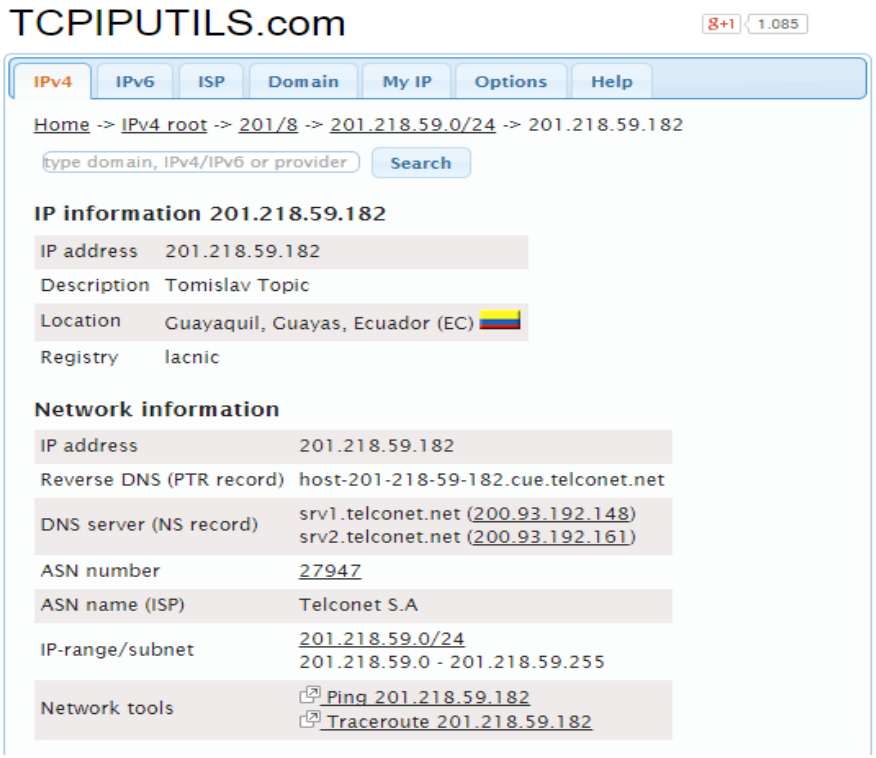


Figura 2-6 Resumen de resultados de la intranet emp.lns.com.ec

Esta herramienta resulta muy útil para obtener información instantánea pública de portales web, obteniendo en este caso información de importancia sobre la intranet la siguiente.

Tabla 2-4 Resumen de resultados de la intranet emp.lns.com.ec

Información IPV4 – proveedor	
Dirección IP	xxx.218.58.182
Locación	Guayaquil – Ecuador
DNS inverso (Registro PTR)	Host:xxx.218.59.182.cue.telconet.net
DNS server	Srv1.telconet.net (200.93.192.148) Srv2.telconet.net (200.93.192.161)
Nombre y número ASN	27947 – Telconet S.A
Teléfono	+593 4 2680555

e-mail	hostmaster@TELCONET.NET
RIR	Lacnic
Información página	
Nombre del dominio	lns.com.ec
Servidor de correo	lns-com-ec.mail.eo.outlook.com (207.46.163.215) mail.lns.com.ec (xxx.218.59.181)
Información del registro (Datos públicos Whois)	
Registrante	Lcdo. Jorge Sánchez
Organización.	Librerías Nacionales Salesianas
Dirección.	Vega Muñoz 1068 – Cuenca, Azuay
E-mail	edibosco@lns.com.ec
Teléfono/ Fax	5937-2831745/5937-2842722
Información del gerente (Datos públicos Whois)	
Nombre:	Lcdo. Marcelo Mejia
Organización.	Editorial Don Bosco
Dirección.	Vega Muñoz 1068 – Cuenca, Azuay
E-mail	edibosco@lns.com.ec
Teléfono/ Fax	5937-2831745/5937-2842722
Información del contacto técnico (Datos públicos Whois)	
Nombre:	Christian Saquicela
Organización.	Editorial Don Bosco
Dirección.	Vega Muñoz 1068 – Cuenca, Azuay
E-mail	csaquicela@lns.com.ec
Teléfono/ Fax	5937-2831745/5937-2842722
Información del administrador (Datos públicos Whois)	
Nombre:	Ing. Hernando Abril
Organización.	Editorial Don Bosco
Dirección.	Vega Muñoz 1068 – Cuenca, Azuay
E-mail	habril@lns.com.ec
Teléfono/ Fax	5937-2831745/5937-2842722.

Otro punto a tomar y de importancia dentro de la fase de descubrimiento es tratar de generar eventos que nos lancen errores y que revelen información valiosa como: el sistema y la versión que usa, una dirección IP o un simple contacto.

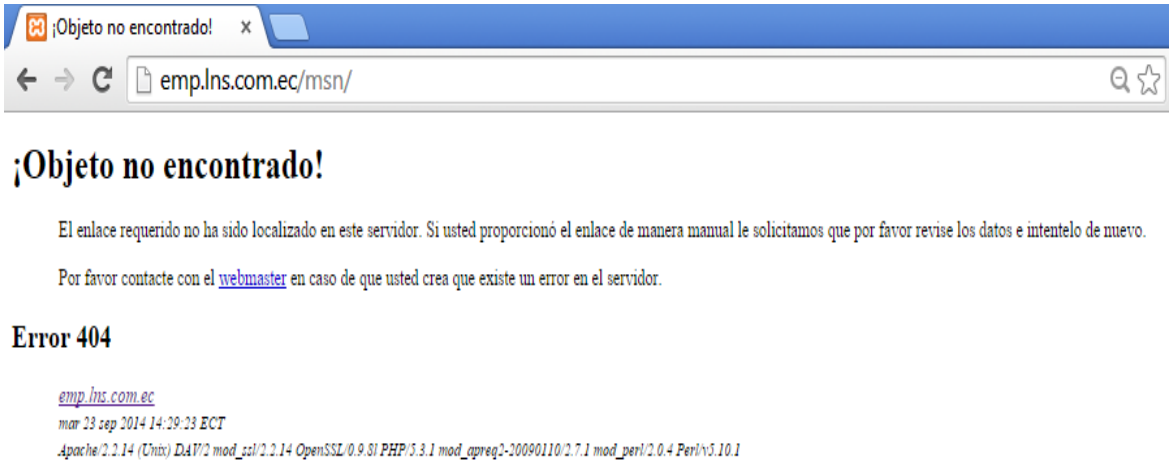


Figura 2-7 Presentación del error dentro de emp.lns.com.ec

En este caso mediante la manipulando el URL, ubicando una ruta inexistente, la página nos lanza hacia una nueva ventana donde nos indica cual es el error y esta nos presenta la siguiente información.

Tabla 2-5 Resultados obtenidos de la página con el error.

Dominio de la página	**emp.lns.com.ec**
Sistemas y versiones	
Apache	2.2.14
(Unix)DAV/2mod_ssl	2.2.14
OpenSSL	0.9.SI
PHP	5.3.1
Mod_apreq2-20090110	2.7.1
Mod_perl/2.0.4	Perl/v5.10.0

Cuando se trata de un test de caja blanca y tenemos acceso directo a la red de la empresa podemos generar acciones indebidas consideradas de esta forma por los dispositivos de seguridad, en este caso un firewall, el cual trata de restringir y controlar el acceso lanzando una advertencias, especificándonos la restricción de dicho suceso, por lo que se debe probar el acceso a páginas comúnmente restringidas por los

administradores de red, en este caso se trató con YouTube obteniendo los siguientes datos.

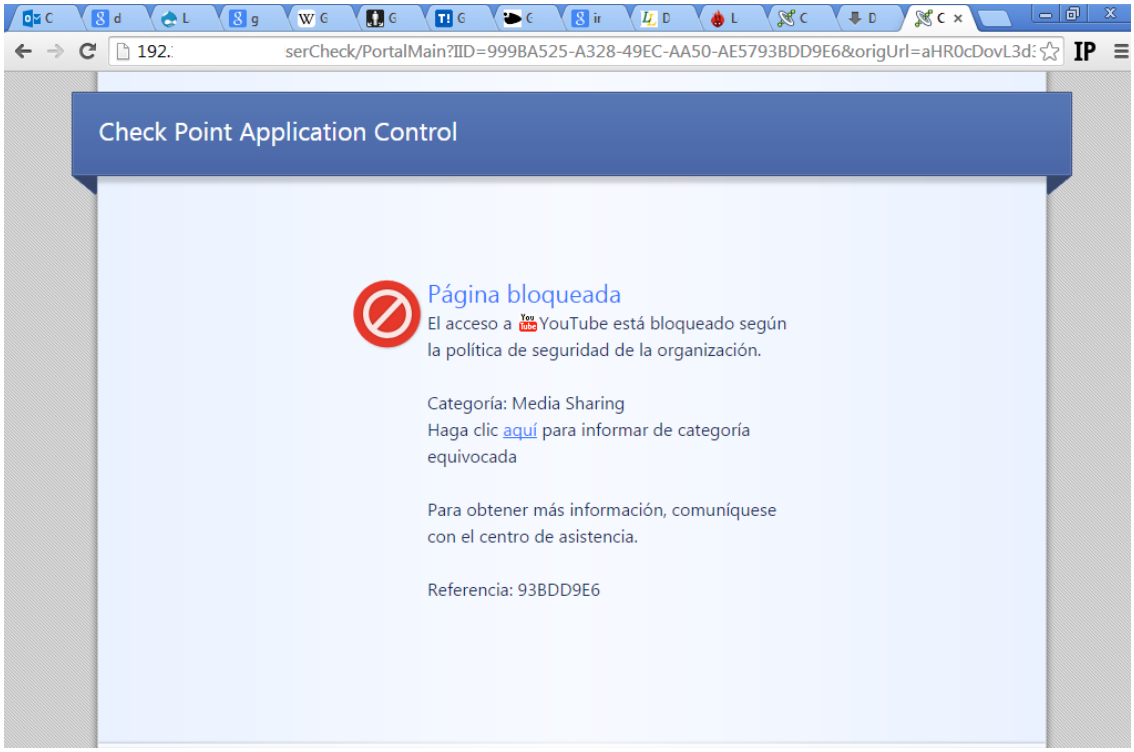


Figura 2-8 Presentación de la advertencia generada por el firewall.

En esta página de advertencia, podemos recopilar información importante que nos servirá de mucho al momento de evadir el firewall, como: tipo, marca y dirección IP del dispositivo, permitiéndonos delimitar uno de nuestros principales objetivos.

Tabla 2-6 Datos obtenidos del mensaje de restricción del firewall.

Tipo de Firewall	Check Point
Ip del firewall.	192.xxx.xxx.254

Otra fuente importante de información son los directorios telefónicos de la empresa, en este caso dichos directorios los pudimos encontrar dentro de la intranet de la empresa, el cual contenía las extensiones de cada departamento y el nombre del responsable a cargo.

Tabla 2-7 Directorio telefónico de la empresa.

Directorio Editorial Don Bosco		
Lns Ambato	Susana Arcos <20401> Santiago Jordan <20403>	Ventas Ambato <20405>
Lns Quito	Vinicio Idrovo <20201> Ventas <20207> Evelin Manya <20202> BodegaIn <20208> Mayte Andrango <20204> Ventas2 <20209>	Subgerencia Quito <20203> Abya-Yala <20211> Ventas <20205> BodegaAlm <20210> Roberto Calle <20206>
Editorial	Gerencia-Qui <22001> Isabel Luna<22051> Eder Acuna <22011>	Fabricio Benalcazar <22031> Pamela Cueva <22021> Edwin Ceballos <22041>
Audiovisuales	Audiovisual <22101> Ximena Paez <22102> Mario Serrano <22103>	Gustavo Naranjo <22104> Monica Ulloa <22105> Paola Brito <22106>
Centro de publicaciones pastorales	Gabriela Chiriboga <22xxx>	
Cuenca	Gerente <20001> Subgerente <20002> movil-Habril <20006> movil-garias <20008> Caty Vega <20100>	Porteria <20101> Jenny Ganan <20111> Nely Portilla <20112> Jose Andrade <20113> Elvira Leon <20114>
RRHH	Carmita Vargas <20121>	Cristina Pena <20122>
Auditoria	Miguel Cabrera <20131>	
Sistemas	Hernando Abril <20141> Cristian Saquicela <20142>	Mary Bermeo <20143>
Esemtia	Verónica Cajamarca <20151>	
Comercialización	Edison Pauta <20801> Gabriela Estrella <20802> Darwin Vivanco <20803>	Rolando Villavicencio <20804> Ricardo Valencia <20805> AsisCompras <20806>
Machala	Machala <20901> Machala2 <20902>	Machala3 <20903>
Ibarra	Ibarra <21101>	
LNS Cuenca	Gustavo Arias <21201> Diana Loja <21202> Patricio Esparza <21203>	Jesica Alvarez <21204> Ventas <21205>
Cgs	Mónica Silva <21901>	Carla Bermeo <21905>

	Carmita Pinos <21902> Rebeca Benavidez <21903> Patricio Sánchez <21904>	Patricio Llivicura <21911> Marcia Pena <21912>
	Pablo Moscoso <21921> Willian Faican <21931>	Auxiliar Planta <21932> Andres Macancela <21941>
PCS	Pc-mbermeo <30145> Pc-Epauta <30146>	Pc-Tecnico <30151>
Guayaquil	Jefe Almacen GYE <20301> Contabilidad GYE <20302> Bodega GYE <20303> Almacen GYE <20304>	Ventas GYE <20305> Auxiliar Com GYE <20306> Mary Cabanilla <20307> Pc-Asistente Con <20308>
Manta	Lilian Flores <20701> Kenia Mendoza <20702> Jose Delgado <20703>	Silvia Macias <20704> Ventas-MAN <20705>

Otro medio para recopilar información acerca de los recursos de la empresa es husmear en anuncios publicitarios donde se busca oportunidades laborales y se pide un perfil específico, permitiéndole al atacante delimitar su área de intrusión. Como se puede ver en la Figura 2-9, el perfil que se requiere nos da una idea general de qué tipo de características tendrá nuestro objetivo como por ejemplo podrá usar base de datos Oracle, MySql, Postgress o las tres, también nos da una ida de la posibilidad de que el objetivo posea diferentes aplicaciones que requieran diferentes plataformas, etc.

Editorial Don Bosco

Publicado 03 de julio de 2014
Área Programación (ver más empleos en Programación) ▸
Tipo de puesto Full-time (ver más empleos Full-time) ▸
Salario No especificado
Lugar de trabajo Quito, Pichincha ▸

La empresa dio por finalizado este aviso.

La persona será responsable del diseño de la arquitectura, implementación, desarrollo o modificación de portales web y aplicaciones en redes sociales. Implementación de portales open source (joomla, wordpress), desarrollo de aplicaciones móviles android
Edad: 23 a 40 años
Estudios: Ingeniería en sistemas, Análisis de sistemas .
Conocimientos:
- Amplios conocimientos en HTML, CSS y JavaScript.
- Lenguajes de programación: PHP o .net.
- Base de datos Oracle, MySql, Postgress.
- Conocimientos de PL/SQL
- Conocimientos de Asterisk (opcional)
- Desarrollo de aplicaciones para redes sociales o uso del API.
- Desarrollo de aplicaciones para dispositivos móviles con android, apple.
- Conocimiento e implementación de SEO y SEM.
- Manejo de framework PHP
- Frameworks: JQuery, Bootstrap.
- Flash (opcional).
- Responsive Design

Figura 2-9 Perfil de tecnologías en anuncios de trabajo.

2.2. Identificación de Equipos.

Dentro del proceso de descubrimiento se debe tratar en lo posible de identificar y recopilar características de equipos insignia como servidores y dispositivos de seguridad que podrían encontrarse expuestos, esto se realizará de una forma no intrusiva buscando delimitar mucho más nuestros objetivos, además hay que tener en cuenta como un factor de riesgo cuan al descubierto esta este tipo de información y que tan fácil o difícil resulta obtenerla.

Basándonos en datos anteriormente encontrados y con ayuda de la herramienta nslookup trataremos de identificar la IP de equipos que tengan cierta importancia dentro del proceso de evaluación de la seguridad, en este caso nos centraremos en los servidores DNS.

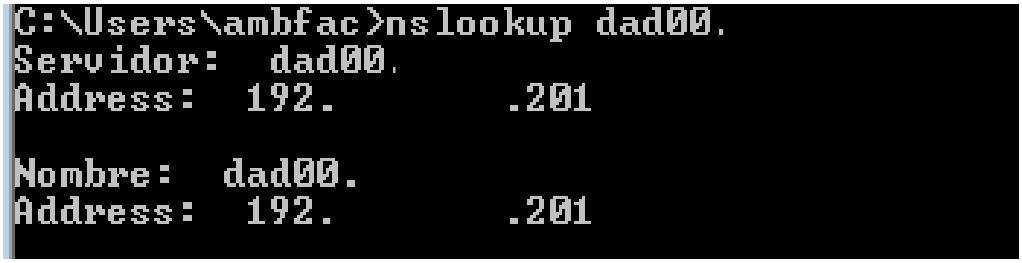


Figura 2-10 Obtención de ip de servidor dad00.xxx.xxx

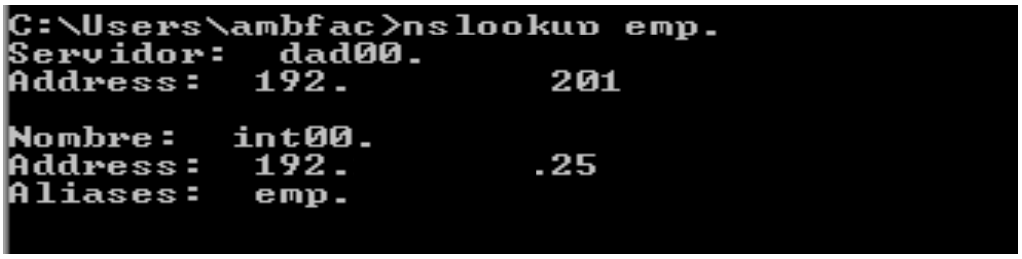


Figura 2-11 Obtención de ip de servidor emp.lns.com.ec

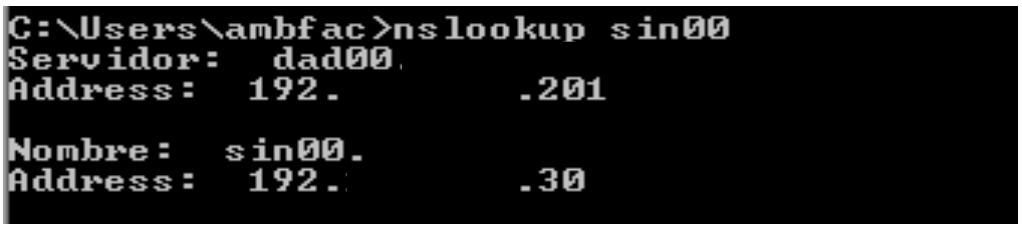


Figura 2-12 Obtención de ip de servidor sin00.xxx.xxx

Figura 2-13 Obtención de ip de servidor spw00.xxx.xxx

Recopilando la información obtenida hemos identificado los siguientes dispositivos de importancia dentro de la infraestructura de la red.

Tabla 2-8 Identificación de equipos.

IP	TIPO	NOMBRE
192.xxx.xxx.254	Firewall	Check Point
192.xxx.xxx.xxx	DNS	dad00.xxx.xxx
192.xxx.xxx.30	DNS	sin00.xxx.xxx
192.xxx.xxx.7	DNS	spw00.xxx.xxx

Es siempre importante mantenerse alerta de cualquier dato que se pueda obtener, en esta ocasión como datos adjuntos hemos obtenido dos rangos de IP, los cuales fueron constatados por el administrador de la red los cuales citamos a continuación.

Tabla 2-9 Identificación de Equipos

RANGOS IP	TIPO DE TRÁFICO
192.xxx.xxx.0/24	Datos
192.xxx.xxx.0/24	Voz

2.3. Descubrimiento de la red.

Como se ha visto la fase de descubrimiento es un proceso recursivo, donde se hace uso de la información obtenida para generar nuevos datos y con ellos poder tener una idea general de cómo se encuentra nuestro escenario de penetración y así determinar cuáles serás nuestros posibles objetivos, además de brindarnos la posibilidad de realizar una mejor planificación de los ataques que llevaremos a cabo. Tomando esto en cuenta se

creará como referencia un esquema genérico de cómo se encuentra la red, el mismo que nos ayudará a tener una idea más acertada de la red, especialmente de la ubicación de dispositivos de seguridad como el firewall.

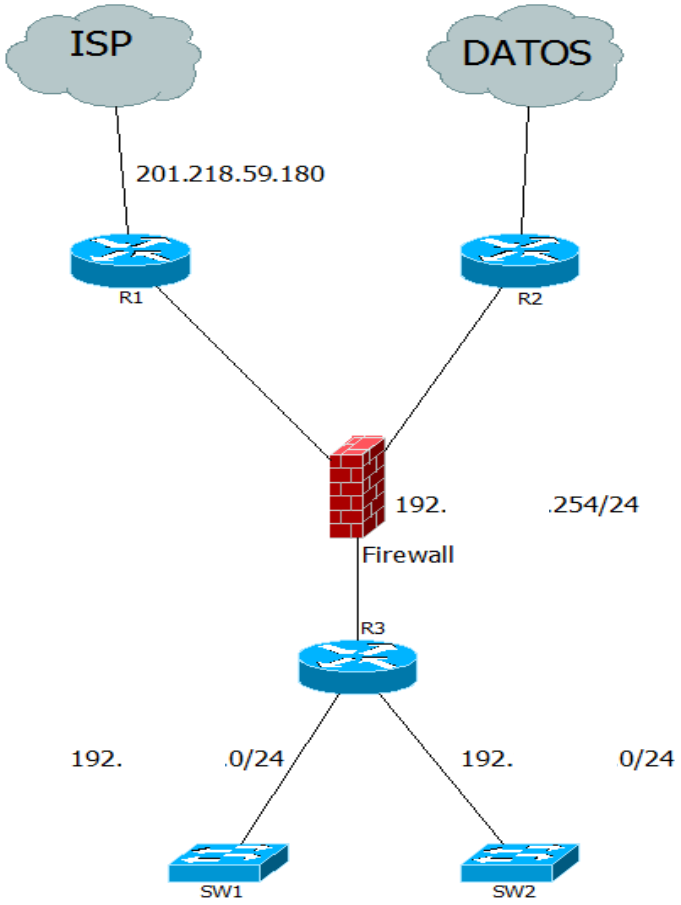


Figura 2-14 Tendencia diagrama de la red según resultados.

2.4. Detección de redes WIFI.

En este caso la empresa ha puesto a nuestro conocimiento el SSID de los equipos inalámbricos para las posteriores pruebas a realizarse, pero antes de ello obtendremos algunos datos de estas redes médiate un escaneo con la herramienta aircrack-ng la cual nos muestra la existencia de las redes edbuse y wcgs pertenecientes a la edibosco, con ella confirmamos la información antes brindada.

En el caso de que esta información no sea facilitada es muy sencillo determinar cuáles podrían ser las redes pertenecientes a la empresa, para ello nos basaremos en la

potencia de la señal, donde aquellas señales que sean más fuertes nos indicarán que son las más cercanas y por ende estarían dentro del área de la empresa.

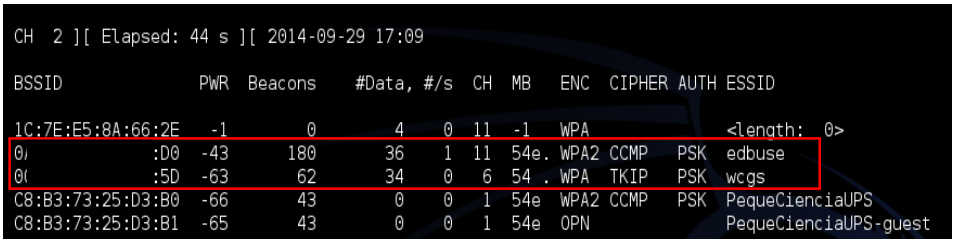


Figura 2-15 Escaneo de redes wifi.

Finalmente debemos tomar en cuenta las recomendaciones, las cuales nos indican que se deben realizar las pruebas iniciales para la obtención de información desde un segmente de red que sepamos no nos afectaría si nuestras direcciones IP son bloqueadas, o haciendo uso de alguna herramienta que clone nuestra dirección u algún otro método, que si por algún motivo el dispositivo de seguridad detectara nuestra presencia y nos bloqueara, simplemente sea cuestión de cambiar nuestros identificadores para continuar el análisis. Esto es importante tener en cuenta cuando realizamos escaneos con herramientas como NMAP, que a pesar de poseer métodos no intrusivos de exploración, dependiendo de la sensibilidad del dispositivo de seguridad este podría ver el escaneo como una amenaza y proceder al bloqueo de la IP.

Capitulo III

3. Fase de Exploración.

Esta fase es más activa que la fase de descubrimiento y el objetivo es encontrar puertos abiertos y localizar aplicaciones vulnerables, para ello es necesario saber que máquinas están activas así como también identificar Access points, rangos de ip, análisis de protocolos, levamiento de plataforma y barreras de protección, scanning telefónico, scanning de puertos TCP y UDP, detección remota de servicios y sistemas operativos, análisis de banners y búsqueda de aplicaciones web, es decir todos los potenciales blancos, con el uso de técnicas no intrusivas como por ejemplo la ejecución del comando ping a cada una de las máquinas para determinar si el host está activo o inactivo. La Tabla 3-1 muestra los resultados esperados de esta fase. (Peter Vincent Herzog, 2003)[14]

Tabla 3-1 Resultados esperados en la fase de Exploración.

Resultados Esperados:	Puertos abiertos, cerrados y filtrados.
	Direcciones IP de los sistemas activos.
	Direccionamiento de los sistemas de la red interna.
	Lista de los protocolos descubiertos de tunelizado y encapsulado.
	Lista de los protocolos descubiertos de enrutado soportados.
	Servicios activos.
	Tipos de Servicios.
	Tipo y nivel de parcheado de las Aplicaciones de los Servicios.
	Tipo de Sistema Operativo.
	Nivel de parcheado.
	Tipo de Sistema.
	Lista de sistemas activos
	Mapa de la red

[14] Peter Vincent Herzog, t. I. (2003). *OSSTMM 2.1*.

3.1 Detección de host activos.

La detección de host activos es muy importante ya que nos ayuda a identificar el perímetro y el límite exterior del sistema, crear exactamente el mapa de la red objetivo, con lo que podemos crear un inventario de los sistemas que son accesibles en la red a ser analizada. Las principales utilidades empleadas para la detección de host activos son: el comando ping y traceroute.

Para la identificación de host activos se puede utilizar el comando **ping** que es una utilidad muy simple que diagnostica la velocidad a la cual los paquetes son transportados a través de la red, detalles del TTL (Time To Live) e incluso resuelve el nombre del host, todo esto mediante el envío de paquetes ICMP de petición y la espera de paquetes ICMP de respuesta desde el host activo.

Sin embargo utilizar individualmente el comando ping para cada una de las posibles direcciones ip puede consumir mucho tiempo y volverse un proceso tedioso para ello existe una técnica llamada ping Sweep. La misma que consiste en el mismo ping pero a un lote de direcciones, lo que ayuda a determinar cuáles de ellos están activos, obviamente los host que no responden a la petición ICMP significa que están apagados o tienen bloqueado el protocolo ICMP.

Existen una variedad de herramientas ping que proveen varios niveles de funcionalidad y características entre las principales tenemos: WS_PingProPack, NetScan Tools, Hping, Nmap.

A continuación se ilustra una imagen de la herramienta utilizada para la detección de los host activos:

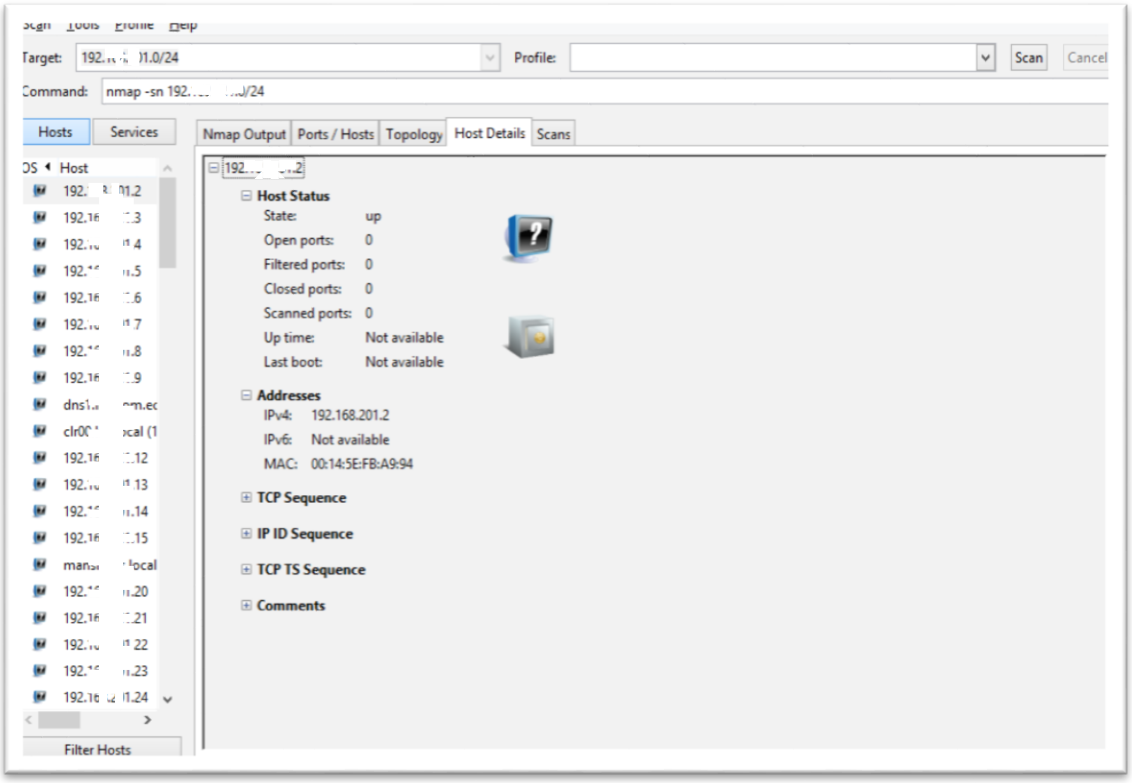


Figura 3-1 NMap, descubrimiento de host activos mediante ping sweep.

De acuerdo al resultado obtenido al ejecutar el comando nmap –sn tanto para la red 192.xxx.xxx.0/24 y 192.xxx.xxx.0/24 se obtuvo la siguiente tabla de host activos.

Tabla 3-2 Hosts activos de las redes 192.xxx.xxx.0/24 y 192.xxx.xxx.0/24

RANGO DE DIRECCIONES IP ACTIVAS 192.xxx.xxx.0/24	RANGO DE DIRECCIONES IP ACTIVAS 192.xxx.xxx.0/24
192.xxx.xxx.1	192.xxx.xxx.2
192.xxx.xxx.2	192.xxx.xxx.3
192.xxx.xxx.11	192.xxx.xxx.4
192.xxx.xxx.12	192.xxx.xxx.5
192.xxx.xxx.21	192.xxx.xxx.6
192.xxx.xxx.31	192.xxx.xxx.7
192.xxx.xxx.32	192.xxx.xxx.8
192.xxx.xxx.41	192.xxx.xxx.9
192.xxx.xxx.81	xxxx.lns.com.ec (192.xxx.xxx.10)
192.xxx.xxx.82	clr00.xxx.xxx (192.xxx.xxx.11)
192.xxx.xxx.83	192.xxx.xxx.12
192.xxx.xxx.85	192.xxx.xxx.15
192.xxx.xxx.86	mansis.xxx.xxx (192.xxx.xxx.16)
192.xxx.xxx.91	192.xxx.xxx.20
192.xxx.xxx.92	192.xxx.xxx.21

192.xxx.xxx.94 192.xxx.xxx.95 192.xxx.xxx.100 192.xxx.xxx.xxx 192.xxx.xxx.111 192.xxx.xxx.112 192.xxx.xxx.113 192.xxx.xxx.114 192.xxx.xxx.121 192.xxx.xxx.122 192.xxx.xxx.131 192.xxx.xxx.141 192.xxx.xxx.142 192.xxx.xxx.143 192.xxx.xxx.151 192.xxx.xxx.xxx 192.xxx.xxx.202 192.xxx.xxx.204 192.xxx.xxx.205 192.xxx.xxx.250 192.xxx.xxx.253 192.xxx.xxx.254	192.xxx.xxx.22 192.xxx.xxx.23 192.xxx.xxx.24 emp.lns.com.ec (192.xxx.xxx.25) 192.xxx.xxx.26 192.xxx.xxx.27 sts03.xxx.xxx (192.xxx.xxx.28) sin00.xxx.xxx (192.xxx.xxx.30) 192.xxx.xxx.31 192.xxx.xxx.32 192.xxx.xxx.33 sts02.lns.com.ec (192.xxx.xxx.34) 192.xxx.xxx.39 192.xxx.xxx.41 192.xxx.xxx.42 192.xxx.xxx.45 192.xxx.xxx.46 192.xxx.xxx.50 192.xxx.xxx.52 192.xxx.xxx.53 192.xxx.xxx.54 192.xxx.xxx.55 192.xxx.xxx.56 192.xxx.xxx.58 192.xxx.xxx.59 192.xxx.xxx.60 192.xxx.xxx.63 SEP0026CBBDEA63.lns.com.ec (192.xxx.xxx.65) 192.xxx.xxx.66 SEP001C58576AA3.lns.com.ec (192.xxx.xxx.67) 192.xxx.xxx.68 192.xxx.xxx.69 192.xxx.xxx.70 SEP001BD4609C8D.lns.com.ec (192.xxx.xxx.71) 192.xxx.xxx.72 CUEALM.lns.com.ec (192.xxx.xxx.73) 192.xxx.xxx.74 cueasis.lns.com.ec (192.xxx.xxx.75) 192.xxx.xxx.76 192.xxx.xxx.77 192.xxx.xxx.78 192.xxx.xxx.79 192.xxx.xxx.80 192.xxx.xxx.81

	192.xxx.xxx.84 192.xxx.xxx.85 192.xxx.xxx.86 192.xxx.xxx.88 192.xxx.xxx.89 192.xxx.xxx.90 192.xxx.xxx.91 192.xxx.xxx.92 192.xxx.xxx.93 192.xxx.xxx.94 192.xxx.xxx.95 192.xxx.xxx.100 192.xxx.xxx.xxx 192.xxx.xxx.102 192.xxx.xxx.105 192.xxx.xxx.107 192.xxx.xxx.111 192.xxx.xxx.112 192.xxx.xxx.113 192.xxx.xxx.115 192.xxx.xxx.116 192.xxx.xxx.121 192.xxx.xxx.122 192.xxx.xxx.124 192.xxx.xxx.127 192.xxx.xxx.131 192.xxx.xxx.134 192.xxx.xxx.135 192.xxx.xxx.138 192.xxx.xxx.145 192.xxx.xxx.155 192.xxx.xxx.179 192.xxx.xxx.181 192.xxx.xxx.185 192.xxx.xxx.186 192.xxx.xxx.188 192.xxx.xxx.193 192.xxx.xxx.195 192.xxx.xxx.198 192.xxx.xxx.199 dad00.lns.com.ec (192.xxx.xxx.xxx) 192.xxx.xxx.214 192.xxx.xxx.215 192.xxx.xxx.223 192.xxx.xxx.247 192.xxx.xxx.248

	192.xxx.xxx.249 192.xxx.xxx.250 192.xxx.xxx.251 192.xxx.xxx.252 192.xxx.xxx.253 192.xxx.xxx.254

3.2. Detección de servicios activos.

Luego de haber determinado el rango de red y obtenido un inventario de todos los host activos es preciso localizar los puertos en las maquinas activas e identificar los servicios que están corriendo sobre los mismos, lo que nos ayudará a determinar puertos potenciales para crear vectores de ataque, además se obtendrá información de los sistemas operativos y se identificaran aplicaciones específicas. Para ello se utiliza el escaneo de puertos que es una de la técnicas más reconocidas y que son utilizadas por los pentesters para descubrir vulnerabilidades, el mismo que es un método que permite descubrir más sobre la red, dicho método envía paquetes de datos a los puertos TCP y UDP para verificar que servicios y aplicaciones están corriendo en el dispositivo objetivo. Por ejemplo si el puerto 25 y 80 están abiertos, los servicios que están corriendo en un determinado dispositivo son SMTP y HTTP correspondientemente.

Antes de realizar el escaneo de puertos es preciso saber que los puertos tienen tres estados que se mencionan a continuación:

Abierto: El puerto acepta la comunicación desde el dispositivo objetivo.

Cerrado: El puerto no acepta conectividad.

Filtrado: Indica que un cortafuego, filtro u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que no se puede saber si se encuentra abierto o cerrado.

En la figura 3-2 se muestra los comandos utilizados para obtener los puertos que están abiertos en cada host activo.

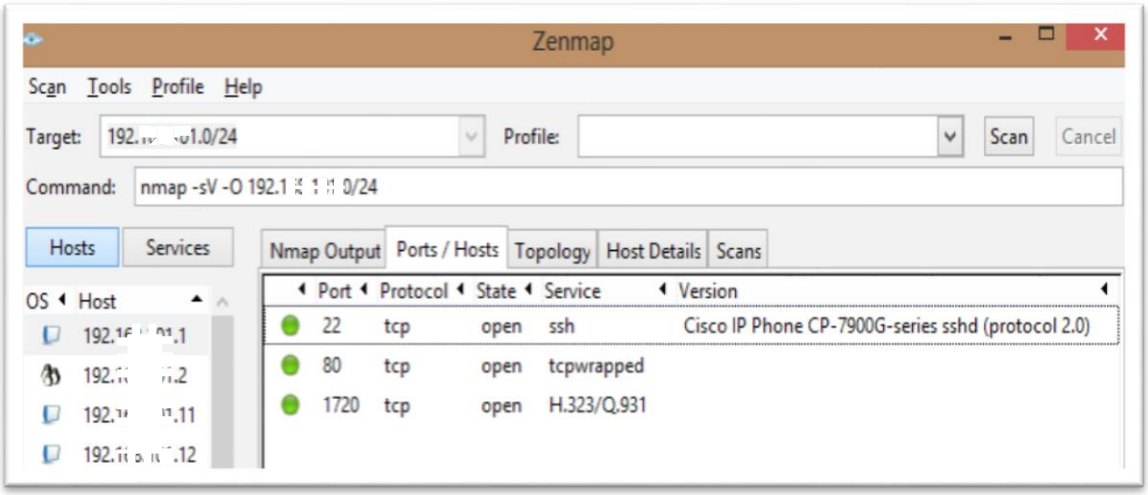


Figura 3-2 Detección de host activos mediante nmap -sV –O

De acuerdo al escaneo de puertos realizado con el comando nmap –sV –O tanto para la red 192.xxx.xxx.0/24 y 192.xxx.xxx.0/24 se obtuvo una lista de los servicios activos (ver anexo 2 y anexo 3), sin embargo a continuación se presenta un resumen de los resultados obtenidos.

Tabla 3-3 Resumen de servicios activos en los host de la red 192.xxx.xxx.0/24

Servicios	Direcciones IP	Puertos	Estado
bandwidth-test	192.xxx.xxx.254	2000	Abierto
domain	192.xxx.xxx.31, 192.xxx.xxx.85	53	Abierto
H.323/Q.931	192.xxx.xxx.1, 192.xxx.xxx.2, 192.xxx.xxx.11, 192.xxx.xxx.12, 192.xxx.xxx.21, 192.xxx.xxx.31, 192.xxx.xxx.32, 192.xxx.xxx.41, 192.xxx.xxx.81, 192.xxx.xxx.82, 192.xxx.xxx.83, 192.xxx.xxx.85, 192.xxx.xxx.86, 192.xxx.xxx.91, 192.xxx.xxx.92, 192.xxx.xxx.94, 192.xxx.xxx.95, 192.xxx.xxx.100, 192.xxx.xxx.xxx, 192.xxx.xxx.111, 192.xxx.xxx.112, 192.xxx.xxx.114, 192.xxx.xxx.114, 192.xxx.xxx.121, 192.xxx.xxx.122, 192.xxx.xxx.131, 192.xxx.xxx.141, 192.xxx.xxx.142, 192.xxx.xxx.143, 192.xxx.xxx.151, 192.xxx.xxx.xxx, 192.xxx.xxx.202, 192.xxx.xxx.204, 192.xxx.xxx.205, 192.xxx.xxx.250, 192.xxx.xxx.253, 192.xxx.xxx.254	1720	Abierto
http	192.xxx.xxx.2, 192.xxx.xxx.31, 192.xxx.xxx.32, 192.xxx.xxx.41, 192.xxx.xxx.83, 192.xxx.xxx.85, 192.xxx.xxx.100, 192.xxx.xxx.xxx, 192.xxx.xxx.204, 192.xxx.xxx.250, 192.xxx.xxx.253	80	Abierto
http-alt	192.xxx.xxx.250	8000	Abierto
https	192.xxx.xxx.91, 192.xxx.xxx.250, 192.xxx.xxx.253	443	Abierto
imap	192.xxx.xxx.253	993,143	Abierto
iss-realsecure	192.xxx.xxx.250	902	Abierto
Mysql	192.xxx.xxx.253	33.06	Abierto

Netbus	192.xxx.xxx.41	12345	Abierto
pop3	192.xxx.xxx.253	995,110	Abierto
Pptp	192.xxx.xxx.254	1723	Abierto
rcpbind	192.xxx.xxx.253	111	Abierto
Smtp	192.xxx.xxx.253	25	Abierto
Ssh	192.xxx.xxx.1, 192.xxx.xxx.11, 192.xxx.xxx.12, 192.xxx.xxx.21, 192.xxx.xxx.32, 192.xxx.xxx.81, 192.xxx.xxx.82, 192.xxx.xxx.86, 192.xxx.xxx.92, 192.xxx.xxx.94, 192.xxx.xxx.95, 192.xxx.xxx.100, 192.xxx.xxx.111, 192.xxx.xxx.112, 192.xxx.xxx.113, 192.xxx.xxx.114, 192.xxx.xxx.121, 192.xxx.xxx.122, 192.xxx.xxx.131, 192.xxx.xxx.141, 192.xxx.xxx.142, 192.xxx.xxx.143, 192.xxx.xxx.151, 192.xxx.xxx.xxx, 192.xxx.xxx.202, 192.xxx.xxx.205, 192.xxx.xxx.250, 192.xxx.xxx.253	22	Abierto
Status	192.xxx.xxx.253	749	Abierto
Svrloc	192.xxx.xxx.250	427	Abierto
tcpwrapped	192.xxx.xxx.1, 192.xxx.xxx.11, 192.xxx.xxx.12, 192.xxx.xxx.21, 192.xxx.xxx.81, 192.xxx.xxx.82, 192.xxx.xxx.86, 192.xxx.xxx.92, 192.xxx.xxx.94, 192.xxx.xxx.95, 192.xxx.xxx.111, 192.xxx.xxx.112, 192.xxx.xxx.113, 192.xxx.xxx.114, 192.xxx.xxx.121, 192.xxx.xxx.122, 192.xxx.xxx.131, 192.xxx.xxx.141, 192.xxx.xxx.142, 192.xxx.xxx.143, 192.xxx.xxx.151, 192.xxx.xxx.xxx, 192.xxx.xxx.202, 192.xxx.xxx.205, 192.xxx.xxx.254	808,291	Abierto
telnet	192.xxx.xxx.31, 192.xxx.xxx.85	23	Abierto
Tmi	192.xxx.xxx.250	8300	Cerrado
upnotifyp	192.xxx.xxx.253	4445	Abierto
wbem-http	192.xxx.xxx.250	5988	Cerrado
wbem-https	192.xxx.xxx.250	5989	Abierto
x11	192.xxx.xxx.250	6025	Cerrado
X11	192.xxx.xxx.250	6000	Cerrado
X11:1	192.xxx.xxx.250	6001	Cerrado
X11:2	192.xxx.xxx.250	6002	Cerrado
X11:3	192.xxx.xxx.250	6003	Cerrado
X11:4	192.xxx.xxx.250	6004	Cerrado
X11:5	192.xxx.xxx.250	6005	Cerrado
X11:59	192.xxx.xxx.250	6059	Cerrado
X11:6	192.xxx.xxx.250	6006	Cerrado
X11:7	192.xxx.xxx.250	6007	Cerrado
X11:9	192.xxx.xxx.250	6009	Cerrado
xprint-server	192.xxx.xxx.250	8100	Cerrado

Tabla 3-4 Resumen de servicios activos en los host de la red 192.xxx.xxx.0/24

Servicios	Direcciones IP	Puertos	Estado
telnet	192.xxx.xxx.8, 192.xxx.xxx.20, 192.xxx.xxx.21, 192.xxx.xxx.22, 192.xxx.xxx.23, 192.xxx.xxx.24, 192.xxx.xxx.26, 192.xxx.xxx.70, 192.xxx.xxx.89, 192.xxx.xxx.115, **192.xxx.xxx.124**, 192.xxx.xxx.185, 192.xxx.xxx.186, 192.xxx.xxx.188, 192.xxx.xxx.193, 192.xxx.xxx.195, 192.xxx.xxx.223, 192.xxx.xxx.247, 192.xxx.xxx.248, 192.xxx.xxx.249, 192.xxx.xxx.250, 192.xxx.xxx.251, 192.xxx.xxx.253	23 tcp	Abierto
Ssh	192.xxx.xxx.6, 192.xxx.8, 192.xxx.xxx.10(dns1.lns.com.ec), 192.xxx.xxx.20, 192.xxx.xxx.25(emp.lns.com.ec), 192.xxx.xxx.26, **192.xxx.xxx.30(sin00.xxx.xxx), 192.xxx.xxx.31**, 192.xxx.xxx.85, 192.xxx.xxx.86, 192.xxx.xxx.100, **192.xxx.xxx.124,** 192.xxx.xxx.253, 192.xxx.xxx.254	22 tcp	Abierto
Websm	192.xxx.xxx.8, 192.xxx.xxx.26	9090 tcp	Abierto
wbem http	192.xxx.xxx.7	5988 tcp	Abierto
wbem https	192.xxx.xxx.7	5989 tcp	Abierto
vnc-http	192.xxx.xxx.9, 192.xxx.xxx.41, 192.xxx.xxx.45, 192.xxx.xxx.50, 192.xxx.xxx.52, 192.xxx.xxx.54, 192.xxx.xxx.56, 192.xxx.xxx.58, 192.xxx.xxx.60, 192.xxx.xxx.63, 192.xxx.xxx.67(SEP001C58576AA3.lns.com.ec), 192.xxx.xxx.68, 192.xxx.xxx.76, 192.xxx.xxx.77, 192.xxx.xxx.80, 192.xxx.xxx.84, 192.xxx.xxx.92, 192.xxx.xxx.93, 192.xxx.xxx.95, 192.xxx.xxx.111, 192.xxx.xxx.113, 192.xxx.xxx.116, **192.xxx.xxx.124,** 192.xxx.xxx.131, 192.xxx.xxx.135, 192.xxx.xxx.138, 192.xxx.xxx.xxx(dad00.lns.com.ec)	5800 tcp	Abierto
Vnc	192.xxx.xxx.9, 192.xxx.xxx.41, 192.xxx.xxx.45, 192.xxx.xxx.50, 192.xxx.xxx.52, 192.xxx.xxx.54, 192.xxx.xxx.56, 192.xxx.xxx.58, 192.xxx.xxx.60, 192.xxx.xxx.63, 192.xxx.xxx.67(SEP001C58576AA3.lns.com.ec), 192.xxx.xxx.68, 192.xxx.xxx.76, 192.xxx.xxx.77, 192.xxx.xxx.80, 192.xxx.xxx.84, 192.xxx.xxx.85, 192.xxx.xxx.92, 192.xxx.xxx.93, 192.xxx.xxx.95, 192.xxx.xxx.111, 192.xxx.xxx.113, 192.xxx.xxx.116, **192.xxx.xxx.124,** 192.xxx.xxx.131, 192.xxx.xxx.135, 192.xxx.xxx.138, 192.xxx.xxx.xxx(dad00.lns.com.ec)	5900 tcp	Abierto
Vmware-auth	192.xxx.xxx.27, 192.xxx.xxx.30(sin00.xxx.xxx), 192.xxx.xxx.31, 192.xxx.xxx.32, 192.xxx.xxx.85	902 tcp	Abierto
ttdbserverd	192.xxx.xxx.8, 192.xxx.xxx.26	32770, 32772	Abierto
Time	192.xxx.xxx.8, 192.xxx.xxx.26, **192.xxx.xxx.124**	37 tcp	Abierto
Svrloc	192.xxx.xxx.8, 192.xxx.xxx.26, 192.xxx.xxx.27, 192.xxx.xxx.30(sin00.xxx.xxx), **192.xxx.xxx.31,** 192.xxx.xxx.32, **192.xxx.xxx.124**	427 tcp	Abierto
Status	192.xxx.xxx.8, 192.xxx.xxx.25(emp.lns.com.ec), 192.xxx.xxx.26	32772, 32769, 32771 tcp	Abierto
Soap	192.xxx.xxx.111(clr00.xxx.xxx), 192.xxx.xxx.33, 192.xxx.xxx.254	50006, 14000, 8099 tcp	Abierto

Smux	192.xxx.xxx.8, 192.xxx.xxx.26, **192.xxx.xxx.124**	199 tcp	Abierto
Smtp	192.xxx.xxx.8, 192.xxx.xxx.26, **192.xxx.xxx.124**	25, 587 tcp	Abierto
skype2	192.xxx.xxx.71(SEP001BD4609C8D), 192.xxx.xxx.113	443 tcp	Abierto
Sip	192.xxx.xxx.88, **192.xxx.xxx.124**	5060 tcp	Abierto
sentinelsm	192.xxx.xxx.46, 192.xxx.xxx.55, 192.xxx.xxx.66, 192.xxx.xxx.74, 192.xxx.xxx.78, 192.xxx.xxx.94, 192.xxx.xxx.121, **192.xxx.xxx.124**	1947 tcp	Abierto
rpcbind	192.xxx.xxx.8, 192.xxx.xxx.10(dns1.lns.com.ec), 192.xxx.xxx.25(emp.lns.com.ec), 192.xxx.xxx.26, 192.xxx.xxx.85, **192.xxx.xxx.124**, 192.xxx.xxx.181	111 tcp	Abierto
printer	192.xxx.xxx.70, 192.xxx.xxx.79, 192.xxx.xxx.89, 192.xxx.xxx.115, **192.xxx.xxx.124,** 192.xxx.xxx.179, 192.xxx.xxx.185, 192.xxx.xxx.186, 192.xxx.xxx.188, 192.xxx.xxx.193, 192.xxx.xxx.195, 192.xxx.xxx.198, 192.xxx.xxx.199	515 tcp	Abierto
oracle-tns	192.xxx.xxx.8, 192.xxx.xxx.26, 192.xxx.xxx.56	1521 tcp	Abierto
Oracle	**192.xxx.xxx.124**	1521 tcp	Cerrado
Nfs	192.xxx.xxx.8, 192.xxx.xxx.26, **192.xxx.xxx.124**	2049 tcp	Abierto
ncacn_http	192.xxx.xxx.xxx(dad00.lns.com.ec)	49158, 593 tcp	Abierto
Mysql	192.xxx.xxx.25(emp.lns.com.ec), **192.xxx.xxx.124,** 192.xxx.xxx.135	3306 tcp	Abierto
Mysql	**192.xxx.xxx.124**	1112	Desconocido
ms-wbt-server	192.xxx.xxx.2, 192.xxx.xxx.3, 192.xxx.xxx.4, 192.xxx.xxx.5, 192.xxx.xxx.7, 192.xxx.xxx.16(mansis.xxx.xxx), 192.xxx.xxx.28(sts03.xxx.xxx), 192.xxx.xxx.33, 192.xxx.xxx.34(sts02.xxx.xxx), 192.xxx.xxx.52, 192.xxx.xxx.56, **192.xxx.xxx.65(SEP0026CBBDEA63.lns.com.ec),** 192.xxx.xxx.113, **192.xxx.xxx.124,** 192.xxx.xxx.131, 192.xxx.201135, 192.xxx.201145, 192.xxx.201155, 192.xxx.xxx.xxx(dad00.lns.com.ec)	3389	Abierto
Login	192.xxx.xxx.8, 192.xxx.xxx.26, **192.xxx.xxx.124,** 192.xxx.xxx81	513 tcp	Abierto
Ldap	192.xxx.xxx.124, 192.xxx.xxx.xxx(dad00.lns.com.ec)	389, 3268 tcp	Abierto
kerberos-sec	192.xxx.xxx.46, 192.xxx.xxx.55, 192.xxx.xxx.66, 192.xxx.xxx74, 192.xxx.xxx.94, 192.xxx.xxx.105, 192.xxx.xxx.121, **192.xxx.xxx.124,** 192.xxx.xxx.xxx(dad00.lns.com.ec)	88 tcp	Abierto
isakmp	**192.xxx.xxx.124**, 192.xxx.xxx.254	500 tcp	Abierto
http-proxy	192.xxx.xxx.25(emp.lns.com.ec), **192.xxx.xxx.31, 192.xxx.xxx. 124**	8080 tcp	Abierto
http-alt	192.xxx.xxx.27, 192.xxx.xxx.30(sin00.xxx.xxx), 192.xxx.xxx.31, 192.xxx.xxx.32, **192.xxx.xxx.124**	8000 tcp	Abierto
ftp	192.xxx.xxx.8, 192.xxx.xxx.25(emp.lns.com.ec), 192.xxx.xxx.26, 192.xxx.xxx.46, 192.xxx.xxx.63, 192.xxx.xxx.70, 192.xxx.xxx.89, 192.xxx.xxx.115, **192.xxx.xxx.124,** 192.xxx.xxx.185, 192.xxx.xxx.186, 192.xxx.xxx.188, 192.xxx.xxx.193, 192.xxx.xxx.195	21 tcp	Abierto
flexlm	192.xxx.xxx.11(clr00.xxx.xxx)	27000, 1070 tcp	Abierto
domain	192.xxx.xxx.10(dns1.lns.com.ec), **192.xxx.xxx.124,** 192.xxx.xxx.xxx(dad00.lns.com.ec)	53 tcp	

3.3. Detección de sistemas operativos.

Otro objetivo de la fase de exploración es la detección del tipo de sistema operativo, ya que esto determinará qué tipo de ataque será utilizado. Existen varias formas de determinar el sistema operativo, ya sea mediante Telnet Banner, FTP servers, TCP/IP stack fingerprinting, TCP initial sequence number sampling. Con un escaneo de puestos también se puede obtener tipo y versión del sistema operativo de los hosts, detalles del DNS, que servicios de red que están corriendo; como pueden ser FTP, email e incluso inicios de sesión remotos en los host objetivos.

Es por eso que para la detección de sistemas operativos se ha utilizado el comando nmap –sV –O de las redes objetivo.

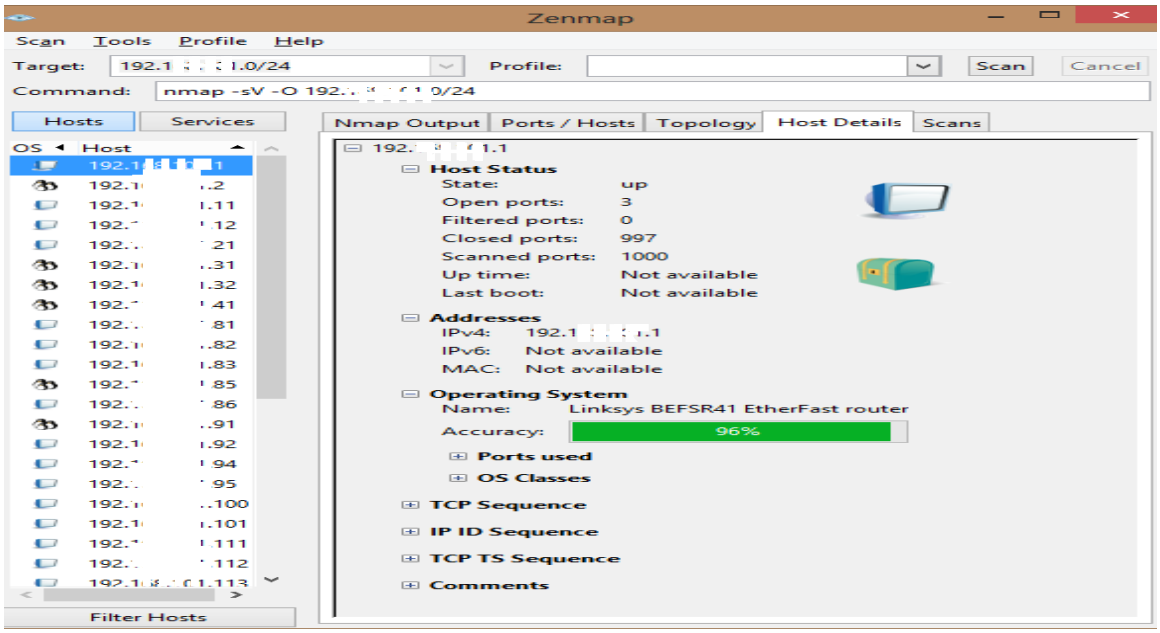


Figura 3-3 Detección de sistemas operativos mediante Nmap -sV –O

Tabla 3-5 Sistemas operativos encontrados en los host activos de la red 192.xxx.xxx.0/24.

Sistema Operativo	IP	Dispositivo
Linksys BEFSR41 EtherFast router Cisco IP Phone CP-7900G-series sshd(protocol 2.0)	192.xxx.xxx.1, 192.xxx.xxx.11, 192.xxx.xxx.12, 192.xxx.xxx.21, 192.xxx.xxx.81, 192.xxx.xxx.82 192.xxx.xxx.86, 192.xxx.xxx.92, 192.xxx.xxx.94, 192.xxx.xxx.95, 192.xxx.xxx.100, 192.xxx.xxx.111 192.xxx.xxx.112, 192.xxx.xxx.121, 192.xxx.xxx.122, 192.xxx.xxx.141, 192.xxx.xxx.142, 192.xxx.xxx.143, 192.xxx.xxx.151, 192.xxx.xxx.xxx, 192.xxx.xxx.202, 192.xxx.xxx.205	Teléfonos Cisco

Logitech Alert 750i camera(Linux 2.6.18)	192.xxx.xxx.2	Cámara IP
Linux 2.6.16 – 2.6.28	192.xxx.xxx.31,192.xxx.xxx.32, 192.xxx.xxx.41, 192.xxx.xxx.85, 192.xxx.xxx.91	PC
Xerox WorkCentre Pro 7245 printer	192.xxx.xxx.83	Impresora
Efficient Networks SpeedStream 4100 ADSL router	192.xxx.xxx.xxx, 192.xxx.xxx.204	Router
AVtech Room Alert 26W enviromental monitor	192.xxx.xxx.113, 192.xxx.xxx.114, 192.xxx.xxx.131	
WMware ESXi Server 4.0.1	192.xxx.xxx.250	
Linux 2.6.9 – 2.6.27	192.xxx.xxx.253	
OpenBSD 4.0	192.xxx.xxx.254	

Tabla 3-6 Sistemas operativos Windows encontrados en los host activos de la red 192.xxx.xxx.0/24.

WINDOWS	Microsoft Windows XP SP2 o Windows Server 2003 SP1 o SP2	192.xxx.xxx.2, 192.xxx.xxx.5, 192.xxx.xxx.7, 192.xxx.xxx.39, 192.xxx.xxx.45, 192.xxx.xxx.33, 192.xxx.xxx.155 192.xxx.xxx.11(clr00.xxx.xxx), 192.xxx.xxx.28(sts03.xxx.xxx), 192.xxx.xxx.34(sts02.xxx.xxx)
	Microsoft Windows Vista SP2, Windows 7 SP1, o Windows Server 2008	192.xxx.xxx.3
	Microsoft Windows Vista SP0 o SP1, Windows Server 2008 SP1, o Windows 7	192.xxx.xxx.4, 192.xxx.xxx.56, 192.xxx.xxx.60, 192.xxx.xxx.72, 192.xxx.xxx.78
	Microsoft Windows 7 SP0 – SP1, Windows Server 2008 SP1, o Windows 8	192.xxx.xxx.9, 192.xxx.xxx.68, 192.xxx.xxx.76, 192.xxx.xxx.77, 192.xxx.xxx.80, 192.xxx.xxx.92 192.xxx.xxx.93, 192.xxx.xxx.111, 192.xxx.xxx.113, 192.xxx.xxx.127, 192.xxx.xxx.131, 192.xxx.xxx.138
	Microsoft Windows Server 2003 SP1 o SP2	192.xxx.xxx.16(mansis.xxx.xxx)
	Microsoft Windows XP SP2 o SP3	192.xxx.xxx.41
	Microsoft Windows XP SP2 o SP3, o Windows Server 2003	192.xxx.xxx.45, 192.xxx.xxx.50, 192.xxx.xxx.52, 192.xxx.xxx.58, 192.xxx.xxx.59, 192.xxx.xxx.81, 192.xxx.xxx.75(cueasis.lns.com.ec) 192.xxx.xxx.95, 192.xxx.xxx.116, 192.xxx.xxx.134
	Microsoft Windows 7 Professional	192.xxx.xxx.53, 192.xxx.xxx.122

		192.xxx.xxx.73 (CUEALM.lns.com.ec)
	Microsoft Windows Server 2008 SP2	192.xxx.xxx.65 (SEP0026CBBDEA63.lns.com.ec) 192.xxx.xxx.67 (SEP001C58576AA3.lns.com.ec) 192.xxx.xxx.71 (SEP001BD4609C8D.lns.com.ec) 192.xxx.xxx.84
	Microsoft Windows Vista SP0 – SP2, Windows Server 2008, o Windows 7 Ultimate	192.xxx.xxx.135, 192.xxx.xxx.xxx (dad00.lns.com.ec)

Tabla 3-7 Sistemas operativos Linux encontrados en los host activos de la red 192.xxx.xxx.0/24.

L I N U X	Linux 2.6.9 – 2.6.30	192.xxx.xxx.6, 192.xxx.xxx.10(dns1.lns.com.ec)
	Linux 2.6.18 – 2.6.21	192.xxx.xxx.20
	Linux 2.6.5 – 2.6.12	192.xxx.xxx.25
	Tomato 1.28 (Linux 2.4.20)	192.xxx.xxx.69
	Linux 2.6.32 – 3.6	192.xxx.xxx.85, 192.xxx.xxx.88
	Linux 2.6.13 – 2.6.32	192.xxx.xxx.112
	Linux 2.6.8 – 2.6.12	192.xxx.xxx.214
	Linux 2.6.9 – 2.6.33	192.xxx.xxx.223

Tabla 3-8 Sistemas operativos MAC encontrados en los hosts activos de la red 192.xxx.xxx.0/24.

M A C	Apple Mac OS X 10.5 – 10.6.8 (Leopard –Snow Leopard) (Darwin 9.0.0b5 – 10.8.0) o iOS 4.0 – 4.2.1	192.xxx.xxx.46
	Apple Mac OS X 10.4.8 – 10.4.11 (Tiger) (Darwin 8.8.0 – 8.11.0)	192.xxx.xxx.54
	Apple Mac OS X 10.4.8 – 10.4.11 (Tiger) (Darwin 8.8.0 – 8.11.1)	192.xxx.xxx.63
	Apple Mac OS X 10.7.0 – 10.7.4 (Lion) (Darwin 11.0.0 – 11.4.0)	192.xxx.xxx.66, 192.xxx.xxx.94, 192.xxx.xxx.121
	Apple Mac OS X 10.8.0 – 10.8.2 (Mountain Lion) o iOS 4.4.2 – 6.0.0 (Darwin 11.0.0 – 12.2.0)	192.xxx.xxx.74, 192.xxx.xxx.105

Tabla 3-9 Sistemas operativos Cisco encontrados en la red 192.xxx.xxx.0/24

CISCO	Cisco IP Phone (7911, 7941, 7961, o 7970)	192.xxx.xxx.100
	Cisco 2940 router o 3750 switch(IOS 12.1)	192.xxx.xxx.247, 192.xxx.xxx.248, 192.xxx.xxx.249
	Cisco 2950, 2960, 3550, 3560, 3750, o 4500 switch (IOS 12.1 – 15.0)	192.xxx.xxx.250, 192.xxx.xxx.253
	Cisco 806, 1712, 1721, o 2600 router (IOS 12.2 – 12.3)	192.xxx.xxx.251
	Cisco Catalyst Express 500 switch	192.xxx.xxx.252

Tabla 3-10 Sistemas operativos de impresoras HP encontrados en la red 192.xxx.xxx.0/24

IMPRESORAS HP	HP LaserJet 2420 printer	192.xxx.xxx.70
	HP LaserJet 2055dn, 2420, P3005, CP4005, 4250, o P4014 printer	192.xxx.xxx.89, 192.xxx.xxx.115, 192.xxx.xxx.193, 192.xxx.xxx.195
	HP LaserJet CP2025dn o P2035n printer	192.xxx.xxx.179, 192.xxx.xxx.199
	HP ProCurve 2524 switch o 9100c Digital Sender printer	192.xxx.xxx.181
	HP JetDirect 635n print server	192.xxx.xxx.185, 192.xxx.xxx.186
	HP LasertJet 3800, 4250, 4345, 9040 printer	192.xxx.xxx.188
	HP LaserJet CMxxx7 o P2015 printer	192.xxx.xxx.198

Tabla 3-11 Otros Sistemas operativos encontrados en los host activos de la red 192.xxx.xxx.0/24.

OTROS SO	Wireless broadband router (3Com OfficeConnect 3CRWDR100A-72, Philips SNB6500, Sinus 154, SMC SMCWEBT-G, o SMC SMCWBR14-G2)	192.xxx.xxx.12
	British Gas GS-Z3 data logger	192.xxx.xxx.15
	Satel ETHM-2 intruder alarm	192.xxx.xxx.22
	VxWorks 6.5 (NAS device)	192.xxx.xxx.23, 192.xxx.xxx.24
	VMware ESXi Server 5.0	192.xxx.xxx.27, 192.xxx.xxx.31, 192.xxx.xxx.30(sin00.xxx.xxx)

	FreeNAS 0.68(FreeBSD 6.2-RELEASE) o VMware ESXi Server 3.0 – 4.0	192.xxx.xxx.32
	Mitel 3300 CXi VoIP PBX	192.xxx.xxx.79
	AVM FRITZ!Box FON WLAN 7240 WAP	192.xxx.xxx.86
	Sony Bravia KDL-46HS720 Tv	192.xxx.xxx.254

3.4. Exploración de la aplicación web.

En la fase de descubrimiento ya habíamos obtenido algo de información relacionada a la aplicación web, pero es importante recalcar que existe una gran diferencia entre ambos procesos, en la fase de descubrimiento obtuvimos toda la información posible de forma no intrusiva haciendo uso de la observación, del sentido común y de una que otra herramienta que recopilaba datos públicos, pero en la fase de exploración se busca recopilar información mucho más detallada, por lo que realizaremos un escaneo completo al portal web de la empresa buscando posibles fallos, ya sea en el código o en la implementación.

Para este proceso nos basaremos en el proyecto OWASP de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro, para ello usaremos la herramienta ZAP que es basada en el proyecto OWASP, de forma que nos permitirá realizar un escaneo completo en búsqueda de fallos en el sistema (OWASP, 2014) .[15]

[15] OWASP. (17 de Noviembre de 2014). *owasp.org*. Obtenido de www.owasp.org: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

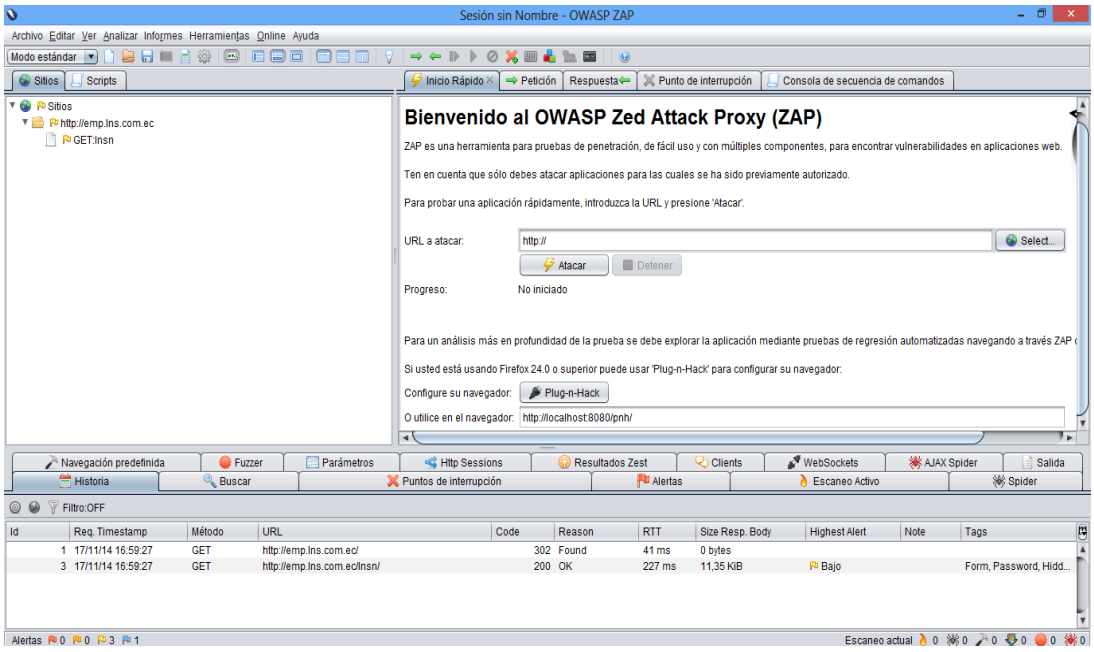


Figura 3-4 Página de inicio del proyecto ZAP

ZAP es una herramienta con un sin número de alternativas, su forma de trabajo es simular un servidor proxy, filtrando y analizando tráfico web a manera de un intermediario entre el cliente y el servidor, para ello se hará uso de su complemento mediante la instalación de un plugin para Firefox al cual lo obtendremos una vez arrancado el sistema ZAP del URL: http://localhost:8000.

Figura 3-5 Obtención del complemento ZAP para Firefox.

Ahora habilitaremos nuestro complemento y este de manera automática nos dará la configuración del proxy, una vez hecho esto lo siguiente será ingresar al sitio web y navegar por él, haciendo uso de todas las opciones que nos provea el sitio, como:

- Navegación por menús.
- Navegación entre vínculos.
- Pruebas de logueo.

- Creación de usuarios.
- Pruebas de impresión.
- Recuperación de usuarios y contraseñas.
- Navegación entre imágenes, etc.

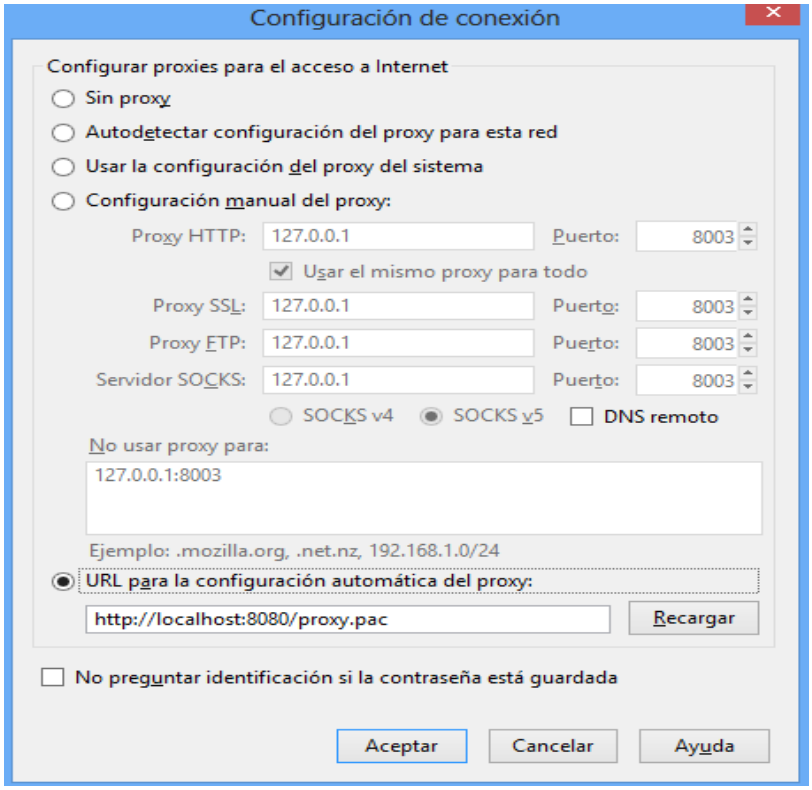
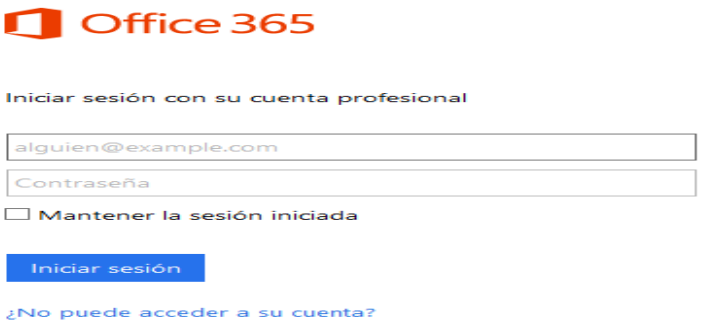
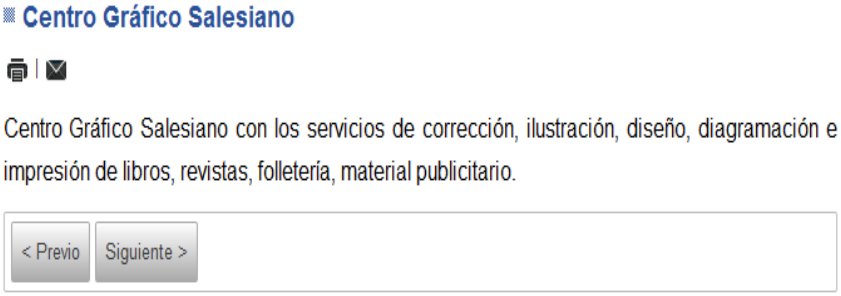


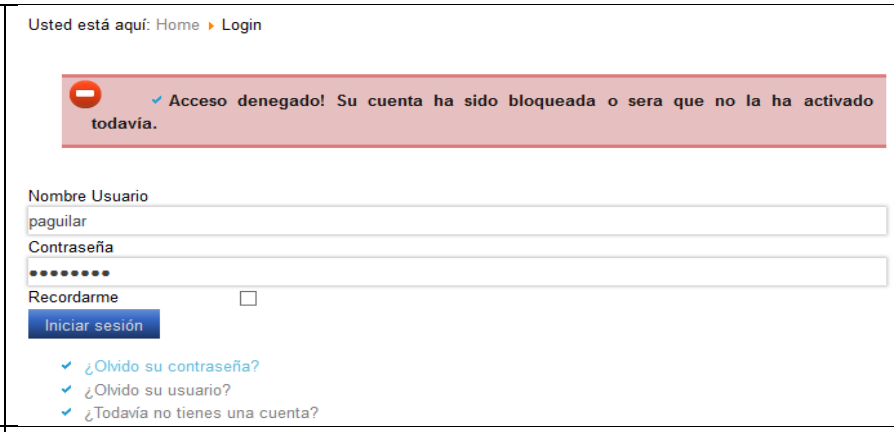
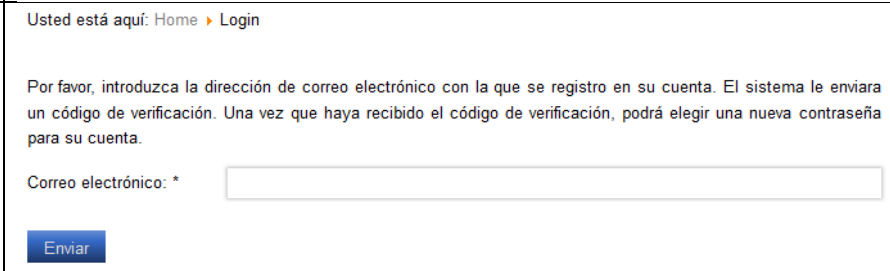
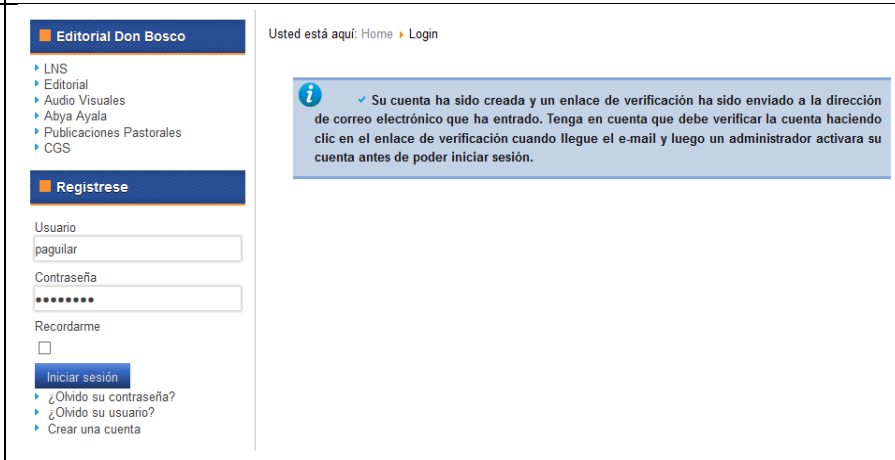
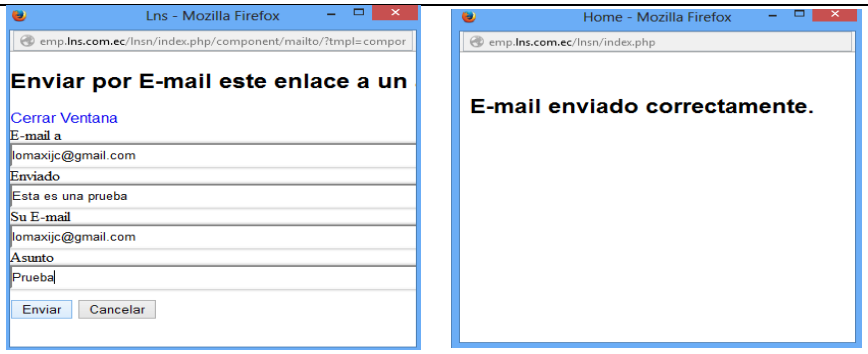
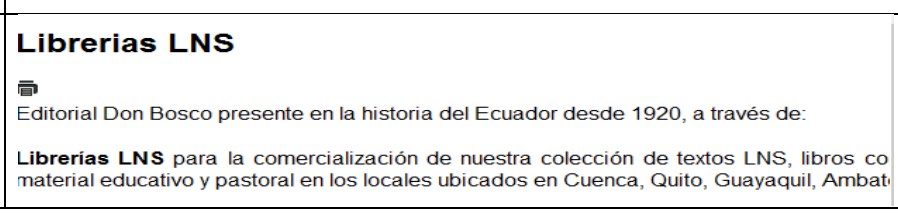
Figura 3-6 Configuración del proxy.

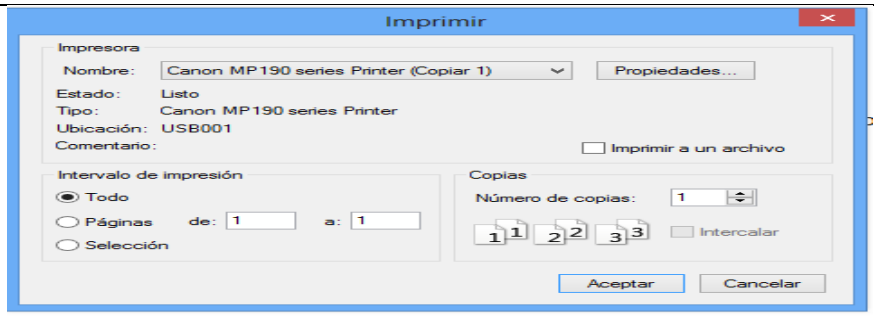
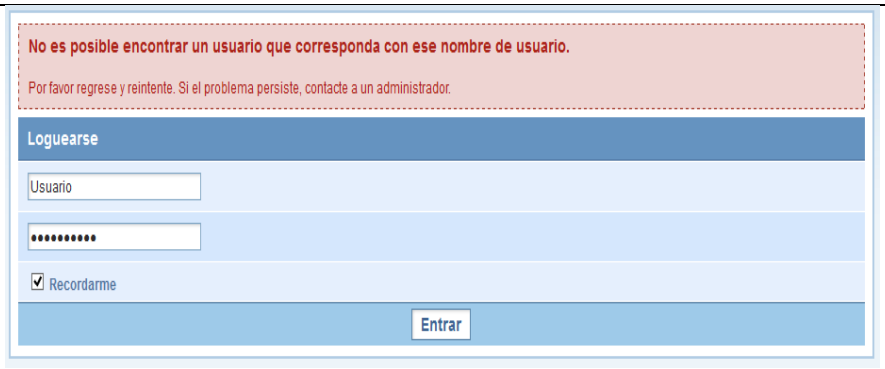
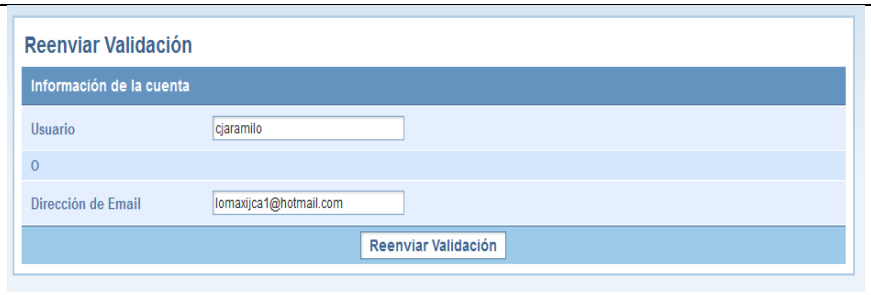
En este proceso es importante hacer uso en lo posible de todo lo que disponga el sitio puesto que de ello dependerá el éxito de la exploración, a manera que se avance en la navegación por la página web, ZAP ira creando directorios con rutas de los posibles objetivos a ser escaneados, a continuación se muestra una tabla con los accesos a cada contenido de la página.

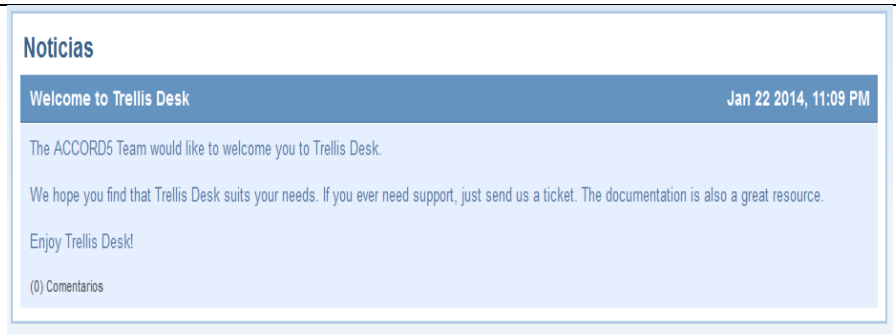
Tabla 3-12 Componentes Web explorados.

DESCRIPCIÓN	CAPTURA
Navegación de menús	Home | Centro de Ayuda | Agenda Telefonica | Correo

Centro De Ayuda	
Directorio Telefónico	
Correo Electrónico	
Centro Gráfico Salesiano	

Logueo De Usuarios	
Recuperación de contraseñas y cuentas de usuarios.	
Creación de cuentas de usuarios	
Envió de e-mail	
Pruebas de impresión	

	
Logueo de usuarios Helpdesk	
Creación de usuarios Helpdesk	
Foros Helpdesk	
Validación Tickets	

Noticias Helpdesk	

Como se había indicado una vez realizada la exploración, ZAP creará directorios para cada posible objetivo, permitiéndonos de esta manera ir a cada uno de ellos y obtener información de cada componente escaneado.

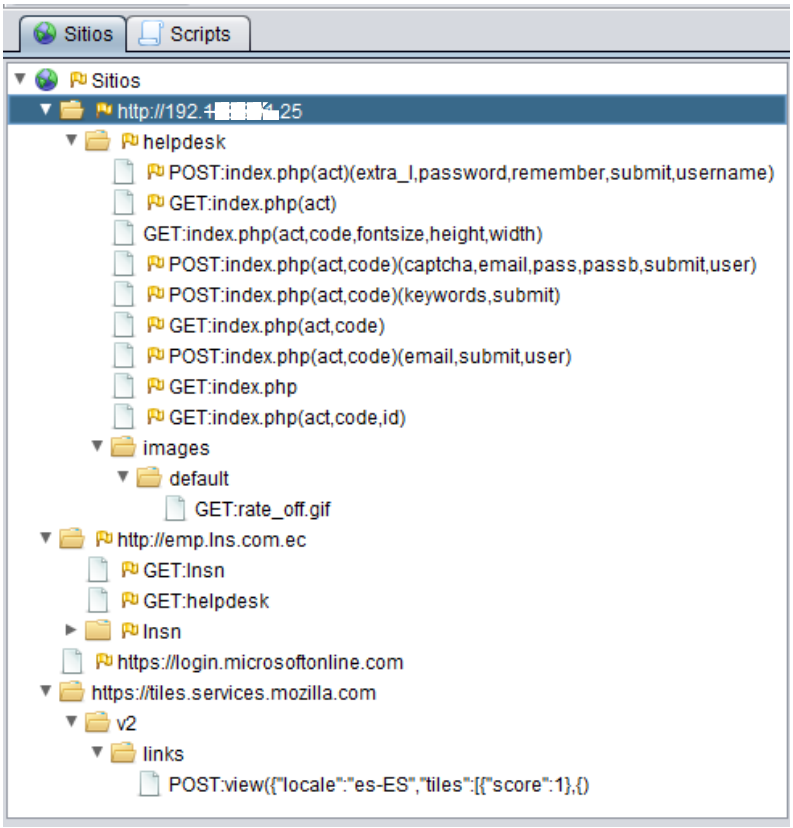


Figura 3-7 Directorio creado por ZAP.

Haciendo uso de ZAP de OWASP se ha podido recopilar la siguiente información del proceso de exploración, permitiéndonos así delimitar mucho más nuestros objetivos,

de esta forma vemos cómo vamos delimitando nuestra área de intrusión. En la siguiente tabla se resume los resultados obtenidos con este proceso. (OWASP, 2014)[16]

Tabla 3-13 Resultados de la exploración Web

ESCANEO DEL SITIO WWW.EMP.LNS.COM.EC	
POSIBLES OBJETIVOS PARA INYECCIÓN SQL	
Dominios	**Link del objetivo**
192.xxx.xxx.25 (Help Desk)	http://192.xxx.xxx.25/helpdesk/index.php?act=article&code=view&id=1+AND+1%3D1+--+
	http://192.xxx.xxx.25/helpdesk/index.php?act=tickets&code=open+AND+1%3D1+--+
	http://192.xxx.xxx.25/helpdesk/index.php?act=kb&code=search
	http://192.xxx.xxx.25/helpdesk/index.php?act=login
	http://192.xxx.xxx.25/helpdesk/index.php?act=login
	http://192.xxx.xxx.25/helpdesk/index.php?act=login
	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=new
PUBLICACIÓN DE DIRECTORIOS DE CONFIGURACIÓN	
emp.lns.com.ec	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/css/
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/js/
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/default/
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/orman/
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/pascal/
COOKIE ACCESIBLE POR JAVA CRIPT	
192.xxx.xxx.25 (Help Desk)	http://192.xxx.xxx.25/helpdesk/index.php
	http://192.xxx.xxx.25/helpdesk/index.php?act=article&code=view&id=1
	http://192.xxx.xxx.25/helpdesk/index.php?act=kb
	http://192.xxx.xxx.25/helpdesk/index.php?act=myaccount
	http://192.xxx.xxx.25/helpdesk/index.php?act=news
	http://192.xxx.xxx.25/helpdesk/index.php?act=portal
	http://192.xxx.xxx.25/helpdesk/index.php?act=register
	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=sendval
	http://192.xxx.xxx.25/helpdesk/index.php?act=tickets&code=history
	http://192.xxx.xxx.25/helpdesk/index.php?act=tickets&code=open
	http://192.xxx.xxx.25/helpdesk/index.php?act=kb&code=search
	http://192.xxx.xxx.25/helpdesk/index.php?act=kb&code=search
	http://192.xxx.xxx.25/helpdesk/index.php?act=login
	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=dosendval
	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=new
emp.lns.com.ec	http://emp.lns.com.ec/helpdesk/
ACCESO A SCRIPTS DESDE TERCEROS	
emp.lns.com.ec	http://emp.lns.com.ec/helpdesk/
USO DEL AUTOCOMPLETAR EN EL LOGUEO	
192.xxx.xxx.25 (Help Desk)	http://192.xxx.xxx.25/helpdesk/index.php
	http://192.xxx.xxx.25/helpdesk/index.php?act=article&code=view&id=1

[16] OWASP. (13 de Marzo de 2014). *www.owasp.org*. Obtenido de OWASP Joomla Vulnerability Scanner Project: https://www.owasp.org/index.php?title=Category:OWASP_Joomla_Vulnerability_Scanner_Project&setlang=es

	http://192.xxx.xxx.25/helpdesk/index.php?act=kb
	http://192.xxx.xxx.25/helpdesk/index.php?act=myaccount
	http://192.xxx.xxx.25/helpdesk/index.php?act=news
	http://192.xxx.xxx.25/helpdesk/index.php?act=portal
	http://192.xxx.xxx.25/helpdesk/index.php?act=register
	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=sendval
	http://192.xxx.xxx.25/helpdesk/index.php?act=tickets&code=history
	http://192.xxx.xxx.25/helpdesk/index.php?act=tickets&code=open
	http://192.xxx.xxx.25/helpdesk/index.php?act=kb&code=search
	http://192.xxx.xxx.25/helpdesk/index.php?act=login
	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=new
emp.lns.com.ec	http://emp.lns.com.ec/helpdesk/
	http://emp.lns.com.ec/lnsn/
	http://emp.lns.com.ec/lnsn/index.php/2014-01-28-13-04-54
	http://emp.lns.com.ec/lnsn/index.php/2014-01-28-13-05-40
	http://emp.lns.com.ec/lnsn/index.php/getting-started
	http://emp.lns.com.ec/lnsn/index.php/index.php
	http://emp.lns.com.ec/lnsn/index.php/joomlaorg
	http://emp.lns.com.ec/lnsn/index.php/login
	http://emp.lns.com.ec/lnsn/index.php/login?view=registration
	http://emp.lns.com.ec/lnsn/index.php/login?view=registration&layout=complete
	http://emp.lns.com.ec/lnsn/index.php/login?view=remind
	http://emp.lns.com.ec/lnsn/index.php/login?view=reset
	http://emp.lns.com.ec/lnsn/index.php/the-joomla-project
	http://emp.lns.com.ec/lnsn/index.php/using-joomla
DIRECCIONES IP EN RESPUESTAS HTTP	
192.xxx.xxx.25 (Help Desk)	http://192.xxx.xxx.25/helpdesk/index.php
	http://192.xxx.xxx.25/helpdesk/index.php?act=article&code=view&id=1
	http://192.xxx.xxx.25/helpdesk/index.php?act=kb
	http://192.xxx.xxx.25/helpdesk/index.php?act=myaccount
	http://192.xxx.xxx.25/helpdesk/index.php?act=news
	http://192.xxx.xxx.25/helpdesk/index.php?act=portal
	http://192.xxx.xxx.25/helpdesk/index.php?act=register
	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=sendval
	http://192.xxx.xxx.25/helpdesk/index.php?act=tickets&code=history
	http://192.xxx.xxx.25/helpdesk/index.php?act=tickets&code=open
	http://192.xxx.xxx.25/helpdesk/index.php?act=kb&code=search
	http://192.xxx.xxx.25/helpdesk/index.php?act=login
	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=dosendval
	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=new
emp.lns.com.ec	http://emp.lns.com.ec/helpdesk/
PROTECCIÓN XSS NO HABILITADA EN NAVEGADOR WEB	
192.xxx.xxx.25 (Help Desk)	http://192.xxx.xxx.25/helpdesk/index.php
	http://192.xxx.xxx.25/helpdesk/index.php?act=article&code=view&id=1
	http://192.xxx.xxx.25/helpdesk/index.php?act=kb
	http://192.xxx.xxx.25/helpdesk/index.php?act=myaccount
	http://192.xxx.xxx.25/helpdesk/index.php?act=news
	http://192.xxx.xxx.25/helpdesk/index.php?act=portal
	http://192.xxx.xxx.25/helpdesk/index.php?act=register
	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=sendval
	http://192.xxx.xxx.25/helpdesk/index.php?act=tickets&code=history
	http://192.xxx.xxx.25/helpdesk/index.php?act=tickets&code=open

emp.lns.com.ec	http://emp.lns.com.ec/helpdesk/
	http://emp.lns.com.ec/lnsn/
	http://emp.lns.com.ec/lnsn/index.php/2014-01-28-13-04-54
	http://emp.lns.com.ec/lnsn/index.php/2014-01-28-13-05-40
	http://emp.lns.com.ec/lnsn/index.php/component/mailto/?tmpl=component&template=emailmarketing_22&link=abfb5323dcb7d3fecfcd20663e69b67ce90d7596
	http://emp.lns.com.ec/lnsn/index.php/getting-started
	http://emp.lns.com.ec/lnsn/index.php/getting-started?tmpl=component&print=1&page=
	http://emp.lns.com.ec/lnsn/index.php/index.php
	http://emp.lns.com.ec/lnsn/index.php/joomlaorg
	http://emp.lns.com.ec/lnsn/index.php/login
	http://emp.lns.com.ec/lnsn/index.php/login?view=registration
	http://emp.lns.com.ec/lnsn/index.php/login?view=registration&layout=complete
	http://emp.lns.com.ec/lnsn/index.php/login?view=remind
	http://emp.lns.com.ec/lnsn/index.php/login?view=reset
	http://emp.lns.com.ec/lnsn/index.php/the-joomla-project
	http://emp.lns.com.ec/lnsn/index.php/using-joomla
	http://emp.lns.com.ec/lnsn/media/system/css/system.css
	http://emp.lns.com.ec/lnsn/media/system/js/caption.js
	http://emp.lns.com.ec/lnsn/media/system/js/core.js
	http://emp.lns.com.ec/lnsn/media/system/js/mootools-core.js
	http://emp.lns.com.ec/lnsn/media/system/js/mootools-more.js
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/css/nivo-slider.css
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/css/style.css
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/css/template.css
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/css/template.responsive.css
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/jquery.js
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/js/jquery-1.6.1.min.js
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/js/jquery.nivo.slider.pack.js
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/js/scroling.js
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/script.js
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/script.responsive.js
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/default/default.css
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/orman/orman.css
	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/pascal/pascal.css
	http://emp.lns.com.ec/lnsn/templates/system/css/general.css
	http://emp.lns.com.ec/lnsn/templates/system/css/system.css
	http://emp.lns.com.ec/lnsn/index.php

3.5. Evasión de IPS

Un IPS (Sistema de prevención de Intrusos), es un mecanismo dedicado a la prevención de intrusiones a partir de la identificación y bloqueo de patrones específicos, donde sus funciones principales son: identificar la actividad maliciosa, registrar información sobre dicha actividad, intentar bloquear o parar la actividad, y generación del reporte de dichas actividades. (Ditech , 2010)[17]

Los IPS trabajan a nivel de la capa 7, tiene la capacidad de descifrar protocolos como HTTP, FTP y SMTP, algunos IPS permiten establecer reglas de control de acceso (ACL), buscan anomalías a nivel del sistema operativo, comprueban los módulos cargados por el núcleo, monitorean la actividad del sistema de archivos, monitorean la actividad de la red (LAN, WLAN) para identificar amenazas que generan flujos de tráficos inusuales, para ello un IPS puede basarse en firmas digitales, estadísticas de detección o en el análisis de protocolos.

Como se puede ver un IPS es un mecanismo de detección que tiene la capacidad de restringir el acceso de cualquier tipo de tráfico que sea visto como una amenaza o como algo inusual, por lo cual es importante poner a prueba el nuestro IPS considerándolo como el corazón de la red en cuanto a la seguridad y determinar cuan vulnerable puede ser, para esto aremos uso de diferentes técnicas que nos permitirán lograr evadir el IPS y asegurar una entrada para nuestros ataques, entre los más usuales tenesmos:

Ofuscación. Es el proceso de ocultar o dificultar el acceso a la información mediante técnicas de camuflaje, encriptación, compresión, etc. Cuando se trata de un pentest se habla de una técnica para ocultar el flujo de control del software, así como la estructura de datos que contienen información sensible. Simplemente hablando, la ofuscación es el proceso de tomar una cadena de caracteres legibles, y convirtiéndolo en algo que no se puede leer (ofuscado). Esta técnica es muy usada por los atacantes para ocultar actividades maliciosas en código ejecutable. (Fuente, 2013)[18]

[17] Ditech . (2010). *ditech.com.co*. Obtenido de ditech.com.co: http://ditech.com.co/soluciones-integrales/seguridad-informatica-en-redes/revencion-de-intrusos-ips/

[18] Fuente, R. C. (2013). *Virus Cascade.* Madrid: Universidad Complutense de Madrid.

Con el tiempo han aparecido diferentes técnicas de ofuscación de código malicioso entre las más comunes y más usadas tenemos:

- **Cifrado**. Un virus cifrado posee un bucle de cifrado y el cuerpo principal o bucle de descifrado, el cual constituye en un fragmento de código que cifra o descifra el código del cuerpo principal, donde el cuerpo principal es el código real del malware cifrado. En este caso cuando el virus empieza a actuar en el huésped el bucle descifrador debe decodificar el cuerpo principal, de esta forma un IPS o un antivirus no puede detectar inmediatamente la amenaza debido a que primero necesita descifrar el cuerpo del virus para analizarlo y determinar que es potencialmente peligroso.

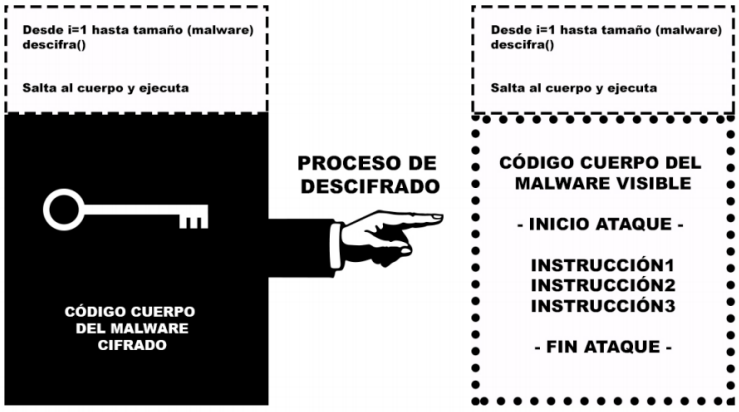


Figura 3-8 Cifrado de Malware

Fuente: *(Fuente, 2013, pág. 8)*[19]

- **Oligomorfismos**. Constituye en una forma avanzada de cifrado la cual contiene una colección de descifradores diferentes, que son elegidos al azar para cada nueva víctima de tal forma que el código descifrador sea siempre diferente para cada víctima.

[19] Fuente, R. C. (2013). *Virus Cascade.* Madrid: Universidad Complutense de Madrid.

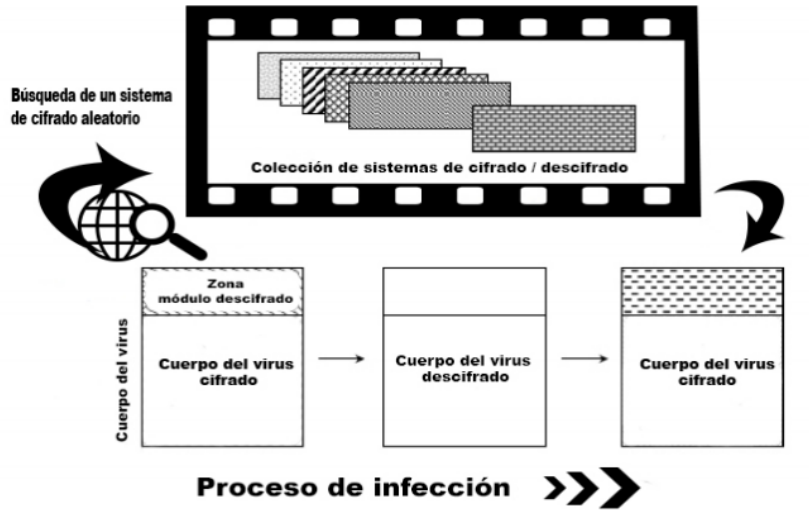


Figura 3-9 Cifrado virus oligomórfico

Fuente: *(Fuente, 2013, pág. 9)*[20]

- **Polimorfismo**. Muy similares a los virus cifrados y oligomórficos, con la única diferencia de que este tipo de virus tienen la capacidad de generar un número ilimitado de nuevos descifradores diferentes, siendo su regla principal modificar el aspectos del código constantemente de una copia a otra, como es de suponer tanto su implementación como su administración suponen ser complicadas.

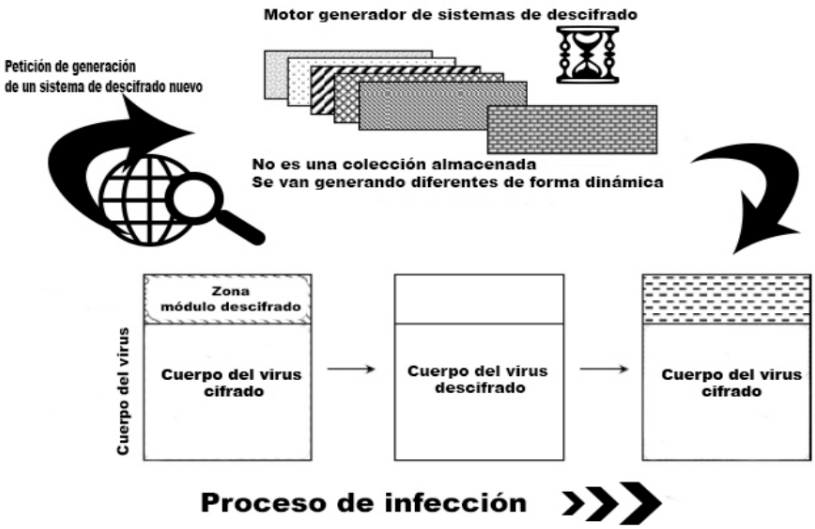


Figura 3-10 Cifrado virus polimórfico

Fuente:*(Fuente, 2013, pág. 10)*

[20] Fuente, R. C. (2013). *Virus Cascade.* Madrid: Universidad Complutense de Madrid.

Cifrado y Tunelización. Esta es otra estrategia que se puede utilizar para evadir un IPS. Básicamente consiste en cifrar el ataque mediante el envío de datos o paquetes a través de una conexión SSH o de un túnel VPN que hace que sea prácticamente imposible que el IPS pueda monitorear y analizar los datos, para esto el IPS tiene que encontrarse en un punto de la red anterior al de la terminación del túnel. Se recalca que este método se lo utiliza cuando se quiere realizar ataques de penetración externos (Michael Dyrmose, 2013, pág. 3). [21]

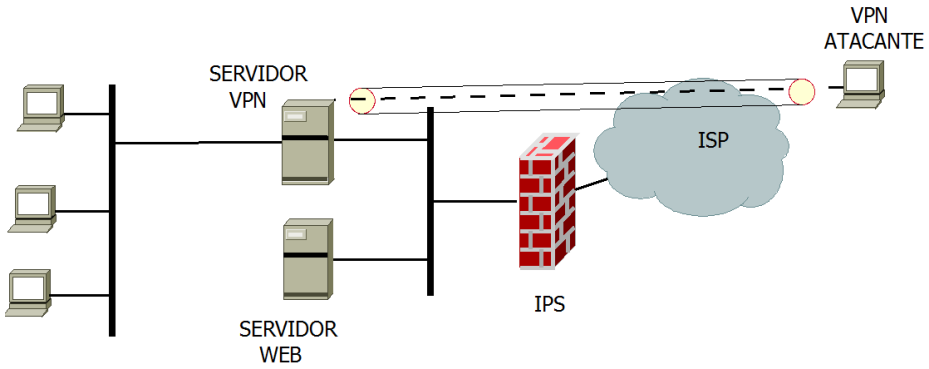


Figura 3-11 Evasión IPS Mediante tunel VPN

Fragmentación. La fragmentación es un mecanismo que permite separar o fragmentar un paquete IP entre varios bloques de datos más pequeños, lo que se hace con esta técnica es dividir a los paquetes maliciosos en fragmentos más pequeños asegurándose que en cada datagrama individualmente no exista la cadena de bytes que identifica el ataque.

El IPS tratará de reensamblar adecuadamente todos los fragmentos para poder analizar correctamente el flujo de datos, pero para ello se debe esperar a recibir todos los datos; de esta manera se puede evadir un IPS, enviandole infinidad de fragmentos parciales, que nunca llegarán a completar un paquete. El IPS albergará en memoria cada fragmento esperando a recibir todas las partes, lo cual se convertirá en un ataque de denegación de servicio (Dos), pero muchos IPS tienen un sistema de tiemeout que consiste en desechar o liberar los paquetes de llegada para evitar la saturación de la memoria, pero al hacer esto abre una brecha para que se filtren paquetes maliciosos y

[21] Michael Dyrmose, S. C. (2013). *Beating the IPS.* Dubex A/S.

de esta forma evadir el IPS (Gil, Evasión de Sistemas de Detección de Intrusos, 2013).[22]

Para iniciar el proceso de evasión de un IPS es importante tener una idea clara de su topología de red de tal manera que se pueda identificar características como: puerta de enlace, ip del dispositivo, ip del atacante e ip de la víctima; toda esta información ya ha sido obtenida previamente en fases anteriores, pero para tener una idea más clara aremos uso del traceroute de NMAP, el cual nos indicará toda esta información de forma gráfica.

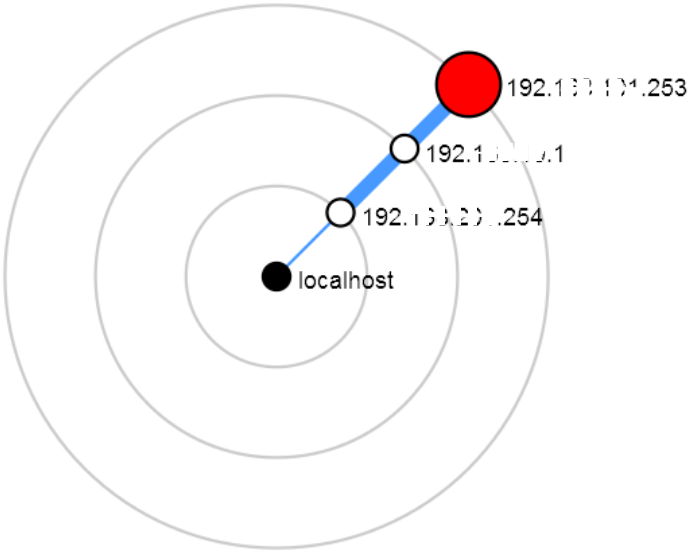


Figura 3-12 Traceroute de NMAP

Partiendo de esto y con la información ates recolectada realizaremos un esquema el cual seguiremos para nuestras pruebas de evasión, teniendo en cuenta que el objetivo es poder demostrar que de alguna manera se puede llegar desde el atacante hasta la victima sea para perpetuar un ataque o simplemente para obtener información confidencial.

[22] Gil, R. G. (2013). *Evasión de Sistemas de Detección de Intrusos.*

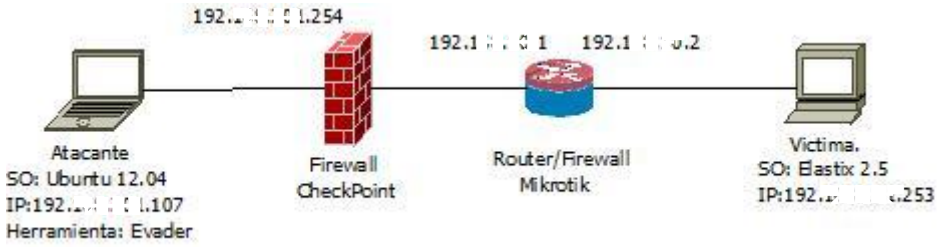


Figura 3-13 Topología a utilizar para la evasión del firewall.

En este caso se recalca que el firewall posee problemas tanto en su implementación como en su configuración por lo cual usar fragmentación de paquetes será más que suficiente para lograr evadir el IPS, pero antes de ello realizaremos una prueba de escaneo de puertos, versiones y sistemas operativos con NMAP y aremos un análisis de los resultados para determinar si se logra evadir o no el IPS.

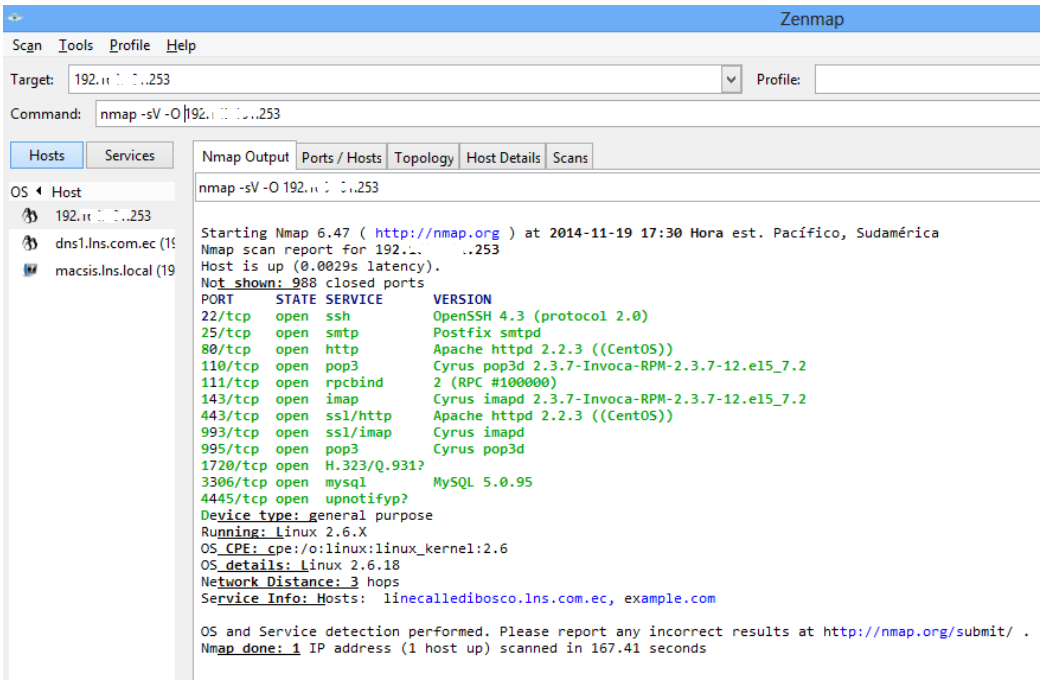


Figura 3-14 Exploración de puertos, versiones y SO

En la figura anterior podemos ver que sin necesidad de realizar la fragmentación de paquetes logramos tener acceso a nuestro objetivo y recopilar información, esto es debido a la incorrecta implementación y configuración del proxy, donde podemos determinar que no existen reglas ni la creación de zonas de seguridad, como son: DMZ, LAN, WLAN, WAN o una simple VLAN.

En la figura 3-15 podemos ver el tráfico capturado al momento de realizar el ataque, donde se identifica y se ve claramente que el tráfico está siendo filtrado, esto debido a que como se muestra hay paquetes que no reciben una respuesta o ACK, lo que indica la presencia de algún firewall (wireshark, 2011).[23]

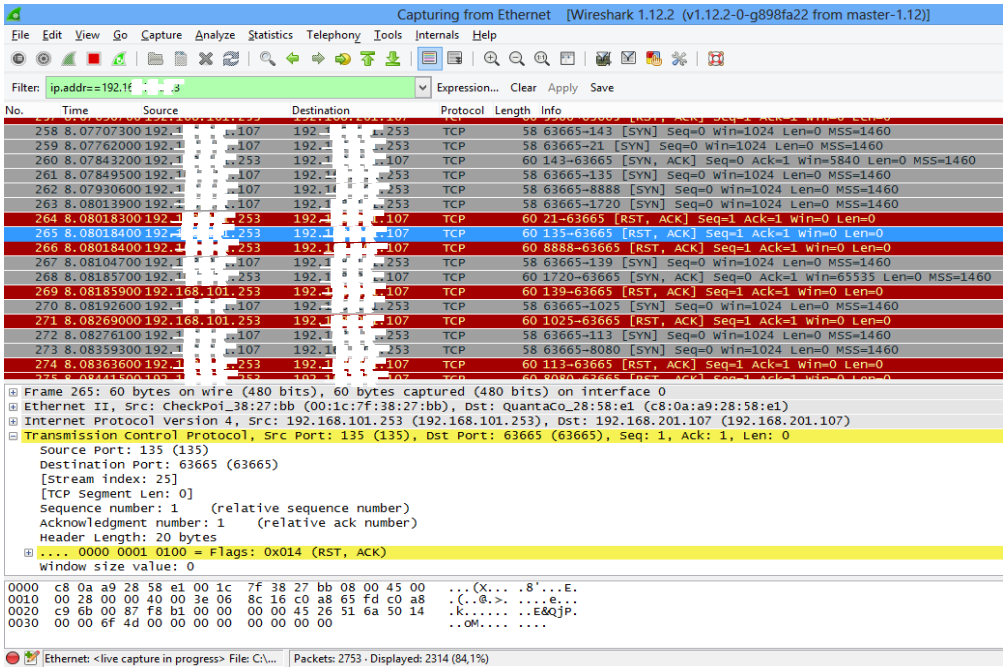


Figura 3-15 Captura del tráfico sin Fragmentación de paquetes.

Una vez comprobado que de alguna manera se nos está realizando un filtrado de paquetes, vamos a proceder a realizar el mismo ataque pero esta vez con la opción –f para filtrado de paquetes y compararemos con los resultados obtenidos anteriormente.

[23] wireshark. (10 de Mayo de 2011). */wiki.wireshark.org/*. Obtenido de wiki.wireshark.org/: http://wiki.wireshark.org/TCP_Analyze_Sequence_Numbers

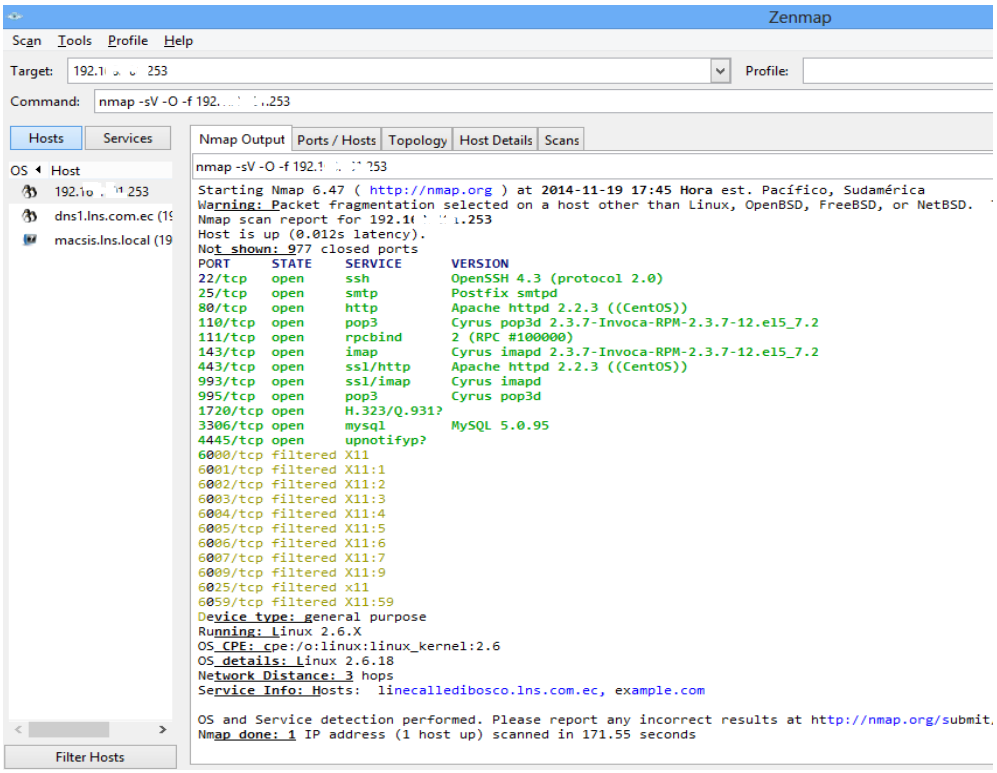


Figura 3-16 Exploración de puertos, versiones y SO con filtrado de paquetes.

En este ataque vemos que ya nos arroja los puertos que están siendo filtrados lo que nos indica que la el ataque ha sido un éxito, ahora analizaremos la captura del tráfico donde vamos a reconocer dos factores primordiales, en primer lugar al ser paquetes fragmentados no loa encontraremos como tráfico TCP si no como ipv4, cuya principal característica será que en la Data sus paquetes no excederán los 8 bytes y además veremos que estos paquetes no están siendo filtrados.

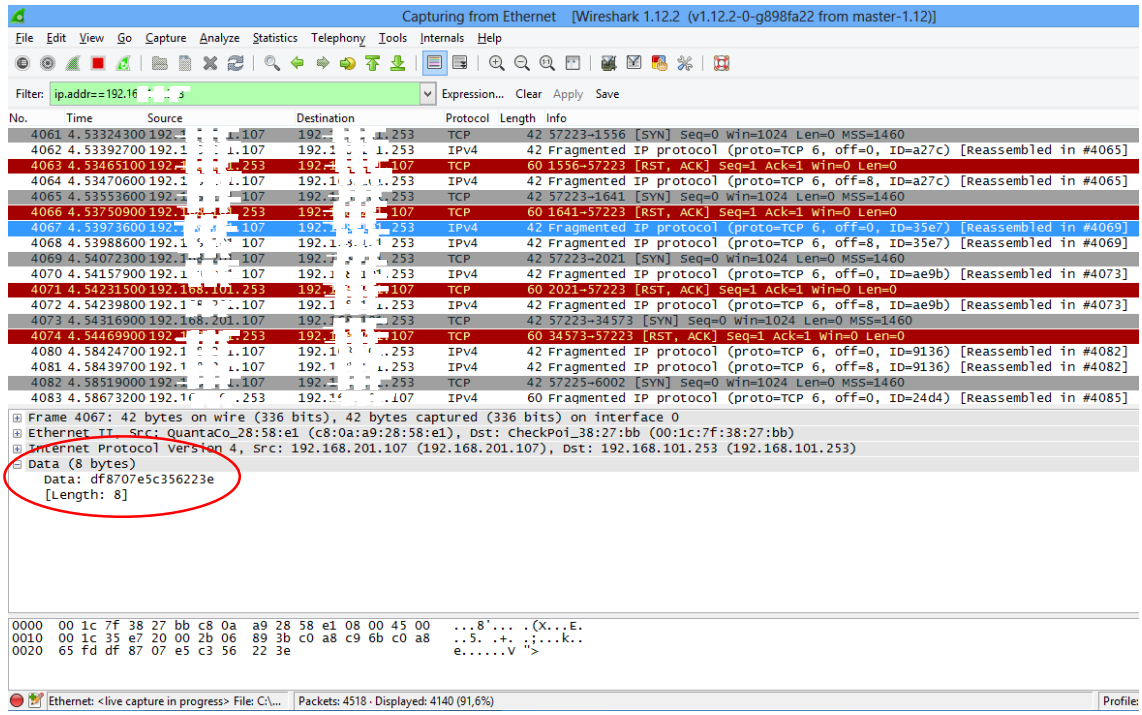


Figura 3-17 Captura del tráfico con fragmentación de paquetes.

3.6. Determinación de mecanismos de encriptación en redes WIFI.

Hay que tomar en cuenta que la empresa cuenta con redes inalámbricas las misma que a más de presentar numerosas ventajas presentan también muchas debilidades es por eso que en esta sección se busca determinar los mecanismos de encriptación de las redes Wifi pertenecientes a la empresa objetivo para así identificar las vulnerabilidades más frecuentes y dar las recomendaciones para generar un nivel de seguridad adecuado en este tipo de redes.

El método consiste en la verificación de acceso a redes WLAN 802.11 las cuales presentan problemas alarmantes de implementación debido a la rápida creación y no se implementan medidas de seguridad si se implementan con la configuración básica.

Un punto muy importante es la configuración de la encriptación, ya que se debe establecer la encriptación más fuerte disponible para el producto, es decir si se escoge protocolos de seguridad de mayor nivel tales como WPA WPA2 se disminuye drásticamente riesgos de explotación de vulnerabilidades.

Antes de empezar con la determinación de los mecanismos de encriptación es necesario conoces las especificaciones de 802.11, el estándar que describe a los productos WLAN:

Tabla 3-14 Especificaciones 802.11

Fuente: (Peter Vincent Herzog, 2003)[24]

Capa Física	Secuencia Directa en Espectro Ensanchado (DSSS), Saltos de Frecuencia en Espectro Ensanchado (FHSS), infrarrojos (IR)
Cifrado por defecto	Algoritmo de cifrado basado en RC4 para confidencialidad, autenticación e integridad. Gestión de claves limitada.
Rango de Operación	150 pies en interiores y 1500 en exterior

A continuación se realiza el escaneo de las redes de la empresa para identificar los mecanismos de encriptación que utilizan.

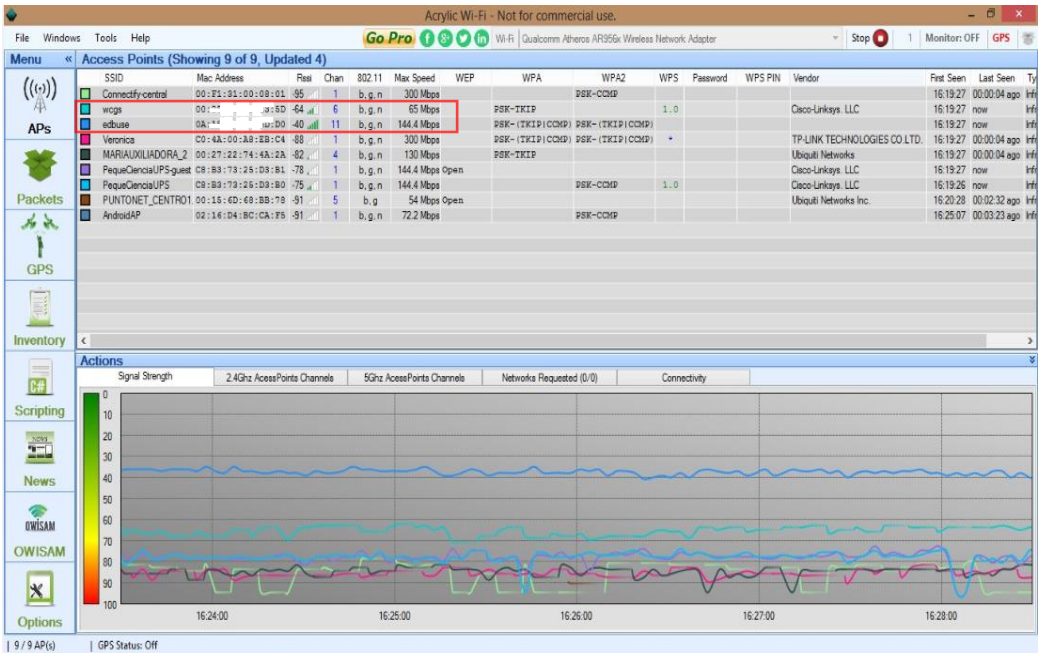


Figura 3-18 Escaneo de las redes inalámbricas de la empresa.

Tabla 3-15 Encriptación utilizada en las redes escaneadas en la empresa

Encriptación	Número de Redes Wifi	SSID
Sin Encriptación	0	
WEP	0	
WPA	1	wcgs
WPA2	1	Edbuse
Total	2	

[24] Peter Vincent Herzog, t. I. (2003). *OSSTMM 2.1*.

Como se puede observar en la tabla 3-15, la empresa utiliza encriptación WPA ya que es una buena opción en cuanto a la seguridad de la red inalámbrica, seguida de WPA2. Lo que significa que los ataques basados en diccionarios resultarían sin éxito.

3.7. Escaneo de Telefonía IP

El escaneo de la red de telefonía IP tiene como objetivo la identificación de dispositivos VoIP para posterior realizar una verificación de la robustez y seguridad de la implementación de la telefonía IP.

Para esto se utiliza la herramienta SiVuS (Sip Vulnerability Scanner) que es un escáner de vulnerabilidades para redes VoIp que usen el protocolo SIP dicho escáner nos permite verificar la seguridad de la implementación del componente SIP.

Dentro de las funcionalidades que presenta esta herramienta está la generación de Mensajes Sip que se utiliza para enviar varios tipos de mensajes a un componente SIP incluso contenido SDP (Session Description Protocol) para demostrar problemas con SIP.

Sin embargo la funcionalidad que nos será de utilidad en este capítulo es aquella que permite el descubrimiento de los componentes SIP ya que la herramienta puede escanear un rango de direcciones IP para identificar los hosts que usan el protocolo SIP. En la Figura 3-19 se muestra esta funcionalidad.

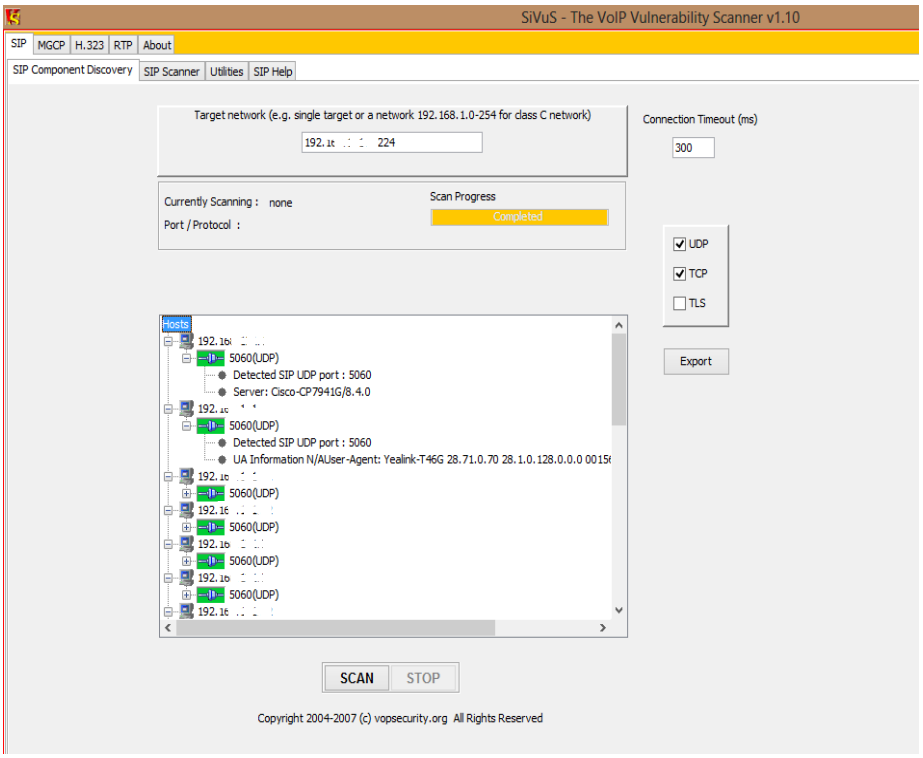


Figura 3-19 Descubrimiento de componentes SIP con SiVuS.

A continuación se presenta la lista de dispositivos que utilizan SIP, de acuerdo al scanning realizado por SiVuS.

Tabla 3-16 Host que usan SIP detectados por SiVuS.

Host que usan SIP		
192.xxx.xxx.1	192.xxx.xxx.86	192.xxx.xxx.131
192.xxx.xxx.2	192.xxx.xxx.91	192.xxx.xxx.141
192.xxx.xxx.11	192.xxx.xxx.92	192.xxx.xxx.142
192.xxx.xxx.12	192.xxx.xxx.95	192.xxx.xxx.143
192.xxx.xxx.21	192.xxx.xxx.100	192.xxx.xxx.151
192.xxx.xxx.31	192.xxx.xxx.xxx	192.xxx.xxx.xxx
192.xxx.xxx.32	192.xxx.xxx.111	192.xxx.xxx.202
192.xxx.xxx.41	192.xxx.xxx.112	192.xxx.xxx.204
192.xxx.xxx.81	192.xxx.xxx.113	192.xxx.xxx.205
192.xxx.xxx.82	192.xxx.xxx.114	192.xxx.xxx.250
192.xxx.xxx.83	192.xxx.xxx.121	192.xxx.xxx.253
192.xxx.xxx.85	192.xxx.xxx.122	192.xxx.xxx.254

Otra funcionalidad que se utilizará en el desarrollo del capítulo 4, es el escáner de vulnerabilidades SIP el mismo que provee una configuración flexible con varias opciones para la verificación de la robustez y seguridad de la implementación SIP.

3.8. Identificación de motores de base de datos.

En este punto se trata de descubrir el Motor de base de datos con el cual trabaja la empresa y no es más que la obtención del **servicio** principal donde se almacena, procesa y protege los datos además proporciona acceso controlado y procesamiento de transacciones rápido para cumplir con los requisitos de las aplicaciones consumidoras de datos más exigentes de la empresa. Entre los principales motores de base de datos tenemos:

Oracle: Es uno de los sistemas de gestión de bases de datos relacional más completos ya que permite realizar transacciones además de ser escalable, estable y soporta multiplataforma. En este caso el Listener, el cual es un proceso servidor que provee la conectividad de red con la base de datos, escucha la conexión en un puerto específico en el servidor de base de datos que por defecto es el 1521. La figura 3-20 muestra el servicio Oracle que especifica el puerto 1521 por lo que se dice que la empresa utiliza el motor de base de datos Oracle.

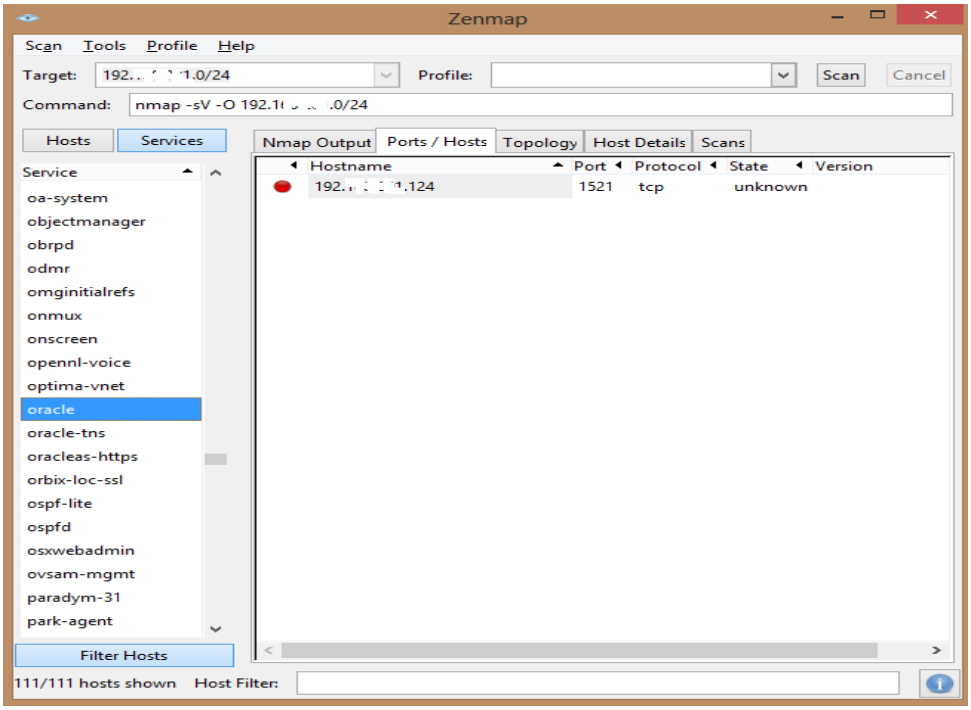


Figura 3-20 Identificación de motor de base de datos Oracle.

Sin embargo por lo que se puede observar en los datos obtenidos en el escaneo de puertos y servicios además de Oracle la empresa cuenta con el motor MySQL.

MySQL: Es un sistema de gestión de base de dato relacional de libre distribución y está disponible para Linux, Windows y otros sistemas operativos, por defecto el servidor MySQL se ejecuta en el puerto 3306 y por ende el cliente se conecta al servidor por dicho puerto.

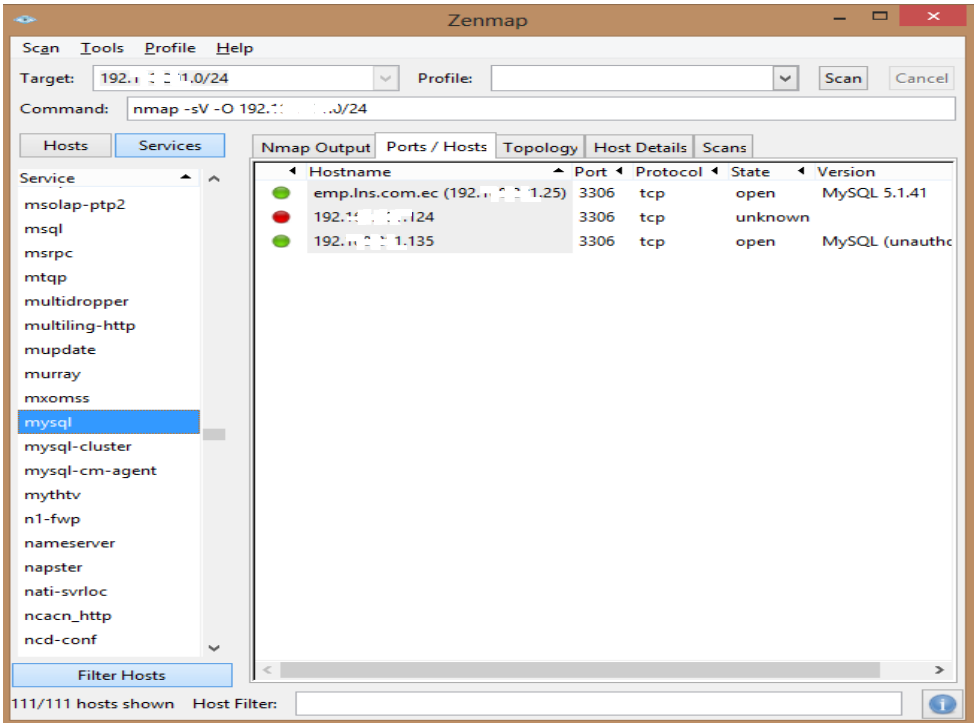


Figura 3-21 Identificación del motor de base de datos MySQL

Por último se identificó también el motor PostgreSQL como se muestra en la figura 3-22.

PostgreSQL: Es un motor de base de datos relacionales, aunque es un poco más lenta que otros motores. Escucha por el puerto 5432.

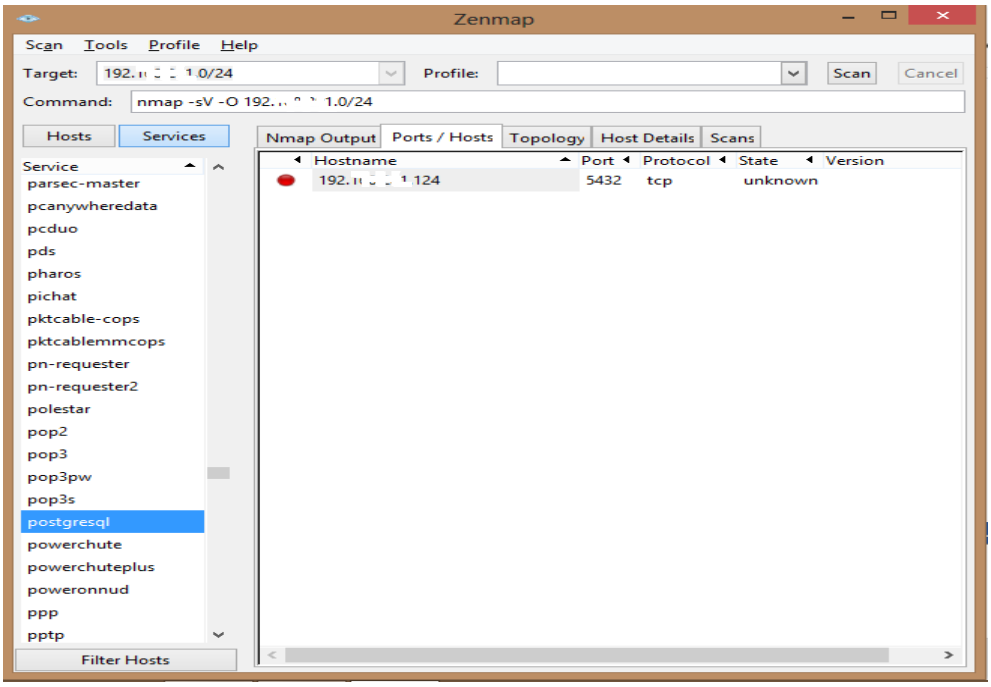


Figura 3-22 Identificación de motor de base de datos Postqresql

CAPÍTULO IV

4. Fase de Evaluación

Se basa en el análisis de todos los datos encontrados para la detección, determinación y clasificación de vulnerabilidades de seguridad informática que afectan a los sistemas evaluados, realizando evaluaciones de seguridad en todos los posibles niveles mediante la ejecución de herramientas de scanning de vulnerabilidades, búsquedas en manuales de vulnerabilidades, enumeración de usuarios y datos de configuración. (Ramos J. L., 2013).[25]

En este proceso se llevarán a cabo las evaluaciones de seguridad de todos los posibles sistemas (DATOS, VOIP, WEB, etc.), destacándose las siguientes tareas:

- Ejecución de herramientas de *scanning* de vulnerabilidades.
- Búsqueda manual de vulnerabilidades.
- Enumeración de usuarios y datos de configuración.

El análisis de vulnerabilidades es un proceso de identificación proactiva de falencias de los sistemas informáticos en una red, generalmente se realiza mediante un escáner donde primero se identifica el sistema operativo y el número de versión, incluyendo paquetes de servicio que puedan estar instalados para posteriormente identificar las vulnerabilidades en los sistemas, las mismas que serás explotadas por el evaluador de la seguridad más adelante (JORGE ORELLANA, 2012)[26].

Las vulnerabilidades las podemos clasificar en (Mifsud, 2012):

Vulnerabilidades en el diseño.

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

[25] Ramos, J. L. (2013). PRUEBAS DE PENETRACIÓN O PENT TEST. *Revista de Información, Tecnología y Sociedad*.

[26] JORGE ORELLANA, C. V. (2012). *PROPUESTA DE BEST PRACTICE PARA EL ANALISIS DE VULNERABILIDADES, MÉTODOS DE PREVENCIÓN Y PROTECCIÓN APLICADOS A LA INFRAESTRUCTURA DE RED DEL LABORATORIO DE SISTEMAS.* RIOBAMBA – ECUADOR: ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

- Implementación

Errores de programación.

- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.

Uso

- Mala configuración de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

Vulnerabilidad del día cero

- Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución “conocida”, pero se sabe cómo explotarla.

4.1 Análisis de datos encontrados.

El análisis de los datos recopilados es el resultado que surge de la comprensión de la estructura y por ende de los niveles se seguridad pertenecientes a la empresa según la información antes recolectada, El análisis de datos encontrados permite concluir las siguientes estadísticas como se muestran en las siguientes figuras.

La figura 4-1 indica la existencia de dos redes las mismas que cuentan con un número de host activos, concluyendo que la res 192.xxx.xxx.0/24 tiene la mayor cantidad de hosts.

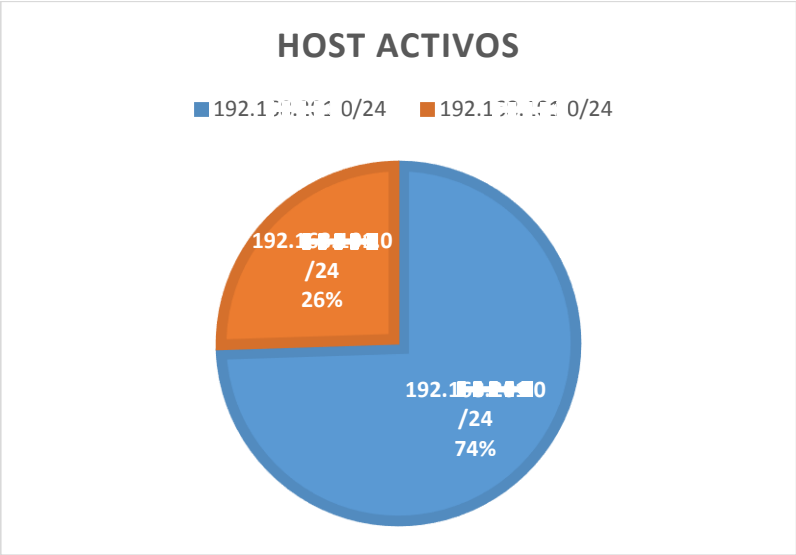


Figura 4-1 Porcentaje de host activos en cada una de las redes de la empresa.

La figura 4-2 presenta los principales servicios activos en las dos redes, se concluye que el servicio h.323 es el que predomina en la red 192.xxx.xxx.0/24 al tratarse de una red de VoIP. El servicio ssh está activo en los host de las dos redes, otro dato que llama la atención es la presencia dominante del servicio VNC-htp en la red 192.xxx.xxx.0/24 lo que indica que la mayoría de hosts tienen instalado un software de monitoreo remoto.

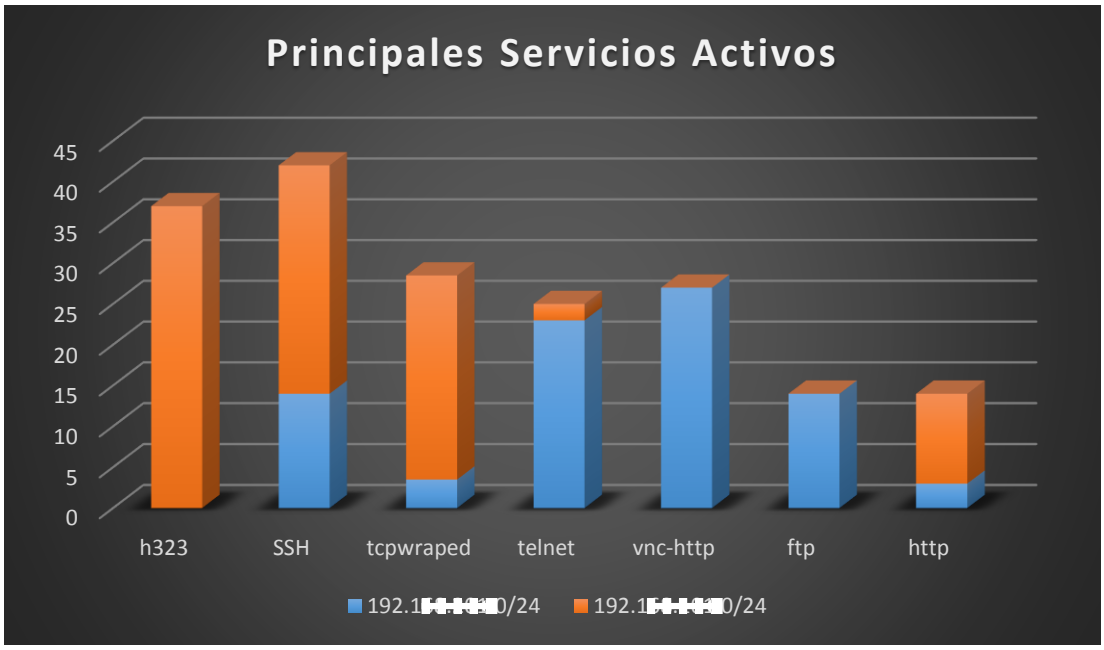


Figura 4-2 Principales servicios activos en las redes de la empresa

La figura 4-3 indica el porcentaje de hosts con los sistemas operativos encontrados en la red 192.xxx.xxx.0, y se observa que la mayor cantidad de hosts tienen el sistema operativo perteneciente a teléfonos Cisco. Los demás sistemas operativos pertenecen a cámaras ip y monitores.

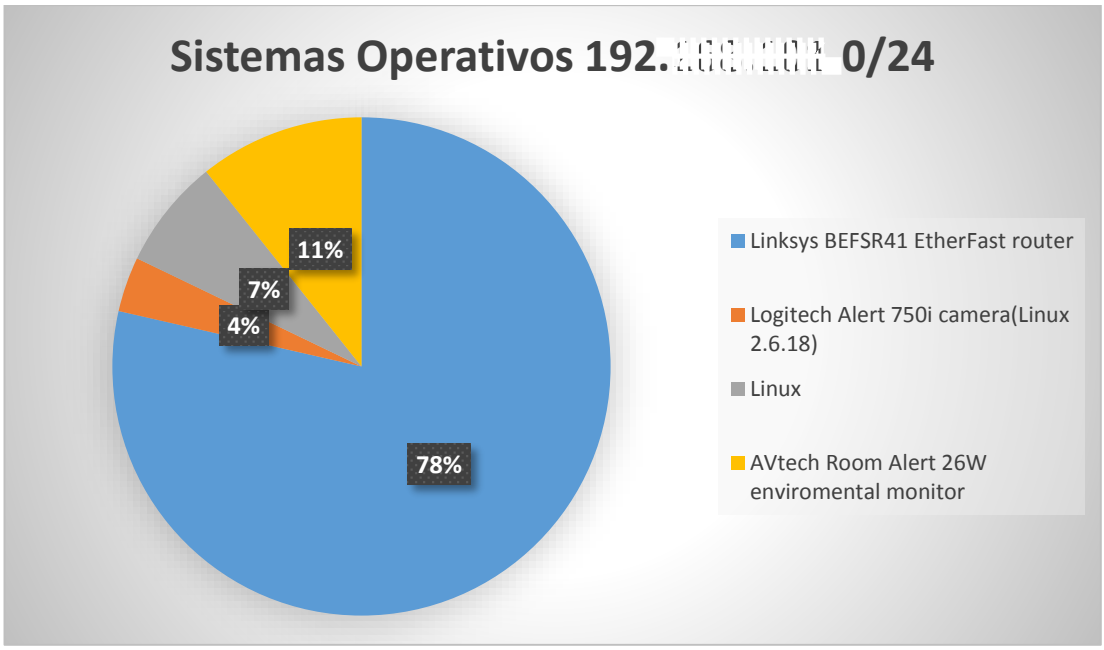


Figura 4-3 Porcentaje de Sistemas operativos en la red 192.xxx.xxx.0/24

La figura 4-4 representa la cantidad de equipos de la red 192.xxx.xxx.0/24 con su respectivo sistema operativo, se observa que la mayor cantidad de equipos tienen sistema operativo Windows, seguido del sistema operativo Linux dentro de los más popularizados.

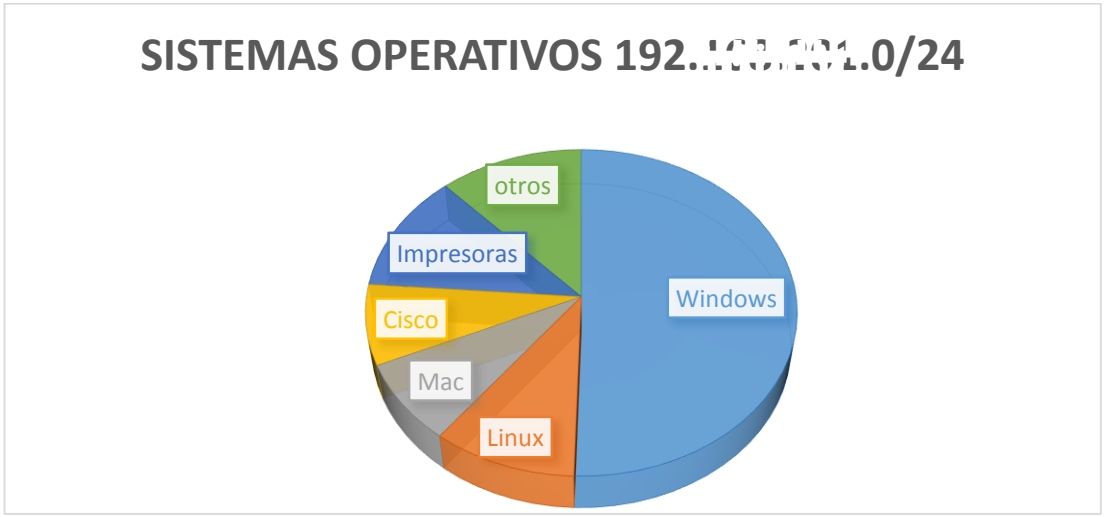


Figura 4-4 Porcentaje de sistemas operativos en la red 192.xxx.xxx.0/24

4.1.1. Análisis de servicios en servidores Windows

A continuación se presenta un análisis de los servidores Windows con sus puertos abiertos y por ende el servicio que corre en ese puerto, se puede observar que todos los servidores Windows poseen servicios que pueden causar problemas de seguridad, en las siguientes tablas presentan información que fue sintetizada y analizada con los datos recolectados en la fase de exploración.

Tabla 4-1 Puertos abiertos en el servidor 192.xxx.xxx.20.

IP	Tipo de Sistema	Sistema Operativo	Puertos Abiertos		
			Puerto	Protocolo	Servicio
192.xxx.xxx.xxx dad00.lns.com.ec	Server	Windows Server 2008	42	TCP	tcpwrapped
			53	TCP	domain
			88	TCP	kerberos-sec
			135	TCP	msrpc
			139	TCP	netbios-ssn
			389	TCP	ldap
			445	TCP	netbios-ssn
			464	TCP	kpasswd5
			5800	TCP	vnc-http
			5900	TCP	vnc
			49152 49153 49154 49156 49157 49158 49163 49165	TCP	msrpc

Tabla 4-2 Puertos abiertos en el servidor 192.xxx.xxx.65

IP	Tipo de Sistema	Sistema Operativo	Puertos Abierto		
			Puerto	Protocolo	Servicio
192.xxx.xxx.65 SEP0026CBBDEA63.lns.com.ec	Server	Windows Server 2008 SP2	49152 49153 49154 49155	TCP	msrpc

Tabla 4-3 Puertos abiertos en el servidor 192.xxx.xxx.67

IP	Tipo de Sistema	Sistema Operativo	Puertos Abiertos		
			Puerto	Protocolo	Servicio
192.xxx.xxx.67 SEP001C58576A A3.lns.com.ec	Server	Windows Server 2008 SP2	135	TCP	msrpc
			139	TCP	netbios-ssn
			445	TCP	netbios-ssn
			5800	TCP	vnc-http
			5900	TCP	vnc
			49152 49153 49154 49157 49160 49161	TCP	msrpc

Tabla 4-4 Puertos abiertos en el servidor 192.xxx.xxx.16

IP	Tipo de Sistema	Sistema Operativo	Puertos Abiertos		
			Puerto	Protocolo	Servicio
192.xxx.xxx.16 mansis.xxx.xxx	Server	Windows Server 2003 SP1	135	TCP	msrpc
			139	TCP	netbios-ssn
			445	TCP	microsoft-ds
			1045	TCP	msrpc
			3389	TCP	ms-wbt-server

Tabla 4-5 Puertos abiertos en el servidor 192.xxx.xxx.11

IP	Tipo de Sistema	Sistema Operativo	Puertos Abierto		
			Puerto	Protocolo	Servicio
192.xxx.xxx.11 clr00.xxx.xxx	Server	Windows Server 2003 SP1	135	TCP	msrpc
			139	TCP	netbios-ssn
			445	TCP	microsoft-ds
			1025	TCP	msrpc
			1070	TCP	flexlm
			27000	TCP	flexlm
			50006	TCP	soap

Tabla 4-6 Puertos abiertos en el servidor 192.xxx.xxx.28

IP	Tipo de Sistema	Sistema Operativo	Puertos Abiertos		
			Puerto	Protocolo	Servicio
192.xxx.xxx.28 sts03.xxx.xxx	Server	Windows Server 2003 SP1	135	TCP	msrpc
			139	TCP	netbios-ssn
			445	TCP	microsoft-ds
			1038	TCP	msrpc
			3389	TCP	ms-wbt-server

Tabla 4-7 Puertos abiertos en el servidor 192.xxx.xxx.34

IP	Tipo de Sistema	Sistema Operativo	Puertos Abiertos		
			Puerto	Protocolo	Servicio
192.xxx.xxx.34 Sts02.lns.com.ecg	Server	Windows Server 2003 SP1	135	TCP	msrpc
			139	TCP	netbios-ssn
			445	TCP	microsoft-ds
			1025	TCP	msrpc
			1047	TCP	msrpc
			3389	TCP	Ms-wbt-server

4.1.2. Análisis de servicios en servidores Linux

El servidor Linux con el que cuenta la empresa, cuenta con los siguientes puertos abiertos:

Tabla 4-8 Puertos abiertos en el servidor 192.xxx.xxx.10

IP	Tipo de Sistema	Sistema Operativo	Puertos Abiertos		
			Puerto	Protocolo	Servicio
192.xxx.xxx.10 dns1.lns.com.ec	Server	Linux 2.6.9	22	TCP	ssh
			53	TCP	domain
			111	TCP	rpcbind

4.1.3. Análisis de Wifi Interno

Este análisis se realiza con el único propósito de identificar claramente las propiedades de las redes inalámbricas internas, es decir de las redes inalámbricas que posee la empresa, A continuación se presenta una tabla con la información valiosa de dichas redes.

Tabla 4-9 Análisis de redes inalámbricas de la empresa.

Encriptación	Número de Redes Wifi	SSID	Potencia	Cifrado	Autenticación
Sin Encriptación	0				
WEP	0				
WPA	1	wcgs	-78	TKIP	PSK
WPA2	1	edbuse	-36	CCMP	PSK
Total	2				

4.2. Clasificación de Objetivos

De acuerdo al análisis de datos encontrados se procede a la clasificación de objetivos que no es más que la identificación de los posibles blancos para realizar sobre estos los ataques.

La siguiente tabla muestra todos los objetivos que serán blanco durante esta evaluación:

Tabla 4-10 Clasificación de Objetivos.

Categoría	Objetivo
Red VoIP	192.xxx.xxx.0/24
Redes inalámbricas	wcgs edbuse
Servidores	Servidores Windows Y linux

Personal administrativo con ingeniería social	Maria del Carmen Bermeo Christian Saquicela
Intranet	Emp.lns.com.ec
Firewall	192.xxx.xxx.254
Dispositivos de Red	Routers y Switch
Puertos abiertos	Todos los principales puertos abiertos: Telnet SNMP ssh entre otros.

4.3. Ejecución de herramientas de scanning de vulnerabilidades.

4.3.1. SiVuS

En el capítulo 3 utilizamos la herramienta SiVuS para realizar el escaneo de la telefonía ip, ahora utilizaremos la misma herramienta pero con la funcionalidad de scanning de vulnerabilidades de la telefoía IP.

La ejecución de SiVus da como resultado el escaneo de los dispositivos que utilicen el protocolo SIP, a continuación se muestra una imagen en la que se puede ver la identificación y listado de todos los dispositivos SIP.

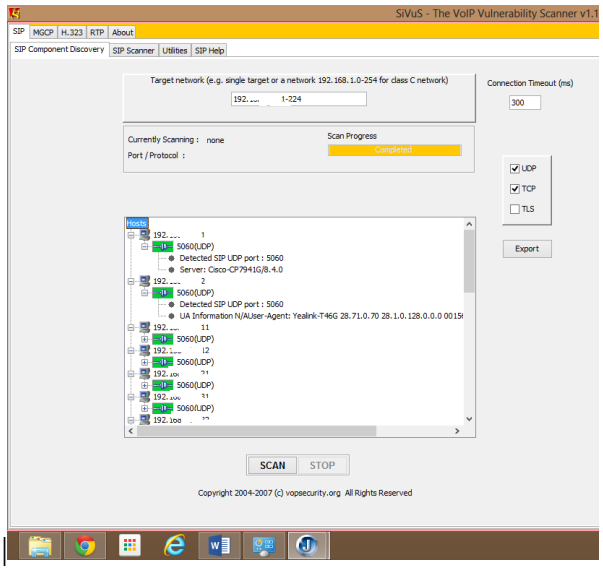


Figura 4-5 Identificación y listado de Dispositivos SIP mediante SiVuS.

Luego de la identificación de los dispositivos SIP, SiVuS realiza el scanning de vulnerabilidades de acuerdo a la configuración establecida en la herramienta. La imagen 4-6 muestra el menú de configuración en el cual se especifica los hosts o rango de hosts objetivo, además de que se debe ingresar varios datos del usuario y protocolos.

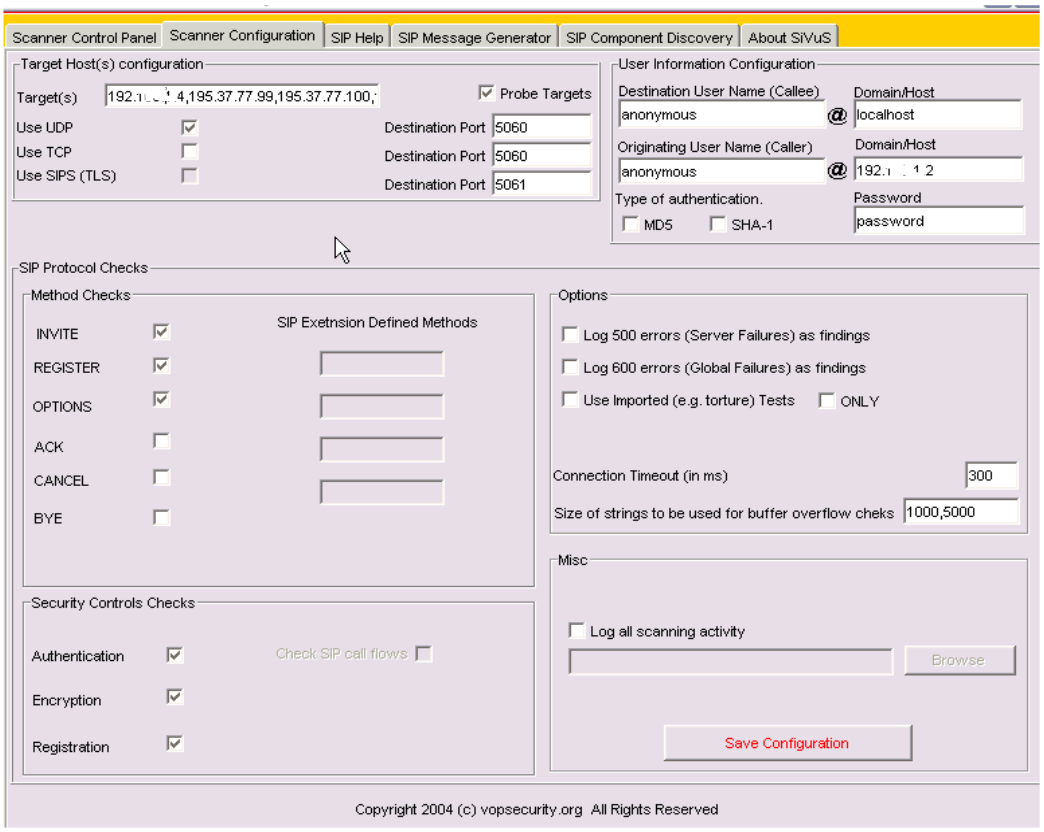


Figura 4-6 Menú de configuración de SiVuS

La figura 4-7 muestra que se está realizando el respectivo escaneo de vulnerabilidades de la red VoIP 192.xxx.xxx.0/24.

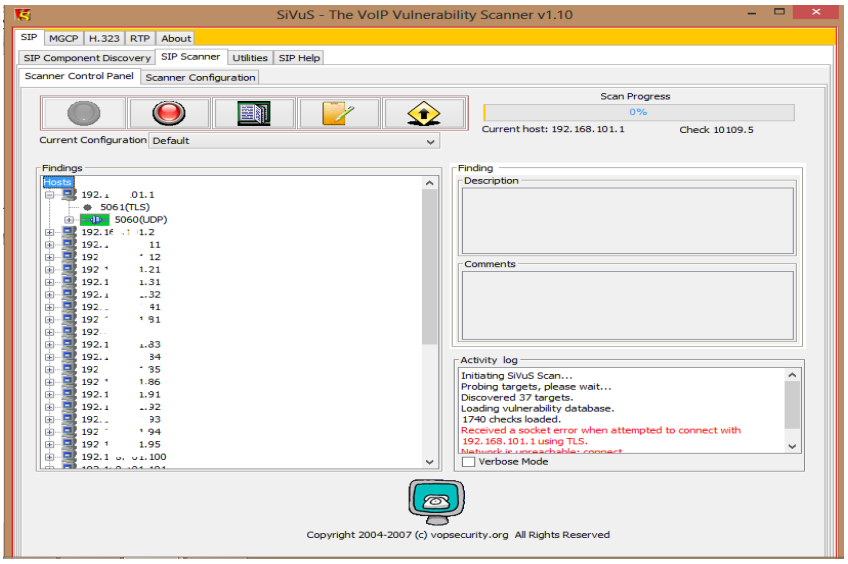
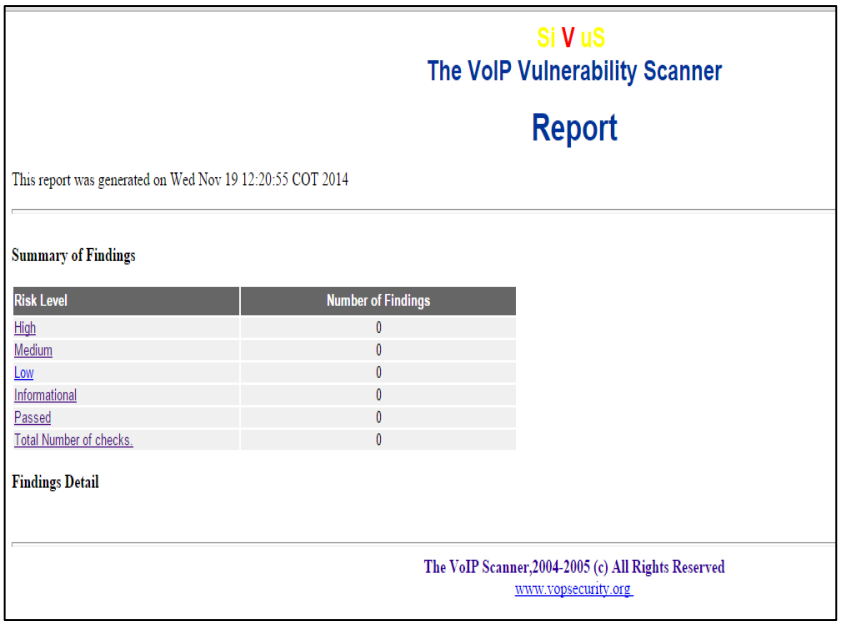


Figura 4-7 Escáner de vulnerabilidades de VoIP

Posterior al escaneo se obtendrá un reporte de las vulnerabilidades encontradas en cada uno de los dispositivos SIP. En la figura 4-8 se muestra el formato de Reporte de vulnerabilidades en el que se identifica el número de vulnerabilidades de alto medio y bajo riesgo asi como también muestra información de configuración de los dispositivos:



SiVuS

The VoIP Vulnerability Scanner

Report

This report was generated on Wed Nov 19 12:20:55 COT 2014

Summary of Findings

Risk Level	Number of Findings
High	0
Medium	0
Low	0
Informational	0
Passed	0
Total Number of checks.	0

Findings Detail

The VoIP Scanner,2004-2005 (c) All Rights Reserved

www.vopsecurity.org

Figura 4-8 Reporte de vulnerabilidades de SiVuS.

4.3.2. NESSUS

Nessus es una herramienta que permite comprobar si un sistema es vulnerable a un conjunto muy amplio de problemas de seguridad almacenados en su base de datos, por

lo tanto con esta herramienta podemos realizar una búsqueda de aquellas deficiencias de seguridad con los servicios remotos que ofrecen los equipos analizados.

La versión del Nessus es la versión Home la misma que nos permite escanear la red de hasta 16 direcciones IP por escáner, con alta velocidad y evaluaciones a fondo, siempre y cuando tengamos una suscripción por lo que está disponible para propósitos sin fines comercial.

Es necesario conocer correctamente las distintas posibilidades de configuración de esta herramienta, además de debe recalcar que las pruebas deben ser realizadas en horarios programados. En figura 4-9 se puede observar la página de inicio de Nessus home.

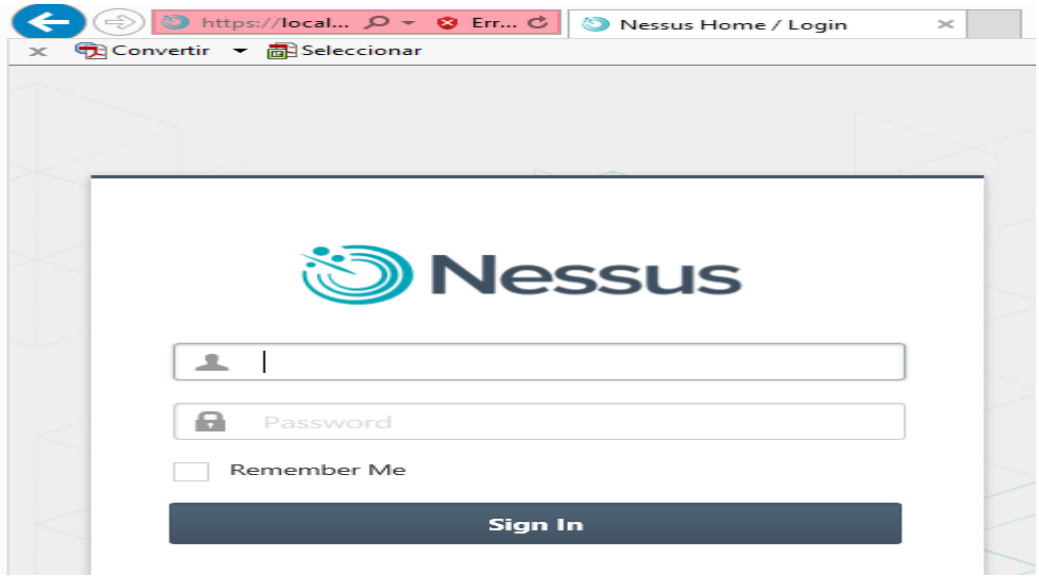


Figura 4-9 Nessus Home

Al ingresar el usuario y la contraseña se presenta el menú del nessus Home en el que se puede crear los scans que necesitemos en nuestro caso se crearon 5 scans los cuales contienen ciertas categorías en las que hemos dividido el número de host anteriormente detectados.:

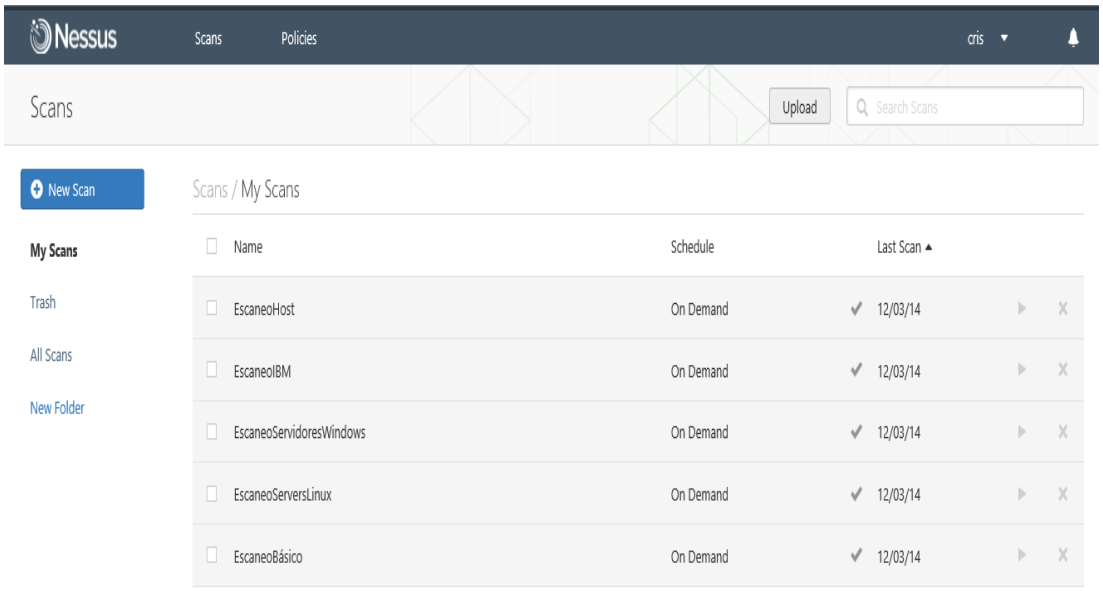


Figura 4-10 Scans realizados por Nessus

Al término del escaneo de cada grupo de hosts, se obtiene el resultado con el porcentaje de vulnerabilidades detectadas con su nivel de riego que se diferencian unas con otras debido a los distintos colores que se presentan. La figura 4-11 muestra dicho resultado.

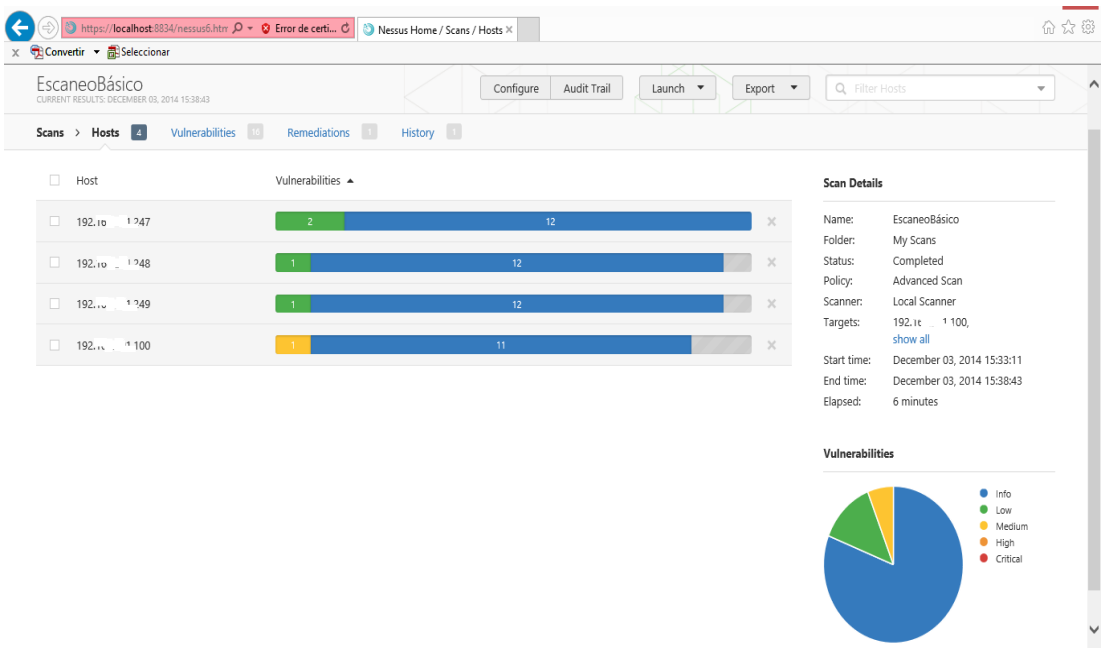


Figura 4-11 Detalle del scan

Por ultimo si se quiere obtener un reporte en distintos formatos con las vulnerabilidades detectadas, basta con utilizar la funcionalidad de reportes que

presenta la herramienta en los cuales se detallan los problemas, el nivel de riesgo, la solución sugerida como se muestra en la figura 4-12.

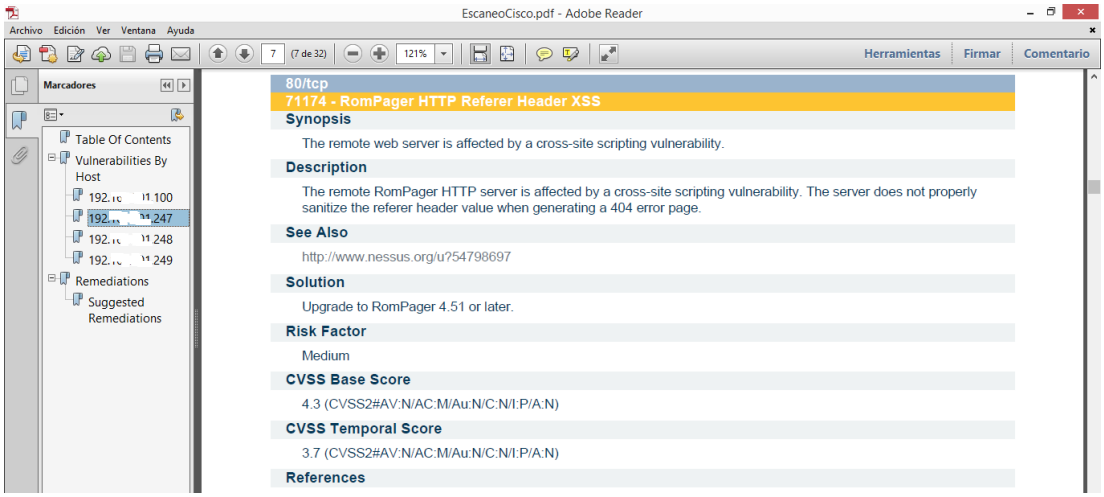


Figura 4-12 Reporte de vulnerabilidades en formato PDF

4.3.3. Determinación de vulnerabilidades.

Una vez definidas y ejecutadas las herramientas para la obtención de vulnerabilidades tendremos que obtener un reporte de las mismas, las cuales serás clasificadas según su nivel de riesgo en: crítico, alto, medio y bajo.

A continuación se interpreta principales vulnerabilidades de mayor riesgo se detectaron con la herramienta SiVuS:

Tabla 4-11 Vulnerabilidad 9999 TLS.

Dirección IP(5061/TLS)	[High] : Check No [9999] TLS
Descripción	This test identifies the encryption capabilities of the target host.The connection was refused during a communication with the target host which implies that the target host does not support SIPS.
Recomendación	If the organizational policy requires protection of the signaling messages, enable the TLS (SIPS) feature on the target host. TLS provides additional protection from various attacks including eavesdroping.(Escuchar secretamente una conversación privada)

Interpretación	Esto indica que el medio seguro SIP no está en servicio. Recomienda activación (el protocolo de transporte TLS) para evitar "tocando a las puertas" de los piratas.

De acuerdo a la anterior tabla en la que se identifican las principales vulnerabilidades que se encontraron en la red de VoIP se construye la siguiente tabla en la que se muestra los host con sus respectivas vulnerabilidades

Tabla 4-12 Determinación de vulnerabilidades de telefonía Ip.

Host	**Check No [9999] TLS**	**Observaciones**
192.xxx.xxx.1		No se encontraron vulnerabilidades
192.xxx.xxx.2	✓	
192.xxx.xxx.11	✓	
192.xxx.xxx.12	✓	
192.xxx.xxx.21	✓	
192.xxx.xxx.31	✓	
192.xxx.xxx.32	✓	
192.xxx.xxx.41	✓	
192.xxx.xxx.81	✓	
192.xxx.xxx.82	✓	
192.xxx.xxx.83		No se encontraron vulnerabilidades
192.xxx.xxx.85	✓	
192.xxx.xxx.86	✓	
192.xxx.xxx.91	✓	
192.xxx.xxx.92	✓	
192.xxx.xxx.95	✓	
192.xxx.xxx.100	✓	
192.xxx.xxx.xxx	✓	
192.xxx.xxx.111	✓	
192.xxx.xxx.112		

192.xxx.xxx.113		
192.xxx.xxx.114		
192.xxx.xxx.121	✓	
192.xxx.xxx.122	✓	
192.xxx.xxx.131		No se encontraron vulnerabilidades
192.xxx.xxx.141	✓	
192.xxx.xxx.142	✓	
192.xxx.xxx.143	✓	
192.xxx.xxx.151	✓	
192.xxx.xxx.xxx	✓	
192.xxx.xxx.202	✓	
192.xxx.xxx.204	✓	
192.xxx.xxx.205	✓	
192.xxx.xxx.250		No Se encontró vulnerabilidades.
192.xxx.xxx.253	✓	
192.xxx.xxx.254		No Se encontró vulnerabilidades.

Luego de ejecutar Nessus, la herramienta de scanning de vulnerabilidades se obtuvo las principales vulnerabilidades que se muestran a continuación:

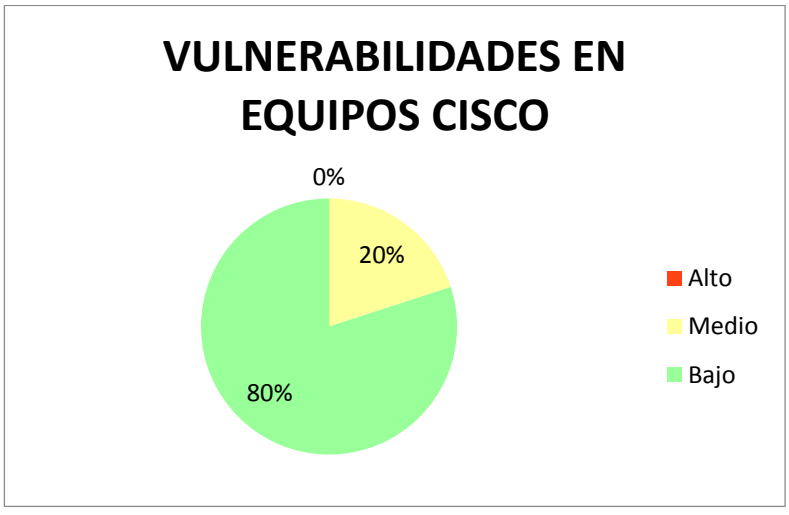


Figura 4-13 Vulnerabilidades en equipos cisco

Como se puede observar en la figura 4-13 no existen vulnerabilidades de alto riesgo en los equipos cisco sin embargo a continuación se presenta una tabla con la descripción de cada una de las vulnerabilidades de medio y bajo riesgo. Aunque se puede observar todas las vulnerabilidades detectadas en el anexo 4 (Ver anexo 4).

Tabla 4-13 Descripción de vulnerabilidades en equipos cisco

Información	Puerto	Vulnerabilidad	Riesgo	Solución
IP: 192.xxx.xxx.100 **MAC**:16:e : : : :87 **OS**: CISCO IP Telephone	TCP/80	El servidor web remoto se ve afectado por una vulnerabilidad de cross-site scripting.	MEDIO	Actualizar a RomPager 4.51 o posterior.

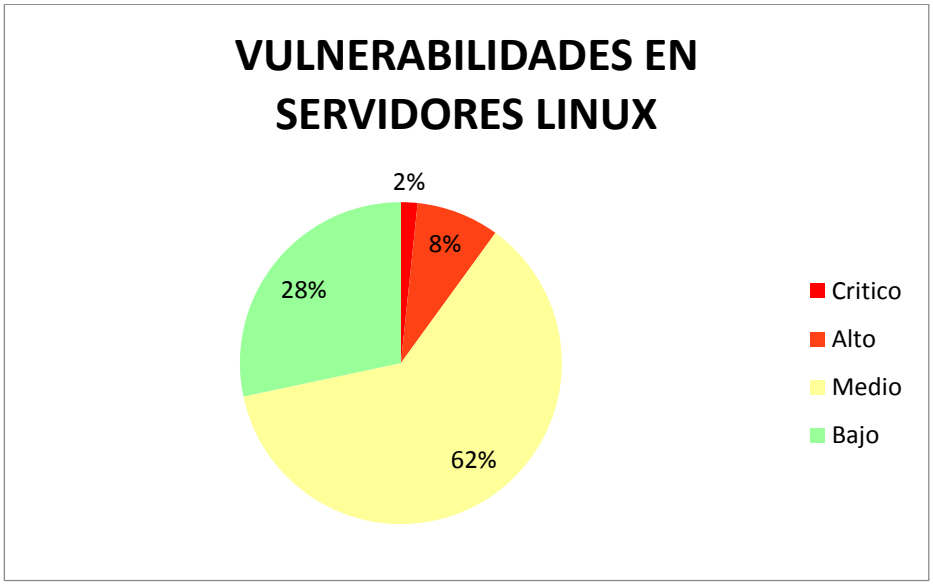


Figura 4-14 Vulnerabilidades en Servidores Linux

En la figura 4-14 se puede observar que en estos servidores existen vulnerabilidades de un riesgo mayor como son las vulnerabilidades críticas, también existe un porcentaje de vulnerabilidades de algo riesgo las mismas que se detallan en la tabla 4-14, el resto de vulnerabilidades no se listan sin embargo se pueden encontrar en el anexo 5 (ver anexo 5).

Tabla 4-14 Descripción de vulnerabilidades en Servidores Linux

Información	Puerto	Vulnerabilidad	Riesgo	Solución
IP:192.xxx.xxx.20 MAC:5c:[illegible]: 10 OS:Linux Kernel 2.6.27.19-158 (ppc)	UDP/161	El nombre de comunidad SNMP del servidor remoto se puede adivinar.	ALTO	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza. Cualquiera de filtrar los paquetes UDP entrantes van a este puerto, o cambiar la cadena de comunidad predeterminado.
IP:192.xxx.xxx.25 MAC:00.[illegible] [illegible] DNS:emp.lns.com.ec OS:Linux Kernel 2.6	TCP/80	El host remoto contiene una versión sin soporte de un lenguaje de programación de aplicaciones web.	ALTO	Actualizar a una versión de PHP que se soporta actualmente.
	TCP/443	El host remoto contiene una versión sin soporte de un lenguaje de programación de aplicaciones web.	ALTO	Actualizar a una versión de PHP que se soporta actualmente.
IP:192.xxx.xxx.85 MAC:00.[illegible] d6:18 OS:Linux Kernel 2.6 en Fedora liberación 15, Linux Kernel 3.0 en Fedora liberar 16, Linux Kernel 3.3 en Fedora liberar 17	TCP/0	El host remoto ejecuta un sistema operativo obsoleto.	CRITICO	Actualizar a una versión más reciente.
IP:192.xxx.xxx.214 MAC:[illegible]: a2:27 OS:Linux Kernel 2.6.12	UDP/161	Los nombres de comunidad del servidor SNMP remoto se pueden adivinar.	ALTO	Deshabilitar el servicio SNMP en el host remoto si no lo usas, filtrar paquetes UDP entrantes van a este puerto, o cambiar la cadena de comunidad predeterminado.
	UDP/161	El nombre de comunidad SNMP del servidor remoto se puede adivinar.	ALTO	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza. Cualquiera de filtrar los paquetes UDP entrantes van a este puerto, o cambiar la cadena de comunidad predeterminado.

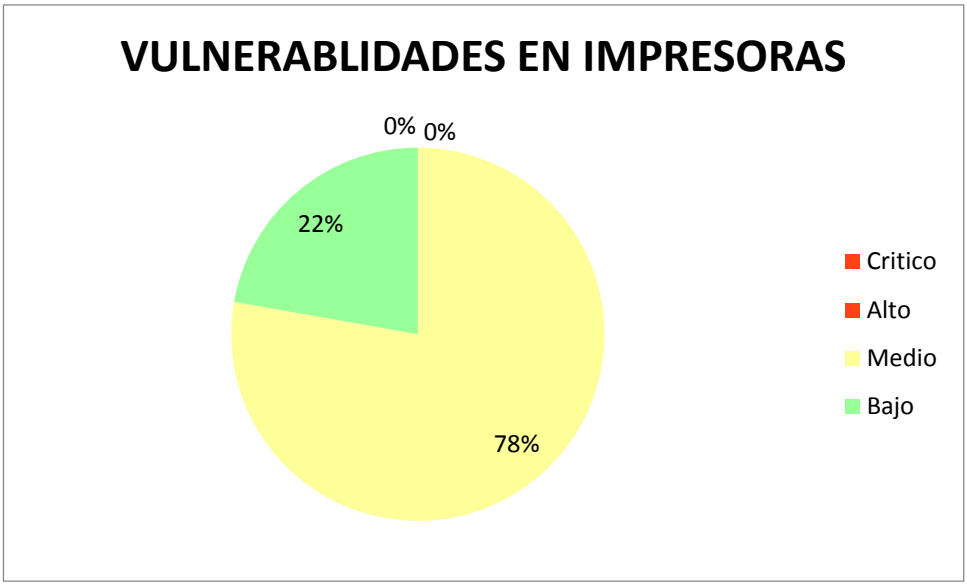


Figura 4-15 Vulnerabilidades en Impresoras

En este caso no existen vulnerabilidades de riego significativo por lo que se detallaran las de riego medio, pudiendo observar las demás vulnerabilidades de bajo riesgo en el anexo 6 (ver anexo 6).

Tabla 4-15 Descripción de Vulnerabilidades en Impresoras.

Información	Puerto	Vulnerabilidad	Riesgo	Solución
IP:192.xxx.xxx.112 MAC:5c:a3 f : a) 5 t)4 OS:Impresora KYOCERA, Linux Kernel 2.6	TCP/443	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	MEDIO	Desactivar SSLv3. Servicios que deben soportar SSLv3 debe activar el mecanismo de TLS repliegue SCSV hasta SSLv3 se puede desactivar.
	TCP/443	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.

	TCP/443	Un certificado SSL en la cadena de certificados se ha firmado utilizando un algoritmo de hash débil.	MEDIO	Póngase en contacto con la entidad emisora de certificados de haber certificado reeditado.
	TCP/443	El servicio remoto es compatible con el uso de la fuerza media cifrado SSL.	MEDIO	Vuelva a configurar la aplicación afectada, si es posible evitar el uso de sistemas de cifrado de fuerza media.
	TCP/443	El servicio remoto cifra el tráfico utilizando un protocolo con debilidades conocidas.	MEDIO	Consulte la documentación de la aplicación que permite deshabilitar SSL 2.0 y utilizar SSL 3.0, TLS 1.0, o superior en su lugar.
	TCP/443	El servicio remoto es compatible con el uso de sistemas de cifrado SSL débiles.	MEDIO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados débiles.

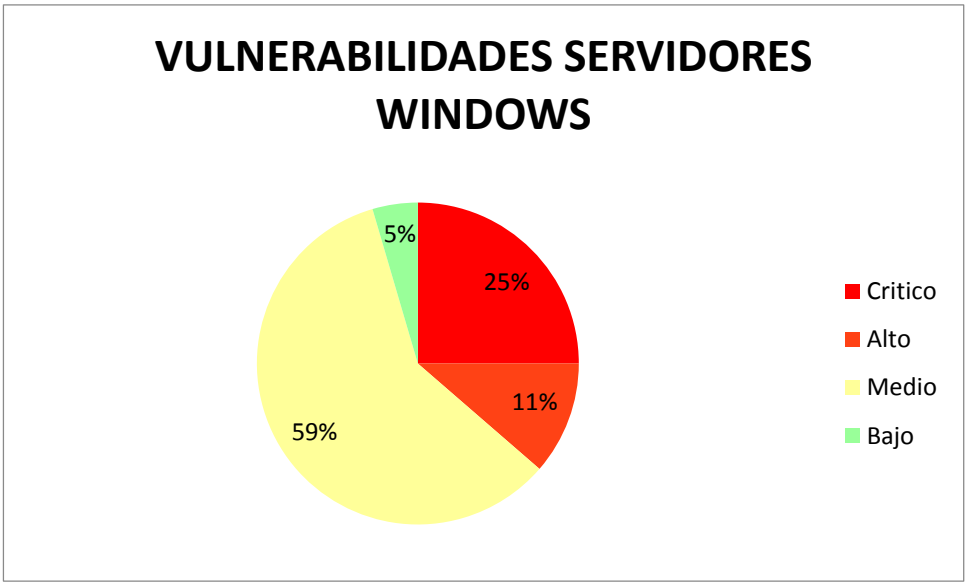


Figura 4-16 Vulnerabilidades en servidores Windows

La figura 4-16 muestra el porcentaje de vulnerabilidades según el riesgo que se encontraron en los servidores Windows y se puede decir que son los servidores con mayor número de vulnerabilidades de riesgo crítico y riego alto. El detalle del total de las vulnerabilidades se encuentra en el anexo 7 (ver anexo 7) ya que a continuación en la tabla 4-16 solo se detallan las vulnerabilidades de mayor riesgo.

Tabla 4-16 Descripción vulnerabilidades en Servidores Windows.

Información	Puerto	Vulnerabilidad	Riesgo	Solución
IP:192.xxx.xxx.16 MAC:00.[illegible] DNS/NetBios:edb-sistema.lns.com.ec.xxx.xxx.192.in-addr.arpa / STS06 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Código arbitrario puede ser ejecutada en el host remoto debido a una falla en el servicio "Servidor"	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.
IP:192.xxx.xxx.30 MAC:40:[illegible] DNS/Netbios:edbmail.lns.com.ec.xxx.xxx.192.inaddr.arpa OS:VMware ESXi	TCP/0	El VMware ESXi 5.1 host remoto se ve afectado por múltiples vulnerabilidades de seguridad.	ALTO	Aplicar ESXi510-201212xxx-SG.
IP:192.xxx.xxx.34 MAC:00:[illegible] DNS/NetBios:sts02.lns.com.ec / STS02 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Código arbitrario puede ser ejecutada en el host remoto debido a una falla en el servicio "Servidor"	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta

				vulnerabilidad para Windows 2000.
IP:192.xxx.xxx.75 MAC:00:[illegible] 5f DNS/NetBios:cueasis.lns.com.ec/PASANTERRHH OS:Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3	TCP/0	El sistema operativo remoto ya no es compatible.	CRITICO	Actualizar a una versión de Windows que se soporta actualmente.
	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Es posible ejecutar código arbitrario en el host remoto de Windows debido a fallas en su implementación SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows XP, Vista, 2008, 7 y 2008 R2.
	TCP/445	Es posible ejecutar código arbitrario en el host remoto de Windows debido a fallas en su implementación SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows XP, Vista, 2008, 7 y 2008 R2.
	TCP/445	Código arbitrario puede ser ejecutada en el host remoto debido a una falla en el servicio "Servidor".	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Es posible acceder a un recurso compartido de red.	ALTO	Para restringir el acceso con Windows, abra el Explorador, haga un clic derecho sobre cada acción, vaya a la pestaña "compartir", y haga clic en 'Permisos'.
IP:192.xxx.xxx.xxx MAC:00.[illegible]:80 DNS/NetBiosdad00.lns.com.ec/DAD00	UDP/53	El host remoto está ejecutando una versión sin soporte de servidor DNS de Microsoft.	CRITICO	Actualizar a una versión compatible de Microsoft Windows.

OS:Microsoft Windows Server 2008 Enterprise Service Pack 1	TCP/445	Código arbitrario puede ser ejecutada en el host remoto a través del puerto SMB	CRITICO	Microsoft ha lanzado un parche para Windows Vista y Windows Server 2008.
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000

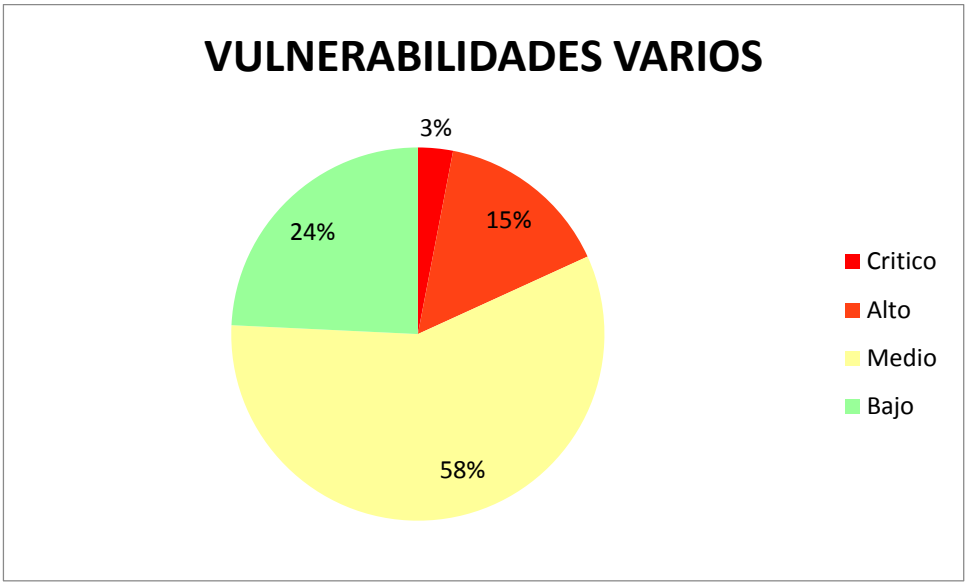


Figura 4-17 Vulnerabilidades en equipos varios.

Se identificó también vulnerabilidades en equipos con sistemas operativos no comunes, en la figura 4-17 se puede observar que existe un pequeño porcentaje de vulnerabilidades de mayor riesgo las mismas que se detallan a continuación en la tabla 4-17. Hay que recalcar que la descripción de todas las vulnerabilidades se encuentran en el anexo 8 (Ver anexo 8).

Tabla 4-17 Descripción de vulnerabilidades en equipos varios

Información	Puerto	Vulnerabilidad	Riesgo	Solución

IP:192.xxx.xxx.22 MAC:5c.[illegible] 10 OS:KYOCERA Impresora	UDP/161	El nombre de comunidad SNMP del servidor remoto se puede adivinar.	ALTO	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza. Cualquiera de filtrar los paquetes UDP entrantes van a este puerto, o cambiar la cadena de comunidad predeterminado.
IP:192.xxx.xxx.27 MAC:3[illegible]:58 OS:VMware ESXi	TCP/0	El VMware ESXi 5.0 host remoto se ve afectado por múltiples vulnerabilidades de seguridad.	ALTO	Aplicar ESXi500-201205401-SG o implementar las soluciones temporales / mitigaciones señaladas por el vendedor,Aplicar ESXi500-201207101-SG, Aplicar ESXi500-201212101-SG, Aplicar ESXi500-201310101-SG, ESXi500-201310201-UG, o ESXi500-Update03,Aplicar ESXi500-201206401-SG, Aplicar ESXi500-201112401-SG.
IP:192.xxx.xxx.30 MAC:[illegible]ca OS:VMware ESXi	TCP/0	El VMware ESXi 5.1 host remoto se ve afectado por múltiples vulnerabilidades de seguridad.	ALTO	Aplicar ESXi510-201212101-SG
IP:192.xxx.xxx.31 MAC:3[illegible]7:92 OS:VMware ESXi	TCP/0	El VMware ESXi 5.5 host remoto está potencialmente afectada por múltiples vulnerabilidades.	ALTO	Aplique el parche ESXi550-201404420 para ESXi 5.5 o ESXi550-101404401 para ESXi 5.5 Update 1.
IP:192.xxx.xxx.32 MAC:00:[illegible]7c OS:VMware ESXi	TCP/0	El host remoto está ejecutando una versión no soportada de una aplicación de virtualización.	CRITICO	Actualizar a una versión de VMware ESX / ESXi que se soporta actualmente.
	TCP/0	El host VMware ESX / ESXi remoto se ve afectado por múltiples vulnerabilidades de seguridad.	ALTO	Aplique los parches faltantes.

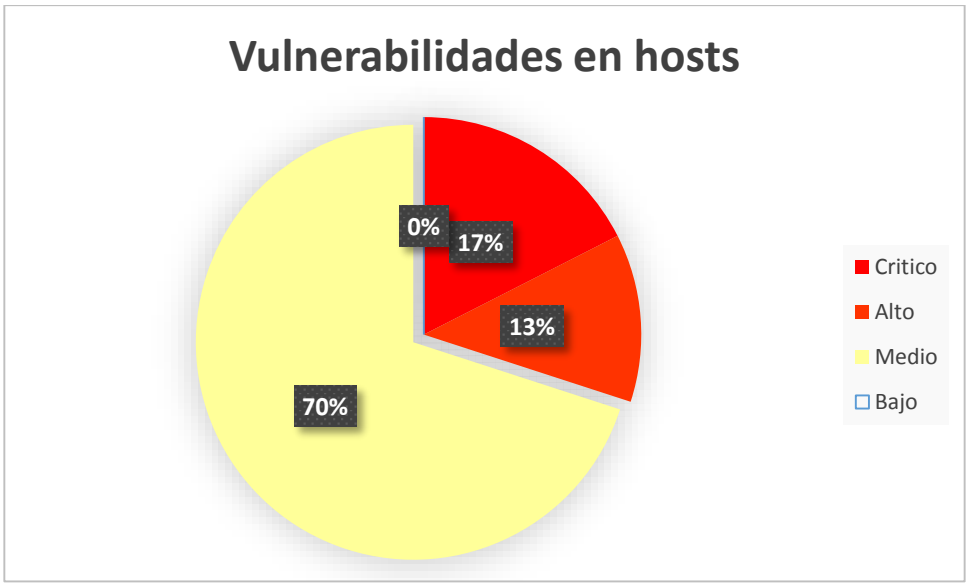


Figura 4-18 Vulnerabilidades en hosts

La figura 4-18 muestra las vulnerabilidades detectadas en un conjunto de hosts Windows, se puede observar que contiene un alto porcentaje de vulnerabilidades de muy alto riesgo, toda la información referente a la totalidad de las vulnerabilidades se detallan en el anexo 9(ver anexo 9).

En la tabla 4-18 solo se detallan las vulnerabilidades marcadas como críticas y de alto riesgo.

Tabla 4-18 Descripción de vulnerabilidades en host

Información	**Puerto**	**Vulnerabilidad**	**Riesgo**	**Solución**
IP:192.xxx.xxx.2 MAC:00. : : : : 94 DNS/NetBios:STS03 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Código arbitrario puede ser ejecutada en el host remoto debido a un defecto en el . servicio "Servidor"	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008
	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2.

IP:192.xxx.xxx.3 MAC:00: 2 . 5 . . 2a: 68 DNS/NetBios:STS00 OS:Microsoft Windows Server 2008 Service Pack 1 Datacenter	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.
IP:192.xxx.xxx.5 MAC:00 . . . . : 1e: b2 DNS/NetBios:STS05 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Código arbitrario puede ser ejecutada en el host remoto debido a una falla en el servicio "Servidor".	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.
IP:192.xxx.xxx.7 MAC:00: . . . . . 5: 40 DNS/NetBios:SPW00 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.
IP:192.xxx.xxx.33 MAC:00: . . . . . 5: 46 DNS/NetBios:ANT00 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Código arbitrario puede ser ejecutada en el host remoto debido a una falla en el servicio "Servidor".	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.

	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.
IP:192.xxx.xxx.78 MAC:fc:[illegible] DNS/NetBios:ORIS/ORIS OS:Microsoft Windows 7 Professional	UDP/5355	Código arbitrario puede ser ejecutada en el host remoto a través del cliente DNS de Windows instalado.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2

Tabla 4-19 Vulnerabilidades de la página web

METODO	LINK	VULNERABILIDAD	RIESGO	SOLUCIÓN
GET	http://192.xxx.xxx.25/helpdesk/index.php?act=article&code=view&id=1+AND+1%3D1+--+	Falla por Inyección SQL puede ser posible	ALTO	Si la aplicación utiliza JDBC, utilice PreparedStatement o CallableStatement, con parámetros pasados por '?' Si la aplicación utiliza ASP, utilice comandos de objetos ADO y consultas con parámetros. No crear consultas SQL dinámicas utilizando concatenación de cadenas. Aplique una 'lista blanca' de caracteres permitidos, o una "lista negra" de caracteres no permitidos en la entrada del usuario. Aplicar privilegios mínimos a los usuarios dentro de la base de datos Evitar el uso de la 'sa' o usuarios de bases de datos 'db-owner'. Esto no elimina la inyección de SQL, pero minimiza su impacto. Conceder el acceso mínimo y necesario a la base de datos para la aplicación.
GET	http://192.xxx.xxx.25/helpdesk/index.php?act=tickets&code=open+AND+1%3D1+--+			
POST	http://192.xxx.xxx.25/helpdesk/index.php?act=kb&code=search			
POST	http://192.xxx.xxx.25/helpdesk/index.php?act=login			
POST	http://192.xxx.xxx.25/helpdesk/index.php?act=login			
POST	http://192.xxx.xxx.25/helpdesk/index.php?act=login			

POST	http://192.xxx.xxx.25/helpdesk/index.php?act=register&code=new			
GET	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/css/	Es posible ver el listado del directorio, estas listas pueden revelar guiones ocultos, incluyen archivos, archivos de origen de copia de seguridad, etc, a los que se puede acceder para leer la información sensible.	MEDIO	Desactivar la exploración de directorios. Si esto es necesario, asegúrese de que los archivos de la lista no induzcan riesgos.
GET	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/js/			
GET	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/			
GET	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/default/			
GET	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/orman/			
GET	http://emp.lns.com.ec/lnsn/templates/emailmarketing_22/themes/pascal/			

4.4. Búsqueda manual de vulnerabilidades.

Hasta el momento hemos venido determinando las vulnerabilidades con la ayuda de varias herramientas. Muchas de estas herramientas nos permiten hacer una búsqueda de vulnerabilidades de manera rápida y sencilla, pero en ocasiones es mejor buscar las vulnerabilidades nosotros mismos, ya que los escáneres de vulnerabilidades si bien pueden ser potentes pero no significa que sean 100% fiables sin embargo ahorran mucho tiempo.

Pero analizar nuestro objetivo sin un escáner que lo haga automáticamente, siempre será mucho más potente aunque más lento.

Por lo general los escáneres de vulnerabilidades se basan en vulnerabilidades ya publicadas y en fallos de seguridad concretos y característicos. Esto deja a un lado la ingeniería social, donde se puede llegar a extraer mucha información para después explotar un fallo.

Una de las desventajas de herramientas, es que suelen hacer falsos positivos. Sin embargo nos hemos apoyado en ellas para tener una imagen global de la seguridad de nuestro objetivo y pistas sobre el tipo de fallo que podemos explotar.

Por lo general los escáneres de vulnerabilidades están muy enfocados a los pentesting de aplicaciones web.

En este caso, no está de más utilizar estas herramientas para ahorrar tiempo. Se podría lanzar un escaseo de la red o del servidor que estemos auditando y luego ir descartando falsos positivos. Esto reduce bastante el tiempo que tendríamos que dedicarle si lo hiciéramos de manera manual.

Sin embargo la búsqueda manual de vulnerabilidades se realiza generalmente cuando no se tiene éxito con el escaneo de vulnerabilidades mediante el uso de herramientas, entonces se procede a realizar búsquedas en repositorios de vulnerabilidades que son actualizados diariamente.

También se lo puede realizar como complemento a la ejecución de herramientas automáticas, para verificar la existencia de vulnerabilidades conocidas que puedan afectar a las versiones del software identificado en cada servicio.

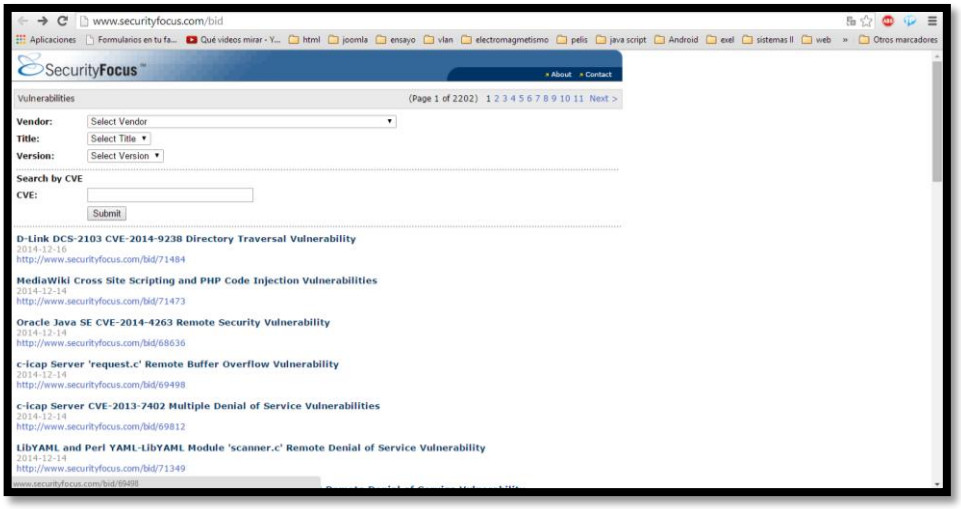


Figura 4-19 Página www.securityfocus.com, para la búsqueda de vulnerabilidades

Para esto aremos usos de los repositorios de expolits, teniendo como los más usados los siguientes:

Tabla 4-20 Tabla de sitios que poseen repositorios de vulnerabilidades.

SITIOS WEB	LINK
Security Focus	http://www.securityfocus.com/bid
Packet Storm Security	http://packetstormsecurity.org
SecuriTeam:	http://www.securiteam.com
Security Tracker	http://www.securitytracker.com/
Open Source Vulnerability Database	http://osvdb.org/ http://osvdb.org/
Security Forest	http://www.securityforest.com/
CERT	http://www.cert.org/
CVE	http://cve.mitre.org/
Exploit World	http://www.insecure.org/sploits.html
Phrack	http://www.phrack.org/

4.5.Enumeración de usuarios y datos de configuración.

Durante el desarrollo de esta fase, un punto que no hay que obviar es la enumeración de usuarios ya que el único objetivo es identificar cuentas de usuarios y grupos válidos, para

lo cual existen varias técnicas entre la principal y la que hemos utilizado es el establecimiento de sesiones nulas y enumeración de nombres NetBIOS.

En general, NetBIOS ofrece los tres servicios siguientes:

Nombre del servicio: UDP / 137

Servicio de datagramas: UDP / 138

Sesión de servicio: TCP / 139

En los sistemas que tienen habilitado este servicio podemos utilizar algunas herramientas con el fin de descubrir información sobre los nombres de host y dominios especialmente en redes windows. En algunos casos este protocolo se puede encontrar y en sistemas Linux.

Las dos herramientas básicas son nbtstat y nbtscan. Nbtstat es una utilidad de línea de comandos que se integra en los sistemas windows y puede revelar información sobre los nombres NetBIOS y la tabla de nombre de equipo remoto o local, pero sólo para un equipo. Por otra parte la nbtscan es un escáner de servidor de nombres de NetBIOS, que tiene las mismas funciones que nbtstat pero opera en un rango de direcciones en lugar de un solo equipo.

Nbtscan está instalado en kali Linux .Se puede también utilizar esta herramienta con el fin de escanear toda la red objetivo. En la figura 4-20 podemos ver que se ha descubierto las direcciones IP, los nombres NetBIOS, usuarios que han iniciado sesión y las direcciones MAC de los hosts que ejecutan el servicio NetBIOS en la red

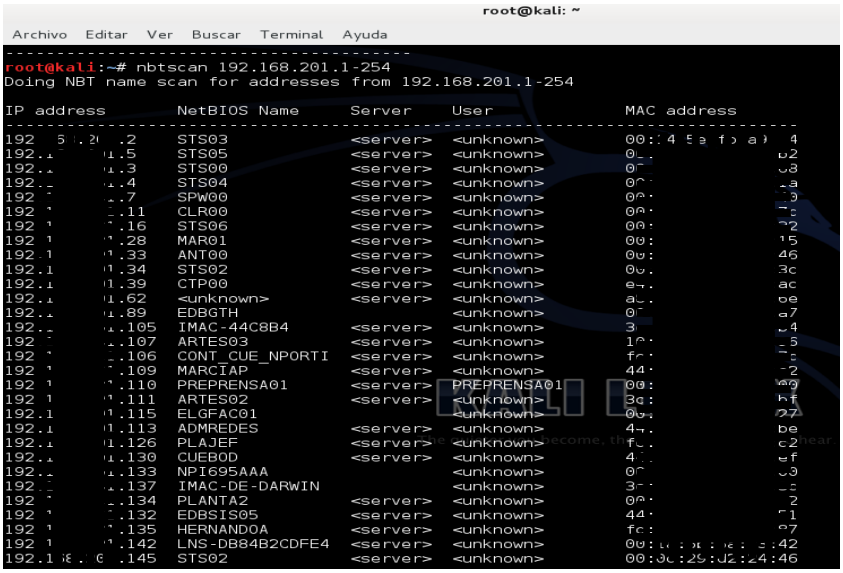


Figura 4-20 Uso de nbtscan en dentro de kali

Con la opción de detalle nbtscan –v el formato de salida contiene información más detallada ya que contiene sufijos tales como <01> y <1D> que indica el examinador principal, el <20> que en la máquina está en funcionamiento el servicio de servidor de archivos, el <03> que un servicio de mensajería está en marcha y el <00 > significa que un servicio de estación de trabajo se está ejecutando bien. El <1E> es el Navegador Elecciones servicio. La figura 4-21 muestra el uso de esta opción.

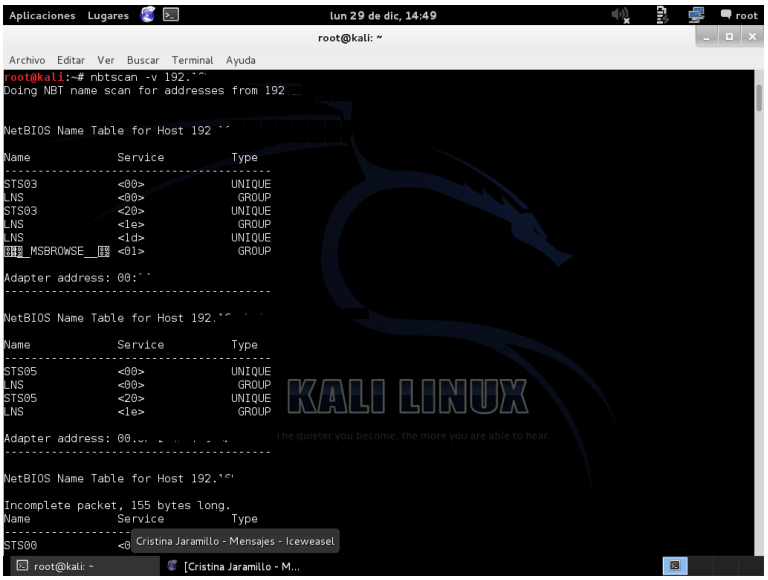


Figura 4-21 Opción nbtscan – v

En la tabla 4-21 se detalla la información obtenida con el uso de nbtscan y la opción nbtscan –v, se complementaron los dos resultados obtenidos.

Tabla 4-21 Resumen de los datos obtenidos mediante la herramienta nbtscan y la opción nbtscan -v

IP Address	NetBios Name	Server	User	MAC address	Name Service Time
192.xxx.xxx.2	STS03	<server>	<unknown>	00 :94	STS03 <00> UNIQUE LNS <00> GROUP STS03 <20> UNIQUE LNS <1e> GROUP LNS <1d> UNIQUE __MSBROWSE__<01> GROUP
192.xxx.xxx.3	STS00	<server>	<unknown>	00:2 68	STS00 <00> UNIQUE LNS <00> GROUP STS00 <20> UNIQUE
192.xxx.xxx.4	STS04	<server>	<unknown>	00: l:1a	STS04 <00> UNIQUE LNS <00> GROUP STS04 <20> UNIQUE
192.xxx.xxx.7	SPW00	<server>	<unknown>	00: 5:40	SPW00 <00> UNIQUE LNS <00> GROUP SPW00 <20> UNIQUE
192.xxx.xxx.5	STS05	<server>	<unknown>	00: :b2	STS05 <00> UNIQUE LNS <00> GROUP STS05 <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.11	CLR00	<server>	<unknown>	00: :7c	CLR00 <00> UNIQUE WORKGROUP <00> GROUP CLR00 <20> UNIQUE WORKGROUP <1e> GROUP WORKGROUP <1d> UNIQUE __MSBROWSE__<01> GROUP
192.xxx.xxx.16	STS06	<server>	<unknown>	00 4:32	STS06 <00> UNIQUE LNS <00> GROUP STS06 <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.28	MAR01	<server>	<unknown>	00: :15	MAR01 <00> UNIQUE LNS <00> GROUP MAR01 <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.34	STS02	<server>	<unknown>	00: :3c	STS02 <00> UNIQUE LNS <00> GROUP STS02 <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.33	ANT00	<server>	<unknown>	00: :46	ANT00 <00> UNIQUE LNS <00> GROUP ANT00 <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.39	CTP00	<server>	<unknown>	e4:1 ac	CTP00 <00> UNIQUE LNS <00> GROUP

					CTP00 <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.62	<unknown>	<server>	<unknown>	a8: 5:6e	CGSADM <20> UNIQUE LNS <00> GROUP
192.xxx.xxx.89	EDBGTH		<unknown>	00: ɔ:a7	EDBGTH <00> UNIQUE
192.xxx.xxx.105	IMAC-44C8B4	<server>	<unknown>	3c :8:b4	IMAC-44C8B4 <00> UNIQUE IMAC-44C8B4 <20> UNIQUE WORKGROUP <00> GROUP
192.xxx.xxx.106	CONT_CUE_NPORTI	<server>	<unknown>	fc: ɔ:7c	LNS <00> GROUP CONT_CUE_NPORTI <00> UNIQUE CONT_CUE_NPORTI <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.107	ARTES03	<server>	<unknown>	10: :96	ARTES03 <00> UNIQUE ARTES03 <20> UNIQUE WORKGROUP <00> GROUP
192.xxx.xxx.109	MARCIAP	<server>	<unknown>	44:[illegible] a2	MARCIAP <20> UNIQUE MARCIAP <00> UNIQUE LNS <00> GROUP LNS <1e> GROUP
192.xxx.xxx.111	ARTES02	<server>	<unknown>	3c: e:bf	ARTES02 <00> UNIQUE ARTES02 <20> UNIQUE WORKGROUP <00> GROUP
192.xxx.xxx.113	ADMREDES	<server>	<unknown>	44: l:be	ADMREDES <00> UNIQUE WORKGROUP <00> GROUP ADMREDES <20> UNIQUE WORKGROUP <1e> GROUP
192.xxx.xxx.115	ELGFAC01		<unknown>	00: l:27	ELGFAC01 <00> UNIQUE
192.xxx.xxx.126	PLAJEF	<server>	<unknown>	fc:[illegible] :c2	PLAJEF <00> UNIQUE LNS <00> GROUP PLAJEF <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.130	CUEBOD	<server>	<unknown>	44:[illegible] :ef	CUEBOD <00> UNIQUE LNS <00> GROUP CUEBOD <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.133	NPI695AAA		<unknown>	a0:[illegible] :aa	__MSBROWSE__<01> GROUP WORKGROUP <00> GROUP NPI695AAA <00> UNIQUE
192.xxx.xxx.132	EDBSIS05	<server>	<unknown>	44:[illegible] :51	EDBSIS05 <20> UNIQUE EDBSIS05 <00> UNIQUE WORK_GROUP <00> GROUP WORK_GROUP <1e> GROUP WORK_GROUP <1d> UNIQUE __MSBROWSE__<01> GROUP
192.xxx.xxx.135	HERNANDOA	<server>	<unknown>	fc: [illegible] 3:87	LNS <00> GROUP HERNANDOA <00> UNIQUE HERNANDOA <20> UNIQUE LNS <1e> GROUP

192.xxx.xxx.134	PLANTA2	<server>	<unknown>	00:1 :a2	PLANTA2 <00> UNIQUE GRUPO_TRABAJO <00> GROUP PLANTA2 <20> UNIQUE GRUPO_TRABAJO <1e> GROUP GRUPO_TRABAJO <1d> UNIQUE __MSBROWSE__<01> GROUP
192.xxx.xxx.142	LNS-DB84B2CDFE4	<server>	<unknown>	00:1 42	LNS-DB84B2CDFE4 <00> UNIQUE LNS <00> GROUP LNS-DB84B2CDFE4 <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.145	STS02	<server>	<unknown>	00: 4:46	STS02 <00> UNIQUE LNS <00> GROUP STS02 <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.148	IMACVICENTE	<server>	<unknown>	3c:(:5a	IMACVICENTE <00> UNIQUE IMACVICENTE <20> UNIQUE LNS <00> GROUP
192.xxx.xxx.137	IMAC-DE-DARWIN		<unknown>	3c:(:3c	IMAC-DE-DARWIN <00> UNIQUE
192.xxx.xxx.150	HABRIL	<server>	<unknown>	fc:4 :d4	HABRIL <20> UNIQUE HABRIL <00> UNIQUE WORKGROUP <00> GROUP WORKGROUP <1e> GROUP
192.xxx.xxx.155	STS02	<server>	<unknown>	00: 4:50	STS02 <00> UNIQUE LNS <00> GROUP STS02 <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.163	LNSBOD	<server>	<unknown>	00:1 ac	LNSBOD <00> UNIQUE LNS <00> GROUP LNSBOD <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.165	SHERNANDEZ	<server>	<unknown>	90: :34	SHERNANDEZ <00> UNIQUE GRUPO_TRABAJO <00> GROUP SHERNANDEZ <20> UNIQUE GRUPO_TRABAJO <1e> GROUP
192.xxx.xxx.164	PATRICIOS	<server>	<unknown>	fc:4 :47	PATRICIOS <20> UNIQUE PATRICIOS <00> UNIQUE LNS <00> GROUP LNS <1e> GROUP
192.xxx.xxx.167	DLOJA	<server>	<unknown>	00:1 :94	DLOJA <00> UNIQUE LNS <00> GROUP DLOJA <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.169	CGSEDUARDO	<server>	CGSEDUARDO	c8:2 3:5	CGSEDUARDO <03> UNIQUE CGSEDUARDO <20> UNIQUE CGSEDUARDO <00> UNIQUE CGSEDUARDO <03> UNIQUE

					CGSEDUARDO <20> UNIQUE WORKGROUP <1e> GROUP WORKGROUP <00> GROUP WORKGROUP <1e> GROUP WORKGROUP <00> GROUP
192.xxx.xxx.170	PLAIMP	<server>	<unknown>	44 2:6e	PLAIMP <00> UNIQUE LNS <00> GROUP PLAIMP <20> UNIQUE LNS <1e> GROUP
192.xxx.xxx.174	VENDEDOR	<server>	<unknown>	00:(:0c	VENDEDOR <00> UNIQUE VENDEDOR <20> UNIQUE LNS <00> GROUP LNS <1e> GROUP
192.xxx.xxx.179	EDBSRI		<unknown>	2c: ɔ:e8	EDBSRI <00> UNIQUE
192.xxx.xxx.185	NPIEF6A52		<unknown>	00: ı:52	NPIEF6A52 <00> UNIQUE
192.xxx.xxx.193	CUEFACNUEVA		<unknown>	38:ɛ :7c	CUEFACNUEVA <00> UNIQUE
192.xxx.xxx.195	SERSIS		<unknown>	2c: ⁷:da	SERSIS <00> UNIQUE
192.xxx.xxx.198	NPI0F9FF6	<server>	<unknown>	00 f:f6	NPI0F9FF6 <00> UNIQUE NPI0F9FF6 <20> UNIQUE
192.xxx.xxx.xxx	DAD00	<server>	<unknown>	00 e:80	DAD00 <00> UNIQUE LNS <1c> GROUP LNS <00> GROUP DAD00 <20> UNIQUE LNS <1b> UNIQUE
192.xxx.xxx.220	MARCELOMEJIA	<server>	<unknown>	f0: :f0	MARCELOMEJIA <20> UNIQUE MARCELOMEJIA <00> UNIQUE WORKGROUP <00> GROUP WORKGROUP <1e> GROUP
192.xxx.xxx.222	ORIS	<server>	<unknown>	fc: ɬ:e9	ORIS <00> UNIQUE ORIS <20> UNIQUE WORKGROUP <00> GROUP WORKGROUP <1e> GROUP
192.xxx.xxx.224	RBENAVIDES	<server>	<unknown>	68 ɔ:c9	RBENAVIDES <20> UNIQUE RBENAVIDES <00> UNIQUE WORKGROUP <00> GROUP WORKGROUP <1e> GROUP
192.xxx.xxx.218	EDBSUB	<server>	<unknown>	a0:ɜ :ab	EDBSUB <20> UNIQUE EDBSUB <00> UNIQUE WORKGROUP <00> GROUP WORKGROUP <1e> GROUP
192.xxx.xxx.237	SISTEMAS04	<server>	<unknown>	90: ⁷:18	SISTEMAS04 <20> UNIQUE SISTEMAS04 <00> UNIQUE WORKGROUP <00> GROUP

Capítulo V

5. Fase de Intrusión.

Esta fase se focaliza en realizar pruebas de las vulnerabilidades encontradas mediante secuencias controladas propias para los sistemas identificados, aquí se utilizará el conocimiento adquirido en etapas previas para buscar alternativas que permitan acceder a los sistemas o a datos relevantes de la empresa y obtener el control de los mismos.

En esta fase se determinará la eficiencia del equipo que lleva a cabo el Test de penetración.

Esta etapa puede llegar a ser la más compleja y delicada de todas, así como la más satisfactoria para el equipo de trabajo debido a los resultados a obtener, donde se verá reflejado en mayor medida el conocimiento y profesionalismo del mismo. (Alfon, Seguridad y Redes, 2010)[27]

Durante esta etapa se utiliza todas las herramientas e información disponibles para evaluar todas las alternativas posibles que nos permitir efectuar una intrusión y escalamiento de privilegios exitosa.

Es importante que nuestro cliente esté informado de aquellas pruebas que puedan acarrear problemas en el funcionamiento de servicios, de modo que se requiere una planificación en conjunto para determinar el momento más indicado para realizar las tareas (Montero, Técnicas del penatration testing, 2015)[28].

5.1 Planificación de la Intrusión.

Planificar la intrusión es un proceso en el cual se debe reunir el equipo de penetración con nuestro cliente y realizar un cronograma con fechas específicas donde se llevaran a cabo las pruebas de penetración, generalmente en días no laborales o de baja afluencia, se debe

[27] Alfon. (2010). *Seguridad y Redes.* Obtenido de http://seguridadyredes.wordpress.com

[28] Montero, V. H. (2015). *Técnicas del penatration testing.* Buenos Aires: CYBSEC.

recordar que se está manipulando un bien invaluable como es la información y consecuentemente esta necesita de un correcto trato y manipulación.

5.2.Determinación y configuración de ataques.

Antes de realizar las pruebas se debe determinar el tipo de ataque a utilizar tomando en cuenta el sistema sobre el cual se actuará, este puede ser desde un cableado eléctrico hasta un sistema computacional. Una vez que se ha definido nuestro sistema se debe revisar si se posee todos los datos necesarios para la configuración del ataque como (IP, MAC, DOMINIO, CVE de la víctima, etc.).

Ya con esto podemos escoger cual será el ataque más apropiado entre los cuales tenemos los siguientes:

- Denegación de servicio, también llamado ataque DoS (Denegación de Servicio), es un ataque a un dispositivo, sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.
- Man in the middle, a veces abreviado MitM, es una situación donde un atacante supervisa (generalmente mediante un rastreador de puertos) una comunicación entre dos partes y falsifica los intercambios para hacerse pasar por una de ellas.
- Ataques de REPLAY ó ARP, una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado.
- Ataque de día cero, ataque realizado contra un ordenador, a partir del cual se explotan ciertas vulnerabilidades, o agujeros de seguridad de algún programa o programas antes de que se conozcan las mismas, o que, una vez publicada la existencia de la vulnerabilidad, se realice el ataque antes de la publicación del parche que la solvente.
- Ataque por fuerza bruta. No es necesariamente un procedimiento que se deba realizar por procesos informáticos, aunque este sistema ahorraría tiempos, energías y esfuerzos. El sistema de ataque por fuerza bruta, trata de recuperar una clave probando todas las

combinaciones posibles hasta encontrar aquella que se busca, y que permite el acceso al sistema, programa o archivo en estudio. (SYKRAYO Y LAS F.C.S)[29]

5.3.Ataques de fuerza bruta sobre servicios de autenticación.

Este es uno de los métodos más empleados para romper seguridades de los sistemas protegidos por autenticación el cual aprovecha del ser humano como vulnerabilidad, esto debido a que las personas no utilizan contraseñas que sean lo suficientemente difíciles de adivinar, como por ejemplo una combinaciones de letras, números, caracteres especiales y una longitud mayor a 8 caracteres de forma que implique un mayor grado de complejidad, esto sucede debido a que los usuarios para no olvidar sus contraseñas prefieren usar combinaciones sencillas como sus nombres y apellidos o fechas de nacimiento. (ÁLVAREZ, s.f.)[30]

En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso, es decir define al procedimiento por el cual a partir del conocimiento del algoritmo de cifrado empleado y de un par texto claro/texto cifrado, se realiza el cifrado (respectivamente, descifrado) de las posibles combinaciones de clave. (wikipedia, 2013)[31]

Se debe tomar en cuenta que la complejidad impuesta por la cantidad de caracteres en una contraseña es logarítmica pero involucra un coste en tiempo computacional demasiado alto dado que utilizan el método de prueba y error.

Tabla 5-1 Dificultad de contraseñas según longitud y variedad de caracteres

Longitud	Minúscula	Mayúsculas	Números y Símbolos
6 caracteres	10 min.	10 horas	18 días
7 caracteres	4 horas	23 días	4 años
8 caracteres	4 días	3 años	463 años
9 caracteres	4 meses	178 años	44.530os

[29] *SYKRAYO Y LAS F.C.S.* (s.f.). Obtenido de https://sites.google.com/site/sykrayolab/ataques-informaticos

[30] ÁLVAREZ, C. (s.f.). *www.informatica-juridica.com*. Recuperado el 18 de 11 de 2014, de www.informatica-juridica.com: http://www.informatica-juridica.com/trabajos/Ataques_de_fuerza_bruta.asp

[31] *wikipedia.* (9 de Marzo de 2013). Obtenido de http://es.wikipedia.org/wiki/Ataque_de_fuerza_bruta

5.4.Ingeniería Social.

La ingeniería social se define como el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros. (Hack Story, 2013)[32]

No hay un limitante respecto al tipo de información que se pueda obtener ni mucho menos la utilización que se le pueda dar a esta. Puede ser visto como un ataque de ingeniería social el obtener de un profesor las preguntas de un examen hasta la obtención de la clave de acceso de la caja fuerte de una institución bancaria, llegando a su fin dicho ataque social en el momento en el que se ha obtenido la información buscada.

Las formas de ataque son muy variadas ya que dependen de la imaginación del atacante y sus intereses, pero por lo general los ataques se realizan en dos niveles el físico y el psicosocial. El primero describe los recursos y medios a través de los cuales se llevará a cabo el ataque, y el segundo es el método con el que se engañará a la víctima. (Castellanos, 2011)[33]

Formas usadas a nivel físico:

- Ataque por teléfono. Este tipo de ataque es uno de los más usados donde el atacante realiza una llamada telefónica a la víctima haciéndose pasar por alguien más, como un técnico de soporte o un empleado de la misma organización aprovechando de su anonimato, pues las expresiones del rostro no son reveladas y lo único que se requiere es un teléfono.
- Ataque vía Internet. En internet se puede llevar a cabo una variedad de ataques siendo los más comunes: por correo electrónico (obteniendo información a través de un phishing o infectando el equipo de la víctima con malware), web (haciendo llenar a

[32] http://hackstory.net/Ingenier%C3%ADa_social

[33] Castellanos, E. J. (4 de Mayo de 2011). revista.seguridad.unam.mx. Recuperado el 3 de 12 de 2014, de revista.seguridad.unam.mx: http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

la persona objetivo un formulario falso) o inclusive conversando con personas específicas en salas de chat, servicios de mensajería o foros.

- Dumpster Diving o Trashing (zambullida en la basura). Consiste en buscar información relevante en la basura, como: agendas telefónicas, organigramas, agendas de trabajo, unidades de almacenamiento (CD's, USB's, etc.), entre muchas otras cosas.
- Ataque vía SMS. Ataque que aprovecha las aplicaciones de los celulares. El intruso envía un mensaje SMS a la víctima haciéndola creer que el mensaje es parte de una promoción o un servicio, luego, si la persona lo responde puede revelar información personal, ser víctima de robo o dar pié a una estafa más elaborada.
- Ataque vía correo postal. Uno de los ataques en el que la víctima se siente más segura, principalmente por la fiabilidad del correo postal. El perpetrador envía correo falso a la víctima, tomando como patrón alguna suscripción de una revista, cupones de descuento, etc. Una vez que diseña la propuesta para hacerla atractiva, se envía a la víctima, quien si todo sale bien, responderá al apartado postal del atacante con todos sus datos.
- Ataque cara a cara. El método más eficiente, pero a la vez el más difícil de realizar. El perpetrador requiere tener una gran habilidad social y extensos conocimientos para poder manejar adecuadamente cualquier situación que se le presente. Las personas más susceptibles suelen ser las más "inocentes", por lo que no es un gran reto para el atacante cumplir su objetivo si elige bien a su víctima.

Formas usadas a nivel psicológicol:

- Mostrar familiaridad. El atacante aprovecha la confianza que la gente tiene en sus amigos y familiares, haciéndose pasar por cualquiera de ellos. Un ejemplo claro de esto ocurre cuando un conocido llega a una fiesta con uno de sus amigos. En una situación normal nadie dudaría de que ese individuo pudiera no ser de confianza. Pero ¿de verdad es de fiar alguien a quien jamás hemos tratado?
- Crear una situación hostil. Crear una situación hostil provoca el suficiente estrés para no revisar al intruso o responder sus preguntas.

- Compartir el ambiente laboral. Cuando la recompensa lo amerita, estar cerca de la víctima puede ser una buena estrategia para obtener toda la información necesaria. Muchas pequeñas y medianas empresas no realizan una revisión meticulosa de los antecedentes de un nuevo solicitante, por lo que obtener un empleo donde la víctima labora puede resultar fácil.
- Leer el lenguaje corporal. El lenguaje corporal puede generar, con pequeños detalles una mejor conexión con la otra persona. Respirar al mismo tiempo, corresponder sonrisas, ser amigable, son algunas de las acciones más efectivas. Si la víctima parece nerviosa, es bueno reconfortarla. Si está reconfortada se tiene mayores posibilidades de que la víctima seda.
- Explotar la sexualidad. Jugar con los deseos sexuales de las personas, esto requiere una gran capacidad de manipulación, ya que se debe lograr que el individuo baje sus defensas y su percepción para obtener nuestro objetivo, esto sucede con mayor certeza en los hombres.

5.4.1. Ataque de ingeniería social sobre usuarios de Facebook.

En este caso aremos uso de la herramienta Social-Engineer Toolkit (SET) la cual se encuentra incorporada en el sistema kali Linux, SET es una software que posee un conjunto de herramientas especializadas para realizar ataques de Ingeniería Social en auditorías de seguridad, es programado en Python por David Kennedy siendo su principal objetivo automatizar y facilitar las tareas del experto en seguridad. (TrustedSec)[34]

Esta herramienta posee algunos tipos de ataques que podríamos clasificarlos en:

- **Spearphishing.** Es una técnica muy parecida al phishing, con la gran diferencia que esta es una estafa focalizada donde se establece y delimita nuestra víctima, principalmente un grupo u organización específicos para posteriormente mediante correo electrónico enviar un link de un sitio web que se encuentra lleno de malware cuyo objetivo es obtener acceso no autorizado a datos confidenciales. (KasperskyLab)[35]

[34] https://www.trustedsec.com/social-engineer-toolkit/
[35] http://latam.kaspersky.com/internet-security-center/definitions/spear-phishing

- **Sitios Web.** En este caso lo que se busca es clonar una página web y remplazarla con la original, mediante el envio de un link a la víctima haciéndole creer que es la página original, o con la manipulación del servidor de dominios para que se acceda siempre a dicho sitio, lo que se intenta es hacer creer a nuestra victima que está accediendo a un sitio seguro de forma que esta provea sus datos personales (usuario y contraseña).
- **USB malicioso.** Este ataque consiste en crear un archivo ejecutable que tendrá cargado en su interior un exploit el cual se ejecutará en el equipo de la víctima, permitiéndole al atacante según el tipo de exploit usado desde tener el control del dispositivo hasta sustraer sensible.

A continuación se muestra el proceso a seguir para realizar un ataque de ingeniería social basado en la clonación de un sitio web, en este caso uno muy conocido como Facebook, siendo lo primero cargar la herramienta Social Engineer Toolkit.

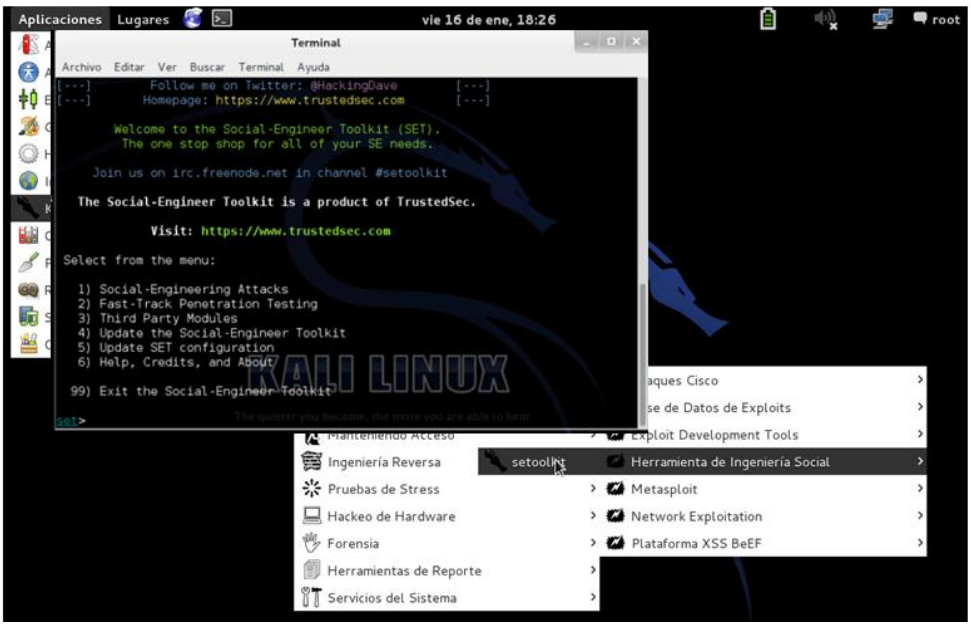


Figura 5-1 Inicio de la herramienta social engineer toolkit (set) en kali linux

Ahora procederemos a realizar el ataque de ingeniería social para lo cual escogeremos la opción **1** que nos desplegará varias opciones de ataques a realizar.

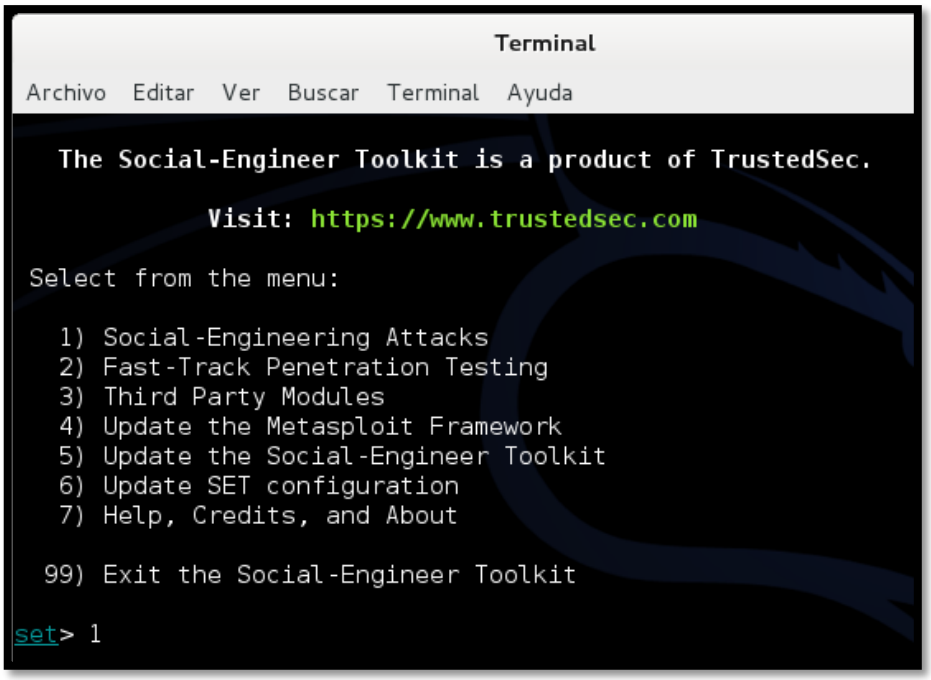


Figura 5-2 Despliegue del menú set y selección de set - attacks

Una vez hecho esto lo siguiente será realizar la clonación del sitio que usaremos como carnada para nuestras victimas para ello seleccionaremos la opción 2 de vectores de ataque a sitios web.

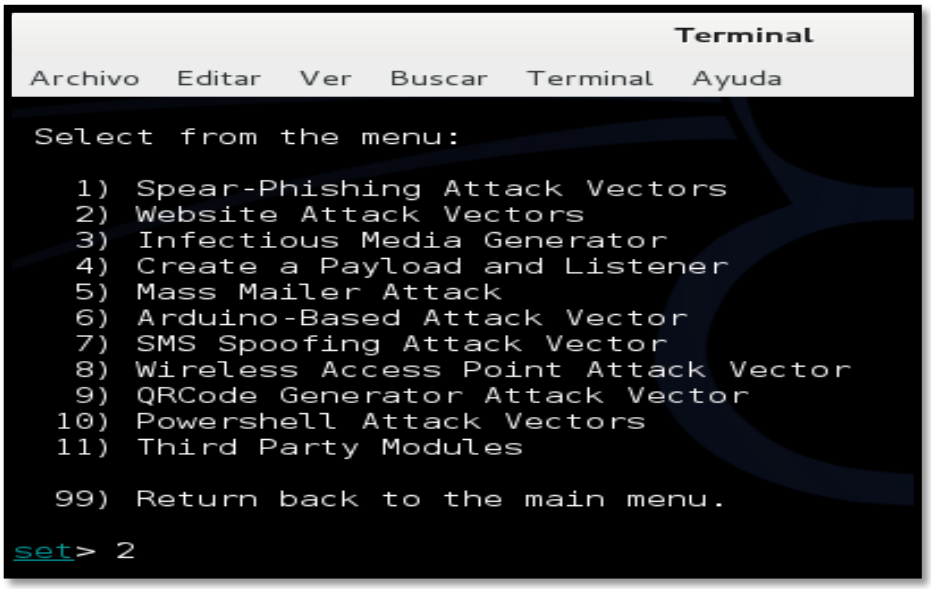


Figura 5-3 Selección de vectores de ataques a sitios web

A continuación se escogerá el método de ataque a realizar sobre el sitio web, este puede ser desde insertar código malicioso, crear un certifico u obtener las credenciales de la víctima, para esta demostración aremos uso del cosechador de credenciales, para esto escogeremos la opción tres.

Figura 5-4 Selección del método de ataque sobre el sitio web

Ya definido el ataque que se realizará ahora se procederá a crear la copia del sitio web, para esto se puede realizar un clon del sitio original, importar un modelo ya predefinido por el atacante o usar uno de los modelos que SET incluye en sus repositorios. En este caso realizaremos la clonación del sitio para lo cual definiremos la IP del atacante o un dominio y posterior se ingresará el URL del sitio a clonar.

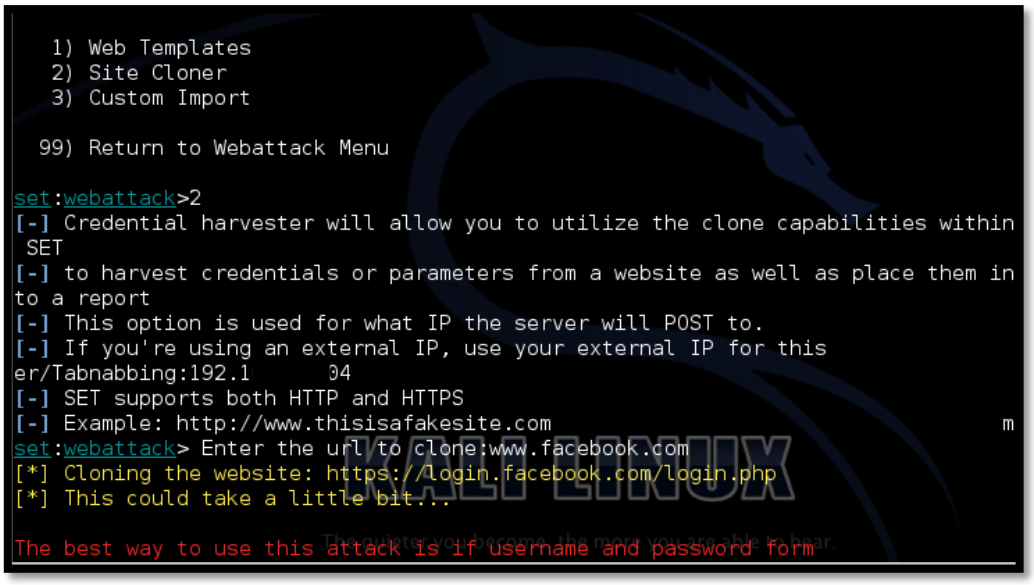


Figura 5-5 Clonación del sitio www.facebook.com

Finalmente SET se encuentra configurado y a la escucha de credenciales, donde ya clonado nuestro sitio bastará con enviar el link a nuestra víctima la cual ingresará sus credenciales y se las enviará al atacante al momento de presionar el botón de iniciar sesión.

Figura 5-6 Ingreso de credenciales del usuario

En la siguiente imagen se ve como SET recoge las credenciales ingresadas por el usuario, por lo que diremos que el ataque ha sido exitoso.

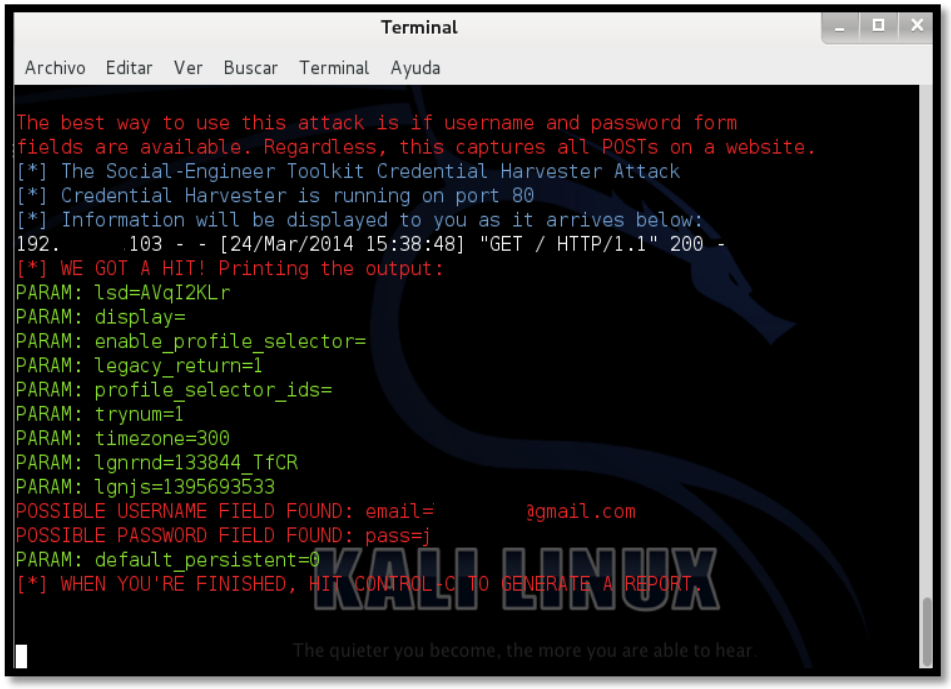


Figura 5-7 Recolección de credenciales por set

5.5.Intrusión a través de redes WLAN.

El Penetration test que se realiza en este trabajo de investigación, es un proceso para encontrar vulnerabilidades en los sistemas y redes de la empresa sin dejar de lado las redes inalámbricas lo que conducirá a un conjunto de mejores prácticas que mitiguen los riesgos de la Empresa.

Una vez encontradas las vulnerabilidades en las redes inalámbricas perteneciente a la empresa, se presentará un reporte técnico estructurado y consistente para proporcionar un conjunto de recomendaciones y prácticas que ayudarán a asegurar las redes inalámbricas del acceso de usuarios no autorizados por la empresa.

La herramienta que se utiliza para la intrusión a través de redes WLan y para realizar la auditoria de seguridad de las redes inalámbricas es Wifislax, ya que incluye varias herramientas avanzadas para comprobar la seguridad de los routers y descifrar claves.

Una de las herramientas que vienen integradas en wifislax es minidwep-pdk, la cual hemos utilizado para realizar el escaneo de las diferentes redes así como también la obtención del handshake para posterior realizar el ataque de diccionario.

5.5.1 Man in the middle.

Man in the middle (Hombre en el Medio) es un ataque que se emplea para referirse a manipulaciones activas de los mensajes, y no denota la interceptación pasiva de la comunicación de acuerdo a lo expuesto puede incluir algunos de los siguientes ataques:

- Intercepción de la comunicación, incluyendo análisis del tráfico.
- Ataques a partir de textos cifrados escogidos, en función de lo que el receptor haga con el mensaje descifrado.
- Ataques de sustitución.
- Ataques de repetición.
- Ataque por denegación de servicio (denial of service). Cuando se realiza este ataque, se bloquea las comunicaciones antes de atacar una de las partes. Que es precisamente lo que hace la herramienta de wifislax cuando obtiene el handhake para realizar el ataque de diccionario, lo que a continuación se detalla.

En el capítulo 3 se identificó los mecanismos de encriptación que utilizan las redes inalámbricas que pertenecen a la empresa a ser evaluada sin embargo se dará a conocer varios casos para poder acceder a las redes inalámbricas.

WEP

Se captura información específica que interesa mediante la tarjeta inalámbrica, de la red inalámbrica que se seleccionará y que obviamente utilice encriptación WEP, sin embargo este no es nuestro caso ya que no existen en la empresa redes que utilicen WEP, y dicho mecanismo ha sido sustituido por WPA y WPA2

WPA

Se captura información específica de la red inalámbrica que se seleccionará y que obviamente utilice encriptación WAP que interesa mediante la tarjeta inalámbrica, en este caso podemos identificar la red wifi con SSID wcgs como se muestra en la figura:

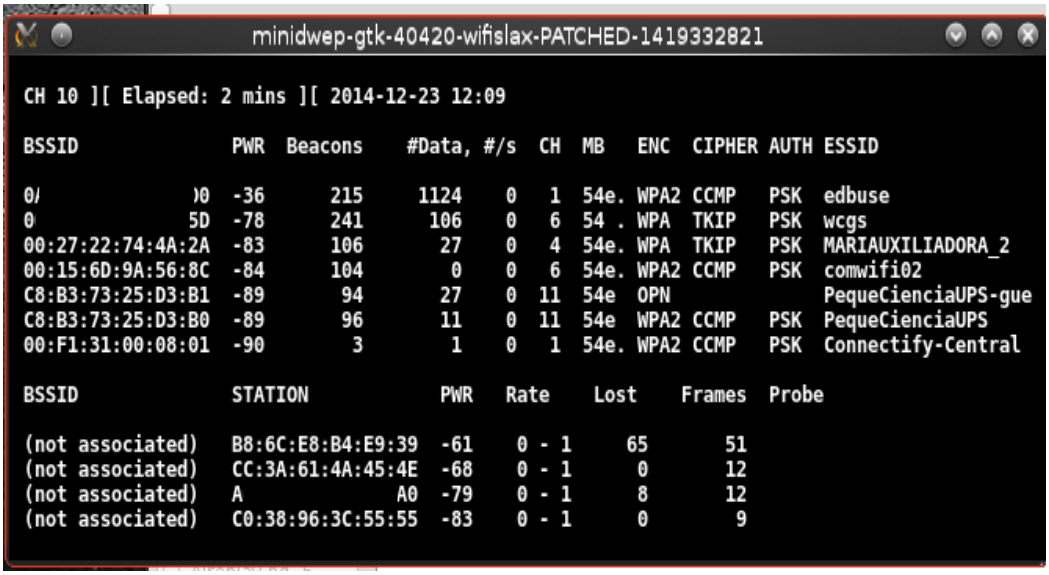


Figura 5-8 Identificación de las redes inalámbricas de la empresa mediante minidwep-gtk-40420 de wifislax

Luego de haber identificado todas las redes inalámbricas presentes, se procede a la elección de la red objetivo para tratar de romper la seguridad, para eso elegimos la red wcgs que como se puede observar cuenta con mecanismo de encriptación WPA. Todo lo dicho se ilustra en la figura 5-9.

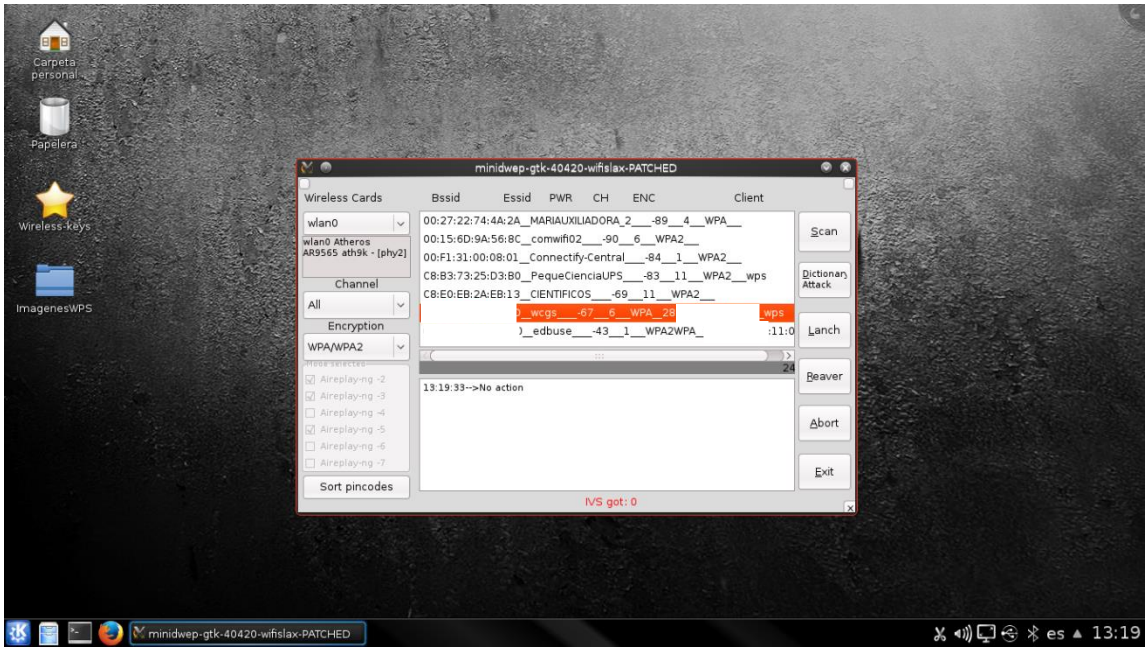


Figura 5-9 Selección de la red objetivo

Luego de presionar el botón launch de la herramienta se inicia la captura y se puede ver los usuarios conectados, sin embargo WPA se crackea por fuerza bruta y no descifrando mensajes como en el caso de WEP, lo que nos interesa es obtener el (handshake) que es el acuerdo entre el pc y el router de la forma en la que trabajaran. En la figura se muestra la obtención del hanshake.

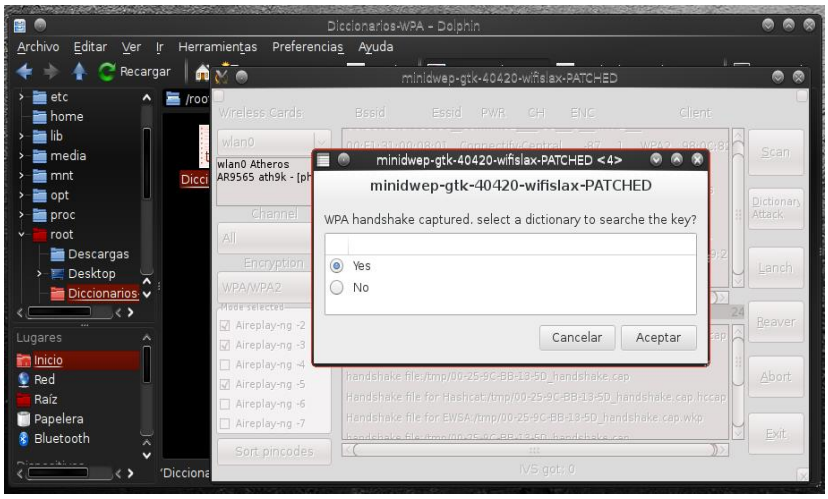


Figura 5-10 Obtención del Handshake

Al contar con el handshake se puede empezar a lanzar el ataque de fuerza bruta, para ello se procede a seleccionar el diccionario creado anteriormente el mismo que contiene una serie de combinaciones de letras y números para realizar el ataque.

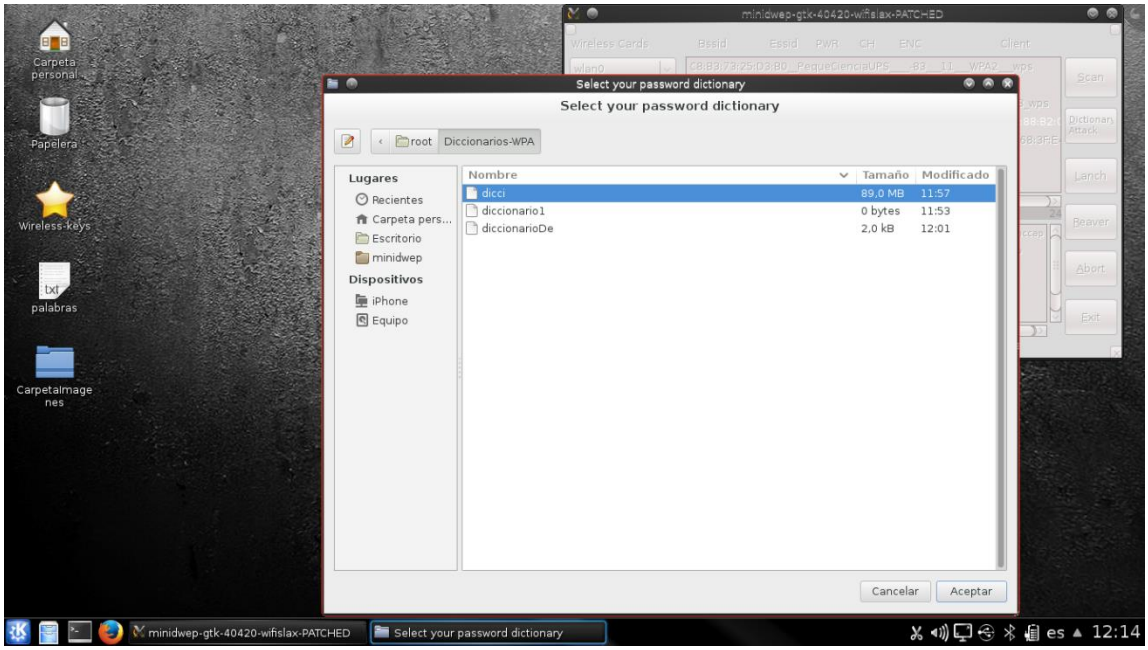


Figura 5-11 Selección del diccionario para el ataque

Una vez que aparece WPA KEY FOUND, se encuentra la clave de la red WPA, después ya que afortunadamente estaba en el diccionario que se utilizó. El tiempo que ha tomado obtenerla es de 3 horas 40 minutos.

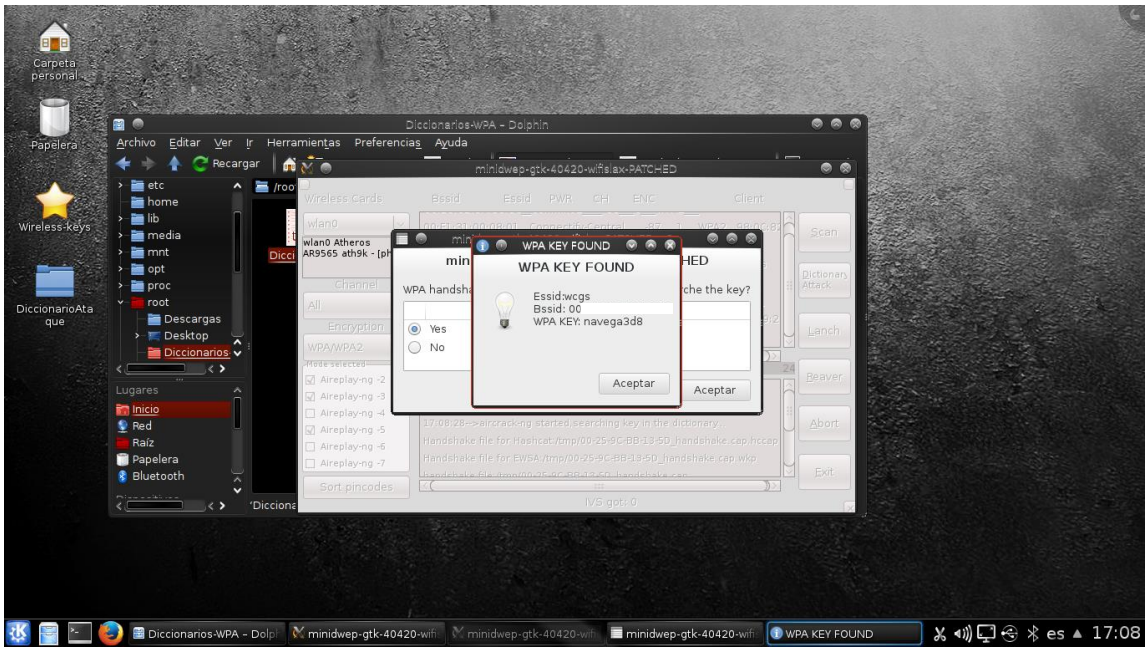


Figura 5-12 Clave encontrada en diccionario luego de 3 horas 40 minutos

WPA2

Es similar a WPA en los pasos que se detallaron anteriormente, ya que captura información específica de la red inalámbrica que utilice encriptación WAP2, en este caso la red wifi con SSID edbuse, como se muestra en la figura 5-13.

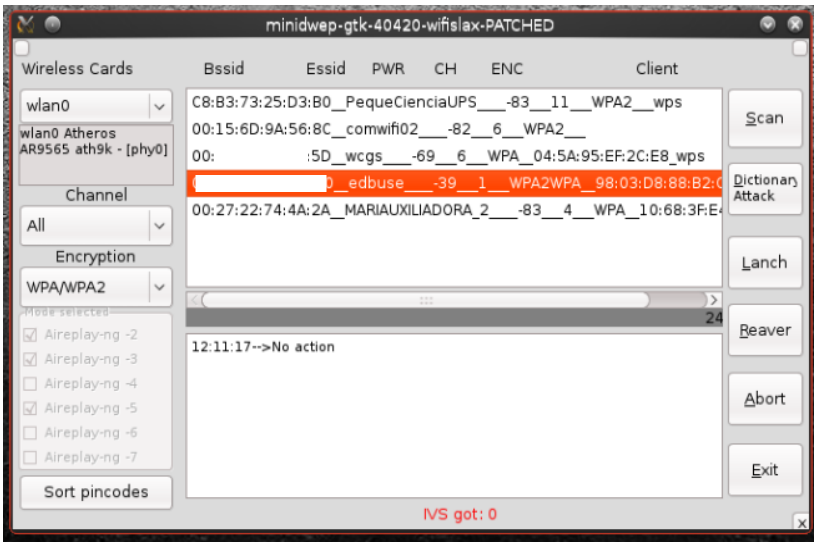


Figura 5-13 Selección de la red objetivo con encriptación WPA2

Por lo tanto luego de presionar el botón **launch** de la herramienta se inicia la captura y se puede ver los usuarios conectados, sin embargo WPA2 al igual que WPA se crackea por fuerza bruta, para lo que es necesario obtener el handshake.

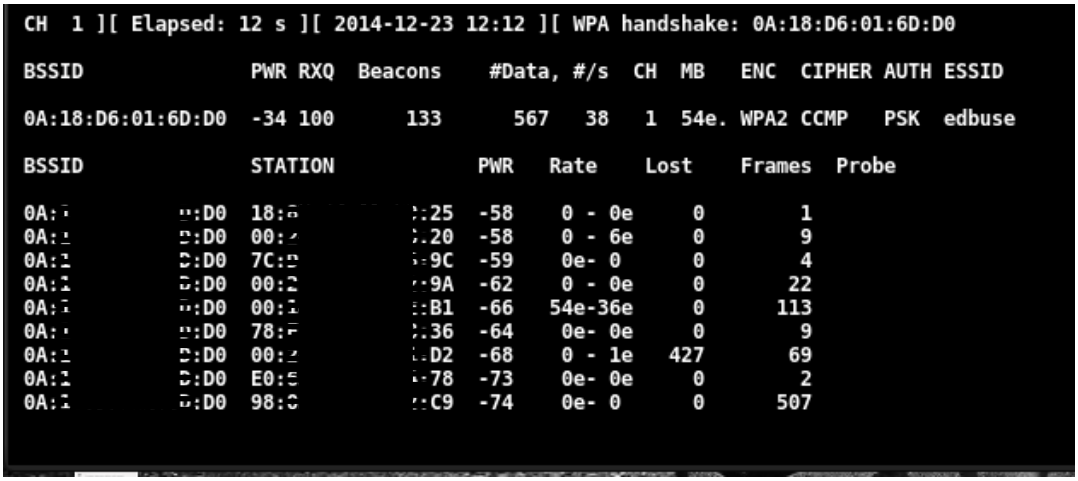


Figura 5-14 Captura de usuarios conectados a la red objetivo WPA2

Con el handshake capturado se puede empezar a realizar el ataque de fuerza bruta, con el diccionario creado anteriormente el mismo que contiene una serie de combinaciones de letras y números para realizar el ataque. En la figura 5-15 se muestra la obtención del hanshake.

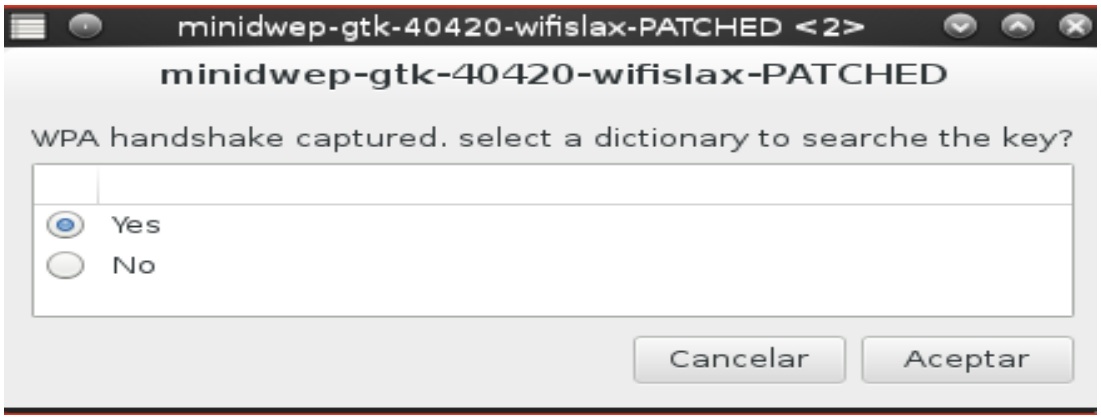


Figura 5-15 Obtención del handshake.

Una vez que aparece WPA KEY FOUND, se encuentra la clave de la red WPA2, ya que afortunadamente estaba en el diccionario que se utilizó.

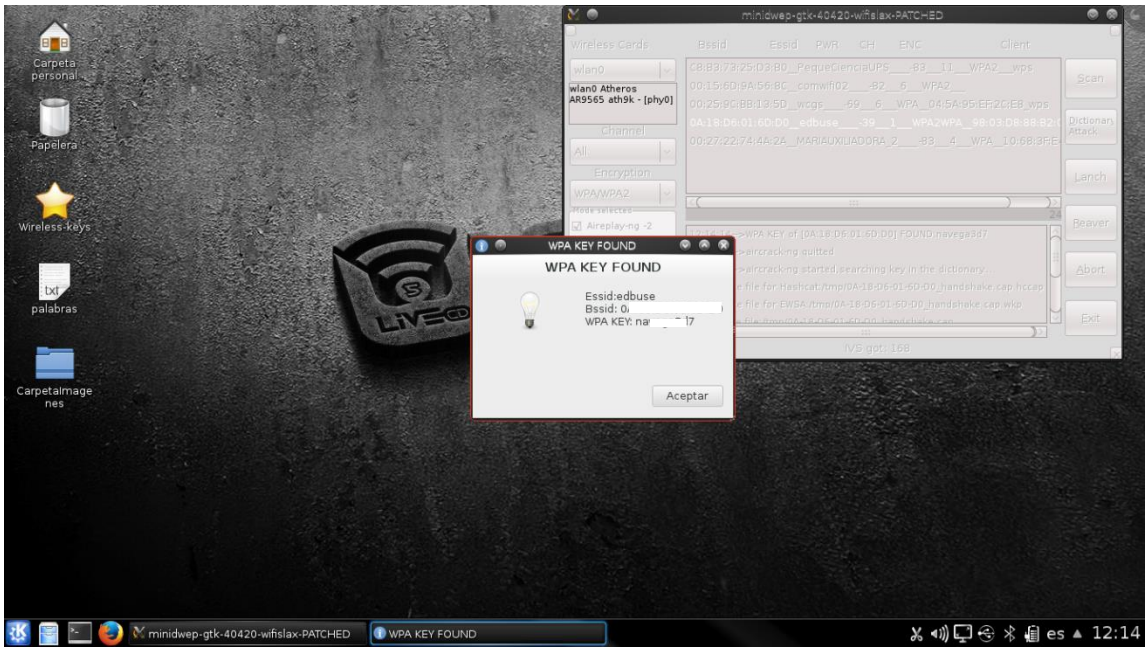


Figura 5-16 Clave encontrada

Cabe recalcar que los diccionarios fueron creados a parir de posibles combinaciones de palabras que maneja la empresa, es por eso que los ataques dieron resultado, sin embargo las contraseñas son robustas ya que tenían una extensión de 9 caracteres que combina números y letras.

5.5.2. Inyección de tráfico.

En redes wifi hay ataques que utilizan técnicas de inyección de tráfico para generar el tipo de tráfico que necesitamos. Por ejemplo en un ataque a una red con clave web la inexistencia de clientes puede causar que el ataque dure mucho tiempo, sin embargo existen herramientas que generar paquetes ARP en una red sin clientes y así poder usar dichos paquees para inyectar tráfico con aireplay.

5.5.3. Ataques del lado del cliente.

El ataque del lado del cliente consiste en crear e infectar un archivo malicioso con el fin de obtener acceso a la computadora victima por la red local. Para ello tenemos nuestra maquina victima que se trata de un equipo perteneciente a la empresa, y nuestra máquina atacante el cual tiene instalado kali Linux. El archivo malicioso lo crearemos utilizando la herramienta metasploit que viene incorporada en Kali Linux.

En la siguiente figura se muestra la inicialización de metasploit y los respectivos comandos para realizar el ataque del lado del cliente.

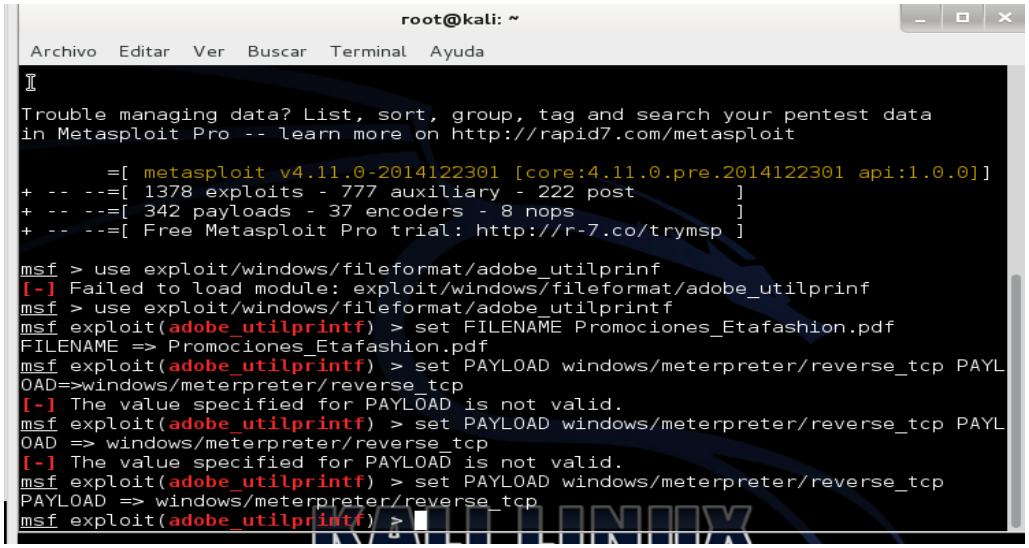


Figura 5-17 Inicialización y creación del archivo malicioso

A continuación se define el nombre con el cual pretendemos engañar a la víctima , el nombre del archivo debe insentivar a que la victima se sienta interesado en abrir dicho archivo, y tambien se configura la ip y el puerto de maquina atacante como se muestra en la siguiene figura.

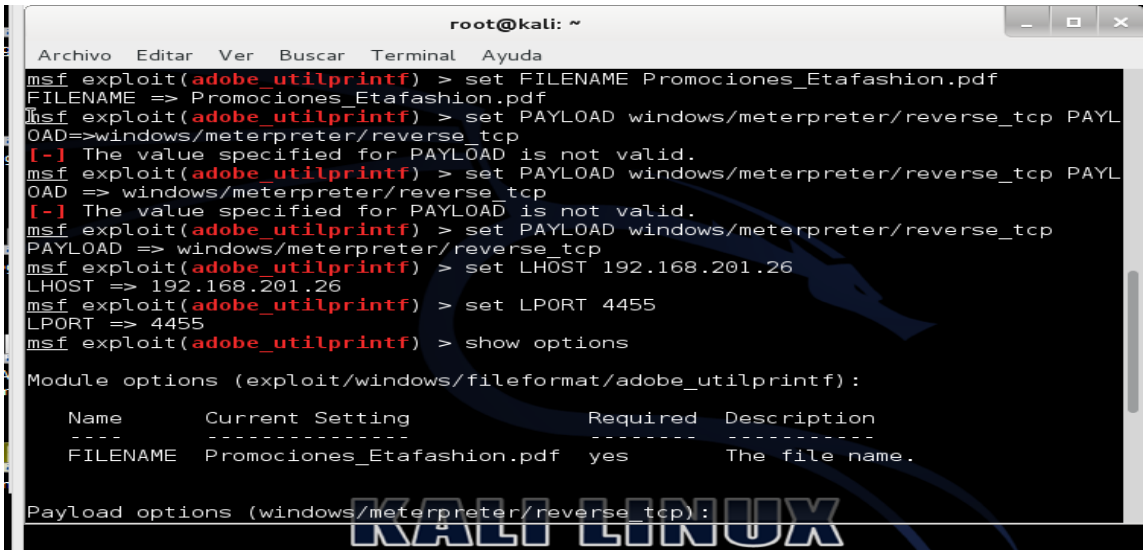


Figura 5-18 Definición del nombre y configuración de la maquina atacante

El archivo se crea en una ruta la cual se muestra en la siguiente figura:

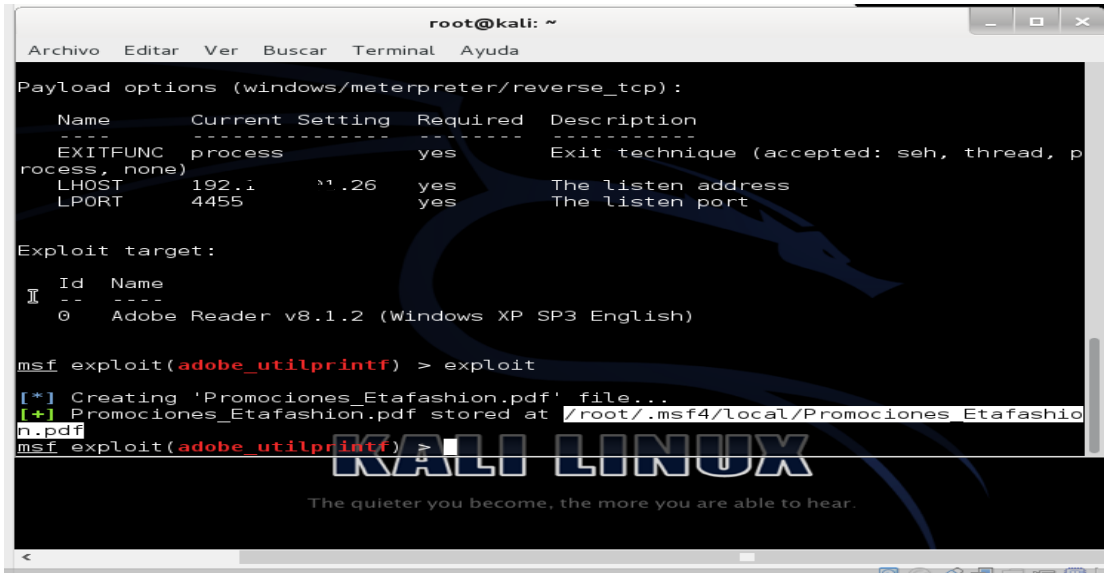


Figura 5-19 Ruta en la que se crea el archivo malicioso

Luego de haber creado dicho archivo es necesario enviarlo a la víctima ya sea por correo o páginas sociales. La siguiente figura muestra que el archivo malicioso fue copiado en la máquina a ser atacada.

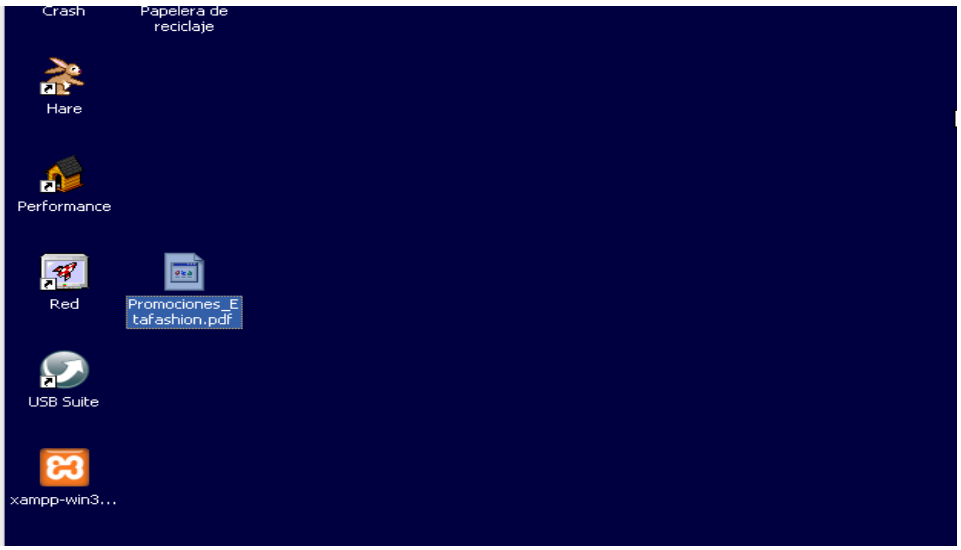


Figura 5-20 Archivo malicioso en máquina de la víctima

A continuación ejecutamos el exploit para poder acceder a la máquina víctima

Figura 5-21 Ejecución del exploit

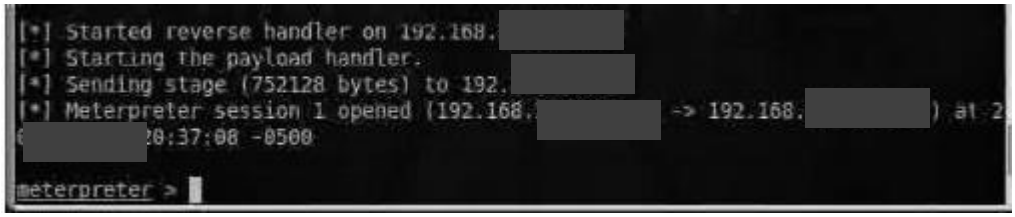


Figura 5-22 Acceso a la máquina de la víctima

Luego de acceder a la máquina de la víctima se puede ver todo lo que esta contiene.

5.5.4. Denegación de servicio.

Los ataques de Denegación de Servicio sobre redes inalámbricas son ataques que se pueden realizar con varias herramientas y son difíciles de detectar, ya que cuando una red inalámbrica no está disponible y sus usuarios no pueden realizar sus tareas, el hacker habrá conseguido el objetivo de denegar el servicio. A continuación se presenta un ejemplo de este ataque utilizando arimong-ng y aireplay-ng de kali lunux:

- Con el comando airmon-ng start wlan0 ponemos la tarjeta de red en modo monitor
- Con el comando airmon-ng –c 8 mon0 revisamos el canal del punto de acceso y ponemos en modo monitor en ese canal específico donde 8 es el canal del AP y mono es la tarjeta en modo monitor.
- Para realizar la denegación de servicio a AP(Punto de Acceso) se utiliza el comando aireplay-ng -0 0 –a (mac del AP) mon0, el mismo que envía paquetes de desautenticación en un bucle infinito (-0 0) al punto de acceso.

- Por otra parte si queremos realizar denegación de servicio al cliente enviamos paquetes de desautenticación en un bluque infinito a un cliente determinado con el siguiente comando: airplay-ng -0 0 –a (Mac del AP) -c mac del cliente.

5.6.Intrusión a redes de VOIP

VoIP (Voice Over Internet Protocol) o voz sobre IP, hace referencia a la emisión de voz en paquetes IP sobre redes de datos como puede ser Internet permitiendo la transmisión de voz y la de datos a la vez. (Gil, Seguridad en VoIP: Ataques, Amenazas y Riesgos, 2012)[36]

La tecnología VoIP trata de transportar la voz previamente procesada, encapsulándola en paquetes para poder ser transportadas sobre redes de datos sin necesidad de disponer de una infraestructura telefónica convencional. De esta forma se consigue crear una única red homogénea en la que se envía todo tipo de información obteniendo múltiples ventajas siendo la principal el proporcionar varios servicios sobre un mismo medio.

Una red de este tipo incorpora ciertos inconvenientes siendo los principales la seguridad, la fiabilidad y la Calidad de Servicio. En este caso analizaremos uno de sus factores más críticos como es la seguridad, teniendo en cuenta que VoIP es una tecnología basada sobre el protocolo IP y UDP respecto a la capa de transporte existe la posibilidad de que los paquetes puedan perderse o sean intersectados, esto se debe tener muy en cuenta ya que nuestro tráfico circulará por redes potencialmente inseguras como internet o una simple red LAN, esto plantea riesgos a nivel de la confidencialidad, integridad y disponibilidad.

5.6.1. Protocolos, estándares y funcionamiento SIP.

VoIP trabaja con un conjunto de protocolos lo cual abre una gran brecha para posibles ataques sobre este sistema, siendo sus principales H.323 y SIP.

H.323 es una recomendación de la ITU que define los protocolos para la comunicación multimedia a través de redes de paquetes el cual ha evolucionado para brindar soporte y convertirse en un estándar de VoIP, constituyéndose en un conjunto de normas ITU para

[36] Gil, R. G. (2012). *Seguridad en VoIP: Ataques, Amenazas y Riesgos.* Valencia - España: Universidad De Valencia.

comunicaciones multimedia que hacen referencia a los terminales, equipos y servicios estableciendo una señalización en redes IP. No garantiza una calidad de servicio, y en el transporte de datos puede, o no, ser fiable; en el caso de voz o vídeo, nunca es fiable.

SIP (Protocolo de Inicio de Sesiones) es un protocolo simple de señalización y control utilizado para telefonía y videoconferencia sobre las redes IP. Fue creado por el *IETF MMUSIC Working Group* y guarda cierta similitud en su estructura con protocolos como STMP(Simple Transportation Management Protocol o Protocolo Simple de Administración de Transporte) y HTTP (Hypertext Transfer Protocol o Protocolo de transferencia de hipertexto). Es un protocolo abierto y ampliamente soportado que no depende de ningún fabricante. Su simplicidad, escalabilidad y facilidad para integrarse con otros protocolos y aplicaciones lo han convertido en un estándar de la telefonía IP.

SIP es un protocolo de señalización por lo que solo maneja el establecimiento, control y terminación de las sesiones de comunicación. Una vez se ha establecido la llamada se produce el intercambio de paquetes mediante RTP (Protocolo de tiempo real) que transportan el contenido de la voz. Encapsula también otros protocolos como SDP utilizado para la negociación de las capacidades de los participantes, tipo de codificación, etc.

[37]SIP es un protocolo de aplicación y funciona sobre TCP y UDP el cual posee los siguientes componentes:

- Agentes de Usuario (UA) consta de dos partes, el cliente y el servidor. El primero genera peticiones SIP y recibe las respuestas, el segundo genera las respuestas a las distintas peticiones.
- Agentes de usuario cliente (UAC) que son los que inician las peticiones de llamada.
- Agentes de usuario servidor (UAS) que reciben las peticiones del UAC.

Dentro de una red estructurada SIP podemos encontrar cuatro tipo de servidores que se describen a continuación.

[37] http://www.redesyseguridad.es/voip-protocolo-sip/

- **Proxy Server**.- tiene la tarea de enrutar las peticiones de otras entidades más próximas a su destino. Actúa como cliente y servidor para el establecimiento de llamadas entre usuarios se pueden distinguir dos tipos, los stateful que mantienen el estado de las transacciones durante el procesamiento de las peticiones y permiten la división de una petición en varias y el otro tipo son los stateless, que al contrario no mantienen estado, únicamente se limitan a reenviar los mensajes.
- **Registrar Server.-** este servidor acepta peticiones de registro de los usuarios y guarda la información de estas para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.
- **Redirect Server**.- este genera respuestas de redirección a las peticiones que recibe y reencamina las peticiones hacia el próximo servidor.

5.6.2. Establecimiento la llamada.

Previo a tratar de establecer un enlace entre nuestros dispositivos primero se debe realizar el registro de los usuarios, ya con esto podemos iniciar con una petición INVITE hacia el Proxy Server que será el encargado de enrrutar el mensaje. El Proxy Server reenvía la petición al destinatario mediante un mensaje de información provisional (100 Trying), a continuación se envía un mensaje (180 Ringing) el cual alertará al destinatario de que hay una llama entrante, cuando este levanta la bocina se transmite un mensaje (200 OK) al emisor de la llamada. Una vez se hayan enviado los mensajes ACK la llamada se habrá establecido correctamente y se podrán enviar paquetes de voz mediante el protocolo RTP, una vez terminada la llamada se asienta la bocina y se envía un Bye indicando el término de la llamada o sesión para finalmente enviar un mensaje de confirmación (200 OK) indicando a que la llamada se ha establecido y ha sido cerrada con éxito

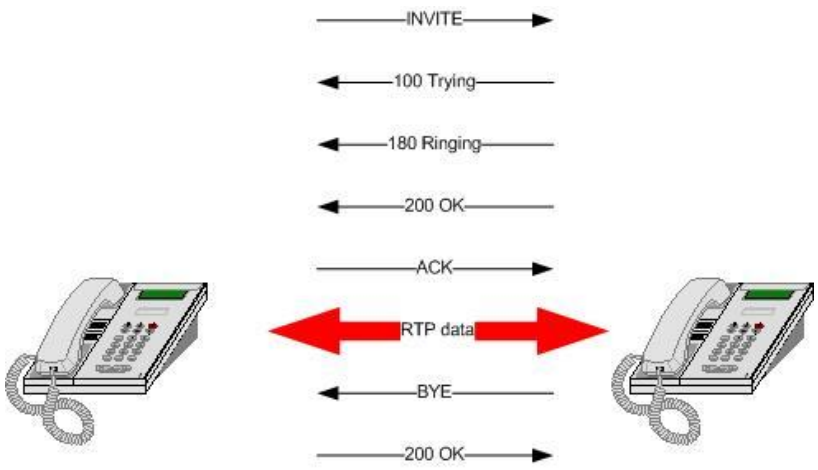


Figura 5-23 Llamada SIP entre 2 usuarios

Fuente: (Redes y Seguridad) [38]http://www.redesyseguridad.es/voip-protocolo-sip/

Al mantener cierta similitud con STMP y HTTP, SIP posee coditos de respuesta similares a los de HTTP, un código de retorno 200 significa OK, el 404 es no encontrado, la localización se basa en DNS y su funcionamiento incluye el intercambio de peticiones y respuestas que reciben el nombre de request line e incluyen el nombre del método a invocar, el identificador del destinatario y el protocolo SIP que se está utilizando. A continuación se muestra los métodos a invocar por SIP. (Wikipedia)[39]

Tabla 5-2 Métodos usados por el protocolo SIP para establecer una llamada

MÉTODO	**DESCRIPCIÓN**
INVITE	Permite invitar un usuario o servicio para participar en una sesión o para modificar parámetros en una sesión ya existente.
ACK	Confirma el establecimiento de una sesión.
OPTION	Solicita información sobre las capacidades de un servidor
BYE	Indica la terminación de una sesión
CANCEL	Cancela una petición pendiente de llamada.

[38] *Redes y Seguridad.* (s.f.). Obtenido de http://www.redesyseguridad.es/voip-protocolo-sip/

[39] *Wikipedia.* (s.f.). Obtenido de http://en.wikipedia.org/wiki/Session_Initiation_Protocol

REGISTER	Registrar al User Agent.

De igual forma que HTTP, SIP usa una serie de códigos correspondientes a las respuestas de los métodos:

Tabla 5-3 Mensajes de repuesta a métodos sip

1xx.	Mensajes de información. Provisionales (100 Trying)
2xx.	Respuesta de Exito. Se recibió el requerimento y es acpetado. (200 Ok)
3xx.	Respuesta de redirección. Se requiere de otros procesamientos antes de determinar si es posible la llamada. (302 Moved Temporaly) o (305 Utiliza Proxy).
4xx.	Respuesta de fallo en petición o fallo del cliente. (404 Not Found)
5xx.	Respesta de fallos en servidor a pesar de tratarse de un requerimiento valido. (504 Server Time-out) o (503 Servicio no disponible)
6xx.	Respuesta de fallos globales. (603 Decline)

En esta imagen se muestra un ejemplo de mensajes de información provisional representada por el código 100.

Figura 5-24 Captura de tráfico de un mensaje de respuesta con código 100

Ahora analizaremos un paquete correspondiente a un **método SIP** de tipo **Request**, en este caso particular un **INVITE** el cual se encarga de establecer la llamada o la sesión.

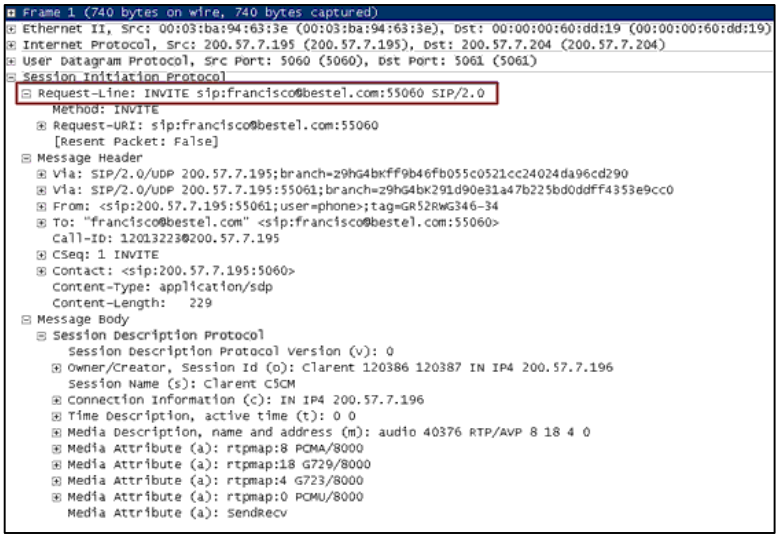


Figura 5-25 Captura del paquete de un método request tipo invite

Dentro de la cabecera del paquete hemos obtenido los siguientes parámetros:

- **Via.-** Campo que usado para el registro de ruta. De esta forma la respuesta seguirá el mismo camino que el Request o petición INVITE. También indica el tipo de protocolo de transporte usado (SIP/UDP) y el branch o identificación de la transacción.
- **From.-** Cliente que realiza la llamada o petición.
- **To.-** Cliente al que se realiza la petición.
- **Call-ID.-** Identificador único de la sesión. Identifica a los mensajes que corresponden a la misma llamada.
- **C-Seq**.- Número de secuencia.
- **Contact**.- URI SIP Contact address. Contiene la IP y puerto donde se va a realizar la petición INVITE y espera recibir resupesta.
- **Message Body o cuerpo del mensaje**.- contiene el Session Description Protocol SDP con los siguientes campos:
    - **Versión de Session Description Protocol. SDP.-** En este caso 0
    - **Propietario/Creador de la sesión o Owner/Creator**.- Se trata de una identificación formada por:
    - **Owner username**.- Usuario.
    - **Session ID o ID de la sesion**.- Número aleatorio como identificador único de la sesion.

- **Session Version.** - Versión.
- **Network Type**.- Tipe de red. Siempre IN.

Time Description, active time.- Aquí se indica el inicio y final de la sesión. En este caso tenemos (t): 0 0, es decir start time= o y stop time = 0. Esto significa que la sesión es Ilimitada y permanente.

Media Description, name and address (m).- audio 40376 RTP/AVP 8 18 4 0. Aquí tenenemos información sobre el tipo de datos que se transporta (audio o sesión telefónica en este caso), el puerto UDP usado (40376), el protocolo usado (RTP Real Time Transport Protocol /AVP Audio video Profiles). (Alfon, Seguridad y Redes, 2010)[40]

5.6.3. Interceptación de llamadas usando la vulnerabilidad No [9999] TLS.

Para explotar esta vulnerabilidad aremos uso de la herramienta CAIN Y ABEL la cual ha sido diseñada para la evaluación de la seguridad en un entorno cerrado, esta se encuentra disponible en su página oficial *http://www.oxid.it/cain.html* de forma gratuita y presenta diversas herramientas para: la recuperación de contraseña en sistemas operativos Windows, u otros diferentes mediante el escaneo de la red aprovechando grietas en los sistemas o descifrándolas mediante ataques de fuerza bruta, intervención y grabación de conversaciones VoIP, decodificación de contraseñas, recuperación de claves de redes WLAN, descubrimiento de contraseñas en caché y análisis de enrutamiento de protocolos. Es importante recalcar que este programa no explota ninguna vulnerabilidad de software o errores que no pudieron ser corregidos con poco esfuerzo. Cubre algunos aspectos de seguridad presente en protocolos, métodos de autenticación y mecanismos de almacenamiento en caché; su principal objetivo es la recuperación simplificada de contraseñas y credenciales de varias fuentes.

CAIN Y ABEL son dos herramientas distintas pero complementarias CAIN permite realizar análisis de paquetes, envenenamiento ARP y recuperación de contraseñas y ABEL ofrece la posibilidad de descifrar algoritmos, realizar ataques de fuerza bruta, etc. En

[40] Alfon. (2010). *Seguridad y Redes.* Obtenido de http://seguridadyredes.wordpress.com/2010/04/05/wireshark-captura-conversaciones-voip-protocolo-sip-sdp-y-rtp-extraccion-de-audio/

nuestro caso lo que aremos será realizar un análisis de tráfico con CAIN para encontrar paquetes SIP que nos entregará información acerca del usuario, duración de la llamada, etc. Y los paquetes RTP que como ya habíamos visto anteriormente son quienes contiene encapsulada la voz o el audio, pero para esto tenemos que realizar un ataque de MAN IN THE MIDLE mediante un envenenamiento ARP.

Lo primero que aremos será configurar nuestra interfaz de red a explorar y definiremos que tipo de paquetes vamos a analizar en este caso serán paquetes SIP y RTP.

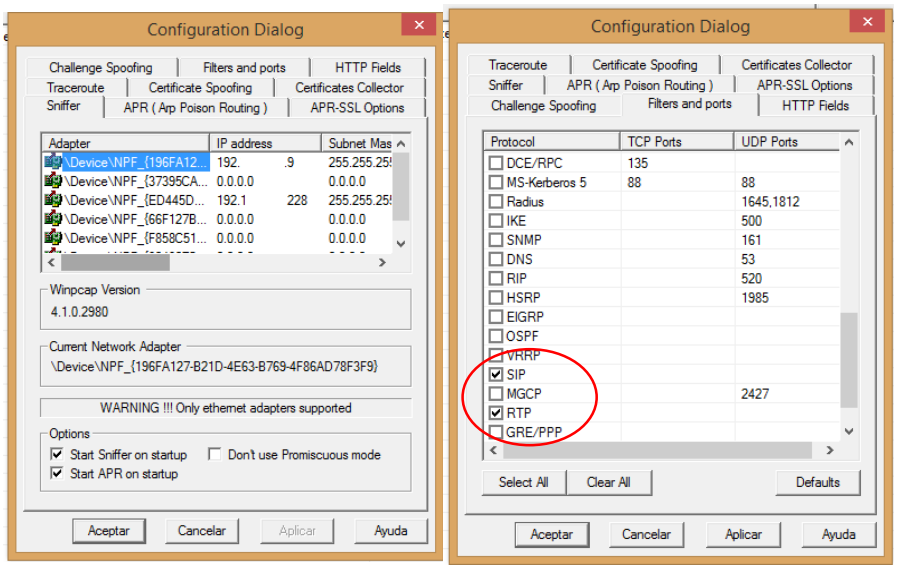


Figura 5-26 definición de la interfaz de red a usar y tipo de paquetes a analizar.

Ahora definiremos un rango un rango de direcciones IP a escanear para posteriormente usarlas en un ataque de envenenamiento ARP.

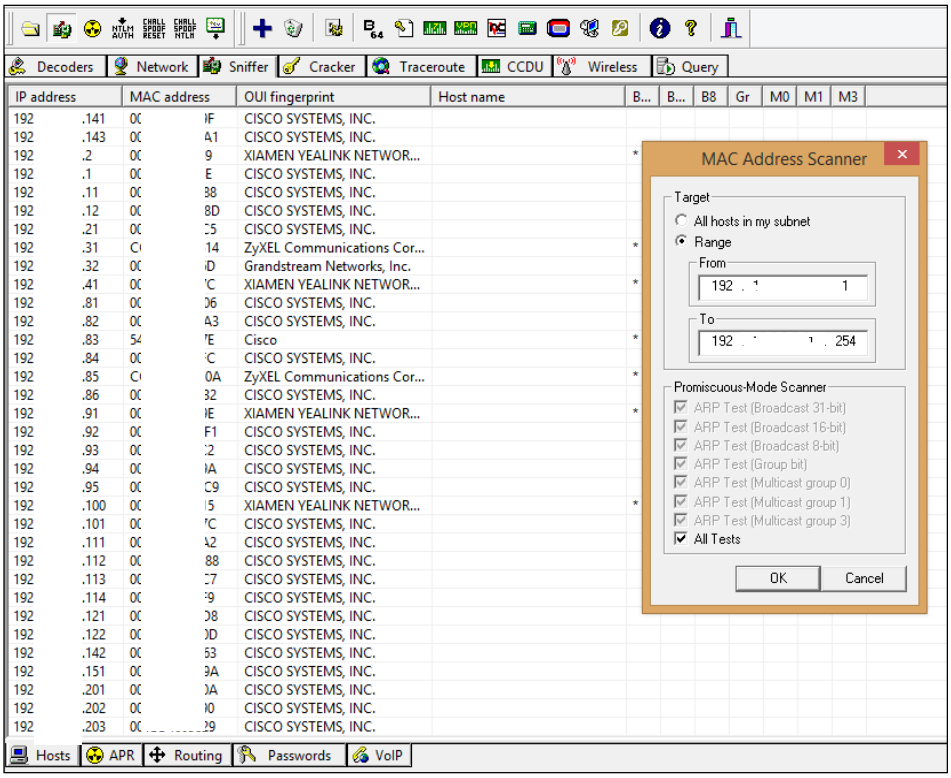


Figura 5-27 Definición de rango de ip´s a escanear

Una vez que ya hemos definido nuestro rango de IP a usar añadiremos los host a monitorear A y B respectivamente e iniciaremos el envenenamiento ARP para dar comienzo con la captura de paquetes.

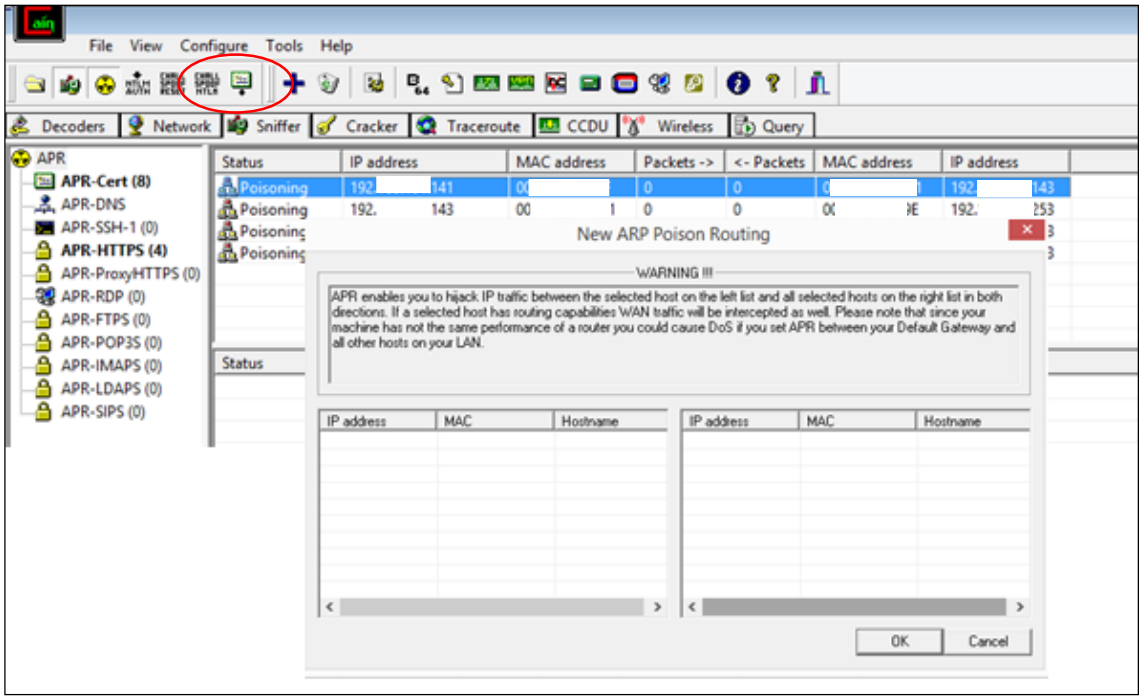


Figura 5-28 Añadiendo host a y b para envenenamiento ARP (Man in the Midle)

Ahora basta con dirigirse a la sección de VOIP del Sniffer para ver los paquetes RTP capturados, los cuales se encontraran ya decodificados listos para reproducirlos.

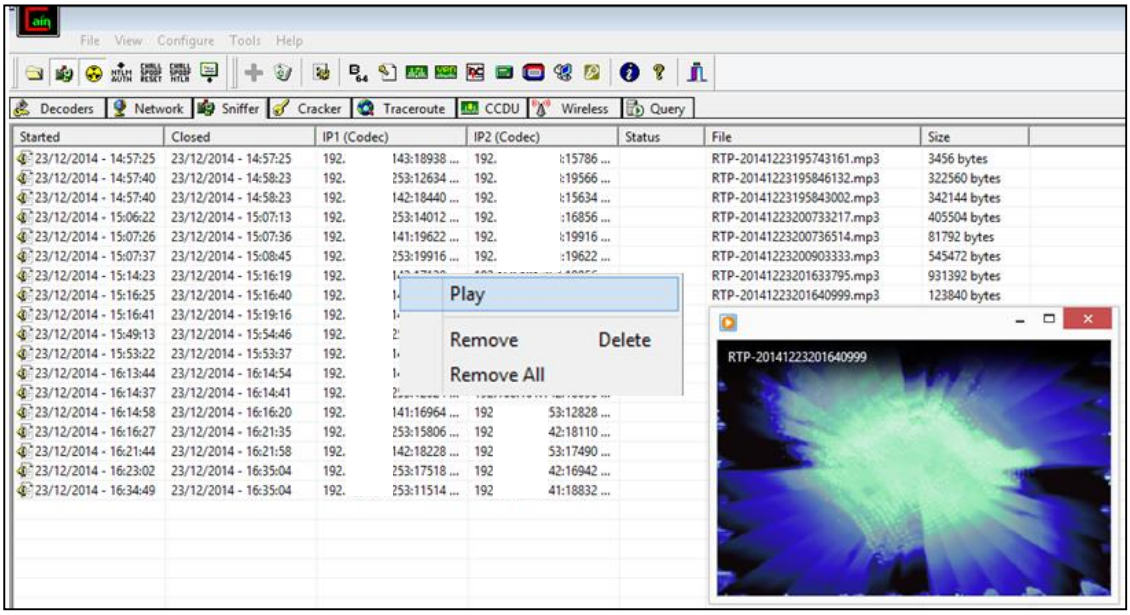


Figura 5-29 Reproducción de paquetes RTP

Con los paquetes SIP capturados CAIN toma los métodos REGISTER de los cuales se puede obtener SIP Hashes encriptados con MD5 a los cuales trataremos de desencriptar mediante el uso de ataques de fuerza bruta, en este caso nos interesa evaluar la seguridad del servidor ASTERISK por lo que tomaremos el hash MD5 de este equipo.

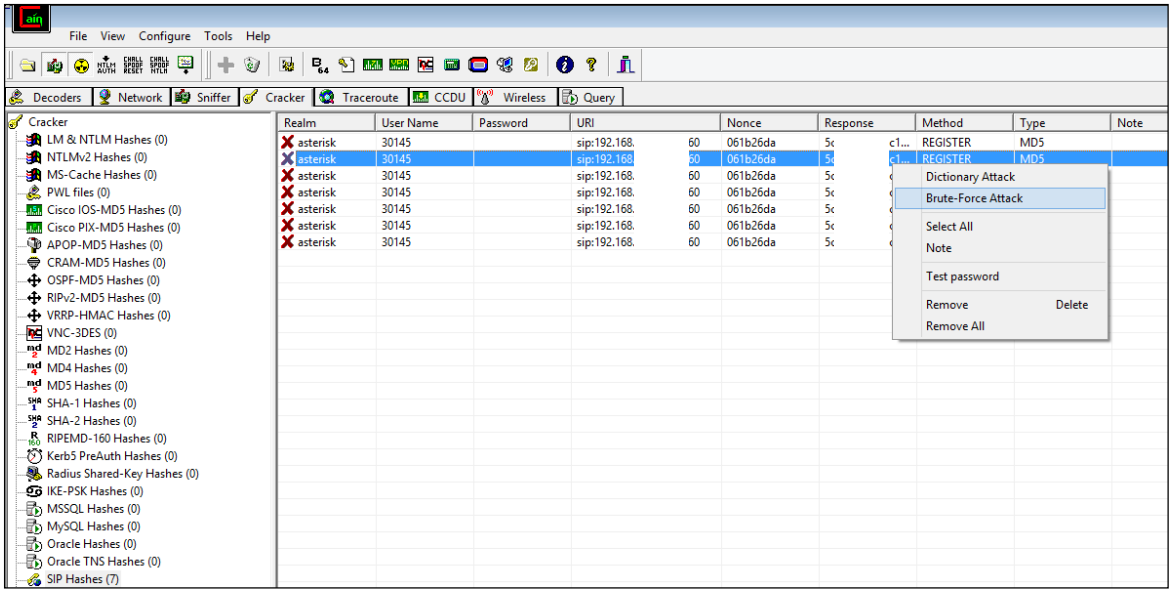


Figura 5-30 Ataques de fuerza bruta servidor asterisk

Se realiza la primera prueba con combinaciones de letras minúsculas y números con una longitud de cuatro caracteres con los cuales no se tuvo ningún resultado.

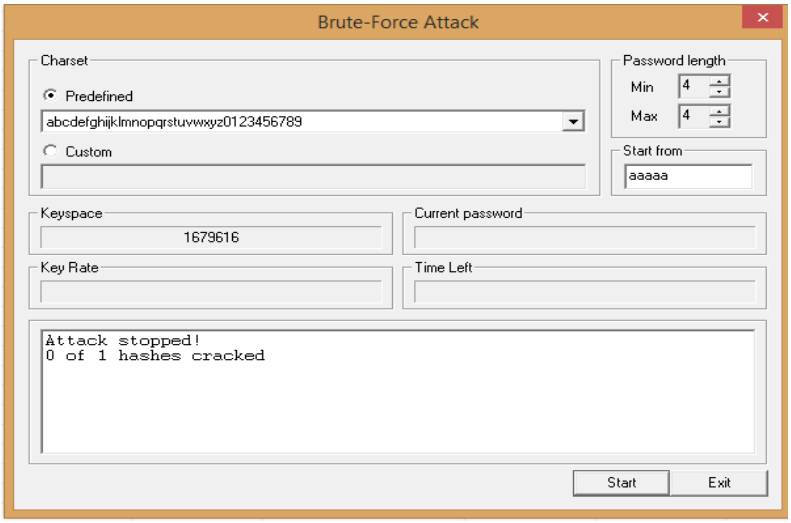


Figura 5-31 ataque de fuerza bruta con longitud de 4 caracteres y combinaciones de minúsculas y números

A continuación se prueba la misma combinación con 5, 6 y 7 caracteres sin tener ningún resultado positivo y se estima el tiempo que demoraríamos en descifrar la contraseña con una combinación más compleja y de mayor tamaño, deduciendo que la contraseña usada por este equipo es robusta.

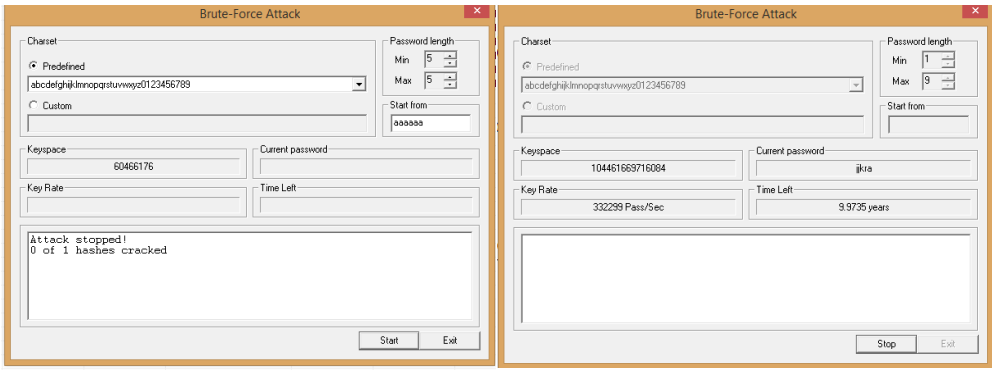


Figura 5-32 Ataque de fuerza bruta con longitud de 4 caracteres y combinaciones de minúsculas y números

5.7.Análisis de vulnerabilidades WEB.

Para llevar a cabo pruebas de penetración WEB aremos uso de la guía OWASP, la cual nos brindará una serie de procedimientos y sugerencias. Las pruebas de intrusión han demostrado ser efectivas en seguridad de redes pero esto no es igual en el caso de las aplicaciones. Cuando se realizan pruebas de intrusión en redes y sistemas operativos, todo el trabajo se centra en encontrar y explotar vulnerabilidades conocidas en tecnologías específicas, pero en el caso de las aplicaciones web que son casi todas echas según requerimientos específicos y cada una varía según su diseño, las pruebas de intrusión se asemejan mucho más a la investigación pura.

Existen herramientas que automatizan el proceso de intrusión pero por la naturaleza de las aplicaciones web no siempre resultan efectivas, esto se debe a que por lo general estas

herramientas se basan en un modelo específico según el tipo de tecnología usada y cada aplicación puede variar según su caso. (OWASP, 2008)[41]

5.7.1. Comprobación de vulnerabilidad OWASP Listado de directorios.

Si el servidor web se encuentra mal configurado será posible ver el listado de los directorios, estos listados pueden revelar guiones ocultos con información importante incluyendo archivos, archivos de configuración, copias de seguridad, etc., a los que se puede acceder para leer la información sensible. (OWASP, 2008)[42]

En la siguiente imagen se puede ver que mediante la manipulación directa de la URL se puede acceder a los directorios de la página web.

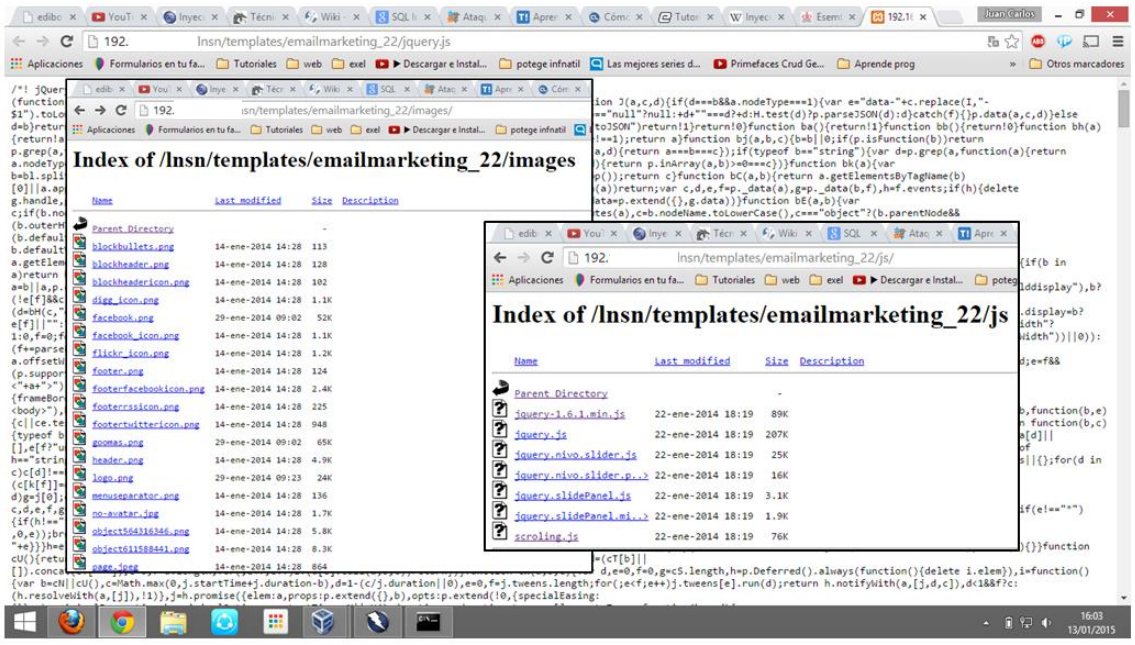


Figura 5-33 Listado de directorios de la página web

[41] OWASP. (2008). *Guia De Pruebas OWASP*. OWASP.

[42] OWASP. (2008). *Guia De Pruebas OWASP*. OWASP.

5.7.2. Comprobación de vulnerabilidades SQL injection.

[43]Un ataque de Inyección SQL consiste en la inserción de datos en una consulta SQL desde un cliente siendo su objetivo principal obtener acceso a la base de datos y posteriormente poder crear, actualizar, leer y borrar registros además de realizar operaciones administrativas.

Se podría decir que un ataque de este tipo consiste en enviar órdenes SQL que son inyectadas en el texto para afectar la correcta realización de una consulta SQL predefinida, pudiendo clasificar los ataques de Inyección SQL en:

- **Inband:** En este caso los datos se extraen usando el mismo canal que es usado para inyectar el código SQL, es decir que los datos recibidos se mostrarán en la propia aplicación web.
- **Out-of-band:** Al contrario del inband los datos son extraídos usando un canal diferente pudiendo ser este un correo con el resultado de la consulta realizada, etc.
- **Inferetial:** Con este ataque no hay transferencia de datos, pero el experto en seguridad deberá reconstruir la información enviando peticiones y observando el comportamiento que mantiene el servidor de bases de datos.

Siendo cualquiera el tipo de ataque a usar, el éxito de una correcta Inyección SQL dependerá de que tan bien se pueda [44]construir una consulta SQL, si la aplicación retorna un mensaje de error como resultado de una consulta incorrecta será fácil reconstruir de forma lógica la consulta original, en el caso de que la aplicación oculte los mensajes de error aremos uso de una Inyección SQL Ciega o Blind SQL Injeccion que consiste en intentar conseguir por medio de ingeniería inversa la lógica de la consulta original, refiriéndonos por lógica de la consulta a su estructura. (OWASP, 2014)

En el desarrollo de esta técnica será importante seguir los siguientes pasos y recomendaciones que nos permitirán conseguir el éxito de nuestras pruebas los cuales citamos a continuación.

[43] OWASP. (2008). *Guia De Pruebas OWASP*. OWASP.

[44] https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)

a) Primero debemos entender cuando nuestra aplicación se conecta a un servidor de bases de datos (BBDD) para acceder a algún dato, como: un formulario de autenticación, motores de búsqueda, etc.

b) Lo siguiente será comprobar tratar de generar un error para que nos retorne un mensaje con información que nos servirá de ayuda para crear nuestra consulta SQL, para ello se añadirá en el campo a probar una comilla “ ’ ” indicando el fin de la cadena o un punto y coma “;” que indica el fin de la consulta, también se puede intentar con otros campos, lo importante es tratar de generar el error SQL. Si se fracasa en el caso anterior quiere decir que los mensajes de error se encuentran ocultos y tendremos que recurrir al uso de una Inyección SQL Ciega

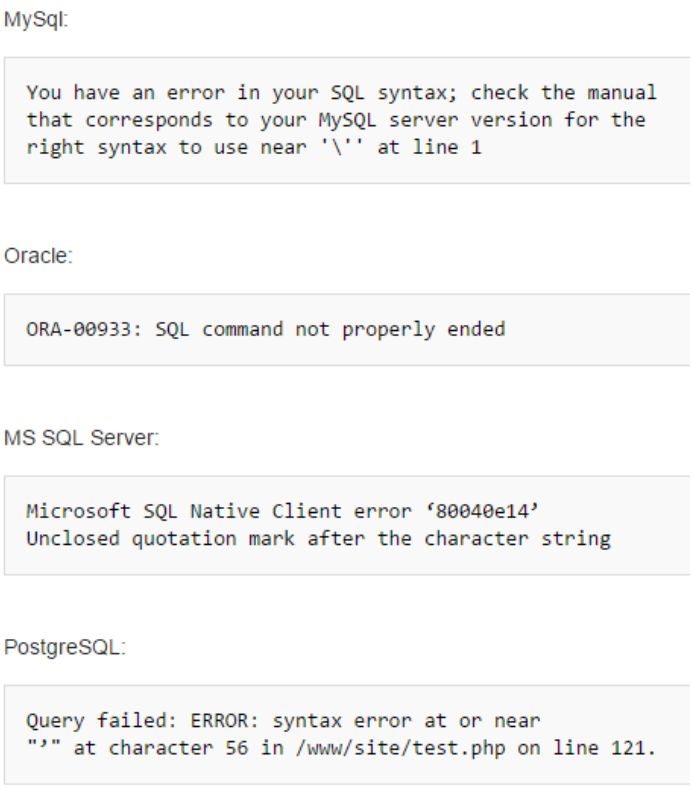


Figura 5-34 Ejemplo de errores SQL según distintas bases de datos

c) Una vez comprobada la existencia de la vulnerabilidad de inyección SQL, procederemos a realizar diferentes combinaciones de consultas hasta lograr obtener algún dato concreto.

En la siguiente imagen se muestra la comprobación de la inyección SQL, donde se intentó provocar el error con el uso de diferentes caracteres y combinaciones sin tener éxito alguno por lo que se concluye que esta vulnerabilidad es un falso positivo ya que no pudo ser explotada.

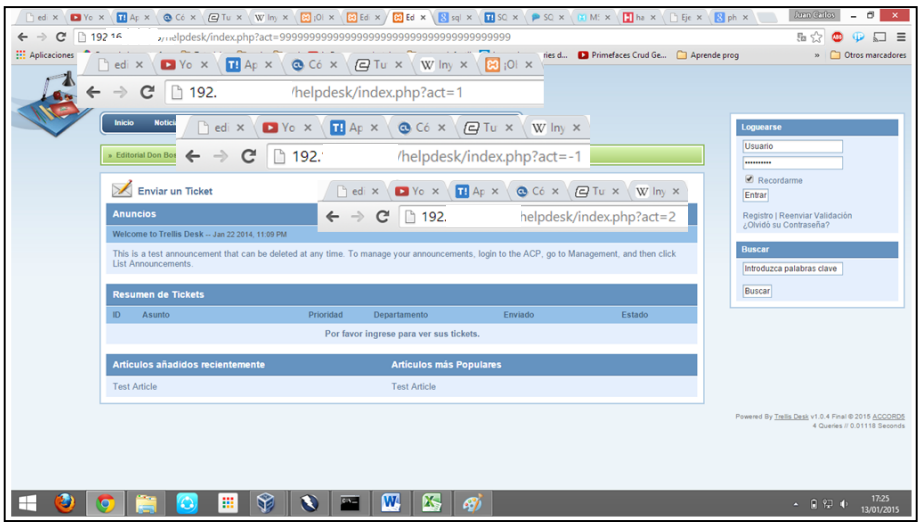


Figura 5-35 Comprobación de la inyección sql sin éxito al generar errores sql

Para verificar y demostrar lo antes expuesto aremos uso de la herramienta sqlmap que es una herramienta de código abierto que automatiza el proceso de explotación de vulnerabilidades de inyección SQL compatible con distintas bases de datos y que nos permite realizar ataque tipo OUT OF BAND, donde nos indica que el método GET con el parámetro “CAT” no es inyectable confirmando lo antes expuesto.

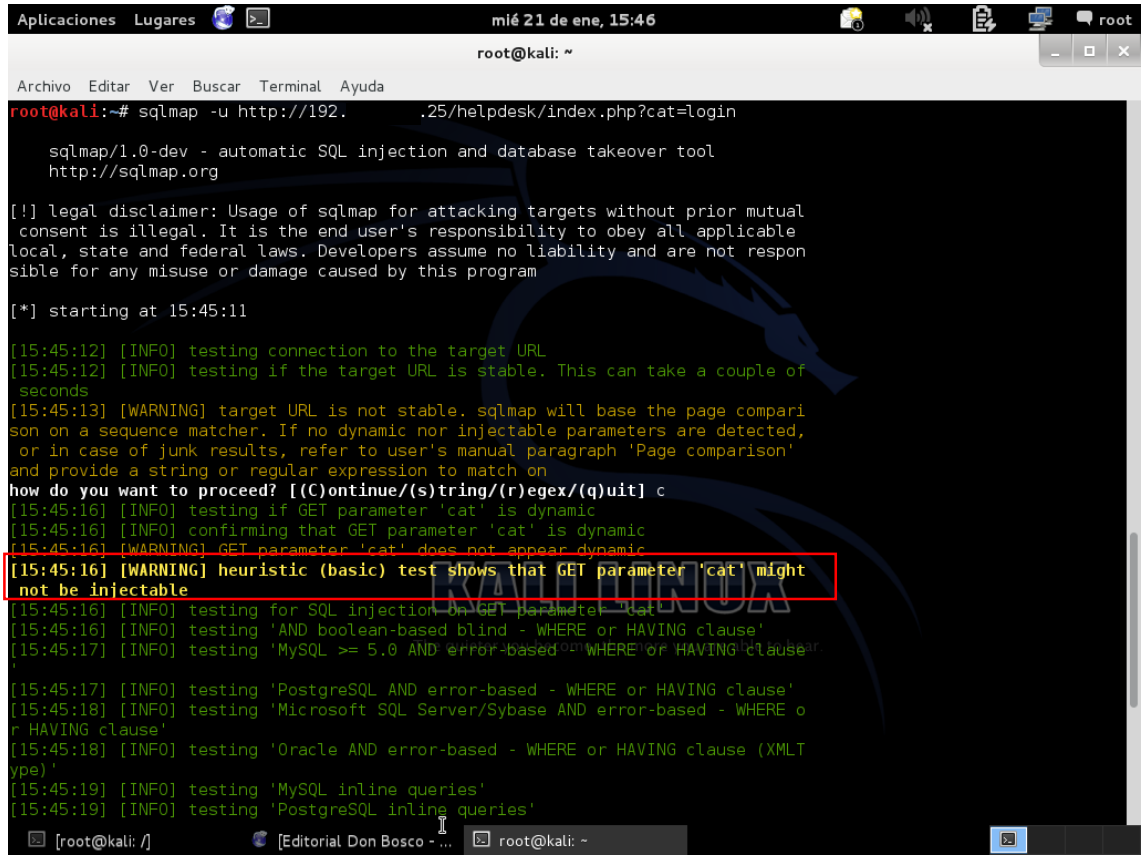


Figura 5-36 Comprobación de que el método get con el parámetro cat no es inyectable.

5.7.3. Análisis criptográfico.

La criptografía es usada ampliamente en aplicaciones web, por lo general para permitir al usuario registrarse automáticamente.

Cuando se realiza un análisis criptográfico de una aplicación WEB es importante comprobar la configuración de los servidores, analizar si se usan protocolos seguros como HTTPS u otros servicios encapsulados sobre SSL/TLS. (OWASP, 2008)[45]

Si se ha comprobado que nuestra aplicación trabaja sobre protocolos seguros bar la validez de los certificados SSL cliente – servidor.

[45] OWASP. (2008). *Guia De Pruebas OWASP*. OWASP.

Cada vez que se accede a una aplicación web mediante el protocolo HTTPS, se establece un canal seguro entre el cliente (un navegador web) y el servidor, donde la identidad de estas es determinada por medio de certificados digitales.

Lo primero que se hará en un análisis criptográfico será comprobar la validez de un certificado, para lo cual seguiremos los siguientes pasos:

a) Se debe comprobar si la Autoridad de Certificación (Certificate Authority - CA) es conocida, es decir si se la considera confiable.
b) Se comprobará que el certificado es válido actualmente.
c) Verificaremos que el nombre del sitio y el nombre indicado en el certificado coinciden.
d) Comprobaremos si nuestro navegador se encuentra actualizado debido a que los certificados CA expiran y en cada nueva distribución de un navegador se incluyen nuevos certificados CA. Marcados como confiables o seguros.

5.8.Toma de control de servidores.

Para la toma de control de servidores como nuestro objetivo principal dentro del desarrollo de las pruebas de penetración aremos uso del conocimiento adquirido en etapas previas, de esta manera buscaremos alternativas que permitan acceder a los sistemas y obtener el control de los mismos, haciendo uso principalmente de nuestro análisis de vulnerabilidades donde cada vulnerabilidad será explotada permitiéndonos lograr el escalamiento de privilegios y finalmente la toma de control de nuestros equipos .

5.8.1. Metasploit framework.

Metasploit es un proyecto open source de seguridad informática que proporciona un repositorio completo de información acerca de vulnerabilidades de seguridad y sirve de apoyo en pruebas de penetración y en el desarrollo de firmas para sistemas de detección de intrusos, dentro de él se encuentra Metasploit framework que es una de sus

herramientas más completas para el desarrollo y la ejecución de exploits contra un objetivo determinado. (Caridad), 2011)[46]

Esta herramienta aprovecha de las vulnerabilidades encontradas anteriormente mediante exploits y payloads, los exploits son un fragmento de datos o secuencia de comandos y acciones, utilizadas con el fin de aprovechar una vulnerabilidad de seguridad de un determinado sistema. (Wikipedia)[47]

Los payloads son un programa que acompañan a un exploit para realizar funciones específicas, una vez que el sistema objetivo es comprometido. (Técnicas de Hacking THW)[48]

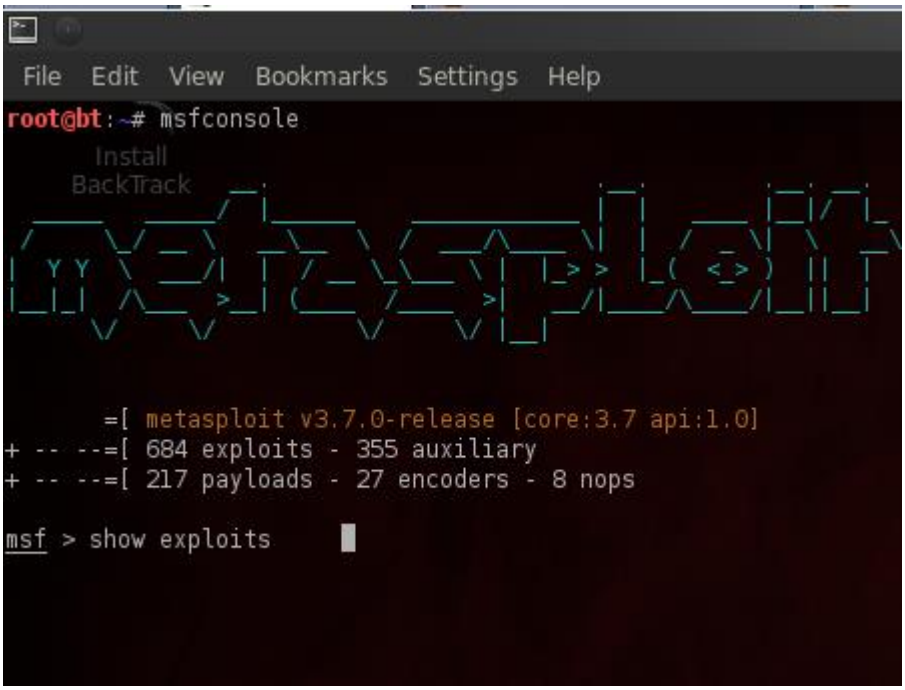


Figura 5-37 Metasploit framework

[46] Caridad), H. (. (2011). *Tutorial de Metasploit Framework de Offensive-Securitty*.

[47] *Wikipedia.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Exploit

[48] *Técnicas de Hacking THW.* (s.f.). Obtenido de http://thehackerway.com/2011/03/11/comandos-y-conceptos-basicos-metasploit-framework/

5.8.2. Explotación de las vulnerabilidades detectadas.

Para llevar a cabo este procedimiento nos apoyaremos en el sistema Kaly Linux que es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general, esta herramienta trae preinstalados numerosos programas incluyendo Nmap, Wireshark, John the Ripper (Un crackeador de passwords) y la suite Aircrack-ng (Software para pruebas de seguridad en redes inalámbricas).

Una vez realizado el análisis de las vulnerabilidades descubiertas, el siguiente paso es explotar las mismas mediante el uso de exploits que se encuentran disponibles para cada caso, estas vulnerabilidades puede ser por errores en el código, por una mala configuración de los equipos, por dejar opciones por defecto en las aplicaciones, mala configuración del firewall, etc.

Existe una herramienta llamada armitage que no es más que una interfaz gráfica de Metasploit que nos permite visualizar gráficamente nuestros objetivos, esta herramienta tiene la ventaja de agrupar todo lo necesario para trabajar con metasploit, se puede ejecutar un análisis con NMAP sin necesidad de salir del framework, nos recomienda que exploit usar, expone las opciones avanzadas de metasploit framework como explorar el equipo comprometido o simplemente usar una consola CDM, además de que proporciona una interfaz ordenada e intuitiva de como explotar y hacer uso de una vulnerabilidad. En la siguiente imagen se muestra la herramienta en funcionamiento.

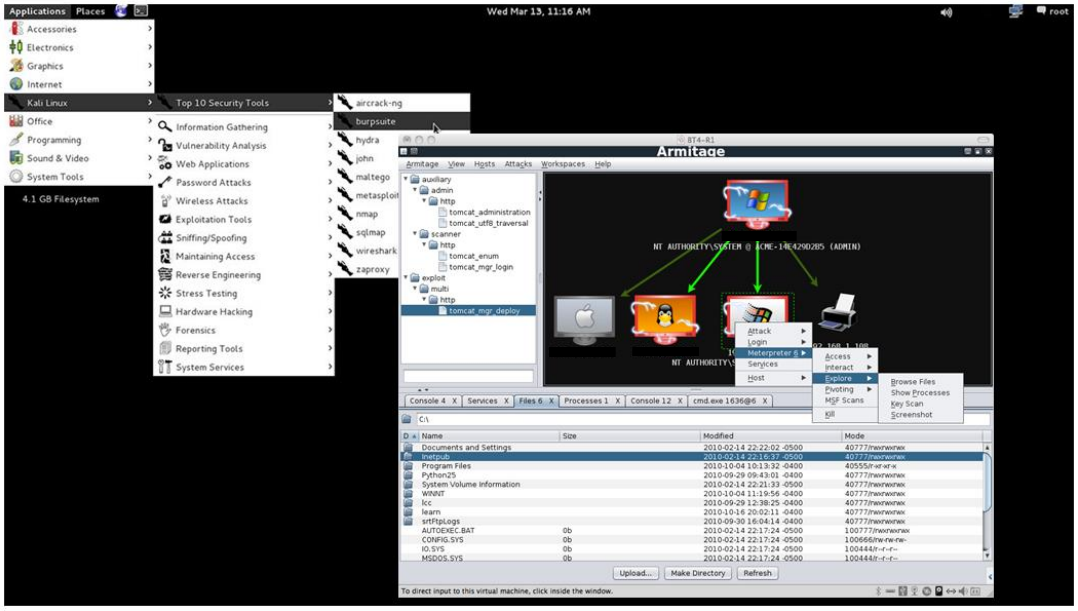


Figura 5-38 Ejecución del armitage para metasploit framework

5.8.2.1.Comprobación de vulnerabilidades en sistemas Windows.

Comprobación de vulnerabilidad MS09-001

Esta vulnerabilidad consta dentro del grupo de vulnerabilidades calificadas como críticas en el bloque de mensajes del servidor (SMB) para equipos con sistemas Windows 2008/Vista/2003/XP/2000, que permiten ejecutar remotamente código arbitrario y lanzar ataques de denegación de servicio a un sistema vulnerable. El protocolo de bloque de mensajes de servidor (SMB) es un protocolo creado por IBM y mejorado por Microsoft para compartir archivos o dispositivos de la red utilizada en Windows, esta vulnerabilidad se da debido a que el protocolo SMB no valida de forma suficiente el tamaño de búfer antes de escribir en él. (Panda Security)[49]

Si se explota con éxito MS09-001 se habrá realizado un ataque DOS donde el sistema afectado dejara de responder y se reiniciara automáticamente

[49] *Panda Security.* (s.f.). Obtenido de http://www.pandasecurity.com/spain/homeusers/security-info/204670/information/MS09-001

Para comprobar esto vamos a hacer uso de Metasploit Framework con su interfaz armitage, donde lo primero que aremos será identificar nuestro equipo victima mediante el uso de NMAP para posteriormente buscaremos el exploit MS09-001 y completar los campos requeridos.

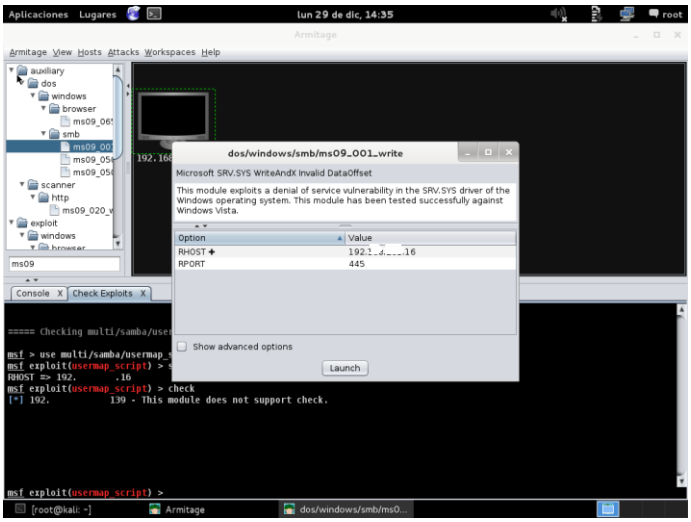


Figura 5-39 Identificación de nuestra víctima y configuración de vulnerabilidad ms09-001

Ya con los parámetros ingresados como IP del host remoto y puerto a atacar, ya solo queda hacer correr nuestro ataque.

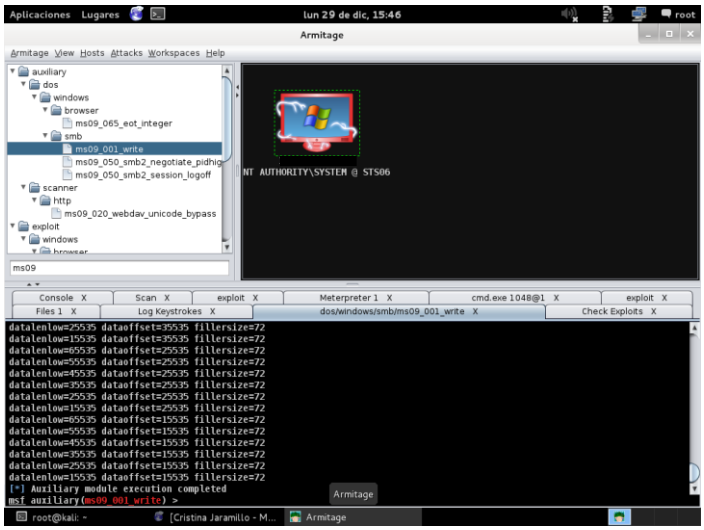


Figura 5-40 Ejecución exitosa de vulnerabilidad ms009-001 en metasploit

Finalmente como resultado de nuestro ataque vemos que nuestra victima ha sido forzada a reiniciar el equipo por un error de tipo Blue Screen el cual se genera debido a un desbordamiento del buffer creado por el protocolo SMB.

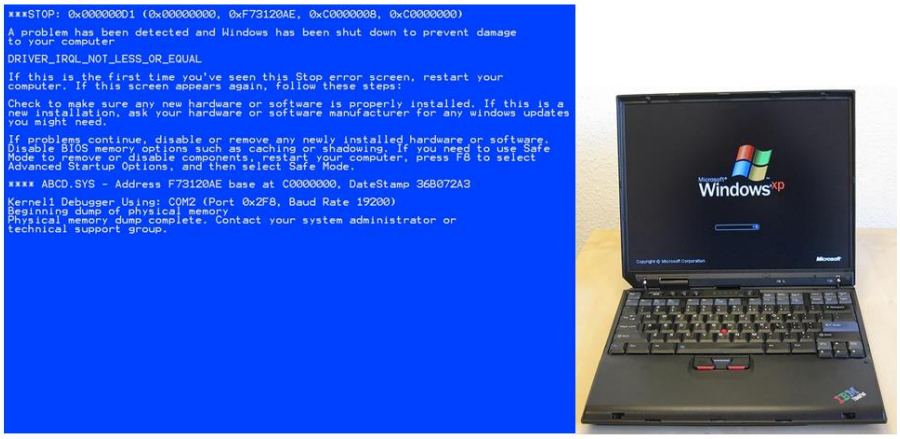


Figura 5-41 Comprobación exitosa de un ataque dos mediante MS09-001

Comprobación de vulnerabilidad MS08-067 Windows.

Se trata de una vulnerabilidad crítica en el servicio de servidor sobre equipos Windows 2008/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario en sistemas vulnerables. El servicio de servidor permite compartir recursos locales como discos e impresoras con otros usuarios de la red, para lo cual hace uso del protocolo de llamada a procedimiento remoto (RPC) que es un protocolo utilizado por una aplicación para solicitar un servicio de un equipo remoto. Esta vulnerabilidad se da porque este servicio no maneja correctamente las peticiones RPC especialmente diseñadas. (Panda Security)[50]

Si se logra explotar esta vulnerabilidad se logrará conseguir control remoto del ordenador afectado con los mismos privilegios que el usuario tenga al iniciar sesión, es decir que si el usuario tuviera permisos de administrados se tuviera control total sobre la victima sin limitaciones.

[50] *Panda Security.* (s.f.). Obtenido de http://www.pandasecurity.com/spain/homeusers/security-info/202013/information/MS08-067

A continuación explotaremos esta vulnerabilidad para comprobar su existencia mediante el uso de la aplicación Armitage realizando como primer paso el escaneo de la víctima con NMAP para posteriormente realizar un escaneo de vulnerabilidades, en nuestro caso buscaremos la vulnerabilidad MS08-067.

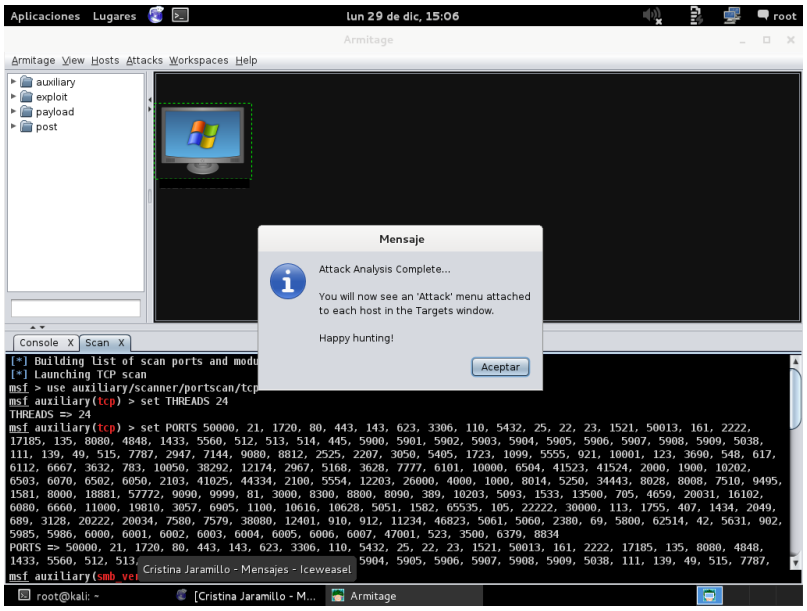


Figura 5-42 Escaneo del equipo y búsqueda de vulnerabilidad MS08-067

Una vez escaneado el equipo y con la vulnerabilidad encontrada procederemos a la configuración de la misma ingresando la IP y PUERTO remoto.

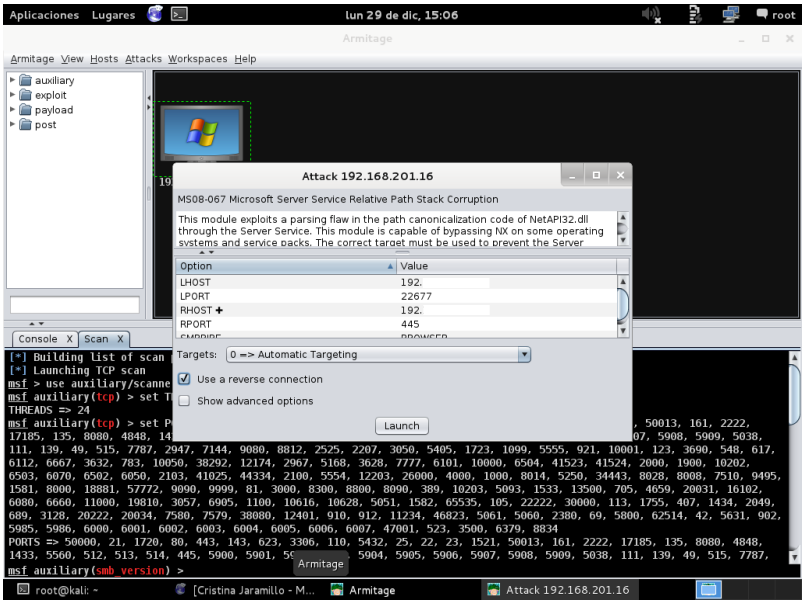


Figura 5-43 Configuración del ataque para la vulnerabilidad MS08-067

Lo siguiente será explotar la vulnerabilidad, como se ve en la siguiente figura el ataque resulta un éxito al lograr el control del dispositivo, lo cual se puede demuestra viendo el equipo de la víctima que aparece en nuestro panel el cual cambia de aspecto a un rojizo venoso.

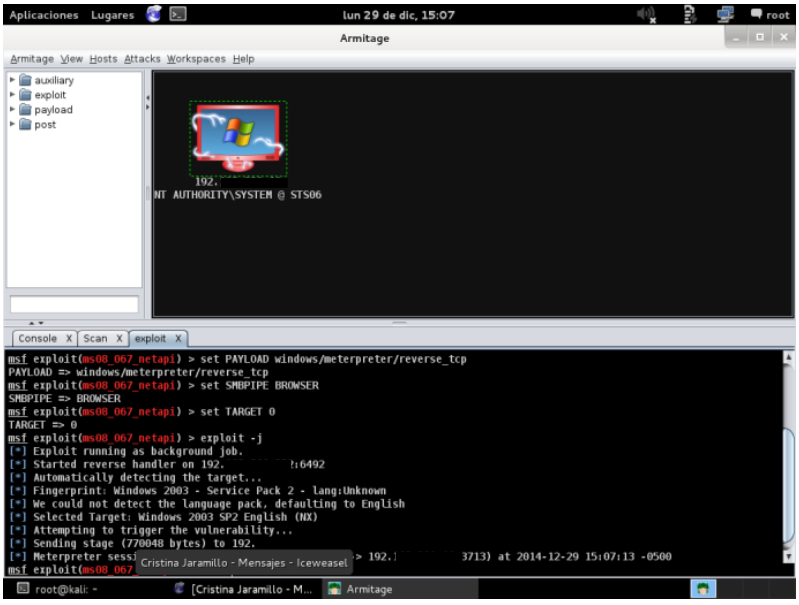


Figura 5-44 Toma de control del equipo de la víctima

Una vez que hemos logrado obtener el control de la víctima podemos realizar lo que se quiera según los permisos que haya tenido el usuario, en este caso el usuario se ha logueado con permisos de administrador, esto lo podemos ver por la descripción de la víctima la cual señala AUTHORITY/SYSTEM, lo que nos indica que podremos hacer lo que queramos, como explorar y descargar información de sus directorios, tener acceso a la SHELL, etc.

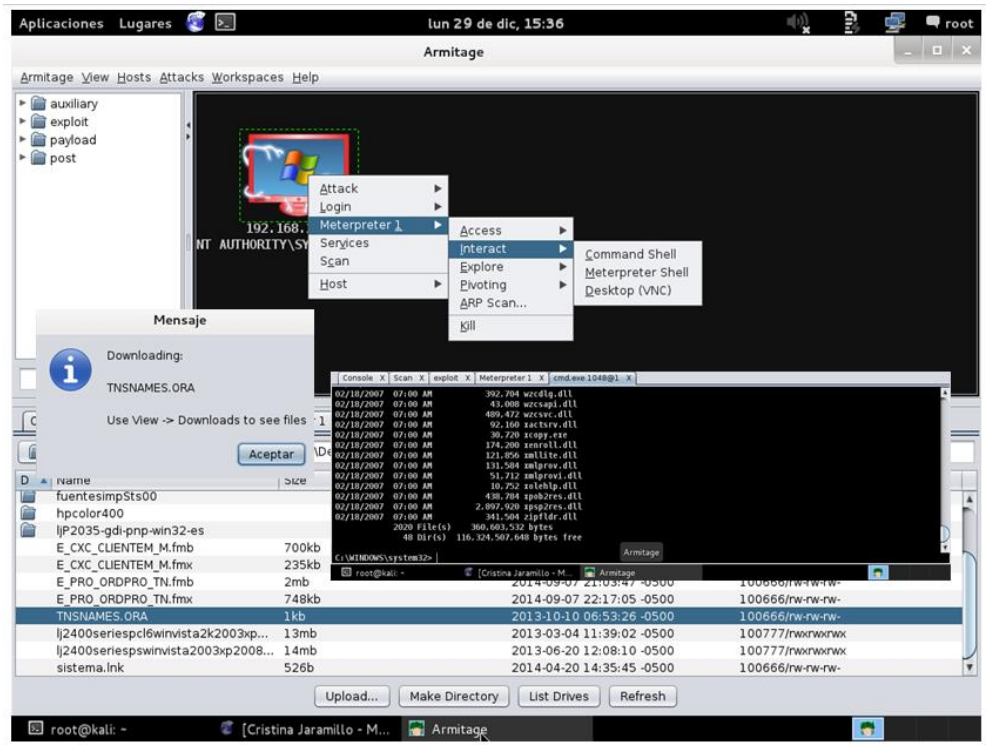


Figura 5-45 Exploración de directorios y acceso al shell de windows

Comprobación de vulnerabilidad MS09-050

MS09-050 es una vulnerabilidad calificada como crítica dentro del protocolo de bloque de mensajes de servidor (SMB) el cual permite compartir archivos y se encuentra de forma predeterminada en equipos Windows afectando a las distribuciones Windows 2008/Vista permitiendo ejecutar remotamente código arbitrario. (Panda Security)[51]

[51] *Panda Security.* (s.f.). Obtenido de http://www.pandasecurity.com/spain/homeusers/security-info/214066/information/MS09-050

Esta es una vulnerabilidad de código remoto que se da debido a que la implementación de SMB no usa una copia validada al tratar paquetes de solicitud de negociación del protocolo múltiple de SMB.

Si se logra explota con éxito esta vulnerabilidad conseguiremos control remoto del equipo afectado, con los mismos privilegios que el usuario que haya iniciado sesión.

Para comprobar esta vulnerabilidad agregaremos nuestro host victima al Armitage mediante un escaneo NMAP el que nos permitirá conocer con exactitud puertos abiertos, disponibilidad del equipo, etc. Una vez hecho esto buscaremos la vulnerabilidad a explotar como se muestra en la siguiente imagen.

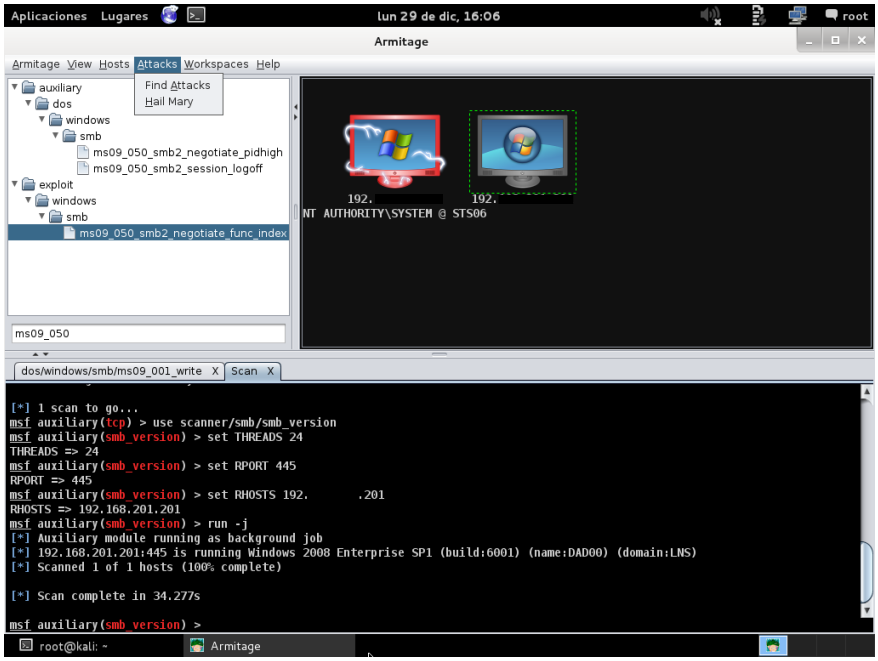


Figura 5-46 Escaneo del dispositivo y búsqueda de vulnerabilidad ms09-050

Ya con la vulnerabilidad encontrada procedernos a configurar sus parámetros para su posterior explotación, en este caso se añadirá la IP y puerto remoto por donde se realizará el ataque.

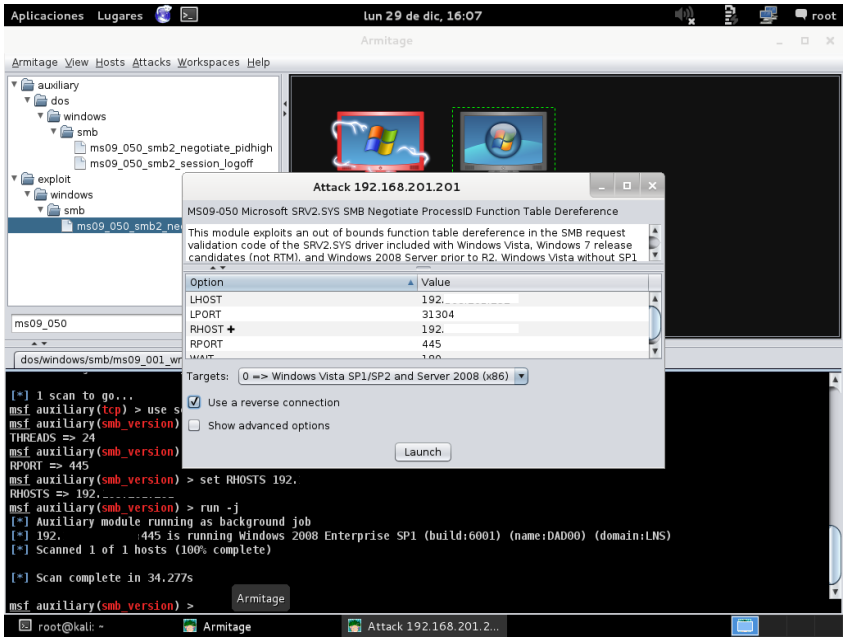


Figura 5-47 Configuración del ataque MS09-050

Finalmente se procede a explotar dicha vulnerabilidad comprometiendo al equipo y tomando el control del mismo, en este caso se logra obtener permisos de administrador permitiéndonos tener control total sobre la víctima.

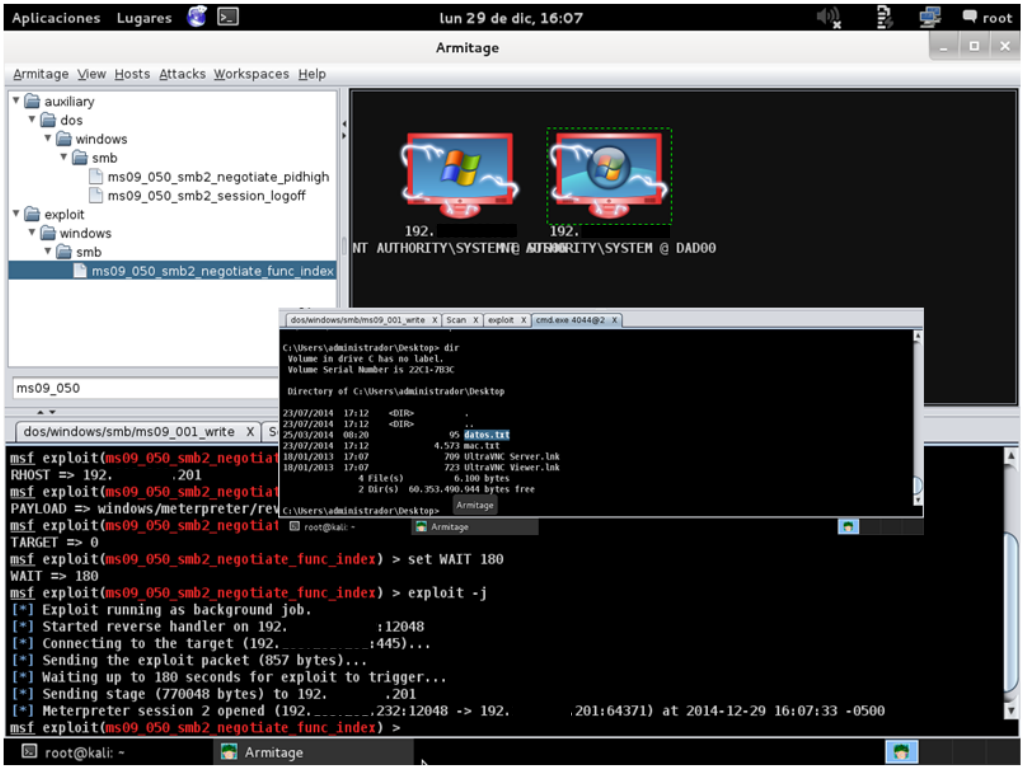


Figura 5-48 Explotación de la vulnerabilidad MS09-050 y toma de control de la víctima.

Comprobación de vulnerabilidad 74496-DNS obsoleto.

Esta vulnerabilidad se da por el uso de software que ya no recibe soporte por parte del proveedor, en este caso Microsoft Windows DNS 6.0.6001.18000, lo que implica que no se crearán parches nuevos haciendo a esta aplicación altamente vulnerable. (Soporte Microsoft)[52]

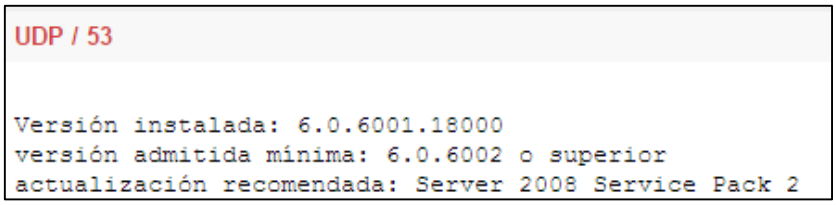


Figura 5-49 Versión mínima admitida de Microsoft Windows DNS

[52] *Soporte Microsoft.* (s.f.). Obtenido de http://support2.microsoft.com/lifecycle/?c2=1163

Comprobación de vulnerabilidad 70882 - ESXi 5.0. (VMWARE)

Esta vulnerabilidad se refiere a múltiples vulnerabilidades creadas como resultado del uso de software de virtualización sin actualizar, esta vulnerabilidad incluye revelación de la huella digital del software, posibilita ataques de diccionario, facilita información sobre la versión del sistema usada, etc.

Para comprobar esta vulnerabilidad aremos uso de algunos módulos, el primero será el modulo auxiliar esx-fingerprint el cual trata de acceder a la interfaz web VMware ESX / ESXi en el puerto 443 / TCP e intenta identificar la versión que se ejecuta de ESX / ESXi. (Eric Romang Blog)[53]

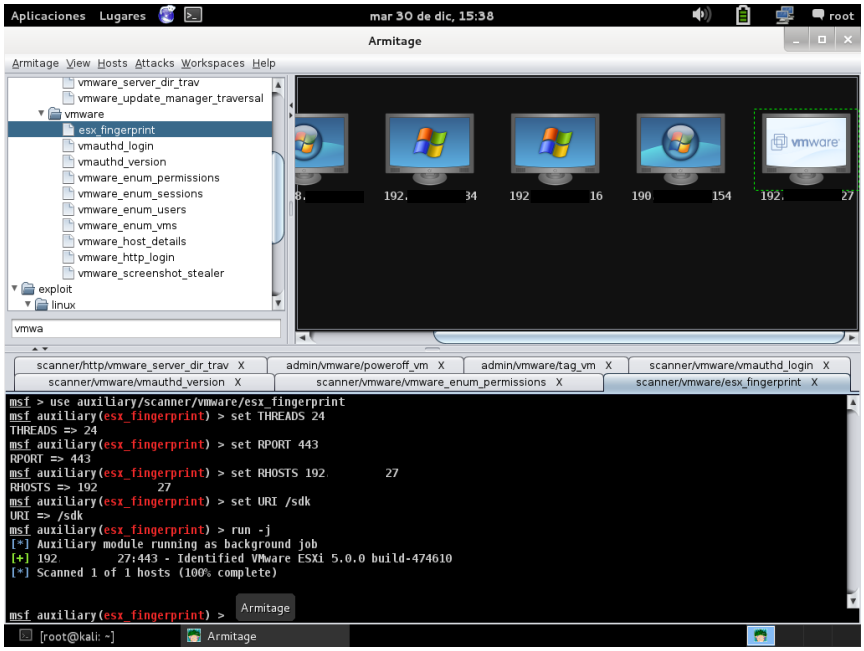


Figura 5-50 Explotación del módulo auxiliar esx-fingerprint (vmware)

El siguiente módulo nos permitirá tener acceso a al sistema de virtualización WMWARE mediante ataques de fuerza bruta, esto puede ser mediante un diccionario o probando directamente con una combinación específica para ello se debe proporcionar un usuario y

[53] *Eric Romang Blog.* (s.f.). Obtenido de http://eromang.zataz.com/2012/05/06/metasploit-vmware-auxiliary-modules/

contraseña válidos, si el ataque tiene éxito se puede complementar este módulo con HW_DETAILS para enumerar detalles del hardware del huésped.

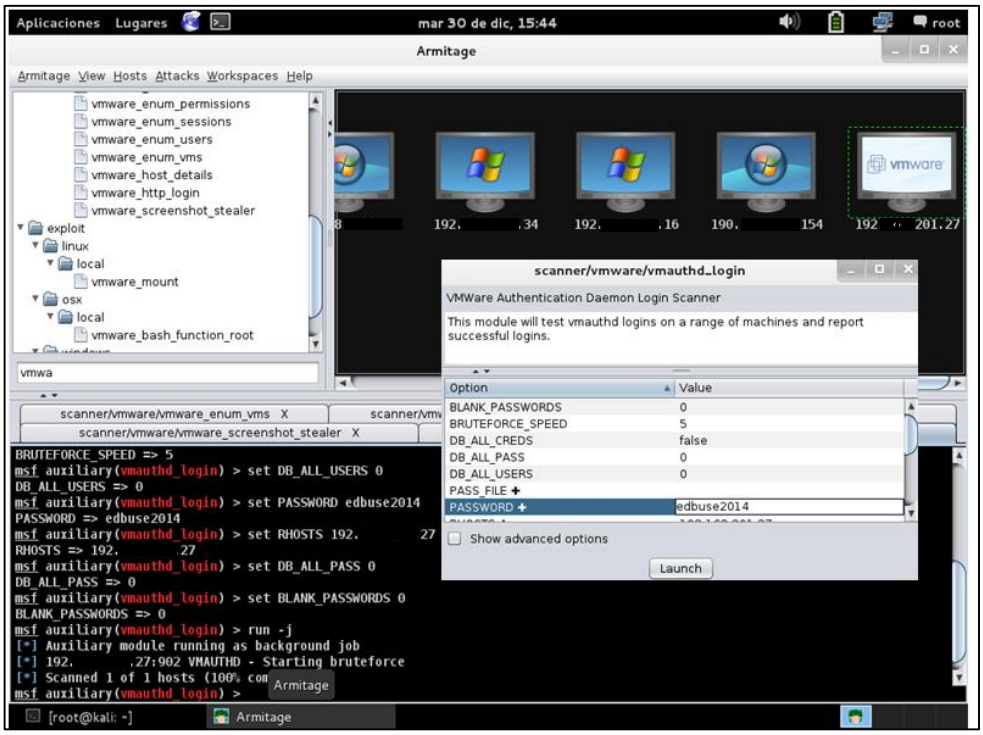


Figura 5-51 Explotación del módulo auxiliar vmauthd_login (vmware)

El último modulo que probaremos será vmauthd_version, el cual reunirá información del servidor ESX / ESXi a través del puerto 902 / TCP, para lo cual necesitamos ingresar el puerto y la IP del equipo remoto como se muestra en la siguiente imagen.

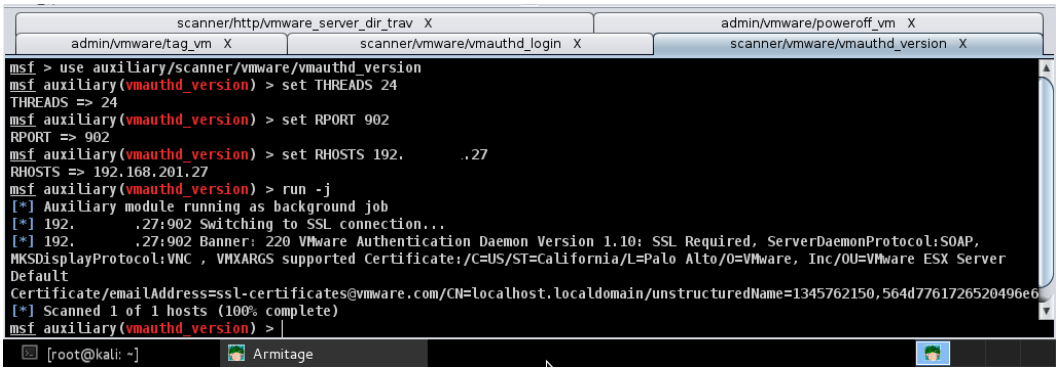


Figura 5-52 Explotación del módulo auxiliar vmauthd_version (vmware)

5.8.2.2.Comprobación de vulnerabilidades en sistemas GNU-Linux

Comprobación de vulnerabilidad 33850 sistema operativo Fedora sin soporte.

Esta vulnerabilidad se da por que la versión del sistema operativo Unix usado en el equipo remoto en este caso la versión 15 es obsoleta y el proveedor ya no brinda soporte lo que implica que no hay nuevos parches de seguridad porque es probable que contenga vulnerabilidades de seguridad. (Fedora)[54]

Figura 5-53 Versiones de fedora sin soporte

Comprobación de vulnerabilidad 58987- PHP sin soporte.

Esta vulnerabilidad se da debido a que la versión de PHP usada en el equipo remoto ya no tiene soporte por parte del proveedor, esto implica que no existen nuevos parches

[54] *Fedora.* (s.f.). Obtenido de https://fedoraproject.org/wiki/End_of_life?rd=LifeCycle/EOL

de seguridad por lo que esta versión puede contener vulnerabilidades de seguridad. (PHP)[55]

```
Fuente: Servidor: Apache / 2.2.14 (Unix) DAV / 2 mod_ssl / 2.2.14
OpenSSL / 0.9.8l PHP / 5.3.1 mod_apreq2-20090110 / 2.7.1 mod_perl /
2.0.4 Perl / v5.10.1
versión instalada: 5.3.1
Fecha de fin de soporte: 14/08/2014
```

Figura 5-54 Versión de PHP sin soporte.

Comprobación de vulnerabilidad 41028 – Nombre por defecto del agente SNMP (public)

SNMP (Simple Network Management Protocol) es un servicio que proporciona capacidades de gestión de red y monitoreo. SNMP ofrece la capacidad de sondear los dispositivos de red y los datos del monitor. SNMP es también capaz de cambiar las configuraciones en el host, lo que permite la gestión remota del dispositivo de red. El protocolo utiliza una cadena de comunidad para la autenticación del cliente SNMP para el agente SNMP en el dispositivo gestionado. La cadena de comunidad predeterminado que proporciona la vigilancia a menudo es "públic". El exploit para SNMP aprovecha estas cadenas de comunidad predeterminadas para permitir a un atacante obtener información acerca de un dispositivo que utiliza la cadena de comunidad de lectura "públic", y el atacante puede cambiar una configuración de sistemas utilizando la cadena de comunidad de escritura "private". La oportunidad de este exploit se incrementa debido a que el agente SNMP a menudo se instala en un sistema por defecto, sin conocimiento del administrador. A continuación se muestra la figura en la que se puede observar una herramienta muy útil presente en Kaly Linux para enumerar los atributos del protocolo SNMP.

[55] *PHP.* (s.f.). Obtenido de http://php.net/eol.php

Figura 5-55 SNMP Enumerator kaly linux

SNMP es vulnerable porque a menudo se instala automáticamente en muchos dispositivos de red con "públic" como la cadena de lectura y "private" como la cadena de escritura. Esto significaría que los sistemas pueden ser instalados en una red sin ningún conocimiento de que SNMP está funcionando y el uso de estas claves por defecto. Por lo tanto proporciona a un atacante los medios para llevar a cabo el reconocimiento en un sistema. MIB de SNMP proporcionan información como el nombre del sistema, la ubicación, contactos, e incluso a veces los números de teléfono. Esta inteligencia suave puede ser muy útil en la ingeniería social. Un atacante podría llamar a una organización y utilizar el nombre de contacto del sistema y del sistema para tener una contraseña de un usuario desprevenido. (Sans)[56]

Una MIB proporciona la descripción del sistema que revela el sistema operativo que el host está utilizando. Esto puede ser igualada contra exploits conocidos que permitirían al atacante obtener aún más el acceso al host SNMP. También proporciona descripciones de la interfaz, tipos, y otra información de configuración de interfaz. Esta información de la interfaz puede ser obtenida de más de un sistema para permitir a un atacante para armar

[56] *Sans.* (s.f.). Obtenido de http://www.sans.org/security-resources/idfaq/snmp.php

un mapa de la red de una organización que muestra cómo están interconectados los sistemas. Algunos MIB son grabable permitiendo al atacante para cambiar la configuración del sistema creando una negación de oportunidades de servicio. La siguiente figura muestra todos los datos del host con comunidad SNMP public.

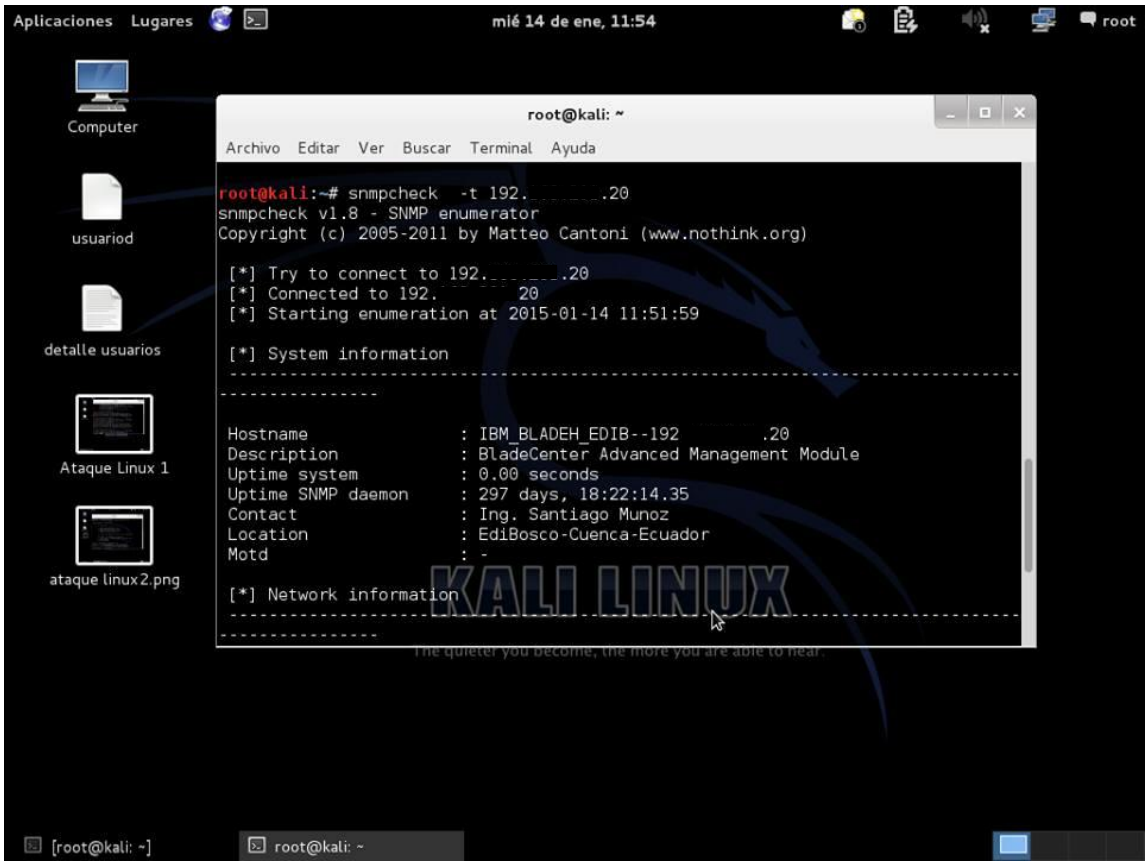


Figura 5-56 Información de configuración del host con nombre de dominio SNMP "public “.

Por lo tanto se comprobó que dicha vulnerabilidad relacionada con el protocolo SNMP puede ser aprovechada con el fin de acceder a los equipos remotamente.

5.8.3. Escalamiento de privilegios.

Cuando se realiza la explotación de una vulnerabilidad el sistema es comprometido, pero por lo general se tendrá los mismos permisos o privilegios con los que el usuario este logueado, cuando no tenemos los privilegios necesarios es importante hacer una escala de

privilegios para lo cual aremos uso de los comandos getuid y getsystem dentro del meterpreter el primero nos permitirá ver el usuario y los permisos que este posee y el segundo nos permitirá realizar la escala de privilegios para loguearnos como SYSTEM. (Conociendo Meterpreter, 2013)[57].

Tal como se ve en la siguiente figura.

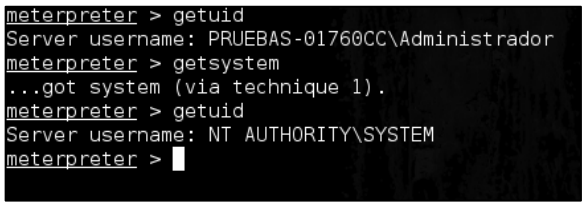


Figura 5-57 Escalamiento de privilegios con getsystem

En nuestro caso esto no fue necesario ya que en todos los dispositivos el usuario poseía todos los privilegios es decir estaba logueado como SYSTEM tal como se muestra a continuación.

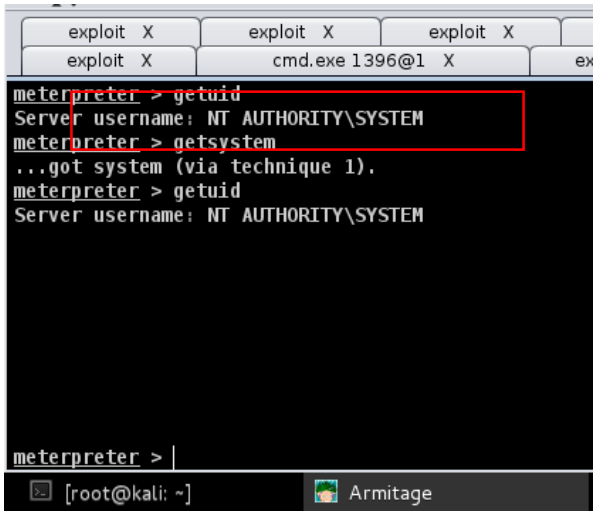


Figura 5-58 Obtención directa de privilegios system

Si el caso fuera distinto y no se tuviera privilegios, en Windows se puede hacer uso del exploit bypassuac el cual forza al sistema a que se logue como SYSTEM, para lo cual se debe terminar con cualquier sesión iniciada anteriormente y continuación indicarle cual

[57] *Conociendo Meterpreter.* (08 de Diciembre de 2013). Obtenido de http://highsec.es/2013/08/conociendo-meterpreter-parte-ii-escalar-privilegios/

será la sesión a usar para el ataque, posterior a esto procederemos aexplotar la vulnerabilidad con lo que lograremos tener total control sobre el sistema comprometido. En la siguiente imagen se muestra un ejemplo de cómo sería si se tuviera éxito con este ataque donde con al ejecutar el comando getuid nos muestra textualmente "AUTORITY\SYSTEM" que nos indica que tenemos permisos totales sobre el sistema.

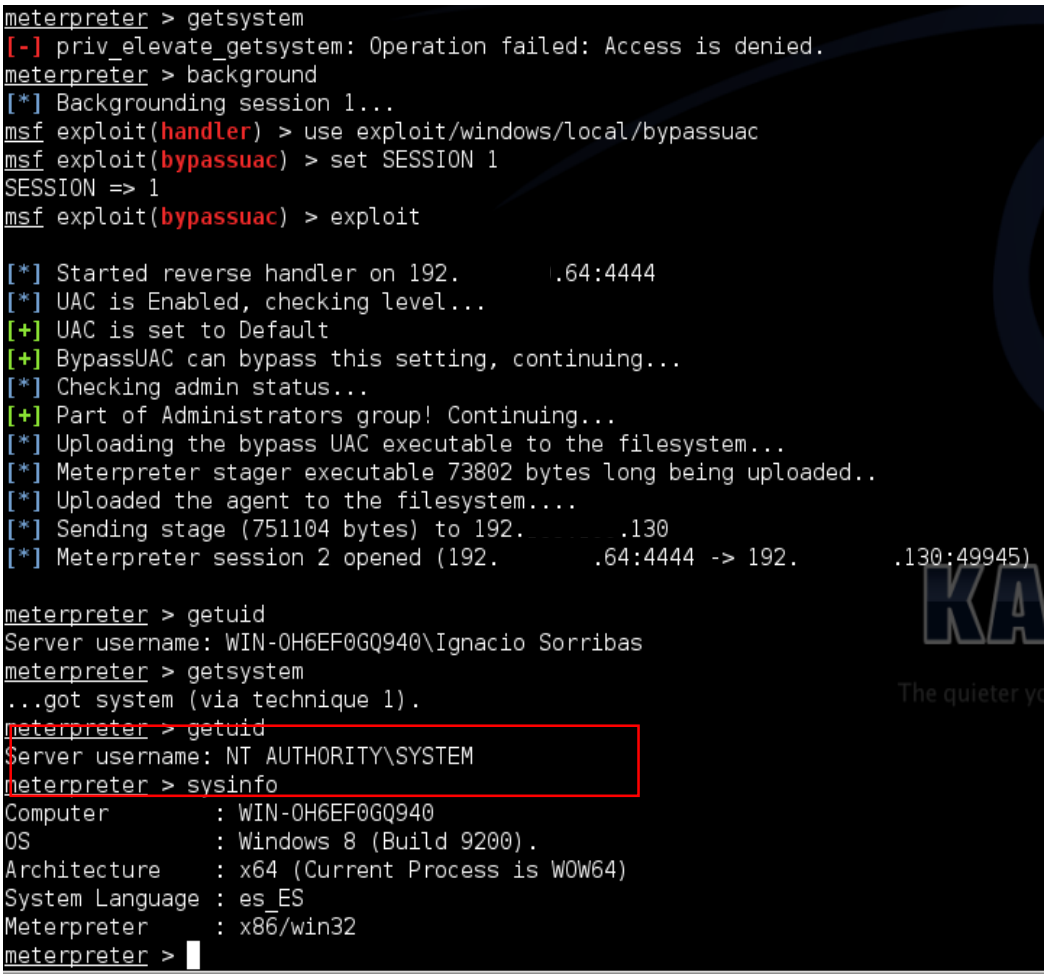


Figura 5-59 Obtención de privilegios mediante exploit bypassuac

Fuente: http://hardsec.net/escalado-de-privilegios-con-bypassuac-en-win8/

5.8.4. Repositorios de exploits.

En la actualidad se reportan diversos tipos de vulnerabilidades, sin embargo solo una pequeña parte de ellas son expuestas o publicadas de manera gratuita. Algunos de estos

"exploits", puede ser descargados desde sitios webs donde se mantienen repositorios de ellos. A continuación en la tabla se detallan algunas de estas páginas

Tabla 5-4 Repositorios de Exploits

Nombre Repositorio	Sitio Web
Exploit DataBase	http://www.exploit-db.com/
Inj3ct0r	http://1337day.com/
ExploitSearch	http://www.exploitsearch.net/
Packet Storm	http://packetstormsecurity.com/files/tags/exploit/
Metasploit Auxiliary Module & Exploit Database	http://www.metasploit.com/modules/

Kali Linux, la herramienta que se utilizó para realizar los ataques a ciertas vulnerabilidades, mantiene un repositorio local de exploits de "Exploit-DB". Esta base de datos local tiene un script de nombre "searchsploit", el cual permite realizar búsquedas dentro de esta base de datos local. (Quezada)[58]

5.8.5. Combinación de vulnerabilidades para tomar el control.

La combinación de vulnerabilidades nos será de utilidad en el caso de no tener resultados después de haber usado alguna herramienta, entonces lo que se realizará a continuación será utilizar dos o más vulnerabilidades aprovechando las características de cada una de estas para lograr un acceso en la victima, este es un proceso complejo y exige de parte del evaluador los conocimientos suficientes para llevarlo a cabo, por lo general esto suele ser útil con vulnerabilidades cuyo impacto sobre el sistema es medio y no compromete completamente a los sistemas para lo cual se necesita el apoyo de otras vulnerabilidades.

[58] Quezada, A. E. (s.f.). *Kaly Linux.* Obtenido de http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf

5.8.6. Acceso a información interna.

Antes de indicar el acceso a información interna de la empresa es necesario definir este tipo de información y además diferenciar los diferentes prototipos pertenecientes a esta clase: el conocimiento que es la fusión de la información interna y externa que generan beneficios para la empresa y por otra parte la información operacional que es la que es generada por pal organización debido al funcionamiento rutinario de la empresa. Por lo tanto la información interna puede ser definida como la información que es tratada internamente para que puede ser dirigida por los gestores. (Cavañate)[59]

5.9.Iteración sobre las fases

La iteración comprende un periodo de tiempo dentro de las fases del penetration test en el cual se produce una versión del entregable de dicho proyecto. Lo que permite demostrar el progreso del proceso de evaluación de la seguridad, de tal forma que puedan entender lo que se requiere hacer y obtener retroalimentación sobre el proyecto, Cada iteración se construye sobre el resultado de la iteración previa y produce un incremento del entregable que en nuestro caso se trata de un documento en el que conste las principales vulnerabilidades y sus contramedidas ,y un paso más cerca del producto final.

En cada iteración, los documentos a ser entregados son actualizados. Por lo tanto la iteración sobre las fases es bastante disciplinada.

Cada iteración debe tomar en cuenta los riesgos más críticos que se pueden presentar durante la ejecución de las fases e implementar los elementos de trabajo de mayor prioridad. Esto asegura que cada iteración adiciona el máximo valor a la empresa que contrata el servicio de Penetration test, mientras se reduce la incertidumbre.

[59] Cavañate, A. M. (s.f.). *Universitat Pompeu Fabra.* Obtenido de http://www.upf.edu/hipertextnet/numero-1/sistem_infor.html#3.2.2

5.10. Recolección de los accesos logrados y dificultades durante el proceso.

Dentro de un test de penetración siempre es importante tener una bitácora de los accesos logrados donde registraremos que tipo de exploit se usó y que resultados se obtuvieron incluyendo el nivel de riesgo que involucra cada uno de ellos, también se deberá registrar toda aquella vulnerabilidad que haya sido comprobada con éxito aunque esta no haya generado un acceso como tal. (ISECOM, 2003)[60]

En el caso de poseer un falso positivo este debe ser registrado al igual que un acceso logrado ya que la presencia de este fenómeno no concluye que el objetivo no posee esta deficiencia, si no que únicamente nos indica que la prueba en particular con la herramienta que se haya escogido y durante el tiempo previsto no se logró explotarla. También podría significar que el objetivo es vulnerable, pero que está protegido por algún elemento en particular esto permite que en una evaluación posterior el problema sea observado con mayor detenimiento y desde un punto de vista diferente. (ISECOM, 2010)[61]

A continuación se muestra una tabla que recolecta toda esta información que le servirá al experto en seguridad para la elaboración del informe final.

Tabla 5-5 Tabla de accesos logrados y vulnerabilidades comprobadas

VULNERABILIDAD	ACCESO	RESULTADOS	NIVEL DE RIESGO
MS09-001	MEDIO.	Con esta vulnerabilidad se logró concluir con éxito a un ataque DOS (denegación de servicios) con el uso del protocolo SMB	CRITICO
MS08-067	TOTAL	Se obtuvo acceso total al dispositivo mediante el protocolo RPC, teniendo así la capacidad de crear, modificar y eliminar registros, acceso a la Shell y permisos de súper usuario.	CCRITICO

[60] ISECOM. (2003). OSSTMM 2.1. En P. Herzog, *Manual de la metodología abierta de testeo de seguridad* (págs. 98-107)

[61] ISECOM. (2010). OSSTMM V3. En P. Herzong, *The Open Source Security Testing and Analysis* (págs. 59-62).

MS09-050	TOTAL	Se obtuvo acceso total al dispositivo mediante el protocolo SMB, teniendo así la capacidad de crear, modificar y eliminar registros, acceso a la Shell y permisos de súper usuario.	CRITICO
74496-DNS	BAJO	No se comprometió el sistema pero se demostró que la versión que se usa de DNS corresponde a una muy antigua que no posee soporte por lo que se le considera vulnerable.	CRITICO
70882 - ESXi 5.0. (VMWARE)	MEDIO	Fue posible obtener información importante del sistema de virtualización como huellas digitales y versiones del software, además que se demostró que existe la posibilidad de realizar ataques de fuerza bruta aunque no se tuvo éxito por lo que se deduce las credenciales usadas son seguras	ALTO
33850 SO. Fedora sin soporte	BAJO	No se comprometió el sistema pero se demostró que la versión del SO es obsoleta por lo que se le considera vulnerable.	CRITICO
58987- PHP	BAJO	No se comprometió el sistema pero se demostró que la versión de PHP es obsoleta por lo que se le considera vulnerable.	CRITICO
[9999] TLS- SIP (VOIP)	TOTAL	Con esta vulnerabilidad mediante el protocolo SIP se logró capturar paquetes RTP que nos permitieron interceptar conversaciones desde los equipos terminales mediante un ataque ARP de hombre en el medio.	CRITICO

Listado de directorios en intranet (emp.lns.com.ec)	TOTAL	Se pudo comprobar que mediante la manipulación del URL se puede lograr el acceso a los directorios raíz de la página web lo cual permite exhibir información sensible para el sistema.	CRITICO
41028 – Nombre por defecto del agente SNMP (public)	Total	Se obtuvo datos de configuración del dispositivo que presentaba esta vulnerabilidd	Alto
Ecriptación WPA/WPA2 redes inalambraicas	Total	Mediante la utilización de wifislax y por ende el uso de ataque de fuerza bruta se obtuvo la contraseña de dichas redes	Medio

Si durante el proceso de evaluación de la seguridad no se logró realizar alguna prueba sea porque el tiempo límite concluyo o por que no se dieron las condiciones ideales para realizar dichas pruebas se debe realizar otra bitácora indicando cuales fueron estos inconvenientes y por qué no se pudieron realizar, esto ayudará tanto al evaluador como al evaluado para mostrar la transparencia del proceso el cual servirá como un punto de referencia para una evaluación posterior. También se deberá incluir como observación si la razón por la que no se realizó dicha prueba fue una limitación es decir que la prueba podría ser peligrosa o muy costosa pudiendo causar daños colaterales al objetivo los cuales podrían ser inaceptables o incluso criminales.

Tabla 5-6 Tabla de falsos positivos

VULNERABILIDAD	ACCESO	RESULTADOS	NIVEL DE RIESGO
SQL Injection en intranet (emp.lns.con.ec)	BAJO	No se logró respuesta de la base de datos mediante la manipulación del url, también se intentó realizar el ataque con la herramienta sqlmap la cual dío como resultado que la vulnerabilidad no era inyectable, por lo que se	ALTO

		consideró esta vulnerabilidad como un falso positivo.	

Capítulo VI

6. Informe de las pruebas de penetración

El informe de las pruebas de penetración contendrá toda la información referente a las vulnerabilidades encontradas en la red y sistemas de la empresa, se describirá la metodología utilizada durante el proceso, los métodos de explotación y finalmente crearemos recomendaciones y contramedidas a cada uno de los problemas encontrados, no obstante al ser un test de penetración un proceso incierto basado en experiencias pasadas, en la información que se disponga en la actualidad y en las amenazas conocidas, será importante recalcar que todos los sistemas de información son dependientes de los seres humanos y estos son vulnerables a un cierto grado, por lo tanto no se puede considerar que las recomendaciones que se darán en el informe mitigarán por completo las amenazas, pero sí reducirán al máximo las probabilidades de un ataque de penetración. De igual manera tendremos muy en cuenta que nuevas vulnerabilidades pueden presentarse a lo largo del tiempo dando lugar a nuevas amenazas por lo que se recomendará realizar evaluaciones periódicas de la seguridad especialmente cuando se hagan cambios importantes en el hardware o software.

En cuanto a la seguridad del informe se incluirá como información adicional cláusulas respecto a la divulgación y uso del mismo que describirán el alcance, las limitaciones e impacto que tendrá este documento. Una vez concluida la redacción del informe se procederá a la entrega del mismo donde se deberán tomar todas precauciones posibles para proteger su confidencialidad debido a que esta información es considerada altamente sensible, para esto el experto en seguridad deberá resguardar una copia y entregar todas las demás a la empresa evaluada mediante canales que sean considerados seguros.

El informe detallado de los resultados obtenidos se adjuntara en el anexo 10 (ver anexo 10)

6.1.Información Legal

Al ser el informe un documento de gran importancia se deberá incluir información y cláusulas que servirán como guía para su correcto uso y limitarán la manipulación del

mismo, garantizando su confidencialidad como tal. La información contenida en este apartado está relacionada con: la descripción al respecto del tipo de contenido que se incluirá en el documento y a quien va destinado; en cuanto a las limitaciones se deberá prohibir la reproducción total o parcial, se indicará quien es el autor, quién podrá hacer uso del documento, las garantías que existen de que la información contenida sea verdadera y de ser necesario cualquier otro tipo de información que permita garantizar la correcta utilización del informe.

6.2.Detalles del documento.

En esta parte es donde irá la descripción del informe el cual contendrá información básica respecto al documento y permitirá tener una idea general de lo que se tratará en él, por ejemplo: el tipo de documento es decir cuál será su contenido, puede ser un documento de seguridad, un manual de usuario, etc., también incluirá quien es el cliente o hacia quien va dirigido, el nombre del consultor, la versión del documento y la fecha de creación.

6.3.Revisión Histórica.

La revisión histórica trata de recopilar información acerca de pruebas de penetración realizadas anteriormente, esto permitirá a quien vaya dirigido el informe tener un histórico de lo que se ha venido realizando, de esta manera podrá llevar un control de los cambios que han habido y se podrá comprobar si en realidad las amenazas encontradas en pruebas anteriores han sido correctamente eliminadas. Dentro de este apartado incluiremos información como la versión del documento anterior, la fecha en que se realizó, el autor que llevo a cabo la evaluación y una breve descripción del documento.

6.4.Limitaciones a la divulgación y uso del informe.

Dentro de un informe de seguridad siempre es importante definir de forma correcta las reglas para el uso adecuado de la información contenida en el documento, para ello se creará cláusulas de forma clara delimitando el uso y las aplicaciones del informe, entre estas tendremos que definir quienes podrán acceder a dicha información ya que este es un documento de tipo confidencial, se dará a conocer que el documento no puede ser reproducido de forma total o parcial al menos que sea autorizado por los altos mandos de

la empresa, en el caso de que el auditor haga quedar una copia este deberá garantizar la protección de la misma e informarlo en este apartado, se deberá indicar de forma clara cuál será el alcance del informe y el impacto que tendrá sobre la empresa. También deben constar cláusulas que protejan al consultor en el caso del mal uso por parte de la empresa, para lo cual se indicará que el informe contiene un reporte de vulnerabilidades a la fecha evitando así malos entendidos por la presencia de vulnerabilidades posteriores a la misma, de igual forma se indicará que las recomendaciones y contramedidas no garantizan una protección completa al cien por ciento debido principalmente al factor humano pero si reducen al máximo la posibilidad de que se realice un ataque de penetración.

6.5.Resumen Ejecutivo.

El informe ejecutivo no es más que el resumen de otro informe de mayor envergadura y contenido, este puede ser presentado como parte del informe general a manera de un resumen completo de lo que se tratará o se lo puede presentar de forma individual, en cualquiera de los casos la información será enfocada de forma clara y entendible tratando de economizar el tiempo de quien lo leerá, este empezará con una breve introducción para posteriormente resumir cada apartado y de ser necesario se agregarán graficas concisas tratando de que estas hablen por si solas. Un resumen ejecutivo viene a ser la parte más importante del documento ya que a más de ser un resumen completo este deberá estar escrito en palabras claras y sin tecnicismos para que sea entendible por los altos mandos. En este resumen básicamente incluiremos: cuál fue el objetivo de realizar las pruebas de penetración, cuál será el alcance que estas tendrán incluyendo que daños podrían causar, se indicarán las vulnerabilidades encontradas refiriéndose únicamente a aquellas vulnerabilidades de riesgo o de mayor importancia indicando conjuntamente los resultados que se obtuvieron y cuáles son las recomendaciones y contramedidas a tomar.

6.6.Detalles Técnicos.

En este segmento se realizará una descripción a detalle y de forma técnica de cada una de las herramientas usadas, así como de las metodologías empleadas en cada proceso, se deberá indicar cada uno de los objetivos a analizar para finalmente comprobar y clasificar las vulnerabilidades encontradas en cada caso.

6.6.1. Impacto de las pruebas.

Las pruebas de penetración son una de las formas más efectivas de evaluar la seguridad debido a que estas van dirigidas directamente a los dispositivos y controles (hardware y software) encargados de la seguridad. Además estas permiten demostrar de forma real el impacto de las vulnerabilidades simulando un ataque tal cual lo hiciera un delincuente informático. (403Labs Security, Simplified)[62]

Cada prueba realizada tiene un valor que demuestra cual es el impacto que tendrá sobre los sistemas, estos valores están dados en escala del 1 (Bajo) al 10 (Alto) donde 10 representa una vulnerabilidad que podría tener un impacto crítico como la toma de control de un servidor o la posibilidad de permitir sustraer información de gran valor y 1 que representa a una vulnerabilidad que no tiene un impacto directo sino más bien esta puede indicar la presencia de información que no podría ser causante de un ataque.

6.6.2. Descripción de objetivos.

Dentro de un test de penetración es importante identificar nuestros objetivos a atacar, esto debido a que hay equipos y sistemas con niveles de prioridad más altos que otros como el caso de un servidor vs un host, lo cual exigirá clasificarlos según sus características y roles que desempeñan dando prioridad a dispositivos y sistemas primarios como servidores y sistemas de VOIP para luego proseguir con otros no menos importante como los sistemas WLNA, una vez clasificados tendremos que describirlos dentro del informe, lo cual permitirá tener una idea de a que equipos se realizó las pruebas y que resultados se obtuvieron, para ello añadiremos información como: IP, MAC, Nombre del host, en el caso de una página web su URL, etc.

[62] *403Labs Security, Simplified.* (s.f.). Obtenido de http://www.403labs.com/es/professional_services/penetration_testing

6.6.3. Descripción de la metodología y estándares usados.

Es muy importante definir las metodologías usadas ya que para cualquier tarea que se desee llevar a cabo necesitaremos basarnos en algún método que nos permitirá alcanzar nuestros objetivos sin problemas y concluir nuestras pruebas con éxito, por lo cual tendremos que seguir una programación metódica que afrontará organizadamente la ejecución de nuestros ataques, lo que implica: organización, conocimiento de los antecedentes, puntos críticos a resolver, hipótesis a comprobar, datos a organizar y conclusiones a llegar.

La incorporación de la metodología usada en el informe a más de servir como referencia para realizar cada una de las pruebas, permitirá demostrar el nivel de credibilidad dentro del proceso de intrusión además de brindar un mayor grado de confianza en cuanto al proceso llevado a cabo.

6.6.4. Herramientas Usadas.

En el desarrollo del informe también es importante indicar que herramientas se utilizaron para realizar las pruebas de penetración y en que procesos estas intervinieron, esto permitirá tener una mejor idea del proceso que se siguió para determinar los distintos problemas de seguridad, además servirá como referencia para evaluaciones futuras ya que en el caso de no haber logrado concretar la comprobación de alguna vulnerabilidad sea por factores de tiempo u algún otro motivo el documentar el uso de las herramientas nos servirá como referencia para una posterior evaluación donde partiendo del informe se podrá hacer una mejor selección de herramientas lo cual minimizará esfuerzos y garantizará mejores resultados.

6.6.5. Clasificación de vulnerabilidades según su impacto en la seguridad.

Durante el proceso de la evaluación de la seguridad, cada vulnerabilidad ha sido categorizada según NESSUS como **Critica, Alta, Media, Baja y de Información,** lo cual indica que tan comprometido se puede ver un dispositivo ante una amenaza real. Además, se etiqueta y asocia a cada vulnerabilidad con un color dependiendo del riesgo que se

corra. Estas vulnerabilidades son puntuadas según CVSS (Scoring System Common Vulnerability) o Sistema de puntuación de vulnerabilidades en común donde si la vulnerabilidad es crítica tomará un valor igual a 10, si es alta su valor será entre 7 y 9.99, si es media su valor estará entre 4.1 y 6.99, si la vulnerabilidad es baja su cvss estará entra 0.1 y 4 y si es solo información tendrá un valor de 0, de esta manera se muestra a continuación un cuadro con el significado de cada una de estas clasificaciones. (Wikipedia)[63]

Tabla 6-1 Clasificación de vulnerabilidades según su impacto en la seguridad.

RIESGO	DESCRIPCIÓN
CRITICO CVSS=10	Estos hallazgos identifican situaciones que comprometerán directamente a la víctima o lograrán un acceso no autorizado como SYSTEM a la red, sistema, aplicación o información.
ALTO CVSS ENTRE 7 y 9.99	Estos hallazgos identifican situaciones que comprometerán directamente a la víctima o lograr un acceso no autorizado a la red, sistema, aplicación o información, pero sin privilegios de SYSTEM.
MEDIO CVSS ENTRE 4.1 6.99	Estos hallazgos identifican condiciones que no resultan inmediatamente o directamente en el compromiso o acceso no autorizado de una red, sistema, aplicación o información, pero proporcionan una capacidad o información que podría, en combinación con otras capacidades o información, dar lugar al compromiso o el acceso no autorizado de una red, sistema, aplicación o información. Ejemplos de Riesgos Medianos incluyen sistemas desprotegidos, archivos y servicios que podrían resultar en la denegación de servicios o sistemas no críticos.
BAJO CVSS ENTRE 0.1 Y 4	Estos hallazgos identifican situaciones que no resultan inmediatamente o directamente en el compromiso de una red, sistema, aplicación o información, pero no proporcionar información que

[63] *Wikipedia.* (s.f.). Obtenido de http://en.wikipedia.org/wiki/CVSS

	podría ser utilizada en combinación con otra información para obtener acceso no autorizado a una red, sistema, aplicación o información. Ejemplos de bajos riesgos incluyen cookies no marcadas como seguras; sesiones concurrentes, etc.
INFORMACIÓN CVSS IGUAL A 0	Estos hallazgos incluyen únicamente información que no comprometen a los sistemas en absoluto.

El informe también deberá contener los diagramas de la red según sea el caso, un diagrama de la red interna si estamos trabajando sobre una prueba de penetración interna y uno externo si estamos trabajando sobre un pentest externo o ambos si es necesario, esto permitirá identificar posibles fallas en cuanto al diseño, implementación o configuración de los dispositivos de red. En este apartado también se deberá documentarse problemas que se encuentren como la falta o mala configuración de un firewall, inexistencia de zonas de seguridad, separación entre datos, audio (VOIP), etc.

6.6.6. Red Externa.

Las redes externas hacen referencia a una red que se extiende fuera del perímetro local de la empresa y no es de su propiedad, este tipo de redes hace referencia a internet un conjunto de redes que podrían interconectar sucursales de la empresa mediante el transporte de información por accesos extendidos y seguros de un lugar a otro, lo importante en este caso es identificar los posibles ISP y DNS para determinar rutas y lograr un acceso desde el equipo del atacante hacia la víctima y en base a esto identificar si su implementación es correcta o no. (Blog Tecnológico)[64]

6.6.7. Red Interna.

Una red interna corresponde al conjunto de redes, tuberías, accesorios y equipos, que integran un sistema de comunicaciones, que se encuentra al interior de los predios de la empresa y es de su propiedad, estas redes están diseñadas para permitir que solo usuarios

[64] *Blog Tecnológico.* (s.f.). Obtenido de http://programoweb.com/redes-internas-y-externas/

con los privilegios y contraseñas adecuados puedan acceder, donde se identificarán componentes importantes como Reuters, rangos de IP, Firewalls, etc., de forma que determinemos la estructura de la red y en base a esto concluir si es su implementación adecuada . (Cómputo Práctico)[65]

6.7.Hallazgos y Resumen de los resultados.

Una vez que se han detallado metodologías, herramientas, nivel de vulnerabilidades, será momento de realizar una bitácora con el resumen de los resultados obtenidos, donde se indicará a detalle cuales son las vulnerabilidades encontradas, dentro de que sistema fueron descubiertas y que impacto tendrían estas en caso de ser explotadas. Para complementar este informe se deberá incluir capturas de pantalla donde se compruebe y verifique que en realidad se pudo explotar dichas vulnerabilidades.

6.8.Posibles Soluciones.

En este apartado se tratarán las posibles contramedidas o recomendaciones que serán expuestas para brindar soluciones a cada una de las vulnerabilidades encontradas, estas recomendaciones podrán ir desde una simple actualización hasta la completa renovación del hardware y software.

6.9.Conclusiones de las pruebas.

Finalmente se detallarán las conclusiones a las que ha llegado el evaluador de la seguridad, estas deben ser muy concretas y explicitas, tratando de dar una idea global de cómo se encuentra la seguridad en la institución recalcando cuáles son sus debilidades y fortalezas. Una buena conclusión resumirá los puntos principales del trabajo realizado con respecto a la evaluación de la seguridad y permitirá al evaluado tener una visión más clara del informe y le permitirá ser más asertivo al momento de tomar alguna decisión.

[65] *Computo Práctico.* (s.f.). Obtenido de http://computopractico.blogspot.com/2009/09/ccna-1-2112-redes-internas-y-externas.html

Conclusiones:

Concluimos del presente trabajo de investigación que la metodología desarrollada y usada para la evaluación de vulnerabilidades dentro de Editorial Don Bosco es: útil, versátil y confiable, la cual posee un marco claro, organizado y bien definido que brindo muy buenos resultados en un periodo de tiempo razonable.

Es de vital importancia dentro del proceso de la evaluación de la seguridad que el personal que llevará a cabo las pruebas de penetración posean una formación adecuada y con una buena experiencia, esto garantizará que el proceso sea transparente garantizando buenos resultados al terminar la evaluación.

La fase de exploración constituye una de las más importantes al momento de tratar de determinar cuan expuestos se encuentran nuestros sistemas al público ya que nos brinda una perspectiva de cómo nos vemos fuera del perímetro empresarial.

Un test de penetración de caja blanca debe ser lo primero a realizar dentro de toda empresa que va iniciar a evaluar sus sistemas de seguridad, debido a que este tipo de prueba nos proporcionará una lista completa de fallos con mucho más éxito que un test de penetración de caja negra.

La fase de exploración dentro del proceso de penetración será de la que dependa el éxito de las pruebas, y mientras más minuciosa sea y se consiga sustraer mayor cantidad de datos, esta permitirá que sea más fácil llevar a cabo la evaluación de la seguridad.

El análisis de datos, la clasificación de objetivos y la enumeración de usuarios llevada a cabo dentro de la fase de evaluación, permitirán identificar los blancos críticos como servidores u otros sistemas de importancia que nos permitirán obtener un control total sobre algún activo de la empresa.

La fase de intrusión nos permitirá comprobar las vulnerabilidades encontradas en los sistemas analizados, siendo su principal objetivo el tomar el control y escalar privilegios de las victimas descartando con esto falsos positivos.

Un falso positivo no implica que la vulnerabilidad no exista, pero sí que no se la pudo comprobar con las herramientas usadas y en el periodo de tiempo establecido, lo cual crea un punto de partida para una posterior evaluación.

El informe debe ser redactado adecuadamente y con la información necesaria, permitiendo que su lector pueda tener una idea clara del proceso que se llevó a cabo, al ser este un documento confidencial se debe tener en cuenta cláusulas que indicarán su correcto uso.

Dentro de un test de penetración se debe tener en claro que no se podrá brindar una completa solución para convertir nuestros sistemas en impenetrables, esto debido a que todos estos sistemas dependen de la manipulación de los ser humanos los cuales poseen un cierto nivel de vulnerabilidad.

Recomendaciones:

Se recomienda hacer uso de esta metodología sin saltarse ninguno de los pasos aquí descritos, ya que de esto dependerá el éxito o fracaso en el proceso de la evaluación de la seguridad.

Mantener total confidencialidad y apegarse a las políticas de seguridad de la empresa, teniendo en cuenta al acuerdo firmado con anterioridad el cual es documento que no puede ser olvidado durante todo el proceso de desarrollo.

Capacitar a los empleados en aspectos de seguridad para que no sean fácilmente vulnerables a ataques de ingeniería social e implementar y definir políticas y procedimientos claros que permitan tomar acciones rápidas en caso de la presencia de un ataque.

Mantener aislados y por separados sistemas de DATOS con sistemas VOIP de tal forma que no se facilite la intromisión de un sistema a otro, haciendo uso de herramientas como la creación de VLANS y la correcta definición de zonas de seguridad (DMZ, LAN, WLAN, WAN).

Definir con claridad roles y permisos según el nivel de acceso que tendrán los usuarios para evitar la escala de privilegios o el mal uso del sistema.

Se recomienda a la Empresa mantenerse al día con las actualizaciones de todos sus sistemas operativos, firewalls, antivirus, etc., con el fin de reducir vulnerabilidades creadas por la falta de algún parche, dejando así al descubierto puertas para un posible ataque de penetración.

Concientizar a los Autoridades de la empresa que evaluar los sistemas es un procedimiento necesario y que el implementar acciones oportunas puede evitar el desprestigio de la empresa y pérdidas económicas.

Bibliografía

(s.f.). Obtenido de http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39612

wikipedia. (9 de Marzo de 2013). Obtenido de http://es.wikipedia.org/wiki/Ataque_de_fuerza_bruta

403Labs Security, Simplified. (s.f.). Obtenido de http://www.403labs.com/es/professional_services/penetration_testing

Al Sabbagh, B. D. (26-28 de Junio de 2012). ST(CS)2 - Featuring socio-technical cyber security warning systems. 978-1-4673-1425-1.

Alfon. (2010). *Seguridad y Redes.* Obtenido de http://seguridadyredes.wordpress.com

Alfon. (2010). *Seguridad y Redes.* Obtenido de http://seguridadyredes.wordpress.com/2010/04/05/wireshark-captura-conversaciones-voip-protocolo-sip-sdp-y-rtp-extraccion-de-audio/

ÁLVAREZ, C. (s.f.). *www.informatica-juridica.com*. Recuperado el 18 de 11 de 2014, de www.informatica-juridica.com: http://www.informatica-juridica.com/trabajos/Ataques_de_fuerza_bruta.asp

Blog Tecnológico. (s.f.). Obtenido de http://programoweb.com/redes-internas-y-externas/

Caire, R. (s.f.). *Segurida y Ética.* Obtenido de http://seguridadetica.wordpress.com/2012/05/17/7-consejos-utiles-al-contratar-un-servicio-de-pen-testing/

Caridad), H. (. (2011). *Tutorial de Metasploit Framework de Offensive-Securitty.*

Castellanos, E. J. (4 de Mayo de 2011). *revista.seguridad.unam.mx*. Recuperado el 3 de 12 de 2014, de revista.seguridad.unam.mx: http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

Cavañate, A. M. (s.f.). *Universitat Pompeu Fabra.* Obtenido de http://www.upf.edu/hipertextnet/numero-1/sistem_infor.html#3.2.2

Cibernautas, |. C. (22 de Julio de 2009). Los usuarios, la principal amenaza informática. *SinMordaza*, pág. 1.

Cómputo Práctico. (s.f.). Obtenido de http://computopractico.blogspot.com/2009/09/ccna-1-2112-redes-internas-y-externas.html

Conociendo Meterpreter. (08 de Diciembre de 2013). Obtenido de http://highsec.es/2013/08/conociendo-meterpreter-parte-ii-escalar-privilegios/

Cornejo, S. (Julio de 2013). *highsec.es*. Obtenido de http://highsec.es/2013/07/buenas-practicas-para-realizar-una-auditoria-de-seguridad-a-empresas/

Council, P. S. (Marzo de 2008). Obtenido de https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/doc/information_supplement_11.3.pdf

Ditech . (2010). *ditech.com.co*. Obtenido de ditech.com.co: http://ditech.com.co/soluciones-integrales/seguridad-informatica-en-redes/revencion-de-intrusos-ips/

Eric Romang Blog. (s.f.). Obtenido de http://eromang.zataz.com/2012/05/06/metasploit-vmware-auxiliary-modules/

Espinoza, A. C. (6 de Marzo de 2013). *El Observatorio.* Obtenido de http://oiprodat.com/2013/03/06/delitos-informaticos-y-comercio-electronico-ecuador/

Fedora. (s.f.). Obtenido de https://fedoraproject.org/wiki/End_of_life?rd=LifeCycle/EOL

Fuente, R. C. (2013). *Virus Cascade.* Madrid: Universidad Complutense de Madrid.

Gil, R. G. (2012). *Seguridad en VoIP: Ataques, Amenazas y Riesgos.* Valencia - España: Universidad De Valencia.

Gil, R. G. (2013). *Evasión de Sistemas de Detección de Intrusos.*

Gotterbarn, D. E. (14-17 April 2008). Using the Software Engineering Code of Ethics in Professional Computing Issues. *Software Engineering Education and Training, 2008. CSEET '08. IEEE 21st Conference on* (pág. 273). Charleston, SC: IEEE.

Graves, K. (20 de Octubre de 2012). *CEH Certified Ethical Hacker Review Guide.* Obtenido de http://www.it-docs.net/ddata/863.pdf

Guerrero, E. G. (12 de Enero de 2012). *revista.seguridad*. Recuperado el 16 de Septiembre de 2014, de http://revista.seguridad.unam.mx/numero-12/la-importancia-de-las-pruebas-de-penetraci%C3%B3n-parte-i

Guirado, A. R., CISA, & CGEIT. (2009). *Penetration Testing - Conceptos generales y situación actual.* ISACA.

Hack Story. (22 de Julio de 2013). Obtenido de http://hackstory.net/Ingenier%C3%ADa_social

ISECOM. (2003). OSSTMM 2.1. En P. Herzog, *Manual de la metodología abierta de testeo de seguridad* (págs. 98-107).

ISECOM. (2010). OSSTMM V3. En P. Herzong, *The Open Source Security Testing and Analysis* (págs. 59-62).

JORGE ORELLANA, C. V. (2012). *PROPUESTA DE BEST PRACTICE PARA EL ANALISIS DE VULNERABILIDADES, MÉTODOS DE PREVENCIÓN Y PROTECCIÓN APLICADOS A LA INFRAESTRUCTURA DE RED DEL LABORATORIO DE SISTEMAS.* RIOBAMBA – ECUADOR: ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

Juan Antonio Calles García, P. G. (2011). *La biblia del Footprinting.* Flu Project.

KasperskyLab. (s.f.). Obtenido de http://latam.kaspersky.com/internet-security-center/definitions/spear-phishing

Managing Director of ISECOM - pete<at>isecom.org. (s.f.). Open-Source Security Testing Methodology Manual.

Michael Dyrmose, S. C. (2013). *Beating the IPS.* Dubex A/S.

Mifsud, E. (26 de Marzo de 2012). *Introducción a la seguridad informática - Políticas de seguridad.* Recuperado el 11 de 12 de 2014, de recursostic.educacion.es: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

Montero, V. H. (2005). *Técnicas del penetration test.* Buenos Aires: CYBSEC S.A.

Montero, V. H. (2015). *Técnicas del penatration testing.* Buenos Aires: CYBSEC.

OWASP. (2008). *Guia De Pruebas OWASP.* OWASP.

OWASP. (2008). Guía de pruebas OWASP. En O. Foundation, *Guía de pruebas OWASP* (págs. 75-76). OWASP.

OWASP. (17 de Noviembre de 2014). *owasp.org*. Obtenido de www.owasp.org: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

OWASP. (13 de Marzo de 2014). *www.owasp.org*. Obtenido de OWASP Joomla Vulnerability Scanner Project: https://www.owasp.org/index.php?title=Category:OWASP_Joomla_Vulnerability_Scanner_Project&setlang=es

Panda Security. (s.f.). Obtenido de http://www.pandasecurity.com/spain/homeusers/security-info/204670/information/MS09-001

Panda Security. (s.f.). Obtenido de http://www.pandasecurity.com/spain/homeusers/security-info/214066/information/MS09-050

Panda Security. (s.f.). Obtenido de http://www.pandasecurity.com/spain/homeusers/security-info/202013/information/MS08-067

Peter Vincent Herzog, t. I. (2003). *OSSTMM 2.1.*

PHP. (s.f.). Obtenido de http://php.net/eol.php

Plata, A. R. (2010). *Ethical Hacking.* Mexico: UNAM-CERT Equipo de Respuesta a Incidentes UNAM.

Quezada, A. E. (s.f.). *Kaly Linux.* Obtenido de http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf

Ramos, J. L. (2013). PRUEBAS DE PENETRACIÓN O PENT TEST. *Revista de Información, Tecnología y Sociedad*.

Ramos, J. V. (2011). *CICLO DE VIDA DE UNA PRUEBA DE PENETRACIÓN FÍSICA.* Guatemala: Universidad de San Carlos de Guatemala.

Redes y Seguridad. (s.f.). Obtenido de http://www.redesyseguridad.es/voip-protocolo-sip/

Reyna, R. Z. (s.f.). Obtenido de http://www.cec.espol.edu.ec/blog/rzambrano/files/2012/08/DELITOS-INFORM%C3%81TICOS-CONTEMPLADOS-EN-LA-LEY-ECUATORIANA.pdf

Sans. (s.f.). Obtenido de http://www.sans.org/security-resources/idfaq/snmp.php

Soporte Microsoft. (s.f.). Obtenido de http://support2.microsoft.com/lifecycle/?c2=1163

SYKRAYO Y LAS F.C.S. (s.f.). Obtenido de https://sites.google.com/site/sykrayolab/ataques-informaticos

Técnicas de Hacking THW. (s.f.). Obtenido de http://thehackerway.com/2011/03/11/comandos-y-conceptos-basicos-metasploit-framework/

TrustedSec. (s.f.). Obtenido de https://www.trustedsec.com/social-engineer-toolkit/

Weik, M. (2001). Computer Science and Communications Dictionary. 978-0-7923-8425-0. doi:10.1007/1-4020-0613-6_13786

Wikipedia. (s.f.). Obtenido de http://en.wikipedia.org/wiki/Session_Initiation_Protocol

Wikipedia. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Exploit

Wikipedia. (s.f.). Obtenido de http://en.wikipedia.org/wiki/CVSS

Wildauer, E. D.-U. (19-22 June 2013). Ethical, social, privacy, security and moral issues in an e-society. *Information Systems and Technologies (CISTI), 2013 8th Iberian Conference on* (págs. 1-6). Lisboa: IEEE.

wireshark. (10 de Mayo de 2011). */wiki.wireshark.org/*. Obtenido de wiki.wireshark.org/: http://wiki.wireshark.org/TCP_Analyze_Sequence_Numbers

Anexos

Anexo 1 Acuerdo de Confidencialidad.

ACUERDO DE CONFIDENCIALIDAD ESPECÍFICO PARA LA REALIZACIÓN DEL PROYECTO DE TESIS "METODOLOGÍA PARA REALIZAR LA EVALUACIÓN, DETECCIÓN DE RIESGOS, VULNERABILIDADES Y CONTRAMEDIDAS EN EL DISEÑO E IMPLEMENTACION DE LA INFRAESTRUCTURA DE LA RED DE LA EDITORIAL DON BOSCO, MEDIANTE UN TEST DE INTRUSIÓN DE CAJA BLANCA" A REALIZAR EN LA EDITORIAL DON BOSCO.

PRIMERA: DE LAS PARTES.- En Cuenca, al 30 de Agosto de 2014, suscriben el presente acuerdo de confidencialidad, por una parte Cristina Maribel Jaramillo Castillo, con domicilio en la ciudadela Kennedy, Cuenca Provincia del Azuay con CI. 0302355656, Juan Carlos Riofrío Herrera, con domicilio en Barrial Blanco, Cuenca Provincia del Azuay con CI. 1104915937, estudiantes de la carrera de Ingeniería de Sistemas, mención Telemática de la Universidad Politécnica Salesiana y por otra parte Hernando Abril en calidad de Jefe del Departamento de Sistemas de la Editorial Don Bosco con domicilio en Vega Muñoz, Cuenca Provincia del Azuay con CI. 0102600079, quienes reconocen capacidad jurídica suficiente para suscribir el presente documento.

SEGUNDA: ANTECEDENTES.- Para proteger adecuadamente los activos de la información de la Editorial Don Bosco, el departamento de sistemas requiere valorar el estado de la seguridad periódicamente, mediante la realización de pruebas de penetración y evaluaciones de vulnerabilidades. Estas actividades implican la exploración de los equipos de escritorio, portátiles, servidores, elementos de red, dispositivos de VOIP y página web de la empresa, de forma regular y periódica para descubrir las vulnerabilidades presentes en estos sistemas donde sólo con el conocimiento de estas deficiencias puede la empresa aplicar parches de seguridad u otros controles de compensación para mejorar la seguridad en su entorno.

TERCERA: OBJETO.- A fin de regular las relaciones, conforme a lo descrito en los antecedentes, los estudiantes acuerdan que, toda la información que intercambie o a la que tengan acceso de manera directa o indirecta, estará amparada, alcanzada y protegida por los términos del presente Acuerdo de Confidencialidad y que dicho intercambio se regirá por las condiciones enunciadas a continuación.

CUARTA: NATURALEZA DEL ARCUERDO.-El propósito de este acuerdo es conceder la autorización a los estudiantes, quienes llevarán a cabo la evaluación de vulnerabilidades y pruebas de penetración a manera de trabajo de fin de carrera, ellos tendrán permiso para para realizar el escaneo de los equipos informáticos y página web de la organización, evaluaciones de vulnerabilidades y pruebas de penetración. Este permiso se concede desde el 30 de Agosto de 2014 hasta 28 de Febrero de 2015.

QUINTA: DERECHOS DE PROPIEDAD INTELECTUAL.- Se deja constancia expresa de que el desarrollo de cualquier metodología o proceso que se obtuviere durante el tiempo del presente acuerdo, es de propiedad de quien la desarrolle, sin embargo se deja constancia que Editorial Don Bosco podrá utilizar dichos descubrimientos para su beneficio

SEXTA: CONFIDENCIALIDAD.- Los comparecientes expresamente acuerdan guardar la confidencialidad de la información de cualquier naturaleza que llegaren a tener con ocasión del desempeño de sus labores. Por lo tanto, los comparecientes se obligan a no revelar ningún tipo de información relacionada con la operación de los estudiantes, la empresa y sus clientes, proveedores o consultores. La confidencialidad abarca, sin excluir otra clase de información, a cualquier cifra, sistema, procedimiento o conocimiento técnico al que hayan tenido acceso. Sin embargo para efectos académicos los estudiantes podrán divulgar y comunicar la información técnica relacionada con la metodología sin revelar información susceptible, si fuera necesario dicha información deberá ser cifrada o alterada de forma que no sea identificada para mantener la confidencialidad de la misma.

SÉPTIMA: OBLIGACIONES DE LOS ESTUDIANTES.- Los estudiantes se obligan a entregar todo el material e información necesaria correspondiente a su trabajo de investigación y se comprometen a:

a) No utilizar la información o fragmentos de esta para fines distintos a la evaluación de la seguridad.
b) Cumplir con el cronograma de actividades establecido previamente, junto con el jefe de sistemas de Editorial Don Bosco a fin de concluir exitosamente con la valoración de la seguridad de la empresa.

OCTAVA: OBLIGACIONES DE LA EMPRESA.- La empresa se obliga a permitir a los estudiantes la publicación académica del trabajo de investigación y se compromete a:

a) Brindar el acceso físico a la empresa y a la información necesaria para llevar a cabo las pruebas de penetración.
b) Proporcionar a los estudiantes un espacio físico para la realización de sus labores.

c) Impedir la copia o revelación de esa información a terceros, salvo que gocen de aprobación escrita del Gerente General, y únicamente bajo los términos de tal aprobación.

NOVENA: VIGENCIA Y DURACIÓN DEL ACUERDO.- El presente acuerdo estará en vigencia a partir de la fecha de su suscripción y tendrá una duración de 6 meses

Las partes se comprometen a cumplir con todos los términos fijados en el presente acuerdo, y especialmente aquellos relativos a las cláusulas sobre propiedad intelectual y confidencialidad.

DÉCIMA: TERMINACIÓN.-El presente acuerdo se dará por terminado, sin perjuicio de las demás causales establecidas en la ley, en los siguientes eventos:

a) Vencimiento del plazo pactado de este acuerdo o de cualquiera de sus prorrogas.
b) Mutuo acuerdo.
c) Aviso escrito que una de las partes de a la otra, con treinta (30) días de antelación a la fecha en que se pretenda dar por terminado.

Las partes acuerdan que este documento podrá ser expuesto como anexo en el trabajo de fin de carrera realizado por los estudiantes.

Anexo 2 Servicios activos red 192.xxx.xxx.0.724

RED 192.xxx.xxx.0/24					
Host	Puerto	Protocolo	Estado	Servicio	Versión
192.xxx.xxx.1	22	tcp	open	ssh	Cisco IP Phone CP-7900G-series sshd (protocol 2.0)
	80	tcp	open	tcpwrapped	
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.2	80	tcp	open	http	lighttpd
	443	tcp	open	http	lighttpd
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.11 192.xxx.xxx.12 192.xxx.xxx.21	22	tcp	open	ssh	Cisco IP Phone CP-7900G-series sshd (protocol 2.0)
	80	tcp	open	tcpwrapped	
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.31					
	23	tcp	open	telnet	NASLite-SMB/Sveasoft Alchemy firmware telnetd
	53	tcp	open	domain	
	80	tcp	open	http	GoAhead-Webs embedded httpd
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.32	22	tcp	open	ssh	Dropbear sshd 2013.58 (protocol 2.0)
	80	tcp	open	http	mini_httpd 1.19 19dec2003
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.41	80	tcp	open	http	mini_httpd 1.19 19dec2003
	1720	tcp	open	H.323/Q.931	
	12345	tcp	open	netbus	
192.xxx.xxx.81 192.xxx.xxx.82	22	tcp	open	ssh	Cisco IP Phone CP-7900G-series sshd (protocol 2.0)
	80	tcp	open	tcpwrapped	
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.83	80	tcp	open	http	
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.85	23	tcp	open	telnet	NASLite-SMB/Sveasoft Alchemy firmware telnetd
	53	tcp	open	domain	
	80	tcp	open	http	GoAhead-Webs embedded httpd
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.86	22	tcp	open	ssh	Cisco IP Phone CP-7900G-series sshd (protocol 2.0)
	80	tcp	open	tcpwrapped	
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.91	443	tcp	open	https	
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.92 192.xxx.xxx.94 192.xxx.xxx.95	22	tcp	open	ssh	Cisco IP Phone CP-7900G-series sshd (protocol 2.0)
	80	tcp	open	tcpwrapped	
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.100	22	tcp	open	ssh	Cisco IP Phone CP-7900G-series sshd (protocol 2.0)
	80	tcp	open	http	Allegro RomPager 4.34
	1720	tcp	open	H.323/Q.931	
192.xxx.xxx.xxx	80	tcp	open	http	Cisco ATA186 VoIP adapter http config
	1720	tcp	open	H.323/Q.931	

192.xxx.xxx.111 192.xxx.xxx.112 192.xxx.xxx.113 192.xxx.xxx.114 192.xxx.xxx.121 192.xxx.xxx.122 192.xxx.xxx.131 192.xxx.xxx.141 192.xxx.xxx.142 192.xxx.xxx.143 192.xxx.xxx.151 192.xxx.xxx.xxx 192.xxx.xxx.202 192.xxx.xxx.205	22 80 1720	tcp tcp tcp	open open open	ssh tcpwrapped H.323/Q.931	Cisco IP Phone CP-7900G-series sshd (protocol 2.0)	
192.xxx.xxx.204	80 1720	tcp tcp	open open	http H.323/Q.931	Cisco ATA186 VoIP adapter http config	
192.xxx.xxx.250	22 80 427 443 902 1720 5988 5989 6000 6001 6002 6003 6004 6005 6006 6007 6009 6025 6059 8000 8100 8300	tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp	closed open open open open open closed open closed closed closed closed closed closed closed closed closed closed closed open open closed	ssh http svrloc https iss-realsecure H.323/Q.931 wbem-http wbem-https X11 X11:1 X11:2 X11:3 X11:4 X11:5 X11:6 X11:7 X11:9 x11 X11:59 http-alt xprint-server tmi		
192.xxx.xxx.253	22 25 80 110 111 143 443 749 993 995 1720 3306 4445	tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp tcp	open open open open open open filtered open open open open open open	ssh smtp http pop3 rpcbind imap https status imap pop3 H.323/Q.931 mysql upnotifyp	OpenSSH 4.3 (protocol 2.0) Postfix smtpd Apache httpd 2.2.3 ((CentOS)) Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-12.el5_7.2 2 (RPC #100000) Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-12.el5_7.2 1 (RPC #100024) Cyrus imapd Cyrus pop3d MySQL 5.0.95	
192.xxx.xxx.254	1720 1723 2000 8291	tcp tcp tcp tcp	open open open open	H.323/Q.931 pptp bandwidth-test tcpwrapped	MikroTik (Firmware: 1) MikroTik bandwidth-test server	

Anexo 3 Servicios activos en los hosts de la red 192.xxx.xxx.0/24

RED 192.xxx.xxx.0/24					
Host	Puerto	Protocolo	Estado	Servicio	Versión
192.xxx.xxx.254	22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
	80	tcp	open	http	
	264	tcp	open	fw1-topology	Checkpoint FireWall-1 Topology
	443	tcp	open	http	Connectra Check Point Web Security httpd
	500	tcp	open	isakmp	
	8099	tcp	open	soap	gSOAP soap 2.7
192.xxx.xxx.253	22	tcp	open	ssh	Cisco SSH 1.25 (protocol 1.99)
	23	tcp	open	telnet	Cisco router telnetd
	80	tcp	open	http	Cisco IOS http config
	443	tcp	open	http	Cisco IOS http config
192.xxx.xxx.252	80	tcp	open	http	Cisco IOS http config
192.xxx.xxx.251 192.xxx.xxx.250 192.xxx.xxx.249 192.xxx.xxx.248 192.xxx.xxx.248	23	tcp	open	telnet	Cisco router telnetd
	80	tcp	open	http	Cisco IOS http config
192.xxx.xxx.223	23	tcp	open	telnet	BusyBox telnetd
	80	tcp	open	http	
	9000	tcp	open	tcpwrapped	
192.xxx.xxx.214	80	tcp	open	http	thttpd 2.25b 29dec2003
	443	tcp	open	http	thttpd 2.25b 29dec2003
192.xxx.xxx.xxx (dad00.lns.com.ec)	42	tcp	open	tcpwrapped	
	53	tcp	open	domain	Microsoft DNS 6.0.6001
	88	tcp	open	kerberos-sec	Windows 2003 Kerberos (server time: 2014-09-10 15:06:49Z
	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	389	tcp	open	ldap	
	445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
	464	tcp	open	kpasswd5	
	593	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
	636	tcp	open	tcpwrapped	
	3268	tcp	open	ldap	
	3269	tcp	open	tcpwrapped	
	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
	5800	tcp	open	vnc-http	Ultr@VNC (Name dad00; Resolution 1152x896; VNC TCP p
	5900	tcp	open	vnc	VNC (protocol 3.8)
	49152	tcp	open	msrpc	Microsoft Windows RPC
	49153	tcp	open	msrpc	Microsoft Windows RPC
	49154	tcp	open	msrpc	Microsoft Windows RPC
	49156	tcp	open	msrpc	Microsoft Windows RPC
	49157	tcp	open	msrpc	Microsoft Windows RPC
	49158	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
	49163	tcp	open	msrpc	Microsoft Windows RPC
	49165	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.199	7	tcp	open	echo	
	80	tcp	open	http	HP LaserJet P2035n printer http config 4.7.1.12
	515	tcp	open	printer	
	8290	tcp	open	unknown	
	9100	tcp	open	jetdirect	

192.xxx.xxx.198	🟢	80	tcp	open	http	Virata-EmWeb 6.0.1
	🟢	139	tcp	open	netbios-ssn	
	🟢	515	tcp	open	printer	
	🟢	9100	tcp	open	jetdirect	
	🟢	10002	tcp	open	documentum	
192.xxx.xxx.195 192.xxx.xxx.193	🟢	21	tcp	open	ftp	HP LaserJet P4014 printer ftpd
	🟢	23	tcp	open	telnet	HP JetDirect telnetd
	🟢	80	tcp	open	http	Virata-EmWeb 6.2.1 (HP LaserJet http config)
	🟢	280	tcp	open	http	Virata-EmWeb 6.2.1 (HP LaserJet http config)
	🟢	443	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	🟢	515	tcp	open	printer	
	🟢	631	tcp	open	http	Virata-EmWeb 6.2.1 (HP LaserJet http config)
	🟢	9100	tcp	open	jetdirect	
192.xxx.xxx.188	🟢	21	tcp	open	ftp	HP JetDirect ftpd
	🟢	23	tcp	open	telnet	HP JetDirect printer telnetd (No password)
	🟢	80	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	🟢	280	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	🟢	443	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	🟢	515	tcp	open	printer	
	🟢	631	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	🟢	7627	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	🟢	9100	tcp	open	jetdirect	
	🟢	14000	tcp	open	tcpwrapped	
192.xxx.xxx.186	🟢	21	tcp	open	ftp	HP LaserJet P4014 printer ftpd
	🟢	23	tcp	open	telnet	HP JetDirect telnetd
	🟢	80	tcp	open	http	Virata-EmWeb 6.2.1 (HP printer http config)
	🟢	280	tcp	open	http	Virata-EmWeb 6.2.1 (HP printer http config)
	🟢	443	tcp	open	http	Virata-EmWeb 6.2.1 (HP printer http config)
	🟢	515	tcp	open	printer	
	🟢	631	tcp	open	http	Virata-EmWeb 6.2.1 (HP printer http config)
	🔴	1025	tcp	filtered	NFS-or-IIS	
	🔴	1026	tcp	filtered	LSA-or-nterm	
	🔴	1027	tcp	filtered	IIS	
	🔴	1028	tcp	filtered	unknown	
	🔴	1029	tcp	filtered	ms-lsa	
	🔴	1030	tcp	filtered	iad1	
	🟢	4242	tcp	open	http	RapidLogic httpd 1.1
	🟢	9100	tcp	open	jetdirect	
192.xxx.xxx.185	🟢	21	tcp	open	ftp	HP LaserJet P4014 printer ftpd
	🟢	23	tcp	open	telnet	HP JetDirect telnetd
	🟢	80	tcp	open	http	HP JetDirect printer webadmin (HP-ChaiServer 3.0)
	🟢	280	tcp	open	http	HP JetDirect printer webadmin (HP-ChaiServer 3.0)
	🟢	443	tcp	open	http	HP JetDirect printer webadmin (HP-ChaiServer 3.0)
	🟢	515	tcp	open	printer	
	🟢	631	tcp	open	http	HP JetDirect printer webadmin (HP-ChaiServer 3.0)
	🟢	9100	tcp	open	jetdirect	
192.xxx.xxx.181	🟢	111	tcp	open	rpcbind	2 (RPC #100000)
	🟢	513	tcp	open	login	

192.xxx.xxx.179		7	tcp	open	echo	
		80	tcp	open	http	HP LaserJet P2035n printer http config 4.7.1.12
		515	tcp	open	printer	
		8290	tcp	open	unknown	
		9100	tcp	open	jetdirect	
192.xxx.xxx.155 192.xxx.xxx.145		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
		1025	tcp	open	msrpc	Microsoft Windows RPC
		1047	tcp	open	msrpc	Microsoft Windows RPC
		3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
192.xxx.xxx.138		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
		1110	tcp	filtered	nfsd-status	
		5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
		49152	tcp	open	msrpc	Microsoft Windows RPC
		49153	tcp	open	msrpc	Microsoft Windows RPC
		49154	tcp	open	msrpc	Microsoft Windows RPC
		49155	tcp	open	msrpc	Microsoft Windows RPC
		49156	tcp	open	msrpc	Microsoft Windows RPC
		49159	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.135		80	tcp	open	http	Apache httpd 2.2.11 ((Win32) DAV/2 mod_ssl/2.2.
		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		443	tcp	open	http	Apache httpd 2.2.11 ((Win32) DAV/2 mod_ssl/2.2.
		445	tcp	open	netbios-ssn	
		3306	tcp	open	mysql	MySQL (unauthorized)
		3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
		5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
		49152	tcp	open	msrpc	Microsoft Windows RPC
		49153	tcp	open	msrpc	Microsoft Windows RPC
		49154	tcp	open	msrpc	Microsoft Windows RPC
		49155	tcp	open	msrpc	Microsoft Windows RPC
		49156	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.134		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds

192.xxx.xxx.131		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
		777	tcp	filtered	multiling-http	
		1110	tcp	open	tcpwrapped	
		2869	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
		3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
		4567	tcp	filtered	tram	
		5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583 (
		5900	tcp	open	vnc	VNC (protocol 3.3; Locked out)
		19780	tcp	open	unknown	
		31038	tcp	open	msrpc	Microsoft Windows RPC
		49152	tcp	open	msrpc	Microsoft Windows RPC
		49153	tcp	open	msrpc	Microsoft Windows RPC
		49154	tcp	open	msrpc	Microsoft Windows RPC
		49155	tcp	open	msrpc	Microsoft Windows RPC
		49156	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.127		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
		5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
		9999	tcp	open	abyss	
		49152	tcp	open	msrpc	Microsoft Windows RPC
		49153	tcp	open	msrpc	Microsoft Windows RPC
		49154	tcp	open	msrpc	Microsoft Windows RPC
		49155	tcp	open	msrpc	Microsoft Windows RPC
		49158	tcp	open	msrpc	Microsoft Windows RPC
		49159	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.122		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
192.xxx.xxx.121		88	tcp	open	kerberos-sec	Heimdal Kerberos (server time: 2014-09-10 15:02:00Z)
		548	tcp	open	afp	Apple AFP (name: CGSVICENTE; protocol 3.4; Mac OS
		631	tcp	open	ipp	CUPS 1.5
		1947	tcp	open	sentinelsrm	
192.xxx.xxx.116		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
		1110	tcp	filtered	nfsd-status	
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
192.xxx.xxx.115		21	tcp	open	ftp	HP LaserJet P4014 printer ftpd
		23	tcp	open	telnet	HP JetDirect telnetd
		80	tcp	open	http	Virata-EmWeb 6.2.1 (HP LaserJet http config)
		280	tcp	open	http	Virata-EmWeb 6.2.1 (HP LaserJet http config)
		443	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
		515	tcp	open	printer	
		631	tcp	open	http	Virata-EmWeb 6.2.1 (HP LaserJet http config)
		9100	tcp	open	jetdirect	

192.xxx.xxx.113	80	tcp	open	http	Microsoft IIS httpd 8.5
	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	443	tcp	open	skype2	Skype
	445	tcp	open	netbios-ssn	
	2869	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
	3389	tcp	open	ms-wbt-server	
	5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
	5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
	5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
	49152	tcp	open	msrpc	Microsoft Windows RPC
	49153	tcp	open	msrpc	Microsoft Windows RPC
	49154	tcp	open	msrpc	Microsoft Windows RPC
	49155	tcp	open	msrpc	Microsoft Windows RPC
	49156	tcp	open	msrpc	Microsoft Windows RPC
	49159	tcp	open	msrpc	Microsoft Windows RPC
	49160	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.112	443	tcp	open	http	lighttpd 1.4.13
	30000	tcp	open	unknown	
192.xxx.xxx.111	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	netbios-ssn	
	5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd
	5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
	10000	tcp	filtered	snet-sensor-mgmt	
	10001	tcp	filtered	scp-config	
	10002	tcp	filtered	documentum	
	10003	tcp	filtered	documentum_s	
	10004	tcp	filtered	emcrmirccd	
	10009	tcp	filtered	swdtp-sv	
	10010	tcp	filtered	rxapi	
	10012	tcp	filtered	unknown	
	10024	tcp	filtered	unknown	
	49152	tcp	open	msrpc	Microsoft Windows RPC
	49153	tcp	open	msrpc	Microsoft Windows RPC
	49154	tcp	open	msrpc	Microsoft Windows RPC
	49155	tcp	open	msrpc	Microsoft Windows RPC
	49156	tcp	open	msrpc	Microsoft Windows RPC
	49157	tcp	open	msrpc	Microsoft Windows RPC
	49158	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.105	88	tcp	open	kerberos-sec	Heimdal Kerberos (server time: 2014-09-10 15:00:46Z)
	445	tcp	open	microsoft-ds	
	548	tcp	open	afp	Apple AFP (name: iMac de framirez; protocol 3.4; Mac
192.xxx.xxx.100	22	tcp	open	ssh	
	80	tcp	open	tcpwrapped	
192.xxx.xxx.95	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
	5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3
	5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)

192.xxx.xxx.94		88	tcp	open	kerberos-sec	Heimdal Kerberos (server time: 2014-09-10 15:00:59Z)
		445	tcp	open	microsoft-ds	
		548	tcp	open	afp	Apple AFP (name: CGSDARWIN; protocol 3.4; Mac OS
		631	tcp	open	ipp	CUPS 1.5
		1947	tcp	open	sentinelsrm	
192.xxx.xxx.93		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
		1110	tcp	open	tcpwrapped	
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
		49152	tcp	open	msrpc	Microsoft Windows RPC
		49153	tcp	open	msrpc	Microsoft Windows RPC
		49154	tcp	open	msrpc	Microsoft Windows RPC
		49155	tcp	open	msrpc	Microsoft Windows RPC
		49157	tcp	open	msrpc	Microsoft Windows RPC
		49160	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.92		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
		1110	tcp	filtered	nfsd-status	
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd I
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
		49152	tcp	open	msrpc	Microsoft Windows RPC
		49153	tcp	open	msrpc	Microsoft Windows RPC
		49154	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.89		21	tcp	open	ftp	HP FTP Print Server 3.0 (HP LaserJet 4250 printer)
		23	tcp	open	telnet	HP JetDirect telnetd
		80	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
		280	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
		443	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
		515	tcp	open	printer	
		631	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
		9100	tcp	open	jetdirect	
		14000	tcp	open	tcpwrapped	
192.xxx.xxx.88		5060	tcp	open	sip	(SIP end point; Status: 200 OK)
192.xxx.xxx.86		22	tcp	open	ssh	Dropbear sshd 2013.59 (protocol 2.0)
192.xxx.xxx.85		22	tcp	open	ssh	OpenSSH 5.6 (protocol 2.0)
		80	tcp	open	http	Apache httpd 2.2.22 ((Fedora))
		111	tcp	open	rpcbind	2-4 (RPC #100000)
		139	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: MYGROUP)
		445	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: MYGROUP)
		902	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC,
		5900	tcp	open	vnc	VNC (protocol 3.7)
		9220	tcp	open	unknown	

192.xxx.xxx.84	🟢	135	tcp	open	msrpc	Microsoft Windows RPC
	🟢	139	tcp	open	netbios-ssn	
	🟢	445	tcp	open	netbios-ssn	
	🔴	1110	tcp	filtered	nfsd-status	
	🟢	2869	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
	🟢	5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r
	🟢	5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
	🟢	49152	tcp	open	msrpc	Microsoft Windows RPC
	🟢	49153	tcp	open	msrpc	Microsoft Windows RPC
	🟢	49154	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.81	🟢	135	tcp	open	msrpc	Microsoft Windows RPC
	🟢	139	tcp	open	netbios-ssn	
	🟢	445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
	🟢	1110	tcp	open	tcpwrapped	
192.xxx.xxx.80	🟢	135	tcp	open	msrpc	Microsoft Windows RPC
	🟢	139	tcp	open	netbios-ssn	
	🟢	445	tcp	open	netbios-ssn	
	🔴	1110	tcp	filtered	nfsd-status	
	🟢	5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd
	🟢	5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
	🟢	49152	tcp	open	msrpc	Microsoft Windows RPC
	🟢	49153	tcp	open	msrpc	Microsoft Windows RPC
	🟢	49154	tcp	open	msrpc	Microsoft Windows RPC
	🟢	49156	tcp	open	msrpc	Microsoft Windows RPC
	🟢	49157	tcp	open	msrpc	Microsoft Windows RPC
	🟢	49158	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.79	🟢	80	tcp	open	http	Epson printer httpd 1.0
	🟢	515	tcp	open	printer	
	🟢	9100	tcp	open	jetdirect	
192.xxx.xxx.78	🟢	135	tcp	open	msrpc	Microsoft Windows RPC
	🟢	139	tcp	open	netbios-ssn	
	🟢	445	tcp	open	netbios-ssn	
	🟢	1947	tcp	open	sentinelsrm	
192.xxx.xxx.77	🟢	80	tcp	open	http	Microsoft IIS httpd 7.5
	🟢	135	tcp	open	msrpc	Microsoft Windows RPC
	🟢	139	tcp	open	netbios-ssn	
	🟢	445	tcp	open	netbios-ssn	
	🔴	1110	tcp	filtered	nfsd-status	
	🔴	1761	tcp	filtered	landesk-rc	
	🟢	5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
	🟢	5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
	🟢	5900	tcp	open	vnc	VNC (protocol 3.3; Locked out)
	🟢	49152	tcp	open	msrpc	Microsoft Windows RPC
	🟢	49153	tcp	open	msrpc	Microsoft Windows RPC
	🟢	49154	tcp	open	msrpc	Microsoft Windows RPC
	🟢	49167	tcp	open	msrpc	Microsoft Windows RPC
	🔴	49400	tcp	filtered	compaqdiag	

192.xxx.xxx.76	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	netbios-ssn	
	1110	tcp	filtered	nfsd-status	
	5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
	5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
	49152	tcp	open	msrpc	Microsoft Windows RPC
	49153	tcp	open	msrpc	Microsoft Windows RPC
	49154	tcp	open	msrpc	Microsoft Windows RPC
	49156	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.75(cueasis.lns.com.ec)	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
192.xxx.xxx.74	88	tcp	open	kerberos-sec	Heimdal Kerberos (server time: 2014-09-10 1
	548	tcp	open	afp	Apple AFP (name: ImacP; protocol 3.4; Mac
	1947	tcp	open	sentinelsrm	
192.xxx.xxx.73(CUEALM.lns.com.ec)	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	netbios-ssn	
	5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
	49155	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.72	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	netbios-ssn	
192.xxx.xxx.71(SEP001BD4609C8D.lns.com.ec)	80	tcp	open	http	
	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	443	tcp	open	skype2	Skype
	445	tcp	open	netbios-ssn	
	2869	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
	5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
	49152	tcp	open	msrpc	Microsoft Windows RPC
	49153	tcp	open	msrpc	Microsoft Windows RPC
	49154	tcp	open	msrpc	Microsoft Windows RPC
	49155	tcp	open	msrpc	Microsoft Windows RPC
	49157	tcp	open	msrpc	Microsoft Windows RPC
	49158	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.70	21	tcp	open	ftp	HP JetDirect ftpd
	23	tcp	open	telnet	HP JetDirect printer telnetd (No password)
	80	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	280	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	443	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	515	tcp	open	printer	
	631	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	7627	tcp	open	http	HP-ChaiSOE 1.0 (HP LaserJet http config)
	9100	tcp	open	jetdirect	
	14000	tcp	open	tcpwrapped	
192.xxx.xxx.69	135	tcp	open	msrpc	Microsoft Windows RPC

192.xxx.xxx.68		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
		5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
		49152	tcp	open	msrpc	Microsoft Windows RPC
		49153	tcp	open	msrpc	Microsoft Windows RPC
		49154	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.67(SEP001C58576AA3.lns.com.ec)		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
		1110	tcp	filtered	nfsd-status	
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
		49152	tcp	open	msrpc	Microsoft Windows RPC
		49153	tcp	open	msrpc	Microsoft Windows RPC
		49154	tcp	open	msrpc	Microsoft Windows RPC
		49157	tcp	open	msrpc	Microsoft Windows RPC
		49160	tcp	open	msrpc	Microsoft Windows RPC
		49161	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.66		88	tcp	open	kerberos-sec	Heimdal Kerberos
		445	tcp	open	microsoft-ds	
		548	tcp	open	afp	Apple AFP (name:
		1947	tcp	open	sentinelsrm	
192.xxx.xxx.65(SEP0026CBBDEA63.lns.com.ec)		135	tcp	filtered	msrpc	
		139	tcp	filtered	netbios-ssn	
		445	tcp	filtered	microsoft-ds	
		1110	tcp	filtered	nfsd-status	
		2869	tcp	filtered	icslap	
		3389	tcp	filtered	ms-wbt-server	
		19780	tcp	filtered	unknown	
		49152	tcp	open	msrpc	Microsoft Windows RPC
		49153	tcp	open	msrpc	Microsoft Windows RPC
		49154	tcp	open	msrpc	Microsoft Windows RPC
		49155	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.63		21	tcp	open	ftp	tnftpd 20061217
		80	tcp	open	http	Apache httpd 1.3.41 ((Darwin) PHP/4.4.9)
		139	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
		445	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
		548	tcp	open	afp	Apple AFP (name: PREPRENSA01; protocol 3.2; I
		5800	tcp	open	vnc-http	
		5900	tcp	open	vnc	RealVNC Enterprise (protocol 4.1)
192.xxx.xxx.60		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd
		5900	tcp	open	vnc	VNC (protocol 3.3; Locked out)
192.xxx.xxx.59		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
		1110	tcp	filtered	nfsd-status	

192.xxx.xxx.58		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
192.xxx.xxx.56		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
		808	tcp	open	tcpwrapped	
		1521	tcp	open	oracle-tns	Oracle TNS Listener
		1688	tcp	open	msrpc	Microsoft Windows RPC
		3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
		5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
		8080	tcp	open	http	Oracle XML DB Enterprise Edition httpd
		49152	tcp	open	msrpc	Microsoft Windows RPC
		49153	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.55		88	tcp	open	kerberos-sec	Heimdal Kerberos (server time: 2014-09-10 14:54:39Z)
		445	tcp	open	microsoft-ds	
		548	tcp	open	afp	Apple AFP (name: CGSMosCositeM; protocol 3.4; Mac
		1947	tcp	open	sentinelsrm	
192.xxx.xxx.54		548	tcp	open	afp	Apple AFP (name: Ordenador de CGS CGS;
		5800	tcp	open	vnc-http	RealVNC E4
		5900	tcp	open	vnc	RealVNC Enterprise (protocol 4.1)
192.xxx.xxx.53		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	netbios-ssn	
192.xxx.xxx.52		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
		1110	tcp	filtered	nfsd-status	
		3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
		4899	tcp	open	tcpwrapped	
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)
192.xxx.xxx.50		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	
		445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
		1110	tcp	open	tcpwrapped	
		5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
		5900	tcp	open	vnc	RealVNC Personal (protocol 4.0)

192.xxx.xxx.46	🟢	21	tcp	open	ftp	tnftpd 20080929
	🟢	88	tcp	open	kerberos-sec	Mac OS X kerberos-sec
	🟢	139	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
	🟢	445	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
	🟢	548	tcp	open	afp	Apple AFP (name: CGSEDUARDO; protocol 3.3;
	🟢	1947	tcp	open	sentinelsrm	
192.xxx.xxx.45	🟢	135	tcp	open	msrpc	Microsoft Windows RPC
	🟢	139	tcp	open	netbios-ssn	
	🟢	445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
	🟢	5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
	🟢	5900	tcp	open	vnc	VNC (protocol 3.3; Locked out)
192.xxx.xxx.41	🟢	5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd E4.4.3 r16583
	🟢	5900	tcp	open	vnc	VNC (protocol 3.3; Locked out)
192.xxx.xxx.39	🟢	135	tcp	open	msrpc	Microsoft Windows RPC
	🟢	139	tcp	open	netbios-ssn	
	🟢	445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
	🟢	1025	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.34(sts02.lns.com.ec)	🟢	135	tcp	open	msrpc	Microsoft Windows RPC
	🟢	139	tcp	open	netbios-ssn	
	🟢	445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
	🟢	1025	tcp	open	msrpc	Microsoft Windows RPC
	🟢	1047	tcp	open	msrpc	Microsoft Windows RPC
	🟢	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
192.xxx.xxx.33	🟢	135	tcp	open	msrpc	Microsoft Windows RPC
	🟢	139	tcp	open	netbios-ssn	
	🟢	445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
	🟢	1025	tcp	open	msrpc	Microsoft Windows RPC
	🟢	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
	🟢	14000	tcp	open	soap	gSOAP soap 2.7
192.xxx.xxx.32	🟢	80	tcp	open	http	VMware ESXi Server httpd
	🟢	427	tcp	open	svrloc	
	🟢	443	tcp	open	http	VMware ESXi Server httpd
	🟢	902	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
	🟢	5989	tcp	open	tcpwrapped	
	🟢	8000	tcp	open	http-alt	
	🟢	8100	tcp	open	tcpwrapped	
192.xxx.xxx.31	🔴	22	tcp	closed	ssh	
	🟢	80	tcp	open	http	VMware ESXi Server httpd
	🔴	427	tcp	closed	svrloc	
	🟢	443	tcp	open	http	VMware ESXi Server httpd
	🟢	902	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
	🔴	5988	tcp	closed	wbem-http	
	🟢	5989	tcp	open	tcpwrapped	
	🟢	8000	tcp	open	http-alt	
	🔴	8080	tcp	closed	http-proxy	
	🟢	8100	tcp	open	tcpwrapped	
	🔴	8300	tcp	closed	tmi	

192.xxx.xxx.30(sin00.xxx.xxx)	🔴	22	tcp	closed	ssh	
	🟢	80	tcp	open	http	VMware ESXi Server httpd
	🟢	427	tcp	open	svrloc	
	🟢	443	tcp	open	http	VMware ESXi Server httpd
	🟢	902	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
	🔴	5988	tcp	closed	wbem-http	
	🟢	5989	tcp	open	tcpwrapped	
	🟢	8000	tcp	open	http-alt	
	🟢	8100	tcp	open	tcpwrapped	
	🔴	8300	tcp	closed	tmi	
192.xxx.xxx.28(sts03.lns.com.ec)	🟢	135	tcp	open	msrpc	Microsoft Windows RPC
	🟢	139	tcp	open	netbios-ssn	
	🟢	445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
	🟢	1038	tcp	open	msrpc	Microsoft Windows RPC
	🟢	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
192.xxx.xxx.27	🟢	80	tcp	open	http	VMware ESXi Server httpd
	🟢	427	tcp	open	svrloc	
	🟢	443	tcp	open	http	VMware ESXi Server httpd
	🟢	902	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
	🔴	5988	tcp	closed	wbem-http	
	🟢	5989	tcp	open	tcpwrapped	
	🟢	8000	tcp	open	http-alt	
	🟢	8100	tcp	open	tcpwrapped	
192.xxx.xxx.26	🟢	13	tcp	open	daytime	
	🟢	21	tcp	open	ftp	HP-UX or AIX ftpd 4.2
	🟢	22	tcp	open	ssh	OpenSSH 5.8 (protocol 2.0)
	🟢	23	tcp	open	telnet	AIX telnetd
	🟢	25	tcp	open	smtp	Sendmail AIX6.1/8.14.4
	🟢	37	tcp	open	time	(32 bits)

	111	tcp	open	rpcbind	2-4 (RPC #100000)
	199	tcp	open	smux	
	427	tcp	open	svrloc	
	512	tcp	open	exec	AIX rexecd
	513	tcp	open	login	
	514	tcp	open	tcpwrapped	
	587	tcp	open	smtp	Sendmail AIX6.1/8.14.4
	1334	tcp	open	writesrv	
	1521	tcp	open	oracle-tns	Oracle TNS Listener
	2049	tcp	open	nfs	2-4 (RPC #100003)
	5500	tcp	open	http	Oracle Application Server 10g httpd 10.1.3.4.0 (
	5988	tcp	open	http	Web-Based Enterprise Management CIM serve
	5989	tcp	open	http	Web-Based Enterprise Management CIM serve
	6112	tcp	open	dtspc	
	8181	tcp	open	http	Oracle XML DB Enterprise Edition httpd
	9090	tcp	open	websm	AIX wsmserver
	32768	tcp	open	filenet-tms	
	32769	tcp	open	filenet-rpc	
	32770	tcp	open	nlockmgr	1-4 (RPC #100021)
	32771	tcp	open	status	1 (RPC #100024)
	32772	tcp	open	ttdbserverd	1 (RPC #100083)
	32777	tcp	open	sometimes-rpc17	
	32779	tcp	open	sometimes-rpc21	
	32782	tcp	open	unknown	
192.xxx.xxx.25(emp .lns.com.ec)	21	tcp	open	ftp	vsftpd (before 2.0.8) or WU-FTPD
	22	tcp	open	ssh	OpenSSH 3.6.1p2 (protocol 1.99)
	80	tcp	open	http	Apache httpd 2.2.14 ((Unix) DAV/2
	111	tcp	open	rpcbind	2 (RPC #100000)
	443	tcp	open	http	Apache httpd 2.2.14 ((Unix) DAV/2
	3306	tcp	open	mysql	MySQL 5.1.41
	8080	tcp	open	http-proxy	Squid http proxy 2.5.STABLE5
	32769	tcp	open	status	1 (RPC #100024)
192.xxx.xxx.24 192.xxx.xxx.23	23	tcp	open	telnet	VxWorks telnetd
192.xxx.xxx.22 192.xxx.xxx.21	23	tcp	open	telnet	
	80	tcp	open	http	
	646	tcp	open	tcpwrapped	
192.xxx.xxx.20	22	tcp	open	ssh	OpenSSH 5.1 (protocol 2.0)
	23	tcp	open	telnet	IBM BladeCenter Advanced
	80	tcp	open	http	
	427	tcp	open	tcpwrapped	
	1022	tcp	filtered	exp2	
	1023	tcp	filtered	netvenuechat	
	1080	tcp	filtered	socks	
	1443	tcp	filtered	ies-lm	
192.xxx.xxx.16(man sis.xxx.xxx)	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
	1045	tcp	open	msrpc	Microsoft Windows RPC
	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service

192.xxx.xxx.12	8080	tcp	open	http	Apache httpd
192.xxx.xxx.11(clr00.xxx.xxx)	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
	1025	tcp	open	msrpc	Microsoft Windows RPC
	1070	tcp	open	flexlm	FlexLM license manager
	27000	tcp	open	flexlm	FlexLM license manager
	50006	tcp	open	soap	gSOAP soap 2.6
192.xxx.xxx.10(dns1.xxx.xxx)	22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
	53	tcp	open	domain	
	111	tcp	open	rpcbind	2 (RPC #100000)
192.xxx.xxx.9	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	netbios-ssn	
	1110	tcp	filtered	nfsd-status	
	5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd
	5900	tcp	open	vnc	VNC (protocol 3.3; Locked out)
	49152	tcp	open	msrpc	Microsoft Windows RPC
	49153	tcp	open	msrpc	Microsoft Windows RPC
	49154	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.8	13	tcp	open	daytime	
	21	tcp	open	ftp	HP-UX or AIX ftpd 4.2
	22	tcp	open	ssh	OpenSSH 6.0 (protocol 2.0)
	23	tcp	open	telnet	AIX telnetd
	25	tcp	open	smtp	Sendmail AIX6.1/8.14.4
	37	tcp	open	time	
	111	tcp	open	rpcbind	2-4 (RPC #100000)
	199	tcp	open	smux	
	427	tcp	open	svrloc	
	512	tcp	open	exec	AIX rexecd
	513	tcp	open	login	
	514	tcp	open	tcpwrapped	
	1334	tcp	open	writesrv	
	1521	tcp	open	oracle-tns	Oracle TNS Listener
	2049	tcp	open	nfs	2-4 (RPC #100003)
	5988	tcp	open	http	Web-Based Enterprise Management CIM
	5989	tcp	open	http	Web-Based Enterprise Management CIM
	6000	tcp	open	X11	
	6112	tcp	open	dtspc	
	8181	tcp	open	http	Oracle XML DB Enterprise Edition httpd
	9090	tcp	open	websm	AIX wsmserver
	32768	tcp	open	filenet-tms	
	32769	tcp	open	filenet-rpc	
	32770	tcp	open	ttdbserverd	1 (RPC #100083)
	32772	tcp	open	status	1 (RPC #100024)
	32776	tcp	open	nlockmgr	1-4 (RPC #100021)
	32781	tcp	open	unknown	

192.xxx.xxx.7	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
	1030	tcp	open	msrpc	Microsoft Windows RPC
	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
	5988	tcp	open	wbem-http	
	5989	tcp	open	wbem-https	
192.xxx.xxx.6	22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
	80	tcp	open	http	Apache httpd 2.2.3 ((CentOS))
192.xxx.xxx.5	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
	1042	tcp	open	msrpc	Microsoft Windows RPC
	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
192.xxx.xxx.4	80	tcp	open	http	Microsoft IIS httpd 7.5
	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	443	tcp	open	http	Microsoft IIS httpd 7.5
	445	tcp	open	netbios-ssn	
	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
	49154	tcp	open	msrpc	Microsoft Windows RPC
	49156	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.3	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	netbios-ssn	
	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
	49154	tcp	open	msrpc	Microsoft Windows RPC
192.xxx.xxx.2	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	
	445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
	1029	tcp	open	msrpc	Microsoft Windows RPC
	3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
192.xxx.xxx.215 192.xxx.xxx.124 192.xxx.xxx.107 192.xxx.xxx.102 192.xxx.xxx.xxx 192.xxx.xxx.91 192.xxx.xxx.90 192.xxx.xxx.42 192.xxx.xxx.15	En estos host no se encontraron puertos abiertos.				

Anexo 4 Vulnerabilidades en equipos Cisco

Información	Puerto	Vulnerabilidad	Riesgo	Solución
IP: 192.xxx.xxx.100 **MAC**:18 7 **OS**: CISCO IP Telephone	TCP/80	El servidor web remoto se ve afectado por una vulnerabilidad de cross-site scripting.	MEDIO	Actualizar a RomPager 4.51 o posterior.
IP: 192.xxx.xxx.247 **MAC:**0 c0 **OS:** CISCO	TCP/0	El host remoto ha habilitado el reenvío de IP.	BAJO	En Linux, se puede desactivar el reenvío IP haciendo: echo 0> / proc / sys / net / ipv4 / ip_forward En Windows, establezca la clave 'IPEnableRouter' a 0 bajo HKEY_LOCAL_ MACHINE \ System \ CurrentControlSet \ Services \ Tcpip \ Parámetros En Mac OS X, puede desactivar el reenvío IP el comando: sysctl -w net.inet.ip.forwarding = 0 Para otros sistemas, consulte con su proveedor.
	TCP/23	El servidor Telnet remoto transmite tráfico sin cifrar.	BAJO	Deshabilitar este servicio y utilizar SSH en lugar.
IP: 192.xxx.xxx.248 **MAC**:0 :0 **OS:** CISCO	TCP/23	El servidor Telnet remoto transmite tráfico sin cifrar.	BAJO	Deshabilitar este servicio y utilizar SSH en lugar.
IP: 192.xxx.xxx.249 **MAC**:(:c0 **OS:** CISCO	TCP/23	El servidor Telnet remoto transmite tráfico sin cifrar.	BAJO	Deshabilitar este servicio y utilizar SSH en lugar.

Anexo 5 Vulnerabilidades en Servidores Linux

Información	Puerto	Vulnerabilidad	Riesgo	Solución
IP:192.xxx.xxx.6 MAC:0 a1 OS: Linux Kernel 2.6.18-274.3.1.el5 (i386)	TCP/80	Funciones de test están habilitados en el servidor web remoto.	MEDIO	Deshabilitar estos métodos. Consulte la salida de extensión para más información.
	TCP/80	El servidor web que se ejecuta en el host remoto tiene una vulnerabilidad de divulgación de información.	MEDIO	Actualiza a la versión 2.0.65 de Apache / 2.2.22 o posterior.
	UDP/123	El servicio de hora de red remoto podría ser utilizado para el reconocimiento de la red o abusado en un ataque de denegación de servicio.	MEDIO	Si utiliza NTP del Proyecto Network Time Protocol, actualizar a 4.2.7 NTP-p26 o posterior, o añadir 'monitor de desactivar "al" ntp.conf' archivo de configuración y reiniciar el servicio. De lo contrario, póngase en contacto con el vendedor. De lo contrario, limitar el acceso al servicio afectado hosts de confianza.
	TCP/22	SSH está configurado para permitir MD5 y algoritmos MAC de 96 bits.	BAJO	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar MD5 y algoritmos MAC de 96 bits
	TCP/22	El servidor SSH está configurado para utilizar Cipher Block Chaining.	BAJO	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar el cifrado de modo de cifrado CBC, y permitir CTR o cifrado de modo de cifrado GCM.
IP:192.xxx.xxx.10 MAC:0(4: 68 DNS:dns1.lns.com.ec OS:Linux Kernel 2.6, Palo Alto Networks PAN-OS	TCP/53	El servidor de nombres remoto permite transferencias de zona	MEDIO	Limite las transferencias de zona DNS sólo a los servidores que necesitan la información.
	TCP/53	El servidor DNS remoto es vulnerable a ataques Snooping caché.	MEDIO	Póngase en contacto con el proveedor del software DNS para una solución.

	TCP/22	El servidor SSH está configurado para utilizar Cipher Block Chaining.	BAJO	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar el cifrado de modo de cifrado CBC, y permitir CTR o cifrado de modo de cifrado GCM.
	TCP/22	SSH está configurado para permitir MD5 y algoritmos MAC de 96 bits	BAJO	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar MD5 y algoritmos MAC de 96 bits.
IP:192.xxx.xxx.20 MAC:ᵋ ᵇ: 10 OS:Linux Kernel 2.6.27.19-158 (ppc)	UDP/161	El nombre de comunidad SNMP del servidor remoto se puede adivinar.	ALTO	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza. Cualquiera de filtrar los paquetes UDP entrantes van a este puerto, o cambiar la cadena de comunidad predeterminado.
	UDP/161	El demonio SNMP remoto se ve afectado por una vulnerabilidad que permite a un ataque distribuido de denegación de servicio ataque reflejado.	MEDIO	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza. De lo contrario, restringir y controlar el acceso a este servicio, y considerar cambiar el valor por defecto cadena de comunidad "público".
	UDP/123	El servicio de hora de red remoto podría ser utilizado para el reconocimiento de la red o abusado en un ataque de denegación de servicio.	MEDIO	Si utiliza NTP del Proyecto Network Time Protocol, o actualizar a 4.2.7 NTP-p26 o posterior, o añadir 'monitor de desactivar "al" ntp.conf' archivo de configuración y reiniciar el servicio. De lo contrario, póngase en contacto con el vendedor. De lo contrario, limitar el acceso al servicio afectado hosts de confianza.
	TCP/80	El servidor web que se ejecuta en el host remoto tiene una	MEDIO	Actualiza a la versión 2.0.65 de Apache / 2.2.22 o posterior.

		vulnerabilidad de divulgación de información.		
	TCP/0	El host remoto ha habilitado el reenvío de IP.	BAJO	En Linux, se puede desactivar el reenvío IP haciendo: echo 0> / proc / sys / net / ipv4 / ip_forward En Windows, establezca la clave 'IPEnableRouter' a 0 bajoHKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Tcpip \ Parámetros En Mac OS X, puede desactivar el reenvío IP ejecutando el comando: sysctl -w net.inet.ip.forwarding = 0 Para otros sistemas, consulte con su proveedor.
	TCP/22	El servidor SSH está configurado para utilizar Cipher Block Chaining.	BAJO	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar el cifrado de modo de cifrado CBC, y permitir CTR o cifrado de modo de cifrado GCM.
	TCP/22	SSH está configurado para permitir MD5 y algoritmos MAC de 96 bits.	BAJO	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar MD5 y algoritmos MAC de 96 bits.
	TCP/23	El servidor Telnet remoto transmite tráfico sin cifrar.	BAJO	Deshabilitar este servicio y utilizar SSH en lugar.
	TCP/2023	El servidor Telnet remoto transmite tráfico sin cifrar.	BAJO	Deshabilitar este servicio y utilizar SSH en lugar.
IP:192.xxx.xxx.25 MAC:(ce:ce DNS:emp.lns.com.ec OS:Linux Kernel 2.6	TCP/80	El host remoto contiene una versión sin soporte de un lenguaje de programación de aplicaciones web.	ALTO	Actualizar a una versión de PHP que se soporta actualmente.
	TCP/443	El host remoto contiene una versión sin soporte de un lenguaje de	ALTO	Actualizar a una versión de PHP que se soporta actualmente.

		programación de aplicaciones web.		
	TCP/22	El servicio remoto ofrece un protocolo criptográfico inseguro.	MEDIO	El demonio SSH remoto admite conexiones realizadas utilizando la versión 1.33 y / o 1.5 del protocolo SSH. Estos protocolos no son completamente criptográficamente seguro para que no se deben utilizar.
	TCP/80	Funciones de test están habilitados en el servidor web remoto.	MEDIO	Deshabilitar estos métodos. Consulte la salida de extensión para más información.
	TCP/80	El servidor web remoto contiene un script CGI que revela información.	MEDIO	Retire printenv desde / cgi-bin.
	TCP/443	Certificado SSL del servidor remoto ya ha expirado.	MEDIO	Compra o generar un nuevo certificado SSL para reemplazar el existente.
	TCP/443	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	Un certificado SSL en la cadena de certificados se ha firmado utilizando un algoritmo de hash débil.	MEDIO	Póngase en contacto con la entidad emisora de certificados de haber certificado reeditado.
	TCP/443	Funciones de test están habilitados en el servidor web remoto.	MEDIO	Deshabilitar estos métodos. Consulte la salida de extensión para más información.
	TCP/443	El servicio remoto es compatible con el uso de la fuerza media cifrado SSL.	MEDIO	Vuelva a configurar la aplicación afectada, si es posible evitar el uso de sistemas de cifrado de fuerza media.

	TCP/443	El servicio remoto cifra el tráfico utilizando un protocolo con debilidades conocidas.	MEDIO	Consulte la documentación de la aplicación que permite deshabilitar SSL 2.0 y utilizar SSL 3.0, TLS 1.0, o superior en su lugar.
	TCP/443	El servicio remoto es compatible con el uso de sistemas de cifrado SSL débiles.	MEDIO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados débiles.
	TCP/443	El servidor web remoto contiene un script CGI que revela información.	MEDIO	Retire printenv desde / cgi-bin.
	TCP/22	El servidor SSH está configurado para utilizar Cipher Block Chaining.	BAJO	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar el cifrado de modo de cifrado CBC, y permitir CTR o cifrado de modo de cifrado GCM
	TCP/22	SSH está configurado para permitir MD5 y algoritmos MAC de 96 bits.	BAJO	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar MD5 y algoritmos MAC de 96 bits.
	TCP/443	El servicio remoto es compatible con el uso del sistema de cifrado RC4.	BAJO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de algoritmos de cifrado RC4. Considere el uso de TLS 1.2 con suites AES-GCM sujetas a navegador y soporte de servidor web.
IP:192.xxx.xxx.85 MAC:0 d6:18 OS:Linux Kernel 2.6 en Fedora liberación 15, Linux Kernel 3.0 en Fedora liberar 16, Linux Kernel 3.3 en Fedora liberar 17	TCP/0	El host remoto ejecuta un sistema operativo obsoleto.	CRITICO	Actualizar a una versión más reciente.
	TCP/80	Funciones de test están habilitados en el servidor web remoto.	MEDIO	Deshabilitar estos métodos. Consulte la salida de extensión para más información.

	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
	TCP/22	El servidor SSH está configurado para utilizar Cipher Block Chaining.	BAJO	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar el cifrado de modo de cifrado CBC, y permitir CTR o cifrado de modo de cifrado GCM.
	TCP/22	SSH está configurado para permitir MD5 y algoritmos MAC de 96 bits.	BAJO	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar MD5 y algoritmos MAC de 96 bits.
IP:192.xxx.xxx.112 MAC:5(.: b4 OS:Impresora KYOCERA, Linux Kernel 2.6	TCP/443	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	MEDIO	Desactivar SSLv3. Servicios que deben soportar SSLv3 debe activar el mecanismo de TLS repliegue SCSV hasta SSLv3 se puede desactivar.
	TCP/443	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	Un certificado SSL en la cadena de certificados se ha firmado utilizando un algoritmo de hash débil.	MEDIO	Póngase en contacto con la entidad emisora de certificados de haber certificado reeditado.

	TCP/443	El servicio remoto es compatible con el uso de la fuerza media cifrado SSL.	MEDIO	Vuelva a configurar la aplicación afectada, si es posible evitar el uso de sistemas de cifrado de fuerza media.
	TCP/443	El servicio remoto cifra el tráfico utilizando un protocolo con debilidades conocidas.	MEDIO	Consulte la documentación de la aplicación que permite deshabilitar SSL 2.0 y utilizar SSL 3.0, TLS 1.0, o superior en su lugar.
	TCP/443	El servicio remoto es compatible con el uso de sistemas de cifrado SSL débiles.	MEDIO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados débiles.
	TCP/443	El servicio remoto es compatible con el uso del sistema de cifrado RC4.	BAJO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de algoritmos de cifrado RC4. Considere el uso de TLS 1.2 con suites AES-GCM sujetas a navegador y soporte de servidor web.
IP:192.xxx.xxx.214 MAC:0[illegible]3: a2:27 OS:Linux Kernel 2.6.12	UDP/161	Los nombres de comunidad del servidor SNMP remoto se pueden adivinar.	ALTO	Deshabilitar el servicio SNMP en el host remoto si no lo usas, filtrar paquetes UDP entrantes van a este puerto, o cambiar la cadena de comunidad predeterminado.
	UDP/161	El nombre de comunidad SNMP del servidor remoto se puede adivinar.	ALTO	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza. Cualquiera de filtrar los paquetes UDP entrantes van a este puerto, o cambiar la cadena de comunidad predeterminado.

	UDP/161	El demonio SNMP remoto se ve afectado por una vulnerabilidad que permite a un ataque distribuido de denegación de servicio ataque reflejado.	MEDIO	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza. De lo contrario, restringir y controlar el acceso a este servicio, y considerar cambiar el valor por defecto cadena de comunidad "público".
	TCP/443	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	MEDIO	Desactivar SSLv3. Servicios que deben soportar SSLv3 debe activar el mecanismo de TLS repliegue SCSV hasta SSLv3 se puede desactivar.
	TCP/443	El servicio remoto permite renegociación insegura de conexiones TLS / SSL.	MEDIO	Póngase en contacto con el proveedor para obtener información específica parche.
	TCP/443	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	El servicio remoto es compatible con el uso de la fuerza media cifrado SSL	MEDIO	Vuelva a configurar la aplicación afectada, si es posible evitar el uso de sistemas de cifrado de fuerza media
	TCP/443	El servicio remoto cifra el tráfico utilizando un protocolo con debilidades conocidas.	MEDIO	Consulte la documentación de la aplicación que permite deshabilitar SSL 2.0 y utilizar SSL 3.0, TLS 1.0, o superior en su lugar.
	TCP/443	El servicio remoto es compatible con el uso de sistemas de cifrado SSL débiles.	MEDIO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados débiles.

	TCP/443	La cadena de certificados X.509 utilizado por este servicio contiene certificados con claves RSA de menos de 2.048 bits.	BAJO	Vuelva a colocar el certificado de la cadena con la clave RSA menos de 2048 bits de longitud con una clave más larga, y vuelva a emitir los certificados firmados por el antiguo certificado.
	TCP/443	El servicio remoto es compatible con el uso del sistema de cifrado RC4.	BAJO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de algoritmos de cifrado RC4. Considere el uso de TLS 1.2 con suites AES-GCM sujetas a navegador y soporte de servidor web.

Anexo 6 Vulnerabilidades en Impresoras

Información	Puerto	Vulnerabilidad	Riesgo	Solución
IP:192.xxx.xxx.181 MAC:0 3a OS:HP Guardian Service Processor, HP JetDirect Printer	TCP/0	El host remoto ha habilitado el reenvío de IP.	BAJO	En Linux, se puede desactivar el reenvío IP haciendo: echo 0> / proc / sys / net / ipv4 / ip_forward En Windows, establezca la clave 'IPEnableRouter' a 0 bajo HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Tcpip \ Parámetros En Mac OS X, puede desactivar el reenvío IP ejecutando el comando: sysctl -w net.inet.ip.forwarding = 0 Para otros sistemas, consulte con su proveedor.
IP:192.xxx.xxx.112 MAC:5c 1 OS:Impresora KYOCERA, Linux Kernel 2.6	TCP/443	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	MEDIO	Desactivar SSLv3. Servicios que deben soportar SSLv3 debe activar el mecanismo de TLS repliegue SCSV hasta SSLv3 se puede desactivar.
	TCP/443	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	Un certificado SSL en la cadena de certificados se ha firmado utilizando un algoritmo de hash débil.	MEDIO	Póngase en contacto con la entidad emisora de certificados de haber certificado reeditado.
	TCP/443	El servicio remoto es compatible con el uso de la fuerza media cifrado SSL.	MEDIO	Vuelva a configurar la aplicación afectada, si es posible evitar el uso de sistemas de cifrado de fuerza media.

	TCP/443	El servicio remoto cifra el tráfico utilizando un protocolo con debilidades conocidas.	MEDIO	Consulte la documentación de la aplicación que permite deshabilitar SSL 2.0 y utilizar SSL 3.0, TLS 1.0, o superior en su lugar.
	TCP/443	El servicio remoto es compatible con el uso de sistemas de cifrado SSL débiles.	MEDIO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados débiles.
	TCP/443	El servicio remoto es compatible con el uso del sistema de cifrado RC4.	BAJO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de algoritmos de cifrado RC4. Considere el uso de TLS 1.2 con suites AES-GCM sujetas a navegador y soporte de servidor web.

Anexo 7 Vulnerabilidades en Servidores Windows

Información	Puerto	Vulnerabilidad	Riesgo	Solución
IP:192.xxx.xxx.11 MAC00 c DNS/NetBios:clr00.xxx.xxx/CLR00 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible iniciar sesión en el host remoto de Windows con una sesión nula.	MEDIO	Aplicar los siguientes cambios en el registro por los avisos de Technet referencia: Ajuste: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ Lsa \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ RestrictNullSessAccess = 1 Retire NAVEGADOR de: - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ NullSessionPipes Reinicie una vez que los cambios en el registro están completas.
	TCP/445	Firma no necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
IP:192.xxx.xxx.16 MAC:0 2 DNS/NetBios:edb-sistema.lns.com.ec.xxx.xxx.192.in-addr.arpa / STS06 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Código arbitrario puede ser ejecutada en el host remoto debido a una falla en el servicio "Servidor"	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido

				con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.
	TCP/445	Es posible iniciar sesión en el host remoto de Windows con una sesión nula.	MEDIO	Aplicar los siguientes cambios en el registro por los avisos de Technet referencia: Ajuste: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ Lsa \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ RestrictNullSessAccess = 1 Retire NAVEGADOR de: - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ NullSessionPipes Reinicie una vez que los cambios en el registro están completas.
	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
IP:192.xxx.xxx.28 MAC:0 15 DNS/NetBios: SN /Mar01 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible iniciar sesión en el host remoto de Windows con una sesión nula.	MEDIO	Aplicar los siguientes cambios en el registro por los avisos de Technet referencia: Ajuste: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ Lsa \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ RestrictNullSessAccess = 1 Retire NAVEGADOR de: - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ NullSessionPipes Reinicie una vez que los cambios en el registro están completas.

	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
IP:192.xxx.xxx.30 MAC:4 ca DNS/Netbios:edbmail.lns .com.ec.xxx.xxx.192.inad dr.arpa OS:VMware ESXi	TCP/0	El VMware ESXi 5.1 host remoto se ve afectado por múltiples vulnerabilidades de seguridad.	ALTO	Aplicar ESXi510-201212xxx-SG.
	TCP/0	El VMware ESXi 5.1 host remoto se ve afectado por múltiples vulnerabilidades de seguridad.	MEDIO	Aplicar ESXi510-201304xxx-SG.
	TCP/0	El VMware ESXi 5.1 host remoto se ve afectada por la denegación de múltiples vulnerabilidades de servicio.	MEDIO	Aplicar ESXi510-201401xxx-SG.
	TCP/0	El VMware ESXi 5.1 host remoto se ve afectado por una vulnerabilidad de elevación de privilegios.	MEDIO	Aplicar ESXi510-201320101-SG.
	TCP/0	El VMware ESXi 5.1 host remoto se ve afectado por múltiples vulnerabilidades.	MEDIO	Aplique el parche ESXi510-201406401-SG para ESXi 5.1.
	TCP/0	El VMware ESXi 5.1 host remoto se ve afectada por vulnerabilidad de denegación de servicio.	MEDIO	Aplicar ESXi510-201307xxx-SG.

	TCP/443	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	MEDIO	Desactivar SSLv3. Servicios que deben soportar SSLv3 debe activar el mecanismo de TLS repliegue SCSV hasta SSLv3 se puede desactivar.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	El servicio remoto tiene una configuración que puede hacer que sea vulnerable al ataque CRIMEN.	MEDIO	Desactivar la compresión y / o el servicio SPDY.
IP:192.xxx.xxx.34 MAC:ł:3c DNS/NetBios:sts02.lns.com.ec / STS02 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Código arbitrario puede ser ejecutada en el host remoto debido a una falla en el servicio "Servidor"	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.
	TCP/445	Es posible iniciar sesión en el host remoto de Windows con una sesión nula.	MEDIO	Aplicar los siguientes cambios en el registro por los avisos de Technet referencia: Ajuste: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ Lsa \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ RestrictNullSessAccess = 1 Retire NAVEGADOR de: - HKLM \ SYSTEM \ CurrentControlSet \ Services \

				LanmanServer \ Parameters \ NullSessionPipes Reinicie una vez que los cambios en el registro están completas.
	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
IP:192.xxx.xxx.67 MAC:90 3 DNS/NetBios:SEP001C58576AA3.lns.com.ec/EDBRRHH-PC OS:Microsoft Windows 7 Professional	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
IP:192.xxx.xxx.75 MAC:00: DNS/NetBios:cueasis.lns.com.ec/PASANTERRHH OS:Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3	TCP/0	El sistema operativo remoto ya no es compatible.	CRITICO	Actualizar a una versión de Windows que se soporta actualmente.
	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.

	TCP/445	Es posible ejecutar código arbitrario en el host remoto de Windows debido a fallas en su implementación SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows XP, Vista, 2008, 7 y 2008 R2.
	TCP/445	Es posible ejecutar código arbitrario en el host remoto de Windows debido a fallas en su implementación SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows XP, Vista, 2008, 7 y 2008 R2.
	TCP/445	Código arbitrario puede ser ejecutado en el host remoto debido a una falla en el servicio "Servidor".	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Es posible acceder a un recurso compartido de red.	ALTO	Para restringir el acceso con Windows, abra el Explorador, haga un clic derecho sobre cada acción, vaya a la pestaña "compartir", y haga clic en 'Permisos'.
	TCP/445	Es posible iniciar sesión en el host remoto.	MEDIO	En la directiva de grupo cambie el valor de "acceso de red: compartir y modelo de seguridad para cuentas locales de 'Sólo invitado - usuarios locales autenticados como invitado' a 'Clásico - usuarios locales autenticados como ellos mismos'. Desactivar la cuenta de invitado en su caso. Si el demonio SAMBA está en ejecución, vuelva a comprobar la configuración de SAMBA en torno al acceso de usuarios invitados y el acceso para invitados desactivar su caso

	TCP/445	Es posible iniciar sesión en el host remoto de Windows con una sesión nula.	MEDIO	Aplicar los siguientes cambios en el registro por los avisos de Technet referencia: Ajuste: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ Lsa \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ RestrictNullSessAccess = 1 Retire NAVEGADOR de: - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ NullSessionPipes Reinicie una vez que los cambios en el registro están completas.
	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
IP:192.xxx.xxx.xxx MAC:0[redacted]80 DNS/NetBiosdad00.lns.com.ec/DAD00 OS:Microsoft Windows Server 2008 Enterprise Service Pack 1	UDP/53	El host remoto está ejecutando una versión sin soporte de servidor DNS de Microsoft.	CRITICO	Actualizar a una versión compatible de Microsoft Windows.
	TCP/445	Código arbitrario puede ser ejecutada en el host remoto a través del puerto SMB	CRITICO	Microsoft ha lanzado un parche para Windows Vista y Windows Server 2008.
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000

	UDP/53	El servidor DNS que se ejecuta en el host remoto es vulnerable a ataques de spoofing DNS.	MEDIO	Microsoft ha publicado parches para Windows 2000, 2003, y 2008 Server.
	TCP/3389	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/3389	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/3389	El certificado SSL para este servicio es para un host diferente.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/3389	El control remoto de Terminal Services no utiliza a nivel de red de autenticación.	MEDIO	Habilitar a nivel de red de autenticación (NLA) en el servidor RDP remoto.Esto se hace generalmente en la ficha 'Remote' de la configuración del 'sistema' en Windows.
	TCP/3389	El host remoto está utilizando la criptografía débil.	MEDIO	Cambie el nivel de cifrado RDP a uno de: 3. Alto 4. Compatible con FIPS
	TCP/3389	Puede ser posible obtener acceso al host remoto.	MEDIO	- Forzar el uso de SSL como una capa de transporte por este servicio si es compatible, y / o - Seleccione la opción 'Permitir sólo las conexiones desde equipos que ejecuten Escritorio remoto con Autenticación a nivel de red' ajuste si está disponible.
	TCP/3389	El host remoto no es compatible con FIPS-140.	BAJO	Cambie el nivel de cifrado RDP a: 4. Compatible con FIPS
	TCP/3389	El servicio remoto es compatible con el uso del sistema de cifrado RC4.	BAJO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de algoritmos de cifrado RC4. Considere el uso de TLS 1.2 con suites AES-GCM sujetas a navegador y soporte de servidor web.

Anexo 8 Vulnerabilidades en equipos varios

Información	Puerto	Vulnerabilidad	Riesgo	Solución
IP:192.xxx.xxx.12 MAC:00 5 e OS:Linksys Router - WRT120N	TCP/80 80	El servidor web remoto es propenso a ataques de cross-site scripting.	MEDIO	Póngase en contacto con el vendedor de un parche o actualización.
	TCP/80 80	El servidor web remoto es propenso a un ataque de inyección de galletas.	MEDIO	Póngase en contacto con el vendedor de un parche o actualización.
	TCP/0	El host remoto ha habilitado el reenvío de IP.	BAJO	En Linux, se puede desactivar el reenvío IP haciendo: echo 0> / proc / sys / net / ipv4 / ip_forward En Windows, establezca la clave 'IPEnableRouter' a 0 bajo HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Tcpip \ Parámetros En Mac OS X, puede desactivar el reenvío IP ejecutando el comando: sysctl -w net.inet.ip.forwarding = 0 Para otros sistemas, consulte con su proveedor.
IP:192.xxx.xxx.22 MAC:5 L0 OS:KYOCERA Impresora	UDP/16 1	El nombre de comunidad SNMP del servidor remoto se puede adivinar.	ALTO	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza. Cualquiera de filtrar los paquetes UDP entrantes van a este puerto, o cambiar la cadena de comunidad predeterminado.

	TCP/0	El host remoto ha habilitado el reenvío de IP.	BAJO	En Linux, se puede desactivar el reenvío IP haciendo: echo 0> / proc / sys / net / ipv4 / ip_forward En Windows, establezca la clave 'IPEnableRouter' a 0 bajo HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Tcpip \ Parámetros En Mac OS X, puede desactivar el reenvío IP ejecutando el comando: sysctl -w net.inet.ip.forwarding = 0 Para otros sistemas, consulte con su proveedor
	TCP/23	El servidor Telnet remoto transmite tráfico sin cifrar.	BAJO	Deshabilitar este servicio y utilizar SSH en lugar.
IP:192.xxx.xxx.23 MAC:00 :7 4 OS:VxWorks	TCP/0	El host remoto ha habilitado el reenvío de IP.	BAJO	En Linux, se puede desactivar el reenvío IP haciendo: echo 0> / proc / sys / net / ipv4 / ip_forward En Windows, establezca la clave 'IPEnableRouter' a 0 bajo HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Tcpip \ Parámetros En Mac OS X, puede desactivar el reenvío IP ejecutando el comando: sysctl -w net.inet.ip.forwarding = 0 Para otros sistemas, consulte con su proveedor.
	TCP/23	El servidor Telnet remoto transmite tráfico sin cifrar.	BAJO	Deshabilitar este servicio y utilizar SSH en lugar.
IP:192.xxx.xxx.24 MAC:0 7:0 e	TCP/0	El host remoto ha habilitado el reenvío de IP.	BAJO	En Linux, se puede desactivar el reenvío IP haciendo: echo 0> / proc / sys / net / ipv4 / ip_forward En Windows, establezca la clave 'IPEnableRouter' a 0 bajo HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Tcpip \ Parámetros En Mac OS X, puede desactivar el

				reenvío IP ejecutando el comando: sysctl -w net.inet.ip.forwarding = 0 Para otros sistemas, consulte con su proveedor.
	TCP/23	El servidor Telnet remoto transmite tráfico sin cifrar.	BAJO	Deshabilitar este servicio y utilizar SSH en lugar.
IP:192.xxx.xxx.27 MAC:3[illegible]l:5 8 OS:VMware ESXi	TCP/0	El VMware ESXi 5.0 host remoto se ve afectado por múltiples vulnerabilidades de seguridad.	ALTO	Aplicar ESXi500-201205401-SG o implementar las soluciones temporales / mitigaciones señaladas por el vendedor,Aplicar ESXi500-201207101-SG, Aplicar ESXi500-201212xxx-SG, Aplicar ESXi500-201320101-SG, ESXi500-201310101-UG, o ESXi500-Update03,Aplicar ESXi500-201206401-SG, Aplicar ESXi500-201112401-SG.
	TCP/0	El VMware ESXi 5.0 host remoto se ve afectado por una vulnerabilidad de desbordamiento de búfer.	MEDIO	Aplicar ESXi500-201303101-SG,Aplicar ESXi500-201203101-SG, Aplicar ESXi500-201407001 parche para ESXi 5.0, Aplicar ESXi500-201308101-SG.
	TCP/443	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	MEDIO	Desactivar SSLv3. Servicios que deben soportar SSLv3 debe activar el mecanismo de TLS repliegue SCSV hasta SSLv3 se puede desactivar.
	TCP/443	El servicio remoto tiene una configuración que puede hacer que sea vulnerable al ataque CRIMEN.	MEDIO	Desactivar la compresión y / o el servicio SPDY.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.

IP:192.xxx.xxx.30 MAC:4(:ca OS:VMware ESXi	TCP/0	El VMware ESXi 5.1 host remoto se ve afectado por múltiples vulnerabilidades de seguridad.	ALTO	Aplicar ESXi510-201212101-SG
	TCP/0	El VMware ESXi 5.1 host remoto se ve afectado por múltiples vulnerabilidades de seguridad.	MEDIO	Aplicar ESXi510-201304201-SG, Aplicar ESXi510-201401101-SG, Aplicar ESXi510-201320101-SG, Aplique el parche ESXi510-201406401-SG para ESXi 5.1, Aplicar ESXi510-201307101-SG.
	TCP/443	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	MEDIO	Desactivar SSLv3. Servicios que deben soportar SSLv3 debe activar el mecanismo de TLS repliegue SCSV hasta SSLv3 se puede desactivar.
	TCP/443	El servicio remoto tiene una configuración que puede hacer que sea vulnerable al ataque CRIMEN.	MEDIO	Desactivar la compresión y / o el servicio SPDY.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio
IP:192.xxx.xxx.31 MAC:3(92 OS:VMware ESXi	TCP/0	El VMware ESXi 5.5 host remoto está potencialmente afectada por múltiples vulnerabilidades.	ALTO	Aplique el parche ESXi550-201404420 para ESXi 5.5 o ESXi550-201404401 para ESXi 5.5 Update 1.
	TCP/0	El VMware ESXi 5.5 host remoto se ve afectado por múltiples vulnerabilidades.	MEDIO	Aplique el parche ESXi550-201409101-SG para ESXi 5.5, Aplicar ESXi550-201406001 parche para ESXi 5.5.
	TCP/0	El VMware ESXi 5.5 host remoto se ve afectado por una vulnerabilidad de elevación de privilegios.	MEDIO	Aplicar ESXi550-201312201-SG.

	TCP/443	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	MEDIO	Desactivar SSLv3. Servicios que deben soportar SSLv3 debe activar el mecanismo de TLS repliegue SCSV hasta SSLv3 se puede desactivar.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.
IP:192.xxx.xxx.32 MAC:0[illegible]:7c OS:VMware ESXi	TCP/0	El host remoto está ejecutando una versión no soportada de una aplicación de virtualización.	CRITICO	Actualizar a una versión de VMware ESX / ESXi que se soporta actualmente.
	TCP/0	El host VMware ESX / ESXi remoto se ve afectado por múltiples vulnerabilidades de seguridad.	ALTO	Aplique los parches faltantes.
	UDP/123	El servicio de hora de red remoto tiene una vulnerabilidad de denegación de servicio.	MEDIO	Actualizar a NTP 4.2.4p8 / 4.2.6 o posterior.
	UDP/123	El servicio de hora de red remoto podría ser utilizado para el reconocimiento de la red o abusado en un ataque de denegación de servicio.	MEDIO	Si utiliza NTP del Proyecto Network Time Protocol, o actualizar a 4.2.7 NTP-p26 o posterior, o añadir 'monitor de desactivar "al" ntp.conf' archivo de configuración y reiniciar el servicio. De lo contrario, póngase en contacto con el vendedor. De lo contrario, limitar el acceso al servicio afectado hosts de confianza.
	TCP/443	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	MEDIO	Desactivar SSLv3. Servicios que deben soportar SSLv3 debe activar el mecanismo de TLS repliegue SCSV hasta SSLv3 se puede desactivar.

	TCP/443	El servicio remoto permite renegociación insegura de conexiones TLS / SSL.	MEDIO	Póngase en contacto con el proveedor para obtener información específica parche.
	TCP/443	El servicio remoto tiene una configuración que puede hacer que sea vulnerable al ataque CRIMEN.	MEDIO	Desactivar la compresión y / o el servicio SPDY.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	La cadena de certificados X.509 utilizado por este servicio contiene certificados con claves RSA de menos de 2.048 bits.	BAJO	Vuelva a colocar el certificado de la cadena con la clave RSA menos de 2048 bits de longitud con una clave más larga, y vuelva a emitir los certificados firmados por el antiguo certificado.
	TCP/443	El servicio remoto es compatible con el uso del sistema de cifrado RC4.	BAJO	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de algoritmos de cifrado RC4. Considere el uso de TLS 1.2 con suites AES-GCM sujetas a navegador y soporte de servidor web.

Anexo 9 Vulnerabilidades en hosts

Información	Puerto	Vulnerabilidad	Riesgo	Solución
IP:192.xxx.xxx.2 MAC:0 94 DNS/NetBios:STS03 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Código arbitrario puede ser ejecutado en el host remoto debido a un defecto en él. servicio "Servidor"	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008
	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2.
	TCP/445	Es posible iniciar sesión en el host remoto de Windows con un NULL (sin usuario ni contraseña)	MEDIO	Aplicar los siguientes cambios en el registro por los Technet referenciados avisos: Conj unto: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ Lsa \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ RestrictNullSessAccess = 1 Retire NAVEGADOR de:- HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ NullSessionPipes Reboot una vez que los cambios en el registro están completa
	TCP/445	La firma no es necesaria en el servidor SMB remoto	MEDIO	Hacer cumplir mensaje de firmar en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor

IP:192.xxx.xxx.3 MAC:(2a: 68 DNS/NetBios:STS00 OS:Microsoft Windows Server 2008 Service Pack 1 Datacenter	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.
	TCP/445	La firma no es necesaria en el servidor SMB remoto	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
	TCP/3389	El control remoto de Terminal Services no utiliza a nivel de red de autenticación.	MEDIO	Habilitar a nivel de red de autenticación (NLA) en el servidor RDP remoto.Esto se hace generalmente en la ficha 'Remote' de la configuración del 'sistema' en Windows.
IP:192.xxx.xxx.4 MAC:0)d: 1a DNS/NetBios:STS04 OS:Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	TCP/443	Certificado SSL del servidor remoto ya ha expirado.	MEDIO	Compra o generar un nuevo certificado SSL para reemplazar el existente.
	TCP/443	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	MEDIO	Desactivar SSLv3. Servicios que deben soportar SSLv3 debe activar el mecanismo de TLS repliegue SCSV hasta SSLv3 se puede desactivar.
	TCP/443	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/443	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.

	TCP/443	El servicio remoto cifra el tráfico utilizando un protocolo con debilidades conocidas.	MEDIO	Consulte la documentación de la aplicación que permite deshabilitar SSL 2.0 y utilizar SSL 3.0, TLS 1.0, o superior en su lugar.
	TCP/443	El certificado SSL para este servicio es para un host diferente.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
	TCP/3389	El control remoto de Terminal Services no utiliza a nivel de red de autenticación.	MEDIO	Habilitar a nivel de red de autenticación (NLA) en el servidor RDP remoto.Esto se hace generalmente en la ficha 'Remote' de la configuración del 'sistema' en Windows.
IP:192.xxx.xxx.5 MAC:0 1e: b2 DNS/NetBios:STS05 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Código arbitrario puede ser ejecutada en el host remoto debido a una falla en el servicio "Servidor".	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.

	TCP/445	Es posible iniciar sesión en el host remoto de Windows con una sesión nula.	MEDIO	Aplicar los siguientes cambios en el registro por los avisos de Technet referencia: Ajuste: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ Lsa \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ RestrictNullSessAccess = 1 Retire NAVEGADOR de: - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ NullSessionPipes Reinicie una vez que los cambios en el registro están completas.
	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
IP:192.xxx.xxx.7 MAC:0[redacted]5: 40 DNS/NetBios:SPW00 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.
	TCP/3389	El host remoto está utilizando la criptografía débil.	MEDIO	Cambie el nivel de cifrado RDP a uno de: 3. Alto 4. Compatible con FIPS

	TCP/3389	Puede ser posible obtener acceso al host remoto.	MEDIO	Forzar el uso de SSL como una capa de transporte por este servicio si es compatible, y / o - Seleccione la opción 'Permitir sólo las conexiones desde equipos que ejecuten Escritorio remoto con Autenticación a nivel de red' ajuste si está disponible.
IP:192.xxx.xxx.33 MAC:00: : 46 DNS/NetBios:ANT00 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible bloquear el host remoto debido a un defecto en SMB.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/445	Código arbitrario puede ser ejecutada en el host remoto debido a una falla en el servicio "Servidor".	CRITICO	Microsoft ha publicado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
	TCP/3389	El host remoto de Windows podría permitir la ejecución de código arbitrario.	ALTO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.
	TCP/445	Es posible iniciar sesión en el host remoto de Windows con una sesión nula.	MEDIO	El host remoto está ejecutando Microsoft Windows. Es posible acceder a él mediante una sesión NULL (es decir, sin ningún usuario o contraseña).Dependiendo de la configuración, puede ser posible que un atacante remoto no autenticado para aprovechar este tema para obtener información sobre el host remoto.

	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
	TCP/8060	El servidor web remoto se ve afectado por una vulnerabilidad de recorrido de directorios.	MEDIO	Póngase en contacto con el proveedor para obtener una actualización, utilice un producto diferente, o desactivar el servicio por completo.
IP:192.xxx.xxx.39 MAC:e4: : DNS/NetBios:CTP00 OS:Microsoft Windows Server 2003 Service Pack 2	TCP/445	Es posible iniciar sesión en el host remoto de Windows con una sesión nula.	MEDIO	Aplicar los siguientes cambios en el registro por los avisos de Technet referencia: Ajuste: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ Lsa \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ RestrictNullSessAccess = 1 Retire NAVEGADOR de: - HKLM \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters \ NullSessionPipes Reinicie una vez que los cambios en el registro están completas.
	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también

				«enlaces para obtener más detalles.
IP:192.xxx.xxx.78 MAC:fc :9 DNS/NetBios:ORIS/ORIS OS:Microsoft Windows 7 Professional	UDP/5355	Código arbitrario puede ser ejecutado en el host remoto a través del cliente DNS de Windows instalado.	CRITICO	Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2
	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
IP:192.xxx.xxx.111 MAC:3 ɔe: bf DNS/NetBios:ARTES02 OS:Mac OS X 10.7	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
	TCP/548	Los usuarios remotos pueden ver las otras direcciones de red.	MEDIO	Actualización a OS X versión 10.10 o superior.

IP:192.xxx.xxx.113 MAC:4 31: ser DNS/NetBios:admredes OS:Microsoft Windows 8.1 Pro	TCP/445	Firma no es necesaria en el servidor SMB remoto.	MEDIO	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva "Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre) ". En Samba, el ajuste se llama 'firma servidor'. Ver los 'Véase también «enlaces para obtener más detalles.
	TCP/1985	El servidor web remoto es propenso a ataques de cross-site scripting.	MEDIO	Póngase en contacto con el vendedor de un parche o actualización.
	TCP/3389	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	MEDIO	Compra o generar un certificado adecuado para este servicio.
	TCP/3389	El certificado SSL para este servicio no se puede confiar.	MEDIO	Compra o generar un certificado adecuado para este servicio.

Anexo 10

Informe de resultados

INFORME DE LAS PRUEBAS DE PENETRACIÓN

EVALUACIÓN DE VULNERABILIDADES

Por: Cristina M. Jaramillo, Juan C. Riofrío

EDITORIAL DON BOSCO | CUENCA - ECUADOR

INFORMACIÓN LEGAL.

Estas pruebas han sido llevadas a cabo por Cristina M. Jaramillo y Juan C. Riofrío, estudiantes de la carrera de Ingeniería de Sistemas de la Universidad Politécnica Salesiana como parte de su trabajo de fin de carrera, quienes garantizan que la información contenida en este informe es verdadera a medida que se pueda verificar en internet.

Las pruebas de penetración llevadas a cabo revelan todas las vulnerabilidades encontradas hasta la fecha de este informe, como es de conocimiento a medida que avance el tiempo irán apareciendo nuevas vulnerabilidades por lo que se sugiere realizar evaluaciones de seguridad de forma periódica cada 3 o 6 meses y cada vez que se realicen cambios importantes en el hardware o software.

DETALLES DEL DOCUMENTO.

Tipo de documento.	Informe de evaluación de seguridad.
Cliente.	Editorial Don Bosco
Consultores.	Cristina M. Jaramillo, Juan C. Riofrío
Versión del documento	1
Fecha de creación	26/01/2015

REVISIÓN HISTÓRICA.

La empresa Editorial Don Bosco no presenta antecedentes en cuanto apruebas de penetración, por lo que este constituye su primera evaluación de seguridad.

CONTENIDO

LIMITACIONES A LA DIVULGACIÓN Y USO DEL INFORME

Este informe contiene información referente a las vulnerabilidades presentes en la red y sistemas de la Editorial Don Bosco así como los posibles métodos de explotación, por lo que se recomienda se tomen las precauciones necesarias para proteger la confidencialidad de este documento y la información contenida en él. La Universidad Politécnica Salesiana conservará una copia de este documento previa documentación de información que sea considerada como sensible y pasará a formar parte de sus repositorios. Todas las demás copias del informe han sido entregadas a la Editorial Don Bosco.

La evaluación de la seguridad es un proceso incierto basado en experiencias pasadas, en la información disponible en la actualidad y las amenazas conocidas, por lo que se debe tener en cuenta que todos los sistemas de información son dependientes de los seres humanos los cuales son vulnerables a un cierto grado, esto implica que no existe ninguna garantía de que mediante una prueba de penetración se identificarán todas las vulnerabilidades existentes o se pueda recomendar soluciones que mitiguen todas estas fallas.

El siguiente análisis de vulnerabilidades se basa en las tecnologías y las amenazas conocidas a partir de la fecha de este informe y debido a que las tecnologías y los riesgos cambian con el tiempo, debido a esto las vulnerabilidades asociadas a la Editorial Don Bosco descritas en este informe, así como las acciones necesarias para reducir la exposición a este tipo de vulnerabilidades, también cambiarán.

Este informe puede recomendar a la Editorial Don Bosco utilizar ciertas herramientas de software o hardware por lo que se recalca que dichas recomendaciones son basadas en opiniones tomadas de internet y los consultores no se harán responsables si un determinado producto no funciona según lo anunciado por el proveedor.

Este informe fue preparado como un trabajo de fin de carrera para el uso y beneficio exclusivo de la Editorial Don Bosco y es considerado como información confidencial.

El Acuerdo de confidencialidad vigente entre los estudiantes y la Editorial Don Bosco regula la divulgación de este informe a las demás partes.

RESUMEN EJECUTIVO.

El principal objetivo del penetration test interno fue examinar plenamente los sistemas y la red de la Editorial Don Bosco para identificar las vulnerabilidades que podrían permitir a un atacante situado dentro de la red interna comprometer la confidencialidad, integridad y disponibilidad de dichos sistemas. A continuación se presenta un resumen ejecutivo de los problemas encontrados:

Los servidores tanto Windows como Linux presentan varias vulnerabilidades. Estos fallos comprenden el mayor riesgo para la seguridad de los sistemas bajo prueba. Hubo vulnerabilidades que se consideran crítica en gravedad, sin embargo también se encontraron vulnerabilidades de alta gravedad y hallazgos de gravedad media.

Se llevó a cabo pruebas en las redes inalámbricas, las mismas que implicaban la ingeniería social para posterior realizar pruebas de diccionario con el fin de obtener las claves y acceder sin ningún inconveniente.

En cuanto a la red VoIP presenta una vulnerabilidad muy importante al no usar protocolos seguros lo que puede permitir que un atacante escuche conversaciones privadas.

Las bases de datos no fueron probadas, ni se llevó a cabo pruebas. Ya que una denegación de servicio implicaba riesgos muy altos de una caída del sistema en la Empresa que hubiera puesto en peligro las actividades que realiza diariamente.

OBJETIVO DE LAS PRUEBAS DE PENETRACIÓN.

El objetivo de llevar a cabo una evaluación de la seguridad mediante un test de penetración sobre la red y las aplicaciones de la Editorial Don Bosco, es determinar el nivel de seguridad de la empresa poniendo a prueba cada segmento de la red y hosts dentro del alcance del área trabajo y de esta manera verificar bajo situaciones extremas cuál es el comportamiento de los mecanismos de defensa e identificar vulnerabilidades, mala configuración de los equipos y errores en el diseño.

ALCANCE DE LAS PRUEBAS DE PENETRACIÓN.

La evaluación de vulnerabilidades se ha centrado principalmente en explorar fallas presentes en la red y en los sistemas de la empresa, tomando como objetivos principales servidores, sistemas de VOIP, WLAN e intranet. El resultado de este proceso pretende ser una evaluación global de la red, equipos y página web de la Editorial Don Bosco. .

Durante el desarrollo de este proceso no se tomó en cuenta las bases de datos por el alto riesgo existente de un colapso del sistema y de las funciones primarias del negocio y tampoco se tomó como competencia de los evaluadores la realización de pruebas de penetración externas.

SISTEMAS OBJETIVO A EVALUAR.

A continuación se muestran la URL dela la intranet y los equipos que fueron tomados como blanco durante esta evaluación de seguridad.

OBJETIVOS WEB	
Aplicación	**Intranet de la Editorial Don Bosco**
URL 1	http://emp.lsn.com.ec
URL 2	http://192.xxx.xxx.25/helpdesk/index.php
EQUISPOS OBJETIVO	
Categoría	**Descripción**
Red VOIP	192.xxx.xxx.0/24
Redes inalámbricas	ESSID: wcgs BSSID: 00:xx:xx:xx:xx:5D ESSID: edbuse BSSID: 0A:xx:xx:xx:x:D0
Servidores Windows	192.xxx.xxx.201 (dad00.[illegible]) 192.xxx.xxx.65 (SEP0026CBBDEA63.xxx.xxx.ec) 192.xxx.xxx.67 (SEP001C58576AA3.xxx.xxx.ec) 192.xxx.xxx.16 (mansis.l[illegible]) 192.xxx.xxx.11 (clr00.xxx.xxxx) 192.xxx.xxx.28 (sts03.xxx.xxxx) 192.xxx.xxx.34 (Sts02.xxx.xxx.ecg)
Servidor Linux	192.xxx.xxx.10 (dns1.lns.com.ec)
Personal administrativo sometido a ingeniería social	• Maria del Carmen Bermeo • Christian Saquicela
Firewall	192.xxx.xxx.254

TABLA 1. OBJETIVOS A EVALUAR

METODOLOGÍA PARA LAS PRUEBAS DE PENETRACIÓN.

Para el desarrollo de las pruebas de penetración hemos seguido tres metodologías, una para referente en el proceso de evaluación de la seguridad en páginas WEB, otra que ha servido como guía en el resto de áreas y una tercera que consiste en una metodología propia la cual aglomera las anteriores y describe paso a paso cual es el proceso a seguir dentro de un test de penetración tomando los fragmentos más importantes y útiles. Para una mejor ilustración de estas metodologías las explicaremos con mayor detalle a continuación:

- OWASP v4.0 (Open Web Application Security Project) o Proyecto abierto de seguridad de aplicaciones web que contiene definiciones básicas y describe todos los principios importantes de seguridad, agentes de amenaza, ataques, vulnerabilidades, contramedidas e impactos técnicos.
- OSSTMM v3.0 (The Open Source Security Testing Methodology Manual) o Manual De Metodología Abierta De Testeo, es uno de los manuales más completos y comúnmente utilizados en Auditorías de Seguridad el cual incluye un marco de trabajo que describe a detalle las fases a seguir dentro del proceso de la evaluación de la seguridad.
- Metodología propia, la cual la llamaremos como metodología por fases, esta nos mostrará el proceso a seguir dentro de la evaluación de la seguridad, la misma que consta de 5 fases claramente definidas, en la fase de descubrimiento se ha realizado un escaneo sobre servidores y otros medios que nos han provisto de información pública lo cual nos permitirá conocer que tan expuesta se encuentra la empresa, posterior a esto tenemos a la fase de exploración para lo cual se ha hecho uso de técnicas intrusivas obteniendo información que apoyará mas adelante el proceso de intrusión, en la fase de evaluación se ha determinado mediante un análisis cuales serán nuestros objetivos y sus vulnerabilidades según el impacto que tendrán estos, en la fase de intrusión se procedió a realizar la explotación de vulnerabilidades para finalmente concluir con la elaboración del informe.

IMAGEN 1. METODOLOGÍA PROPIA

HERRAMIENTAS USADAS.

ACTIVIDAD	HERRAMIENTA
Footprinting y Escaneo de puertos	Nmap y ZenMap, SpiderFoot, "IP Address and Domain Information", NsLookup
Exploración de la página Web	ZAP
Valoración de vulnerabilidades VoIp	Sivus
Valoración de Vulnerabilidades Red Datos	Nessus v 5.2 Home
Penetration Test	Metasploit Framework
Penetration Test Página Web	Sqlmap

Investigación y Verificación de Vulnerabilidades	http://www.securityfocus.com/bid http://packetstormsecurity.org http://www.securiteam.com http://www.securitytracker.com/ http://osvdb.org/ http://osvdb.org/ http://www.securityforest.com/ http://www.cert.org/ http://cve.mitre.org/ http://www.insecure.org/sploits.html http://www.phrack.org/

TABLA 2. HERRAMIENTAS USADAS

CLASIFICACIÓN DE RIESGOS DE VULNERABILIDADES.

A lo largo de la evaluación, cada vulnerabilidad identificada ha sido etiquetada y categorizada según el nivel de riesgo que esta represente, para ello hemos tomado como referencia la clasificación seguida por TENABLE-NESSUS, la cual se basa en sistema de puntuaciones mediante CVSS (Scoring System Common Vulnerability) o Sistema de puntuación de vulnerabilidades en común donde si la vulnerabilidad es crítica tomará un valor igual a 10, si es alta su valor estará entre 7 y 9.99, si es media su valor estará entre 4.1 y 6.99, si la vulnerabilidad es baja su cvss estará entra 0.1 y 4 y si es solo información tendrá un valor de 0. Esto se indica de forma mucho más clara y precisa en la siguiente tabla.

RIESGO	DESCRIPCIÓN
CRITICO CVSS=10	Estos hallazgos identifican situaciones que comprometerán directamente a la víctima o lograrán un acceso no autorizado como SYSTEM a la red, sistema, aplicación o información.
ALTO CVSS ENTRE 7 y 9.99	Estos hallazgos identifican situaciones que comprometerán directamente a la víctima o lograr un acceso no autorizado a la red, sistema, aplicación o información, pero sin privilegios de SYSTEM.
MEDIO CVSS ENTRE 4.1 6.99	Estos hallazgos identifican condiciones que no resultan inmediatamente o directamente en el compromiso o acceso no autorizado de una red, sistema, aplicación o información, pero proporcionan una capacidad o información que podría, en combinación con otras capacidades o información, dar lugar al compromiso o el acceso no autorizado de una red, sistema, aplicación

	o información. Ejemplos de Riesgos Medianos incluyen sistemas desprotegidos, archivos y servicios que podrían resultar en la denegación de servicios o sistemas no críticos.
BAJO CVSS ENTRE 0.1 Y 4	Estos hallazgos identifican situaciones que no resultan inmediatamente o directamente en el compromiso de una red, sistema, aplicación o información, pero no proporcionar información que podría ser utilizada en combinación con otra información para obtener acceso no autorizado a una red, sistema, aplicación o información. Ejemplos de bajos riesgos incluyen cookies no marcadas como seguras; sesiones concurrentes, etc.
INFORMACIÓN CVSS IGUAL A 0	Estos hallazgos incluyen únicamente información que no comprometen a los sistemas en absoluto.

TABLA 3. CLASIFICACIÓN DE VULNERABILIDADES

DIAGRAMA DE LA RED INTERNA.

Dentro de la fase de descubrimiento se logró encontrar la presencia de dos segmentos de red en los cuales nos hemos basado para la realización de la evaluación de vulnerabilidades, el primero es usado para datos 192.xxx.xxx.0/24 y el segundo se encuentra dedicado para voz 192.168.101.0/24, como se muestra en la siguiente imagen.

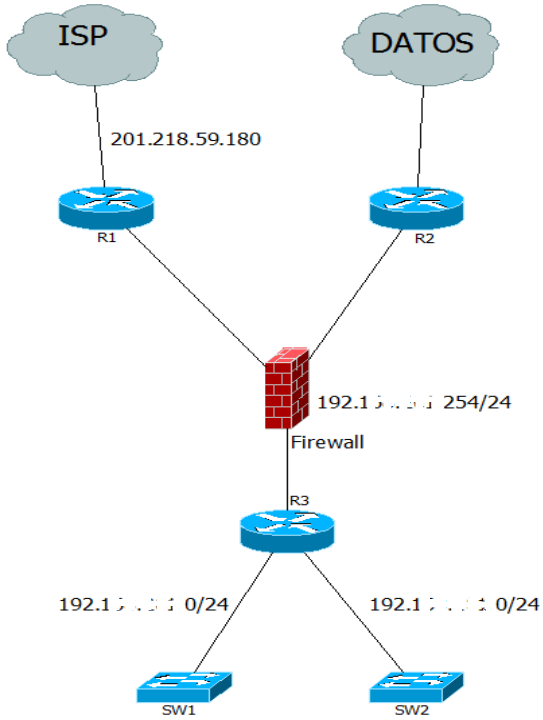


IMAGEN 2. DIAGRAMA DE LA RED INTERNA

HALLAZGOS Y RESUMEN DE RESULTADOS.

Durante el proceso de descubrimiento de vulnerabilidad se realizó escaneos y búsquedas de las mismas en distintos sistemas donde tuvimos como resultados lo siguiente:

En servidores con sistemas operativos Windows destacaron vulnerabilidades como MS08-067 y MS09-050 las cuales son vulnerabilidades que constan dentro del grupo de vulnerabilidades críticas y pueden permitir desde un ataque DOS hasta la completa toma de control del equipo, también se encontraron vulnerabilidades que parten del echo de usar sistemas obsoletos como en el caso de la vulnerabilidad 74496-DNS la cual implica que la versión del DNS es obsoleta. A continuación se muestra un cuadro estadístico donde se indica el porcentaje de vulnerabilidades encontradas según el riesgo que estas implican para los equipos, donde se puede ver que existe una cantidad considerable de vulnerabilidades críticas y altas.

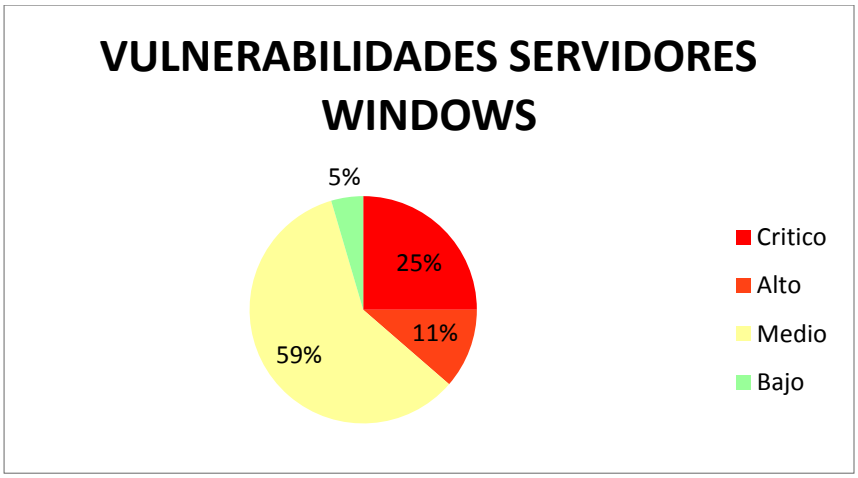


IMAGEN 3. CUADRO ESTADÍSTICO VULNERABILIDADES WINDOWS

En terminales de trabajo con sistemas operativos Windows se encontraron equipos que aun operan bajo sistemas Windows XP, el cual al no poseer soporte por parte del proveedor es visto como un equipo vulnerable y que puede afectar a la seguridad de otros equipos, en el resto de estaciones de trabajo resaltaron vulnerabilidades como MS09-001 que indican que la víctima es vulnerable a ataques de denegación de servicios. Seguidamente mostramos un cuadro estadístico referente al porcentaje de vulnerabilidades encontradas clasificadas según su nivel de riesgo, lo que indica que en su mayoría los equipos poseen vulnerabilidades medias que no comprometen al equipo directamente, esto implica una cantidad menor de vulnerabilidades críticas y altas respecto a los servidores, pero que de igual forma deberán ser atendidas.

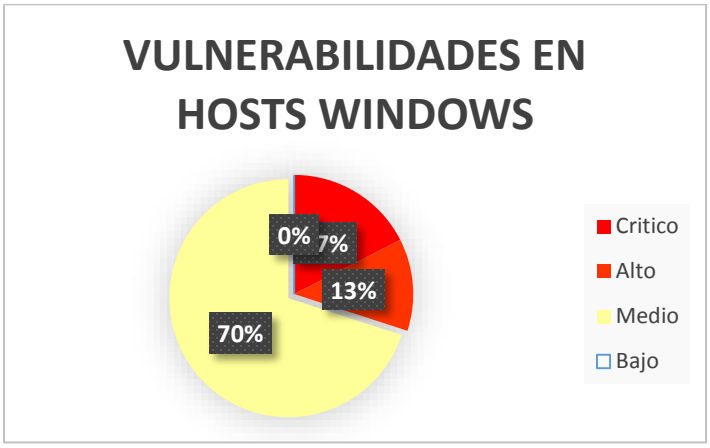


IMAGEN 4. CUADRO ESTADÍSTICO VULNERABILIDADES HOST WINDOWS

Respecto a los servidores con sistemas operativos GNU/LINUX se encontró muy pocas vulnerabilidades y en su mayoría fueron vulnerabilidades relacionas al uso de software obsoleto,

entre las que destacaban 3385-SO-Fedora, que hace referencia a que el sistema usado ya no posee soporte, 58987-PHP indica que la versión de usada PHP es obsoleta y 41028-SNMP que se refiere a que el servicio de SNMP es de tipo público y puede proporcionar información acerca de su identidad, mostrando a continuación su cuadro estadístico lo cual corrobora lo antes expuesto.

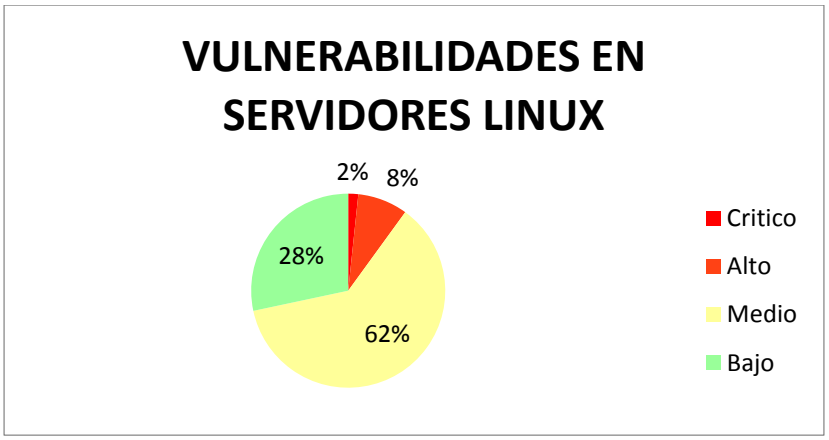


IMAGEN 5. CUADRO ESTADÍSTICO VULNERABILIDADES LINUX

En cuanto a equipos CISCO e IMPRESORAS no se encontraron vulnerabilidades críticas ni altas que podrían permitir un ataque informático, tal como se muestra en el siguiente cuadro estadístico la mayor parte de vulnerabilidades son según su impacto de nivel bajo y existe un pequeño porcentaje de vulnerabilidades con un nivel medio que no impactarán directamente sobre los dispositivos.

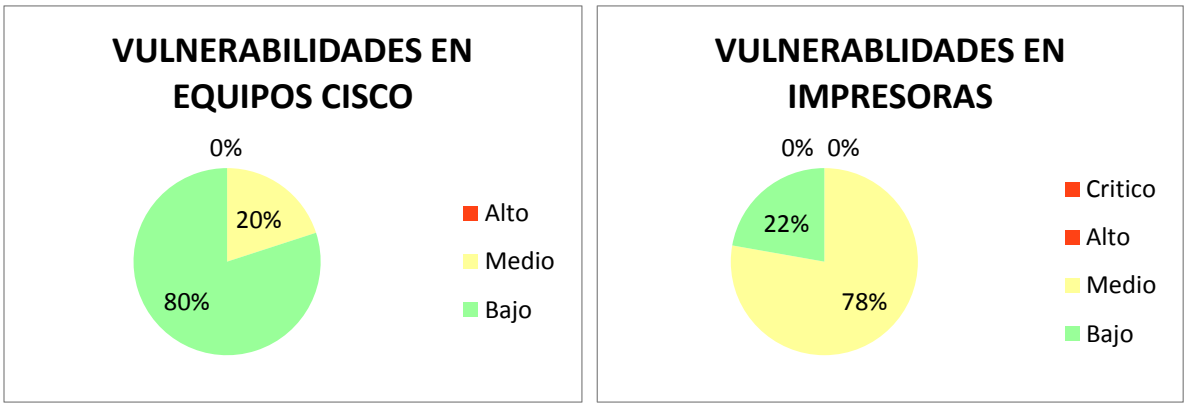


IMAGEN 5. CUADRO ESTADÍSTICO VULNERABILIDADES EN IMPRESORAS Y EQUIPOS CISCO

Las vulnerabilidades encontradas en equipos con sistemas varios es decir equipos con software de virtualización, dispositivos móviles (no son tomado en cuenta en el desarrollo de estas pruebas), etc., se encontró una cantidad baja de vulnerabilidades consideradas críticas o altas, las cuales se debían a la falta de actualizaciones o uso de parches sobre los sistemas de virtualización, destacando

entre estas 70882-ESXI 5.0 la cual indica múltiples vulnerabilidades de nivel crítico y alto que lo que haces es revelar información acerca del software de virtualización, lo cual podemos confirmarlo mediante el siguiente cuadro estadístico.

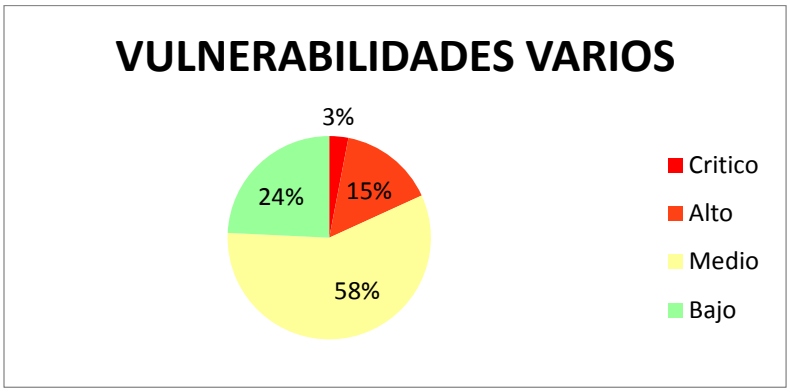


IMAGEN 6. CUADRO ESTADÍSTICO VULNERABILIDADES VARIOS

Otro de los sistemas que se puso a prueba fue el sistema de VOIP cuyas pruebas consistieron en realizar una análisis del segmento de red y de los terminales dando como resultado una falla de encriptación en el protocolo SIP el cual se da por no usar un protocolo seguro como TLS lo que permitía realizar capturas de paquetes RTP y escuchar conversaciones afectando la confidencialidad de la información, tal como se muestra en la siguiente figura, donde se puede ver los paquetes RTP capturados y la reproducción de los mismos.

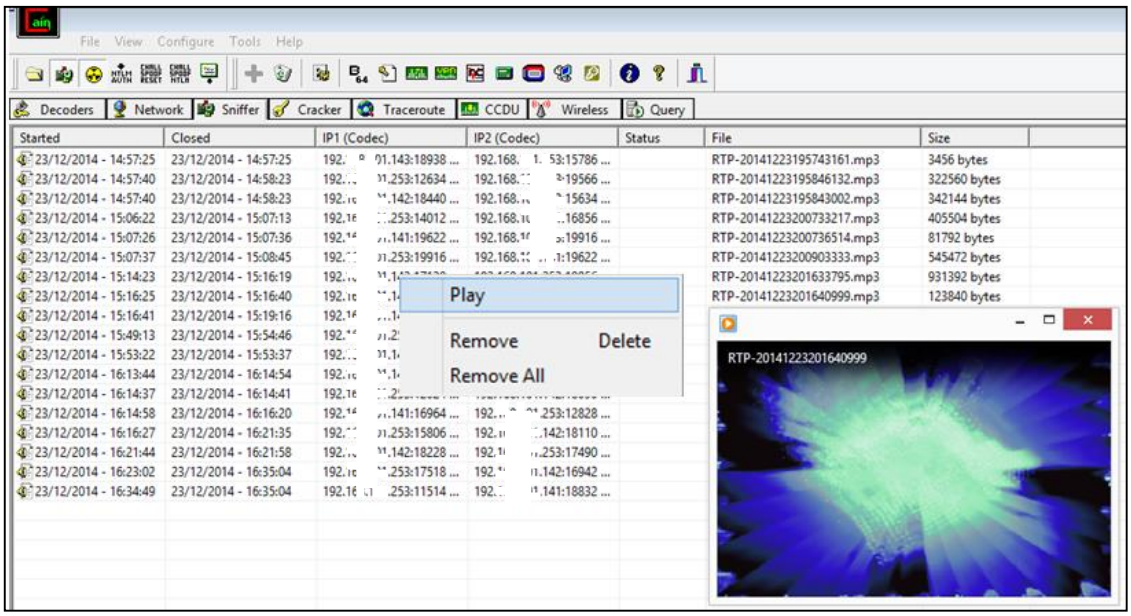


IMAGEN 7. CAPTURA Y REPRODUCCIÓN DE PAQUETES RTP

Otro objetivo que fue evaluado fue la intranet de la empresa, donde se encontró dos vulnerabilidades, la primera con respecto al listado del directorio raíz el cual publica información acerca de la configuración del servidor web, como se puede ver en la siguiente imagen.

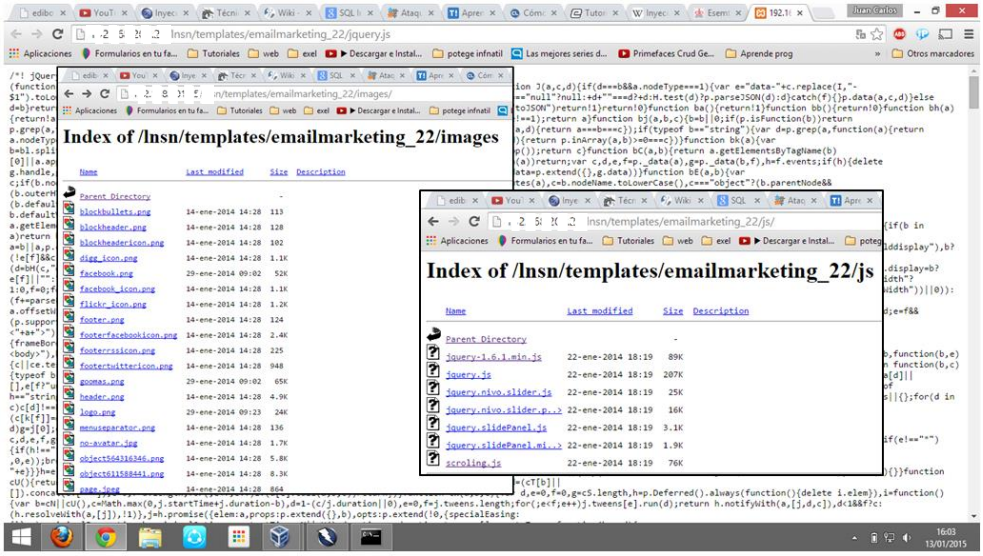


IMAGEN 8. LISTADO DE DIRECTORIOS DE LA PÁGINA WEB

La siguiente vulnerabilidad encontrada fue la posibilidad de realizar un ataque de inyección SQL, la misma que fue puesta a prueba sin tener éxito y constituyéndose en un false positivo como se muestra en la imagen.

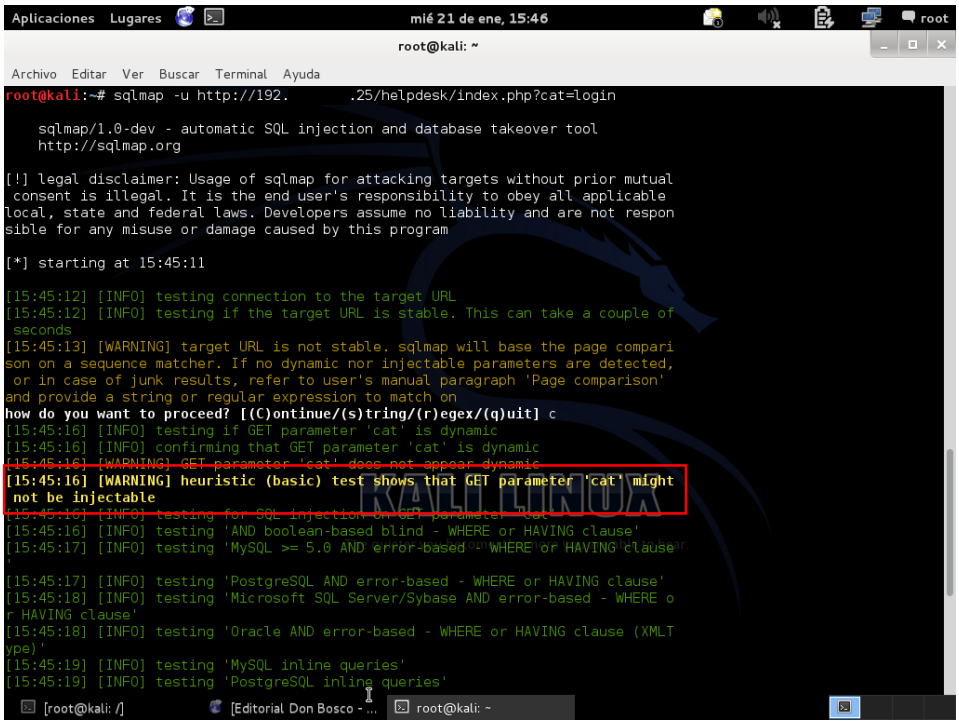


IMAGEN 9. PRUEBA FALLIDA DE UN ATAQUE DE INYECCIÓN SQL

Finalmente como último punto de comprobación tenemos las redes WLAN las cuales fueron sometidas a ataques de fuerza bruta sin tener éxito demostrando que poseían una contraseña posiblemente robusta, por lo que se prosiguió con un ataque de diccionario donde se ingresó palabras y contraseñas usadas en otros sistemas obtenidas mediante la indagación de las mismas a los empleados de la empresa logrando así obtener la contraseña correcta, tal como se indica en la siguiente imagen.

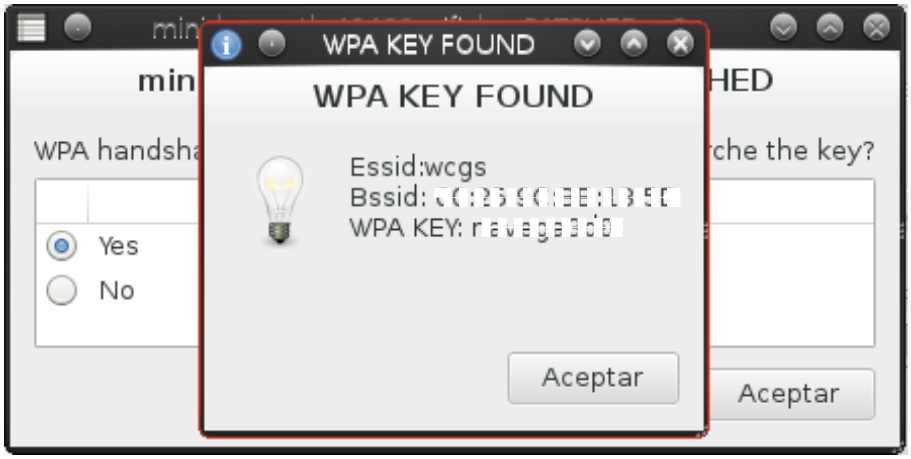


IMAGEN 10. OBTENCIÓN CORRECTA DE LA CLAVE WLAN WCGS

Para brindar una mejor comprensión acerca de los ataques realizados y los resultados obtenidos así como el nivel de impacto que representan estos para los diferentes sistemas, se muestra a continuación una tabla con esta información. Si se desea más detalles acerca de las vulnerabilidades encontradas se puede consultar esta información en los anexos: 4, 5,6, 7,8, 9

VULNERABILIDAD	ACCESO	RESULTADOS	NIVEL DE RIESGO
MS09-001	MEDIO.	Con esta vulnerabilidad se logró concluir con éxito a un ataque DOS (denegación de servicios) con el uso del protocolo SMB	CRITICO
MS08-067	TOTAL	Se obtuvo acceso total al dispositivo mediante el protocolo RPC, teniendo así la capacidad de crear, modificar y eliminar registros, acceso a la Shell y permisos de súper usuario.	CCRITICO
MS09-050	TOTAL	Se obtuvo acceso total al dispositivo mediante el protocolo SMB, teniendo así la capacidad de crear, modificar y eliminar registros, acceso a la	CRITICO

		Shell y permisos de súper usuario.	
74496-DNS	BAJO	No se comprometió el sistema pero se demostró que la versión que se usa de DNS corresponde a una muy antigua que no posee soporte por lo que se le considera vulnerable.	CRITICO
70882 - ESXi 5.0. (VMWARE)	MEDIO	Fue posible obtener información importante del sistema de virtualización como huellas digitales y versiones del software, además que se demostró que existe la posibilidad de realizar ataques de fuerza bruta aunque no se tuvo éxito por lo que se deduce las credenciales usadas son seguras	ALTO
33850 SO. Fedora sin soporte	BAJO	No se comprometió el sistema pero se demostró que la versión del SO es obsoleta por lo que se le considera vulnerable.	CRITICO
58987- PHP	BAJO	No se comprometió el sistema pero se demostró que la versión de PHP es obsoleta por lo que se le considera vulnerable.	CRITICO
[9999] TLS- SIP (VOIP)	TOTAL	Con esta vulnerabilidad mediante el protocolo SIP se logró capturar paquetes RTP que nos permitieron interceptar conversaciones desde los equipos terminales mediante un ataque ARP de hombre en el medio.	CRITICO
Listado de directorios en intranet (emp.lns.com.ec)	TOTAL	Se pudo comprobar que mediante la manipulación del URL se puede lograr el acceso a los directorios raíz de la página web lo cual permite exhibir información sensible para el sistema.	CRITICO
41028 – Nombre por defecto del agente SNMP (public)	TOTAL	Se obtuvo datos de configuración del dispositivo que presentaba esta vulnerabilidd	ALTO
Ecriptación WPA/WPA2 redes inalambraicas	TOTAL	Mediante la utilización de wifislax y por ende el uso de	MEDIO

		ataque de fuerza bruta se obtuvo la contraseña de dichas redes	
VULNERABILIDADES INTRANET			
SQL Injection en intranet (emp.lns.con.ec)	BAJO	No se logró respuesta de la base de datos mediante la manipulación del url, también se intentó realizar el ataque con la herramienta sqlmap la cual díio como resultado que la vulnerabilidad no era inyectable, por lo que se consideró esta vulnerabilidad como un falso positivo.	ALTO

TABLA 4. RESUMIDA DE VULNERABILIDADES Y SU IMPACTO EN LOS SISTEMAS

CONTRAMEDIDAS.

A continuación indicaremos las posibles soluciones o contramedidas a cada una de las vulnerabilidades encontradas.

VULNERABILIDAD	CONTRAMEDIDAS
MS09-001	Utilizar el conjunto de parches publicados por Microsoft para Windows 2000, XP, 2003, Vista y 2008.
MS08-067	Utilizar conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
MS09-050	Utilizar parche para Windows Vista y Windows Server 2008.
74496-DNS	Actualizar a una versión compatible de Microsoft Windows.
70882 - ESXi 5.0. (VMWARE)	Aplicar ESXi510-201212101-SG (Actualización).
33850 SO. Fedora sin soporte	Actualizar a una versión más reciente.
58987- PHP	Actualizar a una versión de PHP que se soporta actualmente.
[9999] TLS- SIP (VOIP)	Activación de protocolos de seguridad (el protocolo de transporte TLS) para evitar capturas de paquetes RTP
Listado de directorios en intranet (emp.lns.com.ec)	Configura el servidor web para que oculte esta información y es caso de que sea necesario visualizarla implementar controles sólo para permitir conexiones a la interfaz de administración de hosts conocidos. Un método potencial para lograr esto podría ser a través de permitir únicamente el acceso de los clientes que están detrás de la VPN de la

	empresa o crear una lista blanca de conocidos de confianza o anfitriones.
41028 – Nombre por defecto del agente SNMP (public)	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza o cambiar el nombre de la comunidad SNMP predeterminado es decir cambiar las configuraciones por defecto.
Ecriptación WPA/WPA2 redes inalambraicas	Utilizar contraseñas más robustas para que puedan ser difíciles de descifrar mediante ataque de diccionario
SQL Injection en intranet (emp.lns.con.ec)	No se pudo explotar la vulnerabilidad por lo que se considera un falso positivo.

IMAGEN 11. CUADRO ESTADÍSTICO VULNERABILIDADES WINDOWS

Además de estas posibles soluciones se recomienda como contramedida principal, crear políticas de seguridad acorde a las necesidades de la empresa las cuales permitan mitigar cualquier situación que tenga que ver con la seguridad. También se sugiere implementar un modelo de red segura la cual involucra segmentar la red mediante VLANs para evitar que se filtre tráfico de un segmento de la red a otro, crear y dividir zonas seguras estableciendo claramente DMZ, LAN, WLAN y WAN.

Configurar de forma correcta el servidor de dominios (DNS), para que no proporcione direcciones IP de los equipos y sistemas de la empresa.

CONCLUSIONES Y RECOMENDACIONES

Se ha demostrado y comprobado que la seguridad con la que cuenta la Editorial Don Bosco es deficiente a nivel de la red, por lo que se debe realizar una restructuración completa en la que se debe tomar en cuenta el concepto de seguridad en profundidad y delimitar los servicios internos y externos a ofrecer.

La red no cuenta con segmentación de tráfico, por lo que es posible realizar capturas de paquetes desde la red de dataos hacía la de VOIP y viceversa, esto implica problemas con la confidencialidad por lo que se sugiere segmentar la red mediante el uso de VLANS.

El Firewall se encuentra con la configuración por defecto, lo cual lo vuelve prácticamente inservible permitiendo así evadirlo sin ningún esfuerzo, siendo necesario e inmediato una correcta configuración e implementación de políticas de seguridad adecuadas.

El servidor de dominios no se encuentra bien configurado permitiendo identificar con facilidad las direcciones IP tanto del Firewall como de la intranet, lo que da paso a una fácil identificación del objetivo a atacar, para evitar esto es necesario configurar adecuadamente el DNS evitando así que se publique información innecesaria.

En la mayoría de equipos, principalmente en servidores Windows se ha demostrado que carecen de actualizaciones e instalación de parches, siendo esta la principal razón de la presencia de vulnerabilidades en sus sistemas, por lo que se sugiere el uso de herramientas como WSUS propio de Windows que provee actualizaciones de seguridad mediante *Windows Server Update Services*, permitiendo a los administradores poder manejar centralmente la distribución de parches a través de actualizaciones automáticas a todas las computadoras de la red corporativa.

En cuanto a los sistemas de VOIP existe una completa carencia del uso de protocolos seguros, siendo urgente su pronta implementación ya que se ha demostrado que es posible realizar una intervención de las líneas telefónicas, esto mediante la captura de tráfico RTP los cuales llevan cargado en si las conversaciones.