UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de:
INGENIEROS ELECTRÓNICOS

TEMA:
DESARROLLO DE UN PROTOTIPO HONEYNET COMO MEDIDA DE SEGURIDAD PARA LA RED INFORMÁTICA DE LA UPS SEDE QUITO CAMPUS SUR

AUTORES:
CARCELÉN MÉNDEZ DENNIS FABRICIO
RÍOS MENDOZA CARLOS ALFREDO

TUTOR:
CUICHÁN MORALES CARLOS AUGUSTO

Quito, mayo del 2017

Cesión de derechos de autor

Nosotros, Dennis Fabricio Carcelén Méndez, con documento de identificación N° 1717700049, y Carlos Alfredo Ríos Mendoza con documento de identificación N°1714660691, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de grado/titulación intitulado: DESARROLLO DE UN PROTOTIPO HONEYNET COMO MEDIDA DE SEGURIDAD PARA LA RED INFORMÁTICA DE LA UPS SEDE QUITO CAMPUS SUR, mismo que ha sido desarrollado para optar por el título de: Ingenieros Electrónicos, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

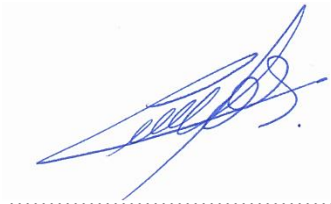
En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....

Nombre: Dennis Fabricio Carcelén Méndez

Cédula: 1717700049

Fecha: mayo, 2017



.....

Nombre: Carlos Alfredo Ríos Mendoza

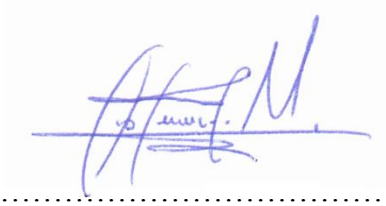
Cédula: 1714660691

Fecha: mayo, 2017

Declaratoria de coautoría del docente tutor

Yo, declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación DESARROLLO DE UN PROTOTIPO HONEYNET COMO MEDIDA DE SEGURIDAD PARA LA RED INFORMÁTICA DE LA UPS SEDE QUITO CAMPUS SUR, realizado por Carcelén Méndez Dennis Fabricio y Ríos Mendoza Carlos Alfredo, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerados como trabajo final de titulación.

Quito, mayo del 2017



……

Ing. Carlos Augusto Cuichán Morales

CI: 1714389721

DEDICATORIA

A mi Dios, siempre fiel e incondicional, por darme la lucidez y paciencia para poder ver hoy mi objetivo culminado. A la virgen María por hacerme sentir su presencia y llevarme de su mano a lo largo de mi vida. Esto tiene un gran significado moral y sentimental para mí porque puedo dedicárselo a la gente que más amo en esta vida: mi mami Carmita, mi papi Clímaco y mis hermanas Laidy y Kathy, que son la única motivación que necesito para poder seguir luchando por todo lo que sueño.

Quiero dedicarle estas pequeñas líneas a mis abuelitos: Celia y Alamiro, y a mi tío Frank, para que (si es verdad que las letras transcienden en el tiempo y que llegan a los lugares que los autores jamás habrían soñado que existen, espero que uno de esos lugares sea el cielo) sepan que siempre los llevo conmigo en cada pensamiento del día y que su paso por mi vida ha sido de extrema e incontable importancia.

A mi gente negra, para que sepan que también es por todos ellos, porque no se dejan vencer y continúan demostrando que somos los verdaderos descendientes de la realeza. Los que me hacen sentir muy orgulloso de mis raíces y de mi historia

A mis amigos, los reales, los que se quedaron para ahora formar parte de mi familia, con los que he compartido tanto, los que sé que aunque sea con un mensaje me preguntan cómo estoy y estarán ahí pendientes de mi camino.

¡Muchas Gracias a todos ustedes!

Dennis

Para la persona que sintió el más inmenso orgullo de haberme creado al tenerme en brazos por primera vez, la única amiga que lo perdona todo y que me enseñó el valor de la sencillez y el arrebato: A mi madre…. La que me dio una gota de esencia y me soltó a dar pelea al mundo. ¡Leyla te amo! Me enseñaste que a pesar de todo uno ama, porque le brota de las mismísimas entrañas del ser y hoy te puedo decir que es cierto.

Para mi Señor Padre, aquel que nunca me dejo caer. A él, que me enseñó a ver la otra cara de la moneda. Me diste el regalo de entender la constancia, el esfuerzo, a ser selectivo y como luchar cada día. Nunca vi a alguien caer tantas veces y levantarse solo. Te debo todas las oportunidades de superación…. ¡Gracias por confiar en mi tantas veces! Eres un modelo a seguir.

Por la autenticidad de tu ser y la grandeza de tu alma, a ti Sabrina. Contigo aprendí un millón de veces más que en cualquier libro, a ti que eres mi escudo, espada, legión y causa. A ti, que llevas en tu corazón solo lo mejor de cada uno de nosotros, porque solo conoces de entrega, porque transmites amor sin mesura, porque verte y escucharte me atan a la vida, porque nadie como tu sabe y me ha enseñado a soltar…

A mis amigos Xavier y Dennis, la familia que siempre está en las malas y en las más malas.

Al amor de mi herida… tú sí que me enseñaste quién no será jamás, ve despacio y la mejor de las suertes. Para todos ustedes que fueron parte de mis días y a la vida que me trajo hoy hasta aquí.

«…Si alguna vez me cruzas, por la calle… regálame tu beso y no te aflijas ché! Si ves que estoy pensando en otra cosa, no es nada malo es que paso una brisa; la brisa de la muerte enamorada, que ronda como un ángel asesino… ¡Mas no te asustes flaca! siempre se me pasa… es solo la intuición de mi destino…» – Fito.

Carlos

AGRADECIMIENTOS

A nuestros maestros.

A los Ingenieros: Verónica Soria, Germán Oñate, Jhonny Barrera, Juan Carlos Domínguez, Milton Tipán y en especial al Ing. Carlos Cuichán Morales, coautor de este proyecto por su gran apoyo y motivación para la culminación de nuestros estudios profesionales y para la elaboración de este proyecto; y en general a nuestra querida Universidad la cual nos permitió recorrer sus aulas y formar parte de esta gran familia Salesiana durante este gran ciclo de nuestras vidas.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto técnico se desarrolla con el objetivo de proponer una herramienta complementaria de seguridad informática, para la red LAN del campus Sur de la Universidad Politécnica Salesiana, Sede Quito, iniciando con la recopilación de información sobre la situación actual de la red del laboratorio, lugar donde se propone la utilización del prototipo de Honeynet y se realizan las pruebas. Adicionalmente, se realiza un estudio sobre el comportamiento por parte de los usuarios hacia los servicios de red dentro del campus, para determinar sus hábitos de uso y su interacción con los componentes de seguridad de la información implementados, para caracterizar las posibles brechas y vulnerabilidades que pudiera tener la red de datos de la institución. Para probar el correcto funcionamiento de la herramienta propuesta, se realizan ataques de penetración planificados basados en pruebas de hackeo ético a los servicios implementados en el prototipo diseñado, para demostrar las ventajas y funcionalidad de dicha herramienta así como el correcto uso de la misma. Y finalmente, los resultados de las pruebas realizadas se documentan para demostrar de forma concluyente los resultados positivos de esta solución y su beneficio para el grupo de interés, que en este caso son las diferentes áreas y departamentos que se encuentran en el Campus Sur de la Universidad Politécnica Salesiana.

ABSTRACT

The present technical project was developed with the aim of proposing a complementary computer security tool for the LAN network of the Networking Laboratories of the South campus of Universidad Politécnica Salesiana, Sede Quito, starting with the collection of information on the current situation of the laboratory network, place where the use of the Honeynet prototype is proposed and tests are performed. In addition, a study is carried out on the behavior of users to the network services within the campus, to determine their usage habits and their interaction with the implemented information security components, to characterize the possible gaps and vulnerabilities that **c**ould have the data network of the institution. To test the correct operation of the proposed tool, planned penetration attacks based on ethical hacking tests are performed on the services implemented in the designed prototype to demonstrate the advantages and functionality of this tool as well as the correct use of it. Finally, the results of the tests performed are documented to conclusively demonstrate the positive results of this solution and its benefit to the interest group, which in this case are the different areas and departments that are located in the South Campus of the Universidad Politécnica Salesiana.

INTRODUCCIÓN

Actualmente, con el aumento constante en el flujo de datos y personas, la seguridad informática se ha convertido en una herramienta de vital importancia a nivel mundial debido a las vulnerabilidades que presentan las redes de información, provocando riesgos a los cuales están expuestos los usuarios y corporaciones, dado que los atacantes pueden obtener información personal o institucional sumamente importantes que podrían usarse para fines dañinos.

El presente trabajo de titulación tiene como su objetivo primordial implementar un mecanismo denominado Honeynet para incrementar los niveles de seguridad de la información para el campus Sur de la Universidad Politécnica Salesiana, en la Sede Quito.

Como Objetivo General del proyecto técnico se plantea:

- Diseñar e implementar un prototipo de Honeynet de detección y registro de los "exploits" de atacantes en la red de la Universidad Politécnica Salesiana Campus sur, mediante la instalación de honeypots en el sistema operativo GNU/Linux y el uso de herramientas de hacking y análisis, para la interpretación de la información recopilada e incremento de las medidas de seguridad.

Los Objetivos Específicos, a lograse con el prototipo son:

- Analizar el estado actual de la red tomando en consideración su topología, para la disposición de la estructura que dé viabilidad a la incorporación de la honeynet en la red de campus.
- Diseñar un prototipo de honeynet basado en esquemas de arquitectura empresarial y redes de datos desde el punto de vista interno, para la especificación de los dispositivos básicos indispensables y herramientas necesarias que garanticen el funcionamiento de la red trampa.
- Implementar varios honeypots vinculando el software de monitoreo de tráfico y actividad sobre la red, para la persuasión a presuntos y potenciales atacantes a la realización de intrusiones en la red trampa.

- Realizar prácticas de penetración y hackeo ético contra la red de pruebas, utilizando herramientas de software libre, para la comprobación del correcto funcionamiento del honeynet y diagnostico acerca de sus parámetros de seguridad.
- Describir los perfiles de usuario de red existentes en el campus sur de la Universidad Politécnica Salesiana con la interpretación de la información obtenida, dando a conocer cuáles son las principales amenazas internas y vulnerabilidades de la estructura, para la definición del riesgo de ataque en el entorno y los cambios a realizarse en temas de seguridad para la posterior aplicación de esta herramienta en la educación del grupo objetivo.

El capítulo 1 abarca la fundamentación teórica en la que se describen a los conceptos más importantes sobre seguridad de la información y la tecnología Honeynet, así como sus herramientas y modo de funcionamiento.

En el capítulo 2 se define la situación actual del Laboratorio de Redes de la Universidad Politécnica Salesiana, ubicado en el bloque C del Campus-Sur, que será el lugar en donde será implementado el prototipo propuesto.

En el capítulo 3 se documenta el diseño y la implementación del prototipo Honeynet, describiendo sus componentes de software y el hardware requerido.

Finalmente, en el capítulo 4 se muestran los resultados obtenidos en cuanto a las pruebas realizadas del prototipo Honeynet propuesto.

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

(Mifsud, 2012) y (Ventura & Rodriguez, 2008) mencionan en sus respectivos documentos, la importancia del conocimiento e interpretación de los siguientes conceptos referentes a la seguridad informática:

1.1 Seguridad

Se pueden desglosar dos tipos de seguridad:

- **Seguridad Lógica**

Es el uso de la criptografía y sus técnicas de encriptación para la protección de la información. Este tipo de seguridad se da en el propio medio.

- **Seguridad Física**

Se asocia a las precauciones físicas que se toman para evitar el robo o sustracción y daño (ya sean estos por: incendios, inundaciones, u otro tipo de calamidad) de los equipos y sistemas.

1.2 Seguridad de la Información

El concepto de seguridad de la información tendrá sentido solo si se protege un sistema o medio de información de personas sin autorización y cuyo fin sea su uso malicioso, su propagación indebida o su corte o destrozo total o parcial.

Dicha seguridad se liga a la ausencia de riesgo y la certeza. Se puede entender entonces como medio de información o sistema de información seguro, si este no presenta daño, peligro o amenaza alguna, cuando se tiene claro que un peligro es aquel que afecte directamente el correcto desempeño o funcionamiento de un determinado sistema o a la solución obtenida.

Se debe mencionar que la seguridad informática es una utopía dado que lograr una seguridad en un ciento por ciento no es posible. El factor de riesgo se encontrará perpetuamente concurrente, sin importar las diferentes seguridades o medidas que se

tome para garantizar la perfección de este modelo, es en donde entran en el tema los niveles de seguridad.

Un sistema será seguro si cumple con las siguientes cualidades o características:

1.2.1 Integridad

Al mencionar el termino de integridad, se alude a la fidelidad de los medios o de la información, entonces lo que se busca con la integridad es la prevención de transformaciones o cambios que no hayan sido previamente autorizados. Estas alteraciones pueden darse durante el proceso de envió del paquete o en el ordenador o dispositivo de origen del mismo.

Cuando un atacante o persona maliciosa no puede acceder directamente a la información contenida en algún paquete, es muy común que lo retenga o recoja y simplemente lo descarte.

1.2.2 Disponibilidad

Se refiere a que toda la información debe presentarse como accesible a todo aquel elemento y sistema que esté autorizado.

La información debe poder ser recuperada en cualquier lugar o momento que sea necesario, es decir, se debe tratar de que dicha información sufra de bloqueos, alteraciones o perdidas en cualquier situación, ya sean estas por mala operación o por motivos externos al operador.

1.2.3 Confidencialidad

La confidencialidad trata sobre el hecho de que la información solo debe darse a conocer a personas que tengan autorización para obtenerla. Determinada información debe mantenerse como secreta o ser oculta para el público en general.

Muchos de los ataques se encuentran encaminados hacia la privacidad. Los medios de transmisión pueden presentarse como susceptibles a estos ataques y mostrar falencias para que el atacante pueda copiar o interceptar paquetes de información.

1.3 Maneras comúnmente utilizadas para el ultraje de la seguridad de la información

Se considera como amenaza a todo acto o acción que, si se presentara la oportunidad, derive en la violación de la seguridad (disponibilidad, confidencialidad, integridad). Existen dos recursos que harán que las amenazas puedan ser resistidas o neutralizadas: El *análisis de riesgos* y las *políticas de seguridad*.

Los ataques o amenazas se pueden categorizar en cuatro formas que se describen enseguida:

- **Interrupción**: Se da cuando cualquier medio o recurso del medio o sistema, se torna como no disponible o es eliminado. Se le conoce como *Ataque a la disponibilidad*. En este tipo de ataque se destruyen los elementos de hardware del sistema. Este tipo de ataques se ilustra en la figura 1.1.a.

- **Intercepción**: Se da cuando un ente sin autorización, logra acceder o ingresa a un recurso: este tipo de ataque se conoce como *Ataque a la confidencialidad.* El atacante puede lograr acceder a la cabecera de los paquetes para recopilar información acerca de la identidad de los usuarios. Este tipo de ataques se ilustra en la figura 1.1.b.

- **Fabricación**: Conocido como *Ataque contra la Autenticidad*. Se da cuando un ente sin autorización, logra introducir elementos adulterados o falsificados en el medio. Este tipo de ataque se ilustra en la figura 1.1.c.

- **Modificación**: Se da cuando un ente sin autorización, logra cambiar o modificar la estructura de un archivo al que logro acceder. Este ataque es en contra de la *integridad.* El atacante puede hacer que un programa funcione de manera distinta a la inicial entre otros aspectos. Este tipo de ataque se ilustra en la figura 1.1.d.

Tráfico normal de información

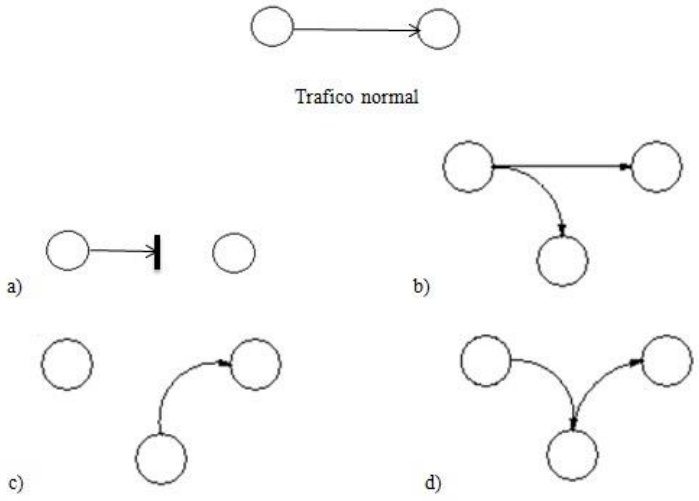


Figura 1.1. Trafico normal de información entre origen y destino e ilustración de posibles amenazas

Fuente: (Mifsud, 2012)

1.4 Tipos de Ataques a los Sistemas de Información

Los ataques pueden internarse en los sistemas informáticos con diferentes métodos y complejidad. Estos ataques pueden ser de dos tipos:

1.4.1 Ataques Pasivos

Este tipo de ataques buscan reunir la información para luego lanzar un ataque activo. Existe una gran probabilidad de nulidad para detectar los ataques pasivos. Entre estos ataques se encuentran:

- Sniffing
- Reuniendo Información.

1.4.2 Ataques Activos

Los ataques activos son premeditados y persiguen la obtención de la información. Se dice que son fáciles de detectar, pero la razón por la que las compañías u organizaciones a veces no lo consiguen, es porque ignoran que es lo que deben observar. Algunos de estos ataques son:

- Denegación de Servicios (DoS): Agotamiento de sus recursos como el ancho de banda, por ejemplo, para q no se puede acceder al servidor.
- Penetración.

1.5 “Honeypots” y “Honeynets”

Existen sistemas con enfoques muy creativos en comparación a los sistemas de seguridad convencionales con los cuales se puede monitorear e inventariar las acciones que realizan los atacantes en contra de algún sistema que lo requiera, en lugar de desecharlas y repelerlas.

1.5.1 Honeypot

Un honeypot, según lo mencionado en (Chavarri, 2015), es un sistema que se encarga de timar al intruso para poder analizar su labor y así instruirse con sus métodos. La instrucción básica es la de aprender del enemigo, para así lograr batallar contra él.

Estos sistemas están proyectados a copiar la conducta de un archivo, o sistema completo que puede despertar el interés de un usuario no autorizado o intruso, y la idea es que el atacante no pueda dañar la red ni pueda percatarse de dicho engaño. En la figura 1.2. se presenta una estructura de lo anteriormente mencionado.

Ejemplo de Arquitectura Honeypot

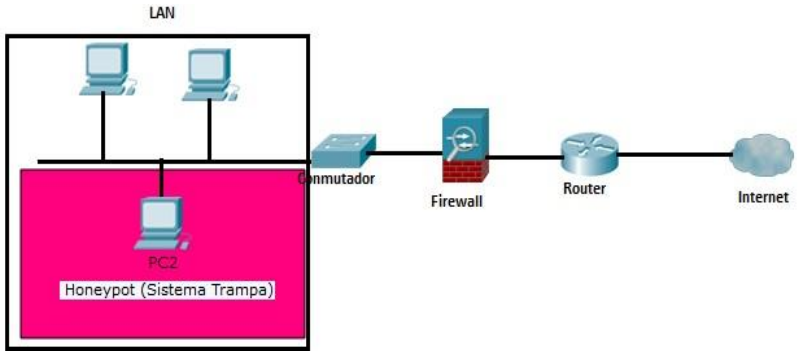


Figura 1.2. Ilustración de una arquitectura Honeypot

Fuente: (Gonzalez, 2003).

Por lo general estos sistemas se colocan después de un firewall o cortafuegos, en su línea trasera, sin que esto sea una regla. El firewall se programa de tal forma que permita la libre circulación del tráfico entrante, pero restringiendo las conexiones que salen del sistema.

A continuación en la tabla 1.1, se definen algunas de las ventajas y desventajas que presentan los honeypots.

Tabla 1.1. Comparativa de ventajas y desventajas de los Honeypots

Ventajas	***Desventajas***
Logran registrar una cantidad pequeña de información, pero de mucho valor. Reduce significativamente el número de falsos positivos y falsos negativos. Presenta un ahorro de recursos significativo al no necesitar un aumento en el ancho de banda ni múltiples dispositivos que realicen su tarea. Un solo ordenador puede ser usado para este trabajo. Registra los ataques que se hacen de IPV_6 utilizando túneles de IPV_4, que los IDS no logran registrar.	El sistema se vuelve obsoleto, en el caso de que un intruso logre identificarlo, pudiendo evadirlo y atacando la red de producción. Se puede atacar el sistema trampa o honeypot y se lo puede usar para atacar a la red, por lo que presenta un riesgo. Solo percibe los ataques que van destinados a él y no los que van destinados a otros recursos.

Fuente:(Ventura & Rodriguez, 2008)

Nota: Elaborado por Dennis Carcelén, Carlos Ríos

1.5.2 Honeynet

Las Honeynets o *Redes Trampa*, como se recopila y se manifiesta en el documento («Spanish Honeynet Project», s. f.), nacen a partir de la idea de mejorar los honeypots, por lo que se dice que son el desarrollo de estos, teniendo una alta interacción con los atacantes.

Este concepto fue recogido por el denominado "The Honeynet Project" el cual es un grupo u organización, no lucrativa. Esta organización se encuentra formada por entendidos y diestros en el tema de la seguridad de la información, encabezados por su fundador Lance Spitzner, y cuyo propósito es aprender lo más posible, sobre las tácticas, técnicas, mecanismos y motivos que pudieran tener los intrusos.

Una red trampa es entonces, un mecanismo o instrumento para la investigación. Es un conjunto de varias clases de honeypots que se fundamenta en ser diseñada para lograr atrapar y controlar, a través de un firewall, el tráfico que pasa por esta red, para ser expuesta ante los atacantes, y el consiguiente análisis del tráfico obtenido. Esto se hace para poder aprender sobre los métodos que son usados por dichos atacantes que han logrado comprometer la *Honeynet.*

Una Honeynet tiene muchas diferencias con un sistema trampa común y típico, entre las cuales se pueden citar las más sobresalientes:

- Una Honeynet posee equipos que actúan como honeypots, es decir la Honeynet no es un solo sistema trampa, es toda una red. Puede estar formada por sistemas Windows, Unix, Solaris, dispositivos Cisco (switches, routers, etc.). Lo que se busca hacer con esto es instaurar una infraestructura en la que además de tener sistemas reales, se tengan *servicios reales* como lo son HTTP, FTP, Web Server, correo electrónico, etc., lo que hará que el atacante se interne en este entorno controlado sin percatarse del propósito del mismo.
- Con las Honeynets, al ser estos sistemas de producción, se puede además implementar infraestructuras de iguales características que las originales, para así poder estudiar sobre los peligros y contingencias que se pudieran presentar en este tipo de entornos. Un servidor Apache que contenga una base de datos de tipo MySql y PHP, pueden ser un claro ejemplo de esto.

Para las Honeynets se han concretado tres tipos de infraestructuras en un nivel básico por parte de *The Honeynet Project*, los cuales son: GenI, GenII y la más reciente: GenIII.

Para el presente trabajo de titulación se hará uso de la arquitectura Honeynet de tercera generación.

1.5.3 GenIII (Honeynets de Tercera Generación)

Las Honeynets de tercera generación se empezaron a desarrollar en el año 2005 y permiten profundizar más aún en la captación de información y además mejorar el análisis de los datos obtenidos, adquiriendo avances sobre sus versiones anteriores. En este punto se debe mencionar a Sebek, el Honeynet más utilizado por el rendimiento que ofrece y por las soluciones de alta calidad que brinda. Todo esto se puede visualizar mejor en la ilustración de la figura 1.3.

Arquitectura Honeynet GenIII

Figura 1.3. Ejemplo de Arquitectura de Honeynet de Tercera Generación

Fuente: (Spitzner, s. f.)

En el documento de (Montalván, 2010), se manifiesta que para facilitar el estudio de los datos, las Honeynets GenIII muestran los subsistemas que se encuentran citados en la Tabla 1.2.

Tabla 1.2. Subsistemas en una Honeynet GenIII

SUBSISTEMAS	Control de Datos	Captura de Datos	Análisis de Datos
HERRAMIENTAS	Limitación de velocidad	FirewallD Logs	MySQL
	Iptables	p0f	Walleye
	NIDS Snort en línea	Hpots Sebek	Argus+Hflow
		Alertas Snort	Swatch (alertas)
		Tcpdump	

Fuente: (Montalván, 2010)

Nota: Elaborado por Dennis Carcelén, Carlos Ríos

- **Control de Datos**

El fin de este subsistema es la comprobación de las acciones que el intruso puede realizar tanto en la entrada como en la salida de la Honeynet para poder limitar la información que puede salir del sistema Honeynet y poder permitir intencionalmente la entrada de los datos hacia la Honeynet.

Con el uso de las IPTables es posible la realización de lo anteriormente mencionado ya que entre las funciones de este tipo de firewall para Linux, se encuentran la demarcación de conexiones entrantes y salientes y el mecanismo de traducción de direcciones de red (NAT).

Lo que se debe hacer es la configuración de las IPTables para que actúen como filtradores de conexiones en la maquina física o HostOS, haciendo que se realice un conteo de los paquetes salientes para que cuando se logre alcanzar un numero predeterminado de enlaces salientes, el siguiente intento de conexión sea bloqueado para evitar que algún honeypot que haya logrado llegar a estar vulnerable, comprometa a los demás.

The Honeynet Project implementó un archivo tipo script para favorecer la implementación de las mencionadas IPTables. Este archivo es denominado ***rc.firewall*** el cual deberá ser rectificado en ciertas variables según las necesidades de cada Honeynet para su funcionamiento y posterior ejecución.

En el Honeynet GenIII se trabaja con Honeywall el cual será el gateway con su operatividad en modo *puente* de capa dos ("*layer two bridging mode*") por lo que no existirá enrutamiento ni tampoco disminuirá en TTL (tiempo de vida) de los paquetes, haciendo que se torne como un dispositivo filtrante casi invisible para los intrusos.

Las herramientas para el control de datos se listan a continuación:

- IPTables (limitación de paquetes y/o tráfico de red)
- Snort Inline (manejo de paquetes de red)
- Bridge de capa 2 (Honeywall).

- **Captura de Datos**

Es una de las partes fundamentales en el esquema Honeynet, ya que se trata de obtener la información sobre la actividad que el atacante se encuentra realizando en el sistema tratando de mermar las posibilidades de percepción sobre el accionar de la Honeynet y del administrador.

La actividad del intruso se logra registrar por medio de diferentes herramientas.

- El accionar del firewall para la manipulación y registro de las conexiones entrantes y salientes en la localidad /var/log/messages.
- El NIDS Snort tiene por defecto, un procedimiento para registrar las acciones suscitadas en la red además de capturar la información que contienen los paquetes que transitan por la interfaz de red contenida internamente (por defecto eth1) incluyendo también a toda el movimiento presentado por Sebek.
- Otra herramienta de Snort se encarga de monitorear la interfaz interna y después desplegar los avisos o alarmas IDS en dos modalidades: full y fast. Las actividades registradas tanto por Snort como por Snort in-line estarán almacenadas en la localidad de archivos/var/log/snort/$DAY.

La configuración manual de Sebek debe darse en las opciones de registro, es decir configurar a donde (dirección IP y puerto) se deben enviar los registros por parte de los clientes de Sebek. También se debe indicar si todos los paquetes generados en Sebek, deberán ser registrados por el firewall.

La generación automática de alertas cuando el sistema haya sido vulnerado es otra de las características de la captura de datos.

Las herramientas para la captura de datos con su descripción, se listan a continuación:

- FirewallD (logs de FirewallD)
- pOf (Identificación pasiva del Sistema Operativo)
- Hpots Sebek (captura, a un grado mayor, de datos)
- Tcpdump (captura del tráfico en la red)
- Alertas Snort (alertas IDS).

- **Análisis de Datos**

Una mejoría totalmente notable en comparación con las arquitecturas de GenI y GenII, se presenta para las Honeynets de GenIII para un correcto análisis de los datos recopilados.

La capacidad de poder examinar dichos datos en base a una búsqueda más minuciosa, dado que se puede indagar un dato por su fecha de creación, dirección IP, puerto de conexión y/o tiempo, se puede visualizar en la interfaz GUI de Walleye, y posteriormente estos archivos pueden ser arrojados como un fichero o archivo PCAP (interfaz de una aplicación de programación para captura de paquetes) o en la interfaz "Walleye Flow View" para que con el uso de alguna herramienta de análisis de trafico de red, como pudiera ser Wireshark, lograr la deducción y estudio de los datos obtenidos.

Las herramientas para el análisis de datos se listan a continuación:

- MySQL (Base de datos de la Honeynet para su recaudación).
- Walleye (Interfaz gráfica para el usuario).
- Argus + Hflow (Análisis del flujo del tráfico de la red, recolección de datos)
- Swatch (Logs de Firewall, alertas del sistema de detección de intrusos IDS).

CAPÍTULO 2

ESTADO ACTUAL

La Sede Quito de la Universidad Politécnica Salesiana, está conformada por 3 campus: Campus El Girón ubicado en la Av. 12 de Octubre 2422 y Wilson, el Campus Kennedy ubicado en la Av. Rafael Bustamante s/n, y el Campus Sur que se encuentra ubicado en el sector de Chillogallo, en la Av. Rumichaca y Av. Moran Valverde s/n.

Ubicación de la UPS Sede Quito-Campus Sur

Figura 2.1. Foto Aérea del Campus Sur de la UPS Sede Quito Campus Sur y su distribución de bloques

Fuente: (Borja & Jarrin, 2015)

2.1 Descripción de las Edificaciones Principales del Campus Sur

El campus Sur se encuentra distribuido en 9 bloques de edificios, nombrados para su fácil identificación desde la letra A hasta la letra I. El edificio correspondiente al bloque G, está en las etapas finales de construcción y se espera la pronta entrega de la obra concluida.

Cada bloque posee su respectiva infraestructura tecnológica, misma que permite las comunicaciones así como la transmisión de datos desde y hacia cada una de las dependencias que funcionan en cada uno de ellos. Esta infraestructura se encuentra interconectada con los otros bloques y de ellos hacia el centro de datos ubicado en el bloque A. A continuación se realiza una breve descripción, de acuerdo al documento redactado por (Moreno & Tipán, 2015), del equipamiento existente en cada bloque:

- **Bloque A**

Este bloque posee cinco pisos y una planta baja. Este edificio posee además áreas de: centro de cómputo e informática, que posee un *Marco de Distribución Principal o MDF*; un área para el departamento financiero y administrativo y para vicerrectorado, dicha área posee dos *Marcos de Distribución Secundarios o SDF;* un área para la biblioteca, en el que se ubica un Marco de Distribución Secundario, y un área que funciona como Centro de Capacitación y Servicios Informáticos o CECASIS y que dispone de un *distribuidor intermedio o IDF*. En este edificio se disponen los cuartos de comunicaciones que se encuentran en las áreas de la sala de profesores y la biblioteca, además de los pisos tres y cuatro.

- **Bloque B**

Este bloque está constituido por dos pisos y posee áreas de secretaria, direcciones de carrera, salas de profesores, pastoral y bienestar estudiantil. También se encuentra ya en funcionamiento la nueva área que corresponde al espacio de coworking de la institución denominado como StartUPS, con distribuciones de *SDF* nombradas como SDF-BB-P1-2, SDF-BF-P1 y SDF-BB-PB respectivamente. En este edificio se encuentra situado un rack de pared, ubicado en el primer piso, en la sala de profesores específicamente.

- **Bloque C**

Este bloque está construido con dos pisos en los que se ubica un rack de pared en la actual sala de profesores. Este edificio cuenta con áreas para laboratorios de electrónica y sala de profesores, en donde se ubica un *SDF* nombrado como SDF-C-P1, y con áreas para laboratorios de física.

- **Bloque D**

Este edificio posee dos pisos. En el primer piso está situado el rack de pared para este bloque, específicamente en el laboratorio 3 de la academia CISCO. Este bloque posee un *SDF* denominado como SDF-D-PB para los departamentos de Cisco, Academia SUN y Auditorio.

- **Bloque E**

El bloque E está construido con un solo piso en el cual se sitúa un rack de pared que funciona en el área del laboratorio de Suelos con un *SDF* denominado como SDF-E-PB.

- **Bloque F**

Este edificio está construido con una planta baja y un piso en el cual se sitúan las áreas para los laboratorios y aulas de clase para Ingeniería Ambiental. En el primer piso se sitúa el rack de pared de este bloque con un SDF denominado como SDF-F-PB para el cuarto de comunicación.

- **Bloque H**

En este bloque se encuentra ubicada la nueva área correspondiente a los laboratorios de Ingeniería Eléctrica en conjunto con su sala de profesores y está construido con un único piso con un SDF denominado como SDF-H-PB para el cuarto de comunicación.

- **Bloque I**

En este nuevo bloque, donde antes funcionaba la cafetería, se encuentran ubicados los laboratorios correspondientes a la carrera de Ingeniería Mecánica junto con un área para la sala de profesores. Está construido en un único piso con un SDF denominado como SDF-I-PB.

- **Bloque G**

Este bloque se encuentra ubicada la nueva cafetería además de un nuevo auditorio. Posee un IDF que está conectado a través de fibra óptica a un switch cisco 3750.

2.2 Levantamiento

Para una correcta caracterización de los equipos y seguridades presentes en el campus, y para poder desarrollar de manera sistemática el diseño de la Honeynet, se realiza la descripción de su topología física y también lógica.

2.1.1 Topología Física

En el edificio primario del Campus, denominado como Bloque A, se encuentra situado el Data Center, específicamente en el piso número seis. Aquí existen los equipos de networking que se usan para la implementación de la red funcional de la universidad, en dicho campus (Mena & Jara, 2013).

Los equipos que se utilizan son los siguientes:

- Routers de Core
- Switch Core
- Switch de Distribución
- 2 Servidores
- WLAN Controller.

En este punto se debe mencionar que la Universidad en su sede Quito cuenta con dos proveedores de servicios o ISP, los cuales son CNT y TELCONET, para disponer de enlaces redundantes desde el Campus central de esta sede (Campus Girón), los cuales en conjunto, proveen los servicios de internet, voz y datos. Este esquema se encuentra representado en la figura 2.2.

Topología Física Red del laboratorio de Redes de la UPS Sede Quito Campus-Sur

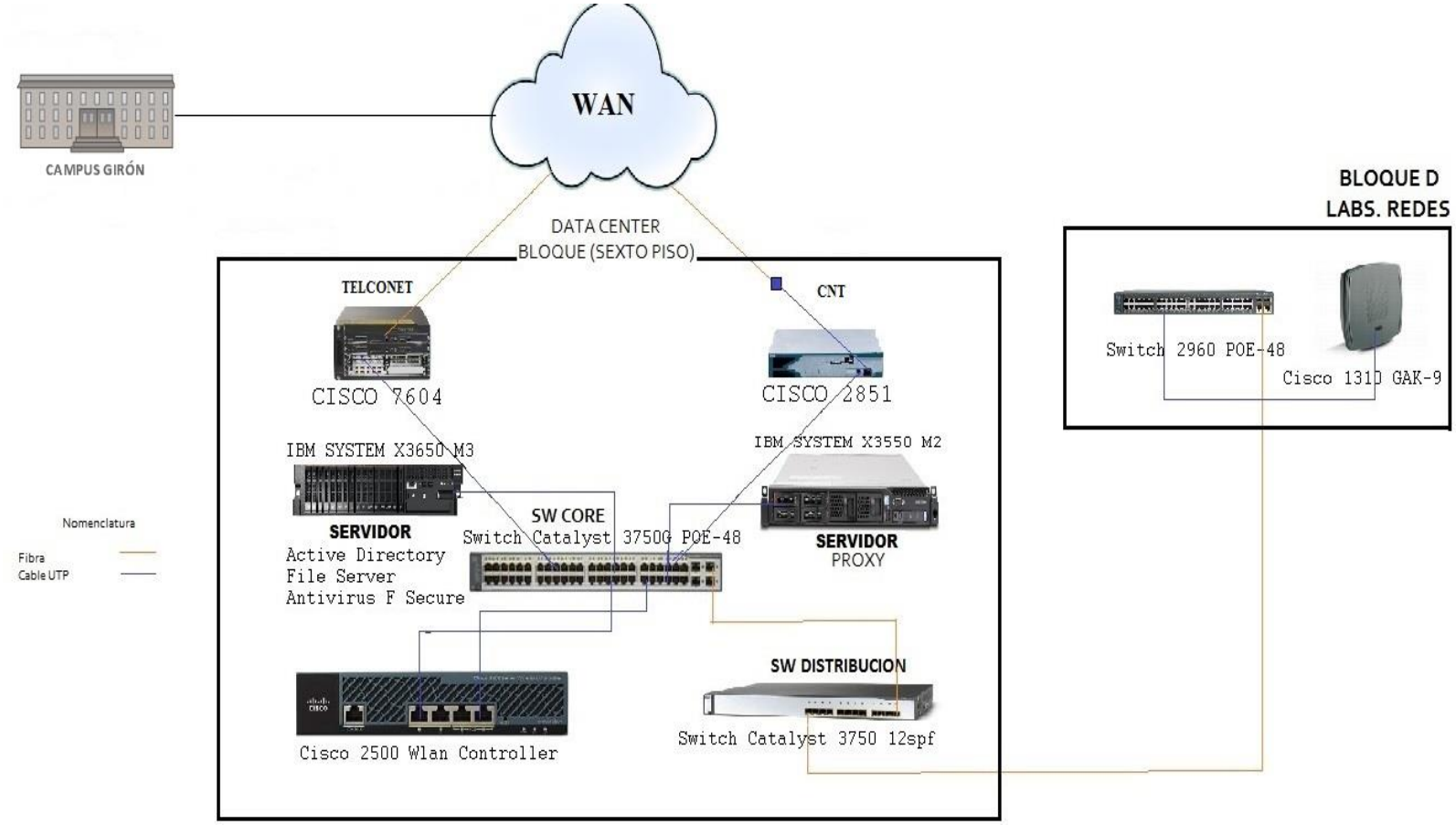


Figura 2.2. Infraestructura de la Topología Física del laboratorio de Redes de la UPS Sede Quito Campus-Sur

Elaborado por: Dennis Carcelén, Carlos Ríos

2.1.1.1 Equipos de Conectividad

En los documento de (Mena & Jara, 2013) y (Moreno & Tipán, 2015), se menciona el uso de los siguientes dispositivos en la Red Institucional:

- **Router de CNT**

Se usa un transceiver o transformador de fibra óptica a cable UTP, para acoplarse con el equipo Cisco 2851, ilustrado en la figura 2.3, el cual provee un único servicio de datos.

Equipo Cisco 2851

Figura 2.4. Imagen del Router Cisco 2851

Fuente: («Cisco 2851 Integrated Services Router - Cisco», s. f.).

Características:

- Anchura 43.8 cm
- Profundidad 41.7 cm
- Altura 8.9 cm
- Peso 11.4 kg
- Memoria RAM 256 MB (instalados) / 1 GB (máx.) - SDRAM
- Memoria Flash 64 MB (instalados) / 256 MB (máx.)
- Conexión de redes
- Tecnología de conectividad: Cableado
- Protocolo de interconexión de datos Ethernet, Fast Ethernet, Gigabit Ethernet
- Red / Protocolo de transporte IPSec

- Protocolo de gestión remota SNMP 3, entre otras («CISCO 2851 Integrated Services Router - CISCO2851 : Almacen Informatico», s. f.).

- **Router de Telconet**

Se emplea un equipo de marca Cisco, modelo 7604, el cual se visualiza en la Figura 2.4, con el que se provee los servicios de Internet, datos y voz mediante fibra óptica.

Equipo Cisco 7604

Figura 2.5. Imagen del router Cisco 7604

Fuente: («Cisco 7604 Chassis Data Sheet - Cisco», s. f.)

Características:

- Dos modos de configuración: Un motor de supervisor único y un máximo de tres tarjetas de línea, o motores de doble supervisor y un máximo de dos tarjetas de línea de alta disponibilidad y redundancia.
- Adaptadores modulares de puerto que son intercambiables en todas las plataformas de enrutamiento de Cisco
- Tasa de transmisión de hasta 144 Mbps de distribución y 320 Gbps de rendimiento total, proporciona un rendimiento y fiabilidad con opciones para los procesadores de rutas y fuentes de alimentación redundantes («UltimaTecnología » ranura», s. f.).

- **Switch de Core**

Se emplea un switch de 48 puertos de marca Cisco Catalyst 3750G PoE, ilustrado en la Figura 2.5, con 4 interfaces ópticas. Todos los dispositivos convergen en este dispositivo por lo que es muy importante para la utilización en la comunicación de la red.

Equipo Cisco Catalyst 3750G PoE

Figura 2.6. Imagen switch Cisco Catalyst 3750G PoE

Fuente: («Cisco Catalyst 3750 Series - Netsource GlobalNetsource Global», s. f.).

El Campus Sur de la Universidad, presenta una administración de su red mediante el uso de VLAN's para su segmentación del tráfico según los sectores de trabajo distribuidos de la siguiente manera:

- VLAN-WLAN-IPCAM-ELECTRONICA
- VLAN SALA-INTERNET
- VLAN ADMINISTRATIVA
- VLAN CISCO
- VLAN SUN
- VLAN SALA-CECACIS
- VLANHP
- VLAN SALAPROF
- VLAN SALA-CECACIS
- VLAN CECASIS
- VLAN de VIDEO
- VLAN ELECTRONICA

- VLAN-TELCONET
- VLAN-IPCAM-CECASIS.

- **Switch de Distribución**

Se emplea un switch funcional, a través de fibra óptica, de marca Cisco Catalyst 3750G 12-SPF, el cual se puede visualizar en la Figura 2.6, ubicado en el data center del Campus denominado como Bloque A. Este switch posibilita la conexión entre el Core Switch y el switch de IDF o de acceso que están en los diferentes bloques de la sede Quito-Campus Sur.

Cisco Catalyst 3750G 12-SPF

Figura 2.7. Imagen del switch Cisco Catalyst 3750G 12-SPF

Fuente: («Cisco Catalyst 3750 Series Switches Data Sheet - Cisco», s. f.).

- **Switches de Acceso**

El modelo que se usa es un Cisco Catalyst 3750G POE-24/48P, cuya imagen se puede observar en la Figura 2.7., para el acceso a las diferentes áreas en el campus. Dichas áreas se listan a continuación:

- Departamento administrativo
- Biblioteca (Bloque A)
- Cecasis (Bloque A)
- Secretaria (Bloque B)
- Laboratorios de Electrónica (Bloque C)
- Auditorio (Laboratorio de Redes)
- Laboratorio de suelos
- Ambiental (Bloque F)

- Bloque H
- Bloque G

Cisco Catalyst 3750G POE-24/48P

Figura 2.8. Imagen del switch Cisco Catalyst 3750G PoE-24/48P

Fuente: («Cisco Catalyst 3750-48PS Switch - Cisco», s. f.)

Para el actual trabajo de titulación, compete el estado actual del bloque D denominado como auditorio y en específico los laboratorios de redes de comunicaciones ubicados en este sitio.

- Auditorio: Esta zona es usada por parte de los educadores, personal encargado y estudiantes. Un Cisco Catalyst 3750G POE-48P es el switch utilizado en este punto y se encuentra ubicado en una de las aulas de la Academia Cisco.

  La función de este switch es la de enlazar la red LAN para las zonas de trabajo de los laboratorios de las academias CISCO (laboratorios de redes de comunicaciones) y SUN. También conecta el Access Point de marca Cisco 1131-A que proporciona servicio de internet Wi-Fi al bloque D del campus.

- **Wlan Controller**

Utilizado para la administración y el control de las antenas que se encuentran en las áreas externas a los edificios y bloques, dentro del campus, además de los Access Points. El modelo usado es un Cisco 2500, el cual se puede visualizar en la Figura 2.8., que se conecta al Core Switch en el data center a través de un enlace redundante con cable Ethernet.

Wlan Controller Cisco 2500

Figura 2.9. Imagen del WLAN Controller Cisco 2500

Fuente: («Cisco 2500 Series Wireless Controllers - Cisco 2500 Series Wireless Controllers - Cisco», s. f.).

Características:

- Diseñado para pequeñas y medianas redes y sucursales políticas de seguridad centralizadas para detectar puntos de acceso no autorizados y proteger contra ataques de denegación de servicio
- Capa 2 y Capa 3 la movilidad y la calidad de servicio para voz y video el acceso de alta seguridad inalámbrico para invitados
- La tecnología integrada de Cisco CleanAir para una auto-curación , red de auto - optimización que evita la interferencia de RF (Preguntas Frecuentes sobre el Diseño y las Funciones de Wireless LAN Controller (WLC), 2008).

Se debe mencionar que la salida hacia el internet en el campus se da por medio de CEDIA TELCONET. Este enlace está provisto de un ancho de banda de 162.5 Mbps, haciendo notar que el enlace existente entre los Campus Sur y Girón son netamente de datos con un ancho de banda de 6 Mbps y es provisto por los proveedores de servicio TELCONET y CNT como se mencionó anteriormente en el presente capítulo.

2.1.1.2 Servidores

- **Equipo IBM System X3650 M3**

En este equipo se encuentran alojados los servidores de Active Directory, File Server y el Antivirus F-Secure.

- **Equipo IBM System X3550 M2**

En este equipo se encuentra alojado el servidor Proxy de la Institución.

2.2.1 Topología Lógica

La red de la Universidad está diseñada con una topología de tipo estrella extendida como se muestra en la Figura 2.9., para así brindar características jerárquicas a la red, como mencionan (Mena & Jara, 2013), en la que los switches de acceso convergen todos hacia el switch de Core, por el que pasaran todos los paquetes para la comunicación de los distintos bloques del Campus y que esta se mantenga de forma local.

Topología Lógica de Red del Laboratorio de Redes de la UPS Sede Quito Campus-Sur

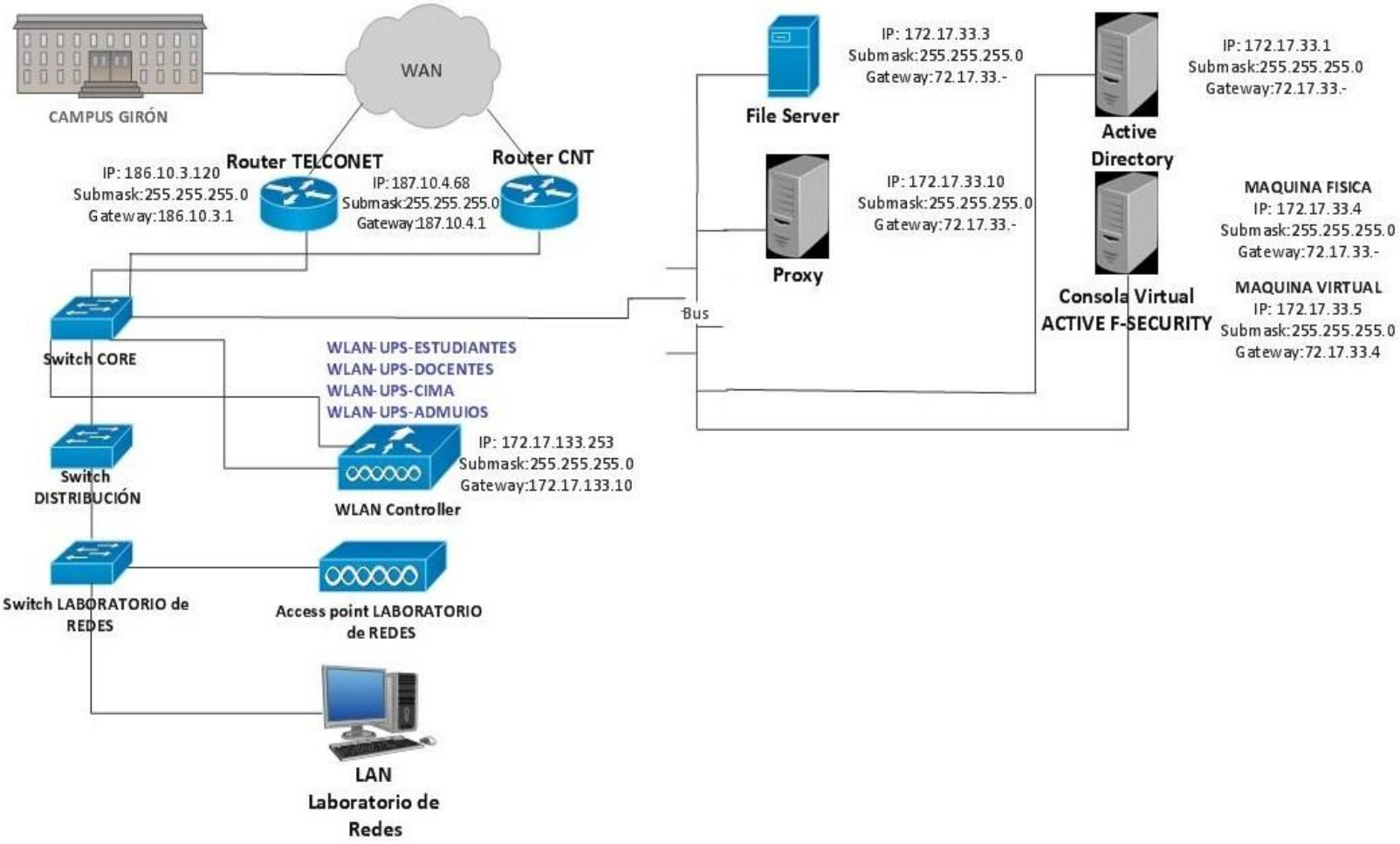


Figura 2.10. Infraestructura de la Topología Lógica de la Red UPS Sede Quito Campus-Sur

Elaborado por: Dennis Carcelén y Carlos Ríos

2.2.2.1 Direccionamiento Lógico

Después de analizar el documento de (Moreno & Tipán, 2015), en esta sección se detallan las direcciones de cada dispositivo y aplicaciones o servicios de la topología ilustrada en la figura anterior.

- **Routers**

El router del proveedor de servicios CNT posee la IP Address: 187.10.4.68, una máscara de red de 255.255.255.0 y su Gateway es: 186.10.3.1/24.
El router de la empresa TELCONET posee la IP Address: 187.10.4.68, una máscara de red de 255.255.255.0 y su Gateway es la: 187.10.4.1/24.

- **Servidores**

En el campus sur de la sede Quito de la Universidad se tienen los siguientes servicios

- **Active Directory:** Establecido en el equipo **IBM SYSTEM X335 M2.** Este servicio tiene la IP Address: 172.17.33.1, la submáscara es la: 255.255.255.0 y su puerta de enlace es la 172.17.33.10.
- **F-Secure Server:** Este servidor está establecido en el equipo **IBM SYSTEM X335 M2** en una máquina virtual. El equipo de la marca IBM (física) tiene la IP Address: 172.17.33.4, la submáscara de red es: 255.255.255.0 y el Gateway tiene la dirección: 172.17.33.10.

  El server con el antivirus se establece con la dirección IP: 172.17.33.5, con una submáscara de: 255.255.255.0, con una puerta de enlace de: 172.17.33.4
- **Proxy:** El servidor proxy está instalado en el equipo IBM SYSTEM X335 M2 puesto en funcionamiento con una dirección IP: 172.17.33.10, con una submáscara de red: 255.255.255.0 y su puerta de enlace es la 186.10.3.120.
- **File Server:** Este servicio se encuentra instalado en el equipo **IBM SYSTEM X335 M2**. Tiene la siguiente dirección IP: 172.17.33.3, con una submáscara de red de: 255.255.255.0 y la dirección de la puerta de enlace es: 172.17.33.10.

- **WLAN Controller**

Este equipo se utiliza para dirigir o controlar todos los Access Point y antenas Wi-Fi externas que están en las diferentes partes del campus Sur de la Universidad. A este equipo se le ha asignado la siguiente IP Address: 172.17.133.253, posee una sub máscara de red de: 255.255.255.0 y la dirección de Gateway es la: 186.10.3.1.

Al estar conectados todos los access points y las antenas externas al controlador de redes LAN inalámbricas, estas se comportarán como repetidoras por lo que tendrán las configuraciones y todas las redes inalámbricas que se establezcan en el dispositivo controlador.

Las redes inalámbricas administradas por el controlador se listan a continuación:

- WLAN-UPS-DOCENTES: Es la red LAN inalámbrica asignada a los educadores. Está en el rango de direcciones que inicia con: 172.17.131.0, con una máscara de: 255.255.254.0 y su Gateway es la: 172.17.131.254.
- WLAN-UPS-ADMUIOS: Es la red LAN inalámbrica asignada para el personal administrativo de la Universidad. Está en el rango de direcciones IP que inicia con: 172.17.34.0, con una máscara de 255.255.255.0 y su puerta de enlace o Gateway es la: 172.17.34.254.
- WLAN-ESTUDIANTES: Es la red LAN inalámbrica asignada a los estudiantes. Su rango de direcciones IP se encuentra en: 172.17.49.0 con una máscara de red de: 255.255.254.0 y su Gateway con la dirección: 172.17.49.254.
- WLAN-CIMA: Es la red LAN inalámbrica asignada para el Centro de Investigación en Modelamiento Ambiental o CIMA. El rango de direcciones usado es el: 172.17.128.0, posee una máscara de red de 255.255.255.192 y su Gateway es la: 172.17.128.62.
- WLC-BIBLIOTECA: Usada por los dispositivos de alquiler que se encuentren en la biblioteca. Se configura el WLAN Controller para que la SSID de este enlace LAN inalámbrico permanezca oculto. Su rango de direcciones IP se encuentra en: 172.17.41.0 con una máscara de red de: 255.255.255.192 y su Gateway con la dirección: 172.17.41.126. Lo anteriormente descrito, se visualiza en la Tabla 2.1.

Tabla 2.1. Direccionamiento de las Redes LAN Inalámbricas

NOMBRE DE RED (SSID)	RANGO DE DIRECCIONES IP	MÁSCARADE RED	PUERTA DE ENLACE (GATEWAY)	PROXY
WLAN-UPS-DOCENTES	172.17.131.0	255.255.254.0	172.17.131.254	172.17.33.10
WLAN-UPS-ADMUIOS	172.17.34.0	255.255.255.0	172.17.34.254	172.17.33.10
WLAN-UPS-ESTUDIANTES	172.17.49.0	255.255.254.0	172.17.49.254	172.17.33.10
WLAN-CIMA	172.17.128.0	255.255.255.192	172.17.128.62	172.17.33.10
WLAN-BIBLIOTECA	172.17.41.0	255.255.255.192	172.17.41.126	172.17.33.10

Fuente:(Mena & Jara, 2013)

Nota: Elaborado por Dennis Carcelén, Carlos Ríos

2.2.2 Servicios Web de la Universidad

La Universidad Politécnica Salesiana Sede Quito Campus Sur usa los siguientes servicios y aplicaciones:

- **Correo Electrónico Institucional**

La institución cuenta con el servicio de correo electrónico para el cual utiliza el servicio de datos prestado por la Compañía Nacional de Telecomunicaciones CNT. Este servicio es dado a través de Microsoft Exchange Server.

- **F-Secure**

Este antivirus se encuentra puesto en funcionamiento en una máquina virtual dispuesta en VMWare que se distribuye a toda la disposición del campus.

- **Página Web Institucional**

Esta página es la tarjeta de presentación de la Universidad. Es administrada desde la Sede de la Universidad ubicada en Cuenca, Campus "El Vecino". Este servicio usa las prestaciones dadas por la empresa TELCONET y brinda beneficios tanto para alumnos, docentes, aspirantes y público en general. El dominio de la página está dado por: www.ups.edu.ec.

- Servicios Académicos y Financieros

La sede cuenta también gestiona los siguientes servicios:

- AVAC: Es el Ambiente Virtual de Aprendizaje Cooperativo de la Universidad Politécnica Salesiana. Es usado por los estudiantes y docentes de la Universidad, para la realización de tareas, retroalimentaciones de los profesores acerca de estas, información sobre calificaciones, noticias, etc. También para el uso de foros estudiantiles. Está basado en Oracle.
- SNA: Es el Sistema de Nacional Académico y se usa por parte del personal docente y administrativo, para el registro y acceso de la información académica y detalles de los estudiantes.
- SIGAC: Es el medio de contabilidad para el registro de abonos, pagos, retribuciones y demás que se hace por parte de todo el personal de la Universidad. Su uso se remite únicamente al personal administrativo.
- SQUAD: Usado para el registro del talento humano que labora en la Universidad.

Todos estos servicios usan las prestaciones de la Corporación Nacional de Telecomunicaciones o CNT, los cuales hacen que el campus Sur se enlace con el Campus Girón y estos tengan comunicación con la Sede ubicada en Cuenca.

El servicio de Internet usa las prestaciones del proveedor de servicios TELCONET, el cual está dado por medio de un servidor Proxy ubicado en el Campus Central de la Universidad en la sede Quito, el cual es el Campus Girón. Se gestiona este servicio desde el campus Sur a través de una conexión basada en SSH.

El resumen de todos los servicios listados, se puede visualizar en la Tabla 2.2.

Tabla 2.2. Servicios Web de la Universidad

SERVICIO	DESCRIPCIÓN	GRUPO DE INTERÉS
PAGINA WEB	Información General de la Universidad. Brinda acceso a servicios como el AVAC, etc.	Estudiantes, Educadores, Administrativos y CIMA
F-SECURE	Servicio de Antivirus con actualizaciones periódicas vía web	Estudiantes, Educadores, Administrativos y CIMA
CORREO INSTITUCIONAL	Correo Electrónico por medio de Microsoft Exchange	Educadores, Administrativos y CIMA
AVAC	Sistema de Aulas Virtuales	Estudiantes, Educadores, Administrativos y CIMA y público en general
SNA	Historial Académico e información general estudiantil	Educadores, Administrativos
SIGAC	Sistema contable con registro de pagos y transacciones monetarias.	Personal Administrativo
SQUAD	Información sobre talento Humano docente y administrativo de la Universidad	Personal Administrativo
INTERNET	Servicios Web y VoIP	Estudiantes, Docentes, Administrativos y CIMA

Fuente:(Mena & Jara, 2013)

Nota: Elaborado por Dennis Carcelén, Carlos Ríos

2.2.3 Seguridades

En el Regulador de Wireless Cisco se encuentran configurados dos protocolos que proporcionan seguridad a los enlaces inalámbricos dentro del campus:

- **Protocolo LWAPP**

Es el Protocolo Ligero para Puntos de Acceso, que es usado para centralizar el manejo de un conjunto de puntos de acceso en una red WLAN, trayendo una serie de beneficios entre el que destaca el ahorro del tiempo de gestión y supervisión de los puntos de acceso.

- **Protocolo CAPWAP**

El Protocolo de Control y Aprovisionamiento de Puntos de Acceso Inalámbricos, es un protocolo que se basa en su antecesor LWAPP, que además de ser estándar, es interoperable, lo que quiere decir que se puede intercambiar información y utilizar dicha información entre sistemas, sin ningún impedimento. Permite así, el manejo y administración de los Access Points de una red WLAN.

Los usuarios de la red de Administración, CIMA, docentes y Estudiantes tienen acceso mediante la autenticación por portal cautivo.

- **Firewall**

La seguridad a profundidad con la que cuenta la institución consta de un firewall ASA (Adaptive Security Appliance) de cisco además de una lista de control de acceso o ACL.

- **Grupo de Interés**

El campus Sur cuenta con casi 4000 usuarios, en cuanto al grupo de interés, por cuanto se realiza además una caracterización en el capítulo 3 del pseudo-perfil de estos usuarios, para determinar su comportamiento y uso de la red de la Institución.

CAPÍTULO 3

DISEÑO E IMPLEMENTACIÓN

3.1 Auditoría para la identificación de las vulnerabilidades en los servicios web de la Universidad Politécnica Salesiana

Con el fin del conocimiento del estado, en cuanto a integridad y disponibilidad, de los servicios web prestados en la red de la institución, se realiza la auditoria de las aplicaciones instituciones como son su página oficial y el Ambiente Virtual de Aprendizaje Cooperativo *AVAC*.

Con este proceso y la información obtenida se puede proponer los procedimientos correctos a realizar para la debida corrección de los errores encontrados.

- **Herramienta utilizada para la auditoría**

Al investigar sobre las herramientas de escaneo de vulnerabilidades, se encontró que Vega es una de las mejores, dado que al ser automatizada, permite al *pentester (Penetration Tester*) o auditor de seguridad, hallar las falencias en los códigos ejecutados en las aplicaciones web, ejecutándola en su modo de escaneo, presentado una interfaz GUI muy instintiva. Además de esto, esta herramienta es de código abierto y multiplataforma, anteponiéndose a las mecanismos de pago o comerciales.

Vega también permite, en su modo proxy, la intercepción de paquetes. Si se requiere visualizar el grado de riesgo que implica para la aplicación web, poseer una vulnerabilidad, Vega informa sobre este hecho, presentando las vulnerabilidades obtenidas con un nivel de criticidad, para su correcto y oportuno tratamiento.

Para hacer un correcto uso de esta herramienta, se debe tener en cuenta que el análisis que se debe realizar después de la obtención de los datos, debe ser minucioso debido a los posibles falsos positivos que se pudieran presentar.

- **Procedimiento**

La auditoría del sitio web de la Universidad Politécnica Salesiana, se la realiza en la herramienta Vega, escribiendo el nombre de dominio de la página ups.edu.ec o su URL, cuando ya se haya seleccionado la opción de *Start New Scan* en la interfaz GUI de Vega, como se muestra en la Figura 3.1.

Interfaz de usuario de Vega

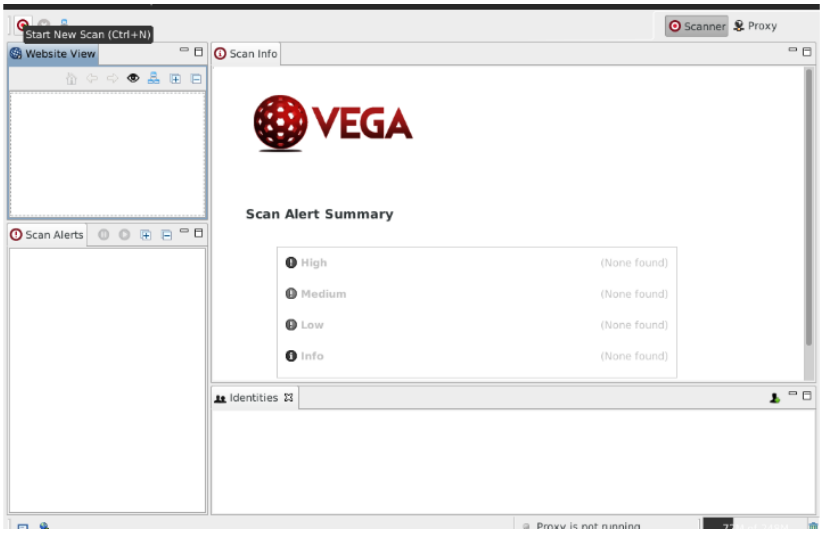


Figura 3.1. Interfaz GUI de la Herramienta de Auditoria Web Vega

Elaborado por: Dennis Carcelén y Carlos Ríos

- **Resultados obtenidos en la Auditoria Web**

En la Figura 3.2. se observa que en la dirección web de la universidad existen problemas de alto riesgo, pero también de mediano riesgo, que necesitan tratamiento oportuno para evitar el comprometimiento por parte de un intruso en la red.

Auditoria web a la Universidad Politécnica Salesiana

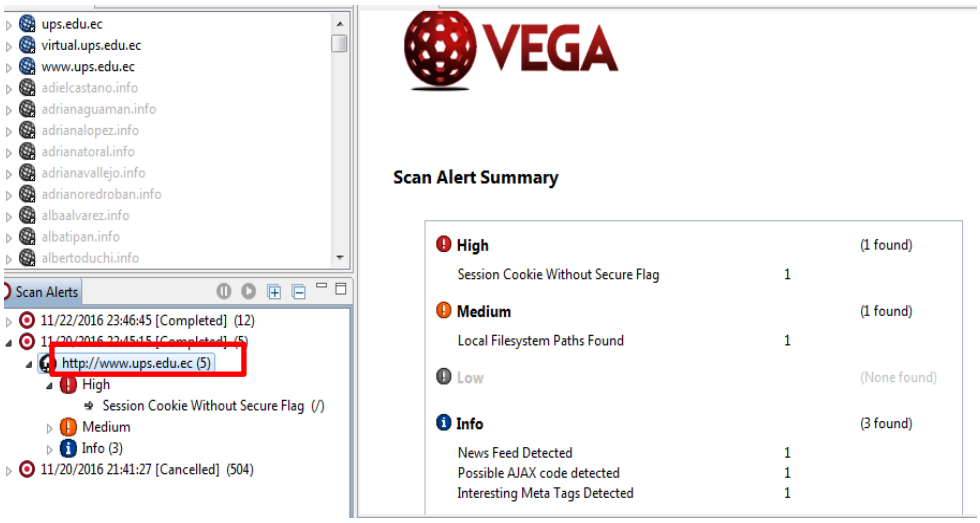


Figura 3.2. Resultados obtenidos de la Auditoría realizada a la aplicación web de la UPS

Elaborado por: Dennis Carcelén y Carlos Ríos

La mayor vulnerabilidad captada por la herramienta utilizada, es una de tipo *Session Cookie Without Secure Flag* (Cookie de Sesión Sin Bandera Segura). Este tipo de riesgos exponen a la red a escuchas externas. Al ser dichas *cookies* credenciales de autenticación, los atacantes que los obtengan pueden obtener acceso no autorizado a las aplicaciones web que se encuentren afectadas. En la Figura 3.3. se muestra el resultado de esta auditoría.

Vulnerabilidad de Alto Riesgo Detectada

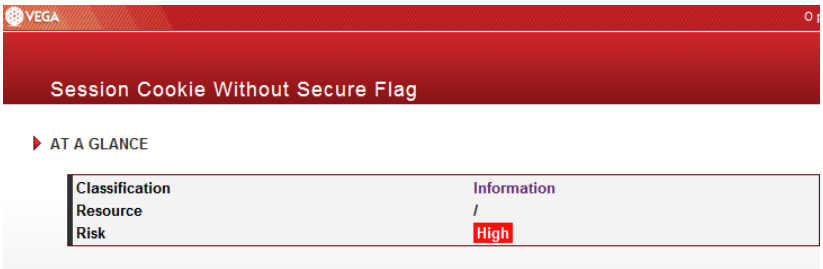


Figura 3.3. Vulnerabilidad de Alto Riesgo Sujeta a Análisis

Elaborado por: Dennis Carcelén y Carlos Ríos

Al analizar la petición que se realizó para obtener el registro de vulnerabilidad, se encontró la línea de código en la que se encontraría el problema y a la cual se deberá apuntar la posible solución. Lo descrito se observa en la Figura 3.4.

Análisis de riesgos encontrados en el sitio web de la Universidad Politécnica Salesiana

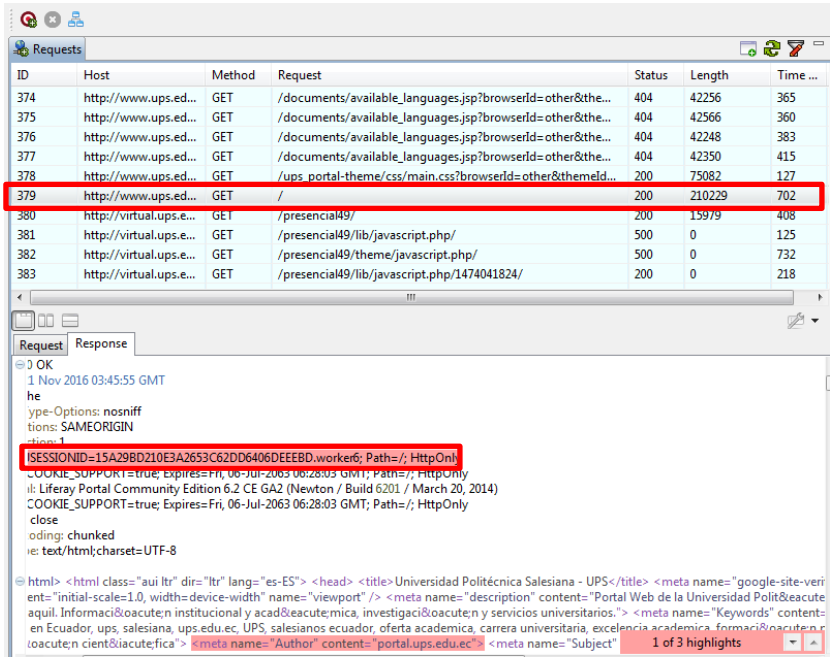


Figura 3.4. Análisis de la vulnerabilidad de alto Riesgo encontrada

Elaborado por: Dennis Carcelén y Carlos Ríos

Para la remediación de este error es conveniente que al crear el cookie en el código se establezca el indicador seguro en *true*.

En la Figura 3.5. se puede visualizar que se ha encontrado además una posible ruta absoluta del sistema de archivos locales (Local Filesystem Paths). Este tipo de vulnerabilidad se considera de medio riesgo y se describen como información sensible porque al realizarse una intrusión, el atacante puede conocer cosas sobre el entorno del servidor. Esta de brecha de seguridad aumentaría la probabilidad de éxito para los atacantes que no conocen el entorno previamente.

Las salidas de errores deben ser redireccionadas hacia un registro de errores, y ya que contienen las rutas completas, los administradores y desarrolladores del sistema deben proceder con su análisis correspondiente.

Análisis de riesgos encontrados en el sitio web de la Universidad Politécnica Salesiana

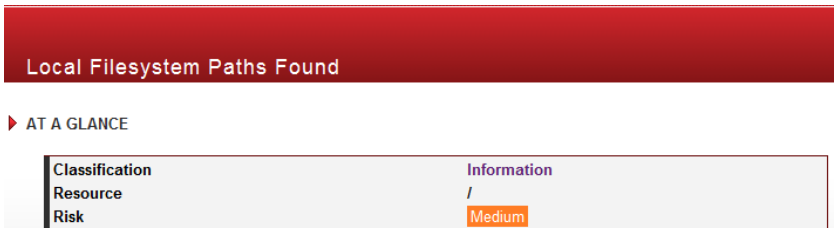


Figura 3.5. Análisis de la vulnerabilidad de riesgo medio encontrada

Elaborado por: Dennis Carcelén y Carlos Ríos

3.1.1 Problemática

En la Universidad Politécnica Salesiana, Campus Sur, actualmente se trabaja con seguridades a profundidad para la protección de la información. Sin embargo, no consta con un mecanismo diseñado especialmente para detección del comportamiento de usuarios malintencionados o usuarios con hábitos inadecuados que pudieran tener algún nivel de acceso o uso autorizado a la red y en base a eso explotar alguna vulnerabilidad y comprometer la información. Adicionalmente no se tiene un escenario aislado y controlado para realizar pruebas de penetración avanzadas y hacking ético que permita poner en práctica nuevas habilidades y competencias sin poner en riesgo la integridad de la red.

- **Obtención del Pseudo-Perfil de usuario de los servicios web de la UPS, Sede Quito-Campus Sur**

Dado que los ataques a la seguridad de la información han tenido un crecimiento del 38% con cada año, y este aumento involucra tanto frecuencia, severidad e impacto, las organizaciones poseen métodos cada vez menos efectivos para mitigar, prevenir y detectar dichos ataques; se ha procedido, como parte del diseño propuesto, a realizar una descripción del perfil de los usuarios de la red de la UPS, con la presentación de

datos acerca de los hábitos y conocimientos sobre la seguridad de la información, que poseen dichos usuarios en el uso cotidiano de los servicios web prestados por la institución.

Se realizan una serie de preguntas a una muestra de 400 individuos del grupo objetivo, para conseguir este fin.

En la Figura 3.6. se demuestra que el 74,3% de los encuestados no posee conocimientos acerca del concepto de BYOD (Bring Your Own Device) y que tampoco tiene una correcta práctica referente al aseguramiento de sus datos si se conectan a una red que en teoría es desconocida. Solamente el 25,7%, del mismo grupo encuestado, parece tener interés palpable en que sus datos no sean comprometidos.

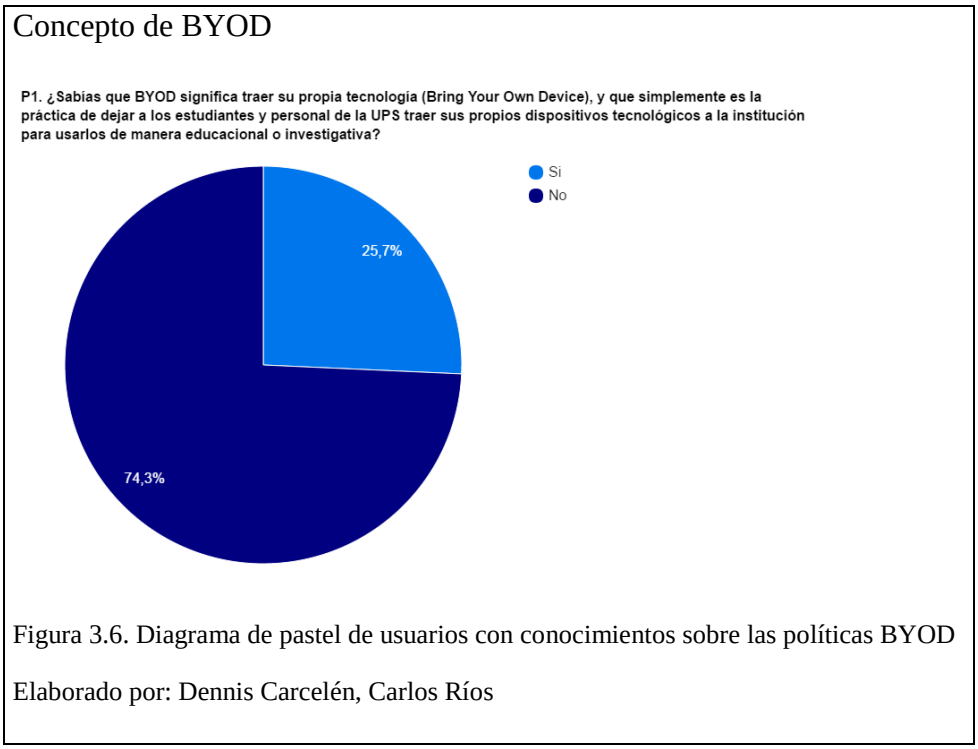


Figura 3.6. Diagrama de pastel de usuarios con conocimientos sobre las políticas BYOD

Elaborado por: Dennis Carcelén, Carlos Ríos

La siguiente pregunta realizada tiene relación con los hábitos de almacenamiento de datos. En la Figura 3.7. se observa que el grupo objetivo, tomando en cuenta la muestra encuestada va teniendo cada vez más conocimiento y preferencia por el almacenamiento en la nube. El 86,7% utiliza este tipo servicios, a diferencia de un reducido 6,7% que aun usa dispositivos de almacenamiento extraíble. Esto es debido a que los dispositivos más

empleados en la jornada diaria, ofrece servicios de carga de datos automática hacia la nube, por lo que los usuarios pueden acceder a sus documentos e información desde cualquier parte y usando cualquier otro dispositivo.

Servicios de almacenamiento de información en la nube

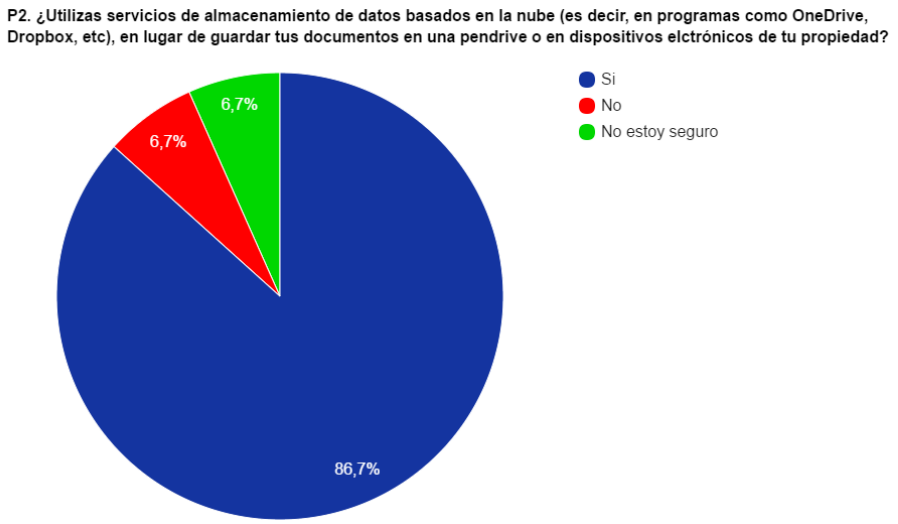


Figura 3.7. Diagrama de pastel sobre usuarios que utilizan almacenamiento en la nube

Elaborado por: Dennis Carcelén, Carlos Ríos

Existe un muy buen número de usuarios (diecinueve) que aseguran que la cyber-seguridad tiene como su principal beneficio la detección de anomalías en la redes de la institución, seguido de que ayuda en la comprensión de las amenazas externas que pudieran comprometer la información.

Se deja un poco de lado la conciencia de que los usuarios, influyen en las amenazas que pueden suscitarse en la seguridad de la información con solo siete usuarios que piensan que con la mejor comprensión de ese comportamiento, se mejoraría la cyber-seguridad de la institución. En la Figura 3.8. se puede observar lo descrito en esta parte.

Beneficios de la cyber-seguridad

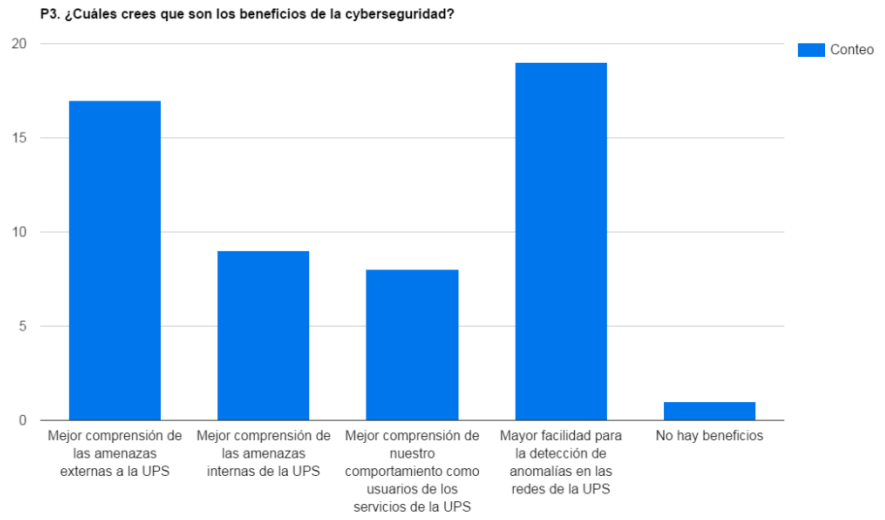


Figura 3.8. Diagrama de barras sobre usuarios que consideran que la cyber-seguridad conlleva beneficios

Elaborado por: Dennis Carcelén, Carlos Ríos

Entre las malas prácticas en contra de la seguridad de la información, se encuentra el uso de contraseñas débiles y fáciles de obtener. En uno de los servicios web ofertados en la institución, la clave por defecto es el número de cedula de identidad del usuario y como se cree que la información ofertada en este ambiente no es de mucho interés para un atacante, estas contraseñas muchas veces no son cambiadas. En la Figura 3.9. se observa que el 60% de los encuestados sigue usando su clave por defecto.

Contraseñas débiles

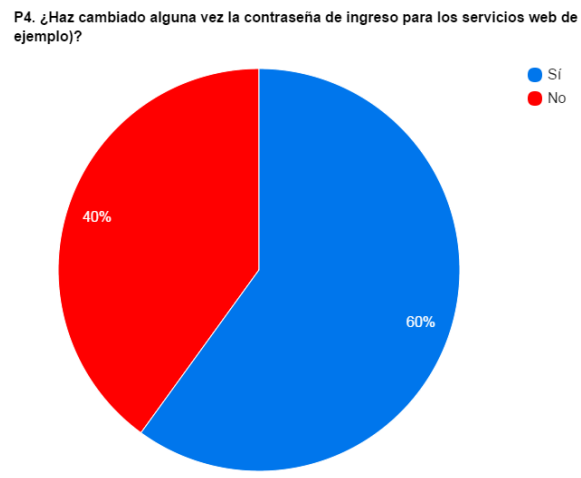


Figura 3.9. Diagrama de pastel sobre usuarios que tienen contraseñas débiles en sus servicios web institucionales

Elaborado por: Dennis Carcelén, Carlos Ríos

Entre los delitos informáticos más comunes hoy en día, se encuentra el Phising, el cual consiste en la suplantación de la identidad informática de una identidad para poder adquirir información confidencial de los usuarios. Con la clonación de la página de la institución se pudo demostrar que hacer spoofing de este servicio es plenamente viable, por lo que adquirir datos de los usuarios puede ser muy factible. Teniendo esto en cuenta, se puede notar que los encuestados tienen una buena educación en cuanto a esta posible amenaza, visualizando en la Figura 3.10 que el 46,7% siempre revisa que la URL de la institución sea la correcta, el 36,7% se fija a menudo en este detalle y solo el 16,7% nunca lo hace, sin querer decir con esto que el porcentaje de personas que nunca lo revisan sea bajo.

Verificación de sitios oficiales

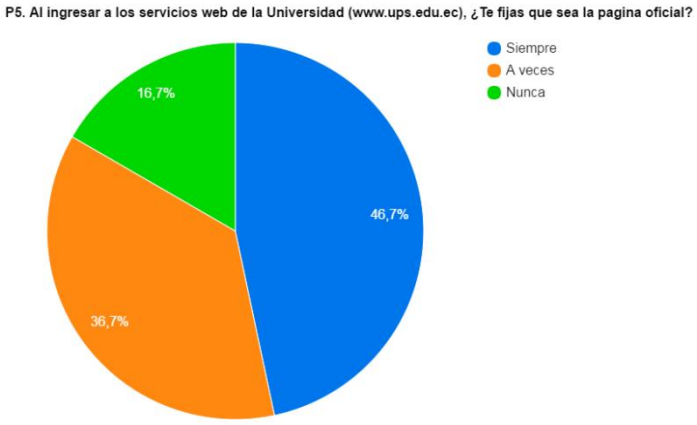


Figura 3.10. Diagrama de pastel sobre los usuarios que verifican que la URL a la que desean ingresar, es la correcta.

Elaborado por: Dennis Carcelén, Carlos Ríos

La mayoría de personas encuestadas están conscientes de que las amenazas y las vulnerabilidades en el mundo digital son muy variadas y de varios tipos, por lo que el 66,7% considera que no tiene conocimiento pleno sobre este tema. En la Figura 3.11. se puede observar los datos obtenidos sobre esta pregunta.

Conocimiento sobre los riesgos en la seguridad de la información.

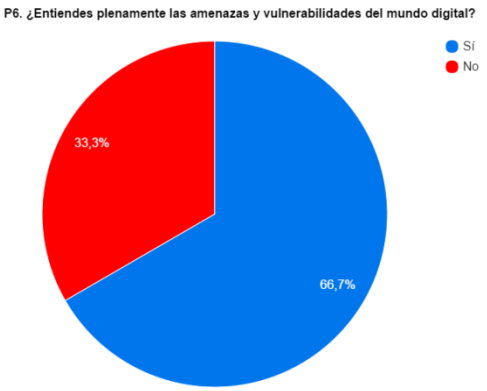


Figura 3.11. Diagrama de pastel sobre usuarios que conocen a plenitud los riesgos existentes en la red.

Elaborado por: Dennis Carcelén, Carlos Ríos

A nivel de la institución, sale a relucir, en la Figura 3.12., el desconocimiento por parte de los usuarios, sobre los mecanismos, herramientas, prácticas y proyectos que se dan para mejorar la seguridad de los datos que se manejan dentro de la red de la UPS. Apenas el 13,3% de los encuestados conoce sobre este caso. Por lo que se puede prever que el 86,7% *asume* que sus datos están seguros y que de alguna manera no se encuentran comprometidos en la red.

Análisis de riesgos informáticos institucionales

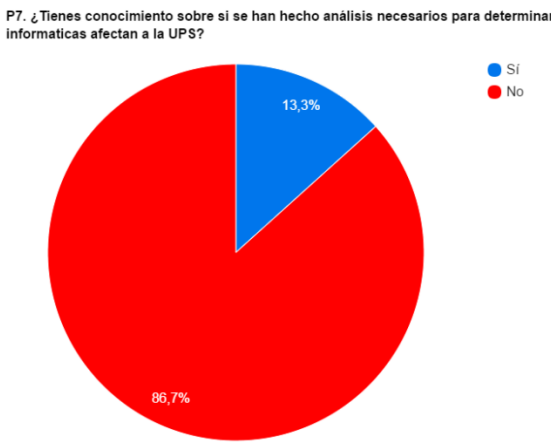


Figura 3.12. Diagrama de pastel sobre el conocimiento de los usuarios sobre las practicas institucionales en contra de los usos malintencionados de la red

Elaborado por: Dennis Carcelén, Carlos Ríos

En cuanto a las amenazas y vulnerabilidades que los usuarios consideran que van en aumento, y que se considera que podrían causar una brecha en la seguridad de la información, se destacan las que tienen relación con el uso de las redes sociales y con la inserción de malware en la red institucional. Se puede notar con esto que los usuarios tienen fácil acceso al contenido en redes sociales dentro del campus y que son conscientes de que ellos como usuarios tienen todavía mal uso de la red universitaria dado que debería ser usada para fines educativos y de investigación preferencialmente. En la Figura 3.13. se ilustra lo descrito.

Riesgos crecientes en la red de la UPS

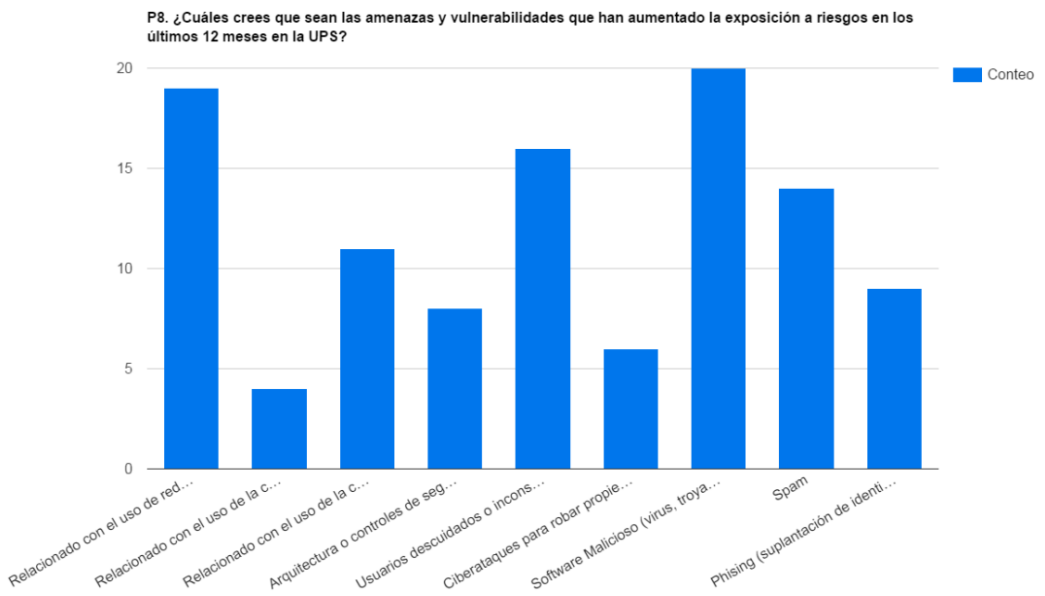


Figura 3.13. Diagrama de barras sobre el conocimiento de diferentes tipos de riesgos que pudieran presentar los servicios web institucionales

Elaborado por: Dennis Carcelén, Carlos Ríos

3.2 Recolección de datos en la Honeynet

La recolección de los datos por parte de la Honeynet en la Universidad Politécnica Salesiana Sede Quito, Campus Sur, permite poder tomar acciones pertinentes y en tiempos muy oportunos para brindar una mayor seguridad a los servicios web de la entidad. Además se puede tener acceso al prototipo Honeynet para propósitos investigativos contra amenazas recientemente creadas por lo que se considera realmente adecuado utilizar la arquitectura de tercera generación o *GenIII* para aprovechar las herramientas de control, análisis y captura de los datos que se logren obtener.

3.3 Diseño de la Honeynet

Para proceder a realizar el diseño de la Honeynet se debe tomar en cuenta el nivel de interacción que se requiere obtener con el intruso, considerando que para conseguir una alta interacción se debe montar los servicios en sistemas operativos reales y no en virtuales.

3.3.1 Comparativa entre honeypot de alta interacción (sistema operativo real) y honeypot de media interacción (software)

Para la correcta selección del tipo de honeynet a implementarse, se compara mediante pruebas, las ventajas y falencias que tienen los honeypots de media interacción, frente a los honeypots de alta interacción.

- **Media interacción**

El Honeypot de media interacción usado para esta comparativa es Honeydrive. Cabe mencionar que HoneyDrive no es una honeypot en sí, se trata de una distribución que puede ejecutarse utilizando el software de virtualización VirtualBox y que ofrece una gran cantidad de herramientas de despliegue de honeypots, con la posibilidad de *emular* muchos sistemas y servicios.

Gracias a Honeydrive el usuario puede centrarse en el despliegue de herramientas sin tener que profundizar en su instalación previa. Se puede descargar la distribución desde *http://sourceforge.net/projects/honeydrive/* de forma totalmente gratuita (Castaño, 2014).

- **Sesión remota con SSH**

Establecimiento de sesión vía SSH

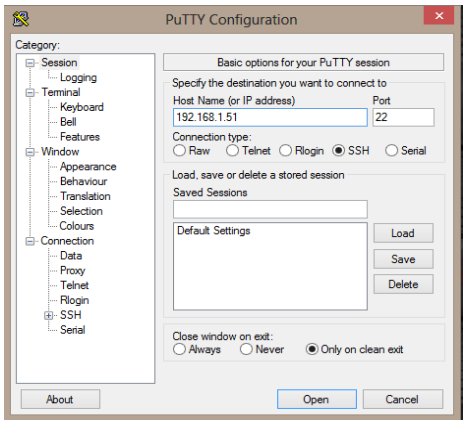


Figura 3.14. Establecimiento de sesión hacia el honeypot de media interacción via SSH con PuTTY

Elaborado por: Dennis Carcelén, Carlos Ríos

Al iniciar una sesión mediante conexión remota en ssh (secure shell), como se muestra en la Figura 3.14. y en la Figura 3.15., en un honeypot de mediana interacción, el fin de este es recopilar los intentos de inicios de sesión y mostrar las estadísticas de las combinaciones de usuario y contraseña más utilizadas para evitar el uso de estas en servidores pertenecientes a producción.

El honeypot registra paso a paso todas las instrucciones ejecutadas en el Shell para ser estudiadas a futuro.

Establecimiento de sesión vía SSH

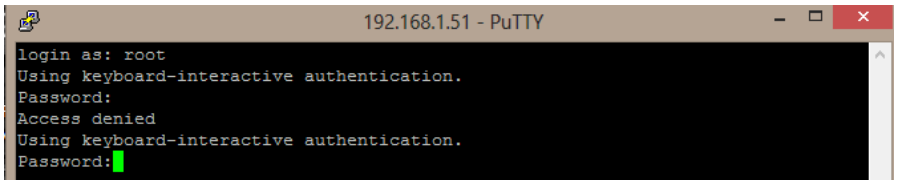


Figura 3.15. Inicio de sesión en PuTTY para la realización de la conexión via SSH

Elaborado por: Dennis Carcelén, Carlos Ríos

En caso de un ingreso exitoso, dado por un ataque de fuerza bruta o similar, el honeypot interactúa con el atacante y retorna mensajes de manera que este no sospeche que no se encuentra frente al control de una terminar ilegítima. En este punto surge la desventaja dada por la limitación del *script*, ya que las respuestas que se encuentran programadas en lenguaje Python dentro del programa son limitadas, además no se trata de un emulador.

En la Figura 3.16., se muestran los resultados obtenidos de los intentos de registro mediante el uso de nombres de usuario y contraseña.

Top 10 de intentos de ingreso al honeypot

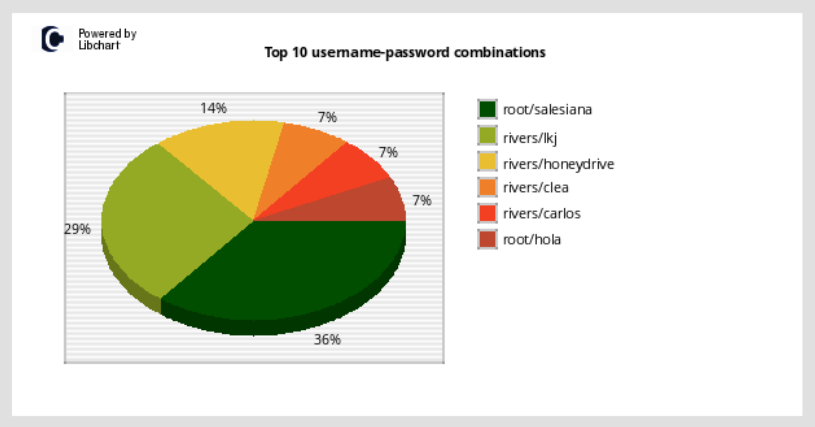


Figura 3.16. Top 10 de claves y nombres de usuario para intentar acceder al honeypot

Elaborado por: Dennis Carcelén, Carlos Ríos

Fallos en la petición de la versión del servidor OpenSSH

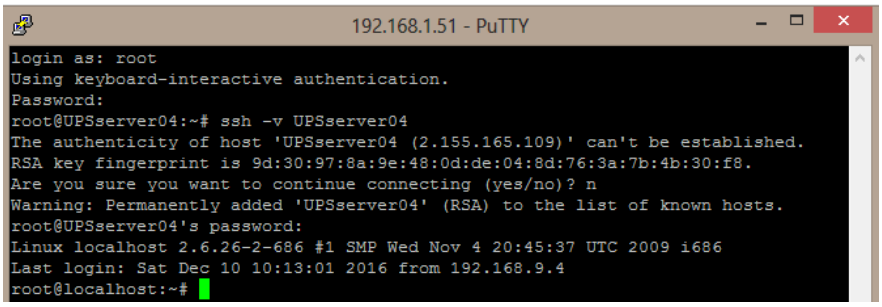


Figura 3.17. Fallo en la petición de la versión del servidor OpenSSH

Elaborado por: Dennis Carcelén, Carlos Ríos

En la Figura 3.17. se puede apreciar que el script omite la opción –V, la cual debería proporcionar de retorno la versión del servidor OpenSSH que está corriendo y en la cual se tiene iniciada una sesión. Al contrario, interpreta la instrucción como un nuevo inicio de sesión remoto hacia otro host. Además omite la respuesta negativa que se le proporciona a la pregunta de si se desea continuar con la conexión.

- **Alta Interacción**

A diferencia del honeypot de media interacción, en este caso se dispone de un terminal real, de esta manera no solo se dispondrá de respuestas prefabricadas a los comandos proporcionados en el Shell.

- **Sesión remota con SSH**

La dificultad de pasar de un programa medianamente interactivo a un sistema operativo real radica en la forma de captación de la actividad del presunto atacante, por lo que es necesario recurrir a la implementación de un keylogger que reemplace al programa de registro de actividad.

Verificación mediante petición de la versión del servidor OpenSSH

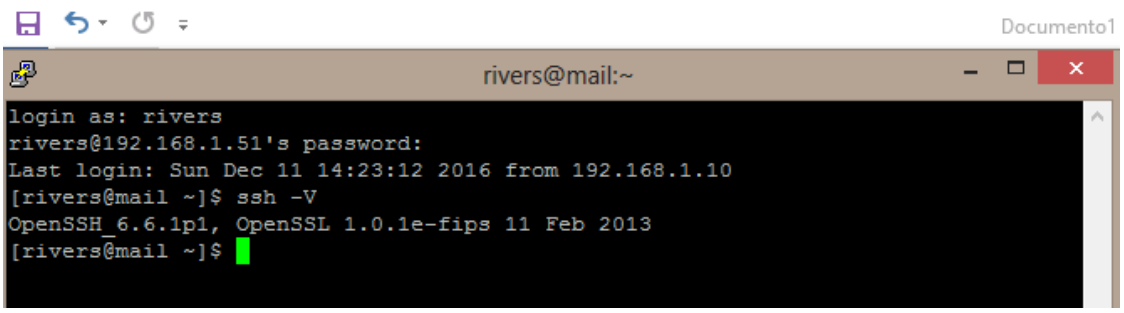


Figura 3.18. Verificación mediante petición de la versión del servidor OpenSSH

Elaborado por: Dennis Carcelén, Carlos Ríos

En la Figura 3.18., se puede apreciar el inicio satisfactorio de un acceso remoto en el cual registra la hora de entrada al sistema operativo real. Resultado que en comparación con los honeypots de mediana interacción no se obtiene, de la misma forma se puede verificar la versión del servicio.

Verificación mediante petición de inicio de sesión del servidor OpenSSH

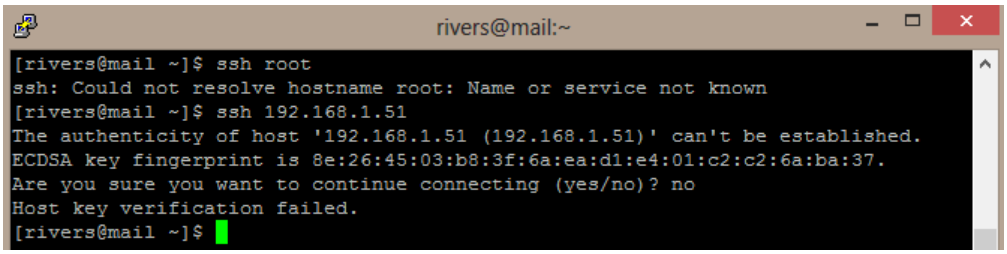


Figura 3.19. Verificación mediante petición de inicio de sesión del servidor OpenSSH

Elaborado por: Dennis Carcelén, Carlos Ríos

En la Figura 3.19., se puede observar que ahora los comandos responden de acuerdo a lo esperado al intentar acceder a iniciar otra sesión a otro host, no así en el caso de un honeypot de mediana interacción que solo devuelve la respuesta más cercana según encuentre entre sus líneas de programación, lo que lo convierte en un riesgo para su detección de acuerdo al grado de experticia del atacante.

Con esta experiencia, se decide optar por el diseño de una Honeynet de alta interacción para el correcto aprovechamiento de sus herramientas. La Honeynet se diseña con el fin de asegurar el mayor grado de interacción por parte de los usuarios de la red, lo cual permitirá recopilar una gran cantidad de información válida, que servirá para realizar los respectivos análisis aplicando las herramientas que posee la arquitectura Honeynet descrita en el capítulo 1.

Adicionalmente se debe mencionar, que las Honeynets de tercera generación ofrecen muy buenas herramientas para la administración de la información con el fin de detectar las amenazas y ataques que pudieran darse y gracias a que en la arquitectura, la distribución de los honeypots se da de manera centralizada, se puede tener escalabilidad o adaptabilidad a los posibles cambios en la infraestructura que pudieran presentarse a futuro.

- **Disposición y Uso de Honeywall**

La interfaz web *Walleye* de las Honeynets de tercera generación, permite observar las actividades elaboradas por los intrusos en la red de información de manera gráfica, con la previa configuración de los criterios para el control y análisis de datos en el *Honeywall.*

Con este componente se hace una buena generación de los *logs* o reportes requeridos y sirve de apoyo para la realización de estrategias para la prevención de nuevas intrusiones malintencionadas en la red de la UPS debido a que permite la generación de usuarios y conjuntos de usuarios que deban trabajar en la administración y monitoreo de las actividades que se realicen en la Honeynet desde algún sitio en la red dentro del campus.

La centralización de los mensajes y registros obtenidos en la Honeynet es de mucha utilidad en la arquitectura que se desea implementar, para tener una gran facilidad de administración de la información generada. El equipo central puede vincularse a la red local de la UPS.

En el presente trabajo de titulación se utiliza la virtualización como respuesta al problema planteado por las siguientes razones:

- La reducción de los costos de desarrollo e implementación
- La facilidad de traslado de los equipos y la fácil vinculación con la red de la UPS.

Por dichos motivos, se ha considerado que la mejor opción para la implementación del presente trabajo, es la arquitectura denominada como Honeynet virtual auto-contenida.

- **Disposición y uso de los Honeypots**

En esta arquitectura, se tiene como mínimo dos máquinas virtuales contenidas en una maquina física, para el despliegue en la primera de un honeypot y de la segunda del Gateway denominado Honeywall.

Se debe colocar la Honeynet en un lugar que no perjudique a la red de datos de la institución, por lo que se tendrá que crear una *VLAN aislada*, para la ubicación del prototipo, esto permitirá la libre circulación del tráfico saliente y entrante de la Honeynet

sin un previo control por parte de las seguridades y firewalls instalados en la red de campus, y la recopilación en mayor proporción de la información necesaria para el análisis.

La VLAN aparecerá visible para los usuarios y posibles intrusos en Internet, por lo que se podrá tener la mayor interacción posible con los usuarios no autorizados.

Los honeypots que se constituyan estarán totalmente visibles, como cualquier otro servicio que presta la UPS, por medio de la VLAN aislada y la interfaz física de la máquina real.

- **Disposición y uso de las Interfaces**

Se puede observar además la herramienta que se usará principalmente para otorgar los permisos de conexión, control y captura de información, esto se logra gracias a que sus interfaces se configuran en modo *bridge.*

En la Figura 3.20. se visualiza el diseño propuesto para la puesta en funcionamiento de la Honeynet, la cual consta de una Honeynet virtual auto contenida para que pueda funcionar en una única maquina real para el aprovechamiento de las herramientas y recursos disponibles.

Tabla 3.1. Distribución de las Interfaces en la Honeynet

Interfaz 1 en modo Bridge	Administración de Honeywall
Interfaz 2 en modo Bridge	Comunicación de Honeywall con la Máquina Anfitrión.
Interface 3 en modo Host-Only	Comunicación de Honeywall con los Honeypots

Nota: Elaborado por Dennis Carcelén, Carlos Ríos

Esquema de diseño propuesto para el prototipo Honeynet

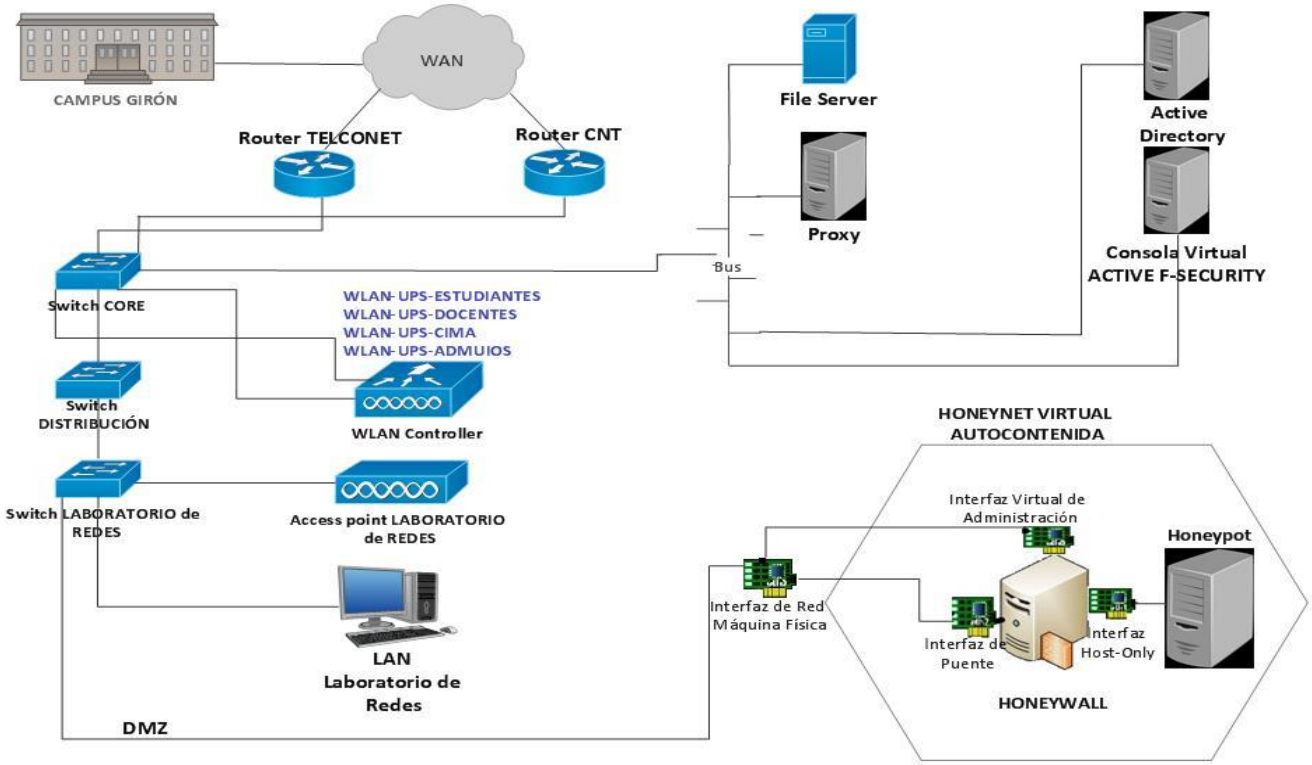


Figura 3.20. Elementos del prototipo Honeynet y su distribución en la Red

Elaborado por: Dennis Carcelén, Carlos Ríos

3.4 Implementación de la Honeynet

Para la implementación se requiere que el administrador de la red del campus Sur, asigne direcciones IP locales o privadas para el o los honeypots creados. Estas direcciones IP locales deben ser traducidas por medio de un NAT a direcciones IP públicas para el acceso a internet, así se puede recolectar correctamente y en buena cantidad, la información para su respectivo y posterior análisis.

3.4.1 Hardware y Software disponible

Para la implementación de la solución planteada, se dispone de un equipo Lenovo T430 con las siguientes características, que aseguran el correcto despliegue y funcionamiento de la Honeynet:

Procesador: Intel Core i5-3320M CPU 2.60GHz

Memoria RAM: 4.00 GB

Tipo de Sistema operativo: 64 Bits Windows 8 PRO

Tarjeta de red: Gigabit Intel ® 82579LM

Espacio de disco: 367 GB

En esta máquina se pone en funcionamiento el honeypot con los respectivos servicios implementados en el sistema operativo CentOS 7 en una consola virtual desplegado a través del software de virtualización VirtualBox.

- **Bloques de componentes de la Honeynet**

El sistema honeynet propuesto consta de los siguientes bloques de componentes:

3.4.2 Interfaces

Para la instalación del Honeywall se deben configurar dos interfaces de red, una en modo “Puente” o *bridge* para la comunicación con la maquina física y la otra para la gestión, y otra adicional en modo de “Solo invitado” para que pueda tener intercambio de información con el honeypot.

3.4.3 Honeywall

Honeywall CDROM es la herramienta estrella de alta interacción para capturar, controlar y analizar ataques. Crea una arquitectura que le permite implementar honeypots de baja interacción y de alta interacción, pero está diseñado principalmente para una alta interacción.

El Honeywall de la Honeynet está contenido en una consola virtual, con su sistema operativo basado en CentOS e instalada a través del Roo CDROM (roo-1.4.h20080424215740) (Spitzner, 2008).

3.4.4 Honeypots

El honeypot que se pone en funcionamiento provee los siguientes servicios:

- DHCP: para la asignación dinámica de las direcciones en los hosts de la red
- DNS: para los nombres de dominio
- FTP: para el envío y recepción de archivos
- Webmail: para el envío y recepción de mensajes electrónicos
- HTTP: para la transferencia de información en internet

Estos servicios se instalan mediante una máquina virtual con sistema operativo CentOS 7 y se tiene el mínimo de seguridades posibles, para obtener el máximo aprovechamiento de la recolección de la información en caso del exitoso acceso por parte de posibles usuarios no autorizados.

En la Tabla 3.2. se muestra el detalle de los servicios instalados y el proceso de instalación de estos servicios se muestra en el Anexo 1.

Tabla 3.2. Servicios instalados en el Honeypot.

Servicio	Descripción	Versión
DHCP	Servidor DHCP	dhcp-4.2.5-42.el7.centos.x86_64
DNS	Servidor BIND (Berkeley Internet Name Domain)	bind-9.9.4-29.el7_2.4.x86_64
Web (HTTP)	Servidor web HTTP Apache	httpd-2.4.6-40.el7.centos.4.x86_64
FTP	Servidor very secure FTP daemon	vsftpd-3.0.2-11.el7_2.x86_64
Mail (SMTP – POP3)	Servidor mail SMTP Servidor mail POP3	postfix-2.10.1-6.el7.x86_64 dovecot-2.2.10-5.el7.x86_64
Webmin	herramienta de configuración de servicios con interfaz gráfica vía web	webmin-1.820-1.noarch
SSH	Servidor Secure Shell OpenSSH	openssh-6.6.1p1-25.el7_2.x86_64

Nota: Elaborado por Dennis Carcelén, Carlos Ríos

CAPÍTULO 4

PRUEBAS Y RESULTADOS

Con la VLAN aislada proporcionada se tuvo un área de pruebas en el cual se pudo replicar cinco servidores y proporcionar conectividad de internet a 8 clientes conectados en dicha red local y un promedio de entre cinco usuarios inalámbricos. Se creó así un ambiente controlado mediante la virtualización de cuatro computadores donde se pudo realizar pruebas y recopilar información del funcionamiento y los usuarios cercanos al laboratorio de redes en un periodo aproximado de tres meses en que se hizo uso de la disponibilidad de red inalámbrica abierta, por medio de un ataque a nivel de enlace de datos (ettercap –IPspoofing y sniffing), a nivel de capa red (ping y nmap) y a nivel de capa aplicación (set tool kits - harvesting).

4.1 Pruebas de funcionamiento y vulnerabilidad de los Servicios implementados

Al analizar las vulnerabilidades presentes en los servicios instalados en el honeypot, se considera realizar una serie de pruebas de penetración que van desde ataques al entorno, hasta ataques de datos y de lógica.

La primera prueba se la realiza con la herramienta Metasploit contenida en Kali Linux para el conocimiento de puertos abiertos y que pueden ser víctimas de un posible ataque, en el Honeypot implementado. Este escaneo es considerado en sí como un principio de intrusión o ataque y violación de la privacidad de las redes puesto que es la manera más básica de hacer un sondeo del estado de la red y su estructura sin el consentimiento del administrador de red, esto con el propósito de tener indicios de la posible topología y encaminar un ataque a mayor escala.

En la Figura 4.1. se visualiza la consola de Metasploit para la realización de los ataques hacia el honeypot y la comprobación de su funcionamiento.

Consola de Metasploit

Figura 4.1. Consola de la herramienta Metasploit contenida en Kali Linux

Elaborado por: Dennis Carcelén, Carlos Ríos

Desde esta herramienta, se ejecuta un *nmap* a la dirección del honeypot para verificar que los puertos correspondientes a cada servicio, se encuentren abiertos como se propuso en la fase de diseño. La Figura 4.2. muestra lo descrito en esta parte.

Se puede observar el estado de los puertos correspondientes a los servicios implementados en el honeypot y se verifica que los puertos de ftp, ssh, dns, http y el 10000 de tcp que corresponde a webmin, se encuentran abiertos.

Mapeo de puertos del honeypot

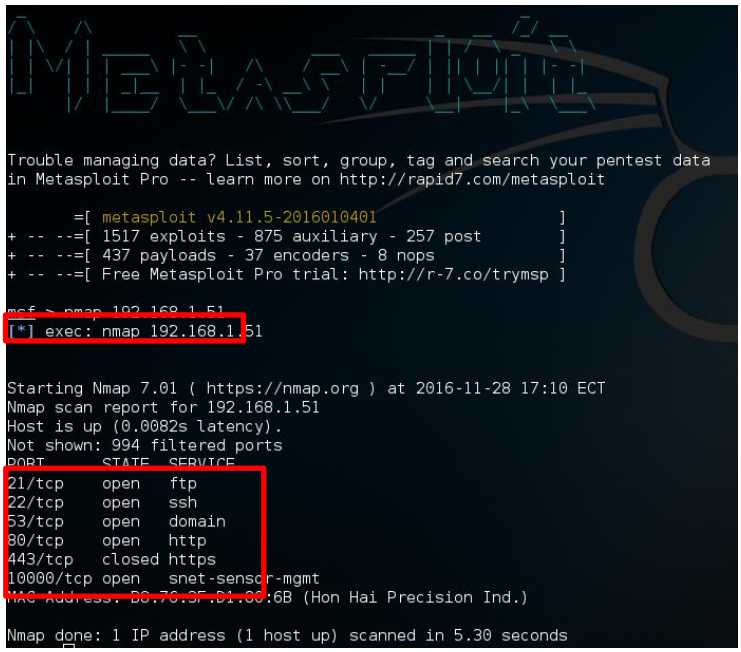


Figura 4.2. Mapeo de determinación de puertos abiertos en el Honeypot

Elaborado por: Dennis Carcelén, Carlos Ríos

4.1.1 Pruebas de las Versiones de los servicios con Metasploit

Ahora se procede a las pruebas de verificación de las versiones de los servicios implementados en el honeypot.

4.1.1.1 Prueba de verificación del servidor FTP

En la Figura 4.3. se observa el ataque para el conocimiento de la versión que se ha instalado en el servidor FTP. Esta prueba se la realiza con el comando *nmap –sV 192.168.1.51 –p 21* en donde:

- -sV: Se usa para que Metasploit examine la versión del servicio.
- -p 21: Se usa para la examinación del puerto del servicio (en este caso el puerto 21 correspondiente a ftp).

Comprobación del servidor FTP

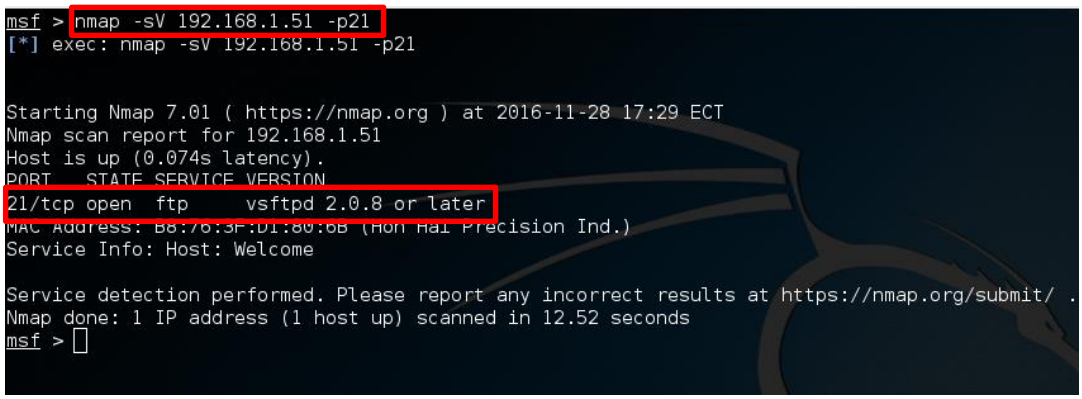


Figura 4.3. Ataque Comprobación de la versión implementada del servidor de FTP y el estado de puerto.

Elaborado por: Dennis Carcelén, Carlos Ríos

En la Figura 4.4. se muestra otro mecanismo para el escaneo de puerto además de nmap, el modulo auxiliar que se usa es *use auxiliary/scanner/ftp/ftp_version*. Cuando se complete el escaneo, se mostrarán los parámetros que son necesarios para el lanzamiento de un *exploit* para poder acceder a la información de la versión del servidor FTP instalada.

Lanzamiento de exploit para vulnerar el servidor FTP

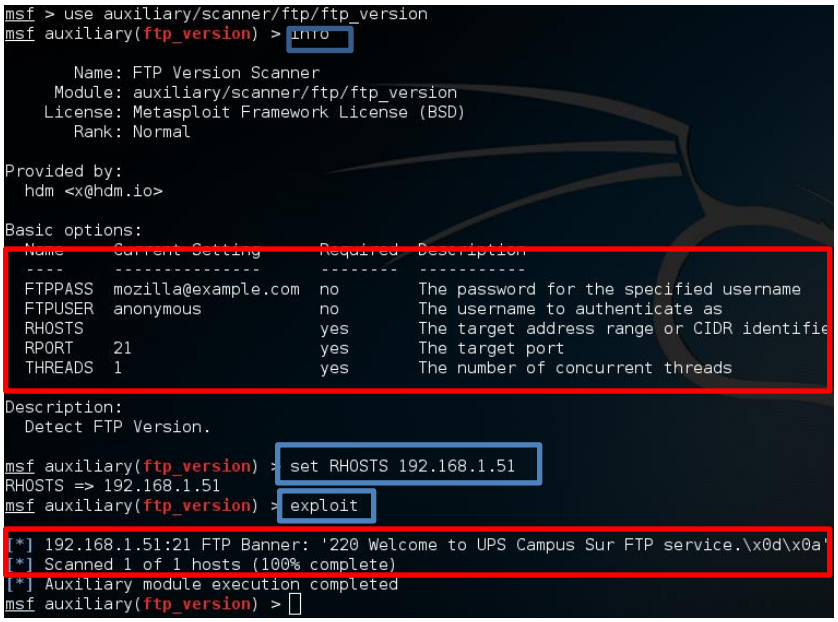


Figura 4.4. Ataque realizado mediante un exploit hacia el servidor de FTP para conocer la versión implantada.

Elaborado por: Dennis Carcelén, Carlos Ríos

Búsqueda de exploit para vulnerar el servidor FTP

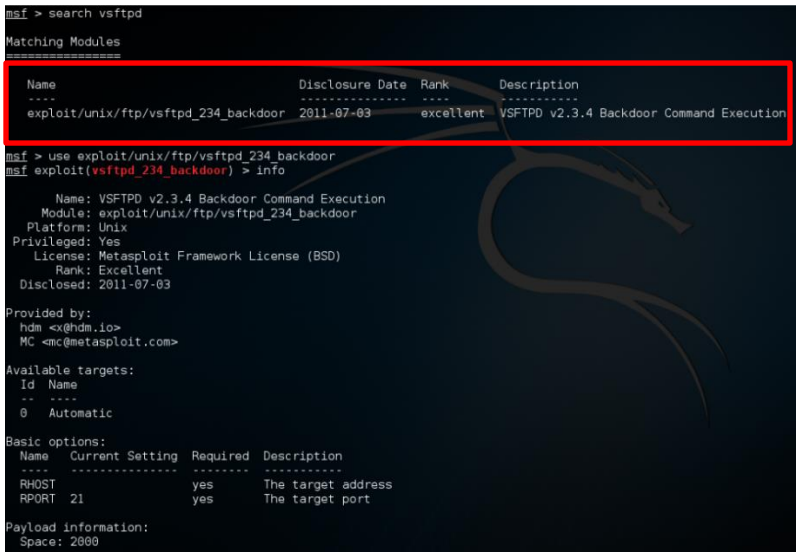


Figura 4.5. Búsqueda de un exploit para vulnerar el servidor de FTP.

Elaborado por: Dennis Carcelén, Carlos Ríos

En la Figura 4.5. se muestra la búsqueda, con el comando *search vsftpd*, de un exploit para poder vulnerar el servicio FTP. Se utiliza el comando use seguido de la ruta del exploit que se ha seleccionado, en este caso es *use exploit/unix/ftp/vsftpd_234_backdoor*, el comando muestra los campos requeridos para realizar la explotación de la vulnerabilidad del servicio. Luego de introducir uno de los campos necesarios con el comando *set*, se ejecuta la orden *exploit* para vulnerar el servidor. Lo descrito se aprecia mejor en la Figura 4.6. y en la Figura 4.7.

Lanzamiento de exploit para vulnerar el servidor FTP

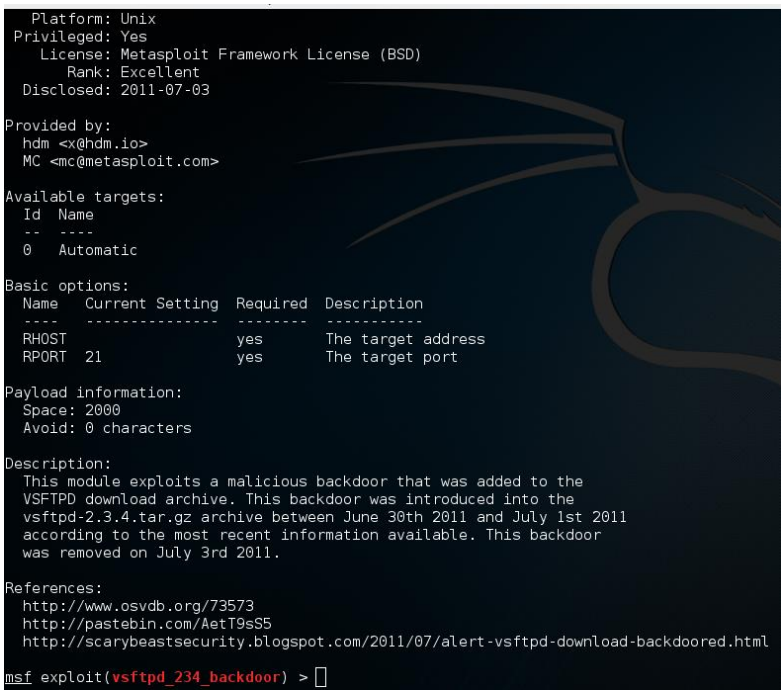


Figura 4.6. Ejecución del exploit requerido para vulnerar el servidor FTP.

Elaborado por: Dennis Carcelén, Carlos Ríos

Lanzamiento de exploit para vulnerar el servidor FTP

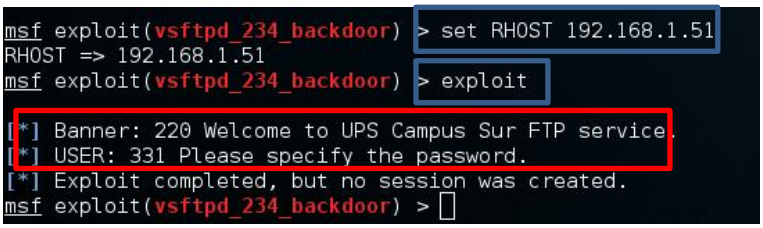


Figura 4.7. Ataque realizado mediante un exploit hacia el servidor de FTP.

Elaborado por: Dennis Carcelén, Carlos Ríos

4.1.1.2 Prueba de verificación del servidor HTTP

En la Figura 4.8. se observa el ataque para el conocimiento de la versión que se ha instalado en el servidor HTTP. Esta prueba se la realiza con el comando *nmap –sV 192.168.1.51 –p 80*.

Comprobación del servidor HTTP

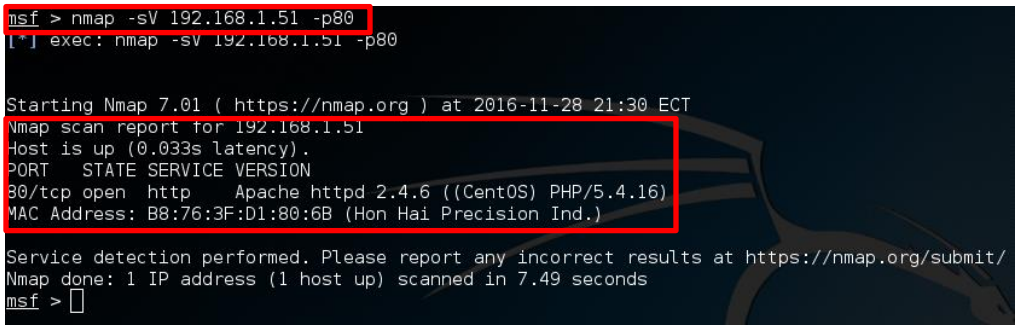


Figura 4.8. Ataque Comprobación de la versión implementada del servidor de HTTP y el estado de puerto.

Elaborado por: Dennis Carcelén, Carlos Ríos

4.1.1.3 Prueba de verificación del servidor SSH

En la Figura 4.9. se observa el ataque para el conocimiento de la versión que se ha instalado en el servicio SSH. Esta prueba se la realiza con el comando *nmap –sV 192.168.1.51 –p 22*.

Comprobación del servidor SSH

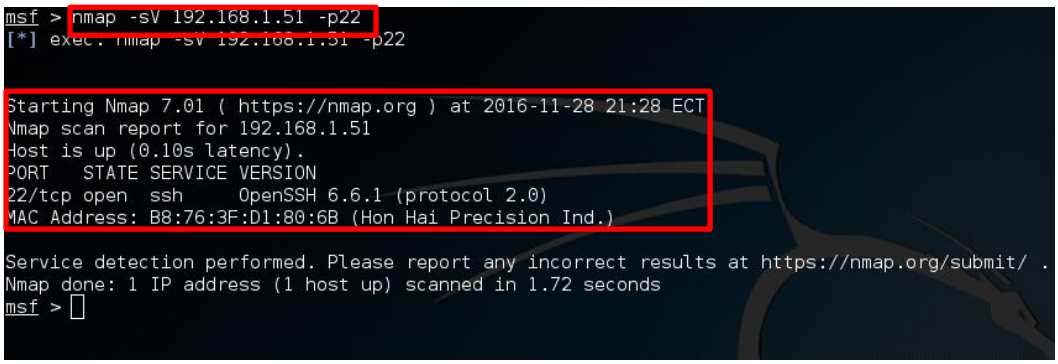


Figura 4.9. Ataque Comprobación de la versión implementada del servidor de SSH y el estado de puerto.

Elaborado por: Dennis Carcelén, Carlos Ríos

4.1.2 Prueba de verificación del servidor DNS

En la Figura 4.10. se observa el ataque para el conocimiento de la versión que se ha instalado en el servidor DNS. Esta prueba se la realiza con el comando *nmap –sV 192.168.1.51 –p 53*.

Comprobación del servidor DNS

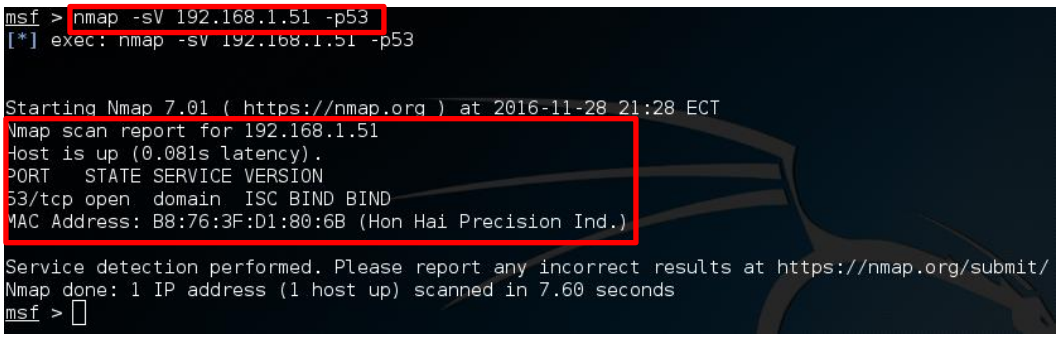


Figura 4.10. Ataque Comprobación de la versión implementada del servidor de DNS y el estado de puerto.

Elaborado por: Dennis Carcelén, Carlos Ríos

4.1.3 Pruebas de penetración a la Honeynet mediante ataques de fuerza bruta por diccionario

A continuación se realiza el proceso para poder vulnerar uno de los servicios disponibles en la honeynet mediante la herramienta Hydra, contenida en la suite de Kali Linux, que también puede vulnerar servicios tales como: Mysql, POP3, SNMP, SMTP, SSH, Telnet, entre otros. Se ha seleccionado el servidor ftp para medir la efectividad de la contraseña establecida por uno de los usuarios registrados en el servidor.

Estos ataques se realizan por medio de diccionarios que están disponibles en la web, compilados según temas específicos como: usuarios, peores contraseñas utilizadas, idiomas, etc. y también con diccionarios provistos en la suite de Kali.

En la Figura 4.11. se muestra el resultado obtenido del ataque realizado al servidor mediante un diccionario que contiene 500 palabras (descritas en un top de las más inseguras por su popularidad) para lograr obtener la contraseña, conociendo con antelación el nombre de usuario.

Este ataque ha tomado un tiempo de un minuto y se registra como fallido debido a la poca cantidad de palabras contenidas en el archivo con formato *.txt* seleccionado.

Ataque de fuerza bruta fallido mediante Hydra

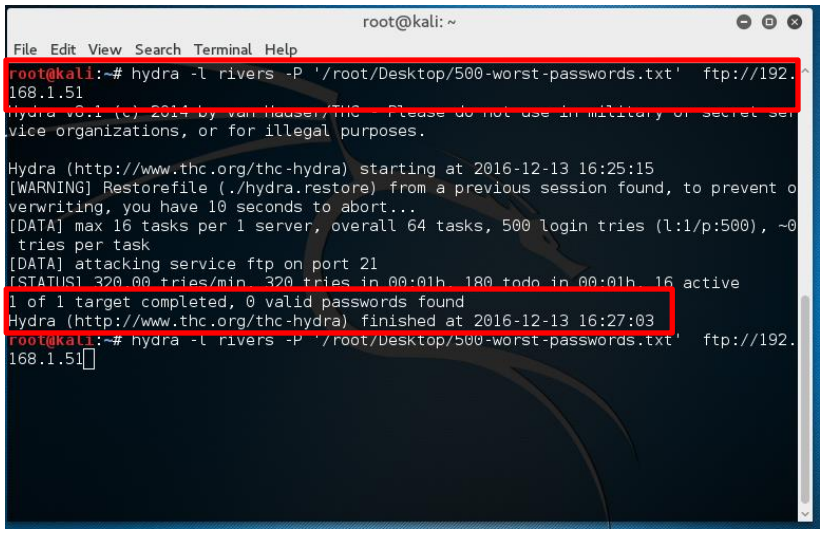


Figura 4.11. Ataque de diccionario para recuperación de contraseña

Elaborado por: Dennis Carcelén, Carlos Ríos

Después de este primer intento, se realiza la prueba con un diccionario al azar de 3560 palabras, contenido en John The Ripper, logrando recuperar la contraseña del usuario del que se tiene conocimiento, a los 317 intentos en un tiempo de un minuto. La Figura 4.12. muestra el resultado de lo descrito en esta parte.

Ataque de fuerza bruta exitoso mediante Hydra.

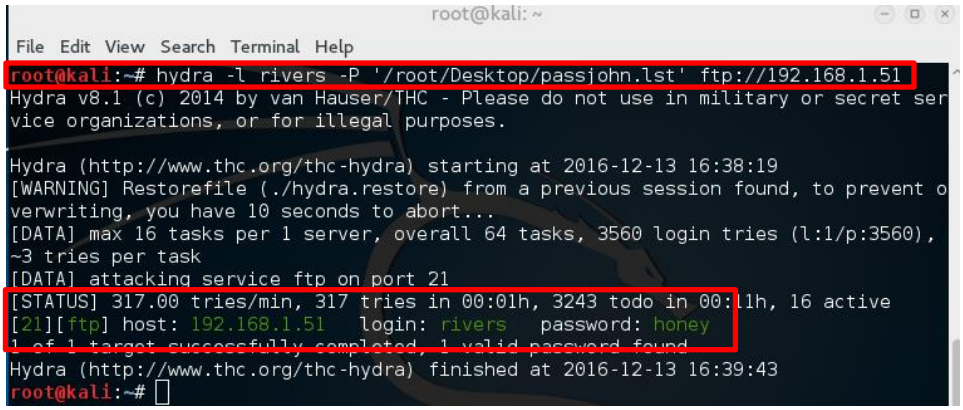


Figura 4.12. Ataque de diccionario para recuperación de contraseña

Elaborado por: Dennis Carcelén, Carlos Ríos

4.2 Detección por parte de Honeywall de los ataques realizados.

Debido a que, entre la máquina atacante y el servidor, se encuentra colocada la herramienta Honeywall, el escaneo es detectado sin que el atacante lo note, logrando registrarlo en el *registro de intrusiones*. El detector de intrusiones registra en la bitácora con hora, fecha y la dirección IP de origen y detalla el barrido de puertos como alertas de intrusión, una por cada sondeo de un puerto específico. El lanzar un barrido de puertos desde la suite Kali conlleva a realizar un barrido de 1000 puertos posibles entre los cuales se encuentran los puertos predeterminados por defecto de cada servicio.

Los resultados mostrados en por el Honeywall se visualizan en la Figura 4.13. y en la Figura 4.14.

Interfaz Walleye

Figura 4.13. Registros obtenidos de los ataques de barrido de puertos realizados con nmap desde Kali Linux yde los intentos de conexión por parte de los usuarios.

Elaborado por: Dennis Carcelén, Carlos Ríos

El IDS Snort incorporado en la herramienta Honeywall funciona según lo esperado frente a los ataques realizados mostrando los 1000 paquetes ICMP enviados en el barrido de puertos y el único paquete ICMP enviado mediante el nmap ejecutado a cada puerto de servicio específico. Además se pudo visualizar que al realizar el despliegue de la honeynet de modo virtualizado, la herramienta Honeywall obtiene una cantidad aproximada de 167 intentos de conexión (paquetes de tipo Universal Plug and Play o uPnP) por cada mes al interactuar con la máquina virtual del honeypot en la prueba realizada

Interfaz Walleye

Figura 4.14. Registros obtenidos de los ataques de barrido de puertos realizados con nmap desde Kali Linux

Elaborado por: Dennis Carcelén, Carlos Ríos

La figura 4.15 muestra el registro por parte de Honeywall de los intentos de intrusión al servidor ftp mediante los ataques de fuerza bruta realizados desde Hydra.

Registro de ataques al servidor FTP

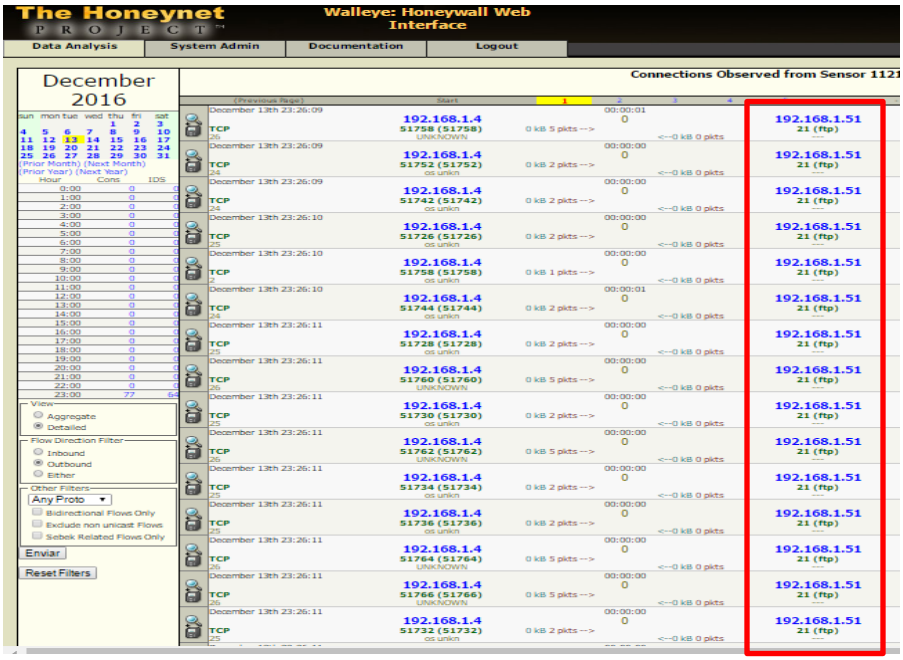


Figura 4.15. Registro de intentos de ataque de diccionario al servicio FTP

Elaborado por: Dennis Carcelén, Carlos Ríos

4.3 Clonación de la página web institucional para el servidor HTTP del Honeypot

La clonación de páginas es un método considerado de ataque, estipulado bajo el término de ingeniería social. El atacante induce a la víctima a visitar una página de apariencia similar (clonada), pero que se aloja en un servidor web diferente al original (otra dirección IP), esto con la finalidad de obtener información crucial como son las credenciales de acceso. El atacante realiza la obtención de las credenciales mediante un método conocido como “Credential Harvester” o segador, lo que implica escribir las credenciales en el portar de registro por parte del usuario víctima, esperando conseguir un inicio de sesión y por el contrario estas son registradas en un archivo en texto plano.

El procedimiento de clonación de páginas web puede ser resuelto de varias maneras. En esta parte se describe el proceso de clonación usando las herramientas provistas en Kali Linux.

4.3.1 Proceso de clonación de la página institucional.

Existe la posibilidad de clonar páginas en su totalidad (todas las imágenes y vínculos contenidos en la página) por medio de un software de licencia abierta llamado HTTrack website copier. El software hace un barrido de todos los elementos que conforman la página web corrigiendo el fallo de ciertas imágenes no accesibles. Lo descrito en esta parte se muestra en la Figura 4.16.

Interfaz HTTrack

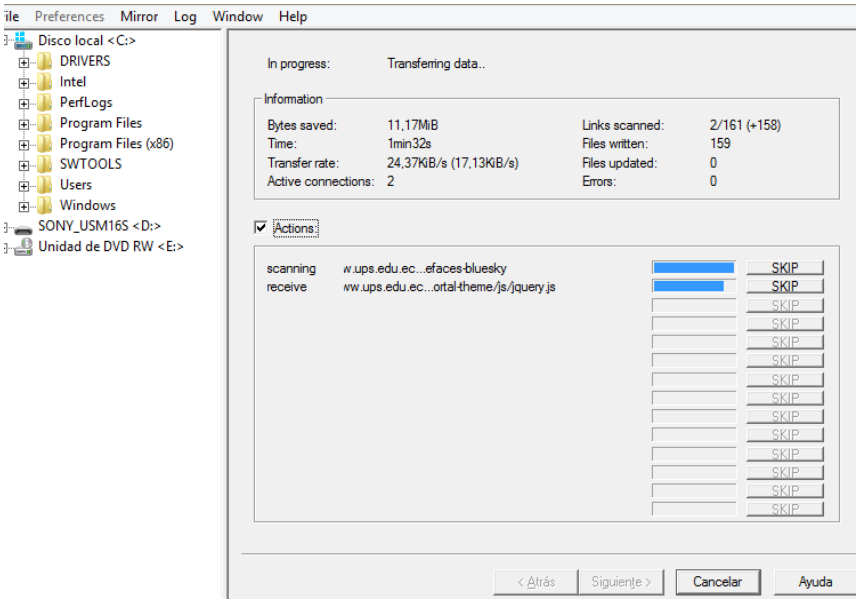


Figura 4.16. Clonación de la página web de la UPS por medio de HTTrack

Elaborado por: Dennis Carcelén, Carlos Ríos

4.3.1.1 Clonación de la página web usando Ettercap

Para automatizar el proceso completo, en la suite de Kali existen herramientas precargadas que realizan de manera global todas las etapas. Este procedimiento se considera un ataque de principio a fin, puesto que para redirigir a la víctima, la herramienta SET TOOL KIT clona una página (de preferencia que tenga cuadros de dialogo en los que se requiera ingreso de cuenta y contraseña), esta página consta ya de un cambio en el código que permite guardar la información en un archivo de texto (credential harvesting). Posteriormente, se requiere envenenar las peticiones al servidor

DNS disponible en la red y crear una respuesta ilegitima a la petición de nombre de dominio. Con lo cual el usuario escribirá una dirección URL correcta pero el dns responde con otra dirección que no corresponde a la original del sitio web. Esto es posible mediante la herramienta ETTERCAP, la cual realiza un ataque denominado DNS spoofing, que es el proceso ya descrito anteriormente.

En la Figura 4.17. se puede observar la selección de la herramienta SET Tool Kit en la suite Kali Linux.

Selección de SET Tool Kit.

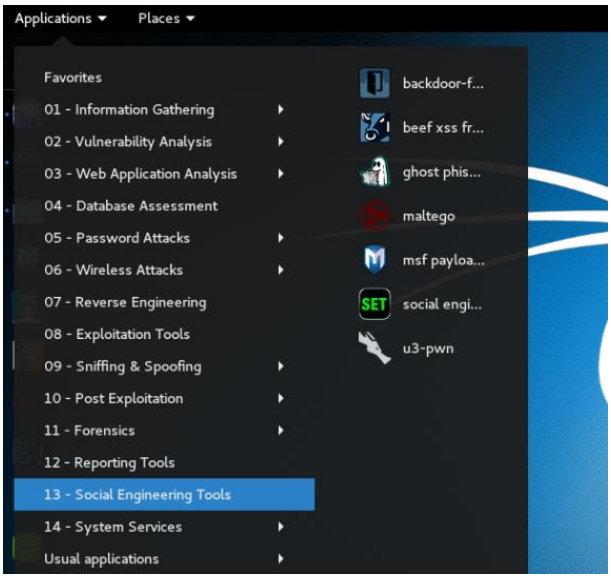


Figura 4.17. Clonación de la página web de la UPS por medio de Set Tool Kit

Elaborado por: Dennis Carcelén, Carlos Ríos

El resultado de la clonación de la página se visualiza dirigiéndose en el navegador a la dirección IP que tiene establecida la maquina con la suite Kali-Linux, que en este caso es la *192.168.1.3*. La página presenta ciertas fallas por el idioma español por lo que podría detectarse que no es el sitio oficial de la institución. Lo anteriormente descrito se muestra en la Figura 4.18.

Página Web Institucional Clonada

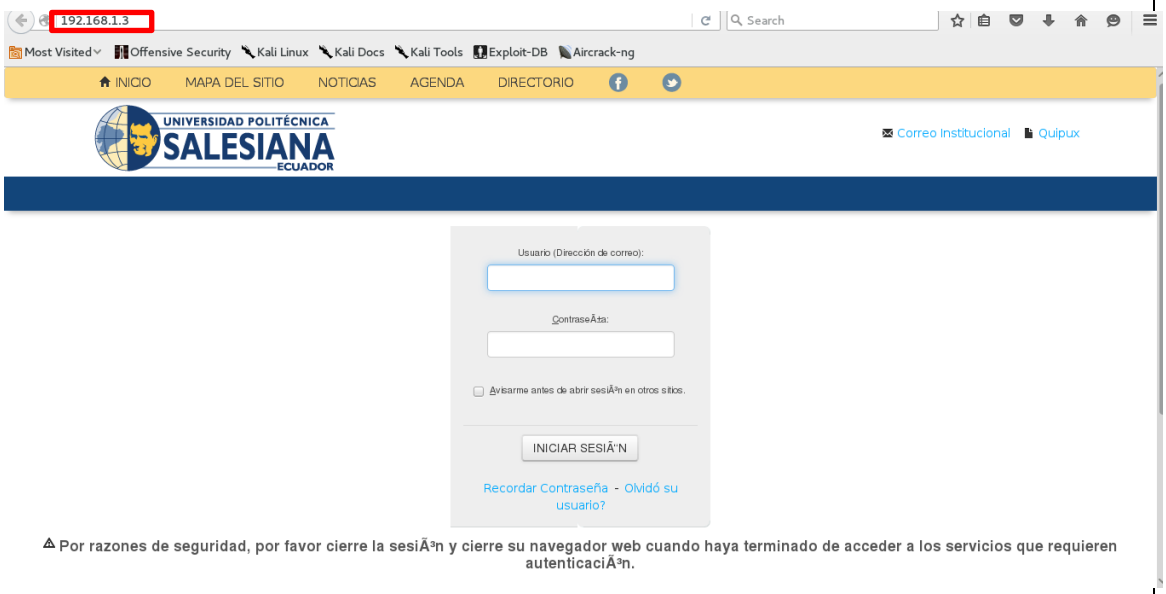


Figura 4.18. Resultado de la Clonación de la página web de la UPS

Elaborado por: Dennis Carcelén, Carlos Ríos

Los archivos de esta página están contenidos en un archivo de tipo HTML. Adicionalmente en este fichero se encuentra un archivo que tiene una matriz que irá guardando las credenciales de las posibles víctimas. La Figura 4.19. muestra el resultado de este proceso.

Archivo de Registro

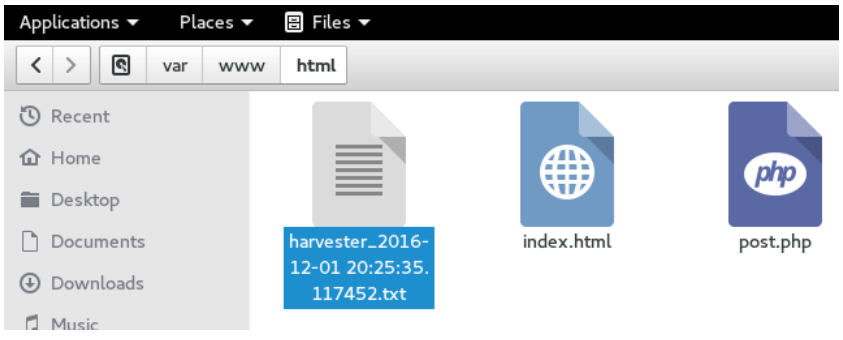


Figura 4.19. Fichero en donde se guardan las credenciales obtenidas

Elaborado por: Dennis Carcelén, Carlos Ríos

Se efectúa el ataque por medio de la herramienta Ettercap y el resultado se muestra en la Figura 4.20. donde se visualiza el sitio con spoofing. Se debe notar que la dirección URL no corresponde al sitio desplegado.

Spoofing de la página Web Institucional

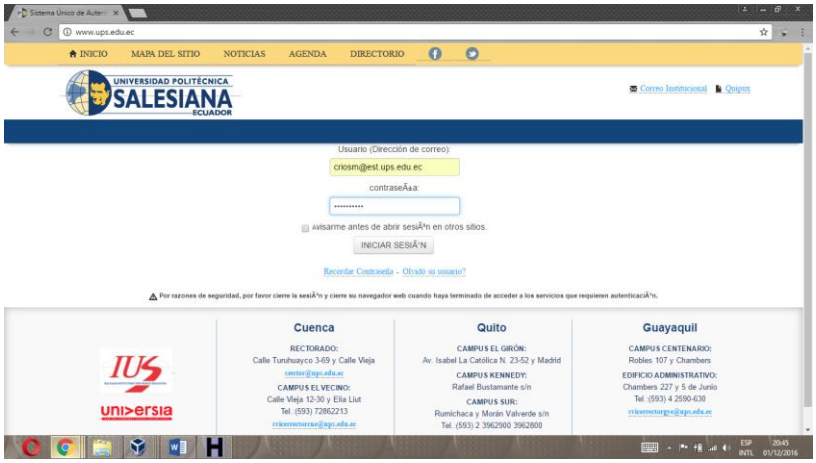


Figura 4.20. Resultado del spoofing de la página institucional

Elaborado por: Dennis Carcelén, Carlos Ríos

En la consola de ettercap se muestra las credenciales obtenidas de la víctima. El resultado se muestra en la Figura 4.21.

Resultado de la captura de datos introducidos por la victima

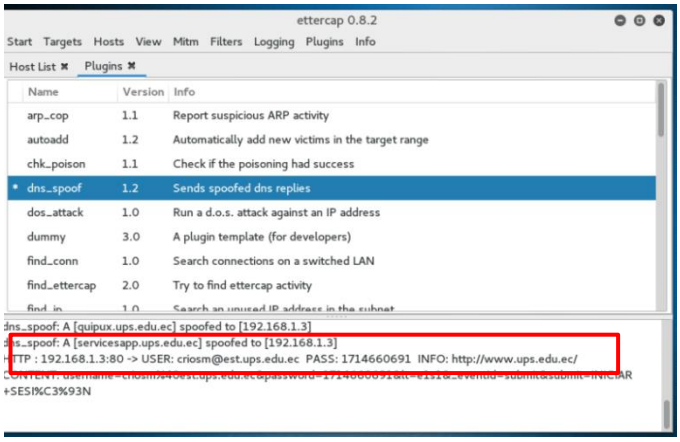


Figura 4.21. Captura de credenciales obtenidas por ettercap

Elaborado por: Dennis Carcelén, Carlos Ríos

CONCLUSIONES

La honeynet fue realizada desde el punto de vista de vector interno, con lo cual se concluye que el desconocimiento y la falta de capacitación del personal que hace uso de la red, en el tema de seguridad y las potenciales amenazas existentes, hace que la parte más vulnerable en la seguridad informática sean los propios usuarios, puesto que si amenazas como el malware están siempre latentes, es el usuario y sus malas prácticas los que aumentan el riesgo y la efectividad del software malicioso. La falta de preocupación y desconocimiento sobre cómo mantener la privacidad de la información, hace que el vector interno de seguridad siempre represente una vulnerabilidad ante amenazas que no dependen de las seguridades implementadas a nivel de red del campus sur.

Mientras que la red de la Universidad consta de una seguridad a profundidad, la cual es aplicada por niveles y sirve para afrontar cualquier amenaza desde el exterior, el conocimiento estructural tanto físico del establecimiento como lógico de la red por parte de personal administrativo, docencia, estudiantado o en caso de filtración de información sensible hacia terceros, puede ser aprovechado ventajosamente para realizarse ataques de intrusión o incluso ser víctima de uno por desconocimiento, descuido o negligencia. Para llevar a cabo estas técnicas se puede usar ingeniería social y además utilizar áreas del campus en los que no figure seguridad física permanente, principalmente en laboratorios con equipo computacional (uso de BadUSB), los cuales no tienen un acceso restringido de personal y que podrían representan cierto riesgo.

En primera instancia, la seguridad lógica radica en establecer claves robustas para restringir el acceso a personas no autorizadas a la red; al llevar a cabo un proceso satisfactorio de crackeo por fuerza bruta se comprueba que para el honeypot, siendo este un sistema que figura como una supuesta parte sensible de red (servidores), la clave establecida no es la adecuada. Con esto se puede concluir que el uso no responsable de contraseñas facilita un proceso de crackeo y que, en determinados casos, el tiempo a

invertir para acceder en áreas restringidas puede ser mayor que el beneficio de obtener información confidencial; no obstante, no ocurre así con los usuarios dentro de la red, ya que fácilmente se pueden realizar ataques de phishing o MITM (man in the middle) haciendo que la información que el usuario maneja llegue de forma más rápida y sencilla al atacante.

El honeypot KIPPO de media interacción no es muy fiable puesto que de realizarse una intrusión exitosa, se puede detectar que es un script y no un sistema operativo, debido a la devolución por parte del honeypot de respuestas erróneas e inesperadas a los comandos proporcionados en el Shell, por lo que los honeypots de alta interacción satisfacen las necesidades y los propósitos de investigación planteados.

Se constató que el IDS Snort incorporado en la herramienta Honeywall al realizarse el despliegue de la honeynet de modo virtualizado, capta que el anfitrión por si solo levanta una cantidad promedio de 80 falsos positivos por cada hora al interactuar con la máquina virtual del honeypot, y que en la prueba realizada, funciona según lo esperado frente a los ataques realizados, mostrando los 1000 paquetes ICMP enviados en el barrido de puertos y un único paquete ICMP enviado mediante el nmap ejecutado a cada puerto de servicio específico.

RECOMENDACIONES

Dada la gran cantidad de usuarios inalámbricos que existen en la UPS y a la gran cantidad de personas con conocimientos en diferentes departamentos de ciencia y tecnología, es pertinente implementar este tipo de sistemas de seguridad en diferentes áreas físicas del Campus con el propósito de establecer y personalizar las seguridades por cada una de las áreas dependiendo del perfil del usuario. Esta medida se puede llevar a cabo con el uso del Wireless lan controller para difundir la red trampa en el campus y mediante HoneySpots (*Honeypot-HotSpot*) aumentar la escalabilidad de auditoria hacia pentesting en dispositivos móviles (como el Smartphone Pentest Framework, o su predecesor Dagah Mobile Penetration Testing Software, por ejemplo).

Se recomienda llevar la implementación a equipos físicos en su totalidad para la puesta en funcionamiento de la red, ya que el proyecto tiene un diseño con características de prototipo, es decir que replica un escenario lo más semejante a un área de trabajo y producción con la utilización del mínimo número de hardware de computación y redes, para no incurrir en costos de los mismos, y fue necesario el uso de tecnología de virtualización, de lo cual la mayor desventaja encontrada fue la disminución del rendimiento del equipo anfitrión y ciertos fallos ocasionales en los adaptadores de red, dejando así ordenadores sin conectividad y por ende la red inoperativa.

Utilizar herramientas que permitan ambientes gráficos en Linux proporciona ciertas facilidades para los usuarios preferencialmente familiarizados con Windows, permitiendo así, para este caso específico, una mejor administración de puertos de red. Resulta conveniente utilizar la distribución CentOS 7, la cual viene con cambios significativos de interfaz e incorpora FirewallD que adicionalmente con la herramienta Webmin es sencillo administrar que puertos permanecerán activos después de un reinicio del sistema según convenga para las pruebas posteriores.

REFERENCIAS BIBLIOGRÁFICAS

¿Qué es el Hacking? | Seguridad en Sistemas y Técnicas de Hacking. TheHackerWay (THW). (s. f.). Recuperado 20 de diciembre de 2016, a partir de https://thehackerway.com/about/

Borja, E. R., & Jarrin, J. R. (2015). *Implementacion e integracion de la Red WLAN de la Universidad Politecnica Salesiana (UPS), Sede Quito-Campus Sur, al proyecto Internacional EDUROAM*. Universidad Politécnica Salesiana.

Castaño, P. (2014). Honeypots (Nivel básico – Aspectos prácticos). Recuperado 14 de diciembre de 2016, a partir de http://www.gr2dest.org/honeypots-nivel-basico-aspectos-practicos/

Chavarri, J. (2015). Conociendo al Enemigo: Honeypots.

Cisco 2500 Series Wireless Controllers - Cisco 2500 Series Wireless Controllers - Cisco. (s. f.). Recuperado a partir de http://www.cisco.com/c/en/us/products/wireless/2500-series-wireless-controllers/index.html#

Cisco 2851 Integrated Services Router - Cisco. (s. f.). Recuperado a partir de http://www.cisco.com/c/en/us/products/routers/2851-integrated-services-router-isr/index.html

CISCO 2851 Integrated Services Router - CISCO2851 : Almacen Informatico. (s. f.). Recuperado a partir de http://www.almacen-informatico.com/CISCO_2851-integrated-services-router-CISCO2851_32762_p.htm

Cisco 7604 Chassis Data Sheet - Cisco. (s. f.). Recuperado a partir de http://www.cisco.com/c/en/us/products/collateral/routers/7604-router/product_data_sheet0900aecd8027cc3e.html

Cisco Catalyst 3750-48PS Switch - Cisco. (s. f.). Recuperado a partir de http://www.cisco.com/c/en/us/support/switches/catalyst-3750-48ps-

switch/model.html

Cisco Catalyst 3750 Series - Netsource GlobalNetsource Global. (s. f.). Recuperado a partir de https://netsourceglobal.com/products/cisco/switches/cisco-catalyst-3750-series/

Cisco Catalyst 3750 Series Switches Data Sheet - Cisco. (s. f.). Recuperado a partir de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/product_data_sheet0900aecd80371991.html

Deyvi, I., & Perez, B. (s. f.). γένεσις.

El fenómeno BYOD genera adictos al trabajo - BAQUIA. (s. f.). Recuperado 20 de diciembre de 2016, a partir de https://www.baquia.com/emprendedores/2012-08-24-el-fenomeno-byod-genera-empleados-adictos-al-trabajo

Escobar, F. (s. f.). Sistema de Prevención de Intrusos (IPS) | blog-del-informatico. Recuperado 20 de diciembre de 2016, a partir de http://frankyagami28.wixsite.com/blog-del-informatico/single-post/2015/09/13/Sistema-de-Prevención-de-Intrusos-IPS

Gallego, R. (s. f.). Honeypot. Recuperado 20 de diciembre de 2016, a partir de http://documents.mx/documents/-se-denomina-honeypot-al-software-o-conjunto-de-computadores-cuya-intencion.html

Gonzalez, D. (2003). *Sistemas de Detección de Intrusiones*. https://doi.org/10.1017/CBO9781107415324.004

IDS - EcuRed. (s. f.). Recuperado 20 de diciembre de 2016, a partir de https://www.ecured.cu/IDS

Introducción a las Honeynets. (s. f.).

Mena, D. X., & Jara, J. J. (2013). *Análisis, Diseño y Propuesta de Implementación de un Portal Cautivo para la Red Inalámbrica de la Universidad Politécnica Salesiana Sede Quito Campus Sur*. Universidad Politecnica Salesiana.

Mifsud, E. (2012). MONOGRÁFICO: Introducción a la seguridad informática -

Seguridad de la información / Seguridad informática. Recuperado 26 de octubre de 2016, a partir de http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=1

Montalván, C. A. (2010). *Análisis del tráfico maliciosos de los servicios externos de la UTPL*.

Moreno, M. A., & Tipán, L. A. (2015). *Diseño de una Red de Alta Disponibilidad para la Universidad Politécnica Slaesiana Sede Quito Campus Sur*. Universidad Politécnica Salesiana.

Preguntas Frecuentes sobre el Diseño y las Funciones de Wireless LAN Controller (WLC). (2008). Recuperado a partir de http://www.cisco.com/cisco/web/support/LA/10/106/106618_wlc-design-ftrs-faq.html

Quinchaguano, D. F. (2016). *Diseño e implementación de un prototipo de Honeynet en la red de datos de la Escuela Politécnica Nacional*. Quito, 2016.

Santana, C. (s. f.). Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? - Aprende a Programar - Codejobs. Recuperado 20 de diciembre de 2016, a partir de https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

Sepa qué es el hacking. (s. f.). Recuperado 20 de diciembre de 2016, a partir de http://rpp.pe/tecnologia/mas-tecnologia/sepa-que-es-el-hacking-noticia-457084

Spanish Honeynet Project. (s. f.). Recuperado a partir de http://pt.slideshare.net/vaceitunofist/spanish-honeynet-projectv1

Spitzner, L. (s. f.). Know Your Enemy: Sebek A kernel based data capture tool. Recuperado a partir de http://www.honeynet.org

Spitzner, L. (2008). Honeywall CDROM | The Honeynet Project. Recuperado 24 de noviembre de 2016, a partir de https://www.honeynet.org/project/HoneywallCDROM

UltimaTecnología » ranura. (s. f.). Recuperado a partir de http://viasatelital.com/blogs/?tag=ranura

Ventura, Y. L., & Rodriguez, N. A. (2008). *Diseño y desarrollo de Honeynets virtuales utilizando VMWARE, para la detección de intrusos informáticos*. Universidad Francisco Gavidia. Recuperado a partir de http://hdl.handle.net/11592/7102