INVESTIGACIÓN

PENTESTING EMPLEANDO TECNICAS DE ETHICAL HACKING EN REDES IPv6

PENTESTING ETHICAL HACKING TECHNIQUES USING NETWORK

Ing. Jorge Armando Rojas Osorio [a] Msc. Yurley Constanza Medina Cardenas [b] MSc. Dewar Rico Bautista [c]

[a]Universidad Francisco de Paula Santander Ocaña. Grupo de Ingeniería en Innovación, Tecnología y Emprendimiento – GRIITEM. Ocaña, Colombia, jorgearmandor@gmail.com

[b]Universidad Francisco de Paula Santander Ocaña. Grupo de Investigación en Ingenierías Aplicadas – INGAP, Ocaña, Colombia, ycmedinac@ufpso.edu.co

[c]Universidad Francisco de Paula Santander Ocaña. Grupo de Ingeniería en Innovación, Tecnología y Emprendimiento – GRIITEM, Ocaña, Colombia, dwricob@ufpso.edu.co

Fecha de recepción: 02-10-2016 **Fecha de aprobación:** 04-12-2016

Resumen: A través de este artículo se muestran los resultados de un proyecto de investigación, realizando un pentesting empleando técnicas de ethical hacking en redes implementadas en el Protocolo IP en su versión 6 (IPv6), a través de una herramienta de distribución GNU/Linux de seguridad informática, BackTrack, la cual es aplicada en el ámbito de las auditorias, facilitando la búsqueda de vulnerabilidades en los sistemas. Se realiza la recolección de datos, predicción e identificación de las relaciones que existen entre dos o más variables, se exponen, se resume la información de manera cuidadosa y luego se analizan los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

Palabras clave: Acceso a la información, Protección de datos, Red informática, Sistema informático, Transmisión de datos.

Abstract: Through this paper, it present the results of a research project, conducting a pentesting using techniques of ethical hacking into networks implemented in the IP protocol version 6 (IPv6), through a tool for GNU / Linux security computer, BackTrack, which is applied in the field of audits, facilitating the search for vulnerabilities in systems. It performs data collection, prediction and identification of relationships between two or more variables, are presented, summarizing the information carefully and then analyzed the results, in order to draw meaningful generalizations that contribute to knowledge.

Keywords: Access to information, Computer networks, Computer systems, Data protection, Data transmission.

1. INTRODUCCIÓN

La seguridad de la información que se transmite en las redes de datos es un aspecto fundamental, debido a que la aplicación de estas técnicas protege el acceso abusivo de personas que atentan diariamente en contra de organizaciones. (Lobo & Rico, 2012) (Santos & Rico, 2007) (Rico & Medina, 2008)

Existen diferentes kits de herramientas automatizadas con las cuales se aplican distintos tipos de pruebas de ataques reales, para luego corregir los fallos presentados. De manera gratuita se distribuyen algunos de los mencionados kits, siendo estos accesibles a muchos expertos de auditorías de seguridad, además a personas que aplican las herramientas de manera delictiva.

La herramienta GNU/Linux BackTrack 5.0 es un kit desarrollado por una comunidad de expertos, ver figura 1, la cual contiene diferentes módulos de herramientas para ser empleados en distintas pruebas de penetración, en las que se pueden usar aplicaciones para búsqueda de información, scanners de puertos y vulnerabilidades, testeo en aplicaciones web, ruptura de contraseñas, auditorías a infraestructuras Wirelees y redes Bluetooth; además un módulo para la realización de análisis forense digital. (A. Peterson, 2009) (Bonetti & Viglione, 2013)

Fig. 1. Logo distribución BackTrack.
Fuente: Autor

El proceso estuvo fundamentado en una investigación descriptiva, la cual consiste en llegar a conocer situaciones y actitudes predominantes de un objeto de estudio a través de la descripción exacta de las actividades, objetos, procesos a llevar a cabo la investigación. El objetivo no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables. Los investigadores no son tabuladores, sino que recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento. (Boynton, 2007) (Carrier, 2005)

2. METODOLOGÍA

- ***2.1 Técnicas e instrumentos de recolección de información***

Para la presente investigación fue necesario aplicar la técnica de observación estructurada la cual se lleva a cabo cuando se pretende probar una hipótesis o cuando se quiere hacer una descripción sistemática de algún fenómeno. El instrumento mediante el cual se va a obtener la información para aplicar esta técnica es una ficha de observación para los laboratorios que se van a realizar durante el desarrollo del presente estudio.

El respectivo análisis de la información se realizará cuando la ficha de observación contenga los resultados de los laboratorios, los cuales se generaran durante la ejecución de la investigación.

2.2 Metodología del pentest

El desarrollo de fases basadas en metodologías de testeo, permite la ejecución y la obtención de resultados paso a paso de manera organizada, con la aplicación de las respectivas técnicas de ethical hacking.

2.2.1 Fases de pentest

Las fases que se representan en la figura 2, corresponden a un ataque pasivo, en donde no se altera la información contenida en los sistemas, aquí solo se analiza la red de datos y se observan que servicios se prestan dentro de esta misma.

Fig 2. Fases de Pentesting.
Fuente: Autor

Respectivamente las fases que se representan con color rojo, son ataques activos, donde se consiguen accesos abusivos a los sistemas, intercepción de las comunicaciones y modificaciones en los diferentes equipos de la red.

2.2.2 TÉCNICAS DE HACKING Y RESULTADOS

Las pruebas de laboratorio se desarrollaron en una red de área local en los dos Protocolos de Internet IPv4 e IPv6 configurada en ambientes controlados, donde se arrojan los resultados de los tests correspondientes en cada fase. (Chi-Hsiang & Dwen-Ren , 2009) (Jaquith, 2007) (KRUTZ & VINES, 2007) (Lyubimov, 2010)

a. **Recopilación de información**. En esta fase se llevan a cabo las pruebas que consiste en la búsqueda de servidores DNS y sus subdominios dentro de la red de datos, empleando la interrogación a los mismos, con el fin obtener las direcciones IP correspondientes de cada servidor de la red; además se trata de realizar un transferencia de zona DNS usando la

técnica de diccionarios a fuerza bruta, para así obtener la información detallada de la configuración que contiene el host analizado, ver figura 3. (Stallings, 2011)

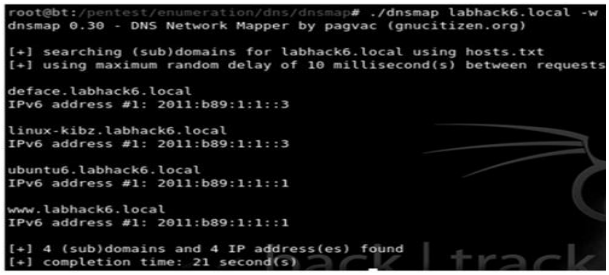


Fig. 3. Enumeración subdominios Dnsmap.
Fuente: Autor

b. **Escaneo.** En esta etapa se aplican diferentes técnicas empleadas sobre la red de datos, la primera es la identificación de equipos vivos en la red, esto se hace por medio de sondeos de ping; el escaneo consiste en enviar paquetes ICMP Echo Request a todos los equipos de la red y se enumeran los equipos que responden de manera exitosa a este llamado con paquetes ICMP Echo Reply, ver figura 4. (Zhihong & Wei, 2014) (Yadav & Dong, 2014) (Wysopal & L. , 2006)

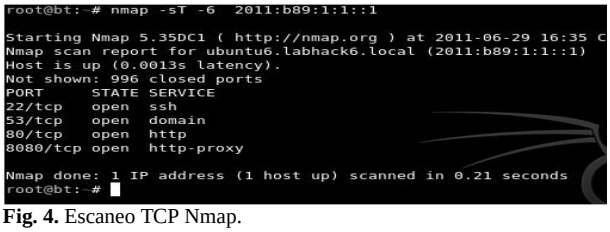


Fig. 4. Escaneo TCP Nmap.
Fuente: Autor

La segunda técnica usada consiste en el escaneo de puertos de comunicaciones, utilizando para esto sondeos TCP y UDP, para la búsqueda de servicios prestados en la red; donde, en la comunicación se lleva a cabo el proceso de saludo de las tres vías, en el cual el cliente aplica el envío de paquetes SYN a todos los puertos del servidor, en donde se solicita la conexión al servicio por el puerto especifico, y de esta forma el host analizado retorna el estado en el que se encuentra el puerto; el resultado del escaneo depende del sondeo empleado, ver figura 5. (Sansurooah, 2006) (Rico Bautista, Quel Hermosa, & Carvajal Mora, 2011)

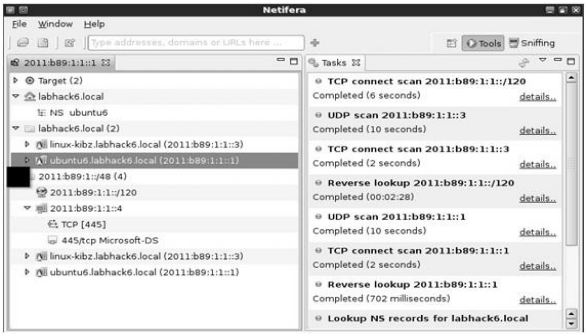


Fig. 5. Múltiples escaneos.
Fuente: Autor

La otra técnica es el escaneo de sistema operativo denominada OS fingerprinting, la cual se basa en la respuesta de que sistema operativo usa el sistema escaneado, esto dependiendo de los valores que contengan los flags de los escaneos y las técnicas empleadas.

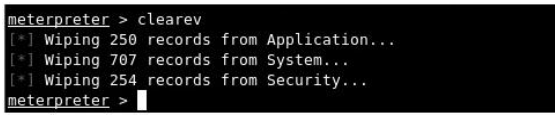
c. **Ataque.** Esta fase corresponde a la acción que se tomara en contra del host objetivo ya analizado en los pasos

anteriores, con el empleo de esta técnica se busca tratar de obtener información relevante de bases de datos, credenciales de otros usuarios de la red, así como el acceso o la caída del mismo.

Se destacan tres tipos de ataques comunes:

- **SQL Injection.** Esta técnica se emplea para la infiltración de código dentro de las aplicaciones que emplean motores de bases de datos, con el fin de conseguir información y la alteración de la misma; los códigos son aplicados en campos validación de entradas que generan errores de sintaxis SQL, en estos campos se emplean varias técnicas de consultas a base de datos para obtener de forma abusiva la información contenida en ellas, ver figura 6.

Fig. 6. Tabla extraída de base de datos.
Fuente: Autor

- 

Cros Site Scripting. Es un agujero de seguridad en aplicaciones web, basado en la explotación de vulnerabilidades del sistema de validación de HTML incrustado. Este método consiste en la inserción y ejecución de código de "scripting", como VBScript o JavaScript dentro de campos de validación o búsqueda, y así alterar el contenido de las páginas o aprovechar acceso a los sistemas, ver figura 7.

Fig. 7. Acceso a cliente.
Fuente: Autor

- Un desbordamiento de buffer es un error de programación que se produce cuando la aplicación no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada, de manera que si dicha cantidad es superior a la capacidad pre asignada los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original generando el desbordamiento del buffer.

d. **Escalada de privilegios.** En la técnica de escalada de privilegios se busca que un usuario con limitaciones que toma el control del objetivo es capaz, mediante algún fallo de seguridad, subir su rol hasta hacerse con más privilegios, esto con el fin de ejecutar sus códigos sin complicaciones, de igual forma tener la administración sobre el objetivo, borrar los rastros dejados del ataque y garantizar que su acceso no sea interrumpido, ver figura 8.

Fig. 8. Comandos escalada de privilegios.
Fuente: Autor

e. **Instalación de puertas traseras.** En esta fase del test de penetración el objetivo es la instalación de un *backdoor*, esta técnica consiste en que el atacante luego del acceso al sistema, crea un canal encubierto de comunicación entre los dos hosts, esto con el fin de realizar posteriores accesos a los sistemas de una manera más rápida, de esta manera no es necesario volver a repetir las técnicas empleadas en el momento que se consiguió el acceso, ver figura 9.

Fig. 9. Instalación de un Backdoor.
Fuente: Autor

f. **Borrado de Logs.** La fase del borrado de logs o de rastros, es la última que se lleva a cabo, en la cual el objetivo primordial es limpiar todos los registros del sistema o eventos creados en el momento del ataque y las posteriores acciones que hayan sido cometidas en contra del mismo; esta técnica se aplica con el fin de que no quede rastro alguno de los ataques en el sistema comprometido, dando parte de tranquilidad al atacante al no encontrase prueba alguna de modificaciones y accesos causados en los sistemas de cómputo, ver figura 10.

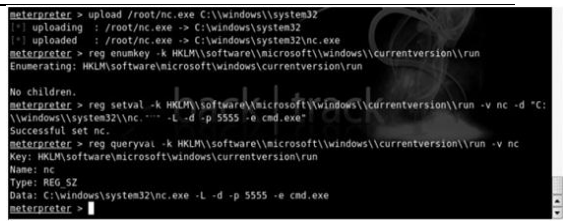


Fig. 10. Eliminación de rastros.
Fuente: Autor

3. RESULTADOS

Las pruebas llevadas a cabo para la presente investigación se desarrollaron en una Red de Área Local bajo la arquitectura cliente servidor y la aplicación de los laboratorios se realizó implementando los módulos de herramientas que correspondan a cada una de las fases planeadas para el desarrollo del test de penetración. (Mcclure & Scambray, 2010) (Melchor Medinaa, Lavín Verástegui, & Pedraza Melo, 2012) (Mora Luis & Carrau Mellado,, 2013)

La estructura de los laboratorios está dada por la siguiente metodología propuesta por el autor de la investigación: Título, Objetivos, Escenario de trabajo, Programas, Configuraciones, Pruebas, Conclusiones

3.1 Laboratorios realizados

3.1.1 Interrogación y escaneo a fuerza bruta los servidores de sistema de nombres de dominio con herramientas del módulo DNS de recopilación de información.

Objetivos

- Escanear rangos de direcciones **IP** para la búsqueda de servidores **DNS** para la posterior búsqueda de subdominios y registros de las zonas aplicando la herramienta **Dnsrecon**.

- Interrogar los diferentes hosts encontrados con las herramientas de consulta **dig**, **host** y **nslookup.**
- Transferir la zona del servidor de nombre de dominios para obtener las configuraciones correspondientes a dicho servidor empleando la herramienta **DNS-Walk**.
- Enumerar y transferir a fuerza bruta la configuración de las zonas **DNS** de la red utilizando la herramienta **DnsEnum.**
- Buscar todos los subdominios existentes en la red aplicando la herramienta **Dnsmap** con técnicas de diccionarios de fuerza bruta.
- Escanear rangos de direcciones **IP** para la búsqueda de subdominios en la red y transferir las zonas correspondientes por medio de la herramienta **Fierce.**

Escenario de trabajo

La práctica de laboratorio se elaboró en la red configurada bajo la arquitectura cliente-servidor empleando para este laboratorio dos hosts como servidores y un host como cliente. Los sistemas operativos que componen la red experimental van a estar configurados bajo los siguientes parámetros de red, ver figura 11.

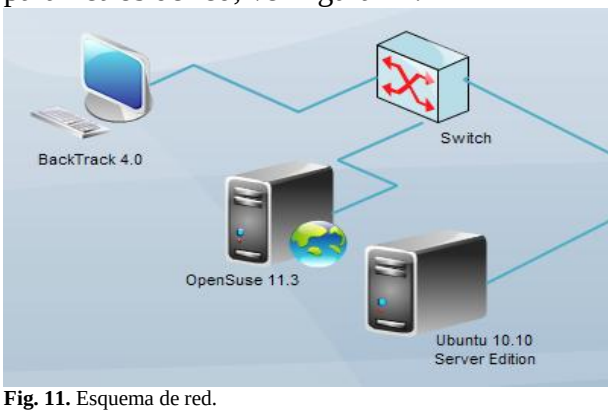


Fig. 11. Esquema de red.
Fuente: Autor

Computador 1 (Servidor 1)

Sistema Operativo: *Ubuntu 10.10 Server Edition*
Dirección IPv4: *192.168.42.200*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.200*
Servidor DNS Alternativo: *Ninguno*

Computador 2 (Servidor 2)

Sistema Operativo: *Open Suse 11.3*
Dirección IPv4: *192.168.42.242*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.200*
Servidor DNS Alternativo: *Ninguno*

Computador 3 (Cliente)

Sistema Operativo: *BackTrack 4.0*
Dirección IPv4: *192.168.42.103*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.200*
Servidor DNS Alternativo: *Ninguno*

Programas (Software utilizados)

Ubuntu 10.10 Server Edition, OpenSuse 11.3, BackTrack 4.0, Servidor LAMP (Linux, Apache, Mysql, PHP), Servidor Bind 9, Servidor DHCP3-Server, Aplicación DVWA 1.0.7, Webmin 1.560, Dnsrecon, Dig, Host, Nslookup, DNS-Walk, DnsEnum, Dnsmap, Fierce

Conclusiones

- El escaneo de rangos de direcciones **IP** permite enumerar los diferentes servidores **DNS** y subdominios existentes dentro de la red de datos escaneada.
- Por medio de la interrogación de los servidores **DNS** se descubren las direcciones **IP** correspondiente a los mismos.

- El uso de técnicas de diccionarios a fuerza bruta puede permitir la transferencia de zona de los servidores escaneados propietarios de la misma.
- En muchos casos las transferencias de zona no se hacen de forma completa, ya que muchos servidores traen por defecto permitir la operación solo a los equipos especificados.

3.1.2 Identificación de equipos vivos en la red, escaneo de puertos, servicios y sistema operativo empleando herramientas del módulo de mapeo de red.

Objetivos

- Identificar los equipos vivos en la red aplicando la técnica de sondeos de Ping utilizando **Fping**.
- Enumerar el listado de direcciones **IP** que responde a un sondeo de Ping con la herramienta **Genlist.**
- Listar todos los equipos vivos de la red con múltiples sondeos aplicados con la herramienta **Angry IPScan.**
- Llevar a cabo diferentes escaneos de puertos y servicios, así como consultas de servidores **DNS** con la herramienta **Netifera.**
- Emplear la herramienta **Nmap** para la realización de diferentes sondeos para identificación equipos vivos en la red, puertos y servicios, sistema operativo, evadiendo Firewalls e **IDS**.
- Identificar los sistemas operativos de los equipos empleando la técnica OS-Fingerprinting por medio de la herramienta **Xprobe2.**

Escenario de trabajo

La práctica de laboratorio se elaboró en una red de área local bajo la arquitectura cliente-servidor con tres hosts y un host respectivamente. Los sistemas operativos que componen la red experimental van a estar configurados bajo los siguientes parámetros de red, ver figura 12.

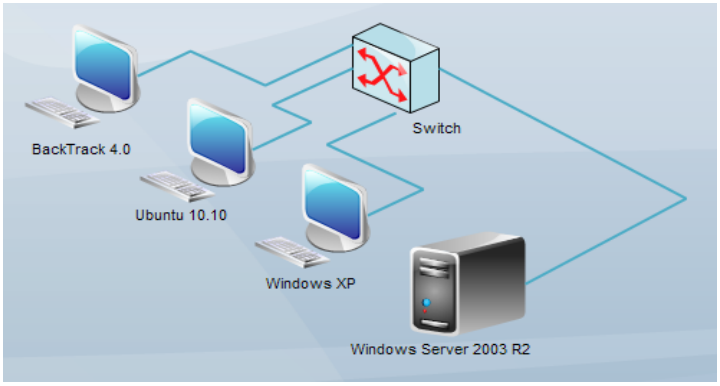


Fig. 12. Esquema de red.
Fuente: Autor

Computador 1 (Servidor)
Sistema Operativo: *Windows Server 2003 R2*
Dirección IPv4: *192.168.42.210*
Mascara de Subred: *55.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Computador 2 (Cliente 1)
Sistema Operativo: *Ubuntu 10.10*
Dirección IPv4: *192.168.42.111*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Computador 3 (Cliente 2)
Sistema Operativo: *BackTrack 4.0*
Dirección IPv4: *192.168.42.113*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Computador 4 (Cliente 3)
Sistema Operativo: *Windows XP SP3*
Dirección IPv4: *192.168.42.114*

Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Programas (Software utilizados)
Windows Server 2003 R2, BackTrack 4.0, Windows XP SP3, Ubuntu 10.10 Desktop Edition, Servidor WAMP (Windows, Apache, Mysql, PHP), EasyFTP Server (Servidor FTP), Fping, Genlist, AngryIPScan, Xprobe2, Netifera. Nmap. Zenmap. Wireshark

Conclusiones

- El sondeo de ping es una de las técnicas empleadas para la búsqueda de hosts vivos en la red, esto se realiza de una manera rápida ya que solo se llevan a cabo envíos de paquetes **ICMP**.
- El bloqueo de paquetes tipo **ICMP** en los equipos, los cuales son restringidos por firewalls, hacen que los hosts se vuelvan indetectables en la red.
- El escaneo de puertos y servicios es una técnica fundamental, ya que de esta manera se obtiene la información de que servicios se están prestando en la red de datos, con la información obtenida se pueden planear las estrategias para atacar.
- La técnica de OS-Fingerpriting para la detección del sistema operativo juega un papel importante en los escaneos, ya que con los registros obtenidos se confirman las técnicas para obtener el acceso o caída del sistema.
- La detección del sistema operativo depende del tipo de escaneo que haga la herramienta empleada, en caso de operaciones que empleen bases de datos de registros, el acierto depende de los datos contenidos en las mismas.

3.1.3 Búsqueda de vulnerabilidades y ataques a servidores y clientes utilizando las técnicas de SQL Injection, Cross Site Scripting y Buffer Overflow.

Objetivos

- Emplear técnicas de Inyecciones **SQL** automatizadas con las sentencias de consultas más comunes a las bases de datos bajo **MYSQL** empleando **Sqlmap**.
- Enumerar registros como administradores de bases de datos y registros contenidos en los motores de la aplicación con técnicas contenidas en **Sqlmap.**
- Acceder al servidor con la aplicación de las inyecciones automatizadas adicionando exploits y cargas con código vulnerable.
- Buscar vulnerabilidades en códigos **HTML** y directorios abiertos a fuerza bruta de la aplicación contenida en el servidor utilizando la herramienta **nikto2**.
- Escanear la aplicación para la búsqueda de fallos en códigos **HTML** y búsqueda de directorios y archivos contenidos en la misma usando **Webshag GUI.**
- Emplear el escáner **Web Securify** para la enumeración de fallos en las aplicaciones vía web.
- Explotar los campos de la aplicación para obtener credenciales de usuarios y redirección de los mismos a otros servidores de forma manual.
- Explotar navegadores de clientes por medio de un servidor web comprometido para obtener el acceso al sistema con **XSSF** módulo de **metasploit framework**.

- Realizar el desbordamiento de buffer de un servidor **FTP** sencillo instalado dentro de Windows Server 2003 empleando un exploit encargado de la tarea incluido dentro de los cientos contenidos en **metasploit framework.**

Escenario de trabajo

La práctica de laboratorio se elaboró en una red de área local bajo la arquitectura cliente-servidor de tres formas distintas en los cuales se aplicaran tres técnicas de ataque para toma de control de máquinas o caída en los servicios prestados en las redes de datos escaneadas. Para la práctica correspondiente a pruebas de inyecciones SQL a una aplicación web se contó con un servidor donde se tiene instalado un sencillo software en ***PHP*** y el cliente atacante, ver figura 13.

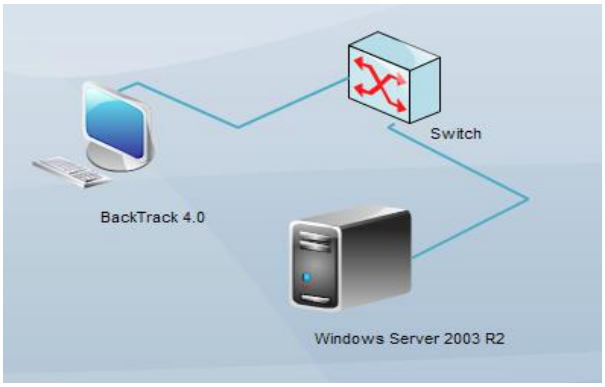


Fig. 13. Esquema de red.
Fuente: Autor

Computador 1 (Servidor)
Sistema Operativo: *Windows Server 2003 R2*
Dirección IPv4: *192.168.42.210*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Computador 2 (Cliente)
Ver taller 3.2.2.

La práctica correspondiente a Cross Site Scripting se compone de dos servidores y dos clientes donde en un servidor se aloja la aplicación web a atacar, el otro es el host a donde se redireccionan a las víctimas y además sirve como interceptor de *cookies*; los clientes corresponden al atacante y a la víctima, ver figura 14.

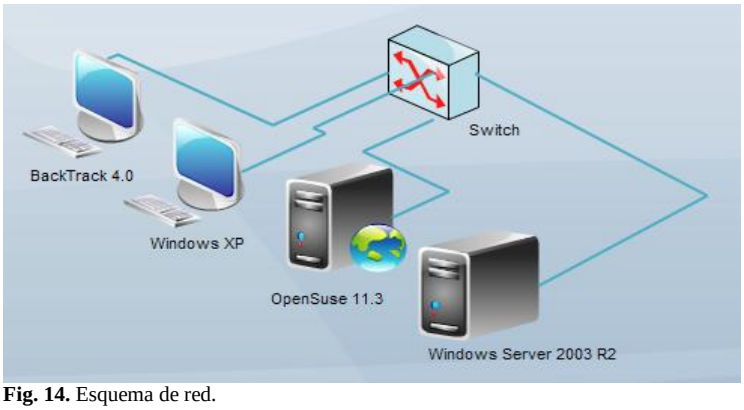


Fig. 14. Esquema de red.
Fuente: Autor

Computador 1 (Servidor 1)
Ver taller 3.2.1.

Computador 2 (Servidor 2)
Ver taller 3.2.1.

Computador 3 (Cliente 1)
Ver taller 3.2.1.

Computador 4 (Cliente 2)
Sistema Operativo: *Windows XP SP3*
Dirección IPv4: *192.168.42.104*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.200*
Servidor DNS Alternativo: *Ninguno*

La práctica de Buffer Overflow se compone de un servidor **FTP** independiente instalado en Windows Server y un cliente que tiene el rol de atacante, ver figura 15.

Fig. 15. Esquema de red.
Fuente: Autor

Computador 1 (Servidor)
Sistema Operativo: *Windows Server 2003 R2*
Dirección IPv4: *192.168.42.210*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Computador 2 (Cliente)
Sistema Operativo: *BackTrack 4.0*
Dirección IPv4: *192.168.42.113*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Programas (Software utilizados)
Windows Server 2003 R2, Ubuntu 10.10 Server Edition, OpenSuse 11.3, BackTrack 4.0, Windows XP SP3, Ubuntu 10.10, EasyFTP Server (Servidor FTP), Servidor LAMP (Linux, Apache, Mysql, PHP), Servidor WAMP (Windows, Apache, Mysql, PHP), Servidor Bind 9, Servidor Postfix, Servidor Dovecot, Servidor DHCP3-Server, Webmin 1.560, Aplicación sencilla en PHP, Aplicación DVWA 1.0.7, Mozilla Firefox, Internet Explorer, Editor Cookie (extensión firefox), Sqlmap, Nikto2, Webshag, Web Securify, Metasploit Framework, Sesión de Meterpreter.

Conclusiones

- Las técnicas de inyecciones SQL automatizadas permiten la búsqueda de errores en las aplicaciones para la enumeración de información importante.
- En ocasiones con la aplicación de inyecciones SQL y la ejecución de exploits se obtiene el acceso y toma de control de la maquina atacada.
- Los directorios abiertos en las aplicaciones web son fundamentales para llevar a cabo la carga de archivos al servidor web donde se alojan dichas aplicaciones
- Los fallos en código **HTML** permiten a atacantes la inyección de scripts con los cuales se modifican páginas webs, se consiguen secuestro de sesiones con intercepción de cookies y redirección de páginas.
- Las vulnerabilidades de los navegadores web permiten la ejecución de códigos malignos con los cuales se obtienen accesos a los clientes.
- Los errores de programación por la no asignación de los espacios de memoria RAM por parte de los desarrolladores a las aplicaciones algunas veces permiten el desbordamiento de buffer obteniendo así la caída del servicio.

3.1.4 Escalada de privilegios y creación de un usuario oculto en el sistema comprometido.

Objetivos

- Elevar los privilegios para ejecución de órdenes en el sistema donde se obtuvo el acceso.
- Crear un usuario oculto en el sistema para administración completa del sistema de manera anónima.

Escenario de trabajo

La práctica comprende un cliente el cual fue penetrado por medio de cualquier técnica, la otra máquina corresponde al atacante, ver figura 16.

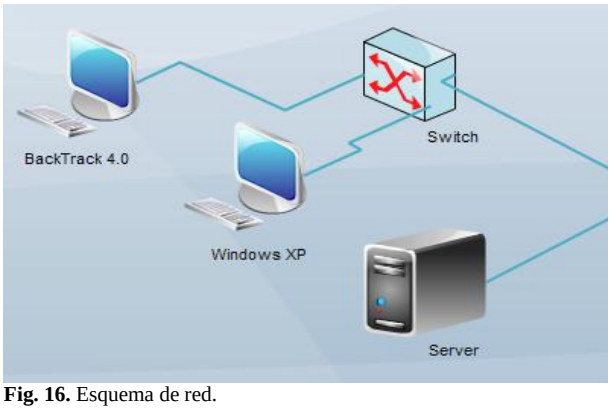


Fig. 16. Esquema de red.
Fuente: Autor

Computador 1 (Servidor)
Sistema Operativo: *Windows Server 2003 R2*
Dirección IPv4: *192.168.42.210*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Computador 2 (Cliente 1)
Sistema Operativo: *BackTrack 4.0*
Dirección IPv4: *192.168.42.113*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Computador 3 (Cliente 2)
Sistema Operativo: *Windows XP SP3*
Dirección IPv4: *192.168.42.114*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Programas (Software utilizados)

Windows Server 2003 R2, Windows XP SP3, BackTrack 4.0, Metasploit Framework, Sesión Meterpreter

Conclusiones

- La aplicación de la técnica de escalada de privilegios permite la ejecución de numerosos códigos y comandos de forma libre debido a la obtención de roles similares a los administradores y usuarios reservados del sistema.
- La creación de un usuario oculto dentro de los equipos permite la administración total de la maquina sin que el administrador se percate de la sesión activa y de que exista ese usuario anonimo.

3.1.5 Instalación de una puerta trasera para posteriores accesos al sistema atacado.

Objetivos

- Instalar un backdoor con **netcat** con extensiones de la carga **meterpreter**

obtenida con el ataque con **metasploit framework.**

- Comprobar la instalación correcta del backdoor conectándose de manera rápida a la Shell instalada en la victima.

Escenario de trabajo

Para la práctica de este laboratorio se emplearon dos máquinas, una corresponde al servidor comprometido del ataque y la otra al cliente atacante, ver figura 17.

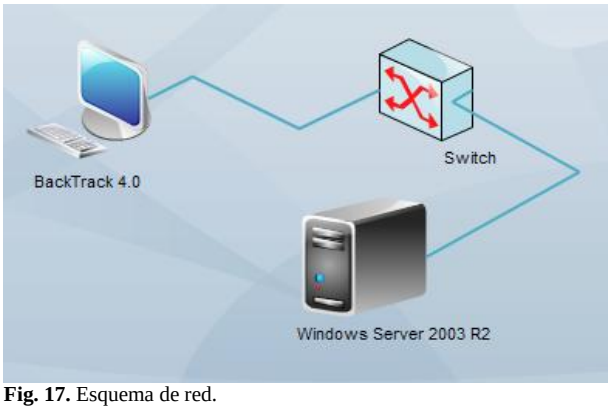


Fig. 17. Esquema de red.
Fuente: Autor

Computador 1 (Servidor)
Sistema Operativo: *Windows Server 2003 R2*
Dirección IPv4: *192.168.42.210*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Computador 2 (Cliente)
Sistema Operativo: *BackTrack 4.0*
Dirección IPv4: *192.168.42.113*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Programas (Software utilizados)

Windows Server 2003 R2, BackTrack 4.0, Measploit Framework, Sesión Meterpreter, Netcat

Conclusiones

- La instalación de una puerta trasera facilita posteriores accesos a los hosts comprometidos ya que no es necesario llevar a cabo de nuevo los procesos en la fase de ataque para obtener el acceso a la máquina.
- La asignación de la Shell de comandos a una sola maquina es muy importante ya que otros clientes no podrán utilizar la puerta trasera instalada.
- **Netcat** es muy utilizada como backdoor, aunque es una herramienta de administración remota, la desventaja es que no requiere autentificación a la hora de la conexión a la maquina donde se ejecuta.

3.1.6 Borrado de logs del sistema.

Objetivos

- Eliminar los rastros en la maquina dejados después de la realización del ataque y las modificaciones que se llevaron a cabo.
- Comprobar que dichos logs fueron eliminados de manera exitosa y así obtener un parte de tranquilidad.

Escenario de trabajo

El escenario correspondiente a la aplicación de la práctica se compone de dos hosts, uno es el servidor comprometido del ataque con varios registros comprometedores y el otro es el atacante, ver figura 18.

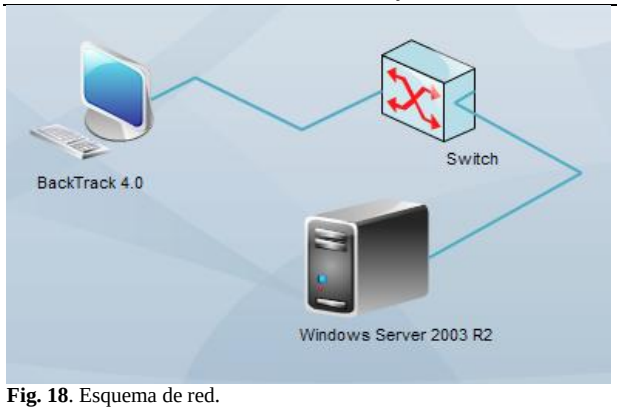


Fig. 18. Esquema de red.
Fuente: Autor

Computador 1 (Servidor)
Sistema Operativo: *Windows Server 2003 R2*
Dirección IPv4: *192.168.42.210*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Computador 2 (Cliente)
Sistema Operativo: *BackTrack 4.0*
Dirección IPv4: *192.168.42.113*
Mascara de Subred: *255.255.255.0*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *192.168.42.210*
Servidor DNS Alternativo: *Ninguno*

Programas (Software utilizados)
Windows Server 2003 R2, BackTrack 4.0, Measploit Framework, Sesión Meterpreter

Conclusiones
- El borrado de los rastros permite al atacante quedar tranquilo ya que los registros de modificaciones y accesos al sistema se eliminan.
- El no borrar los logs se convierte en peligro para el atacante, porque con un análisis de los registros se podría localizar desde que usuario se realizaron alteraciones al sistema.

3.1.7 Test con herramientas que soportan el Protocolo de Internet versión 6 (IPv6).

Objetivos
- Realizar pruebas con herramientas que soportan el nuevo protocolo de internet **IPv6** en los servicios configurados en la red.

Escenario de trabajo
La práctica de laboratorio se va a elaborar en una red de área local con soporte para el protocolo de Internet ***IPv6*** bajo la arquitectura cliente-servidor. Los sistemas operativos que componen la red experimental van a estar configurados bajo los siguientes parámetros de red, ver figura 19.

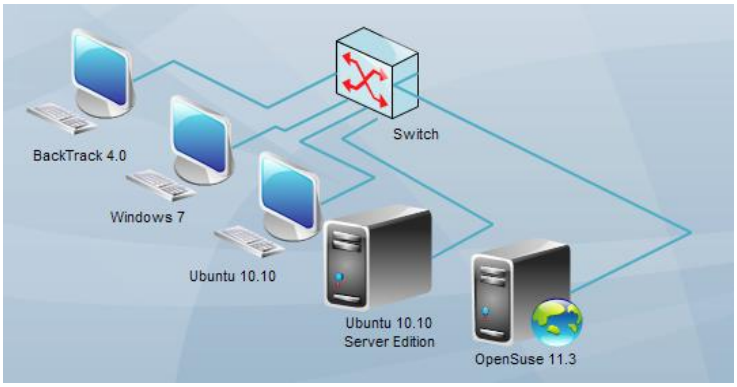


Fig. 19. Esquema de red.
Fuente: Autor

Computador 1 (Servidor 1)
Sistema Operativo: *Ubuntu 10.10 Server Edition*
Dirección IPv6: *2011:b89:1:1::1*
Longitud de Prefijo de red: */125*
Puerta de Enlace Predeterminada: *Ninguno*

Servidor DNS Preferido: *2011:b89:1:1::1*
Servidor DNS Alternativo: *Ninguno*

Computador 2 (Servidor 2)
Sistema Operativo: *Open Suse 11.3*
Dirección IPv6: *2011:b89:1:1::3*
Longitud de Prefijo de red: */125*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *2011:b89:1:1::1*
Servidor DNS Alternativo: *Ninguno*

Computador 3 (Cliente 1)
Sistema Operativo: *BackTrack 4.0*
Dirección IPv6: *2011:b89:1:1::2*
Longitud de Prefijo de red: */125*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *2011:b89:1:1::1*
Servidor DNS Alternativo: *Ninguno*

Computador 4 (Cliente 2)
Sistema Operativo: *Windows 7*
Dirección IPv6: *2011:b89:1:1::4*
Longitud de Prefijo de red: */125*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *2011:b89:1:1::1*
Servidor DNS Alternativo: *Ninguno*

Computador 5 (Cliente 3)
Sistema Operativo: *Ubuntu 10.10*
Dirección IPv6: *2011:b89:1:1::5*
Longitud de Prefijo de red: */125*
Puerta de Enlace Predeterminada: *Ninguno*
Servidor DNS Preferido: *2011:b89:1:1::1*
Servidor DNS Alternativo: *Ninguno*

Programas (Software utilizados)
Ubuntu 10.10 Server Edition, OpenSuse 11.3, BackTrack 4.0, Ubuntu 10.10 Desktop Edition, Windows 7, Servidor LAMP (Linux, Apache, Mysql, PHP), Servidor Bind 9, Webmin 1.560, Aplicación DVWA 1.0.7, Aplicación sencilla en PHP, Mozilla Firefox, Dig, Nslookup, Dnsmap, AngryIPScan, Nmap, Netifera, Web Securify, Metasploit Framework

Conclusiones

- Pocas herramientas cuentan con soporte para el Protocolo de Internet versión 6, con los que muchas técnicas no pueden ser aplicadas en redes configuradas bajo este protocolo.
- No todas las herramientas que cuentan con el soporte del Protocolo de Internet versión 6 llevan a cabo sus tareas de forma exitosa, existen herramientas que realizan escaneos erróneos y otras que no cuentan con el soporte completo para el protocolo.

3.1.8 Herramientas de la distribución Linux BackTrack 5 con soporte IPv6

De acuerdo a los resultados de las diferentes pruebas llevadas a cabo, se observan las herramientas de la distribución *Linux BackTrack 5* en la tabla I, que presentan un soporte en los escaneos que se realizan en redes de datos configuradas bajo el Protocolo de Internet versión 6 *IPv6.*

Herramienta	Soporte IPv4	Soporte IPv6
Dnsrecon	Si	No
DNS–Walk	Si	No
DnsEnum	Si	No

Tabla I. *Comparación de soporte de herramientas.*

Dnsmap	Si	Si
Fierce.	Si	No
Dig	Si	Si
Host	Si	No
Nslookup	Si	Si *
Fping	Si	No
Genlist	Si	No
AngryIPScan	Si	Si **
Lanmap2	Si	No
Xprobe2	Si	No
Netifera	Si	Si
Namap – Zenmap	Si	Si ***
Sqlmap	Si	No
Nikto2	Si	No
Webshag GUI	Si	No
Web Securify	Si	Si
Metasploit Framework	Si	Si
Meterpreter	Si	Si
Nectat	Si	—

** Soporte incompleto, ** Defecto en el escaneo, *** Soporte limitado solo a algunas opciones.*
Fuente: Autor

4. CONCLUSIONES

Las auditorias aplicadas en redes de datos con el nuevo Protocolo de Internet versión 6 no obtendrán resultados satisfactorios, ya que la versión de la distribución *BackTrack* no cuenta con suficientes herramientas para testear redes en *IPv6* y las que existen no dan un soporte completo o lo lleva a cabo de forma errónea.

Una distribución *GNU/Linux* que sobresale en el campo de la seguridad informática es la denominada *BackTrack*, la cual posee muchas herramientas, que son usadas por administradores de red y por usuarios normales que con un amplio conocimiento sobre estas herramientas, realizan ataques, auditorias e implementan seguridad a los sistemas de información.

La definición de fases basadas en metodologías de testeo de redes, le permiten al auditor una mejor organización para cubrir paso a paso el cumplimiento del objetivo trazado en el momento de la planeación de la auditoria.

La aplicación del *pentest* usando herramientas y las técnicas de ataque correspondientes en cada fase, facilitó el estudio de varios de los módulos de *GNU/Linux BackTrack 5.0*, ya que se evaluó el comportamiento del *tool kit* en el momento de realizar las pruebas de laboratorio.

La evaluación del comportamiento de le herramienta de seguridad *BackTrack 5.0* se llevó a cabo de acuerdo a los resultados obtenidos en las pruebas con los criterios propuestos en la ficha de observación. De este modo, en cada prueba se constató una efectividad completa en los laboratorios realizados en cada fase del test en la red con servicios configurados sobre *IPv4*. En pruebas sobre *IPv6* no se obtuvieron los resultados esperados.

La seguridad informática es un campo de estudio crítico de las redes de comunicación, lo que conlleva a pensar que esta disciplina debería contemplarse como una capa transversal de los modelos de comunicaciones *TCP/IP* y *OSI*.

Este caso particular el modelo de la Universidad Francisco de Paula Santander Ocaña.

5. AGRADECIMIENTOS

La Universidad Francisco de Paula Santander Ocaña (UFPSO), mediante la División de Investigación y Extensión (DIE) vincula a docentes, administrativos y estudiantes para que participen en la ejecución y desarrollo de proyectos de investigación. Este articulo muestra resultados de una fase del proyecto inscrito, avalado y financiado en dicha dependencia llamado "*Seguridad en redes*", propuesto por el Grupo de Investigación en Ingenierías Aplicadas (INGAP) y el Grupo de Ingeniería en Innovación, Tecnología y Emprendimiento (GRIITEM), y a su Semillero de Investigación GNU/Linux And Security (SIGLAS).

6. BIBLIOGRAFÍA

A. Peterson, C. (2009). Business continuity management & guidelines. *In 2009 Information Security Curriculum Development Conference (InfoSecCD '09)*. *ACM*, 114-120.

Bonetti, G., & Viglione, M. (2013). A comprehensive black-box methodology for testing the forensic characteristics of solid-state drives. *In Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13). ACM*, 269-278.

Boynton, B. (2007). Identification of process improvement methodologies with application in information security. *In Proceedings of the 4th annual conference on Information security curriculum development (InfoSecCD '07)*. *ACM*, 5 pages.

Carrier, B. (2005). *File system forensic analysis.* Addison Wesley.

Chi-Hsiang , W., & Dwen-Ren , T. (Octubre de 2009). Integrated installing ISO 9000 and ISO 27000 management systems on an organization. *Security Technology. 43rd Annual 2009 International Carnahan Conference on, 265*(267), 5-8.

Jaquith, A. (2007). *Security Metrics.* Addison Wesley.

KRUTZ, R., & VINES, R. (2007). *The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking.* Wiley Publishing.

Lobo, J., & Rico, D. (Enero de 2012). Implementación de la seguridad del protocolo de internet versión 6. *REVISTA GERENCIA TECNOLOGÍA INFORMÁTICA, 11*(29), 35-46.

Lyubimov, A. (2010). Integral engineering technique for information security methodologies. *In Proceedings of the 3rd international conference on Security of information and networks (SIN '10)*. *ACM*, 3-11.

Mcclure, S., & Scambray, J. (2010). *HACKERS 6: Secretos y soluciones de seguridad en redes.* Mexico D.F.: McGraw-Hill.

Melchor Medinaa, J., Lavín Verástegui, J., & Pedraza Melo, N. (Diciembre de 2012). Seguridad en la administración y calidad de los datos de un sistema de información contable en el desempeño organizacional. *Contaduría y administración*, 11-34.

Mora Luis, C., & Carrau Mellado,, R. (2013). PBL Methodologies with Embedded Augmented Reality in Higher Maritime Education: Augmented Project Definitions for Chemistry Practices. *Procedia Computer Science, 25*, 402-405.

Rico Bautista, D., Quel Hermosa, E., & Carvajal Mora, H. (2011). REDES Y TECNOLOGÍAS DE BANDA ANCHA.TECNOLOGÍAS DE ACCESO DE BANDA ANCHA. *Revista Colombiana de Tecnologías de Avanzada, 1*(17), 113-120.

Rico, D., & Medina, Y. (Septiembre de 2008). IPSec DE IPv6 EN LA UNIVERSIDAD

DE PAMPLONA. *Scientia et Technica*, 320-326.

Sansurooah, K. (2006). *Taxonomy of computer forensics methodologies and procedures for digital evidence seizur.*

Santos, L. M., & Rico, D. (Septiembre de 2007). IPv6 EN LA UNIVERSIDAD DE PAMPLONA: ESTADO DEL ARTE. *Scientia et Technica, 13*(37), 415-421.

Stallings, W. (2011). *Network security essentials applications and standards.* Prentice Hall.

Wysopal, C., & L. , N. (2006). *The Art Software Security Testing.* Addison Wesley.

Yadav, S., & Dong, T. (2014). A comprehensive method to assess work system security risk. *Communications of the Association for Information Systems, 34*(8), 169-198.

Zhihong, T., & Wei, J. (Mayo de 2014). A digital evidence fusion method in network forensics systems with Dempster-shafer theory. *Communications, China, 11*(5), 91,97.