Hacker Highschool
SECURITY AWARENESS FOR TEENS

LECCIÓN 7
ATTACK ANALYSIS

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Información sobre la "Licencia de Uso"

Las lecciones y cuadernos de trabajo siguientes son de acceso público y están disponibles bajo las siguientes condiciones de ISECOM:

Todos los trabajos del proyecto "Hacker Highschool" son proporcionados para su uso no comercial con estudiantes de escuelas primarias, secundarias, bachilleratos y ciclos formativos dentro de las actividades académicas propias de la institución. Dichos materiales no pueden ser reproducidos con fines comerciales de ningún tipo. La impartición con estos materiales de cualquier clase, curso o actividad de formación para el que sea necesario pagar un importe, queda totalmente prohibida sin la licencia correspondiente, incluyendo cursos en escuelas y universidades, cursos comerciales o cualquier otro similar. Para la compra de una licencia visite la sección "LICENSE" de la página web del proyecto "Hacker Highschool" en www.hackerhighschool.org/license.

El proyecto HHS es una herramienta de aprendizaje y, como tal, la formación final debe proceder realmente de la influencia del instructor y no basarse únicamente en el uso de la herramienta.

ISECOM no puede aceptar bajo ningún concepto responsabilidad alguna sobre la forma de aplicar, ni sus consecuencias, de cualquier información disponible dentro del proyecto. El proyecto HHS es un esfuerzo de una comunidad abierta, por lo que si encuentra útil este proyecto le invitamos a patrocinarlo a través de la compra de una licencia, una donación o un patrocinio.

Todos los Derechos Reservados ISECOM, 2004.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Índice

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Contribuciones

Pete Herzog, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Rafael Acosta Serrano, T&E Solutions

José María Fernández Ardavín, T&E Solutions

Jaume Abella, La Salle, URL - ISECOM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura

Universitat Ramon Llull

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

7.0 Introducción

Existen muchos programas dentro de tu computadora que intentan abrir conexiones de red. Algunos de estos programas tienen razones válidas para hacerlo (tu explorador de Internet no funcionaría muy bien sin una conexión de red), pero otros son escritos por personas con motivos que van desde lo cuestionable hasta lo criminal. Si deseas proteger tu computadora necesitas aprender a como detectar accesos a la red e identificar el origen del acceso y el motivo de éste. No todo intento de acceso a la red es un ataque, pero si no sabes diferenciar a un amigo de un desconocido podrías fácilmente dejar la puerta abierta.

7.1 Netstat y Cortafuegos –firewall - de aplicaciones de hospedaje

Para poder identificar un ataque necesitas conocer qué aplicaciones y qué procesos corren normalmente en tu computadora. Con sólo mirar en un ambiente gráfico como Windows o Linux no es posible conocer que procesos corren debajo de la superficie. Puedes utilizar Netstat y un Cortafuegos para ayudarte a identificar aquellos programas que puedan permitírseles conectar a la red.

7.1.1 Netstat

El comando "netstat" muestra el estado de las conexiones de red. Netstat puede proporcionarte información sobre qué puertos están abiertos y qué direcciones IP los están utilizando, qué puertos están siendo utilizados por un protocolo en particular, el estado de un puerto, e información acerca de los procesos o programas que utilizan dicho puerto.

Escribe sobre la línea de comando:

netstat –aon (para Windows) ó

netstat –apn (para Linux)

netstat desplegará información similar a ésta:

```
Active Connections
  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:1134           0.0.0.0:0              LISTENING       3400
  TCP    0.0.0.0:1243           0.0.0.0:0              LISTENING       3400
  TCP    0.0.0.0:1252           0.0.0.0:0              LISTENING       2740
  TCP    257.35.7.128:1243      64.257.167.99:80       ESTABLISHED     3400
  TCP    257.35.7.128:1258      63.147.257.37:6667     ESTABLISHED     3838
  TCP    127.0.0.1:1542         0.0.0.0:0              LISTENING       1516
  TCP    127.0.0.1:1133         127.0.0.1:1134         ESTABLISHED     3400
  TCP    127.0.0.1:1134         127.0.0.1:1133         ESTABLISHED     3400
  TCP    127.0.0.1:1251         127.0.0.1:1252         ESTABLISHED     2740
  TCP    127.0.0.1:1252         127.0.0.1:1251         ESTABLISHED     2740
```


WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Ahora necesitas relacionar el número en la columna "PID" - indicador del proceso - con los nombres de los procesos que están corriendo. En Windows, debes abrir el *Administrador de Tareas* presionando las teclas CTRL+ALT+DEL de manera simultánea (si no se muestra la columna PID da un click sobre *Ver*, *Seleccionar Columnas* y selecciona *PID*.) En Linux ve al intérprete de comandos y escribe "ps auxf" para ver el estado del procesador.

En el caso de nuestro ejemplo de resultados, listados en la figura anterior, encontramos que el PID 3400 corresponde a nuestro explorador de Internet y el PID 2740 corresponde a nuestro cliente de correo. Ambos sabemos que están siendo ejecutados y que tienen una razón válida para establecer una conexión a Internet. Sin embargo, el PID 3838 corresponde a un programa llamado 6r1n.exe, y el PID 1516 corresponde a un programa llamado buscanv.exe con los cuales no estamos familiarizados.

Sin embargo, no por el hecho de que no reconozcas el nombre de un programa no quiere decir que no tenga una razón válida para estarse ejecutando en el sistema. El siguiente paso será averiguar en Internet en cualquier máquina de búsqueda qué hacen estos programas.

En nuestra búsqueda descubrimos que "buscanv.exe" debe estar corriendo para el funcionamiento de nuestro programa de antivirus. Por otra parte encontramos que "6r1n.exe" puede ser un troyano. Viendo otra vez la lista de resultados del netstat, podemos ver que el puerto asociado con el programa "6r1n.exe" es el 6667, el cual es un puerto IRC comúnmente utilizado por troyanos para tener acceso remoto. En este punto, comenzaremos la investigación de métodos para remover el troyano.

7.1.2 Cortafuegos (Firewalls)

Ahora, te puedes sentar en tu computadora y correr el comando netstat una y otra, y otra, y otra vez para mantener una vigilancia constante de los datos que entran y salen de tu computadora, o puedes utilizar un cortafuego para que lo haga por ti.

Un cortafuego monitorea el tráfico de la red en tu computadora y utiliza un número de reglas o filtros para determinar si un programa tiene o no permiso para acceder a la red. Un cortafuego puede filtrar los datos de acuerdo a la dirección IP y los nombres de dominio, puertos y protocolos, o incluso datos transmitidos. Esto significa que puedes hacer cosas como:

- Bloquear o permitir toda información proveniente de una dirección IP específica
- Bloquear o permitir toda información proveniente de un dominio específico
- Cerrar o abrir puertos específicos
- Bloquear o permitir ciertos protocolos
- Bloquear o permitir paquetes de datos con alguna cadena de datos específica.

También puedes combinar esta serie de reglas para un control más cuidadoso de los datos que son permitidos a través de la red. Por ejemplo, tú puedes:

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Permitir datos que provengan de www.ibiblio.com a través de los puertos 20 o 21 solamente.

Permitir datos que provengan de www.google.com que usa el protocolo UDP

Permitir datos que provengan de www.yahoo.com sólo a través del puerto 80 y sólo si el paquete contiene la cadena de texto "No desperdiciaré el ancho de banda".

No es necesario que gastes tu tiempo configurando todas las reglas de un cortafuego, puedes tomar ventaja de que algunos cortafuegos establecen ciertas reglas por sí solos. Después de que hayas instalado un cortafuego, vas a ser inundado de peticiones de control de acceso y tienes que determinar que programa, puede o no, hacer uso de la red. (Es posible que el programa del cortafuego proporcione la opción de dejar que él mismo determine que programas pueden hacer uso de la red, pero no aprenderías nada, ¿es lo que quieres?). Este proceso será similar al que utilizamos para identificar los procesos con netstat. Un programa llamado "iexplorer.exe" es obviamente Microsoft Internet Explorer y, si tú lo usas como tu explorador de Internet el cortafuego debe permitirle acceder a la Internet, pero un programa llamado "cbox.exe" puede ser cualquier cosa. No tienes otra opción más que ir a tu explorador y averiguar en el motor de búsqueda de tu preferencia de qué es el programa. (Claro que antes de hacer esto, le tienes que indicar a tu cortafuego que permita el acceso de tu explorador a la Internet).

Un cortafuego puede darte la opción de permitir el acceso a un programa de manera repetida o sólo por una ocasión. Algunos programas, tales como tu explorador de Internet, deberán tener acceso a la red en cualquier momento, pero con otros programas – como aquéllos que requieren verificar actualizaciones – puedes aprender mucho acerca de cómo funciona tu computadora dejando que te pregunte cada vez que un programa trate de pedir acceso.

Los cortafuegos están disponibles como programas individuales (incluyendo versiones de distribución libre para las plataformas Windows y Linux) o existen versiones que vienen junto con programas de antivirus. Adicionalmente, Windows XP contiene dentro de su arquitectura un cortafuego instalado, pero, en el caso del explorador de Internet de Windows, es un objetivo para la gente que busca explotarlo – los defectos en otros cortafuegos pueden no encontrase, pero los existentes en un cortafuego de Microsoft serán encontrados y explotados.

7.1.3 Ejercicios

Abre una línea de comando en tu computadora y teclea:

netstat –aon (para Windows) ó

netstat –apn (para Linux)

Encuentra los números PID y trata de determinar que programas se están ejecutando en el sistema. (Esto es algo que puedes hacer también en tu casa.)

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

7.2 Analizadores de paquetes

Netstat te dirá qué programas están conectados a la red, pero no te dirá que datos del programa se están enviando. Un analizador de paquetes, sin embargo, te brinda la facultad de registrar y estudiar los datos de los programas que están siendo enviados a través de la red.

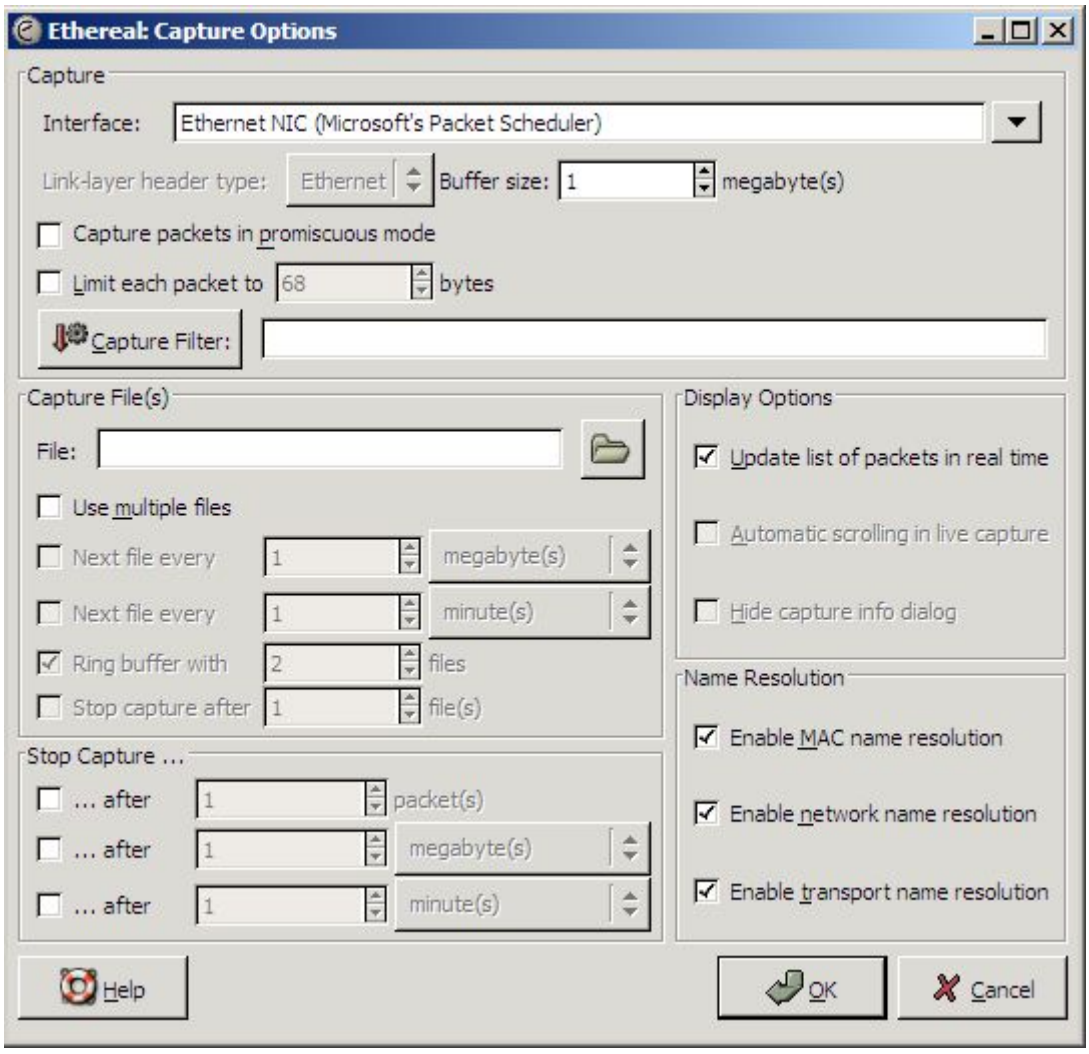
7.2.1 Analizando

Un analizador de paquetes registrará el tráfico de la red en tu computadora, permitiéndote observar todos los datos. Tcpdump (y en su versión para Windows, windump) están considerados como el arquetipo de los analizadores de paquetes, sin embargo utilizaremos *Ethereal* para nuestros ejemplos, debido a que tiene una interficie gráfica muy sencilla, permitiéndote registrar y guardar los registros en un archivo de manera rápida.

Si no tienes Ethereal, podrás bajarlo de *www.ethereal.com*. Para los usuarios de Windows, para utilizar Ethereal en una plataforma Windows, deberás bajar e instalar el controlador de captura de paquetes Winpcap. Winpcap está disponible en la página de descargas de Ethereal, o bien, lo encontrarás directamente en la página www.winpcap.polito.it para descargarlo.

Cierra cualquier otra aplicación que se esté ejecutando e inicia Ethereal. En el menú haz click en *View>Autoscroll in Live Capture*. Luego, haz click en *Capture* y *Start* para ir al menú de *Capture Options*. En esta pantalla, asegúrate de que esté activado el campo de "Capture packets in promiscuous mode", y que tanto los tres apartados bajo "Name Resolution" estén activados, así como el apartado de "Update list of packets in real time".

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.



Ahora da un click en el botón de "OK".

En teoría, nada debería pasar por ahora. Verás una pantalla de Ethereal que despliega el número de paquetes que están siendo capturados y, detrás de esto, verás la pantalla de Ethereal que despliega los datos de esos paquetes. Verás una pequeña cantidad de tráfico originado por otras computadoras en tu red local tratando de mantener la pista de los otros (ARP, NBNS, ICMP) seguido por una actividad de resolución de nombres DNS por parte de Ethereal.

Para ver actividad, tendrás que generarla. Mientras está ejecutándose Ethereal, abre tu explorador de Internet. Minimiza cualquier otra aplicación exceptuando Ethereal y el explorador de Internet. Ordena estas dos ventanas para que puedas verlas de manera simultánea. Ahora, ve a un motor de búsqueda en tu explorador, como www.google.com.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

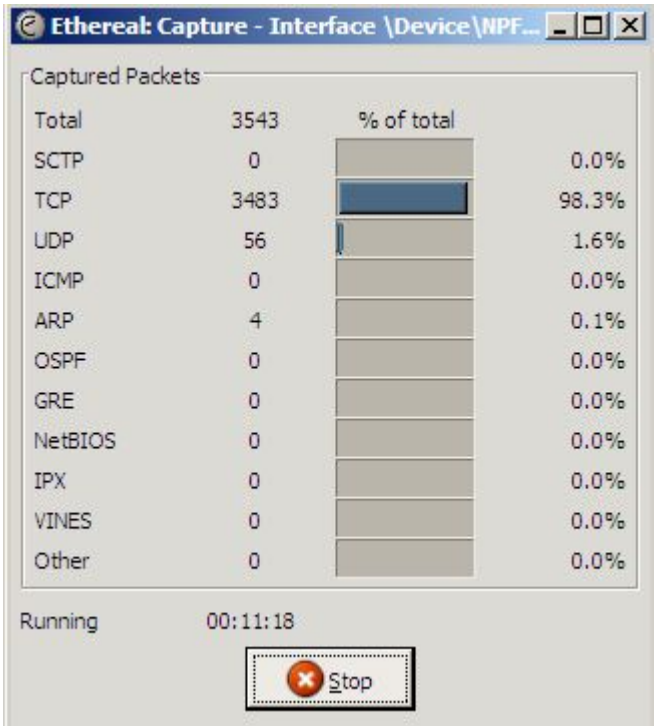
Mientras la página es cargada, deberás ver información acerca de los paquetes capturados. Elige un tópico a buscar y búscalo, haz click en alguna de las páginas que te mostró el buscador y observa lo que sucede en Ethereal.

Nota: Si Ethereal no reporta algún tipo de tráfico, lo más seguro es que no elegiste la tarjeta de red correcta. Ve al apartado de *Interface* en *Capture Options* y elige otra interfaz de red (NIC).

7.2.2 Decodificando el tráfico de red

Ahora que ya puedes ver el tráfico de la red que se genera a través de tu computadora, deberás saber como decodificarla para interpretarla.

En el programa de Ethereal, el primer paso después de que incluso hayas terminado de capturar paquetes, es ir a la pantalla donde se muestra el resumen de la captura que el programa genera cuando está capturando. Para nuestra sesión de búsqueda web muchos de los paquetes deben ser paquetes TCP (aunque si paraste para ver un video en demanda, el número de paquetes UDP seguramente se incrementó). De cualquier forma, si estás capturando una simple sesión de búsqueda web y aparecen paquetes de tipo ARP o ICMP, ésto podría indicar que hay un problema.



WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Después de que hayas terminado la sesión de captura de paquetes, deberás ver algo similar a esto:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	257.10.3.250	rodan.mozilla.org	TCP	1656 > 8080 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
2	0.045195	257.10.3.250	rheet.mozilla.org	TCP	1657 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
3	0.335194	rheet.mozilla.org	257.10.3.250	TCP	http > 1657 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
4	0.335255	257.10.3.250	rheet.mozilla.org	TCP	1657 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
5	0.338234	257.10.3.250	rheet.mozilla.org	HTTP	GET /products/firefox/start/ HTTP/1.1
6	0.441049	rheet.mozilla.org	257.10.3.250	TCP	http > 1657 [ACK] Seq=1 Ack=580 Win=6948 Len=0
7	0.441816	rheet.mozilla.org	257.10.3.250	HTTP	HTTP/1.1 304 Not Modified
8	0.559132	257.10.3.250	rheet.mozilla.org	TCP	1657 > http [ACK] Seq=580 Ack=209 Win=17312 Len=0
9	2.855975	257.10.3.250	rodan.mozilla.org	TCP	1656 > 8080 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
10	4.475529	257.10.3.250	name.server.com	DNS	Standard query PTR 250.3.10.257.in-addr.arpa
11	4.475776	257.10.3.250	name.server.com	DNS	Standard query PTR 205.111.126.207.in-addr.arpa
12	4.475854	257.10.3.250	name.server.com	DNS	Standard query PTR 202.111.126.207.in-addr.arpa

En este ejemplo, estos 12 paquetes ilustran la actividad que el explorador de Internet tiene cuando se conecta a cada página de inicio. La información más fácil de decodificar esta en las columnas de origen y destino. La dirección IP 257.10.3.250 es la computadora local, las otras direcciones han sido resueltas por su nombre a través de Ethereal. Debido a que utilizamos Mozilla Firefox como explorador de Internet, y debido a que tiene como página de inicio la página de Mozilla Firefox, no es de sorprenderse el ver direcciones del dominio de mozilla.org. Las peticiones enviadas a *name.server.com* fueron probablemente generadas por Ethereal cuando envía peticiones de tipo DNS para resolver direcciones IP a nombres. (Nota: estos accesos producidos por el programa de Ethereal fueron debidos a las opciones configuradas en el apartado de *Display Options* y el apartado de *Name Resolution*. Estos apartados fueron activados, para fines de ilustración en éste ejemplo, para obtener una salida más legible. Si deshabilitas estas opciones, no verás éstos datos adicionales).

Observar la información de origen y destino pueden ayudarte a detectar alguna actividad no autorizada. Por ejemplo, un nombre de dominio desconocido que aparezca constantemente puede indicarte que tienes un programa de tipo espía – spyware – instalado en tu computadora.

La siguiente columna es la de Protocolo, la cual indica qué protocolo están utilizando los paquetes. Otra vez, para saber si algo anda mal, deberás saber qué puedes esperar. En la sesión de exploración web esperamos respuestas TCP y http, y sabes el porqué de los paquetes de tipo DNS. Sin embargo, una gran cantidad de paquetes de tipo ICMP pueden significar que tu máquina está siendo rastreada (mediante el uso de la herramienta PING).

La última columna, Información, provee mayor detalle de la información acerca de los paquetes. Los paquetes 2, 3 y 4 muestran el proceso de comunicación TCP – three-handed handshake – de SYN, SYN/ACK, ACK, los cuales indican que se ha establecido una conexión. El paquete 5 muestra un comando HTTP GET seguido por el paquete 7 que indica una respuesta de tipo *304 Not modified*.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Si deseas mayor información sobre los paquetes, al final de las dos ventanas en la pantalla de Ethereal, se muestran explicaciones más detalladas. La ventana de en medio muestra el detalle del encabezado del paquete. La ventana inferior muestra el volcado ASCII y hexadecimal – hex – de los datos dentro del paquete.

7.2.3 Analizando otras computadoras

Algunos de ustedes han mirado en la información de esta sección – y habiéndose fijado en los datos registrados por Ethereal, se preguntarán acerca de las posibilidades del uso de aplicaciones del tipo analizador de paquetes para registrar actividades en las computadoras de otras personas. ¿Es esto posible?

Sí – y no. A esto se le denomina modo promiscuo, lo cual permite que un analizador de paquetes pueda monitorear la actividad de la red para todas las computadoras en una red. Esto significa que podrás registrar cualquier actividad de red en otra computadora que se encuentra en tu misma red (dependiendo de cómo está configurado el hardware), pero lo que sí es cierto es que no podrás elegir cualquier otra computadora de manera aleatoria y que mágicamente analices sus datos – las dos computadoras deberán estar conectadas entre sí físicamente, y el hardware y software deberá estar configurado de manera apropiada.

7.2.4 Sistemas de Detección de Intrusos –IDS por sus siglas en inglés

Probablemente te habrás dado cuenta de que el uso de un analizador de paquetes puede detectar actividad no autorizada en tiempo real, la cual requiere que estés sentado en frente de tu computadora, observando las salidas del analizador de paquetes y deseando de manera desesperada ver algún tipo de patrón. Un sistema de detección de intrusos realiza éste tipo de tareas por ti. Estos programas combinan la habilidad de registrar actividad de la red a partir de una serie de reglas que le permiten señalar actividades no autorizadas y generar avisos en tiempo real.

7.2.5 Ejercicios

1. Abre la aplicación de Ethereal y comienza a capturar en vivo. Ahora abre tu explorador de Internet y busca descargar un documento en texto plano. Descárgalo y sálvalo en tu disco duro, cierra el explorador y finaliza la sesión de Ethereal. Busca en los paquetes capturados por Ethereal, prestando mucha atención al volcado ASCII al final de la ventana. ¿Qué es lo que ves? Si tienes acceso a una cuenta de correo electrónico, trata de leer tu correo mientras Ethereal realiza una captura de paquetes. ¿Qué es lo que ves?
2. Abre Ethereal. En la pantalla de *Capture Options* cerciórate que esté marcado el apartado de "*Capture packets in promiscuous mode*". Esta opción te permitirá capturar paquetes hacia o provenientes de otras computadoras. Comienza a capturar y ve qué es lo que pasa. ¿Ves algún tráfico que no sea el de tu máquina?

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

¿Qué sabes acerca del hardware que conecta tu computadora a la red? ¿Te conecta a otras computadoras a través de un concentrador, conmutador o encaminador? Trata de indagar en una máquina de búsqueda qué pieza o piezas hardware harían más difícil el capturar paquetes de otras computadoras. ¿Qué hardware lo haría más fácil?

3. Ve al sitio www.snort.org, o utiliza una máquina de búsqueda para investigar sistemas de detección de intrusos. ¿Cuál es la diferencia entre éstos y los cortafuegos? ¿Qué tienen en común con los analizadores de paquetes? ¿Qué tipos de actividad no autorizada pueden detectar? ¿Qué tipos de actividad pueden no ser detectados?

7.3 Redes y Sistemas Tipo Señuelo (Honeypots y Honeynets)

A la gente que le gusta observar chimpancés van a un zoológico, debido a que regularmente encontrarían chimpancés ahí. A la gente que le gusta observar pájaros ponen bebedores para aves con la finalidad de que vayan los pájaros hacia ellos. A la gente que le gusta observar peces tienen acuarios, y compran peces para ponerlos ahí. Pero, ¿qué harías para observar a los hackers?

Pondrías un *sistema tipo señuelo* – honeypot.

Piénsalo de ésta manera –eres un oso. No sabrás mucho (y más siendo un oso) pero sabes que la miel es deliciosa, y que no hay nada mejor en un verano caluroso que un puñado de miel. De repente, sentado afuera en el campo ves un gran panal lleno de miel, y piensas… "Yum!". Pero una vez que pones tu garra en el panal, corres el riesgo de quedarte atorado. Si no hay nadie más, dejarás una gran y pegajosa huella por donde camines, y cualquiera que las siga terminaría por descubrir que fuiste tú quien tomó la miel. Más de un oso ha sido descubierto debido a su irresistible adicción a la deliciosa miel.

Un *sistema tipo señuelo* es un sistema informático, red o máquina virtual, con el único propósito de atrapar hackers. En un sistema tipo señuelo existen usuarios no autorizados –no contienen información real almacenada ni algún tipo de aplicación real instalada – por lo que, cualquier acceso y/o cualquier intento de ser utilizados, puede ser identificado como no autorizado. En lugar de verificar registros del sistema para identificar intrusiones al mismo, el administrador del sistema sabe que cada acceso registrado es una intrusión, así que gran parte del trabajo ya está hecho.

7.3.1 Tipos de Sistemas Tipo Señuelo

Existen dos tipos de Sistemas Tipo Señuelo: de *producción* y de *investigación*.

Los *Sistemas Tipo Señuelo de Producción* son generalmente utilizados como sistemas de avisos. Un Sistema Tipo Señuelo de producción identifica una intrusión y genera una alarma. Pueden mostrar que un intruso ha logrado identificar el sistema o red y que está siendo de su interés, pero no más allá. Por ejemplo, si deseas saber si viven otros osos cerca de tu morada, pondrías diez pequeños tarros de miel. Si al revisarlos a la mañana siguiente encuentras uno o

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

más vacíos, entonces sabrás que los osos han estado cerca del lugar sin conocer nada más de ellos.

Los Sistemas Tipo Señuelo de *Investigación* son utilizados para recolectar información sobre las actividades de los Hackers. Un Sistema Tipo Señuelo de Investigación atrapa a los hackers y los mantiene ocupados mientras están siendo registradas todas sus acciones. Por ejemplo, si –en lugar de documentar simplemente su presencia – deseas estudiar a los osos, entonces te sentarías cerca de un gran, delicioso y pegajoso panal en el campo, pero pondrías cámaras, grabadoras y asistentes de investigación con sus libretas de apuntes y cascos alrededor del panal.

Los dos tipos de Sistemas Tipo Señuelo difieren principalmente en su complejidad. Es más fácil que configures y mantengas un sistema de producción debido a su simplicidad y al poco manejo de información que deseas obtener. En un Sistema Tipo Señuelo en producción sólo deseas saber si te están "pegando"; no te interesa saber si los hackers se quedan rondando por ahí. Sin embargo, en un Sistema Tipo Señuelo de investigación desearás que los hackers se queden con la finalidad de ver qué es lo que están haciendo. Esto hace más complejo la configuración y el mantenimiento de un sistema de este tipo, debido a que el sistema deberá parecer como un sistema real, en producción y que ofrece archivos y/o servicios interesantes para los hackers. Un oso que sabe cómo es un panal, gastará sólo un minuto en un panal vacío, pero sólo un panal repleto de deliciosa miel lo mantendrá merodeando el lugar, tanto como te sea necesario para que puedas estudiarlo.

7.3.2 Construyendo un Sistema Tipo Señuelo

En el sentido más básico, un sistema de tipo señuelo no es nada más que un sistema informático configurado con la esperanza de que sea comprometido por intrusos. Esencialmente, esto significa que si tú conectas una computadora con un sistema operativo inseguro a la Internet, sólo bastará que te sientes a esperar el momento en que la máquina esté comprometida. ¡Ahora, ya has creado un sistema de tipo señuelo!

Pero en realidad, este sistema no es tan útil como parece. Es como si dejaras tu miel en el campo y te fueras a tu casa en la ciudad. Cuando regreses, lo más seguro es que la miel haya desaparecido y no sabrás ni quién, ni cómo, ni porqué desapareció. No aprenderás nada de tu sistema tipo señuelo, a menos de que exista una manera para obtener información de él. Para que te sea útil, incluso en los sistemas más sencillos, deberá tener algún sistema de detección de intrusos.

El sistema de detección de intrusos puede ser tan simple como un cortafuego. Generalmente el cortafuego es utilizado para prevenir el acceso de usuarios no autorizados a un sistema, aunque también para registrar todo aquello que sucede y/o saber si una aplicación ha sido detenida. El revisar los archivos de registro producidos por un cortafuego puede brindarte información básica sobre los intentos de acceso al sistema tipo señuelo.

Otros sistemas más complejos de tipo señuelo contemplan el uso de hardware, tales como concentradores, conmutadores o encaminadores, a fin de monitorear o controlar accesos futuros a la red. También es común que utilicen analizadores de paquetes para obtener información adicional acerca del tráfico de red.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Los sistemas tipo señuelo de Investigación deberán ejecutar programas para simular el uso normal, haciéndoles parecer que el sistema tipo señuelo está siendo accedido por usuarios autorizados, engañando a intrusos potenciales con correos, contraseñas y datos falsos. Este tipo de programas también pueden ser utilizados para disfrazar sistemas operativos, hacerlos parecer como por ejemplo, que una computadora con plataforma Linux esté corriendo Windows.

Pero el asunto acerca de la miel – es que es pegajosa, y que siempre existe la posibilidad de que el sistema tipo señuelo se torne en un nido de abejas. Y cuando las abejas regresan a su casa no te gustaría ser el que se le atoró la mano en el panal. Un sistema tipo señuelo mal configurado puede fácilmente convertirse en un punto de lanzamiento de otros ataques. Si un hacker compromete tu sistema tipo señuelo, de manera instantánea realizará un asalto sobre una gran empresa o utilizará tu sistema para distribuir spamm de tipo inundación, y lo más seguro es que tú seas identificado como el responsable.

Un sistema tipo señuelo bien configurado puede controlar el tráfico de red entrante y/o saliente de la computadora. Un sistema sencillo de producción podrá permitir la entrada de tráfico a través de tu cortafuego, pero frenará todo el tráfico saliente. Ésta es una sencilla pero de eficaz solución, pero algunos intrusos se percatan rápidamente que no existe tráfico saliente, aunque no todos.

Los sistemas tipo señuelo de investigación –que deseen mantener a los intrusos interesados por el mayor tiempo posible – en algunas ocasiones utilizan software que "mutilan", los cuales auditan el tráfico saliente y desarman los datos potencialmente peligrosos mediante su modificación haciéndolos inofensivos.

7.3.3 Ejercicios

Los sistemas tipo señuelo pueden ser herramientas útiles para la investigación y para la identificación de intrusos, pero el utilizarlos para atraparlos y procesarlos es otro asunto. Distintas jurisdicciones tienen diferentes definiciones y estándares, jueces y jurados pueden discrepar en los puntos de vista, por lo que muchas preguntas deberán ser consideradas. ¿Los sistemas tipo señuelo representan un intento de trampa? ¿El registrar las actividades de un hacker resulta, de alguna manera, en la intercepción de la comunicación como en el caso de los teléfonos?

Y de acuerdo a preguntas específicas de éstos sistemas –¿puede ser ilegal el comprometer un sistema que esté diseñado para ser comprometido? Estas preguntas todavía tendrán que ser revisadas, estudiadas y probadas a fondo.

Discute tus opiniones con respecto a la legalidad del uso de sistemas tipo señuelo para atrapar a hackers involucrados en actividades criminales. ¿Piensas que puede ser una herramienta útil para las agencias protectoras de la ley? ¿Es una trampa? ¿Piensas que constituye un "conocimiento atractivo pero molesto"? Si un hacker compromete un sistema tipo señuelo, ¿quién crees que sería el responsable?

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Lecturas Recomendadas

Netstat

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/netstat.mspx

Información General de los Cortafuegos:

http://www.howstuffworks.com/firewall.htm

http://www.interhack.net/pubs/fwfaq

Uno de muchos programas libres tipo cortafuego:

http://www.agnitum.com/index.html

Protegiendo con cortafuegos – para Linux:

http://www.iptables.org

Analizadores de Paquetes

http://www.robertgraham.com/pubs/sniffing-faq.html

Snort y sistemas de detección de intrusos – IDS's:

http://www.linuxsecurity.com/feature_stories/feature_story-49.html

http://www.snort.org/docs/lisapaper.txt

Sistemas de Tipo Señuelo – Honeypots:

http://www.honeypots.net/honeypots/links

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.