Hacker Highschool
SECURITY AWARENESS FOR TEENS

LECCIÓN 5
IDENTIFICACIÓN DE SISTEMAS

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"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.

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 esponsorizarlo a través de la compra de una licencia, una donación o una esponsorización.

Índice

Contribuciones

Chuck Truett, ISECOM

Jaume Abella, La Salle URL Barcelona – ISECOM

Guiomar Corral, La Salle URL Barcelona

Pete Herzog, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

5.1. Introducción

Es obvio que qualquiera que se siente en el teclado de tu ordenador puede obtener información sobre el mismo, incluyendo el sistema operativo y los programas que se están ejecutando, pero también es posible para alguien que utiliza una conexión de red recoger información sobre un ordenador remoto. Esta lección describe algunas de las formas en las que se puede obtener esta información. Saber como se recoge esta información te ayudará a asegurar que tu ordenador local esté a salvo de estas actividades.

5.2. Identificación de un servidor

Hay un buen número de fuentes útiles en la web que te ayudarán a recoger información sobre nombres de dominio y direcciones IP.

5.2.1 Identificación del propietario de un dominio

El primer paso para identificar un sistema remoto es determinar el nombre de dominio y su dirección IP. Haciendo una búsqueda de *Whois (whois lookup)*, puedes descubrir información valiosa, incluyendo el propietario del dominio e información de contacto, que puede incluir direcciones y números de teléfono. Has de saber que ahora hay unos cuantos registradores de nombres de dominio, y que no todas la bases de datos *whois* contienen toda la información de todos los dominios. Puede que tengas que buscar en más de una base de datos *whois* para encontrar la información que estás investigando.

5.2.2 Identificación de la dirección IP de un dominio

Hay unas cuantas formas de determinar la dirección IP de un dominio. La dirección puede estar contenida en la información de *whois* o puede que tengas que buscar en un DNS o Servidor de Nombres de Dominio. (Hay motores de búsqueda que proporcionan un buen número de recursos para el descubrimiento de direcciones IP de nombres de dominio).

Una vez se dispone de la dirección IP, se puede acceder a los registros de diversos miembros de la *Number Resource Organization* (http://www.arin.net/ y http://www.ripe.net/), para obtener información sobre cómo se distribuyen las direcciones IP. Los números IP se asignan a los proveedores de servicios y a las redes en grandes agrupaciones. Conocer en qué grupo está contenida la dirección IP y quién tiene los derechos de ese grupo puede ser de gran ayuda. Esto puede ayudarte a determinar información sobre el servidor o el proveedor de servicios que utiliza el servidor web.

Ejercicios:
Escoge un nombre de dominio válido (isecom.org) y realiza una búsqueda de *whois* para encontrar quién es el propietario de ese dominio (http://www.whois.com -> "isecom.org"+Go -> Whois Lookup). ¿Qué otra información está disponible? ¿Cuando se creó el dominio? ¿Cuando expirará? ¿Cuando fue actualizada por última vez?

Encuentra la dirección IP para este nombre de dominio. Utilizando los *whois lookups* de diversos miembros de la *Number Resource Organization*, determina a quién se ha asignado esta dirección IP. (Empieza con la pagina **www.arin.net**, que también tiene enlaces a otros miembros de la NRO -> ripe). ¿Cual es el margen de direcciones IP que también tiene registrado esta entidad?

5.3. Identificación de servicios

Una vez se ha establecido el propietario y la dirección IP de un dominio, entonces se puede empezar a buscar información sobre el servidor al que este dominio se refiere.

5.3.1 Ping y Traceroute

Ahora que sabes a quién pertenece el dominio y a quién se ha asignado el número IP, puedes comprobar si el servidor web está actualmente activo. El comando *ping* te dirá si hay un ordenador o servidor asociado con ese nombre de dominio o IP. El comando

```
ping dominio o
ping direcciónip
```

te dirá si hay un ordenador activo en esa dirección.

Si el resultado del comando *ping* indica que se están recibiendo los paquetes ping enviados, entonces puedes asumir que el ordenador está activo.

Otro comando, *tracert* (en Windows) o *traceroute* (en Linux) muestra los pasos que realiza la información a medida que viaja desde tu ordenador al remoto. Trazando la ruta que realizan los paquetes a veces té ofrecerá información adicional sobre los ordenadores de la red donde está situado el objetivo de tu traza. Por ejemplo, ordenadores con direcciones IP similares muy a menudo formarán parte de la misma red.

Ejercicios:
Haz un ping a un *website* o dirección IP (ping www.isecom.org o ping 216.92.116.13). Si obtienes una respuesta exitosa, haz ping sobre la dirección IP consecutiva (.14). ¿Ha sido positivo el resultado? ¿A qué dominio pertenece esta nueva dirección IP?

Utiliza *tracert* o *traceroute* para trazar la ruta desde tu ordenador local hasta la IP que has utilizado en el ejercicio previo. ¿Cuántos pasos se necesitan? ¿Alguno de los ordenadores listados tiene direcciones IP similares?

5.3.2 Obtención del banner

El próximo paso para identificar al sistema remoto es intentar conectarse utilizando telnet o FTP. El servidor programa para estos servicios mensajes de texto de bienvenida llamados *banners*. Un *banner* puede mostrar claramente y con precisión qué programa se está ejecutando para este servicio. Por ejemplo, cuando te conectas a un servidor FTP anónimo, podrías obtener el mensaje siguiente:

```
Connected to anon.server.
220 ProFTPD Server (Welcome . . . )
User (anon.server:(none)):
```

El número 220 es un código para FTP que indica que el servidor esta preparado para recibir un nuevo usuario y el mensaje de texto ProFTP Server identifica el programa FTP que se está ejecutando en el ordenador remoto. Utilizando un motor de búsqueda, puedes aprender qué sistema operativo utiliza y otros detalles sobre sus requerimientos, capacidades, limitaciones y defectos.

El principal defecto en el uso de esta técnica de obtención de *banners* sobre un sistema es que los administradores de sistemas inteligentes pueden poner *banners* engañosos. Un *banner* que muestre "Estonoesasuntotuyo" no puede ser obviamente confundido, pero un sistema Unix con un *banner* que muestra "WS_FTP Server" (FTP Server basado en Windows) va a complicar mucho cualquier intento de obtención de datos que se intente.

5.3.3 Identificación de servicios a partir de puertos y protocolos

También se puede determinar qué programas están funcionando en un sistema mirando qué puertos (TCP y UDP) están abiertos y qué protocolos los utilizan.

Puedes empezar mirando tu propio ordenador. Abre un shell MS-DOS o linea de comandos (Windows: ejecutar -> cmd) y ejecuta el programa *netstat* usando el sufijo –a (o todos):

```
netstat -a
```

El ordenador mostrará la lista de puertos abiertos y algunos de los servicios que utilizan estos puertos.

```
Active Connections
Proto Local Address                 Foreign Address         State
TCP   YourComputer:microsoft-ds     YourComputer:0          LISTENING
TCP   YourComputer:1025             YourComputer:0          LISTENING
TCP   YourComputer:1030             YourComputer:0          LISTENING
TCP   YourComputer:5000             YourComputer:0          LISTENING
TCP   YourComputer:netbios-ssn      YourComputer:0          LISTENING
TCP   YourComputer:1110             216.239.57.147:http     TIME_WAIT
UDP   YourComputer:microsoft-ds     *:*
UDP   YourComputer:isakmp           *:*
UDP   YourComputer:1027             *:*
UDP   YourComputer:1034             *:*
UDP   YourComputer:1036             *:*
UDP   YourComputer:ntp              *:*
UDP   YourComputer:netbios-ns       *:*
UDP   YourComputer:netbios-dgm      *:*
```

A partir de aquí puedes ver muchos de los programas que se están ejecutando en tu ordenador local, muchos de los cuales ni siquiera sabes que están funcionando.

Otro programa, llamado *fport*, proporciona información similar a la de *netstat*, pero detalla, además, qué programas están utilizando estos puertos y protocolos. (fport está disponible gratuitamente en www.foundstone.com).
Otro programa, llamado *nmap* (proviene de *network mapper*), analizará más concienzudamente los puertos abiertos de tu ordenador. Cuando *nmap* se ejecuta, muestra una lista de puertos abiertos y los servicios o protocolos que utilizan estos puertos. También puede ser capaz de determinar que sistema operativo está usando un ordenador. Por ejemplo, si se ejecuta *nmap* en tu ordenador local, podrías observar el siguiente resultado:

```
Por        State    Service
22/tcp     open     ssh
68/tcp     open     dhcpclient
139/tcp    open     netbios-ssn
445/tcp    open     microsoft-ds
Device type: general purpose
Running: Linux 2.4X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 1.024 days (since Sat Jul 4 12:15:48 2004)
```

Nmap está disponible para descargar en www.insecure.org.

Ejercicios

Ejecuta *netstat* en tu ordenador local, utilizando el sufijo –a.

netstat -a

¿Qué puertos están abiertos? Utilizando un motor de búsqueda web (www.google.com) ¿Puedes encontrar a qué servicios pertenecen estos puertos? (este sería un buen ejercicio para realizar en casa para comprobar si se están ejecutando servicios innecesarios o potencialmente peligrosos, como FTP o Telnet).

Ejecuta *nmap* utilizando los sufijos –sS (para escaneo SYN Stealth) i –O (para que intente adivinar el sistema operativo) con la dirección IP 127.0.0.1 como objetivo del escaneo.

nmap -sS -O 127.0.0.1

La dirección IP 127.0.0.1 especifica el host local (o ordenador local). (Nota: esta dirección es diferente de la que utilizan otros ordenadores en Internet para conectarse contigo; en cualquier máquina la dirección IP 127.0.0.1 se refiere siempre al ordenador local). ¿Qué puertos abiertos encuentra *nmap*?¿Qué servicios y programas utilizan estos puertos? Intenta ejecutar *nmap* mientras tienes abierta una página web de Internet o un cliente de Telnet. ¿Cambia esto los resultados?

5.4. Identificación de un sistema

Ahora que sabes cómo identificar un servidor, cómo escanear los puertos abiertos y utilizar esta información para determinar qué servicios se estan ejecutando, puedes poner esta información junta para identificar (*fingerprint*) un sistema remoto, estableciendo cual debe ser el sistema operativo y qué servicios están ejecutándose en ese ordenador remoto.

5.4.1 Escaneo de ordenadores remotos

Utilizar una dirección IP o un nombre de dominio que no sea 127.0.0.1 como argumento para *nmap* permite escanear puertos abiertos de ordenadores remotos. Esto no quiere decir que haya puertos abiertos o que los encuentres, pero permite buscarlos.

Por ejemplo, imagina que has estado recibiendo una gran cantidad de e-mails de *spam* y quieres descubrir información sobre la persona que los está enviando. Mirando las cabeceras de cualquiera de estos e-mails, puedes ver que muchos de estos e-mails se han originado desde la misma dirección IP: 256.92.116.13 (ver "Lección 9: Seguridad del e-mail" para ver más detalles al respecto).

Un *whois lookup* muestra que la dirección forma parte de un bloque asignado a un gran ISP, pero no te da información sobre esta dirección en particular.

Si utilizas *nmap* para escanear el ordenador de esa dirección, podrías obtener los siguientes resultados.

```
nmap -sS -O 256.92.116.13


Starting nmap 3.50 ( http://www.insecure.org/nmap ) at 2004-07-03 20:13
Eastern Daylight Time
Interesting ports on 256.92.116.13:
(The 1632 ports scanned but not shown below are in state: closed)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    open     smtp
80/tcp    open     http
110/tcp   open     pop3
113/tcp   open     auth
135/tcp   filtered msrpc
136/tcp   filtered profile
137/tcp   filtered netbios-ns
```

```
138/tcp   filtered netbios-dgm
139/tcp   filtered netbios-ssn
143/tcp   open     imap
144/tcp   open     news
161/tcp   filtered snmp
306/tcp   open     unknown
443/tcp   open     https
445/tcp   filtered microsoft-ds
513/tcp   open     login
514/tcp   open     shell
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.50%P=i686-pc-windows-windows%D=7/3%Time=40E74EC0%O=21%C=1)
TSeq(Class=TR%IPID=RD%TS=1000HZ)
T1(Resp=Y%DF=Y%W=FFFF%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)


Uptime 1.877 days (since Thu Jul 01 23:23:56 2004)


Nmap run completed -- 1 IP address (1 host up) scanned in 775.578 seconds
```

Los puertos marcados como *filtered* son conocidos como vulnerables a ser atacados, por lo que no es una sorpresa encontrarlos listados como filtrados. Lo más interesante es que los puertos 21, 22 y 23 –por FTP, SSH y Telnet- están listados como abiertos.

La última cosa que hace *nmap* es intentar identificar el sistema operativo que se está ejecutando en el ordenador escaneado. En este caso, las pruebas que ha realizado *nmap* no son concluyentes al respecto ("*no exact OS matches*"), aunque como nmap muestra que los puertos de FTP y Telnet están abiertos, puedes intentar conectarte a través de cada uno de estos puertos para ver si devuelve un *banner*.

Cuando te conectas a través de FTP podrías ver un *banner* como el siguiente:

```
220 ftp316.pair.com NcFTPd Server (licensed copy) ready.
```

Cuando te conectas a través de Telnet podrías ver un *banner* como el siguiente:

```
FreeBSD/i386 (ttyp7)
```

Una búsqueda rápida vía web (www.google.com) muestra que NcFTPd es un programa de Unix y que FreeBSD es un tipo de sistema operativo basado en Unix, así que es probable que el servidor este ejecutando alguna versión del sistema operativo FreeBSD. No se puede estar completamente seguro (se pueden modificar estos *banners*), pero es aceptable pensar que es una pista admisible.

Así pues, utilizando *nmap*, conjuntamente con FTP y Telnet, has determinado que el servidor que ha estado enviando e-mails de *spams* utiliza un sistema operativo basado en Unix – probablemente FreeBSD- y está configurado para enviar y recibir una gran cantidad de información a través de múltiples servicios, incluyendo FTP, Telnet, http, SMTP y POP3.

5.5. Lecturas recomendadas

Nmap: http://www.insecure.org/nmap/

Más sobre Nmap:
http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8702942&classroom

Fport:
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/fport.htm

Sitios web detallando puertos y los servicios que los utilizan:
http://www.chebucto.ns.ca/~rakerman/port-table.html
http://www.chebucto.ns.ca/~rakerman/port-table.html#IANA
http://www.iana.org/assignments/port-numbers
http://www.networksorcery.com/enp/protocol/ip/ports00000.htm

Diversos DNS lookups: http://www.dnsstuff.com/

Ping: http://www.freesoft.org/CIE/Topics/53.htm