Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEZIONE 5
IDENTIFICAZIONE DI UN SISTEMA

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.

All works copyright ISECOM, 2004.

Informazioni sulla licenza d’uso

Le seguenti lezioni ed il materiale per gli esercizi (workbook) sono materiale di tipo "open" e pubblicamente disponibili, secondo i seguenti termini e condizioni di ISECOM:

Tutto il materiale inerente il progetto Hacker Highschool è fornito esclusivamente per utilizzo formativo di tipo “non-commerciale” verso gli studenti delle scuole elementari, medie e superiori ed in contesti quali istituzioni pubbliche, private e/o facenti parte di attività del tipo “doposcuola”.

Il materiale non può essere riprodotto ai fini di vendita, sotto nessuna forma ed in nessun modo.

L’erogazione di qualunque tipologia di classe, corso, formazione (anche remota) o stage tramite questo materiale a fronte del corrispondimento di tariffe o denaro è espressamente proibito, se sprovvisti di regolare licenza, ivi incluse classi di studenti appartenenti a college, università, trade-schools, campi estivi, invernali o informatici e similari.

Per comprendere le nostre condizioni di utilizzo ed acquistare una licenza per utilizzi di tipo commerciale, vi invitiamo a visitare la sezione LICENSE del sito web Hacker Highschool all’indirizzo http://www.hackerhighschool.org/license.

Il Progetto HHS è uno strumento per apprendere e, come ogni strumento di questo tipo, la chiave formativa consiste nella capacità e nell'influenza dell'istruttore, e non nello strumento formativo. ISECOM non può accettare e/o farsi carico di responsabilità per il modo in cui le informazioni qui contenute possono essere utilizzate, applicate o abusate.

Il Progetto HHS rappresenta uno sforzo di una comunità aperta: se ritenete il nostro lavoro valido ed utile, vi chiediamo di supportarci attraverso l'acquisto di una licenza, una donazione o una sponsorizzazione al progetto.

Tutto il materiale e' sotto copyright ISECOM, 2004

Indice

Hanno contribuito

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Pete Herzog, ISECOM

Per la versione in lingua italiana:

Raoul Chiesa, ISECOM

Doriano Azzena, centro CSAS del progetto Dschola IPSIA Castigliano - Asti

Sophia Danesino, centro CSAS del progetto Dschola ITIS Peano – Torino

Nadia Carpi, centro CSAS del progetto Dschola ITIS Peano – Torino

Fabrizio Sensibile, OPST&OPSA Trainer, @ Mediaservice.net Srl, Torino - ISECOM Authorized Training Partner

Claudio Prono, @ Mediaservice.net Srl, Torino – ISECOM Authorized Training Partner

5.0 Introduzione

E' ovvio che chiunque si sieda alla tastiera di un computer può ottenere informazioni su di esso, incluso il sistema operativo e i programmi attivi, ma è anche possibile utilizzare una connessione di rete per ottenere informazioni su un computer remoto.
Questa lezione descriverà alcuni meccanismi per ottenere tali informazioni.
Conoscere come si possano ottenere tali informazioni vi aiuterà a far sì che il vostro computer locale sia sicuro nei confronti di tali azioni.

5.1 Identificare un Server

Ci sono molti siti sul Web che consentono di collezionare informazioni sui nomi di dominio e indirizzi IP.

5.1.1 Identificare il Proprietario di un Dominio

Il primo passo nell'identificazione di un sistema remoto è quello di esaminare il nome di dominio o indirizzo IP. Utilizzando la ricerca tramite *Whois* è possibile scoprire preziose informazioni, inclusa l'identità del proprietario di un dominio e informazioni su come contattarlo, che possono includere indirizzo e numeri di telefono. Va sottolineato che oggi ci sono così tanti nomi di dominio registrati che non tutti i database *whois* contengono le informazioni su tutti i domini. E' possibile che si debbano esaminare più database *whois* prima di trovare le informazioni sul dominio che vi interessa.

5.1.2 Identificare l'indirizzo IP di un dominio

Esistono molti modi per determinare l'indirizzo IP di un dominio. L'indirizzo si può trovare tra le informazioni *whois* o può essere necessario utilizzare una ricerca tramite *DNS* o *Domain Name Service* (potete ricavare molte informazioni su come scoprire l'indirizzo IP dal nome del dominio tramite un semplice motore di ricerca).

Una volta ottenuto l'indirizzo IP, potete accedere alle informazioni relative ai vari membri della *Number Resource Organization* (http://www.arin.net/ or http://www.ripe.net/), per capire come vengono distribuiti gli indirizzi IP.

I numeri IP vengono assegnati ai fornitori di servizi e reti in grandi quantità, e sapere a quale gruppo appartiene un indirizzo IP e chi ha i diritti in tale gruppo, può essere molto utile. Questo può aiutarvi a ricavare informazioni sul server o sul fornitore di servizi che il sito web utilizza.

Esercizi:

Scegliete un nome di dominio valido e utilizzate la ricerca *Whois* per scoprire chi è il proprietario di quel dominio (http://www.whois.com -> "isecom.org"+Go -> Whois Lookup) Quali altre informazioni sono disponibili? Quando è stato creato tale dominio? Quando scadrà? Quando è stato modificato l'ultima volta?

Trovate l'indirizzo IP di questo dominio. Utilizzando una ricerca tramite *whois* per i vari membri della *Number Resource Organization* determinate a chi è stato assegnato questo indirizzo IP (iniziate con la pagina *www.arin.net*, che fornisce dei collegamenti agli altri membri della NRO). Qual è l'intervallo di indirizzi che sono stati registrati a questa entità?

5.2 Identificare Servizi

Una volta stabilito il proprietario e l'indirizzo IP di un dominio, potete iniziare a cercare informazioni sul server cui si riferisce quel dominio.

5.2.1 Ping e TraceRoute

Ora che sapete chi è il proprietario del dominio e a chi è stato assegnato l'indirizzo IP, potete verificare se il server su cui è caricato il sito web sia attivo. Il comando *ping* vi dirà se c'è attualmente un computer attivo associato a quel dominio e con quale indirizzo IP. Il comando:

ping <dominio> o
ping <indirizzo ip>

vi dirà se c'è un computer attivo a quale indirizzo.

Se l'output del comando *ping* indica che i pacchetti sono stati ricevuti, potete desumere che il server è attivo.

Un altro comando, *tracert* (in Windows) o *traceroute* (in Linux) vi mostrerà i passi effettuati dalle informazioni per transitare dal vostro computer a quello remoto.

Tenere traccia del percorso dei pacchetti vi darà ulteriori informazioni sui computer della rete in cui si trova l'obiettivo del vostro percorso. Ad esempio, computer con indirizzi IP simili saranno parte della stessa rete.

Esercizi:

Effettuate un *Ping* ad un sito web valido o un indirizzo IP (ping www.isecom.org o ping 216.92.116.13). Se ottenete una risposta positiva, effettuate un *ping* all'indirizzo IP successivo. Questo produce una risposta positiva?

Utilizzate *tracert* o *traceroute* per rilevare il percorso dal vostro computer locale all'indirizzo IP che avete usato nell'esercizio precedente. Quanti passi sono necessari? Alcuni computer elencati nel percorso hanno indirizzi simili?

5.2.2 Catturare Banner

Il passaggio successivo nell'identificazione di un sistema remoto consiste nell'utilizzo di telnet e FTP. I programmi server relativi a questi servizi visualizzano messaggi di testo chiamati banner. Un banner può identificare chiaramente e precisamente quale programma server è in esecuzione. Ad esempio, quando vi connettete ad un server FTP anonimo, potete ottenere il seguente messaggio:

Connected to anon.server.

220 ProFTPD Server (Welcome . . .)

User (anon.server:(none)):

Mentre il numero 220 è un codice FTP che indica che il server è pronto per un nuovo utente, il messaggio di testo ProFTPD Server identifica il programma server FTP che è attivo sul computer. Utilizzando un motore di ricerca, potete capire quale sistema operativo utilizza quel programma ed altri dettagli sui suoi requisiti, capacità, limiti e punti deboli.

Il principale difetto dell'uso del *banner grabbing* per ottenere informazioni su un sistema è che un amministratore di sistema astuto può ingannarvi modificando i banner. Un banner del tipo *NonSono AffariTuoi* è ovviamente fuorviante, ma un sistema Unix con un banner del tipo *WS_FTP Server* (un server FTP basato su Windows) può complicare qualunque ricerca intelligente che venga fatta.

5.2.3 Identificare Servizi da Porte e Protocolli

Potete anche determinare quali programmi siano in esecuzione su un sistema osservando quali porte siano aperte e quali protocolli siano utilizzati.

Iniziate ad esaminare il vostro computer locale. Andate in linea di comando o prompt di shell e mandate in esecuzione il programma *netstat* utilizzando il qualificatore *-a* (o all):

```
netstat -a
```

Il computer visualizzerà una lista di porte aperte ed alcuni servizi che stanno utilizzando tali porte:

```
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     *:*
```

Da questo potete esaminare molti programmi e servizi che sono in esecuzione sul vostro computer – molti dei quali probabilmente non immaginavate fossero attivi.

Un altro programma, chiamato *fport*, che fornisce informazioni simili a quelle di *netstat,* ma che dettaglia anche quali programmi utilizzano le porte aperte ed i protocolli (Fport è disponibile per essere scaricato gratuitamente dal sito *www.foundstone.com.*)

Un altro programma, chiamato *nmap* (*network mapper*), indagherà completamente il vostro computer alla ricerca di porte aperte.

nmap visualizza la lista delle porte aperte e dei servizi o protocolli che le utilizzano. Può anche riuscire a determinare quale sistema operativo stia utilizzando il computer. Ad esempio, se eseguite *nmap* sul vostro computer locale, potreste ricevere il seguente output:

```
Port  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 è disponibile sulla Hacker Highschool o L. A. S. cd. E' anche disponibile per il download da www.insecure.org.

Esercizi:

Mandate in esecuzione netstat sul vostro computer locale, utilizzando il qualificatore -a.

```
netstat -a
```

Quali porte sono aperte? Utilizzando un motore di ricerca, potete associare tali porte ai servizi che le utilizzano (questo può anche essere un buon esercizio da fare a casa per esaminare se sul vostro computer siano attivi servizi non necessari – e potenzialmente dannosi – quali FTP e telnet).

Mandate in esecuzione *nmap*, utilizzando il qualificatore -sS (per attivare la scansione di tipo SYN Stealth) e -O (per l'individuazione del sistema operativo) e l'indirizzo IP 127.0.0.1 come obiettivo.

```
nmap -sS -O 127.0.0.1
```

L'indirizzo IP 127.0.0.1 identifica il vostro computer locale (si noti che questo è diverso dall'indirizzo IP che gli altri computer su Internet utilizzano per comunicare con voi; su ogni macchina l'indirizzo IP 127.0.0.1 identifica il computer locale). Quali porte aperte trova nmap? Quali servizi e programmi stanno utilizzando queste porte? Cercate di eseguire nmap mentre avete un browser web o un client telnet aperto. Questo cambia i risultati?

5.3 Individuare le caratteristiche di un sistema

Ora che sapete come identificare un server e come effettuare una scansione delle porte aperte e utilizzare queste informazioni per determinare quali servizi siano attivi, potete mettere insieme le informazioni per individuare le caratteristiche (*fingerprint*) di un sistema remoto, stabilendo quale sia il sistema operativo che il computer remoto utilizza.

5.3.1 Scansione di Computer Remoti

Utilizzando un indirizzo IP o un nome di dominio diverso da 127.0.0.1 come argomento per *nmap* consente di ricercare le porte aperte sui sistemi remoti. Ciò non significa che ci siano porte aperte o che le troverete, ma vi permette di provare.

Per esempio, immaginate di avere ricevuto una grande quantità di e-mail spazzatura, e che vogliate scoprire informazioni sulla persona che vi manda tutta questa posta. Esaminando l'intestazione delle e-mail, potete scoprire che molte provengono dallo stesso indirizzo IP: 256.92.116.13 (si veda **Lezione 9: Sicurezza della Posta** per ulteriori dettagli sulla lettura delle intestazioni delle e-mail).

Una ricerca *whois* mostra che l'indirizzo è parte di un gruppo assegnato ad un grande ISP, ma non vi fornisce informazioni su questo particolare indirizzo.

Se utilizzate *nmap* per scansionare il computer a quell'indirizzo, ottenete il seguente risultato:

```
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
```

Le porte identificate come *filtered* sono note come potenzialmente vulnerabili a attacchi, così non ci sorprende trovarle filtrate. Ciò che è più interessante è che le porte 21, 22 and 23 – cioè ftp, ssh e telnet – siano tutte aperte.

L'ultima cosa che *nmap* fa è identificare il sistema operativo del sistema scansionato. In questo caso le prove che *nmap* effettua sono inconcludenti, tuttavia, dal momento che *nmap* ha rilevato che i servizi ftp e telnet sono entrambi attivi, potete cercare di connettervi con entrambi per vedere se viene visualizzato un banner.

Quando vi connettete attraverso FTP viene visualizzato un banner che informa:

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

Quando vi connettete tramite telnet, il computer visualizza il seguente banner:

FreeBSD/i386 (ttyp7)

Con una ricerca veloce scoprite che *NcFTPd* è un programma Unix program e che *FreeBSD* è un tipo di sistema operativo simile a Unix, così probabilmente sul server è in esecuzione una versione di FreeBSD come sistema operativo. Non potete essere sicuri che questo sia esatto (i banner possono essere alterati), ma potete pensare che sia una supposizione ragionevole.

Così, utilizzando *nmap*, insieme a FTP e telnet, avete determinato che il server che vi sta inviando spamming, gira con un sistema tipo Unix - probabilmente FreeBSD – e che è impostato per ricevere una grande varietà di informazioni incluse FTP, telnet, http, smtp e pop3.

Letture di approfondimento

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

Approfondimento su 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

Un numero di siti in cui potete trovare una lista dettagliata delle porte e dei servizi che le usano:

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

Ricerche DNS: http://www.dnsstuff.com/

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