Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEZIONE 7
ANALISI DI UN ATTACCO

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

Pete Herzog, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, 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

7.0 Introduzione

Vi sono molti programmi sul computer che aprono connessioni di rete. Alcuni di essi hanno una valida ragione per farlo (il vostro browser non funzionerebbe così bene senza l'accesso alla rete), altri invece sono stati scritti da persone con motivazioni discutibili se non criminali. Se si vuole proteggere il proprio computer è necessario imparare come rilevare gli accessi alla rete e identificarne la sorgente e l'intento. Non tutti i tentativi di accesso alla rete sono attacchi, ma se non sapete come distinguere gli amici dai nemici potete anche lasciare la porta aperta !

7.1 Netstat e gli Host Application Firewalls

Per essere in grado di identificare un attacco, dovete sapere quali applicazioni e quali processi sono normalmente in esecuzione sul vostro computer. Osservare semplicemente l'interfaccia grafica, sia in Windows che in Linux, non consente di capire cosa sia in funzione sotto di essa. Netstat ed un firewall possono essere utilizzati per aiutarvi ad identificare quali programmi debbano essere autorizzati a connettersi alla rete.

7.1.1 Netstat

Il comando *netstat* visualizza lo stato della rete. Netstat può darvi informazioni su quali porte sono aperte e sugli indirizzi IP che vi stanno accedendo, su quali protocolli stanno usando tali porte, lo stato delle porte e informazioni sul processo o programma che le utilizza.

Al prompt di comando digitate:

`netstat -aon` (per Windows) o

`netstat -apn` (per Linux)

e netstat visualizzerà una schermata simile a questa:

```
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
```

Ora, dovete far corrispondere i numeri nella colonna PID ai nomi dei processi che sono in esecuzione. In Windows, dovete utilizzare il *Windows Task Manager*, digitando *CTL+ALT+DEL* (se non viene visualizzata la colonna PID, fate click su *Visualizza*, poi *Seleziona Colonne*, e successivamente selezionate *PID*). In Linux, andate nel prompt di comando e digitate *ps auxf* per visualizzare lo stato dei processi.

Nel nostro esempio troviamo che il PID 3400 appartiene al vostro *browser web* e che il PID 2740 appartiene al vostro *client di posta*, entrambi mandati in esecuzione consapevolmente ed entrambi con una buona ragione per connettersi ad Internet. Tuttavia il PID 3838 appartiene ad un programma chiamato *6r1n.exe* e il PID 1516 ad un programma chiamato *buscanv.exe*, nessuno dei quali vi è familiare. Tuttavia la sola ragione che non riconoscete il nome di un programma, non significa che non ci sia un valido motivo per cui sia in esecuzione sul sistema. Il passo successivo è andare su un motore di ricerca e cercare di scoprire a cosa servono tali programmi.

Nella nostra ricerca, scopriamo che *buscanv.exe* è necessario al nostro programma di scansione virus e che deve essere in esecuzione. Tuttavia *6r1n.exe* potebbe essere un trojan. Osservando nuovamente l'output di netstat, possiamo notare che la porta associata al programma 6r1n.exe è la 6667, una porta IRC comunemente utilizzata dai trojans per l'accesso remoto. A questo punto iniziamo la ricerca del metodo per rimuovere il trojan.

7.1.2 I Firewalls

Ora potete sedervi al computer e mandare in esecuzione continuamente netstat per controllare i dati che transitano per il vostro computer o potete usare un programma *firewall* che lo faccia per voi. Un firewall controlla il traffico presente sul vostro computer e utilizza un numero di regole o *filtri* per determinare se ad un programma debba o meno essere consentito l'accesso alla rete. Un firewall può filtrare i dati in base ad un indirizzo IP e a nomi di dominio, porte e protocolli, o anche dati trasmessi. Questo significa che potete fare cose quali:

- bloccare o consentire l'accesso a tutti i dati provenienti da un indirizzo IP specifico
- bloccare o consentire l'accesso a tutti i dati provenienti da un dominio specifico
- chiudere o aprire porte specifiche
- bloccare o abilitare protocolli specifici
- bloccare o consentire l'accesso a tutti i pacchetti che contengono particolari stringhe di dati.

Potete anche combinare questi filtri per consentire il controllo dei dati abilitati a transitare attraverso la rete. Ad esempio potete:

- abilitare i dati provenienti da www.ibiblio.com solo tramite le porte 20 o 21
- abilitare i dati provenienti da www.google.com che utilizzano il protocollo UDP
- abilitare i dati provenienti da *www.yahoo.com* solo attraverso la porta 80 e solo se il pacchetto contiene la stringa di testo "io non sprecherò ampiezza di banda".

Non è comunque necessario che scriviate tutte queste regole da soli. Potete anche sfruttare la capacità di un firewall di impostare autonomamente tali regole. Dopo aver installato per la prima volta un firewall verrete tempestati da una grande quantità di avvertimenti e di richieste di accesso e dovrete decidere se un programma debba o meno accedere alla rete (il firewall può anche darvi l'opzione di demandargli la determinazione di quali programmi debbano giustamente accedere alla rete, ma non imparereste nulla, non vi pare?). Questo processo è simile a quello utilizzato per identificare i programmi visualizzati da netstat. Un programma chiamato *iexplorer.exe* è ovviamente Microsoft's Internet Explorer e, se lo utilizzate come vostro browser web, allora il firewall deve consentirgli l'accesso a Internet. Ma un programma chiamato *cbox.exe* potrebbe essere qualcos'altro. Non avete altra scelta che utilizzare il vostro motore di ricerca preferito per scoprire di cosa si tratta (naturalmente, prima di fare ciò, bisogna indicare al firewall di consentire l'accesso ad Internet al vostro browser).

Il firewall dovrebbe anche darvi l'opzione di accedere ad un programma ripetutamente o solo una volta. Alcuni programmi – come il vostro browser web – dovrebbero avere la possibilità di accedere alla rete in qualunque momento, ma per altri programmi – come quelli che cercano automaticamente gli aggiornamenti del software – potete imparare molto su come lavora il vostro computer impostando il firewall in modo tale che chieda il permesso ad ogni richiesta di accesso del programma.

I Firewall sono disponibili come programmi stand-alone (incluso un numero di versioni free sia per Windows che per Linux) o sono spesso inclusi in software anti-virus. In più Windows XP ha un firewall integrato, ma, come nel caso di Windows Internet Explorer, è stato oggetto di studio da parte di persone alla ricerca di exploits: falle in altri firewall non saranno mai trovate, ma quelle di un firewall Microsoft saranno trovate e utilizzate.

Esercizi

Aprite un prompt di comandi sul vostro computer e digitate:

`netstat -aon` (per Windows) o

`netstat -apn` (per Linux)

Collegate i numeri di PID con i nomi di programmi e cercate di determinare quali programmi sul vostro computer stiano accedendo alla rete (potete anche farlo a casa).

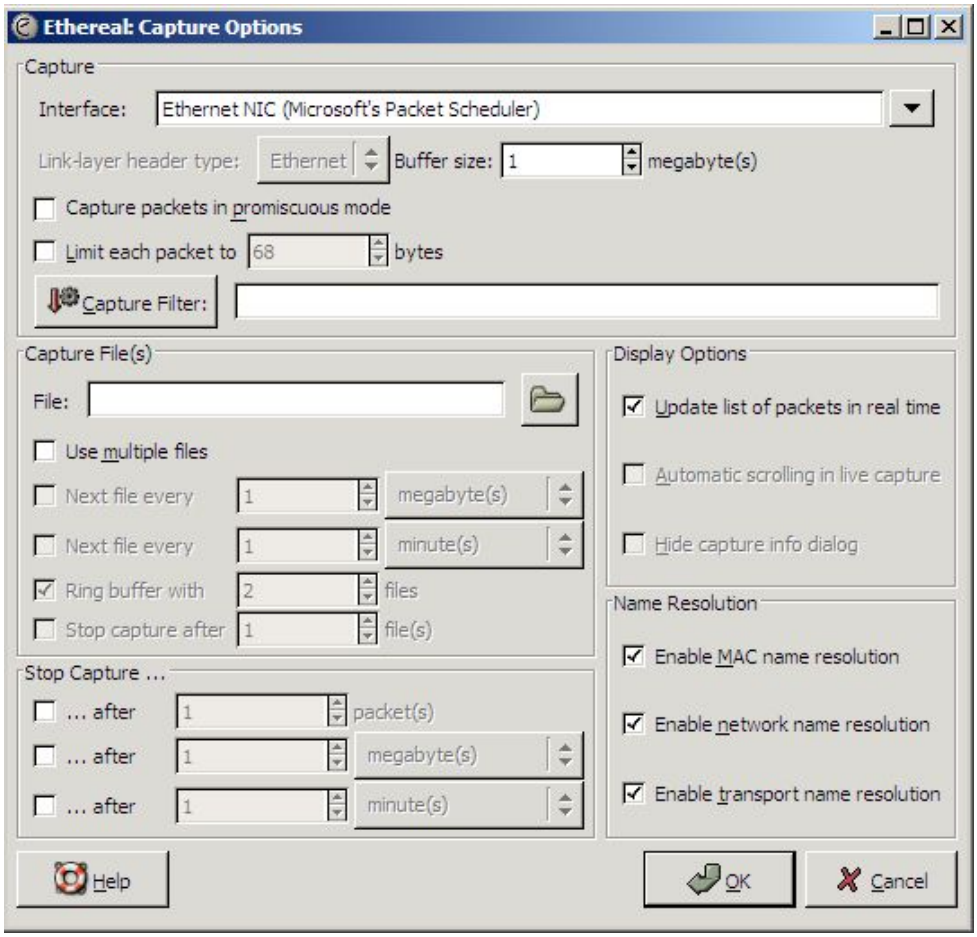
7.2 Packet Sniffers

Netstat individua i programmi connessi alla rete, ma non visualizza quali dati essi stiano inviando. Un *packet sniffer,* tuttavia, vi dà il mezzo per memorizzare e studiare i dati che i programmi stanno inviando sulla rete.

7.2.1 Sniffing

Un packet sniffer memorizza il traffico di rete sul vostro computer, consentendovi di esaminare i dati. *Tcpdump* (e in Windows *windump*) può essere considerato l'archetipo di un packet sniffers, ma useremo *Ethereal* per i nostri esempi poichè l'interfaccia grafica è più semplice e consente più velocemente di memorizzare e esaminare i dati catturati. Se non avete già Ethereal, può essere scaricato da *www.ethereal.com.* Nota per gli utenti Windows: per usare Ethereal su un sistema Windows, dovete prima scaricare e installare il driver per catturare i pacchetti *WinPcap*. WinPcap è disponibile alla pagina di download di Ethereal o su *www.winpcap.polito.it.*

Chiudete tutte le altre applicazioni e mandate in esecuzione Ethereal. Nel menù *Autoscroll in Live Capture* selezionate *View*. Successivamente, fate click su *Capture,* poi *Start* per andare nella videata *Capture Options*. Nella videata *Capture Options*, assicuratevi che non sia selezionata la voce "Capture packets in promiscuous mode", che le tre voci sotto "Name Resolution" siano selezionate e che lo sia anche "Update list of packets in real time".



Ora fate click sul bottone "OK". In teoria non dovrebbe accadere nulla. Verrà visualizzata una finestra in cui sarà presente il numero di pacchetti che sono stati catturati e sotto di essa, vedrete i dati in essi presenti. Vedrete una bassa quantità di traffico causata dai computer presenti nella rete locale per tenere traccia degli altri (ARP, NBNS, ICMP) seguiti da un'attività di DNS poichè Ethereal cerca di risolvere i nomi. Per vedere attività dovete generare traffico. Con Ethereal attivo, aprite il vostro browser. Minimizzate qualunque applicazione tranne lo schermo Ethereal e il browser e fate in modo che siano visibili contemporaneamente. Ora accedete ad un motore di ricerca come *www.google.com*.

Appena la pagina web si carica, dovreste vedere le informazioni sui pacchetti catturati che scorrono nello schermo Ethereal. Selezionate un termine e inseritelo nel campo di ricerca. Selezionate qualche pagina web restituita dal motore di ricerca ed esaminate cosa accade in Ethereal.

Nota: se Ethereal non rileva alcuna attività potreste avere scelto l'interfaccia di rete errata. Andate nella lista *Interface* della videata *Capture Options* e selezionatene una diversa.

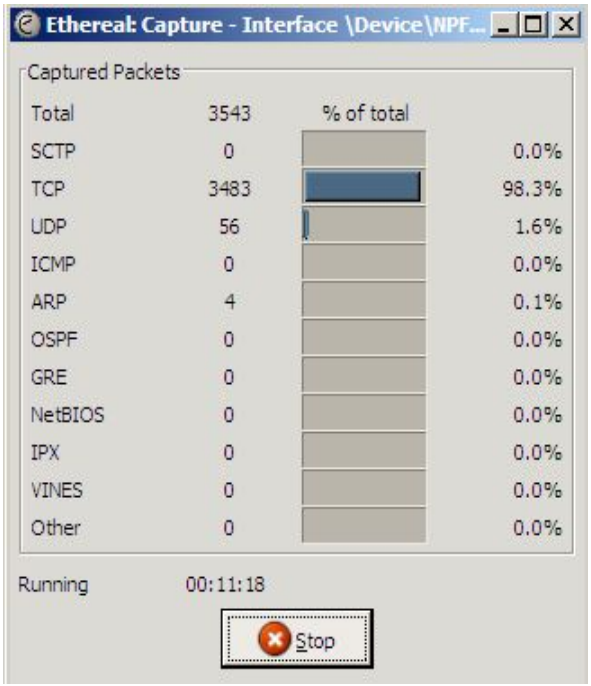
7.2.2 Decodificare il traffico di Rete

Ora che potete esaminare i dati che vengono trasferiti attraverso il vostro computer, dovete capire come decodificarli.

In Ethereal, il primo passo, prima di terminare la sessione di cattura, è quello di osservare la videata di riepilogo che il programma visualizza mentre sta eseguendoo la cattura dei dati.

Per la nostra sessione di browsing la maggior parte dei pacchetti dovrebbero essere pacchetti TCP (se state effettuando uno streaming video il numero di pacchetti UDP è maggiore).

Tuttavia se state catturando una semplice sessione di browsing e vedete un alto numero di pacchetti ARP o ICMP questo può evidenziare un problema.



Dopo aver terminato la sessione di cattura vedrete un output simile a questo:

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

In questo esempio, questi 12 pacchetti illustrano l'attività del browser appena si connette con la pagina specificata. L'informazione più facilmente decifrabile è nella colonna *Source* and *Destination*. L'indirizzo IP 257.10.3.250 è il computer locale; l'altro indirizzo IP è stato risolto da Ethereal. Dal momento che il browser utilizzato è Mozilla Firefox e poichè la pagina di avvio èquella di default di Mozilla Firefox, non ci sorprende vedere l'indirizzo del dominio *mozilla.org* . La richesta inviata a *name.server.com* è probabilmente generata da Ethereal quando effettua una chiamata DNS per risolvere l'indirizzo IP in un nome (nota: questi accessi effettuati da Ethereal sono stati causati dall'opzione che avete selezionato *DisplayOptions* and *Name Resolution;* sono stati impostati a *on* in questo esempio per produrre un output più leggibile; se impostate l'opzione a *off*, non vedrete questi dati aggiuntivi).

Osservando l'informazione sul mittente e destinatario potete scoprire attività non autorizzate. Per esempio, un dominio non familiare a cui si faccia accesso ripetutamente può indicare che avete un programma spyware installato.

La colonna successiva è quella *Protocol*, che indica quale protocollo hanno usato i pacchetti. Nuovamente per sapere se qualcosa è sospetto, dovete sapere cosa aspettarvi. Nella sessione di browsing ci aspettiamo TCP e HTTP, e capiamo perchè ci siano dei pacchetti DNS ma, ad esempio, un numero elevato di pacchetti ICMP potrebbero indicare che sulla macchina è stato effettuato un ping o un trace.

L'ultima colonna, *Info*, fornisce informazioni più dettagliate circa i pacchetti. I pacchetti 2, 3 e 4 mostrano il *three-handed handshake di* SYN, SYN/ACK, ACK, del TCP che indica che è stata effettuata una connessione. Il pacchetto 5 mostra un comando HTTP GET seguito nel pacchetto 7 da una risposta 304 Not Modified response.

Se volete ulteriori informazioni sui pacchetti, gli ultimi due pannelli nella videata di Ethereal visualizzano spiegazioni dettagliate. Il pannello centrale mostra i dettagli dell'intestazione dei pacchetti.

Il pannello in basso mostra un dump in esadecimale e ascii dei dati presenti nel pacchetto.

7.2.3 Sniffing di altri Computers

Alcuni di voi, dopo aver esaminato le informazioni in questa sezione ed aver osservato i dati registrati da Ethereal, si staranno chiedendo se è possibile utilizzare il software di sniffing di pacchetti per registrare l'attività sui computer di altri. E' possibile? Sì e no. Si chiama *modalità promiscua* (promiscous mode) e consente ad uno sniffer di pacchetti di monitorare l'attività di rete di tutti i computer connessi alla rete stessa. Questo significa che potreste essere in grado di registrare l'attività di un altro computer che si trova nella vostra stessa rete (a seconda della modalità con cui è stato settato l'hardware), ma che non è possibile registrare magicamente l'attività di un computer a caso – i due computer devono essere fisicamente connessi e l'hardware e il software opportunamente configurati.

7.2.4 Intrusion Detection Systems

Avete probabilmente capito che, per poter utilizzare uno sniffer di pacchetti e rilevare attività non autorizzata in tempo reale, è necessario sedere al proprio computer osservando l'output del programma di sniffing e sperare disperatamente di vedere un qualche tipo di messaggio. Un *intrusion detection system* effettua questa operazione per voi. Questi programmi combinano l'abilità di registrare l'attività di rete con un insieme di regole che gli consentono di segnalare attività non autorizzate e generare degli avvisi in tempo reale.

Esercizi

1. Aprite *Ethereal* e iniziate a catturare pacchetti. Ora aprite il browser e cercate un documento di testo per il download. Effettuate il download e il salvataggio del file di testo sul vostro hard disk, poi chiudete il browser e chiudete la sessione in Ethereal. esaminate i pacchetti catturati da Ethereal, prestando attensione al dump ASCII nel pannello in basso. Cosa vedete?

Se avete accesso ad un account di posta, verificate la vostra posta mentre Ethereal sta collezionando dati. Cosa vedete?

2. Aprite *Ethereal*. Sullo schermo *Capture Options* Screen, assicuratevi che sia selezionato "Capture packets in promiscuous mode". Questa opzione vi consente di catturare pacchetti diretti a o provenineti da altri computer. Iniziate la raccolta e esaminate cosa accade.

Vedete traffico destinato a computer diversi dal vostro?

Cosa sapete sull'hardware che connette il vostro computer alla rete?

Si connette agli altri computer attraverso uno switch, un router o un hub?

Andate in un motore di ricerca e cercate di capire quali apparecchiature hardware rendono più difficile catturare pacchetti agli altri computer. Quale hardware lo facilita?

3. Collegatevi a *www.snort.org*, o utilizzate un motore di ricerca per cercare sistemi di rilevamento intrusioni. In cosa si differenziano dai firewall?

Cosa hanno in comune con gli sniffer di pacchetti? quale tipo di attività non autorizzata possono rilevare?

Quale tipo di attività non sono in grado di rilevare?

7.3 Honeypots e Honeynets

Le persone che amano guardare le scimmie vanno allo zoo, perchè lì si trovano le scimmie. Le persone a cui piacciono gli uccelli mettono fuori del mangime per uccelli ed questi li raggiungono. Le persone a cui piacciono i pesci comprano un acquario e vi mettono i pesci. Ma cosa si fa se si vuole osservare un hacker?

Si predispone un vaso di miele (*honeypot)*.

Possiamo pensarla in questa maniera: siete un orso. Potete non sapere molto (essendo un orso), ma sapete che il miele è gustoso e che non c'è nulla di meglio in un caldo giorno d'estate che una grande manciata di miele. Così vedete un grande vaso pieno di miele al centro di una radura e state pensando 'Yum!". Ma una volta che infilate la zampa nel vaso di miele, vi rimane incollato. Rischiate di lasciare impronte della zampa così che chiunque sa che qualcuno ha toccato il miele e c'è una buona possibilità che scoprano che siete stato voi. Più di un orso è stato intrappolato per la propria golosità.

Una *honeypot* è un sistema di computer, rete o macchina virtuale che non serve ad altro scopo che come esca per gli hackers. In una honeypot, non ci sono utenti autorizzati – nessun dato reale viene memorizzato nel sistema, nessun lavoro viene realmente effettauato su di esso – così ogni accesso, ogni tentativo di utilizzo, può essere identificato come non autorizzato. Invece di passare al setaccio i log per rilevare intrusioni, l'amministratore di sistema sa che ogni accesso corrisponde ad un'intrusione, così una gran parte del lavoro è già fatta.

7.3.1 Tipi di Honeypots

Ci sono due tipi di honeypots: di *produzione* e *ricerca.*

Le honeypots di *Produzione* sono usate principalmente come sistemi di avvertimento. Identificano un'intrusione e generano un allarme. Possono segnalare che un intruso ha identificato il sistema o la rete come oggetto di interesse, ma non molto altro. Ad esempio, se volete sapere se gli orsi vivono vicini alla vostra radura, potete posizionare dieci vasi di miele. Se li osservate al mattino e ne trovate uno o più vuoti, avrete scoperto che gli orsi si trovano nelle vicinanze, ma null'altro di più.

Le honeypots di *Ricerca* sono usate per raccogliere informazioni sull'attività degli hacker. Esse attirano gli hacker e li tengono occupati, mentre memorizzano le loro azioni. Nel nostro esempio se volete studiare gli orsi invece che semplicemente documentarne la presenza, potete predisporre un grande e gustoso vaso di miele nel mezzo della radura, poi circondarlo di telecamere, registratori e assistenti ricercatori.

Le due tipologie di honeypots differiscono prima di tutto nella loro complessità. Potete installare e mantenere più facilmente una honeypot di produzione per la sua semplicità e per la quantità limitata di informazioni che sperate di collezionare. Si vuole solo sapere di essere stati colpiti, non interessa perchè. Tuttavia in una honeypot di ricerca, volete che gli hacker si fermino in modo tale da capire cosa stiano facendo. Questo rende più difficile l'installazione ed il mantenimento di una honeypot di ricerca, perchè dovete rendere il sistema simile ad uno reale e tale da offrire file o servizi che gli hacker trovino interessanti. Un orso che sa come è un vaso di miele può passare un minuto osservando un vaso vuoto, ma solo un vaso pieno di delizioso miele terrà impegnato l'orso abbastanza a lungo da permettere di studiarne il comportamento.

7.3.2 Costruire una honeypot

Una honeypot non è niente di più che un computer predisposto pensando che sarà compromesso da un intruso. Essenzialmente questo significa connettere un computer con un sistema operativo non sicuro a Internet e lasciarlo lì aspettando che sia colpito: è stata creata una honeypot!

Ma questo non è una honeypot molto utile. E' come lasciare un vaso di miele nella radura e tornare a casa in città. Quando ritornate il miele non ci sarà più, ma voi non saprete nulla su chi, come, quando o perchè. Non imparerete nulla dalla vostra honeypot. Affinchè sia utile, anche l'honeypot più elementare deve avere un qualche tipo di intrusion detection system.

L'intrusion detection system può essere semplice come un firewall. Normalmente un firewall è utilizzato per prevenire l'accesso non autorizzato ad un computer, ma essi memorizzano anche qualunque cosa passi attraverso o la fermano. L'esame dei log prodotti dal firewall può fornire informazioni di base circa i tentativi di accesso alla honeypot.

Honeypots più complesse possono aggiungere hardware, come switches, routers o hubs, per monitorare ulteriormente o controllare l'accesso alla rete. Esse possono anche usare sniffer per raccogliere ulteriori informazioni sul traffico di rete.

Le honeypots di ricerca possono anche mandare in esecuzione programmi che simulano l'uso normale, facendo credere che sull'honeypot stiano facendo accesso utenti autorizzati e si prendono gioco di potenziali intrusi con false e-mail, password e dati. Questi tipi di programmi possono anche essere usati per camuffare sistemi operativi, facendo apparire, ad esempio, un computer di tipo Linux come se stesse utilizzando Windows.

Ma il miele è appiccicoso e c'è sempre la possibilità che il vaso si rilevi un nido di vespe. E quando le vespe tornano a casa non vorresti essere quello che ha la mano incastrata nel vaso. Una honeypot malamente configurata può essere facilmente trasformata in una piattaforma di lancio per ulteriori attacchi. Se un hacker compromette la vostra honeypot, può immediatamente lanciare un attacco ad una grande società o utilizzarlo per inviare spam, e c'è una buona possibilità che siate *voi* ad essere identificati come il responsabile.

Le honeypots correttamente configurate possono controllare il traffico di rete che attraversa il vostro computer. Questa è una soluzione semplice ed efficace, ma gli intrusi comprenderanno facilmente che non si tratta di un sistema reale. Una honeypot più complesso può consentire solo certo traffico in uscita, ma non tutto.

Le honeypots di ricerca – che vogliono trattenere gli intrusi il più a lungo possibile – talvolta utilizzano i *manglers,* che monitorano il traffico in uscita e disarmano i dati potenzialmente pericolosi modificandoli in modo da renderli inoffensivi.

Esercizi

Le honeypots possono essere mezzi utili per cercare e localizzare intrusi, ma utilizzarle per catturare gli intrusi è un'altra questione. Giurisdizioni differenti hanno definizioni e standard differenti e giudici e giurie hanno spesso visioni diverse, così ci sono molte questioni che devono essere prese in considerazione.

Le honeypots rappresentano un tentativo per intrappolare?

Memorizzare l'attività di un hacker è una forma di intercettazione?

E sulla questione specifica delle honeypots: può essere illegale compromettere un sistema progettato per essere compromesso? Queste questioni devono ancora essere approfondite.

Discutete le vostre opinioni sulla legalità dell'utilizzo di honeypots per catturare gli hacker coinvolti in attività criminali. Pensate che sarebbe uno strumento utile garantire l'applicazione della legge? Pensate che costitutisca una "infrazione attraente"? Se un hacker compromette una honeypot, chi pensate sia responsabile in ultima analisi?

Ulteriori approfondimenti

Netstat

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/enus/netstat.mspx

Informazioni generali sui Firewall:

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

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

Uno dei molti firewall free:

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

Firewalling per Linux:

http://www.iptables.org/

Packet Sniffing

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

Snort e IDS:

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

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

Honeypots:

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