Hacker Highschool

SECURITY AWARENESS FOR TEENS



LEZIONE 5
IDENTIFICAZIONE DI UN SISTEMA

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

Creative Commons 3.3 Attribution-Non-Commercial-NoDerivs 2012, ISECOM
WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG

ATTENZIONE

Il progetto Hacker Highschool è uno strumento di apprendimento e come tutti gli strumenti di apprendimento non è esente da pericoli. Alcune lezioni, se usate in modo improprio, possono causare danni fisici. Eventuali pericoli possono emergere anche in caso non si sia svolta una sufficiente ricerca in merito agli effetti di particolari tecnologie. Gli studenti che usano queste lezioni dovrebbero essere incoraggiati ad imparare, provare e testare. Ad ogni buon conto ISECOM non potrà essere ritenuto responsabile per un uso improprio di quanto esposto.

Le seguenti lezioni ed esercizi sono "open" e disponibili pubblicamente alle seguenti condizioni e termini stabiliti da ISECOM:

Tutti i contenuti del progetto Hacker Highschool vengono forniti per uso non-commerciale per gli studenti delle scuole elementari, scuole medie inferiori e scuole medie superiori sia per le istituzioni pubbliche che per quelle private, ammettendone l'uso per le esercitazioni a casa. Non è ammessa la riproduzione del materiale per la vendita. L'utilizzo del materiale presente in queste lezioni è consentito per i corsi di ogni tipo che prevedono il pagamento di una tassa/quota d'iscrizione o frequenza, previa acquisizione di regolare licenza. Sono soggetti a tale norma anche i corsi presso le università, campi estivi e tutto quanto sia inteso come formazione. Per acquistare una licenza è possibile visitare la sezione LICENSE della pagina web della HHS all'indirizzo web http://www.hackerhighschool.org/licensing.html.

Il progetto Hacker Highschool rappresenta lo sforzo di una comunità "open". Pertanto se trovi utile questo materiale ti invitiamo a supportarci tramite l'acquisto di una licenza, attraverso una donazione o una sponsorizzazione.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Indice

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Hanno contribuito

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Bob Monroe, ISECOM
Jaume Abella, ISECOM
Greg Playle, ISECOM
Simone Onofri, ISECOM
Guiomar Corral, Barcelona
Ashar Iqbal

Per la versione in lingua italiana

Raoul Chiesa, ISECOM (Coordinatore Team di lavoro edizione italiana)
Matteo Benedetti, Security Brokers SCpA
Ing. Selene Giupponi, Security Brokers SCpA
Francesco Mininni, Ing. PhD., Uff. E.I.
Riccardo Trifonio, Mar.Ca. CC
Dott. Sandro Bruscino, CISSP
Dott.ssa Sophia Danesino, I.I.S. "G.Peano" TO

ISECOM

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Introduzione

"Penso che il mio portatile abbia un virus", mi disse uno dei miei studenti. "Può darci un'occhiata?"

Presi il portatile, non lo aprii, ma lo inclinai in ogni direzione, osservandolo attentamente. "A me pare un computer," dissi, porgendoglielo.

"Ma qualcosa non funziona," insistette Aidan. "Sono andato a casa di miei amici, mi sono collegato ad Internet e qualcosa è entrato nella mia posta e ha iniziato a inviare messaggi a tutti i miei amici."

"Okay, come è entrato nella tua posta? Hai installato un'applicazione?" Chiesi.

"No, L'ho fatto sul web. Intendo dire su Internet."

"Intendi un browser web?" Lui annuì. "Questo significa che la tua posta è online, non sul tuo computer. In questo caso inizierei con il tuo account di posta. Hai cambiato la password?"

"Sì. Mi avevano bloccato l'account fino a che non l'ho modificata." Guardò in basso come se ci fosse qualcos'altro nella storia, ma non gli feci pressione. Scommetto che gli avevano lo avevano già insultato. Un sacco.

"I tuoi amici hanno ricevuto altri messaggi?" chiesi invece.

"No." Rispose fissando le sue scarpe.

"E hai scelto una password decente? Non 12345?"

Ora sorrise. "E' veramente una difficile. Nessuno la scoprirà mai."

Avevo dubbi su questo, ma annuii. "Okay, allora, sembra che tu abbia risolto tutto."

"No," insistette. "Perchè qualcuno farebbe questo?"

Ora aveva abboccato. "Perchè non lo scopri? Hai qualcuna di queste mail che I tuoi amici hanno ricevuto?"

"Sì. Un mucchio. Le persone me le hanno rigirate." Ah: eccola. Scommetto che nella sua lista i contatti si contano a centinaia. O a migliaia. Deve essere stato divertente.

"Allora credo che tu debba scoprire esattamente dove porta quel link nelle email."

I suoi occhi brillarono. "Significa che si può fare?"

"Oh," risi. "Significa che TU lo puoi fare. Ma ti farò vedere come."

Aidan si fermò. "È questo che intendi dire quando parli della pecora e del lupo?"

"Sì, esattamente questo. Puoi essere l'uno o l'altro. Scegli ora" Gli dissi.

Improvvisamente non sembrò più un bambino. "Lupo" mi disse.

* * *

I sistemi di identificazione possono facilmente essere il passo più importante di attacco ad un computer o di difesa. Tutto quello che si fa dopo dipende dai dati che sono stati raccolti in questa fase. Qual è il sistema operativo dell'host che ti sta attaccando o che si sta difendendo? Riesci a vedere quali applicazioni o servizi sono in esecuzione? Cosa puoi sapere sui dati personali dell'amministratore: sono reperibili in chiaro ovunque? Queste sono le domande a cui si deve rispondere in questa fase. A seconda della parte in cui vi trovate, potete essere felici o inorriditi di scoprire quello che è facilmente ottenibile se si sa cosa cercare.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Sapere come funziona un attacco è fantastico. Sapere come proteggere da un attacco o come sconfiggerlo lo è anche di più. Da qui inizieremo a scavare ed imparare come identificare un sistema e trovare le sue debolezze – sia che sia il proprio sistema o quello di qualcun altro.

Useremo strumenti pubblicamente disponibili e mostreremo anche come usarli. Non ha molto senso mostrare del software ma non insegnare come usarlo. Ogni programma per la sicurezza può essere usato per scopi buoni o cattivi. Il nostro scopo è mostrare entrambi gli scopi in modo tale che possiate risolvere le vostre sfide di sicurezza, e proteggervi allo stesso tempo da attacchi simili.

In questa lezione seguirete due persone di cui una insegna e l'altra impara. L'insegnante non conosce sempre la risposta così come il lettore non sarà sempre imboccato con le informazioni. Impara a esaminare le cose e impara come sistemare le cose che hai individuato. Ripeti se necessario.

Fate attenzione alle opzioni usate nei vari programmi. Un piccolo cambiamento da maiuscola a minuscola può restituire dati completamente differenti, in quali tutti i sistemi operativi. Queste prime poche lezioni sono la base delle reti e di come funziona Internet. Ogni lezione è costruita su ciò che si è imparato nelle precedenti quindi non abbiate fretta, ma salterellare tra I paragrafi e le pagine è un buon modo di familiarizzare con questi materiali prima di tornare indietro e leggerli in dettaglio. Ovviamente non volete lasciarvi sfuggire un'informazione cruciale.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Identificare Server

"Okay, Aidan, cosa hai scoperto?" Stavo cercando di non stringere i denti dalla paura che se ne fosse andato e avesse cliccato quello stupido link nella mail che il suo account hackerato aveva inviato.

"Non ho fatto un click a sinistra," Aidan mi disse, sorridendo come se mi avesse letto nella mente. "Ho fatto un copia-incolla in un file di testo."

"Puoi vedere il testo? O il vero link?"

Fece un'espressione accigliata. "Non sono stupido. Ho fatto click a destra e scelto 'Copia il collegamento'. Poi ho incollato qui. Guarda, link.txt."

"Scusa. Solo per essere sicuro. Allora va bene. Dove porta?"

"Questo dominio da pazzi. Chewmoogoo.com o qualcosa di simile. Ci sono anche un mucchio di altri caratteri dopo quelli," disse, aprendo il suo portatile e mostrandomi il link.

"Oh sì," gli dissi. "Ora ci siamo. Vediamo quali informazioni possiamo raccogliere e gli strumenti che ci possono aiutare a recuperarle. Prima di tutto parliamo di nomi di dominio e indirizzi IP."

Identificare il Proprietario di un Dominio

Il primo passo quando si vuole identificare un sistema remoto è osservare il nome dell'host, il nome di dominio o il suo indirizzo IP. Una ricerca **whois** relativa ad un nome di dominio restituisce molte informazioni:

- L'identità del possessore del dominio, generalmente nome e cognome
- Informazioni di contatto, che possono includere indirizzi, numeri di telefono e indirizzi email
- Il server DNS dove è stato registrato il dominio, che può anche dire quale sia l'ISP che serve il dominio
- L'indirizzo IP del server, un altro indizio potenziale dell'ISP
- Informazioni sul nome di dominio, come la data in cui è stato creato, quando è stato aggiornato e quando scadrà.

Tenete a mente che ci sono moltissimi enti di registrazione di nomi di dominio, e che non tutte le basi di dati *whois* contengono le informazioni di tutti i domini. Potreste avere bisogno di cercare in più di un *database whois* per trovare le informazioni sul dominio su cui state investigando.

Aidan recepì all'istante. "Okay, cosa faccio?"

"Ecco il tuo compito" dissi.

Esercizio

5.1 Trova il nome di dominio su cui stai investigando (se non sei Aidan, scegli isecom.org). Prova il seguente comando su Linux, Windows e OSX.

```
whois isecom.org
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Chi è il proprietario del dominio?
Quando è stato creato? Quando scadrà? (La data di scadenza è un'opportunità?)
Quando è stato aggiornato l'ultima volta?
Quali sono I differenti contatti elencati?
Quali sono I nomi dei server primario e secondario?

5.2 Ora fai la stessa ricerca in un browser (ad esempio, http://www.whois.net -> "sample.com"). Qui c'è la domanda critica: corrisponde a quello che hai scoperto con il comando whois?
Cerca almeno due siti whois (prova http://whois.domaintools.com; puoi trovarne altri?).

Identificare l'indirizzo IP di un Dominio

"Allora cosa hai scoperto?" Chiesi ad Aidan.

"Tutte queste informazioni. Le ho copiate qui." Mi fece vedere il suo file di testo.

"Bene. Tieni ogni piccola informazione. Qual è il dominio IP?"

"Questa cosa, vero?" Aidan mostrò un numero molto lungo.

"Sì. Puoi recuperare l'indirizzo IP di un dominio con il comando whois, o puoi fare una ricerca DNS (DNS lookup) con il comando **ping**:

```
ping isecom.org
```

"La prima cosa che vedrai sarà l'indirizzo IP del dominio."

> Se riesci a catturare una email dall'obiettivo, esamina le **intestazioni della mail** (vedi Lezione 9, Sicurezza delle Email); vi daranno l'indirizzo IP dell'host da cui è partita la mail. Puoi anche usare risorse come motori di ricerca (Lezione 20, Social Engineering) o strumenti come **Maltego** o **FOCA**. Cerca informazioni basate su parole chiave come il nome dell'organizzazione, il contatto presente nella registrazione del dominio, numeri di telefono e indirizzi. Ognuno di questi può portare altre informazioni.

"Una volta che hai ottenuto un IP – o più di uno – dovrai cercare dove si trova. I numeri IP vengono assegnati a fornitori di servizi sparsi in tutto il mondo in grandi gruppi. Trova a quale gruppo è stato assegnato un indirizzo IP (e chi ha i diritti su quel gruppo, se ci riesci). Questo ti può aiutare a scoprire quale server o *service provider* usa quel sito web e - oro colato per te – quale paese ospita quel server," dissi ad Aidan. "scommetto che non è questo. Quindi ecco cosa farai ora."

Esercizi

Ora esaminerai i record DNS direttamente. Un altro modo per trovare informazioni su un dominio e un server è usare le informazioni nel DNS. Qui ci sono i comandi per iniziare.

5.3 Apri una finestra terminare. Prova questo comando:

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
dig isecom.org
```

Il comando funziona sul tuo sistema operativo? Provalo in Windows, Linux e OSX.

5.4 Ora prova questo comando:

```
host isecom.org
```

Il comando funziona sul tuo sistema operativo? Provalo in Windows, Linux e OSX.

5.5 Infine prova questo comando:

```
nslookup isecom.org
```

Il comando funziona sul tuo sistema operativo? Provalo in Windows, Linux e OSX.

Qual è il server DNS per il tuo obiettivo? L'organizzazione ha un server di posta? Il server di posta ha lo stesso indirizzo IP di un server web? Cosa suggerisce questo? Cos'altro puoi imparare?

5.6 Una volta che hai l'indirizzo IP, puoi accedere ai record dei vari membri della **Number Resource Organization** (http://www.arin.net/, http://www.ripe.net/, o http://www.apnic.net/), per capire a fondo come sono distribuiti gli indirizzi IP.

Game On: Taglia e Brucia

Era una sfida all'ultimo sangue per Jace. La battaglia del secolo, ecco come la pensava. Non importava quando sudore, sangue, dolore, forza fisica e intellettuale richiedesse, l'ambiziosa ragazza era decisa a vincere la sua battaglia. Doveva vincere dal momento che non c'era un piano B. I capelli color cacao le ondeggiavano sugli occhi come un torero brandisce il mantello rosso. Un ultimo sospiro profondo e la killer della rete si preparava ad iniziare.

Con le sue dita veloci che scorrevano sulla tastiera, valutò la situazione e immagazzinò le risorse disponibili. Jace aveva già una copia di Nmap memorizzata nel computer. Aveva già eseguito Ping e Traceroute così la combattiva hacker era pronta per iniziare ad affondare il coltello.

Iniziò con una rapida successione di picchiettii sulla tastiera. Una mitragliatrice non avrebbe potuto sparare così velocemente come fece Jace quando iniziò a lavorare sui comandi. I comandi IP non avevano nessuna possibilità contro quella raffica di tasti. Ping, vai! Traceroute, vai! Time to live, vai! Lo spargimento di sangue fu orrendo, un susseguirsi di cadute di bit e byte attraverso il monitor. La CLI sembrava guidare l'assalto di potenti comandi, con attacchi di opzioni al fianco della grande rete.

Jace manovrò il suo attacco principale per ottenere un punto di appoggio all'interno della rete. I suoi esploratori effettuarono una ricognizione intensiva dei firewall, server e router dislocati. Confrontò questi dati con le Common Vulnerabilities and Exposures (CVE) e le incrociò con le informazioni di Network Scanning ottenute con Nmap. Esaminò ogni debolezza, ogni vulnerabilità e exploit per ottenere un vantaggio e valutare il danno. Una tregua non era un'opzione per Jace. Stava vincendo.

Non aveva ancora finito, disse tra sé. Anzi tutto quello che aveva fatto era catturare

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

una piccola parte delle risorse del nemico, ma ciononostante le informazioni di spionaggio erano inestimabili. Jace subì piccole casualità. Le dita e le nocche erano leggermente doloranti. Aveva un livido vicino alla fronte dove aveva battuto contro il monitor per la frustrazione. I TTL la stavano uccidendo.

Alla fine i banner della battaglia mollarono i dettagli senza la necessità si interrogazioni o torture ripetute utilizzando la tecnica "bread-boarding"

Il Raspberry pie venne lasciato come riserva. Jace aveva abbastanza informazioni sul nemico per passare alla fase due dell'attacco di rete. La fase successiva richiedeva il caricamento di email e l'aiuto di un membro interno involontario.

Questa è la parte più spaventosa di qualunque battaglia, ottenere voltagabbana. Jace aveva bisogno di utenti interni che fossero vicini alla sua causa. Ora era tempo di rompere tutte le abitudini di buona sicurezza. La social engineering fu l'arma di distruzione di massa dell'arsenale. Avrebbe creato email legittime caricate con soldati troiani per penetrare le mura interne della rete.

Appena Jace iniziò a costruire la mail malvagia, sapeva che era dalla parte giusta di questo scontro. Non importava cosa avrebbe preso, quanto sarebbe durato, Jace era determinata a scoprire a quale gusto segreto di gelato il caseificio locale stava lavorando.

Il gioco continua...

Identificare i Servizi

"Allora hai salvato tutte queste informazioni, giusto?" Sorrisi ma cercai di non farlo, perché sapevo la risposta anche se la mia natura di insegnante mi fece fare la domanda.

Aidan a malapena mi diede retta: *testa di rapa* stava pensando, ma disse, "Controlli" e mi sporse blocco note.

"Ora ci sono molte informazioni, vero?" feci scorrere le pagine.

"Sì. Devo trovare un modo migliore di tenerne traccia," disse Aidan, riprendendo il computer.

"Certamente. Qual è l'IP obiettivo?" Questa volta sorrisi apertamente.

"Be … sono circa cinque. Può darsi anche di più. Sto cercando di capire perché posso effettuare un ping su alcuni e non su altri"

Buon uomo pensai. Una volta che hai gli IP per un dominio puoi iniziare a scavare nei servizi, e questo significa host in esecuzione. *Oh divertente*.

Ping e Traceroute

"Stai iniziando nel posto giusto. Devi essere sicuro che siano macchine realmente attive. E hai ragione il ping è un tuo amico. Ti sei ricordato di fare un ping al nome di dominio, all'indirizzo IP e ai nomi degli host, vero?"

"Quali sono i nomi degli host?" chiese Aiden.

"Sono quelli con lettere e un punto prima del nome di dominio, come www.isecom.org," gli dissi.

"Non ne vedo nessuno."

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

"Guarda I risultati dei dig. Non hai provato gli altri. Hai provato www.isecom.org e ftp.isecom.org e mail.isecom.org?"

"No...."

"Bene, se ricevi una risposta, c'è qualcosa di attivo a quell'indirizzo. E hai attraversato il firewall. E lasciano anche passare gli ICMP." Aprii una CLI e diedi un comando.

```
C:\>ping isecom.org

Pinging isecom.org [216.92.116.13] with 32 bytes of data:
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56
Reply from 216.92.116.13: bytes=32 time=186ms TTL=56

Ping statistics for 216.92.116.13:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 186ms, Maximum = 186ms, Average = 186ms
```

"Ti dà un'idea di quanto sia lontano I server da te, sia sulla rete che fisicamente, con il *round trip times*. Dividi a metà, e avrai un'idea della distanza del server. Voglio che tu provi anche un altro strumento, traceroute. Si chiama **tracert** in Windows e **traceroute** in Linux. Ti mostra I passi che I pacchetti fanno dal tuo computer a quello obiettivo. Come questo," dissi e digitai di nuovo.

```
C:\>tracert isecom.org
```

"Ora, qui c'è quello che voglio che tu faccia."

Esercizi

5.7 Usa traceroute/tracert per mettere insieme tutte le informazioni che puoi trovare sui computer e I router tra il tuo computer e l'obiettivo.

5.8 I computer con indirizzi IP simili sono spesso parte della stessa rete. Effettua un ping ad un sito o indirizzo IP valido (ad esempio, ping www.isecom.org o ping 216.92.116.13). Se ricevi una risposta positiva, fai un ping al prossimo indirizzo IP. Hai ricevuto una risposta? Prova altri indirizzi vicini.

5.9 Usa un motore di ricerca per scoprire come stimare la distanza dal server.

5.10 Cerca uno strumento che ti aiuti a mappare una server ad una locazione fisica.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

5.11 Cerca uno strumento Visual Trace Route online. Ci sono alcuni siti che offrono strumenti come questo. Questo dovrebbe darti un'idea migliore di dove sia diretto il tuo traffico.

Nmap

"Trovato tutto? Ora ti presento il mio piccolo amico," Dissi, cercando di fare la voce di Scarface. Aidan mi guardò come se avessi due teste, così schiarii la voce e, um, dissi "nmap."

"Può essere veramente semplice, o puoi trovarti veramente in difficoltà. Esegui il comando nmap con un nome host o un indirizzo IP, e lui scandirà quell'host. O usa un insieme di attribuiti per fare cose molto complicate. Se fai la domanda giusta, cercherà di dirti il sistema operativo del tuo obiettivo. Useremo l'opzione 'scan TCP' che è -sT."

```
nmap -sT 216.92.116.13
Starting Nmap 5.51 ( http://nmap.org ) at 2012-05-28 10:58 GTB Daylight
Time
Nmap scan report for 216.92.116.13
Host is up (1.1s latency).
Not shown: 969 closed ports
PORT   STATE SERVICE
25/tcp  open smtp
80/tcp  open http
110/tcp  open pop3
119/tcp  open nntp
135/tcp  open msrpc
139/tcp  open netbios-ssn
143/tcp  open imap
445/tcp  open microsoft-ds
465/tcp  open smtps
554/tcp  open rtsp
Nmap done: 1 IP address (1 host up) scanned in 215.42 seconds
```

E' importare ricordare che nmap non è l'unico strumento per fare queste scansioni, e questa è una buona cosa. Strumenti diversi possono restituire risultati diversi e anzi ognuno di essi può essere deliberatamente fuorviato.

Puoi dire a nmap, ad esempio, di indovinare il sistema operativo – ma non devi aver fiducia nel risultato! Verifica questa ipotesi con altri strumenti.

Banner Grabbing

Aidan era allegro. "Guarda cosa ho trovato ora!" Aveva dei documenti di testo e un foglio di calcolo sul suo portatile, disegni in un taccuino e stampe a colori che dovevano essere costate una fortuna a qualcuno in cartucce di inchiostro.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

"Okay, ora sai che abbiamo alcune macchine attive, chi le gestisce e indicativamente dove si trovano. Ora dobbiamo scoprire di che tipo di macchina si tratta: quale sistema operativo sta girando? Quali servizi sono attivi?" Gli chiesi.

Questo lo rese meno allegro. "Um, come lo scopro?"

"Non ne hai bisogno. Lascia che la macchina riveli i suoi segreti: sistema operativo, servizi e livelli di patch. Quando sei un attaccante, questo rende il tuo lavoro veramente facile; tutto quello che devi fare è cercare gli exploits per quel servizio, software e versione. Se sei il difensore, vorrai negare tali informazioni. O meglio mentire." Questo lo rese pensoso.

"Quindi quello che faremo ora si chiama **banner grabbing**. Parola curiosa: è una **tecnica di numerazione** per reperire tutte queste informazioni sui servizi e le porte attive dell'obiettivo. Ti mostrerò alcuni altri comandi. Puoi usare telnet, ftp o netcat per afferrare un banner. Il banner è quel messaggio di testo che ricevevi in linea di comando nelle vecchie scuole quando ti connettevi e che ti diceva quale programma era attivo sul server. Allora controlla: quando mi connetto ad un FTP server anonimo, ricevo un banner." Digitai alla mia finestra terminale:

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

"Quel numero 220 è un codice che dice che il server è pronto per un altro utente. E non è carino questo: ProFTPD Server è il programma FTP che gira su quell'host. Ora cerchiamo sul web su quali sistemi operativi gira ProFTPD, cosa posso fare … che pasticci ci sono, se ce ne sono." Feci sbattere la tastiera. "Ecco: il tuo prossimo compito è usare il comando ftp."

Esercizio

5.12 Puoi usare FTP o con un nome host o con un indirizzo IP, come questo:

```
ftp isecom.org
```

o

```
ftp 216.92.116.13
```

Provali tutti e due per vedere quale banner restituisce il server FTP. Il tuo risultato può essere simile a questo:

```
Connected to isecom.org.
220 ftp316.pair.com NcFTPd Server (licensed copy) ready.
User (isecom.org:(none)):
```

5.13 Puoi usare anche Telnet o con un nome di host o con un indirizzo IP. Con entrambi puoi specificare la porta, che è 21 quando ti connetti a FTP:

```
telnet isecom.org 21
```

o

```
telnet 216.92.116.13 21
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Di nuovo, vedi quale banner restituisce il server – se lo restituisce. Potresti ottenere qualcosa tipo questo:

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

5.14 Usa netcat o con un nome di host o con un indirizzo IP. Proprio come con Telnet, puoi specificare la porta, che è 21 con FTP:

```
nc isecom.org 21
```

o

```
nc 216.92.116.13 21
```

Di nuovo, vedi quale banner restituisce il server – se lo restituisce.

Banner ingannevoli

"Qui c'è il trucco," dissi ad Aidan. "E' possibile cambiare il banner. Questo è un tipo di **spoofing** – mentire su chi sei. Così posso modificare il banner per leggere *Server NonSonoAffariTuoi,* che è divertente, ma un sistema Unix con un banner che legge *WS_FTP Server* confonderà le persone, perché è un Server Windows FTP server."

"Aspetta un minuto – come si cambia il banner?" chiese.

"Sono contento che tu lo abbia chiesto," dissi.

Esercizio

5.15 Vai sul web e cerca come si cambiano I banner per SMTP, FTP, SSH, HTTP e HTTPS. E' difficile? In altre parole, dovresti semplicemente fidarti di quello che dicono I banner?

Banner Grabbing Automatico

"Ora abbiamo verificato questo. Possiamo tornare a nmap e automatizzarlo; dovremo usare l'attributo -sTV per ottenere i banner." Digitai la prima linea e ottenni questa risposta:

```
nmap -sTV -Pn -n --top-ports 10 --reason -oA hhs_5_06 hackerhighschool.org
Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 05:10 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.30s latency).
PORT    STATE  SERVICE    REASON     VERSION
21/tcp  open   ftp        syn-ack    NcFTPd
22/tcp  open   ssh        syn-ack    OpenSSH 5.9 (protocol 2.0)
23/tcp  closed telnet     conn-refused
25/tcp  filtered smtp     no-response
80/tcp  open   http       syn-ack    Apache httpd 2.2.22
110/tcp open   pop3       syn-ack    Dovecot pop3d
139/tcp closed netbios-ssn  conn-refused
443/tcp open   ssl/http   syn-ack    Apache httpd 2.2.22
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
445/tcp closed  microsoft-ds conn-refused
3389/tcp closed  ms-wbt-server conn-refused
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.32 seconds
```

"Nmap ha trovato NcFTPd, OpenSSH 5.9 (protocol 2.0) e Apache httpd 2.2.22. Tombola: il sistema operativo è Unix. Qualche volta I banner danno la versione del sistema operativo, ma avremmo bisogno di più informazioni per essere così specifici," continuai. "Ecco cosa voglio che tu faccia."

Esercizi

5.16 Usa nmap sull'obiettivo (hackerhighschool.org, se non sei Aidan).

5.17 Prova di nuovo con l'opzione **–version-intensity number** usando numeri da 0 a 9 per avere risultati più accurati. Quali differenze noti in questi risultati?

Identificare i Servizi dalle Porte e dai Protocolli

"Nmap ha effettuato l'ultima scansione guardando i servizi di default. Ma puoi anche farlo nella direzione opposta: cerca prima le porte aperte, poi guarda quale servizio c'è realmente dietro di loro," dissi.

"Aspetta un attimo," Aidan chiese. "le porte non sono sempre le stesse?"

"Sì, in teoria lo sono. Ma in realtà, I numeri di porta sono una sorta di accordo tra gentiluomini. Posso associare I miei servizi a porte diverse se lo voglio."

"Okay, come si fa?"

"Inizia dal tuo computer. Vai in riga di comando e esegui il comando **netstat** con l'attributo **-a** per scandire tutte le porte. Come questo," feci vedere.

```
netstat –a
```

Il giovane hacker seguì il mio esempio, poi esclamò, "Wow! Tutte queste sono aperte?"

Guardai lo schermo. "Il tuo computer si chiama Quasimodo?"

```
Active Connections
Proto  Local Address                  Foreign Address        State
TCP    Quasimodo:microsoft-ds         Quasimodo:0            LISTENING
TCP    Quasimodo:1025                 Quasimodo:0            LISTENING
TCP    Quasimodo:1030                 Quasimodo:0            LISTENING
TCP    Quasimodo:5000                 Quasimodo:0            LISTENING
TCP    Quasimodo:netbios-ssn          Quasimodo:0            LISTENING
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
TCP    Quasimodo:1110         216.239.57.147:http    TIME_WAIT
UDP    Quasimodo:microsoft-ds *:*
UDP    Quasimodo:isakmp       *:*
UDP    Quasimodo:1027         *:*
UDP    Quasimodo:1034         *:*
UDP    Quasimodo:1036         *:*
UDP    Quasimodo:ntp          *:*
UDP    Quasimodo:netbios-ns   *:*
UDP    Quasimodo:netbios-dgm  *:*
```

"Sì, Quasimodo," Aidan sorrise. "Il Gobbo."

"Okay allora, Victor. Questo è quello che voglio che tu faccia."

Esercizi

5.18 Esegui netstat sul tuo computer, con l'opzione -a.

```
netstat -a
```

Quali porte sono aperte?

5.19 Esegui netstat sul tuo computer, con l'opzione -o.

```
netstat -o
```

Quali servizi sono in ascolto dietro a quelle porte?

5.20 Esegui netstat sul tuo computer, con la combinazione di opzioni -aon.

```
netstat -aon
```

Cosa restituisce questa combinazione?

5.21 Usando un motore di ricerca, associa queste porte con I servizi che girano su di loro. Hai bisogno di alcune di loro per servizi come il networking. Ma hai bisogno proprio di tutti I servizi che vedi in esecuzione?

5.22 Esegui nmap, usando l'opzione -sS (per fare un SYN o uno scan chiamato "invisibile", "stealth") e con l'opzione -O (per indovinare il sistema operativo) e indirizzo IP 127.0.0.1 come obiettivo. L'indirizzo IP 127.0.0.1 è chiamato indirizzo di **loopback**. Indica sempre il localhost, il tuo computer locale.

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

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Quali porte aperte ha trovato nmap? Quali servizi e programmi stanno usando queste porte?
Prova ora ad eseguire nmap mentre hai un web browser o un client telnet aperto. Come cambia il risultato del comando?

> Lo "stealth" scan usa solo la prima parte del TCP three-way handshake – il pacchetto SYN – per sondare una porta senza stabilire completamente una connessione. Sebbene questo consenta di superare i log di sistema (che non memorizzeranno il tuo tentativo di connessione a meno che non sia completo), NON è irrilevabile. Qualunque sistema di rilevamento intrusioni è in grado di vedere le tue grosse e grasse impronte su tutta la rete, quindi non illuderti di essere veramente invisibile.

5.23 Nmap ha altre opzioni addizionali a riga di comando. Cosa fanno -sV, -sU, -sP, -A, --top-ports e --reason? Quali altre possibilità ci sono? Se tu fossi un attaccante e volessi rimanere invisibile piuttosto che dare dei colpi al server, quali opzioni *non* dovresti usare, o usare?

5.24 Vai su www.foundstone.com, e trova, effettua il download e installa **fport** sulla tua macchina Windows. È' simile a netstat, ma dettaglia anche quali programmi stanno usando le porte aperte ed I protocolli. Eseguilo. Confrontalo con nstat.

Fingerprinting di un Sistema

"Non sei andato a intralciare in giro e suonare campanelli, vero?" Chiesi.

Aidan rispose lentamente, pensandoci veramente, "No, non penso. Ma è veramente importante? Voglio dire i loro server sono sempre sopra ..."

Lo interruppi. "Non so dove sono, non mi interessa, tu devi operare eticamente - e attentamente – fino a quando lavorerai con me."

"Okay," rispose docilmente.

"E' una buona pratica non lasciare tracce. Cosa che è quasi impossibile. Ma dovresti sempre provarci. Perché le tracce sono esattamente ciò su cui andremo a lavorare ora. O esattamente le impronte...."

"Hey! Non sono la stessa cosa!"

"Okay, giusto. Ma nonostante ciò, noi stiamo per mettere tutto insieme per prendere le impronte al tuo obiettivo, trovare il sistema operativo e tutti i servizi."

Scansire Computer Remoti

"Cosa hai ottenuto dalle tue scansioni? Chiesi. Aidan mi fece vedere un report che aveva copiato in un documento di testo.

```
nmap -sS -O 216.92.116.13
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
Starting Nmap 5.51 ( http://nmap.org ) at 2012-05-28 16:54 GTB Daylight
Time
Nmap scan report for isecom.org (216.92.116.13)
Host is up (0.19s latency).
Not shown: 965 closed ports

PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
25/tcp  filtered smtp
26/tcp  open   rsftp
80/tcp  open   http
110/tcp  open   pop3
111/tcp  filtered rpcbind
113/tcp  filtered auth
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open   imap
161/tcp  filtered snmp
179/tcp  filtered bgp
306/tcp  open   unknown
443/tcp  open   https
445/tcp  filtered microsoft-ds
465/tcp  open   smtps
514/tcp  filtered shell
543/tcp  open   klogin
544/tcp  open   kshell
587/tcp  open   submission
646/tcp  filtered ldp
800/tcp  filtered mdbs_daemon
993/tcp  open   imaps
995/tcp  open   pop3s
1720/tcp filtered H.323/Q.931
2105/tcp open   eklogin
6667/tcp filtered irc
7000/tcp filtered afs3-fileserver
7001/tcp filtered afs3-callback
7007/tcp filtered afs3-bos
7777/tcp filtered cbt
9000/tcp filtered cslistener
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
12345/tcp filtered netbus

31337/tcp filtered Elite

Device type: general purpose|storage-misc

Running (JUST GUESSING): FreeBSD 7.X|6.X (88%)

Aggressive OS guesses: FreeBSD 7.0-BETA4 - 7.0 (88%), FreeBSD 7.0-RC1
(88%), FreeBSD 7.0-RELEASE - 8.0-STABLE (88%), FreeBSD 7.0-STABLE (88%),
FreeBSD

 7.1-RELEASE (88%), FreeBSD 6.3-RELEASE (86%), FreeNAS 0.7 (FreeBSD 7.2-
RELEASE) (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 8 hops

OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 24.09 seconds
```

"Vedi tutte queste porte identificate come **filtered**? Significa che sono protette da un firewall. Sono ben note (well-known) e vulnerabili, quindi devono essere sempre bloccate. Ma guarda: le porte 21, 22 e 80 – cioè FTP, Secure Shell e HTTP – sono tutte aperte." Guardai Aidan.

"Pecore?" chiese speranzoso.

"Bene, preda meritata, quanto meno. Okay. L'ultima cosa che fa nmap è cercare di capire quale sistema operativo sia sul tuo obiettivo. La maggior parte delle volte, come ora, fa solo una 'ipotesi aggressiva,' ma è quasi sempre abbastanza corretta. Poichè la scansione mostra che FTP e SSH sono aperti, I banner che hai trovato saranno l'altra prova.

"Cerca sul web, ci dice che NcFTPd è un programma Unix e che FreeBSD è un sistema operativo tipo Unix. SSH si trova generalmente su sistemi operativi tipo Unix. Quindi è probabile che sul server giri qualche versione di FreeBSD. Questi banner possono essere modificati, ma è un'ipotesi ragionevole.

"Ora, a seconda di dove si trova il tuo obiettivo, il prossimo passo può essere trovare l'ISP. L'ISP stesso può essere famoso per ospitare macchine di spam o siti malevoli – fai una ricerca – potresti lamentarti e ottenere che l'attaccante venga spento. Nel tuo caso non penso che si tratti di un ISP con cui puoi veramente trattare ...

"Perchè non è in..." Aidan esclamò, ma io alzai il mio dito.

"Ferma. La tua informazione è la tua informazione. Non ne ho bisogno, fino a che sei etico e sicuro. Cosa che sei."

Aidan annuì.

"Allora cosa facciamo?" Chiesi.

"Bene, abbiamo un server attivo, giusto?" Aidan iniziò, e tutto quello che potei fare fu un sorriso.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Nutri la mente: Approfindisci Nmap

Diciamo che tu hai identificato l'hostname, il proprietario, la rete e verificato che la macchina di attiva. Ora per identificare un sistema è necessario trovare alcune porte aperte. Non dimenticare che la macchina potrebbe avere tutte le porte chiuse (o anche filtrate).

Per effettuare questo puoi usare il famoso strumento Network Mapper (detto anche **nmap**) da Fyodor. Nmap è un port scanner ed è in grado di sondare da remoto computer per cercare le porte aperte e i servizi di rete associati. Quando esegui nmap, a seconda delle opzioni che usi dalla riga di comando puoi ottenere una lista delle porte aperte e dei servizi o protocolli che usano tali porte. Nmap può anche essere in grado di determinare quale sistema operativo è in uso su quel computer.

Nmap ha molte opzioni e tipi di scansione. Useremo poche opzioni, ma è possibile anche usare

```
nmap --help
```

o

```
man nmap
```

per esaminare I dettagli del comando.

Prima di iniziare, avete letto la lezione 3? Ora è tempo di farlo! Già di ritorno? No? Allora partiamo!

Ok, spieghiamo le differenze tra TCP e UDP e descriviamo il three-way handshake. Conoscere come funziona è importante per capire come funziona nmap.

La sintassi di nmap è:

```
nmap scan-techniques host-discovery options target
```

- **scan-techniques** specifica quale tipo di pacchetto sarà usato e come dovrebbero essere interpretate le risposte dall'obiettivo. Le tecniche principali disponibili sono:
  - **-sS** SYN scan (sì, solo la prima parte del three-handshake)
  - **-sT** TCP Connect scan (three-way handshake completo)
  - **-sA** ACK scan (invia solo pacchetti ACK)
  - **-sU** UDP Scan
  - **-O** OS Detection
  - **-A** Tutte le funzionalità come il rilevamento del SO, plugins, traceroute
- **host-discovery** specifica le tecniche usate per definire se un host è attivo o no. Se l'host è attivo sarà scandito, altrimenti no.
  - **-PE** controlla se un host risponde ad un ping
  - **-PS** controlla se un host risponde ad un SYN
  - **-PA** c controlla se un host risponde ad un ACK
  - **-PU** controlla se un host risponde ad un datagramma UDP
  - **-PN** non controlla, considera tutti gli host attivi (useremo questo perchè sappiamo che il nostro obiettivo è attivo, dal momento che lo abbiamo

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

verificato in precedenza)

- **options** specificano ulteriori dettagli per il tipo di scansione, come
  - **-p1-65535** numeri di porta da scandire (in questo esempio da 1 a 65535).
  - **--top-ports <number>** nmap sa quali sono le porte più frequentemente utilizzate, e può scandire solo per il numero <number> specificato
  - **-T0, -T1, -T2, -T3, -T4** per la velocità di scansione, dove 0 è bassa e 4 è alta (più lento significa più anonimato e meno congestione di rete)
  - **-oA <filename>** per l'output in tutti i tre formati nmap (lo useremo sempre per tenere traccia delle nostre attività)
  - **--reason** nmap scrive in merito ai suoi risultati interpretati (raccomandato)
  - **--packet-trace** simile a –reason ma visualizza le tracce del traffico (si usa per imparare le tecniche di scansione e per la ricerca di errori nella scansione)
  - **-n** not risolve i DNS (non useremo I DNS perché abbiamo già analizzato manualmente)

TCP Scan

La nostra prima scansione inizia con il seguente comando:

```
nmap -sT -Pn -n --top-ports 10 -oA hhs_5_tcp hackerhighschool.org
```

Che fornisce il seguente output:

```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:10 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up (0.23s latency).
PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
23/tcp  closed  telnet
25/tcp  filtered smtp
80/tcp  open   http
110/tcp open   pop3
139/tcp closed  netbios-ssn
443/tcp open   https
445/tcp closed  microsoft-ds
3389/tcp closed  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
```

Abbiamo trovato alcune porte aperte, alcune chiuse e una filtrata. Cosa significa? Dipende dal tipo di scansione (in questo caso -sT). E possiamo usare l'opzione --reason per capire perchè nmap abbia fornito uno Stato particolare.

```
nmap -sT -Pn -n --top-ports 10 --reason -oA hhs_5_tcp_02
hackerhighschool.org
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:17 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.22s latency).
PORT    STATE  SERVICE     REASON
21/tcp  open   ftp         syn-ack
22/tcp  open   ssh         syn-ack
23/tcp  closed telnet      conn-refused
25/tcp  filtered smtp      no-response
80/tcp  open   http        syn-ack
110/tcp open   pop3        syn-ack
139/tcp closed  netbios-ssn  conn-refused
443/tcp open   https       syn-ack
445/tcp closed  microsoft-ds conn-refused
3389/tcp closed  ms-wbt-server conn-refused

Nmap done: 1 IP address (1 host up) scanned in 2.26 seconds
```

Ora abbiamo capito come nmap associ le risposte agli stati in **TCP Scan**:

- **open**: l'obiettivo risponde con un pacchetto SYN ACK
- **closed**: connessione TCP rifiutata
- **filtered**: nessuna risposta dall'obiettivo

Quando trovi porte aperte e filtrate usa altre tecniche di scansione per capire esattamente perché.

SYN Scan

Un'altra famosa tecnica di scansione è lo scan SYN. Quando si effettua questo tipo di scansione, nmap invia solo pacchetti SYN senza completare il three-way handshake. Questo è anche chiamato "half-open" o "stealth" scan perché e connessioni TCP non vengono completate. (deve essere molto chiaro che mentre un obiettivo può non memorizzare una connessione, si sta comunque facendo un "rumore" digitale che può essere intercettato). Usate la scansione di tipo SYN come segue:

```
nmap -sS -Pn -n --top-ports 10 --reason -oA hhs_5_syn
hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-24 12:58 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.15s latency).
PORT    STATE  SERVICE     REASON
21/tcp  open   ftp         syn-ack
22/tcp  open   ssh         syn-ack
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
23/tcp  closed  telnet    reset
25/tcp  filtered smtp     no-response
80/tcp  open    http      syn-ack
110/tcp open    pop3      syn-ack
139/tcp filtered netbios-ssn  no-response
443/tcp open    https     syn-ack
445/tcp filtered microsoft-ds no-response
3389/tcp closed  ms-wbt-server reset

Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
```

I risultati sono simili a quella TCP ma notate le differenze tra "full" TCP Scan e "half-open" SYN scan, confrontando I risultati (con –reason e –packet-trace) utilizzando lo stesso obiettivo con -sT, -sS e -sA (ACK scan).

UDP scan

Un'altra tecnica di scansione è quella UDP: conoscere il motivo è fondamentale per ottenere buoni risultati.

```
nmap -sU -Pn -n --top-ports 10 --reason -oA hhs_5_udp
hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:28 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.23s latency).
PORT    STATE         SERVICE    REASON
53/udp  closed        domain     port-unreach
67/udp  open|filtered dhcps      no-response
123/udp closed        ntp        port-unreach
135/udp closed        msrpc      port-unreach
137/udp closed        netbios-ns  port-unreach
138/udp closed        netbios-dgm port-unreach
161/udp closed        snmp       port-unreach
445/udp closed        microsoft-ds port-unreach
631/udp closed        ipp        port-unreach
1434/udp closed       ms-sql-m   port-unreach

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
```

Può confondere un po'. Cosa è successo? Vediamo alcune ragioni: port-unreach (irraggiungibile, cioè chiusa) e no-response (open | filtered). Perchè? Abbiamo bisogno di ulteriori dettagli. Possiamo usare l'opzione –packet-trace e limitare la

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

scansione a due porte, ad esempio la 53 e 67 UDP:

```
nmap -sU -Pn -n -p53,67 --reason --packet-trace -oA hhs_5_udp_02
hackerhighschool.org


Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:32 CEST
SENT (0.0508s) UDP 192.168.100.53:54940 > 216.92.116.13:67 ttl=46
id=54177 iplen=28
SENT (0.0509s) UDP 192.168.100.53:54940 > 216.92.116.13:53 ttl=37
id=17751 iplen=40
RCVD (0.3583s) ICMP 216.92.116.13 > 192.168.100.53 Port unreachable
(type=3/code=3) ttl=54 id=1724 iplen=56
SENT (2.5989s) UDP 192.168.100.53:54941 > 216.92.116.13:67 ttl=49
id=33695 iplen=28
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.31s latency).
PORT STATE SERVICE REASON
53/udp closed domain port-unreach
67/udp open|filtered dhcps no-response


Nmap done: 1 IP address (1 host up) scanned in 4.15 seconds
```

Abbiamo scoperto che il 192.168.100.53 ha inviato pacchetti UDP alle porte 53 e 67 di hackerhighschool.org. Cosa è successo là? La porta 67 non risponde e per la 53 abbiamo ricevuto un Port Unreachable (T03C03).

Port Unreachable (porta irraggiungibile) significa che la porta è chiusa, e come per no-response – anche se è una risposta normale per UDP – non sappiamo se il servizio sia attivo o no perché il protocollo UDP può solo rispondere se ricevere i pacchetti corretti. Possiamo investigare ulteriormente? Sì, utilizzando -sV Service Scan in cui nmap cerca di inviare pacchetti ben-noti per I servizi UDP.

Service Scan (UDP)

```
nmap -sUV -Pn -n -p53,67 --reason --packet-trace -oA hhs_5_udp_03
hackerhighschool.org


Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 04:44 CEST
SENT (0.1730s) UDP 192.168.100.53:62664 > 216.92.116.13:53 ttl=48
id=23048 iplen=40
SENT (0.1731s) UDP 192.168.100.53:62664 > 216.92.116.13:67 ttl=48
id=53183 iplen=28
RCVD (0.4227s) ICMP 216.92.116.13 > 192.168.100.53 Port unreachable
(type=3/code=3) ttl=54 id=20172 iplen=56
SENT (2.4252s) UDP 192.168.100.53:62665 > 216.92.116.13:67 ttl=50
id=39909 iplen=28
NSOCK (3.8460s) UDP connection requested to 216.92.116.13:67 (IOD #1)
EID 8
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
NSOCK (3.8460s) Callback: CONNECT SUCCESS for EID 8 [216.92.116.13:67]
Service scan sending probe RPCCheck to 216.92.116.13:67 (udp)
...and 80 more packets...
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.25s latency).
PORT  STATE     SERVICE REASON    VERSION
53/udp closed    domain port-unreach
67/udp open|filtered dhcps  no-response
```

Questa volta non siamo stati fortunati, dal momento che abbiamo ricevuto gli stessi risultati. Un buon hacker può anche specificare manualmente I pacchetti UDP, o con il client corretto sulla porta 67. Abbiamo già usato il servizio di scansione, il prossimo passo per identificare i servizi. Imparate i servizi ben noti sulla vostra macchina e fate alcuni esercizi, poi continuate con il banner grabbing.

Esercizi

5.25 Andate su http://nmap.org, effettuate il download e l'installazione dell'ultima versione di nmap per il vostro sistema operativo.

5.26 Ripetete tutte le scansioni di questa sezione utilizzando più porte. Tenete a mente che avrete bisogno del comando sudo sui sistemi Linux, o I diritti di amministratore su macchine Windows.

5.27 Create una tabella riassuntiva con tutte le associazioni relative a tutte le tecniche di scansione, le ragioni e la risposta reale dell'obiettivo (packet-trace).

Rilevamento del SO

Conoscere I servizi è importante per identificare la macchina obiettivo. Nmap può anche aiutare utilizzando opzioni come -A per tutte le scansioni e -O per il rilevamento del SO, utilizzando le porte di default:

```
sudo nmap -A -Pn -n --reason -oA hhs_5_all hackerhighschool.org

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 05:38 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up, received user-set (0.21s latency).
Not shown: 971 closed ports
Reason: 971 resets
PORT   STATE  SERVICE     REASON   VERSION
21/tcp  open   ftp       syn-ack   NcFTPd
22/tcp  open   ssh       syn-ack   OpenSSH 5.9 (protocol 2.0)
|  ssh-hostkey:  1024  cd:27:c2:bf:ad:35:e5:67:e0:1b:cf:ef:ac:2b:18:9a
(DSA)
|_1024 17:83:c5:8a:7a:ac:6c:90:48:04:0b:e5:9c:e5:4d:ab (RSA)
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
25/tcp  filtered smtp      no-response
26/tcp  open   tcpwrapped   syn-ack
80/tcp  open   http      syn-ack   Apache httpd 2.2.22
|_http-title: Hacker Highschool - Security Awareness for Teens
110/tcp  open   pop3      syn-ack   Dovecot pop3d
|_pop3-capabilities: USER CAPA UIDL TOP OK(K) RESP-CODES PIPELINING
STLS SASL(PLAIN LOGIN)
111/tcp  filtered rpcbind     no-response
113/tcp  open   tcpwrapped   syn-ack
143/tcp  open   imap      syn-ack   Dovecot imapd
|_imap-capabilities: LOGIN-REFERRALS QUOTA AUTH=PLAIN LIST-STATUS
CHILDREN CONTEXT=SEARCH THREAD=REFERENCES UIDPLUS SORT IDLE
MULTIAPPEND CONDSTORE ESEARCH Capability UNSELECT AUTH=LOGINA0001
IMAP4rev1 ID WITHIN QRESYNC LIST-EXTENDED SORT=DISPLAY THREAD=REFS
STARTTLS OK completed SEARCHRES ENABLE I18NLEVEL=1 LITERAL+ ESORT
SASL-IR NAMESPACE
161/tcp  filtered snmp      no-response
179/tcp  filtered bgp       no-response
306/tcp  open   tcpwrapped   syn-ack
443/tcp  open   ssl/http    syn-ack   Apache httpd 2.2.22
| ssl-cert: Subject: commonName=www.isecom.org/organizationName=ISECOM
-       The       Institute       for       Security       and       Open
Methodologies/stateOrProvinceName=New York/countryName=US
| Not valid before: 2010-12-11 00:00:00
|_Not valid after: 2013-12-10 23:59:59
|_http-title: Site doesn't have a title (text/html).
|_sslv2: server supports SSLv2 protocol, but no SSLv2 cyphers
465/tcp  open   ssl/smtp    syn-ack   Postfix smtpd
|_smtp-commands: kunatri.pair.com, PIPELINING, SIZE 41943040, ETRN,
AUTH PLAIN LOGIN, AUTH=PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME,
DSN,
|   ssl-cert:   Subject:   commonName=*.pair.com/organizationName=pair
Networks, Inc./stateOrProvinceName=Pennsylvania/countryName=US
| Not valid before: 2012-01-10 00:00:00
|_Not valid after: 2015-01-09 23:59:59
543/tcp  open   tcpwrapped   syn-ack
544/tcp  open   tcpwrapped   syn-ack
587/tcp  open   smtp      syn-ack   Postfix smtpd
|_smtp-commands: kunatri.pair.com, PIPELINING, SIZE 41943040, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|   ssl-cert:   Subject:   commonName=*.pair.com/organizationName=pair
Networks, Inc./stateOrProvinceName=Pennsylvania/countryName=US
| Not valid before: 2012-01-10 00:00:00
|_Not valid after: 2015-01-09 23:59:59
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
646/tcp  filtered ldp          no-response
800/tcp  filtered mdbs_daemon   no-response
993/tcp  open   ssl/imap    syn-ack   Dovecot imapd
|   ssl-cert:   Subject:   commonName=*.pair.com/organizationName=pair
Networks, Inc./stateOrProvinceName=Pennsylvania/countryName=US
| Not valid before: 2012-01-10 00:00:00
|_Not valid after: 2015-01-09 23:59:59
|_sslv2: server supports SSLv2 protocol, but no SSLv2 cyphers
|_imap-capabilities:   LOGIN-REFERRALS   completed   OK   SORT=DISPLAY
Capability   UNSELECT   AUTH=PLAIN   AUTH=LOGINA0001   IMAP4rev1   QUOTA
CONDSTORE LIST-STATUS ID SEARCHRES WITHIN CHILDREN LIST-EXTENDED ESORT
ESEARCH   QRESYNC   CONTEXT=SEARCH   THREAD=REFS   THREAD=REFERENCES
I18NLEVEL=1  UIDPLUS  NAMESPACE  ENABLE  SORT  LITERAL+  IDLE  SASL-IR
MULTIAPPEND
995/tcp  open   ssl/pop3    syn-ack   Dovecot pop3d
|_sslv2: server supports SSLv2 protocol, but no SSLv2 cyphers
|_pop3-capabilities: OK(K) CAPA RESP-CODES UIDL PIPELINING USER TOP
SASL(PLAIN LOGIN)
|   ssl-cert:   Subject:   commonName=*.pair.com/organizationName=pair
Networks, Inc./stateOrProvinceName=Pennsylvania/countryName=US
| Not valid before: 2012-01-10 00:00:00
|_Not valid after: 2015-01-09 23:59:59
2105/tcp open   tcpwrapped   syn-ack
6667/tcp filtered irc          no-response
7000/tcp filtered afs3-fileserver no-response
7001/tcp filtered afs3-callback  no-response
7007/tcp filtered afs3-bos     no-response
7777/tcp filtered cbt          no-response
9000/tcp filtered cslistener   no-response
31337/tcp filtered Elite       no-response
Device type: general purpose|firewall|specialized|router
Running (JUST GUESSING): FreeBSD 6.X|7.X|8.X (98%), m0n0wall FreeBSD
6.X (91%), OpenBSD 4.X (91%), VMware ESX Server 4.X (90%), AVtech
embedded (89%), Juniper JUNOS 9.X (89%)
OS    CPE:    cpe:/o:freebsd:freebsd:6.3    cpe:/o:freebsd:freebsd:7.0
cpe:/o:freebsd:freebsd:8.1                    cpe:/o:m0n0wall:freebsd
cpe:/o:openbsd:openbsd:4.0                     cpe:/o:vmware:esxi:4.1
cpe:/o:m0n0wall:freebsd:6 cpe:/o:juniper:junos:9
Aggressive OS guesses: FreeBSD 6.3-RELEASE (98%), FreeBSD 7.0-RELEASE
(95%), FreeBSD 8.1-RELEASE (94%), FreeBSD 7.1-PRERELEASE 7.2-STABLE
(94%), FreeBSD 7.0-RELEASE - 8.0-STABLE (92%), FreeBSD 7.1-RELEASE
(92%), FreeBSD 7.2-RELEASE - 8.0-RELEASE (91%), FreeBSD 7.0-RC1 (91%),
FreeBSD  7.0-STABLE  (91%),  m0n0wall  1.3b11  -  1.3b15  FreeBSD-based
firewall (91%)
No exact OS matches for host (test conditions non-ideal).
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
Network Distance: 12 hops
Service Info: Host: kunatri.pair.com; OS: Unix

TRACEROUTE (using port 1723/tcp)
HOP RTT    ADDRESS
[...]
8  94.98 ms 89.221.34.153
9  93.70 ms 89.221.34.110
10 211.60 ms 64.210.21.150
11 ...
12 209.28 ms 216.92.116.13

OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.94 seconds
```

Utilizzando -A è possibile visualizzare più dati. Plugin specializzati consentono di estrarre più informazioni dal server, effettuare ipotesi sul SO e usare una variante di traceroute che usa metodi diversi rispetto al normale traceroute o tracert. Per fare ipotesi sul SO è meglio usare più porte.

Esercizi

5.28 Scansiona la tua macchina con nmap. Il SO ipotizzato è corretto?

5.29 Usa l'opzione traceroute su nmap utilizzando diverse porte:

```
nmap -n -Pn --traceroute --version-trace -p80 hackerhighschool.org
```

5.30 Esistono differenze su nmap traceroute se si utilizzano porte diverse e tracert o traceroute dal tuo SO?

5.31 Cerca TCP/IP stack fingerprinting. Come lo sai? E' a prova di spoofing?

Utilizzo di Script

Nmap usa anche molti script utili per lo scanning. Puoi usare l'opzione `-script script-name` per caricare gli scripts. Uno script interessante è `ipidseq`, che effettua una ricerca per IPID di tipo Incrementale. Questo script può essere usato per trovare host adatti all'Idle Scan (-sI).

Questo tipo di scansione sfrutta una caratteristica/falla del protocollo IP, che permette l'esecuzione di scansioni "zombie" per lanciare port scan verso altri indirizzi IP target.

```
nmap --script ipidseq -oA hhs_5_ipidseq hackerhighschool.org
```

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-23 05:47 CEST
Nmap scan report for hackerhighschool.org (216.92.116.13)
Host is up (0.23s latency).
rDNS record for 216.92.116.13: isecom.org
Not shown: 971 closed ports
```

Esercizi

5.32 Cerca la tecnica di Idle Scan. Cos'è e cosa si può fare con essa?

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Conclusioni

Sapere dove cercare e cosa cercare è solo una parte della battaglia per la sicurezza. Le reti sono continuamente esaminate, analizzate, frugate e punzecchiate. Se la rete che state proteggendo non viene osservata allora non state usando gli strumenti giusti per rilevare quel comportamento. Se la rete che state attaccando non è osservata, potete (potete) andare avanti senza effettuare una scansione. Come esperti di sicurezza, dovreste conoscere ogni piccola parte del sistema che state proteggendo – o testando. Dovete conoscere dove sono le debolezze e anche I punti di forza, indipendentemente dalla parte in cui vi trovate.

Raccogliere semplicemente informazioni su un server, come il sistema operativo usato e le porte aperte, non è abbastanza oggigiorno. Un Advanced Persistent Threat cercherà di imparare tutto quello che gli è possibile sulla vostra rete. Queste informazioni includono

- Marca del firewall, modello, versione del firmware e patch software che esistono
- Autenticazione per connessioni remote, privilegi di accesso e processi
- Altri server connessi alla vostra rete, questo include Email, HTML, back-up, ridondanti, off-site, servizi ingaggiati o out-sourced, e anche appalti che possono aver usato la vostra rete o che la stiano usando ora
- Stampanti, fax, fotocopiatrici, router wireless, e connessioni si rete nella sala d'attesa della vostra azienda
- Dispositivi portatili come tablet, smartphone, cornici per foto digitali e qualunque cosa possa essere connessa alla rete.

Anche se sono stati esaminati molti punti in questa lezione, l'identificazione di un sistema copre un'area ben più ampia. Ci sono molte informazioni che attraversano la rete che identificano parti di ogni dispositivo. Ogni dispositivo sulla rete può essere espugnato ed essere così usato come punto di accesso per un attaccante. Affrontare questa sfida che intimorisce richiede più del giusto software. Analizzate le vostre apparecchiature e imparate più che potete. Questa conoscenza vi ripagherà

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Al giorno d'oggi i ragazzi vivono in un mondo in cui possono accedere ai principali canali di comunicazione, ma non hanno le conoscenze per difendersi contro le frodi, i furti d'identità, le violazioni della privacy ed altri attacchi che subiscono quotidianamente per il semplice fatto di utilizzare Internet.
È per questoche esiste Hacker Highschool.

Il progetto Hacker Highschool punta a sviluppare dei materiali per l'apprendimento e la formazione su temi della sicurezza e della privacy per gli studenti delle scuole medie e superiori.

Hacker Highschool è composto da un set di lezioni ed esempi pratici per diventare degli hacker.

Oltre a renderli consapevoli riguardo a temi di cybersecurity ed a fornire le skill necessarie per navigare su Internet, dobbiamo insegnare ai giovani di oggi ad essere pieni di risorse, creativi e ad usare la logica, tutti tratti distintivi di un hacker. Il programma contiene materiali didattici su sicurezza e privacy e supporta gli insegnanti di scuole medie, superiori e private accreditate. Queste lezioni offrono delle sfide ai ragazzi per stimolarli ad essere creativi come un hacker e trattano l'utilizzo sicuro di Internet, la privacy sul web, le ricerche su Internet, evitare virus e trojan, temi legali ed etici ed altro.

Il programma HHS è sviluppato da ISECOM, un gruppo di ricerca no profit, open source, concentrato sulla sensibilizzazione alla sicurezza ed allo sviluppo della sicurezza professionale ed al suo accreditamento.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

Creative Commons 3.3 Attribution-Non-Commercial-NoDerivs 2015, ISECOM