Politiche per la sicurezza delle reti informatiche

Castaldo Luca - Gaito Raffaele

24-10-2008

Sommario

Il seguente documento ha lo scopo di offrire una panoramica su quelli che sono gli strumenti e tecniche utilizzate per l'intrusione in reti informatiche e sistemi informativi. Relative ad ogni attacco e tecnica sono illustrate tutte le contromisure che possono essere adottate per rendere sicuro il sistema che si gestisce. Verrà nel corso del documento seguito un percorso, che mostrerà come possono essere acquisite informazioni relative a reti di calcolatori, ad utilizzare tali informazioni per ricostruire l'architettura di rete ed infine riuscire a trovare calcolatori che possono permettere ad un attaccante di introdursi all'interno del sistema. Verranno quindi mostrate, di pari passo, le tecniche utili ad evitare perdite di informazioni riguardante la rete che si amministra, a nascondere le eventuali topologie di rete e a rendere sicure le singole macchine presenti nel sistema.

Indice

Capitolo 1

Introduzione

La definizione dei termini "hacker" e "cracker" è costante soggetto di discussioni in ambito informatico. Attualmente, al termine "hacker" sono associate due figure: una negativa e l'altra positiva. Nell'uso popolare che ne fanno i media, è utilizzato per indicare intrusi informatici o criminali, con delle connotazioni negative (ad esempio vengo pubblicate news del tipo: "Un hacker ha bucato il sistema di sicurezza statale..."). Nella comunità informatica, il termine viene usato per descrivere un programmatore brillante o tecnicamente esperto (ad esempio Linus Torvalds, creatore del kernel linux, è considerato un hacker). La maggior parte dei componenti della comunità esperta di informatica insiste nel precisare che quest'ultimo è il significato corretto del termine.
I primi usi, da parte dei media, del termine "hacker" risalgono al 1980. Quando il termine è stato introdotto con ampio uso, i molti della comunità informatica hanno etichettato le intrusioni informatiche in generale come operazioni di "hacking". A fronte dell'abuso eccessivo del termine fatto dai media, i più della comunità informatica iniziarono a differenziare maggiormente la terminologia. Termini alternativi, quali "black hat" e "cracker", sono stati introdotti per differenziare le attività criminali, storicamente etichettate con il termine "hack", da quelle legali che sono etichettate con i termini "white hats" e "gray hats". Nonostante questa continua diatribba i media e il grande pubblico continuano a riferirsi ai criminali informatici con il termine "hacker".
In questo lavoro il termine "hacker" non verrà usato per indicare attaccanti criminali intenti all'intrusione in sistemi informatici, ma verrà utilizzato il termine "attaccante" a fronte di eventuali ambiguità. Per quanto riguarda le differenze nei termini "hacker", "cracker", "whitehats" e "blackhats", essi sono perenne soggetto di discussione, e chiunque si sia minimamente addentrato nel settore della sicurezza informatica, può comprendere la differenza tra questi termini. In questo articolo[1] è possibile approfondire tale aspetto.
In questo documento ci occuperemo di analizzare il lavoro svolto da un potenziale "cracker". Quali sono le operazione di ricognizione che potrebbe effettuare, operazioni che gli consentono il recupero parziale o totale di informazioni relative all'organizzazione obiettivo. Successivamente sono analizzate le operazioni di scanning, che gli permettono di effetturare una ricostruzione parziale della topologia di rete in cui intende introdursi, ed infine quali tecniche di break-in

[1] http://en.wikipedia.org/wiki/Hacker_(computing)

sono disponibili per consentirgli di avere accesso al sistema attraverso lo sfruttamento di bug presenti nelle macchine che compongono la rete informatica. In ciascuna di queste fasi sono illustrate quali contromisure possono essere considerate a fronte di tali attacchi, quindi di come rendere sicuro il sistema che si amministra.

Capitolo 2

Ricognizione

In questa sezione verranno illustrate delle tecniche, a disposizione di un possibile attaccante, che gli permettono di ottenere una panoramica sulla struttura di una particolare rete informatica e della sua organizzazione.
Un enorme numero di fonti di informazione sono disponibili in rete, fonti che l'attaccante deve solo saper cercare. Dato che il recupero di tali informazioni, che sono tra l'altro pubbliche, avviene attraverso semplici ricerche utilizzando funzionalità offerte dalla rete, tutte le attività illustrate saranno perfettamente legali e potranno essere condotte da chiunque abbia un interesse verso l'organizzazione oggetto della ricerca. Utilizzando i mezzi che verranno illustrati, un attaccante può ottenere nomi di dominio, indirizzi di rete, contatti personali e altre utili informazioni relative all'organizzazione per cui nutre un particolare tipo di interesse.
Questa fase è essenziale per eseguire un attacco che sia ben focalizzato sull'obiettivo e con una solida strategia di base. La ricognizione (detta anche footprinting) richiede molta pazienza ma permetterà all'attaccante di iniziare con un'entità sconosciuta e finire con una serie di nomi di dominio, reti e sottoreti, indirizzi IP, ecc.
Il footprinting viene classificato solitamente in base al tipo di ambiente nel quale è realizzato: Internet, intranet, accesso remoto o extranet. Questa fase è necessaria perché permette di mostrare quello che l'attaccante vedrà. E' sorprendente la quantità di informazioni pubbliche che si possono trovare su un'organizzazione. Conoscendo quali sono queste informazioni possiamo anche capire quali sono i punti nei quali rivedere le nostre politiche di sicurezza.
Un possibile inizio di ricognizione potrebbe essere fatto facendo delle ricerche utilizzando popolari motori di ricerca presenti sul web, utilizzando ad esempio la funzionalità di ricerca offerta da Google.

2.1 Web searching

Una delle migliori fonti di ricerca utile ad ottenere delle informazioni relative ad una particolare organizzazione, è il sito stesso dell'organizzazione, attraverso l'uso del relativo motore di ricerca interno. Se il sito web non offre tale servizio, le operazioni di ricerca sono sempre praticabili, in quanto le pagine saranno state sicuramente indicizzate dai bot di Google.

Analizzando nel dettaglio il motore di ricerca che offre Google e le sue funzionalità, si scopre che è possibile utilizzare numerosi parametri per effettuare una ricerca, possibilità che viene data affinché possano essere raffinati i risultati dati in output, ma se usate opportunamente consente anche di recuperare informazioni particolari, non propriamente destinate all'utenza generica.
Alcuni dei parametri più interessanti di google sono:

- `site:www.sito.it` si ricerca all'interno del dominio www.sito.it;
- `intitle:stringa` si ricerca stringa all'interno del titolo del sito;
- `allinurl:stringa` si ricerca stringa dentro l'url del sito;
- `filetype:pdf` si ricerca un tipo di file specifico (pdf in questo caso).

I parametri elencati possono essere combinati in speciali richieste consentendo, ad un possibile attaccante, di ottenere più informazioni di quante un webmaster possa voler dare, relative al sito web che cura, informazioni talvota riguardanti dati sensibili. Ad esempio, una ricerca generica del tipo `filetype:bak inurl:htaccess|passwd|shadow|htusers` o `allinurl:auth_user_file.txt`, potrebbe consentire l'accesso a copie di backup di liste contententi credenziali di accesso degli utenti del sistema. Un altro tipo di richiesta, come `intitle:"Index of"`, potrebbe restituire liste di file generate dal server. Tale funzionalità è usualmente disabilitata dai webmaster scrupolosi, in quanto potrebbe fornire informazioni sulla struttura di una directory all'interno del webserver.
Interi libri sono stati scritti su questo argomento, una lettura interessante per approfondirlo potrebbe essere "Google Haks"[1] oppure se si cerca qualcosa di più pratico, "Google Hacking for Penetration Testers"[2].
Anche se un attaccante non riesce a recuperare file di backup contenenti preziose informazioni o script interni, può comunque essere in grado di ottenere informazioni su un'organizzazione, quali:

- contatti dei dipendenti con numeri telefonici;
- informazioni sulla cultura dell'azienda e la lingua;
- informazioni sui propri partner;
- informazioni sui progetti recenti;
- informazioni su acquisizioni e fusioni aziendali;
- informazioni sulle tecnologie utilizzate.

Possedendo queste informazioni, l'avversario può avere una visione della compagnia che potrebbe essere di aiuto in una fase di social engineering[3]. In questo tipo di tecnica, l'attaccante cerca di conquistare la fiducia degli utenti del sistema, facendo sfoggio delle informazioni ottenute opportunamente contestualizzate, permettendogli di acquisire nuove informazioni o addirittura guadagnare l'accesso al sistema informativo.

[1] Tara Calishain and Rael Dornfest. Google Hacks: 100 Insider-Tricks und Tools. O'Reilly.
[2] Johnny Long, Ed Skoudis, and Alrik van Eijkelenborg. Google Hacking For Penetration Testers. Syngress.
[3] Tecnica di raccolta di informazioni basata su strumenti sociali.

Altre funzionalità di Google possono essere sfruttate per ottenere informazioni utili. Si pensi al servizio google maps ed in particolare al servizio street view. Attraverso di essi, un potenziale attaccante può ricavare informazioni che in passato sarebbero state disponibili solo dopo un sopraluogo del posto. In particolare, attraverso google maps, è possibile avere una panoramica dall'alto del quartiere dove è collocata l'organizzazione. In questo modo si possono recuperare informazioni anche a riguardo delle compagnie presenti nelle vicinanze; le strade che permettono l'arrivo agli edifici dell'organizzazione; le eventuali strade interne (se si tratta di una sede con più edifici), ecc. Tutta questa conoscenza potrà, ancora una volta, essere usata dall'attaccante durante la fase di ingegneria sociale. Stesso discorso vale per il nuovissimo servizio street view attraverso il quale addirittura si può accedere alle strade non dall'alto ma, bensì, dalla posizione di un'auto. In questo modo si moltiplicano le informazioni che possono essere ottenute.
Altro fattore da tenere in considerazione è quello riguardante le informazioni pubblicate e poi cancellate. Si può, erroneamente, pensare che una volta cancellate delle informazioni dal proprio sito web esse non siano più disponibili. Ancora una volta, attraverso servizi di google e non, invece è possibile recuperare tali informazioni. Esempi di servizi che offrono la navigazione "storica" sono google cache e archive.org. Attraverso il primo è possibile recuperare pagine web salvate nell'enorme cache di google. Anche quando si tratta di pagine non più disponibili online. Archive.org invece fornisce un archivio storico delle pagine web attraverso il quale si può accedere a vecchie versioni di siti web anche vecchie di alcuni anni. Qualiasi persona potrebbe controllare la presenza su vecchie pagine di informazioni utili che dopo sono state cancellate.
Un'ulteriore area di ricerca che può essere sfruttata quando si possiedono parziali informazioni sull'organizzazione, sono i forum. I forum sono siti web che nascono con l'obiettivo di risolvere problemi presentati da utenti in maniera cooperativa. L'attaccante, avendo ottenuto in qualche modo contatti di dipendenti di una particolare azienda, potrebbe effettuare ricerche all'interno di tali piattaforme al fine di trovare informazioni utili, su hardware o software con cui i dipendenti hanno riscontrato problemi, venendo così a conoscenza di informazioni parziali o totali della struttura hardware e software dell'organizzazione.
In un contesto pratico, una possibile ricerca potrebbe essere fatta su Usenet, protocollo di rete su cui lavorano i newsgroup. I newsgroup rappresentano un contenitore di informazioni su larga scala nei quali, spesso l'utenza espone dettagliate questioni tecniche relative ad esempio a problemi di confgiurazione di un particolare sistema o risoluzione di uno specifico problema hardware o software. Queste situazioni facilitano di molto il lavoro degli attaccanti, in quanto tali discussioni forniscono informazioni delicate, relative a prodotti hardware utilizzati dall'organizzazione o a specifiche configurazioni di sistema su cui l'organizzazione si poggia per svolgere il suo lavoro. In aggiunta, un attaccante può partecipare attivamente a discussioni di questo tipo e suggerire soluzioni errate ai problemi presentati, cercando di facilitare i sui tentativi di attacchi futuri.
Come strumento di ricerca per i Newsgroup, può essere utilizzato l'engine di Google attraverso il quale sono raccolti e organizzati tutti i post sotto una comoda interfaccia grafica.
Ultimi, ma non per importanza, sono i servizi di social network diffusisi moltissimo negli ultimi anni. Siti come facebook.com, twitter.com, myspace.com, flickr.com, ecc., sono, oggigiorno, la principale fonte di informazioni riguardan-

te le persone. La fase di ricerca di dati (molto spesso anche sensibili) viene enormemente facilitata dagli utenti di questi servizi che, spesso e volentieri, pubblicano informazioni personali (nome, cognome, email, età, foto, ecc.) in grande quantità non tenendo in considerazione minimamente i possibili risvolti negativi.

2.1.1 Contromisure per la perdita di informazioni sul web

Un certo numero di profili di una società si possono sempre ottenere. É sempre un po' difficile riuscire a nascondere informazioni relative a prodotti, progetti, partners, e così via. Una contromisura che può essere considerata, tra l'altro anche la più naturale, è quella di prestare attenzione al tipo di informazioni che si rendono accessibili via web. Ad esempio diagrammi tecnici dell'architettura aziendale non dovrebbero essere disponibili sul sito web, o quantomeno non in un'area accessibile a tutti. Molti file possono essere indicizzati dagli spider utilizzati dai motori di ricerca e finire nelle varie liste pubbliche di ricerca.
Una ulteriore contromisura è quella di evitare di postare su Usenet materiale tecnico dettagliato relativo a risorse o a problemi tecnici riscontrati nel sistema informativo. A tal fine potrebbe essere molto utili fornire corsi educativi al personale, volti alla sensibilizzazione rispetto all'argomento sicurezza, ed in particolare mostrare ai dipendenti come il rilascio di alcune informazioni, in questo caso sui newsgroup o forum, possano essere dannose per la sicurezza dell'intero sistema. Stesso discorso per i rischi che si corrono pubblicando dati personali sui social network.
Inoltre, per i web master, conoscere la configurazione del proprio webserver e quali informazioni sono rese accessibili all'utenza. Un buon punto di partenza potrebbe essere quello di disabilitare il "directory-listing" che abilita il webserver a listare il contenuto delle cartelle, evitando di rendere la gerarchia dei file del sito web pubblica.
Molte delle informazioni, come abbiamo visto, si ottengono tramite google e altri motori di ricerca. Sarebbe, quindi, utile disabilitare l'indicizzazione di quelle aree del sito che non si vogliono mostrare al mondo intero (ad es. le pagine riservate al personale).

2.2 Whois databases

Internet ha una organizzazione gerarchica e molte delle informazioni sulla sua struttura sono, contrariamente a quanto si potrebbe pensare, gestite in modo centralizzato. Un'organizzazione no-profit di nome ICANN [4] ha la responsabilità di gestire dati (nomi di dominio, indirizzi ip, ecc.) riguardante la struttura di Internet. Molte informazioni interessanti possono essere trovate sul sito dell'ICANN e su quello di altre organizzazioni del genere:

- APNIC [5] per la zona Asia/Pacifico;
- ARIN [6] per la zona America e parte di quella Africa;

[4] Internet Corporation for Assigned Names and Numbers, http://www.icann.org
[5] http://www.apnic.net
[6] http://www.arin.net

- LACNIC [7] per alcune zone dell'America latina e Caraibi;
- RIPE [8] per la zona Europa, parte di quella Africa e regioni dell'est.

Enormi archivi di questo tipo gestiti sono i database whois. Degli attaccanti possono ottenere informazioni sullo staff tecnico utilizzando questi database sul nome di dominio dell'organizzazione a cui sono interessati. Molto spesso sono presenti i contatti, come indirizzi, email, numeri teleforici, degli amministratori di rete. Il database whois può essere utilizzato sia sottomettendo query utilizzando un terminale (con il tool *whois* presente in tutti i sistemi *nix) oppure utilizzando comode interfacce web.
Di seguito viene riportato le informazioni che possono essere ottenute attraverso una query fatta al database whois per il domino "www.unisa.it" dell'Università degli Studi di Salerno:

```
Domain
Domain:  unisa.it
Status:  ACTIVE
Created:  1996-01-29 00:00:00
Expire Date:  2009-01-29
Last Update:  2008-02-14 00:03:05

Registrant
Name:  Universita' di Salerno
ContactID: UNIV410-ITNIC
Address:  Universita' di Salerno
84081 - Baronissi (SA)
IT
Nationality:  IT
Phone:  +39.89822330
Fax:  +39.89822272
Created:  2007-03-01 10:47:03
Last Update:  2007-03-01 10:47:03

Admin
Name:  Giuseppe Cattaneo
ContactID: GC1419-ITNIC
Address:  Universita' di Salerno
84081 - Baronissi (SA)
IT
Phone:  +39.89822330
Fax:  +39.89822272
Email:  cattaneo@udsab.dia.unisa.it
Created:  1994-11-12 00:00:00
Last Update:  2007-03-01 07:37:02


Tech
```

[7] http://www.lacnic.net
[8] http://www.ripe.net

```
Name:  Vittorio Galdi
ContactID: VG491-ITNIC
Address:  Centro Elaborazione Dati
Via Ponte Don Melillo
84084 - Fisciano (SA)
IT
Phone:  +39.089966423
Fax:  +39.089966344
Email:  galdi@unisa.it
Created:  2000-06-21 00:00:00
Last Update:  2007-03-01 07:37:02

Name:  Salvatore Ferrandino
ContactID: SF1707-ITNIC
Address:  Centro Elaborazione Dati
Via Ponte Don Melillo
84084 - Fisciano (SA)
IT
Phone:  +39.089966349
Fax:  +39.089966346
Email:  salfer@unisa.it
Created:  2000-06-21 00:00:00
Last Update:  2007-03-01 07:49:16

Registrar
Organization:  Consortium GARR
Name:  GARR-MNT

Nameserver
ns.unisa.it
dns-001.unisa.it
ns1.garr.net
```

Questa semplice query ci permette di ottenere informazioni su tre persone in particolare: una che ricopre il ruolo di amministratore (Giuseppe Cattaneo) e di alte due che ricoprono il ruolo di tecnici (Vittorio Galdi e Salvatore Ferrandino) del sistema. La query fornisce infomazioni relative a recapiti telefonici e indirizzi email, informazioni che potranno essere utili in fasi successive.
Altri link con informazioni utili sono i seguenti:

- Allocazione IP v4: http://www.iana.org/assignments/ipv4-address-space;
- Servizi indirizzi IP: http://www.iana.org/ipaddress/ip-addresses.htm;
- Indirizzi IP: http://www.rfc-editor.org/rfc/rfc3330.txt Special-use;
- Numeri di porta registrati: http://www.iana.org/assignments/port-numbers;
- Numeri di protocollo registrati: http://www.iana.org/assignments/protocol-numbers.

Tabella 2.1: Record DNS più importanti

Tipo di Record	**Significato**
Address (A Record)	Mappa un nome di dominio su un IP
Host Information (HINFO Record)	Identifica il sistema dell'host associato ad un dominio
Mail Exchanger (MX Record)	Identifica il sistema mail di un dominio
Name Server (NS Record)	Identifica i server DNS associati ad un dominio
Text (TXT Record)	Testo arbitrario associato ad un dominio

2.2.1 Difesa contro la perdita di informazioni whois

Una soluzione molto semplice per porre rimedio a tale perdita di informazione, potrebbe essere quella di rendere visibile un generico indirizzo email per i contatti (del tipo admin@nomedominio.it), anziché rilasciare il nome o i nomi degli amministratori di rete.
In ogni caso l'attenzione a questi dati rilasciati deve essere elevata. Per le organizzazioni di grosse dimensioni si può pensare di pubblicare informazioni non direttamente riferibili all'azienda ma che rimandino ad un ufficio esterno che si occupi di rilevari potenziali attacchi di ingegneria sociale.
Esistono, inoltre, servizi che permettono di registrare nomi di dominio in modo anonimo attraverso i quali, pagando una cifra aggiuntiva, si possono lasciare vuoti i campi del database whois riguardanti indirizzo, numero di telefono, email, ecc.

2.3 DNS

Il DNS (Domain Name System) è una delle più importanti componenti di Internet. Il DNS è un database gerarchico distribuito nel mondo che memorizza numerose informazioni: indirizzi ip, nomi di dominio, email e altre informazioni relative a server. Mostreremo ora come un attaccante può sfruttare funzionalità messe a disposizione da un server DNS per ottenere informazioni utili.
Innanzitutto è possibile ottenere l'indirizzo ip associato ad un particolare nome di dominio. Oltre a questa informazione, ce ne sono altre che possono essere recuperate, se memorizzate all'interno dei database DNS. Nella tabella 2.1 sono riassunte tutte le più importanti informazioni che possono essere recuperate.
É possibile quindi recuperare informazioni relative al nome di dominio come indirizzo IP, informazioni sull'host, informazioni sul mail server, ed altro ancora, ovviamente se presenti nei record DNS.
Ogni organizzazione con sistemi accessibili via Internet, per poter essere raggiunta attraverso un nome di dominio, deve necessariamente possedere dei record memorizzati in dei server DNS.
Un server DNS ospita solo una parte dei record come quelli presenti nella tabella 2.1. Ad esempio, un'azienda può avere 20 records dedicati agli indirizzi dei mail server, FTP server e web server, alcuni mail exchange records specificano quali server possono accettare posta elettronica e altri records di server DNS

mostrano il server stesso.
Una società può scegliere di implementare per conto proprio un server DNS in cui salvare le informazioni relative ai propri server. Alternativamente, può scegliere un provider che gli fornisca servizi di DNS.
Indipendentemente dalla scelta effettuata, possono essere recuperate una grossa mole di informazioni utili. Consultando i DNS di un'organizzazione, un attaccante può pianificare una strategia di attacco all'organizzazione a cui è interessato. Inoltre, se presente anche il record HINFO, l'attaccante può ottenere informazioni relative al sistema operativo utilizzato dal server, informazioni preziose nella ricerca degli exploits.

2.3.1 Interrogare un server DNS

Come un attaccante ottiene informazioni DNS? La prima operazione che viene eseguita è quella di individuare uno o più server DNS che ospitano le informazioni relative all'organizzazione obiettivo. I nomi dei server sono ottenuti attraverso il comando `whois` sul dominio in questione. I server DNS, nell'output del comando, sono elencati sotto le voci "name server" e "domain server".
Nell'esempio precedente (relativo al dominio "www.unisa.it") abbiamo visto per ultimo il record "nameserver", contenente i domini "ns.unisa.it", "dns-001.unisa.it", "ns1.garr.net", nomi che corrispondono ai DNS del dominio "www.unisa.it".
Ottenuti tali riferimenti, un attaccante ha la possibilità di scegliere tra un numero rilevante di tools, che gli consentono di ottenere delle informazioni contenute sui server trovati attraverso delle interrogazioni. Uno dei tool più popolari è `nslookup` (presente sia per *nix che per windows).
Una tecnica che un attaccante potrebbe utilizzare è quella del *trasferimento di zona*. La tecnica in questione è abbastanza vecchia ma va considerata perché permette all'attaccante di ottenere informazoni importanti e non tutti i server DNS l'hanno disabilitata. Il trasferimento di zona permette ad un secondo server di aggiornare il suo database DNS partendo da un server primario. Questa feature utilizzata per la ridondanza dei server DNS può, però, essere sfruttata da un attaccante. Alcuni server DNS inviano una copia del loro database a chiunque ne faccia richiesta e la perdita di dati riguardanti la propria struttura interna a un utente qualsiasi è pericoloso.
Un modo per effettuare un trasferimento di zona è quello di specificare nel comando `nslookup` il server DNS a cui si fa la richiesta, attraverso la direttiva *server [server_target]*. Usando la direttiva *set type=any*, si chiede al server di tenere restituire tutti i tipi di record che possiede. Un trasferimento di zona può essere fatto attraverso l'esecuzione del comando *ls -d [dominio_target]*, comando che mostra in output le informazioni restituite dal nameserver.
Un modo alternativo di procedere (specie quando il comando ls non è implementato) è quello di lanciare il comando *nslookup*, settando il tipo di richiesta con *set type=any* e il dominio sul quale ottenere informazioni.
Un tool alternativo, molto utilizzato in ambiente *nix per effettuare richieste ai server DNS, è `dig`. Per effettuare un trasferimento di zona, utilizzando questo comando, è necessario rispettare la seguente sintassi: *dig @server_dns dominio_obiettivo tipo_richiesta*.
Il trasferimento di zona non sempre è possibile perché il alcuni casi può essere disabilitato tale funzionalità sui server DNS. La figura 2.1 mostra un trasferi-

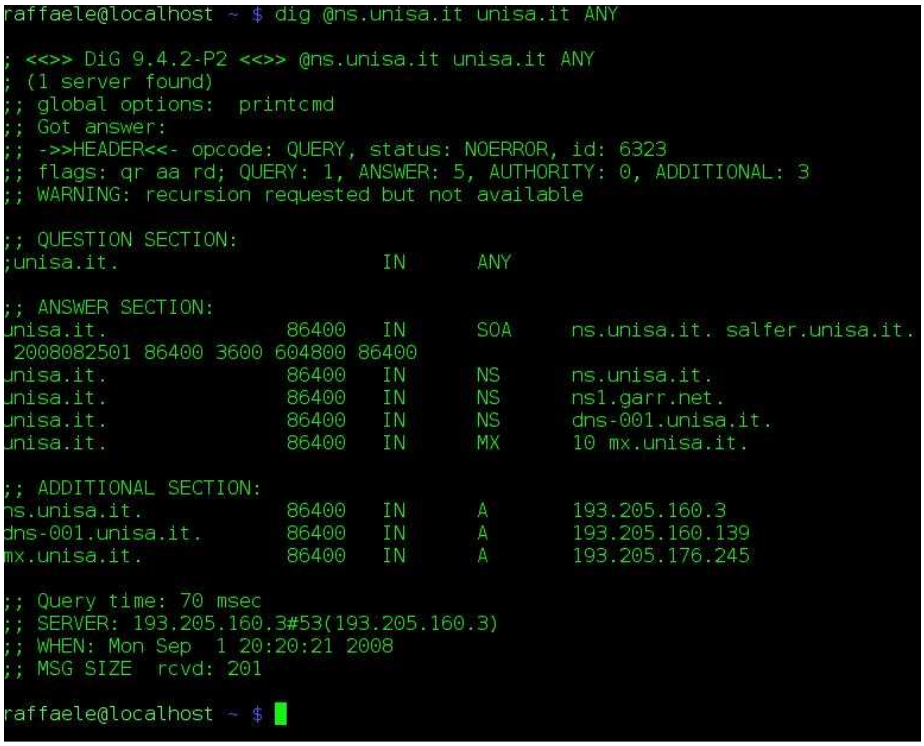

Figura 2.1: esempio pratico dell'utilizzo del comando dig sul dominio unisa.

mento di zona effettuata sul solito dominio www.unisa.it con l'utilizzo del tool *dig*. Altri tools utili per la ricerca di informazioni DNS sono:

host: presente in tutti i sistemi *nix;

adig: alternativa a dig per i sistemi windows.

Come si evince dalla figura 2.1, per effettuare il trasferimento di zona abbiamo utilizzato il server DNS "ns.unisa.it" che avevamo ricavato in precedenza attraverso la funzionalità di *whois*. Alcune di queste informazioni potrebbero aiutare un potenziale attaccante nella ricerca di vulnerabilità note.

2.3.2 Difesa contro la ricognizione dns-based

Quali contromisure possono essere prese per la perdita di informazioni da un server DNS? Ci sono alcune tecniche che potrebbero essere conbinate a tale scopo. Come prima operazione, occorre accertarsi di non fornire informazioni non necessarie attraverso i DNS. Per svolgere la sua attività principale, un server DNS necessita solo di conoscere la corrispondenza tra nome di dominio ed indirizzo IP, di conoscere il name server ed un eventuale mail server. Tutte le altre informazioni sono superflue, e se inserite, potrebbero essere d'aiuto ad un potenziale attaccante. In particolare, il nome di dominio non dovrebbe indicare il tipo di sistema operativo utilizzato (molto spesso, infatti, si usano nomi del tipo debian.dominio.it oppure win.dominio.it). Ugualmente, è buona norma non

inserire testo nei campi HINFO e TXT, campi di tipo descrittivi, che non sono posti con lo scopo di migliorare il lavoro del server DNS, ma sono presenti solo a titolo informativo.
Il passo successivo potrebbe essere quello di limitare il trasferimento di zona. Di solito tale operazione viene richiesta quando si vuole tenere un DNS secondario. L'operazione, infatti, permette di sincronizzarlo con uno principale. In aggiunta a questo caso specifico, non ci sono scenari in cui si evince l'utilità di tale operazione, quindi, per limitare il rilascio di informazioni attraverso questa funzionalità occore configurare il proprio DNS appropriatamente. In **bind** (tra i server DNS più popolari) è possibile utilizzare la direttiva "allow-transfer" o quella "xfernets" specificando esattamente l'indirizzo ip e la rete che vogliamo abilitare al trasferimento di zona. Si può inoltre configurare il proprio firewall o router esterno con regole per abilitare l'accesso alla porta 53 solo ai server dedicati al backup. É importante considerare che la porta UDP 53 è utilizzata per lo scambio richieste e risposte DNS e che deve essere accessibile per permettere al server di risolvere nomi di dominio. La porta TCP 53 è usata per il trasferimento di zona e quindi dovrebbe essere abilitata solo per una lista di DNS secondari.
Una ulteriore tecnica per limitare la perdita di informazione è quella dello *split DNS*che permette di limitare la quantità di informazioni da pubblicare sulla propria infrastruttura. La maggior parte degli utenti di internet ha la necessita di accedere solo al servizio di risoluzione di un nome di dominio per la propria impresa. Se si posseggono decine di migliaia di sistemi a cui si fornisce il servizio, il pubblico necessita solo di accedere ad un numero ridotto di sistemi (web, mail, ftp). Non ci sono ragioni quindi di rendere accessibile a tutti i record che contengono dati sensibili relativi ai sistemi interni. Uno split DNS, chiamato anche Split-Brain, permette di separare i record DNS che si vogliono pubblicare da quelli che si vogliono tenere interni. La figura 2.2 mostra una infrastruttura

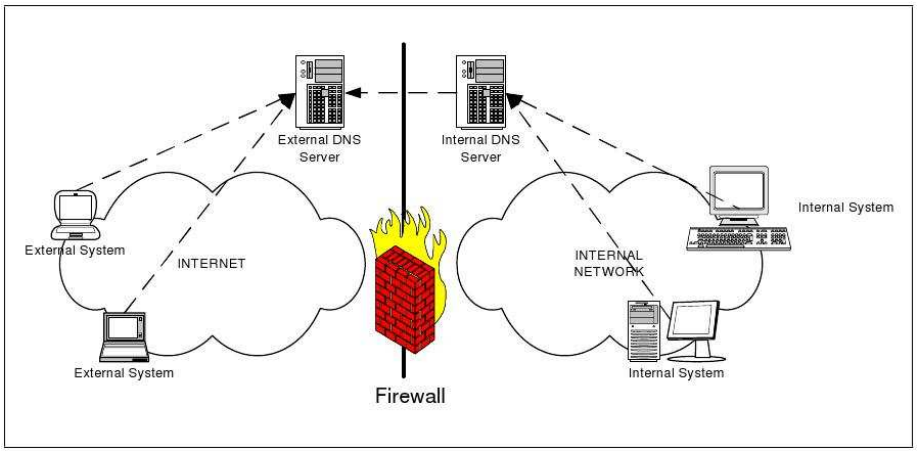

Figura 2.2: rappresentazione dello split-dns.

di Split DNS. Ci sono due server DNS, uno esterno ed uno interno. Il server DNS esterno contiene solo informazioni sugli host pubblicamente accessibili. Il server DNS interno contiene informazioni per tutti i sistemi interni (in questo modo gli utenti interni possono accedere alle macchine della rete interna). Quando un

utente nella rete esterna vuole connettersi ad una macchina del proprio dominio pubblico, il DNS esterno risolverà il nome. Ugualmente, il server DNS interno risolverà il nome per gli utenti interni. In aggiunta, gli utenti interni hanno la possibilità di risolvere domini di sistemi esterni attraverso il forward delle richieste da parte del DNS interno verso quello esterno. Il DNS interno lavora piuttosto come un server proxy, prendendo le richieste interne e instradandole verso l'esterno.
Il DNS esterno risolverà il nome di dominio effettuando una richiesta ad altri server su Internet e restituendo la risposta al server DNS interno, che potrà inoltrare la richiesta all'utente che l'ha effettuata. Con uno Split DNS, quindi, gli utenti interni alla rete possono risolvere sia i nomi di dominio sia interni che esterni, mentre gli utenti esterni (tra cui dei potenziali attaccanti) possono soltanto risolvere nomi di dominio esterni.

Capitolo 3

Scanning

Nel capitolo precedente sono state illustrate tecniche utili, che un attaccante potrebbe utilizzare, per ottenere informazioni su una specifica organizzazione o della sua infrastruttura informatica. Questo capitolo, invece, ha come scopo il mostrare quali tecniche sono a disposizione di un potenzale attaccante per poter apprendere informazioni sui singoli host ed, in generale, sulla sua rete di appartenenza.

3.1 Trovare hosts attivi

Per avere un elenco dei singoli host accessibili, un potenziale attaccante potrebbe *pingare* tutti i possibili indirizzi della rete locale per determinare quali host sono attivi. Il ping è implementato attraverso l'invio di un pacchetto ICMP Echo Request al quale però è associata una opzionale risposta inviata attraverso un pacchetto ICMP Echo Reply Message. Se viene ricevuta una risposta di questo tipo, allora l'attaccante potrà dedurre che l'indirizzo corrisponde ad un host attivo della rete. Se non viene restituita nessuna risposta dopo un certo intervallo di tempo, in questo caso l'attaccante potrà assumere o che l'indirizzo non corrisponde ad un host attivo, oppure che l'host è stato configurato in modo tale da replicare con nessuna risposta a questo tipo di richiesta.
Ci sono casi in cui router di rete bloccano messaggi di tipo ICMP in ingresso, un potenziale attaccante,in questo caso, potrebbe inviare richieste su porte TCP o UDP che corrispondono a servizi che usualmente sono attivi sulle macchine di una particolare rete (la scelta della porta dipende dalla rete interessata e dalle sue caratteristiche). Se la porta è aperta un pacchetto SYN-ACK verrà restituito indicando quindi che all'indirizzo corrisponde effettivamente ad una macchina attiva. Questa tecnica è conosciuta come TCP scan "half-open", tecnica basilare di port scanning, che verrà illustrata nella prossima sezione.

3.2 Port scanning

La forma più semplice di port scanning prende il nome di "half-open" TCP/UDP scan.
Ogni macchina che utilizza un protocollo di comunicazione remoto TCP/IP ha 65.535 porte TCP e 65.534 porte UDP a disposizione. Ad ogni porta può essere

associato un particolare servizio accessibile per vie remote, che resta attivamente in ascolto per eventuali richieste che possono pervenire da utenti remoti. Per un potenziale attaccante, una "porta attiva"[1] potrebbe risultare un possibile punto di accesso alla macchina. A tale motivo, una scansione delle porte attive, attraverso dei tools di scanning, è tra le tecniche più gettonate dagli attaccati. Per comprendere meglio la tecnica di scanning si darà un'occhiata ad uno dei tool, tra i più conosciuti e sofisticati, disponibili per questa operazione.

3.2.1 Nmap

Nmap[2], è probabilmente uno dei migliori port-scanner a disposizione in Internet. Possiede numerosi porting, per quasi tutte le piattaforme (unix, linux, windows, bsd, solaris, macOS, ecc.).
Quando viene eseguita una scansione di un sistema, per individuare porte attive, il sistema di scanning invia pacchetti al sistema interessato cercando di interagire con ogni porta attiva trovata. Il tipo di pacchetti inviati e l'interpretazione delle risposte, dipendono molto dal tipo di scanning che viene effettuato.
In questa sezione saranno illustrati i differenti tipi di scansione delle porte, e saranno mostrati degli esempi utilizzando nmap. Verranno utilizzate solo una piccola parte delle opzioni che nmap offre. Da notare che possono essere eseguite molte operazioni con questo tool che vanno dai semplici ping fino ad arrivare ad operazioni complesse quali, ad esempio, di "fingerprinting" sugli host remoti.

TCP CONNECT-SCAN Tipo di scansione base dove si effettua un handshake 3-way.
`Opzioni di nmap: -sT`

TCP SYN-SCAN Si invia solo il pacchetto iniziale SYN e si attende per una risposta SYN-ACK per capire se la porta è aperta. Se la porta è chiusa, di solito si riceve una risposta RESET oppure nessuna risposta.
`Opzioni di nmap: -sS`

TCP FIN-SCAN Si invia un pacchetto TCP-FIN su una porta. Una risposta di tipo RESET indica che la porta è chiusa, nessuna risposta potrebbe, invece, indicare che la porta è aperta.
`Opzioni di nmap: -sF`

TCP XMAS TREE-SCAN Si invia un pacchetto con i bit di codici FIN, URG e PUSH settati. Se si riceve una risposta RESET allora la porta è chiusa, mentre se non si riceve nessuna risposta la porta è aperta.
`Opzioni di nmap: -sX`

TCP CONNECT-SCAN Tipo di scansione base dove si effettua un handshake 3-way.
`Opzioni di nmap: -sT`

[1] nel testo ci riferiremo a tale termine anche con l'aggettivo *aperta*, intendendo una porta a cui è associato un particolare processo in attesa di richieste da remoto.
[2] http://insecure.org/nmap

NULL-SCAN Si invia un pacchetto con nessun bit di codice settato. Una risposta di tipo RESET indica che la porta è chiusa, nessuna risposta potrebbe, invece, indicare che la porta è aperta.
`Opzioni di nmap: -sN`

TCP ACK-SCAN Si invia un pacchetto con il bit di codice ACK settato. Questo permette di capire se ci sono regole di filtro dei pacchetti sulla connessione stabilita.
`Opzioni di nmap: -sA`

WINDOW-SCAN Simile alla precedente ma focalizzato sulla dimensione della finestra TCP per determinare se una porta è aperta o chiusa su una varietà di sistemi operativi.
`Opzioni di nmap: -sW`

FTP BOUNCE-SCAN Si fa rimbalzare la scansione TCP su un server FTP per oscurare l'origine della scanzione. Questa techica richiede, chiaramente, che ci sia un server FTP disponibile e ciò non è molto semplice.
`Opzioni di nmap: -b`

UDP-SCAN Invia un pacchetto UDP su una porta per determinare se un servizio UDP è in ascolto su di essa.
`Opzioni di nmap: -sU`

PING-SCAN Invia una richiesta ICMP su ogni macchina della rete obiettivo permettendo di determinare gli host attivi.
`Opzioni di nmap: -sP`

La descrizione precedente contiene le più comuni tecniche di portscanning che possono essere effettuare con nmap. Seguono in dettaglio due tra le più facili tecniche descritte.

3.2.2 Connessioni TCP

Per comprendere le basi dello scanning su connessione TCP, e di conseguenza tutte le altre tipologie di scansione, è necessario conoscere come il protocollo TCP stabilisce una connessione tra due macchine. In questo caso vogliamo stabilire una connessione tra la macchina Cesare e la macchina Cleopatra. Il 3-way handshake permette di stabilire una sequenza numerica tra i due sistemi. Questa sequenza è usata affinché il protocollo TCP possa trasportare pacchetti nell'ordine corretto.
Per realizzare il 3-way handshake, Cesare invia un pacchetto con l'inizio di una sequenza numerica (ISN_A) e il bit SYN TCP settato su una specifica porta della macchina con cui intende comunicare, Cleopatra (es. porta 80 per il webserver). Se un servizio è in ascolto su questa porta, Cleopatra risponderà con un pacchetto che ha settati sia i bit SYN che ACK, utilizzati per riconoscere ISN_A, e una risposta alla sequenza iniziale (ISN_B). Dopo aver ricevuto il pacchetto SYN-ACK, Cesare completa il 3-way handshake inviando un pacchetto ACK che conferma la corretta ricezione del numero di sequenza ISN_B. A questo punto, il 3-way handshake è completo. Tutti i pacchetti scambiati tra Cesare e Cleopatra che saranno inviati sulla connessione appena stabilita, avranno un numero di serie incrementale a partira da ISN_B.

Usando questa sequenza numerica, lo stack TCP di ogni sistema ritrasmetterà i pacchetti persi e potrà riordinare i pacchetti in un eventuale arrivo fuori sequenza.

TCP-CONNECT SCAN Il TCP-Connect scan cerca di effettuare un 3-way handshake su ogni porta di un sistema destinazione. Per effettuare un connect scan, l'attaccante invia pacchetti di tipo SYN e attende pacchetti di tipo SYN-ACK dalla porta specificata. Se la porta è aperta, la macchina iniziale completerà il 3-way handshake con un ACK e chiuderà la connessione con un pacchetto FIN.
Visto che questo è il tipo di scansione più "gentile", un rilevamento di una scansione di questo tipo è facile da realizzare. Una scansione sulla macchina interessata può venire memorizzata nei log di sistema, se su di esso è attivo un sistema di logging. Ad esempio, se l'attaccante sta effettuando una scansione di un web server, nei log di quest'ultimo saranno indicate le numerose connessioni aperte dall'IP dell'attaccante, su tutte le porte del sistema. Essendo questa caratteristica non proprio a favore degli attaccanti, di solito vengono usate tecniche più furtive.

TCP-SYN SCAN Mentra una scansione TCP effettua il 3-way handshake completamente, la scansione SYN si ferma a due delle tre parti dell'handshake. A volte viene definita scansione "half-open". La scansione SYN viene effettuata dalla macchina attaccante inviando un pacchetto SYN su ogni porta. Se una porta è aperta la macchina target invierà una risposta SYN-ACK. La macchina attaccante invierà, a questo punto, un pacchetto RESET, chiudendo la connessione prima che essa venga completata. Se la porta è chiusa, il sistema attaccante potrebbe non ricevere risposte, oppure un pacchetto RESET oppure un pacchetto "ICMP Port Unreachable", in base al tipo di macchina e al tipo di architettura di rete.
Seguendo il precedente esempio del log sul webserver, una scansione di tipo SYN non può essere loggata perché la connessione non viene mai completata. É importante notare che i router e molti firewall che hanno un sistema di logging abilitato, non potranno memorizzare il pacchetto SYN.
Un altro vantaggio della scansione SYN rispetto a quella Connect è la velocità. La scansione Connect necessita di inviare un numero maggiore di pacchetti per attendere di completare il 3-way handshake. Un problema che può nascere con scansione SYN è che il sistema target potrebbe essere inondato di pacchetti SYN causando un Denial of Service.

TCP FIN/SCAN/XMAS/TREE-SCAN/NULL Connect Scan segue le specifiche TCP alla perfezione; lo scan TCP SYN lo segue, invece, per due terzi. Il pacchetto FIN viola il protocollo inviando pacchetti non attesi all'inizio della connessione.
Un pacchetto FIN indica al sistema obiettivo che la connesssione potrebbe essere caduta. Tuttavia, durante una scansione FIN, non viene mai stabilita una connessione. Il sistema interessato riceve solo alcuni pacchetti che specificano la chiusura di una connessione che non è stata mai stabilita. In accordo alle specifiche TCP, se su una porta, dove non è stabilita nessuna connessione, si riceve un pacchetto FIN, il sistema interessato potrebbe rispondere con un RESET. Quindi se non viene restituito nulla, c'è una

buona probabilità che la porta sia aperta ed in ascolto. In questo modo una scansione FIN può essere usata per aiutare un attaccante a determinare quali porte sono aperte e quali chiuse.
Allo stesso modo, la scansione XMAS-Tree invia pacchetti con i bit FIN, URG e PUSH settati. Il nome insolito di questa scansione deriva dall'osservazione che questi bit settati nell'header TCP ricordano le luci di un albero di natale.
Un Null scan consiste nell'inviare pacchetti TCP con nessun bit code settato. Ancora, *Xmas scan* e *Null scan* prevedono lo stesso comportamento del FIN scan: una porta chiusa invia un pacchetto RESET mentre un porta in attesa non invia nessuna risposta.
Le tecniche di scansione su un sistema remoto, usando Xmas Tree scan o Null scan, non funzionano con sistemi basati su Microsoft Windows, in quanto non seguono le specifiche RFC quando si invia un pacchetto RESET. Per altre piattaforme invece questo tipo di scansione è molto utile.

3.2.3 Fingerprinting

In aggiunta alla scansione delle porte di uno specifico sistema, un attaccante può voler determinare quale sistema operativo è in esecuzione su di una macchina specifica. Informazione importante in quanto un attaccante potrebbe cercare vulnerabilità per quel particolare tipo di sistema. Un attaccante più sofisticato potrebbe attrezzare un laboratorio simile alla rete interessata per cercare di scoprire vulnerabilità nell'infrastruttura.
Con nmap è possibile determinare il tipo di sistema operativo in esecuzione usando una tecnica chiamata *TCP stack fingerprinting*. Le RFC definiscono delle specifiche TCP riguardanti le possibili risposte da parte di un sistema durante l'inizializzazione di una connessione (3-way handshake). Da notare che le RFC non definiscono come il sistema debba rispondere alle errate combinazioni illegali di codici TCP. A causa di questa mancanza di standard relative a tali combinazioni, diverse implementazioni dello stack TCP rispondono in maniera diversa. Ad esempio, un'implementazione Windows risponderà diversamente da una Solaris. Nmap usa questa inconsistenza per determinare quale sia il sistema operativo in esecuzione sulla macchina interessata. Per fare ciò, nmpa invia una serie di pacchetti su varie porte:

- pacchetti SYN su porte aperte;
- pacchetti NULL su porte aperte;
- pacchetti SYN|FIN|URG|PSH sulle porte aperte;
- pacchetti ACK sulle porte aperte;
- pacchetti SYN sulle porte chiuse;
- pacchetti ACK sulle porte chiuse;
- pacchetti FIN|PSH|URG sulle porte chiuse;
- pacchetti UDP sulle porte chiuse.

Figura 3.1: esempio di finger printing.

In aggiunta, nmap misura la prevedibilità della sequenza iniziale inviata da una porta aperta nella risposta SYN-ACK (del 3-way handshake). Inviando una serie di pacchetti SYN su una porta aperta e analizzando i cambiamenti dei pacchetti SYN-ACK nel tempo, nmap determina se un pattern della sequenza è prevedibile e può essere determinato. Questa tecnica è utile per determinare il sistema operativo. Inoltre, le sequenze numeriche prevedibili possono aiutare l'attaccante ad eseguire un IP spoofing (come vedremo successivamente). Nmap contiene un database di sistemi operativi per oltre 500 piattaforme. Un esempio di fingerprinting andato a buon fine è rappresentato nella figura 3.1. C'è da notare che nmap non è l'unico tool disponibile per fare operazioni di questo tipo, esistono anche tools come `xprobe` e `Queso`. Tutti i tool menzionati in questo capitolo sono di tipo "fingerprinting attivo", ciò significa che iniziano la comunicazione con il sistema obiettivo.
Ci sono anche tool che effettuano "fingerprinting passivo" (ad esempio siamo su un webserver e vogliamo informazioni sui sistemi operativi dei nostri visitatori) come ad esempio `POf` o `siphon`. Il concetto alla base del "fingerprinting passivo" è quello non di inviare pacchetti verso il sistema target ma analizzare il traffico di rete tra diversi sistemi. Per effettuare questo tipo di analisi bisogna però avere una posizione centrale nella rete e trovarsi su di una porta che permetta cattura dei pacchetti.
L'analisi dei pacchetti viene fatta generalmente su alcune caratteristiche tipiche delle sessioni TCP/IP che possono variare da un sistema operativo ad un altro.

- TTL
- Dimensione finestra
- Bit DF

Confrontando questi attributi con database di valori noti si può determinare il sistema operativo del sistema. Questa tecnica essendo molto semplice porta con se dei limiti evidenti quali ad esempio: molte applicazioni generano pacchetti con attributi settati indipendentemente dal sistema operativo in uso; si deve essere in una posizione che permetta la cattura dei pacchetti; questi attributi sono valori settabili su qualsiasi sistema operativo e un amministratore può modificarli a suo piacimento.

3.2.4 Difese contro port scanning e finger printing

La più importante difesa contro il port scanning è di effettuare personalmente una scansione personale del proprio sistema, prima che lo faccia un attaccante. Verificare che tutte le porte sono chiuse verso l'esterno, tranne quelle necessarie, è un'operazione fondamentale.
Ci sono, inoltre, alcuni trucchi utili (come delle patch per il kernel) per ridurre le capacità di nmap (e altri software) di effettuare fingerprinting ma, ancora una volta, la miglior difesa è mantenere al massimo il proprio sistema irraggiungibile in una rete interna e monitorare gli host esposti a potenziali attacchi.
Per ulteriori informazioni riguardo alla difesa dal fingerprinting su sistemi Linux e BSD usando patch per il kernel e moduli per il kernel, e possibile leggere "A pratical approach for defeating nmap OS-Fingerprinting". Se un amministratore di sistema ha fatto bene il suo lavoro, nmap non riuscirà a determinare il tipo di sistema operativo.
Ultimo, ma non per importanza, un IDS (Intrusion Detection System) come ad esempio `Snort` può aiutare l'amministratore a trovare tracce di possibili finderprinting. Si sappia, però, che esistono anche numerose tecniche per evadere gli IDS, come l'inserire un delay tra i pacchetti inviati sul sistema scansionato. Inserendo qualche minuto tra ogni pacchetti, molti IDS li ignorano e non considerano quel traffico interessante da analizzare.

3.3 Ricostruire l'architettura delle reti

Una volta che l'attaccante ha determinato quali host sono attivi, vorrà conoscere informazioni sulla topologia di rete. Userà una tecnica conosciuta come tracerouting per determinare i vari router e gateway che mantengono l'infrastruttura di rete. Il tracerouting si basa sul TTL (time-to-live) dei pacchetti IP. Il campo TTL indica quanti hop un pacchetto deve percorrere prima di essere rilasciato da un router. Sfortunatamente, TTL non si basa sul tempo ma sugli hop. Focalizzando l'attenzione sul contare le macchine il time-to-live si sarebbe dovuto chiamare hops-to-live.
Come lavora il campo TTL? Quando un router riceve un pacchetto IP in ingresso, decrementa il valore del TTL di uno. Quindi, prima di inviare il pacchetto alla propria destinazione, il router controlla il campo TTL per vedere se vale zero. Se tale è il suo valore, il router invia indietro un messaggio "ICMP Time Exceeded" all'origine del pacchetto in ingresso.
Il campo TTL fu creato per dare ai pacchetti un ciclo di vita finito e fare in modo che non ci fosse una circolazione infinita di pacchetti all'interno della rete Internet.
Gli attaccanti (così come gli utenti normali) utilizzano questa caratteristiche del campo TTL per determinare il percorso di un pacchetto su una rete. Inviando una serie di valori TTL, si possono tracciare tutti i router da una sorgente ad una destinazione. Come si può vedere nella figura 3.2, si inizia inviando un pacchetto da una macchina sorgente con un TTL di uno. Il primo router riceve il pacchetto, decrementa il TTL a zero, e invia indietro un messaggio "ICMP Time Exceeded". L'indirizzo sorgente di questo pacchetto sarà l'indirizzo del primo router nel path per raggiungere la destinazione. Se si vuole conoscere l'indirizzo del secondo router interposto tra sorgente e destinazione, un pacchetto

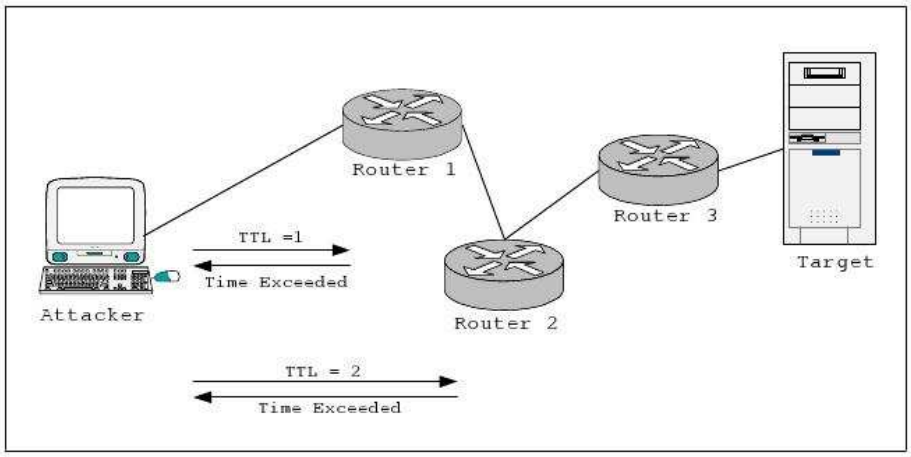

Figura 3.2: scenario di un tentativo di ricostruzione di rete attraverso il conteggio dei ttl.

```
raffaele@delluccio ~ $ traceroute www.unisa.it
traceroute to www.unisa.it (193.205.160.14), 30 hops max, 40 byte packets
 1  www.routerlogin.com (192.168.0.1)  3.866 ms  4.469 ms  7.979 ms
 2  93.144.128.1 (93.144.128.1)  60.191 ms  62.033 ms  64.680 ms
 3  * * *
 4  93.179.134.61 (93.179.134.61)  74.400 ms  76.370 ms  79.738 ms
 5  83.224.40.113 (83.224.40.113)  82.021 ms  83.952 ms  86.231 ms
 6  garr.mix-it.net (217.29.66.39)  88.753 ms  76.124 ms  78.190 ms
 7  193.206.134.230 (193.206.134.230)  94.141 ms  67.482 ms  70.072 ms
 8  rt-na1-rt-rm2.rm2.garr.net (193.206.134.245)  75.088 ms  78.216 ms  81.290 ms
 9  193.206.141.10 (193.206.141.10)  83.639 ms  90.045 ms  91.592 ms
```

Figura 3.3: Esempio di esecuzione di traceroute sul dominio www.unisa.it

con TTL settato a due potrà essere usato allo stesso modo. Per automatizzare questo processo, può essere usato il programma `traceroute` presente in tutte le distribuzioni linux e nei sistemi operativi windows. La figura 3.3 mostra un traceroute del dominio www.unisa.it.

Un attaccante può usare traceroute per determinare il pache di ogni host scoperto. Con queste informazioni è possibile realizzare un grafo della rete, operazione che può essere automatizzata con tools come *Cheops*, disponibile per Linux e Unix.

Cheops si può vedere in esecuzione nella figura 3.4. Questo software include una serie di tool di network-mapping e raggruppa tutte le informazioni ottenute con un'intuitiva e semplice interfaccia che mostra, allo stesso tempo, la struttura della rete, i sistemi operativi dei nodi, ecc.

3.3.1 Difesa contro il network mapping

Come si può prevenire un attacco di network mapping con tool come ping, traceroute, cheops e altri? E' necessario filtrare alla base i messaggi che questi programmi inviano, sfruttando le regole dei firewall o le caratteristiche di filtraggio dei router. Nel proprio gateway si potrebbero bloccare tutti i messaggi ICMP in ingresso eccetto per gli host che si vuole vengano pingati. L'utenza

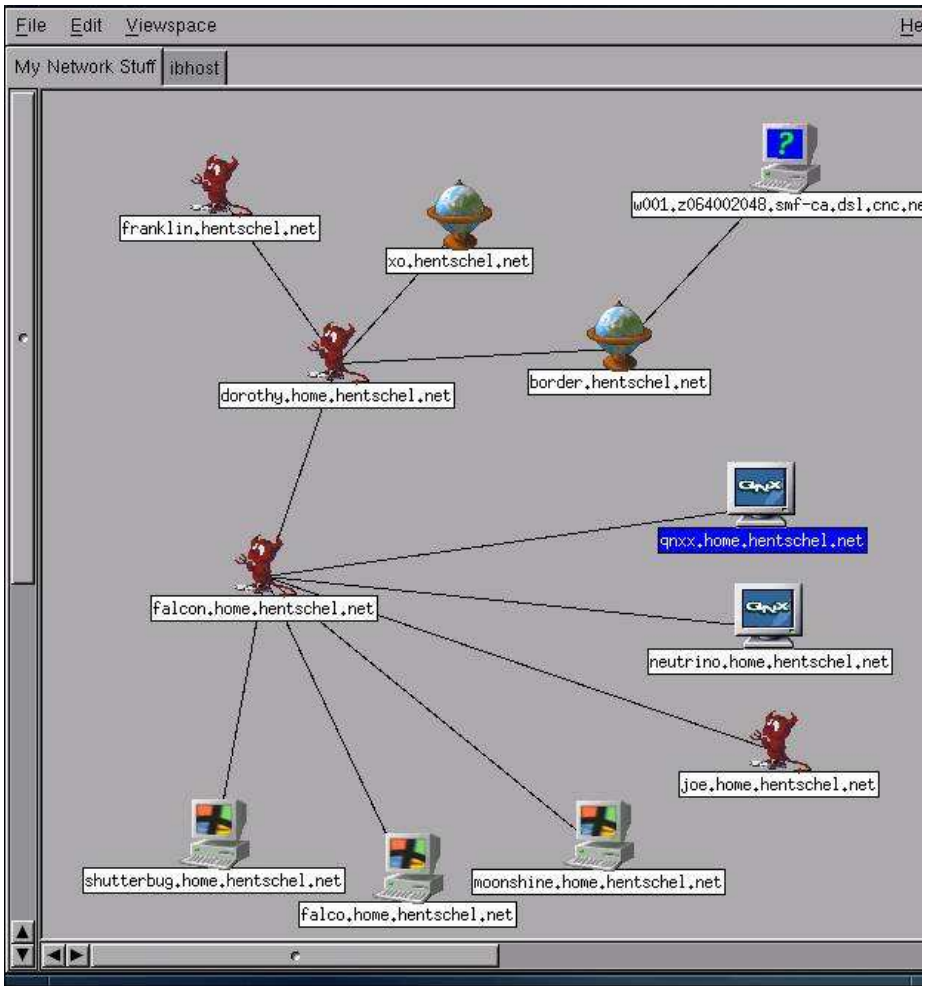

Figura 3.4: Esempio di esecuzione di cheops

dovrebbe poter pingare il proprio webserver? Forse. É necessario che il pubblico possa pingare il proprio database DMZ? Forse no. É necessario che si possa pingare i propri host interni? Chiaramente no. Domande necessarie per poter adottare una buona politica preventiva. In aggiunta, si possono filtrare i messaggi "ICMP Time Exceeded" in uscita dalla propria rete.

Capitolo 4

Enumerazione

La fase che ora verrà illustrata è definita "enumeration" e si distingue dalle precedenti per il fatto che il livello di intrusione è più elevato. Da questo momento in poi ci saranno delle connessioni vere e proprie al sistema per eseguire query atte ad ottenere informazioni. Riconoscere versione dei software installati, recuperare gli account di una macchina, trovare risorse condivise, sono alcuni tra gli obiettivi di questa fase.
Tutti i passi illustrati da ora in avanti si distinguono in base al sistema operativo, informazioni che possono essere ottenute dalle fasi precedenti illustrate.

4.1 Banner Grabbing

La tecnica del banner grabbing è una delle più semplici e consiste nel connettersi ad un'applicazione remota e osservarne l'output. Dai dati restituiti, spesso si può ricavare la versione del software usato e altre informazioni utili. Il metodo più semplice di eseguire banner grabbing è quello di effettuare connessioni telnet o netcat su varie porte del sistema target e osservarne le risposte. Anche le risposte negative (connessioni negate) contengono informazioni utili.

4.1.1 Difesa contro il Banner Grabbing

La prima difesa contro il banner grabbing è, come detto già in precedenza, quella di disattivare i servizi non strettamente necessari. Per i servizi che invece sono essenziali è importante modificare, quando possibile, le informazioni che questi restituiscono in output. Modificare o eliminare la versione e il nome del software usato può prevenire danni futuri.

4.2 Enumerazione Telnet

Telnet è stato uno dei servizi più usati in passato. Il problema principale delle connessioni telnet è il fatto che i dati viaggiano in chiaro. Chiunque abbia la possibilità di sniffare traffico di una rete può accedere anche a username e password usate per la connessione. Col tempo l'uso di telnet sta diminuendo lasciando spazio all'uso di SSH che fornisce la possibilità di accedere da remoto ad una macchina utilizzando una connessione cifrata.

Con questa tecnica un attaccante potrebbe cercare di instaurare delle connessioni via telnet ad una macchina e utilizzare le informazioni restituite dal sistema per individuare il tipo di sistema operativo e altri tipi di informazioni (banner grabbing via telnet), possibilità che si è ridotta notevolmente grazie all'evoluzione dei software per router e firewall che non prevedono la restituzione di nessuna informazione in output in caso di tentativi di connessioni anomale.
Una procedura potenzialmente dannosa risulta essere quella che sfrutta telnet per la ricerca di username validi, effettuando dei tentativi di login. Conoscendo un servizio attivo su una determinata macchina, un attaccante potrà effettuare numerosi tentativi di login ed osservando i messaggi del sistema potrebbe individuare quali nomi utenti sono validi. Ad esempio un messaggio del tipo "username non valido" fa capire che l'account utilizzato per il tentativo di login non esiste, mentre un messaggio del tipo "password non valida per l'utente inserito" fa pensare che l'username utilizzato sia esistente. In questo modo l'attaccante ha già un'informazione in più (l'username) e si potrà concentrare sulla ricerca della password.
Questa tecnica è valida per la maggior parte dei servizi diffusi su Internet (enumerazione FTP, enumerazione SMTP, enumerazione HTTP, ecc.) e la sua semplicità la rende una delle più usate in assoluto.

4.2.1 Difesa dall'Enumerazione Telnet

Le contromisure da prendere per questi tipi di attacchi sono simili a quelle già illustrate più volte in precedenza. Innanzitutto è essenziale sostituire telnet con SSH sul proprio sistema. Inoltre si dovrebbero modificare i messaggi restituiti per cercare di fornire meno informazioni possibili ad un potenziale attaccante.

4.3 Enumerazione DNS

Una delle tecniche di enumerazione più vecchia è quella sui sistemi DNS atta a effettuare un trasferimento di zona. In base al tipo di server DNS utilizzato il trasferimento di zona può essere una operazione semplice eseguibile con `nslookup`, `ls -d <dominio>` oppure con `dig`. Si otterranno informazioni come la mappa di hostname-indirizzi IP e tutti i dati collegati ad un hostname (come il campo HINFO).
Anche per questa tecnica esistono dei tool di automazione. Uno dei più famosi è `dnsenum`[1] che raccoglie informazioni utilizzando varie tecniche incrociate: brute forcing, reverse lookup, richieste whois, ecc.

4.3.1 Difesa dall'Enumerazione DNS

Ancora una volta, se il servizio non è necessario, è preferibile disabilitarlo. Se invece si necessita di un servizio DNS una contromisura da prendere è quella di separare il sistema DNS in due server distinti: uno esterno ed uno interno, in modo da non esporre quello interno a potenziali attaccanti. Un'altra modifica da fare al proprio server DNS è quella di bloccare il trasferimento di zona o permetterlo solo a determinati host autorizzati.

[1] http://code.google.com/p/dnsenum

4.4 Altre tecniche di enumerazione

Come già accennato in precedenza l'enumerazione è una tecnica generica che si può applicare a molti servizi Internet. Ne abbiamo illustrato solo alcuni, ma esistono varianti che permettono di ottenere informazioni da HTTP, FTP, SMTP, NetBIOS, Samba, ecc. Quando si va nello specifico di diversi sistemi operativi, ci sono tecniche ben più evolute e complesse di quelle illustrate che permettono di: ottenere privilegi di accesso su macchine target, accedere a risorse condivise in lettura e scrittura, eseguire query SQL da remoto, ecc.

Capitolo 5

Breaking in Windows

Seguendo il percorso tracciato dai capitoli precedenti, abbiamo visto quali strumenti sono a disposizione dell'attaccante per raccogliere delle informazioni generiche o di tipo strutturale sull'architettura di una rete informatica appartenente ad una particolare organizzazione. Lo scopo di questo capitolo è quello di illustrare quali tecniche esistono a disposizione dell'attaccante che gli consentono di utilizzare le informazioni raccolte durante le varie fasi, per poter effettare delle operazioni di break in, ossia operazioni di intrusione fisica all'interno di alcune o tutte le macchine che compongono il sistema informativo aziendale. Nello specifico verranno trattate tecniche di password cracking, sniffing, spoofing ed infine di session hijacking.

5.1 Attacchi non autenticati

5.1.1 Password guessing

Al giorno d'oggi il mezzo più utilizzato al mondo, per garantire la sicurezza nell'ambito informatico, è l'utilizzo delle password. In molte organizzazioni, le password servono a proteggere molti dei più inimmaginabili segreti aziendali, includendo informazioni sanitarie, strategie di mercato confidenziali, dati finanziari sensibili, e così via. Sfortunatamente, a causa del loro ruolo così centrale nella sicurezza informatica, password "facili" rappresentano talvolta una debolezza per la sicurezza informatica. Per esempio, ottenendo una singola password, un attaccante potrebbe guadagnare l'accesso ad informazioni sensibili oppure causare il crash di sistemi.
Oltre alla sensibilità dei dati protetti dalle password, c'è da notare che ogni utente all'interno di un sistema informatico possiede almeno una password, molti dei quali ne hanno in media una dozzina. Gli utenti sono forzati a ricordare e gestire password per il login nel sistema, accesso alla rete e ai servizi offerti dal web e così via. La politica adottata in molti sistemi informatici lascia agli utenti la scelta delle password, molte delle quali sono scelte in maniera superficiale, senza badare alla sicurezza dei dati o privilegi protetti. Vengono spesso scelte password facili da ricordare, e che quindi possono facilmente essere scoperte. La scoperta anche di una sola password "debole", può dare ad un attaccante un punto d'appoggio al sistema. In aggiunta, molti utenti utilizzano una stessa

password per più sistemi a cui hanno accesso, permettendo così ad un attaccante di guadagnare velocemente l'accesso a più sistemi ottenendo soltanto una singola password. Una volta ottenuta una password, un attaccante potrebbe continuare nei tentativi di scoperta nuove password oppure sfruttare vulnerabilità del sistema per guadagnare dei nuovi privilegi.
Nelle sezioni successive verranno mostrate delle tecniche utili a scoprire password di utenti presenti in un sistema.

5.1.2 Guessing password di default

Molte applicazioni e sistemi operativi includono una generazione di password di default stabilite dai relativi produttori. Spesso l'eccessivo carico di lavoro, la disinformazione o la pigrizia dell'aministratore di sistema, causano la mancata sostituzione delle password di default del sistema. Un attaccante può velocemente e facilmente scoprire tali password di default e cercare di guadagnare l'accesso al sistema. Alcune aziende lasciano all'interno dei sistemi delle backdoor-password, utilizzate per effettuare delle operazioni di manutenzione o riparazione di guasti in maniera efficiente. Questa strategia lascia, talvolta, una strada aperta per gli attaccanti che possono, una volta scoperte tali backdoors, introdursi all'interno del sistema.
password di default, ad esempio, per tutti i differenti dispositivi di rete sono collezionati e pubblicati su vari siti Internet[1].

5.1.3 Guessing automatizzato

Se con le password di default non si ha successo, in quanto l'amministratore è stato prudente abbastanza da cambiare tutte le password di default, allora in questo caso è possibile generare delle password e testarle all'interno del sistema finché non viene trovata quella giusta. Esistono alcuni modi per generare una lista di possibili password e qui di seguito ne riportiamo alcuni.

Dictionary Attacks: è il più semplice tipo di attacco che possa essere fatto. Viene presa una lista di parole da un dizionario e ognuna di essa viene testata all'interno del sistema, finché quella corretta non viene trovata. Ci sono numerosi dizionari disponibili in rete che contengono possibili password in tutti i differenti linguaggi incluso l'inglese, il tedesco, l'italiano, il russo, il giapponese, il francese e sono perfino presenti dizionari per il *sindarin*[2]. Ovviamente se la password non è presente nel dizionario, l'attacco sicuramente fallirà. Fortunatamente per gli attaccanti, quasi sempre l'attacco ha successo. Inoltre, a casua del limitato ammontare di combinazioni di password che sono testate (comparate con gli attacchi basati su brute-force), rende questo attacco di password cracking più veloce rispetto agli altri possibili attacchi.

Brute-Force Attack: oltre agli attacchi a dizionario, molti strumenti per il password-craking supportano il brute-force craking. Per questo tipo di attacco, sono previsti tentativi che coprono tutte le possibili combinazioni di caratteri per determinare quale sia la password. I tentativi possono

[1] http://www.phenoelit.de/dpl/dpl.html
[2] linguaggio utilizzato dagli elfi.

cominciare iniziando a coprire tutte le parole che contengono caratteri alfanumerici (a-z e 0-9) e progressivamente includendo i caratteri speciali (ad esempio: !, @, #, $). Questo tipo di attacco richiede una enorme quantità di tempo, tempo che può andare da settimane a secoli. Daltronde, se la password che si intende scoprire risulta essere piccola abbastanza, allora un attacco di questo tipo più essere ragionevole.

Hybrid Password Cracking: questo tipo di attacco risulta essere un buon compromesso tra il veloce ma limitato attacco basato sui dizionari e il lento ma efficiente attacco di forza bruta. In un attacco ibrido, si parte utilizzando parole contenute in un dizionario. Dopo averle tutte testate, vengono create delle nuove parole aggiungendo all'inizio o alla fine nuovi caratteri alle parole presenti nel dizionario. Questo tipo di attacco risulta essere molto efficiente rispetto all'attacco brute-force.

5.1.4 Login scripting

Una volta generata una lista di possibili password si vorrebbe avere la possibilità di testarle su un particolare account. Esistono due possibilità per procedere. Se si ha accesso alla rappresentazione cifrata della password, si può tentare di risalire alla password lavorando sulla nostra stessa macchina. Nella maggior parte dei casi si ha bisogno di utilizzare una tecnica chiamata `login scripting` per scoprire la password utilizzata su una macchina remota.
`Login scripting` è inteso semplicemente come la scrittura di uno script che iterativamente cerca di effettuare un login su una macchina target attraverso la rete. L'attaccante configurerà lo script con un nome utente comune oppure con uno conosciuto. Le password vengono prese una ad una dalla lista creata con i metodi illustrati precedentemente. L'attaccante fa interagire lo script con la macchina target, la quale può avere un'interfaccia prompt, una web-based oppure un'altra di qualsiasi altro tipo per la richiesta delle credenziali di accesso. A questo punto, l'attaccante trasmette userid e password (se sono le sole credenziali d'accesso) e lo script automaticamente rileva se il tentativo ha avuto successo oppure è fallito. In caso negativo automaticamente vieni effettuato un nuovo tentativo.
Molti attaccanti creano da loro stessi gli script per effettuare tentativi di login da remoto, altri usano alcuni tools pronti per l'uso. Ne citiamo alcuni:

- **authforce** http://freshmeat.net/projects/authforce/
- **brute_ssl**
  http://ftp2.de.freebsd.org/pub/misc/www.rootshell.com/hacking/
- **xavior** http://downloads.securityfocus.com/tools/XaviorBeta7.exe

Tools di questo genere sono molto popolari tra hackers e crakers di tutti i tipi, è possibile trovare dozzine di altri programmi per il password cracking semplicemente navigando il web o su siti di sicurezza specializzati come Packetstorm Security[3].
La scoperta di password attraverso il login scripting può essere molto tedioso, infatti ciascun tentativo di login usualmente prende tempo dai 5 ai 10 secondi.

[3] http://packetstormsecurity.org/

Si provi ad immaginare di testare 40.000 parole contenute in media in un dizionario, il processo potrebbe richiedere giorni, e cercare di scoprire una password costruite attraverso combinazioni random di caratteri, potrebbe richiedere mesi prima che la password sia scoperta. Da considerare che c'è la possibilità che tutti i tentativi di login falliti possano essere registrati in un file di log dall'amministratore di sistema, se il sistema ne possiede uno. Cosiderare anche che alcuni sistemi bloccano un account se per molte volte viene inserita una password sbagliata.

5.1.5 Offline password cracking

Tentativi di accesso utilizzando password di default in genere non hanno successo. Se si considerano i tentativi che possono essere effettuati attraverso le tecniche di login scripting, c'è da dire che richiedono molto tempo e c'è, nel caso peggiore, il rischio di essere individuadi attraverso file di log. Un più sofisticato approccio per determinare password, che permette di evitare i rischi considerati precedentemente, è noto come (offline) password cracking. Per analizzare come la tecnica del password cracking funziona occore dare un'occhiata a come le password sono conservate sulla maggior parte dei sistemi.
Quando viene effettuato il login su una macchina, sia un sistema UNIX, come un NT box, un server Novell, un router Cisco, o un altro tipo di macchina, bisogna fornire una userid e una password per l'autenticazione. Il sistema effettua un check sulla validità delle informazioni inserite per consentire l'accesso al sistema oppure negarlo. Il sistema potrebbe utilizzare un file locale dove sono presenti le password di tutti gli utenti. In questo caso il sistema deve solo controllare se la password inserita è presente nell'elenco delle password, relativa ovviamente all'utente che tenta di effettuare il login. Sfortunatamente, un file che contiene tutte le password degli utenti del sistema potrebbe costituire una forte debolezza nel sistema. Un attaccante, infatti, guadagnando l'accesso a tale file, sarà capace di effettuare un login con qualsiasi nome utente.
I progettisti di sistemi, considerata la necessita della presenza di un file contenente le password di tutti gli utenti, ma che costituiva una grossa falla di sicurezza, decisero di ovviare a questo problema utilizzando tecniche crittografiche per mascherare ciascuna password presente nel file. Quindi, il file delle password è composto dalle userid di ciascun utente e le relative rappresentazioni crittografate delle password di ciascuno di essi. Per questo scopo, esistono una vasta gamma di algoritmi crittografici in uso, alcuni dei quali sono puramente algoritmi di cifratura, come ad esempio il `Data Encryption Standard` (DES), il quale richiede l'uso di una chiave segreta. Altri, per il mascheramento, utilizzano tecniche di hash, quale ad esempio il `Message Digest 5` (MD5), una one-way hash function che può lavorare con o senza l'utilizzo di una chiave segreta. In entrambi i casi, le password sono mascherate utilizzando algoritmi crittografici che non consentono all'attaccante, attraverso una semplice vista del file, di ottenere alcuna informazione.
Quando l'utente si presta ad effettuare l'accesso al sistema, fornisce la propria password, alla quale il sistema applica la trasformazione crittografica prevista. Una volta applicata la procedura, viene confrontato il risultato del processo con il valore presente nel file delle password. Se viene trovato riscontro positivo, viene consentito l'accesso, altrimente l'accesso viene negato. Nei sistemi unix, ad esempio, tali informazioni sono contenute nel file `/etc/shadow`. Per

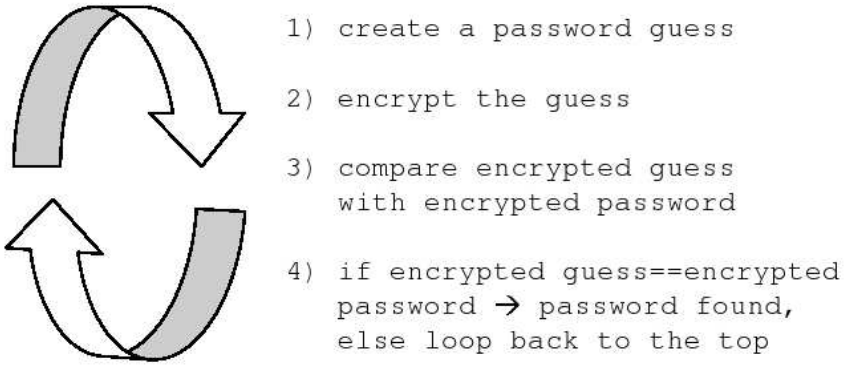

Figura 5.1: Ciclo classico più usato nei sistemi di password cracking

poter effettuare un (offline) password craking, l'attaccante dovrebbe ottenere la cifratura o il valore hash della password che intende ottenere, per poter così permenttere ad un tool già esistente o implementato personalmente di lavorare sul testo mascherato. A seconda del sistema vengono adottati algoritmi di cifratura o funzioni hash differenti, di conseguenza i tools per il craking variano a seconda del sistema target. In generale il comportamento dei tools è lo stesso, cambia solo il tipo di algoritmo utilizzato. Il procedimento può essere generalizzato nella Figura5.1. La quantità di tempo, necessaria a questi tools di risalire alla password originaria, dipende notevolmente dalla qualità[4], lunghezza della password scelta dall'utente e potenza di calcolo a disposizione dell'attaccante.

5.1.6 Contromisure

La migliore difesa contro il password cracking è quella di prestare attenzione alla scelta delle password. Per dare un'idea di password debole verrà mostrato un elenco di alcune caratteristiche di cui una buona password non dovrebbe godere.

- La password contiene meno di otto caratteri.
- La password è una parola che può essere trovata in un dizionario (di lingua Italiana per esempio).
- La password è una parola comunemente usata (nomi di familiari, amici, e così via).
- Termini o nomi informatici, comandi, siti, compagnie, hardware, software.
- Pattern di nomi come **qwerty, 112233, asdfg**.
- Basata su informazioni personali.

Una buona politica di scelta delle password potrebbe invece basarsi su alcuni dei principi che verranno ora elencati.

[4] dove per qualità si intende la combinazione non prevedibile di caratteri.

- Composta da caratteri minuscoli e maiuscoli (a-z, A-Z).
- Potrebbe contenere numeri, caratteri di punteggiatura o anche caratteri spericali.
- Lunga almeno 8 caratteri alfanumerici.
- Non scritta in nessun posto oppure salvata on-line.

Un buon modo per creare una password, facile da ricordare ma allo stesso tempo difficile da scoprire, potrebbe essere quello di prendere una frase nota ed estrarne dall'interno solo alcuni caratteri. Ad esempio la frase potrebbe essere: `Quanto è buona la mamma`; e la password potrebbe essere: `q1E2b!L>m`, oppure `q<E3b.L>m`, oppure variazioni di questo tipo.
Una buona politica per la gestione delle password potrebbe essere anche quella di forzare l'utente a cambiare regolarmente le password utilizzate o applicare delle semplici variazioni. Se si è quindi amministratori di una rete o di un sistema, come si evince dal contesto, una buona prevenzione per la sicurezza del sistema che si cura, è quella di sensibilizzare gli utenti riguardo all'aspetto della sicurezza, facendo capire l'importanza della scelta di una buona password e incitarli ad adottare password differenti per i differenti servizi di cui usufruiscono. Stabilita la bontà delle password esaminiamo ora delle contromisure da adottare contro il password cracking e il login scripting. Per il password cracking una buona contromisura è quella di custodire e proteggere con ogni genere di mezzo il file contente le password mascherate degli utenti, impedendo che tali informazioni possano uscire dalla macchina, ulteriormente occore tenere in cosiderazione anche tutti i backup del sistema che possono contenere i dati contenuti nel file. Per il login scripting, una contromisura potrebbe essere quella di attivare i file di log e bloccare accounts per cui vengono fatti numerosi tentativi di accesso.

5.1.7 Exploit remoti non autenticati

Questa categoria di exploit è volta a sfruttare bug presenti nei software del sistema operativo Windows oppure eventuali configurazioni di sistema errate. Questo tipo di attacchi spaziano dallo sfruttare servizi di Windows fino ad applicazioni utenti tipo Microsoft Office.
Data il numero elevato e la larga diffusione di bug di Windows, esistono numerose applicazioni user-friendly che con estrema facilità permettono di sfruttare le più note vulnerabilità di Windows. Uno dei software più conosciuti in questo campo è Metasploit [5]. Metasploit fornisce un semplice wizard che guida l'utente nella ricerca di moduli di Windows buggati. Una volta trovata la vulnerabilità fornisce il relativo exploit ed alla fine di testarlo sulla specifica macchina.
L'altra famiglia di exploit a cui si è accennato è quella che riguarda le applicazioni del sistema operativo. Considerando che i software destinati alla maggioranza dell'utenza, molte volte inesperta, siano sottoposti a pochi controlli durante lo sviluppo li rende molto appetibili per potenziali attaccanti. Una volta scoperto un bug all'interno di uno di esso, lo si può sfruttare per arrivare direttamente all'utente con il minimo sforzo. Ancora una volta, l'utilizzo di tool come Metasploit potrebbe aiutare l'utente nella ricerca delle ultime vulnerabilità note su software per Windows.

[5] http://framework.metasploit.com

5.1.8 Difesa contro gli exploit remoti non autenticati

Per quanto riguarda il primo tipo di exploit (basati sui servizi di rete di Windows) è necessario essere sempre aggiornati con le patch di sicurezza che Microsoft rilascia periodicamente. Avere dei sistemi di monitoring e logging sempre attivi sono utili a rilevare operazioni sospette sul proprio sistema. Nel caso in cui si individuino dei bug per i quali non esistono ancora aggiornamenti di sicurezza, è necessario procedere con la disabilitazione dei servizi vulnerabili. Buona norma sarebbe anche quella di tenersi aggiornati leggendo i bolletini di sicurezza di Microsoft nei quali sono descritti in dettaglio i bug rilevati e le patch realizzate. Il suggerimento relativo agli aggiornamenti è valido anche per le applicazioni "end-user". Utilizzare il servizio di Microsoft per l'update automatico è una buona abitudine. Inoltre è consigliato l'utilizzo di un firewall per settare manualmente i permessi alle applicazioni che possono e non possono accedere alla rete. I software che si eseguono sulla propria macchina dovrebbero sempre essere eseguiti con i privilegi più bassi possibili. Se si ottiene il controllo di un'applicazione eseguita come amministratore è ovvio che si ha il completo accesso al sistema.

5.2 Attacchi autenticati

Questa categoria di attacchi sono possibili dopo aver acquisito dei privilegi di sistema sfruttando una delle tecniche descritte in precedenza. Un utente che ha avuto accesso ad un sistema Windows con i privilegi di amministratore o, quantomeno, privilegi di sistema ha la possibilità di ottenere molte più informazioni che in precedenza.

5.2.1 Password cracking

La prima operazione che di solito compie chi ha avuto privilegi su un sistema è quella di ottenere più account possibili. La raccolta di altri username e password gli permetterà in futuro di avere più possibilità di accedere al sistema in caso in cui venga scoperto e può, inoltre, più facilmente confondere le sue tracce agendo da diversi account.
Ogni sistema Windows mantiene un file con gli username attivi sul sistema e gli hash delle password equivalenti. Queste password sono memorizzate in posti diversi in base alla versione di Windows ma solitamente se ne trova una copia nel file memorizzato in DIRECTORY_DI_SISTEMA/system32/config/SAM e un'altra nel registro di sistema nella chiave HKEY_LOCAL_MACHINES/SAM. Esistono appositi tool che si occupano di estrarre le password dalle locazioni indicate. `pwdump` è uno dei tool più utilizzati per questo compito, ne sono state realizzate diverse versioni con numerose funzioni accessorie. Il tool va ad inserirsi nei processi con privilegi di sistema e ha, così, la possibilità di estrarre le password anche col sistema a runtime.
Se gli hash delle pagine sono stati realizzati con un algoritmo valido, non ci sarà modo di ottenerne il testo in chiaro dato che il processo di hashing è "one-way". Nonostante questo esiste comunque un modo di ottenere le password originali. Di solito gli algoritmi di hashing sono noti e eseguendoli su un insieme di parole, si ottengono un elenco di valori hash con i quali confrontare le password che abbiamo ottenuto. Questo processo richiede molto tempo ed è, per questo,

eseguito offline.
Questo tipo di procedura è di solito basato su due strategie:

Attacco a dizionario Questo tipo di attacco prevede che le parole iniziali sulle quali far girare l'algoritmo di hashing siano parole note nella lingua del sistema. Chiaramente più è grande il file dizionario e più possibilità ci sono di crackare password, d'altro canto la lunghezza del dizionario influenza anche la durata del processo di hashing.

Attatto brute force Questo approccio invece prevede di effettuare tutte le combinazioni possibili

5.2.2 Controllo remoto e backdoor

Una volta che l'attaccante ha avuto accesso alla macchina con i privilegi necessari, l'operazione che segue è quella di assicurarsi il controllo della macchina da remoto. Gli strumenti per permettere il controllo da remoto sono noti con il nome di backdoor.
Il modo più semplice di avere una backdoor su un sistema è, ancora una volta, usare netcat. Questo versatilissimo strumento permette infatti di essere lanciato in modalità "listening" per attendere connessioni in ingresso. All'arrivo di una connessione netcat provvederà ad eseguire qualsiasi programma vogliamo. Basta quindi eseguire netcat sul sistema sul quale si vuole avere controllo remoto e selezionare come programma da eseguire `cmd.exe` per ottenere una shell windows ad ogni connessione da remoto.
Chiaramente un sistema dotato di firewall non permette l'accesso diretto dall'esterno. L'operazione che di solito esegue l'attaccante a questo punto è quella di effettuare un port-redirection. La redirezione lavora ascoltando i pacchetti in arrivo su una certa porta e inoltrandoli su uno specifico target. Per i sistemi Windows esistono numerosi tool per effettuare il port redirection, tra cui uno dei più utilizzati è sicuramente `fpipe`.
Come in altre fasi analizzate in precedenza, anche per il controllo remoto su windows esistono tool grafici per velocizzare e facilitare le operazioni. In questo caso si tratta di comunissimi sistemi client-server VNC[6]. Sul mercato ci sono numerosi software di questo tipo, di cui molti sono addirittura free. Installando sulla macchina target il server e lasciandolo in esecuzione, sarà poi possibile connettersi da remoto con la controparte client e avere l'accesso, completamente grafico, al sistema target.
Data l'intrusività di queste tecniche ogni attaccante cercherà di nascondere le tracce del proprio passaggio. Per i sistemi Windows, Microsoft rilascia un software, `auditpol`, che permette di disabilitare in un solo colpo (con l'uso del parametro /disable) i criteri di controllo locale del computer. Altro passo necessario per nascondere le proprie tracce è quello di ripulire i file di log. Anche in questo caso esistono tool ad hoc per i sistemi Windows, come `elsave`, che permettono di eliminare informazioni dal log system.

5.2.3 Contromisure

Come è stato visto nelle sezioni precedenti, molte delle tecniche che un attaccante può utilizzare su un sistema Windows dipendono strettamente dalla

[6] Virtual Network Computing

struttura dell'architettura di Windows. Non esistono quindi contromisure mirate ma è possibile comunque seguire alcune linee guida per ridurre al minimo i punti deboli.

Nomi dei file Ogni attaccante che si rispetti eseguirà sicuramente software malevoli rinominandoli. Buona norma è, quindi, tenere sotto controllo i processi in esecuzione osservando possibili nomi sospetti. Lo stesso andrebbe fatto per le directory di sistema che riguardano l'esecuzione automatica di programmi all'avvio.

Registro di sistema Molte delle applicazioni descritte in precedenza possono essere rinominate ma richiedono la presenza di apposite chiavi di registro. Utilizzare dei tool di ispezioni del registro di sistema può essere utile ad individuare la presenza di applicazioni sospette. Come per il punto precedente, si dovrebbero controllare le chiavi di sistema relative all'esecuzione automatica di programmi all'avvio.

Porte Anche se rinominati, alcuni dei software descritti, possono essere individuati analizzando le porte aperte sul proprio sistema. Un semplice uso di `netcat -an` permette di elencare tutte le connessioni remote presenti indicando il protocollo utilizzato, l'indirizzo remoto e locale e le relative porte utilizzate.

Capitolo 6

Breaking in Unix

Dopo aver analizzato tecniche di breaking per sistemi Windows, vediamo quali sono alcune delle più note per i sistemi Unix. Allo stesso modo nel quale per windows si richiedeva un accesso con privilegi di amministratore (o comunque a livello sistema), anche per Unix è essenziale ottenere una shell `root` per poter sfruttare le tecniche che andremo ad illustrare.

6.1 Sniffing

Gli sniffers sono tra i più popolari strumenti utilizzati dagli attaccanti, che hanno come obbiettivo il Data Link Layer dello stack TCP/IP. Lo sniffer è uno strumento che permette di accumulare traffico da una rete locale, ed è molto utile sia per l'attaccante che può analizzare il traffico di rete, si per l'amministratore che può utilizzarlo per cercare di correggere errori nella rete. Utilizzando uno sniffer, l'attaccante ha la possibilità sia di leggere i dati che attraversano una data macchina, sia di salvarli e utilizzarli successivamente. Dato che lo sniffer permette di raccogliere i dati nel livello del Data Link Layer, potenzialmente ha la possibilità di catturare tutte le informazioni che passano attraverso una data macchina su cui lo sniffer è attivo. Quindi, lo sniffer permette di catturare tutte le informazioni che circolano all'interno di una rete LAN, comprese dati sensibili, quali: userids, password, messaggi email, file trasferiti, e così via. Quindi, a meno che i dati sulla rete non sono trasmessi in forma cifrata, l'attaccante ha la possibilità di leggere tutti dati trasmessi dalla macchina su cui è attivo.
La quantità di dati che possono essere catturati, e di conseguenza la quantità di dati sensibili che lo sniffer può raccogliere, dipendono pesantemente dalla grandezza e dalla topologia della rete utilizzata. Degna di nota è la cosiderazione che l'attaccante può utilizzare tutte le tecniche di sniffing a patto che sia in possesso di una macchina che faccia parte della rete.
Verranno ora illustrate delle possibili architetture di rete e i relativi attacchi che possono essere fatti utilizzando uno sniffer.

Ethernet con Hub. Tipo di sniffing completamente passivo, in quanto tutto il traffico è inoltrato in tutti gli ingressi dell'hub (Figura 6.1).
`possibile attacco: sniffing passivo utilizzando tcpdump`[1].

[1] http://www.tcpdump.org/

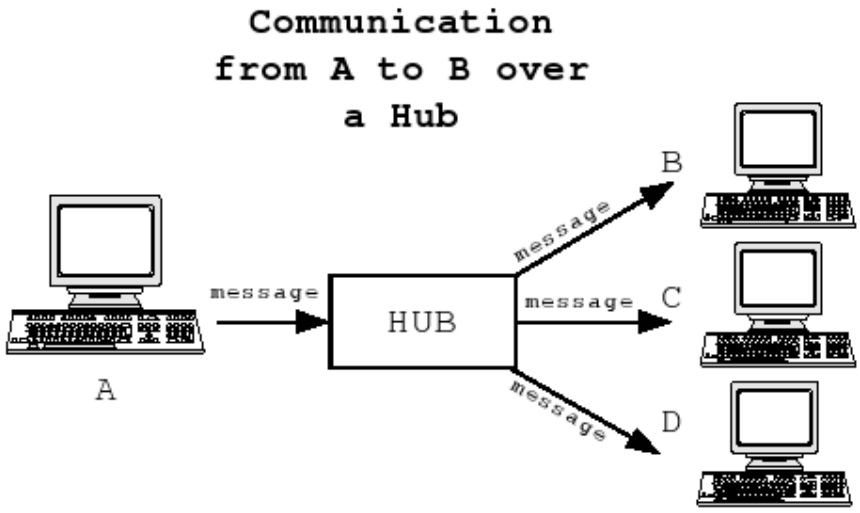

Figura 6.1: in una rete ethernet basata sull'utilizzo di un hub, la comunicazione tra A e B viene inoltrata a tutte le macchine presente nella rete.

Ethernet con Switch. A differenza delle reti ethernet in cui vengono usati gli hub, nelle reti in cui vengono utilizzagli gli switch i dati non vengono trasmessi in broadcast a tutti le macchine presenti in rete (Figura 6.2). Nelle reti in cui sono presenti degli switch è richiesta un'attività di sniffing attiva.
É possibile infatti raggirare lo switch attraverso ARP-Spoofing, MAC-Duplication oppure MAC-Flooding.
`possibile attacco: sniffing attivo utilizzando dsniff`[2].

Reti wireless. Dato che i pacchetti, in questa tipologia di rete, sono trasmessi in broadcast nell'aria, l'attaccante può registrare tutti i dati trasmessi se riesce a ricevere il segnale della rete. Da notare che spesso le reti wireless sono protetti da schemi di cifratura come WPA, che possono essere rotti se vengono raccolti molte dati cifrati con la stessa chiave.
`possibile attacco: uso di sniffer come kismet`[3] `e airodump`[4].

Uno sniffer non deve essere solo capace di catturare i dati che viaggiano su una rete. La raccolta grezza di dati non è molto utile se poi si lascia all'utente l'interpretazione dei dati raccolti. Ad esempio, l'output grezzo di una sessione FTP è praticamente inutilizzabile, a meno che non ci sia un lavoro manuale fatto dall'attaccante al fine di tirar fuori userids, password, nomi di comandi e così via. Un buon sniffer, che offre un'ottima interpretazione di dati inviati utilizzando vari protocolli, è dsniff[5]. É capace di interpretare FTP, telnet, HTTP, POP, pop-pass, NNTP, IMAP, SNMP, LDAP, rlogin, RIP, OSPF, NFS, YP/NIS, SOCKS,

[2] http://www.monkey.org/dugsong/dsniff/
[3] http://www.kismetwireless.net/
[4] http://www.aircrack-ng.org/
[5] http://www.monkey.org/dugsong/dsniff/

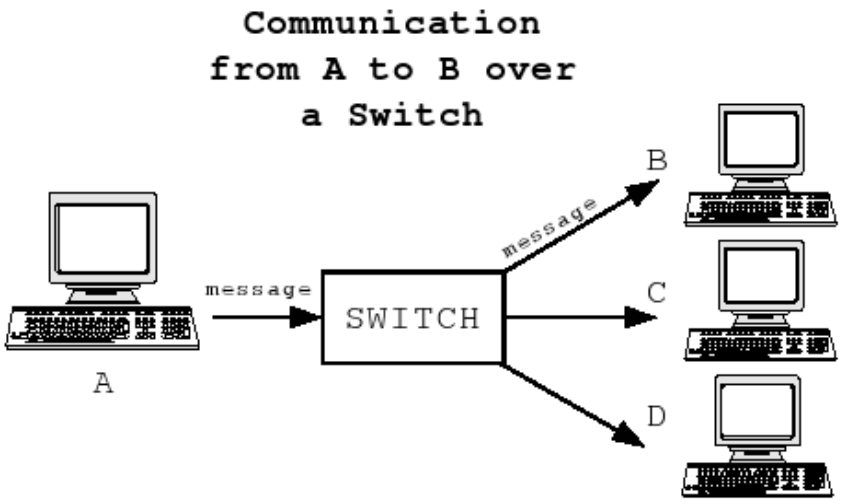

Figura 6.2: in una rete basata sull'uso degli switch, la comunicazione tra A e B è visibile solo alle due parti in gioco.

X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, MS SMB, Oracle SQL*Net, Sybase SQL. La capacità da parte dello sniffer di rilevare e interpretare questa enorme lista di protocolli dell'application-level, risulta essere un'ottimo e potente aiuto per un attaccante.

6.2 Spoofing

Un altro componente fondamentale di numerosi attacchi include il cambiamento o trasferimento dell'indirizzo ip sorgente di un sistema, tecnica comunemente conosciuta come *spoofing dell'indirizzo ip*. Lo spoofing è molto utile per gli attaccanti che non voglio lasciare alcun tipo di tracce quando operano all'interno della rete, infatti grazie a questa tecnica i pacchetti inviati dall'attaccante sembreranno essere stati inviati dal sistema che ha impersonificato. In aggiunta, lo spoofing dell'indirizzo ip permette all'attaccante di raggirare quelle applicazioni che basano su di esso sia l'autenticazione che il filtraggio del traffico.
Il semplice IP spoofing è molto efficiente per raggiungere particolari scopi. Se un attaccante vuole inviare pacchetti che sembrino essere stati inviati da un'altro sistema, semplicemente può cambiare l'indirizzo ip sorgente dei pacchetti da inviare, ed il tutto funziona. In questo caso l'attaccante potrebbe oscurare la sorgente di un attacco basato sul packet flood, oppure causare un attacco denial of service. Daltronde, questa tecnica presenta alcune limitazioni. Il semplice spoofing dell'ip permette di inviare pacchetti alla macchina target senza riceverne però alcuna risposta, in quanto a causa delle tecniche di instradamento, tutte le risposte dei pacchetti inviati saranno inviate alla macchina che si è impersonificata. Di conseguenza il semplice spoofing non permette all'attaccante di interagire con la macchina che intende attaccare in quanto tutte le risposte

saranno inviate ad un altro sistema.
Verrà ora mostrata la dinamica di un attacco spoofing fatto contro una qualsiasi applicazione basata sul protocollo TCP. Da notare che lo spoofing entra in azione, in questo protocollo, nella fase iniziare, proprio quando viene eseguito il three-way handshake[6]. Consideriamo ora lo scenario in Figura 6.3: Eve, l'attaccante vuole impersonificare l'utente Alice, usando il suo indirizzo ip in un attacco di spoofing; Bob, invece, è l'utente con cui Eve vuole interagire, a cui vuol far credere di essere l'utente Alice; a questo punto Eve inizia la comunicazione aprendo una connessione TCP con Bob e inviando il primo dei tre pacchetti previsti nell'handshake, un pacchetto TCP SYN con l'indirizzo ip sorgente di Alice (la notazione SYN(A, ISN_A) si indica che il pacchetto con il bit code SYN attivato è inviato con l'indirizzo ip sorgente di A, e il numero di sequenza iniziale di ISN_A[7]); una volta ricevuto il pacchetto, Bob replica con ACK(A, ISN_A)SYN(B,ISN_B), un pacchetto di acknowledg per il numero di sequenza fornito da A e un pacchetto per fornire il proprio; i due sono inviati all'indirizzo ip presente nel primo pacchetto ricevuto da Bob, quindi ad Alice; quando Alice riceve il messaggio di Bob, invia un messaggio RESET, che essenzialmente serve a dire che lei non ha mai iniziato una conversazione con Bob, lasciando cadere la connessione. In questo scenario si può notare che l'attaccante non ha nessuna possibilità di vedere la risposta inviata da Bob, ne tantomeno di tenere attiva la connessione continuando così ad impersonificare Alice. Daltronde, se Eve si trova nella stessa LAN in cui si trova Bob, potrebbe, attraverso lo sniffing, vedere la risposta e usare un ARP spoofing per impedire che il RESET inviato da Alice arrivi a Bob, ed impedire quindi che la comunicazione cada.
Questo esempio serve soltanto per rendere un'idea di quello che è un classico scenario di spoofing fatto su un protocollo TCP. Esistono numerosi altri attacchi fatti su altri tipi di protocolli, quale il protocollo ARP, DNS e molti altri.

6.3 Session hijacking

Lo sniffing permette ad un attaccante di osservare il traffico della rete in cui si trova, mentre lo spoofing da la possibilità all'attancante di impersonificare un'altra macchina. Il session hijacking è praticamente un composto delle due tecniche precedenti. Consente all'attaccante la possibilità di poter rubare un una sessione di login interattiva (ad esempio usando Telnet, rLogin, FTP, e così via) effettuata da un utente su un sistema. La maggior parte delle vittime dell'hijacking che vede la propria connessione cadere, attribuisce la causa ad un malfunzionamento della rete. Se poi una vittima cerca di riacquistarla effettuando un nuovo login, prende coscenza che la connessione non era caduta, ma che era stata rubata.
Il modo migliore per rendere l'idea di cosa sia un session hijacking, è quella di mostrarne un esempio pratico. Nella Figura 6.4, Alice stabilisce una sessione telnet con Bob (il protocollo telnet è giusto un esempio, infatti possono essere considerate molte altre applicazioni che supportano il login interattivo con sessioni non cifrate come, FTP e rlogin). Eve si trova in un segmento della rete, da cui può vedere la comunicazione tra Bob e Alice. In questa posizio-

[6] scambio di messaggi per la sincronizzazione tra due applicazioni che comunicano sul protocollo TCP.
[7] valore iniziale con cui vengono numerati i pacchetti spediti.

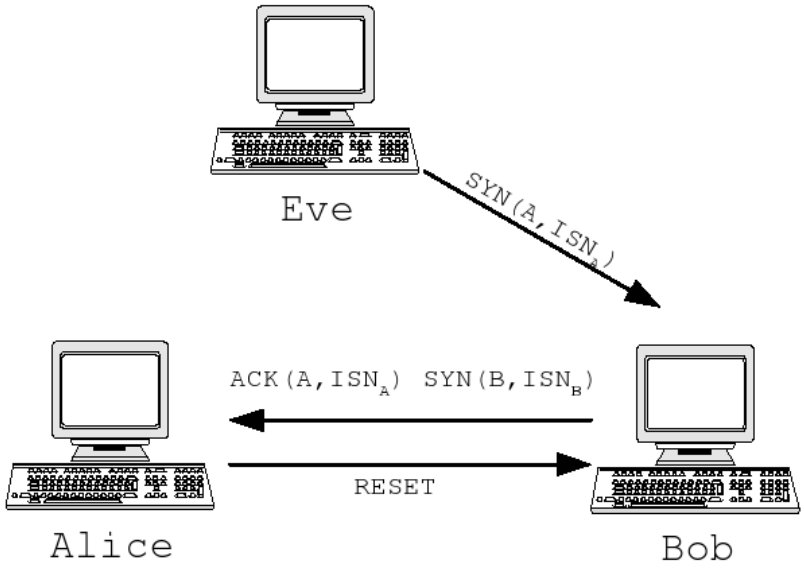

Figura 6.3: three-way handshake impedito dallo spoofing.

ne strategica, può osservare la connessione appena effettuata, utilizzando delle tecniche di sniffing. Avendo la possibilità di leggere i messaggi che Bob e Alice si scambiano, può conoscere quale sia il numero di sequenza dei pacchetti TCP scambiati in quel momento[8]. A questo punto, Eve decide di effettuare un hijack nella connessione tra Bob ed Alice. Invia dei messaggi a Bob utilizzando tecniche di spoofing, sostituendo quindi l'indirizzo ip sorgente con quello di Alice ed utilizzando il numero di sequenza opportuno per i pacchetti TCP, ricavato nella fase di filtraggio dei pacchetti. Se l'hijacking ha avuto successo, Bob eseguirà dei comandi inviati da Eve, pensando che siano stati dati da Alice.
Dato che la sessione è stata rubata in rete, in quanto era di tipo remoto, il session hijacking effettuato è di tipo network-based. Esistono sessioni che presentano un forte livello di sicurezza nella fase iniziale. Un attaccante ha la possibilità di impadronirsi anche di questo tipo di sessioni solo se la comunicazione successiva alla fase di autenticazione non è protetta crittograficamente.
Oltre a quelle network-based esistono tecniche di session hijacking host-based. Per session hijacking network-based si intende il prendere possesso di una sessione stabilita in rete, mentre per session hijacking host-based, si prevede che l'attaccante abbia già privilegi da super utente nel sistema sorgente o in quello destinazione. Esistono al giorno d'oggi molti strumenti che consentono di effettuare il session hijacking, sia host-based che network-based. Ne suggeriamo alcuni:

- **Hunt**: strumento molto noto per il session hijacking network-based; `http://www.l0t3k.net/tools/Hijacking/hunt-1.5.tgz.gz`

[8] molti strumenti di hijacking non solo includono funzionalità di sniffing, ma anche funzionalità che permettono in maniera facile di rubare la sessione che si sta osservando, per cui esiste l'esigenza di conoscere tale valore.

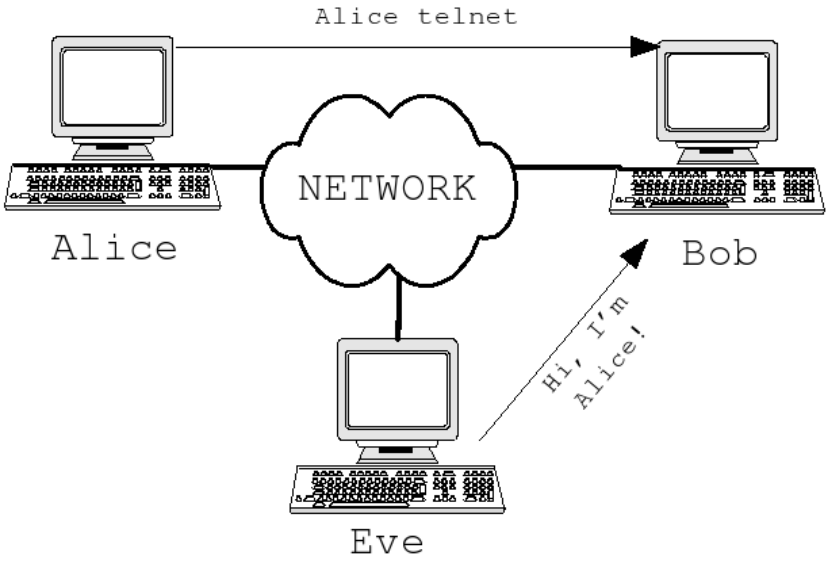

Figura 6.4: scenario di un attacco session hijack fatto in rete.

- **Juggernaut**: strumento per il session hijacking network-based; `http://www.l0t3k.net/tools/Sniffing/1.2.tar.gz`
- **TTYsnoop**: strumento per il session hijacking host-based. `http://freshmeat.net/projects/ttysnoop/`

6.4 Contromisure per Sniffing e Spoofing

Difendersi contro lo sniffing risulta alquanto semplice. Dato che la quantità dei dati accumultati da un'operazione di sniffing può essere limitata dalla topologia di rete utilizzata, una buona soluzione può essere quella di sceglierne una buona, non annullando così il problema ma notevolmente limitarlo. In aggiunta può essere adottata la politica di cifrare tutti i dati sensibili che viaggiano all'interno della rete. Rimpiazzare protocolli come: Telnet, FTP, POP3 o HTTP; con i relativi protocolli sicuri, rispettivamente con: SSH, SFTP, SALS o HTTPS, dove necessari e possibi. Per comunicazioni su canali ad altro rischio, quali la rete internet, è possibile adottare delle tecniche di tunnelling, che permenttono di inviare i dati in maniera sicura su un canale insicuro.
Esistono molte buone tecniche che permettono di evitare lo spoofing dell'indirizzo ip. Come primo passo, occorre essere sicuri che il numero di sequenza dei pacchetti TCP generati sia difficile da predire. É possibile testare quest'ultima catatteristica, ad esempio, utilizzanto `nmap`.
É possibile inoltre impostare delle regole di filtraggio di pacchetti *anti-spoof* al router che offre il collegamento, ad esempio, della rete aziendale con la rete internet oppure un'altra rete dello stesso tipo. É possibile avere una semplice idea dello scenario guardando la Figura 6.5. Il filtro non fa altro che cancellare tutti i pacchetti che hanno un indirizzo di una rete differente da quello dell'interfaccia

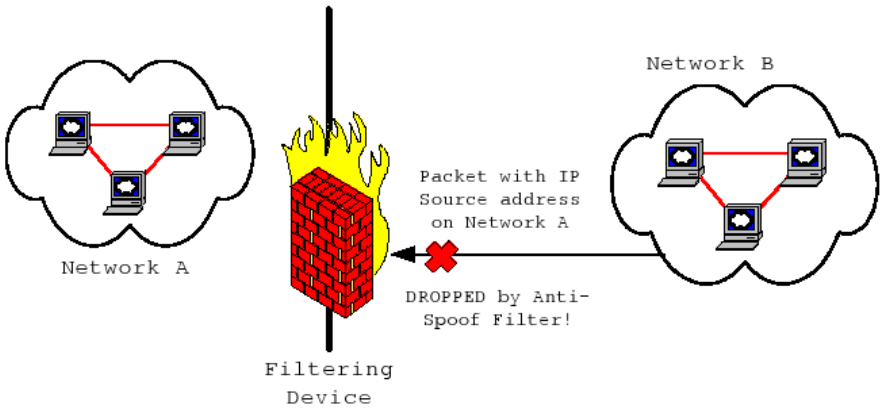

Figura 6.5: raffigurazione dell'implementazione di un filtro anti-spoofing.

da cui sono stati spediti. Tali pacchetti, se presenti all'interno della rete, possono mettere in evidenza o un errata configurazione di qualche macchina oppure un attacco spoofing. Da notare che i filtri dovranno essere implentati sia per il traffico in ingresso che per quello in uscita. In molti casi i filtri per il traffico in uscita non sono implementati. Questo potrebbe consentire ad un possibile attaccante, che ha già preso possesso di una macchina all'interno della rete, di effettuare degli attacchi ad altre reti.
In aggiunta si potrebbe non consentire l'instradamento dalla sorgente[9], in quanto potrebbe consentire ad un attaccante di ricevere traffico non destinato a lui. Infine, si potrebbe consentire di stabilire connessioni tra hosts che hanno acquisito l'indirizzo ip attraverso metodi di autenticazione.

[9] è un opzione che consente al mittente di specidicare il percoso i pacchetti devono seguire per arrivare a destinazione.

Capitolo 7

Conclusioni

Dopo aver visto la quantità di informazioni che possono essere recuperate da un attaccante e l'uso malintenzionato che ne può essere fatto, è facilmente intuibile che nessuna organizzazione può sentirsi completamente al sicuro. La consapevolezza di ciò è il primo passo necessario per affrontare il problema "sicurezza informatica". Le contromisure per limitare il più possibile il reperimento e l'uso di queste informazioni ci sono, ed è strettamente necessario che vengano messe in atto da ogni organizzazione che è presente sulla rete.
E' importante ricordare che la sicurezza informatica è un processo e non un prodotto. Non bisogna mai pensare di aver risolto il problema "sicurezza" e accantonarlo ma è necessario portarlo avanti per tutto il tempo.

Riferimenti

1. Stuart McClure, Joel Scambray, George Kurtz. *Hacking exposed.* McAfee.
2. Tara Calishain e Rael Dornfest. *Google Hacks: 100 Insider-Tricks & Tools.* O'Reilly.
3. Johnny Long. *Google Hacking For PenetrationTesters.* Syngress.
4. http://en.wikipedia.org/wiki/Hacker_(computer_security).