Virus

Anatomia di un attacco

Sui virus si è ormai detto tutto. In realtà l'utente comune poi ne sa ben poco, tant'è che si continua ad attribuire ai "virus", veri o presunti, la responsabilità di qualsiasi cosa vada storta sul proprio computer, proprio come dieci anni fa.
Un semplice collegamento a Internet costituisce per la maggioranza degli utenti un'incognita in più. Pubblicizzata in modo martellante, la rete per eccellenza viene usata spesso senza una vera comprensione di ciò che sta "dietro al modem". E quando qualcosa va storto è ancor più difficile comprendere cosa sia realmente accaduto.

di Stefano Toria

Una schematica slide preparata da un gruppo di consulenza di una nota università americana schematizza le fasi di un attacco in rete in questo modo:

1. Localizzare il sistema-bersaglio
2. Ottenere accesso come utente
3. Ottenere accesso privilegiato
4. Coprire le tracce
5. Installare una backdoor per usi futuri
6. Svolgere attività non autorizzata/illegale
7. Passare al bersaglio successivo.

Non tutte le tipologie di attacchi in rete eseguono tutte queste operazioni in modo esplicito; talvolta non le eseguono affatto. In questo articolo cercheremo di illustrare come funziona un attacco in rete, evitando – come è ormai consuetudine di questi articoli – di fornire informazioni potenzialmente "pericolose", ma al tempo stesso indicando ai lettori le modalità migliori per difendersi da questa tipologia di rischio.

Il caso più semplice

Ma cos'è un "attacco in rete"? Possiamo tentarne una definizione, più che altro in forma di proposta, dato che stiamo parlando di qualcosa che al momento è in estrema evoluzione e non si sa bene in che direzione potrà muoversi.

Un attacco in rete è sostanzialmente un collegamento effettuato verso un sistema connesso a una rete, con finalità e/o modalità aggressive. Analizzando le interazioni che si verificano nel corso di quello che viene riconosciuto come "attacco" ci si rende conto facilmente della precisa finalità aggressiva della persona che ha messo in atto la procedura. In altre parole, è difficile trovarsi davanti a situazioni dubbie: un attacco non capita per caso, ma è frutto di un'azione ben determinata.

Quasi tutti gli attacchi in rete prendono l'avvio da una sistematica azione di "probing" da parte dell'attaccante. E' bene chiarire un concetto: mentre nel caso dei virus l'intervento umano diretto e consapevole si limita quasi sempre alla sola programmazione del virus, che successivamente viene messo in circolazione e si diffonde da solo, nel caso di un attacco in rete il centro dell'attenzione è su una precisa persona che compie deliberatamente una serie di azioni: l' hacker.

Il "probing" consiste nell'effettuare una scansione di tutti i possibili "punti di accesso" sui sistemi più prossimi, per identificare un candidato all'attacco. Già un buon sistema di difesa può essere in grado di rilevare questa azione e sventarla.

Successivamente, identificate una o più vittime potenziali, l'aggressore mette a segno il colpo: vediamo il caso più semplice. Una delle applicazioni più diffuse su Internet è IRC, l'Internet Relay Chat, ossia una enorme messaggeria mondiale con centinaia di canali, responsabile di una buona fetta del traffico quotidiano. Una particolare sequenza di comandi TCP/IP inviata a un utente collegato a IRC determina l'interruzione del collegamento tra l'utente e il proprio server IRC; l'utente, conoscendo l'inaffidabilità di molti collegamenti tramite Internet, tutto sospetterà fuorché l'attività di un hacker.

Il danno provocato da questo tipo di attacco è pressoché nullo, tuttavia è importante comprenderlo a fondo perché contiene in nuce tutte le caratteristiche di attacchi ben più gravi. Vediamo la sequenza dei passi logici:

- l' hacker identifica la vittima in base al suo indirizzo IP
- l' hacker invia alla vittima una speci-

fica sequenza di pacchetti
- il collegamento tra la vittima e il server IRC si interrompe
- l' hacker passa alla vittima successiva.

Uno schema leggermente diverso ipotizza che l' hacker abbia preso di mira quella specifica vittima:

- l' hacker identifica la vittima in base al suo indirizzo IP
- l' hacker invia alla vittima una specifica sequenza di pacchetti
- il collegamento tra la vittima e il server IRC si interrompe
- la vittima si riconnette
- l' hacker invia nuovamente alla vittima la sequenza di pacchetti
- il collegamento tra vittima e server IRC si interrompe di nuovo
- le operazioni continuano a ripetersi fino al punto in cui la vittima abbandona il gioco e chiude la connessione a Internet.

Qualsiasi buon firewall mette al riparo da questo tipo di attacco.

Kevin Mitnick, forse uno dei più noti hacker, arrestato nel 1995 dopo due anni di investigazioni e ricerche.

Un concetto fondamentale: l'IP-spoofing

Perché l'attacco abbia successo, tuttavia, è essenziale che la sequenza di pacchetti che l' hacker invia alla vittima sembri provenire dal server IRC. Si tratta di un punto fondamentale, perché altrimenti l'intero schema non avrebbe senso: un client IRC connesso al proprio server (su uno specifico indirizzo IP) non ha alcun problema a ricevere una segnalazione secondo cui un certo server Web non è più disponibile. Per contro, il client IRC è sensibile alle segnalazioni che riguardano il server a cui è connesso, e infatti dopo un determinato numero di segnali di sistema non più disponibile è lo stesso client a interrompere la connessione.

Ma normalmente i pacchetti trasmessi da un PC connesso a Internet indicano come mittente l'indirizzo assegnato al PC all'atto del collegamento. E' quindi necessario che l' hacker metta in atto una tecnica particolare, che va sotto il nome di "IP-spoofing" (lett. truffa IP), che consiste semplicemente nel generare pacchetti IP che nel valore del mittente contengano qualsiasi cosa, definita dall'utente nel momento in cui il pacchetto viene generato. Non sempre la tecnica ha successo (molti firewall sono programmati per riconoscerla e sventarla) ma costituisce un primo importante strumento di aggressione da cui l'utente deve guardarsi.

Possiamo quindi modificare la sequenza di operazioni descritta sopra:

- l' hacker identifica la vittima in base al suo indirizzo IP
- l' hacker invia alla vittima una specifica sequenza di pacchetti apparentemente provenienti dal server IRC
- il collegamento tra la vittima e il server IRC si interrompe
- la vittima si riconnette
- l' hacker invia nuovamente alla vittima la sequenza di pacchetti apparentemente provenienti dal server IRC

eccetera.

Secondo le statistiche pubblicate dai principali enti di controllo e consulenza per la sicurezza in rete, questo tipo di attacco è di gran lunga il più frequente. E' anche il più subdolo, perché toglie all'utente la possibilità di sentirsi sicuro scegliendo gli IP dei sistemi con cui desidera stabilire connessioni e escludendo tutti gli altri: un hacker può farsi passare per un corrispondente legittimo e accedere là dove l'utente cercava di escluderlo.

Tsutomu Shimomura ha condotto un' abilissima investigazione per identificare Mitnick, riuscendo infine a intrappolarlo servendosi di un'esca appositamente preparata.

Bersaglio predestinato

Gli attacchi in rete sono tutt'altro che una novità degli ultimi tempi. All'inizio dello scorso articolo abbiamo rammentato uno dei casi più celebri, che risale alla fine degli anni '80. E lo stesso Cliff Stoll raccontava di questo episodio in appendice al suo libro in cui descriveva un altro caso, di cui era stato personalmente testimone e su cui aveva indagato, avvenuto poco prima.

Caratteristica comune di tutti gli hacker è il costante sforzo di aggiornamento, che li spinge a cercare mete sempre nuove per i loro tentativi di intrusione. Per conseguire questo scopo hanno a disposizione alcuni mezzi, di cui il più semplice è tentare di individuare, su un sistema a cui hanno già ottenuto l'accesso, le indicazioni che possano portarli ad altri sistemi. E il modo più facile è di prelevare il file /etc/passwd.Una grandissima maggioranza dei sistemi connessi a Internet è gestita da una delle varie versioni del sistema operativo Unix. Tutte queste versioni hanno in comune alcune cose fondamentali, tra cui ad esempio il fatto che il file contenente le password è pubblico, si chiama /etc/passwd, e riporta i nomi degli utenti in chiaro e le password in cifra.

L'algoritmo di cifratura delle password è relativamente semplice ed è "a senso unico", ossia non è possibile risalire, dal valore contenuto in /etc/passwd, al valore che lo ha originato. Quindi il sistema controlla la password cifrando quello che l'utente scrive all'atto del collegamento e confrontando il risultato con quello che c'è in /etc/passwd; se corrisponde si dà per scontato che la password sia stata inserita correttamente.

Questa caratteristica rende particolarmente sicuro il sistema delle password, e per questo motivo gli ideatori del sistema Unix non hanno ritenuto necessario proteggere ulteriormente uno dei file più delicati di tutto il sistema. Ma hanno fatto i conti senza la pigrizia e lo scarso senso di sicurezza degli utenti: vedia-

mo perché.

Chi dovesse venire in possesso di un file /etc/passwd preso da un sistema qualsiasi, in teoria non dovrebbe essere in grado di farci nulla: le password sono in cifra, non si riesce ad accedere al sistema. Tuttavia un tentativo può farlo: partendo da una lista di parole (va bene anche un vocabolario) può cifrare una dopo l'altra le parole della lista e confrontare il risultato con il valore della password cifrata di un utente qualsiasi; quando si trova un valore che corrisponde, la parola da cui si è partiti è la password di quel particolare utente.

Il sistema funziona perché, come dicevamo, gli utenti sono pigri e non hanno voglia di trovarsi una password non banale. L'utente Rossi, codice di login "rossi", come password quasi certamente utilizzerà "mario", oppure il nome della moglie, della fidanzata, di un figlio, della squadra del cuore. Tutti nomi che un attacco basato su un dizionario impiega pochi minuti a trovare, mentre basterebbe usare alcuni semplici trucchi per evitarlo, come ad esempio servirsi di password composte da due o più parole separate da segni di punteggiatura, es. casa*albero è una password di gran lunga più sicura di qualsiasi nome di battesimo, numero di telefono o data di primo incontro.

Una volta trovato un numero sufficiente di password sul sistema-vittima, l'hacker esplorerà gli archivi di ciascun utente in cerca di istruzioni per l'accesso ad altri sistemi; e c'è da scommetterci che ne troverà. L'operazione quindi si ripete su ciascuno dei nuovi sistemi-bersaglio, e così proseguendo.

Alcuni sistemi implementano uno specifico controllo per impedire agli utenti di scegliere password banali. Solitamente sono piuttosto poco popolari tra gli utenti, che spesso sono più sensibili al problema di dover memorizzare la password che al rischio di intrusione; la vera difesa contro questo tipo di rischio consiste nel formare nell'utenza la cultura della sicurezza.

Sfruttare il lato debole...

Sovente le tecniche di attacco sfruttano una debolezza riconosciuta di un sistema operativo. E' un caso tipico quello del cosiddetto "ping of death", che alcuni anni fa attirò l'attenzione di sistemisti e utenti evoluti.

I fatti: inviando a un sistema Windows NT un pacchetto appositamente confezionato se ne determinava l'arresto completo, compariva la schermata azzurra di blocco irreversibile, e si doveva riavviare il sistema. La Microsoft prese immediati provvedimenti e distribuì una soluzione temporanea e poco dopo un nuovo service pack, in cui il problema veniva risolto.

Una delle attività principali degli hacker, un'attività sulla quale vige nel loro ambiente la regola del massimo scambio di informazioni possibile, consiste nell'identificare, studiare e trovare il modo di sfruttare le debolezze dei più diffusi sistemi operativi installati sui computer connessi a Internet.

E' piuttosto frequente infatti leggere, nei bollettini tecnici emessi dagli enti come il CERT (Computer Emergency Response Team), l'indicazione di queste vulnerabilità e delle modalità per aggirarle o rimuoverle. Spesso si tratta di situazioni riferite a sistemi operativi Unix, nei quali particolari configurazioni di esecuzione di comandi di sistema possono portare utenti qualsiasi a ottenere arbitrariamente lo status di utente privilegiato.

E' difficile tuttavia che questo genere di problemi possa impattare sull'utente medio di personal computer; quando ciò dovesse accadere, solitamente la pubblicità che viene data al fatto è enorme e quindi l'utente ne viene comunque a conoscenza. In ogni caso può essere utile consultare saltuariamente il sito del CERT all'indirizzo www.cert.org per avere informazioni specifiche e istruzioni su come fronteggiare eventuali vulnerabilità del proprio PC.

Lacrime e terra

Sta divenendo piuttosto comune trovare, in giro per la rete, programmi che offrono ad aspiranti hacker la possibilità di far danni senza aver fatto "la gavetta", e quindi senza la necessità di possedere quel bagaglio di conoscenze tecniche che servono per mettere le mani nelle reti a un livello tale da poter mettere a segno, o almeno tentare, intrusioni in sistemi altrui.

La tendenza, come si diceva altrove, è preoccupante, perché se da un lato questi programmi per hacker fai-da-te sono piuttosto rudimentali e facili da contrastare, dall'altro mostrano chiaramente una tendenza che, unita all'esperienza decennale coi virus, deve far riflettere sui possibili futuri sviluppi di questo tipo di rischi.

Teardrop ("lacrima") e Land ("terra") sono i nomi di due tra i più diffusi programmi di questa categoria. Facilmente reperibili su Internet, sviluppano attacchi destinati a privare uno o più utenti di risorse di cui si stanno servendo, analogamente a quanto descritto nel caso di IRC all'inizio di questo articolo.

Anche qui, un buon firewall personale mette al riparo dal rischio; si prevede che questo genere di strumenti diventerà nei prossimi anni almeno tanto comune quanto gli antivirus, nella misura in cui gli utenti di Internet si renderanno conto di trovarsi in situazione di rischio e cercheranno appositi strumenti di difesa.

E-commerce in pericolo?

Nel nostro Paese il commercio elettronico non ha ancora preso piede, nonostante diversi interessanti tentativi siano già stati realizzati. Ciò che manca in Italia è una vera cultura dell'acquisto per corrispondenza, che negli Stati Uniti, quanto meno per motivi storici, è invece estremamente diffusa.

Ciononostante il numero di siti che offrono di acquistare beni e servizi online aumenta continuamente, ponendo problemi specifici ai responsabili dei siti. Infatti, oltre ai soliti ovvi tentativi di ottenere beni e servizi senza pagare, gli attacchi contro questo tipo di siti possono essere condotti in modo indiretto, cercando di sfruttare le vulnerabilità del sistema di "common gateway interface" o CGI che solitamente sovrintende all'esecuzione dei programmi in ambiente Web per l'esecuzione delle funzioni di commercio elettronico.

In questo caso l'obiettivo dell' hacker non sono i prodotti venduti tramite il sito, bensì il sito stesso, in cui mira a mettere le mani per prelevare file o modificare informazioni. L'interfaccia CGI ha dimostrato di non essere particolarmente adatta a situazioni in cui la sicurezza sia un elemento fondamentale, e infatti sono disponibili in commercio strutture alternative più adeguate agli ambienti commerciali. MC

Siamo pronti.

In un mercato così competitivo essere dei punti di riferimento è necessario. E' per questo che nasce la Facal product S.p.A., un vero e proprio colosso commerciale composto da ben 16 PUNTI VENDITA. Solo se si è grandi è possibile offrire ai propri clienti più servizi, maggiore organizzazione, e perchè no! anche prodotti a prezzi interessanti.

Venite a scoprite i vantaggiosi servizi Facal in uno dei negozi più vicino a casa tua.

FACAL POINT CARD

Finalmente è arrivata la Facal point card. La carta che vi farà accedere agli sconti Special Price!!! non c'è che dire, è proprio un bel risparmio e possederla è semplicissimo, basta acquistare presso un Facal point un personal computer completo oppure materiale superiore a 2.000.000 di lire, e la tessera sara' vostra.

SPECIAL BONUS

Presentando l'abbonamento S.S. Lazio 1998-1999 è possibile ottenere lo special BONUS. Uno speciale sconto accordato per il periodo di validità dell'abbonamento.

CONSEGNA 24 - 48 ORE In tutta Italia

Ogni nostro punto vendita è in grado di spedire in tutta Italia in 24-48 ore. Ci serviamo di corrieri espresso come DHL o UPS, che garantiscono un servizio porta a porta eccezionale.

ASSISTENZA TECNICA

La Facal product S.p.A. segue i suoi clienti, garantendo un servizio post-vendita ai massimi livelli di qualità. Inoltre importando dagli Stati Uniti e dai Paesi asiatici, la Facal è in grado di fare assistenza diretta anche per prodotti importati.

SIAMO SUL WEB

D'ora in poi acquistare da Facal point è più facile. Via Internet, http://www.facal.it potrete rimanere comodamente in casa e consultare i nostri prodotti con prezzi sempre aggiornatissimi.

Facal®

La catena italiana dell'informatica di qualità

FACAL POINT GROUP - ROMA CASILINO: via Silicella, 84 00169 Roma Tel. 062389887 - ROMA NOMENTANO: via Michele di Lando, 81 00162 0644242135- ROMA EUR: via Francesco Acri, 54/56 00142 Tel 065460732 - ROMA TORRE ANGELA: via di Torrenova, 91/e-f 00133 Tel. 0620630726 - ROMA MONTE MARIO: via Augusto conti, 3a/b 00135 Tel. 063060090 - ROMA CENTOCELLE: via delle Betulle, 132 00171 Tel. 062596700 - ROMA NUOVO SALARIO: Via F.A. Gualterio, 52/a 00139 Tel. 0688643046 - ROMA MONTEVERDE: via Laura Mantegazza, 62 00152 Tel. 0653272451 - VELLETRI - CAMPO SPORTIVO: Via Edoardo di Filippo, 11 (zona camposportivo) 00049 Tel.0696100034 - VILLA ADRIANA - CENTRO: via di Villa Adriana, 29 00010 Tel. 0774509042 - SAN LORENZO NUOVO - CENTRO: corso Umberto I, 6 01020 Tel 0763726004 - NAPOLI FERROVIA: via S.Anna alle Paludi, 126/128 80142 Tel. 081266325 - VERONA ARENA: piazza Cittadella, 17 37122 Tel. 0458015648 - CATANIA ZONA VENETO: largo Bordighera, 37 95127 Tel. 095372197