

RETI DI CALCOLATORI

COSA È INTERNET?

Torniamo indietro, al 1962..

L'idea di una rete mondiale è stata proposta per la prima volta nel corso di una conferenza sul concetto di "Galactic Network", composta un insieme mondiale di computer interconnessi in rete, da questa tutti avrebbero potuto accedere a dati e programmi, indipendentemente dalla propria posizione.

Occorre però arrivare al 1969 per avere una prima forma d'interconnessione tra macchine.

Il Ministero della Difesa Statunitense creò un'agenzia l'Advanced Research Projects Agency (ARPA) incaricata di sviluppare una rete in grado di resistere ad una guerra nucleare. Il progetto interessò, università, centri di ricerca ed aziende private. All'inizio furono collegati quattro grandi computer nelle università del sud-ovest degli Stati Uniti.

Nel 1972 iniziò lo sviluppo di una nuova versione del protocollo allora utilizzato, per venire incontro alle esigenze di un ambiente ad architettura aperta nel quale le informazioni potessero essere inviate da un computer ad un altro. Questo protocollo sarebbe stato successivamente chiamato Transmission Control Protocol/Internet Protocol (TCP/IP).

Nel 1985 Internet mette in contatto una larga comunità di ricercatori e sviluppatori ed altre comunità cominciano ad usarlo per comunicazioni e per scambio di Email.

Nel 1993 I media cominciano a prendere notizie da Internet, la Casa Bianca e le Nazioni Unite vanno online. Nel dicembre del 1993 ci sono 623 siti Web nel mondo.

Nel 1994 Netscape utilizza un nuovo sistema di distribuzione del software: rende disponibili le prime copie del suo Netscape Navigator per il download attraverso Internet.

Nel 1995 Vengono fondati fornitori di accesso ad Internet (Provider) quali CompuServe, AOL e Prodigy.

Nel gennaio 1996 vengono censiti 100 000 siti Web nel mondo.

Alla fine dell'anno 1998 ci sono all'incirca 3.7 milioni di siti Web e più di 150 milioni di utenti Internet nel mondo.

Oggi solo in Italia si contano circa 2,7 milioni di famiglie con un collegamento internet in casa.

Come funziona una rete di calcolatori

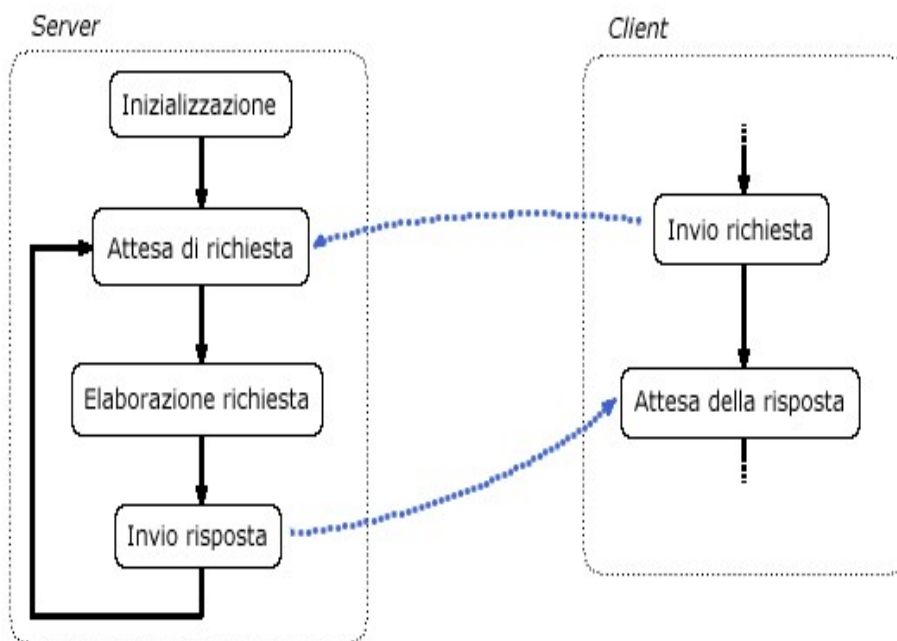
Un'interfaccia di rete è costituita fisicamente da una scheda di rete o un modem. Generalmente, ma non necessariamente, ogni interfaccia di rete ha un proprio indirizzo.

Un'applicazione in esecuzione su di un sistema potrà utilizzare un'interfaccia di rete per comunicare con un'altra applicazione che è in esecuzione, in generale, su un altro sistema.

Si distinguono quindi **due categorie di applicazioni** che utilizzano la comunicazione via rete: le applicazioni di tipo **client** e quelle di tipo **server**.

Semplicemente, quindi, un servizio non è altro che una "richiesta di dati", fatta da un client ad server, utilizzando la rete per "trasferire" questi dati.

Internet è un insieme di computer, fisicamente collegati tra di loro, ogni macchina è chiamata Host.



Le macchine, così come le applicazioni, possono essere divise in tre categorie:

- Client: richiedono un servizio – sono le macchine utilizzate per lavorare (si parla infatti anche di workstation) e per utilizzare i servizi messi a disposizione dai server presenti sulla rete;
- Server: forniscono un servizio - generalmente si tratta di macchine con hardware in grado di offrire prestazioni elevate (bassi tempi di accesso ai dischi, grande quantità di memoria centrale, affidabilità, sicurezza);
- Apparati trasmissivi: instradano i collegamenti.

L'indirizzamento

Dove esistono milioni di host, il trasferimento dei dati deve essere legato a regole precise.

Quando ci colleghiamo ad internet ci viene assegnato un indirizzo numerico (ad esempio: 212.100.231.233), a consegnarcelo è un server DHCP. Grazie a questo indirizzo siamo riconosciuti in modo univoco e possiamo accedere alle risorse dei server.

Anche i server hanno degli indirizzi, dietro al nostro sito preferito c'è infatti un indirizzo numerico, che per semplificare chiameremo semplicemente "indirizzo IP".

Siccome ricordarsi tutti gli IP dei siti normalmente visitati e dei server utilizzati è praticamente impossibile, quando ci colleghiamo ad un sito o configuriamo il nostro client di posta elettronica, possiamo scrivere il suo nome "mnemonico" (facile da ricordare), ad esempio www.yahoo.it o mail.tiscali.it o [ftp.tin.it](ftp://tin.it) ecc.. Esistono infatti dei server (i server DNS), che associano al nome mnemonico di ogni host il suo indirizzo IP.

Il nome di un host è composto da **più campi, divisi da un punto**

1. il **suffisso finale** (".it " nell'esempio precedente) indica:

il **tipo di utilizzo del dominio**:

- .com per i siti commerciali;
- .edu per le istituzioni scolastiche;
- .gov per le istituzioni governative...

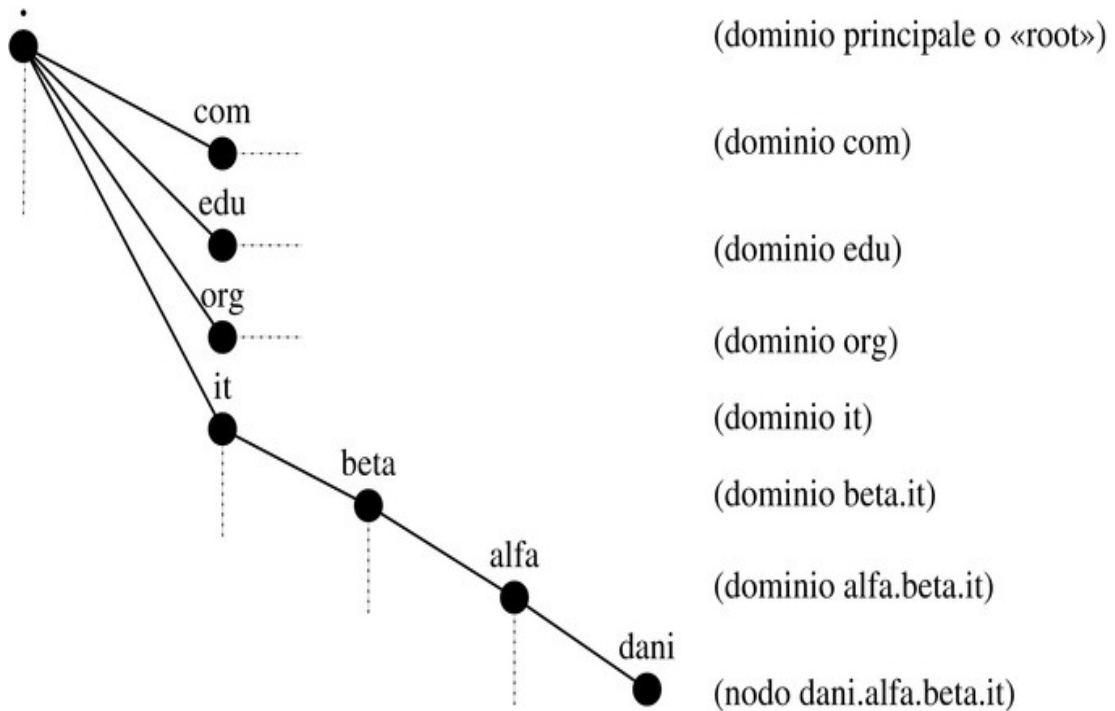
oppure **domini nazionali**:

- .it per i domini in Italia;
- .fr per la Francia;
- .uk per la Gran Bretagna...

2. il **nome del sito** (yahoo, tiscali e tin nell'esempio);

3. il **servizio** (www, mail, ftp in questo caso).

Non è una norma, ma indicando con *www* i siti web, *ftp* i server ftp, *mail* i server di posta ecc, si evita confusione rendendo la vita più semplice agli utenti...



La suite di protocolli TCP/IP

È la base di tutti i protocolli utilizzati sui nostri pc casalinghi per accedere ad internet.

IP (Internet Protocol) rappresenta il protocollo di base della Internet suite. Fornisce il servizio di consegna dei pacchetti esegue le operazioni necessarie al trasporto dell'informazione senza connessione.

TCP (Transmission Control Protocol) serve a garantire affidabilità e certezza di arrivo dei dati. È un protocollo a connessione.

Time	Event	DIAGRAM
t	Host A sends a TCP SYNchronize packet to Host B	
$t+1$	Host B receives A's SYN	
$t+2$	Host B sends its own SYNchronize	
$t+3$	Host A receives B's SYN	
$t+4$	Host A sends ACKnowledge	
$t+5$	Host B receives ACK. TCP connection is established.	

UDP (User Datagram Protocol) è usato per servizi dove sia l'affidabilità che la gestione dello scambio dati sono demandati all'applicazione (user è in questo senso).

ICMP (Internet Control Message Protocol) serve alla diagnostica della connessione. È usato per controllare che un computer in rete sia raggiungibile, oppure per notificare errori di instradamento (routing) sulla rete.

Per capire meglio di cosa parliamo facciamo un esempio che risulterà utile:

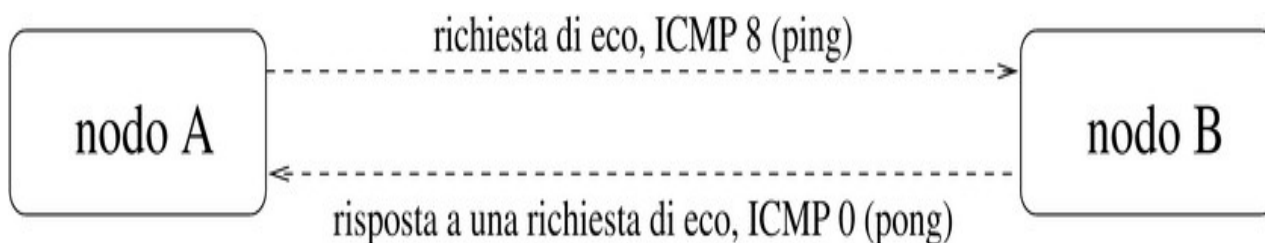
aprite una console sul vostro PC e digitate questo comando

```
ping 66.102.9.104
```

avrete come risposta

```
PING 66.102.9.104 (66.102.9.104) from 127.0.0.1 : 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=0.352 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=255 time=0.108 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=255 time=0.114 ms
```

come vedete con l'invio di un semplice pacchetto si ottengono delle informazioni, ossia se il computer è acceso e collegato in rete, il tempo di transito della connessione, indicazione della velocità di trasmissione dei dati, e sulla qualità della connessione, data dalla regolarità nel tempo di round trip e dalle statistiche stampate al termine del comando ping, che informano sul numero di pacchetti trasmessi, ricevuti e percentuale dei pacchetti persi.



La pila protocollare

L'accesso alle funzionalità della comunicazione avviene a vari livelli di astrazione a partire da quello più basso che è quello dei segnali coinvolti nell'effettiva comunicazione (la cui natura e tipologia dipendono dalla natura del mezzo di trasmissione) fino a quello più elevato che è quello che "vedono" le applicazioni che vogliono comunicare attraverso la rete.

In questo modo un'applicazione che intende inviare delle informazioni sulla rete, utilizzerà l'interfaccia software messa a disposizione dal livello più alto, che si preoccuperà di trattare opportunamente le informazioni passandole al livello immediatamente inferiore e così via fino ad arrivare al livello più basso in cui i segnali logici saranno trasformati in segnali elettrici o elettromagnetici e quindi inviati sulla rete.

Allo stesso modo, l'interfaccia di rete che riceve le informazioni le tratterà in maniera opportuna passandole man mano ad un livello sempre più elevato, fino ad arrivare all'applicazione di destinazione. Ogni livello passa le informazioni a quello immediatamente inferiore (in trasmissione) o superiore (in ricezione) tramite un insieme di funzioni che costituiscono l'interfaccia di comunicazione tra un livello e l'altro.

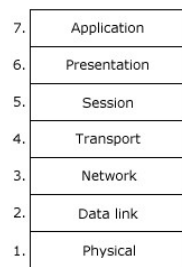
Per riassumere, un pacchetto che entra nel nostro computer fa questo percorso, dal basso verso l'alto:

```
Applicazione (UDP/TCP)  
Protocolli superiori (ICMP/UDP/TCP)  
Protocollo IP  
Driver (ethernet/ppp)  
Interfaccia fisica
```

ed ovviamente il percorso contrario nel caso di pacchetto che esce.

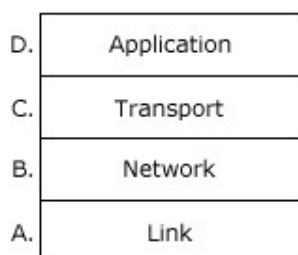
ISO/OSI:

Il modello che è stato la pietra miliare nella definizione degli stack di protocolli di rete, ma di cui non esiste nessuna implementazione pratica, è il modello OSI (Open System Interconnection) proposto da ISO2, che si suddivide nei 7 livelli di seguito elencati



TCP/IP

Per le reti ci sono stati vari standard di protocolli di comunicazione che ovviamente hanno portato a problemi di interconnessione tra reti diverse. Quello che oggi prevale (e sarà destinato a farlo sempre di più) è il TCP/IP, una suite di protocolli nata con Internet, per le reti geografiche (WAN), poco affidabili rispetto alle LAN, ma che ha buone prestazioni anche su LAN (sebbene su LAN esistono dei protocolli più efficienti in termini di rapporto tra i codici di controllo e le effettive informazioni da trasmettere).



Vedremo in seguito, parlando di sicurezza, che più in alto arriva un pacchetto e più strati software deve attraversare, con la conseguenza che è più facile trovare un errore. Vedremo più avanti cosa può significare un errore nel software quando sono coinvolti i protocolli di network.

A questo punto sappiamo per grandi linee come avvengono le connessioni in una rete, sappiamo anche, avendo magari ascoltato trasmissioni televisive o letto giornali più o meno tecnici, che spesso avvengono degli incidenti, dei problemi causati da "problemi di sicurezza"...

COSA SI INTENDE PER SICUREZZA NELL'AMBITO DI UNA RETE DI CALCOLATORI?

Si intende la legittima aspettativa che ha l'utente **autorizzato all'uso di un computer** di usufruire dei servizi, dei file, dei documenti che il computer mette a disposizione. Nel momento in cui hanno accesso a documenti e servizi persone non autorizzate si ha quello che si chiama *"buco di sicurezza"* (della rete o del calcolatore).

Ma quando un dato è effettivamente trattato in modo "sicuro" ? Quali caratteristiche deve avere?

- **Riservatezza** - le informazioni devono essere fruibili soltanto dal destinatario e non da altri;
- **Integrità** - il destinatario deve essere in grado di verificare se le informazioni che gli sono arrivate hanno subito delle modifiche rispetto a quelle inviate dal mittente;
- **Autenticazione** - il destinatario deve essere in grado di verificare se le informazioni ricevute sono state effettivamente inviate da chi afferma di essere il mittente;
- **Non ripudiabilità** - il mittente che ha inviato le informazioni non può disconoscere di aver inviato le informazioni stesse;

Purtroppo l'esperienza ci insegna che, seppure un sistema possa essere amministrato con tutti i criteri di sicurezza possibili, esiste sempre la possibilità che un attacco riesca a superarli, per cui occor-

re prevedere ogni volta sia possibile sistemi di ripristino dei dati, di controllo delle intrusioni, ridondanza hardware ecc.

Quando colleghiamo in rete un nostro elaboratore, rendendolo accessibile al pubblico, ci assumiamo delle responsabilità: altri sistemi potrebbero risultare danneggiati da un attacco condotto con successo dal nostro PC, vittima a sua volta di una intrusione dall'esterno. Quindi l'aspetto "sicurezza" non può essere ignorato, anche quando non lo si ritiene importante per se stessi.

IN CHE MODO UN HOST PUÒ ESSERE VIOLATO?

I modi sono tanti e diversissimi fra loro, come pure diversi sono i tipi di intrusione dal punto di vista dello scopo. Ci sono le intrusioni per danneggiare, quelle per rubare dati e quelle per usare il nostro computer a fini poco etici a nostra totale insaputa.

Vediamo quali sono le casistiche ed i problemi più comuni:

1. Computer poco protetti

Se per intuito avete pensato a computer senza firewall, avete intuito male. Per poco protetti si intende computer in cui gli *accessi leciti* sono poco o per nulla protetti.

La maggior parte delle intrusioni è dovuta a mancanza di politiche di protezione adeguate. Server mal configurati, password semplici e prevedibili, o addirittura assenti.

Spesso in casa o in ufficio non usiamo password, o sappiamo quelle dei colleghi, o le scriviamo su un post-it, o sotto la tastiera... lo faremmo con il PIN della carta di credito?

2. Errori nel software

E' il sistema più subdolo e pericoloso di intrusione. A differenza del punto precedente, l'intrusione avviene anche se le nostre password e configurazioni sono blindate.

Prendiamo un **esempio reale: il virus Nimda**. Questo virus ha usato vari metodi per propagarsi e per infettare altri computer, tutti basati su due bug in software ben noti: un web browser ed un web server.

Per infettare i pc degli utenti Nimda sfrutta un errore di programmazione di un software comunissimo perchè preinstallato in noti sistemi operativi commerciali.

Detto in modo impreciso, ma essenziale, grazie a questo errore di programmazione, relativo ad una parte che si occupa di processare gli allegati, inganna il programma facendogli credere che l'allegato sia un contenuto multimediale, in modo che questo venga aperto in anteprima, cioè vada in esecuzione senza che l'utente abbia modo di impedirlo.

Una volta infettato il computer, Nimda si autospedisce come allegato agli indirizzi di posta elettronica che trova nella rubrica e nella cache delle pagine web, estraendoli dai link mailto: contenuti nelle pagine stesse.

Se poi trova una connessione Internet, cerca dei siti web dove si installa, sfruttando in questo caso un errore nel programma server nella decodifica degli URL, modificando pagine web sostituendole con false form.

Da questi siti compromessi si propaga ad altri computer quando utenti ignari visitano quelle pagine.

Altro tipo di danno che può essere causato è l'**interruzione del servizio**, o Denial of Service (DoS).

Se un server web di un certo tipo contiene un errore che lo fa andare in crash quando riceve una specifica richiesta, qualcuno potrebbe sfruttare questo errore per mandare fuori servizio i server della concorrenza.

Se poi i server vengono riavviati, basta rimandare la richiesta illegale per rimandarli down (in gergo si dice così quando un computer o un servizio di rete viene fermato o spento), rendendoli completamente inutilizzabili.

Immaginate l'entità del danno se questo succede ad un sito di Internet Banking o di e-commerce...

Altri tipi di errori comprendono ad esempio il famigerato "buffer overflow" di cui avrete sentito parlare. Di solito questo tipo di errore è sfruttato per far eseguire al computer vittima codice binario contenuto nel pacchetto stesso, che può essere un pacchetto perfettamente legale per il protocollo, ma improvvisamente dal software.

Il trucco dei pacchetti con contenuto di lunghezza errata veniva usato anni or sono in server tipo sendmail (gestore di posta elettronica) o in bind (server DNS).

E' recente la segnalazione di un problema simile nel codice che gestisce le immagini JPEG in Windows.

Il codice ha un errore che può essere usato per far eseguire dati dell'immagine errata come se fossero un programma. Un malintenzionato può creare una immagine particolare che se visualizzata da un browser causa l'errore e manda in esecuzione il codice nascosto dentro l'immagine. Dato che questo codice viene eseguito ad un livello privilegiato può virtualmente fare di tutto. In questo caso addirittura non c'è neanche bisogno di avere servizi di rete attivi, basta navigare su Internet e andare in un sito contenente le immagini deleterie.

Altro esempio di attacco realizzato con un pacchetto perfettamente legale per il protocollo, ma deleterio per il server, è stato usato dal worm SQHell (conosciuto anche come SQL Slammer o Sapphire).

Questo virus (worm) si è propagato tramite UDP verso la porta 1434 dei server, e la semplice ricezione del pacchetto ha comportato l'infezione su tutti i server che utilizzavano versioni di programmi aventi lo stesso bug (da notare che questo attacco, meno di un anno or sono ha paralizzato per giorni molti siti istituzionali e di aziende di pubblici servizi).

Esiste una sola soluzione in questi casi: **correggere il software errato.**

Come? Applicando quella che in gergo è chiamata "patch" (pezza). Se il software è commerciale, si è sottoposti alla prontezza del produttore, che non sempre è ricettivo su questo fronte, anche se in questi ultimi tempi qualcosa è cambiato, anche grazie ad una maggiore coscienza degli utenti.

3. Uso improprio di protocolli e servizi

In questo caso, purtroppo, non c'è una negligenza di qualcuno o un errore nel software. Semplicemente, qualche malintenzionato sfrutta meccanismi propri di un protocollo o uno specifico servizio per creare problemi o per generare confusione. E proprio per questo motivo non c'è una difesa specifica. Non ci sono configurazioni da correggere o patch da applicare.

In genere comunque, quando si evidenzia un problema di questo tipo, l'implementazione dei sottosistemi di rete dei sistemi operativi, la configurazione e il funzionamento degli apparati di rete o addirittura le regole che definiscono i protocolli possono adeguarsi (anche molto rapidamente) e superare questo genere di malfunzionamenti.

TIPI DI INTRUSIONE

Vediamo quindi rapidamente come esistano dei software malevoli che, sfruttando i problemi sopra elencati, possono causare problemi:

1. Virus

La parola virus è diventata di uso generico, indicando un software capace di autoreplicarsi, diffondersi e provocare danni all'insaputa del legittimo proprietario/utente, sfruttando le risorse disponibili all'interno del computer ospite, esattamente come la loro controparte biologica da cui prendono il nome.

Altro non è che un programma che si attiva con l'esecuzione da parte dell'utente o di un altro programma infetto o del programma che è il virus stesso. Si propaga in vari modi, e quando la propagazione avviene attraverso la rete si parla di worm.

Possono contenere virus: allegati di posta mascherati da testo o screensaver, file compressi, dischetti, file scaricati da reti Peer to Peer. Possono sfruttare buchi nella sicurezza di un programma di posta elettronica per attivarsi alla semplice lettura del messaggio, anche senza aprire l'allegato, sfruttando la funzione di anteprima. Il grado di pericolosità varia dalla sola propagazione, quindi consumo di risorse, al danneggiamento irreparabile di file, con conseguente blocco del funzionamento del sistema operativo vittima.

2. Trojan

Devono il loro nome al Cavallo di Troia, per il loro modo di attivazione. Si presentano come programmi utili per qualche cosa, che all'interno contengono invece codice virale. A volte sono versioni di programmi noti che sono stati modificati per diventare veicolo di infezione. L'incauto utente viene indotto in vari modi ad installare un programma che contiene il trojan, attivando così anche la funzione dannosa. Di solito non hanno un meccanismo proprio di propagazione, sfruttando appunto l'inganno dell'apparenza "utile".

3. Worm

Si propagano senza intervento diretto dell'utente, attraverso la rete, per cui è sufficiente essere connessi, anche senza navigare o leggere posta elettronica. Sfruttano errori nel software di servizi di rete per installarsi nei computer e da lì cercano altre vittime per infettarle. I danni possono andare dal consumo di risorse, alla distruzione di dati, al blocco del servizio.

Qui il firewall può molto, ma dipende dal servizio di rete che viene attaccato. Il worm Blaster sfrutta un errore nel servizio RPC di Windows NT/2000/Xp in ascolto sulla porta 135/TCP. Se si chiude questa porta a qualsiasi accesso, si impedisce a Blaster di infettare il PC.

Non sempre però le cose vanno così bene. La famiglia di worm descritta in [Gaobot](#) usa fra l'altro errori nel servizio di condivisione disco e password deboli sulle condivisioni stesse. Le porte di questi servizi sono la 139/TCP e 445/TCP ed entrambe servono per accedere ai file ed alle stampanti condivise su una rete. Quindi di solito il firewall lascia libero accesso a questi servizi se l'accesso proviene da PC nella stessa sottorete. Il problema quindi sorge quando si usano collegamenti a provider non ADSL e non PPP, ma in LAN distribuita detta MAN, con i computer degli utenti connessi con una normale scheda di rete ethernet.

4. Backdoor

Letteralmente "porta sul retro". Era una pratica usata da molti sviluppatori quando temevano di non essere pagati per il loro lavoro, o quando si voleva avere accesso ai dati gestiti dall'applicazione aggirando le protezioni e l'accesso previsto per i normali utenti, prevenendo il caso non infrequente che l'utente rimanesse "chiuso fuori" da qualche manovra errata.

Da qualche tempo, molti virus e worm installano delle backdoor sul computer vittima creando dei punti di accesso da cui è possibile prendere il controllo completo del computer dall'esterno ad insaputa della vittima. Oppure collegano il computer ad un server IRC da cui il virus può prendere ordini. E' una tecnica usata negli ultimi virus in circolazione per poi coordinare attacchi in massa a siti pubblici.

5. Dialer

Non sarebbero virus veri e propri, ma per il particolare comportamento malevolo vengono classificati comunque come intrusioni.

Attraverso falle nei browser, siti web poco "etici" installano dei programmi per la connessione via modem telefonico (da cui deriva il nome dialer, dall'inglese dial, comporre un numero sul telefono) che modificano le impostazioni dell'account utente, chiamando numeri internazionali o con tariffe a valore aggiunto, con prezzi che arrivano a 3 euro al minuto, senza avvisare l'utente. Spesso vengono usati anche trucchi come azzerare il volume del modem in modo da non far sentire che si sta componendo un numero differente. Ne esistono alcuni che arrivano a sostituire i driver del modem, per cui l'utente non ha nessun sentore che qualcosa è cambiato.

6. Spyware

Questa è una categoria piuttosto recente di intrusioni, ed è relativamente pericolosa non in modo diretto, quanto per problemi di privacy. In sostanza questo tipo di intrusioni sono realizzate attraverso software ritenuti utili, analogamente al caso dei trojan, che invece di far danni alla maniera dei virus, si limitano a spiare alcune attività dell'utente durante la navigazione su Internet, comportamento da cui deriva il nome: *spy software*.

Vengono raccolte informazioni sui siti che visitate, le parole chiave che inserite nei motori di ricerca, i dati che

inserite nei moduli che riempite sul web e così via. I dati raccolti da questi programmi vengono silenziosamente inviati ad un server remoto del produttore del software che rivende questi dati statistici a chi interessa. Tutto questo spesso senza informarvene e ovviamente senza il vostro consenso. Alcuni tipi di spyware collezionano l'elenco del software installato sul computer o dei file multimediali, o ancora gli indirizzi di posta che avete nella vostra rubrica. Capite bene che è un vero e proprio spionaggio, e nel caso di dati sensibili costituisce un reato, oltre al fatto che si viene tenuti all'oscuro di questo comportamento.

7. Keylogger

E' l'antenato dello spyware, e di solito va in combinazione con virus, worm, rootkit o trojan. Una volta installato nel vostro computer, memorizza tutte le sequenze di tasti che digitate, e le invia ad un server remoto, dove chi ha creato il keylogger analizza le sequenze ed estrae cosette come password di accesso e codici di carte di credito. Può usare una backdoor o una mail per spedire i dati collezionati.

8. Combinazioni micidiali

Questa categorizzazione in realtà è riduttiva in molti sensi, dato che le minacce in circolazione sono combinazioni dei precedenti codici malevoli.

Il virus Blaster (e i suoi parenti stretti Sasser e Korgo) è un worm che si diffonde installando una backdoor TFTP, creato per sferrare un attacco DDoS. La famiglia di worm Gaobot/Agobot/Sdbot una volta installati creano una backdoor collegandosi via IRC ad un server remoto, e nel cercare altri computer da infettare in rete causano continui DoS ai server che condividono file e stampanti attraverso il consumo eccessivo di banda. Alcune varianti contengono spyware e keylogger.

Ad esempio l'interruzioni di servizio (**Denial of Service o DoS**) E' un tipo di intrusione realizzata senza toccare direttamente il computer vittima, sfruttando modi di funzionamento dei servizi di rete o falle nei server di rete.

Se si mandano milioni di pacchetti TCP SYN al secondo ad un server si può arrivare a bloccarlo (se il programmatore non ha previsto questa eventualità, cosa non infrequente) o ad impedire ad altri utenti di accedere al servizio (da qui il nome Denial of Service che significa "rifiuto del servizio").

Se l'attacco viene portato usando molti computer contemporaneamente, magari infettati con un virus che installa una backdoor, viene chiamato DDoS Distributed Denial of Service per indicare appunto la natura multipla dell'attacco. I virus della famiglia MyDoom sono progettati per questo tipo di attacco.

STUDIARE UNA POLITICA DI DIFESA

Vediamo ora, sempre molto rapidamente, quali programmi esistano per analizzare la nostra rete e le nostre macchine per conoscere e prevenire i problemi che si possono verificare, in modo da utilizzare al meglio gli strumenti esistenti per garantire una protezione accettabile e sufficienti garanzie nell'integrità dei nostri dati.

Sistemi di protezione ed analisi, Strumenti per il controllo e l'analisi del traffico IP

L'analisi del traffico della rete, sia per mezzo dell'intercettazione di tutti i pacchetti che attraversano una rete fisica, sia per mezzo del controllo di ciò che riguarda esclusivamente una singola interfaccia di rete del nodo locale, è molto importante per comprendere i problemi legati alla sicurezza e per scoprire inconvenienti di vario genere.

Rimandando ad un livello successivo la spiegazione nel dettaglio e lo studio necessario a progettazione di una infrastruttura di controllo, installazione degli apparati e del software, configurazione, messa a punto e manutenzione, vediamo, in modo molto molto rapido, i programmi che possono essere utilizzati:

1. Netstat

Mostra la situazione delle porte TCP, in particolare quelle dei servizi in ascolto.

2. Fuser

Fuser è un programma specifico per sistemi GNU/Linux, che consente di individuare facilmente il processo elaborativo che ha aperto un file, oppure una porta (TCP o UDP).

3. Tcpdump

Tcpdump è lo strumento fondamentale per l'analisi del traffico che avviene nella rete fisica a cui si è collegati. Permette sia di ottenere una visione sintetica dei pacchetti, sia di visualizzarne il contenuto

4. Ethereal

Ethereal è un programma per l'analisi del traffico di rete, fino al livello due del modello ISO-OSI (collegamento dati), riuscendo a riconoscere all'interno di questo una serie di protocolli al livello tre e quattro del modello ISO-OSI (rete). In particolare, individua correttamente molti protocolli collegati a IPv4 e Ipv6.

Ethereal è pensato principalmente per accumulare il traffico intercettato, allo scopo di consentire un'analisi dettagliata in un momento successivo; nello stesso modo è predisposto per accedere a informazioni di questo genere accumulate da programmi diversi, così come è in grado di esportare i propri dati in formati alternativi.

Ethereal consente anche una visualizzazione in tempo reale del traffico in corso, in modo analogo a quanto fa IPTraf, con la differenza che le informazioni fornite sono molto più chiare. In questo senso, Ethereal è un ottimo strumento didattico per lo studio delle reti.

Ethereal viene usato normalmente attraverso il sistema grafico X e deve funzionare con i privilegi dell'utente root, per poter accedere direttamente all'interfaccia di rete da sondare.

5. Snort

Snort è un IDS (Intrusion Detection System) cioè un programma che consente di rilevare eventuali tentativi di intrusione in un sistema tramite il confronto delle "impronte" dei pacchetti di rete in arrivo e quelle conservate in un database (rules). Rilevata un'attività sospetta può svolgere sia compiti di registrazione che di avviso all'amministratore.

Snort è stato progettato per funzionare in 3 modi differenti:

-Sniffer intercetta i pacchetti che viaggiano nella rete e li visualizza in console.

-Packet Logger salva su disco locale i pacchetti

-Network Intrusion Detection analizza il traffico di rete attraverso delle regole customizzabili ed esegue operazioni configurabili in caso di corrispondenza.

6. Nessus

Nessus è un security auditing tool, cioè uno strumento per la verifica della sicurezza. Cerca, in base a un archivio aggiornato, quali tipo di falle sono presenti nel vostro sistema, suggerendo il metodo migliore per la sua risoluzione. Nessus è uno strumento molto potente ed è stato sempre considerato efficiente nel rilevare i problemi più noti.

Effettua scansioni per i sistemi Linux, BDS, Solaris, Unix e crea report completi in formato HTML, XML, LATEX, e ASCII. Supporta GTK.

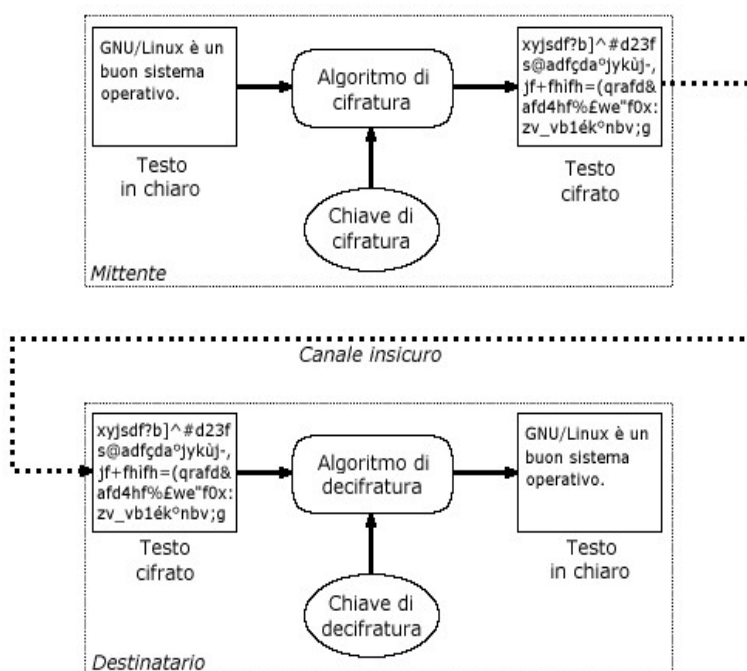
SISTEMI SICURI DI TRASMISSIONE

La crittografia

dal greco $\kappa\rho\upsilon\pi\tau\acute{o}s$ = nascosto) e $\gamma\rho\alpha\phi\epsilon\iota\nu$ = scrivere) è la scienza che studia i metodi per “camuffare” le informazioni affinché chi dovesse venirne in possesso non sia in grado di risalire all’informazione originale senza la chiave di decodifica.

La chiave è un parametro che, fornito al meccanismo di cifratura, è in grado di permettere la decodifica corretta dell’informazione.

Questi metodi garantiscono la protezione delle informazioni trasmesse da un mittente ad un destinatario attraverso un canale insicuro, al quale chiunque può accedere, in particolare forniscono un certo livello di riservatezza (o privacy) alle informazioni trasmesse



La cifratura a **chiave asimmetrica** utilizza **due chiavi diverse**: una per la cifratura dell’informazione e l’altra per la decifratura. Le informazioni cifrate con una delle due chiavi possono essere decifrate solo con l’altra. Le due chiavi prendono generalmente il nome di chiave pubblica e chiave privata dal fatto che una delle due chiavi deve essere fornita a tutti quelli dai quali si vogliono ricevere messaggi cifrati, mentre l’altra deve essere tenuta segretamente nascosta dal proprietario della coppia di chiavi.

Il messaggio viene cifrato dal mittente per mezzo della chiave pubblica del destinatario ed inviato al destinatario stesso, il quale è in grado di decifrarlo poiché è a conoscenza della sua chiave privata

GNU Privacy Guard

GNU Privacy Guard, o più comunemente GNUPG o ancora GPG, è una suite per la gestione di chiavi crittografiche e della cifratura stessa. Tale strumento costituisce il backend utilizzabile da qualunque altra applicazione che desideri far uso di chiavi per cifrare/decifrare informazioni crittografate. GPG è un sostituto di PGP (Pretty Good Privacy), un’applicazione creata da P. Zimmermann nel 1991, implementa il protocollo OpenPGP (RFC 2440) utilizzando soltanto algoritmi di cifratura non coperti da patent (DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 e TIGER). Le chiavi sono memorizzate in insiemi detti portachiavi o keyring che sono rappresentati da file all’interno della directory `~/gnupg`.

I certificati digitali

Un certificato digitale è un documento che attesta la relazione di appartenenza di una chiave pubblica ad certa una entità (una persona, una azienda, una macchina, ...). Tale legame è garantito dall'ente emittente il certificato, ovvero una terza parte fidata che costituisce l'autorità di certificazione o Certification Authority (CA).

Un certificato digitale contiene la chiave pubblica ed il nominativo dell'entità di cui viene garantita la corrispondenza, indicazioni relative all'algoritmo utilizzato per la generazione della chiave, una data di scadenza, il nome della CA che ha rilasciato il certificato, il suo numero di serie e la firma digitale della CA stessa a garanzia del fatto che il certificato digitale è stato rilasciato proprio da tale CA. In questo modo, chiunque può verificare l'autenticità del certificato con la chiave pubblica della CA e quindi essere sicuro che la chiave pubblica contenuta nel certificato appartenga proprio all'entità specificata dal certificato stesso.

La firma digitale

La firma digitale è una garanzia del messaggio o documento elettronico, alla stregua della sottoscrizione di un documento cartaceo, attestandone con certezza l'integrità, l'autenticità e la non ripudiabilità anche dal punto di vista legale, poiché la legislazione italiana attribuisce ad un documento elettronico con firma digitale lo stesso valore dello stesso in forma cartacea sottoscritto con firma autografa (v. art. 15 comma 2 della legge n. 59 del 15/3/1997 "Bassanini-1", D.P.R. n. 445 del 28/12/2000, D.P.C.M. 08/02/1999)

SSH - Secure SHell

Il protocollo SSH permette di accedere in maniera sicura alla shell di una macchina remota. Questo fa sì che tale protocollo sia molto utilizzato dagli amministratori di rete.

Il server che gestisce la comunicazione cifrata è il daemon sshd.

Il comando ssh è un client di comunicazione che, utilizzando il protocollo SSH (SSH1 o SSH2), permette di effettuare il login su una macchina remota. Se il login va a buon fine si avrà l'accesso alla shell definita per l'utente che ha effettuato il login e si potrà così interagire con il sistema remoto come se si impartissero i comandi direttamente sulla sua tastiera.

SISTEMI PER LA PROTEZIONE

I filtri

In commercio esistono apparecchi dedicati a svolgere il compito di filtro, per separare le reti interne da internet. Spesso sono denominati "firewall hardware" per contraddistinguerli dai software che svolgono tale compito su macchine con sistemi operativi multipurpose, utilizzabili cioè per poterci lavorare in generale, che possono avere, come GNU/Linux, un firewall software. Questo non deve trarre in inganno poiché la politica di firewalling è comunque gestita attraverso un insieme di regole che vengono attuate attraverso un software.

Esistono almeno due tipologie di filtro:

1. **Packet filter** - esegue un filtraggio sui pacchetti che lo attraversano, dal livello fisico fino al livello di trasporto dello stack OSI . Ad esempio, un firewall di questo tipo può scartare i pacchetti che arrivano da interfacce di rete con un determinato indirizzo IP, o far passare soltanto il traffico relativo a determinate porte (TCP o UDP).
2. **Proxy server** - esegue un filtraggio sui pacchetti che lo attraversano, ai livelli più alti dello stack OSI.

Un firewall di questo tipo (spesso denominato soltanto proxy server), può permettere, oltre alla gestione di caching delle pagine visitate, anche l'accesso o meno a determinate pagine web basandosi sul contenuto delle stesse.

Per realizzare un firewall è sufficiente un calcolatore anche di tipo non recente (un compatibile Intel 80486

con 16 Mbyte di RAM, ad esempio) ed una distribuzione con kernel Linux recente in quanto il firewall non necessita di interfaccia grafica. Un firewall ha usualmente almeno due schede di rete, una viene collegata verso l'esterno ed una collegata con la nostra rete interna.

Proxy Server

Il filtro a livello applicazione viene comunemente chiamato "server Proxy" o più semplicemente "Proxy"; questi tipi di server comunicano con la rete esterna per conto degli host della rete interna, in altre parole i Proxy controllano il traffico tra due reti.

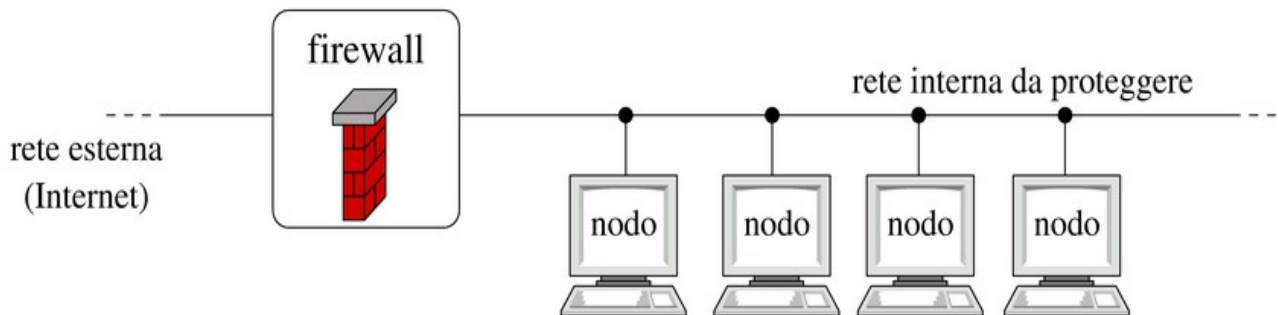
Con questo tipo di filtri abbiamo una netta distinzione tra rete interna e esterna, infatti ogni pacchetto viene ricevuto processato e inoltrato dal Proxy sia verso l'interno che verso l'esterno, non c'è quindi un collegamento fisico tra le due reti. I firewall a livello applicazione operano sui protocolli quali HTTP, FTP, SMTP, BOOTP, TFTP, etc. abilitandoli disabilitandoli o limitandone l'uso.

A differenza dei firewall qui abbiamo un server Proxy per ogni protocollo interessato: http, Telnet, Gopher, Ftp; i server Proxy più diffusi tra sistemi UNIX sono TIS, SOCKS, Squid.

Per l'uso dei server Proxy bisogna usare applicazioni client che li supportino, esempio tutti i client Web moderni (Netscape Navigator, Mozilla Navigator, Firefox, Konqueror, Internet Explorer) è possibile settare il proxy http per la navigazione.

Il funzionamento di un firewall

Il principale lavoro di un firewall è di esaminare ogni pacchetto che transita nel suo spazio di rete e di controllare che questi pacchetti siano rispondenti a certe restrizioni, chiamate anche *regole del firewall*. I pacchetti che soddisfano questi requisiti sono liberi di passare, quelli che non sono conformi vengono scartati o rifiutati.



Di solito ha una struttura piuttosto semplice, come semplici sono le regole che è in grado di applicare.

Ad esempio, per il protocollo TCP potrebbe essere impostato semplicemente per rifiutare o eliminare tutti i pacchetti in arrivo che abbiano il flag SYN impostato, ossia di richiesta inizio connessione. Il risultato è che chiunque richieda una connessione al nostro computer, si vede rispondere o "connection refused" o "connection timed out".

Ma se non abbiamo servizi in ascolto?

In questo caso il firewall non aggiunge nulla a quello che fa il computer già di suo, ossia è inutile e dannoso, in quanto aggiunge uno strato software al gestore del protocollo IP, o subito prima. Se il gestore IP fa già il suo lavoro, scartando richieste di connessione a servizi inesistenti, mettere un software che prende comunque i pacchetti e li esamina, può essere nefasto.

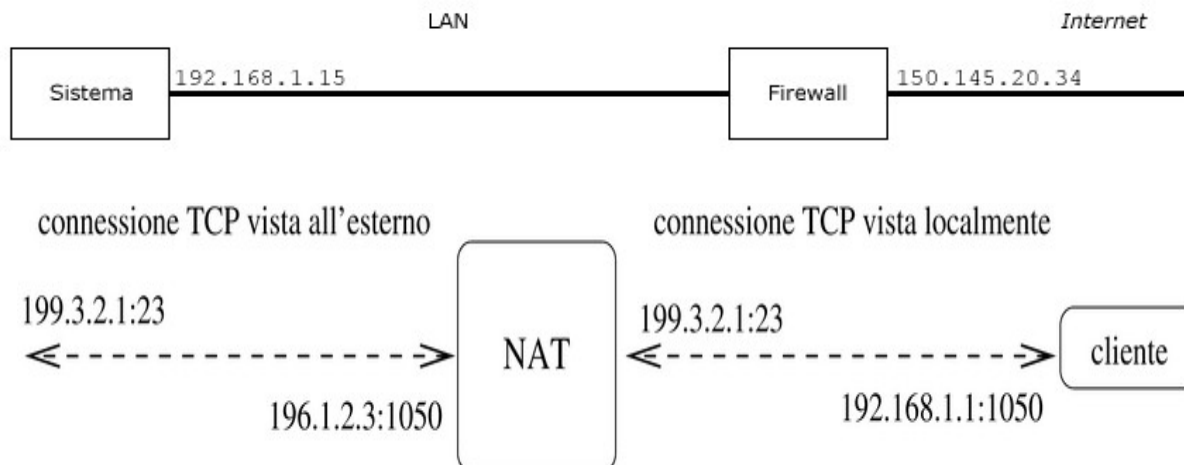
Si è infatti verificato il caso di un software di firewall che a causa di un errore di programmazione era vulnerabile a certe condizioni. Installandolo su un computer senza servizi in listen e quindi inattaccabile dalla rete, lo si rendeva vulnerabile.

Facciamo un altro esempio: abbiamo un computer con due interfacce di rete, una per Internet ed una sulla nostra rete interna. Sul computer è in esecuzione un server FTP che può essere usato da tutti gli utenti interni, mentre non deve essere accessibile da Internet. In questo caso il firewall può essere utilizzato (può in quanto non è il solo modo per fare la stessa cosa), e deve essere impostato in modo da bloccare i pacchetti TCP SYN provenienti dall'esterno e diretti sulla porta 21, quella dell'FTP.

Se sullo stesso computer è attivo anche un server HTTP che deve essere accessibile sia dall'interno che dall'esterno, allora il firewall conterrà una regola che permette il transito a tutti i pacchetti TCP diretti alla porta 80.

NAT

I firewall usano anche sistemi di traduzione e manipolazione dei pacchetti, chiamati NAT (Network Address Translation), in modo da nascondere gli indirizzi dei computer interni. Il vantaggio è doppio: da un lato si ha la protezione perché i computer interni non sono mai raggiungibili, e dall'altro si usa un solo indirizzo sulla rete esterna, cosa che vista la penuria di indirizzi IP su Internet non fa mai male.



Netfilter

Un sofisticato sistema di filtraggio dei pacchetti di rete è integrato nel kernel di Linux ed è controllabile con le utility iptables, che permettono di inserire, cambiare, cancellare regole, basandole su un numero cospicuo di parametri, relativi al protocollo, alle interfacce di rete, alla sorgente ed alla destinazione, al tipo di servizio, ai flag TCP e tantissimi altri.

L'uso di iptables presuppone una buona conoscenza dei protocolli IP e del concetto di regole di filtro dei firewall, esistono delle interfacce grafiche per aiutare un po' nella configurazione, ma è comunque necessario sapere cosa fare.

Di contro, la possibilità di inserire regole estremamente dettagliate e mirate, permette di calibrare il comportamento del firewall di Linux in modo efficiente e professionale.

SISTEMI PER LA VERIFICA

Verifica dell'integrità dei file

Attraverso l'accumulo di codici di controllo è possibile verificare l'integrità di file e di directory, contro l'uso improprio del sistema, comprendendo eventualmente l'azione di un virus, un worm, un intruso.

AIDE & tripwire

AIDE e Tripwire sono programmi per la verifica dell'integrità dei file; attraverso il confronto con le informazioni accumulate precedentemente segnalano le aggiunte, le rimozioni e le alterazioni di file e directory. Si tratta di strumenti preziosi per scoprire gli utilizzi impropri del sistema o l'azione di cavalli di Troia.

POLITICHE DI SICUREZZA

Come detto, e come avrete capito, la sicurezza del vostro computer non è solo nel firewall, o solo nelle password, o nell'antivirus o chissà dove, è anche, e soprattutto, nel *vostro comportamento*.

Per cui quali sono le azioni, che ci aiuteranno a migliorarlo, aumentando la sicurezza del sistema?

1. Chiudere le porte

che non servono disattivando i servizi inutili e gestendo il software

Usare il comando netstat per vedere le porte di rete aperte, e decidere quali non servono. Il modo dipende dal sistema operativo e dalla versione.

2. Non abilitare l'esecuzione di script

e programmi incorporati in documenti ottenuti attraverso la rete (file HTML e posta elettronica principalmente).

3. Tenere aggiornati i software

non solo quelli di rete.

Non deve essere un impegno costante, ma ogni tanto occorre dare una occhiata al sito del sistema operativo che avete installato, e controllare che non siano usciti aggiornamenti critici per la sicurezza, relativi ai software che usate (attenzione, perché installare un aggiornamento di Apache, se non l'avete mai usato, è del tutto inutile, è arrivato anzi il momento di rimuoverlo).

Tenere sotto controllo in particolare i browser web, i programmi per la posta elettronica, i programmi per chat e Instant Messenger, i programmi per scambio file P2P (Peer to Peer) e non dimenticare gli stessi firewall ed antivirus.

4. Non rincorrere l'ultima versione di ogni programma!

Non è detto che sia più stabile, anzi, a meno di non aver bisogno dell'ultima funzionalità (o voler partecipare allo sviluppo), evitare l'installazione di prodotti immaturi e attendere che vengano testati in modo sufficiente dalla collettività;

5. Usare solo software originale

I software non originali ed i vari crack/keygen usati per eliminare le protezioni da copia hanno una probabilità altissima di contenere dell'altro. Molti virus si propagano tramite reti P2P mascherandosi come programmi per togliere protezioni ai software commerciali. Abbiamo giornalmente l'esperienza di persone che, girando per siti "poco raccomandabili" in cerca del crack per un software originale, vengono infettati da dialer e spyware, rimanendo senza il software cercato e col computer inutilizzabile.

Quando potete, usate software libero.

Questo è un problema che tocca poco o nulla chi usa Software Libero, la nostra filosofia è contraria al software pirata, e inoltre non abbiamo bisogno;

6. Non eseguire programmi di dubbia provenienza

può capitare che in una chat qualcuno vi mandi un file, e vi chieda di vedere se funziona. Potete ricevere e-mail con allegati da persone sconosciute, o da persone dalle quali non li aspettate. Se proprio dovete eseguire programmi ricevuti in questo modo, create un utente apposito in GNU/Linux, con pochissimi diritti.

Evitate inoltre di utilizzare software che non sia stato compilato personalmente partendo da sorgenti affidabili, o che provenga da repository non ufficiali e, comunque, evitare di utilizzare software compilato da persone sconosciute o per le quali non si possa verificare l'autenticità dell'origine.

7. Usare un firewall

se avete dei servizi attivi che non volete o non potete disattivare. Se avete una connessione ADSL ed usate un computer per la condivisione della connessione Internet al vostro portatile, o alla rete interna della vostra azienda, viene di solito naturale mettere su quel computer anche un servizio di condivisione disco come Samba o NFS e il servizio di smistamento della posta (anche se per motivi di sicurezza è altamente sconsigliato usare lo stesso computer come firewall e come server).

In questo caso un firewall configurato opportunamente aumenta la protezione del vostro computer e della vostra rete. Ma se un utente della rete interna naviga su un sito "apposito" e contrae un virus o scarica un dialer, il firewall non vi aiuta.

8. Usare l'utente root/Administrator lo stretto indispensabile

perché è pericoloso. Se prendete un virus o un worm mentre siete root, ossia fate girare il browser come root, il virus avrà accesso a tutto il sistema. Se invece usate un utente normale, sarà molto difficile che il virus possa fare danni, in quanto non ha accesso a niente altro che le directory dell'utente.

Certo, GNU/Linux non è molto vulnerabile ai virus, ma ci sono virus per GNU/Linux, pochi, ma ci sono.

9. Non affidarsi ciecamente ad uno strumento solo

un firewall non deve farvi sentire al sicuro. Né vi deve risparmiare di controllare periodicamente gli aggiornamenti per i vostri software, o per i vostri antivirus.

FREE SOFTWARE E SICUREZZA

Ovviamente, uno dei vantaggi del Free Software e dell'OpenSource è di avere a disposizione il sorgente del prodotto ed è quindi possibile risolvere il problema facilmente. Le aziende che vendono software proprietario affermano che avere accesso al codice sorgente facilita la vita dei crackers in quanto essi non si trovano davanti una scatola chiusa dove devono trovare, a tentoni, eventuali errori ma, avendo il sorgente a disposizione, possono trovare un errore e usarlo per tentare di fare breccia sul computer dove il software è installato.

Ma, in realtà, le cose non stanno proprio così in quanto non è solo il cracker ad avere accesso al sorgente ma è tutta la comunità di Internet quindi quello che ha trovato il cracker lo può trovare anche uno sviluppatore serio che mi contatta e mi dice : "Guarda Ciccio che qui hai sbagliato". Ma se anche nessun'altro se ne accorge e se ne accorge solo il cracker, beh tempo 12-24 ore e state sicuri che sulla rete si possono trovare già due o tre patch, soluzioni al problema perché, appunto, c'è il sorgente.

Se invece si tratta di un software chiuso, allora occorre aspettare quei due o tre mesi affinché il produttore rilasci i famosi "service packs" di 20 e oltre MByte.

“Ci vuole tutta una vita per capire che non è necessario capire tutto.”

– (Proverbio cinese)

Riferimenti

- A. N. Kuznetsov, "IP Command Reference" <http://linux-ip.net/gl/ip-cref>
- R. Becker, "ISDN Tutorial" <http://www.ralphb.net/ISDN/>
- R. Day, "xDSL Technology" <http://www.tuketu.com/dsl/xdsl.htm>
- "YoLinux Tutorial - Linux Networking" <http://www.yolinux.com/TUTORIALS/LinuxTutorialNetworking.html>
- A. Menezes, P. van Oorschot, and S. Vanstone "Handbook of Applied Cryptography", CRC Press, 1996
<http://www.cacr.math.uwaterloo.ca/hac>
- Elenco dei FIPS <http://www.itl.nist.gov/fipspubs>
- Sorgenti degli algoritmi di cifratura <http://the-other.wiretapped.net/security/cryptography/algorithms/>
- Sorgenti delle funzioni hash <http://the-other.wiretapped.net/security/cryptography/hashes>
- Dettagli sugli algoritmi di cifratura <http://www.wikipedia.org>
- Legislatura italiana sulla firma digitale <http://www.cnipa.gov.it>
- "Iptables Tutorial" <http://iptables-tutorial.frozentux.net/iptables-tutorial.html>
- "Netfilter Hacking HOW-TO"
- Olaf Kirch, NAG, The Linux Network Administrators' Guide <http://www.netfilter.org/unreliable-guides/netfilter-hacking-HOWTO/index.html>
- the linux network administrators guide
- Terry Dawson, Linux NET-3-HOWTO <http://www.linux.org/docs/ldp/howto/HOWTO-INDEX/howtos.html>
- S. Gai, P. L. Montessoro, P. Nicoletti, Reti locali: dal cablaggio all'internetworking, UTET, edizione Scuola superiore G. Reiss Romoli, 1997
- Charles Hedrick, TCP/IP introduction, 1987 <http://www.ii.uib.no/~magnus/TCP.html>
- Mike Oliver, TCP/IP Frequently Asked Questions <http://www.itprc.com/tcpipfaq/>
- K. Egevang, P. Francis, RFC 1631, The IP Network Address Translator (NAT), 1994
<http://www.ietf.org/rfc/rfc1631.txt>
- Rusty Russell, Linux 2.4 packet filtering HOWTO
- Terry Dawson, Linux NET-3-HOWTO, Linux Networking
- Mark Grennan, Firewalling and Proxy Server HOWTO
<http://www.linux.org/docs/ldp/howto/HOWTO-INDEX/howtos.html>
- Oskar Andreasson, IPTables Tutorial <http://iptables-tutorial.haringstad.com/>
- Axel Boldt, Bliss, a Linux "virus" <http://math-www.uni-paderborn.de/~axel/bliss/>
- Andrea Colombo, Le nuove tecnologie di crittografia http://impresa-stato.mi.camcom.it/im_43/colo.htm
- InterLex, Introduzione alla firma digitale <http://www.interlex.com/docdigit/intro/intro1.htm>
- The GNU Privacy Handbook, 1999 <http://www.gnupg.org/gph/en/manual.html>

Indice

RETI DI CALCOLATORI.....	1
COSA È INTERNET?	1
Come funziona una rete di calcolatori.....	1
L'indirizzamento	2
La suite di protocolli TCP/IP.....	3
La pila protocollare	4
ISO/OSI:.....	4
TCP/IP.....	5
COSA SI INTENDE PER SICUREZZA NELL'AMBITO DI UNA RETE DI CALCOLATORI?.....	5
IN CHE MODO UN HOST PUÒ ESSERE VIOLATO?.....	6
1. Computer poco protetti.....	6
2. Errori nel software.....	6
3. Uso improprio di protocolli e servizi.....	7
TIPI DI INTRUSIONE	7
1. Virus.....	7
2. Trojan.....	8
3. Worm.....	8
4. Backdoor.....	8
5. Dialer.....	8
6. Spyware.....	8
7. Keylogger.....	9
8. Combinazioni micidiali.....	9
STUDIARE UNA POLITICA DI DIFESA.....	9
Sistemi di protezione ed analisi, Strumenti per il controllo e l'analisi del traffico IP	9
1. Netstat	10
2. Fuser	10
3. Tcpcmdump	10
4. Ethereal	10
5. Snort.....	10
6. Nessus.....	10
SISTEMI SICURI DI TRASMISSIONE.....	11
La crittografia.....	11
GNU Privacy Guard.....	11
I certificati digitali.....	12
La firma digitale.....	12
SSH - Secure SHell.....	12
SISTEMI PER LA PROTEZIONE.....	12
I filtri.....	12
Proxy Server.....	13
Il funzionamento di un firewall.....	13
NAT.....	14
Netfilter.....	14
SISTEMI PER LA VERIFICA	14
Verifica dell'integrità dei file	14
AIDE & tripwire.....	14
POLITICHE DI SICUREZZA.....	14
1. Chiudere le porte	15
2. Non abilitare l'esecuzione di script	15
3. Tenere aggiornati i software.....	15
4. Non rincorrere l'ultima versione di ogni programma!	15
5. Usare solo software originale.....	15
6. Non eseguire programmi di dubbia provenienza.....	15
7. Usare un firewall.....	16
8. Usare l'utente root/Administrator lo stretto indispensabile.....	16
9. Non affidarsi ciecamente ad uno strumento solo.....	16
FREE SOFTWARE E SICUREZZA.....	16
Riferimenti.....	17