

## INTRODUZIONE STORICA

Internet ha una lunga storia che comincia nei primi anni 60, quando al **MIT** vengono mossi i primi passi nella direzione delle reti packet-switching: contemporaneamente nasce anche l'idea di una rete globale, in cui sia possibile connettersi da ogni parte del mondo per inviare o ricevere programmi e dati. Gli studi teorici e le sperimentazioni convergono nel 1969 nella realizzazione di **ARPANET**, in principio costituita da 4 nodi, e dei primi protocolli di comunicazione.

Il 1969 è anche l'anno della nascita di **UNIX**, realizzato sperimentalmente all'interno di AT&T. Negli anni 70 ARPANET cresce enormemente soprattutto in termini di strumenti e protocolli: risalgono a quegli anni i primi programmi di posta elettronica, lo standard **Ethernet**, il TELNET e il primo **TCP/IP**.

UNIX nel frattempo viene riscritto interamente in C, diventando facilmente portabile e modificabile: viene così adottato dalle grandi università americane, soprattutto **Berkeley**, che lo modificano e lo migliorano continuamente. Lo UNIX AT&T diventa commerciale e in ambito universitario si diffonde invece la versione sviluppata a Berkeley (BSD). Il TCP/IP diviene rapidamente il riferimento per tutta ARPANET, che per il 1983 organizza la grande transizione adottandolo ufficialmente per tutti i calcolatori connessi.

La spinta maggiore alla crescita di Internet viene da un altro ente americano, il National Science Foundation (NSF), che nel 1986 decide di investire nelle nuove tecnologie a supporto della ricerca e della didattica: nasce **NSFNET**, alla quale tutte le università americane possono connettersi a spese di NSF a patto di concedere poi l'accesso gratuito a tutto il personale e a tutti gli studenti. Questo porta Internet a raddoppiare in pochi mesi e a diventare 50 volte più grande in soli 3 anni. NSFNET rimane riservata all'ambiente pubblico fino al 1991: il modello americano viene copiato nel resto del mondo, dove vengono create tante reti governative che promuovono l'uso della rete soprattutto in ambito accademico. Internet nasce quindi con una identità ben precisa di supporto alla ricerca scientifica.

Un altro grande impulso allo sviluppo di Internet viene dal **WWW** (World Wide Web), sviluppato all'interno del CERN nel 1991. Nello stesso anno Linus Torvalds scrive la prima versione sperimentale di **Linux**, che viene subito seguito con interesse dalla comunità internazionale: molti si uniscono al team di sviluppo coordinato da Torvalds e il sistema evolve rapidamente verso una prima versione stabile.

Gli anni 90 rappresentano un periodo di forte crescita numerica di Internet e dei servizi ad essa collegati: la grande varietà di strumenti, protocolli e sistemi risultato da questa evoluzione pone grandi responsabilità nel ruolo prima del progettista e poi dell'amministratore dei sistemi informativi aziendali. Quest'ultimo deve confrontarsi da un lato con le forti esigenze degli utenti in termini di affidabilità e buone prestazioni e dall'altro con la complessità degli strumenti a sua disposizione. Per questo è importante che le sue scelte siano sempre mirate ad ottenere soluzioni semplici, aperte, di facile manutenzione e soprattutto completamente comprensibili. In questo senso, nel campo dell'amministrazione di reti e di sistemi, Linux e il software pubblico in generale sono oggi una valida alternativa ai prodotti proprietari, spesso meno versatili e inutilmente complessi, oltre che molto costosi.

## INTRODUZIONE A LINUX

Di recente il mercato dei server, in continua evoluzione, è stato caratterizzato da una crescente diffusione di soluzioni basate su **Linux**.

Linux è un sistema operativo (il software di base necessario per il funzionamento di un computer) disponibile per molte piattaforme hardware, nato nel 1991 come semplice esperimento di programmazione, per approfondire la conoscenza sui processori 386, è cresciuto rapidamente grazie alla lungimiranza del suo creatore (**Linus Torvalds**) e al patrimonio software e culturale derivato dal progetto **GNU** (e dal software **OpenSource** in generale). Un altro fondamento di Linux è l'eredità del mondo Unix: pur essendo stato sviluppato senza utilizzare alcuna riga di codice **Unix**, Linux si è avvantaggiato di tutti i principi di progettazione dei sistemi operativi derivati da questi ambienti (gestione dei file, gestione dei processi, gestione dei dispositivi).

Da un punto di vista formale Linux rappresenta solo il “cuore” del sistema operativo (chiamato **kernel**). Tutti i programmi di “contorno” sono principalmente di derivazione GNU (per questo motivo bisognerebbe utilizzare il termine GNU/Linux per indicare questo sistema operativo) e formano il sistema “completo”.

Mentre il kernel di Linux è univocamente determinato dalla sua versione (al momento la versione stabile è la 2.2.12), i “sistemi Linux completi” possono differire secondo il tipo di distribuzione. Ogni distribuzione organizza in modo diverso i file del sistema operativo e dispone di un numero di versione proprio (come ad esempio la RedHat 6.0).

### La crescita di Linux

In questi ultimi anni Linux ha registrato una crescita vertiginosa (nel 1998 è stata del 213%), tanto da posizionarlo alle spalle di Microsoft Windows nella classifica dei sistemi operativi più diffusi. In particolare, nel mercato dei server una stima attendibile sulla quota occupata dai sistemi Linux è di circa il 20% (in costante crescita).

Guardando invece il “mercato” dei software, si nota una predominanza dei software OpenSource in alcuni servizi offerti dai Internet: **Apache** è utilizzato da più del 50% dei web server, **sendmail** è utilizzato da più del 70% dei mail server e **bind** è utilizzato dalla quasi totalità dei DNS server.

Un altro dato indicativo della crescente diffusione di Linux è che nell'ultimo anno sono apparsi numerosi articoli riguardanti Linux, non solo sulla stampa del “settore”. Inoltre, l'aspetto forse di maggior impatto, è stato l'annuncio della disponibilità di numerosi prodotti commerciali (Corel, Oracle, IBM, Lotus, SAP, ...) e del supporto a Linux di molte aziende d'informatica.

## LINUX COME SERVER

Nel mercato server, i principali punti di forza di Linux sono rappresentati dalla sua elevata stabilità (molti server Linux lavorano per più di un anno senza interruzione), dalla scalabilità molto versatile (sia a livello orizzontale, con più macchine, sia a livello verticale, aumentando la potenza del server), dalla semplicità di amministrazione remota (ogni servizio può essere configurato in remoto), dalle ottime prestazioni (soprattutto in rapporto al tipo di hardware del server) e dal tipo di licenza.






Inoltre, nonostante sembri un prodotto relativamente giovane, è già caratterizzato da una notevole maturità, sia per il numero elevato di utenti che lo hanno testato (e che lo stanno testando e migliorando), sia per il buon numero di driver e software attualmente disponibili, sia per la sua “immunità” ad alcuni dei gravi problemi che affliggono altri sistemi operativi (virus, Y2K bug, ...).

A livello nativo supporta i protocolli della famiglia TCP/IP, ma si integra egregiamente anche in reti basate su protocolli Microsoft, Novell e AppleTalk. Inoltre è già pronto per utilizzare i nuovi protocolli (in particolari IPv6).

Un server Linux può offrire tutti i servizi TCP/IP (web, mail, DNS, FTP, news, ...), i servizi di internetworking (firewall, proxy, router, bridge, ...), molti servizi proprietari (reti Microsoft, Novell Netware, AppleShare), funzionalità di database server e numerosi altri servizi (fax server, print server, virus-scanner).

Esiste inoltre una ricca documentazione, principalmente sviluppata nel progetto **LDP** (Linux Documentation Project).

### Per saperne di più

	<a href="http://www.linux.{org com}">http://www.linux.{org com}</a>	<i>un buon punto di partenza</i>
	<a href="http://www.linuxbusiness.com">http://www.linuxbusiness.com</a>	<i>per un utilizzo professionale di Linux</i>
	<a href="http://freshmeat.net">http://freshmeat.net</a>	<i>per cercare un programma</i>
	<a href="http://www.{gnu opensource}.org">http://www.{gnu opensource}.org</a>	<i>per approfondire l'OpenSource</i>
	<a href="http://www.linux.it/GNU/">http://www.linux.it/GNU/</a>	<i>documentazione italiana sull'OpenSource</i>

## LA GESTIONE DELLA POSTA ELETTRONICA

Alla vigilia del XXI secolo, la comunicazione e l'informazione assumono un ruolo sempre più importante nella nostra società. La trasmissione di dati, soprattutto quella di tipo telematico, è di vitale importanza; di conseguenza è necessario dedicare alla loro gestione una attenzione sempre maggiore.

Quando un nuovo cibernavigatore si affaccia sul mondo di Internet, si rende conto della potenza della posta elettronica, principe dei servizi di comunicazione; egli comprende che si tratta di un mezzo che gli consente, quasi istantaneamente, di spedire testi; ma non solo, anche filmati, immagini e dati in generale, in tutto il mondo, con un notevole risparmio di tempo e di denaro rispetto alla posta tradizionale.

Ma la posta elettronica si scopre un valido strumento di comunicazione interaziendale, che può sostituire l'uso del telefono e l'uso della carta. Alla luce di quanto detto risulta evidente come è strategica la gestione della posta elettronica.

L'invio di messaggi email avviene solitamente attraverso l'uso di un programma (client) adatto alla loro composizione, che poi si mette in comunicazione con il server per l'inoltro del messaggio. Per inviare messaggi di posta elettronica vengono usati programmi client detti **MUA** (Mail User Agent) che si interfacciano tra l'utente ed il server di posta. I client più diffusi sono Pine, Mutt, Eudora, Outlook, Outlook Express e risiedono sulla macchina dell'utente che vuole inviare o ricevere un messaggio.

I server che trasportano il messaggio dal mittente al destinatario si chiamano **MTA** (Mail Transport Agent). In una intranet aziendale ci sarà almeno un server che si occupa di raccogliere i messaggi e di smistarli verso un altro MTA presso l'indirizzo di destinazione, o se necessario in una destinazione intermedia, che si prenderà cura di consegnare il messaggio o di inoltrarlo. I server di posta ricevono messaggi da spedire e dialogano tra di loro mediante il protocollo **SMTP** (Simple Mail Transport Protocol). Tutto questo sembra molto semplice a dirsi, in realtà la configurazione di un server potrebbe essere molto complessa.

I client "scaricano" la posta dal server mediante il protocollo **POP3** (Post Office Protocol) o mediante protocolli equivalenti (es. IMAP). Anche i server intranet, che non sono collegati permanentemente con Internet, scaricano la posta dal server Internet mediante il protocollo POP3 e/o IMAP.

### Programmi



<http://www.sendmail.org>

*Sendmail*

Sendmail è l'MTA più utilizzato in Internet e sicuramente quello più completo. Implementa tutti gli strumenti per indirizzare la posta, aliasing e forwarding.

Tipo di licenza: OpenSource



<http://www.qmail.org>

*Qmail*

Qmail è un moderno rifacimento di sendmail, con l'intento di avere un MTA più veloce, più semplice e molto più sicuro di Sendmail.

Tipo di licenza: freeware

## IL PROXY GERARCHICO PER L'ACCESSO AL WEB

Per ridurre al minimo il traffico prodotto dalla navigazione sul web si usano più proxy server in relazione gerarchica tra loro. Il proxy interpellato richiede la pagina web ad Internet o al proxy al livello superiore solo se è effettivamente necessario, cioè se non è presente nella sua cache.

Il proxy può discriminare gli utenti tramite un'autenticazione con password, tramite l'indirizzo del client e può discriminare i siti visitati, utilizzando filtri basati su parole chiave, indirizzi di destinazione, orari o una combinazione dei precedenti.

Vantaggi nell'utilizzo di un proxy server:

- ❑ velocità di navigazione (nel caso di hit, cioè di pagina recuperata dalla cache)
- ❑ riduzione dell'occupazione di banda (la banda non utilizzata può essere disponibile per velocizzare anche altri servizi)
- ❑ discriminazione sulla navigazione
- ❑ logging

### Programmi



<http://squid.nlanr.net>

*Squid*

Squid è un web proxy dalle spiccate qualità di performance che può essere utilizzato in maniera gerarchica per aumentare il tempo di risposta e per ridurre l'occupazione di banda.

Tipo di licenza: GPL



<http://www.gedanken.demon.co.uk/wwwoffle>

*Wwwoffle*

WWWOFFLE è stato pensato per quelle situazioni dove computer si trovano offline/online. È possibile con questo software navigare pagine web pur restando scollegati da Internet.

Tipo di licenza: GPL

## LINUX COME ROUTER PER L'ACCESSO "INTELLIGENTE" AD INTERNET

Una degli utilizzi di Linux in modalità "black box" è quella di router per collegare una rete aziendale ad Internet. Il router può utilizzare la linea telefonica commutata o **ISDN**, ma linux supporta anche le tecnologie emergenti (quali **ASDL**). Esistono programmi (**isdn4linux** e **diald**) che sentono la richiesta di connessione ad Internet ed automaticamente stabiliscono la connessione (dial-on-demand). Automaticamente la interrompono dopo un timeout di inattività.

Per accedere ad Internet dai computer della rete aziendale è possibile utilizzare il proxy o il mascheramento.

Il mascheramento (**IP masquerating**) è una particolare caratteristica di Linux. Se un computer sul quale viene installato Linux, viene a connettersi ad Internet con il mascheramento abilitato, allora i computer che si collegano ad esso tramite una LAN possono raggiungere di conseguenza Internet sebbene questi non abbiano un indirizzo IP ufficiale. Questa tecnica è utile in tutte quelle situazioni nella quale più computer in una stessa LAN devono connettersi ad Internet. Una soluzione sarebbe quella di dotare ogni stazione di un modem e di un abbonamento al provider.

## Cosa si può fare e cosa non si può fare con il mascheramento

Il mascheramento consente di concentrare tutta la rete aziendale in un unico computer che sta fisicamente in Internet, di conseguenza tutti i computer della rete interna, esternamente vengono visto con un unico IP (quello della macchina Linux).

Il vantaggio è un evidente incremento della sicurezza, visto che nessun computer interno può essere raggiunto direttamente. Per contro alcuni servizi di rete, proprio per questo motivo, potrebbero non funzionare o funzionare in modo parziale (come ad esempio la chiamata dall'esterno in videoconferenza).

Esistono anche alcuni router hardware che implementano il mascheramento (oppure in NAT, che è una meccanismo più generico) e sono in grado di collegare la LAN tramite PSDN o ISDN.

## Programmi



<http://www.xos.nl/linux/ipfwadm>

*ipfwadm*

Programma per gestire il mascheramento e le funzioni di firewall del kernel Linux.



<http://ipmasq.cjb.net>

*mascheramento*

Documentazione sul mascheramento.



<http://www.rustcorp.com/linux/ipchains>

*ipchains*

Ipchains è l'interfaccia per l'amministratore del codice di packet filter implementato nel nuovo kernel di Linux, a partire dalla versione 2.1.102, sostituendo ipfwadm e rendendo disponibili funzionalità evolute, quali il NAT (Network Address Translation).

Tipo di licenza: GPL



<http://diald.unix.ch>

*diald*

Diald significa Dial Daemon. Questo programma gestisce il collegamento ad Internet attraverso tramite una connessione SLIP/PPP (via modem analogico). Si occupa di comporre il numero per collegarsi al provider e di chiudere la connessione quando non è più necessaria.

Tipo di licenza: GPL



<http://www.isdn4linux.de>

*isdn4linux*

Analogamente a diald, questo programma serve per connettere il server ad Internet, ma utilizzando una scheda ISDN.

## AUTENTICAZIONE CENTRALIZZATA DEI SERVIZI PROXY, POSTA E WEB

È possibile creare un database SQL centralizzato per l'autenticazione delle password, utilizzabile per i servizi di accesso HTTP ad aree riservate (con server apache), proxy (con server squid) e mail (con server qmail), aggiornabili tramite **ODBC** (con un database client come Access, per esempio) o tramite Web (con script in PHP).

### Programmi



<http://www.mysql.com>

#### *MySQL*

MySQL è un database server SQL (Structured Query Language). L'SQL è il linguaggio dei database più famoso nel mondo. MySQL è un a sua implementazione client/server consistente in un demone mysqld e una nutrita serie di programmi e librerie client.

Questo prodotto è libero per uso personale e per uso commerciale. Devo pagare una licenza solo se lo rivendi insieme ad una tua applicazione.

Tipo di licenza: libera ma limitata

## DISPOSITIVI DI MEMORIZZAZIONE DI MASSA FAULT-TOLERANT

L'esponenziale crescita della potenza delle CPU, e dei computer in generale, si trova a fare i conti con la zavorra rappresentata dall'utilizzo di memorie di masse, nel nostro caso gli hard disk, che per ragioni di natura meccanica soffrono di uno sviluppo più lento, più costoso e meno affidabile.

I risultati degli studi, dettati da ragioni di natura prettamente economica, intrapresi alla fine degli anni '80, per l'attuazione di nuove soluzioni che permettessero un più basso costo di immagazzinamento dei dati, ci permettono, oggi, di avere a disposizione, maggiori prestazioni in termini di trasferimento dati e di sicurezza senza incorrere, necessariamente, in ulteriori spese ed artifici hardware.

L'implementazione, in forma di codice scritto nel kernel di Linux, del lavoro dei ricercatori Garth Gibson, Randy Katz, prima, e David Patterson, poi, dell'Università di Berkeley, è iniziata nel giugno del 1995.

Da allora, e il continuo lavoro di un nutrito gruppo di hacker, e il costante utilizzo della tecnologia denominata **RAID** (Redundant Arrays of Inexpensive Disks) da parte di un vasto numero di utenti, soprattutto in contesti dove necessita di efficienza e integrità dei dati la fanno da padrone, ha permesso di avere, funzionanti e ben testate, soluzioni relative a casi in cui:

- ☐ si necessita di maggior capacità di memorizzazione;
- ☐ si necessita di maggior velocità nel trasferimento dati;
- ☐ si necessita di un sistema funzionante anche a fronte di guasti fisici del hardware relativo agli hard disk

La concretizzazione, sempre in ambiente Linux, di tali tipi di sistemi a livello puramente software, ma che per questo non vanno ad inficiare l'eventuale utilizzo di soluzioni hardware dedicate, permette di operare senza costrizioni di alcun tipo sia sul piano delle scelte degli hard disk, sia sul piano delle scelte dei controller, offrendo anche una notevole flessibilità nel fronteggiare situazioni di recupero dati partendo da condizioni particolarmente critiche, o impreviste, in cui può versare il sistema informatico interessato.

In questi termini avverrà una, seppur breve, analisi dei modi disponibili ad ogni system administrator per poter compiere ulteriori passi avanti nel raggiungimento, o meglio nell'avvicinamento, al miraggio rappresentato dalla realizzazione di macchine che possano offrire una soluzione di continuità di servizio, qualsiasi siano le condizioni in cui si trovino ad operare.



## INTEGRAZIONE IN RETI ETEROGENEE

Non è difficile nelle reti attuali, specialmente di media complessità, trovare sistemi Windows, Mac, Unix, Novell, Hosts (come AS/400 e sistemi 390) che devono convivere ma soprattutto dialogare attraverso la stessa rete locale e non. Linux ha tutte le caratteristiche ed i requisiti per inserirsi in reti altamente eterogenee e dialogare con tutte le macchine presenti.

Oltre che implementare nativamente il protocollo TCP/IP che è lo standard mondiale per quello che riguarda le comunicazioni fra computer, Linux dispone di programmi e protocolli che gli consentono di interfacciarsi anche in modo nativo con i principali sistemi operativi presenti sul mercato.

Linux può essere presente in rete sia in qualità di server che in qualità di client: può utilizzare risorse condivise da altri, condividere risorse proprie, con la particolarità di poter condividere la stessa risorsa, attraverso più modalità o protocolli. Come ultimo utilizzo, Linux può essere impiegato con middleware, cioè come collante fra reti e protocolli diversi.

Vediamo in dettaglio i principali sistemi che possono essere interfacciati a Linux.

## MAINFRAME/SISTEMI HOST

### Le reti locali ed i mainframe/hosts

I mainframe sono molto diffusi nelle reti aziendali, specialmente nelle realtà medio-grandi, dove il volume dei dati da gestire è molto elevato. In particolare, in Italia, troviamo diversi sistemi host, fra i quali l'AS/400 è senz'altro il più diffuso.

Ai sistemi host, si può accedere con terminali "stupidi", oppure, nelle realtà più al passo con i tempi, attraverso personal computer con funzioni di emulazione di terminale. L'emulazione terminale fatta con un pc, consente agli utenti di utilizzare anche strumenti di office automation, di navigare in internet, di lavorare con sistemi di grafica, impaginazione ecc., cioè tutte quelle cose che vengono negate da sistemi prevalentemente text-only.

Ci sono due modalità per accedere ai sistemi host: direttamente, attraverso la rete locale, quando il mainframe monta una scheda, in genere ethernet, ed è connesso alla lan, oppure attraverso un computer che funge da gateway. Alla seconda categoria appartengono gli *SNA server*, cioè middleware che si connettono ai sistemi host attraverso questa suite di protocolli e "condividono" questa connessione sulla rete locale.

### Linux e lo SNA server

Anche Linux dispone di uno SNA server. Inizialmente nato come progetto GPL, è stato "venduto" alla ICE Networking Solution. L'indirizzo per avere informazioni a riguardo è:

<http://www.icenetworking.com/products/sna/index2.html>

Purtroppo non ci è stato possibile testare il prodotto, in quanto è disponibile solamente a pagamento.

## Telnet 5250 e 3270 su linux

Nel caso in cui mainframe e client appartengano ad una rete locale o geografica ed implementino un protocollo comune (TCP/IP), è possibile connettere direttamente client e mainframe/host.

Questa modalità di connessione prende il nome di Telnet **5250** e **3270**: nel primo caso viene effettuata un'emulazione di terminale 5250 (as400) mentre nel secondo caso ci si riferisce ai terminali 3270, cioè connessi a sistemi mainframe quali il 390 IBM. L'ovvio vantaggio di questo tipo di connessione, qualora sia implementabile, è di non dover installare e mantenere software che solitamente hanno un costo elevato.

## Link utili

	<a href="http://www.freshmeat.net/appindex/1999/04/18/924490793.html">http://www.freshmeat.net/appindex/1999/04/18/924490793.html</a>	<i>Linux SNA</i>
	<a href="http://www.blarg.net/~mmadore/5250.html">http://www.blarg.net/~mmadore/5250.html</a>	<i>Telnet 3270</i>
	<a href="http://www.geocities.com/SiliconValley/Peaks/7814/">http://www.geocities.com/SiliconValley/Peaks/7814/</a>	<i>Telnet 5250</i>
	<a href="http://www.snipix.freemove.co.uk/">http://www.snipix.freemove.co.uk/</a>	<i>Info varie</i>
	<a href="http://www.ietf.org/ids.by.wg/tn3270e.html">http://www.ietf.org/ids.by.wg/tn3270e.html</a>	<i>Info su 3270</i>

## LINUX E MACINTOSH

### Linux come server Macintosh

I client Mac hanno la possibilità di colloquiare in rete con Linux mediante due protocolli: *Appletalk* e *Appleshare over IP* (AFP/TCP). Linux supporta nativamente, a livello di kernel, AppleTalkDDP, mentre si affida a programmi che girano in user level per il supporto AFP/TCP.

Fra i programmi trovati, c'è da segnalare *Netatalk+asun* che permette di condividere risorse Linux sia via appletalk che attraverso AFP/TCP.

Fondamentale la visione del sito <http://www.thehamptons.com/anders/netatalk/> che contiene la FAQ, parecchia documentazione, esempi di configurazione e consigli.

### Linux come client Macintosh

Il supporto client per reti Mac è ancora in fase sperimentale, e sembra che non ci sia più interesse verso lo sviluppo di questa modalità di connessione. Si possono comunque trovare informazioni al seguente indirizzo:

<http://www.panix.com/~dfoster/afpfs/>

## LINUX E NOVELL NETWARE

### Linux come router di reti Netware

Linux implementa nativamente il supporto per il protocollo **IPX**, che gli permette di funzionare come router o come bridge tra reti Netware. Questi tool, sviluppati da un collaboratore della Caldera (uno dei principali produttori di distribuzioni Linux), sono disponibili all'indirizzo:

<ftp://sunsite.unc.edu/pub/Linux/system/filesystems/ncpfs/ipx.tgz>

### Linux come client di reti Netware

Linux può anche accedere a risorse condivise da Novell Netware presenti sulla rete mediante il tool **ncpfs** disponibile all'indirizzo:

<ftp://ftp.gwdg.de/pub/linux/misc/ncpfs/>

L'ultima versione di questi tool permette anche l'accesso a risorse **NDS**, anche se purtroppo tale supporto è ancora in versione beta. Caldera produce un tool che permette di accedere da Linux a risorse NDS. Tale tool è chiamato CND, e viene distribuito gratuitamente.

### Linux come NCP server

**NCP** server è il file/print server per reti su protocollo IPX; ci sono 3 pacchetti che permettono di condividere con Linux delle risorse Netware:

- ❑ **mars\_nwe**: permette di condividere sia file che stampanti; anche se non è ancora in versione definitiva il numero di bug è in costante diminuzione. Il suo problema principale, risiede nel fatto che la lista degli utenti non coincide con quella degli utenti linux, ma consta di un file di configurazione separato. A questi indirizzi sono disponibili ulteriori informazioni:

[http://www.compu-art.de/mars\\_nwe/index.html](http://www.compu-art.de/mars_nwe/index.html)

<ftp://sunsite.unc.edu/pub/Linux/system/filesystems/ncpfs/>

- ❑ **lwarded**: meno sviluppato rispetto al mars\_nwe, ma funzionante a livello più basso, può inizializzare il sottosistema IPX di per se (mars\_nwe necessita di tool esterni, forniti con il pacchetto stesso). Esistono alcuni problemi quando viene utilizzato con client windows 9x & NT.

<ftp://sunsite.unc.edu/pub/Linux/system/network/daemons>

<ftp://klokan.sh.cvut.cz/pub/linux/linware/>

- ❑ **Caldera Netware for Linux**: la distribuzione Linux Caldera fornisce in bundle con la propria distribuzione commerciale un server Netware completamente compatibile con il protocollo utilizzato dalla versione 4 del sistema operativo di Novell, comprensivo quindi anche del supporto NDS, ed inoltre offre la possibilità di amministrazione come una macchina Novell da remoto. Tale server emulator è anche distribuito in forma gratuita, con alcune restrizioni sul numero di client connessi (3); per informazioni dettagliate:

<http://www.calderasystems.com/products/netware/index.html>

### Che cosa manca?

In tutti i casi manca ancora il supporto al protocollo Netware versione 5, che cambia il protocollo di trasporto da IPX a IP. Inoltre, non è presente il supporto agli NLM (Network Loadable Module).

## IL MONDO WINDOWS/LAN MANAGER

In una rete Windows/LAN Manager, i client si rivolgono al controller di dominio prevalentemente per essere autenticati e poter quindi accedere a cartelle, stampanti, risorse condivise, e tutto ciò che viene messo a disposizione in rete.

**Samba** per Linux è un insieme di programmi che implementano il protocollo SMB (Server Message Block), dal quale trae il nome e che è alla base di tutte le comunicazioni che avvengono nelle reti Windows. Samba agisce sia sul versante server, che in quello client.

### Linux + Samba come server

Per quello che riguarda il lato server, attraverso samba, Linux può apparire a tutti gli effetti un server NT poiché è in grado di:

- ☐ Svolgere funzioni di authentication server
- ☐ Condividere file, cartelle, e stampanti
- ☐ Gestire centralmente gli utenti ed i loro profili
- ☐ Implementare la risoluzione dei nomi Netbios (WINS Server)

Ad oggi risultano esserci alcuni problemi con le workstation NT, qualora si voglia implementare un dominio a 360 gradi (senza NT server in rete).

### Linux + samba come client

Riguardo al lato client, è possibile accedere a directory condivise da NT e Win95/8, sia mediante un tool a riga di comando simile a FTP, sia montando le directory direttamente nel filesystem e quindi utilizzandole come risorse locali. È inoltre possibile utilizzare le stampanti condivise, purché esse siano supportate da Linux.

### Pregi e difetti di samba

- ☐ **Pregi:** stabilità e velocità, configurabilità, sicurezza, snellezza, gestisce in toto un dominio NT (autenticazione e gestione dei profili utente), la home directory viene vista attraverso SMB, emulazione di uno o più domini dalla stessa macchina, condivisione delle stampanti con la possibilità di autoinstall, gestione degli utenti centralizzata: gli utenti linux e windows vengono gestiti da un'unica macchina.
- ☐ **Difetti:** supporto per il PDC in beta, nessun supporto Netbeui (è necessario utilizzare il Netbios over TCP/IP), interfaccia grafica per la configurazione migliorabile, browser per reti non ancora disponibile, prestazioni leggermente inferiori a Windows NT Server.

### Link utili



<http://www.samba.org>

*Per scaricare Samba*



<http://www.freshmeat.net>

*Per scaricare le utility per Samba*

## DHCP – DOMAIN HOST CONFIGURATION PROTOCOL

Il DHCP è un tool che permette la configurazione di reti IP in maniera centralizzata: ogni macchina, al boot, cerca un server DHCP e lo interroga per ottenere un indirizzo ed eventuali altre configurazioni riguardanti il protocollo TCP/IP (la netmask, l'indirizzo del server DNS, l'indirizzo del gateway, ecc.). Per informazioni, consultare il sito:

<http://www.isc.org/view.cgi?products/DHCP/index.phtml>

## ESERCITAZIONE PRATICA

### DHCP + file sharing con linux in reti Microsoft

Nell'esempio seguente, vengono presentati i passi per installare e configurare i demoni DHCP e Samba, al fine di utilizzare Linux in una rete con client Windows 95/8 NT come "configuratore" per il protocollo TCP/IP (DHCP) e come file server.

Si presuppone di avere un client Windows 95 con la scheda di rete (e il driver già configurato) e con il protocollo TCP/IP installato con autoconfigurazione dell'indirizzo di rete, ed una macchina Linux con scheda di rete e protocollo TCP/IP configurati correttamente.

#### 1) DHCP server

Dopo aver effettuato il mount del CD (si suppone di utilizzare il CD del primo Linux Day), installare il pacchetto dhcp-2.0b1pl6-6.i386.rpm o equivalente:

```
$ rpm -i /mnt/cdrom/RedHat/RPMS/dhcp-2.0b1pl6-6.i386.rpm
```

di seguito copiare il file di configurazione di esempio da /usr/doc/dhcp-2.0/dhcpd.conf.sample a /etc/dhcpd.conf:

```
$ cp /usr/doc/dhcp-2.0/dhcpd.conf.sample /etc/dhcpd.conf
```

editare tale file di configurazione per adattarlo alle proprie esigenze (settare il pool di indirizzi sulla sottorete che si vuole utilizzare, la netmask opportuna, i leases time, l'eventuale DNS server), quindi creare il file vuoto /etc/dhcpd.leases dove verranno registrati i leases che il demone effettuerà:

```
$ touch /etc/dhcpd.leases
```

avviare il servizio DHCP:

```
$ /etc/rc.d/init.d/dhcp start
```

passare alla macchina w9x e controllare che la configurazione di rete venga presa correttamente con winipcfg (utilizzare RINNOVA INDIRIZZI), provare un ping e un telnet...

## 2) Samba server

Installare il pacchetto Samba:

```
$ rpm -i /mnt/cdrom/RedHat/RPMS/samba-2.0.3-8.i386.rpm
```

editare il file di configurazione (**/etc/smb.conf**) per adattarlo alle proprie esigenze (come inizio è sufficiente dare il giusto nome al workgroup), quindi aggiungere un utente Samba:

```
$ smbadduser username_unix:username_nt
```

A questo punto, avviare Samba con il comando:

```
$ /etc/rc.d/init.d/smb start
```

e provare dalla macchina Windows se funziona, facendo un browsing della rete mediante “Risorse di rete”. Se tutto è a posto, si può creare una directory da condividere:

```
$ mkdir /home/prova
```

È necessario cambiare i diritti di scrittura sulla directory:

```
$ chmod 777 /home/prova
```

ed aggiungere a **/etc/smb.conf** le seguenti righe:

```
[prova]
public = no
writable = yes
printable = no
```

salvare il file di configurazione e riavviare Samba

```
$ /etc/rc.d/init.d/smb restart
```

Se tutto è stato effettuato correttamente, dalla macchina Windows è possibile scrivere e leggere in /home/prova.

## CONSIDERAZIONI FINALI

Come si è potuto constatare, Linux è veramente aperto verso tutti i principali sistemi operativi/sistemi disponibili sul mercato. La stabilità, la scalabilità e la configurabilità di Linux, lo rendono l'ideale sostituto di software commerciali molto costosi, candidandolo al ruolo di server aziendali “tuttofare” ad alta disponibilità.

## SICUREZZA DEI SISTEMI E DELLE RETI

Internet ed in generale le reti di calcolatori, sebbene nate all'interno della società scientifica ed utilizzate in principio solamente da esperti del settore, negli ultimi anni sono divenute uno strumento alla portata di chiunque ed il numero di utenti è cresciuto enormemente. La connessione globale ha portato notevoli vantaggi, tuttavia comporta alcuni inconvenienti. All'interno di ogni società è infatti possibile pensare che esista un piccolo numero di soggetti male intenzionati. Se si considera che ad oggi gli utenti di Internet risultano essere intorno ai 30 o 40 milioni, la percentuale di male intenzionati, per quanto esigua possa essere, risulta di cospicua rilevanza.

Nessuno è in grado di fornire una stima attendibile riguardo il numero di attacchi informatici. Una ricerca svolta negli Stati Uniti ha dimostrato che su di un campione di aziende che erano state utilizzate come bersagli per degli attacchi da parte di una commissione autorizzata dalle aziende medesime, solamente il 4% di esse si era resa conto di essere stata vittima di un attacco. È utile sottolineare che il 40% di tali attacchi comportava l'accesso ai sistemi con il massimo dei privilegi.

Ultimamente non solo è aumentato il numero di attacchi informatici, ma è aumentata anche la complessità. Al momento della fondazione del CERT, avvenuta in seguito alla diffusione del noto Internet Worm del 1988, le tipologie di attacchi informatici erano essenzialmente due, il furto di password e l'esplorazione dei punti deboli di sistemi operativi e programmi. Ultimamente si può assistere ad un notevole aumento della complessità tecnica degli attacchi. Tale fenomeno è dovuto al sempre più rapido diffondersi della conoscenza informatica e telematica. È dunque possibile assistere ad attacchi che sfruttano alcuni punti deboli del protocollo TCP/IP o dei più comuni protocolli di trasferimento dati utilizzati in Internet. Bisogna poi aggiungere che anche le tipologie di attacco classiche, di cui si conoscono la struttura ed il modo in cui difendersi, non sono state del tutto debellate. Tale fenomeno è dovuto al fatto che negli ultimi tempi collegarsi ad Internet è divenuto molto semplice, e spesso molti siti Internet sono gestiti da persone che non possiedono una sufficiente competenza in materia.

Sebbene il numero di attacchi informatici e la loro complessità sia in continuo aumento, sono oggi disponibili numerosi sistemi di difesa e varie documentazioni scientifiche al riguardo. È compito di coloro che sono preposti all'amministrazione dei vari siti aggiornare i propri sistemi al fine di renderli sicuri. È infine utile sottolineare che in un mondo totalmente connesso, la diffusione della conoscenza riguardante la sicurezza informatica non porta vantaggi solamente ai singoli siti, ma concorre alla trasformazione di Internet in un sistema globalmente più sicuro e dunque efficiente.

### Tipi di sicurezza

- ❑ Sicurezza dei **dati**: i dati possiedono tre caratteristiche principali di cui bisogna curare la sicurezza : la segretezza, l'integrità e la disponibilità.
- ❑ Sicurezza delle proprie **risorse**: un determinato sito potrebbe necessitare di un sistema di sicurezza anche solo per proteggersi dall'utilizzo non autorizzato dei propri sistemi, o anche più semplicemente dal fatto che qualcuno possa curiosare all'interno di essi.
- ❑ Sicurezza della propria **reputazione**: per molti siti, come ad esempio banche o aziende informatiche, il semplice fatto di essere stati vittima di attacco significa perdere credibilità nei confronti di possibili investitori ed in generale nei confronti del mercato.

La diffusione di sistemi di sicurezza sempre migliori renderà Internet un sistema molto più efficiente tramite il quale si potranno compiere operazioni oggi ancora non del tutto affidabili. I sistemi di sicurezza più evoluti permettono inoltre il controllo e la gestione del traffico in entrata ed uscita ad una rete locale.

## Tipi di attacchi

- ❑ **Intrusioni:** tutte quelle operazioni che permettono l'accesso non autorizzato ad un sistema.
- ❑ **Sabotaggio:** tipo di attacco la cui finalità è quella di impedire il corretto utilizzo di un sistema fino a renderlo del tutto inutilizzabile nei casi più gravi.
- ❑ **Furto** di informazioni: tutti gli attacchi il cui fine è quello di venire in possesso di informazioni che dovrebbero rimanere riservate.

## Tipi di attaccanti

- ❑ **Joyrider:** tentano di penetrare all'interno dei sistemi informatici per svago o per curiosità, ma le loro azioni nocive sono spesso frutto di ignoranza o del tentativo di mascherare l'attacco medesimo. Gli obiettivi preferiti da tali attaccanti sono i siti più noti ed i calcolatori non comuni.
- ❑ **Vandali:** rappresentano il pericolo maggiore per un sito connesso ad Internet, perché il loro scopo principale è quello di arrecare il maggior numero possibile di danni al sistema preso di mira. Le prede preferite da tali personaggi sono i siti con maggior visibilità o quegli enti come le compagnie telefoniche e gli uffici governativi verso i quali esiste un certo risentimento popolare.
- ❑ **Giocatori:** alcuni attaccanti che cercano di violare i sistemi di sicurezza senza alcuna finalità particolare, se non quella di riuscire in tale operazione.
- ❑ **Spie:** costituiscono la categoria di attaccanti più difficilmente rilevabile, infatti operano con uno scopo preciso e con una notevole competenza. Le loro finalità sono spesso costituite dal furto di informazioni riservate o vendibili ad altre persone.

Spesso incidenti che provocano il blocco del sistema non sono dovuti ad attacchi informatici. Non è possibile proteggersi dai danni provocati da errori umani e da incidenti, tuttavia bisogna tenere conto della possibilità che tali evenienze si verifichino.

## Tipi di protezione

- ❑ Mancanza di sicurezza o nessuna connessione: sono due atteggiamenti estremi nei confronti del problema sicurezza, il primo consiste nel disinteressarsi di tutti i meccanismi di protezione, il secondo nel decidere di non connettersi ad Internet per non correre alcun rischio.
- ❑ Sicurezza attraverso la riservatezza: consiste nel mantenerne segreta l'esistenza ed i meccanismi di protezione adottati. Tale sistema non risulta efficiente, in quanto ogni sito che si collega ad Internet deve sottoporsi ad alcune registrazioni e tale materiale è disponibile pubblicamente.
- ❑ Sistemi di sicurezza applicati ai singoli calcolatori: sono i sistemi di sicurezza maggiormente utilizzati. Tuttavia tale modo di operare non è applicabile su larga scala.
- ❑ Sistemi di sicurezza applicati alla rete locale: comprende il progetto di sistemi **Firewall**, il meccanismo delle autenticazioni e l'uso della crittografia per proteggere i dati più critici che transitano attraverso di essa.

Nella progettazione di un sistema di sicurezza bisogna tenere conto di alcuni assiomi fondamentali. Nessun sistema potrà mai essere considerato completamente sicuro. Inoltre il fatto di connettersi ad Internet comporterà sempre dei rischi. A tal proposito è necessario tenere continuamente aggiornato il sistema stesso e documentarsi riguardo alle evoluzioni nel settore sicurezza. Bisogna poi aggiungere che qualsiasi sistema di sicurezza comporterà dei disagi per gli utenti della rete protetta.



## STRATEGIE DI REALIZZAZIONE DI UN SISTEMA DI SICUREZZA

Il compito principale di un addetto alla sicurezza è quello di aiutare le organizzazioni a decidere quanto tempo e quanto denaro investire nella sicurezza. Un secondo compito è definire politiche, standard e procedure per rendere proficuo il denaro ed il tempo speso nella prima fase. Infine il personale addetto alla sicurezza si deve preoccupare di monitorare i sistemi per assicurarsi che le varie politiche di sicurezza vengano realmente attuate e siano conformi con gli obiettivi preposti.

Le strategie per la realizzazione di un sistema di sicurezza si possono riassumere nei punti seguenti:

- ❑ Pianificazione: durante questa fase vanno considerate diverse categorie (riservatezza, integrità dei dati, disponibilità, consistenza, controllo e registrazione).
- ❑ Valutazione dei rischi: consiste nel rispondere ad alcune domande (“che cosa sto cercando di proteggere”, “contro quali pericoli mi voglio proteggere”, “quanto tempo e denaro intendo investire per sviluppare il sistema di protezione”)
- ❑ Analisi costi/benefici: terminata l’analisi dei rischi, è possibile assegnare un costo ad ogni rischio e determinare il costo necessario per difendersi da tale pericolo. In particolare vanno analizzati il costo della perdita e il costo della prevenzione.
- ❑ Definizione di politiche che rispecchiano le esigenze: le politiche aiutano a stabilire che cosa sia da ritenere importante ed a stabilire quali passi intraprendere per proteggere tali fattori critici.
- ❑ Implementazione del sistema: comprende tutte le operazioni per lo sviluppo tecnico del sistema.
- ❑ Monitoraggio e risposta agli inconvenienti: ogni sistema di sicurezza deve consentire il monitoraggio degli eventi e la possibilità di rispondere in maniera adeguata ai problemi che si possono verificare.

## LA SICUREZZA A LIVELLO DI SISTEMA

### Utenti ed account

Nei sistemi Unix ogni utente è identificato attraverso una Login ed una Password. Tali informazioni sono mantenute in un file `/etc/passwd`. Le password sono registrate in maniera criptata secondo un particolare algoritmo (a volte viene registrata in un file diverso detto shadow password file).

Una delle prime operazioni da svolgere consiste nel modificare la propria Password, tale operazione andrebbe ripetuta periodicamente al fine di aumentare la sicurezza del sistema. Molti degli attacchi informatici sono stati effettuati in seguito alla scoperta della password di qualche utente, è quindi necessario riporre particolare attenzione nella scelta delle password ( ad esempio utilizzando caratteri maiuscoli e minuscoli, caratteri di controllo e spazi, utilizzare password di almeno 7 o 8 caratteri, ...)

Ultimamente molte organizzazioni utilizzano reti di calcolatori. Al fine di consentire una gestione centralizzata dei vari account, vengono utilizzati dei meccanismi di che rendano disponibili via rete le informazioni relative agli utenti.

I sistemi più diffusi comprendono: Sun Microsystem’s Network Information System (NIS), Sun Microsystem’s NIS+, Open Software Foundation’s Distributed Computing Environment (DCE), NeXT Computer’s NetInfo.

## **Difesa e sicurezza di un account**

Ogni account rappresenta un punto di accesso al nostro sistema. In tal senso rappresenta un possibile pericolo. L'amministratore di sistema accorto deve allora controllare periodicamente i vari account e sviluppare tutti quegli accorgimenti atti a renderli sicuri.

In particolare è necessario tenere sotto controllo gli account senza una password (account aperti), gli account di default, gli account che eseguono un singolo comando, gli account di gruppo. Alcuni utili accorgimenti sono la restrizione di un account solo in alcuni momenti (specificando l'ora o il giorno della settimana) e la disabilitazione degli account non utilizzati per un certo periodo di tempo.

## **L'account di root**

Tutti i sistemi (Unix e non) dispongono di un account per gestire completamente il sistema. Tale account è detto generalmente *superuser*. Nel mondo Unix corrisponde all'utente root, nel mondo Windows è l'utente administrator, nel mondo AS/400 è qsecofr. Generalmente tale utente è in grado di svolgere ogni operazione sul sistema e dunque il suo account è da difendere in maniera particolare. In generale poi si sconsiglia caldamente di utilizzare l'utente superuser per lavorare con i sistemi a meno che non si debbano svolgere operazioni di tipo amministrativo.

Per aumentare la sicurezza, in molti sistemi operativi è possibile bloccare l'accesso all'account di superuser solamente se si sta utilizzando la console del sistema o limitare gli utenti che hanno accesso a programmi "privilegiati".

## **Sicurezza del Filesystem**

Uno degli aspetti più importanti nella difesa del filesystem consiste nella cura della sua integrità. Tale aspetto si concretizza nei seguenti accorgimenti:

- ❑ **Prevenzione:** per impedire a persone non autorizzate la modifica o la cancellazione di file. Di solito si agisce opportunamente sui permessi di file e directory, si limita l'accesso all'account di root e si regola l'accesso ai filesystem di rete. Esistono poi accorgimenti più specifici che tuttavia dipendono dalla particolare versione di sistema operativo che si sta utilizzando (ad esempio, alcuni sistemi permettono di definire file come immutabili o append-only). Altri accorgimenti consistono poi nel limitare la visibilità del filesystem a determinati account, secondo una modalità detta chrooted.
- ❑ **Rilevazione:** è utile tenere sotto controllo i file critici al fine di scoprire eventuali modifiche o alterazioni. Esistono tre metodi principali per scoprire modifiche a file o directory: confronto (bit a bit) con copie, monitoraggio dei metadata (informazioni aggiuntive che caratterizzano ogni file come la data di creazione o di modifica), utilizzo di signature e delle checksum.
- ❑ **Ripristino:** per recuperare i file in seguito a cancellazioni o alterazioni.

## **Monitoraggio e Registrazione**

Una volta realizzato un sistema di sicurezza è necessario monitorarlo. I sistemi Unix utilizzano molti file in cui viene registrato tutto quello che avviene in un sistema, che rappresentano una fonte di informazioni molto preziosa e dunque vanno difesi con particolare cura. In tal senso un accorgimento utile può essere quello di mantenerli su PC diversi dal calcolatore al quale si riferiscono. Un'altra raccomandazione è poi quella di effettuare backup periodici dei propri file di log.

## **Software pericoloso**

- ❑ Security tools and toolkit: strumenti utilizzati dagli amministratori di sistema. Tuttavia possono venire utilizzati da persone non autorizzate per tentare di forzare i sistemi.
- ❑ Back door: sono scappatoie che consentono l'accesso al sistema.
- ❑ Logic bomb: sono istruzioni nascoste all'interno dei programmi che entrano in funzione in determinate condizioni
- ❑ Virus: programmi in grado di modificare altri programmi inserendo copie di sé stessi
- ❑ Worm: si propagano da un computer all'altro senza necessariamente modificare altri programmi.
- ❑ Trojan Horse: programmi che apparentemente svolgono una funzione ma in verità fanno altro.
- ❑ Bacteria o Rabbit Program: programmi che eseguono copie di sé stessi per sovrascrivere risorse o programmi del sistema.

In generale i pericoli maggiori che si possono incontrare nel mondo Unix sono le Back Door ed i Trojan Horse, che portano alterazioni della shell o delle procedure di start up, la modifica di alcune procedure automatiche e interazioni inaspettate.

I meccanismi di difesa contro tali attacchi consistono fondamentalmente nel controllo meticoloso del file system. In particolare vanno tenuti sotto controllo i file che sono accessibili da chiunque.

## **LA SICUREZZA A LIVELLO DI RETE**

### **Sicurezza dei collegamenti telefonici**

I modem costituiscono un aspetto critico della sicurezza in quanto realizzano collegamenti tra il mondo esterno e la nostra rete. I modem attuali consentono inoltre di effettuare operazioni di test e configurazione in remoto, il che costituisce una notevole comodità per gli amministratori di rete ma rappresenta anche un pericolo per quanto riguarda la sicurezza.

Uno dei primi accorgimenti per rendere sicuri i modem consiste nel proteggere le linee telefoniche, ovvero i numeri di telefono ai quali i modem rispondono. I numeri di telefono sono per i modem simili alle password per i sistemi. Altre strategie di difesa sono l'utilizzo di collegamenti monodirezionali, la verifica dell'identificativo del chiamante e il controllo di intercettazioni.

### **Sicurezza delle reti TCP/IP**

Durante gli ultimi anni si è potuto assistere a numerosi attacchi informatici in ambiente TCP/IP. La cosa è dovuta principalmente ai seguenti motivi:

- ❑ il protocollo TCP/IP è stato progettato per operare in ambienti ostili dal punto di vista dell'affidabilità dei collegamenti ma non della sicurezza delle operazioni,
- ❑ non era stato previsto un meccanismo di autenticazione,
- ❑ IP è un protocollo sperimentale ed è in continua evoluzione in quanto oggi viene utilizzato da utenti diversi da quelli per i quali era stato inizialmente pensato.

Il protocollo TCP/IP è progettato per trasmettere pacchetti da un computer all'altro. Non vi è nessuna garanzia che i pacchetti trasmessi non vengano intercettati. L'unico metodo per proteggersi da tale pericolo consiste nel codificare i pacchetti di dati. Esistono alcuni metodi per codificare i pacchetti:

- ❑ codifica a livello di collegamento: i pacchetti vengono codificati e decodificati quando attraversano una rete non sicura; tale funzionalità è oggi fornita solo in alcune reti (reti radio);
- ❑ codifica end-to-end: i pacchetti vengono codificati e decodificati dagli host o dai dispositivi che effettuano il collegamento; oggi esistono router in grado di offrire tale funzionalità;
- ❑ codifica a livello applicativo: esistono applicativi in grado di codificare i pacchetti in transito su una rete, ad esempio il sistema kerberos.

## **Sicurezza dei servizi TCP/IP**

Un accorgimento generale per rendere sicuri i servizi di rete consiste nel rendere sicuro l'accesso ad un sistema che offra servizi di rete. I sistemi Unix offrono oggi alcuni utili strumenti per proteggere un sistema collegato ad una rete. Tali strumenti vengono ormai forniti all'interno del sistema operativo stesso e sono di facile utilizzo.

Nel caso in cui il sistema in uso non offrisse meccanismi di controllo per l'accesso ai servizi di rete è possibile utilizzare due meccanismi principali di difesa e controllo:

- ❑ **TCPWrapper**: programma che si integra ai vari servizi di rete offerti dall'host e ne regola la modalità di utilizzo. Come precedentemente illustrato oggi molti sistemi operativi integrano meccanismi di gestione delle modalità di accesso ai servizi simili al TCPWrapper.
- ❑ **Firewall**: sono in grado di regolamentare l'utilizzo dei servizi di rete. Mentre il TCPWrapper è in grado di proteggere un'unica macchina, un Firewall è in grado di proteggere un'intera rete.

Di seguito vengono illustrati i principali servizi TCP/IP, i loro limiti e le strategie di difesa da perseguire. In generale è bene valutare attentamente quali servizi si intende fornire attraverso un particolare calcolatore e disabilitare tutti quelli che non si intende utilizzare al fine di ridurre i possibili punti di debolezza dell'intero sistema.

- ❑ **Sysstat**: utilizzato per fornire informazioni sullo stato delle connessioni di rete di un calcolatore. Non è particolarmente pericoloso tuttavia può fornire molte informazioni che potrebbero essere utili per un attacco, dunque conviene disabilitarlo.
- ❑ **FTP**: utilizzato per trasferire file. Richiede l'autenticazione utente tramite password, che viene trasmessa in chiaro e dunque è intercettabile. Per questo motivo FTP viene spesso disabilitato.
- ❑ **FTP Anonimo**: può operare in due modalità, attiva e passiva. Nei collegamenti passivi è il client ad iniziare la connessione utilizzata per il trasferimento dei dati vero e proprio. Tale modalità consente una facile configurazione dei sistemi Firewall che possono essere utilizzati per proteggere il server FTP. Oggi la maggior parte dei software client prevede la modalità passiva.
- ❑ **Telnet**: richiede l'invio in chiaro di nome utente e password. Inoltre vengono inviati in chiaro anche tutti i comandi digitati ed è possibile inserirsi in una sessione telnet in corso e digitare comandi all'interno di tale sessione secondo una tecnica detta session hijacking. Tale servizio costituisce dunque un notevole pericolo per la sicurezza del sistema e dell'intera rete locale. Per ovviare ai rischi di sopra è utile utilizzare one-time password e connessioni codificate.

- ❑ **SMTP**: è il protocollo più diffuso per trasferire posta elettronica tra una computer de un altro. Nel mondo Unix esiste un programma *Sendmail* che implementa sia la parte client sia la parte server del sistema di trasferimento della posta. Il problema principale di Sendmail deriva dal fatto che è costituito da un unico programma monolitico che svolge tutte le operazioni e che viene eseguito con privilegi di superuser. Fortunatamente esistono programmi alternativi che suddividono le operazioni in più programmi e che possono essere controllati attraverso TCPWrapper o Firewall.
- ❑ **DNS**: è un database distribuito che consente di ottenere gli indirizzi IP dai nomi degli host. Il trasferimento delle informazioni da un DNS server all'altro costituisce un pericolo per la sicurezza in quanto vengono mandate un rete molte informazioni sugli host della nostra rete. Può essere utile in tal senso limitare le macchine alle quali il nostro DNS invia informazioni. Dal momento che molte applicazioni Unix vengono configurate per controllare gli accessi in base al nome dell'host, un hacker che riuscisse a ottenere le informazioni da un DNS server ed a corrompere il suo database potrebbe compromettere facilmente la sicurezza dei sistemi.
- ❑ **TFTP**: consente il trasferimento dei file senza richiedere password o nome utente. Dal momento che tale servizio è totalmente insicuro andrebbe disabilitato o per lo meno dovrebbero essere limitati i file che si possono trasferire tramite tale protocollo.
- ❑ **Finger**: è in grado di offrire informazioni su utenti collegati ad un sistema e in alcuni sistemi opera con privilegi di root. È possibile allora sfruttare tale servizio per leggere il contenuto di un file qualsiasi. Si consiglia di disabilitare finger o di sostituirlo con uno script di shell.
- ❑ **HTTP**: è il protocollo utilizzato per trasferire e ricevere documenti dal Word Wide Web. Il Web è uno degli aspetti trainanti di Internet e dunque la diffusione del servizio HTTP è ormai capillare. Un aspetto interessante del Web è la possibilità di associare alle pagine Web dei programmi. I server Web sono costituiti da software complesso e dunque presentano dei rischi. Inoltre, la presenza di script CGI complica ulteriormente il sistema rendendolo ancora più vulnerabile.
- ❑ **POP**: permette ad un utente di accedere alla propria casella di mail per accedere ai propri file senza bisogno di dover montare dei dischi di rete. In genere i client ed i server POP utilizzano un nome utente ed una password per verificare l'identità di un utente. Dunque il servizio può essere monitorato da uno sniffer per rubare nomi utenti e password. Esistono tuttavia alcuni server più sicuri che utilizzano password criptate o addirittura l'autenticazione kerberos.

## **Monitoraggio della rete**

Lo strumento principale per monitorare le connessioni di rete in ambiente Unix è *netstat*. Utilizzando tale strumento con le varie opzioni ad esso associate è possibile analizzare l'utilizzo di ogni servizio.

Esistono tuttavia molti programmi e tool per monitorare la rete ed i suoi punti critici. Tra i vari disponibili si ricordano SATAN, IIS (Internet Security Scanner) e PingWare.

## INDICE

### **Introduzione**

*Paolo Cremascoli e Andrea Mauro*

Introduzione storica.....	1
Introduzione a Linux .....	2
Linux come server.....	3

### **Internetworking per reti aziendali**

*Luciano Ghezzi*

La gestione della posta elettronica .....	4
Il proxy gerarchico per l'accesso al web.....	5
Linux come router per l'accesso "intelligente" ad internet .....	5
Autenticazione centralizzata dei servizi proxy, posta e web .....	7

### **Dispositivi di memorizzazione di massa fault-tolerant**

*Andrea Gelmini*

RAID .....	8
------------	---

### **Integrazione in reti eterogenee**

*Michele Bonera e Marco Ghidinelli*

Mainframe/sistemi host .....	9
Linux e macintosh.....	10
Linux e novell netware .....	11
Il mondo windows/lan manager.....	12
Dhcp - domain host configuration protocol.....	13
Esercitazione pratica .....	13
Considerazioni finali .....	14


### **Sicurezza dei sistemi e delle reti**

*Paolo Colombini e Francesco Tomasoni*

Strategie di realizzazione di un sistema di sicurezza .....	17
La sicurezza a livello di sistema .....	17
La sicurezza a livello di rete .....	19


## IL LUG BRESCIA


Da dove partire:

 <http://lugbs.linux.it> *sito web*

Per contattarci:

 <mailto:lug@lugbs.linux.it> *per contattare tutti i "soci"*

 <mailto:lug-attivisti@lugbs.linux.it> *per contattare gli "attivisti"*

 <mailto:lug-cd@lugbs.linux.it> *per richiedere i CD del lugBS*