Linux: come avere tutta la sicurezza

Il problema: avere la garanzia della sicurezza e della riservatezza del proprio sistema e dei propri dati, soprattutto nel caso in cui il computer sia condiviso tra più utenti, sia accessibile da parte di estranei o si stia navigando in Internet

La soluzione: Linux implementa i tradizionali metodi di sicurezza di tutti i sistemi Unix, quali l'accesso limitato ai soli utenti registrati e protetto da password, la creazione di gruppi di utenti e il sistema dei permessi a livello di file

Avrete spesso sentito dire o letto che Linux è un sistema "sicuro". Effettivamente questo sistema operativo, così come più in generale tutte le varie versioni di Unix, offre la possibilità di impostare la propria macchina in modo da garantire agli utenti un grande livello di sicurezza, sia nell'accesso locale che in quello in rete. Non tutti però conoscono bene come viene gestita la sicurezza in un sistema operativo Unix e quindi spesso non sfruttano tutte le potenzialità messe a disposizione dalla propria macchina; in alcuni casi una cattiva gestione della sicurezza rischia di compromettere l'integrità del sistema che, se gestito correttamente, risulta uno dei più sicuri disponibili oggi come oggi su computer della classe dei personal.

Gli utenti

Un primo problema riguardo la sicurezza consiste nel permettere l'accesso al sistema solamente alle persone autorizzate, negandolo a chiunque altro. Con Linux per potere accedere al sistema bisogna essere uno degli utenti abilitati. Questo significa che l'amministratore di sistema deve avere inserito nel computer il nostro nominativo e i nostri dati, assegnandoci così un identificativo utente ed una password.

All'avvio del sistema ci troveremo davanti ad una richiesta di login: solo attraverso l'inserimento del nostro nome utente e, subito dopo, della password corretta, avremo la possibilità di accedere al sistema. Se il nome utente non viene riconosciuto o se la password digitata non corrisponde a quella dell'utente inserito l'accesso ci verrà negato. Probabilmente è superfluo dirlo, ma a differenza di altri sistemi operativi, dove semplicemente premendo il tasto Esc si salta la richiesta di password e si accede allegramente al sistema (almeno in locale, dato che restano delle limitazioni per l'accesso ad una eventuale rete), con Linux l'inserimento di nome utente e password è un'operazione indispensabile per potere accedere al sistema e non può essere evitata in alcun modo.

A questo punto molti di voi si staranno chiedendo come sia possibile allora che spesso si legga di siti e computer "crackati", ovvero dove qualcuno di non autorizzato sia riuscito ad accedere al sistema; in realtà ci sono dei modi di accesso per così dire "alternativi", ma non sono assolutamente alla portata dei normali utenti, richiedono una grande esperienza e una profonda conoscenza del sistema e in molti casi possono essere intercettati e quindi è possibile prendere adeguate contromisure. Comunque nella maggior parte dei casi quando un sistema subisce attacchi da parte di estranei e viene violato significa che c'era qualche errore nell'impostazione del sistema di sicurezza del quale l'amministratore non si è accorto.Vediamo ora più nel dettaglio cosa succede quando viene creato un nuovo utente. Prima di tutto gli viene assegnato un numero che permette al sistema di identificarlo in modo univoco: questo numero si chiama *User Id* o, più brevemente, *Uid*. Quindi l'utente viene assegnato ad uno dei gruppi presenti sul sistema e viene specificata la sua shell standard, ovvero il tipo di programma che verrà normalmente utilizzato per permettere a quell'utente di inserire sulla linea di comando le istruzioni necessarie per la gestione dei suoi file, il lancio delle applicazioni e così via. Al nuovo utente viene quindi assegnata la *Home directory*, ovvero una sua cartella personale dove può memorizzare e organizzare tutti i suoi dati (essendo sicuro che non vengano letti da occhi estranei, come vedremo meglio più avanti).

Infine il nuovo utente sceglie il proprio nome identificativo da inserire alla richiesta di login e la password di protezione che permette di autenticarne l'identità.

Questa procedura viene eseguita ogni volta che sul sistema viene registrato un nuovo utente; ricordiamo infatti che Linux, così come tutti i sistemi Unix, è un sistema operativo multiutente e come tale è predisposto in modo nativo alla gestione della presenza su una stessa macchina di più utenti contemporaneamente.

I dati relativi a tutti gli utenti registrati su un sistema vengono memorizzati in un apposito file che si trova generalmente nella directory */etc* e che si chiama *passwd*.

La struttura di questo file è piuttosto semplice: ogni riga contiene i dati di un utente diverso, ordinati a partire dalla login, quindi password, *Uid*, *Id del gruppo*, una eventuale descrizione estesa, il percorso completo della home directory ed infine la shell utilizzata; ognuno di questi dati è separato dal successivo dal simbolo di due punti ":".

Come abbiamo visto nel file *passwd* vengono memorizzate anche le password di tutti gli utenti; ciò che potrà stupire un po' è che questo file non è affatto segretissimo, ma può tranquillamente essere letto da chiunque abbia accesso al sistema. Questo non significa, però che sia semplice carpire la password ad un altro utente. Le password vengono infatti memorizzate in forma criptata e quindi del tutto incomprensibile. Ciò non toglie che, essendo il file leggibile da tutti, qualche malintenzionato possa farsene una copia locale e poi utilizzare tutto il tempo e i mezzi a sua disposizio-

I temi del corso su Linux

Maggio: Le interfacce utente: introduzione al *K desktop environment*, le sue componenti di base, i desktop virtuali, il *Pannello*, l'esecuzione di applicazioni e la gestione delle finestre.
Giugno: Gestire i file con Linux: il *K file manager* e le sue funzioni di base; modalità di visualizzazione, apertura delle cartelle, gestione dei file, il cestino e il drag and drop.
Luglio/Agosto: La gestione dei file: altre funzionalità offerte da *Kfm* come l'associazione dei tipi alle applicazioni, la gestione trasparente dei file remoti attraverso la rete internet e degli archivi compressi.
Settembre: I moduli di configurazione e il *Centro di controllo* di *Kde*: tutte le funzionalità offerte da questo ambiente desktop per impostare funzionalità ed aspetto estetico.
Ottobre: Come collegarsi a Internet gestendo più provider e sfruttando al meglio tutte le risorse messe a disposizione dalla grande rete, utilizzando appositi programmi.
Novembre: Il sistema per la sicurezza: utenti e gruppi, i permessi sui file, l'utente root, sicurezza in rete e virus.
Prossimamente: altri ambienti desktop e window manager diversi da *Kde*, le applicazioni disponibili.

ne per riuscire a decifrare qualche password. Proprio per evitare questo tipo di pericoli la maggior parte dei sistem Linux attuali utilizzano un sistema detto *shadow password*. In pratica le password degli utenti non vengono più memorizzate nel file passwd (dove al loro posto appare una semplice *x*) ma in un altro file (che normalmente si chiama *shadow* e si trova sempre nella directory */etc*) che risulta, però adeguatamente protetto da sguardi indiscreti. Il sistema di *shadow* password consente inoltre di avere un maggiore controllo sugli utenti, aumentando così il livello di sicurezza del sistema; è infatti possibile, ad esempio, impostare una data di validità di una password, scaduta la quale l'utente sarà obbligato a cambiarla, pena la disattivazione della sua login; oppure, al contrario è possibile vietare ad un utente di modificare la propria password (a questo proposito ricordiamo che per modificare la propria password è sufficiente digitare il comando passwd sulla linea di comando, inserire la password attuale e quindi due volte quella nuova).

Andando a curiosare nel file passwd scoprirete che anche su un normale sistema desktop vi sono molti più utenti di quanto ci si aspetti e che la maggior parte di questi utenti non corrispondono ad una persona fisica. Linux infatti, così come tutte le versioni di Unix, utilizza il paradigma degli utenti per gestire molti importanti criteri di sicurezza e quindi per alcuni compiti particolari vengono creati degli utenti specifici. Ad esempio l'utente ftp serve per potere permette l'accesso remoto alla macchina attraverso il protocollo ftp con un accesso di tipo anonimo senza che per questo venga ridotto il livello di sicurezza del sistema.

I gruppi

Come abbiamo detto, quando viene creato un nuovo utente, esso viene assegnato ad un gruppo.

I gruppi non sono altro che delle strutture logiche che permettono di suddividere gli utenti in insiemi di vario tipo.

Il sistema operativo permette di creare nuovi gruppi in qualsiasi momento; in questo modo è possibile suddividere gli utenti in modo ordinato in base alle proprie esigenze.

Ad esempio in un ufficio potrebbero esistere il gruppo *Amministrazione*, il gruppo *Grafica* e il gruppo *Laboratorio*: gli utenti del sistema a secondo del tipo di lavoro che svolgono possono essere assegnati ad un gruppo piuttosto che ad un altro.

Ovviamente è anche possibile che uno stesso utente appartenga a più di un gruppo; infatti il sistema permette l'assegnazione di un utente a più gruppi. In alcune delle distribuzioni Linux, quando si crea un nuovo utente, viene automaticamente creato anche un nuovo gruppo, con lo stesso nome dell'utente, al quale esso viene inizialmente assegnato. Altre distribuzioni utilizzano invece un metodo più tradizionale: generalmente esiste sempre un gruppo *Users*, al quale vengono assegnati tutti gli utenti del sistema.

Chiaramente queste sono solamente le impostazioni iniziali: l'amministratore di sistema può sempre cambiare il gruppo di appartenenza di un utente, oppure assegnarlo ad altri gruppi.

Il sistema di sicurezza del file system

Ora che abbiamo visto che su un sistema Linux esistono utenti e gruppi, vediamo come questo si rifletta sulla gestione della sicurezza, in particolare nel settore del file system.

Una delle principali preoccupazioni di ogni utente, soprattutto nel momento in cui si ritrova a dovere dividere una stessa macchina con altre persone è quella relativa alla sicurezza dei suoi dati personali, ovvero di tutti quei documenti e file da lui creati.

Generalmente ci si preoccupa soprattutto di due aspetti: prima di tutto che i propri dati non vengano (più o meno) accidentalmente cancellati e in secondo luogo che non venga letto da estranei il contenuto (magari riservato) dei propri documenti personali.

Con un sistema come Linux, così come con tutte le altre varianti del sistema Unix, è possibile impostare i parametri di sicurezza in modo da essere ragionevolmente sicuri che non ci possano essere intrusioni di alcun tipo da parte degli altri utenti.

Nel file system di Linux, infatti, è possibile assegnare ad ogni file degli specifici permessi: di lettura, di scrittura e di esecuzione. Questi permessi possono essere impostati in modo del tutto indipendente per tre tipologie d'utenti: il proprietario del file (generalmente chi lo ha creato), gli utenti appartenenti al suo stesso gruppo ed infine tutti gli altri utenti. Attraverso l'uso di una corretta combinazione di questi parametri è possibile impostare con precisione il livello di sicurezza che vogliamo ottenere per un certo file di dati.

Facciamo un esempio concreto: supponiamo che l'utente pcopen stia lavorando su tre documenti, *segreto.txt*, *condiviso.txt* e *pubblico.txt*. Come si può capire dal nome *segreto.txt* è un file personale il cui contenuto non deve venire a conoscenza di altre persone; quindi l'utente pcopen attiverà per questo file i permessi di lettura e scrittura solamente per sé stesso, mentre li disattiverà per gli utenti del suo gruppo e per tutti gli altri. Il file *condiviso.txt*, invece è un documento che viene redatto in stretta collaborazione con gli utenti appartenenti al proprio gruppo, ma il suo contenuto deve restare riservato ai soli componenti del gruppo. Dovremo quindi impostare i parametri di lettura e scrittura per l'utente e per il gruppo e disattivarli per tutti gli altri.

Infine il file *pubblico.txt* contiene informazioni a disposizione di tutti, ma gestite dall'utente pcopen, che non desidera, quindi, che qualcun altro possa modificare i dati in esso presenti. Per ottenere il risultato voluto verranno impostati i permessi di lettura e scrittura per l'utente, mentre per il gruppo e per gli altri verrà attivato il solo parametro di lettura.

Esiste poi la possibilità di impostare alcuni permessi speciali: *Uid*, che significa che chi esegue il file acquisisce temporaneamente gli stessi permessi dell'utente a cui il file appartiene, *Gid*, per indicare che a chi esegue il file vengono assegnati gli stessi permessi del gruppo di appartenenza del possessore del file e Stiky, un vecchio parametro che serviva per mantenere il testo del programma sul device di swap e che oggi non è più molto utilizzato, se non per una particolare gestione delle directory.

Infatti tutti questi permessi possono essere impostati non solo sui normali file ma anche sulle directory (che non sono altro che file un po' speciali); in questo caso alcune impostazioni cambiano leggermente significato. Ad esempio il permesso di esecuzione, nel caso delle directory significa in realtà permesso di accesso all'interno della directory, mentre il permesso di lettura consente di ottenere (da fuori) l'elenco dei file contenuti nella directory e il permesso di scrittura da la possibilità di creare nuovi file all'interno della directory o di cancellare quelli in essa già presenti. Infine il famoso bit Stiky consente di impostare una directory in modo che solo il proprietario della directory o di un file possa rimuovere un file da detta directory.

Questo anche se può sembrare complicato ha in realtà un uso molto pratico: potere avere directory condivise tra tutti gli utenti garantendo ad ognuno un buon livello di sicurezza. Ad esempio il bit Stiky viene spesso utilizzato per la directory temporanea, dove tutti gli utenti possono inserire dei file ma dove, grazie a questa speciale impostazione, un utente non può cancellare i file degli altri.

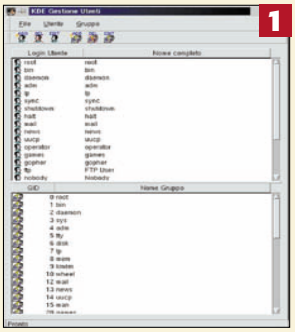
Quindi come abbiamo visto, agendo adeguatamente sui permessi di un file possiamo controllare con estrema precisione le modalità di accesso da parte degli altri utenti ai dati contenuti nel file medesimo.

Alcuni criticano il sistema di sicurezza di Linux in quanto permetterebbe di proteggere solamente i file e non altre componenti del sistema.

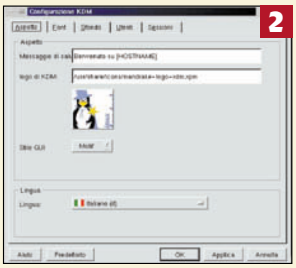
In realtà il sistema di sicurezza di Linux, così come quello di tutti i sistemi Unix, può essere al limite accusato di essere un po' "datato", ma non certo di essere incompleto. Infatti è vero che questo sistema di permessi agisce solamente a livello di file, ma è altrettanto vero che nei sistemi Unix e quindi anche in Linux, tutto, compreso l'hardware del computer, viene visto come se fosse un file. In Linux infatti esiste una directory, */dev*, che contiene un grande numero di file ognuno dei quali in pratica corrisponde ad un particolare dispositivo hardware: dischi, porte seriali, mouse, schede audio e così via.

Quindi se ad esempio si desidera che gli utenti non possano leggere e scrivere dati da un disco floppy, è sufficiente andare nella directory */dev*, selezionare il file *fd0* (che corrisponde a quello che sotto altri sistemi viene visto come *disco floppy a:*) e togliere i permessi di lettura/scrittura. Questo sistema di sicurezza permette, se adeguatamente sfruttato, di impostare il computer in modo che sia, se non proprio impossibile, per lo meno alquanto improbabile che un nor- ▶▶▶

Come configurare correttamente i livelli di sicurezza di Linux per gruppi di utenti a partire dal *login*

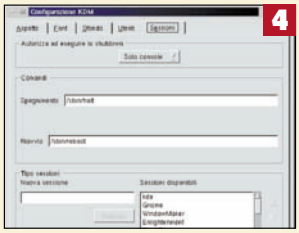


1 Il sistema di sicurezza di Linux prevede la presenza sul sistema di utenti registrati, suddivisi in gruppi. Se non si è stati registrati come utenti sul sistema non è possibile accedervi. In questo modo si impedisce l'accesso al computer da parte di estranei. Per la gestione di *utenti* e *gruppi Kde* mette a disposizione un apposito programma: *Kde Gestione utenti*.



2 Per potere accedere ad un qualsiasi sistema Linux bisogna prima di tutto effettuare l'operazione di *login* che può avvenire sulla linea di comando e in modalità grafica. *Kde* mette a disposizione un proprio programma per la *login* che si chiama *Kdm* e che può essere configurato dettagliatamente attraverso un'apposita interfaccia.

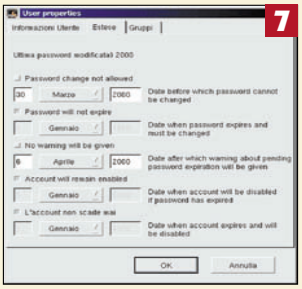
3 Tra le configurazioni possibili vi è anche la scelta degli utenti ai quali è permesso effettuare l'operazione di *login*; in Linux infatti esiste sempre un grande numero di utenti, alcuni dei quali sono nascosti in quanto non corrispondono a delle persone fisiche ma sono utenti virtuali che il sistema utilizza per la gestione della sicurezza e di alcune operazioni particolari.



4 Il programma di *login Kdm* permette anche di effettuare le operazioni di chiusura e di riavvio del sistema, così come di scegliere il tipo di interfaccia grafica da utilizzare una volta connessi al sistema e avviato X Window.

5 Per mezzo del pannello *Kde Gestione utenti* è possibile inserire tutte le informazioni necessarie alla registrazione di un utente, come il *nome*, l'*Id*, la *shell* utilizzata e il *percorso* della directory home.

6 Ogni utente è dotato di una password personale che gli permette di confermare la propria identità durante la fase di *login*.

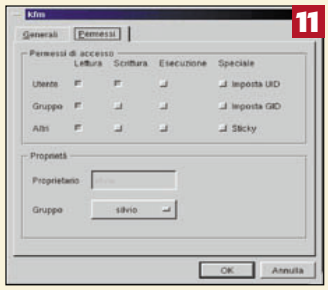


7 Se il sistema è dotato del meccanismo delle *shadow password* o di una funzionalità analoga è possibile impostare anche alcuni parametri avanzati che regolano l'obbligo o meno da parte dell'utente di cambiare la password e la frequenza con cui questa operazione deve essere effettuata.

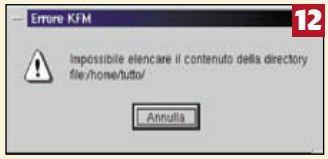
8 Un'altra componente fondamentale del sistema di sicurezza di Linux sono i gruppi, che permettono di suddividere gli utenti in insiemi logici ai quali potere assegnare impostazioni globali a livello di permessi di accesso. Ogni utente può appartenere anche a più di un gruppo contemporaneamente. La struttura di ogni gruppo è costituita da una descrizione e da un numero identificativo, il *Group Id* o più brevemente *Gid* che consente al sistema operativo di identificare in modo univoco il gruppo stesso. L'amministratore di sistema può sempre cambiare il gruppo di appartenenza di un utente, oppure assegnarlo ad altri gruppi secondo necessità interne. Ad esempio in un ufficio potrebbero esistere il gruppo *Amministrazione*, il gruppo *Grafica* e il gruppo *Laboratorio* e l'assegnazione avviene secondo il tipo di lavoro.

9 *Kde Gestione utenti* permette anche la creazione e la configurazione, oltre che di nuovi utenti anche di nuovi gruppi.

10 Una volta creato un nuovo gruppo è possibile assegnargli un numero qualsiasi di utenti che andranno a fare parte di quel particolare gruppo.



11 Le informazioni riguardanti *utente* e *gruppo* vengono poi utilizzati per impostare i permessi a livello di file; in questo modo è possibile impostare con estrema precisione il livello di protezione che si desidera raggiungere.



12 Se si tenta di eseguire un'operazione per la quale non si hanno i permessi necessari, il sistema blocca l'operazione e ci da un avviso sull'impossibilità di portare a termine l'operazione richiesta.

male utente possa fare dei danni. Ad esempio tutti file indispensabili al buon funzionamento del sistema, come librerie o file di configurazione, vengono impostati con dei permessi tali da non consentirne la cancellazione; in questo modo un normale utente non potrà compromettere la stabilità del sistema nemmeno per errore.

Generalmente la maggior parte delle distribuzioni Linux installa un sistema con dei parametri di sicurezza già adeguatamente configurati, almeno per garantire un livello di sicurezza sufficiente per il normale uso del computer come desktop. Quindi quando si comincia ad utilizzare un sistema Linux ci si può concentrare sull'impostazione della sicurezza dei propri dati, senza doversi troppo preoccupare della sicurezza generale di tutto il sistema.

L'amministrazione del sistema e l'*utente root*

Proprio grazie al sistema di permessi associati ai file che abbiamo appena visto, vi sono delle operazioni che in Linux sono precluse ad un normale utente: modificare i file di configurazione, installare nuove applicazioni di sistema, accedere ad alcune zone del disco o del tutto ad alcuni dischi, creare nuovi utenti ed altro ancora.

Chiaramente però molte di queste operazioni sono necessarie per la corretta amministrazione ed il mantenimento del sistema; come è possibile effettuarle? Semplicemente ricorrendo ad un utente un po' speciale.

Questo utente così speciale e potente viene generalmente indicato con il termine *superuser* e la sua login è *root*. Quando in un sistema Linux si esegue con successo l'operazione di login come utente root, ci si ritrova l'intero sistema a propria completa disposizione.

Infatti l'*utente root*, appartenente al gruppo root non è soggetto alle restrizioni imposte dal sistema di sicurezza e dai permessi sui file. Viceversa nessun altro utente è in grado di accedere ad un file o ad una directory appartenenti all'*utente root*, a meno che questi non lo abbia esplicitamente permesso. Quindi accedere ad un sistema Linux come root da sì un grande controllo sul sistema, ma mette anche a disposizione una potenza che bisogna conoscere e sapere controllare: quando si è collegati come *utente root* è molto facile fare dei danni, anche molto gravi.

Molti usano il proprio sistema Linux direttamente come *utenti root*. Questo comportamento è assolutamente da evitare in quanto si rischia di danneggiare il sistema anche solo per errore o per distrazione. Non appena terminata l'installazione del sistema bisogna sempre creare un utente, che non goda di particolari privilegi, con il quale lavorare quotidianamente. L'accesso al sistema come *root* va riservato ai momenti in cui sia necessario svolgere il ruolo di amministratore di sistema.

A questo punto si sarà capito che l'*utente root* è, oltre che potente, un po' pericoloso, quindi la sua password di accesso è normalmente uno dei dati più preziosi e meglio custoditi di ogni sistema Unix. Si tenga conto che quando qualcuno riesce a penetrare all'interno di un sistema Unix e a fare danni seri quasi sempre significa che è riuscito a carpire la password dell'*utente root* e a collegarsi al sistema come *superuser*.

Ovviamente per chi utilizza Linux come sistema desktop e non come server, è possibile prendere qualche precauzione in meno nella conservazione della segretezza della password dell'*utente root*. Comunque l'accesso come *superuser* va utilizzato con parsimonia e con cognizione di causa.

A volte nell'uso del sistema come desktop capita di dovere svolgere al volo un'operazione per la quale servirebbero i permessi dell'utente root. Per risolvere questo tipo di problemi è possibile ricorrere al comando *Su (superuser)*.

Questa istruzione che è possibile digitare sulla linea di comando, non fa altro che lanciare una shell con *Id* del gruppo e dell'utente differenti dai propri. Con appositi parametri è possibile comunicare a *Su* quale utente si desidera impersonare; se *Su* viene lanciato senza alcun parametro si suppone che si desideri avere una shell con i permessi dell'*utente root*.

Quindi digitando sulla linea di comando *Su* e premendo invio vi verrà chiesta la password dell'*utente root*; fornendola in modo corretto si otterrà una shell con gli stessi permessi del superuser e quindi perfettamente adatta per effettuare qualsiasi operazione di amministrazione.

Normalmente *Su* mette a disposizione queste shell per un periodo limitato di tempo, ovvero trascorso un po' di tempo dall'ultima operazione effettuata il programma su termina e si ritorna alla normale shell di partenza. Ciò è stato fatto per ragioni di sicurezza: se qualcuno si dimenticasse di avere aperto una shell come root e si assentasse dal suo computer, chiunque passasse di lì per caso e notasse la cosa potrebbe approfittarne e manomettere il sistema.

Sempre nell'uso del sistema come desktop vi possono essere operazioni comuni che non sono permesse ai normali utenti, come ad esempio scrivere dei dati su un floppy o su un'altra partizione del disco fisso.

Generalmente l'impossibilità di eseguire queste operazioni dipende da alcune impostazioni generali del sistema di sicurezza, quindi piuttosto che collegarsi come *root* ogni volta che si devono eseguire queste operazioni o, peggio, utilizzare sempre il sistema come *root*, conviene documentarsi un po' e scoprire come modificare le impostazioni di sistema per permettere alcune operazioni particolari anche agli utenti normali.

La sicurezza per gli accessi in rete

Essendo un sistema operativo in grado di funzionare anche come server, Linux prevede anche un sistema di protezione per gli accessi via rete da parte di altri computer. Il sistema di sicurezza è molto articolato e va dall'esistenza di appositi utenti, ad esempio per gli accessi ftp e http, fino alla possibilità di specificare in modo selettivo gli indirizzi *Ip* di tutti e soli i computer che hanno il permesso di accesso. Ovviamente questi criteri di sicurezza sono importanti soprattutto nel momento in cui si configura un computer per funzionare come server di rete. Anche in modalità desktop, però avere un sistema sicuro e protetto da accessi remoti indesiderati può tornare molto utile: ad esempio Linux è un ottimo sistema per la navigazione in Internet.

Come si difende dai virus

Linux offre una maggiore sicurezza anche nei confronti degli attacchi da virus. Ovviamente è sempre possibile realizzare un virus particolarmente ingegnoso in grado di fare danni anche su un sistema Unix, però utilizzando Linux come sistema operativo, le possibilità di essere infettati e di subire dei danni da parte di un virus sono decisamente ridotte, soprattutto se messe a confronto con quelle caratteristiche di altri sistemi operativi.

Questa affermazione si basa su tre considerazioni: prima di tutto il numero di virus circolanti e funzionanti su Linux è molto più ridotto rispetto al numero di virus dedicati ad altre piattaforme; in secondo luogo realizzare un virus per un sistema Unix è piuttosto difficile e richiede una notevole esperienza; infine il sistema di protezione di Linux evita il successo almeno degli attacchi più banali.

Infatti quando ad esempio si scarica un file da internet, questo viene registrato sul disco fisso come appartenente all'utente che lo ha scaricato; quando si tratta di un file eseguibile, quindi esso godrà degli stessi permessi dell'utente che lo ha memorizzato. Se utilizzate il sistema collegandovi come un normale utente, quindi, un eventuale virus non avrà i permessi necessari a danneggiare il sistema operativo o parti di esso fondamentali per un corretto funzionamento. In teoria un virus particolarmente furbo potrebbe lavorare in silenzio per riuscire a guadagnarsi un accesso al sistema come root, ma come dicevamo non è affatto semplice realizzare un programma di questo tipo.

Ad esempio molti di voi si ricorderanno del virus *I love you* che qualche mese fa fece tali e tanti danni da costituire addirittura una notizia degna dei telegiornali di tutto il mondo.

Ebbene questo virus era scritto in Visual Basic Script (un linguaggio di programmazione piuttosto semplice) ed era essenzialmente elementare nella sua struttura, a tratti perfino banale. Insomma per riuscire a scrivere un virus di questo tipo non bisogna certo essere dei grandi conoscitori del funzionamento interno di un sistema operativo, ma semplicemente avere un po' di esperienza e di malizia. Con Linux questo virus non ha alcun effetto (non è neanche possibile eseguirlo) e dubitiamo molto che si possa scrivere un virus per Linux altrettanto semplice e con mezzi così poveri che faccia un qualsiasi tipo di danno. Ovviamente se usate normalmente il sistema come root e scaricate un virus, anche banale, allora potreste essere nei pasticci; ma ve la siete un po' cercata. ●