LINUX DAY II

SICUREZZA DEI SISTEMI E DELLE RETI

Autore: Paolo Colombini

1. Introduzione: la sicurezza informatica

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.

Il numero di incidenti inerenti la sicurezza informatica riportati al Computer Emergency Response Team Coordination Center (CERT-CC) aumenta ogni anno : nel 1989 venivano riferiti 200 incidenti, nel 1991 400, nel 1993 1400 e 2241 nel 1994. Violazioni della sicurezza informatica si verificano oggi ai danni di enti militari, governi, università ed aziende. Alcune di queste intrusioni riguardano singoli account su calcolatori mentre altre risultano più complesse. Tuttavia tali incidenti costituiscono solamente una piccola parte del fenomeno, in quanto molte violazioni non vengono rese note ed a questo va aggiunto che il più della volte le società vittime di un attacco informatico sono restie a denunciare il fatto per una questione di immagine aziendale.

Nessuno oggi 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 informatici 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. E' utile sottolineare che il 40% di tali attacchi comportava l'accesso ai sistemi vittima 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. E' 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. E' compito di coloro che sono preposti all'amministrazione dei vari siti aggiornare i propri sistemi al fine di renderli sicuri.
E' 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.

2. Minacce informatiche

Punti critici

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.

Tipologie di attacchi

Intrusioni

Le intrusioni sono costituite da tutte quelle operazioni che permettono l'accesso non autorizzato ad un sistema.

Sabotaggio

Il sabotaggio costituisce un 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.
Con il termine furto di informazioni si intendono tutti gli attacchi il cui fine è quello di venire in possesso di informazioni che dovrebbero rimanere riservate.

Tipologie di attaccanti

Joyrider

I Joyrider tentano di penetrare all'interno dei sistemi informatici per svago o per curiosità. Spesso danneggiano i sistemi presi di mira in modo non calcolato, 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

I vandali rappresentano il pericolo maggiore per un sito connesso ad Internet. Il loro scopo principale è infatti 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 cercano di violare i sistemi di sicurezza senza alcuna finalità particolare, se non quella di riuscire in tale operazione.

Spie

Le spie, di tipo industriale o meno, costituiscono la categoria di attaccanti più difficilmente rilevabile. Tali personaggi 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. I loro attacchi non lasciano tracce ed i furti vengono abilmente camuffati.

Stupidità ed Incidenti

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 tener conto della possibilità che tali evenienze si verifichino.

3. Tipologie di protezione

Mancanza di sicurezza e nessuna connessione

Esistono due atteggiamenti estremi nei confronti del problema sicurezza : il primo consiste nel disinteressarsi di tutti i meccanismi di protezione, il secondo, diametralmente opposto, consiste nel decidere di non connettersi ad Internet per non correre alcun rischio. Entrambi gli atteggiamenti risultano perdenti, tuttavia negli ultimi anni costituivano il modus vivendi di molte aziende.

Sicurezza attraverso la riservatezza

Un possibile metodo per rendere un sito sicuro 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

I sistemi di sicurezza applicati alle singole macchine sono sicuramente quelli maggiormente utilizzati. Tuttavia tale modo di operare non è applicabile su larga scala.

Sistemi di sicurezza applicati alla rete locale

Nel caso in cui il sito disponga di molte macchine, si preferisce applicare un sistema di sicurezza all'intera rete. In tal caso ci si concentra sul controllo del traffico in entrata ed uscita e si cerca di rendere sicura la rete nel suo complesso, piuttosto ché concentrarsi su ogni singola macchina. La sicurezza di una 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.

Considerazioni

Nella progettazione di un sistema di sicurezza bisogna tener conto di alcuni assiomi fondamentali. Nessun sistema Unix 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. Spesso allora il progetto di un sistema per la protezione di una rete deriva da un compromesso tra sicurezza ed efficienza della rete in questione. Bisogna poi tener conto del fatto che nessun sistema di sicurezza tradizionale è in grado di coprire da solo l'intero spettro dei possibili pericoli ; per questo è necessario avvalersi di più sistemi. I Firewall costituiscono ad oggi il miglior compromesso tra efficienza della rete e affidabilità del sistema di sicurezza. Possono poi essere integrati con la rete in modo trasparente per gli utenti interni, e, se opportunamente progettati e configurati, costituiscono una barriera ad oggi insormontabile per i possibili attaccanti esterni. Essi inoltre costituiscono un utile strumento di lavoro in quanto permettono il monitoraggio del traffico in entrata ed in uscita.

4. 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 ma importante compito è definire politiche, standard e procedure necessarie a rendere proficuo il denaro ed il tempo speso nella prima fase.
Infine il personale addetto alla sicurezza si deve preoccupare di monitorare i sistemi in maniera da assicurarsi che le varie politiche di sicurezza vengano realmente attuate e che siano conformi con gli obiettivi preposti.

La sicurezza sempre più coinvolge aspetti gestionali ed amministrativi e non solo tecnici per cui devono essere coinvolti nel suo sviluppo anche gli amministratore dell'azienda o ente interessato.

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

1. **Pianificazione**

   Le categorie che vanno considerate in fase di pianificazione sono le seguenti:

   RISERVATEZZA

   Proteggere informazioni non pericolose di per sé, ma che potrebbero venire utilizzate per ricavare altre informazioni utili per un attacco.

   INTEGRITA' DEI DATI

   Impedire che dei dati vengano cancellati o modificati senza l'autorizzazione del proprietario.

   DISPONIBILITA'

   Proteggere i propri servizi in maniera tale che non siano fermati o resi indisponibili senza autorizzazione.

   CONSISTENZA

   Fare in modo che il sistema si comporti nella maniera attesa dagli utenti.

   CONTROLLO

   Regolamentare gli accessi al sistema.

   REGISTRAZIONE

   Sviluppare un sistema che sia in grado di tenere traccia di ciò che è stato fatto.

   Sebbene tali aspetti presentino tutti una notevole importanza, questa ultima varia profondamente a seconda del tipo di ente o organizzazione che intende sviluppare il sistema di sicurezza.

2. **Valutazione dei rischi**

   Il primo passo da compiere nello sviluppo di un sistema informativo è quello di rispondere alle seguenti domande:

- Che cosa sto cercando do proteggere
- Contro quali pericoli mi voglio proteggere
- Quanto tempo e denaro intendo investire per sviluppare il sistema di protezione

La fase di analisi dei rischi è molto importante, in quanto è impossibile difendersi da ciò che non si conosce.

3. Analisi costi/benefici

Una volta 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:

- costo della perdita
- costo della prevenzione

Una volta terminata l'analisi sarà possibile disporre di un quadro completo della situazione e poter prendere le decisioni adeguate.

4. 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.

- Scopo di una politica

  Le politiche hanno tre scopi principali. Il primo è quello di rendere chiaro che cosa si vuole proteggere e perché. Il secondo è quello di fissare le responsabilità per una determinata protezione, ed infine il terzo, fornire uno strumento attraverso il quale poter risolvere eventuali problemi che potrebbero insorgere.

- Standard

  Gli standard servono per codificare dei comportamenti ai quali ci si deve attenere per mettere in pratica le politiche di sicurezza.
  Generalmente sono indipendenti dal tipo di piattaforma e variano di poco nel tempo.

- Linee guida

  Le linee guida sono di solito delle istruzioni utilizzate per interpretare gli standard e per illustrarne il funzionamento in particolari contesti.

5. Implementazione del sistema

La fase di implementazione del sistema comprende tutte le operazioni necessarie allo sviluppo tecnico del sistema di sicurezza. Nei paragrafi a seguire verranno illustrate alcune delle più comuni strategie di implementazione.

6. 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.

5. La sicurezza a livello di sistema

Nel corso del seguente paragrafo verranno illustrati alcuni concetti generali sulla sicurezza di un sistema singolo. In particolare verrà presa in esame a titolo di esempio la sicurezza di un sistema Unix.

5.1 Utenti ed account

Nei sistemi Unix ogni utente è identificato attraverso un *Nome utente* ed una *Password.*
Tali informazioni sono mantenute in un file */etc/passwd*. Le password sono registrate in maniera criptata secondo un particolare algoritmo. Talvolta poi la password stessa non viene registrata nel file ma viene salvata in un file diverso detto *shadow password file.*

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 Distribuited Computing Environment (DCE)
- NeXT Computer's NetInfo

Modificare la propria Password

Una delle prime operazioni da svolgere consiste nel modificare la propria Password.
Tale operazione è direttamente effettuabile dall'utente, sia che si stia utilizzando un file /etc/passwd locale, sia che si stia utilizzando un sistema di autenticazione via rete.
La modifica della propria password andrebbe ripetuta periodicamente al fine di aumentare la sicurezza e pararsi da eventuali fughe di notizie pericolose.

Scelta di una "buona" Password

Molti degli attacchi informatici sono stati effettuati in seguito alla scoperta della password di qualche utente.
E' necessario riporre particolare attenzione nella scelta delle password. Alcuni suggerimenti potrebbero essere:

- Utilizzare caratteri maiuscoli e minuscoli
- Utilizzare caratteri e lettere
- Utilizzare i caratteri di controllo e spazi
- Utilizzare password di facile memorizzazione al fine di non dover scrivere la password
- Utilizzare password di almeno 7 o 8 caratteri

Password su più macchine

Molti utenti utilizzano più macchine ed hanno la necessità di dover memorizzare più password.
In tal caso sono da tenere presenti due suggerimenti:

- Non utilizzare la stessa password per tutti i sistemi, altrimenti una volta scoperta la password di un sistema, tutti i sistemi della rete potrebbero essere a rischio di attacco.
- Non utilizzare password eccessivamente diverse per il medesimo account al fine di non dimenticarle o peggio doverle scrivere.

One time password

Il metodo più sicuro consiste nell'utilizzo di password che devono essere modificate ogni volta che vengono utilizzate. Tale metodo è scarsamente utilizzato nonostante la sua efficacia.

5.2 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 controllarne la sicurezza. Inoltre deve sviluppare tutti quegli accorgimenti atti a rendere sicuro un account.
Di seguito saranno analizzati i vari aspetti da tenere sotto controllo ed alcuni dei più comuni accorgimenti da seguire.

Account senza una password

Una account senza una password rappresenta un punto di accesso al nostro sistema. Chiunque conosca il nome dell'account può entrare nel nostro sistema.
Molti sistemi presentano account senza password. Talvolta l'amministratore di sistema crea account vuoti lasciando agli utenti il compito di inserire la password. Gli utenti spesso dimenticano di svolgere tale operazione o la ritardano mettendo a repentaglio la sicurezza dell'intero sistema.
Tramite semplici script di shell o tools è possibile monitorare tali account e scoprirne l'esistenza.

Default account

I sistemi Unix (ed anche molti altri sistemi) vengono installati con alcuni account di default. Tali account molto spesso utilizzano delle password standard. E' necessario disabilitare tali account o modificarne al più presto le password prima che qualche malintenzionato provi a penetrare nel nostro sistema.

Account che eseguono un singolo comando

Unix permette la creazione di account che semplicemente eseguono un comando quando l'utente tenta di collegarsi al sistema. Tali account non hanno password. Bisogna assicurarsi che tali programmi non consentano a chi di collega delle funzionalità interattive inaspettate.

Account aperti

Molti sistemi prevedono di default la presenza di account senza password da utilizzarsi per ospiti o visitatori che possono usare i sistemi per svago o informazioni. Tali account possono essere utilizzati per avere un primo accesso al sistema dal quale poi condurre attacchi più consistenti.
Per questo motivo tali account andrebbero disabilitati.

Account di gruppo

Talvolta molti utenti utilizzano il medesimo account. Tale modo di operare è comune in quelle realtà ove più persone lavorano allo stesso progetto o con gli stessi file.
Tale modo di operare è tuttavia pericoloso, in quanto non consente di individuare eventuali responsabili a fronte di attacchi o inconvenienti legati a quel particolare account. Inoltre non garantisce alcuna riservatezza per gli utenti dell'account e porta inevitabilmente alla diffusione di informazioni riservate.

Restrizione di un Account

In alcuni sistemi è possibile consentire l'accesso ad un particolare account solo in alcuni momenti specificando l'ora o il giorno della settimana. Nel caso in cui un particolare account venga utilizzato solamente in alcuni momenti della giornata, conviene utilizzare tali restrizioni in maniera tale da scoprire più velocemente eventuali utilizzi non previsti dell'account in questione.
Nei sistemi Unix, ove non fossero presenti strumenti per limitare l'utilizzo degli account, possibile creare dei semplici script di shell che svolgano tale funzione.

Disabilitare account non utilizzati

Nel caso in cui un utente non utilizzi un determinato account per un certo periodo di tempo, conviene disabilitare temporaneamente l'account in maniera tale che non possa essere utilizzato per scopi maligni.

5.3L'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 mando Unix corrisponde all'utente root, nel mondo Microsoft addministrator, nel mondo OS400 qsecofr e cosi via.
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.

Cambiare la password

Talvolta i sistemi vengono installati utilizzando password comuni o peggio ancora quelle di default. Altre volte la password del superuser è addirittura lasciata vuota!!!.
La prima operazione da svolgere è quella di cambiare la password del superuser. Inoltre tale password andrebbe modificata ogni qual volta per vari motivi sia stato necessario rivelarla ad altre persone quali tecnici esterni o colleghi.

Restringere l'accesso

In molti sistemi operativi tra cui Unix è possibile accedere direttamente all'account di superuser solamente se si sta utilizzando la consolle del sistema. E' comunque possibile rilasciare tale vincolo.
Dal momento che un utente autorizzato può comunque diventare superuser una volta entrato in un sistema si ritiene utile limitare l'accesso diretta al sistema come superuser solamente dalla consolle al fine di realizzare anche un meccanismo di sicurezza fisica dell'account di superuser.

Gestione delle autorizzazioni

In alcuni sistemi è possibile limitare gli utenti che hanno accesso a programmi come *su* di Linux che consentono di diventare superuser (conoscendone le password). E' utile limitare al minimo indispensabile il numero di utenti che possono utilizzare tali programmi.

5.4 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 di alterazioni ai file
- prevenzione di cancellazioni di file
- riconoscimento di modifiche o cancellazioni di file
- ripristino di file in seguito a cancellazioni o alterazioni

Prevenzione

Lo scopo della prevenzione è quello di impedire a persone non autorizzate la modifica o la cancellazione di file. Gli accorgimenti base per realizzare un primo meccanismo di sicurezza consistono nell'agire opportunamente sui permessi di file e directory, limitare l'accesso all'account di root e regolamentare l'accesso a filesystem di rete.

Esistono poi accorgimenti più specifici che tuttavia dipendono dalla particolare versione di sistema operativo che si sta utilizzando. Alcuni sistemi permettono infatti di definire alcuni file come *immutabili* o *append-only*.

Altri accorgimenti consistono poi nel limitare la visibilità del filesystem a determinati account, permettendo a determinati utenti di operare in una zona limitata del filesystem secondo una modalità detta *chrooted*.

Rilevazione

Come anticipato il monitoraggio del sistema costituisce un aspetto fondamentale dello sviluppo di un sistema di sicurezza.

In particolare 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 con copie

  Il metodo più diretto e sicuro per scoprire modifiche a file è quello di effettuare confronti bit a bit con copie. Tali confronti possono essere effettuati tramite copie locali, copie su nastro o copie remote via rete.

- monitorare i metadata

  Effettuare i confronti bit a bit può essere molto oneroso e talvolta comporta una quantità di tempo notevole. Un metodo più rapito si basa sul controllo dei metadata di un file, ovvero su quelle informazioni aggiuntive che caratterizzano ogni file come la data di creazione o di modifica.

- utilizzo di segnature

  Il monitoraggio dei metadata può essere talvolta ingannato da un attaccante esperto che può modificare anche tali informazioni. Il controllo delle checksum e delle segnature di un file è invece difficilmente ingannabile.

Infine esistono tools che mantengono traccia di tutte le modifiche effettuate sui file del sistema e che risultano molto utili per l'analisi ed il monitoraggio.

5.5 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.
Tali file sono 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. E' possibile ad esempio utilizzare PC di basso costo (486 o 386) sui quali salvare via rete i file di log di un sistema più complesso.
Un'altra raccomandazione è poi quella di effettuare backup periodici dei propri file di log.

5.6 Software pericoloso

Esistono molti software giudicati pericolosi. Tali software possono essere riassunti nelle seguenti categorie:

- Security tools and toolkit

  Sono strumenti utilizzati dagli amministratori di sistema. Tuttavia possono venire utilizzati da persone non autorizzate per tentare di forzare i sistemi.

- Back doors

  Sono scappatoie che consentono l'accesso al sistema.

- Logic bombs

  Sono istruzioni nascoste all'interno dei programmi che entrano in funzione in determinate condizioni

- Viruses

  Programmi in grado di modificare altri programmi inserendo copie di sé stessi

- Worms

Programmi che si propagano da un computer all'altro senza necessariamente modificare programmi.

- Trojan Horses

Programmi che apparentemente svolgono una funzione ma in verità fanno altro.

- Bacteria o Rabbit Programs

Programmi che eseguono copie di sé stessi per sovrascrivere risorse o programmi del sistema.

Strategie di difesa

In generale i pericoli maggiori che si possono incontrare nel mondo Unix sono le Back Door ed i Troian Horses. In generale gli attacchi comportano:

- alterazioni della shell
- alterazioni delle procedure di start up
- modifica di alcune procedure automatiche
- 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.
Inoltre bisogna riporre particolare attenzione a tutti quelle modifiche che riguardano file di sistema o comandi di shell.

6 La sicurezza a livello di rete

Nel seguente paragrafo verranno analizzati gli aspetti critici della sicurezza nell'ambito delle reti e le strategie generali per lo sviluppo di sistemi di sicurezza.
In particolare saranno presi in considerazione i seguenti aspetti:

- **Sicurezza dei collegamenti telefonici**
- **Sicurezza delle reti TCP/IP**
- **Sicurezza dei servizi TCP/IP**
- **Sicurezza dei server WWW**

6.1 Sicurezza dei collegamenti telefonici

I modem costituisco 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. Conoscendo il numero di telefono di un modem è possibile cercare di configurarlo remotamente per entrare nelle reti.
Le strategie principale di difesa dei numeri telefonici sono le seguenti:

- **Utilizzo di collegamenti monodirezionali**

  Molti modem e sistemi supportano modalità di collegamento bidirezionali. Ovvero un modem può essere utilizzato sia per ricevere sia per effettuare chiamate. Tale modalità di lavoro è detta call back.
  Al fine di controllare e rendere sicuri i collegamenti conviene evitare di utilizzare lo stesso modem per chiamate in entrata ed in uscita ma consentire solamente chiamate monodirezioanali. Inoltre sarebbe consigliabile limitare i numeri di telefono che possono essere chiamati in maniera tale da evitare che sconosciuti utilizzino la funzionalità di call back.

- **Identificativo del chiamante**

  Alcuni sistemi sono in grado di identificare il numero di telefono del chiamante. Ina tal modo è possibile capire chi sta chiamando i nostri sistemi. Limitare i collegamenti in base all'identificativo del chiamante rende particolarmente sicuri i sistemi e permette di identificare l'identità di chi cerca di utilizzare la linea.

- **Controllo di intercettazioni**

  Alcune linee telefoniche possono essere intercettate ed utilizzate in maniera abusiva. In particolare i telefoni cellulari possono essere clonati. Conviene allora monitorare i collegamenti e se necessario richiedere alla compagnia telefonica il controllo della linea.

6.2 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.

Strategie di sicurezza

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 aggi fornita solamente in alcune reti come le reti radio. Non è disponibile su tutti i tipi di reti.

- **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.

6.3 Sicurezza dei servizi TCP/IP

Connettere i propri sistemi ad Internet è un'operazione da effettuare con molta attenzione a causa dei problemi di sicurezza presenti nel protocollo TCP/IP e nei sistemi Unix.
Tali problemi non derivano da limiti dei sistemi ma dalla loro notevole versatilità che comporta dei limiti nella sicurezza.

Accesso al sistema

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**

  TCPWrapper è stato scritto da Wietse Venema. Esso rappresenta un 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 si gestione delle modalità di accesso ai servizi simili al TCPWrapper.

- **Firewall**

  E' possibile posizionare tra il proprio sistema di rete ed Internet un sistema Firewall. Un Firewall è in grado di regolamentare l'utilizzo dei servizi di rete. Mentre il TCPWrapper è in grado di proteggere un'unica machina, un Firewall è in grado di proteggere un'intera rete.

I principali servizi TCP/IP

Nella seguente sezione vengono illustrati i principali servizi TCP/IP, i loro limiti e le strategie di difesa da perseguire. Alcuni servizi sono particolarmente pericolosi, mentre altri meno. 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.

Systat

Systat è un servizio utilizzato per fornire informazioni sullo stato delle connessioni di rete di un calcolatore.
Tale servizio non è particolarmente pericoloso tuttavia fornire molte informazioni che potrebbero essere utili per un attacco, dunque conviene disabilitarlo.

FTP

Il servizio FTP utilizzato per trasferire file richiede l'autenticazione utente tramite password. Tale password viene trasmessa in chiaro e dunque è intercettabile. Per questo motivi spesso il servizio FTP viene disabilitato.

- **FTP Anonimo**

  Una delle modalità più comuni di utilizzo del servizio FTP è la modalità anonima. Tale servizio 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

Telnet richiede l'invio in chiaro di nome utente e password. Inoltre vengono inviati in chiaro anche tutti i comandi digitati. Inoltre è possibile inserirsi in una sessione telnet in corso e digitare comandi all'interno di tale sessione secondo una tecnica detta *session haijacking*. 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.
Inoltre è utile utilizzare diverse password per gli utenti di sistemi che offrono il servizio Telnet, in maniera tale che se una macchina viene compromessa non venga compromessa tutta la rete.

SMTP

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.
Sendmail è stato a lungo uno dei mezzi utilizzati per condurre attacchi informatici in quanto:

- le prime versioni di sendmail permettevano di inviare i file di posta ad un file qualsiasi del sistema, inclusi /etc/passwd.
- Sendmail consente di ottenere una shell su un sistema remoto senza la necessità di entrarvi.
- Sendmail può essere compilato in modalità *debug-mode* che in passati ha consentito l'accesso ai sistemi sui quali sendmail era operativo.
- Sendmail ha una meccanismo di controllo dei job non molto efficiente e dunque è stato utilizzato per inviare ai sistemi comandi dall'effetto pericoloso.

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.
Nel caso in cui si decida di utilizzare comunque Sendmail è necessario installare sempre la versione più aggiornata in quanto i vari problemi di sicurezza di Sendmai vengono costantemente monitorati e corretti.

DNS

Il DNS rappresenta un database distribuito che consente di ottenere gli indirizzi IP dai nomi degli host. Il DNS utilizza sia il protocollo TCP/IP sia il protocollo UDP per trasferire le informazioni di cui necessita tra un host

e l'altro. 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.
E' possibile limitare le modifiche del database del DNS attraverso i seguenti accorgimenti:

- Eseguire il servizio DNS su una macchina dedicata che non dispone di account
- Assicurarsi che i file e le directory utilizzate dal DNS siano accessibili solo all'utente superuser
- Utilizzare programmi che limitino l'invio dei record del DNS ai siti pericolosi.

TFTP
TFTP è un protocollo che consente il trasferimento dei file senza richiedere password o nome utente. Dal momento che tale servizio è totalmente insicuro andrebbe disabilitato se non necessario o per lo meno dovrebbero essere limitati i file che si possono trasferire tramite tale protocollo.

Finger
Finger è un servizio in grado di offrire informazioni su utenti collegati ad un sistema.
In molte versioni di Unix finger legge le informazioni del file *.plan* o *.project* associati ad un utente. In alcuni versioni comunque *finger* opera con privilegi di root. E' possibile allora sfruttare tale servizio per leggere il contenuto di un file qualsiasi.
Bisogna allora monitorare i file letti da finger. Inoltre si consiglia di disabilitare finger o di sostituirlo con uno script di shell.

HTTP
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. Tali programmi vengono scritti con un protocollo detto CGI (Common Gateway Interface).

Il protocollo http presenta alcuni punti deboli in termini di sicurezza ed in particolare:

1. Un attaccante può approfittarsi di alcuni punti deboli del server http o degli script CGI ad esso associati per avere accesso a file.
2. Informazioni confidenziali che risiedono sul server http possono essere distribuite ad altri.
3. Informazioni confidenziali trasmesse dal server al browser possono essere intercettate.

I server http sono progettati per accettare richieste da utenti anonimi e per inviare informazioni nel modo più rapido ed efficiente possibile. 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.
A causa dell'enorme disponibilità di tool, di linguaggi e della capacità di gestire molti utenti collegati contemporaneamente, un sistema Unix non costituisce la scelta migliore per la realizzazione di un derver Web. Anche i sistemi operativi del mondo PC presentano caratteristiche simili e dunque non sono altamente affidabili. IlL miglior sistema per la realizzazione sicura di un server http è rappresenato da una macchina che esegua solamente il servizi oWeb e che non abbia altri punti di accesso o linguaggi di script per operare sulla macchina. In tal senso uno dei sistemi più sicuri e che negli ultimi anni ha subito il minor numero di attacchi è rappresentato dal sistema Macintosh e dal server MacHTTP o WebStar.

Comunque esistono innumerevoli vantaggi nell'utilizzare un sistema Unix come server http che vanno dalle prestazioni alla facilità di interazione nelle reti. Tutto questo però non deve far passare in secondo luogo le valutazioni sulle problematiche di sicurezza legate alla realizzazione di un sito Web tramite Unix.

Le regole principali cui prestare attenzione sono le seguenti:

1. Gli utenti della rete non devono essere in grado di eseguire script di shell o programmi sul server.
2. Gli script CGI devono eseguire solamente i compiti stabiliti o terminare con un messaggio di errore.
3. Se il server viene compromesso, non deve essere possibile condurre attacchi alla rete attraverso di esso.

L'UID del Server

Molti server Web entrano in esecuzione con privilegi di root e poi cambiano il proprio UID ad utenti con privilegi minori. Bisogna assicurarsi che il server non rimanga in esecuzione con privilegi di root.

La struttura delle Directory

Il software che gestisce un server Web è spesso molto complesso e utilizza molti file directory. E' importante capire il contenuto di tali directory e specificare opportunamente i permessi su di esse.

Gli script CGI

Bisogna riporre particolare attenzione nella scrittura di script sicuri.
Non bisogna fare in modo che gli script dipendano da variabili o da valori imposti dagli utenti in maniera determinante. In tal caso bisogna testare ogni singola combinazione nella maniera più esaustiva possibile .

http e FTP

Bisogna porre molta attenzione quando si offre la possibilità di accedere al servizio FTP attraverso il servizio http. Tale funzionalità può infatti dare adito ad accessi a file i configurazione non desiderati sfruttando uno dei due servizi per accedere a file di configurazione dell'altro.

POP

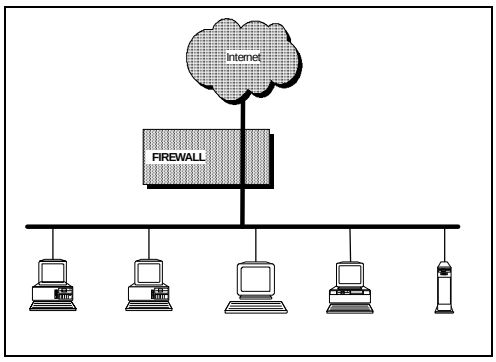
Il servizio POP permette ad un utente di accedere alla propria casella di mail per accedere ai propri file senza bisogno di dover montare dei dischi di rete.
In genere i client ed i server POP utilizzano un nome utente ed una password per verificare l'identità di un utente. Dunque il servizio può essere 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.

6.4 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.

7 I Firewall

Definizione di Firewall



Collocazione tipica di un Firewall 1

I Firewall costituiscono un sistema di sicurezza che si colloca a livello di rete. Esso serve ad impedire che ciò che di minaccioso esiste in Internet possa penetrare all'interno di una rete locale. Un Firewall permette molteplici operazioni. Principalmente esso costituisce un punto di passaggio obbligato per il traffico in entrata ed uscita ; dunque obbliga coloro che vogliono entrare nella rete e coloro che ne vogliono uscire a passare per un punto sicuro e ben sorvegliato. Un Internet Firewall va dunque installato nel punto in cui la rete protetta si collega ad Internet, come mostrato in figura. Dal momento che tutto il traffico passa per il Firewall, esso è in grado di valutare il fatto che tale traffico sia accettabile o meno. Il termine accettabile sta ad indicare che il traffico, a prescindere dal servizio che lo ha originato, sia conforme alla politica di sicurezza che regola la rete locale. Un Firewall costituisce quindi un separatore, un analizzatore ed un censore per quanto riguarda il traffico tra reti. Lo sviluppo e la struttura di un Firewall possono variare notevolmente da sito in sito e molto spesso il sistema non è costituito da un solo calcolatore, ma da una combinazione di router, calcolatori, e reti, tutti dotati di un apposito software. Esistono dunque varie architetture e varie scelte progettuali tra cui scegliere; la decisione va intrapresa in base alle esigenze del sito ed alle disponibilità economiche e tecniche. Un Firewall è in grado di difenderci dagli attacchi esterni, tuttavia non è in grado di difendere le macchine interne da attacchi condotti su di esse dall'interno. Dunque il suo funzionamento risulta ottimale se affiancato ad un sistema di difesa interno. Inoltre bisogna tener conto che la sua realizzazione richiede competenze particolari e che le restrizioni che esso impone agli utenti interni talvolta non sono tollerate da questi ultimi. Nonostante le problematiche e gli svantaggi che comportano, i sistemi Firewall costituiscono il metodo ad oggi più efficiente per connettersi ad Internet in modo sicuro. Bisogna poi sottolineare che i Firewall sono utili anche nel caso in cui vengano utilizzati con finalità diverse da quelle inerenti la sicurezza di una singola rete locale. Essi infatti possono essere impiegati per dividere una rete in sotto reti con politiche di gestione o di sicurezza diverse. Inoltre, consentono una gestione efficiente delle sotto reti, permettendo il monitoraggio e la gestione del traffico che le attraversa.

Potenzialità di un sistema Firewall

Riduzione dei punti critici

E' possibile immaginare il Firewall come un passaggio obbligato verso il mondo esterno. Tutto il traffico in entrata ed uscita dalla rete vi deve passare. In tal modo è possibile concentrarsi solamente su tale sistema e tramite esso stabilire tutte le politiche di sicurezza per l'intera rete locale.

Sviluppo della sicurezza

Molti dei servizi che oggi vengono utilizzati in Internet sono per propria natura insicuri. I Firewall costituiscono un meccanismo di sicurezza distribuito in quanto rendono più sicure le varie reti locali attraverso le quali viaggiano i pacchetti di dati.

Monitoraggio del traffico

Dato che il Firewall costituisce un punto di passaggio obbligato, esso favorisce anche il controllo e la registrazione dei pacchetti in transito.

Riservatezza

Come è stato indicato in precedenza, la riservatezza costituisce un utile ausilio per la sicurezza di una rete. In tale ambito un Firewall risulta particolarmente utile, in quanto limita la visibilità esterna di una rete. Inoltre spesso all'interno di uno stesso sito esistono sotto reti con esigenze di sicurezza e visibilità esterna molto diverse. L'utilizzo di sistemi Firewall permette allora di organizzare in modo semplice ed efficiente la struttura e la visibilità delle varie reti interne.

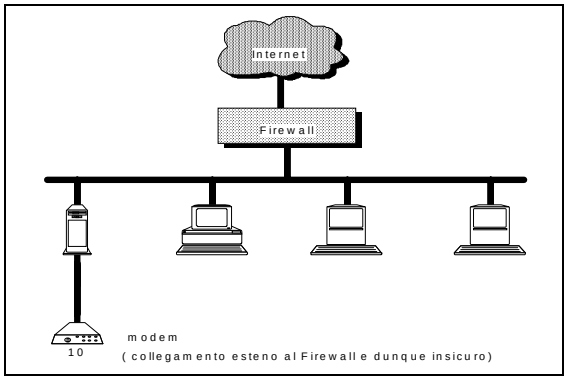
Limiti di un sistema Firewall

Attacchi dall'interno

Un Firewall viene concepito per proteggere una rete locale da attacchi dall'esterno. Tuttavia se un attaccante si trova all'interno della rete un Firewall può fare ben poco. I problemi interni alla rete locale vanno gestiti con sistemi di sicurezza a livello di singola macchina.

Connessioni esterne al Firewall

I Firewall sono in grado di gestire e controllare il traffico che transita attraverso di essi. Tuttavia se una rete locale utilizza collegamenti esterni al Firewall, questo ultimo non può fare nulla contro le possibile minacce che tali collegamenti possono comportare. Per esempio, se un sito consente collegamenti via modem ai calcolatori interni senza il filtro del Firewall, non è possibile controllare il traffico che da essi deriva. Tale situazione è rappresentata in figura.



Connessioni esterne 1

Nuove tipologie di attacchi

Un Firewall è progettato per proteggere un sito da pericoli noti. Nulla ci assicura che le scelte effettuate oggi saranno valide anche in futuro.

Virus

Un Firewall non può bloccare il passaggio di virus all'interno della rete. Sebbene i più recenti sistemi Firewall riescano ad analizzare il contenuto dei pacchetti in transito, i virus in circolazione sono in numero eccessivamente elevato e possiedono diverse nature.

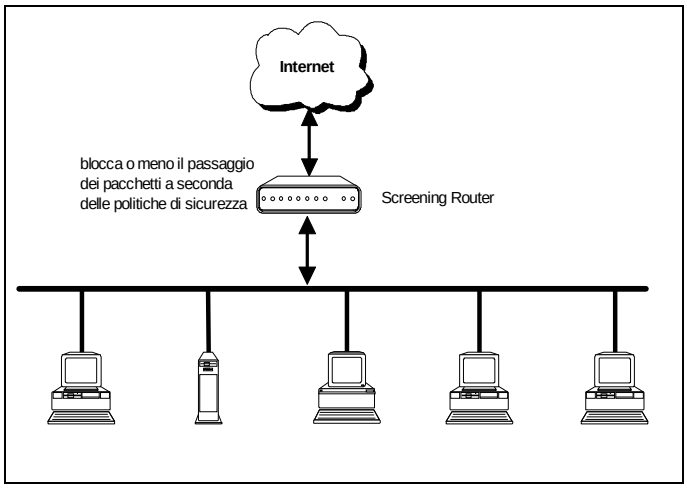
Costruire ed acquistare

Un tempo se un sito desiderava un sistema Firewall era obbligato a costruirselo ed a ricercare persone i grado di svolgere tale compito. Oggi invece esistono prodotti commerciali che offrono diverse funzionalità a seconda dei bisogni. La scelta tra l'acquistare un sistema Firewall ed il costruirselo va effettuata in base a molteplici fattori e non è possibile indicare una strategia di massima. Costruire un Firewall o acquistarlo non costituisce due scelte incompatibili. E' infatti possibile integrare i vari sistemi per configurare il sistema secondo le proprie esigenze. La qualità di un sistema va valutata in base a come esso risponde alle esigenze per cui è stato progettato ed in base alle caratteristiche tecnico-economiche del sito che ne usufruisce.

8 Tecnologie e Tecniche di Progetto dei sistemi Firewall

Sistemi Packet Filtering

I sistemi Packet Filtering regolano il passaggio dei pacchetti di dati tra i calcolatori che sono all'interno della rete protetta e quelli esterni. Essi permettono di bloccare i pacchetti che non rispettano le politiche di sicurezza adottate. Il tipo di *Router* utilizzato per svolgere tali operazioni è detto *Screening Router*.

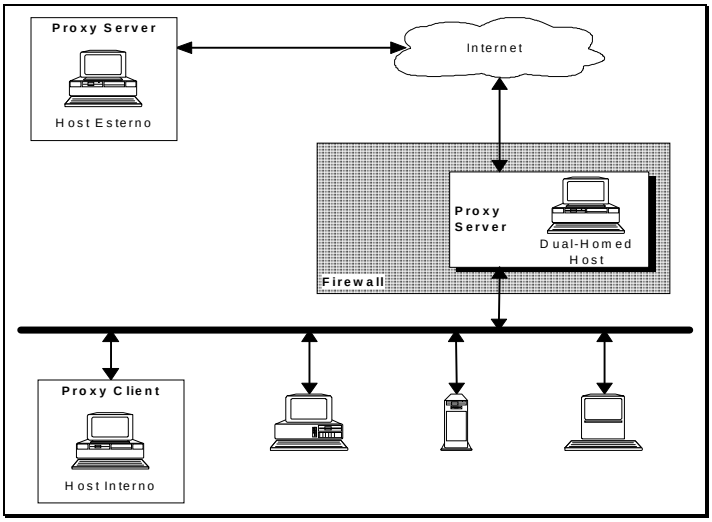


Screening Router 1

I programmi che eseguono i servizi richiesti sono associati a delle porte logiche, le quali vengono indicate attraverso dei numeri. E' allora possibile consentire o impedire alcune connessioni, specificando o meno il numero di porta logica che il servizio in questione è abilitato ad utilizzare, all'interno dell'insieme di regole definite per il sistema *Packet Filtering*. Al fine di comprendere meglio il funzionamento di un sistema *Packet Filtering*, è utile analizzare le differenze esistenti tra un *Router* tradizionale ed uno *Screening Router*.
Un Router tradizionale, analizza la destinazione di un pacchetto di dati e semplicemente seleziona il miglior percorso che conosce per consegnare tale pacchetto. Le decisioni intraprese a proposito della modalità di consegna del pacchetto dipendono solamente dalla sua destinazione.
Uno *Screening Router* analizza il pacchetto di dati in maniera più accurata. Esso infatti oltre a valutare se è in grado di spedire o meno il pacchetto, valuta anche se tale operazione sia più o meno lecita. Tale condizione dipende dalla politica di sicurezza adottata dal sito in questione.

Proxy Service

I *Proxy Service* sono costituiti da programmi che vengono eseguiti su sistemi Firewall, sia che si tratti di sistemi Dual-Homed, con una interfaccia verso la rete interna ed una verso Internet, sia che si tratti di altri tipi di Bastion Host collegati ad Internet. Tali programmi ricevono le richieste per ottenere dei servizi e ne permettono il passaggio a seconda della politica di sicurezza adottata. Tali Proxy si sostituiscono ai programmi tradizionali utilizzati per gestire i vari servizi di comunicazione, ed operano da tramite verso i sistemi che offrono il servizio richiesto. I Proxy risiedono, in maniera più o meno trasparente, tra l'utente all'interno della rete locale ed i sistemi esterni ai quali viene richiesto un determinato servizio. Il calcolatore interno, allora, invece che comunicare direttamente con il *server* esterno, interagisce con un Proxy, il quale lo mette in comunicazione con la macchina desiderata. Al fine di chiarire il funzionamento di un Proxy si analizzerà ora lo schema relativo al caso di un sistema Dual-Homed, illustrato nella figura seguente.



Proxy Server 1

Come illustrato in figura, un collegamento via Proxy è caratterizzato da due componenti : un *Proxy server* ed un *Proxy client*. In tale situazione il *Proxy server* risiede sul Dual-Homed host. Il *Proxy client* è una versione particolare di un normale programma client (per esempio FTP client o TELNET client) in grado di dialogare con il Proxy server piuttosto che con il server reale. Inoltre, seguendo alcuni semplici procedure è possibile utilizzare i programmi client tradizionali anche nel caso in cui si utilizzino dei Proxy. Tali sistemi permettono inoltre di svolgere vari tipi di operazioni che vanno al di là del controllo e dell'instradamento dei pacchetti di dati. Essi infatti dal momento che possono analizzare ogni richiesta di collegamento, sono in grado di controllare tutte le operazioni eseguite dagli utenti.

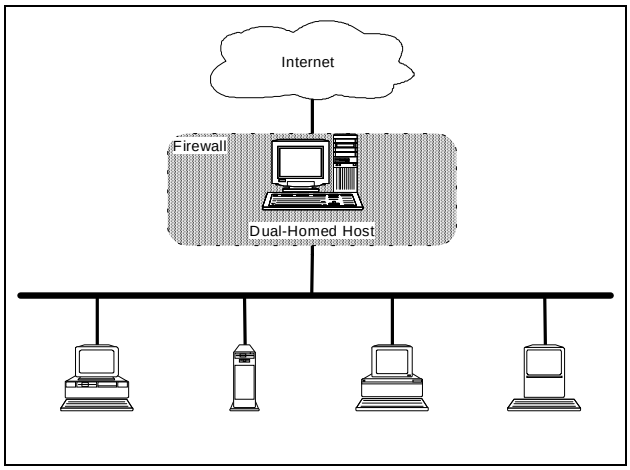
Sistemi Ibridi

Costruire un Firewall raramente comporta il ricorso ad una sola tecnica di progetto. Spesso infatti è necessario utilizzare diverse tecniche al fine di risolvere i vari problemi che il caso in questione comporta. Alcuni protocolli vengono gestiti in maniera più efficiente tramite il meccanismo di *Packet Filtering*, ad esempio l'FTP ed il WWW, altri richiedono l'utilizzo di Proxy. La maggior parte dei Firewall è costituita dalla combinazione di Proxy e Packet Filtering.

9 Architetture e Modelli di Firewall

Dual-Homed Host

L'architettura di tipo *Dual-Homed* viene realizzata basandosi su di un calcolatore *Dual-Homed*, ovvero un calcolatore che possiede almeno due *schede* di rete. Tale calcolatore svolge le funzioni di Router tra le due reti alle quali è collegato tramite le sue schede e dunque è in grado di regolare il traffico dei pacchetti di dati. Tuttavia il primo passo da effettuare per la realizzazione di una architettura di tale tipo, consiste nel disabilitare il meccanismo di *routing* dei pacchetti di dati. In tal modo i pacchetti provenienti da una rete, per esempio Internet, non vengono trasmessi direttamente all'altra rete. I sistemi all'interno della rete protetta possono comunicare con il calcolatore *Dual-Homed* e lo stesso possono fare i calcolatori esterni, tuttavia tali sistemi non possono comunicare direttamente tra di loro. L'architettura per un Firewall è indicata nella figura seguente :

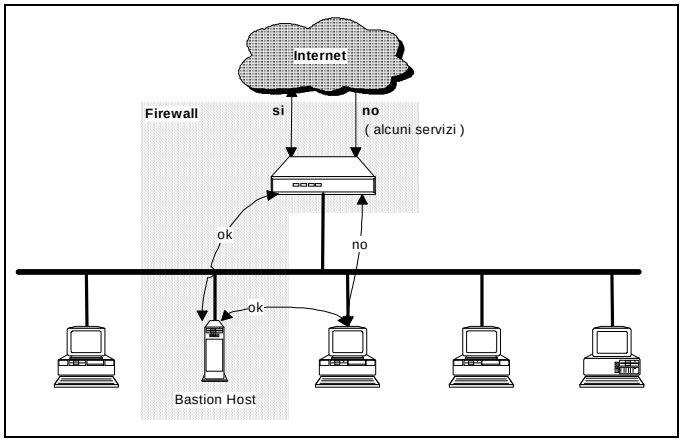


Architettura Dual-Homed 1

Un sistema Dual-Homed consente di utilizzare i servizi di rete tramite dei Proxy, oppure obbligando gli utenti a collegarsi al sistema Dual-Homed stesso. Tuttavia l'ultima soluzione presenta notevoli svantaggi in quanto consente agli utenti un accesso diretto al sistema Dual-Homed, riducendo quindi notevolmente, la sicurezza del sistema in questione.

Screened Host

Nei sistemi che utilizzano una architettura con *Screened Host* i servizi sono forniti ai calcolatori della rete locale attraverso un *Host* che è collegato solamente alla rete locale, la quale utilizza un *router* separato dagli altri calcolatori. All'interno di tale architettura il traffico dei pacchetti di dati viene regolato attraverso un sistema *Packet Filtering.* Lo schema generale è illustrato nella figura seguente :

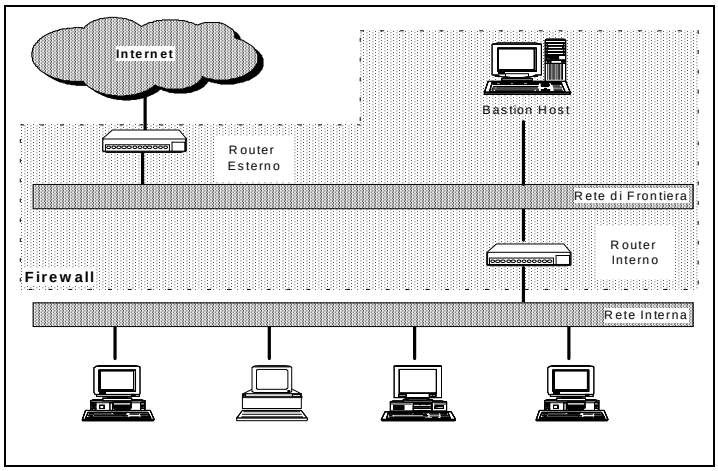


Architettura Screened Host 1

Il Bastion Host risiede all'interno della rete locale. Il sistema Packet Filtering operante all'interno dello Screening Router è strutturato in modo tale che il Bastion Host rappresenta l'unico calcolatore della rete locale al quale è possibile collegarsi dall'esterno. Inoltre solamente alcuni tipi di connessioni sono consentite. Ogni calcolatore esterno che volesse accedere alla rete locale deve prima collegarsi al Bastion Host. Il sistema Packet Filtering permette inoltre che il Bastion Host stabilisca o meno delle connessioni verso l'esterno, a seconda delle politiche di sicurezza stabilite dal sito in questione. Difendere uno Screening Router risulta abbastanza agevole, in quanto il calcolatore non deve fornire particolari servizi. L'architettura Screening Host, allora, rappresenta in molti casi una soluzione efficiente soprattutto in termini di sicurezza ed efficienza. Tale soluzione presenta tuttavia alcuni svantaggi. Infatti nel caso in cui un attaccante riesca a compromettere il sistema di sicurezza del Bastion Host, l'intera rete locale risulta compromessa, in quanto priva di difese. Lo Screening Router inoltre rappresenta un ulteriore punto debole. Infatti, nel caso in cui venisse violato il suo sistema di sicurezza, la rete locale sarebbe completamente esposta ad attacchi dall'esterno, ed il Bastion Host non avrebbe più alcuna utilità.

Screened Subnet

L'architettura Screened Subnet aggiunge un livello di sicurezza ulteriore rispetto all'architettura Screened Host analizzata precedentemente, grazie all'introduzione di una *rete di frontiera* che isola ulteriormente la rete locale dall'esterno. Il modello più semplice di Screened Subnet è costituito da due Screening Router, ognuno dei quali connesso alla rete di frontiera. Il primo è situato tra la rete di frontiera e la rete interna, ed il secondo è posto tra la rete di frontiera e la rete esterna, tipicamente Internet. Per portare un attacco alla rete interna, un attaccante dovrebbe superare entrambi i Router. La figura seguente illustra una possibile architettura di Firewall realizzata tramite Screened Subnet :

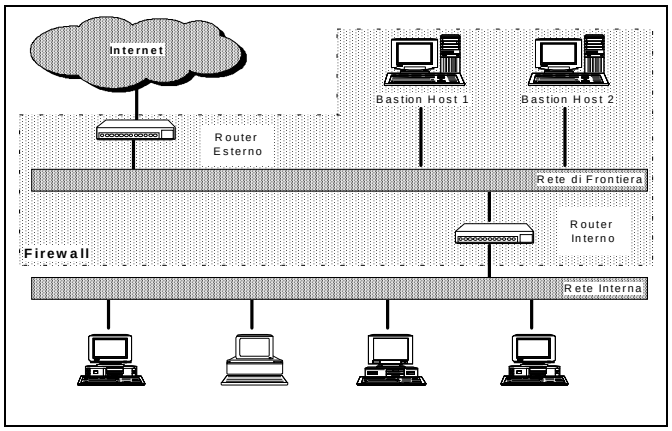


Screened Subnet 1

10 Valutazione di alcune architetture Firewall

Bastion Host multipli

E' possibile utilizzare più di un Bastion Host al fine di aumentare le prestazioni, la ridondanza o per separare dati e servizi. Dividere i servizi ed il traffico di rete tra più calcolatori permette infatti un utilizzo più efficiente di questi ultimi. Inoltre possedere più Bastion Host, consente di aumentare la sicurezza dell'intero sito, in quanto, nel caso in cui uno dovesse venire meno, i servizi possono essere forniti da un altro, senza compromettere la sicurezza dell'intera rete. In figura è mostrato un esempio di Screened Subnet con due

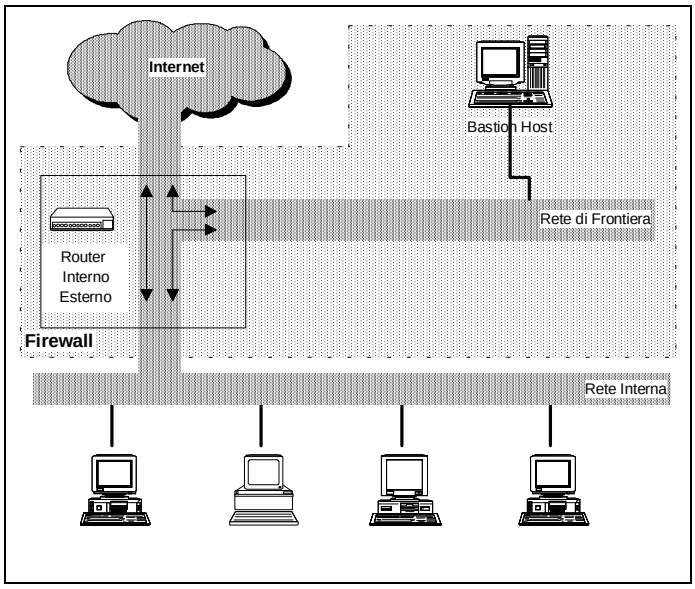


Architettura a due Bastion Host 1

Bastion Host :

Router interno ed esterno uniti

E' possibile conglobare il router interno e quello esterno in un unico router, ma solamente a condizione che questo ultimo sia sufficientemente flessibile e potente. In figura è illustrato un esempio di tale schema :

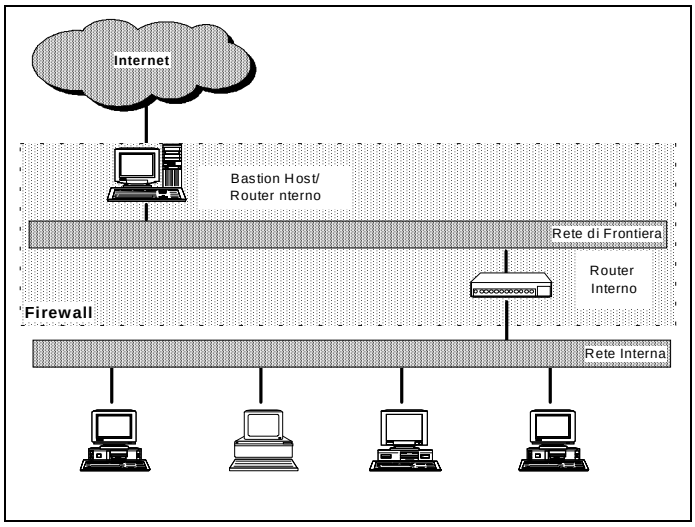


Router uniti 1

Tale architettura rende il sito più vulnerabile, in quanto se il sistema di sicurezza del router viene compromesso, la rete interna risulta completamente indifesa.

Router e Bastion Host uniti

Esistono casi in cui un singolo calcolatore Dual-Homed viene utilizzato come router e Bastion Host. Tale soluzione viene talvolta utilizzata in quanto permette di risparmiare un calcolatore. Tuttavia essa presenta alcuni svantaggi, in quanto espone il Bastion Host aumentandone la visibilità esterna, e rischia di sovraccaricare di lavoro una singola macchina.
In figura è illustrata una possibile realizzazione :

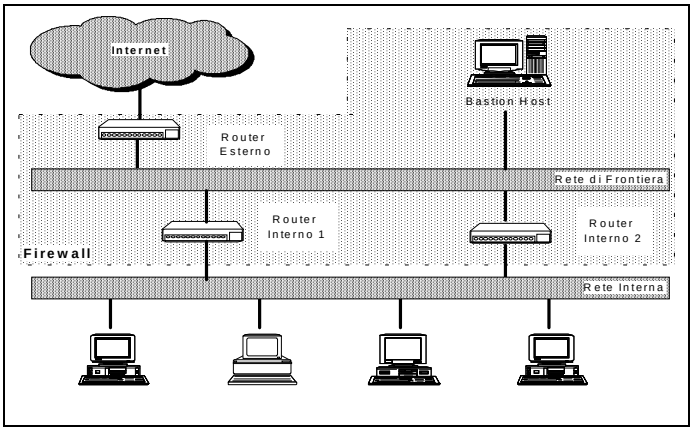


Bastion Host e router uniti 1

Unire il router interno ed il Bastion Host rappresenta invece una soluzione da sconsigliarsi vivamente. I due calcolatori infatti, svolgono compiti relativi alla sicurezza che sono concettualmente diversi. Essi si completano a vicenda e sono utili solo se posizionati uno all'esterno ed uno all'interno della rete di frontiera. Inoltre unendo i due calcolatori verrebbe meno l'utilità di utilizzare una rete di frontiera.

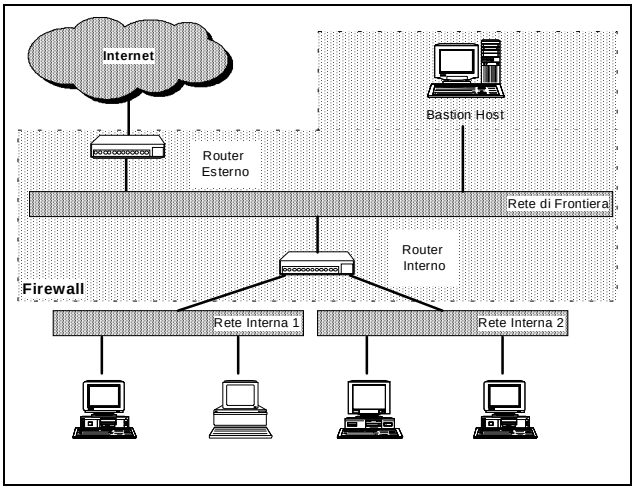
Utilizzo di vari router interni

Utilizzare vari router per connettere la rete di frontiera alla rete interna può causare vari problemi, e dunque è vivamente sconsigliabile. Un pacchetto potrebbe essere intercettato da qualcuno che sta osservando il traffico della rete dall'esterno a causa di errori nel routing interno.
Dunque non è corretta la configurazione illustrata nella figura seguente :



Configurazione sconsigliata 1

Talvolta si rende necessario utilizzare più router poiché la rete interna è costituita da più sotto reti. In tal caso è consigliabile utilizzare ancora un singolo router, con interfacce separate per ogni sotto rete.
Lo schema è illustrato nella figura seguente :



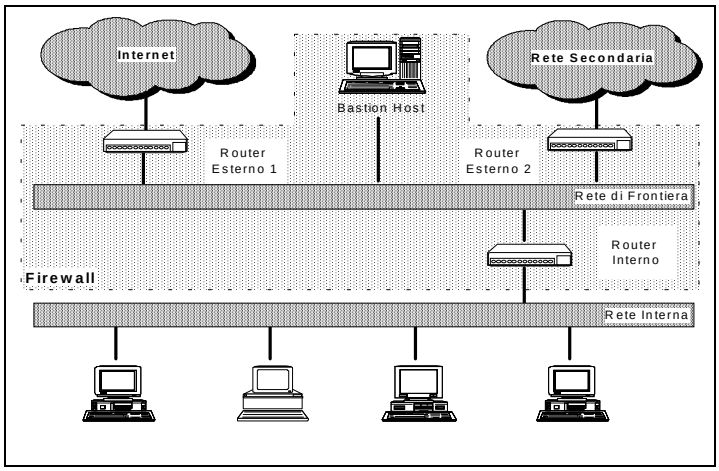
Varie reti interne

Utilizzo di vari router esterni

In alcuni casi si rende necessario collegare la rete di frontiera all'esterno, utilizzando più di un router. Tale situazione si può verificare nei seguenti casi :

- Il sito in questione possiede più di un collegamento ad Internet.
- Il sito in questione possiede un collegamento ad Internet più altri collegamenti a siti diversi.

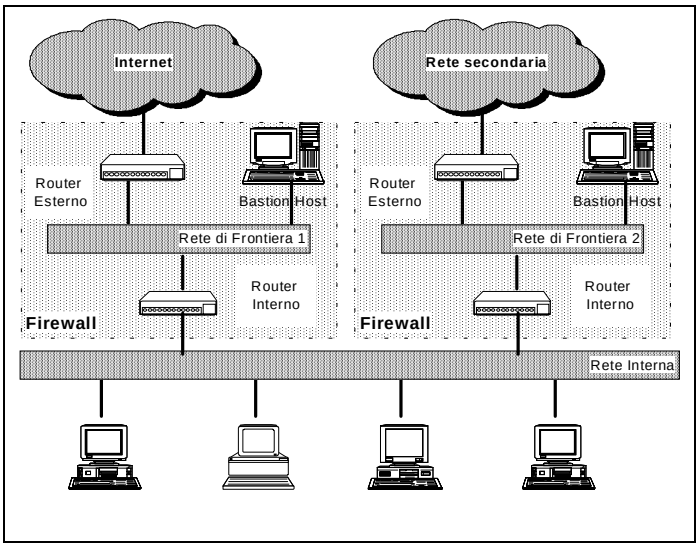
La situazione richiede più attenzione nel caso in cui il sito possiede un collegamento ad Internet ed un collegamento ad un altro sito, se in questo ultimo possono viaggiare informazioni riservate. In alcuni casi potrebbe essere necessario installare più reti di frontiera, piuttosto che più router esterni.
Una possibile realizzazione è illustrata nella figura seguente :



Architettura con più router esterni 1

Varie reti di frontiera

Come illustrato in precedenza, talvolta si rende necessario utilizzare varie reti di frontiera. Una possibile realizzazione è illustrata nella figura seguente :



Varie reti di frontiera 1

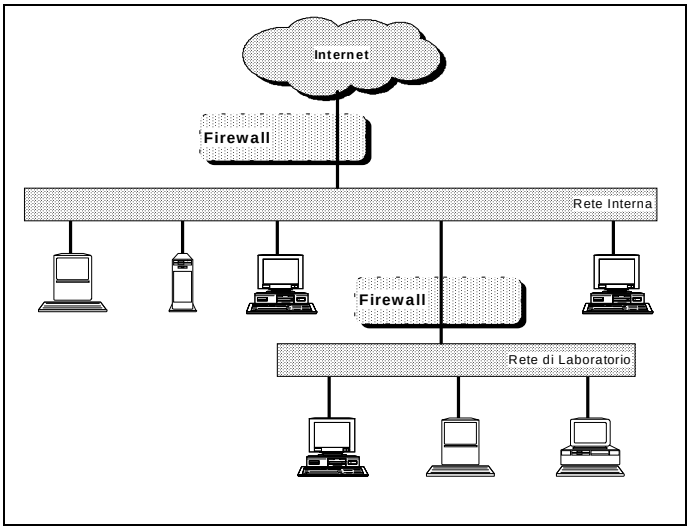
Dual-Homed Host e Screened Subnet

Combinando i sistemi Dual-Homed con l'architettura Screened Subnet è possibile ottenere un notevole aumento della sicurezza. Tale Firewall, se opportunamente configurato, consente un ottimo livello di protezione.

11 Architetture con Firewall Interni

Reti per laboratori

Molto spesso risulta necessario isolare la rete di un determinato laboratorio. Tale operazione è facilmente realizzabile attraverso un Firewall. Spesso è sufficiente utilizzare un sistema Packet Filtering che limiti il numero di servizi disponibili e che permetta agli utenti del laboratorio di eseguire solamente operazioni che sono ritenute sicure. Se il sito possiede varie reti di laboratorio che intende isolare dal resto della propria rete è possibile progettare una rete di frontiera comune a tutti i laboratori, e collegare tutti i laboratori a tale rete tramite dei router. Infine il sistema Packet Filtering viene posizionato tra la rete di frontiera ed il resto della rete del sito. Lo schema generale per isolare la rete di un laboratorio è indicato nella figura seguente :



Firewall per reti di laboratorio 1

Reti non sicure

Le reti di laboratorio sono pericolose, ma non sono necessariamente più insicure di altre reti. Alcuni siti invece possiedono reti che sono intrinsecamente molto insicure. Sono generalmente pericolose quelle reti a cui hanno libero accesso vari tipi di persone. Altre reti poi vengono utilizzate per compiere dimostrazioni o per tenere lezioni. In tal caso si rende necessario utilizzare dei sistemi Packet Filtering ed un Dual-Homed host, per impedire che delle informazioni non pubbliche possano fluire attraverso la rete comune. Inoltre, alcune reti vengono spesso utilizzate da persone che, più o meno consapevolmente, possono provocare danni al resto della rete locale. In tal caso è sufficiente utilizzare un calcolatore Dual-Homed ed obbligare gli utenti a seguire le procedure imposte dai Proxy.

Reti particolarmente sicure

Alcune organizzazioni possiedono delle reti particolarmente sicure. Per esempio i centri di ricerca, le banche o alcuni enti governativi. Reti di questo tipo, non solo devono essere sicure, ma molto spesso devono anche rispettare specifiche norme di sicurezza stabilite dagli enti governativi. In tal caso i sistemi Firewall non sono sufficienti a fornire il grado di sicurezza richiesto. Spesso si rende necessario codificare i dati in transito nella rete, ed utilizzare reti isolate per il trasferimento dei dati più critici.

Reti per collaborazioni aziendali

Talvolta diverse organizzazioni, decidono di unire i propri sforzi per la realizzazione di progetti comuni. In questi casi può essere conveniente, per gli enti interessati, poter condividere dati, calcolatori e risorse, per tutta la durata del progetto. Dunque risulta necessario progettare dei sistemi di sicurezza che consentano solamente lo scambio di quei dati e quelle risorse strettamente necessari per la collaborazione, ma che siano in grado di

impedire ogni altro tipo di accesso. Molto spesso poi, un determinato sito può aver bisogno di collegarsi a dei venditori o a dei fornitori con i quali mantiene rapporti commerciali. In tal caso può essere desiderabile che alcune informazioni possano essere viste solamente da alcuni enti e non da altri. Una delle soluzioni maggiormente utilizzate per risolvere i problemi inerenti le collaborazioni aziendali, è costituita dall'utilizzo di un *rete di frontiera condivisa*. Il più delle volte non è necessario utilizzare dei sistemi Bastion Host, in quanto esiste un rapporto di fiducia tra le aziende che collaborano.

12 Realizzazione di un Firewall tramite Bastion host

Il Bastion Host rappresenta la presenza di un sito all'interno di Internet. Esso costituisce il sistema al quale amici o nemici esterni devono collegarsi per poter accedere ai calcolatori interni al Firewall. A causa della sua collocazione, un Bastion Host è particolarmente esposto al rischio di attacchi, dal momento che la sua esistenza è nota all'esterno. Come conseguenza, si rende necessario curare in maniera particolarmente approfondita lo sviluppo del sistema di sicurezza per tale calcolatore. Esistono due principi generali di cui bisogna tener conto nella progettazione di un Bastion Host : *progettare in maniera semplice ed essenziale,* e *considerare il caso in cui il Bastion Host possa essere compromesso.*

Progettare in maniera semplice ed essenziale :

Ogni servizio che il Bastion Host offre potrebbe possedere errori di tipo software, oppure inerenti la sua configurazione. Dunque è necessario fare in modo che il Bastion Host offra il minor numero possibile di servizi, con privilegi ridotti al minimo.

Considerare il caso in cui il Bastion Host possa essere compromesso :

A prescindere dalla bontà o meno del sistema di sicurezza, un Bastion Host può comunque essere vittima di attacchi. Dunque in fase di progettazione, bisogna sempre considerare il caso peggiore, e le conseguenze derivanti dal fallimento del sistema di sicurezza. A tal fine bisogna fare in modo che anche nel caso in cui il Bastion Host dovesse venire meno, i danni per la rete interna siano ridotti al minimo.

Tipi particolari di Bastion Host

Bastion Host che non effettuano routing

Un Bastion Host che non effettua Routing, è un calcolatore connesso a più reti, che tuttavia non consente il passaggio di dati tra di esse.

Calcolatori vittima

Talvolta si rende necessario utilizzare dei servizi che non risultano sicuri, nemmeno se forniti attraverso sistemi Packet Filtering o attraverso dei Proxy. In altri casi si utilizzano servizi talmente recenti da non poter dire nulla riguardo la loro sicurezza o meno. In tali ambiti può essere utile utilizzare una macchina che funga da cavia. Possibilmente essa dovrebbe fornire un unico servizio insicuro, al fine di evitare operazioni inaspettate.

Bastion Host interni

In molti casi il Bastion Host principale deve interagire con alcuni calcolatori interni. Questi ultimi rappresentano allora dei Bastion Host secondari, e dunque dovrebbero essere configurati come ogni altro Bastion Host.

Scelta della Macchina

Scelta del sistema operativo

E' utile utilizzare dei sistemi con i quali il progettista è familiare. E' necessario utilizzare un sistema che sia in grado di offrire tutti i servizi di Internet, e che sia in grado di gestire varie connessioni contemporaneamente. Unix rappresenta il sistema operativo maggiormente diffuso all'interno di Internet, soprattutto per quanto riguarda l'offerta dei servizi di rete. Di conseguenza esistono molti applicativi per tale ambiente, ed è molto ricca l'offerta di componenti per costruire un Bastion Host. E' poi utile scegliere una versione del sistema operativo che sia largamente diffusa. La grande diffusione comporta infatti una maggiore disponibilità di risorse per lo sviluppo. Inoltre è più probabile che i sistemi maggiormente utilizzati siano quelli che presentano una qualità migliore, in quanto vengono continuamente testati e migliorati.

Scelta del calcolatore

Il Bastion Host non deve essere necessariamente una macchina veloce, anzi spesso non conviene utilizzare un calcolatore particolarmente potente, in quanto il Bastion Host non deve svolgere compiti particolari, ed inoltre la sua velocità è limitata dalla velocità delle connessioni e non tanto dalla capacità della sua CPU.

Scelta dei componenti hardware

Al fine di costruire un sistema affidabile, è buona norma non utilizzare i prodotti più recenti. Tuttavia non è consigliabile servirsi di componenti particolarmente datati, in quanto gli strumenti di sviluppo per tali sistemi possono non essere disponibili. La scelta migliore spesso sta nel mezzo. E' utile disporre di una notevole quantità di memoria e di un vasto spazio su disco.

Scelta della locazione fisica e Disposizione del Bastion Host

Scelta della locazione fisica

Il Bastion Host deve essere posto in una locazione fisica sicura. Esistono due ragioni che motivano tale scelta :

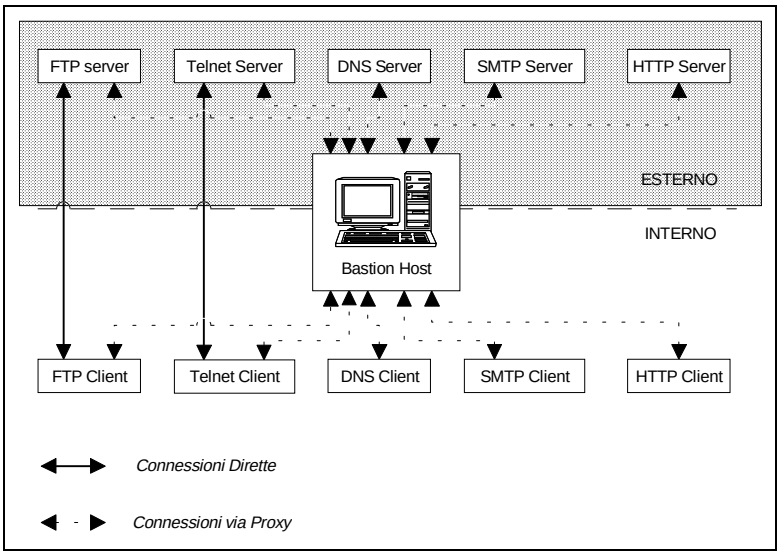
- E' impossibile rendere adeguatamente sicura una macchina, se un attaccante può avere accesso fisico ad essa.
- Il Bastion Host fornisce la maggior parte delle connessioni ad Internet. Nel caso in cui venisse danneggiato, la rete locale potrebbe risultare totalmente disconnessa dal resto del mondo.

Disposizione all'interno della rete

Il Bastion Host non dovrebbe essere posizionato in prossimità di una rete sulla quale transitano informazioni confidenziali. E' utile ricordare che alcune schede di rete possono operare in " modalità promiscua ", nel qual caso una particolare macchina connessa alla rete può intercettare tutti i pacchetti di dati che vi transitano, a prescindere dalla loro destinazione. Una possibile soluzione per ovviare a tale problema, consiste nel non posizionare il Bastion Host su di una rete interna, ma possibilmente su di una rete di frontiera.

Scelta dei servizi offerti tramite il Bastion Host

Il Bastion Host può offrire tutti i servizi di cui necessita il sito, oppure può essere utilizzato per offrire solamente quei servizi che sono ritenuti non sicuri. Non devono essere utilizzati tramite Bastion Host tutti quei servizi che non riguardano connessioni dalla rete locale ad Internet e vice versa.



Il Bastion Host può fornire vari servizi 1

Gestione degli account sul Bastion Host

E' consigliabile non consentire alcun account sul Bastion Host. Infatti, non consentire l'accesso al Bastion Host concorre ad aumentarne la sicurezza. Possibili fattori di rischio sono costituiti da :

- Vulnerabilità degli account stessi.
- Vulnerabilità dei servizi richiesti per gestire gli account.
- Stabilità ed affidabilità ridotte della macchina.
- Maggior difficoltà nel rilevare attacchi.

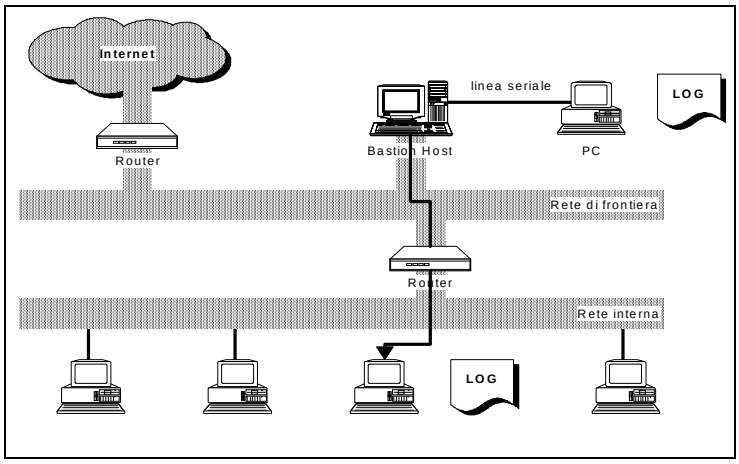
Costruzione del Bastion Host

I passi principali che è necessario compiere nella costruzione di un Bastion Host, sono i seguenti :

1. Rendere sicura la macchina.
2. Disabilitare tutti i servizi non richiesti.
3. Installare o modificare i servizi che si intendono fornire.
4. Configurare la macchina per la modalità operativa.
5. Utilizzare un sistema di verifica.
6. Collegare la macchina alla rete sulla quale sarà utilizzata.

Rendere sicura la macchina

E' consigliabile utilizzare una versione standard ed eseguire una installazione minimale. E' inoltre consigliabile utilizzare un prodotto ben conosciuto, e che non presenti particolari problemi. E' utile procurarsi un elenco dei problemi presentati dal sistema operativo che si sta utilizzando, in modo da potervi porre rimedio. Al fine di essere sicuri di non tralasciare aspetti importanti, è bene utilizzare delle checklist per testare il proprio sistema. Come ogni altro sistema di sicurezza, il Bastion Host necessita di tenere traccia dei vari messaggi di sistema. Tali messaggi vanno non solo registrati, ma anche conservati in maniera sicura.



Uso di un PC per i system log 1

Disabilitare i servizi non richiesti

Una vota resa sicura la macchina, è necessario disabilitare tutti quei servizi che non sono necessari.
Alcuni servizi risultano essenziali per il corretto funzionamento della macchina e dunque non vanno disabilitati, qualsiasi siano le politiche di sicurezza adottate. E' necessario disabilitare tutti i servizi, eccetto quelli che si è deciso di fornire e quelli indispensabili per il corretto funzionamento del sistema. Esistono tre regole generali per capire se disabilitare o meno un servizio :

- Se non si ha bisogno di un servizio, è meglio disabilitarlo.
- Se non si conosce esattamente il funzionamento di un servizio, è necessario :
    a) Studiarlo attentamente per comprenderne le finalità.
    b) Eventualmente disabilitarlo.

- Se disabilitando un servizio nascono dei problemi, è allora possibile capire l'esatto funzionamento del servizio stesso, ed il modo di eliminarlo.

Installare e modificare i servizi che si intendono fornire

Alcuni dei servizi che si intendono fornire potrebbero non essere inclusi nel sistema operativo : per esempio, il WWW generalmente non viene incluso. Altri potrebbero essere forniti con il sistema operativo, tuttavia potrebbero essere inadatti per un utilizzo sicuro (ad esempio *fingerd* e *ftpd* standard). Anche quei servizi che vengono forniti e ritenuti sicuri, dovrebbero comunque venire controllati tramite un il software TCP Wrapper o tramite il software *netacl* del TIS FWTK al fine di aumentarne la sicurezza e l'affidabilità.

Configurazione della macchina per la modalità operativa

A questo punto è necessario passare da una configurazione che era utile in fase di costruzione del Bastion Host ad una configurazione che sia utile per la fase operativa della macchina stessa. E' necessario svolgere le seguenti operazioni :

- Riconfigurare e installare il Kernel.
- Rimuovere tutti i programmi non necessari.
- Configurare il file system in modalità " sola lettura ".

Utilizzare un sistema di verifica

Una volta terminata la configurazione del Bastion Host, è opportuno mettere in esecuzione un sistema per il controllo e la verifica del sistema. I tre prodotti maggiormente utilizzati sono :

- *COPS*, il sistema sviluppato da Dan Farmer e Gene Spafford.
- *Tiger*, sviluppato come parte del pacchetto TAMU presso la A&M University del Texas.
- *Tripwire*, sviluppato da Gene H. Kim e Gene Spafford.

E' poi consigliabile utilizzare della checksum.
Una volta resa sicura la macchina e terminate tutte le operazioni di configurazione, è possibile ricollegarla alla rete desiderata.

Funzionamento del Bastion Host

Una volta che il Bastion Host è divenuto operativo, bisogna infatti essere in grado di analizzare tutte le operazioni che esso compie.

- Analizzare la fase di funzionamento standard
- Utilizzo di un software per il controllo automatico

Protezione della macchina e backup

Una volta che la macchina è operativa, è necessario curare anche la sua sicurezza dal punto di vista fisico, e conservare le copie di backup in un luogo sicuro.

Analizzare le operazioni di Reboot

Talvolta, alcuni tipi attacchi (ad esempio gi attacchi che comportano modifiche al Kernel), possono avere luogo solamente in seguito ad una riattivazione (Reboot) della macchina. In un Bastion Host non dovrebbero verificarsi mai dei Reboot. Nel caso in cui venga effettuato un Reboot, è necessario investigare immediatamente per scoprirne le cause.

Effettuare Backup sicuri

Spesso è necessario effettuare i Backup tramite dispositivi appositi collegati direttamente al Bastion Host. Non è consigliabile fidarsi solamente del disco fisso interno al Bastion Host, ma è necessario possedere anche delle copie dei file e dei dati, su dispositivi rimovibili. I Backup non sono utili solamente per ricostruire il sistema a seguito di disastri, ma possono essere utilizzati anche come termine di paragone per scovare eventuali attacchi.