

**ISTITUTO TECNICO INDUSTRIALE
MAX PLANCK
VILLORBA (TV)**

Specializzazione: ELETTRONICA E TELECOMUNICAZIONI

Tesina per l'esame di Stato

**NORME DI SICUREZZA IN UNA LAN
Difese dagli attacchi in zone riservate**

Studente: LUCICH GIOVANNI

Anno scolastico 2006/07

INDICE

INTRODUZIONE	pag. 1
CAPITOLO 1: STRUTTURA DELLA RETE	pag. 2
1.1 La VLAN	pag. 2
1.2 Il protocollo TCP/IP	pag. 3
1.3 La funzione NAT	pag. 4
1.4 Il gateway	pag. 5
CAPITOLO 2: LE MINACCE	pag. 6
2.1 Pericoli provenienti dall'interno della rete: il "fattore umano"	pag. 6
2.2 Classificazione dei pericoli provenienti dall'esterno: i malware	pag. 7
CAPITOLO 3: COME DIFENDERE LA RETE	pag. 10
3.1 Gli honeypot	pag. 10
3.2 Il firewall	pag. 10
3.3 La zona DMZ	pag. 11
3.4 L'IPsec	pag. 12
3.5 SSH e SSL	pag. 13
3.6 Antivirus e anti-spyware	pag. 14
CONCLUSIONE	pag. 15
BIBLIOGRAFIA	pag. 16
GLOSSARIO	pag. 17

INTRODUZIONE

Il termine sicurezza, con l'attuale straordinario sviluppo delle reti di comunicazione, è diventato, in termini informatici, praticamente irreale.

Una rete informatica non ha confini ed è aperta a tutti, o quasi. Per questo non garantisce protezione contro eventuali abusi, siano essi provenienti dall'interno o dall'esterno della rete locale. In questo frangente sono state sviluppate una grandissima varietà di protezioni che si evolvono continuamente in relazione alla potenza degli attacchi.

La sicurezza totale di un sistema informativo può essere considerata un limite difficilmente raggiungibile; lo è ancora meno mettendo in gioco variabili non controllabili ed imprevedibili. Tra queste, il "fattore umano" gioca indubbiamente un ruolo di primaria importanza.

All'interno di un ambiente intranet si può cercare di ovviare a molti di questi comportamenti mediante l'adozione di *policy* relative alla sicurezza.

Tutti gli utenti del sistema sono tenuti al rispetto di queste norme sia dal punto di vista dei comportamenti nell'uso del sistema stesso che nell'adozione di idonee misure di sicurezza, quali ad esempio: utilizzo sistematico di *firewall* e *software antimalware*, realizzazione frequente di copie di *backup* dei dati ed un aggiornamento dei sistemi tramite i files di correzione resi disponibili dalle *software houses* (le cosiddette "*security patch*") realizzate in seguito alla scoperta di particolari vulnerabilità del *software* sul piano della sicurezza

Il problema poi è ancora più sentito quando i dati trasferiti contengono informazioni riservate, non disponibili a tutti i membri della rete.

Come si difendono coloro che necessariamente devono proteggere i loro dati?

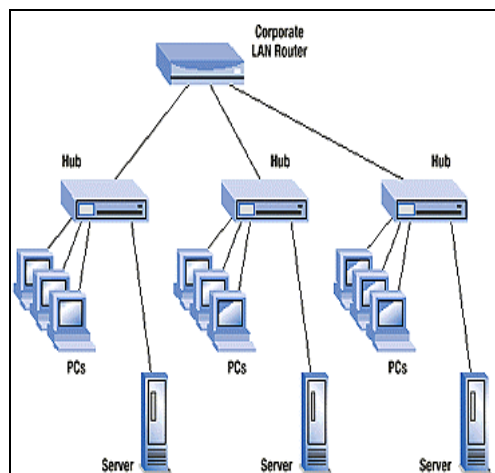
Ponendomi questa domanda mi sono informato e documentato in prima persona presso realtà che convivono ogni giorno con problemi relativi alla sicurezza. Ho ricevuto molte informazioni sulla struttura della rete e sui principali metodi di sicurezza da loro adottati per difendersi.

CAPITOLO 1: STRUTTURA DELLA RETE

Prima di passare ai sistemi sicurezza è utile illustrare la struttura della rete che può essere utilizzata:

1.1 La VLAN

Come rappresentato nell'esempio esemplificato a fianco, la configurazione più usata per collegare molti utenti è una intranet a stella (oppure ad anello). La rete locale che viene a formarsi è definita *Local Area Network* (LAN). Nelle realtà più complesse, allo scopo di migliorarne l'efficienza e la sicurezza, si implementano le VLAN (*Virtual LAN*), che permettono di segmentare il dominio di



broadcast. Tale tecnologia, basata su *switch*, permette di frammentare la LAN in più reti separate e non comunicanti tra loro. Le applicazioni di questa tecnologia sono tipicamente legate ad esigenze di separare il traffico di gruppi di lavoro o dipartimenti di una azienda, per applicare diverse politiche di sicurezza informatica. Le prime versioni permettevano di realizzare su un singolo switch diverse reti "virtuali" (VLAN), assegnando ciascuna porta ad una di queste reti. Gli host collegati ad una rete potevano comunicare solo tra di loro e non con quelli collegati alle altre reti, se non per mezzo di un router connesso ad entrambe le VLAN.

Ad esempio, ipotizziamo di avere un solo switch, e di avere la necessità di incrementare la sicurezza affinché utenti di un gruppo di lavoro non interagiscano con utenti di un altro gruppo. Attivando, via software, la gestione delle VLAN sullo switch, si può impostare che su 24 porte ethernet disponibili, le prime 12 facciano parte del gruppo 1 e le ultime 12 facciano invece parte del gruppo 2.

Il risultato è lo stesso che si otterrebbe utilizzando un diverso *switch* "tradizionale" per ciascuna rete, ma con alcuni vantaggi:

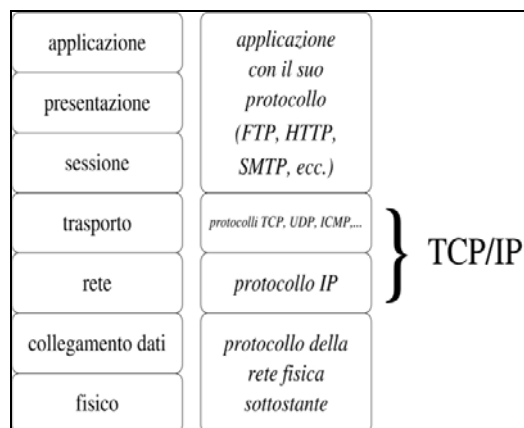
Costi e ingombri: invece di diversi *switch*, è possibile utilizzare un solo *switch* con molte porte, risparmiando in costi di acquisizione e manutenzione, spazio occupato, prese di alimentazione elettrica, indirizzi IP per la gestione remota

Flessibilità: le porte dello *switch* possono essere spostate da una VLAN ad un'altra per mezzo di semplici operazioni di riconfigurazione *software*, spesso effettuabili da remoto. Altre VLAN possono essere aggiunte utilizzando le porte esistenti, e quindi a costo nullo.

In seguito la tecnologia è stata sviluppata, aggiungendo la possibilità di collegare tra loro due switch unendo le VLAN presenti su di essi (*VLAN trunking*). Questo permette di realizzare VLAN che si estendono nelle diverse parti di una rete aziendale, anche su scala geografica.

1.2 Il protocollo TCP/IP

Il protocollo adottato dalla rete è il TCP/IP (vedi immagine), un modello a strati formato principalmente dal protocollo TCP e da quello IP: i protocolli sono gli standard che indicano come avvengono i trasferimenti da una macchina ad un'altra. Per TCP/IP non si intende solo il protocollo di trasmissione TCP ed il protocollo di rete IP, ma una famiglia di



protocolli comprendente anche l'UDP, l'ICMP, l'ARP, il RARP ed altri. Il modello a strati è una comoda rappresentazione dei sistemi di rete che permette concettualmente di separare le diverse funzionalità in livelli di problematica, consentendo così di studiare e risolvere più facilmente le problematiche relative all'implementazione delle reti. La

stratificazione è fondamentale per poter disegnare l'architettura *software* strutturata in livelli, ognuno dei quali con i suoi vari protocolli, tratta una parte specifica dei problemi. Il concetto di stratificazione poggia su un principio basilare: in sostanza, afferma che un determinato livello dell'*host* sorgente comunica con il paritario livello del destinatario. I due principali esempi di modelli stratificati sono rappresentati dal *Open System Interconnection* (OSI) dell'ISO e dal TCP/IP. Inoltre è importante sottolineare che uno strato comunica soltanto con lo strato immediatamente superiore od inferiore (tramite delle interfacce standard) mentre all'interno di ogni strato l'elaborazione dei dati può avvenire in un qualunque modo; infatti non è possibile per uno strato comunicare con un qualsiasi altro senza necessariamente passare attraverso lo strato precedente o seguente. In particolare la *suite* di protocolli TCP/IP è organizzata concettualmente in quattro livelli:

Application Layer: avviene l'interattività tra l'utente e la macchina

Transport Layer: divide il flusso di dati in pacchetti (di solito di circa 500 byte) che vengono passati insieme all'indirizzo di destinazione allo strato sottostante

Internet Layer (IP): crea il datagramma di base della rete, riceve e trasferisce senza garanzie i pacchetti, che gli arrivano da sopra, verso la macchina destinataria

Network Interface Layer: accetta il datagramma IP e lo trasmette con appositi *frame*

1.3 La funzione NAT

Nonostante il protocollo usato sia il comune TCP/IP, un'importante particolarità di una rete protetta è l'esigenza di inaccessibilità dall'esterno, pur mantenendo la disponibilità di tutti i servizi offerti dal "classico" *internet* (rete aperta).

Questo è possibile configurando nel *router* e/o nel *firewall* la funzione NAT (*Network Address Translation*). Questa è una tecnica usata per sostituire nell'intestazione di un pacchetto IP l'indirizzo sorgente con un indirizzo diverso. Il NAT sinteticamente si comporta in questo modo: nel pacchetto in uscita toglie l'indirizzo privato e lo sostituisce con uno pubblico; quando il pacchetto di risposta ritorna compie il processo inverso,

togliendo l'IP pubblico e reimpostando l'indirizzo privato dell'*host* che ha generato la sessione inoltrandolo al destinatario.

1.4 Il gateway

I problemi iniziano quando si devono far comunicare tra loro più reti diverse.

Questa funzione viene gestita dai *gateways* che normalmente sono dei *routers* che lavorano al livello 3, i quali dispongono più interfacce di rete. Nei *gateway* è presente una tabella per l'instradamento dei pacchetti utilizzata da router/gateway per inoltrare i pacchetti verso il successivo router/gateway.

CAPITOLO 2: LE MINACCE

Delineato lo “scheletro” della rete, è opportuno conoscere da cosa la rete deve difendersi.

I pericoli fondamentalmente si dividono in diverse tipologie: quelli interni alla rete, causati dalla volontà o involontarietà degli utenti della rete locale, e quelli esterni alla rete locale, causati da hacker o da fattori esterni alla LAN.

2.1 Pericoli provenienti dall'interno della rete: il “fattore umano”

Nell'introduzione è stato citato il problema del fattore umano, cioè il pericolo dovuto a errori o leggerezze degli utenti. La casistica, purtroppo, fornisce un gran numero di esempi: post-it con la password attaccato sul monitor del PC; l'apertura di e-mail provenienti da sconosciuti e recanti *attachment* "sospetti" (i classici file ".exe", ma non solo...); il computer lasciato acceso e incustodito; la scelta di *password* banali (es. username: nome; *password*: cognome) o troppo corte; l'installazione di programmi contenenti algoritmi in grado di violare la *privacy* (i cosiddetti "*spyware*") inviando a insaputa dell'utente suoi dati personali ad altri computer collegati alla rete; la navigazione nel web senza particolari precauzioni e senza preoccuparsi di verificare la provenienza di eventuali *software* richiesti dal *browser*. Ma questi problemi possono essere (per la maggior parte dei casi) risolti grazie alle password predefinite con lunghezza adatta, con forma (possibilmente un giusto mix di lettere, numeri, simboli) e contenuto non banale, custodia sicura, data di scadenza (la quale implica un obbligo di cambiamento delle password nel tempo). Invece, per evitare l'ingresso di indirizzi o utenti indesiderati, esistono delle *accesslist*, un registro che contiene una lista di questi indirizzi a cui, per un motivo particolare, è stato concesso/negato un particolare servizio o un privilegio.

2.2 Classificazione dei pericoli provenienti dall'esterno: i malware

Per quanto riguarda le vere e proprie “aggressioni” alla rete, gli attacchi possono avvenire in tutti gli strati della pila protocollare precedentemente illustrata. Capire la natura delle minacce e il modo in cui si evolvono è il prerequisito per stabilire componenti e caratteristiche di una soluzione capace di contrastarli.

Queste sono alcune brevi descrizioni dei più importanti tipi di minacce da cui la rete deve difendersi:

Virus: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.

Worm: questi *malware* non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di *social engineering*, oppure sfruttano dei difetti (*bug*) di alcuni programmi per diffondersi automaticamente.

Trojan horse: *software* che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famoso cavallo di Troia.

Backdoor: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un *trojan* o ad un *worm*, oppure costituiscono una forma di accesso di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una *password* dimenticata.

Spyware: *software* che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle *password* e alle chiavi crittografiche di un utente.

Dialer: questi programmi si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono *malware* quando vengono utilizzati in modo non specifico, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.

Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto *browser*) e causano l'apertura automatica di pagine Web indesiderate.

Rootkit: solitamente sono composti da un *driver* e, a volte, da delle copie modificate di programmi normalmente presenti nel sistema. I *rootkit* non sono dannosi in se ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare *spyware* e *trojan*.

Rabbit: sono programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.

DoS (denial of service): letteralmente negazione del servizio. In questo tipo di attacco si cerca di portare il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un sito web, al limite delle prestazioni, lavorando su uno dei parametri d'ingresso, fino a renderlo non più in grado di erogare il servizio. Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito ad un server Web, FTP o di posta elettronica saturandone le risorse e rendendo tale sistema "instabile", quindi qualsiasi sistema collegato ad Internet e che fornisca servizi di rete basati sul TCP è soggetto al rischio di attacchi DoS.

Nell'uso comune il termine virus viene utilizzato come sinonimo di *malware* e l'equivoco viene alimentato dal fatto che gli antivirus permettono di rilevare e rimuovere anche altre categorie di *software* maligno oltre ai virus propriamente detti.

Si noti che un *malware* è caratterizzato dall'intento doloso del suo creatore, dunque non rientrano nella definizione data i programmi contenenti *bug*, che costituiscono la normalità anche quando si sia osservata la massima diligenza nello sviluppo di un software. Un *bug* è un errore nella scrittura di un *software*, che causa un suo funzionamento errato o comunque diverso da quello che l'autore ha previsto ed in alcuni casi anche il suo blocco totale; meno comunemente, il termine *bug* può indicare un difetto di progettazione in un componente *hardware* che ne causa un comportamento imprevisto o comunque diverso da quello specificato dal produttore.

CAPITOLO 3: COME DIFENDERE LA RETE

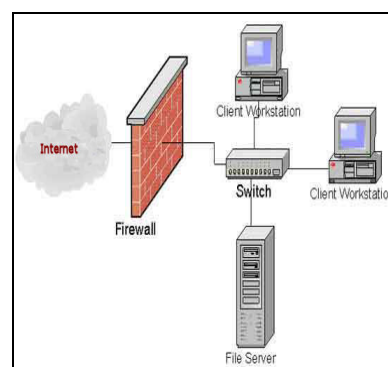
Il campo della sicurezza è un campo vastissimo ed in continua evoluzione, ogni giorno si scoprono nuove vulnerabilità ed ogni giorno vengono proposte nuove soluzioni.

3.1 Gli honeypot

E' risaputo che per proteggersi da una minaccia, bisogna prima conoscerla. Esiste un solo modo per tener traccia in tempi brevissimi delle nuove ed effettive tecniche di *hacking*: gli *honeypot*. L' *honeypot* è uno strumento di rete in attesa di essere attaccato. Tutto il traffico diretto verso di lui ha il solo fine di comprometterlo. Tutto il traffico generato da lui invece è la conferma che è stato compromesso! Per capire meglio il vantaggio di un *honeypot*, potrebbe risultare utile sottolineare la differenza con i normali sistemi di controllo di intrusioni (IDS). A differenza degli *Intrusion Detection System* infatti, che hanno per lo più una funzione passiva e che possono essere sovraccaricati da finti allarmi, un *honeypot* raccoglie sempre con un' elevata determinazione gli attacchi effettivi. Inoltre, per reagire ad un attacco spesso c'è bisogno di scollegare la macchina dalla rete, per lavorare in locale, ma questa procedura in una rete privata di grandi dimensioni non è praticabile. Avendo un *honeypot* a disposizione invece questa procedura può essere svolta senza ripercussioni.

3.2 Il firewall

Mediante opportuni strumenti è possibile collegare ad Internet la propria rete e al contempo mantenere la riservatezza ed un adeguato livello di protezione del Sistema Informativo aziendale. Questo è l'obiettivo dell'utilizzo del *Firewall*, il primo vero strumento difensivo attivo che un probabile aggressore incontra nella sua strada.



E' un sottosistema che, interposto tra la rete interna aziendale ed Internet, controlla tutto

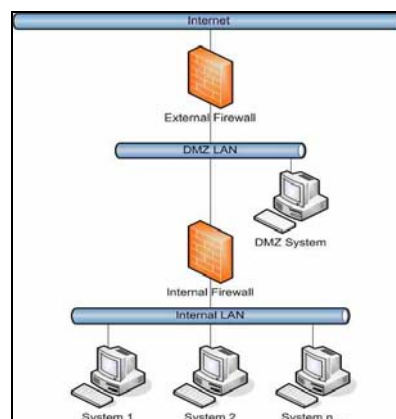
ciò che entra o esce dalla rete a cui è abbinato, evitando che possano venire eseguite operazioni che pregiudichino l'integrità e la sicurezza del sistema.

Naturalmente oltre a garantire un adeguato sistema di difesa nei confronti di attacchi di malintenzionati, esso deve garantire un accesso sicuro ed efficiente a tutti gli utenti che lavorano sul territorio (*mobile user*). La sua funzione consiste, come apparato di rete *hardware* o *software*, nel filtrare/controllare tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della stessa. La funzionalità principale è in sostanza quella di creare un filtro sulle connessioni entranti ed uscenti; in questo modo il dispositivo innalza il livello di sicurezza della rete e permette sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza. Il *firewall* agisce sui pacchetti in transito da e per la zona interna potendo eseguire su di essi operazioni di controllo. Questo grazie alla sua capacità di "aprire" il pacchetto IP per leggere le informazioni presenti sul suo *header* (struttura di un pacchetto IP), e in alcuni casi (*firewall* professionali) anche di effettuare verifiche sul contenuto del pacchetto. Il *firewall* è solo uno dei componenti della strategia di sicurezza informatica, infatti non può in generale essere considerato sufficiente perché la sua configurazione è un compromesso tra usabilità della rete, sicurezza e risorse disponibili per la manutenzione della configurazione stessa (le esigenze di una rete cambiano rapidamente) e perché una quota rilevante delle minacce alla sicurezza informatica proviene dalla rete interna prima citata.

3.3 La zona DMZ

Per quanto riguarda la rete interna, in essa non esiste isolamento tra il server e gli altri nodi, quindi nel malaugurato caso in cui un servizio in VLAN fosse compromesso in seguito ad una vulnerabilità, l'aggressore potrebbe raggiungere anche gli altri *host* della rete.

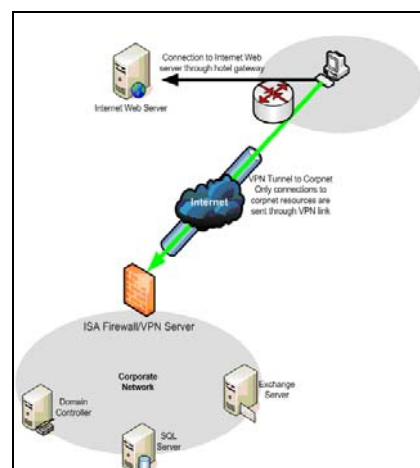
Infatti le più semplici reti locali sono a diretto contatto con la zona WAN (*wide area network*), la quale è la parte esterna (il comune *Internet*).



Nel caso della rete privata, si crea una terza zona: la DMZ. Essa è un'area in cui sia il traffico WAN che quello LAN sono fortemente limitati e controllati; in pratica, si tratta di una zona “cuscinetto” tra interno ed esterno, che viene attestata su una ulteriore interfaccia di rete del *firewall*, oppure viene creata aggiungendo un *firewall*. Generalmente si installano in DMZ i server detti front-end, a cui corrispondono i relativi *back-end* in LAN. Quindi se il problema precedente si verificasse in DMZ, l'attaccante avrebbe grosse difficoltà a raggiungere la LAN, poiché il traffico tra i server *front-end* e *back-end* sarebbe fortemente limitato, impedendone quasi sicuramente l'accesso.

3.4 L'IPsec

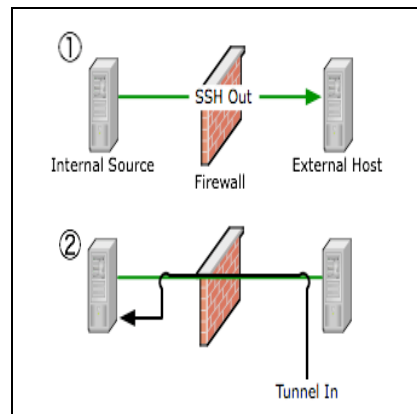
Lo standard usato di una rete che vuole essere ben sicura per ottenere connessioni basate su reti IP sicure è l'IPsec (abbreviazione di **IP Security**). Il suo compito è quello di effettuare una cifratura e l'autenticazione dei pacchetti IP. La capacità di fornire protezione a livello di rete rende questo protocollo trasparente al livello delle applicazioni che non devono essere modificate. Tuttavia l'uso predominante di IPsec è la creazione di *tool* di sicurezza come SSH e SSL.



I *tool* di controllo SSL e SSH usano un insieme di tecniche per cui un protocollo viene incapsulato in un protocollo dello stesso livello o di livello superiore per realizzare configurazioni particolari, questo processo è chiamato *tunnelling*, che in sostanza, consente di creare un “tunnel” fra i due elaboratori connessi entro cui vengono quindi trasmessi i dati.

3.5 SSH e SSL

L'SSH (o *Secure SHell*) è un protocollo che facilita i collegamenti sicuri tra due sistemi, usando un'architettura del tipo *client/server* permettendo agli utenti di registrarsi in sistemi *host server*, in modo remoto. A differenza di altri protocolli remoti di comunicazione, come FTP o Telnet, SSH cripta la sessione di *login*, impedendo alle persone non autorizzate di ottenere le password in chiaro.



SSH è stato progettato per sostituire applicazioni precedenti meno sicure utilizzate per l'accesso a sistemi remoti come telnet o rsh. Un programma chiamato *scp* sostituisce i programmi meno recenti per copiare i file tra *host*, quali *rcp*. Poichè queste applicazioni non cifrano le *password* tra il *client* e il *server*, si consiglia di utilizzarle il meno possibile. Se usate dei metodi sicuri per collegarvi ad altri sistemi remoti, correte meno rischi per la sicurezza del vostro sistema e del sistema a cui vi collegate.

L'SSL, o *Secure Sockets Layer*, è un protocollo che abilita le applicazioni *server-client*, in grado di passare informazioni desiderate in modo sicuro. SSL utilizza un sistema di coppie di chiavi private e pubbliche, per cifrare le comunicazioni che intercorrono tra *client* e *server*. Le chiavi pubbliche possono essere accessibili, mentre sarà necessario rendere sicure le chiavi private.



Il rapporto matematico (una firma digitale) che intercorre tra una chiave privata e una pubblica corrispondente, rende possibile il corretto funzionamento del sistema. Attraverso il suddetto rapporto viene stabilito un collegamento fidato.

3.6 Antivirus e anti-spyware

Oltre ai mezzi citati, non sono da sottovalutare due importanti *software* che dovrebbero essere installati sul *computer* di ogni singolo utente della rete:

L'antivirus, il quale consente di proteggere il proprio *personal computer* dagli “intrusi”. Un buon *antivirus* deve essere costantemente aggiornato ad avere in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l'utente deve avviare con regolarità la scansione dei dispositivi del PC (dischi fissi, CD, DVD e dischetti *floppy*), per verificare la presenza di *virus*, *worm* e qual altro. Per evitare la diffusione di virus è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall'*antivirus* correttamente configurato a tale scopo.

L'Anti-Spyware, il quale è un utilissimo *tool* per la rimozione di *spyware*.

CONCLUSIONE

Questi sono i più importanti accorgimenti che una rete interna privata utilizza per difendere le informazioni in essa circolanti. Questi non garantiscono la totale sicurezza, ma creano una protezione a strati difficilmente superabile. L'accortezza fondamentale per difendersi dalle intrusioni resta comunque quella che ogni gestore di rete deve imporre ad ogni utente: la consapevolezza del pericolo derivante dai comportamenti errati degli operatori, tanto che il "fattore umano" rappresenta l'elemento sensibile nelle policy di sicurezza. Il singolo utente della rete deve conoscere ed essere consapevole dell'esistenza di rischi e consapevolezza delle situazioni di pericolo derivanti dalle proprie azioni nell'ambito della rete. Se i comportamenti umani orientati alla sicurezza venissero a mancare, il rischio di intrusioni, abusi, sottrazioni o alterazioni di dati salirebbe in modo considerevole, quindi, come nella vita "di tutti i giorni", anche nelle reti serve un comportamento responsabile da parte degli utenti. Appare evidente quindi che nelle policies di sicurezza delle reti, i comportamenti irresponsabili degli utenti possono vanificare il lavoro di controllo svolto da software e hardware, con lo svantaggio che tali inadempienze non possono essere facilmente controllabili dagli amministratori di rete.

BIBLIOGRAFIA

- O. Bertazioli; TELECOMUNICAZIONI (vol. B); seconda edizione; luogo di edizione Bologna; Zanichelli; 2004.
- Gai S., Montessoro P.L., Nicoletti P.; RETI LOCALI Dal cablaggio all'internetworking; L'Aquila; Scuola Superiore G. Reiss Romoli; 1999.

GLOSSARIO

Attachment: È un file allegato ad una e-mail. È possibile allegare uno o più file alla stessa e-mail, e questi possono essere file di qualsiasi formato ma con le restrizioni imposte dal proprio provider sul tipo (alcuni non permettono di inviare file eseguibili) e sulla dimensione. Per inviare e leggere gli attachment è necessario avere un client che supporti il protocollo MIME.

Back end: vedi voce Front end

Backup: indica un'operazione tesa a duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita (per esempio una volta al giorno o alla settimana).

Broadcast: è la trasmissione di informazioni da un sistema trasmittente ad un insieme di sistemi riceventi non definito a priori (esempio: un pacchetto inviato ad un indirizzo di tipo broadcast verrà consegnato a tutti i computer collegati alla rete). Un dominio di broadcast è un insieme di computer in una rete che possono scambiare dati a livello datalink, senza che questi debbano risalire fino al livello di rete in altri nodi dello stesso insieme.

Browser: è un programma in grado di interpretare il codice HTML (e più recentemente XHTML) e visualizzarlo in forma di ipertesto.

Chiave: sequenza di dati (stringa) di lunghezza arbitraria impiegata come parametro dall'algoritmo di criptatura/decriptatura. La lunghezza della chiave determina la difficoltà di decodifica del messaggio non conoscendo la chiave di decodifica.

Cifratura/Criptatura: processo di trasformazione dell'informazione (testo in chiaro) in testo cifrato, guidato da una chiave.

Client: si indica una componente che accede ai servizi o alle risorse di un'altra componente, detta server. In questo contesto si può quindi parlare di client riferendosi all'hardware o al software.

Commutazione di pacchetto: è una tecnica di accesso multiplo a ripartizione nel tempo, utilizzata per condividere un canale di comunicazione tra più stazioni in modo non deterministico, utilizzata generalmente per realizzare reti di calcolatori. Si distingue dalla commutazione di circuito, che è tipicamente usata nelle comunicazioni telefoniche.

Crittografia: disciplina che studia l'utilizzo e la creazione di crittosistemi. L'arte (la scienza) di trasformare le informazioni in una forma intermedia sicura. A differenza della steganografia, che cerca di nascondere l'esistenza di qualunque messaggio, la crittografia si occupa di rendere il messaggio illeggibile benché completamente accessibile.

La crittografia comprende necessariamente la segretezza (confidenzialità) e l'integrità (autenticazione del messaggio). Può comprendere il non disconoscimento (l'impossibilità di negare l'avvenuto invio di un messaggio) ed il controllo d'accesso (autenticazione dell'utente).

Datagram o Pacchetti: unità elementare delle informazioni trasmesse su Internet contenente i dati necessari per essere correttamente trasportata dal mittente al destinatario senza che sia necessario avere informazioni su scambi di informazioni precedenti tra le stesse entità. Il termine è stato sostituito, in generale, da pacchetto.

I datagram, o i pacchetti, sono le unità fondamentali che vengono gestite dal protocollo IP.

Ethernet: è il nome di un protocollo per reti locali, sviluppato a livello sperimentale da Robert Metcalfe e David Boggs, suo assistente, alla Xerox PARC. L'obiettivo originale dell'esperimento era ottenere una trasmissione affidabile a 3Mbps su cavo coassiale in condizioni di traffico contenuto, ma in grado di tollerare bene occasionali picchi di carico. Per regolamentare l'accesso al mezzo trasmissivo era stato adottato un protocollo di tipo CSMA/CD (*Carrier Sense Multiple Access / Collision Detection*).

Front end e back end: denotano, rispettivamente, lo stadio iniziale e lo stadio finale di un processo. Il *front end*, nella sua accezione più generale, è responsabile per l'acquisizione dei dati di ingresso e per la loro elaborazione con modalità conformi a specifiche predefinite e invarianti, tali da renderli utilizzabili dal *back end*. Il collegamento del *front end* al *back end* è un caso particolare di interfaccia.

FTP: File Transfer Protocol (*protocollo di trasferimento file*), è un servizio che fornisce gli elementi fondamentali per la condivisione di file tra host.

Gateway: "Porta", o punto di collegamento tra due o più reti differenti. In Internet un gateway indirizza i datagram sulle numerose reti collegate. Nelle reti aziendali il gateway è un computer che serve anche da firewall e da proxy server.

Un gateway viene spesso associato ad un router, il quale sa in che direzione spedire il datagram ricevuto, e uno switch il quale fornisce il percorso d'ingresso e d'uscita dal gateway per un pacchetto di informazioni.

Header: è un file che aiuta il programmatore nell'utilizzo di librerie durante la programmazione.

Host: computer della rete che ospita risorse e servizi disponibili ad altri sistemi.

HTML: è il codice col quale la maggioranza delle pagine web nel mondo sono composte: il web browser consente perciò la navigazione nel web.

Hub: nella tecnologia delle reti informatiche rappresenta un concentratore, un dispositivo di rete che funge da nodo di smistamento di una rete di comunicazione dati organizzata prevalentemente a stella.

IDS: Intrusion Detection System, è un dispositivo software e hardware utilizzato per identificare accessi non autorizzati ai computer o alle reti locali. Le intrusioni rilevate possono essere quelle prodotte da cracker esperti, da tool automatici o da utenti inesperti che utilizzano programmi semiautomatici.

IP Address: indirizzo numerico di un nodo (computer) di Internet. La traduzione da indirizzo testuale a IP-address è possibile attraverso l'interrogazione di un Name Server.

Malware: è un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche codice maligno.

Pacchetto: ciascuna sequenza di dati distinta trasmessa su una rete o in generale su una linea di comunicazione (ad esempio su una linea seriale) che utilizzi la Commutazione di pacchetto.

Polling: operazione sequenziale di test, tra master e slave, dello stato di più dispositivi, effettuata per stabilire quello che richiede un servizio.

Modalità per il controllo delle comunicazioni distribuite in cui un sistema centrale interroga ciclicamente le stazioni ad esso connesse per verificare se hanno messaggi da trasmettere o richieste da evadere.

Proxy: un proxy è un server che si interpone tra un'applicazione client, ad esempio un Browser Web e il server vero e proprio. La sua funzione stà nell'intercettare le richieste rivolte al vero server e nel soddisfarle se è in grado di farlo, altrimenti le inoltra al vero server.

Rete a stella: è caratterizzata da un punto centrale, centrostella, che può essere uno switch o un elaboratore e diversi host connessi ad esso. La rete a stella diventa a stella estesa quando al posto di un host collegato al centrostella c'è un altro apparato attivo, switch o hub con a sua volta altri host collegati ad esso.

Router: rende possibile la connessione tra reti. Un router è in grado di leggere l'indirizzo di destinazione di qualsiasi pacchetto di rete e dirige quest' ultimo a una rete che può raggiungere oppure a un altro router se la rete di destinazione è fuori dalla sua portata.

Scp: è un comando molto utile per trasferire file tramite ssh. In particolar modo si rivela utile per lo scambio di file.

Server: è una componente informatica che fornisce servizi ad altre componenti (tipicamente chiamate client) attraverso una rete. Si noti che il termine *server*, così come pure il termine *client*, possono essere riferiti sia alla componente software che alla componente hardware.

SMTP: sigla di Simple Mail Transfer Protocol, protocollo standard che regola il trasferimento dei messaggi e-mail da un calcolatore all'altro.

Switch: nelle reti di telecomunicazione, lo switch è uno strumento che incanala i dati in entrata provenienti da una qualsiasi tra le molteplici porte, in direzione della porta specificata per l'output.

TCP: sigla di Transmission Control protocol, protocollo che regola il trasferimento dei messaggi: si preoccupa di garantire che il flusso dei dati generati dalla sorgente sia ricevuto alla destinazione.

WAN (Wide Area Network): rete che si estende su un area geografica costruita usando servizi di telecomunicazione pubblici (es. Telecom)