Che cosa è un Server WEB ?

Un server web ha il compito di fornire pagine HTML al Client che ne fa richiesta. Tali pagine, possono essere ***statiche*** - se il loro contenuto è identico tra la copia residente sul server e quella trasmessa al Client - oppure ***dinamiche*** - se invece vengono generate in risposta ad una richiesta specifica.

Esempio:

Supponiamo di mettere su un sito una pagina contenente l'elenco dei continenti della terra, probabilmente avrei una pagina statica, dal momento che i continenti quelli sono e quelli (nella teoria) dovrebbero rimanere.

Se, invece, dovessimo mettere su un sito un catalogo di smartphone, probabilmente opteremo per una pagina dinamica, dal momento che gli smartphone si evolvono e si sostituiscono di continuo.

La comunicazione tra client e Server avviene mediante protocollo **HTTP** il quale utilizza la porta di comunicazione 80 (TCP).

Il Firewall

Un firewall è un dispositivo software (o hardware) in grado di analizzare il contenuto dei pacchetti che viaggiano tra due reti e decidere, in base a regole ben precise e prestabilite, se autorizzarne l'inoltro o meno; esso opera su quattro aspetti fondamentali:

- ***Sicurezza***
- ***Filtro - (per pacchetti sia in entrata che in uscita)***
- ***Gateway***
- ***Estensione della propria LAN (VPN)***

Il compito di un firewall è quello di intercettare e analizzare queste informazioni ed in base a regole prestabilite dall'amministratore della rete su cui è posizionato il firewall, fare in modo che l'host della sua LAN possa o meno dialogare con l'host remoto.

Per i Firewall di tipo Software si va, ad esempio, dal classico **Zone Alarm** - adatto a postazioni Stand Alone - al completissimo **Check Point**, il cui costo è decisamente fuori dalla portata delle tasche del semplice utente "*mortale*".

Per i modelli hardware invece, si va da prodotti come **Zyxel**, **Dlink** fino ai **Watchguard**.

Ritengo che non si possa fare un paragone e stilare una classifica di merito tra hardware e software ma tutto dipende da molti fattori :

- **Postazioni da proteggere**
- **Chi lo deve amministrare**
- **Budget a disposizione**
- **Sistema operativo da utilizzare**

E' chiaro che il funzionamento di un Firewall, si basa sul filtro e quindi sull'ispezione dei pacchetti da e verso la LAN cui è preposto.

Quando viene stabilita una connessione tra due Host, questi si scambiano una serie di informazioni per fare in modo che la comunicazione avvenga tra loro (e solo tra loro).

Questo compito viene assolto tramite l'assegnazione di **policies** o regole di accesso che si dividono **allow** e **deny**.

Le regole **allow** consentono ai pacchetti che le rispettano di entrare e/o uscire da o verso la LAN, quelle **deny** rifiutano i pacchetti che non rispettano queste regole - in conseguenza la comunicazione tra host (tra loro remoti) viene interrotta dal firewall.

Nella configurazione delle regole, dette anche **rules**, si devono indicare:

- il tipo di azione (ALLOW o DENY)
- il tipo di servizio (rappresentabile spesso con il nome stesso - esempio web, mail, ftp ecc... - oppure con il numero della porta TCP di cui il servizio stesso usufruisce per esercitare la sua azione (es. 80, 110, 25, 20, 21 ecc...)
- l'origine (source) del pacchetto:
  a) * - tutte le origini : LAN, WAN, DMZ;
  b) LAN - il filtro verrà applicato solo ai pacchetti in uscita - utile si si vuole, per esempio, impedire l'utilizzo di determinati servizi di file sharing;
  c) WAN - le rules saranno applicate ai pacchetti che dalla WAN tentano di stabilire una connessione con un Host della LAN;
- Destinazione (**destination**): valgono le stesse regole applicate alla sorgente (source), quindi si potranno trovare le identiche tre differenti tipologie di destinazione
- In alcuni dispositivi, inoltre, potremmo trovare ulteriori settaggi da effettuare per le **rules**, come ad esempio i giorni della settimana cui applicare la regola o l'orario in cui le stesse andranno in vigore, in altri dispositivi più evoluti sarà possibile anche configurare la banda e garantirla. Si consideri il caso del collegamento tra due sedi remote A e B e la necessità di consentire che il Server Web (A) debba comunicare con un altro Server DBase (B) e che la comunicazione tra i due server sia essenziale per l'azienda. In questa circostanza, si potrà impostare una regola per cui allo scambio di informazioni tra i due server sia garantita una certa banda, indicando anche la banda minima ed eventualmente le priorità.

Esempio di Configurazione

Allow HTTP Management LAN 192.168.10.22 (LAN)
Deny SMB-CIFS WAN LAN
Deny NetBios WAN LAN
Deny Key Exchange (IKE) LAN *
Deny Napster LAN *
Deny SMB-CIFS LAN *
Deny NetBios LAN *
Allow DHCP LAN LAN
Deny Default 82.57.86.* (WAN) LAN
Deny Default 213.238.41.* (*) LAN
Deny Default 203.166.18.* (*) LAN
Deny Default 67.18.152.* (*) *
Deny Default 215.64.202.* (*) *
Deny Default 215.134.13.* - 217.133.13.254 (WAN) LAN
Deny Default 215.134.208.* - 217.133.208.254 (WAN) *

Questo è un esempio di come si possano configurare delle regole di accesso dalla o verso una LAN.

DMZ

Una funzione presente in tutti i Firewall (si può implementare anche su firewall software) è la cosiddetta DMZ detta anche *zona demilitarizzata*.

Si tratta di una zona fisicamente accanto alla LAN ma ad un livello IP diverso o meglio separato - la stessa LAN risulterebbe fortemente molto più sicura in quanto dall'esterno la DMZ sarebbe l'unica rete accessibile.

Viene in genere attivata quando, per necessità, si deve dirottare il traffico esterno, proveniente da fuori, su alcuni Host interni, che per necessità devono restare isolati dal resto della rete LAN.

Come testare la sicurezza della propria LAN

Uno dei siti da cui poter testare la sicurezza della propria LAN, è la **Gibson Research** che propone il tool ShieldsUP! che provvede a scansionare le porte sull'IP pubblico da cui vi si accede.

ShieldUP! Provvede a indicare tutte le possibili falle di sicurezza del nostro sistema

Le vulnerabilità conosciute e l'accesso non autorizzato

Spesso gli attacchi informatici sono mirati a colpire vulnerabilità conosciute nei software residenti sugli Host remoti. Un esempio calzante è costituito da "*Internet Explorer*".

Dalla sua nascita, che questo browser ha avuto bisogno di decine e decine di patch e update destinati a risolvere falle a livello di programmazione sfruttate da qualcuno che le aveva scoperte prima della Microsoft.

Cosa è l'accesso non autorizzato ?

L'accesso non autorizzato è concettualmente uno degli attacchi più semplici da interpretare.

Infatti, alla base della definizione stessa si trova il *corpus* dell'attacco e quindi *é il collegarsi in modalità illegale e non autorizzata a un host*.

Si immagini, ad esempio, di connettersi senza avere avuto autorizzazione a un server FTP di un'azienda o ad uno spazio web senza averne la necessaria autorizzazione.

Cosa è il Denial of Service (DOS)

ATTENZIONE!!: *Il contenuto di questo articolo ha solo scopo divulgativo ed è inteso con l'obiettivo di conoscere un problema nelle sue diverse sfaccettature. Lo scrivente non si assume responsabilità per l'uso che possa derivare dalla lettura di questo testo.*

Il Denial of Service meglio conosciuto come attacco DOS provoca, in seguito all'invio di una spropositata quantità di richieste verso un servizio ospitato da un host, la sospensione del servizio oggetto dell'attacco (di qui il nome).

Un esempio chiarirà meglio il problema:

L'obiettivo del nostro esempio, sarà Il blocco del servizio web.

Supponiamo di avere una rete di computer dove uno dei quali ha funzioni di Web Server.

*Per effettuare un **DoS**, predisponiamo una pagina Html* – da mettere all'interno del Server web - *in tasta alla quale scriviamo un'istruzione javascript che vada in loop e sia destinata ad effettuare il refresh automatico della pagina ad ogni caricamento e ad ogni 1ms.*

A questo punto ciascuno dei computer della rete caricano la stessa pagina Html predisposta in precedenza. Il Server Web, dopo un po', non riuscendo a evadere tutte le richieste, si bloccherà.

Generalmente un attacco di tipo **DoS** viene effettuato da schiere di Host su cui vengono installati appositi programmi software progettati appositamente per lo scopo.

Sniffing

ATTENZIONE: *Il contenuto di questo articolo ha solo scopo divulgativo ed è inteso con l'obiettivo di conoscere un problema nelle sue diverse sfaccettature. Lo scrivente non si assume responsabilità per l'uso che possa derivare dalla lettura di questo testo.*

Un Host posto in ascolto, ***sniffa***, cioè, cattura dati non diretti a lui stesso. Da qui il termine **sniffing**. Immaginiamo per esempio, di utilizzare un prodotto come Ethereal o EtherPeek o Wireshark su di una rete – vi ricordo che ciò costituisce reato ed "*ascoltiamo*" il traffico generato dall'**utente** X **(**che **potrebbe essere il nostro** ignaro vicino di casa**,** il quale **si sta loggando sulla** pagina della sua Webmail.
Mediante lo **sniffing**, uno ***sniffer*** (personaggio), carpisce informazioni come la *userid, password* ed il *contenuto dei messaggi* che il nostro utente X sta leggendo.

Il Port Scanning

In molti casi gli strumenti posti a protezione della nostra connessione segnalano spesso attività di ***port scanning***:

Un Host remoto vuol sempre sapere se sul nostro Host è attivo qualche servizio, conseguentemente, in linea teorica, sarebbe attaccabile.

Per poter verificare quali servizi offra il nostro host al "*mondo esterno*", si effettuerà un **Netstat** da shell del DOS e provvedere al blocco delle richieste in entrata di alcuni servizi o alla loro limitazione (ad esempio la condivisione Windows - porte 137-138-139 e 445 si può restringere ai soli utenti della LAN via firewall software).

Per gli utenti Linux, l'attenzione va indirizzata alle porte 901 (servizio Swat per la configurazione di **Samba**) e 10000 (connessione a **Webmin** strumento di amministrazione orientato ai server) che sono le più ambite dagli "sniffer".
In ogni caso anche sull'attività di **port scanning** occorre essere prudenti, nel senso che la gran parte di queste attività sono effettuate solo a fini ***didattici***.

Per esempio una volta installato **Nmap** ci viene naturale vedere cosa c'è al di là della propria rete. (Certamente un conto è dare un'occhiata ed un altro è causare danni a terzi).

Cosa fare quando si è vittime di un attacco

Il contenuto di questo articolo non è chiaramente esaustivo dell'argomento, ma ne è un'esemplificazione per darne un idea

Ciascun Host connesso ad internet è esposto continuamente a diversi tipi di attacco, il più diffuso è il **DOS** (Denial of Service) tendente a mettere **KO** un servizio in esecuzione.

Quando si rimane vittima di attacchi e ci si accorge della cosa (router e firewall producono dei log cioè monitorano – se attivo - l'attività sulla porta WAN registrandone le attività su file, prodotti come ad esempio **ZoneAlarm**, avvisano se c'è una qualche forma di attività sospetta in corso e se ciò si verificasse, sarebbe buona norma cercare di:

- trovare l'indirizzo IP di chi sta tentando l'intrusione e annotarne l'ora esatta;
- possibilmente bloccarne immediatamente la connessione mediante l'uso di un filtro sul router o attivando un firewall o mediante prodotti software;
- isolare la tipologia di attività sospetta (DOS, Land Attack ecc);
- eseguire un **Netstat** da prompt per verificare che non ci siano connessione a host sconosciuti.

Chi è o cosa é l'Open Relay

Quando si installa un server di posta elettronica, l'host che offre il servizio espone al pubblico il servizio stesso e può divenire - se non configurato in modo corretto - un veicolo per l'invio indiscriminato di email da parte di terzi - in modalità trasparente rispetto al proprietario del server stesso.

Ciò può comportare di pagare a caro prezzo, anche nel caso di abusi (spam, ad esempio) compiuti da altri che si appropriano dell'identità dell'ignaro open relayer.

Per impedire al proprio server di posta di accettare connessioni non autorizzate, sarà necessario almeno accettare l'invio di messaggi solo tramite autenticazione.

Cosa è un Hijacked IP

Per Hijacked IP (alla lettera) si intende il **furto di indirizzo IP**.

Cosa significa rubare uno indirizzo IP ?

Gli **ISP** (Internet Service Provider), sono coloro che forniscono agli utenti di tutti il mondo un accesso a internet (Vodafone, Telecom, Wind ecc.), hanno a disposizione un certo numero di indirizzi IP da assegnare a chi richiede una connessione:

Va da sè che il vedersi attribuito un IP all'atto di richiedere l'accesso alla rete presuppone una sorta di registrazione.

A questo punto alcuni "*simpatici personaggi*", si sono inventati di prendersi - in maniera illegale - IP destinati ad altri oppure si sono assegnati (*ancora in maniera illecita*) indirizzi IP non più utilizzati.

Questo a grandi linee è il significato di IP hijacking.