Lesson 6: Pubblicazione Servizi

Internet

Durante le precedenti lezioni abbiamo preso in considerazione la sicurezza lato interno alla rete evidenziando il fatto che la percentuale di attacchi informatici effettuati dall'interno è enormemente superiore rispetto a quelli provenienti dall'esterno alla rete stessa.

E' comunque un dato certo che la crescente disponibilità di banda passante, unita ai sempre minori costi di connettività e alla disponibilità sempre maggiore dei punti d'accesso, ha reso di fatto internet il principale mezzo di comunicazione tra le aziende e il mondo esterno che viene sfruttato per la pubblicazione dei servizi.

Purtroppo, come tutte le cose, anche questa magnifica costruzione ha il suo **tallone d'Achille**: "la sicurezza".

Le reti digitali sono intrinsecamente insicure, in quanto "reti aperte", non sono state progettate in modo da garantire autoprotezione e difesa contro eventuali abusi.

Come abbiamo avuto modo di evidenziare nelle precedenti lezioni, le reti dati sono particolarmente sensibili all'intercettazione e all'alterazione dei dati trasmessi, nonché alla violazione dei supporti informatici ad esse connessi.

A seconda dell'applicazione realizzata, il problema può essere più o meno sentito in funzione della tipologia di dati trasferiti. Quando si parla di commercio elettronico o più in generale quando i dati trasferiti contengono informazioni riservate, la sicurezza diventa il presupposto fondamentale sul quale si fonda il rapporto fiduciario fra acquirente e venditore, fra banche e correntisti, fra azienda e collaboratori esterni. Senza la fiducia, ispirata dalla sicurezza delle transazioni, non può essere instaurata nessuna relazione.

Senza garanzie adeguate l'utente non avrà incentivi all'utilizzo di tali tecnologie che, sebbene più convenienti, sono anche più insicure.

Inoltre, il desiderio di garantire il proprio anonimato da parte dell'utente mal si concilia con la necessità del sistema informatico che rende obbligatoria l'imputazione dei dati. Di fatto questa operazione se captata potrebbe svelare l'identità degli utenti e le operazioni fatte.

Anche il tentativo di creare siti completamente anonimi va contro le esigenze di imputabilità, autenticità, integrità, revocabilità o non ripudiazione, e non può certo essere in armonia con la necessità di applicare la legge a fronte di frodi più o meno significative.

L'ideale è trovare un giusto bilanciamento fra tutte le diverse esigenze, ma tale compromesso deve essere adeguatamente protetto.

La protezione delle informazioni trasmesse via Internet, oltre a richiedere tutte le attenzioni normalmente dedicate ai corrispondenti documenti cartacei, richiede anche quelle necessarie a garantire la sicurezza dell'intero processo trasmissivo.

Il passaggio dai documenti tradizionali al relativo documento elettronico deve essere gestito in maniera tale da conservare, ed eventualmente migliorare, le tradizionali politiche di sicurezza al fine di rendere l'intero sistema di comunicazione sicuro.

Il WEB

L'efficacia del Web, come mezzo di divulgazione delle informazioni o come strumento per la vendita di prodotti/erogazione di servizi, è ormai nota a tutti e spinge, giorno dopo giorno, sempre più entità e organizzazioni a scegliere Internet come canale preferenziale di contatto con il pubblico.

L'uso di questo canale, se da un lato apre la strada a possibilità di sviluppo prima impensabili, dall'altro presenta dei rischi che non possono essere sottovalutati.

Le cronache di tutti i giorni riportano sempre con maggiore frequenza notizie relative ad intrusioni perpetrate ai danni di sistemi informatici più o meno noti. Non passa settimana in cui, attraverso la pubblicazione dei principali bollettini di sicurezza, non venga data rilevanza della scoperta di pericolosi "bug o exploit" destinati ad essere sfruttati per compiere attacchi informatici di vario genere.

Ma cosa rende un server Web una risorsa così appetibile ed esposta agli attacchi esterni? Sicuramente una combinazione di molteplici fattori tra i quali vanno citati i seguenti:

- i server Web spesso rappresentano delle vere e proprie porte di accesso alla rete interna (LAN) nella quale sono custodite le informazioni più svariate (informazioni aziendali, dati sul personale, sulla clientela, dati di rilevanza economica e legale, etc..);
- la sottovalutazione dei rischi e la mancanza di risorse economiche ed umane da dedicare al potenziamento delle politiche di sicurezza e la scarsa progettazione e qualità del software possono determinare l'insorgere di una condizione di intrinseca vulnerabilità dei servizi Web resa ancora più grave dalla loro esposizione al pubblico;
- condurre con successo un attacco sul Web utilizzando le classiche porte del servizio http (80, 81, 8000, etc..) è molto più facile dal momento che nella stragrande maggioranza dei casi il traffico veicolato in questo modo non è bloccato dai dispositivi di controllo degli accessi (router e/o firewall).

Dalla combinazione di questi ed altri fattori, possiamo trarre lo spunto per fare una semplice osservazione: via via che si acquisisce visibilità in Internet si accrescono anche le probabilità di vedere, prima o poi, il proprio server violato.

Il rischio di subire intrusioni o attacchi di altro genere non è soltanto circoscritto ai grandi portali del Web ma si estende anche alle semplici risorse di carattere statico le quali, se non debitamente protette, possono attirare l'attenzione, non proprio benevola, di qualche male intenzionato.

Sfortunatamente non esistono nè rimedi nè tecniche tali da poter rendere sicuro al 100% un server contro gli attacchi provenienti dall'esterno, ma si può operare nella direzione di rendere più sicuro il proprio server, iniziando con il tenere lontani problemi e vulnerabilità.

Per fare ciò occorre innanzitutto comprendere la natura e la portata dei pericoli ai quali ci si espone e successivamente adottare delle precauzioni di carattere generale, dirette a circoscrivere i rischi suddetti entro limiti accettabili in relazione alla natura degli interessi da proteggere.

Individuazione dei rischi

I pericoli derivanti dalla mancata adozione di adeguati criteri di sicurezza, nell'allestimento e nel mantenimento di un sito Web pubblicato, sono fondamentalmente riconducibili alla possibilità di un abuso del servizio da parte di soggetti malintenzionati. Questo abuso può essere perpetrato in svariati modi, ma molto spesso viene concepito sfruttando gli errori di configurazione o le vulnerabilità esistenti a livello di:

- sistema operativo;
- servizio http o altri servizi di rete (smtp, database, ftp, etc..);
- programmi/interpreti e script utilizzati per la generazione del contenuto del sito;
- dispositivi di controllo degli accessi (routers e firewalls).

In linea generale, il percorso che un aggressore tenta di seguire nell'attacco di un sistema può essere riassunto nel seguente modo:

- accesso al sistema attraverso l'esecuzione di exploit;
- sfruttamento di condizioni di buffer overflow in script e programmi;
- cattura o intercettazione del file delle password;
- attacchi a forza bruta;
- scalata dei privilegi e/o impersonificazione degli utenti con privilegi amministrativi attraverso il crack delle password e/o l'esecuzione di exploit successivi;
- occultamento delle tracce tramite la cancellazione dei logs;
- uso di rootkits e sfruttamento di particolari caratteristiche del sistema operativo;
- installazione di backdoors cioè di programmi nascosti che permettono all'aggressore un ritorno e una ripresa del controllo del sistema in un secondo momento.

Come conseguenza di queste azioni, l'aggressore può essere portato ad eseguire delle attività che rientrano nelle seguenti aree:

- attività che comportano una manipolazione del server e/o un trafugamento di informazioni;
- atti di vandalismo come la modifica dei contenuti delle pagine Web o la cancellazione del contenuto dell'intero sito;
- trafugamento di informazioni sensibili concernenti l'organizzazione, la configurazione di rete oppure la clientela o gli utenti;
- uso dell'host come base per lanciare attacchi contro altri sistemi (attacchi D.D.O.S - Distributed Denial of Service);
- installazione di strumenti per il monitoraggio del traffico di rete e la cattura di informazioni di autenticazione (sniffing);
- attività che producono una situazione di indisponibilità del servizio (D.O.S. - Denial of Service) cioè l'impossibilità per gli utenti di accedere alle risorse messe a disposizione dal server.

Il diniego del servizio (D.O.S) rappresenta per l'aggressore una soluzione estrema che, oltretutto, richiede spesso competenze tecniche davvero minime. Le conseguenze di simili attacchi sono veramente molteplici e vanno dalla sopportazione dei costi per il ripristino delle risorse al mancato realizzo di introiti. Ma l'aspetto più grave è la perdita di credibilità nei confronti del pubblico che può arrivare anche a conseguenze che implicano una responsabilità di carattere legale (perdita o trafugamento di informazioni sensibili a causa di una negligente gestione del sito).

White Paper.

Strumenti di Sicurezza

La DMZ: cos'è e perché si usa

Dividere la rete in zone è una tecnica considerata di base e rappresenta l'immediato vantaggio di aumentare la sicurezza. Cerchiamo di capire cos'è e come funziona la DMZ il cui acronimo significa "zona demilitarizzata".

La sicurezza perimetrale si occupa di proteggere una rete nei punti in cui essa è a contatto con il mondo esterno. In base al tipo di traffico e alla funzione si identificano diverse zone; nei casi più semplici, le uniche due zone, LAN e WAN sono attestate sui due lati del firewall.

Il lato LAN (local area network) è il segmento privato e protetto, e ad esso appartengono tutti gli host e i server i cui servizi sono riservati all'uso interno. Nelle lezioni precedenti abbiamo parlato di come implementare la sicurezza mediante l'uso delle VLAN per suddividere anche la rete interna.

La zona WAN (wide area network) è la parte esterna, e ad essa appartengono uno o più apparati di routing che sostengono il traffico da e per la rete locale, sia verso internet che verso eventuali sedi remote dell'azienda.

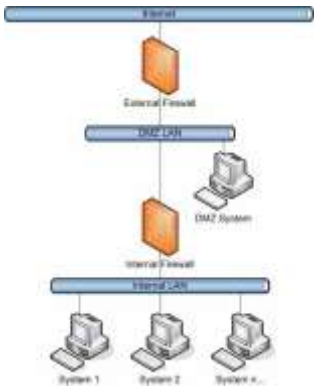
Non appena l'architettura della rete comincia ad evolversi, ci si trova nella necessità di esporre all'esterno alcuni servizi. Il caso più comune è la posta elettronica di cui abbiamo ampiamente discusso nella lezione 2.

L'installazione di un mail server "in casa" comporta la pubblicazione del servizio SMTP. Quando la struttura e il budget non sono particolarmente importanti, spesso si decide di fidarsi del firewall e delle sue tabelle di NAT.

Pubblicare direttamente la porta SMTP del server di posta non è ortodosso dal punto di vista della sicurezza. Questa soluzione è molto spesso adottata dalle piccole aziende che non possono sostenere costi di infrastruttura troppo elevati.

Non appena possibile è fortemente consigliata la creazione di una terza zona: la DMZ.

Una DMZ rappresenta di fatto 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 creata ex novo aggiungendo un firewall, come nello schema di seguito riportato.



Generalmente si installano in DMZ i server detti front-end, a cui corrispondono i relativi back-end in LAN.

Anche in questo caso l'esempio tipico è la posta elettronica. Il server che pubblica il servizio SMTP ed eventualmente la webmail, l'antispam e l'antivirus vengono posti sulla DMZ, mentre in LAN rimane il server che ospita il database delle caselle e gli altri servizi.

Altro caso tipico sono gli "application server", che isolano un database residente in LAN, ma offrono un' interfaccia come servizio verso l'esterno.

Quali sono i vantaggi per la sicurezza?

Nel malaugurato caso in cui un servizio in LAN risultasse compromesso a seguito di una vulnerabilità, l'aggressore potrebbe raggiungere anche gli altri host della rete, in quanto in LAN non esiste isolamento tra il server e gli altri nodi. Ma se lo stesso problema si verificasse in DMZ, l'attaccante avrebbe grosse difficoltà a raggiungere la LAN, poiché il traffico tra i server front-end e back-end è fortemente limitato dal firewall. In genere un server di front-end comunica solo con il suo back-end, e solo con le porte TCP e/o UDP strettamente necessarie.

Ricapitolando: la DMZ è un'area pubblica protetta, dove il traffico è strettamente regolato da entrambi i lati, è utile per pubblicare servizi verso l'esterno minimizzando i rischi per la rete interna. E' possibile realizzare architetture più complesse che possono implicare la presenza di più zone DMZ distinte, con il relativo controllo del traffico su tutti i lati.

Configurazione di base del server

In linea teorica il server Web dovrebbe operare nell'ambito di una configurazione di rete e di sistema davvero minima. Il rispetto di questa semplice regola è effettivamente in grado di produrre come risultato un sensibile miglioramento dei livelli di sicurezza attraverso degli espedienti quali:

- la disabilitazione di tutti i servizi di rete non essenziali e in particolar modo quelli affetti da vulnerabilità conosciute sotto il profilo della sicurezza;
- la rimozione dal sistema dei file corrispondenti ai servizi disabilitati;
- l'eliminazione delle porte TCP ed UDP in ascolto superflue;
- la rimozione o disabilitazione di tutte le risorse non richieste in relazione al ruolo dell'host (compilatori, interpreti, shell, scripts e altri strumenti analoghi);
- la corretta gestione degli utenti e dei loro privilegi;
- la predisposizione di regole adeguate per l'accesso e l'uso delle risorse.

I primi 4 punti sono particolarmente importanti non soltanto in un ottica generale di riduzione dei rischi di compromissione del sistema, ma anche in vista di uno snellimento delle attività di amministrazione e, quindi, della minore probabilità di commettere errori di configurazione che possono essere prontamente sfruttati dagli aggressori.

A tal fine, proprio per evitare di commettere dimenticanze, è conveniente adottare un approccio del tipo "deny all, then allow" che consiste prima nel disabilitare indistintamente tutti i servizi e le porte TCP/UDP e poi nel riabilitare, dopo un attenta analisi e valutazione, soltanto ciò che è veramente essenziale.

Anche per quanto concerne la gestione degli utenti e dei loro privilegi vanno prefissate regole improntate a criteri restrittivi quali:

- impedire che il "servizio http" venga lanciato da un utente con privilegi amministrativi che potrebbero comportare l'acquisizione del controllo completo del sistema in caso di exploit eseguito con successo;
- disabilitare o rimuovere tutti gli account inutili, installati dal sistema operativo o da altri software,in modo da ridurre il rischio di un' "impersonificazione" o scalata di privilegi nel caso di intrusione.
- Modificare il nome dell'account di amministratore.

- Adottare criteri di "robustezza password" sotto il profilo della lunghezza (almeno 8 caratteri), complessità (alfanumerica con un mix di caratteri maiuscoli e minuscoli e l'uso di caratteri non stampabili), riutilizzo (da evitare) e durata (mediamente 30-120 giorni);
- verificare "direttamente le password", preferibilmente mediante gli stessi strumenti usati dagli hackers, per accertarsi che esse rispondano ai criteri voluti;
- impostare il "blocco degli utenti" dopo un certo numero di tentativi falliti di login.

N.B.: il blocco degli utenti è una misura da adottare con cautela dal momento che costituisce un'arma a doppio taglio che potrebbe spingere l'aggressore a provocare una situazione di D.O.S. (Denial of Service) attraverso una serie di tentativi di connessione falliti.

I singoli processi coinvolti nella gestione del servizio http devono avere accesso soltanto ai file e alle directory necessari al loro funzionamento e per i quali occorre specificare delle regole di accesso (acl o access control list) che, oltre a offrire una maggiore granularità nel controllo dell'uso delle risorse, sono in grado di scongiurare o mitigare gli effetti derivanti da un eventuale attacco D.O.S., diretto a provocare una situazione di indisponibilità dell'intero sistema proprio attraverso l'esaurimento delle sue risorse.

Per ridurre significativamente gli effetti derivanti da attacchi di questo genere, è sempre consigliato il ricorso a ulteriori interventi correttivi che consistono nel:

- creare una singola directory radice e da essa far derivare una gerarchia di sottodirectory nelle quali suddividere le risorse che costituiscono il contenuto pubblico del Web;
- limitare a una sola directory, opportunamente configurata e protetta, tutti i programmi "esterni" eseguiti come parte integrante del servizio Web;
- limitare l'uso dei file temporanei da parte dei singoli processi all'interno di apposite directory opportunamente protette consentendone l'accesso soltanto ai processi stessi.
- impedire che file e risorse esterne alla gerarchia di directory del server possano essere forniti come risposta alle richieste degli utenti;
- disabilitare l'uso dei link simbolici per evitare che risorse facenti parte del contenuto del Web possano puntare a file di sistema o ad altre risorse all'interno della LAN;
- aggiustare le priorità dei vari processi di sistema.

Uso di programmi esterni

L'installazione e l'uso di programmi esterni quali "interpreti, plug-in e script" può letteralmente aprire una breccia nei livelli di protezione di qualsiasi server Web. Anche gli host apparentemente più inviolabili possono infatti cadere a causa di un banale exploit che sfrutta un semplice script "cgi" per eseguire localmente sul server comandi diretti ad ottenere l'accesso al sistema.

Siccome la storia è piena di esempi di questo genere, prima ancora di decidere se sfruttare le funzionalità aggiuntive fornite da script, plug-in e altro, è sempre opportuno valutare complessivamente i benefici e i rischi che ne derivano optando per l'adozione soltanto quando i primi siano realmente superiori ai secondi.

In ogni caso la preoccupazione principale deve sempre rimanere quella di ridurre i rischi entro limiti accettabili e per far ciò occorre:

- evitare, se possibile, l'uso di script di terze parti oppure accertarne l'esatta provenienza e autenticità del codice;
- fare uso soltanto dei programmi e degli script veramente indispensabili disabilitando tutti gli altri (ad esempio quelli dimostrativi spesso causa di molteplici problemi);
- impiegare tecniche di programmazione ortodosse nella scrittura del proprio codice prestando la massima attenzione ad aspetti quali la lunghezza e la complessità finale, la presenza di opportuni controlli per la validazione dell'input e l'interazione con altri programmi esterni o l'accesso in lettura e/o scrittura al file system;
- valutare attentamente la presenza di queste stesse caratteristiche anche negli script di terze parti;
- usare possibilmente una macchina di test per verificare il funzionamento di tutti i programmi e degli script prima ancora di impiegarli in una macchina di produzione;
- evitare di collocare i programmi e gli interpreti all'interno della stessa directory dove risiedono gli script (ad esempio la CGI-BIN) e posizionarli invece in una directory separata opportunamente protetta ed accessibile soltanto agli utenti amministratori;
- circoscrivere l'accesso di programmi ed interpreti ai soli file e directory indispensabili al loro funzionamento e comunque soltanto a quelli all'interno del contenuto pubblico del Web;
- verificare costantemente l'integrità degli eseguibili relativi a programmi ed interpreti e degli script.

Firewall

Con il termine FIREWALL si tende ad identificare in modo generico tutta una serie di funzioni e di apparecchiature che servono a proteggere un determinato dominio o rete privata.

E' fondamentale stabilire e creare una politica di regole (policy) per poter compiere le seguenti operazioni:

- determinare i servizi di cui si ha bisogno;
- determinare il gruppo di persone da servire;
- determinare a quali servizi ogni gruppo ha necessità di accedere;
- descrivere per ciascun gruppo come rendere sicuro il servizio;
- scrivere un'espressione che renda tutte le altre forme di accesso una violazione.

Le policy adottate diventeranno con il trascorrere del tempo e con l'aumentare dell'esperienza sempre più complicate e sempre più efficaci nel loro lavoro di prevenzione a protezione dei dati.

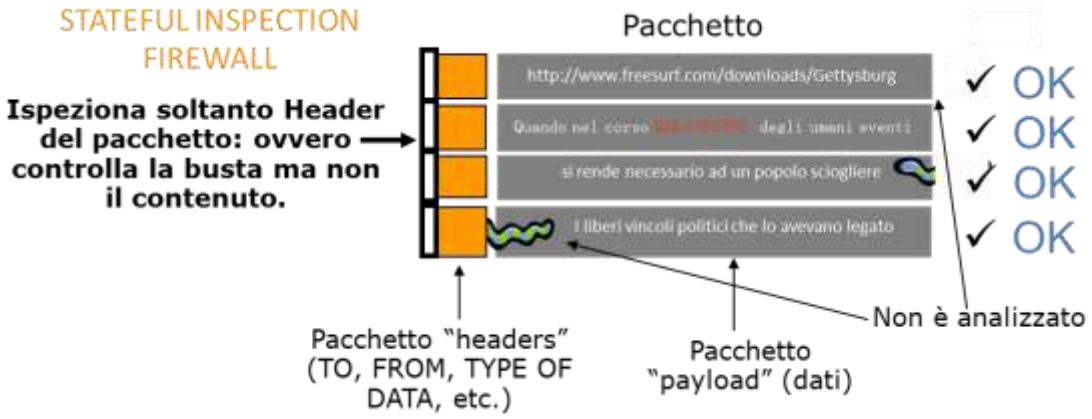
Esistono due tipologie di firewall:

- Firewall Filtranti - che bloccano i pacchetti di rete selezionati;
- Proxy Server (talvolta detti firewall).

Firewall Filtranti (Packet Filtering Firewall)

Il Packet Filtering è il tipo di firewall presente nel kernel Linux. Un firewall filtrante funziona a livello di rete. I dati possono lasciare il sistema solo se lo permettono le regole del firewall. I

pacchetti che arrivano sono filtrati in base alle informazioni sul tipo, sull'indirizzo di provenienza e di destinazione e sulle porte contenute (TCP/UDP) in ciascuno di essi. Molti router di rete hanno la capacità di effettuare servizi firewall. E' possibile immaginare un "firewall filtrante" come un particolare tipo di router, ma per poterci lavorare è necessaria una profonda conoscenza della struttura dei pacchetti IP.



Poiché sono analizzati e registrati pochissimi dati, i firewall filtranti occupano meno la CPU e di conseguenza creano minor latenza all'interno della rete. Non forniscono nessun controllo a livello di password in quanto gli utenti non possono identificarsi, perché la sola identità che un utente ha, consiste nell'indirizzo IP assegnato alla sua macchina. Attenzione se si intende usare il servizio DHCP (assegnazione dinamica dell'IP) in quanto l'indirizzo assegnato all'utente non è univoco ma variabile e assegnato in modalità Random dal servizio e siccome le regole sono basate sugli indirizzi IP, dovranno essere aggiornate ogni volta che vengono assegnati nuovi indirizzi.

I firewall filtranti sono più trasparenti per gli utenti in quanto non richiedono nessuna impostazione di regole per utilizzare Internet.

Proxy Server

I Proxy sono apparati H/W e S/W che vengono principalmente usati per controllare o monitorare il traffico. Alcuni proxy di applicazioni possono fare la cache dei dati richiesti (memorizzazione in locale), ciò abbassa le richieste di banda e diminuisce il tempo d'accesso per il successivo utente che vuole accedere agli stessi dati fornendo nel contempo un'evidenza inequivocabile su quanto trasferito.

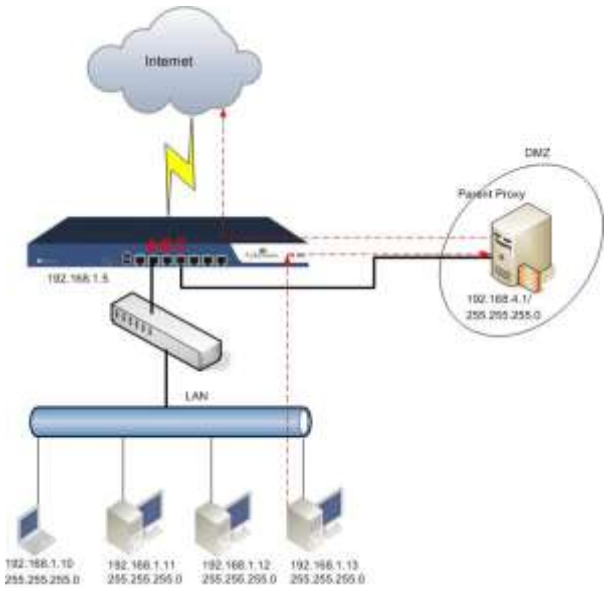
Esistono due tipi di proxy server:

- Application Proxy (Proxy di Applicazione);
- Proxy SOCKS - che "incrociano" le comunicazioni.

Application Proxy

Prendiamo in esame il caso di una persona che effettua un telnet su un altro computer e poi da qui al resto del mondo. Solo attraverso un proxy server di applicazione è possibile automatizzare il processo:

- non appena si fa telnet verso l'esterno il client indirizza al proxy;
- il proxy si connette al server richiesto (il mondo esterno) e restituisce i dati.



Poiché i proxy server gestiscono tutte le comunicazioni, sono anche in grado di registrare qualsiasi parametro si voglia e ciò può includere qualsiasi URL visitata "proxy HTTP (web)" o qualsiasi file scaricato "proxy FTP".

E' possibile anche filtrare parole "inappropriate" dai siti che si visitano, controllare la presenza di virus ed effettuare l'autenticazione degli utenti prima che questi ultimi effettuino una connessione verso l'esterno. Il server prima della connessione potrebbe richiedere all'utente di effettuare un login. Si potrebbe addirittura arrivare a richiedere un login per ogni sito che desidera visitare.

Proxy SOCKS

Un server SOCKS è molto simile ad una vecchia "switch board", che semplicemente incrocia, attraverso il sistema, i "cavi" della propria connessione con un'altra connessione esterna.

La maggior parte dei server SOCKS funziona solamente con connessioni di tipo TCP e come i firewall filtranti non fornisco l'autenticazione degli utenti. Hanno comunque la possibilità di registrare il sito a cui si è connesso l'utente.

Sistemi anti-intrusione

Il rilevamento delle intrusioni, come suggerisce il nome, è quell'attività volta a scoprire tentativi di intrusione, o di intrusioni già avvenute, nei sistemi di calcolo e di avviare azioni appropriate in risposta agli attacchi.

Per il rilevamento delle intrusioni s'impiegano molte tecniche che si differenziano a seconda del fattore che viene preso in esame per rilevare l'aggressione.

Di seguito alcuni di questi fattori:

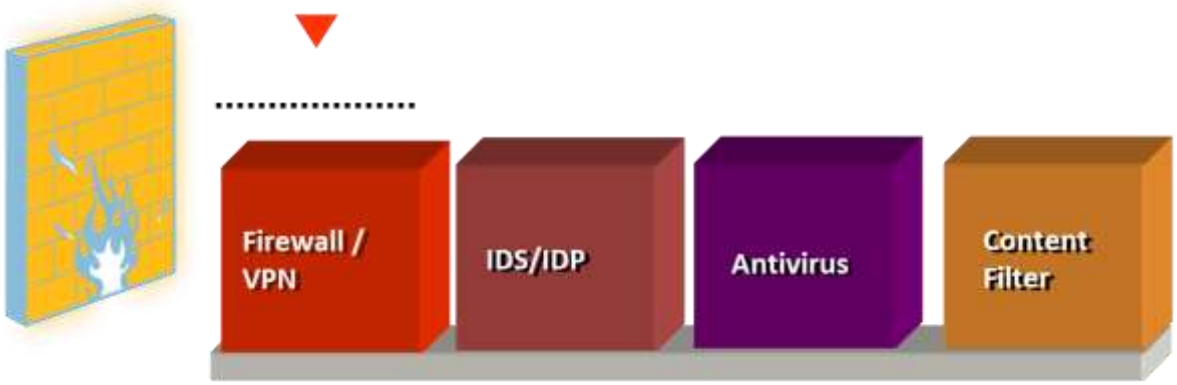
- Fase in cui è avvenuto il rilevamento dell'intrusione: mentre si stava verificando o solo successivamente;
- le informazioni esaminate per scoprire l'attività intrusiva.

Queste potrebbero comprendere comandi per l'interprete impartiti dall'utente, chiamate del sistema da parte dei processi, oltre a intestazioni e contenuto dei pacchetti di rete. Alcune forme d'intrusione si possono rivelare solo attraverso una correlazione delle informazioni acquisite da più di una sorgente.

- L'ampiezza della capacità di risposta.

Alcune semplici forme di risposta consistono nell'informare l'amministratore del sistema della potenziale intrusione oppure nel bloccare in qualche modo la potenziale attività intrusiva, ad esempio arrestando un processo impiegato in un'attività apparentemente intrusiva. Questi gradi di libertà nella progettazione di sistemi impieganti tecniche per il rilevamento delle intrusioni hanno portato a un'ampia gamma di soluzioni che vanno sotto il nome di sistemi di rilevamento delle intrusioni (intrusion-detection systems - IDS).

Esistono anche sistemi che opportunamente istruiti possono identificare a priori e quindi prevenire attacchi informatici. Questi sistemi sono detti "intrusion prevention systems – IPS"



Conclusioni

Gli argomenti trattati nelle precedenti lezioni diventano fondamentali per la verifica della sicurezza dei propri servizi pubblicati sul WEB. Il Man in the Middle trattato durante la prima lezione e la sicurezza della posta elettronica trattata nella seconda lezione, si calano perfettamente in questo ambito.

La nostra esperienza ha evidenziato che portali ritenuti sicuri da test di penetrazione o di vulnerabilità, erano invece attaccabili in quanto semplicemente pubblicati mediante protocolli non sicuri attraverso i quali risultava facile acquisire le credenziali degli utenti connessi al sistema. In altre parole sicuro e protetto il server a livello di configurazione, ma esposto a rischi a livello di infrastruttura.

Quanto trattato nella lezione 5 sugli "Scan Ports" è fondamentale per la verifica della sicurezza dei nostri sistemi. Ci è capitato più volte di riscontrare che i router e i Firewall forniti dai provider sono configurati in modo non propriamente corretto in quanto settati con SNMP abilitato su rete pubblica e accesso non controllato. Un'autentica autostrada d'accesso per un male intenzionato.

Quindi che fare? Il consiglio che possiamo dare è il seguente:

solo un audit mirato consente di avere una fotografia dettagliata dello stato della nostra architettura di rete e delle sue vulnerabilità.

Il Tuo
EterNet Team