-Tabella ARP:Funziona da cache locale ad un nodo.Meccanismo di aggiornamento basato sulla ricezione di un nuovo pacchetto ARP di risposta.Il **TTL** indica quando la entry verrà rimossa dalla ARP table per essere poi rivalicata con il router.
-ARP Poisoning(ARP Spoofing):L'associazione tra MAC address e indirizzo IP destinatario corrispondente viene manipolata,di conseguenza anche le comunicazioni su di un segmento di rete possono esserlo.*Effetti:*l'attacco di tipo ARP Poisoning permette di intercettare e reinviare(eventualmente modificate) le comunicazioni tra nodi della stessa rete locale.*Man in the middle*:una comunicazione che si suppone essere stabilita tra 2 nodi viene invece gestita in maniera nascosta da un terzo nodo.*Criticità:*sono difficili da individuare perché le 2 parti A e B non hanno segnali della presenza di C.Possono avere conseguenze serie perché la comunicazione tra A e B è completamente gestita da C.*Rischio*:Il rischio associato al caso di ARP Poisoning è in generale ridotto poiché vi è un vincolo della presenza fisica sulla stessa rete locale;inoltre nei dispositivi moderni sono stati introdotti dei meccanismi di prevenzione(esempio:ARP table statiche).
-Flag TCP:SYN:richiesta di connessione;ACK:conferma del pacchetto precedente;FYN:intenzione del mittente di terminare la sessione;RST:reset della sessione;PSH:operazione di push,i dati vengono subito inviati al destinatario senza bufferizzarli.URG:dati urgenti vengono inviati con precedenza sugli altri.
-Specifiche TCP:1.Un segmento in arrivo con il flag RST attivo viene sempre scartato senza alcuna risposta. 2.Se una porta è nello stato di closet,se il segmento in arrivo non ha il flag RST attivo allora viene inviato come risposta al mittente un pacchetto con il flag RST attivo.3.Se una porta è nello stato di listen: A. se il segmento in arrivo contiene un ACK allora viene risposto con un RST; B.se il segmento in arrivo contiene un SYN allora viene inviato come risposta al mittente un pacchetto con i flag SYN/ACK attivi. C.se nessuno dei 2 precedenti è vero allora il segmento viene scartato senza risposta.
-Frammentazione IP: ***MTU***(Maximum Trasmission Unit):dimensione massima dei pacchetti ammessi da una rete. Ad esempio se abbiamo un limite di 1500 byte e abbiamo un pacchetto ICMP di 4000 byte dobbiamo suddividerlo,nella prima suddivisione rimangono esattamente il primi 1500 byte del pacchetto da 4000 byte,mentre nei successivi pacchetti suddivisi in testa nei primi 20 byte viene copiato l'IP header.***Identification***:valore identificativo uguale per tutti i frammenti di un pacchetto originario che dovrà essere riassemblato a destinazione.***Flags***:un bit MF per indicare More Fragments settato a 1 per tutti i frammenti tranne l'ultimo che ha il flag a 0.Un secondo bit DF per indicare Don't Fragment cioè per istruire i router che, se fosse necessaria la frammentazione,il datagram va scartato e non frammentato.***Offset***:Rappresenta la posizione relativa dei dati nei diversi frammenti rispetto alla posizione dei dati nel datagram originario.
-Problemi con i frammenti:1. *frammento iniziale mancante*. Il frammento iniziale è l'unico ad avere l'header del livello di trasporto(TCP,UDP,ICMP),quindi potrebbe essere stato bloccatto dalla politica di sicurezza mentre gli altri frammenti non avendo header TCP UDP ICMP superano la verifica. 2. *frammento finale mancante*. Nessuna spiegazione, possibile datagram IP manipolato volutamente.3. *offset ripetuti*.Molti frammenti passano attraverso il firewall e raggiungono l'host di destinazione.Ad esempio un router BSD, riceve i frammenti e li mantiene in cache in attesa di riassemblare il datagram originale; frammento iniziale e frammento finale non arrivano impedendo il riassemblaggio;molti frammenti con stesso FRAG ID continuano ad arrivare,impedendo il timeout del router. Di conseguenza il router BSD non va in timeout → Denial of Service.La capacità di routing del traffico regolare di degrada fino ad annullarsi.
-Scan delle porte:Una informazione necessaria a preparare molte intrusioni consiste nel conoscere lo stato delle porte: Accepted o Open,l'host destinatario genera una risposta che indica che un servizio è in ascolto su quella porta. Denied o Closed,l'accesso all'host è bloccatto oppure non c'è un servizio in ascolto su tale porta. Dropped o Blocked,il tentativo di connessione è stato terminato da qualche componente di rete.
-Obiettivo di uno scan:*Obiettivo predefinito*:lo scan è mirato a uno specifico sito od organizzazione;*Scanning ad ampio spettro*:lo scan viene effettuato su intere classi A o B di indirizzi IP;*Scanning mirato ad un servizio*:lo scan può essere ad ampio spettro ma mirato a verificare le risposte da una porta predefinita.
-TCP scan:E' il metodo più semplice, si tratta solo di cercare di aprire una normale connessione TCP e analizzarne il risultato.Se la connessione ha successo allora la porta dell'host destinatario è open,viceversa è closed.I log dell'host di destinazione mostreranno queste connessioni completate seguite dalla loro interruzione.

-TCP SYN scan:Invia il normale SYN di apertura di una connessione TCP, se riceve il SYN/ACK risponde con un RST.Se riceve il SYN/ACK allora la porta del destinatario è open viceversa è closed.Non tutti i sistemi operativi riportano nei log i casi di connessione half-open(SYN scan).
-TCP FYN,Xmas e Null scan:FYN scan invio di pacchetti isolati con il flag FYN a 1.Xmas scan pacchetti con i flag SYN, URG e PSH a 1(o altre combinazioni).Null scan pacchetti con tutti i flag a 0.Se la porta di destinazione è aperta i pacchetti vengono scartati senza risposta,se la porta è chiusa la risposta è un RST.Alcuni sistemi operativi non rispettano le specifiche del TCP e rispondono con un RST in ogni caso.Spesso non compaiono nei log.
-ACK scan:Invio di pacchetti isolati di ACK.Se la porta è raggiungibile (sia nello stato di closed che di open) è prevista una risposta RST,altrimenti i pacchetti vengono scartati senza risposta.Usato anche in combinazione con altri tipi di scan per verificare il tipo di firewall.
-Statefull o Static Packet Filter: Se usati insieme l'ACK scan e il SYN scan si può dedurre se il FW esegue solo un filtraggio a livello di singolo pacchetto e non mantiene lo stato della sessione.
-UDP scan:Serve per determinare le porte UDP aperte. Viene inviato un pacchetto UDP di 0 byte di dati;se la porta è chiusa viene risposto con un messaggio ICMP unreachable,diversamente si assume che la porta è aperta.
-IDLE scan(di Salvatore Sanfilippo):Tecnica di scan per determinare le porte TCP aperte.Usa indirizzi spoofed.Chi vuole eseguire la scansione sceglie una macchina attiva e raggiungibile;invio di un SYN/ACK per provocare una risposta RST e leggere il valore dell'IP id(header IP);lo scanner crea un pacchetto con SYN attivo e con indirizzo IP sorgente uguale all'indirizzo IP dello zombie e la invia all'host sul quale vuole eseguire una scansione.Il target risponde allo zombie con un RST se la porta è chiusa,con un SYN/ACK se la porta è aperta; si reinvia un SYN/ACK allo zombie per provocare una risposta, se l'IP id è aumentato di 2 unità la porta x del target è aperta,se è aumentato solo di una unità la porta x è chiusa.
-OS Fingerprinting: Tool come nmap e molti altri utilizzano sequenze di pacchetti anomali, oppure pacchetti sequenze note per provocare reazioni dipendenti dalle singole implementazioni dello stack TCP. In questo modo analizzando le risposte riescono a predire con discreta approssimazione il sistema operativo e talvolta la sua specifica versione.
Nmap (sequenza OS fingerprint): 1. Una serie di pacchetti con SYN vengono inviati per analizzare come vengono generati i numeri di sequenza, 2. Un pacchetto NULL (nessun flag) viene inviato ad una porta TCP aperta, 3. Un pacchetto con SYN,FIN,PSH,URG viene inviato ad una
porta TCP aperta, 4. Un pacchetto con ACK viene inviato ad una porta TCP aperta, 5. Un pacchetto con SYN viene inviato ad una porta TCP chiusa, 6. Un pacchetto con ACK viene inviato ad una porta TCP chiusa, 7. Un pacchetto con FIN,PSH,URG viene inviato ad una porta
TCP chiusa, 8. Un pacchetto viene inviato ad una porta UDP chiusa
-Spoofing:Tecnica che consente di presentarsi con l'identità altrui;esistono diverse tecniche di spoofing:*e-mail spoofing*, fare apparire una mail come proveniente da qualcuno diverso dal reale mittente;*web-spoofing*,far apparire un sito web come uno di una diversa organizzazione;*ip spoofing*,generare pacchetti di rete con indirizzo IP diverso da quello assegnato.
-IP spoofing Contromisure:INGRESS FILTERING(filtraggio del traffico in ingresso),nessun pacchetto con IP address interno alla rete può essere ricevuto come proveniente dall'esterno.EGRESS FILTERING,filtraggio del traffico in uscita;nessun pacchetto con IP address non appartenente alla rete può uscire dalla rete stessa.
-Phishing:Combina tecniche di mail spoofing e web spoofing.
-Opzione di source routing:Il protocollo IP permette che il mittente specifichi quale routing dovrà seguire un pacchetto su internet.2 tipologie:*loose source routing*:vengono specificati alcuni indirizzi IP attraverso i quali il pacchetto dovrà passare.Permesso il routing anche su altri indirizzi oltre a quelli specificati.*strict source routing*:il pacchetto dovràè attraversare solo gli indirizzi IP speficati.
-TCP session hijacking:Una sessione attiva tra un client e un server viene dirottata da un intrusore che impersone un client legittimo e prosegue con il server la sessione apparendo il client legittimo.Spesso si accompagna con la necessità di rendere il client legittimo inattivo.*Effetti*:evitare la fase di autenticazione effettuata dal client reale,impersonare l'identità del client e sfruttare i privilegi del client reale o accedere a informazioni riservate.
-Mitnick Attack:L'intrusore invia un SYN con l'IP del client al server vittima.Il server vittima,risponde con un SYN/ACK al client;lì'intrusore fa si che non arrivi al server il reset del client e invia al server un ACK incrementato di 1 con l'IP del client.,cosi l'intrusore riesce ad inviare dei comandi con IP

spoofed.Il problema è che l'intrusore deve conoscere il sequence number senza aver ricevuto il SYN/ACK dal server.
-Categorie Vulnerabilità: Avere una categorizzazione delle vulnerabilità è importante per poter fissare delle priorità nelle contromisure da adottare. Non sempre si puo o si vuole o risulta conveniente adottare contromisure per tutte le vulnerabilità potenziali. Non esiste una metrica standard per misurare la gravità di una vulnerabilità per questo ogni organizzazione ha adottato criteri propri per indicare la gravità associata ad ogni vulnerabilità. Nessuna delle vulnerabilità è causata esclusivamente da problemi delle tecnologie di rete: protocolli TCP/IP, numeri di sequenza ecc..; tutte le vulnerabilità si riferiscono a problemi dei singoli sistemi come: gestione della memoria (i vari casi di overflow), interfacciamento con database (SQL injection), gestione degli input (directory traversal), shell e esecuzione remota di comandi. Molte possono essere sfruttate per accessi non autorizzati via rete; inoltre qualunque genere di sistema presenta vulnerabilità database, sistemi per la sicurezza, semplici utility e sistemi complessi.
-Elementi per classificare una vulnerabilità: Diffusione dei sistemi coinvolti, Tipo di sistema (client/server) e privilegio (root/user); Configurazione standard/default vulnerabile; Criticità/valore dei sistemi coinvolti; Impatto sull'infrastrutture di rete; Grado di difficoltà nello sfruttare la vulnerabilità; Probabilità di attacchi basati sulla vulnerabilità (esistenza di tool e dettagli tecnici).
-Gravità vulnerabilità critica: Sono facili da sfruttare e fanno guadagnare molto all'attaccante. Identificare queste vulnerabilità e indispensabile perchè la probabilità di attacchi è alta e sono gravi i danni che possono essere provocati. Per questi tipi di vulnerabilità occorre adottare immediatamente delle contromisure, anche a scapito delle funzionalità offerte dall'organizzazione.
-Gravità vulnerabilità alta: E' meno facile da sfruttare ma ha ancora probabili target per gli attaccanti. Occorre analizzare con attenzione in ogni contesto specifico per determinare quanto difficile può essere per un attaccante utilizzare tali vulnerabilità e qual è l'impatto che possono avere. Per questo tipo di vulnerabilità se non si adottano immediate contromisure, occore comunque un monitoraggio costante per verificare l'evoluzione, nonché un piano di intervento pronto per essere adoperato.
-Gravità vulnerabilità moderata: Sono complesse da sfruttare e/o di impatto non grave. E' indispensabile verificare caso per caso l'effettivo impatto e difficoltà. Inoltre è indispensabile effettuare un'analisi costi/benefici dei possibili interventi; esisteranno diverse contromisure, occorre valutare quale sia la più conveniente rispetto al rischio che si stima l'organizzazione corra. Sono da evitare reazioni non ponderate e impulsive.
-Gravità vulnerabilità bassa: E' molto difficile da sfruttare e/o di impatto ridotto. Non bisogna ignorarle a priori perche analizzando il contesto specifico potrebbero rivelarsi di categoria superiore. Sono da evitare reazioni impulsive, bisogna analizzare quale attività di gestione/monitoraggio sia adeguato adottare; inoltre è da evitare contromisure che non siano state attentamente vagliate rispetto i loro costi espliciti e impliciti.
-Finestra temporale di esposizione di un sistema: Il tempo nel quale un sistema può risultare vittima di attacchi informatici a causa di una vulnerabilità dipende sia da fattori indipendenti che dipendenti dalla gestione del sistema stesso.
-Cicli di vita di una vulnerabilità: -Creazione, un errore viene introdotto nel codice nel corso dello sviluppo di un sistema, un servizio, una applicazione. –Scoperta, qualcuno scopre l'erroere presente nel codice e intuisce che questo ha conseguenze sulla sicurezza; solo da questa fase in poi si parla di vulnerabilità anziché di errore nel codice. –Condivisione/Automatizzazione, la conoscenza di tale vulnerabilità viene fatta prima circolare in ambito ristretto poi si diffonde grazie anche allo sviluppo di tool automatici che n fanno uso. –Pubblicazione Patch/Upgrade, in questa fase il produttore del sistema corregge l'errore emettendo una patch o una nuova versione del codice. La presenza di tale vulnerabilità, insieme alla presenza della patch disponibile viene resa pubblica.
-Criticità: Tutti i sistemi possono essere soggetti ad una finestra di esposizione anche se gestiti al meglio, la scoperta di nuove vulnerabilità è impredicibile. La conoscenza della vulnerabilità ovvero l'individuazione di siti vulnerabili e disponibilità di tool automatici circola molto velocemente grazie all'ampia disponibilità di informazioni su chat, mailing list, magazine ecc.. . Le patch invece rappresentano spesso una soluzione inefficace a causa, della scarsa consapevolezza di molti sistemisti, della frequenza di emissione troppo elevata e spesso a causa del malfunzionamento o di nuovi problemi.
-Script Kiddies: Successivamente alle prime intrusioni, compiute da esperti, la tecnica per realizzarle viene automatizzata tramite la scrittura di script, e la descrizione delle procedure; inoltre la disponibilità di exploit (tool automatici) permette di sfruttare con successo vulnerabilità nei sistemi anche a persone dotate di scarse competenza tecniche, aumentando drasticamente il numero dei potenziali attaccanti.

-Trojan Horse: E' un programma apparentemente legittimo ma che nasconde funzionalità non dichiarate; a differenza dei virus, non possiede capacità di autoreplicarsi o di infettare altri file e programmi. Spesso è presente in utility, giochi e programmi freeware. Inoltre si sono verificati casi di trojan inseriti in pacchetti software di ampia diffusione a insaputa dei produttori.
-Tipologie di trojan horse: -Remote access trojan, forniscono all'attaccante il controllo remoto attraverso una backdoor; -Password sending trojan, intercettano password locali e le comunicano all'attaccante; -Keylogging trojan, registrano quanto digitato sulla tastiera e lo comunicano all'attaccante; -Destructive trojan, cancellano file critici per creare malfunzionamento; -Denial of service attack trojan, installano tool per DDoS e attendono comandi dall'attaccante; -Proxy/Wingate trojans, installano un proxy/Wingate per consentire connessioni difficili da tracciare; -FTP trojan, abilitano un server FTP; -Detection software killers, cercano di rimuovere o disabilitare software di protezione lacale.
-Backdoor: E' un accesso non controllato ad un computer attivato in maniera non autorizzato. Spesso le funzionalità nascoste dei trojan horse sono backdoor; un'esempio tipico è l'attivazione di servizi di rete su porte non convenzionali per consentire l'accesso remoto e il facile controllo di una macchina.
-Internet Worm: Sono software che automatizzano l'intero processo di una intrusione. Possiedono generalmente le seguenti caratteristiche: -capacità di scannino e sniffing alla ricerca di nuovi target; -tecniche di intrusione automatizzate (exploit); -una interfaccia per ricevere comandi; -delle proprie capacità di comunicazione e propagazione attraverso internet o reti locali. Gli internet worm rappresentano attualmente la maggiore minaccia per numero di intrusioni.
-Internet Worm scanning e sniffing: Lo scanning solitamente è mirato alla ricerca di host con servizi corrispondenti alle vulnerabilità per le quali possiedono gli script che ne automatizzano l'attacco. Li sniffing intercettano traffico dalla rete alla ricerca di informazioni tipo username e password; e registrano gli input della tastiera e successivamente inviano quanto registrato al controllore.
-Effetti di un firewall: Per tutte le sottoreti protette da un firewall si possono definire politiche di accesso inoltre solo i componenti esterni al firewall sono direttamente accedibili. Un'altra caratteristica che distingue la presenza di un firewall è la gestione delle connessioni tra le diverse interfacce del firewall; ad esempio si consentono connessioni da Internet alla rete DMZ, ma non da internet verso la reta interna. Il firewall realizza anche una separazione in zone aventi diverso grado di sicurezza nella architettura di rete.
-Static Packet Filtering: Il controllo del traffico è basato unicamente sulle informazioni contenuti negli header dei singoli pacchetti. I valori dei parametri degli header dei pacchetti vengono confrontati con le regole definite in una ACL (Access Control List) e ammessi o scartati secondo il risultato del confronto. Ogni pacchetto viene quindi esaminato singolarmente dai pacchetti precedentemente ricevuti e da quelli successivi. Lo Static packet filtering è la prima tecnologia adottata per i sistemi di firewall, nei sistemi odierni è stata superata dalla tecnologia di tipo stateful ma continua a essere usata nei sistemi di fascia bassa e nei router per la sua semplicità e per lo scarso impatto sulle performance dei sistemi.
-Filtraggio SPF, protocolli connectionless: I protocolli connectionless (UDP,ICMP) possono essere sia unidirezionali che bidirezionali, in funzione delle diverse applicazioni ad esempio ping (ICMP) e DNS query (UDP) bidirezionali mentre source quench (ICMP) e heartbeat (UDP) unidirezionali.
-Access control list (ACL): Le ACL definiscono le regole pr il filtraggio statico dei pacchetti in transito. La semantica è ACCEPT/DENY. Il criterio di filtraggio è TOP-DOWN ovvero: -la prima regola che viene verificata produce la decisione sul pacchetto; - il test del pacchetto continua fino a che una regola corrisponde alle caratteristiche del pacchetto oppure fino a che la lista di regole termina; -di norma esiste una regola di DEFAULT.
-Tipi di ACL: Secondo gli standard Cisco si hanno: le Standard ACL, che sono numerate tra 0 e 99 e filtrano solo gli indirizzi IP sorgente; e le Extended ACL che sono numerate tra 100 e 199 e filtrano indirizzi IP sorgente, destinatario, protocollo, porte UDP e TCP e tipo o codice messaggiICMP.
-Wild Card: Determina la parte dell'indirizzo IP da verificare e quelle da ignorare. E' simile alla netmask ma ha una semantica dei valori invertita ovvero: valore binario 1 per i bit dell'indirizzo IP che non deve essere verificato e valore binario 0 per i bit dell'indirizzo IP che deve essere verificato.
-Keyword host: Si usa quando si indica un indirizzo IP unico. E' analogo alla *wild card* 0.0.0.0.
-Extended ACL (formato): Il formato è "Access-list Numero Azione Tipo Sorgente [wild card] Opzioni Destinazione [wild card] [log]. *-Numero:* da 100 a 199 per ACL Extended. *–Azione:* permit/deny. *–Sorgente:* indirizzo IP sorgente. *–Destinazione:* Indirizzo IP destinazione. *–Type:* IP,

UDP o TCP. –*Opzioni*: Porte TCP/UDP, Tipo/Codice ICMP, operatori speciali. –*Log:* è opzionale. Scrive un messaggio in un log per ogni pacchetto verificato da una regola.
-Established (operatore): Permette di filtrare il traffico in ingresso verificando se i flag RST o ACK sono attivi; in questo modo si permette l'ingresso di tali pacchetti solo in presenza di una sessione TCP già stabilita, evitando attività di scanning.
-Least Privilegi (regola generale): Dato un insieme di specifiche, è un errore definire una politica più lasca dello stretto necessario. Ovvero, compatibilmente con le specifiche relative alla fornitura dei servizi, la politica di un firewall deve essere la più stringente possibile. *–Considerazione fondamentale sull'uso di Firewall e Politiche:* La protezione che i firewall forniscono è tanto efficace quanto lo è la politica di sicurezza per implementare la quale essi sono configurati.
-Stateful Filtering: Il *controllo del traffico* avviene tramite una ***connection table***, che mantiene lo stato delle connessioni attive ed informazioni degli header di livello 3 e 4 dei singoli pacchetti. La connection table contiene: IP e porta sorgente, IP e porta destinataria, e Timeout (es.18/50). L'*esame dei pacchetti* avviene sia singolarmente per ogni pacchetto che in relazione ai pacchetti precedentemente ricevuti e appartenenti alla stessa sessione. *-Principio di funzionamento:* Se il server/porta è nello stato di "Listen" si deve controllare l'ACL. Se il server/porta è invece nello stato di "Established" i pacchetti possono essere autorizzati verificando le informazioni della connection table. *–Stati di una Sessione TCP e Stateful Filtering:* -Ricezione di un SYN→Verifica dell'ACL (come per Racket Filter). –Se connessione non autorizzata→Deny. –Se connessione autorizzata→Accept e scrittura di una entry nella connection table. –Ricezione di pacchetti successivi→Verifica della connection table. *–Politica:* Definizione delle sole regole relative all'apertura delle connessioni TCP (pacchetto SYN). Non serve specificare le regole per le risposte come nel Racket Filter (gestite automaticamente controllando la connection table). *–Stateful Filtering e UDP:* L'UDP è un protocollo connectionless, cioè che non possiede informazioni di stato. Viene gestito uno pseudo-stato correlando semplicemente indirizzi IP e porte (sorgente/destinazione); inoltre non ha un protocollo di terminazione, in quanto viene settato un time-out predefinito. Non si può definire se una connessione tramite il protocollo UDP abbia o meno una *risposta* dal server al client, in quanto (a differenza del TCP), dipende dalla specifica applicazione. *–Stateful Filtering e Applicazioni:* Il firewall deve interpretare il protocollo applicativo (es. riconoscere il comando PORT). Ciò penalizza pesantemente le performance; per questo spesso è implementato in maniera semplificata, ad esempio con l'interpretazione soltanto di un insieme limitato di protocolli standard. Se non ha la funzione di interpretare la semantica dello scambio applicativo, può essere facilmente bypassato con dei tunnel applicativi, e spesso i moduli per questo tipo di filtraggio applicativo, sono offerti come dei plug-ins addizionali. *-Punti di attenzione dello Stateful Filtering:* Protezione migliore rispetto al caso Static Packet Filtering; Definizione più semplice della politica; Utilizzato in tutti i firewall moderni; Impatta pesantemente sulle performance del router/firewall (quindi necessita di sistemi dedicati); Limitazione principale: scarso o nullo supporto per il filtraggio applicativo.
-Deep Packet Inspection: Miglioramento della tecnologia di Stateful Firewall con funzionalità di *filtraggio applicativo*. La terminologia non è ancora consolidata, spesso è usata a sproposito per motivi puramente commerciali. Il Deep Packet Inspection effettua quindi un'analisi dei contenuti applicativi, e spesso viene implementato sulla base di *pattern di stringhe* specifiche per Internet worm (simile a quanto fatto negli antivirus) che vengono verificate rispetto al contenuto di una sessione applicativa. Solo i pochi produttori di sistemi di gamma alta implementano queste funzionalità significative di Deep Packet Inspection.
-Proxy: Una tecnica di proxy serve per introdurre un componente che media le comunicazioni tra altri due componenti; un proxy infatti disaccoppia la comunicazione tra due componenti, rendendola indiretta. Un proxy agisce sia da client (rispetto al server originale) che da server (rispetto al client originale). TIPI COMUNI DI PROXY: *-Web proxy:* cache di pagine web. *–Anonymizing Proxy:* Anonimizzazione di connessioni web. *–Reverse Proxy:* Garantiscono l'accesso da utenti esterni a risorse interne. Il funzionamento di un Reverse Proxy è il seguente: 1.Connessione da utente esterno verso il Web Server. 2.Redirezione della connessione verso il Reverse Proxy. 3.Autenticazione, verifica, filtraggio, ecc. 4. Inoltro verso il Web Server. *–Proxy Firewall:* Mediano connessioni applicative e gestiscono aspetti di sicurezza dei protocolli. Il Proxy Firewall può essere usato per analizzare i dati delle applicazioni perché opera a livello applicativo. Le sue performance sono potenzialmente molto critiche, e vi è un'analisi migliore del traffico applicativo rispetto ad uno stateful firewall. Esistono soprattutto software di proxy che supportano alcune delle applicazioni più comuni. Dopo essere stato

soppiantato dagli Stateful Firewall, le tecniche di proxy firewall stanno riemergendo per contrastare le vulnerabilità applicative; per questo molto spesso sono anche chiamati *plug-ins* o moduli per *protocol decoding*.

-FTP Bounce Attack: Il comando PORT di FTP ha la seguente sintassi: "PORT h1,h2,h3,h4,p1,p2", dove (h1,h2,h3,h4) rappresentano gli ottetti dell'indirizzo IP del server FTP, mentre (256*p1+p2) restituisce la porta sulla quale il client riceverà la connessione dal server. (es. PORT 159,149,10,5,4,1 → IP:159.149.10.5 – Porta:1025). Supponiamo che siano ammesse connessioni da Internet verso l'FTP Server e verso il Web Server, e che il Telnet Server sia accedibile solo dall'interno della rete. L'attacco avviene in questo modo: l'Attacker si connette all'FTP server (supponendo che l'FTP server accetti connessioni anonime); invia il comando "PORT 159,149,10,8,0,23", con il quale si impone all'FTP server che il successivo trasferimento di file dovrà essere fatto verso l'indirizzo 159.149.10.8, porta 23/tcp (il telnet server); invia il comando RETR, che causa l'apertura di una connessione da parte dell'FTP server verso il telnet server; in questo modo la connessione perimetrale del telnet server è stata bypassata. Uno Stateful Firewall non intercetterebbe questo tentativo di intrusione, mentre un FTP Proxy potrebbe riconoscere che c'è un uso improprio del protocollo e terminare la connessione. Esistono molte varianti, ad esempio per bypassare filtri su download, oltre a forzare l'upload, ma in realtà il problema (che risale al '97) è stato risolto con successivi upgrade degli FTP server che ora impediscono l'FTP Bounce.

-NAT (Network Address Translation): Consente di convertire gli indirizzi IP nel passaggio tra due interfacce del firewall. Tipicamente il NAT viene usato per sfruttare le classi di indirizzi IP riservate e non instradabili (172.16, 10. e 192.168). Non può però essere considerato propriamente una soluzione per la sicurezza della rete aziendale, ma una tecnica di gestione della rete, con la caratteristica di fornire un beneficio rilevante: maschera gli indirizzi effettivamente utilizzati all'interno della rete. TIPOLOGIE DI NAT: *-NAT Statico:* Indirizzi IP interni vengono mappati staticamente in indirizzi IP pubblici. L'associazione è predefinita e fissa. *–NAT Dinamico:* L'associazione tra indirizzo IP interno e indirizzo IP pubblico avviene dinamicamente a run-time. *–PAT (Port Address Translation):* L'associazione tra connessione interna (Host→Proxy) e connessione esterna (Proxy→Internet) avviene modificando la porta sorgente.

-Risorse da proteggere: Le risorse spesso sono rappresentate da *informazioni* (carte di credito dei clienti, progetti di nuovi prodotti, informazioni finanziarie, ecc.); altrettanto frequentemente, le risorse sono *servizi erogati* (e-business, finanziari, di gestione, ecc.). Tutte le risorse devono essere identificate con precisione unitamente ai sistemi che le gestiscono e alle modalità di accesso. Tra i *sistemi di gestione* delle risorse è possibile distinguere: *-Server:* Ogni server deve essere individuato con precisione insieme a tutti i servizi applicativi forniti. Nel caso di applicazioni multilivello e distribuite, è necessario comprendere con esattezza il ruolo applicativo e le funzionalità di ogni server, nonché tutte le modalità di comunicazione con altri sistemi. *–Workstation:* E' indispensabile innanzitutto un livello di protezione locale (antivirus, personal firewall), che non intralci lo svolgimento delle mansioni (cioè le soluzioni di sicurezza non possono essere troppo intrusive). Molto importante è identificare e adottare misure più stringenti (aziendali, hardening, connessioni protette) per le workstation che mantengono dati aziendali critici; di vitale importanza è inoltre adottare un'autenticazione forte, connessioni protette, e policy aziendali per le workstation che accedono a sistemi critici. *–Apparati di rete:* La configurazione degli apparati di rete deve essere documentata e mantenuta sempre aggiornata; devono inoltre essere chiaramente individuati i ruoli dei singoli apparati e tutte le connessioni fornite. In caso di interconnessioni con terze parti (fornitori, clienti, partner), il grado di sicurezza e di fiducia dei partner esterni deve essere valutato; occorrono inoltre policy aziendali e procedure di controllo specifiche per l'uso di connessioni via modem o wireless. *–Altri dispositivi:* L'uso di connessioni IP si sta diffondendo a molti dispositivi che fino a poco tempo fa non ne facevano uso (ad esempio, le stampanti connessi in rete hanno spesso servizi di gestione come FTP, Telnet o SNMP configurati con password di default. Oppure, un altro esempio può essere il VoIP e l'uso di centralini IP).

-Da chi/cosa proteggersi: La percezione del chi/cosa rappresenta la principale minaccia per la sicurezza; tale percezione cambia periodicamente a fronte di eventi esterni: spesso l'ultima e più recente fonte di attacchi cattura l'attenzione generale e condiziona le scelte del momento; trattasi di un comportamento tipico dei fenomeni di moda; una buona gestione, ovviamente, non si basa sulle mode del momento; tutte le possibili fonti di rischio devono essere ugualmente prese in considerazione e valutate; ogni caso aziendale rappresenta uno scenario a sé stante. *Categorie generali:* Attaccanti interni determinati; Attaccanti esterni determinati; Script Kiddies; Software automatici.

-Esigenze di business e funzionali: -*Costi:* Hardware e software iniziale, personale per la progettazione e il deploy, supporto e aggiornamento software annuali, manutenzione e assistenza dei componenti. – *Servizi e funzionalità:* Tutti i servizi indispensabili per il business aziendale devono essere garantiti al meglio. Le misure di sicurezza devono avere un impatto limitato e non riduttivo delle funzionalità. – *Performance (affidabilità ed efficienza):* Le misure di sicurezza hanno un inevitabile impatto sulle performance della rete. Devono essere evitati colli di bottiglia dimensionando opportunamente le soluzioni. Ad esempio, componenti in cascata degradano maggiormente le performance rispetto un singolo componente o componenti in parallelo. Meccanismi crittografici e filtraggi applicativi sono molto pesanti computazionalmente e riducono molto il throughput dei sistemi. Anche i meccanismi di jogging possono impattare negativamente sulle performance. –*Fault tolerance (prevenire i malfunzionamenti):* ..*Ridondanza intra-sistema:* componenti e servizi all'interno dello stesso sistema possono essere resi ridondanti. ..*Ridondanza intra-sito:* Componenti ridondanti nell'architettura, spesso operati in cluster: active-active o active-passive. ..*Ridondanza di firewall:* Molti firewall possono essere configurati in cluster di più nodi: alcuni offrono solo failover, altri anche load balancing.
-Boarder router: Può svolgere filtraggi semplici e statici: ingess e egress filtering. Può essere configurato in maniera sicura (es. non ammettere source routing, rifiutare ping, ecc.).
-Firewall: Può essere dotato di diverse interfacce di rete: rappresenta un single point of failure per l'intera rete se non ridondato; la configurazione e la gestione possono risultare attività complesse.
-Architettura con Firewall Multipli: *Punti di forza:* -Prodotti diversi compensano le rispettive vulnerabilità; -Rafforzamento della separazione in zone a diverso grado di sicurezza; -Migliore protezione da attacchi interni; -Controllo più dettagliato degli accessi alle risorse. *Punti di debolezza:* -Costi più elevati: hardware, software, assistenza, personale; -Gestione di più componenti differenti.
-Architettura con Firewall in Cascata: Vi è una forte separazione delle diverse zone della rete. E' utile un numero limitato di livelli come separazione in macro-zone della rete; la gestione è complessa, anche perché i firewall hanno policy dipendenti le une dalle altre.
-Architettura con Firewall in Parallelo: Le zone della rete sono fortemente separate, con una possibile tecnologia di filtraggio differente per le diverse zone. Vi è indipendenza delle politiche dei firewall, e le risorse non sono protette da diversi livelli di soluzioni di sicurezza, ma sono equidistanti dalla zona a maggior rischio.
-Zona di sicurezza: Consiste in un raggruppamento logico di risorse – sistemi, reti o processi – per le quali si accetta un uguale livello di rischio. Per la definizione della zona di sicurezza occorre identificare il livello di rischio accettabile delle risorse (viene stabilito sulla base di ciò che conviene all'azienda ed in base alla natura/ruolo delle risorse) e i raggruppamenti omogenei di risorse. Il concetto di zona di sicurezza applicato ad un'architettura di rete è più generale e può essere adottato, ad esempio, localmente, nell'hardening di un server. Infatti, alternative all'uso di server dedicati a singole applicazioni, sono ad esempio: virtualizzazioni di server, attraverso l'uso di macchine virtuali (es. VMware) con cui si possono definire ambienti indipendenti e isolati, e "chroot", tool di linux che permette di definire una root virtuale per un insieme di processi, in maniera tale da impedire l'accesso all'intero file system: bisogna però fare molta attenzione alle vulnerabilità.
-Zone di sicurezza multiple: L'idea di base è di partizionare la rete aziendale in sottoreti, ciascuna delle quali corrispondente ad una zona di sicurezza, e regolare attraverso politiche di firewalling la comunicazione tra di esse. In aggiunta al controllo delle comunicazioni, la suddivisione in sottoreti permette di avere *domini di broadcast* (insieme di host che ricevono pacchetti di broadcast di una rete) separati. Limitare il dominio di broadcast permette di ridurre le (molte) vulnerabilità associato all'uso del broadcast. Il partizonamento di sottoreti corrispondenti a zone di sicurezza deve avvenire a fronte di un'analisi della rete aziendale. Rispecchierà l'utilizzo e la struttura della rete stesse e dell'organizzazione. Potrà avere una struttura *piatta* (zone di sicurezza non innestate) o *gerarchica* (zone di sicurezza innestate). Tipicamente si opera una prima suddivisione tra risorse preposte a fornire o supportare servizi per utenti esterni alla rete aziendale, e risorse per servizi dedicati all'operatività interna dell'azienda. All'interno di ogni macro-zona (servizi pubblici, servizi interni), l'ulteriore suddivisione può seguire criteri: *funzionali*: risorse che svolgono funzioni simili; *organizzativi*: risorse allocate in settori/dipartimenti aziendali; *geografici*: risorse localizzate vicine. Tipiche suddivisioni sono tra server aziendali e workstation, server applicativi e database, sottoreti di produzione e sottoreti di test/collaudo, sottoreti per l'amministrazione, produzione, R&D, commerciale, ecc. Spesso di mantengono separate le risorse di gestione della rete (macchine degli amministratori, log server, tool di management).

-Sdoppiamento di servizi: La suddivisione tra zone di sicurezza per servizi pubblici e per servizi interni coninvolge servizi che sono utilizzati da entrambe le zone. Caso tipico sono posta elettronica e DNS. Occorre scegliere se continuare a fornirli con un unico componente, o se sdoppiarli in due componenti da sincronizzare.
-Mail Server e Mail Relay: *Motivi per lo sdoppiamento del server di posta:* -Avere due componenti (uno nella zona pubblica, uno nella zona privata) permette di scegliere software differenti; -Ognuno dei due componenti può essere configurato in maniera appropriata e specifica. -Il componente nella zona pubblica agisce da semplice relay, quindi le email rimangono nella zona più protetta. –Il mail relay può agire da gateway antivirus e antispam. Il mail relay riceve la posta sia dall'esterno che dall'interno della rete e la invia nuovamente. La posta in ingresso viene indirizzata al mail server della rete interna.
-DNS Esterno: Serve richieste di utenti esterni alla rete aziendale e fornisce le informazioni pubbliche (es. da nslookup). Riceve query da utenti esterni per informazioni riguardo host pubblicamente accessibili della rete aziendale, incluso l'MX server (il Mail Relay). Il DNS Esterno mantiene soltanto le informazioni pubbliche.
-DNS Interno: Serve gli utenti e i servizi della rete interna. Riceve query da utenti interni per informazioni su host sia della intranet aziendale che di Internet. Per le query che il DNS Interno non è in grado di risolvere può sia contattare il DNS Esterno che DNS predefiniti (es. DNS dell'ISP). Queste si chiamano *query ricorsive*. A differenza del DNS Esterno, l'Interno mantiene tutte le informazioni della intranet.
-Separazione dei DNS (motivi): -Separazione fisica delle informazioni riguardanti servizi pubblici da quelli riguardanti servizi della intranet; -Assegnazione a diverse zone di sicurezza per la protezione delle informazioni; -Isolamento del DNS pubblico della rete interna nel caso di compromissione.
-DNS Spoofing: I DNS sono da sempre uno dei target preferiti per intrusioni. Tra i motivi la natura pubblica del servizio, che se compromesso, può essere usato come testa di ponte per estendere l'intrusione a componenti interni (così come per qualunque altro servizio pubblico). Altro motivo, specifico dei DNS, è dovuto alla possibilità di corrompere le informazioni fornite dal servizio. Queste tipologie di attacchi sono denominati DNS Spoofing e si compongono di diverse varianti, tra cui: DNS Cache Poisoning e DNS ID Spoofing.
-DNS Cache Poisoning: Un DNS server conserva in maniera permanente solo i record delle macchine del dominio sul quale è autoritativo. Per ogni altro nome deve generare una query ad altri DNS. Le risposte da altri DNS vengono conservate in una cache per un certo tempo. Le informazioni mantenute in cache possono essere soggette a compromissione (*cache poisoning*). Il *principio di funzionamento* dell'attacco è di configurare un DNS esterno in maniera scorretta, tale da tentare un *zone transfer* (trasferimento di tutte le informazioni di dominio) verso il DNS da compromettere. *Esempio:* L'attacker configura un DNS per un proprio dominio (es. www.attacker.org) contenente associazioni fasulle (es. www.abc.it → <IP attacker>). L'attacker invia una DNS query al DNS server vittima chiedendo di risolvere www.attacker.org. Il DNS server vittima, a sua volta, contatterà il DNS autoritativo per il dominio attacker.org, ovvero il DNS dell'attacker (ns.attacker.org). Il DNS dell'attacker (ns.attacker.org) risolve la query e nella risposta restituisce non solo l'IP richiesto, ma anche l'associazione fasulla (es. www.abc.it → <IP attacker>). Il DNS server vittima ora può rispondere all'attacker ma contemporaneamente memorizza in cache le associazioni ottenute, comprese quella fasulla. Il DNS server vittima, fino a che la cache non viene aggiornata, restituirà un'associazione fasulla a tutti i client che lo interrogheranno. *Contromisure:* Questa è una tecnica molto comune, evitabile semplicemente configurando i DNS a non accettare alcun zone transfer da DNS che non siano autenticati.
-DNS ID Spoofing: Un client quando esegue una DNS query genera anche un identificativo pseudo-casuale che il DNS server copierà nella risposta. La comunicazione avviene via UDP, mentre TCP si usa solo per zone transfer. Il problema può risiedere quindi in un attacco di tipo man-in-the-middle. L'attacker è tra utente e DNS server ed è in grado di sniffare la DNS query, leggendo l'ID. L'attacker può quindi facilmente creare un pacchetto UDP con una risposta DNS, contenente l'ID corrotto e una falsa associazione. *–Limitazioni:* La risposta dell'attacker deve giungere al client prima di quella del DNS server. L'attacker deve essere in grado di sniffare la query DNS. L'attacco è possibile a causa dell'assenza di autenticazione del DNS server (l'indirizzo IP usato dall'attacker sarà spoofed), tuttavia per il suo successo ci sono forti limitazioni fisiche.
-IDS (Intrusion Detection System): E' un dispositivo software/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. Gli IDS vengono utilizzati per rilevare tutti gli attacchi alle reti informatiche e ai computer. Questi attacchi includono gli attacchi alle reti informatiche tramite lo sfruttamento di un servizio vulnerabile, attacchi attraverso l'invio di dati malformati e applicazioni malevole, tentativi di accesso agli host tramite innalzamento illecito dei privilegi degli utenti, accessi non autorizzati a computer e file, e i classici programmi malevoli come virus, trojan e worm. Esistono 2 tecnlogie di IDS: Misure e Anomaly.

-Misuse e Anomaly detection system: Conosciuto anche come signature based intrusion detection system identifica le intrusioni ricercando pattern nel traffico di rete o nei dati generati dalle applicazioni. Questa tipologia di applicazioni sono in grado di individuare solo attacchi conosciuti e memorizzati nel loro database. Questa tipologia di analisi dei dati è incapace di individuare violazioni nuove o mutazioni di violazioni già conosciute. Basta modificare anche superficialmente una violazione nota per ingannare questo sistema di analisi. Per ovviare al problema delle mutazioni sono nati gli anomaly based intrusion detection system. Questi sistemi analizzano il funzionamento del sistema alla ricerca di anomalie. Le anomalie vengono analizzate e il sistema cerca di definire se sono pericolose per l'integrità del sistema.