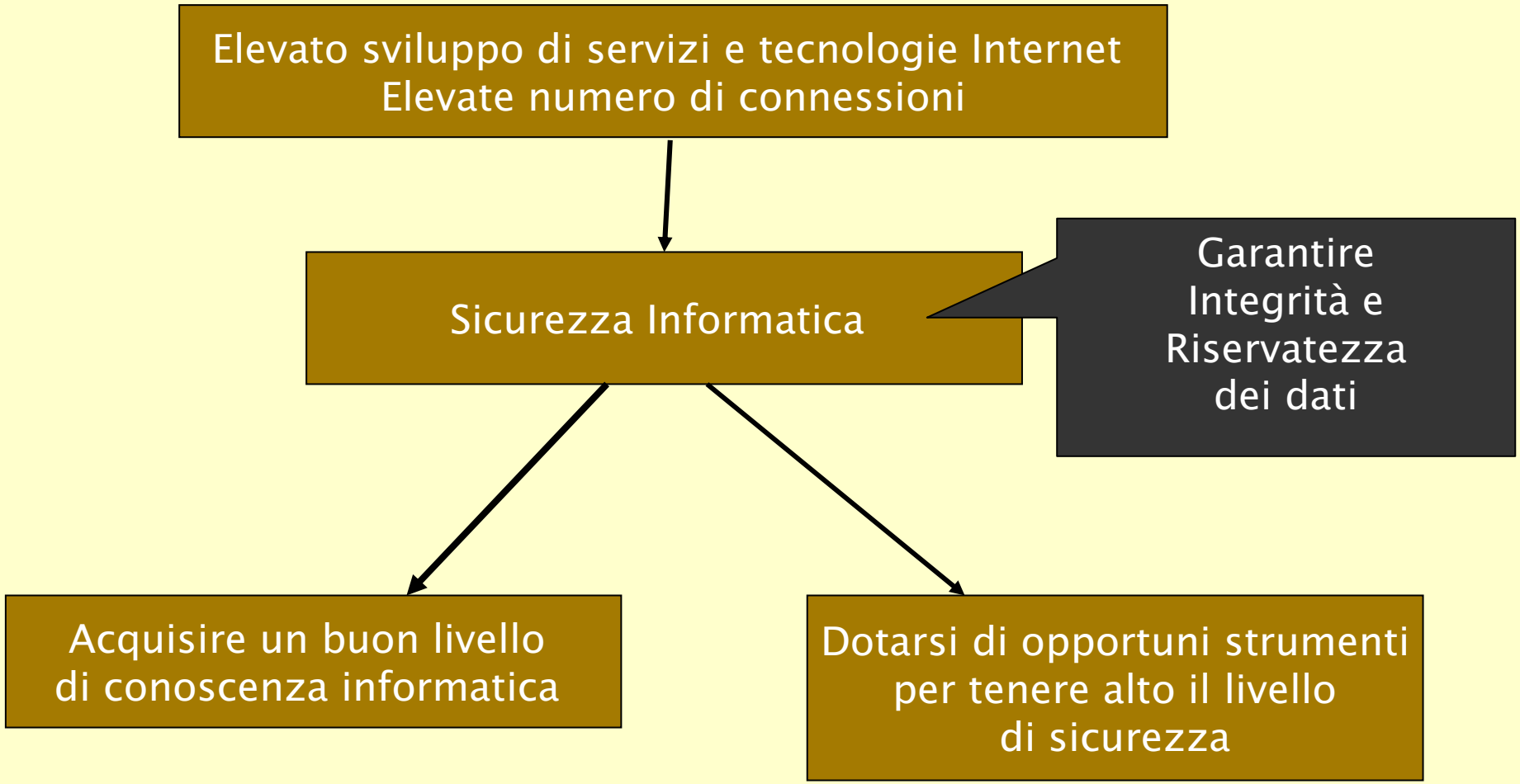
La sicurezza in rete

Sommario

- Il problema della sicurezza in rete: principi di base
- Tipologie di attacchi in rete
  - Intercettazioni
  - Portscan
  - Virus
  - Troiani
  - Spyware
  - Worm
  - Phishing
- Strumenti per la difesa in rete
  - Gestione delle password
  - Antivirus
  - Firewall
  - Antispyware
  - Crittografia
  - IDS

Il problema della sicurezza in rete: principi di base [1]



Il problema della sicurezza in rete: principi di base [2]

Dietro agli attacchi a un sistema si celano motivazioni ben più serie di quello che si può pensare; molti tentativi di violazione di una rete vengono effettuati con scopi diversi:

- spionaggio industriale
- sottrazione di informazioni riservate
- vendetta a scopi personali
- diffamazione pubblica di un'azienda
- guadagno di vantaggi economici

Il problema della sicurezza in rete: principi di base [3]

SICUREZZA indica anche:

"la capacità di salvaguardare riservatezza, integrità e disponibilità dell'informazione (elaborata su computer, memorizzata su supporti di varia natura o trasmessa lungo canali di comunicazione)."

- salvaguardare la riservatezza dell'informazione:
  - Ridurre a livelli accettabili il rischio che un'entità possa accedere ai dati senza esserne autorizzata
- salvaguardare l'integrità dell'informazione:
  - Ridurre il rischio che i dati possano essere cancellati/modificati a seguito di interventi non autorizzate o fenomeni non controllabili e prevedere adeguate procedure di recupero delle informazioni
- salvaguardare la disponibilità dell'informazione:
  - Ridurre il rischio che possa essere impedito alle entità autorizzate l'accesso alle informazioni a seguito di interventi non autorizzate o fenomeni non controllabili

Il problema della sicurezza in rete: principi di base [4]

Aspetti legali

La legge suddivide la tutela in due parti:

1. Da un lato impone l'obbligo di apporre delle misure di sicurezza, anche se minime, al proprio sistema informatico.

   Il codice penale impone l'adozione di misure di sicurezza necessarie ad impedire l'introduzione nel sistema informatico da parte di chi non è autorizzato, per prevenire:

   - Perdita, o distruzione dei dati
   - Ridurre il rischio di accesso non autorizzato
   - Impedire il trattamento dei dati in modo non consentito

Il problema della sicurezza in rete: principi di base [5]

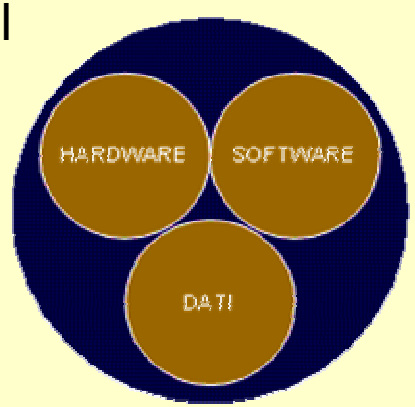
2. Dall'altro la legge si occupa dei vari crimini informatici:

- Delitto di accesso abusivo: fa riferimento all'accesso abusivo ad un sistema informatico protetto da misure di sicurezza anche se minime.
- Abuso di operatore di sistema: fa riferimento all'abuso di un soggetto con tale qualifica, al fine di compiere attività "illegali".
- Delitto di frode informatica: si intende la "ricerca" di modifica, o sfruttamento, dei sistemi informatici al fine di compiere attività criminose.
- Impedimento o turbamento di un sistema informatico: fa riferimento ad abusi che si possono verificare nelle licenze sw, o installazione di particolari programmi, tali da alterare la funzionalità di un sistema a favore dei "produttori" di sw.
- Detenzione e diffusione abusiva di codici di accesso: sanziona l'abusiva acquisizione, in qualunque modo, duplicazione e distribuzione, dei mezzi, o dei codici di accesso ad un sistema informatico.

Il problema della sicurezza in rete: principi di base [6]

Per determinare una politica di sicurezza bisogna anzitutto individuare quali sono le componenti del sistema che devono essere protette.

1. Hardware – le apparecchiature
2. Software – i programmi per il funzionamento del sistema e l'elaborazione
3. Dati – le informazioni gestite dai programmi
4. Supporti di memorizzazione – possono contenere sw e dati (anche backup)
5. Reti – permettono l'interconnessione di vari sistemi e quindi lo scambio di informazioni
6. Accessi – la possibilità che viene data ai soggetti di accedere alle risorse
7. Individui chiave – fa riferimento agli amministratori di sistema, ed eventuali operatori specializzati



Il problema della sicurezza in rete: principi di base [7]

Da chi proteggersi

Per adottare le opportune misure di sicurezza bisogna sapere da chi proteggersi, possiamo fare due distinzioni.

La prima:

1. Hacker: colui che entra nei sistemi altrui per divertimento, studio, curiosità o semplicemente per dimostrare di essere in grado di farlo. Nella maggior parte dei casi l'hacker non causa danni al sistema vittima.
2. Cracker: è colui che viola i sistemi informatici con l'intento ben preciso di provocare un danno.

La seconda:

1. Outsiders: sono coloro che operano dall'esterno del network che intendono attaccare.
2. Insiders: sono coloro che sono autorizzati all'uso della rete e che cercano di abusarne.

Il problema della sicurezza in rete: principi di base [8]

INTERRUZIONE

Un bene viene tolto dal sistema o non è più disponibile o è inutilizzabile.

INTERCETTAMENTO

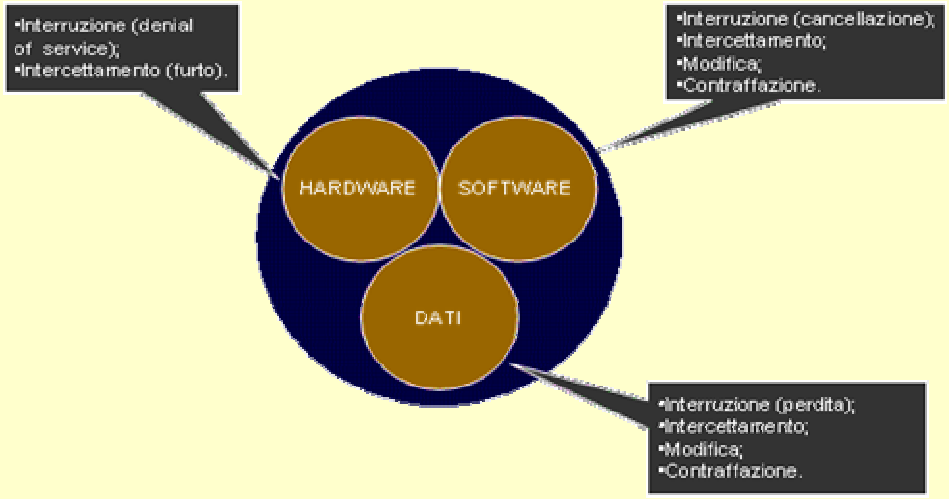
Un'entità (un utente, un programma, un sistema informatico) non autorizzata ottiene l'accesso ad un bene.

MODIFICA

Un'entità (un utente, un programma, un sistema informatico) non autorizzata ottiene l'accesso ad un bene e lo manomette.

CONTRAFFAZIONE

Un'entità (un utente, un programma, un sistema informatico) non autorizzata potrebbe costruire degli oggetti contraffatti all'interno del sistema informatico.



Tipologie di attacchi [1]

Dopo aver individuato le minacce, bisogna capire quali siano i possibili attacchi a cui il sistema può essere sottoposto per adottare le relative misure di sicurezza. Vi sono diverse tipologie di attacco che possono essere così classificate:

- Acquisizione di informazioni: è un insieme di azioni che anticipano un attacco.
- Accesso non autorizzato: un intruso ottiene l'accesso ad una rete, o ad un computer, pur non avendone l'autorizzazione, ottenendo informazioni riservate, o provocando danni di vario genere al sistema.
- Accesso/modifica/cancellazione delle informazioni.
- Denial of Service: l'intruso rende un sistema, un servizio,o una rete non disponibile esaurendone le risorse di rete (banda), connessioni TCP (Syn Floods), o spazio disco (effettuando upload di dati).

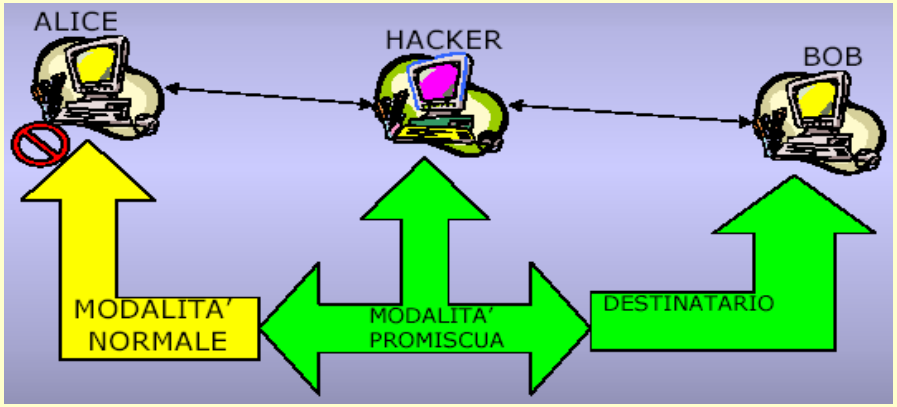
Tipologie di attacchi [2]

Gli attacchi possono essere realizzati seguendo diverse tecniche, quali ad esempio:

- Intercettazioni
- Portscan
- Virus
- Troiani
- Spyware
- Worm
- Phishing

Tipologie di attacchi [3]: intercettazioni

- Si dice sniffer un qualsiasi strumento, software o hardware che raccoglie le informazioni che viaggiano lungo una rete.
- Il nome deriva dal primo software di questo tipo “The Sniffer Network Analyzer”



Tipologie di attacchi [4]: intercettazioni

- Le funzioni tipiche di uno sniffer sono:
  - Conversione e filtraggio dei dati e dei pacchetti
  - Analisi dei difetti di rete
  - Performance Analysis (qualità e portata della rete)
  - Setacciamento di Password e Nomi di Utente
  - Creazione di LOG (elenchi del traffico di rete)
  - Scoperta di intrusioni attraverso l'analisi dei LOG

Tipologie di attacchi [5]: intercettazioni

Componenti di un packet sniffer:

- Hardware:
  - Standard network adapters
  - Con hardware speciale analizzano errori di CRC, problemi della tensioni, del cavo, “dribbles”, errori della negoziazione
- Capture driver:
  - Cattura il traffico della rete
  - Filtraggio
  - Memorizzazione dei dati in un buffer
- Buffer

  Pacchetti catturati dalla rete e immagazzinati in un buffer
  - Cattura finché il buffer non si riempie
  - Usa il buffer come un “round robin”

Tipologie di attacchi [6]: intercettazioni

L'esistenza di uno sniffer in rete rappresenta una minaccia alla sicurezza e alla riservatezza delle comunicazioni.

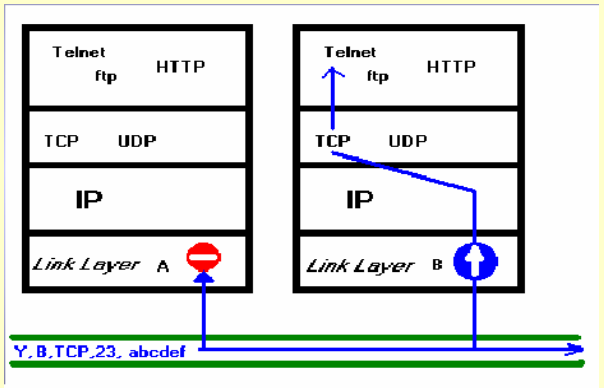
Se la LAN è sottoposta al controllo di uno sniffer significa che

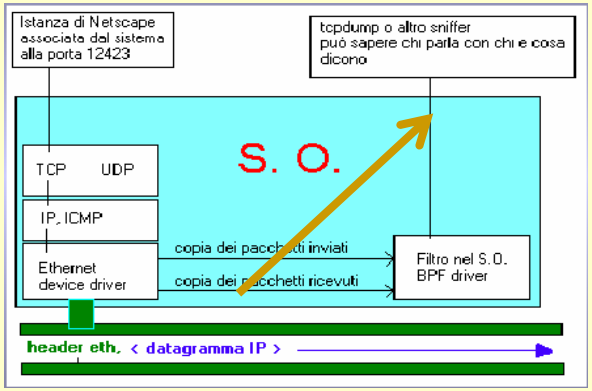
- un intruso è riuscito ad installare uno sniffer all'interno della rete
- un utente interno ne sta facendo un uso improprio
- il gestore della rete sta monitorando (o ne fa un uso improprio)

Lo sniffing è un attacco di secondo livello -> l'intruso è già introdotto all'interno della rete e cerca di compromettere la sicurezza del sistema.

Tipologie di attacchi [7]: intercettazioni

- Un dispositivo di sniffing analizza e processa i pacchetti che arrivano al suo dispositivo di rete, l'hw Ethernet si presta a questo tipo di attacco visto che più macchine condividono lo stesso cavo
- Esiste una tecnica piuttosto evoluta (arp spoofing) tramite la quale è possibile sniffare i pacchetti di terzi anche in una rete di tipo switched
- I pacchetti inviati sono visti dalle interfacce di rete di tutte le macchine, ma, grazie al controllo fatto da un chip dell'interfaccia che confronta MAC locale e MAC destinatario solo l'interfaccia del destinatario passa i dati allo strato superiore.
- Nel caso in cui sia installato un dispositivo di sniffing, il funzionamento è differente: le API del sistema operativo permettono di leggere tutto ciò che passa sul canale ponendo l'interfaccia in modalità promiscua. In tal caso i dati vengono consegnati all'applicazione che li richiede in modo grezzo, senza che essi passino attraverso gli opportuni strati di protocollo; resta a carico dello sniffer effettuare un'interpretazione dei pacchetti e assemblare i dati.





Tipologie di attacchi [8]: intercettazioni

Sniffing di reti di tipo switched:

- Switch jamming: nel caso di reti di tipo switched, per poter sniffare, è prima necessario portare lo switch dalla modalità ”bridge” alla modalità “hub”, effetto ottenibile sovraccaricando la tabella degli indirizzi, cioè generando traffico o inviando un flusso continuo di traffico verso lo switch (provocando un FAIL OPEN: per errori di trasmissione sono rimosse le condizioni di sicurezza).

- ARP redirect: si invia un pacchetto in broadcast sostenendo di essere il router, o inviarlo solo alla macchina vittima, è anche possibile dire al router di essere la macchina vittima (da fare più volte per rinfrescare le entries della cache)

- ICMP redirect: indica alla macchina di inviare i pacchetti in una direzione diversa

- ICMP Router Advertisment: informa gli utenti su chi sia il router

Tipologie di attacchi [9]: intercettazioni

Sniffing con un modem

Un cable-modem si divide in due canali asimmetrici:

- Upstream: canale di sola ricezione ad alta velocità (30-50 mbps)
- Downstream: canale di sola trasmissione a bassa velocità (1 mbps)

I cable-modem separano gli indirizzi MAC dagli indirizzi IP, quindi settare la scheda Ethernet in modalità promiscua non serve.

Solitamente non è possibile sniffare su cavo modem.

Metodi di sniffing:

- ARP: ci si spaccia per qualcun altro tramite l'invio di un pacchetto ARP
- ICMP redirect: ridirezionare il traffico
- ICMP ROUTER ADVERTISEMENT: ridireziona il traffico convincendo una macchina che il proprio sistema è il router

Tipologie di attacchi [10]: intercettazioni

Sniffing senza accesso al cavo

- Si vogliono catturare i pacchetti da una connessione tra due macchine senza avere accesso al cavo; inizialmente impossibile.

- Tecniche di sniffing:
  - Accesso remoto al cavo:
    - Si accede al sistema e si installa un software di cattura controllabile da remoto
    - Si accede al relativo ISP e si installa il software di cattura
    - Trovare un sistema presso l'ISP che supporti la cattura (RMON, DDS)
  - Chiusura del cavo: si reinstrada il traffico (Man In The Middle)
  - Rootkits e Admin Trojan Remoto: possono essere usati in teoria per sniffare traffico in generale, sono solitamente configurati per sniffare e-mail e password

Tipologie di attacchi [11]: intercettazioni

Programmi per packet sniffing

- Windows
  - Ethereal
  - WinDump (versione di tcpdump per WINDOWS)
  - WinNT server
  - Spynet/PeepNet

- Unix
  - Tcpdump
  - esniff (per user e password)
  - Snort
  - sniffit

Tipologie di attacchi [12]: port scan

Port scanning

- Azione di scansione remota delle porte note per rilevare l'elenco dei servizi attivi su una certa macchina
- si manda un pacchetto particolare "costringendo" la macchina target a una determinata risposta, da cui si possono trarre le informazioni del caso
- Letteralmente significa "scansione delle porte" e consiste nell'inviare richieste di connessione al computer bersaglio (soprattutto pacchetti TCP, UDP e ICMP creati ad arte): elaborando le risposte è possibile stabilire (anche con precisione) quali servizi di rete siano attivi su quel computer. Una porta si dice "in ascolto" ("listening") o "aperta" quando vi è un servizio o programma che la usa.

Tipologie di attacchi [13]: port scan

Il risultato della scansione di una porta rientra solitamente in una delle seguenti categorie:

- aperta (accepted): l'host ha inviato una risposta indicando che un servizio è in ascolto su quella porta
- chiusa (denied): l'host ha inviato una risposta indicando che le connessioni alla porta saranno rifiutata
- bloccata (dropped): non c'è stata alcuna risposta dall'host
- filtrata (filtered): rileva la presenza di un Firewall o di un ostacolo di rete in grado di bloccare l'accesso alla porta impedendo a Nmap di individuarne lo stato.

Tipologie di attacchi [14]: port scan

Di per sé il port scanning non è pericoloso per i sistemi informatici, e viene comunemente usato dagli amministratori di sistema per effettuare controlli e manutenzione.

Rivela però informazioni dettagliate che potrebbero essere usate da un eventuale attaccante per preparare facilmente una tecnica mirata finalizzata a destabilizzare la sicurezza del sistema, pertanto viene posta molta attenzione dagli amministratori a come e quando vengono effettuati port scan verso i computer della loro rete.

Un buon amministratore di sistema deve sapere che un firewall ben configurato permette alle macchine di svolgere tutti i loro compiti, ma rende difficile (se non impossibile) la scansione delle porte.

Tipologie di attacchi [15]: virus

I Virus informatici devono penetrare nel programma ospite modificandolo, sia per riprodursi, sia per danneggiare dati e/o programmi presenti su supporti registrabili; sono costituiti da poche centinaia di istruzioni per far notare la loro presenza all'utente del computer.

- Virus di file: Si sostituiscono in parte o completamente ad un programma (.exe, bat, .com …). Quando viene eseguito il programma, sarà eseguito il virus.
- Virus di boot: Sfruttano il settore di boot o MBR del disco per essere eseguiti ad ogni avvio della macchina. Risiedono in memoria.
- Virus multipartiti: Sono i più pericolosi e possono infettare sia il settore di avvio dei dischi che i programmi.
- Virus di macro: Infettano solo file di dati (e non i programmi) e precisamente quei file al cui interno possono essere contenute le macro.

Tipologie di attacchi [16]: troiani

Cosa sono:

Si camuffano bene, sembrano programmi normali e magari anche utili, non si replicano, ma ne richiedono l'esecuzione inconsapevole da parte dell'utente

Come si diffondono:

Tramite Internet (collegamenti peer to peer con Kazaa, WinMX, Edonkey, Emule) ed e-mail

Conseguenze:

Consentono il controllo remoto del PC da qualcuno via Internet, perdita e furto di dati ed informazioni personali (IP, Password..) installando Backdoor o Keylogger all'insaputa dell'utente

Tipologie di attacchi [17]: spyware

Cosa sono:
Software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso; non si replica, ma ne richiede l'esecuzione inconsapevole da parte dell'utente

Come si diffondono:
L'installazione può avvenire, sfruttando le vulnerabilità del browser, visitando pagine Web o con tecniche di social engineering

Conseguenze:
Invio di pubblicità non richiesta (Spam), modifica pagina iniziale del browser, la redirezione su falsi siti di e-commerce (Phishing), l'installazione di dialer truffaldini, occupazione di memoria, instabilità del sistema

Tipologie di attacchi [18]: Worms

Cosa sono:
Frammenti di codice indipendenti ed autonomi che agiscono principalmente in memoria, non hanno bisogno di legarsi ad altri programmi per diffondersi

Come si diffondono:
Tramite Internet ed e-mail, sfruttando i bug del client di posta e S.O. con tecniche di social engineering

Conseguenze:
Non mira a danneggiare i dati; crea malfunzionamenti (rallentamento o blocco) al sistema o peggio a carpire dati ed informazioni personali (IP, Password..)

Tipologie di attacchi [19]: Phishing

Cosa è:
Una tecnica utilizzata (cercando a caso) per ottenere le credenziali (password, Numero di carte di credito, riservate) di altre persone

Come si diffonde:
Tecniche di social engineering, telefonate, e-mail esca con grafica di banca, provider web, aste online

Conseguenze:
Furto di identità, numeri di carte di credito

Strumenti per la difesa in rete [1]

Bisogna fare particolare attenzione al fatto che:

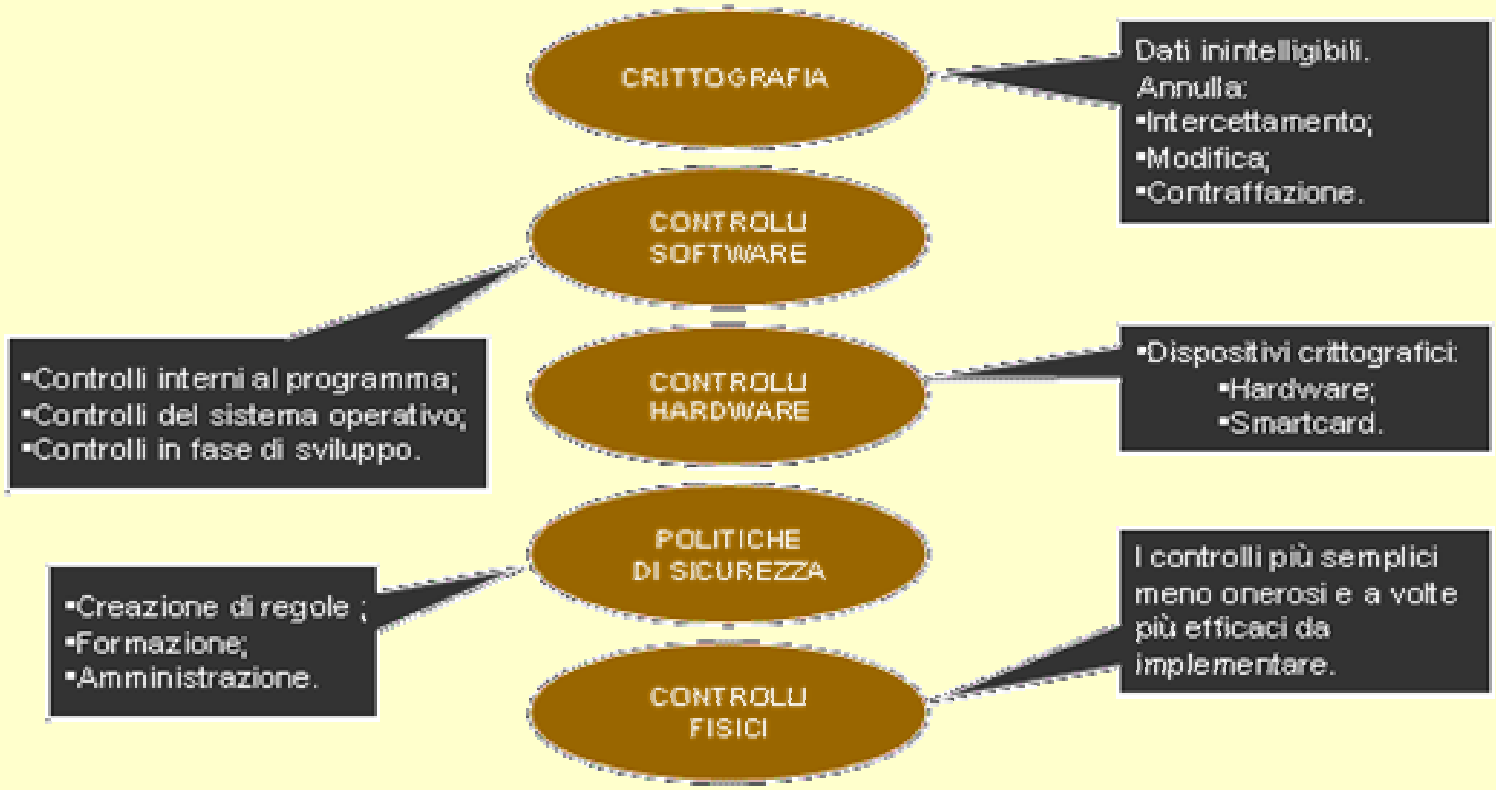
"la sicurezza è un processo, non un prodotto"

Come tale ha molti componenti, che devono essere affidabili e ben studiati e, soprattutto, collaborare fra loro. Infatti, l'efficacia del sistema di sicurezza dipende principale da come i vari componenti collaborano fra loro.

La Progettazione e la realizzazione di un sistema informatico deve tener presente:

- Gestione degli accessi al sistema
- Sistema Antivirus Centralizzato
- Gestione del traffico da e verso Internet (Firewall –antispyware – IDS)
- Protezione dell'informazione (Crittografia)

Strumenti per la difesa in rete [2]



Strumenti per la difesa in rete [3]: gestione delle password

Devono essere garantiti i seguenti punti:

- Autenticazione dell'utente (login e password)
  - E’ la prima barriera che un intruso deve superare, in questo modo si riduce il rischio che utenti "sconosciuti" possano accedere al sistema, ed alle sue risorse, senza averne le autorizzazioni.
- Delimitazione degli spazi logici
  - Garantisce un certo livello di privacy, in quanto un utente può accedere a file dati o programmi per cui è stato autorizzato.
- Tracking dell'attività
  - Permette di controllare le attività svolte da un utente sulla rete e rilevare eventuali comportamenti anomali.

Strumenti per la difesa in rete [3]: gestione delle password

Il primo ostacolo che un cracker deve superato per accedere ad un sistema è quello dell'autenticazione.

Esistono varie metodologie di autenticazione:

- Login e Password: è il metodo più diffuso; se queste non corrispondono a quelle conservate con quelle conservate nel sistema l'accesso viene negato.
- Carta magnetica: il riconoscimento viene effettuato inserendo la carta in un apposito lettore e digitando una password.
- Biometrie: si tratta di lettori di impronte digitali o vocali, analisi della retina, analisi della firma.
- Il sistema biometrico è composto da:
  - Registrazione – vengono misurate ed immagazzinate le caratteristiche dell'utente.
  - Identificazione – l'utente fornisce la sua "account", il sistema esegue delle misurazioni e confronta i valori con quelli già campionati.

Strumenti per la difesa in rete [4]: antivirus

Per proteggere il proprio sistema da virus (di vario tipo), trojan, spyware, ecc… è necessario dotarsi di opportuni SW che rilevano la presenza di strani file all'interno del sistema, quali:

- Anti-Virus: per file infetti da virus, worm, trojan.
- Anti-Trojan: per scovare ed eliminare trojan.
- Spyware Detectors: per scovare ed eliminare i programmi spia.

Perché questi SW risultino efficaci devono essere seguite determinate regole:

- deve essere aggiornato in automatico giornalmente, o settimanalmente
- deve rimanere in esecuzione mentre l'utente lavora
- deve controllare i Files e i contenitori di messaggi di posta
- è opportuno controllare anche tutti i file di dubbia provenienza

Strumenti per la difesa in rete [4]: Firewall

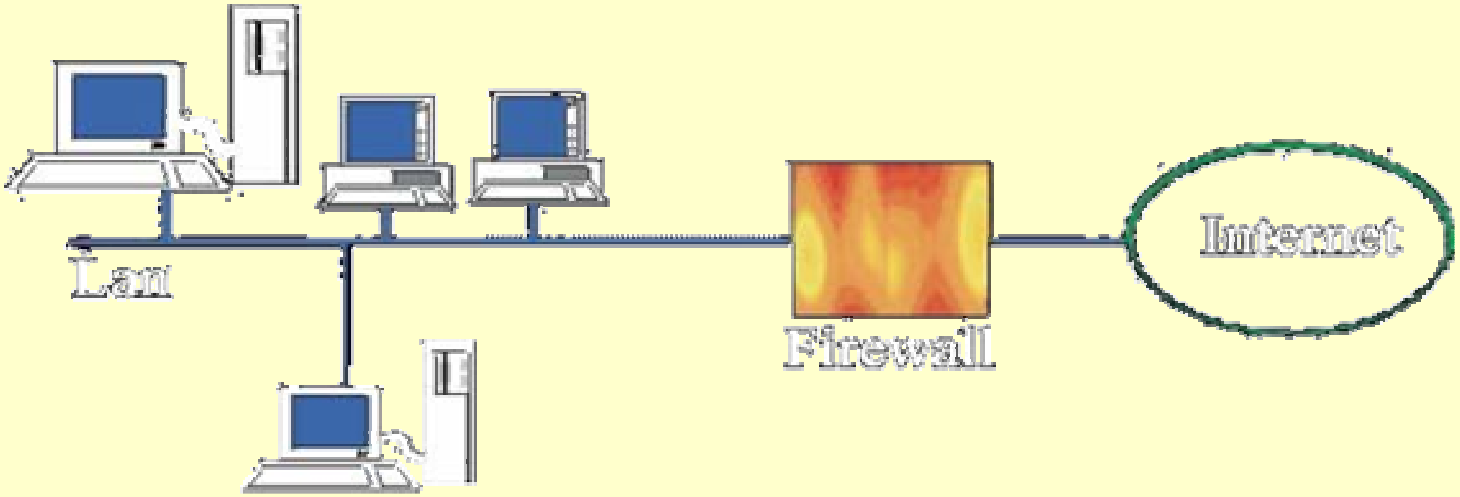
Il Firewall può essere pensato come una coppia di meccanismi: uno serve a bloccare il traffico in ingresso e l'altro per veicolare quello in uscita dalla rete.

Possono essere programmati per “controllare”, o bloccare diverse attività quali:

- Permettere solo il passaggio di mail
- Proteggere da login non autenticati dall’esterno
- Bloccare il traffico dall’esterno all’interno e permettere il contrario

Strumenti per la difesa in rete [5]: Firewall

E' importante ricordare che un firewall non può proteggere da attacchi che non vi passano attraverso, quindi non è sufficiente per realizzare un buon livello di sicurezza.



Strumenti per la difesa in rete [6]: Antispyware

Un antispyware è un programma il cui scopo è quello di cercare ed eliminare dal sistema, tramite un'apposita scansione, Spyware,, trojan e altri programmi potenzialmente dannosi.

Le funzioni di questi programmi sono simili a quelle degli antivirus anche se bisogna stare sempre attenti a non confonderli con essi.

Come gli antivirus, anche gli antispyware necessitano di costante aggiornamento del database delle definizioni per trovare anche gli ultimi spyware.

Strumenti per la difesa in rete [7]: Crittografia

Difendere la privacy individuale in un era di crescente computerizzazione sta diventando un problema cardine, in quanto oggi le nostre vite sono controllate in molti modi (transazioni con carte di credito, telefonate, assegni, ecc…).

Proprio per questi motivi, ed altri ancora, è necessario trovare uno, o più metodi che ci permettano di immagazzinare, o trasmettere in modo sicuro tutte quelle informazioni che sono tutelate dal diritto alla privacy, ma anche quelle che, per qualche motivo personale, o aziendale, sono ritenute “riservate”. Il più diffuso è la crittografia.

Strumenti per la difesa in rete [8]: Crittografia

La Crittologia è la scienza che studia il discorso e la scrittura segreta ed è suddivisa in due grosse branche:

- Crittografia: la scienza di scrivere dei messaggi che nessuno al di là del vero destinatario potrà leggere (dal greco kryptós = nascosto e dal tema, sempre greco, gráphò cioè, scrivere)
- Crittoanalisi: la scienza che si occupa della lettura delle informazioni crittografate attraverso la rottura dei sistemi cifranti

Strumenti per la difesa in rete [9]: Crittografia

Crittografia: è quella scienza che fornisce uno strumento adatto a mantenere segrete tutte quelle informazioni che non si vogliono divulgare pubblicamente, in maniera tale che la possibilità di accedervi sia data solo a persone autorizzate.

Possono essere fatte due operazioni:

- **Crittazione:** è l'operazione tramite la quale si nascondono le informazioni ed è effettuata tramite un apposito algoritmo chiamato cifrario; l'informazione da cifrare è noto come testo chiaro. La crittazione sfrutta come mezzo fondamentale una chiave per convertire il testo chiaro in testo cifrato o crittogramma.

- **Decrittazione:** è l'operazione inversa rispetto alla crittazione, ossia la conversione da testo cifrato a testo chiaro; anch'essa sfrutta la chiave del cifrario.

Strumenti per la difesa in rete [10]: Crittografia

Ci sono due casi generali in cui è necessario avvalersi dell'appoggio della crittografia:

- quando l'informazione deve semplicemente essere conservata sul posto e dunque "confezionata" in modo tale da renderla invulnerabile ad accessi non autorizzati.

- quando l'informazione deve essere trasmessa e dunque la crittazione è necessaria perchè se qualcuno la intercettasse non potrebbe capir nulla di quello che si trova tra le mani.

Strumenti per la difesa in rete [11]: Crittografia

Tecniche

Al giorno d'oggi la parola "crittografia" è usata per indicare una grande varietà di tecniche; entra in gioco la chiave, che è una stringa di caratteri che seleziona una tra le molte cifrature potenziali.

Tutti i moderni metodi utilizzano una chiave per eseguire la crittazione e la decrittazione; un messaggio può essere decrittato solo se la chiave di decifratura si "accoppia" con quella di cifratura.

Per alcuni algoritmi le due chiavi sono uguali, mentre per altri esse sono diverse; in base a questa sostanziale differenza gli algoritmi basati sull'utilizzo di chiavi si dividono in:

- simmetrici (detti anche a chiave simmetrica o a chiave segreta)
- asimmetrici (detti anche a chiave asimmetrica o a chiave pubblica).

Strumenti per la difesa in rete [12]: Crittografia

Sistemi a chiave simmetrica

Tali sistemi possono essere utilizzati per implementare servizi di sicurezza quali:

- Riservatezza: proteggere l'informazione da visione non autorizzata. Spesso la protezione riguarda solo il corpo del messaggio e non la testata, trasmessa in chiaro per semplificare l'instradamento del messaggio fino al destinatario.
- Integrità: garantire che l'informazione non venga alterata e che il messaggio arrivi esattamente come è stato spedito.
- Autenticazione: serve a prevenire la dissimulazione degli utenti, cioè consente al vero mittente di includere nel messaggio informazioni che lo identifichino con certezza.

Strumenti per la difesa in rete [13]: Crittografia

Sistemi a chiave asimmetrica

Le tecniche asimmetriche utilizzano coppie di chiavi complementari invece di una sola chiave segreta.

Un singolo utente possiede una coppia univoca di chiavi complementari:

- una è pubblica, nel senso che può essere conosciuta da tutti, ed è usata per cifrare il messaggio.
- una è privata ed è tenuta al sicuro dal suo proprietario di modo che solo lui possa utilizzarla.

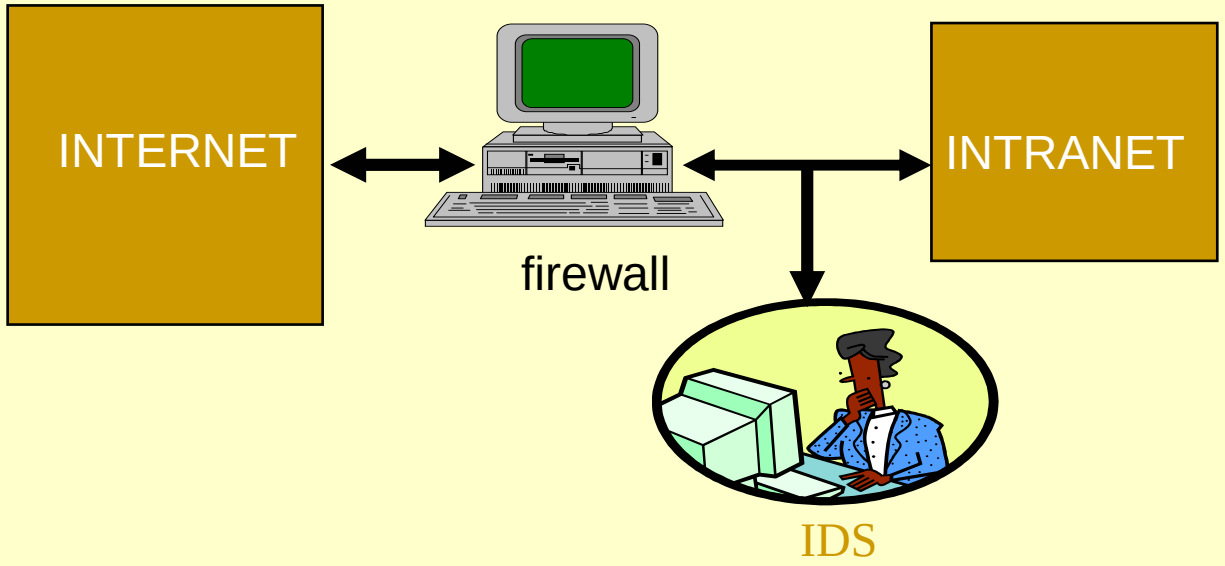
Le due chiavi sono create in maniera tale che un messaggio cifrato da una delle due può essere decifrato solo e soltanto dall'altra.

In pratica se si vuole spedire un messaggio a una certa persona, si critta quel messaggio con la sua chiave pubblica, e si è sicuri che soltanto quella persona potrà decifrarla con la propria chiave privata: neanche la chiave pubblica utilizzata per cifrare riuscirà a decrittare il messaggio.

Strumenti per la difesa in rete [14]: Intrusion Detection System

I Network Analyzer sono dei dispositivi che si occupano di monitorare ed analizzare in tempo reale il traffico di rete.

Gli Intrusion Detection System sono da considerarsi un'estensione dei network analyzer. Il loro incarico, infatti, é quello di registrare e segnalare, nel minor tempo possibile, le violazioni (anche sotto forma di tentativo) dei sistemi informativi.



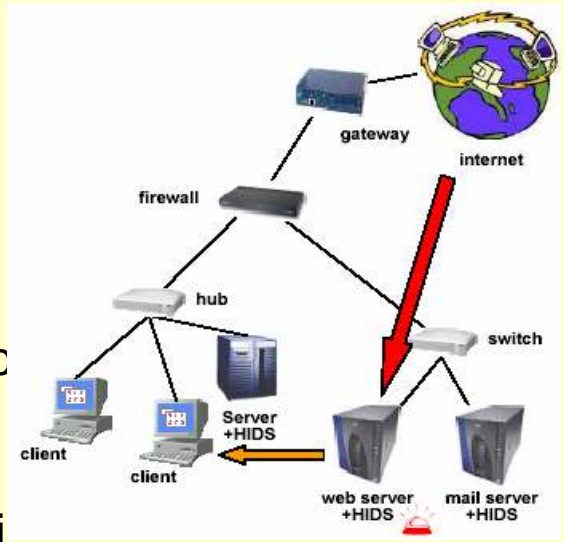
Strumenti per la difesa in rete [15]: Intrusion Detection System

Esistono due tipi di IDS:

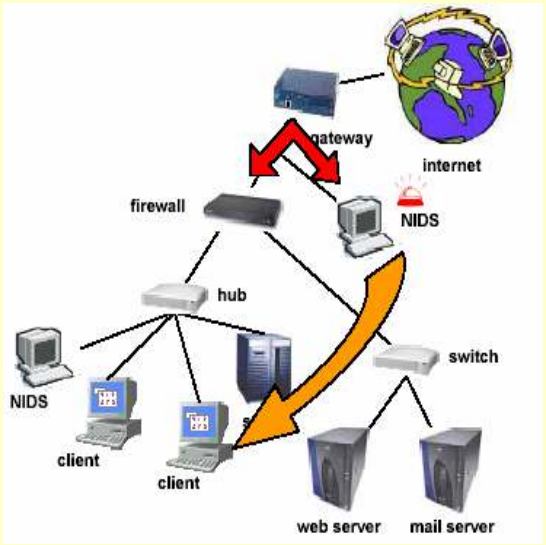
- Host IDS: basati su host ed analizzano in real-time le attività interne al sistema (utenti – applicazioni – log).
- Network IDS: web server basati su traffico di rete, analizzano in real-time tutto il traffico di rete (sniffing), alla ricerca di attacchi sconosciuti, o particolari tipi di traffico.

Alcuni tipi di IDS possono interagire con particolari firewall ed attivare contromisure.

HIDS



NIDS

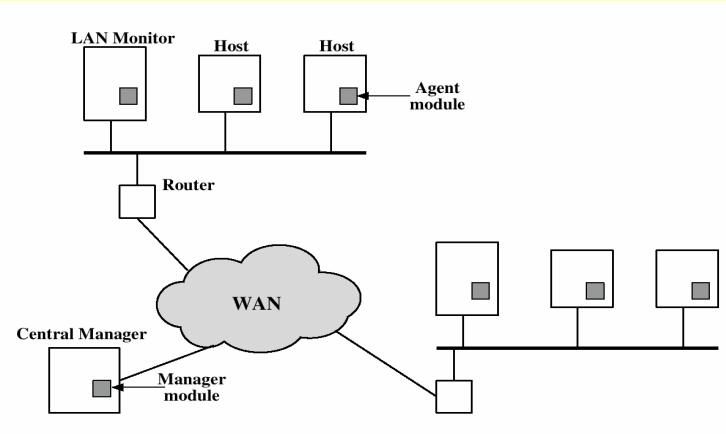


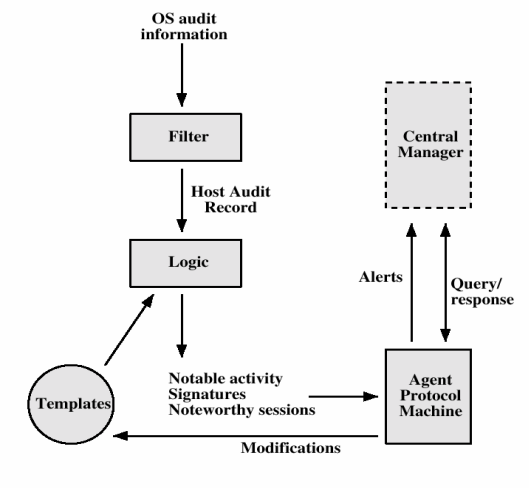
Strumenti per la difesa in rete [16]: Intrusion Detection System

- Un IDS è costituito da una serie di sensori di rete o agenti e da un analizzatore centrale, ognuno di essi risiede su un host dedicato

- I sensori di rete vengono installati su determinate porzioni di rete, solitamente quelle su cui sono presenti i sistemi più critici

- I dati raccolti vengono inviati all'analizzatore che verifica o meno la presenza di traffico sospetto in tal caso attiva una serie di procedure di allarme





Strumenti per la difesa in rete [17]: Intrusion Detection System

Per la realizzazione di questi strumenti si fa ricorso a due strategie di base:

- Anomaly detection
- Misuse detection

Strumenti per la difesa in rete [18]: Intrusion Detection System

Parametri rilevati attraverso la Anomaly datection:

- Login frequency by day and time
- Frequency of login at different locations
- Time since last login
- Password failures at login
- Execution frequency
- Execution denials
- Read, write, create, delete frequency
- Failure count for read, write, create and delete

Strumenti per la difesa in rete [19]: Intrusion Detection System

Funzionamento del misuse detection:

- I caratteri distintivi di attacchi noti (signatures) vengono memorizzati in appositi database di attacchi
- alla ricezione di ogni pacchetto l'analizzatore confronta lo stesso o la sequenza a cui appartiene con le signature memorizzate nel proprio database
- quando trova delle coincidenze attiva una serie di allarmi

Strumenti per la difesa in rete [20]: Intrusion Detection System

Misuse detection:

- Un intrusion detection system può erroneamente riconoscere una sequenza di pacchetti innocua come maligna e quindi provvedere ad attivare un falso allarme
- In questo caso si dice che l'intrusion detection system ha commesso un errore di tipo falso positivo (false positive)

Bibliografia

La comunicazione in rete: sicurezza, privacy, copyright in Internet : soluzioni tecniche e giuridiche - Marcello Morelli - FrancoAngeli, 1999

Qualcuno ci spia. Spyware nel tuo PC - Elio Molteni, Rossano Ferraris - Mondadori Informatica, 2005

Firewalls e sicurezza in rete - William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin - Pearson Education Italia, 2003

Computer sicuro. La guida Symantec contro spyware, worm, virus, spam e intrusi nel tuo PC - Andrew Conry-Murray, Vincent Weafer - Mondadori Informatica, 2006

Introduzione alla crittografia: algoritmi, protocolli, sicurezza informatica - Alessandro Languasco, Alessandro Zaccagnini - HOEPLI EDITORE, 2004