Seguretat activa i accés remot

Josep Maria Arqués Soldevila, Miquel Colobran Huguet, Ivan Basart Carrillo, Carles Caño Valls, Jordi Masfret Corrons, Josep Pons Carrió i Jordi Prats Català

Seguretat i alta disponibilitat

Índex

Introducció

Les tecnologies de la informació, i en especial Internet, han convertit la comunicació en un element clau i a la vegada vulnerable per part de tercers. Així, doncs, la facilitat per realitzar tasques de manera remota i per comunicar-nos s'han d'equilibrar amb la seguretat en aquestes comunicacions. Una gestió incorrecta del trànsit i accés d'aquesta informació pot ocasionar l'exposició, la còpia o l'esborrat de dades sensibles i pot provocar la pèrdua del sistema d'informació i, en conseqüència, la paralització de l'activitat de l'organització i grans pèrdues econòmiques.

Al llarg d'aquest mòdul heu treballat diversos conceptes tècnics i legals relacionats amb la seguretat informàtica. En aquesta unitat, però, veureu com es poden classificar els atacs a sistemes informàtics i quines mesures, ja siguin mitjançant programari o maquinari, es poden adoptar per minimitzar-ne els efectes. Aprendreu que un sistema d'informació pot ser "proactiu" i que amb un conjunt de mesures de seguretat adient es pot pal·liar una de les problemàtiques actuals; l'accés a la informació a través de xarxes insegures o públiques, com és el cas d'Internet.

En l'apartat "Mecanismes de seguretat activa" es descriuen els elements que permeten identificar els atacs, així com les eines per prevenir-los. Conèixer els tipus d'atac us permetrà prevenir-los, detectar-los i evitar-los.

En l'apartat "Implantació de tècniques d'accés remot" s'expliquen el conjunt de configuracions de seguretat, ja siguin de programari, de maquinari o mixtes, que permeten l'accés segur a la xarxa d'informació des de l'exterior.

Al llarg de la unitat veureu que la seguretat està orientada a evitar incidents i a minimitzar-ne els efectes si succeeixen. Us adonareu que aquests incidents tant poden provenir de l'exterior de la xarxa com de l'interior i que, per tant, cal preveure tots els escenaris possibles.

La unitat descriu, des d'un vessant pràctic i teòric, aspectes essencials de la seguretat informàtica. Aquesta es pot entendre com un fenomen "en capes": la de l'ordinador de sobretaula, la dels servidors, la de la xarxa LAN, la dels punts de connexió amb xarxes insegures i la de la interconnexió de xarxes, coneguda com a Internet. Per treballar els continguts d'aquesta unitat didàctica és convenient anar fent les activitats i els exercicis d'autoavaluació, així com llegir els annexos.

Resultats d'aprenentatge

En finalitzar aquesta unitat formativa, l'alumne/a:

1. Implanta mecanismes de seguretat activa, seleccionant i executant contramesures enfront d'amenaces o atacs al sistema.
    - Classifica els principals tipus d'amenaces lògiques contra un sistema informàtic.
    - Verifica l'origen i l'autenticitat de les aplicacions instal·lades en un equip, així com l'estat d'actualització del sistema operatiu.
    - Identifica l'anatomia dels atacs més habituals, així com les mesures preventives i pal·liatives disponibles.
    - Analitza diversos tipus d'amenaces, atacs i programari maliciós, en entorns d'execució controlats.
    - Implanta aplicacions específiques per a la detecció d'amenaces i l'eliminació de programari maliciós.
    - Utilitza tècniques de xifrat, signatures i certificats digitals en un entorn de treball basat en l'ús de xarxes públiques.
    - Avalua les mesures de seguretat dels protocols usats en xarxes sense fil.
    - Reconeix la necessitat d'inventariar i controlar els serveis de xarxa que s'executen en un sistema.
    - Descriu els tipus i característiques dels sistemes de detecció d'intrusions.
2. Implanta tècniques segures d'accés remot a un sistema informàtic, interpretant i aplicant el pla de seguretat.
    - Descriu escenaris típics de sistemes amb connexió a xarxes públiques en els quals es precisa fortificar la xarxa interna.
    - Classifica les zones de risc d'un sistema, segons criteris de seguretat perimètrica.
    - Identifica els protocols segurs de comunicació i els seus àmbits d'utilització.
    - Configura xarxes privades virtuals mitjançant protocols segurs a diferents nivells.
    - Implanta un servidor com a passarel·la d'accés a la xarxa interna des d'ubicacions remotes.
    - Identifica i configura els possibles mètodes d'autenticació en l'accés d'usuaris remots a través de la passarel·la.
    - Instal·la, configura i integra en la passarel·la un servidor remot d'autenticació.

1. Mecanismes de seguretat activa

La protecció de la informació és la conseqüència de l'aplicació d'un conjunt de mecanismes o estratègies de seguretat. A grans trets, aquestes estratègies han de considerar els principis següents:

- La seguretat ha de ser un objectiu global.
- La seguretat s'ha de dissenyar com quelcom que és part de l'organització, tenint en compte tots aquells aspectes que la puguin conformar.
- El marc legal s'ha de considerar, des de l'inici, com una part més del disseny de les polítiques de seguretat.

La gestió i planificació de tota la seguretat és clau. En cas contrari, res del que es faci tindrà un objectiu final, i per tant, només millorarà parcialment la seguretat. A més, la gestió no només és necessària en la implantació de la seguretat, sinó també en el seu control i manteniment.

Tallafoc

Un tallafoc és un exemple de **seguretat activa**. Filtra l'accés a certs serveis en determinades connexions per bloquejar un intent d'atac. Un altre exemple de seguretat activa pot ser l'ús de contrasenyes.

Entenem per **seguretat activa** tots aquells mecanismes i mesures (físics i lògics) que permeten prevenir i detectar possibles intents de comprometre els components d'un sistema informàtic.

Per **seguretat passiva** entenem el conjunt de mesures implementades en els sistemes per minimitzar els efectes d'un incident i mantenir informats els administradors sobre les incidències que puguin comprometre la seguretat.

Són exemples de **seguretat passiva** un sistema de detecció d'intrusos o la realització de còpies de seguretat.

1.1 Sistemes personals. Atacs i contramesures

Amb la revolució tecnològica dels darrers anys els sistemes personals han esdevingut part de la nostra vida. Les tauletes tàctils, els mòbils, les PDA, els ordinadors portàtils i, fins i tot, els equips personals de sobretaula estan, d'una o altra manera, connectats a xarxes de transmissió d'informació i són, per tant, susceptibles de patir atacs per part de tercers.

1.1.1 Classificació dels atacs

La protecció d'un sistema informàtic no només s'ha d'adreçar al maquinari i al programari, sinó també a les dades, tant si es troben circulant per una xarxa com si estan emmagatzemades en un disc dur o en altres suports. Pensem que si bé

gairebé sempre és possible substituir el maquinari o el programari, les dades, objectiu primordial de tot sistema informàtic, no tenen substitut en cas que es perdin definitivament.

Els atacs que es poden produir en un sistema informàtic es poden classificar segons l'objectiu de l'atac, segons la forma de l'atac i segons el tipus d'atacant, entre d'altres formes.

Classificació segons l'objectiu de l'atac

Els atacs que pot patir el maquinari, el programari i les dades es poden classificar en quatre grans grups:

- **Interrupció**: atac contra la disponibilitat en el qual es destrueix, o queda no disponible, un recurs del sistema (per exemple, tallar una línia de comunicació o deshabilitar el sistema de fitxers del servidor).

- **Intercepció**: atac contra la confidencialitat en el qual un element no autoritzat aconsegueix l'accés a un recurs. Aquest tipus d'atac no es limita a possibles usuaris que actuïn com a espies en la comunicació entre emissor i receptor. Per exemple, un procés que s'executa subreptíciament en un ordinador i que emmagatzema en un fitxer les tecles que prem l'usuari que utilitza el terminal (*keylogger*), també constituiria un atac d'intercepció.

Atac de denegació de servei

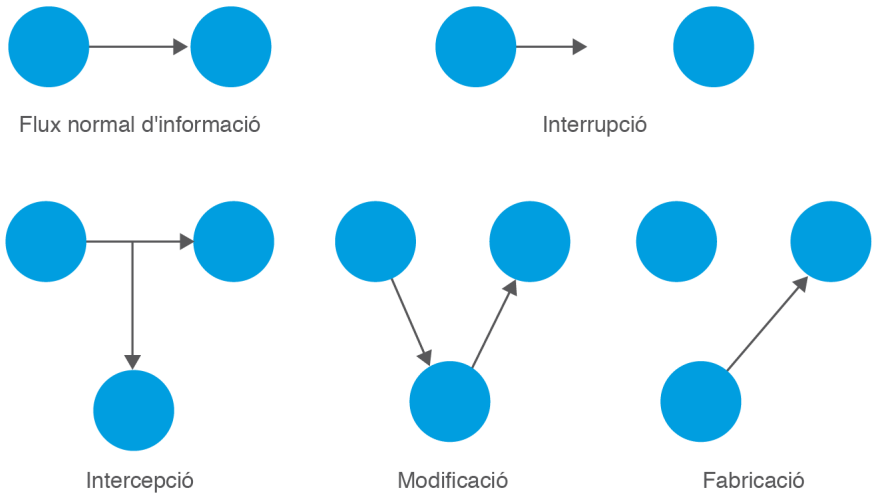
Un exemple característic d'atac d'interrupció és l'atac de denegació de servei, en el qual s'inutilitza el maquinari o programari de manera que no siguin accessibles des de la xarxa.

- **Modificació**: atac contra la integritat en el qual, a més d'aconseguir l'accés no autoritzat a un recurs, també s'aconsegueix modificar-lo, esborrar-lo o alterar-lo de qualsevol manera. Els atacs fets pels intrusos (esborrament de bases de dades, alteració de pàgines web...) són exemples d'aquesta modalitat d'atac.

- **Fabricació**: atac contra la integritat en el qual un element aconsegueix crear o inserir objectes falsificats en el sistema (per exemple, afegir de manera no autoritzada un nou usuari i la contrasenya corresponent al fitxer d'usuaris).

A la figura 1.1 es pot observar una representació gràfica d'aquesta classificació.

Figura 1.1. Tipus d'atacs que pot patir la comunicació entre emissor i receptor



Classificació segons la forma de l'atac

Els atacs provinents de persones es poden classificar en dos grans grups:

- Atacs passius
- Atacs actius

Atacs passius
L'atacant no modifica ni destrueix cap recurs del sistema informàtic, simplement l'observa, normalment amb la finalitat d'obtenir alguna informació confidencial.

Sovint, aquest atac es produeix sobre la informació que circula per una xarxa. L'atacant no altera la comunicació, sinó que senzillament l'escolta i obté la informació que es transmet entre l'emissor i el receptor. Com que la informació que es transmet no resulta alterada, la detecció d'aquest tipus d'atac no és fàcil. Una manera molt eficaç de resoldre aquest problema és usar tècniques criptogràfiques per fer que la informació no es transmeti en text clar i no sigui comprensible per als espies.

Criptografia
La criptografia és la ciència i estudi de l'escriptura secreta.

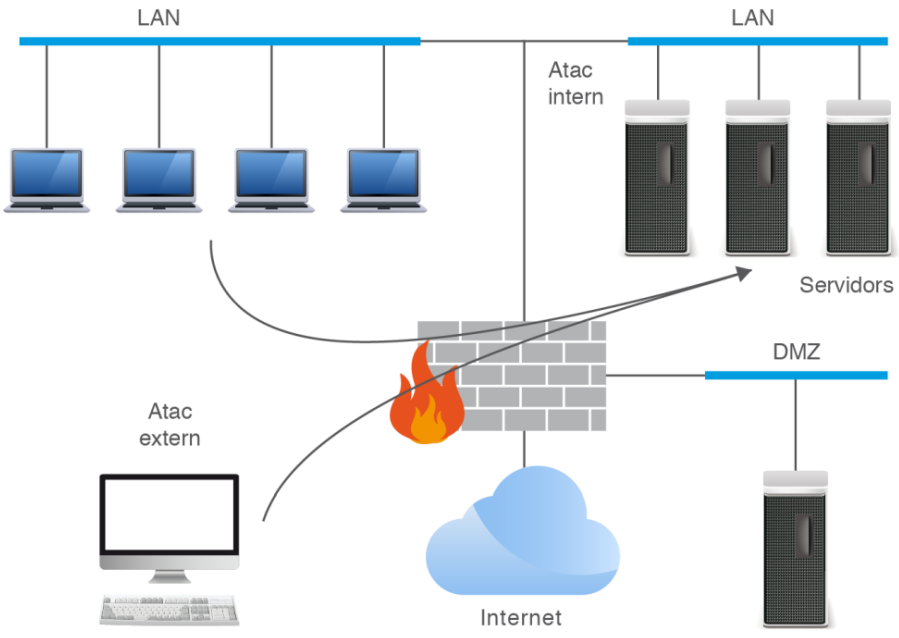
Atacs actius
En una acció d'aquest tipus, l'atacant altera o destrueix algun recurs del sistema.

Un espia que monitora una xarxa podria causar problemes molt seriosos, com els que exposem a continuació:
Suplantació d'identitat: l'espia pot suplantar la identitat d'una persona i enviar missatges en nom seu.
Reactuació: un o diversos missatges legítims són interceptats i reenviats diverses vegades per produir un efecte no desitjat (per exemple, intentar repetir diverses vegades un ingrés en un compte bancari).
Degradació fraudulenta del servei: l'espia evita el funcionament normal dels recursos del sistema informàtic. Per exemple, podria interceptar i eliminar tots els missatges que s'adrecen a un usuari determinat.
Modificació de missatges: es modifica una part del missatge interceptat i es reenvia a la persona a qui anava adreçat originalment.

Classificació segons el tipus d'atacant

La major part dels atacs que pot patir un sistema informàtic es produeixen en mans de persones que, amb diversos objectius, intenten accedir a informació confidencial, destruir-la o aconseguir el control absolut del sistema atacat. Cal tenir present que un atac pot provenir tant de l'interior de la xarxa (*insiders*) com de l'exterior (*outsiders*). Es pot veure esquemàticament a la figura 1.2.

Figura 1.2. Representació esquemàtica de com es realitzen els atacs per part d'insiders i outsiders



Acostumem a pensar que la gran majoria dels atacs provenen de l'exterior de l'organització i que són escassos, però les estadístiques demostren tot el contrari. La realitat és que:

- Els atacs externs són més nombrosos que els interns.
- El percentatge d'èxit en els atacs interns és més elevat.
- El dany causat per atacs interns és molt més gran que el provocat per atacs externs.

Conèixer els objectius dels atacants i les seves motivacions és essencial per prevenir-ne i detectar-ne les accions. Els principals possibles atacants d'un sistema informàtic són:

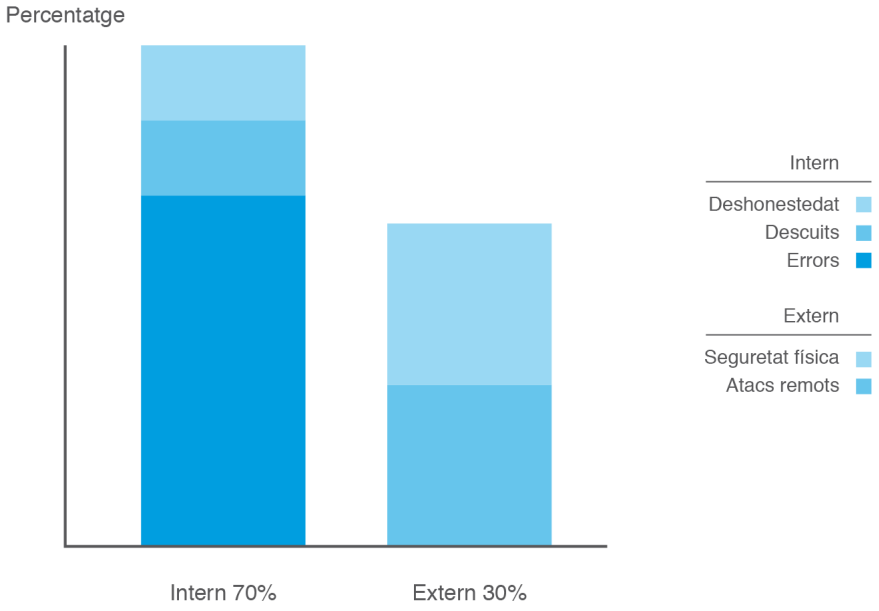
- Personal de la mateixa organització
- Antics treballadors
- Intrusos informàtics (*hackers*)
- Intrusos remunerats

Personal de la mateixa organització
Tot i que normalment el personal intern gaudeix de la confiança de l'organització, cal tenir en compte que alguns atacs es poden produir des de dins mateix de la institució. Sovint no cal que aquests atacs siguin intencionats (tot i que, quan ho són, són els més devastadors que es poden produir); poden ser accidents provocats pel desconeixement del personal (per exemple, el formatat accidental d'un disc dur).

Les tècniques bàsiques o contramesures per minimitzar els riscos d'atacs d'aquest tipus són:

- Assegurar-se que els usuaris amb permisos administratius són persones de confiança.
- Limitar la quantitat de permisos que una única persona posseeix.
- Limitar al màxim el nombre de persones amb permisos de confiança.
- Cercar escletxes de seguretat en els permisos.
- Definir una bona política de formació (pel que fa a la seguretat) per a tot el personal de l'organització.
- Impossibilitar que els usuaris sense privilegis puguin instal·lar programes (la majoria d'usuaris d'una organització no necessiten instal·lar programes, ja que per a la seva feina només necessiten els recursos o programes que els proporciona l'organització).
- Deshabilitar el ports USB per evitar la fuita d'informació (o proveir mecanismes criptogràfics que evitin l'extracció en text clar de la informació del sistema).

Figura 1.3. Percentatge i tipus d'atacs en una organització (www.cybsec.com)



.

Antics treballadors

Una part molt important dels atacs a sistemes informàtics són els fets per antics treballadors que, abans de marxar acomiadats o descontents per les condicions laborals, instal·len programes maliciosos com, per exemple, virus o bombes lògiques que s'activen en la seva absència (per exemple, quan arriba una data determinada). La presència d'aquest tipus de programa no sempre és fàcil de detectar, però almenys sí que es poden evitar els atacs que l'antic treballador pugui dur a terme des de fora amb el nom d'usuari i la contrasenya de què disposava quan encara treballava a l'organització (aquesta situació és més freqüent del que ens pensem). Per tant, una bona contramesura per a aquest problema és donar de baixa tots els comptes de l'extreballador i canviar les contrasenyes d'accés el sistema al més aviat possible. Així mateix, es poden proveir mecanismes d'autenticació més forts que no pas l'ús de només un nom d'usuari i contrasenya, per exemple, mitjançant un testimoni de seguretat.

Testimonis de seguretat

Els testimonis de seguretat o *security tokens* són dispositius físics de mida reduïda (alguns inclouen un teclat per introduir una clau numèrica o PIN), similars a un clauer, que calculen contrasenyes d'un únic ús (canvien a cada inici de sessió o cada cert temps).

Intrusos informàtics (hackers)

Els intrusos informàtics normalment duen a terme atacs passius destinats a obtenir informació confidencial (per exemple, un examen d'un curs) o amb la finalitat de posar-se a prova per obtenir el control del sistema atacat. Si l'atacant és prou hàbil, fins i tot pot esborrar les empremtes de les seves accions en els fitxers que les enregistren. Com que aquest tipus d'accions no produeixen cap efecte visible, no són fàcilment detectables.

Hackers i crackers

Quan la finalitat de la intrusió és destructiva, la persona que fa l'acció rep el nom de *cracker* (pirata). La nostra intenció no és diferenciar entre *hackers* i *crackers*, de manera que s'utilitzarà el terme intrús en relació amb qualsevol tipus d'intrusió, sigui o no destructiva. La mera intrusió en un sistema informàtic pot ésser considerada un delicte, amb independència que es produeixin o no danys en el sistema.

Els intrusos solen aprofitar les vulnerabilitats conegudes de sistemes operatius i programaris per aconseguir el control de tot el sistema informàtic. Per dur a terme aquest tipus d'accions n'hi ha prou d'executar diversos programes que es poden

obtenir a Internet i que automatitzen els atacs als sistemes informàtics sense que l'intrús necessiti disposar de gaires coneixements tècnics.

A vegades, l'únic interès de l'intrús és deixar una empremta de la seva "habilitat" per introduir-se en els sistemes sense autorització. Així, és relativament freqüent que modifiqui, per exemple, un lloc web (*defacement*) i hi deixi el seu pseudònim. No oblidem, però, que aquesta activitat és un delicte de danys recollit en el Codi Penal.

A més d'eines de caràcter tècnic, els intrusos disposen d'altres estratègies més senzilles (almenys des del punt de vista informàtic), però igual d'efectives. Per exemple, poden fer una senzilla recerca de contrasenyes escrites en papers entre la brossa continguda en una paperera (*trashing*) o en les notes adhesives que hom sol enganxar al monitor d'un terminal de treball, o emprar qualsevol tècnica d'enginyeria social.

Enginyeria social

L'enginyeria social és la pràctica d'obtenir informació confidencial mitjançant la manipulació i engany dels posseïdors legítims d'aquesta informació.

Intrusos remunerats

Tot i no ser gaire freqüent, també val la pena tenir en compte l'atac d'intrusos remunerats. En aquest cas, els intrusos estan perfectament organitzats (poden estar en diferents localitzacions geogràfiques fins i tot) i ataquen de manera coordinada una entitat determinada. Disposen de molts mitjans tècnics i reben remuneracions molt elevades de l'organisme rival que dirigeix l'atac, sovint amb l'ànim d'accedir a informació confidencial (un nou disseny, un nou programari...) o bé de provocar un dany important en la imatge de l'entitat atacada.

Atacs distribuïts

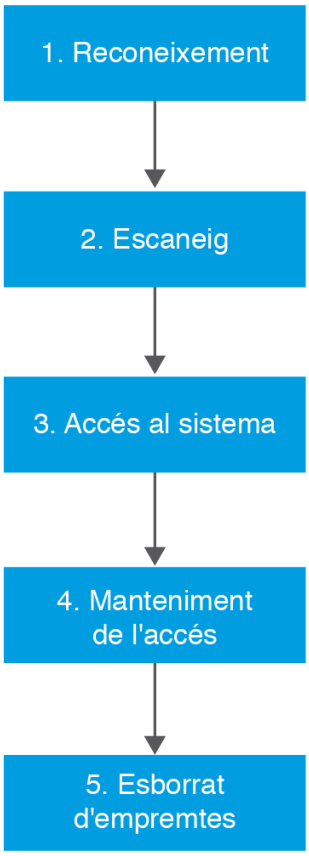
La preparació i realització d'un atac informàtic consta de diverses fases, algunes d'elles molt tècniques. Per aquest motiu, alguns atacs es realitzen de forma distribuïda, de manera que cada membre de la coalició efectua unes determinades fases o accions de l'atac.

1.1.2 Anatomia dels atacs

Els atacs informàtics solen constar d'un cicle de cinc fases (figura 1.4):

1. Reconeixement
2. Escaneig
3. Accés al sistema
4. Manteniment accés
5. Esborrat empremtes

Figura 1.4. Fases d'un atac informàtic



Cal diferenciar entre l'**atac informàtic** i el **delicte informàtic**. No obstant això, les conseqüències dels atacs informàtics poden estar recollides en el Codi Penal.

El coneixement del funcionament intern d'un atac informàtic ens ajuda a avançar-nos als esdeveniments i preveure activitats que podrien comprometre el nostre sistema informàtic.

Fase 1: reconeixement

Aquesta primera fase té caràcter preparatori i consisteix en la recopilació, per part de l'atacant, de tota la informació possible del sistema que pretén comprometre. No oblidem que l'atacant pot tenir tot el temps del món per preparar la seva estratègia, mentre que nosaltres només ens podem preparar de forma general per evitar i minimitzar les conseqüències d'un atac.

L'atacant pot utilitzar diverses tècniques a l'hora de reconèixer un sistema. Per exemple, pot emprar enginyeria social o *trashing*, amb la finalitat d'aconseguir informació valuosa per accedir al sistema. Fixem-nos que, en cas d'emprar tècniques d'enginyeria social, l'atacant ni tan sols hauria hagut d'emprar cap mètode informàtic per obtenir la informació que desitja.

Sniffing

El monitoratge d'una xarxa (*sniffing*) no és, en si mateix, una conducta delictiva. No oblidem que aquests tipus d'eines són emprades lícitament pels administradors de sistemes informàtics.

Altres tècniques pròpies d'aquesta fase són:

- Fer recerques a Internet (notem que, normalment, la informació corporativa de la nostra organització, ha de ser visible a la xarxa per motius comercials

i, per tant, es pot localitzar fàcilment). En tot cas, cal ser curós amb la informació que es mostra a la xarxa i deixar, en la mesura del possible, només aquella que sigui necessària pel funcionament de l'organització i que no pugui comprometre la seguretat del sistema.

- Capturar el trànsit de xarxa (*sniffing*).
- Utilitzar l'ordre whois per esbrinar dades relatives al sistema que volem investigar (per exemple, l'empresa que va enregistrat un domini determinat, o la seva adreça). Les bases de dades consultades per whois (la consulta també es pot fer mitjançant diversos webs) són públiques i, tot i que aquesta informació es podria emprar de forma maliciosa, pot ser molt útil, per exemple, per saber si un domini determinat està disponible.

Fase 2: escaneig

En aquesta fase, l'atacant utilitzarà tota la informació obtinguda en l'apartat anterior per sondejar el sistema que pretén atacar i detectar una vulnerabilitat (o vulnerabilitats) específica, que pugui aprofitar per accedir al sistema (per exemple, una vulnerabilitat del sistema operatiu que usa el sistema objectiu, una vulnerabilitat d'una aplicació...).

En definitiva, l'atacant intentarà, principalment, obtenir informació dels comptes d'usuari, de les versions del sistema operatiu i de les aplicacions, així com els ports oberts. Moltes eines d'administració de sistemes es poden emprar en aquesta fase amb finalitats il·lícites, com per exemple els escàners de xarxa o de ports (***nmap*** executat a la figura 1.5).

Figura 1.5. Exemple d'ús de l'ordre nmap

```
root@ubuntu:/home/user# nmap localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2012-05-06 18:33 EDT
Interesting ports on localhost (127.0.0.1):
Not shown: 1711 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.565 seconds
```

L'eina *nmap* no serveix únicament per conèixer els ports que té oberts una màquina, sinó que també es pot emprar per identificar la seva adreça MAC o el sistema operatiu que utilitza, entre altres utilitats.

Hi ha moltes més eines que es poden emprar en aquesta fase. D'entre elles, podríem destacar, per exemple, les ordres ***tracert*** en entorns Windows o ***traceroute*** en entorns Linux/Unix. Aquesta ordre es pot emprar per esbrinar els canvis de xarxa que realitzen els paquets per la xarxa fins arribar a la seva destinació.

Cal tenir en compte que aquestes eines, vistes aquí amb finalitats malicioses, tenen moltíssima utilitat per l'administrador del sistema i que, per tant, el seu ús principal és lícit.

Vulnerabilitat

S'entén per *vulnerabilitat* qualsevol punt feble que pugui posar en perill la seguretat d'un sistema informàtic. Aquesta feblesa s'ha d'entendre com una qüestió interna (latent) del sistema. Pot ser aprofitada per un atacant per violar la seguretat del sistema informàtic o simplement pot provocar danys de manera no intencionada (per exemple, un error de programació pot fer que un programari tingui comportaments irregulars i insospitats).

Exploits

Els exploits són programes maliciosos (entren dins de la categoria de les anomenades amenaces lògiques) que aprofiten una vulnerabilitat (coneguda o no) d'un programari informàtic, conseqüència d'un error de programació. No existeix un exploit general, sinó que cada programa, a causa dels gairebé inevitables errors de programació, té les seves peculiars vulnerabilitats, que poden ser hàbilment explotades pels programadors experimentats (si bé a Internet es poden trobar exploits per violar la seguretat de tota mena d'aplicacions i sistemes operatius sense necessitat de tenir coneixements de programació).

Port

Un port és un punt pel qual entra o surt la informació d'un ordinador. Els protocols relatius a Internet (FTP, Telnet...) utilitzen emissor i receptor, un port de sortida i recepció comú en ambdós extrems de la comunicació.

Nessus

Nessus és un conegut programa d'escaneig de vulnerabilitats. Escaneja els ports i prova exploits per atacar el sistema que s'està escanejant.

Fase 3: obtenció de l'accés

Aquesta és la fase en la qual es duu a terme l'atac de manera efectiva, aprofitant les vulnerabilitats localitzades a la fase anterior.

Sovint, aquesta fase es desenvolupa atacant, des de la xarxa, l'equip objectiu, però poden haver-hi parts de l'atac que s'efectuïn localment, en el sistema de l'atacant (per exemple, el trencament d'un fitxer de contrasenyes).

La realització d'un atac no sempre requereix coneixements elevats: Internet proveeix molta informació i *exploits*, que es poden, malauradament, emprar sense necessitat de saber programar o de tenir grans coneixements informàtics. Òbviament, les mesures de seguretat de què disposi l'equip objectiu són essencials per evitar l'èxit dels atacants. Si hom té un sistema molt assegurat i actualitzat, la informació d'ús comú a la xarxa serà clarament insuficient per perpetrar una intrusió amb èxit.

Fase 4: manteniment de l'accés

Una vegada l'intrús ha obtingut l'accés al sistema, intentarà preservar la possibilitat d'efectuar nous accessos en el futur. En aquesta tasca l'ajudaran diversos programes de codi maliciós, com els cavalls de Troia i els *rootkits*. No és només la possibilitat de causar danys evidents al sistema (esborrat de fitxers, per exemple) el que ens ha d'inquietar; l'atac també pot servir per instal·lar *malware* que monitori les accions que estem fent (*keylogger*), per capturar tot el trànsit de la xarxa (*sniffing*), instal·lar un FTP de contingut il·lícit o utilitzar el sistema atacat com a plataforma per atacar altres sistemes informàtics.

Una xarxa de zombis

Una xarxa de zombis o botnet està formada per un grup d'ordinadors (fins i tot milers) connectats a la xarxa, infectats per codi maliciós que permet el seu control remot per part d'un atacant o grup d'atacants. Les botnets poden ésser emprades per realitzar accions sense l'autorització dels propietaris de les màquines infectades, com ara atacs massius sobre altres sistemes informàtics (atacs de denegació de servei distribuït o DDoS).

Rootkits

Els *rootkits* (terme que prové d'unir la paraula anglesa root, que és el nom assignat a Unix al compte de màxims privilegis i kit que significa conjunt d'eines o programes) són eines informàtiques emprades normalment amb finalitats malicioses (com l'obtenció d'informació) que permeten l'accés il·lícit al sistema per part d'un atacant remot. Fan servir tècniques per ocultar la seva presència i la d'altres processos que puguin estar realitzant accions malicioses sobre el sistema. Els *rootkits* són molt perillosos, perquè cedeixen el control del sistema a l'atacant remot.

Fase 5: esborrat de les empremtes

És vital per a l'intrús esborrar les empremtes del que ha fet en el sistema. Moltes de les accions que ha dut a terme segurament hauran quedat, amb independència del sistema operatiu emprat, enregistrades en fitxers de registre (*log*). Alguns d'ells són fàcilment editables, però d'altres no ho són tant, ja que no són fitxers de text. En definitiva, el que intentarà l'intrús és eliminar totes aquestes entrades del fitxers de *log* i registres d'alarmes de les eines de detecció d'intrusos (IDS) amb la finalitat que els administradors del sistema no puguin descobrir que algú s'hi ha introduït de manera no autoritzada.

Els **detectors d'intrusos** o IDS s'expliquen amb més detall en l'apartat "Intents de penetració. Detecció d'intrusos" d'aquesta mateixa unitat formativa.

1.1.3 Anàlisi de programari maliciós

Per *programari maliciós* s'entén qualsevol programa que pugui tenir efectes perniciosos en el sistema informàtic que l'allotja. El seu nom anglès, *malware*, prové de la contracció de *malicious software*. Els virus, cucs i cavalls de Troia són exemples típics de programari maliciós.

Sovint, el codi maliciós s'insereix dins d'un programa "autoritzat" i executa una sèrie d'accions desconegudes per l'usuari, les quals actuen normalment en detriment seu. El codi maliciós pot estar ocult i provocar tota mena de danys com, per exemple, l'esborrament de dades o l'enviament d'informació confidencial de l'usuari per correu electrònic. En altres ocasions, el codi maliciós no s'insereix dins d'un programa autoritzat, sinó que es presenta com un nou programa que desenvolupa alguna funció útil. L'usuari l'executa, esperant que implementi aquesta funció, però el programa, en canvi, duu a terme accions desconegudes i normalment pernicioses per a l'usuari.

Amenaces lògiques

El codi maliciós, en totes les seves múltiples variants, es pot enquadrar dins el que s'anomenen amenaces lògiques.

Si bé s'ha de retrocedir fins a l'any 1972 per trobar el que s'ha considerat el primer virus de la història (anomenat Creeper, infectava màquines de l'Arpanet, xarxa antecedent de l'actual Internet), no va ser fins a la dècada dels anys vuitanta que es van començar a desenvolupar i a convertir en un greu problema de seguretat.

Fins a l'any 2005, el codi maliciós es va estendre per la xarxa sobretot en forma de virus, cucs i cavalls de Troia. El seu objectiu era, simplement, causar danys o aportar als seus creadors un cert reconeixement públic. No obstant això, a partir d'aquell moment, apareix un nou objectiu: guanyar diners. Així, els cavalls de Troia sovint persegueixen la captura de les dades bancàries de les operacions efectuades en els ordinadors personals infectats. A més de conceptes nous, com els programes de publicitat (*adware*) i els programes espia (*spyware*), apareix un nou tipus d'engany, la pesca electrònica (*phishing*), també centrada en l'obtenció de diners, però basada en l'enginyeria social.

Programari de publicitat

Es defineix com programari de publicitat o *adware* el programari que mostra publicitat. Per exemple, les versions de demostració d'alguns programaris poden ensenyar publicitat diversa (d'aquí ve que siguin gratuïtes o de demostració). Encara que normalment s'instal·len sense el consentiment de l'usuari, no són maliciosos.

Programa espia

Es defineix com programa espia o *spyware* el programa que recull informació sobre els hàbits dels usuaris sense el seu consentiment. Aquesta recaptació es pot dur a terme amb finalitat publicitària o bé per capturar informació personal.

Els cavalls de Troia bancaris es propaguen normalment, fins i tot en l'actualitat, per mitjà del correu electrònic (encara que es poden difondre d'altres formes, com per exemple a través de dispositius USB) i es basen en l'enginyeria social per persuadir l'usuari que executi el fitxer maliciós. Les dades capturades pel codi maliciós s'envien per correu electrònic a l'atacant, que intentarà fer-ne ús en benefici propi. Per obtenir un guany econòmic significatiu, cal que l'atacant o grup d'atacants infecti el major nombre possible de màquines, de forma completament indiscriminada. Altres codis maliciosos, però, tenen un objectiu molt més concret i específic (una determinada organització, per exemple). En aquests casos es poden arribar a dissenyar de manera específica. Això suposa un elevat cost de desenvolupament, si bé el benefici econòmic esperat pot arribar a ser molt elevat.

Pesca electrònica

La pesca electrònica o *phishing* és una estratègia d'enginyeria social, en la qual s'usa la suplantació de correus electrònics o llocs web per intentar obtenir informació confidencial de l'usuari.

El sistema operatiu que més ha patit l'atac del codi maliciós és Windows, si bé també se n'ha desenvolupat per a la resta de sistemes, no tan majoritaris com aquesta plataforma. Darrerament s'observa una clara tendència al desplaçament d'aquest problema de seguretat als terminals de telefonia mòbil, cada vegada més sofisticats i vulnerables a l'acció del codi maliciós.

Detecció del codi maliciós

A continuació estudiarem algunes de les tècniques que es poden fer servir per detectar i prevenir la presència de codi maliciós en el nostre sistema informàtic. Segons la configuració del sistema, la detecció del codi (normalment fitxers compilats) serà més o menys complicat. Per exemple, si es coneix la darrera data d'actualització del sistema i es localitza algun fitxer de sistema posterior a aquesta data, es pot pensar en la presència de codi maliciós. En aquest sentit, pot ser de molta ajuda l'observació dels paràmetres següents:

- Darrera data de modificació dels fitxers.
- Data de creació dels fitxers.
- Mida dels fitxers.

Malauradament, les dates i mides dels fitxers es poden alterar amb facilitat i, per tant, no són una font d'informació segura. Les funcions *hash* ens poden ser de molta utilitat per garantir la integritat del sistema.

Les **funcions resum o *hash*** permeten obtenir el que podríem anomenar una *empremta* única d'un fitxer o conjunt de fitxers (com un ADN del fitxer). Podeu trobar més informació a l'apartat de criptografia de la unitat "Seguretat física, lògica i legislació"

Així, l'administrador pot generar en qualsevol moment una instantània o empremta *única* del sistema informàtic fent servir funcions *hash*. Qualsevol alteració d'un fitxer, per mínima que sigui, provocarà que quan l'administrador torni a calcular la funció *hash*, obtingui un resultat diferent. L'eina més coneguda per dur a terme aquesta funció rep el nom de **Tripwire** (és una eina de font pública basada en Linux/Unix). El seu funcionament és el següent: una vegada s'ha instal·lat el sistema operatiu, s'obté un valor *hash* per a cadascun dels fitxers rellevants i s'emmagatzema en una base de dades, l'accés a la qual està protegit per contrasenya.

Quan l'administrador vol comprovar la integritat del sistema, executa Tripwire i si s'ha produït algun canvi en algun fitxer, es generarà el senyal d'avís corresponent en el fitxer de sortida de l'aplicació. El funcionament correcte d'aquest procediment només es pot garantir si la base de dades on es guarden les sortides resum no és modificable per cap usuari. Això es pot aconseguir fent que la base de dades tingui atribut de només lectura, o emmagatzemant-la en un suport que no admeti reescriptures com, per exemple, un DVD.

Amb eines com Tripwire es poden detectar els fitxers de sistema als quals s'ha inserit codi maliciós, és a dir que es pot garantir la integritat dels fitxers del sistema, però no ens permet analitzar en línia la presència de programari maliciós, ni ens permet fer una anàlisi, per exemple, dels programes que ens descarreguem d'Internet. Per a aquest tipus d'anàlisis caldrà recórrer als antivirus.

Els **antivirus** són objecte d'estudi a l'apartat "Eines pal·liatives" d'aquesta mateixa unitat.

Anàlisi del codi maliciós

Un dels problemes més greus que podem trobar a l'hora d'analitzar un determinat *malware* és la possibilitat que la mateixa anàlisi impliqui la infecció d'altres equips a través de la xarxa. A grans trets, es realitza preparant l'entorn, recollint la informació i finalment analitzant i documentant el que s'ha recollit.

Preparació d'un medi d'anàlisi controlat

Així, doncs, abans d'iniciar l'anàlisi és important disposar dels mitjans que ens permetin veure quines accions realitza el codi maliciós sense possibilitat d'afectar cap altre equip. Per aquest motiu, procurarem que la màquina amb la qual hem de provar el presumpte codi maliciós estigui desconnectada de la nostra xarxa de treball habitual. No cal disposar d'ordinadors específics i construir una xarxa dedicada a l'anàlisi, ja que, sortosament, els programes de virtualització ens permeten crear un laboratori de màquines i xarxes virtuals sense gaire dificultat i amb un alt grau de control. No obstant això, si disposem dels recursos suficients, sempre podem definir una xarxa específica i aïllada de la resta d'ordinadors.

Cal, doncs, definir dues o més màquines virtuals, en xarxa, amb una instal·lació bàsica de sistema operatiu, una de les quals, la que actua de màquina atacada, allotja el presumpte codi maliciós. A més, han de tenir instal·lades diverses eines que ens permetran analitzar què està passant quan s'activi el codi maliciós. Per exemple, un programa de monitoratge de trànsit de xarxa, com ara **Wireshark**, pot ser de molta utilitat.

Els dos programes de virtualització d'ús més freqüent són VMWare i VirtualBox.

Abans d'iniciar l'anàlisi, també és interessant recollir certes dades del sistema, prèvies a la infecció, com ara quins són els ports oberts, els processos en execució, usuaris i grups definits, quins són els recursos compartits...

Eines com Sysinternals o ***nmap*** ens poden ajudar en aquesta tasca.

Recollida d'informació

Una vegada s'ha executat el *malware*, s'efectua una nova recollida d'informació, adreçada a l'estudi del codi maliciós i als efectes que provoca.

- **Recollida estàtica**. Relacionada directament amb el codi malicós objecte d'estudi: nom del fitxer, versió, com és la interfície gràfica (si és que en té)...

- **Recollida dinàmica**. Es basa en els efectes que produeix el codi maliciós: anàlisi del trànsit de xarxa, processos en execució, canvis en el sistema de fitxers...

Anàlisi i documentació de la informació

Totes les proves efectuades s'han d'analitzar (tinguem present que hi pot haver un volum d'informació molt gran) i documentar amb la finalitat que els resultats obtinguts serveixen per prevenir atacs de *malware* com l'estudiat o semblant.

Aquesta metodologia, centrada en l'estudi en un medi controlat, no és el que habitualment ens trobarem. L'escenari habitual és un sistema informàtic que, de vegades, ni tan sols sabrem si es troba o no infectat, tot i que una sèrie d'indicis ens ho fan pensar. No obstant això, la metodologia explicada també resulta de molta utilitat en aquests casos.

1.2 Eines preventives

Per *eines preventives* entenem totes aquelles eines i mecanismes que ens ajudin a reforçar la seguretat i a detectar febleses en el nostre sistema.

1.2.1 Instal·lació i configuració

Els danys que es poden produir en el cas d'un atac poden ser desastrosos. Així doncs, és necessari instal·lar eines i configurar mecanismes amb l'objectiu de minimitzar els atacs reeixits. Aquests mecanismes i eines poden anar orientats a l'usuari, a l'equip o al sistema informàtic.

Polítiques de seguretat de contrasenyes

Quan hem de triar una contrasenya per a un compte d'usuari, sovint la definim de la forma més òbvia i senzilla de recordar per nosaltres. Hem de tenir en compte, però, que en fer-ho així, podem comprometre la seguretat del sistema informàtic. Per definir correctament una contrasenya, hauríem de prendre les precaucions següents:

- Memoritzar-la i no portar-la escrita.
- Canviar-la periòdicament (amb caràcter mensual, per exemple).
- No repetir la mateixa contrasenya en comptes diferents.
- No llençar documents amb contrasenyes a la paperera.
- Evitar utilitzar paraules de diccionari. Hi ha tècniques de descobriment de contrasenyes basades en la comparació amb diccionaris sencers de paraules, per idiomes, de temes concrets com esports... Aquestes tècniques reben el nom d'**atacs de diccionari**.
- Evitar utilitzar dades que puguin ser conegudes per altres persones (per exemple, nom i cognom de l'usuari, repetir el mateix nom que l'identificador, el DNI, la data de naixement, el número de mòbil...).
- Fer servir contrasenyes d'un mínim de vuit caràcters.
- Evitar la reutilització de contrasenyes antigues.
- No utilitzar contrasenyes exclusivament numèriques.
- Afavorir l'aparició de caràcters especials (!, *, ?, ...).
- No enviar contrasenyes per SMS o correu, ni dir-les per telèfon.

- No utilitzar seqüències de teclat del tipus “qwerty” o “1234” (són seqüències que s’assagen en els atacs de diccionari).
- Fer servir regles mnemotècniques per recordar les contrasenyes (per exemple, “Cada dia al matí canta el gall quiquiriquic” donaria lloc a la contrasenya “CDAMCEGK”).

A més d’aquestes recomanacions sobre la tria de les contrasenyes, també és important disposar d’eines que en permetin el control.

Per exemple, mitjançant **eines de comprovació proactiva** es pot evitar que una mala contrasenya entri a formar part de la base de dades de contrasenyes del sistema. Així, si un usuari tria una contrasenya que apareix en el filtre de l’eina (és a dir que es tracta d’una mala contrasenya) serà rebutjada automàticament.

Un exemple d’eina de comprovació proactiva és `npasswd`, substitut de l’ordre `passwd` en entorns Linux/Unix.

En general, aquestes eines poden permetre, per exemple:

- Registrar totes les sessions i els errors que s’han produït (normalment existeix un límit al nombre d’intents que es poden fer).
- Especificar regles diverses: les contrasenyes han de tenir un nombre mínim de caràcters, no poden consistir en la mateixa contrasenya però a l’inrevés, no poden ser exclusivament numèriques...
- Enviar un missatge a l’usuari que intenti crear una contrasenya feble, segons les regles que s’han definit.

Contrasenya del BIOS i diferents nivells de contrasenyes

Les contrasenyes no apareixen només en els inicis de sessió; les podem trobar en diferents nivells del sistema informàtic, començant per el BIOS.

BIOS

El sistema bàsic d’entrada/sortida o BIOS (*Basic Input-Output System*) és un programa emmagatzemat en un xip ROM que s’ocupa, en el moment en què l’ordinador s’inicia, de carregar el sistema operatiu en la memòria de l’ordinador i de comprovar els dispositius que té connectats.

La utilització de contrasenyes del BIOS en els ordinadors és un aspecte que sovint es descuida, tot i que, si no la posem, l’intrús podria modificar la configuració d’arrencada, de manera que l’ordinador s’iniciés des d’un dispositiu USB, un CD o un DVD. D’aquesta manera, l’intrús podria robar informació, eliminar-la o introduir qualsevol codi maliciós al sistema.

Els nivells en els quals situar un mecanisme d’autenticació en una estació de treball són: BIOS, sector d’arrencada de l’equip, sistema operatiu o, fins i tot, sol·licitat per un programa.

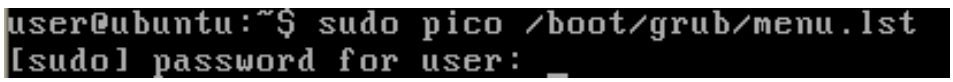
A més del BIOS, també és necessari afegir contrasenyes als gestors d’arrencada, com per exemple GRUB. Així podem evitar que els intrusos puguin modificar les opcions d’inici dels diferents sistemes operatius que controla el gestor.

Debilitats en BIOS

Notem que el BIOS es pot reconfigurar mitjançant els ponts (*jumpers*) allotjats a la placa base, o desconnectant la bateria CMOS (petita memòria que conté la informació de la configuració del sistema i que necessita una bateria per conservar-la). Per tant, si no protegim l’apertura de la carcassa de l’ordinador, un intrús, si té accés físic a l’ordinador, pot saltar-se fàcilment la contrasenya del BIOS.

A la figura **??** i la figura 1.7 s’observa com editant el fitxer menu.lst podem introduir una contrasenya en el GRUB (per a més seguretat, cal xifrar aquesta contrasenya). A més, és possible definir una contrasenya per cadascun dels sistemes operatius que controli el gestor.

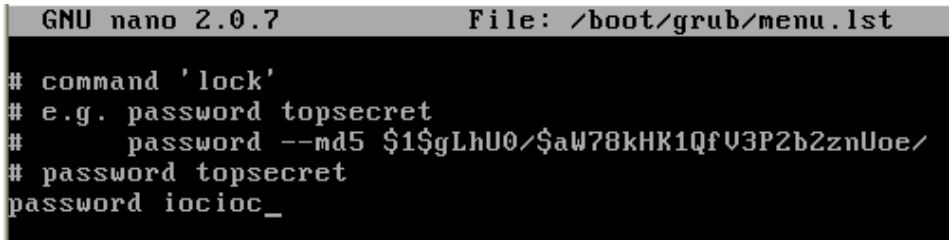
Figura 1.6. Edició del fitxer menu.lst



GNU GRUB

El GNU GRUB (*Grand Unifier Bootloader*) és un gestor d'arrencada per a entorns Linux que s'usa per iniciar un o més sistemes operatius instal·lats en el mateix equip (per exemple, Linux i Windows).

FIGURA 1.7. Definició de la contrasenya "iocioc" dins del fitxer menu.lst



Definició de polítiques d'usuaris i grups

La definició dels permisos dels usuaris (és a dir, la determinació de les tasques i accions que poden dur a terme en un sistema informàtic) és una excel·lent mesura preventiva que evita que els usuaris no puguin fer més que allò que necessiten per a la seva feina.

En termes generals, l'administrador desenvolupa aquesta tasca de definició en quatre nivells:

1. En primer lloc, crea i gestiona i els comptes de usuari (individuals).

2. A continuació defineix els grups d'usuaris segons les similituds de les tasques que han de dur a terme i en funció de les seves necessitats d'accés. Un usuari pot pertànyer a més d'un grup.

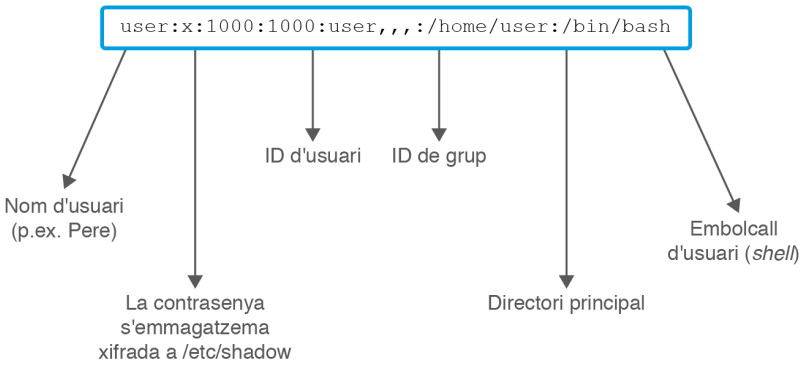
3. Una vegada definits els grups, l'administrador assigna els drets sobre fitxers i directoris (per exemple, podem fer que tots els membres d'un grup anomenat Professors, tinguin permís de lectura i escriptura sobre un directori anomenat Examen).

4. Finalment, es poden acabar de perfilar els drets individuals de cadascun dels usuaris, ja que dins d'un mateix grup, poden haver-hi necessitats diferents.

Tot seguit, i a tall d'exemple, veurem molt breument com dur a terme aquestes operacions en el sistema operatiu Linux/Unix.

- **Definició d'usuaris**. Cada entrada del fitxer /etc/passwd (figura 1.8) conté informació del compte d'un usuari. Entre altres dades, conté el nom d'usuari, el grup primari al qual pertany i el seu directori principal. Les contrasenyes, normalment, no s'emmagatzemen en aquest fitxer, sinó que es troben xifrades en un altre fitxer anomenat /etc/shadow. Per afegir nous usuaris es pot emprar, com a usuari administrador, l'ordre `useradd nom_usuari` (o ***adduser***).

FIGURA 1.8. Descripció dels camps d'una entrada del fitxer /etc/passwd



- **Definició de grups**. La gestió dels grups es realitza de manera similar a la dels usuaris. Les dades dels grups s'emmagatzemen en el fitxer /etc/group, l'estructura del qual és similar a la d'/etc/passwd. Cada línia o entrada del fitxer conté, entre altra informació, el nom del grup, l'identificador del grup (*group ID*) i la llista d'usuaris que en són membres. Per afegir un nou membre, n'hi ha prou d'editar el fitxer /etc/group/ i afegir el nou membre al final de la llista. En cas que hi hagi ocultació de dades, hi haurà un equivalent al fitxer /etc/shadow anomenat /etc/gshadow. De forma similar a la creació de nous usuaris, l'ordre `groupadd nom_usuari` (o addgroup) permet la definició d'un nou grup.

Els fitxers /etc/shadow i /etc/gshadow només són accessibles per l'usuari arrel.

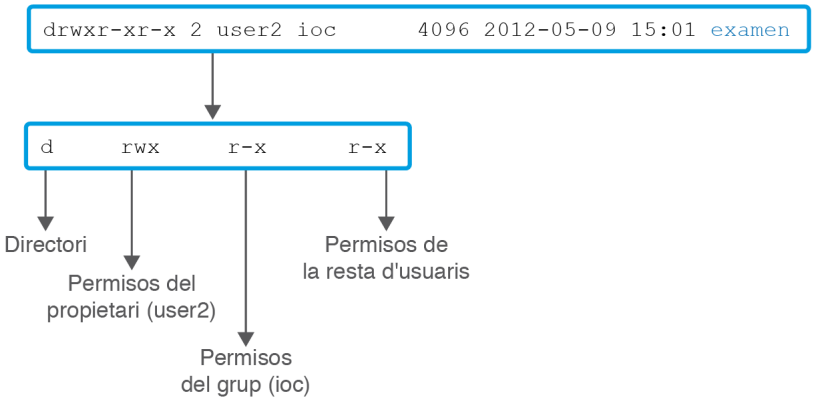
- Ens queda però, veure com ho podem fer perquè un fitxer o un directori **canviï de propietari**. Perquè canviï d'usuari es pot emprar l'ordre `chown nom_usuari nom_fitxer`. De manera similar, amb l'ordre `chgrp nom_usuari nom_fitxer` podem definir que un grup sigui propietari d'un fitxer o directori. A la figura 1.9 podem comprovar que el grup propietari del directori *Examen* després d'executar `chgrp` passa a ser ioc.

FIGURA 1.9. Execució de la instrucció chgrp ioc examen

```
root@ubuntu:/home/user# ls -l
total 22848
drwxr-xr-x 2 user2 root     4096 2012-05-09 15:01 examen
-rw-r--r-- 1 root  root   420935 2011-04-15 04:02 hash_www
-rw-r--r-- 1 root  root   420994 2011-04-15 04:04 hash_www2
-rw-r--r-- 1 user  user  4763163 2009-07-01 00:14 Joomla_1.5.12-Stable-Full_Pack
age.tar.gz
-rw-r--r-- 1 root  root  5051955 2012-04-24 17:19 mac_fls.txt
-rw-r--r-- 1 root  root 12673318 2012-04-24 17:20 timeline.csv
root@ubuntu:/home/user# chgrp ioc examen
root@ubuntu:/home/user# ls -l
total 22848
drwxr-xr-x 2 user2 ioc      4096 2012-05-09 15:01 examen
-rw-r--r-- 1 root  root   420935 2011-04-15 04:02 hash_www
-rw-r--r-- 1 root  root   420994 2011-04-15 04:04 hash_www2
-rw-r--r-- 1 user  user  4763163 2009-07-01 00:14 Joomla_1.5.12-Stable-Full_Pack
age.tar.gz
-rw-r--r-- 1 root  root  5051955 2012-04-24 17:19 mac_fls.txt
-rw-r--r-- 1 root  root 12673318 2012-04-24 17:20 timeline.csv
root@ubuntu:/home/user# _
```

- A Linux/Unix, l'accés del usuaris i grups als fitxers i directoris es determina mitjançant permisos. Hi ha tres tipus de permisos: accés de lectura (r), accés d'escriptura (w) i accés d'execució (x). Així, si observem els atributs del directori *Examen* a la figura 1.9 veurem el que es mostra a la figura 1.10.

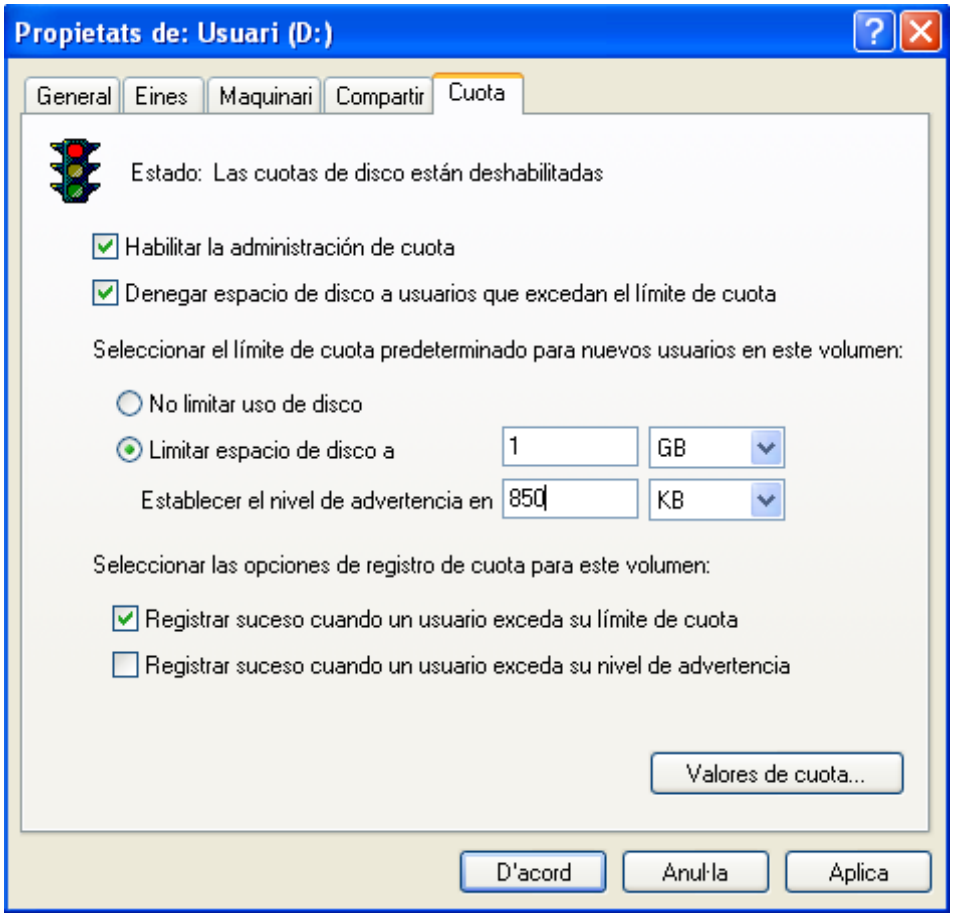
FIGURA 1.10. Permisos del directori Examen



Per executar segons quines ordres ens cal disposar de permisos d'usuari supervisor.

A més, per millorar la seguretat dels fitxers i directoris, es poden emprar les anomenades **llistes de control d'accés** (ACL), amb les quals es poden individualitzar els privilegis que té un usuari sobre un determinat fitxer, sense tenir en compte el grup al qual pertany.

FIGURA 1.11. Assignació d'espai de quota sobre una partició anomenada Usuari



Encara que la captura de pantalla correspon a un Windows XP amb el pedaç de català instal·lat, observem que hi ha parts de la interfície que no estan en català, com la corresponent a la imatge.

Finalment, també és habitual assignar una **quota de disc dur** als usuaris, de manera que no puguin ocupar indiscriminadament tot l'espai de disc dur. Per

exemple, en el sistema operatiu Windows XP podem activar la quota de disc des de les propietats de la partició (ha d'estar en format NTFS) sobre la qual volem definir les quotes d'usuari. En la figura 1.11 podem veure les opcions que tenim per gestionar la quota i denegar l'espai de disc als usuaris que hagin excedit la seva quota. En aquest cas establiríem una quota idèntica per a tots els usuaris, però emprant l'opció *Valors de quota* podríem personalitzar el límit de cadascun dels usuaris. Com podem veure a la imatge, també existeix l'opció d'enregistrar els esdeveniments que excedeixin la capacitat de quota. Després es podran consultar amb el visor d'esdeveniments. En el cas de *windows* és el gestor de consola eventvwr.msc.

En els sistemes Linux es poden establir quotes d'usuari amb l'eina de configuració de sistema **Webmin**.

Ús de tècniques criptogràfiques

La utilització de la criptografia, tant pel que fa a la informació emmagatzemada (per exemple, creant una partició xifrada) com a la informació circulant (per exemple, usant SSH o Telnet segur), permet mantenir la confidencialitat de les dades i impedeix que puguin ser interceptades per intrusos.

A l'annex d'aquesta unitat trobareu un tutorial del programa de criptografia TrueCrypt.

1.3 Eines pal·liatives

Per *eines pal·liatives* entenem aquelles eines i mecanismes que bloquegen els intents de trencar la seguretat de l'equip i eviten els danys provocats pel codi maliciós.

Hi ha moltes eines i mecanismes que pertanyen alhora a la categoria d'eines preventives i a la d'eines pal·liatives.

1.3.1 Instal·lació i configuració

Tal com passa amb els eines preventives, les eines i mecanismes pal·liatius poden anar orientats a l'usuari, a l'equip o al sistema informàtic.

Antivirus

Arran de la proliferació experimentada pels virus informàtics durant la dècada dels vuitanta, van aparèixer els anomenats *antivirus*, és a dir, programes que tenen com a objectiu detectar i eliminar els virus.

Antivirus i codi maliciós

El codi maliciós, en totes les seves variants, es pot enquadrar dins del que s'anomenen amenaces lògiques, els elements més representatius de les quals són els virus, els cucs i els cavalls de Troia.

En l'actualitat, els programes antivirus poden detectar, blocar i eliminar els virus informàtics que trobin, però, a més poden reconèixer altres codis maliciosos.

Els antivirus tenen una part resident en la memòria de l'equip que els permet comprovar en temps real els fitxers que s'executen, creen o modifiquen. També poden revisar, per exemple, els elements adjunts als correus electrònics, així com els scripts o guions que s'executen des dels navegadors web. Per aquest

motiu, els antivirus alenteixen l'arrencada i el funcionament normal del sistema, ja que consumeixen molts recursos per realitzar aquestes comprovacions i mantenir actualitzada la **base de dades de firmes** (patrons binaris que s'utilitzen per identificar possibles virus). No obstant això, òbviament, és molt recomanable, sinó imprescindible, tenir un antivirus instal·lat en el nostre sistema informàtic.

Les tècniques que utilitzen els antivirus per reconèixer nous virus que no apareixen a la seva base de dades s'anomenen **heurístiques**.

Sovint, els creadors dels virus realitzen modificacions dels virus originals per tal de dificultar-ne la detecció. Malgrat això, els antivirus són capaços de reconèixer la firma genèrica que identifica tota la família, sense necessitat d'actualitzar la base de dades de firmes (pensem que si s'haguessin d'identificar tots els virus de forma individual, la mida de la base de dades podria ser enorme).

L'ús d'aquestes tècniques d'identificació pot comportar que es produeixin **falsos positius**, és a dir, fitxers que s'identifiquen falsament com a codi maliciós. De tota manera, el més preocupant, pel que fa a la seguretat del sistema, és que es produeixin **falsos negatius**, és a dir, fitxers que no s'han identificat com a maliciosos, però que ho són.

De vegades, l'antivirus no està instal·lat al sistema, sinó que hi accedeix mitjançant un navegador d'Internet (**antivirus en línia**). En aquest cas, ja que hi accedeix directament al fabricant, la base de dades de firmes sempre està actualitzada. D'altra banda, el fet de treballar via web, fa que no calgui instal·lar el programa i que puguem provar fàcilment antivirus de diferents fabricants. No obstant això, cal tenir en compte que no ofereixen una protecció permanent, a diferència dels **antivirus fora de línia**, els instal·lats en l'equip informàtic. Els antivirus en línia es poden considerar un complement dels fora de línia, si bé no són tan fiables com aquests.

A més de la solució en línia hi ha altres formes d'usar un antivirus sense necessitat d'instal·lar-lo en el sistema. Hi ha antivirus portables (als quals podem accedir, per exemple, des d'un dispositiu USB), i fins i tot **CD autònoms** o *live CD* (és a dir, un CD des de qual podem iniciar el sistema) amb antivirus inclosos, opció molt interessant, ja que evita iniciar el sistema operatiu de la màquina i eludeix, per tant, les tècniques d'ocultació que utilitzen alguns codis maliciosos.

Programes antiespia

A més dels antivirus, existeixen solucions específiques per a la detecció i desinfecció de programes espia i codi maliciós en general, que es poden combinar amb l'antivirus i el tallafoc que fem servir habitualment.

L'objectiu dels programes espia és capturar informació del sistema infectat, bé per conèixer els hàbits de navegació de l'usuari o bé per apropiar-se de la seva informació personal (dades bancàries, per exemple). En qualsevol cas, la instal·lació d'aquest tipus de codi maliciós sempre es fa sense el consentiment de l'usuari afectat. Precisament a causa del seu objectiu de captació, aquest tipus de codi maliciós es troba contínuament en funcionament i pot arribar a alentir considerablement el funcionament del sistema informàtic.

La difusió de l'*spyware* es pot realitzar de moltes maneres. Tenim tendència a pensar que, si no executem cap programari "estrany" no podem ser víctimes de cap codi maliciós. En l'actualitat però, alguns tipus de programa espia no requereixen pràcticament cap acció per part de l'usuari (per exemple, la infecció es pot produir visitant un lloc web) o bé es poden trobar ocults en programes suposadament segurs (com, per exemple, en un controlador de dispositiu).

El comportament de l'*spyware* difereix molt del dels virus i, per aquest motiu, als ulls dels antivirus, pot semblar innocu. Així, és habitual combinar solucions d'antivirus amb programes antiespia, perquè, de fet, no ataquen el mateix problema.

Per evitar l'acció dels enregistradors de teclat que solen incloure els programes espia, s'han desenvolupat teclats virtuals (per exemple, solen aparèixer als web de les entitats bancàries) que eviten que l'usuari hagi d'usar el teclat a l'hora d'introduir dades. Com podem veure a la figura 1.12, els teclats virtuals són teclats gràfics en els quals els usuaris poden seleccionar les lletres amb un clic del ratolí en lloc de prémer una tecla. No obstant això, alguns *keyloggers* poden capturar la pantalla a cada clic, per la qual cosa els teclats virtuals tampoc es poden considerar completament segurs. Per evitar aquest problema, alguns teclats virtuals introdueixen el caràcter quan el ratolí es mou, durant uns segons, sobre la lletra en qüestió, en lloc d'introduir-la amb un clic.

Figura 1.12. Aparença d'un teclat virtual

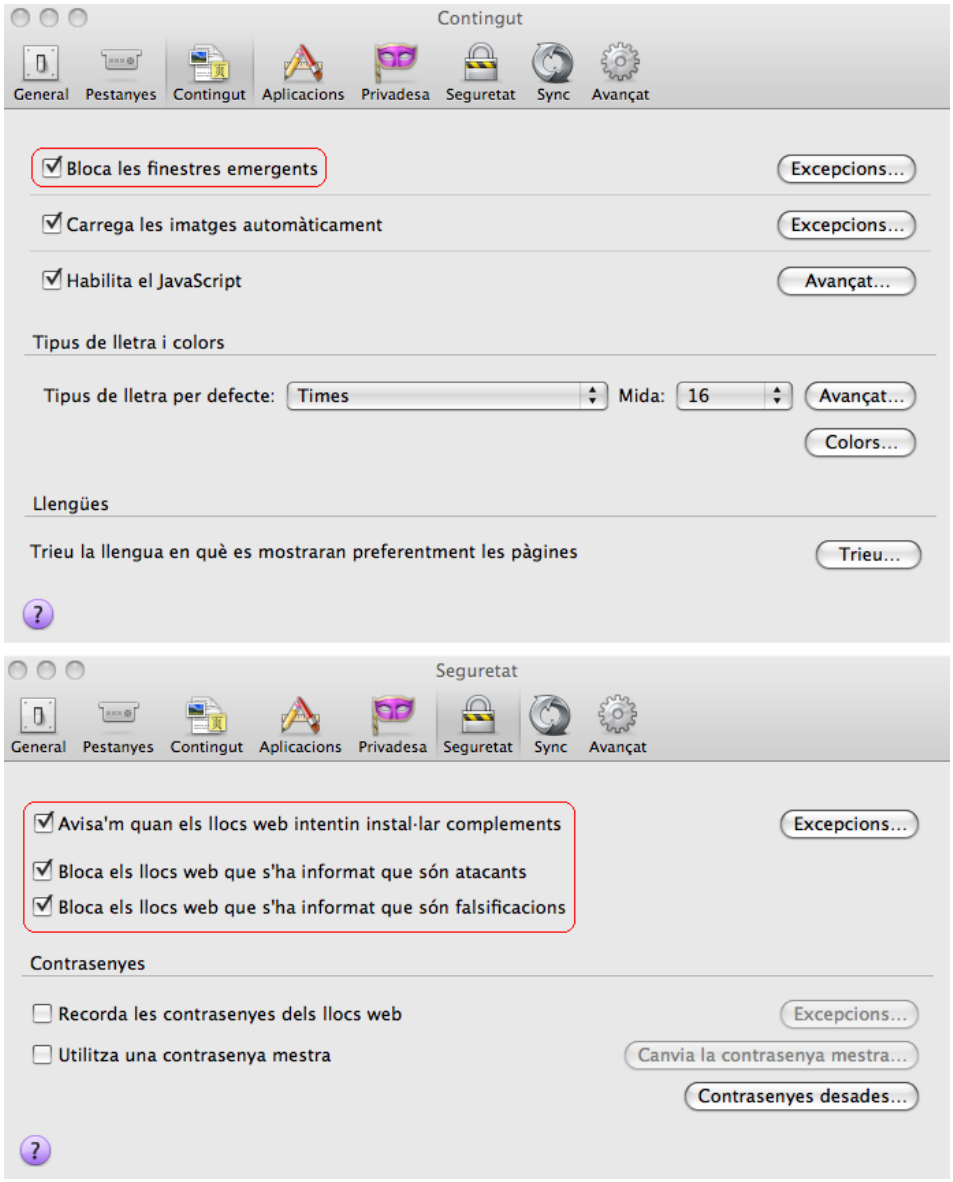
Finalment, com es pot imaginar, no hi ha cap eina que pugui garantir que un sistema informàtic estigui completament lliure de codi maliciós, de manera que el fet que no s'hagi pogut detectar no vol dir que no hi sigui. En tot cas, és essencial que totes les eines pal·liatives tinguin les seves bases de dades actualitzades i que el sistema operatiu i els programaris estiguin actualitzats amb els darrers pedaços publicats.

Eines de bloqueig web

Com s'acaba de veure, la simple navegació web pot comprometre la seguretat d'un sistema informàtic. Per aquest motiu és important que puguem bloquejar els llocs webs que puguin suposar una amenaça per a la seguretat.

De fet, molts navegadors d'Internet es poden configurar perquè bloquin les finestres emergents (filtres *pop-up*) o evitin els adreçaments a llocs de *phishing* (filtres *antiphishing*). Per exemple, a la figura 1.13 podem veure les pestanyes de configuració del navegador Firefox, on podem definir aquests bloquejos (entre d'altres opcions).

FIGURA 1.13. Pestanyes de configuració del navegador Firefox



A més dels navegadors, els antivirus també tenen opcions de bloqueig dels llocs d'Internet que consideren perillosos.

1.4 Actualització de sistemes i aplicacions

L'actualització de sistemes i aplicacions és una faceta sovint poc atesa. Com qualsevol programa d'ordinador, el sistema operatiu i les aplicacions tenen errors

o omissions que poden plantejar problemes de seguretat. En el cas del sistema operatiu és especialment important, ja que és la base a partir de la qual permet el funcionament de la resta de programes instal·lats a l'equip.

1.4.1 Per què cal actualitzar el sistema operatiu i les aplicacions?

Les actualitzacions de sistemes operatius i aplicacions tenen les motivacions següents:

- Corregir les vulnerabilitats detectades. Els intrusos solen aprofitar les vulnerabilitats (tant dels sistemes operatius, com de les aplicacions) per accedir sense autorització al sistema. Per tant, és essencial que les actualitzacions s'instal·lin el més aviat possible per intentar tancar les escletxes de seguretat provocades per aquestes vulnerabilitats. De vegades, encara que no hi hagi ningú dirigint un atac, l'usuari pot executar un programa maliciós que, aprofitant una vulnerabilitat, causi algun dany al sistema. Per tant, com en el cas de l'atac premeditat, convé tenir el sistema operatiu i les aplicacions sempre al dia, amb les darreres actualitzacions publicades.

Un ***exploit 0-day*** implica l'existència d'una vulnerabilitat d'un programa, generalment desconeguda per la comunitat i per la qual encara no s'ha desenvolupat cap actualització. Normalment aquesta vulnerabilitat és desconeguda pel desenvolupador del programari, tot i que de vegades es coneix però no es considera perillosa, i per aquest motiu no es desenvolupa l'actualització que solucionaria el problema. Aquesta manca de resposta fa que els *exploits 0-day* es propaguin amb molta facilitat per tota la xarxa i constitueixen un greu problema de seguretat.

- Permetre la gestió del nou maquinari que, de forma periòdica, va apareixent al mercat.
- Afegir noves funcionalitats i millores a les versions anteriors. Si bé la motivació anterior és més important que aquesta, cal tenir present que les actualitzacions sovint comporten l'afegit de noves funcions i millores en relació a les antigues versions.

1.4.2 Com actualitzar?

Hem vist la importància de mantenir el sistema operatiu i les aplicacions completament actualitzades. Ara bé, com es duu a terme aquesta actualització?

Pel que fa a les aplicacions, moltes es poden configurar perquè, quan detectin l'existència d'una nova actualització a través d'Internet, preguntin a l'usuari si vol baixar-la i, en cas afirmatiu, la descarreguin automàticament.

Pel que fa a les actualitzacions del sistema operatiu, Windows té activada per defecte una opció (Windows Update) que permet descarregar de forma automàtica

les actualitzacions del sistema operatiu. L'usuari pot desactivar aquesta opció i també pot triar si les actualitzacions descarregades s'instal·len automàticament, o si vol veure primer quines són i decidir per si mateix quines vol instal·lar (en general és recomanable veure la descripció de l'actualització i no instal·lar-la per defecte).

A més d'aquesta opció d'actualització individual (per a cada equip), els administradors poden gestionar de forma centralitzada la distribució de les actualitzacions a tota la xarxa mitjançant l'anomenat Windows Server Update Services (WSUS). Amb aquest servei s'aconsegueix que les descàrregues es realitzin des del servidor central i evitar així que cada equip s'hagi de connectar individualment al web de Microsoft.

El sistema operatiu Linux (per exemple, en la distribució Ubuntu) té un gestor d'actualitzacions que funciona de manera similar al de Windows. Com en aquest sistema, permet veure la descripció de les actualitzacions i decidir quines volem instal·lar. També podem comprovar en qualsevol moment si hi ha cap actualització pendent.

També es pot comprovar l'existència d'actualitzacions i ordenar-ne la instal·lació des de la línia d'ordre:

```
1 sudo apt-get update && sudo apt-get upgrade
```

Així mateix, amb l'ordre ***apt-get*** (o ***aptitude***), executada com a usuari arrel, podem instal·lar nous paquets. Per exemple, amb l'ordre següent instal·laríem el conjunt d'eines The Sleuth Kit, molt emprat en informàtica forense:

```
1 apt-get install sleuthkit
```

Continuant amb l'exemple d'Ubuntu, també podem afegir o eliminar aplicacions mitjançant un entorn gràfic, en lloc de fer-ho des de línia d'ordres, emprant el gestor de paquets Synaptic.

1.5 Seguretat en la xarxa corporativa

La seguretat de la xarxa inclou totes les eines i polítiques adoptades per l'administrador del sistema per prevenir i controlar l'accés no autoritzat, mal ús, modificació o inhabilitació d'una xarxa informàtica i els seus recursos.

1.5.1 Monitoratge del trànsit de xarxes

El monitoratge de la xarxa consisteix a supervisar i analitzar el trànsit que hi circula per tal de detectar els incidents de seguretat que s'hi puguin produir, així com per mantenir la qualitat del servei dins dels llindars previstos.

El monitoratge es pot dur a terme amb dues aproximacions diferents, complementàries i no excloents:

- **Monitoratge passiu:** es basa en l'escolta i anàlisi del trànsit real de la xarxa. A diferència de l'aproximació activa, en aquesta no s'injecta trànsit a la xarxa, només es recull la informació i s'analitza. En aquesta aproximació s'usen els anomenats *detectors* o *sniffers*, que es poden trobar en diverses ubicacions com ara encaminadors, commutadors. Amb aquestes tècniques es pot caracteritzar el trànsit de xarxa i veure quin ús se'n fa.
- **Monitoratge actiu:** l'aproximació activa consisteix a injectar paquets de prova a la xarxa, o enviar-ne als servidors i aplicacions, i a mesurar el temps de resposta obtingut. Es pot emprar per supervisar el rendiment de la xarxa, encara que, mitjançant eines actives com els escàners també es poden detectar vulnerabilitats. A diferència de l'aproximació passiva, en el monitoratge actiu s'afegeix trànsit a la xarxa.

Eines passives

Abans de poder emprar cap eina d'anàlisi passiva, cal instal·lar un detector per poder monitorar el trànsit de xarxa.

S'anomenen **detectors (*sniffers*)** els programes que permeten la captura i l'enregistrament de la informació que circula per una xarxa.

El seu funcionament es basa en l'activació del mode promiscu de les interfícies de xarxa (la interfície escolta tot el tràfic de la xarxa enlloc d'estar atenta només a les dades que li envien) de les estacions de treball. Amb l'activació d'aquest mode, l'estació de treball podrà monitorar, a més dels paquets d'informació que s'hi adrecen d'una manera explícita, el trànsit sencer de la xarxa. Això inclou, per exemple, la captura de noms d'usuari i contrasenyes (en cas que circulin en text clar, sense xifrar), o fins i tot la intercepció de correus electrònics o de qualsevol altre document confidencial.

L'ús dels detectors com a eines de supervisió de la xarxa és perfectament lícit, però la captura d'informació personal és una activitat clarament il·lícita.

Si bé els detectors es poden emprar com a eines de supervisió (comptabilització del trànsit, identificació d'aplicacions...) per l'administrador de la xarxa, també poden ser emprats maliciosament amb altres finalitats. L'activitat dels detectors és difícilment detectable perquè no deixen empremtes. No podem tenir constància de la informació que pot haver estat interceptada pels detectors (si no és de manera indirecta, per mitjà dels atacs que pot patir el sistema informàtic). Això sí, com que no hi ha cap raó, normalment, perquè una targeta estigui treballant en mode promiscu, una manera d'esbrinar si hi ha detectors és cercar la presència de targetes en mode promiscu. Això es pot fer amb diverses eines: ***ifconfig***, ***ifstatus*** o Network Promiscous Ethernet Detector (NEPED)...

El detector més conegut és **Wireshark**, conegut antigament com Ethereal.

A més de les mesures de detecció de possibles *sniffers* es poden fer servir mesures de protecció d'abast més general. Per exemple, si es xifren els documents que s'envien per la xarxa amb PGP, encara que puguin ser interceptats, molt difícilment podran ser desxifrats per l'espia. Malauradament, les eines criptogràfiques

protegeixen la informació que circula, però no permeten establir connexions segures. Per això és de vital importància la instal·lació d'altres eines com, per exemple, un servidor de *Secure Shell* (SSH) i les respectives utilitats dels clients. *Secure Shell* permet l'establiment d'inicis de sessió segurs i es pot fer servir com a substitut de l'ordre `telnet`.

Pretty Good Privacy (PGP) és un conegut programa de criptografia que empra tècniques de criptografia de clau pública i privada.

Eines actives

Les eines actives són aquelles que utilitzen la xarxa per descobrir informació a través d'enviar peticions als dispositius de xarxa com ara estacions de treball, servidors o encaminadors.

Escàners

Els escàners de **xarxa** analitzen els serveis i ports disponibles d'ordinadors remots a la recerca de debilitats conegudes que puguin aprofitar els atacants (en certa manera, doncs, automatitzen les tasques que duria a terme un intrús remot).

> Els **escàners** són eines de seguretat que serveixen per detectar les vulnerabilitats d'un sistema informàtic.

TCP i UPD

TCP és la sigla de Transmission Control Protocol, i UPD, la de User Datagram Protocol. Són els protocols que comparteixen tots els ordinadors connectats a Internet per poder-se connectar entre ells.

L'anomenat **escaneig de ports** consisteix a esbrinar els ports TCP/UDP que estan oberts en una màquina remota pertanyent a una xarxa determinada. Els ports oberts constitueixen una informació molt interessant per als possibles intrusos, ja que les vulnerabilitats dels processos que estan en funcionament poden permetre l'accés no autoritzat al sistema.

L'assignació dels ports no és arbitrària, sinó que és determinada per la Internet Assigned Numbers Authority (IANA). Aquests són alguns exemples d'assignació de ports a serveis d'Internet:

- Port TCP/UDP 20: FTP (dades)
- Port TCP/UDP 21: FTP (control)
- Port TCP/UDP 23: Telnet
- Port TCP/UDP 25: SMTP
- Port TCP/UDP 53: DNS
- Port TCP/UDP 80: HTTP
- Port TCP/UDP 110: POP3
- Port TCP/UDP 194: IRC

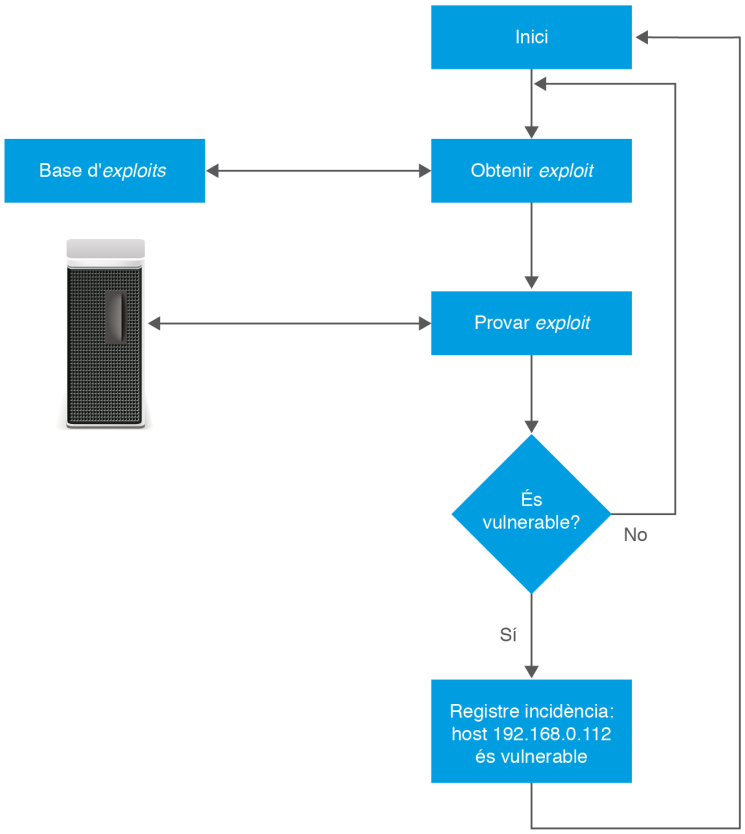
Port

Un **port** és un punt pel qual entra o surt la informació d'un ordinador. Els protocols relatius a Internet (FTP, Telnet…) utilitzen ports emissors i receptors, un port de sortida i recepció comú en els dos extrems de la comunicació.

Els ports 1024 a 65535 s'anomenen *ports registrats*, no estan sota el control de la IANA i poden ser utilitzats per determinades aplicacions. Per exemple, una aplicació client d'una eina de control remot maliciosa podria utilitzar un port d'aquest rang per realitzar les seves tasques i passar desapercebuda per l'usuari local o l'administrador del sistema.

Tots els escàners comparteixen, en trets generals, un esquema de funcionament similar, que podem veure representat en la figura 1.14.

Figura 1.14. Diagrama de flux d'un escàner de xarxa



Tot i que els escàners són eines de molta utilitat per als administradors dels sistemes informàtics, també els intrusos en poden fer un ús maliciós. Els escàners permeten l'automatització de centenars de proves per localitzar les vulnerabilitats d'un sistema. D'altra banda, no cal que l'intrús conegui amb precisió les vulnerabilitats del sistema; pot utilitzar simplement la informació que li proporciona l'escàner, sense necessitat de ser un expert informàtic.

Ordres de sistema

Per a una diagnosi ràpida de possibles errors en la comunicació, és recomanable utilitzar les ordres `ping` i `traceroute`. Amb `ping` es pot determinar si una màquina està connectada o no a la xarxa. Amb `traceroute` es pot obtenir una descripció del camí que es va seguint per arribar a una determinada màquina, de manera que en cas que una estació no respongui es pot determinar el lloc on es produeix el problema.

Al mercat hi ha moltes eines que faciliten el monitoratge de la xarxa, com per exemple MRTG (Multi Router Traffic Grapher) o el conegut Nagios.

1.5.2 Seguretat en els protocols per a comunicacions sense fil

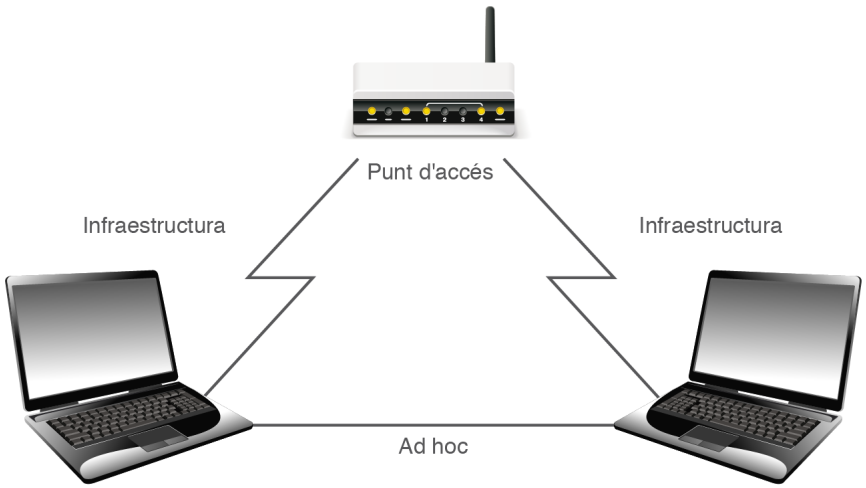
Les comunicacions sense fil, basades en ones de ràdio o infraroges, permeten connectar-se a la xarxa des de qualsevol lloc de l'organització i en qualsevol moment sense necessitat d'estendre cap cablejat, la qual cosa permet la possibilitat d'ampliar les dimensions de la xarxa amb molta facilitat.

Wi-Fi significa *wireless fidelity* (fidelitat sense fil). Les xarxes locals sense fils s'anomenen **WLAN** (*Wireless Local Area Network*).

Les xarxes locals sense fil poden operar en **mode *ad hoc*** o en **mode infraestructura**:

- **Mode ad hoc** (client a client). Totes les màquines que es troben dins de la mateixa àrea es poden comunicar entre si directament. No és habitual, encara que és pràctic, per exemple, per enviar informació entre dos ordinadors.
- **Mode infraestructura** (client a punt d'accés). Les estacions es comuniquen amb els anomenats **punts d'accés**, que actuen de repetidors i difonen la informació a la resta de la xarxa.

FIGURA 1.15. Mode d'operació de les xarxes sense fil



Com que la informació no necessita cap mitjà determinat per circular, aquestes xarxes presenten problemes de seguretat importants. Per exemple, en una configuració normal de xarxa, el tallafoc sol ser un element crític de la seguretat i reuneix una part important de les mesures de protecció als atacs exteriors. En una xarxa sense fil però, els atacants ja no necessiten passar pel tallafoc i poden atacar directament altres dispositius de xarxa. Per aquest motiu, inicialment es va preveure la utilització d'un protocol de xifratge anomenat WEP (*Wired Equivalent Protocol*), que forma part de l'especificació de la norma IEEE 802.11. Amb aquest protocol, una clau WEP predeterminada se situava en cada punt d'accés i en cada client, de manera que només als clients amb la mateixa clau se'ls permetia l'accés. No obstant això, aquest mecanisme no és segur i en l'actualitat es pot desxifrar sense massa problemes. El protocol WEP es basa en un algorisme de xifrat,

anomenat RC4, que és molt feble. Es pot desxifrar interceptant un determinat volum de paquets en circulació (per exemple, amb l'eina Aircrack).

IEEE

L'Institute of Electrical and Electronic Engineers (IEEE) és un organisme que data de l'any 1980 i que va elaborar les normes IEEE 802.X, que defineixen els estàndards de funcionament de les xarxes d'àrea local.

Arran dels problemes de seguretat provocats pel protocol WEP, es va desenvolupar un altre sistema, anomenat WPA (*Wi-Fi Protected Access*), que forma part de l'especificació IEEE 802.11 i, millora l'anterior i proveeix mecanismes d'autenticació. El WPA també utilitza l'algorisme de xifratge RC4, però presenta certes diferències en relació a WEP pel que fa a la gestió de claus.

L'especificació IEEE 802.11 i es va continuar desenvolupant fins a produir el sistema WPA2, que utilitza l'algorisme criptogràfic estàndard de clau privada AES (*Advanced Encryption Standard*) en lloc de l'RC4.

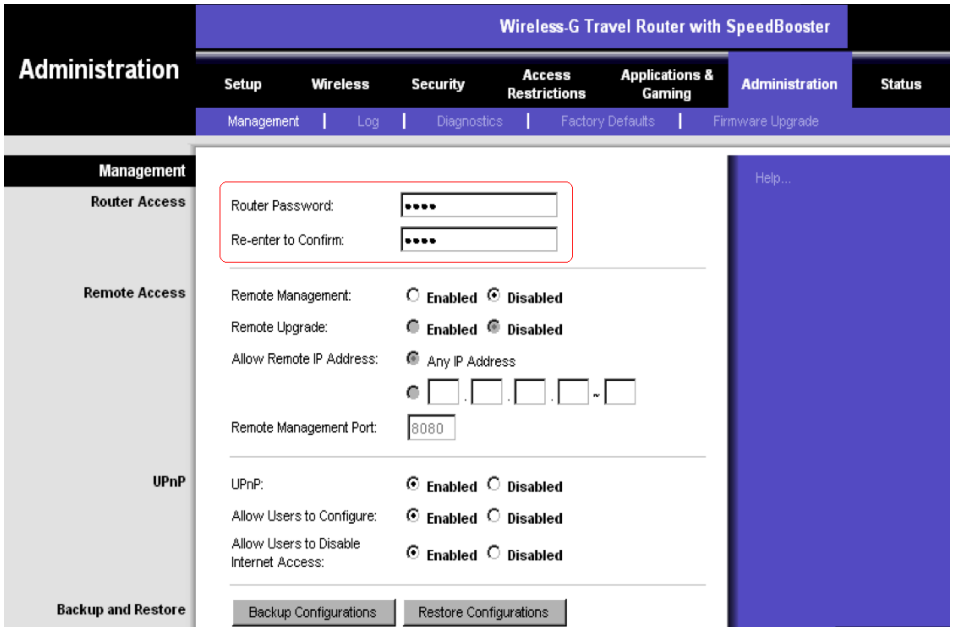
Tant el WPA com el WPA2 presenten vulnerabilitats i es poden atacar. Això és conseqüència del fet que, malgrat les millores criptogràfiques, el mecanisme d'associació d'un client a la xarxa sense fil és molt semblant, amb independència del sistema de seguretat que es triï (WEP, WPA o WPA2).

> Cal tenir present que les xarxes locals sense fil requereixen, a causa de la seva natura intrínseca, unes mesures de seguretat més grans que les que s'adoptarien en una xarxa cablejada.

Vist a grans trets el funcionament de les xarxes sense fil, passem a fer algunes recomanacions per millorar la seguretat de les WLAN:

- Canviar la contrasenya per defecte (pensem que els fabricants solen emprar la mateixa contrasenya per a tots els seus equips).

FIGURA 1.16. Tauler d'administració d'un punt d'accés



- Activar el filtrat d'adreces MAC de manera que només es puguin connectar els dispositius especificats (totes les recomanacions que estem veient es

duen a terme des de menús similars a la figura 1.16). Aquest mecanisme no autentica l'usuari, sinó la interfície del terminal que s'hi connecta. No obstant això, cal tenir present que les adreces MAC poden ésser falsificades fàcilment.

- Activar el xifratge WEP/WPA.
- Desactivar, si no hi ha cap raó tècnica per mantenir-la, l'assignació d'IP per DHCP (d'aquesta manera caldrà assignar la IP de forma manual).

DHCP és l'acrònim de *Dynamic Host Configuration Protocol*.

- Els punts d'accés fan per defecte la difusió (*broadcast*) del SSID, és a dir, del nom lògic associat a la xarxa. Per evitar els accessos no desitjats es pot eliminar aquesta difusió.

SSID

El SSID (*Service Set Identifier*) és un codi format com a màxim per 32 caràcters que han de compartir tots els dispositius que es connecten entre si en una xarxa sense fils. També es coneix com a nom de la xarxa.

Broadcast és la difusió d'informació d'un node emissor a una multitud de nodes receptors de forma simultània.

1.5.3 Riscos potencials dels serveis de xarxa

Una xarxa és un conglomerat de molts elements heterogenis. Per tant, la seva seguretat, així com els riscos a què pot estar exposada, s'ha de cercar en primer lloc en els dispositius individuals que la conformen, i després en les interrelacions existents entre tots aquests dispositius i en la globalitat de la xarxa. Els servidors i les estacions de treball són elements essencials de la xarxa, no obstant això, en aquest apartat ens centrarem en l'estudi de la seguretat dels elements de la xarxa.

Seguretat dels elements de xarxa

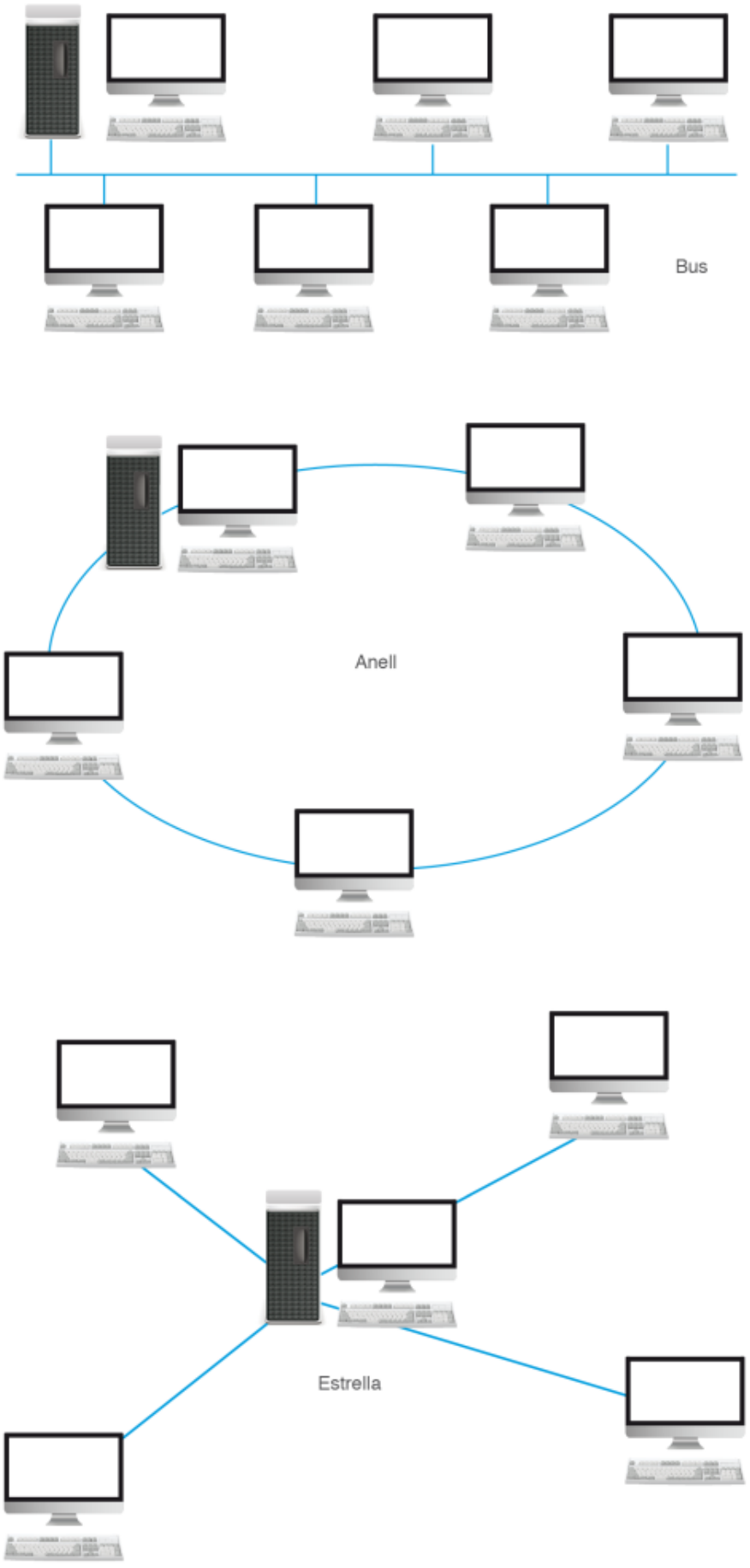
Quan parlem de seguretat dels elements de xarxa hem de tenir en compte les possibles vulnerabilitats de tots els elements que la constitueixen: la topologia, la seguretat del maquinari o els sistemes d'autenticació.

Seguretat de les topologies i els tipus de xarxa

Per *topologia* s'entén la forma o estructura de la xarxa des del punt de vista lògic, que pot diferir del seu disseny físic. Vegem a la figura 1.17 alguns exemples de topologia de xarxa. Notem que, segons la topologia, els riscos que assumeix la xarxa poden ser diferents.

Per exemple, una topologia d'estrella és especialment resistent a la caiguda de les estacions de treball (a diferència de les altres dues), però en canvi té un punt crític, l'element central, que si és atacat o cau per qualsevol motiu pot provocar la caiguda de tota la xarxa.

Figura 1.17. Tipus de topologies de xarxes



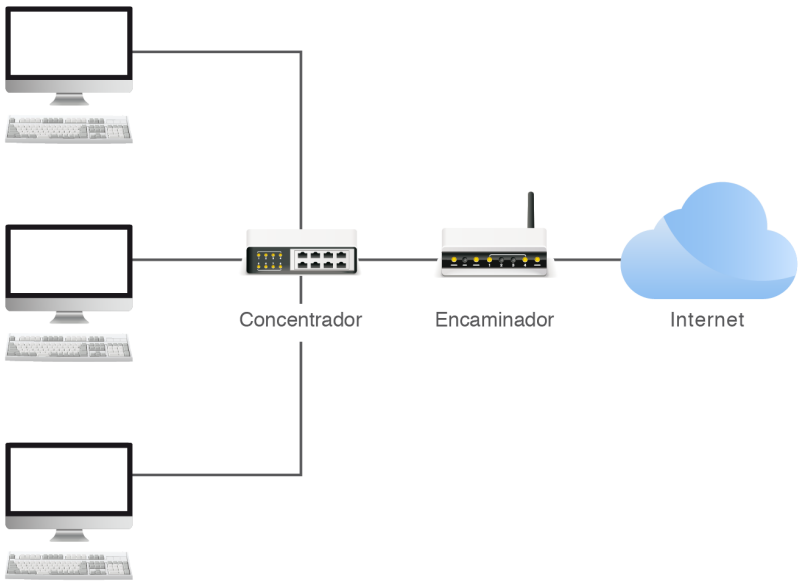
Seguretat del maquinari de xarxa

Pel que fa a la seguretat dels commutadors, concentradors i encaminadors, cal prendre les precaucions següents:

- Activació del xifratge (en cas que els dispositius ho admetin).
- En cas que no sigui necessari, cal desactivar el control remot d'administració.
- Canviar les contrasenyes d'administració predeterminades d'aquests dispositius.
- Usar llistes d'accés que permetin només els protocols, ports i adreces IP que la xarxa i els usuaris necessitin. Denegar la resta.

Com podem veure en la figura 1.18, l'encaminador pot esdevenir el punt més crític d'una xarxa des del punt de vista de possibles atacs externs. Al ser l'encaminador el dispositiu que permet el tràfic entre dues xarxes (molt sovint Internet és una d'elles), aquest element és visible per tothom. Representa, per tant, el punt d'entrada per atacants externs i el primer dispositiu a comprometre ja que és públic.

FIGURA 1.18. L'encaminador com a element de risc de la xarxa



Control d'accés a la xarxa basat en autenticació

IEEE 802.1X

L'IEEE 802.1X és un protocol creat per l'IEEE per al control d'accés a la xarxa basat en ports. Utilitza l'EAPOL (EAP sobre la xarxa d'àrea local) i és utilitzat per transportar les credencials del client a l'autenticador.

A més de les polítiques de contrasenyes d'usuari i tècniques de xifratge de la informació, també cal considerar els mètodes de control d'accés dels dispositius que es volen connectar a la xarxa. Aquest mètode requereix tres components i es basa en l'adreça MAC del dispositiu:

- **Client**: dispositiu (per exemple un portàtil) que desitja connectar-se a la LAN mitjançant una xarxa de telecomunicacions.

- **Autenticador**: és l'element que controla l'accés físic al medi, basant-se en l'estat d'autenticació del client. L'estat inicial dels ports de l'autenticador és "no controlat". Si el procés d'autenticació finalitza afirmativament, el port canvia el seu estat a "controlat" i el dispositiu és autoritzat a accedir al medi.

- **Servidor d'autenticació**: és el dispositiu de "confiança" que s'encarrega d'efectuar la validació de la identitat del client. Notifica el resultat a l'autenticador.

Atacs als serveis de xarxa

Els serveis de xarxa poden ser víctimes de diversos tipus d'atacs, entre els quals podem destacar:

1. Atacs de denegació de servei

2. Atacs de falsejament d'identitat (*spoofing*)

a) Atacs de denegació de servei

S'anomena *atac de denegació de servei (denial of service)* tota acció iniciada per una persona o entitat que inutilitza el maquinari o programari de manera que els recursos del sistema no siguin accessibles des de la xarxa. Els atacs de denegació de servei (DoS) poden atacar el maquinari de la xarxa, el sistema operatiu fins i tot les aplicacions del sistema. Els atacs DoS poden implicar altres ordinadors intermediaris (fins i tot milers), amb la qual cosa s'aconsegueix un dany encara més gran. A més, l'atacant pot ocultar la seva adreça IP gràcies als ordinadors pont (anomenats *zombis*). Aquest tipus d'atac s'anomena atac *DoS distribuït* (DDoS o *distributed denial of service*).

Els atacs de denegació de servei són atacs **contra la disponibilitat** dels recursos d'un sistema informàtic.

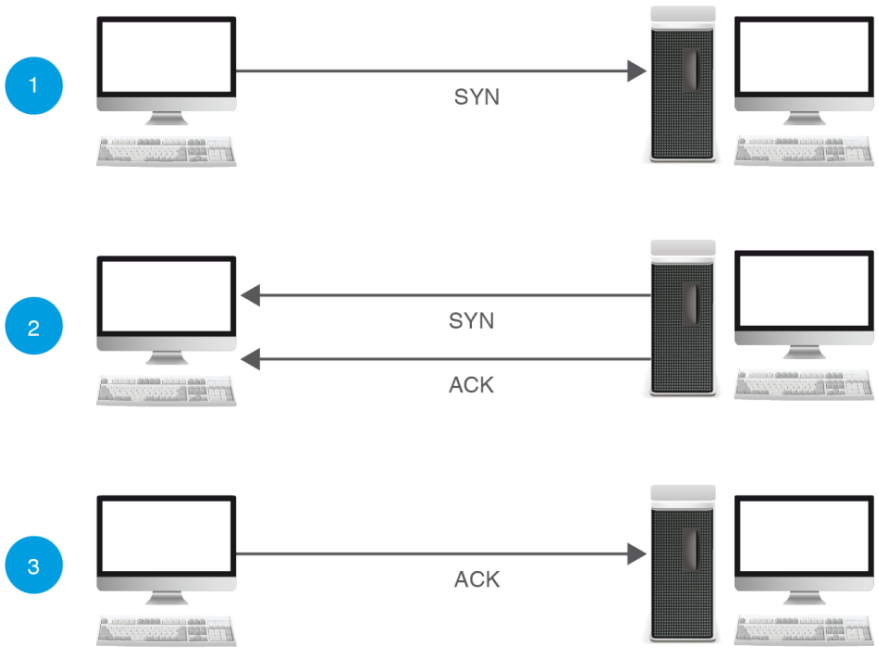
Vegem un exemple d'atac de denegació de servei: l'atac SYN. Aquest atac consisteix en l'enviament d'un gran nombre de sol·licituds de connexió per segon. El sistema atacat respon correctament les sol·licituds de connexió, però en no obtenir resposta del sistema atacant, es col·lapsa i no pot atendre les sol·licituds de connexió legítimes. Aquest atac es basa en el *modus operandi* del protocol d'establiment de sessió entre client i servidor:

1. L'ordinador client envia una sol·licitud de sincronització (SYN) al servidor.

2. El servidor respon amb un missatge ACK (*acknowledgement*) i un missatge de sincronització al client.

3. En resposta a la sol·licitud de sincronització, l'ordinador client envia una resposta ACK al servidor.

FIGURA 1.19. Protocol d'establiment de sessió en tres passos



El servidor manté en cua d'espera tots els paquets SYN que va rebent, fins que són cancel·lats per l'enviament del corresponent ACK per part del client (o bé expira el temps d'espera establert per un temporitzador). L'atac SYN es produeix quan els paquets enviats per l'emissor contenen adreces IP falses i, en conseqüència, el servidor no podrà rebre mai el paquet ACK que alliberaria la cua de recepció. Així, quan aquesta s'omple, les noves (i legítimes) sol·licituds de connexió no es poden servir i es produeix la denegació de servei.

b) Atacs de falsejament d'identitat (*spoofing*)

Observem que amb tècniques de falsejament d'identitat es poden aconseguir atacs de denegació de servei.

En els atacs d'*spoofing* l'intrús fa servir tècniques de suplantació d'identitat. Les formes més conegudes d'aquests atacs són el **falsejament d'IP**, el **falsejament d'ARP** i el **falsejament de DNS**.

En el cas del falsejament d'IP, l'atacant obté accés no autoritzat a una xarxa suplantant la seva adreça IP per la d'un equip en el qual es confia dins de la xarxa. Un dels camps de la capçalera IP conté l'adreça d'origen. Aquest tipus d'atac substitueix l'adreça i fa veure que s'ha enviat des d'una màquina diferent. Com a anècdota, aquest tipus d'atac va convertir a Kevin Mitnick en el *hacker* més conegut del món. Mesos més tard, va ser arrestat per l'FBI per robatori de fitxers.

Les tècniques de falsejament d'ARP es poden fer servir per realitzar els anomenats *atacs man-in-the-middle*.

L'atac *man-in-the-middle* (MITM) és un atac contra la confidencialitat i la integritat.

En aquest tipus d'atac, l'atacant vol conèixer tot el trànsit de xarxa entre l'usuari A i B i viceversa, però, com es pot veure en la figura 1.20, no és possible perquè es troben connectats mitjançant un commutador (element de xarxa que controla el tràfic de xarxa en base a la informació de l'adreça de cada paquet). De manera molt resumida, l'atacant aconsegueix que tant l'usuari A com el B usin la seva adreça MAC (conservant les adreces IP respectives), per la qual cosa pot espiar el trànsit de xarxa entre els dos.

FIGURA 1.20. Atac man-in-the-middle

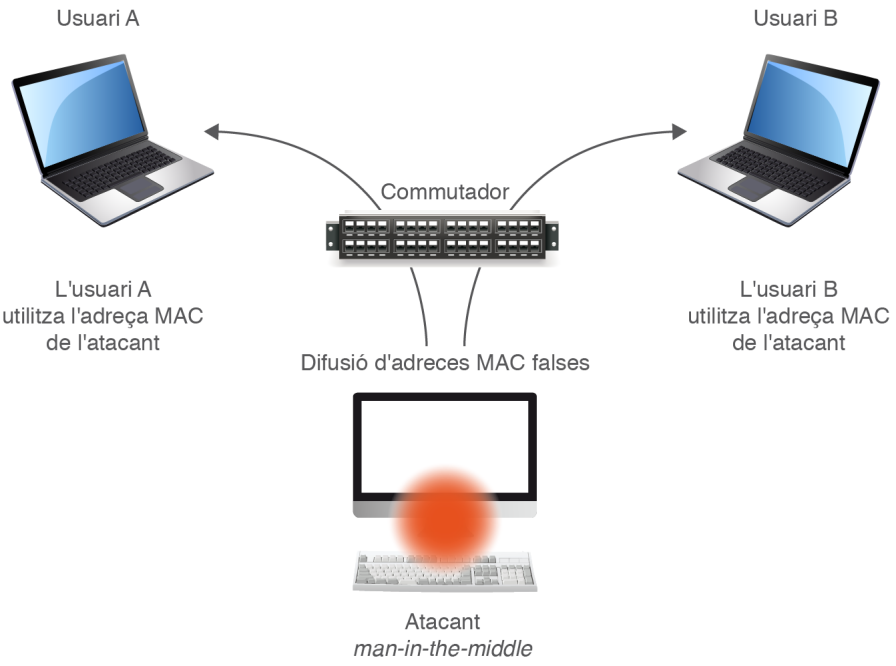
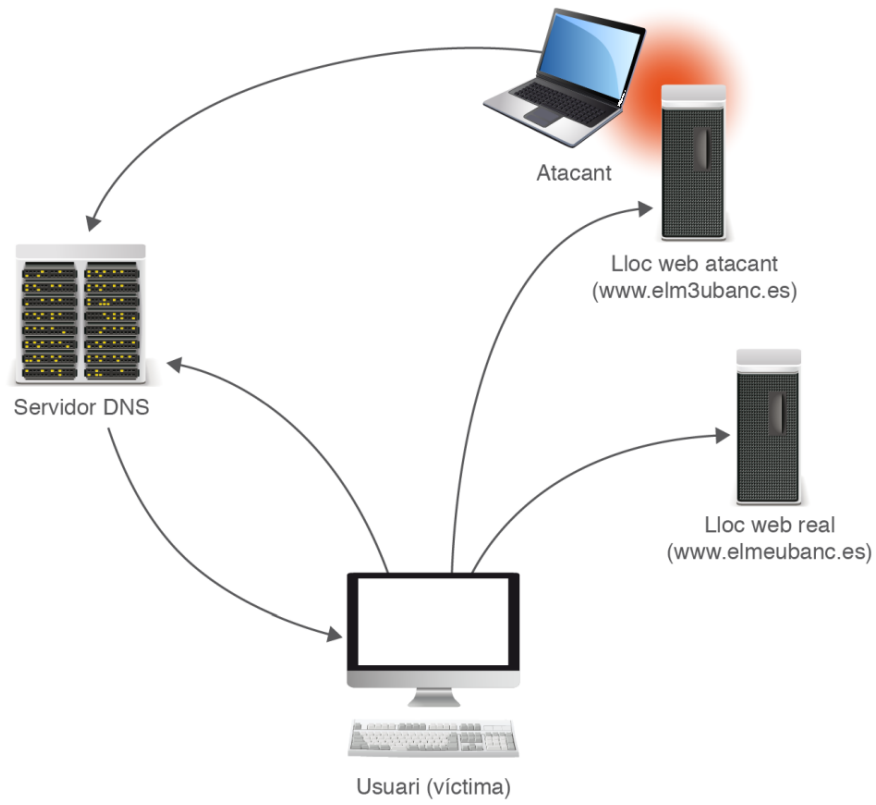


FIGURA 1.21. Esquema d'un atac de desencaminament



Amb la tècnica del **falsejament de DNS** es pot realitzar un tipus d'atac anomenat *desencaminament (pharming)*, en el qual la màquina atacada, quan sol·licita una adreça IP determinada al seu servidor DNS (per exemple, www.el_meu_banc.es),

rep una adreça falsa. Així, continuant amb l'exemple, la víctima suposarà que està accedint al seu banc, mentre que en realitat ho fa al lloc web proporcionat per l'atacant, on es capturaran les claus d'accés de l'usuari a la seva entitat financera (figura 1.21).

Pharming i phishing

No s'ha de confondre el desencaminament (*pharming*) amb la pesca (*phishing*). El desencaminament és un atac molt tècnic, mentre que la pesca és una estratègia d'enginyeria social dissenyada perquè les víctimes accedeixen a llocs web falsos, on capturaran les seves claus personals. Si són reeixits, tots dos atacs acaben, però, amb el mateix resultat.

1.5.4 Intents de penetració. Detecció d'intrusions

Actualment les xarxes informàtiques tenen algun punt que les connecta amb altres xarxes (típicament Internet). Així doncs, la xarxa d'una organització rebrà informació externa com per exemple correus electrònics, peticions de pàgines web al seu servidor, o actualitzacions de programari de les aplicacions i sistemes operatius instal·lats. En aquest escenari, és inevitable qüestionar-se si tota la informació externa que viatja per la xarxa de l'organització és maliciosa. Si n'hi ha que no ho és, com es pot esbrinar?

Sistemes de detecció d'intrusos

Els sistemes de detecció d'intrusos (IDS) monitoren els continguts del flux d'informació de la xarxa a la recerca i rebuig de possibles atacs. Poden combinar maquinari i programari, i normalment s'instal·len en els dispositius més externs de la xarxa, com ara tallafocs. Admeten diferents tipus de classificacions:

- Segons la font de la informació
- Segons el tipus d'anàlisi que realitzen
- Segons el tipus de resposta de l'IDS

Segons la font de la informació

Un *Network IDS* de font oberta molt conegut és l'anomenat **Snort**, usat tant en plataformes Windows com a Linux.

- **Basats en xarxa** (*Network IDS*). Monitoren una xarxa a la recerca d'elements que puguin indicar un atac contra algun dels seus components. Són elements passius que no injecten trànsit a la xarxa (actuen en mode promiscu, escoltant tot el trànsit de xarxa).
- **Basats en màquina** (*Host IDS*). Monitoren una màquina (o diverses, en el qual cas s'anomenen *multihost*) i recullen dades del sistema operatiu (per exemple, el registre d'esdeveniments). Consumeixen recursos de la màquina en la qual s'han instal·lat. Com que treballen amb el sistema

L'eina Tripwire, descrita en l'apartat "Detecció de codi maliciós" d'aquesta mateixa unitat, és un IDS basat en màquina.

operatiu i el sistema de fitxers de la màquina, poden detectar atacs que els IDS de xarxa no detecten. Solen incloure mecanismes de verificació de la integritat de fitxers.

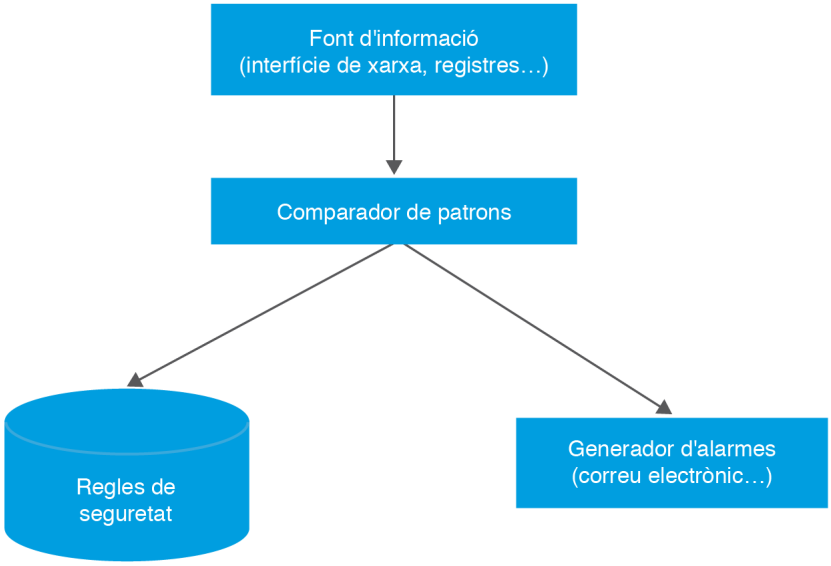
- **Basats en aplicacions**. Monitoren els fitxers de registre d'una aplicació específica per detectar activitats sospitoses (per exemple, els *logs* d'un servidor de l'FTP). Consumeixen molts recursos de la màquina.

Segons el tipus d'anàlisi que realitzen

Una vegada recollida la informació, cal analitzar-la. Segons el tipus d'anàlisi que es realitzi, també tenim diferents tipus d'IDS (no són mútuament excloents):

- **Basats en firmes**. L'anàlisi s'efectua cercant firmes (**patrons d'atac**) que permetin identificar un atac ja conegut. Aquests tipus de IDS requereixen que les bases de dades de firmes siguin actualitzades constantment. A la figura 1.22 es pot veure l'arquitectura bàsica d'aquest tipus IDS.
- **Basats en anomalies**. En aquest cas, l'IDS cerca comportaments anòmals a la xarxa (un escaneig de ports, paquets mal formats...).
- **Segons el tipus de resposta de l'IDS:**
  - **Resposta passiva**. L'IDS enregistra l'alarma generada o avisa el responsable.
  - **Resposta activa**. Aquest IDS, a més de les accions de la resposta passiva, té capacitat de reacció i pot bloquejar les accions intrusives.

FIGURA 1.22. Esquema general d'un IDS basat en firmes

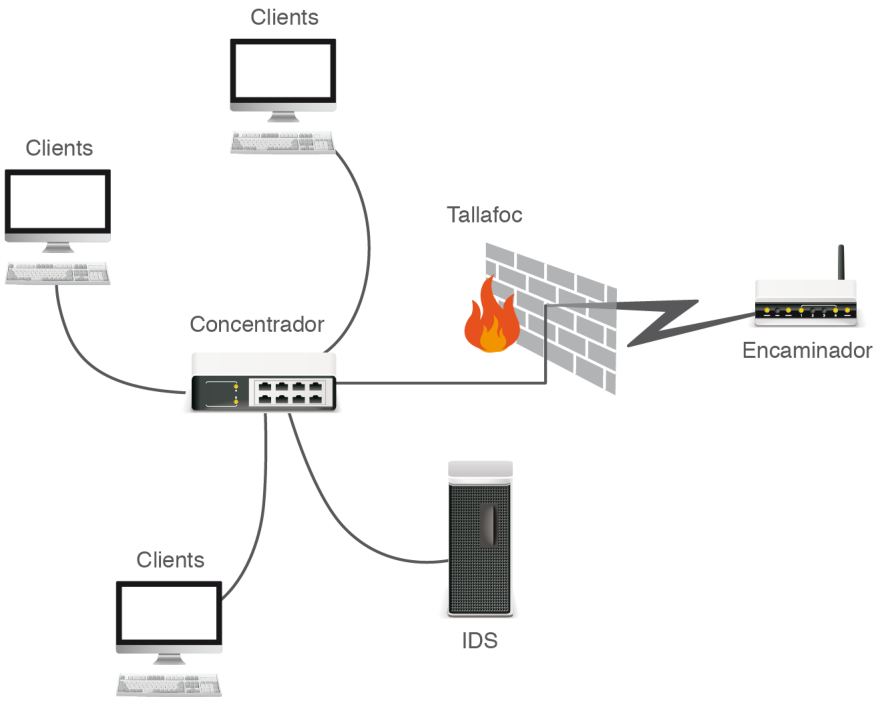


Els IDS poden enviar i obtenir informació d'altres elements (tallafocs, encaminadors...) de la xarxa (**propietat d'interoperabilitat**) i són capaços de relacionar

esdeveniments independents i que vistos de forma aïllada poden no significar cap amenaça pel sistema (**propietat de correlació**).

En la figura 1.23 podem veure una ubicació típica d'un IDS en una xarxa amb concentrador.

Figura 1.23. Ubicació d'un IDS en una xarxa



L'anàlisi dels registres dels IDS és clau quan es realitza un **test de penetració**. El personal que duu a terme aquestes proves analitza els *logs* que enregistren els IDS quan el sistema és sotmès a diversos atacs i extreu conclusions per millorar la seguretat del sistema. Més formalment, els tests de penetració són proves que avaluen la seguretat d'un sistema informàtic simulant que és atacat per personal extern de l'organització (*outsiders*) així com per personal intern (*insiders*). Al personal extern se'l suposa no autoritzat (i, per tant, s'estudia com pot accedir un usuari no autoritzat), mentre que al personal intern se'l suposa algun permís d'accés.

Els **sistemes de prevenció d'intrusos (IPS)** permeten establir polítiques de seguretat per protegir la xarxa dels atacs. Es poden considerar una extensió dels IDS.

Els tests de penetració es poden realitzar des de dos vessants diferents (o bé un terme mig de tots dos):

- Proves de **caixa negra** (*black box*): s'assumeix que no es té cap coneixement previ del sistema que s'ha de testar.

- Proves de **caixa blanca** (*white box*): s'assumeix el coneixement total del sistema a testar.

Esquers (honeypots i honeynets)

Un *honeypot* és un sistema informàtic (o programa) que es posa de manera deliberada a l'accés públic per estudiar les pautes dels seus possibles atacants. Aquests sistemes no poden contenir cap informació important i necessiten eines passives d'auditoria que permetin conèixer, amb posterioritat a l'atac, què ha passat en el sistema. Freqüentment, aquests sistemes també contenen directoris o noms de fitxers amb identificacions llamineres, que despertin la curiositat dels atacants. A més de la seva finalitat d'anàlisi, també poden utilitzar-se per distreure l'atenció dels possibles atacants del veritable sistema, que no ha de ser accessible a través del sistema utilitzat com a esquer. Els *honeypots* no es troben, en general, completament protegits, i les aplicacions i dispositius es configuren amb les opcions per defecte i solen presentar múltiples forats de seguretat.

La translació del concepte de *honeypot* a una xarxa s'anomena *honeynet*. En aquest cas, els atacants, a més de servidors no completament assegurats, també poden trobar dispositius perifèrics a la xarxa, com encaminadors o tallafocs.

1.6 Les xarxes públiques. Seguretat en la connexió

Una xarxa pública és una xarxa de comunicacions que pot ser usada per qualsevol a un preu molt reduït. Aquesta xarxa està gestionada per una operadora de telecomunicacions i, per tant, la informació que hi viatja és susceptible de ser 'observada' durant el seu trànsit fins al destí. Cal prendre mesures per evitar-ho.

Per garantir la impossibilitat que la informació pugui ésser interceptada, les dades no haurien de viatjar a través de les xarxes públiques. Les xarxes no públiques s'anomenen connexions dedicades, les quals són molt costoses i poc flexibles als canvis. No obstant això, és possible usar xarxes públiques i alhora impedir que la informació pugui ésser interceptada, fent que sigui incomprensible (mitjançant tècniques de xifrat), excepte pel receptor autoritzat.

1.6.1 Pautes i pràctiques segures

L'ús de les xarxes públiques requereix l'establiment de relacions de confiança en un entorn gairebé anònim i intangible per definició. En el cas del comerç electrònic, aquesta relació de confiança no només ha de servir per protegir la nostra privacitat, sinó per conformar un espai de seguretat en què les transaccions econòmiques siguin viables. Aquesta és la principal motivació de la **signatura electrònica**.

La **signatura electrònica**, basada en la criptografia de clau pública, permet que un emissor pugui enviar missatges a un receptor complint les tres propietats següents:

- **Autenticitat**: la signatura d'un missatge per l'emissor permet que el receptor estigui segur de la identitat del remitent.
- **Integritat**: certesa que el missatge no s'ha modificat durant la transmissió.
- **No repudi**: l'emissor d'un missatge no pot repudiar o negar que l'ha enviat (per exemple, podria argumentar que l'ha enviat una tercera persona). La inclusió d'una signatura digital evita aquesta possibilitat.

Podeu trobar més informació sobre els **esquemes de clau pública** en la unitat "Seguretat física, lògica i legislació".

Aquestes tres propietats són essencials perquè la signatura digital gaudeixi de confiança en un entorn tan intangible com Internet. Si volem fer activitats tan delicades, com, per exemple, participar en unes votacions electròniques, és imprescindible garantir les tres propietats abans esmentades. Observem que moltes vegades l'entorn en què se signa un document de manera **manuscrita** ofereix en realitat menys garanties que els criptosistemes de clau pública, que presenten una gran robustesa. Suposem, per exemple, el cas de les votacions electròniques. En el món real, el votant introdueix físicament una papereta de vot dins d'una urna electoral. Pot veure com cau dins de l'urna i confia que l'urna només serà oberta al final del procés per les persones autoritzades i que el seu vot serà comptabilitzat correctament. Malgrat tot, aquest procés té tantes baules, punts febles i possibles errors humans, que, en el fons, podria ser tan qüestionat (o més, fins i tot) com el seu homòleg electrònic.

Funcionament d'un criptosistema de clau pública

Quan un usuari A vol **enviar un missatge** a un usuari B, xifra el missatge fent servir la clau pública de B (aquesta clau és coneguda per tots els usuaris del criptosistema). Quan el receptor rebi el missatge, únicament el podrà desxifrar ell mateix, utilitzant la seva pròpia clau privada (que només ell té).

Totes les claus públiques s'obtenen d'un directori públic i, per tant, no podem garantir a qui pertanyen efectivament.

Quan l'usuari emissor vol **signar un missatge**, empra la seva clau privada (només coneguda per ell), que acredita la seva identitat davant de l'usuari receptor del missatge. En el procés de verificació dut a terme per l'usuari B, utilitzarà la clau pública de l'usuari A (coneguda per tots els usuaris del criptosistema).

No repudi

És important observar que, una vegada s'ha signat un missatge, quan la signatura sigui verificada per l'usuari receptor, l'usuari emissor no podrà negar l'emissió del missatge (propietat de no repudi). Les autoritats de certificació, a més d'emetre certificats, també els poden revocar.

Fixem-nos que el punt feble d'aquest protocol es produeix quan hem de fer ús d'una clau pública. Per exemple, quan l'usuari B de l'exemple (el receptor) vol comprovar la identitat de l'emissor mitjançant la clau pública de l'usuari A, com pot saber que la clau que utilitza pertany realment a A?

Autoritats de certificació

Per resoldre el problema de la identitat de l'emissor, es requereix la participació d'una tercera part (anomenada **autoritat de certificació**) que confirmi l'autenticitat de la clau pública d'un usuari determinat. Aquesta certificació s'aconsegueix mitjançant l'expedició d'un **certificat digital**. Aquest document, signat digitalment per un **prestador de serveis de certificació**, vincula unívocament unes dades de verificació de signatura al titular i confirma la seva identitat en qualsevol transacció.

Les autoritats de certificació s'estructuren de forma jeràrquica, de manera que l'autoritat de certificació arrel és autosignada (és a dir que no té cap altra autoritat que la certifiqui) i a cada nivell inferior s'hi poden trobar autoritats de certificació (una o més) que poden signar certificats d'entitat final (persones, aplicacions de programari) o certificats d'altres autoritats de certificació subordinades.

El protocol que descriu tots els processos organitzatius que calen per gestionar els certificats digitals s'anomena **Infraestructura de Clau Pública** (PKI).

Obtenció d'una identificació electrònica

Com a usuaris, és possible obtenir un certificat digital que ens permeti identificarnos a la xarxa i efectuar operacions diverses, com per exemple, fer tràmits amb l'administració a través de les seves oficines virtuals (sense necessitat d'haver-hi d'anar en persona), signar correus i realitzar, entre d'altres, transaccions segures per Internet.

Hi ha diversos organismes autoritzats per expedir aquestes identificacions electròniques, entre els quals cal esmentar l'**Agència Catalana de Certificació**.

Per a més informació sobre la identificació electrònica visiteu el web www.idcat.cat.

Quan anem personalment a la seu física d'aquesta entitat ens proporcionen un programari en un dispositiu com el que podeu veure a la figura 1.24. Seguint les instruccions adjuntes, el podrem instal·lar als nostres ordinadors i començar a utilitzar la nostra signatura digital. Tot i que, com s'ha vist, la teoria dels criptosistemes de clau pública no és senzilla, per usar el nostre certificat no necessitem tenir cap coneixement criptogràfic.

FIGURA 1.24. Clauer idCAT: llapis de memòria que conté la identificació electrònica d'un usuari

Llei de signatura electrònica

A Espanya, la Llei 59/2003 de signatura electrònica, reconeix tres tipus de signatura electrònica:

- **Simple**: permet identificar el firmant (autenticació).
- **Avançada**: permet identificar la persona que signa i detectar qualsevol modificació en les dades signades (autenticació i integritat).
- **Reconeguda**: és la signatura més completa. Es basa en un certificat reconegut i es genera mitjançant un dispositiu segur de creació de signatures. S'equipara a la signatura manuscrita.

2. Implantació de tècniques d'accés remot

Existeix un conjunt de configuracions de seguretat, ja siguin de programari, de maquinari o mixtes, que permeten l'accés segur a la xarxa d'informació des de l'exterior. Sense aquesta possibilitat, la xarxa perdria un dels seus aspectes essencials i no hi hauria la possibilitat d'usar o compartir els seus recursos des de localitzacions remotes. A més de poder efectuar aquesta connexió, cal que les tècniques que s'usin puguin garantir que l'accés remot sigui segur.

2.1 Seguretat perimètrica

Qualsevol xarxa de comunicacions està interconnectada amb altres. El punt on s'enllacen dues xarxes és un dels seus punts més dèbils. Per tant, s'ha de tenir especial cura a assegurar aquestes zones.

Amb l'establiment de seguretat perimètrica es busca:

- Rebutjar connexions a serveis crítics.
- Permetre només determinat trànsit (com per exemple, el correu electrònic) o només entre determinats nodes.
- Proveir la xarxa d'un únic punt d'interconnexió amb l'exterior.
- Tenir un control i dirigir el trànsit entrant exclusivament als sistemes adients dins de la intranet.
- Ocultar sistemes o serveis vulnerables que poden ser complicats de protegir dels atacs de l'exterior.
- Auditar el trànsit entre l'exterior i l'interior.
- Dificultar l'accés a informació que permeti saber coses de la xarxa com ara noms de sistemes, topologia de la xarxa, tipus de dispositius de xarxa o comptes d'usuaris interns.

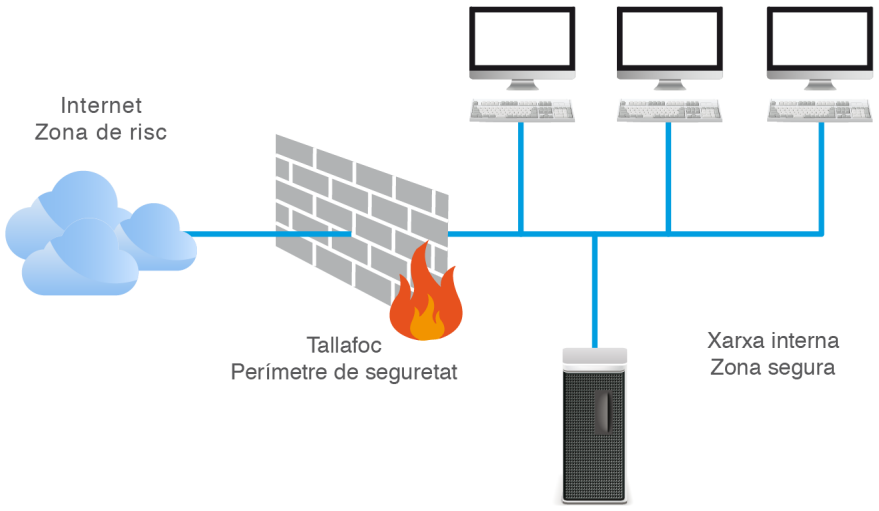
La **seguretat perimètrica** és un dels mètodes de defensa d'una xarxa. Es basa en l'establiment de recursos de seguretat en la zona de contacte de la xarxa amb l'exterior de l'organització. Això permet l'accés d'usuaris interns o externs a determinats serveis.

2.1.1 Elements bàsics de la seguretat perimètrica

Els elements bàsics que configuren la seguretat perimètrica, que es poden veure a la figura 2.1, són els següents:

- **Zona de risc o xarxa externa**. És aquella part que es considera que pot posar en risc el sistema informàtic. Usualment es considera Internet com la zona de risc.
- **Zona segura o xarxa interna**. És la part que volem protegir: els usuaris finals de sistemes, els servidors que contenen dades privades i tots els altres sistemes que no volem que siguin coneguts pel "món exterior".També se'n diu *xarxa protegida*, *xarxa de confiança* o *xarxa interna*.
- **Perímetre de xarxa o tallafoc**. El perímetre de xarxa és la part que separa la zona segura de la de risc. Genèricament s'anomena *tallafoc* al perímetre de xarxa. Entenem per tallafoc, per tant, un sistema o xarxa que aïlla una xarxa d'una altra.

FIGURA 2.1. Elements de seguretat de xarxa



Partint d'aquesta definició, doncs, un tallafoc pot ser un encaminador, un equip que executa un programa especial o qualsevol altre dispositiu o xarxa de dispositius en què es duu a terme un conjunt d'activitats per controlar el trànsit entrant i sortint. Així, les funcions del tallafoc les poden dur a terme dispositius com programes, encaminadors o ordinadors dedicats exclusivament a les tasques de filtració de paquets (servidors intermediaris o *proxy*).

Equip bastió

L'equip que està directament connectat a altres xarxes, com per exemple Internet, s'anomena *equip bastió* (*host bastion* en anglès). És el més vulnerable, i per tant la primera línia de defensa de la xarxa.

La creació d'aquesta zona perimètrica o tallafoc s'ha de fer tenint en compte tant l'estructura de la xarxa com els serveis que han de quedar disponibles per als usuaris.

Els tallafocs són, probablement, un dels elements més importants per a la seguretat de la nostra xarxa, i hem de considerar, a l'hora d'instal·lar-los, els aspectes següents:

- No s'han d'emprar en lloc d'altres eines, sinó conjuntament amb aquestes. Hem de tenir en compte que el tallafoc serà el punt que rebrà tots els atacs sobre el nostre sistema.
- En centralitzar una bona part de les mesures de seguretat de la xarxa en un únic sistema (no cal que sigui un únic dispositiu), si aquest es veu compromès, la xarxa quedarà exposada als atacs dels intrusos.
- Pot proporcionar una falsa sensació de seguretat. No per instal·lar un tallafoc podem assumir que la xarxa és segura i prescindir de vigilar els equips interns de la xarxa.

Un sistema tallafoc realitza les activitats següents:

- **Filtrat de trànsit d'entrada i sortida**. Aquest filtrat es pot fer tant a nivell de connexió, de la capa de xarxa (conegut com a *filtrat de paquets*) o de la capa d'aplicació. Es realitza una inspecció de les capçaleres dels paquets IP. El criteri per deixar-los passar es basa principalment en una combinació de la seva adreça IP d'origen, adreça IP de destinació, port d'origen i port de destinació (de servei).
- **Ocultació** de la configuració de la xarxa a l'exterior.
- **Servidor intermediari**. Es un programari o dispositiu que actua en nom d'un altre. Per exemple, si un ordenador A fa una petició a un ordenador C de fora de la xarxa, no li ho demana directament. A fa la petició a un ordinador B (*proxy*) i aquest la fa a C. Aquesta funcionalitat permet tenir una memòria cau, control d'accés i registre de trànsit.
- **Monitoratge**. Com que tot el trànsit d'entrada i sortida passa pel sistema tallafoc, és possible motoritzar moltes coses, com per exemple connexions, adreces IP, ports o llocs web. Amb el monitoratge es busca descobrir els intents d'atacs i trames sospitoses i registrar els tipus de paquets rebuts, així com la freqüència de paquets, adreces font i destinació, intents d'ús de protocols protegits, intents de falsificació, trames rebudes des d'encaminadors desconeguts... Com que la quantitat de fitxers de registre generats pot ser molt gran, cal considerar l'ús d'eines que automatitzin el monitoratge.

En general, cal prendre unes decisions bàsiques en la configuració d'un tallafoc.

En primer lloc, cal definir una política de seguretat i implementar el nivell de monitoratge i de control desitjat en l'organització. S'ha d'indicar bàsicament què s'ha de permetre i què s'ha de denegar. Existeix la possibilitat d'emprar una política restrictiva, en què es denega tot allò que explícitament no es permet o una política amb permís, en la qual es permet tot, excepte el que s'ha negat explícitament.

D'altra banda, la configuració i el nivell de seguretat potencial del tallafoc depèn de l'ús del dispositiu. Així, si connecta dues subxarxes diferents la política serà diferent que si ha de filtrar els paquets de l'organització amb l'exterior.

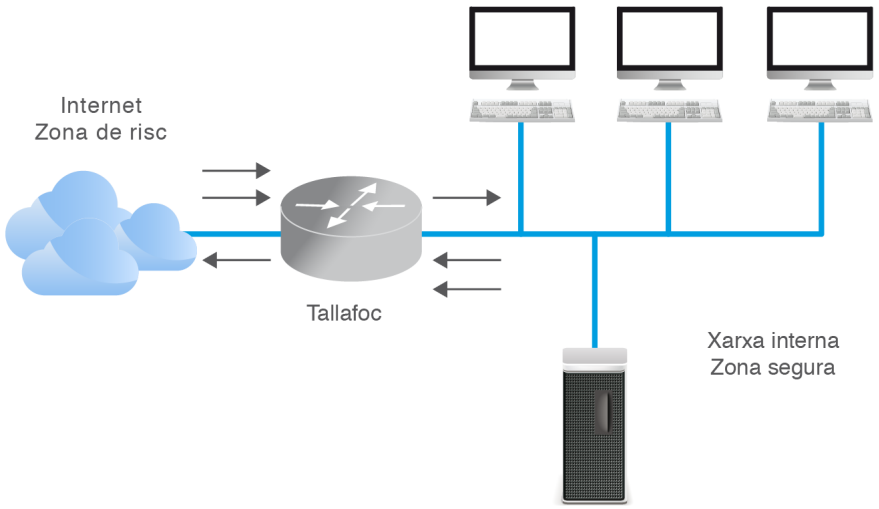
Per últim, cal tenir en compte que la inversió ha d'ésser proporcional al valor estimat del que desitgem protegir. Un sistema de tallafoc pot ser molt barat o costar milers d'euros.

2.1.2 Perímetres de xarxa. Zones desmilitaritzades

El perímetre de xarxa, com hem comentat, conté el que genèricament s'anomena *sistema tallafoc*. Aquest, però, pot ser un o més dispositius amb diverses configuracions d'arquitectures de seguretat possibles.

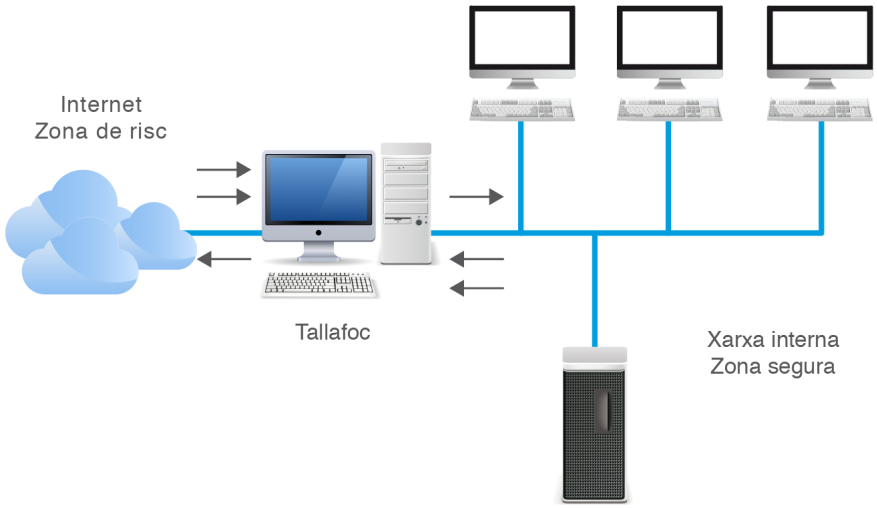
- ***Tallafoc de filtrat de paquets***. És la configuració més simple, tal com es veu a la figura 2.2. Es col·loca un dispositiu que disposa d'una única interfície de xarxa. L'encaminador extern està configurat per enviar les dades al dispositiu i els clients interns hi envien també les dades de sortida. L'encaminador avalua les dades segons unes regles de seguretat. Aquest sistema és conegut en anglès com a *screeneing router*.

FIGURA 2.2. Tallafoc en configuració de filtrat de paquets



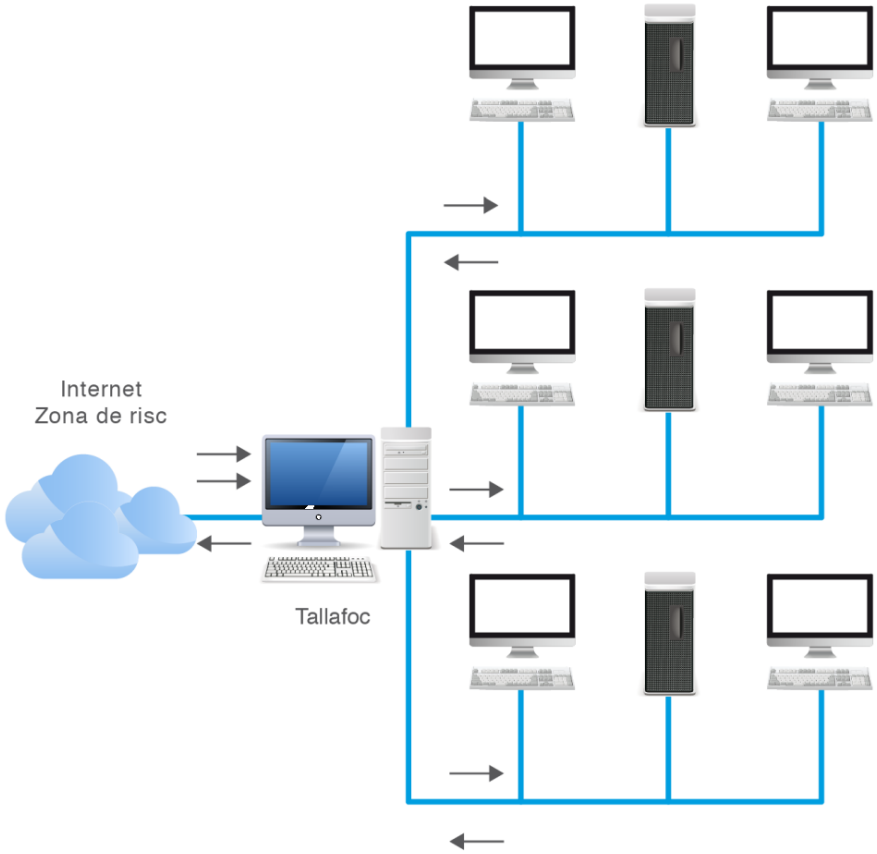
- ***Amfitrió de dues bases (dual-homed host)***. En aquesta arquitectura s'instal·la un dispositiu que té almenys dues interfícies de xarxa. L'avantatge d'usar aquest esquema és que crea una ruptura entre les xarxa externa i interna, la qual cosa permet que tot el trànsit d'entrada i sortida passi per l'equip. El sistema necessita un servidor intermediari per a cadascun dels serveis que vulguem tenir actius. L'esquema bàsic es pot veure a la figura 2.3.

Figura 2.3. Tallafoc en configuració dual-homed



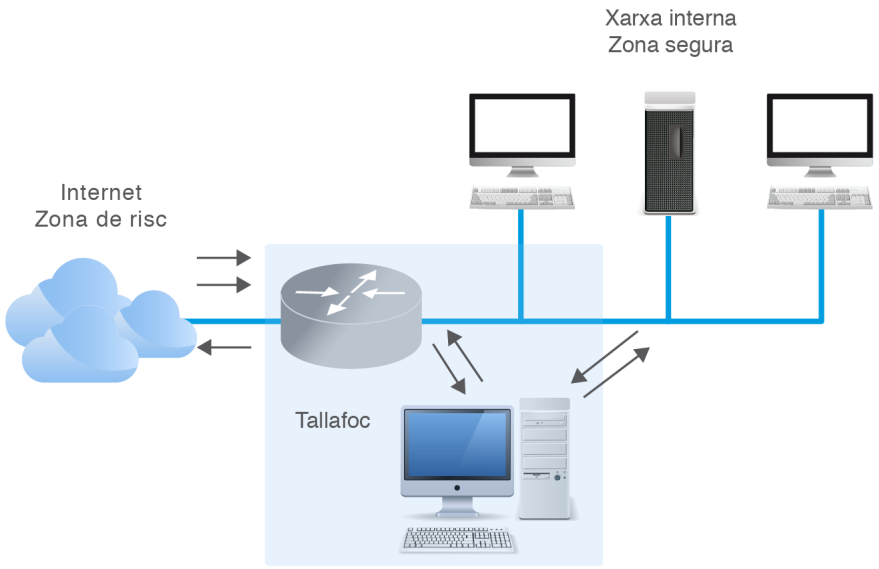
- ***Amfitrió multi-base (multihomed host bastion)***. L'evolució del cas anterior significa tenir més d'una interfície de xarxa en el dispositiu. Habitualment una interfície de xarxa va a la xarxa externa i la resta a la xarxa interna. Aquesta arquitectura permet distribuir el trànsit per les diferents interfícies de xarxa depenent de la destinació. Afegeix un nivell més alt de seguretat, tal com es pot veure a la figura 2.4.

Figura 2.4. Tallafoc en configuració multihomed



- ***Amfitrió de monitoratge (screened host)***. Com es pot veure a la figura 2.5, combina dos elements de seguretat. Un encaminador, connectat a la xarxa insegura i que realitza un filtrat de paquets, i un equip, accessible des de l'exterior on hi ha el servidor intermediari de la xarxa. D'aquesta manera, el filtrat es fa en un equip, protegint la xarxa, i l'accés als serveis es fa en un segon nivell, amb el sistema *proxy*.

FIGURA 2.5. Tallafoc en configuració screened host

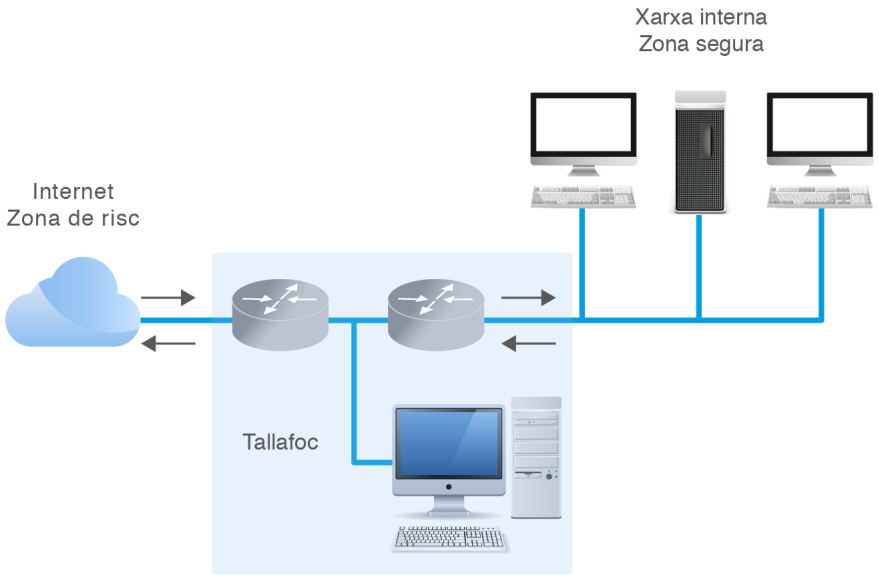


- ***Subxarxa protegida (screened subnet)***. Un pas més en l'arquitectura de seguretat consisteix en que entre la xarxa interna i l'externa hi hagi tot un subsistema que incorpori seguretat d'entrada, seguretat de sortida i el conjunt de serveis que es vol que siguin visibles des de l'exterior. No només aïlla la xarxa interna i externa, sinó que es crea una xarxa intermèdia. Afegeix una xarxa perimetral que aïlla la xarxa interna d'Internet. Aquesta xarxa intermèdia s'anomena **DMZ o zona desmilitaritzada**.

  L'objectiu d'una DMZ és que les connexions que provenen de la xarxa interna i les que provenen de la xarxa externa estiguin permeses. En canvi, les connexions des de la DMZ només estan permeses cap a la xarxa externa. Per tant, els equips (*hosts*) de la DMZ no poden connectar amb la xarxa interna. Això permet que els equips de la DMZ puguin donar serveis a la xarxa externa i a la vegada protegeixen la xarxa interna en el cas que intrusos comprometin la seguretat dels equips situats a la zona desmilitaritzada.

  D'aquesta manera es redueixen considerablement els efectes d'un atac al sistema. En les arquitectures anteriors, tota la seguretat estava centrada en l'equip bastió i si la seguretat es veia compromesa, la resta de la xarxa queda automàticament exposada. Com que l'equip bastió és un objectiu interessant per a molts atacants, l'arquitectura DMZ és un intent d'aïllar-la en una xarxa perimètrica de manera que l'intrús que accedeixi a aquesta màquina no aconsegueixi un accés total a la subxarxa protegida. L'esquema bàsic és a la figura 2.6.

FIGURA 2.6. Tallafoc en configuració screened subnet



En aquesta xarxa perimetral es poden incloure sistemes que facin molt ús de connexió a la xarxa externa. Poden ser, entre altres, servidors de correu, servidors web o DNS. Aquests dispositius seran els únics elements visibles des de l'exterior. D'aquesta manera un atacant hauria de trencar la seguretat d'ambdós encaminadors per accedir a la xarxa protegida. També, si és necessari, es poden definir diverses xarxes perimetrals en sèrie. En aquest escenari, els serveis de menor fiabilitat es posaran a les xarxes més externes.

Les regles de filtrat han de ser diferents en cada nivell. Altrament, no obtindríem major seguretat, ja que si s'aconsegueix trencar-ne una es poden trencar totes.

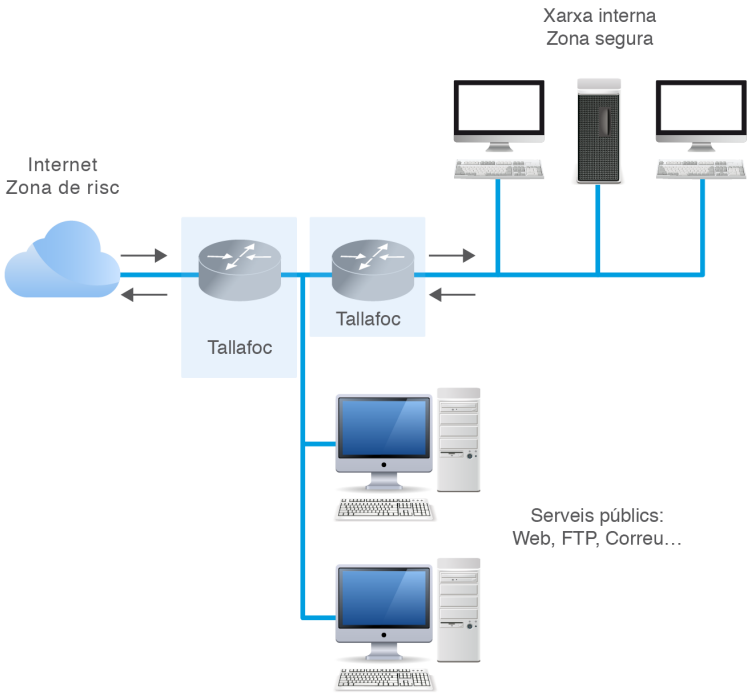
Les arquitectures **DMZ** són les més usades per la seguretat que proporcionen, tot i que són les més complexes de gestionar.

2.1.3 Arquitectura feble de subxarxa protegida

Existeixen diverses arquitectures DMZ. L'arquitectura feble de subxarxa protegida n'és una. Els elements es col·loquen tal com mostra la figura 2.7.

S'utilitzen dos encaminadors, anomenats *exterior* i *interior*, connectats a la xarxa perimètrica. En aquesta xarxa perimètrica, que constitueix el sistema tallafoc, s'inclou l'equip bastió i també s'hi poden incloure sistemes que requereixin un accés controlat, com el servidor web o el servidor de correu. Aquests seran els únics elements visibles des de fora de la xarxa. L'encaminador exterior bloqueja el trànsit no desitjat entre la xarxa perimètrica i la xarxa externa, mentre que l'interior fa el mateix però amb el trànsit entre la xarxa interna i la perimètrica. Un atacant hauria de trencar la seguretat d'ambdós encaminadors per accedir a la xarxa protegida.

FIGURA 2.7. Tallafoc en configuració d'arquitectura feble de subxarxa protegida



Alguns dels avantatges d'aquesta arquitectura són:

- Evitar l'existència d'un un únic punt dèbil. Ara cal trencar més d'un element de seguretat per accedir a la xarxa interna.
- Els serveis que s'han de veure des d'Internet estan a la DMZ.
- La xarxa interna està oculta i no és visible des de la xarxa externa.

L'arquitectura, però, no està exempta de problemes:

- És possible implementar una zona desmilitaritzada amb un únic encaminador que tingui tres o més interfícies de xarxa. Aquesta arquitectura no és gens recomanable perquè si es compromet aquest element es trenca tota la nostra seguretat. La idea de la DMZ és que cal comprometre dos encaminadors, tant l'extern com l'intern.
- Tota la seguretat està basada en els dos encaminadors. Existeixen arquitectures amb elements més segurs que un encaminador.

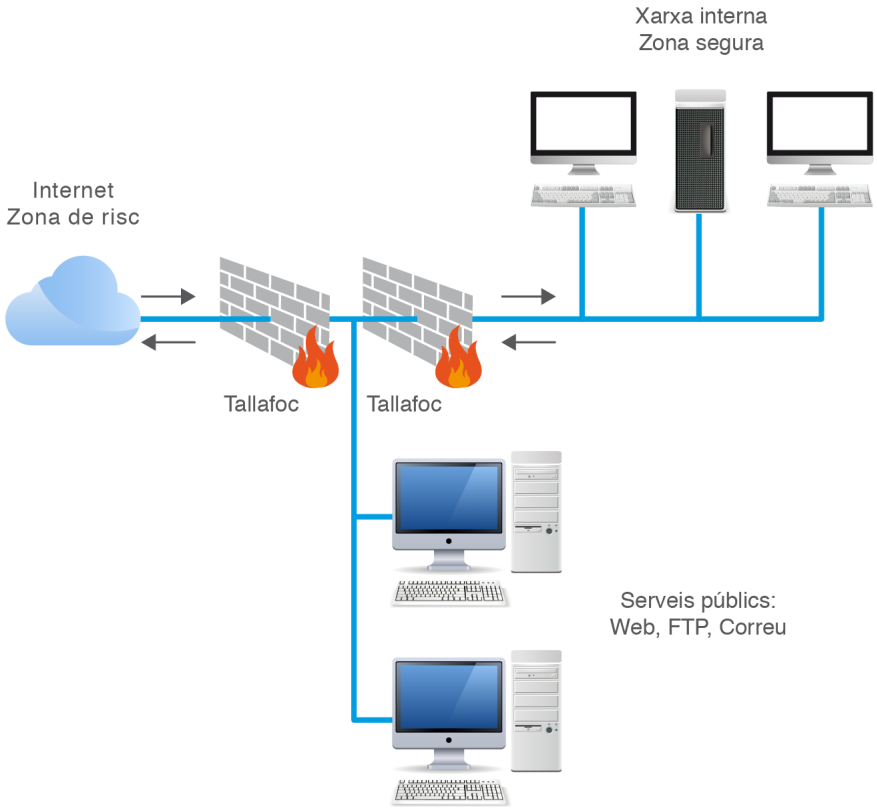
La configuració de DMZ amb un únic encaminador amb tres interfícies de xarxa s'anomena *three-legged firewall*.

2.1.4 Arquitectura forta de subxarxa protegida

L'arquitectura DMZ es basa en dos encaminadors. El principal problema és que els encaminadors són menys segurs que un conjunt de dispositius correctament

configurats. És a dir, un tallafoc. En la figura 2.8 podem veure com es col·loquen els elements per configurar l'arquitectura de seguretat.

Figura 2.8. Tallafoc en configuració d'arquitectura forta de subxarxa protegida



La complexitat d'aquesta arquitectura comporta problemes com la gestió, el cost o el rendiment del trànsit amb la xarxa externa. Alguns dels avantatges són la seva elevada modularització i l'augment de seguretat que comporta.

2.2 Xarxes privades virtuals. VPN

Una **xarxa privada virtual**o VPN (*Virtual Private Network)* és una xarxa privada que s'estén a diferents punts remots mitjançant l'ús d'infraestructures públiques de transport (com per exemple, Internet). La transmissió de paquets de dades es realitza mitjançant un procés d'encapsulació i, per seguretat, de xifrat, ja que no cal oblidar que les dades circulen durant un temps per trams de xarxa pública. Aquests paquets de dades de la xarxa privada viatgen a través d'un "túnel" definit a la xarxa pública. És a dir, s'aprofita el baix cost de l'accés a Internet, s'afegeixen tècniques de xifratge fort per aconseguir seguretat i se simulen les clàssiques connexions punt a punt.

Així, un usuari (una sucursal de l'organització, un teletreballador, un representant comercial...) connectat a través d'Internet a la xarxa corporativa de l'organització,

establint un túnel VPN, pot funcionar com si estigués dins de l'organització a tots els efectes de connectivitat.

En el cas d'accés remot des d'un equip, la VPN permet a l'usuari accedir a la seva xarxa corporativa i li assigna al seu ordinador remot les adreces i privilegis d'aquesta xarxa, encara que la connexió s'hagi efectuat mitjançant una xarxa pública com Internet.

La característica que converteix la connexió "pública" en "privada" és el que s'anomena un *túnel*, terme referit a que únicament ambdós extrems són capaços de veure el que es transmet pel túnel, convenientment xifrat i protegit de la resta d'Internet. La tecnologia de túnel xifra i encapsula els protocols de xarxa que s'utilitzen en els extrems sobre el protocol IP. D'aquesta manera podem operar com si es tractés d'un enllaç dedicat convencional, de forma transparent per a l'usuari.

2.2.1 Beneficis i inconvenients de les VPN envers les línies dedicades

Una connexió VPN permet tenir una connexió de xarxa amb totes les característiques de la xarxa privada a la qual ens volem connectar. El client VPN passa a ser un equip igual que la resta dels connectats al sistema. Tindrà, per tant, tots els permisos i directrius de seguretat d'un ordenador de la xarxa. Tot plegat té un seguit d'avantatges i alguns inconvenients.

Avantatges:

- **Seguretat**: és possible assegurar diversos serveis amb aquest mecanisme.
- **Mobilitat**: tenim una connexió segura entre usuaris mòbils i la nostra xarxa fixa, amb independència de la localització geogràfica.
- **Transparència**: permet la interconnexió d'ordenadors en un sistema informàtic, però també de diferents xarxes. Tot de manera transparent per a l'usuari final, ja que la configuració es pot fer només en l'entorn de passarel·la (sistema de maquinari i programari per interconnectar dues xarxes que utilitzen protocols diferents).
- **Simplicitat**: una VPN aconsegueix que l'equip sigui vist per tota la xarxa, incloent servidors, la qual cosa simplifica l'administració d'equips remots.
- **Estalvi econòmic**: el trànsit segur de paquets per xarxes públiques té un cost econòmic sensiblement menor que la creació d'una xarxa dedicada.

Inconvenients:

- **Fiabilitat**: la dependència del proveïdor de xarxa (ISP) pot produir fallades en la xarxa que poden deixar incomunicats recursos de la nostra VPN.

- **Confiança**: si la seguretat d'un node o subxarxa que forma part d'una VPN queda compromesa es veurà afectada la seguretat de tots els components de la xarxa.

2.2.2 Nivell de xarxa a VPN: SSL, TLS i IPSec

Com hem comentat, per implementar una VPN necessitem un protocol que xifri les comunicacions per evitar que puguin ser vistes per terceres persones. Existeixen diversos protocols criptogràfics per fer comunicacions punt a punt (VPN) a través d'Internet.

SSL

El *Secure Sockets Layer* o SSL ens dona autenticació i privacitat de la informació entre extrems a Internet mitjançant l'ús de criptografia. Habitualment, només s'autentica (es garanteix la seva identitat) el servidor, mentre que el client es manté sense autenticar.

Etapes bàsiques de l'SSL:

- Negociar entre les parts l'algorisme que s'utilitzarà en la comunicació. En aquesta etapa, client i servidor negocien els algorismes criptogràfics a utilitzar. Alguns dels algorismes més usats són RSA, Diffie-Hellman, DSA, RC2, RC4, IDEA (*International Data Encryption Algorithm*), DES (*Data Encryption Standard)*, Triple DES i AES (*Advanced Encryption Standard*) o SHA.
- Intercanviar les claus.
- Fer la transmissió.

TLS

El *Transport Layer Security* o TLS és una evolució del protocol SSL. La connexió es fa mitjançant un canal xifrat entre el client i servidor. D'aquesta manera l'intercanvi d'informació es realitza en un entorn segur i lliure d'atacs. Normalment, el servidor és l'únic que és autenticat, garantint així la seva identitat. El client es manté sense autenticar, ja que per a l'autenticació mútua es necessita una infraestructura de claus públiques.

IPSec

L'*Internet Protocol Security* o (IPSec) és un conjunt d'estàndards industrials que comproven, autentiquen i xifren les dades en els paquets IP. IPSec aporta diverses propietats: confidencialitat mitjançant el xifratge de trànsit IP, autenticació i

prevenció contra els atacs de reproducció i integritat mitjançant el rebuig del trànsit modificat. L'IPSec utilitza certificats (signats digitalment per una entitat emissora de certificats) per comprovar la identitat d'un usuari, equip o servei, que enllacen de forma segura una clau pública a l'entitat que disposa de la clau privada corresponent.

2.2.3 Nivell d'aplicació a VPN. L'SSH

El *Secure Shell* o SSH és un protocol que permet als equips establir una connexió segura, de manera que un client (un usuari o fins i tot un equip) pot obrir una sessió interactiva en una màquina remota (servidor) per enviar ordres o fitxers a través d'un canal segur.

- Les dades que circulen entre el client i el servidor estan **xifrades**, la qual cosa en garanteix la confidencialitat (ningú més que el servidor i el client poden llegir la informació que s'envia per la xarxa).
- **El client i el servidor s'autentifiquen mútuament** per assegurar que les dues màquines que es comuniquen són, de fet, aquelles que les altres parts creuen que són. L'intrús informàtic ja no pot adoptar la identitat del client o del servidor.

Una connexió SSH s'estableix en diverses fases:

- Es determina la **identitat** del servidor i del client per establir un canal segur (capa segura de transport). El client inicia sessió en el servidor.
- Establiment d'un **canal segur**. L'establiment d'una capa segura de transport comença amb la fase de negociació entre el client i el servidor per posar-se d'acord en els mètodes de xifratge que volen utilitzar. El protocol SSH està dissenyat per treballar amb un gran nombre d'algorismes de xifrat, per això, tant el client com el servidor han d'acordar primer els algoritmes que admeten.
- **Autenticació**. Un cop s'ha establert la connexió segura entre el client i el servidor, el client s'ha de connectar al servidor per obtenir un dret d'accés. Hi ha diversos mètodes:
- El mètode més conegut és la **contrasenya** tradicional. El client envia un nom d'accés i una contrasenya al servidor mitjançant la connexió segura i el servidor verifica que l'usuari en qüestió té accés a l'equip i que la contrasenya subministrada és vàlida.
- Un mètode menys conegut, però més flexible, és l'ús de **claus públiques**. Si el client tria la clau d'autenticació, el servidor crearà un desafiament (*challenge)* i donarà accés al client si aquest és capaç de desxifrar el desafiament amb la seva clau privada.

2.3 Servidors d'accés remot

Un **servidor d'accés remot** és un equip que permet a altres equips connectar-s'hi i a través seu permet l'accés a dispositius o informació que estan a la xarxa. La connexió es pot fer, per exemple, per via telefònica o per Internet.

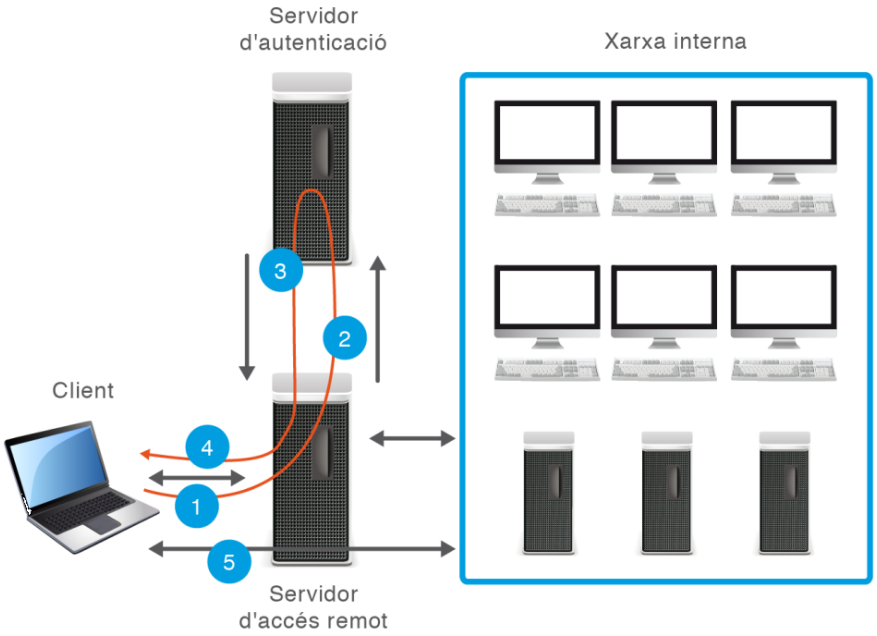
Els servidors d'accés remot també s'anomenen *servidors de comunicacions*. El terme anglès es *Remote Access Server* (RAS).

El servidor RAS controla les línies d'accés, com per exemple mòdems o altres canals de comunicació de la xarxa, perquè les peticions connectin amb la xarxa. El servidor reconeix la petició de la xarxa i realitza l'autenticació i els procediments necessaris per registrar un usuari a la xarxa i permetre-li l'accés als recursos.

Una vegada l'usuari s'ha autenticat, pot accedir a les unitats i impressores compartides com si estigués connectat físicament a la xarxa de l'organització. El servidor RAS conté múltiples canals de comunicació junts. Els canals són bidireccionals i, per tant, diversos equips es poden connectar a un únic recurs o un únic equip es pot connectar a múltiples recursos.

En la figura 2.9 es poden veure els passos necessaris per accedir als recursos de la xarxa.

FIGURA 2.9. Passos per poder accedir a recursos remots des d'un client



Les xarxes de banda ample com ADSL han deixat obsolet l'ús dels mòdems a través de la línia telefònica.

1. El primer pas (tal com es veu a la figura 2.9) és la connexió a l'equip. Es pot fer via mòdem (ja obsolet) o per una xarxa pública com Internet.

2. L'autenticació es realitza mitjançant un servidor d'autenticació, que garanteix que els elements són qui diuen que són. Aquest servidor d'autenticació pot ser un procés dins del mateix servidor d'accés remot, pot ser un altre servidor de l'organització o fins i tot un servidor aliè. Aquest darrer cas s'aplica amb els dipòsits de claus en estructura de clau asimètrica.

3. El servidor d'autenticació dona el vistiplau a les entitats, i envia al servidor d'accés remot els privilegis i credencials que la connexió, ara amb l'usuari conegut, té.
4. El servidor d'accés remot notifica al client que ha estat correctament identificat i que pot iniciar les peticions de recursos remots.
5. Una vegada autenticades les entitats, el servidor d'accés remot proveeix la comunicació entre el client i els recursos sol·licitats (la xarxa interna).

2.3.1 Protocols d'autenticació

La major part dels sistemes informàtics i xarxes mantenen de una manera o altra una relació d'identitats personals (usuaris) associades normalment amb un perfil de seguretat, rols i permisos. L'autenticació d'usuaris és el pas més crític en la connexió a un servidor d'accés remot ja que cal verificar la identitat de l'entitat que demana permís per accedir als recursos. Els sistemes d'autenticació permeten a aquests sistemes assumir amb una seguretat raonable que qui s'està connectant és qui diu ser. Això, posteriorment, permet que les accions que s'executin en el sistema puguin relacionar-se amb aquesta identitat i aplicar els mecanismes d'autorització i d'auditoria oportuns.

Un protocol d'autenticació és un tipus de protocol criptogràfic que té el propòsit d'autenticar (identificar) de manera unívoca entitats que desitgen comunicar-se de forma segura. Els protocols d'autenticació es negocien immediatament després de determinar la qualitat de l'enllaç i abans de negociar el nivell de xarxa.

L'autenticació és el pas preliminar per tenir accés als recursos remots.

El procés general d'autenticació consta dels passos següents:

- L'usuari sol·licita accés al sistema.
- El sistema demana a l'usuari que s'autentiqui.
- L'usuari aporta les credencials que l'identifiquen i permeten verificar l'autenticitat de la identificació.
- El sistema valida segons les seves regles si les credencials aportades són suficients per donar accés a l'usuari o no.

Alguns dels protocols d'autenticació més usats són PAP, CHAP, EAP, PEAP i Kerberos.

PAP

SPAP

El SPAP (*Shiva Password Authentication*) és el protocol d'autenticació de contrasenya de Shiva. És una variant del PAP. El client envia una contrasenya xifrada al servidor d'accés remot. Aquest desxifra la contrasenya i contesta en clar per autenticar al client d'accés remot.

El PAP (*Password Authentication Protocol*) és un protocol d'autenticació simple en el qual el nom d'usuari i la contrasenya s'envien al servidor d'accés remot en text clar (sense xifrar). No es recomana utilitzar PAP, ja que les contrasenyes es poden llegir fàcilment. El PAP només s'usa per connectar a servidors d'accés remot antics basats en Unix que no admeten mètodes d'autenticació més segurs.

CHAP

El CHAP (*Challenge Handshake Authentication Protocol*) és un mètode d'autenticació usat per servidors als quals s'accedeix a través del protocol PPP (*Point-to-Point Protocol*). El CHAP verifica la identitat del client amb un procés de tres etapes. Periòdicament repeteix el procés de verificació.

L'MS-CHAP és una variant del protocol d'autenticació CHAP usat per Microsoft.

- S'estableix l'enllaç i l'autenticador envia un missatge per demanar a l'usuari que s'identifiqui.
- L'equip usuari respon amb un valor calculat, una funció resum d'un sol sentit, com per exemple la suma de comprovació MD5.
- L'autenticador verifica la resposta amb el resultat d'un càlcul propi del *hash*. Si el valor coincideix, l'autenticador informa de la verificació, si no, anul·la la connexió.
- Cada cert temps, a l'atzar, l'autenticador realitza una nova comprovació de veracitat, tot repetint el procés.

EAP: autenticació extensible

L'EAP (*Extensible Authentication Protocol*) és un protocol per donar suport a mecanismes d'autenticació. Ofereix funcions per poder negociar els mecanismes d'autenticació escollits. Aquests mecanismes són anomenats mètodes EAP. Està definit en el memoràndum RFC 3748.

L'EAP s'ha fet molt popular en xarxes sense fil, com per exemple l'estàndard IEEE 802.11, WPA o WPA2.

PEAP: protocol d'autenticació extensible protegit

El PEAP (*Protected Extensible Authentication Protocol)* és un protocol de la família de protocols EAP. Utilitza seguretat de nivell de transport (TLS) per crear un canal xifrat entre un client d'autenticació PEAP (com un equip amb connexió sense fill) i un autenticador PEAP (per exemple un servei d'autenticació remota com RADIUS).

Per millorar els protocols EAP així com la seguretat de xarxa, el PEAP proporciona:

- Protecció de la negociació del mètode EAP. Aquesta es realitza entre el client i el servidor usant un canal TLS. D'aquesta manera s'impedeix que un intrús insereixi paquets entre el client i el servidor. El canal TLS xifrat també ajuda a evitar atacs per denegació de servei.
- Autenticació mútua.
- Protecció contra la creació d'un punt d'accés sense fils (WAP) no autoritzat.
- Reconnexió ràpida, que redueix el temps de retard entre la sol·licitud d'autenticació d'un client i la resposta del servidor d'autenticació.

El procés d'autenticació PEAP entre el client i l'autenticador PEAP es fa en dues etapes. Primer es configura un canal segur entre el client i el servidor d'autenticació. En la segona es produeix l'autenticació EAP entre el client i l'autenticador EAP.

Kerberos

El procediment usat per Kerberos s'anomena *autenticació mútua*. Tant el client com el servidor verifiquen la identitat de l'altre.

Kerberos és un protocol d'autenticació de xarxes basat en el protocol de Needham-Schroeder. Permet a dos ordinadors en una xarxa insegura demostrar la seva identitat. Kerberos es basa en criptografia de clau simètrica i necessita d'una tercera part de confiança.

Hi ha extensions del protocol Kerberos que permeten utilitzar criptografia de clau asimètrica.

La tercera part de confiança s'anomena *centre de distribució de claus* o KDC. Consta de dues parts lògiques separades. Un servidor d'autenticació i un servidor de tiquets. Els tiquets usen per demostrar la identitat dels usuaris. El sistema manté una base de dades de claus secretes. Cada entitat, ja sigui client o servidor la comparteix i és coneguda només per ell i Kerberos. El coneixement d'aquesta clau serveix per provar la identitat de l'entitat i assegurar la comunicació.

El funcionament, bàsicament, és el següent. El client s'autentica a sí mateix contra el servidor d'autenticació. El client rep la verificació i l'utilitza per demostrar al servidor de tiquets la seva identitat. El servidor de tiquets crea un tiquet, l'encripta amb les claus de l'usuari i li envia. A partir d'aquest moment ja es pot fer ús del servei.

El tiquet es configura perquè caduqui al cap d'un temps, habitualment unes hores. Un tiquet compromès, per tant, només serviria a l'intrús durant un breu període de temps.

2.3.2 Configuració de paràmetres d'accés

La connexió d'un equip client a una xarxa necessita diversos paràmetres per assegurar que la connexió es realitza correctament. Aquests paràmetres bàsicament han de contenir els elements per autenticar-se i els elements que ens permeten establir la connexió amb l'equip d'accés remot. Serà l'equip remot, usant el servidor d'autenticació, el que gestionarà els nostres privilegis efectius dins de la xarxa de l'organització.

En l'equip client és necessari:

Al web d'aquesta unitat podeu consultar l'annex "Xarxes Privades Virtuals" on s'explica pas a pas la configuració d'una xarxa pública virtual o VPN.

- El protocol de comunicació que haurà d'usar el client per connectar-se al servidor d'accés remot. A vegades l'equip client no té el controlador amb el protocol i cal instal·lar-lo. Passa , per exemple, amb l'IPSec en Windows XP.
- Els elements d'autenticació de l'entitat, que usualment són l'usuari i la contrasenya.

- El nom o la IP de l'equip d'accés remot amb qui farem la connexió.
- Elements addicionals, com per exemple el certificat digital si s'utilitzen protocols que requereixin criptografia de clau pública.

2.3.3 Servidors d'autenticació

El servidor d'autenticació és un dispositiu que controla qui pot accedir a una xarxa informàtica. Ha de proveir a la xarxa les funcions d'autorització, privacitat i no repudi. L'autorització determina els privilegis atorgats a una entitat o usuari i, per tant, a quins objectes o dades l'usuari pot tenir accés. La privacitat assegura que la informació es divulgui només a persones autoritzades. El no repudi es refereix al fet que el servidor d'autenticació pot registrar tots els accessos a la xarxa i les dades d'identificació. D'aquesta manera, un usuari no pot negar que ha accedit a un equip o que n'ha modificat les dades. Molt sovint, el no repudi és un requisit legal.

El servidor d'autenticació verifica mitjançant un protocol d'autenticació la identitat de l'equip que desitja connectar-se. Una vegada feta l'autenticació, llavors un servidor d'accés remot subministra els recursos.

El servidor d'autenticació conté un "diposit" (algun tipus de base de dades) amb els usuaris, permisos i credencials que el servidor d'accés remot usarà per saber el nivell de privilegis a assignar a la connexió.

Servidor d'autenticació

Un servidor d'autenticació pot estar en un servidor d'accés a la xarxa informàtica, una part d'un tallafoc o un altre tipus de maquinari per controlar l'accés a la xarxa. Independentment del tipus de màquina que allotja el programa d'autenticació, el terme servidor d'autenticació continua sent generalment utilitzat per referir-se a la combinació de maquinari i programari que realitza la funció d'autenticació.

Per tant, independent del protocol d'autenticació usat, el servidor d'autenticació ha de tenir emmagatzemada informació relacionada amb l'entitat (ja sigui un usuari o un equip remot). Existeixen, des d'aquest punt de vista, diferents servidors d'autenticació.

Entre els servidors d'autenticació més coneguts trobem:

- ***OpenLDAP***: és una implementació lliure i de font pública del protocol *Lightweight Directory Access Protocol* (LDAP) desenvolupada pel projecte OpenLDAP. L'LDAP és un protocol de comunicació independent de la plataforma.
- ***Active Directory***: és el nom utilitzat per Microsoft com a magatzem centralitzat d'informació d'un dels seus dominis d'administració.
- ***Novell Directory Services***: també conegut com eDirectory, és la implementació de Novell utilitzada per gestionar l'accés a recursos en diferents servidors i ordinadors d'una xarxa.
- ***Red Hat Directory Server***: és un servidor basat en l'LDAP que centralitza la configuració d'aplicacions, perfils d'usuaris, informació de grups i polítiques, així com informació de control d'accés, dins d'un sistema operatiu independent de la plataforma.