Universitat Oberta de Catalunya (UOC)

Grau Tecnologies de Telecomunicació

(Integració de xarxes telemàtiques)

Títol: " Revisió de la taxonomia dels atacs en xarxes i la seva implicació en les polítiques de seguretat corporativa amb auditoria de seguretat."

(TFC-Juny-2013)

Consultor: Miquel Font Rossello

Professor responsable: Xavi Vilajosana Guillén

ÍNDEX DEL PFG

-Introducció al projecte. Justificació i resum descriptiu. Índex.:(2)

Part I: Resum general del projecte (4)
Part II: Aplicacions i projecció directa del projecte (5)
Part III: Objectius prioritaris del projecte (7)
Part IV: Descripció dels mòduls del projecte (11)

– **Mòdul I: Aspectes organitzatius i legals de la política de seguretat. L'estàndard ISO 17799**

1.1 Principis bàsics (12)
1.2 La seguretat a entorns d'e-comerç.(13)
1.3 La seguretat en sistemes Open Source.(16)
1.4 Tipologia dels atacs i plans de contingència.(17)
1.5 Política de seguretat corporativa.(20)
1.5.1 Aspectes legals de la política de seguretat en xarxes.(24)
1.5.2 Aspectes lògics i de topologia (27)
1.5.3 Repercussió en els aspectes organitzatius i de RR.HH.(34)
1.5.4 Aspectes físics de les polítiques de seguretat de xarxa.(36)

– **Mòdul II: Atacs corporatius i mecanismes de seguretat.**

2.1 Elements bàsics de seguretat.(39)
2.2 Origen de les amenaces: tipologia i normativa de seguretat. (42)
2.3 Mecanismes de seguretat. Plans de contingència empresarial.(45)
2.4 Tipificació i anàlisi dels atacs corporatius.(46)
2.4.1 MITM (Man in the Middle) (46)
2.4.2 Denegació de serveis (DoS) (49)
2.4.3 Atacs remots i intercepció (54)
2.4.4 Spoofing i escaneig de llocs. (57)
2.5 Orientació dels atacs (59)
2.5.1 Atacs al sistema (core attack) (62)
2.5.2 Atacs a la plataforma web (feblesa de plataformes d'e-comerç) (62)
2.5.3 Atacs orientades a objectius BBDD. Virus i troians (66)

– **Mòdul III: sistemes IDS de detecció d'intrusos. Auditoria de seguretat**

3.1 Arquitectura IDS per a administradors (68)
3.1.1 Exploració de dades en temps real (71)
3.1.2 Agents autònoms. Coordinació arquitectura IDS. (71)
3.2 Models de detecció. (72)
3.3 Característiques d'implantació d'un IDS.(72)

-Conclusions finals (74)
-Bibliografia (75)
-Annex I: NESSUS, SATAN,SAINT i altres opcions (78)
-Annex II: Virus i antivirus (89)
-Annex III: Gantt - Openproj GNU (95)

Part I: Resum general del projecte.

L'objectiu d'aquest treball fi de grau és analitzar les diverses característiques i funcionalitats de les polítiques de seguretat corporativa. Al llarg de la meva carrera professional he participat activament en aquest tipus de projectes relacionats amb plans de contingència, seguretat de servidors crítics (SAP) i en aplicacions de models client-servidor amb càrrega alta, i en la meva opinió estic preparat per realitzar un projecte aplicable a la nostra realitat empresarial i ales demandes de seguretat informàtica d'aquest sector.

La planificació temàtica se centraria en els aspectes organitzatius i físics de la Política de seguretat corporativa (amb la meva experiència professional), en l'anàlisi de la taxonomia dels atacs (MITM, Spoofing, Dialers, [DoS] Denial-Of-Service...), alhora de justificar l'arquitectura i topologia IDS, amb una visió global en el cas d'Apatxe (SSL, CRT, CSR...) i de la temàtica de l'autenticació (HTTP Digest/Basic), amb algunes pinzellades de seguretat web pràctica (phpMyAdmin, XAMP...) Malgrat que el tema és basic per la nostra especialització d'enginyeria, el meu desenvolupament serà diferencial i podré exposar gran part dels meus coneixements professionals adquirits al llarg del temps, i sobre les competències assimilades durant aquests anys de formació reglada. Confio que aquesta concepció temàtica del meu projecte obri una finestra cap a un nou interès creixent per part dels professionals d'informàtica i telecomunicacions en la importància crítica d'aquestes polítiques de seguretat, per a poder justificar i desenvolupar en un document preliminar tots els punts aquí esmentats. Aquest PFG vol ser una guia de referència sobre els condicionaments de les Polítiques de Seguretat Corporatives i d'Auditories de Seguretat. El meu nivell d'implicació és molt elevat, ja que finalitzo la meva titulació properament, i a més a més conservo el desig de matricular-me immediatament al màster de Seguretat Informàtica, que és la meva dedicació professional prioritària.

Saluts,

Yago Blanco Presas

PART II: Aplicacions i projecció directa del projecte

Justificació de la tria temàtica: internet ha esdevingut una part essencial del treball i amb el llarg dels anys, el contingut web s'ha tornat més interessant, però alhora més perillós defensar de mirades alienes, en evolucionar des de fullets en línia estàtics amb només texts i fotografies senzills fins a veritables arxius multimèdia dinàmics i interactius.

Segons la xarxa i els seus continguts son més sofisticats i accessibles, també són més variades i freqüents les amenaçes a la seguretat de la xarxa i en serveis telemàtics, a la productivitat dels empleats, a la responsabilitat corporativa i al consum de l'ample de banda.

En realitat, qualsevol sector comercial de qualsevol ciutat del món és també accessible als hackers. Qualsevol transacció econòmica realitzada amb mitjans tradicionals pot ser aprofitada per aquests agents externs per al seu propi benefici.

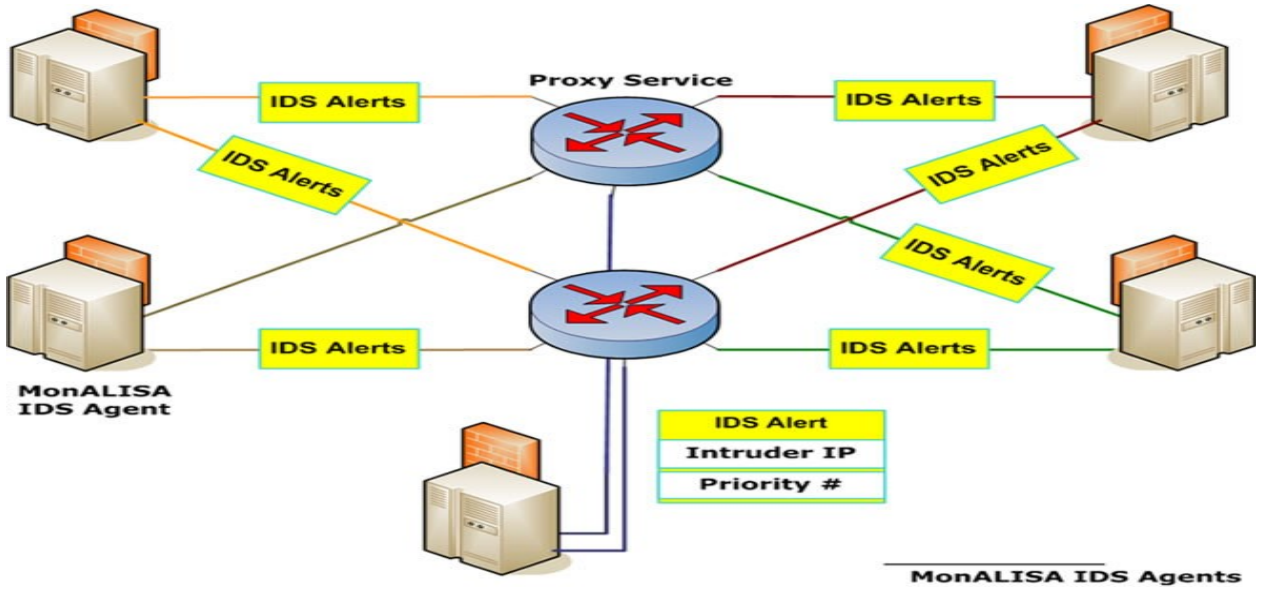
Les comunicacions comercials realitzades amb mitjans tradicionals, cartes o telèfon, són molt més fàcils d'interceptar que les comunicacions que es produeixen a Internet, però la seguretat electrònica exigeix unes competències professionals específiques que solament des d'una titulació d'enginyeria es poden modelar i condicionar per a un estudi detallat d'aquestes amenaces (realitzar activitats delictives en Internet requereix uns coneixements tècnics sofisticats que no es troben a l'abast de qualsevol persona.

Per una altra banda, les possibilitats de protecció de les comunicacions electròniques són molt més grans que les que permeten els mitjans tradicionals. Podem trobar software gratuït i molt fàcils de fer servir que permeten a qualsevol usuari l'encriptació dels seus missatges de manera que es garantiria plenament que només el destinatari podrà entendre'ls.

Els certificats i firmes electròniques garantixen la identitat dels subjectes amb més garantia que qualsevol fedatari tradicional. Els sistemes d'emmagatzematge de dades i la seva protecció front a accidents fortuïts o atacs intencionats són més fàcils, barats i segurs que les caixes fortes o les càmeres de seguretat.

El que ens trobem és que no existeix una cultura de seguretat a Internet. La societat en la que vivim ens ha ensenyat des de que érem petits unes regles bàsiques de protecció de les nostres propietats, però no estem preparats davant d'aquest allau de canvis provinents del boom de l'administració electrònica, les TICs i en general la societat de la informació, amb totes les seves grandioses avantatges e inconvenients.

El fet de tancar la porta de casa, els límits que ens imposem a la quantitat d'efectiu que portem a les butxaques, la forma en la que ens relacionem quan ens trobem amb un estrany pel carrer, són comportaments que hem après al llarg de la nostra vida. En canvi la nostra experiència amb Internet és molt breu i ni els nostres pares ni els nostres professors ens van dir mai com ens havíem de comportar en el ciberespai, i és a nivell professional quan es demanen Administradors de Sistemes implicats en el coneixement intrínsec dels mecanismes de protecció de la informació.



L'augment de les competències de coneixement derivades del boom dels atacs per part d'agents externs en recerca d'informació o col·lapsar sistemes legítims, ens porta a un augment del nivell de professionalitat i aprofundiment en coneixements per part de la secció d'enginyeria derivada a funcions d'Administració de Servidors i creació de topologies IDS, plans de contingència i polítiques de seguretat a tots els nivells. En aquest estudi se centra aquest PFG. Una oportunitat per a la reflexió sobre el que hem aconseguit aquests darrers anys en el sector de la seguretat en xarxes telemàtiques.

Part III: Objectius prioritaris del projecte

La protecció legal del comerç electrònic requereix també l'elaboració de noves formes. La protecció davant la publicitat no desitjada, que que suposa un cost de transmissió recau al consumidor i demana alhora un tractament diferent que quan el cost requeia exclusivament a l'anunciant. El reconeixement jurídic de les firmes electròniques i de l'arbitratge electrònic en els països de la Unió Europea ha establert un marc legal que garanteix la qualitat dels certificats i agilitza els tràmits judicials.

Els governs de tot el món estan interessats en promoure el desenvolupament del comerç electrònic, per això estan impulsant reformes legals i fiscals que permeten i fan més ràpides les transaccions mitjançant internet. En altres assignatures de la carrera de caràcter optatiu com Criptografia o el Màster de Seguretat Informàtica, es tracten aquests temes en profunditat, i és el meu desig obtenir el màxim de coneixement des de la meva perspectiva professional, els meus estudis en formació reglada i la meva dedicació personal.

Una anàlisi general dels principals elements dels plans corporatius relacionats amb Polítiques de Seguretat segons les normatives europees del sector, que serveixi de referència per a projectes concrets d'anàlisi de febleses i auditoria de seguretat informàtica, amb especial cura amb consideracions molt concretes que molts projectes de seguretat obvien o no tracten adequadament perquè són generats per revisió de projectes més antics que no configuren ni visualitzen els nous avenços tant en hardware com en software de seguretat de xarxes. S'analitzen tots els elements constructius tant físics com lògics de l'Administració de la Política de Seguretat, de manera concreta.

La política de seguretat d'una organització seria les normes, regles o lleis (escrites, si són publiques millor) que regeixen la vida de l'organització, tractant sobre el que es pot fer i el que no es pot fer. Algunes de les seves característiques són:

- Serveix per a comunicar un consens de l'ús de dades i aplicacions dintre de l'organització.
- Proporciona una base pera a la demostració de l'ús inapropiat de recursos, per part dels empleats o dels externs.
- Defineix el comportament apropiat per a cada cas.

Estableix quines eines són necessàries i quins procediments.

Una política de seguretat pot ser prohibitiva, si totes les coses que no es troben expressament prohibides estan denegades, o si tot el que no es troba expressament prohibit es permet.

Evidentment la primera aproximació és molt millor que la segona, si parlem de mantenir la seguretat d'un sistema, en aquest cas la política contemplaria totes les

activitats que es poden realitzar en els sistemes, i la resta serien considerades il·legals. És important que qualsevol política contempli sis elements claus en la seguretat d'un sistema informàtic:

- Integritat: la informació del sistema es trobarà disponible, de la mateixa manera que es va emmagatzemar per part d'un agent autoritzat.

- Autenticitat: el sistema serà capaç de verificar la identitat dels seus usuaris, i els usuaris la del sistema.

- Confidencialitat: la informació solament es trobarà disponible per als agents autoritzats, especialment el seu propietari.

- Disponibilitat: és necessari garantir que els recursos del sistema es trobaran disponibles quan siguin necessaris, especialment la informació crítica.

- Utilitat: els recursos del sistema i la informació que es faci servir serà útil per alguna de les funcions.

Per a cobrir de manera adient els sis elements anteriors, amb l'objectiu permanent de garantir la seguretat corporativa, una política normalment es divideix en punts més concrets, de vegades anomenades normatives. L'estàndard **ISO 17799** defineix les següents línies d'actuació:

- Seguretat física i de l'entorn: s'engloben aspectes relatius a la seguretat física dels recintes on es troben els diferents recursos de l'organització i dels sistemes, així com la definició de controls genèrics de seguretat.

- Gestió de comunicacions i operacions: aquest és un dels punts més interessants si l'analitzem tècnicament parlant, ja que es refereix a aspectes de la seguretat relatius a l'operació dels sistemes i telecomunicacions, com els controls de xarxa, la protecció davant del malware, la gestió de còpies de seguretat o l'intercanvi de software dintre de l'organització.

- Controls d'accés: definició i gestió de punts de control d'accés als recursos informàtics de l'organització: contrasenyes, seguretat perimetral, monitorització d'accessos...

- Desenvolupament i manteniment de sistemes: seguretat en el desenvolupament i les aplicacions, xifrat de dades, control de software...

- Seguretat organitzacional: aspectes relatius a la gestió de la seguretat dintre de l'organització (cooperació amb elements externs, outsourcing, estructura de l'àrea de seguretat...).

- Classificació i control d'actius: inventari d'actius i definició dels seus mecanismes de control, així com l'etiquetat i classificació de la informació corporativa.

- Gestió de continuïtat del negoci: definició de plans de continuïtat, anàlisi d'impacte, simulacres de catàstrofes...

- Requeriments legals: evidentment, és necessari que la política compleixi la normativa vigent del país on s'aplica, si una organització s'estén al llarg de diferents països, la seva política serà coherent amb la normativa del més restrictiu d'ells. En aquest apartat de la política s'estableixen les relacions amb cadascuna de les lleis, drets de propietat intel·lectual, tractament de dades de caire personal, exportació de xifrat... juntament amb tots els aspectes relacionats amb registres d'esdeveniments en els recursos (logs) i el seu manteniment.

- Seguretat del personal: formació en matèries de seguretat, clàusules de confidencialitat, report d'incidents, monitorització de personal...

És per això que li donem prioritat a elements de disseny relacionats amb la tipificació dels atacs web, atacs DoS i especialment als temuts atacs MITM, també les febleses pròpies dels diferents bugs de les versions concretes revisades del servir, establint fissures en seguretat provocades per la topologia i infraestructura de la xarxa.

Es completa com objectiu secundari amb la informació actualitzada referida a atacs a plataformes web de comerç electrònic i assumptes de criptografia. El projecte abans que res és una anàlisi de les referències actualitzades per al disseny d'aquest tipus de projectes.

PART IV: Descripció dels mòduls del projecte

Els principals mòduls se subdivideixen en els següents elements constructius del projecte:

- En el primer mòdul es tractarien els aspectes legals de la política de seguretat i la seva implicació en els aspectes de RR.HH i organitzatius de la corporació, realitzant una revisió dels aspectes de topologia, lògics i físics relacionats amb la seguretat de les xarxes telemàtiques, els tipus d'atacs més freqüents, i en el context de la seguretat en aplicacions de càrrega crítica, servidors de bases de dades i ERP/CMR empresarial.

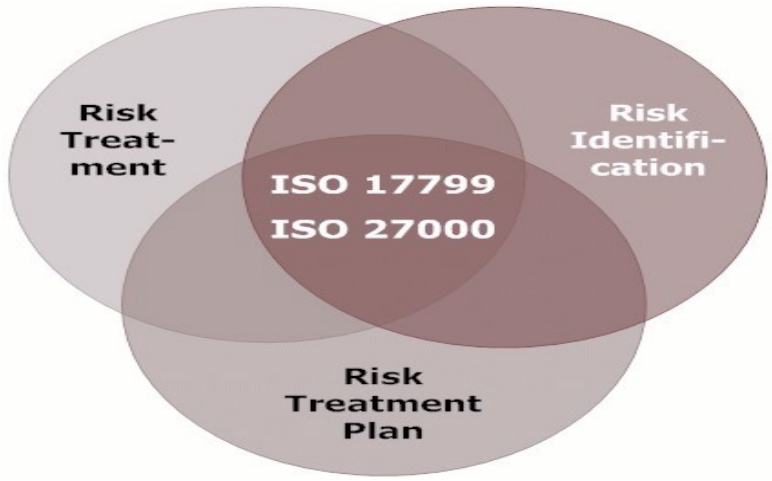
- En el segon mòdul es relacionarien aquests conceptes amb les amenaces lògiques, els atacs DoS, els elements bàsics de seguretat (nivells de Firewall, proxys intel·ligents...), l'origen de les amenaces i en general els mecanismes implicats i la taxonomia dels atacs, justificant la necessitat en la cadena de valor empresarial de les auditories de seguretat.

- En el tercer mòdul es desenvoluparia la implantació d' IDS, la seva arquitectura basada en agents autònoms, l'exploració de dades en temps real i l'ús de mineria de dades per a aspectes relacionats amb la seguretat informàtica, i en l'àmbit de la parametrització bàsica en funció de les necessitats corporatives.

- En el quart mòdul final, s'analitzarà la problemàtica de l'autenticació basada en PHP, els certificats digitals, la firma digital, i la comprovació de l'entorn en servidors Apatxe (l'ús d'eines com Webmin de software lliure), i la interacció amb sistemes de gestió de bases de dades.

És una visió molt ambiciosa per a la concepció d'un projecte d'enginyeria amb competències de grau en telecomunicacions, però duré a bon port aquesta idealització metodològica fins a les seves darreres conseqüències, potenciant una visió real de les necessitats empresarials actuals en xarxes telemàtiques i integració de serveis.

Mòdul I: ASPECTES ORGANITZATIUS I LEGALS DE LA POLÍTICA DE SEGURETAT. L'ESTÀNDARD ISO 17799.



1.1 Principis bàsics

L'objectiu d'aquest projecte fi de carrera és realitzar un estudi exhaustiu de la implicació de desenvolupar sistemes web fiables. En concret hauríem de valorar els requisits necessaris per a adoptar un esquema de seguretat específic i les consideracions pertinents si parlem de polítiques de seguretat corporatives. Per això començarem amb una base teòrica i continuarem amb un desenvolupament pràctic dels coneixements obtinguts al llarg del projecte. Els objectius més rellevants els podem sintetitzar en els següents:

-Realitzar un estudi de l'abast de la seguretat en sistemes software, estudiant la taxonomia dels atacs, estudiant sistemes de detecció d'intrusos (IDS).

-Implantació d'esquemes de seguretat corporatiu.

-Implicació de la seguretat en el cas d'aplicacions web. Estudi d'autenticació d'usuaris mitjançant formularis, sessions, criptografia i firmes digitals.

-Estudiar les facilitats que ofereixen entorns de producció de software vinculats a la web.

-Adoptar alguns esquemes de seguretat específics i recopilar de manera esquemàtica els patrons adoptats.

1.2 La seguretat en entorns d'e-commerce.

El nostre mon és ple de sistemes, composats per màquines i per programes. Podríem dir que pràcticament tots els objectes que ens envolten són sistemes, formats per una o diverses màquines controlades per una o diverses peces de components que es denominen software. Molts d'aquests sistemes formen part de xarxes, privades o d'empresa, públiques, grans o petites, interconnectades unes amb les altres i comunicant-se entre elles mitjançant un altre gran sistema hardware gestionat per un conjunt d'aplicacions amb objectius diversos, als que denominem protocols. La xarxa Internet és, amb una probabilitat molt elevada, el sistema més complex que mai s'ha desenvolupat. Esta composada per milions d'ordinadors interconnectats mitjançant una xarxa física d'una complexitat molt elevada. A més a més, cada ordinador conté una gran quantitat de programes que interactuen entre si o amb uns altres ordinadors de la xarxa. Podem dir que els sistemes són complexos i alhora poden interactuar, també molts d'ells ens poden sorprendre amb accions no pensades ni dissenyades (bugs) pels seus creadors i usuaris, aquestes propietats fan que sigui molt difícil aconseguir que un sistema, com la xarxa d'una universitat, o la xarxa d'una gran empresa o Internet, sigui segura. Fins a finals de 1998 molt poca gent es prenia seriosament la seguretat a la xarxa. Per una banda Internet continua creixent exponencialment, i per altra el boom de la informàtica de consum produeix un augment espectacular en el nombre de pirates informàtics. Malgrat això, el 22 de novembre de 1988, Robert T. Morris va protagonitzar el primer gran incident de la seguretat informàtica: un dels seus programes es va convertir en el famós worm o cuc d'Internet. Milers d'ordinadors connectats a la xarxa es van veure inutilitzats durant dies, i les pèrdues s'estimen en milions de dòlars. Des d'aquell moment la seguretat en sistemes operatius, xarxes, seguretat física i lògica ha estat un factor molt important per a qualsevol organització.

Uns dels assumptes que és inevitable comentar en l'actualitat quan parlem

d'Internet i de la possibilitat de realitzar negocis a la xarxa, és la seguretat. A l'accedir a Internet, estem accedint en una gran societat en xarxa. Com es produeix en tota societat humana, no tot el que trobem és agradable. En el món *online* existeixen amenaces a la seguretat, de la mateixa forma que en la resta del món. Si aprenem a protegir-nos (a protegir l'equip i les dades), ens assegurarem que el temps que transcorre mentre estem online serà productiu i divertit. Els ordinadors i també Internet són alhora una part familiar de les nostres vides. Potser no ho veiem força sovint, però les trobem, involucrades d'una manera o una altra en la major part de les nostres activitats diàries, en els negocis de qualsevol empresa, en les institucions educatives, en les diferents àrees de govern, sense el recolzament d'aquestes eines cap d'elles podria gestionar l'impressionant quantitat d'informació que caracteritza la nostra societat. Però també existeix una problemàtica inherent, la seguretat. Cada cop més persones necessitarem conèixer l'ús dels ordinadors així com les proteccions que dia rere dia ens ofereixen per garantitzar-nos la seguretat en la gestió de la informació.

Podem entendre com a seguretat una característica de qualsevol sistema que ens indica que aquell sistema es troba lliure de tot perill, dany o risc, i que és, d'alguna manera, infal·lible. Com aquesta característica, particularitzant en el cas de la web, sistemes operatius o xarxes d'ordinadors, és impossible assegurar-la, se suavitza la definició de seguretat i ens referirem al terme fiabilitat (probabilitat de que un sistema es comporti tal i com ho esperàvem).

La popularització d'Internet ha aconseguit que la major part de les llars disposin d'ordinadors connectats a la xarxa. En un principi, navegar per Internet era massa car com per fer-ho només per diversió, però l'àmplia oferta de connexions de banda ampla i de tarifes planes ha aconseguit que en les llars on trobem un ordinador, pràcticament tota la família tingui la seva pròpia adreça de correu electrònic o cerquin informació a la xarxa de forma sistemàtica. Per suposat, això inclou també als nens i als adolescents, que han trobat en Internet un entreteniment de magnitud similar al que poden tenir amb la televisió. Una de les principals raons de la popularització i l'èxit d'Internet és que es tracta d'una xarxa oberta. Com el protocol emprat pels ordinadors que es connecten a Internet, TCP-IP, és gratuït, qualsevol xarxa i qualsevol ordinador pot connectar-se només amb els costos de la connexió. No hi ha cap propietari d'Internet, no hi ha cap autoritat central que pugui imposar un preu o unes condicions diferents de les estrictament tècniques. Existeixen centenars de milions d'usuaris a Internet. El càlcul estadístic del nombre d'usuaris que tenen accés a Internet ja no té gairebé sentit. Existeixen clubs, cafès-Internet i locutoris públics gestionats per institucions privades o públiques a ciutats de tot el món, també els

països menys desenvolupats, fet que produeix que milers de milions d'usuaris es puguin connectar en qualsevol moment, amb un cost inferior a un euro. Aquesta extraordinària facilitat d'accés i popularitat són els principals atractius des del punt de vista comercial però també són la causa per la qual Internet es troba oberta a tot tipus d'indesitjables.

Internet ha esdevingut una part essencial del treball, amb el pas del temps, el contingut web s'ha tornat més interessant, en evolucionar de fullets *online* estàtics amb només text i fotografies senzilles fins a arxius multimèdia dinàmics i interactius amb gràfics animats. Segons Internet i els seus continguts son més sofisticats i accessibles, també són més variades i freqüents les amenaces a la seguretat de la xarxa, a la productivitat dels empleats, a la responsabilitat corporativa i al consum de l'ampla de banda. En realitat, qualsevol carrer comercial de qualsevol ciutat del món és també accessible als malfactors. Qualsevol transacció econòmica realitzada per mitjans tradicionals pot ser aprofitada pels lladres. Les comunicacions comercials realitzades per mitjans tradicionals, cartes o telèfon, són molt més fàcils d'interceptar que les comunicacions que es produeixen a Internet. Realitzar activitats delictives en Internet requereix uns coneixements tècnics sofisticats que no es troben a l'abast de qualsevol.

D'altra banda, les possibilitats de protecció de les comunicacions electròniques són també molt més grans que les que permeten els mitjans tradicionals. Existeix software per a ordinadors gratuït i molt fàcil de fer servir que permeten a qualsevol usuari l'encriptació dels seus missatges de forma que esdevé plenament garantit que només el destinatari podrà entendre-ls. Els certificats i firmes electròniques garanteixen la identitat dels subjectes amb més garanties que qualsevol fedatari tradicional. Els sistemes de magatzematge de dades i la seva protecció enfront d'accidents fortuïts o atacs intencionats són més fàcils, barats i segurs que les caixes fortes o càmeres de seguretat.

Ens trobem però, que no existeix una cultura de la seguretat a Internet. La societat en la que vivim ens ha ensenyat des que érem petits unes regles bàsiques de protecció dels nostres béns materials. El fet de tancar la porta de casa, els límits que ens imposem a la quantitat d'efectiu que portem a les nostres butxaques, la forma en la que reaccionem quan ens aborda un estrany pel carrer, són comportaments que hem après al llarg de la nostra vida. Malgrat això, la nostra experiència amb Internet és molt més breu i ni els nostres pares ni els nostres professors ens van explicar com hauria de ser el nostre comportament en el ciberespai. La protecció legal del comerç

electrònic també ha produït una nova elaboració de normes. La protecció enfront de la publicitat no desitjada, que produeix un cost de transmissió que recau en el consumidor requereix ara un tractament diferent que quan el cost només depenia de l'anunciant. El reconeixement jurídic de les firmes electròniques i de l'arbitratge electrònic en els països de la Unió Europea ha establert un marc legal que garanteix la qualitat dels certificats i agilitza els tràmits judicials. Els governs de tot el món es troben interessats en promoure el desenvolupament del comerç electrònic, per això impulsen reformes legals i fiscals que permeten i fan més ràpides les transaccions mitjançant Internet.

La seguretat en Internet i les lleis que la protegeixen es basen principalment en els sistemes d'encriptació. Aquests sistemes són els que permeten que la informació que circula per Internet sigui indesxifrable, inintel·ligible per a qualsevol persona que no sigui la destinatària. En general, podem parlar de dues grans divisions en la seguretat:

-Seguretat física: es refereix a la protecció del hardware i dels suports de dades, així com a la dels edificis e instal·lacions on es troben. Contempla les situacions d'incendis, sabotatges, robatoris, catàstrofes naturals, etc.

-Seguretat lògica: es refereix a la seguretat d'ús del software, a la protecció de les dades, processos i programes, així com a la de l'ordinador i accés autoritzat dels usuaris a la informació.

1.3 La seguretat en sistemes Open Source.

En aquest projecte farem referència a seguretat lògica, ja que si parlem de seguretat física, això formaria part d'unes altres instàncies distintes a les d'un programador web. Fent un esbós general, s'entén que mantenir un sistema fiable consisteix bàsicament en garantir tres aspectes:

-Confidencialitat: als objectes d'un sistema només poden accedir elements autoritzats. Assegura el secret de les comunicacions contingudes als missatges.

-Integritat: significa que els objectes solament poden ser modificats per elements autoritzats i d'una manera controlada. Fa referència al fet que la informació no pugui

ser manipulada en el procés d'enviament.

-Disponibilitat: indica que els objectes del sistema obligatòriament romanen accessibles a elements autoritzats.

L'objectiu és aconseguir la seguretat més completa per als sistemes, per això s'haurà de saber què es protegeix, contra qui es protegeix o en qui es pot confiar i en qui no. Se decidirà quins empleats tenen accés a què actius i perquè, quin tipus d'accés tindrà cada persona de l'organització que col·labori amb l'empresa, així mateix decidirem també quin tipus d'accés tindran els possibles clients de l'organització. Hem de pensar que una gran part dels servidors actuals es basen en desenvolupaments Open Source i existeix una gran quantitat de documentació per a treure profit de les seves febleses. També haurem de meditar el màxim possible qui i perquè voldria atacar a l'organització, però el perfil de l'atacant no s'ha de buscar només en un usuari d'Internet, sinó també dins de la mateixa organització, ja que diverses enquestes sobre pèrdues econòmiques analitzen que:

(i) Al voltant del 65% dels enquestats reconeixen patir atacs en l'últim any.
(ii) Al voltant del 60% dels enquestats reconeixen que alguns dels seus atacs van ser realitzats des de l'interior de les seves organitzacions.
(iii) Al voltant del 60% dels enquestats reconeixen que alguns dels seus atacs van ser realitzats mitjançant conexions des de la xarxa Internet.

1.4 Tipologia dels atacs i plans de contingència

Tipus d'atacants més habituals:

Hacker: els hackers eren persones expertes en un sistema operatiu, protocols, etc. En cas de trobar-se errades de seguretat d'un sistema, notificaven al fabricant, i sovint facilitaven també una possible solució. Però per distintes motivacions (revenja, ira, repte intel·lectual,...) algunes d'aquestes persones ataca les xarxes o sistemes d'una organització. Aquestes motivacions poden ser:

1 Empleats que són acomiadats injustament, sota el seu punt de vista i destrueixen dades de l'organització.
2 Empleats que entenen que el seu salari no és just, i alteren els registres de

personal.

3 Hackers que roben missatges de correu electrònic d'uns polítics per a uns altres polítics.

4 Individus que accedeixen a llocs web molt coneguts per canviar el seu contingut.

Un altre tipus d'atacants és “l'amateur que juga”, cada cop més estès, el seu perfil és el d'una persona jove sense experiència de sistemes ni de xarxes que fa servir eines automatitzades contra sistemes per Internet. Una persona pot crear una aplicació que desconnecti xarxes d'Internet, fent servir les febleses existents, fer-la amb un funcionament senzill, crear un manual d'usuari de l'eina i publicar-la en Internet, accessible a moltes persones al mateix temps, que la podran fer servir de forma incontrolada per aquest fi i moltes altres aplicacions. Finalment es parlarà d'un tercer tipus d'atacant, el menys nombrós però el més perillós, el professional. Es tracta de l'individu que fa servir els seus coneixements i experiència per atacar amb un objectiu concret, que pot ser el robatori, l'alteració d'informació amb fins delictius o el sabotatge. El professional obté una gran quantitat d'informació per assegurar-se de quins són els punts febles i on començar el seu treball. El següent pas normalment és l'atac d'accés a algun sistema, però eliminant les seves empremtes i sense fer cap alteració. Normalment deixa alguns camins de fugida possibles, ataca mitjançant salts i sap exactament on, quan i durant quant temps romandrà segur en el seu atac. Per saber com protegir-nos o quines tecnologies, mecanismes, sistemes concrets, processos que farem servir, haurem de conèixer dos assumptes d'una complexitat elevada:

5 els diversos tipus de possibles atacs.

6 les diverses defenses possibles.

És evident que mai es podran conèixer els diferents tipus d'atacs possibles. Els tipus més importants són:

7 Atacs per tal d'obtenir informació: són atacs que tenen com a objectiu obtenir informació com adreces IP de xarxes i sistemes, sistemes operatius de cada equip, números de ports oberts, aplicacions i les serves versions, contrasenyes, etc.

8 Atacs d'accés no autoritzat: són atacs de persones no autoritzades als sistemes. Normalment són demostracions de major interés que demostrar-se a sí mateixos que poden accedir a aquest sistema. Poder ser perillosos si l'accés es fa mitjançant un compte privilegiat del sistema.

9 Atacs amb revelació d'informació: un cop s'accedeix es pot fer servir aquest accés

per obtenir informació secreta, per tal d'aprofitar-se d'aquesta informació, d'eliminar-la o de modificar-la amb algun objectiu.

10 Atacs de denegació de servei: el seu objectiu és deixar no disponible un sistema, un servei o una xarxa, normalment esgotant el recurs, ja sigui l'ampla de banda, espai en el disc, connexions TCP, etc. Malauradament, per realitzar aquest tipus d'atac no es necessita tenir un accés previ al sistema.

Aquests són els atacs més importants, però cada vegada més solen ser combinacions de varis d'aquests atacs. Quant a les defenses possibles es destaquen les més importants:

11 Esquemes de seguretat de sistemes operatius: Especialment per al cas de servidors són informació molt rellevant i de dispositius de gestió de xarxa, s'han de mantenir uns bons esquemes de seguretat de fitxers, usuaris i aplicacions, així com de serveis de xarxa controlats des de tals sistemes.

12 Sistemes d'identificació o autenticació segurs: hi ha molts, des de les contrasenyes fins als sistemes biomètrics, certificats digitals, targetes d'identificació o diferents combinacions. Es poden usar tant per a accés local a dispositius com per a accés remot.

13 Sistemes de tallafocs (o *firewalls): Sistemes de control de la informació en forma de missatges que entren o surten d'una xarxa. Són molt populars avui dia i els hi ha de molts tipus diferents.

14 Sistemes criptogràfics: són sistemes que permeten, de diverses formes diferents, mantenir la integritat i l'autenticació de missatges o dades, així com la privadesa o confidencialitat dels mateixos. S'integren en protocols i part de diferents sistemes operatius i aplicacions, que usen algorismes criptogràfics.

15 Sistemes antivirus: són aplicacions locals, o distribuïdes, que permeten defensar-se dels virus informàtics, nom que reben algunes aplicacions utilitzades per a qualsevol dels atacs citats a dalt.

16 Sistemes d'anàlisis de vulnerabilitats: són aplicacions que permeten buscar en sistemes i aplicacions instal·lades diferents bugs o vulnerabilitats conegudes, per decidir si es corregeixen, es canvien de versió o es deixen com estan.

17 Sistemes de detecció d'intrusions: són sistemes o aplicacions que permeten, en temps real, detectar determinats tipus d'atacs i alertar sobre ells, alhora que, en alguns casos, poden parar-los.

Finalment, s'ha de saber quant diners es pot emprar a implantar i mantenir el sistema de seguretat, es tindrà en compte els diners que va a ser emprat en cadascuna de les següents tasques:

18 Adquisició d'eines, maquinària i programari, que implementin algunes de les defenses citades.

19 El temps emprat en configuracions i educar als usuaris en el seu ús.

20 El temps emprat en l'administració, manteniment i reconfiguració per permetre nous serveis, auditar les eines, etc.

21 El temps emprat a tornar a una situació estable, després de la inconveniència per als usuaris d'algun dels nous sistemes.

Finalment s'hauria de tractar de condensar tot aquest coneixement en una anàlisi de riscos que tindria 4 punts clau de cara als plans de contingència:

1. Valorar els actius.
2. Entendre totes les possible amenaces
3. Monitoritzar i conèixer totes les debilitats i vulnerabilitats del sistema.
4. Tractar d'engegar totes les mesures possibles per disminuir la probabilitat de tenir pèrdues.

1.5 Política de seguretat corporatives.

El terme política de seguretat se sol definir com el conjunt de requisits definits pels responsables directes o indirectes d'un sistema que indica en termes generals què està i què no està permès a l'àrea de seguretat durant l'operació general d'aquest sistema. En tractar-se de termes generals, aplicables a situacions o recursos molt diversos, sol ser necessari refinar els requisits de la política per convertir-los en

indicacions precises de què és el permès i el denegat en certa part de l'operació del sistema, la qual cosa es denomina política d'aplicació específica.

La política de seguretat és la forma raonable de contestar, de manera ordenada, als diferents problemes de seguretat que poden aparèixer a les xarxes de les organitzacions.

La política de seguretat d'una organització és alguna cosa així com les normes, regles o lleis (escrites, com més públiques, millor) que regeixen la vida de l'organització quant a què es pot fer i que no es pot fer. Algunes de les seves característiques són:

1 Defineix el comportament apropiat per a cada cas.
2 Estableix quines eines són necessàries i quins procediments.
3 Serveix per comunicar un consens de l'ús de dades i aplicacions dins de l'organització.
4 Proporciona una base per a la demostració de l'ús inadequat de recursos, per part d'empleats o d'externs.

Una política de seguretat pot ser prohibitiva, si tot el que no està expressament permès està denegat, o si tot el que no està expressament prohibit està permès. Evidentment la primera aproximació és molt millor que la segona de cara a mantenir la seguretat d'un sistema, en aquest cas la política contemplarà totes les activitats que es poden realitzar en els sistemes, i la resta serien considerades il·legals. Qualsevol política ha de contemplar sis elements claus en la seguretat d'un sistema informàtic:

Disponibilitat: És necessari garantir que els recursos del sistema es trobaran disponibles quan es necessiten, especialment la informació crítica.

Utilitat: Els recursos del sistema i la informació manejada en el mateix ha de ser útil per a alguna funció.

Integritat: La informació del sistema ha d'estar disponible tal com es va emmagatzemar per un agent autoritzat.

Autenticitat: El sistema ha de ser capaç de verificar la identitat dels seus usuaris, i els usuaris la del sistema.

Confidencialitat: La informació només ha d'estar disponible per a agents autoritzats, especialment el seu propietari.

Les aplicacions Web, per definició, permeten l'accés d'usuaris a recursos centrals, el servidor Web i, a través d'aquest, a uns altres com els servidors de base de dades. Amb els coneixements i la implementació correcta de mesures de seguretat, es poden protegir els recursos així com proporcionar un entorn segur on els usuaris treballin còmodes amb la seva aplicació. Una aplicació Web, especialment una que es desplega en Internet, és un objectiu molt més atractiu per a un atacant que una aplicació autònoma o client-servidor típica. Hi ha diverses raons per a això:

-Disponibilitat i accessibilitat: Moltes aplicacions Web estan disponibles per als usuaris públics en qualsevol moment del dia o de la nit. Com els servidors Web han de permetre l'accés a usuaris públics i no tenen la protecció completa dels tallafocs típics d'una empresa.

-Familiaritat: La majoria dels atacants, fins i tot els menys sofisticats, coneixen les interfícies Web. Un navegador Web és fàcil d'obtenir i és un dels programes d'aplicació més comunes. El protocol HTTP està ben definit, i existeixen moltes eines de hacking creats específicament per ajudar als atacants a penetrar i comprometre aplicacions Web.

-Facilitat: La configuració d'un servidor Web, contenidor Web i aplicació Web per a ús públic és extremadament complexa. Els atacants, freqüentment, poden aprofitar aquesta complexitat i explotar deficiències en la configuració de l'aplicació o del sistema.

-Publicitat: L'al·licient d'alguns atacants experimentats és la publicitat, la fama, l'ego o un simple desig de provar que poden fer alguna cosa que poques altres persones poden fer. Desfigurar o comprometre un situat Web popular té molt més valor des de la perspectiva de les “relacions públiques” que comprometre una aplicació interna que utilitzen uns quants empleats corporatius.

-Possessió: Els propietaris d'un sistema han de ser capaços de controlar-ho en tot moment, perdre aquest control en favor d'un usuari maliciós compromet la seguretat del sistema cap a la resta d'usuaris.

Per cobrir de forma adequada els sis elements anteriors, amb l'objectiu permanent de garantir la seguretat corporativa, una política se sol dividir en punts més concrets de vegades anomenats normatives. L'estàndard ISO 17799 defineix les següents línies d'actuació:
1 Seguretat de l'organització: Aspectes relatius a la gestió de la seguretat dins de l'organització (cooperació amb elements externs, outsourcing, estructura de l'àrea de seguretat…).

2 Classificació i control d'actius: Inventari d'actius i definició dels seus mecanismes de control, així com etiquetatge i classificació de la informació corporativa.

3 Seguretat del personal: Formació en matèries de seguretat, clàusules de confidencialitat, reporti d'incidents, monitoratge de personal…

4 Seguretat física i de l'entorn: Sota aquest punt s'engloben aspectes relatius a la seguretat física dels recintes on es troben els diferents recursos de l'organització i dels sistemes en si, així com la definició de controls genèrics de seguretat.

5 Gestió de comunicacions i operacions: Est és un dels punts més interessants des d'un punt de vista estrictament tècnic, ja que engloba aspectes de la seguretat relatius a l'operació dels sistemes i telecomunicacions, com els controls de xarxa, la protecció enfront de malware, la gestió de còpies de seguretat o l'intercanvi de programari dins de l'organització.

6 Controls d'accés: Definició i gestió de punts de control d'accés als recursos informàtics de l'organització: contrasenyes, seguretat perimetral, monitoratge d'accessos…

7 Desenvolupament i manteniment de sistemes: Seguretat en el desenvolupament i les aplicacions, xifrat de dades, control de programari...

8 Gestió de continuïtat de negoci: Definició de plans de continuïtat, anàlisi d'impacte, simulacres de catàstrofes…

9 Requisits legals: Evidentment, una política ha de complir amb la normativa vigent al país on s'aplica, si una organització s'estén al llarg de diferents països, la seva política ha de ser coherent amb la normativa del més restrictiu d'ells. En aquest apartat de la política s'estableixen les relacions amb cada llei, drets de propietat

intel·lectual, tractament de dades de caràcter personal, exportació de xifrat, al costat de tots els aspectes relacionats amb els registres (logs).

1.5.1 Aspectes legals de la política de seguretat.

S'han d'assenyalar les normes legals que cal tenir en compte, avui dia, en el desenvolupament de qualsevol política de seguretat, així com una sèrie de punts clau, que han d'aparèixer en ella, com a conseqüència de l'aplicació de tals normes. Les normes vigents, que caldrà tenir en compte, són:

-Reial decret 994/1999, reglament de mesures de seguretat de fitxers amb dades personals.

-Llei orgànica de protecció de dades 15/1999 (LOPD).

-Llei de serveis de la societat de la informació i de comerç electrònic, *LSSICE, 34/2002.

Pel que fa al reial decret 94/1999, cal tenir en compte, entre unes altres, una sèrie de normes d'obligat compliment:

Segons el seu article 11.
“El responsable de Seguretat de la Direcció de Sistemes, els Responsables de Seguretat designats en altres Direccions i els Encarregats de tractament per tercers, seran els encarregats de coordinar i controlar les mesures de seguretat definides per als fitxers, incloent mitjançant la utilització de les eines necessàries, l'administració en l'assignació als usuaris i fitxers en els nivells i categories de seguretat requerides pel Propietari de les dades per a la seva aplicació quant a l'accés i tractament de les dades es refereix”.

També en l'article 11.
“La Direcciódе Sistemes, establirà un mecanisme que permeti la identificació de forma inequívoca i personalitzada de tot aquell usuari que intenti accedir al sistemes d'informació i la verificació que està autoritzat”.

Segons els seus articles 2 i 18.

“Es limitarà la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació”.

Segons l'article 24.
“De cada accés es guardaran, com a mínim la identificació de l'usuari, la data i hora en què es va realitzar, el fitxer accedit, el tipus d'accés i si ha estat autoritzat o denegat. En cas que l'accés hagi estat autoritzat, s'ha de guardar la informació que permeti identificar el registre accedit. Els mecanismes que permeten el registre del dades detallades, estaran sota el control del Responsable de Seguretat. En cap cas es permetrà la desactivació dels mateixos. El període mínim de conservació és de 2 anys. El Responsable de Seguretat s'encarregarà de revisar periòdicament la informació de control registrada i elaborarà un informe de revisions realitzades i problemes detectats almenys 1 vegada al mes”.

Segons l'article 17.
“Els sistemes d'informació i instal·lacions de tractament de dades se sotmetran a una auditoria interna o externa, que verifiqui l'empleno del Reglament, dels procediments i instruccions vigents en matèria de seguretat de dades, almenys cada dos anys”.

Segons l'article 5.
“En l'accés a dades a través de xarxes de comunicacions, el nivell de seguretat ha de ser equivalent als accessos en manera local”.
D'altra banda aquesta la LOPD, que el seu objectiu és garantir i protegir, en el que concerneix al tractament de les dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i especialment del seu honor i intimitat personal i familiar.

En referència a la LOPD, s'ha de destacar:

Article 4:
Les dades de caràcter personal només es podran recollir per al seu tractament, així com sotmetre'ls a aquest tractament, quan siguin adequats, pertinents i no excessius en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per les quals s'hagin obtingut. Les dades de caràcter personal objecte de tractament no podran usar-se per a finalitats incompatibles amb aquelles per les quals les dades haguessin estat recollits. No es considerarà incompatible el tractament posterior d'aquests amb finalitats històriques, estadístics o científics. En el cas que les dades siguin inexactes, hauran de ser rectificats o cancel·lats, reconeixent en tot caso la possibilitat d'accés

per part de l'interessat. Si les dades perden la seva finalitat originària hauran de ser cancel·lats.

Article 5:

En aquest article es tracta la recollida de dades, sent d'especial importància per a les persones que han de confeccionar els qüestionaris de recollida de dades, atès que els interessats hauran de ser informats del següent:

a) L'existència del fitxer o tractament de dades, la finalitat de la recollida i els destinataris de la informació.

b) El caràcter optatiu o obligatori de les preguntes.

c) Les conseqüències sobre l'obtenció de les dades, així com la negativa a subministrar-los.

d) La possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.

e) La identitat i adreça del responsable del tractament o el seu representant.

Article 6:

En aquest article es tracta el consentiment de l'afectat a l'hora de donar les seves dades. No obstant això, sense perjudici de les normes més rigoroses per a les dades especialment protegides, existeixen algunes excepcions al principi general, atès que, sempre que no es vulnerin els drets i llibertats fonamentals de l'interessat, no caldrà el consentiment en els següents suposats:

a) Quan les dades es recullin per a l'exercici de les funcions pròpies de les Administracions públiques en l'àmbit de les seves competències.

b) Quan es refereixin a les parts en una relació comercial, laboral o administrativa, sempre que sigui necessari per al compliment de la relació que es tracti.

c) Quan el tractament de les dades tingui per finalitat protegir un interès vital de l'interessat.

d) Quan les dades figurin en fonts accessibles al públic i el seu tractament sigui necessari per a la satisfacció de l'interès legítim perseguit.

De totes maneres, en els casos en què no és necessari el consentiment de l'afectat, es reconeix a aquest el dret a quedar exclòs del tractament de les dades, sempre que una llei no disposi el contrari i existeixin motius fundats i legítims relatius a una concreta situació personal.

Article 7:

En aquest article es tracta les dades especialment protegides, com poden ser els relacionats amb ideologies, origen racial, salut, infraccions penals o administratives, etc.

Article 9:
En aquest article es tracta de la seguretat de les dades:
a) El responsable del fitxer, i si escau, l'encarregat del tractament hauran d'adoptar les mesures d'índole tècnica i organitzativa necessàries que garanteixin la seguretat de les dades i evitin la seva alteració, perduda o accés no autoritzat.
b) No es registraran dades de caràcter personal en fitxers que no reuneixin les condicions d'integritat seguretat necessàries.

Articles 11 i 12:
En aquests articles es tracta la comunicació de les dades i els accessos de terceres persones a aquestes dades. Ressaltar el més important de la LSSICE seria molt més extens. Prou assenyalar el seu objectiu i àmbit, la qual cosa dóna una idea de l'important que serà tenir-la en compte per a l'elaboració de qualsevol política de seguretat.

L'objectiu de la llei és: "És objecte de la present Llei la regulació del règim jurídic dels serveis de la societat de la informació i de la contractació per via electrònica, referent a les obligacions dels prestadors de serveis, inclosos els que actuen com a intermediaris en la transmissió de continguts per les xarxes de telecomunicacions, les comunicacions comercials per via electrònica, la informació prèvia i posterior a la celebració de contractes electrònics, les condicions relatives a la seva validesa i eficàcia i el règim sancionador aplicable als prestadors de serveis de la societat de la informació". És una llei jove i està en el període de posada en *macha. Hi haurà molt més que dir quan porti un temps utilitzant-se i hagin aparegut realment problemes.

1.5.2 Aspectes lògics i de topologia.

El EITF (Emerging Issues task force) defineix una política de seguretat com: "Una sèrie de sentències formals (normes) que han de complir totes les persones que tinguin accés a qualsevol informació i/o tecnologia d'una organització". El propòsit general d'una política de seguretat és informar als usuaris, treballadors i equip directiu dels requisits obligatoris per protegir els valors tecnològics i informació de l'organització. La política hauria d'especificar els mecanismes a través dels quals aquests requisits puguin ser coneguts. Un altre propòsit és proporcionar una base per adquirir, configurar i auditar els sistemes d'ordinadors i les xarxes.

Per tant, emprar un conjunt d'eines de seguretat, sense una política de seguretat implícita, no tindria molt sentit. L'ús adequat d'aquestes eines ha de ser part de la política de seguretat. Els objectius concrets que es busquen vindran determinats, en bona part, per la capacitat que es tingui de complir amb una sèrie d'aspectes com són:

1 Ha de poder-se implantar.
2 Ha d'entendre's.
3 Ha de fer-se complir.
4 Ha de definir responsabilitats.
5 Ha de permetre que segueixi realitzant-se el treball normal.
6 Ha de s'exhaustiva.
7 Ha d'incloure mecanismes de resposta.
8 Ha de tenir mecanismes d'actualització.
9 Ha de complir la legislació.

S'ha de contemplar sempre el principi de privilegi mínim, que consisteix a tractar de minimitzar el nombre d'usuaris amb privilegis d'administrador, el conjunt d'equips externs amb accés a sistemes locals i, en general, el nombre de situacions en les quals algú o alguna cosa tenen privilegis d'accés, que no necessita, perquè el treball tiri endavant.

Un altre aspecte que ha de tractar d'aconseguir-se és l'il·lustrat pels principis de defensa en profunditat i de diversitat de defensa. S'ha d'intentar tenir més d'un nivell de defensa i, a poder ser, de diferent naturalesa per, d'aquesta forma, fer més difícil el treball del supòsit atacant que no només ha de vèncer més d'una defensa, sinó que cadascuna li obliga a tenir diferents tipus de coneixement. Si aconseguim tenir un nivell de protecció suficientment segur, hem de disposar d'un punt central de gestió de la seguretat, en el qual centralitzar la gestió de l'autenticació, autorització, del tràfic de seguretat, que suporti així mateix el registre d'esdeveniments centralitzat i les alarmes.

Una altra tècnica és la d'identificar el punt (o els punts) més feble de l'organització. Per exemple, qualsevol configuració avançada del tallafocs més sofisticat del que es disposi és inútil si també es pot accedir a l'organització mitjançant mòdem i una contrasenya estàtica. Seguir el principi del tancament complet que consisteix a garantir que, en el cas d'atac amb èxit a un component de seguretat, el sistema de seguretat no passa a permetre l'accés complet a tota la xarxa, sinó a no permetre ja cap accés. El més important és el principi de simplicitat, que

persegueix que es compleixin tots els anteriors alhora que es pot gestionar tot el sistema, de manera simple i *entendible.A més, és el principi que ha de dirigir la pròpia construcció de cada norma, que no hauria de ser d'una grandària major de 2 pàgines. Les polítiques permeten guiar el procés de manteniment de seguretat:

-La seguretat com un procés i la política com la seva guia.
Com a resultat de la primera versió de la política de seguretat, s'implementaran tots els processos de seguretat física i lògica, la qual cosa inclou, configuració de encaminadors, tallafocs, xarxes privades virtuals, etc. Això es pot considerar com el primer pas del procés, la fase d'engegada del procés de seguretat.

-Fase d'engegada del procés de seguretat.
Si solament féssim això estaríem incomplint normes bàsiques d'una política de seguretat. El següent pas és la fase de monitoratge de la xarxa, a la recerca de:
Incompliments de la política de seguretat. Possibles noves amenaces no tingudes en compte.

-Fase de monitoratge del procés de seguretat.
Aquesta fase implica gestionar els registres d'activitats i d'auditoria i sol implicar l'engegada, configuració i manteniment del que es diu sistemes de detecció d'intrusions. Si en aquesta fase es dedueix que cal fer algun canvi en la política de seguretat, per evitar incompliments o per tenir en compte noves amenaces possibles, s'estarà començant a crear la versió 2 de la política. La següent fase seria la fase d'anàlisi de vulnerabilitats, que serveix per buscar, mitjançant escàners, o analitzadors de vulnerabilitats problemes de seguretat.

-Fase d'anàlisi de vulnerabilitats.
Finalment, amb tots els canvis consolidats, caldrà aplicar la nova versió de la política de seguretat a tots els dispositius que es vegin involucrats, així com als procediments necessaris.

-Consolidació i continuació del procés de seguretat.
A partir d'aquí es repeteix la primera fase, i la roda seguirà girant. La periodicitat amb la qual cadascuna de les fases ha d'engegar-se depèn de la política que tindrà en compte la grandària de la xarxa i uns altres múltiples factors. No es pretén defensar tant una periodicitat concreta com assenyalar la importància de veure la política de seguretat d'una organització com alguna cosa en constant moviment, que permet que el manteniment de la seguretat sigui un procés viu i administrable de forma

estructurada i organitzada.

Qualsevol política de seguretat ha de tenir en compte una sèrie de procediments relacionats amb la seguretat física, tant en l'aspecte del control d'accés físic a equips, com en el de tenir plans de contingència i emergència, així com de recuperació enfront de desastres. Ha d'estar clarament estipulat qui té dret a accedir, i en quins casos concrets, a cadascuna dels següents dispositius:

-Encaminadors, especialment els de perímetre de seguretat.
-Commutadors i concentradors.
-Servidors, concretament aquells que disposin de la informació més sensible de l'organització.
-Qualsevol tipus de tallafocs.
-Qualsevol tipus de punt extrem d'una xarxa privada virtual, que solen ser, realment, encaminadors i tallafocs.
-Qualsevol sistema de mitjans d'emmagatzematge, que permeti accedir a suports magnètics amb informació sensible.

També ha d'haver-hi unes normes clares sobre el control d'accés als edificis on estiguin situats els ordinadors i xarxes de l'organització, identificant:

Qui pot entrar a l'edifici?

Qui pot entrar a determinades sales de l'edifici, on resideixin les màquines identificades com especialment sensibles?

Com ha de garantir-se tal tipus d'accés? Podria ser mitjançant algun tipus de token d'accés o mitjançant mesures biomètriques, etc.

Qui pot accedir a determinats dispositius específics de Sali, com a impressores?

Quins documents no han de tenir còpies en paper soltes i on destruir-les i com destruir-les?

Quin accés se li dóna a una persona que ve a col·laborar, en termes d'ordinador, compte, nivell d'accés? El mateix cal tenir en compte per a una visita, si és que es donés el cas de necessitar accés.

És necessària la implantació de càmeres de seguretat? Si ho és, quines condicions ha de complir l'empresa contractada a tal fi?

És necessària la presència de guàrdies de seguretat?

Una altra sèrie d'idees entre les quals es poden ressaltar són:

10 Les activitats crítiques deuen situar-se lluny de les àrees d'accés públic.
11 Els edificis han de ser discrets i s'han de minimitzar les indicacions sobre el seu propòsit, evitant signes obvis de les activitats realitzades en ells.
12 Les guies dels telèfons i de les sales de l'organització no han d'identificar localitzacions informàtiques (excepte les oficines i àrees de recepció).
13 Els materials perillosos i/o combustibles han d'emmagatzemar-se a una distància de seguretat de l'emplaçament dels ordinadors. Un exemple molt simple és un got d'aigua, si és vessat en un dels servidors podria causar greus danys als serveis que realitza l'empresa.
14 L'equipament de còpies de seguretat i les pròpies còpies de seguretat han de situarse en llocs diferents i a una distància convenient de seguretat.
15 S'ha d'instal·lar equipament apropiat de seguretat: detectors de calor i fums, sortides d'emergència i sistemes d'extinció d'incendis. Tot aquest equipament ha de revisar-se periòdicament d'acord amb les instruccions dels fabricants. Els empleats han d'estar entrenats en el seu ús adequat.
16 Els procediments d'emergència han d'estar ben documentats i revisats regularment.

S'ha d'assenyalar la importància de disposar dels procediments per a la còpia periòdica de la informació, especialment de la més rellevant, que inclogui, a més, un cert control de qualitat, per assegurar que la còpia de dades és immediatament utilitzable.

S'ha de disposar de còpies de:

17 La informació d'ordinadors dels sistemes centrals.
18 La informació d'ordinadors de la xarxes d'àrea local.
19 La informació d'aplicacions i de bases de dades. Podria ser necessari plantejar-se la necessitat de tenir un centre en un altre lloc físic, en el qual resideixin totes aquestes còpies, disposant així d'una seguretat física addicional.

Entre les normes i procediments relacionats amb aspectes lògics es pot separar el que es denomina normes bàsiques o fonamentals, com:

20 Política d'ús acceptable.
21 Política d'accés remot.
22 Política de protecció de la informació.
23 Política de seguretat perimetral, encara que aquesta implicarà, també, procediments de configuració d'encaminadors i de tallafocs i punts finals de xarxes privades virtuals.
24 Política de protecció antivirus.
25 Política de contrasenyes, de la qual dependran els procediments de servidors, estacions de treball i accés remot i a través de xarxes privades virtuals.
26 Política d'actuació enfront d'incidents.

Entre les quals no serien normes bàsiques, però, encara així, en una organització extensa serien importants, es tindrien:

27 Política d'ús de sistemes de detecció d'intrusions, tant de tipus xarxa com de tipus host, de la qual es parlarà en extensió en el capítol.
28 Política de gestió dels*logs de sistemes i de auditories, de les quals es parlarà, també, en el capítol.
29 Política d'administració dels laboratoris de seguretat, en els quals, entre altres coses, es faran tots els test possibles anés de la xarxa real, en cerca de possibles bugs de seguretat en sistemes de tot tipus, amb ajuda d'analitzadors de vulnerabilitats i d'eines pròpies.
30 Política de comunicacions giri'ls.
31 Política d'ús de xarxes privades virtuals.
32 Qualsevol altra política aplicable a les característiques de l'organització.

Tota política de seguretat ha de tenir normes sobre ús acceptable, que defineixin l'ús apropiat dels recursos informàtics de l'organització. Els usuaris haurien de llegir i signar tals normes, com a part del procés de petició de comptes de treball. Ha d'establir clarament la responsabilitat dels usuaris pel que fa a la protecció de la informació emmagatzemada en els seus comptes. Ha d'assenyalar que permisos poden tenir els usuaris sobre fitxers que tinguin accessibles, però no siguin seus. Ha d'estipular l'ús acceptable del correu electrònic, de l'accés Web i de tot tipus d'accés a Internet, així com discutir els usos acceptables, no relacionats amb l'objecte de

l'organització, dels recursos informàtics.

Una altra política és la que fa explícites les normes sobre accés remot als recursos informàtics de l'organització. Ha de cobrir tots els mètodes disponibles per accedir, remotament, als recursos de la xarxa interna:

33 Accés mitjançant mòdem, via ESLIP o PPP.
34 Accés mitjançant RDSI o ADSL.
35 Accés mitjançant ssh o telnet, des d'Internet.
36 Accés mitjançant qualsevol tipus de xarxa privada virtual.

Una altra política fonamental és la que tracta de la protecció de la informació, que ha de donar una guia sobre el processament, emmagatzematge i transmissió de la informació, per part dels usuaris. El seu objectiu fonamental és garantir que la informació està protegida apropiadament enfront de la possible modificació. Un altre aspecte important que ha de cobrir és la definició dels nivells de sensibilitat de la informació de l'organització, quina informació és pública, quin és semipública i quin està restringida i a quins nivells. La següent política és la de protecció enfront de possibles atacs per virus informàtics. Aquesta, ha de proporcionar les línies generals dels informes sobre infeccions per virus, així com els procediments de contenció dels mateixos.

També ha de contenir les explicacions dels diferents nivells de risc depenent del tipus de virus, així com la necessitat de selecció del tipus de programa antivirus que es vagi a utilitzar i ha de discutir-se la freqüència d'actualització de les dades del mateix programari. Una altra política té a veure amb les contrasenyes. Ha de contenir les directrius de com gestionar les contrasenyes d'usuari i d'administrador, així com:

37 Les regles de creació de les contrasenyes.
38 Les regles de com evitar la revelació de contrasenyes.
39 Les regles per al desenvolupament d'aplicacions en les quals faci mancada la contrasenya.
40 Les regles d'ús de tot tipus de contrasenyes de protocols.
Generalment, la taxonomia més elemental d'aquestes amenaces es divideix en quatre grans grups:

-Interrupció
-Intercepció

-Modificació
-Fabricació.

Un atac es classifica com a interrupció si fa que un objecte del sistema es perdi, quedi inutilitzable o no disponible, aquest és un atac contra la disponibilitat. Es tractés d'una intercepció si un element no autoritzat aconsegueix un accés a un determinat objecte del sistema, aquest és un atac contra la confidencialitat i d'una modificació si a més d'aconseguir l'accés aconsegueix modificar l'objecte, alguns autors consideren un cas especial de la modificació: la destrucció, entenent-la com una modificació que inutilitza a l'objecte afectat. Finalment, es diu que un atac és una fabricació si es tracta d'una modificació destinada a aconseguir un objecte similar a l'atacat de manera que sigui difícil distingir entre l'objecte original i el fabricat. En la gran majoria de publicacions relatives a la seguretat informàtica en general, i especialment en les relatives a seguretat en Unix, tard o d'hora s'intenta classificar en grups als possibles elements que poden atacar el nostre sistema. Amb freqüència, se sol identificar als atacants únicament com a persones, això té sentit si parlem per exemple de responsabilitats per un delicte informàtic. Però en aquest projecte és preferible parlar d'elements i no de persones, encara que de vegades ho oblidem, el nostre sistema pot veure's perjudicat per múltiples entitats a part d'humans, com per exemple programes, catàstrofes naturals…

1.5.3 Repercussió en els aspectes organitzatius i de RR.HH.

Es pot fer la següent divisió del personal que interactuarà amb els sistemes i màquines de l'organització:
-L'administrador o responsable directe del sistema.
-Les persones que han de tenir accés al sistema com a usuaris.
-Les persones relacionades amb el sistema pitjor que no necessiten usar-ho.
-Les persones alienes al sistema.
Els administradors han de ser persones correctament qualificades, seran els únics amb accés complet al sistema que administren. És fonamental assegurar a aquesta persona tan ben com s'asseguri a la resta del sistema. No serveix de res disposar del sistema més sofisticat, des del punt de vista de la seguretat, si aquesta persona pot fallar en qualsevol moment. L'única forma d'aconseguir-ho és buscant la seva fidelitat, tant mitjançant recompenses com a penalitzacions adequades i proporcionades al valor

dels béns que custodia. No fer-ho així seria exposar a l'organització a problemes realment greus. Si tals persones reben un salari insuficient, o inadequat, i una penalització insuficient, això els farà més susceptibles al xantatge o al suborn, mentre que unes penalitzacions excessives poden portar a la desesperació, i pèrdua de la por a les conseqüències, o a un estat de nerviosisme permanent, que disminueixi la seva capacitat.

És possible reduir la responsabilitat dels administradors, transferint-la als seus caps, reduint així, aparentment, la necessitat de cuidar dels administradors. En realitat, això no és més que una transferència fictícia: tot el que té accés físic a l'ordinador té en última instància control absolut, i aquest trasllat de responsabilitats només reflecteix una falta de confiança notòria, que trenca la necessària relació de cordialitat i fidelitat, posant en perill el sistema de seguretat.

Els usuaris, típicament empleats fixos, personal temporal o clients d'un sistema no necessiten tenir el control absolut dels sistemes servidors de l'organització. Per això, la solució generalment usada és establir sistemes d'accés parcials, amb requisits de seguretat menors, de tal forma que l'usuari tingui control absolut sobre el seu sistema particular, disminuint la repercussió d'un eventual compromís i la importància de la responsabilitat, però permetent només l'accés necessari als sistemes servidors.

No tots els usuaris han de tenir el mateix grau d'accés a les dades, ni tindran, per tant, la mateixa responsabilitat, per això s'ha d'establir diferents nivells d'usuaris. Cada usuari deu ser conscient de les seves responsabilitats.

Entre les persones relacionades amb els sistemes, especialment servidors de l'organització, però que no necessiten usar-los habitualment, es pot fer una divisió, personal executiu i personal de manteniment. El personal executiu, a causa de la seva disposició dins de l'empresa, no sol necessitar accedir als sistemes servidors en el dia a dia, però, en determinats moments, poden necessitar mostrar dades o informació dels mateixos. Això, sense cap dubte, posa en perill la seguretat del sistema i, per tant serà necessari, prendre les mesures adequades i habilitar els mecanismes que ho permetin, mantenint, alhora, les normes de seguretat sobre el sistema i les dades que es tracti.

El personal de manteniment sol tenir accés al perímetre protegit. En ells conflueixen circumstàncies especials: d'una banda solen ser persones no tècniques, ni relacionades amb els equips i, per tant, és més probables que cometin errors comprensibles en la seva interacció amb ells. D'altra banda, el que no se'ls exigeixi

coneixements en tecnologia per exercir el seu treball no vol dir que no els tinguin. Per això, si han d'accedir al sistema, és recomanable que ho facin sota supervisió d'una persona responsable.

Per a les persones alienes als sistemes, és molt fàcil resumir la política: no han d'accedir, en cap circumstància. Una bona política de seguretat ha de determinar l'accés, controlat correctament, de les persones amb dret a tal accés, però ha de garantir, clarament, la impossibilitat per a la resta de les persones. Hi ha una sèrie de procediments organitzatius a tenir en compte, en relació amb totes les persones de l'organització, que han de ser presos per la direcció de recursos humans, o semblant, que es poden resumir de la següent manera:

-Que les definicions de lloc de treball contemplin tot el necessari quant a responsabilitats de seguretat i els seus sistemes.

-Que els empleats que vagin a fer ús d'informació sensible, hagin estat correctament contractats, tenint especial cura amb el cas dels empleats temporals.

-Tant els nous empleats, com els col·laboradors externs o consultors o tècnics hauran de signar contractes, o acords, de confidencialitat abans de la seva connexió i accés als recursos i sistemes d'informació de l'organització.

-És necessari que tals empleats s'adonin de la importància que tenen en el manteniment de la seguretat de sistemes i equip i dels possibles procediments disciplinaris als quals es veuran exposats, en el cas d'incomplir les seves responsabilitats. La millor manera d'implementar aquest procediment és mitjançant un pla de formació per a tot el personal de l'organització, adequant-ho a les necessitats de cada lloc.

1.5.4 Aspectes físics de les polítiques de seguretat en xarxa.

Els mecanismes de prevenció més habituals són els següents:

-Mecanismes d'autenticació i identificació

-Mecanismes de control d'accés

-Mecanismes de separació

-Mecanismes de seguretat en les comunicacions

Sota l'etiqueta d'amenaces lògiques trobem tot tipus de programes que d'una forma o una altra poden danyar al nostre sistema, creats de forma intencionada per a això (programari maliciós, també conegut com *malware) o simplement per error (bugs o forats)

-Programari incorrecte: Les amenaces més habituals a un sistema Unix provenen d'errors comesos de forma involuntària pels programadors de sistemes o d'aplicacions. Una situació no contemplada a l'hora de dissenyar el sistema de xarxa del kernel o un error accedint a memòria en un fitxer poden comprometre local o remotament a Unix (o a qualsevol altre sistema operatiu). A aquests errors de programació se'ls denomina bugs, i als programes utilitzats per aprofitar un d'aquestes fallades i atacar al sistema, exploits.

Representen l'amenaça més comuna contra Unix, ja que qualsevol pot aconseguir un exploit i utilitzar-ho contra la nostra màquina sense ni tan sols saber com funciona i sense uns coneixements mínims d'Unix, fins i tot hi ha exploits que danyen seriosament la integritat d'un sistema (negacions de servei o fins i tot accés root remot) i estan preparats per ser utilitzats des de MS-DOS, amb el que qualsevol pirata novençà (comunament, se'ls denomina script kiddies) pot utilitzar-los contra un servidor i aconseguir un control total d'una màquina de diversos milions de pessetes des del seu PC sense saber gens del sistema atacat, fins i tot hi ha situacions en les quals s'analitzen els logs d'aquests atacs i es descobreix que el pirata fins i tot intenta executar ordres de MS-DOS.

Podem destacar la semblança entre els atacs a xarxes i servidors i els atacs o amenaces a la seguretat del món real. Els atacs dirigits als dispositius de xarxa que es desitja protegir estan, finalment, realitzats per persones. Es pot pensar en alguns: robatoris de bancs, malversacions i fraus, invasió de la confidencialitat, sabotatge, espionatge, etc. Tot aquest tipus de problemes existeixen a les xarxes de les organitzacions actuals. Es pot dir que on hi ha diners hi ha criminals, amb el que assumptes com el sabotatge remot al control de caixers automàtics o la pornografia infantil, passen a ser perfectament factibles també a les xarxes. Però, des del punt de

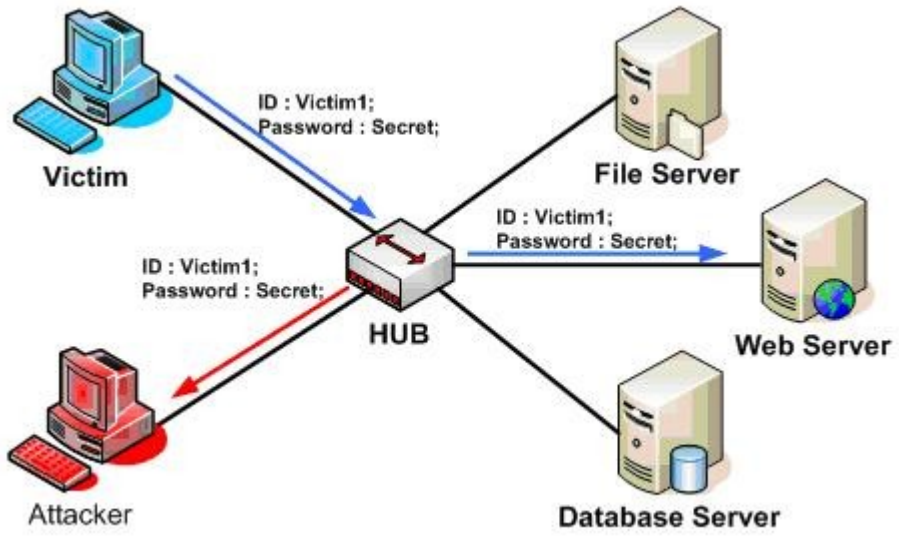
vista més tècnic si hi ha diferències, es podria dir que el ciberespai canvia les formes dels atacs i, com a conseqüència, s'han d'adequar les formes de les defenses. La xarxa Internet té diverses característiques que fan que els citats atacs puguin ser molt pitjors, en cert sentit. Aquestes característiques són:

-L'aspecte automàtic dels atacs. Si en alguna cosa són potents els ordinadors, és en les tasques repetitives. Es pot deixar una màquina tractant de desxifrar contrasenyes de manera automàtica, mentre l'atacant es va a passar el cap de setmana a esquiar, amb la tranquil·litat que el seu treballador no es va a cansar, ni es va a queixar.

-L'aspecte remot dels atacs. És gairebé tan fàcil connectar-se a un ordinador en Paris des de Madrid que des de Tòquio. En aquest sentit, es diu que Internet no té fronteres. El greu és que els aspectes legals de tot això no estan, encara, controlats.

Com va dir John Gilmore: *"The Internet tretas censorship as a damage and routes around it"(Internet tracta a la censura com una cosa nociva i l'envolta)*

Mòdul II: ATACS CORPORATIUS I MECANISMES DE SEGURETAT.



2.1 Elements bàsics de seguretat.

Alguns conceptes clau per a l'anàlisi del projecte són els següents: -Eines de seguretat: Qualsevol eina de seguretat representa un arma de doble tall, de la mateixa forma que un administrador les utilitza per detectar i solucionar fallades en els seus sistemes o en la subxarxa completa, un potencial intrús les pot utilitzar per detectar aquestes mateixes fallades i aprofitar-los per atacar els equips. Eines com nessus, saintt o satan passen de ser útils a ser perilloses quan les utilitzen crackers que busquen informació sobre les vulnerabilitats d'un host o d'una xarxa completa. Si com a administradors no s'utilitzen eines de seguretat que mostrin les debilitats dels sistemes (per corregir-les), cal estar segur que un atacant no va a dubtar a utilitzar tals eines (per explotar les debilitats oposades), per tant, cal agrair als dissenyadors de tals programes l'esforç que han realitzat (i ens han estalviat) en pro de sistemes més segurs.

-Portes posteriors: Durant el desenvolupament d'aplicacions grans o de sistemes operatius és habitual entre els programadors inserir "dreceres" en els sistemes habituals d'autenticació del programa o del nucli que s'està dissenyant. A aquestes dreceres se'ls denomina portes posteriors, i amb ells s'aconsegueix major velocitat a l'hora de detectar i depurar fallades, per exemple, els dissenyadors d'un programari de gestió de bases de dades en el qual per accedir a una taula es necessitin quatre claus diferents de deu caràcters cadascuna poden inserir una rutina per aconseguir aquest accés mitjançant una única clau "especial", amb l'objectiu de perdre menys temps en depurar el sistema. Alguns programadors poden deixar aquestes dreceres en les versions definitives del seu programari per facilitar un manteniment posterior, per garantir el seu propi accés, o simplement per distracció, la qüestió és que si un atacant descobreix una d'aquestes portes posteriors (no ens importa el mètode que utilitzi per fer-ho) va a tenir un accés global a dades que no hauria de poder llegir, la qual cosa òbviament suposa un greu perill per a la integritat del nostre sistema.

-Bombes lògiques: Les bombes lògiques són parts de codi de certs programes que romanen sense realitzar cap funció fins que són activades, en aquest punt, la funció que realitzen no és l'original del programa, sinó que generalment es tracta d'una acció perjudicial. Els activadors més comuns d'aquestes bombes lògiques poden ser l'absència o presència de certs fitxers, l'execució sota un determinat UID o l'arribada d'una data concreta, quan la bomba s'activa va a poder realitzar qualsevol tasca que pugui realitzar la persona que executa el programa, si les activa el root, o el programa que conté la bomba els efectes òbviament poden ser fatals.

-Canales coberts: Els canals coberts són canals de comunicació que permeten a un procés transferir informació de manera que violi la política de seguretat del sistema, és a dir, un procés transmet informació a uns altres (locals o remots) que no estan autoritzats a llegir aquesta informació. Els canals coberts no són una amenaça massa habitual en xarxes de R+D, ja que sol ser molt més fàcil per a un atacant aprofitar qualsevol altre mecanisme d'atac lògic, no obstant això, és possible la seva existència, i en aquest cas la seva detecció sol ser difícil, alguna cosa tan simple com el port finger obert en una màquina pot ser utilitzat a manera de covert channel per un pirata amb una mica d'experiència.

-Virus: Un virus és una seqüència de codi que s'insereix en un fitxer executable (denominat hoste), de manera que quan l'arxiu s'executa, el virus també ho fa, inserint-se a si mateix en altres programes. Tothom coneix els efectes dels virus en

alguns sistemes operatius de sobretaula, no obstant això, en Unix els virus no solen ser un problema de seguretat greu, ja que el que pugui fer un virus ho pot fer més fàcilment qualsevol altre mecanisme lògic. Encara que els virus existents per a entorns Unix són més una curiositat que una amenaça real, en sistemes sobre plataformes IBM-PC o compatibles (hi ha molts sistemes Unix que operen en aquestes plataformes, com Linux, FreeBSD, NetBSD, Minix, Solaris…) certs virus, especialment els de boot, poden tenir efectes nocius, com danyar el sector d'arrencada, encara que es tracta de danys menors comparats amb els efectes d'altres amenaces.

-Cucs: Un cuc és un programa capaç d'executar-se i propagar-se per si mateix a través de xarxes, en ocasions portant virus o aprofitant bugs dels sistemes als quals connecta per danyar-los. En ser difícils de programar el seu nombre no és molt elevat, però el dany que poden causar és molt gran, el major incident de seguretat en Internet va ser precisament el cuc Word comentat en el capitulo 1. Hem de pensar que un cuc pot automatitzar i executar en uns segons tots els passos que seguiria un atacant humà per accedir al nostre sistema, mentre que una persona, per molts coneixements i mitjans que posseeixi, trigués com a mínim hores a controlar la nostra xarxa completa (un temps més que raonable per detectar-ho), un cuc pot fer això mateix en pocs minuts, d'aquí el seu enorme perill i els seus devastadors efectes.

-Cavalls de Troia: Els troians o cavalls de Troia són instruccions amagades en un programa de manera que aquest sembli realitzar les tasques que un usuari espera d'ell, però que realment executi funcions ocultes (generalment en detriment de la seguretat) sense el coneixement de l'usuari, com el Cavall de Troia de la mitologia grega, al que deuen el seu nom, oculten la seva funció real sota l'aparença d'un programa inofensiu que a primera vista funciona correctament. En la pràctica totalitat dels atacs a Unix, quan un intrús aconsegueix el privilegi necessari en el sistema instal·la troians per ocultar la seva presència o per assegurar-se l'entrada en cas de ser descobert. per exemple, és típic utilitzar el que es denomina un rootkit, que no és més que un conjunt de versions troianes de certes utilitats (netstat, ps, who…), per aconseguir que quan l'administrador les executi no vegi la informació relativa a l'atacant, com els seus processos o la seva connexió al sistema, un altre programa que se sol suplantar és login, per exemple perquè en rebre un cert nom d'usuari i contrasenya proporcioni accés al sistema sense necessitat de consultar /etc/passwd.

-Programes conill o bacteris: sota aquest nom es coneix als programes que no fan gens útil, sinó que simplement es dediquen a reproduir-se fins que el nombre de

còpies acaba amb els recursos del sistema (memòria, processador, disc...), produint una negació de servei. Per si mateixos no fan cap dany, sinó que el que realment perjudica és el gran nombre de còpies seves en el sistema, que en algunes situacions poden arribar a provocar la parada total de la màquina. Hem de pensar hi ha certs programes que poden actuar com a conills sense proposar-li-ho, exemples se solen trobar en els sistemes Unix destinats a pràctiques en les quals s'ensenya a programar a l'alumnat, és molt comú que un bucle que per error es converteix en infinit contingui entre les seves instruccions algunes de reserva de memòria, la qual cosa implica que si el sistema no presenta una correcta política de quotes per a processos d'usuari pugui enfonsar-se o degradar enormement les seves prestacions. El fet que l'autor solgui ser fàcilment localitzable no ha de ser cap excusa per descurar aquesta política, no podem culpar a un usuari per un simple error, i a més el dany ja s'ha produït.

-Tècniques salami: Per tècnica salami es coneix al robatori automatitzat de petites quantitats de béns (generalment diners) d'una gran quantitat origen. El fet que la quantitat inicial sigui gran i la robada petita fa extremadament difícil la seva detecció, si d'una compta amb diversos milions d'euros es roben uns cèntims, ningú va a adonar-se d'això, si això s'automatitza para, per exemple, descomptar un cèntim de cada nòmina pagada a la universitat o de cada beca concedida, després d'un mes d'activitat segurament s'hauria robat una enorme quantitat de diners sense que ningú s'hi hagi adonat d'aquest fet, ja que de cada origen s'ha pres una quantitat mínima. Les tècniques salami no se solen utilitzar per atacar sistemes normals, sinó que el seu ús més habitual és en sistemes bancaris, no obstant això, com en una xarxa amb requeriments de seguretat mitjans és possible que hi hagi ordinadors dedicats a comptabilitat, facturació d'un departament o gestió de nòmines del personal, es comenta aquesta potencial amenaça contra el programari encarregat d'aquestes tasques.

2.2 Origen de les amenaces: tipologia i normativa de seguretat.

Aquí es descriuen breument els diferents tipus de persones que d'una o una altra forma poden constituir un risc per als nostres sistemes, generalment es divideixen en dos grans grups, els atacants passius, aquells que “es passegen” pel sistema però no ho modifiquen o destrueixen, i els actius, aquells que danyen l'objectiu atacat, o ho modifiquen a favor seu. Generalment els curiosos i els crackers

realitzen atacs passius (que es poden convertir en actius), mentre que els terroristes i ex-emprats realitzen atacs actius puros, els intrusos remunerats solen ser atacants passius si la nostra xarxa o equip no és el seu objectiu, i actius en cas contrari, i el personal realitza tots dos tipus indistintament, depenent de la situació concreta:

-Personal: Les amenaces a la seguretat d'un sistema provinents del personal de la pròpia organització rares vegades són preses en compte, es pressuposa un entorn de confiança on de vegades no existeix, per la qual cosa es passa per alt el fet que gairebé qualsevol persona de l'organització, fins i tot el personal aliè a la infraestructura informàtica (secretariat, personal de seguretat, personal de neteja i manteniment…) pot comprometre la seguretat dels equips. Encara que els atacs poden ser intencionats (en aquest cas els seus efectes són extremadament nocius, recordem que ningú millor que el propi personal de l'organització coneix millor els sistemes… i les seves debilitats), el normal és que més que d'atacs es tracti d'accidents causats per un error o per desconeixement de les normes bàsiques de seguretat, un empleat de manteniment que talla el subministrament elèctric per fer una reparació pot arribar a ser tan perillós com el més expert dels administradors que s'equivoca en teclejar una ordre i esborra tots els sistemes de fitxers, i en el primer cas, l'atacant ni tan sols ha de tenir accés lògic (ni físic) als equips, ni conèixer gens sobre seguretat en Unix.

-Ex-emprats: Un altre gran grup de persones potencialment interessades a atacar el nostre sistema són els antics empleats del mateix, especialment els que no van abandonar l'entorn per voluntat pròpia (i en el cas de xarxes d'empreses, els que van passar a la competència). Generalment, es tracta de persones descontentes amb l'organització que poden aprofitar debilitats d'un sistema que coneixen perfectament per danyar-ho com a venjança per algun fet que no consideren just, poden inserir troians, bombes lògiques, virus… o simplement connectar-se al sistema com si encara treballessin per a l'organització (moltes vegades es mantenen els comptes oberts fins i tot mesos després d'abandonar la universitat o empresa), aconseguir el privilegi necessari, i danyar-ho de la forma que desitgin, fins i tot fent xantatge als seus ex-companys o ex-caps.

-Curiosos: Juntament amb els crackers, els curiosos són els atacants més habituals de sistemes Unix en xarxes de R+D. Recordem que els equips estan treballant en entorns on es forma a futurs professionals de la informàtica i les telecomunicacions (gent que a priori té interès per les noves tecnologies), i recordem també que les persones solen ser curioses per naturalesa, aquesta combinació produeix un devessall d'estudiants o

personal intentant aconseguir major privilegi del que tenen o intentant accedir a sistemes als quals oficialment no tenen accés. I en la majoria d'ocasions això es fa simplement per llegir el correu d'un amic, assabentar-se de quant cobra un company, copiar un treball o comprovar que és possible trencar la seguretat d'un sistema concret. Encara que en la majoria de situacions es tracta d'atacs no destructius (a excepció de l'esborrat de petjades per evitar la detecció), sembla clar que no beneficien en absolut a l'entorn de fiabilitat que puguem generar en un determinat sistema.

-Crackers: Els entorns de seguretat mitjana són un objectiu típic dels intrusos, ja sigui per tafanejar, per utilitzar-les com a enllaç cap a altres xarxes o simplement per diversió. D'una banda, són xarxes generalment obertes, i la seguretat no és un factor tingut molt en compte en elles, per un altre, el gran nombre i varietat de sistemes Unix connectats a aquestes xarxes provoca, gairebé per simple probabilitat, que almenys alguns dels seus equips siguin vulnerables a problemes coneguts per endavant. D'aquesta forma un atacant només ha d'utilitzar un escàner de seguretat contra el domini complet i després atacar mitjançant un simple exploit els equips que presenten vulnerabilitats, això converteix a les xarxes de R+D, a les d'empreses, o a les de ISPs en un objectiu fàcil i desitjable per a pirates amb qualsevol nivell de coneixements, des dels més novençans (i de vegades més perillosos) fins als experts, que poden utilitzar tota la xarxa per provar nous atacs o com a node intermedi en un atac a altres organismes, amb la conseqüent deterioració d'imatge (i de vegades de pressupost) que suposa per a una universitat ser, sense desitjar-ho, un suport als pirates que ataquen sistemes teòricament més protegits, com els militars.

-Terroristes: Sota aquesta definició s'engloba a qualsevol persona que ataca al sistema simplement per causar algun tipus de dany en ell. Per exemple, algú pot intentar esborrar les bases de dades d'un partit polític enemic o destruir els sistemes de fitxers d'un servidor que alberga pàgines Web d'algun grup religiós, en el cas de xarxes de R+D, típics atacs són la destrucció de sistemes de pràctiques o la modificació de pàgines Web d'algun departament o de certs professors, generalment per part d'alumnes descontents.

-Intrusos remunerats: Aquest és el grup d'atacants d'un sistema més perillós, encara que per fortuna el menys habitual en xarxes normals, sol afectar més a les grans empreses o a organismes de defensa. Es tracta de pirates amb gran experiència en problemes de seguretat i un ampli coneixement del sistema, que són pagats per una tercera part generalment per robar secrets (el nou disseny d'un processador, una base de dades de clients, informació confidencial sobre les posicions de satèl·lits espia…)

o simplement per danyar la imatge de l'entitat afectada. Aquesta tercera part sol ser una empresa de la competència o un organisme d'intel·ligència, és a dir, una organització que pot permetre's una gran despesa en l'atac, d'aquí la seva perillositat, se sol pagar bé als millors pirates, i per si això fos poc els atacants van a tenir tots els mitjans necessaris al seu abast. Encara que com hem dit els intrusos remunerats són els menys comuns en la majoria de situacions, en certes circumstàncies poden aprofitar les nostres xarxes com a plataforma per atacar altres organismes.

2.3 Mecanismes de seguretat. Plans de contingència empresarials.

Taxonomia dels tipus d'atacs: una bona classificació no es pot fer sense un bon criteri. Des del punt de vista de l'origen de l'atac, es pot dir que els atacs són:

1 Externs. Quan l'atacant origina el seu atac des de l'exterior d'una organització concreta, es diu que l'atac és extern. Això pot ser des d'un lloc desconegut d'Internet o des d'una adreça en la qual es confia, però que ha estat suplantada. Aquesta característica és essencial per a cert tipus d'atacs a una xarxa, que realitza el control d'accés basat en adreces IP.

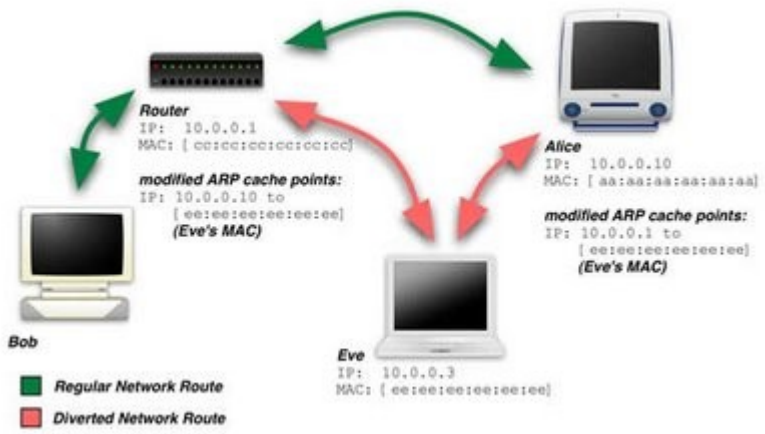
2 Interns. És obvi que estar dins de l'organització facilita molt l'atac. Tal ataqui ha de ser vist, a més, des d'un punt de vista ampli. Pot haver-hi atacs “professionals” interns, però, també, per mala aplicació de la política de seguretat, atacs no maliciosos d'usuaris interns que proven eines amb tota la seva bona intenció.

Origen dels atacs. Un altre criteri que convé utilitzar, per a una millor caracterització de cada atac, és la complexitat. En aquest sentit es pot parlar d'atacs:

3 No estructurats. Són atacs innocents, atacs basats en eines bastant normals, que poden tenir diferents tipus d'objectius, i ser molt perillosos, però, en general, fàcilment recognoscibles. Una característica típica d'aquests atacs és que o bé és una sola eina l'engegada o són vàries, però sense cap estructuració entre elles.

4 Estructurats. Aquí s'està davant els més perillosos. Són atacs que s'enfoquen com un projecte. A més tracten de no deixar caps per lligar, la qual cosa es tracta d'esborrar les petjades i es tenen en compte diferents punts d'atac i de retirada. Encara que siguin

els més perillosos, són els menys habituals.



Un altre criteri aquesta relacionat amb la personalitat de l'atacant. La seva formació, experiència i capacitat de comunicació poden ser fonamentals a l'hora de desenvolupar un atac, especialment si és un estructurat i s'usa en la fase d'obtenció d'informació.

Finalment si es cataloguen per l'objectiu que persegueixen, una necessitat de classificació més granular, es pot parlar dels següents tipus d'atacs:

5 Atacs encaminats a l'obtenció d'informació sobre els objectes a atacar.

6 Atacs orientats a veure, canviar o esborrar informació per la qual no s'està autoritzat, aprofitant-se de la mala administració de les eines, màquines i sistemes de la xarxa.

7 Atacs enfocats a veure, canviar o esborrar informació per la qual no s'està autoritzat, aprofitant-se de les vulnerabilitats del programari dels sistemes, aplicacions i protocols de la xarxa.

8 Atac canalitzats a sabotejar un servei, com un servidor Web, un servidor SMTP, l'espai lliure en disc d'un ordinador, l'accés a (o des de) una xarxa. A tots ells, se'ls denomina atacs de denegació de servei. Si s'utilitza aquest criteri, és molt fàcil ressaltar els altres criteris citats, amb la qual cosa serà aquest el que usarem.

2.4 Tipificació i anàlisi dels atacs corporatius.

2.4.1 MITM (Man in the Middle)

La intercepció lògica de dades més coneguda i estesa és el *sniffing, consisteix a capturar trames que circulen per la xarxa mitjançant un programa executant-se en una màquina connectada a ella o bé mitjançant un dispositiu que s'enganxa directament el cablejat. A les xarxes de difusió, quan una màquina envia una trama a una altra indica en un camp reservat l'adreça del *host destinació, totes les màquines del domini de col·lisió veuen aquesta trama, però només la seva receptora legítima la captura i elimina de la xarxa. Est és el funcionament normal de *TCP/IP, no obstant això, és necessari insistir en un aspecte, totes les màquines veuen la trama, i si no llegeixen tots els seus camps és perquè no volen. Existeix una manera de funcionament de les interfícies de xarxa denominat manera promíscua, en el qual la targeta llegeix totes les trames que circulen per la xarxa, tant dirigides a ella com a altres màquines, el llegir-les no implica l'eliminar-les de la xarxa, per la qual cosa el host destinació legítima la rebrà i eliminarà sense notar res estrany.

Per fer funcionar un interfície de xarxa en manera promíscua és necessari tenir un control total del sistema, és a dir, ser root en la màquina, això ajuda una mica en la defensa, però no soluciona el problema, no podem permetre que qualsevol que sigui superusuari d'un sistema pugui capturar tot el tràfic que passa pel mateix (incloent claus, correu electrònic, i centenars de dades privades). Per si això fos poc, en els sistemes on tots els usuaris tenen un control total de la màquina (per exemple, en tota la família Windows 9x) ni tan sols fa falta aquest privilegi, qualsevol que se sent en un PC pot executar un sniffer i capturar tot el tràfic de la xarxa.

Hi ha programes perquè actuen com sniffer entre ells cal destacar, dsniff i la seva família, capaces fins a de capturar els correus electrònics directament en format smtp o carregar de forma automàtica en un navegador les mateixes pàgines que visita la víctima de l'atac, un altre programa és el snoop de Solaris, que bolca paquets en un format per defecte gairebé il·legible, passant pels clàssics tcpdump o sniffit. Per evitar que programes d'aquest tipus capturin la nostra informació existeixen diferents aproximacions més o menys efectives, com substituir els HUBs de la nostra xarxa per switches que aïllen dominis de col·lisió (això dificulta l'atac però no ho impossibilita) o implantar xarxes privades virtuals. Però la més barata i senzilla és l'ús de protocols xifrats sempre que ens sigui possible (que ho sol ser gairebé sempre), substituir telnet i rlogin per ssh i ftp per scp o sftp és molt senzill, i ens proporciona un increment de seguretat abismal en el nostre entorn. Implantar SSL o túnels segurs potser és una mica més costós, però també en la majoria d'ocasions és alguna cosa que val la pena fer, en tot moment hem de tenir present que el sniffing és un perill real, que no necessita de grans mitjans i, la qual cosa és pitjor, indetectable en la major part de

casos, a pesar que existeixen mètodes per tractar de detectar sistemes amb un interfície en manera promíscua, no solen ser tot l'efectius que un podria esperar, ja que detectar una màquina en aquest estat no és ni des de lluny immediat.

El sniffing és l'atac d'intercepció més conegut i utilitzat, però no és l'únic que es pot posar en pràctica contra un sistema determinat, Unix o no. En algunes versions de Linux existeix un programa denominat ttysnoop capaç de registrar en temps real tot el que un usuari tecleja en una terminal, tant física com a virtual. Encara que el resultat és en molts aspectes similar al sniffing, tècnicament poc té a veure amb est, en cap moment es capturen dades que circulen per la xarxa, la targeta no treballa en manera promíscua (és mes, ni tan sols és necessari un interfície de xarxa), etc, simplement, la informació que un usuari introdueix en una terminal és clonada en una altra, permetent tant l'entrada com la sortida de dades a través d'ambdues. Encara que Linux sigui el sistema Unix natiu de ttysnoop existeixen versions també per a altres entorns.

Un altre atac d'intercepció, menys utilitzat que els anteriors però igual de perillós, és el keylogging, el registre de les tecles premudes per un usuari en una sessió, un altre exemple d'un programa que capturi aquesta informació pot ser una mula de Troia clàssica. En els atacs orientats a l'obtenció d'informació sobre l'objectiu per obtenir informació sobre l'objectiu a atacar hi ha 2 metodologies: l'enginyeria social i les tècniques informàtiques d'obtenció d'informació. Per a l'enginyeria social descrivim dos casos reals:

-En 1994, un hacker francès, anomenat Anthony Zboralski, flama a l'oficina del FBI a Washington, fent-se passar per un representant del FBI, treballant en l'oficina d'EUA a París. Persuadeix a la persona a l'altre costat del telèfon que li expliqui com connectar-se al sistema de conferències telefòniques del FBI. Després es gasta 250000 dòlars en 7 mesos.

-En 1999, tots els clients de AOL, en EE.UU, van rebre diverses vegades missatges com aquest:
“SYSTEM ADMINISTRATOR: A database error has deleted the information for over 25000 accounts, and yours is one. In order for us to access the backup data, we do need your password. Without your password, we will NOT be able to allow you*to sign onto America Online within the next 24 hours after your opening of this letter”.

És una tàctica comuna trucar per telèfon a empleats d'una companyia, fent-se

passar per un administrador de xarxa, oficial de seguretat o personal de manteniment. Si l'atacant sap suficient de la xarxa de la companyia com per sonar convincentment, pot obtenir contrasenyes, noms de comptes, etc. Moltes vegades, tot consisteix a preguntar. La gent vol col·laborar i sol fiar-se d'una altra gent que sap de quina parla, més si li dóna dades del seu lloc de treball. En realitat, el terme enginyeria social és equivalent a enganyar, mentir, aconseguint que una altra persona faci coses que l'atacant vol que es facin. És difícil de parar, almenys tècnicament, doncs no usa mètodes informàtics. Va a la baula més feble de la cadena de seguretat: usa del factor humà. A l'hora de tenir-ho en compte en la política de seguretat, caldrà fer-ho en la part de formació general per a tothom. Encara que hi ha alguna cosa que es pot fer per frenar aquest tipus d'atacs, mai s'aconseguirà parar-los del tot amb eines informàtiques, doncs s'aprofiten de la bona voluntat de la gent. Quant a l'altra opció, les tècniques informàtiques d'obtenció d'informació, es parla, generalment, de com usar comandos i eines, no dissenyades específicament, per a un atac, com a mitjans d'obtenció d'informació.

2.4.2 Denegació de servei (DoS)

El propòsit general de l'atac és denegar a les víctimes l'accés a un recurs particular, aquesta caracteritzat per un intent, per part dels agressors, d'evitar que els legítims usuaris puguin utilitzar un determinat servei. Per exemple:

7 Intent de "inundar" una xarxa, impedint el trafico legítim d'aquesta xarxa.
8 Intent de trencar la connexió entre dues màquines, impedint l'accés a un servei determinat.
9 Intent d'impedir l'accés d'un usuari individual a un servei.
10 Intent de trencar els serveis a un sistema especifico.

Les negacions de servei (Denial of Service, DOS) són atacs dirigits contra un recurs informàtic amb l'objectiu de degradar total o parcialment els serveis prestats per aquest recurs als seus usuaris legítims, constitueixen en molts casos un dels atacs més senzills i contundents contra tot tipus de serveis, i en entorns on la disponibilitat és valorada per sobre d'altres paràmetres de la seguretat global pot convertir-se en un seriós problema, ja que un pirata pot interrompre constantment un servei sense necessitat de grans coneixements o recursos, utilitzant simplement senzills programes i un mòdem i un PC casolans.

Els ataquis "Denegació de Servei" vénen daus en una varietat de formes i es dirigeixen cap a una gran varietat de serveis. Hi ha tres tipus bàsics d'atac:

11 Consum de recursos, limitats o no renovables.
12 Destrucció o alteració d'informació sobre configuració.
13 Destrucció física o alteració de components d'una xarxa.

Tots els sistemes Unix ofereixen mecanismes per evitar que un usuari normal pugui tirar a baix una màquina. El problema real no és que usuaris legítims d'un entorn causin, intencionada o *inintencionadamente, negacions de servei, el major problema és que aquestes negacions siguin causades de forma remota per pirates aliens per complet a la nostra organització, capaces de tombar un servidor de milions de pessetes amb senzills programes, sense deixar cap rastre i el pitjor, sense ser moltes vegades conscients del dany que estan fent. Aquests atacs remots de negació de servei són considerats negatius fins i tot per molts dels propis pirates, ja que realment no solen demostrar res positiu de qui els llança. En la major part dels casos la negació de servei té èxit perquè l'objectiu utilitza versions no actualitzades de dimonis o del propi nucli del sistema operatiu, si es deté o degrada per complet la màquina. Per evitar això, la norma a seguir és evident, mantenir sempre actualitzats els nostres sistemes, tant referent al nivell de patching o versions del nucli, com referent a programes crítics encarregats d'oferir un determinat servei. Les negacions de servei més habituals solen consistir en la inhabilitació total d'un determinat servei o d'un sistema complet, bé perquè ha estat realment bloquejat per l'atacant o bé perquè està tan degradat que és incapaç d'oferir un servei als seus usuaris. En la major part de sistemes, un usuari amb accés *shell no tindrà moltes dificultats a causar una negació de servei que tirés a baix la màquina o la ralentís enormement, això no té perquè ser un atac intencionat, sinó que pot deure's a un simple error de programació.

El consum de recursos estan limitats, ordinadors i xarxes necessiten certes coses per funcionar: ample de banda per a la xarxa, memòria i espai de disc, temps de CPU, estructures de dades, accés a altres equips i xarxes, i uns certs recursos d'entorn com són: potència o aire fred.

1. Connectivitat entre xarxes: Els ataquis denegació de servei es duen a terme freqüentment contra la capacitat de connectivitat entre xarxes. La intenció és evitar que els equips o les subxarxes es puguin comunicar amb la resta de la xarxa. Un exemple d'aquest tipus d'atac és el SYN flood1. En aquest tipus d'atac, es comença pel

procés d'establiment de connexió de la màquina víctima, la culminació de l'atac arriba quan la màquina víctima ha reservat un dels limitats nombres d'estructures de dades requerides per completar la connexió. El resultat és que la legítima connexió es denega mentre que la màquina víctima espera al fet que es completi la connexió, cosa que no arriba a succeir. Cal notar que aquest tipus d'atac no es pretén consumir ample de banda sinó els recursos de memòria i processador que es consumeixen amb les estructures de dades usades per establir una comunicació. Això implica que un atacant pot dur a terme el seu atac des d'un mòdem contra una xarxa molt més ràpida.

2. Utilització dels teus propis recursos contra tu: Un intrús pot usar els teus propis recursos contra tu d'inesperades maneres.

3. Consum d'ample de banda: Un intrús també pot ser capaç de consumir tot l'ample de banda disponible a la xarxa generant una gran quantitat de paquets dirigits a la teva xarxa. Típicament aquests són paquets ICMP TIRO, però en principi poden ser de qualsevol altre tipus. L'intrús no té perquè actuar des d'una de les màquines de la subxarxa, pot ser capaç de coordinar diverses màquines de diferents xarxes per obtenir el mateix resultat.

4. Consum d'altres recursos: Juntament amb el consum d'ample de banda, els intrusos poden ser capaços de consumir altres recursos que el sistema necessita per operar correctament. Per exemple, hi ha sistemes en els quals existeixen un nombre limitat d'estructures de dades per proporcionar informació sobre processos (identificadors de processos, taules d'entrades de processos, etc.). Un intrús pot ser capaç de consumir aquestes estructures de dades escrivint un script que no faci gens, però que repetidament creu còpies de si mateix. Molts sistemes operatius moderns, encara que no tots, tenen quotes per protegir contra aquests atacs. De totes maneres, si la taula de processos no està plena, la CPU pot estar ocupada amb un gran nombre de processos i el corresponent temps per commutar entre processos. Un intrús també pot intentar consumir espai de disc d'altres maneres, per exemple:

-Generar excessiu nombre de missatges de correu.
-Generar intencionadament errors que s'emmagatzemin en fitxers log.
-Col·locar fitxers en àrees de ftps anònims.

En general, qualsevol cosa que permeti dades en disc, pot ser utilitzada per dur a terme un atac denegació de servei. D'altra banda en alguns llocs, apareix el missatge lockout" després d'un cert nombre d'intents fallits d'accés a un determinat compte,

normalment 3 o 5. Un intrús pot usar aquest fet per evitar l'accés al compte al seu legítim usuari. En alguns casos les comptes amb privilegis solen ser blancs d'aquests atacs. El millor és estar segur de tenir un mètode alternatiu per accedir al sistema en cas d'emergència. Un intrús pot fer que un sistema s'enfonsi o que es torni inestable enviant dades inesperades a través de la xarxa. Si el teu sistema s'enfonsa sovint sense causa aparent, pot ser que es tracti d'aquest tipus d'atac. Hi ha altres coses que poden ser vulnerables per a un atac denegació de servei i que és convenient monitorizar:

14 impressores
15 cintes de backup
16 connexions a xarxes
17 qualsevol recurs important per a les operacions de la teva empresa
Els atacs per denegació de servei poden suposar una important pèrdua de temps i diners per a la majoria de les organitzacions. Recomanem considerar les següents opcions depenent de les necessitats personals:

Implementar routers que filtrin. Això disminuirà l'exposició a certs atacs. Addicionalment, això pot prevenir que usuaris de la teva xarxa llancin certs atacs. Si és possible, instal·lar pegats per protegir-se contra atacs TCP SYN flooding. Això pot reduir substancialment l'exposició a aquests atacs, encara que no elimina el risc per complet. Desactivar qualsevol servei de xarxa que no sigui necessari. Això pot limitar la capacitat de l'intrús d'utilitzar aquests serveis per realitzar el seu atac. Activar mecanismes de quota en el sistema operatiu si és possible. Per exemple si el sistema operatiu suporta quotes de disc, activar-les para tots els comptes, especialment per a comptes que operen amb serveis de xarxa. A més si el sistema operatiu suporta la partició de discos, és convenient considerar fer particions dels sistemes de fitxers per separar funcions crítiques d'altres activitats. Observar el rendiment i estabilitat de les línies bàsiques de l'activitat quotidiana. Observar nivells inusuals d'activitat de disc, ús de CPU o tràfic de xarxa. Examinar rutinàriament la seguretat física. Considerar servidors, routers, terminals, punts d'accés a la xarxa i altres components del sistema. Utilitzar Tripwire o una eina similar per detectar canvis en la informació sobre configuració o d'altres fitxers. Col·locar i mantenir "hot spares", màquines que poden ser posades en servei ràpidament en el moment que una màquina s'ha desactivat. Activar a la xarxa configuracions redundants i tolerants a fallades. Establir i mantenir calendaris i polítiques de backup, sobretot per a informació important sobre configuració. Establir i mantenir polítiques de claus apropiades, especialment per a accés a comptes amb privilegis com és la de root. Moltes organitzacions poden sofrir perdudes financeres com a resultat d'aquests atacs i poden decidir presentar càrrecs

contra l'intrús.

D'un temps a ara s'ha popularitzat molt el terme negació de servei distribuïda (Distributed Denial of Service, DDoS), en aquest atac un pirata compromet en primer lloc un determinat nombre de màquines i, en un determinat moment, fa que totes elles ataquin massiva i simultàniament a l'objectiu o objectius reals enviant-los diferents tipus de paquets, per molt grans que siguin els recursos de la víctima, el gran nombre de trames que reben farà que tard o d'hora aquests recursos siguin incapaços d'oferir un servei, amb el que l'atac haurà estat reeixit. Si en lloc de centenars o milers d'equips atacant alhora ho fes un només les possibilitats d'èxit serien gairebé inexistents, però és justament l'elevat nombre de petits atacants el que fa molt difícil evitar aquest tipus de negacions de servei. Segons el CERT els atacs de negació de servei distribuïts més habituals consisteixen en l'enviament d'un gran nombre de paquets a un determinat objectiu per part de múltiples hosts, la qual cosa es coneix com packet ooding. Defensar-se d'aquest tipus d'atacs és difícil, en primer lloc, un pensa a bloquejar d'alguna forma (probablement en un tallafocs o en un router) tot el tràfic provinent dels atacants, però què succeeix quan tenim milers d'ordinadors atacant des d'un gran nombre de xarxes diferents? Els bloquegem un a un? Això suposaria un gran esforç que difícilment ajudarà, ja que el més probable és que en el temps que ens costi bloquejar el tràfic d'una determinada màquina, dues o tres noves ens comencin a atacar. Llavors, bloquegem tot el tràfic dirigit cap a l'objectiu? Si fem això, estem justament ajudant a l'atacant, ja que som nosaltres mateixos els que causem una negació en el servei als usuaris legítims del nostre sistema.

La defensa davant una negació de servei distribuïda no és immediata, en qualsevol cas, podem prendre certes mesures preventives que ens ajudaran a limitar l'abast d'un d'aquests atacs. Un correcte filtrat del tràfic dirigit a les nostres màquines és vital per garantir la nostra seguretat, no cal respondre a pings externs a la nostra xarxa, és necessari activar el antispoofing en els nostres tallafocs i en els elements d'electrònica de xarxa que ho permetin, etc. Establir correctament límits a la utilització dels nostres recursos és també una important mesura preventiva, és possible limitar l'ample de banda dedicat a una determinada aplicació o a un protocol, de manera que les utilitzacions per sobre del marge són negades.

També podem limitar els recursos del sistema CPU, memòria, disc…) que pot consumir en global una determinada aplicació servidora (per exemple, un dimoni servint pàgines Web), a més de restringir els seus recursos per client simultani. Malgrat les dificultats amb les quals ens podem trobar a l'hora de prevenir atacs de

negació de servei, una sèrie de mesures senzilles poden ajudar-nos de forma relativa en aquesta tasca, les negacions de servei són per desgràcia cada dia més freqüents, i cap organització està a resguard de les mateixes. Especialment en els atacs distribuïts, la seguretat de qualsevol usuari connectat a Internet és una baula important en la seguretat global de la xarxa, ja que aquests usuaris es converteixen moltes vegades sense saber-ho en satèl·lits que col·laboren en un atac massiu contra organitzacions de qualsevol tipus. Com més difícil l'hi posem cadascun de nosaltres als pirates, molt millor per a tots.

2.4.3 Atacs remots i intercepció.

Escanejo de ports: una de les primeres activitats que un atacant realitzarà contra el seu objectiu seria sens dubte un escanejo de ports, un portscan, això li permetrà obtenir en primer lloc informació bàsica sobre quins serveis estem oferint en les nostres màquines i, addicionalment, altres detalls del nostre entorn com a quin sistema operatiu tenim instal·lats en cada host o certes característiques de l'arquitectura de la nostra xarxa. Analitzant què ports estan oberts en un sistema, l'atacant pot buscar forats en cadascun dels serveis oferts, cada port obert en una màquina és una porta d'entrada a la mateixa. Comprovar l'estat d'un determinat port és a priori una tasca molt senzilla, fins i tot és possible dur-la a terme des de la línia d'ordres, usant una eina tan genèrica com telnet. Per exemple, per conèixer l'estat del port 5111 en la màquina l'adreça de la qual és www.terra.es, si el telnet ha dit port ofereix una resposta, llavors està obert i escoltant peticions:

```
C:\Documents and Settings\yagonet\telnet www.terra.es 5111
Conectándose a www.terra.es...
No se puede abrir la conexión al host, en puerto 5111:
Error en la conexión
C:\Documents and Settings\yagonet>
```

Si el port està protegit per un tallafocs, el més probable és que no s'obtingui resposta alguna, el telnet llançat es quedaria intentant la connexió fins que es produeixi un timeout o fins que es pari manualment.

En general, ningú en el seu sa judici usarà telnet per realitzar un escanejo de ports massiu contra un sistema o contra tota una xarxa, existeixen eines com *strobe o

nmap (la més coneguda) que poden realitzar aquesta tasca d'una forma més o menys còmoda i automàtica. Evidentment, cap d'aquests programes es dedica a llançar telnet contra els ports d'un sistema, els *escaneadores de ports actuals implementen diferents tècniques que permeten detectar des de la versió del sistema operatiu usat en la màquina atacada, fins a passar inadvertits davant diferents sistemes de detecció d'intrusos. Existeixen diferents aproximacions per classificar els escanejos de ports, tant en funció de les tècniques seguides en l'atac com en funció de quins sistemes o ports concrets va dirigit. Es parla d'un escanejo horitzontal quan l'atacant busca la disponibilitat de determinat servei en diferents màquines d'una xarxa, per exemple, si el pirata disposa d'un exploit que aprofita una fallada en la implementació de sendmail, és normal que tracti d'esbrinar què màquines accepten peticions smtp en un determinat segment per posteriorment atacar a aquests sistemes. Si per contra el pirata només escaneja ports d'una màquina, es denomina a l'atac escanejo vertical, i sol denotar l'interès de l'atacant en aquest host concret. Si comprova tots els ports del sistema a l'escanejo se li denomina vanilla, mentre que si només ho fa contra determinats ports o rangs, se li denomina strobe. Si ens basem en les tècniques utilitzades, podem dividir els escanejos en tres grans famílies:

1 Open.
2 Half-open
3 Stealth

Els escanejos open es basen en l'establiment d'una connexió TCP completa mitjançant el conegut com a protocol d'acord de tres vies o three-way handshake, per la qual cosa són molt senzills de detectar i detenir. Utilitzen la trucada connect(). La segona tècnica half-open, el pirata finalitza la connexió abans que es completi el protocol d'acord de tres vies, la qual cosa dificulta la detecció de l'atac per part d'alguns detectors d'intrusos molt simples (gairebé tots els actuals són capaços de detectar-los). Dins d'aquesta tècnica es troba el SYN Scanning: quan l'origen -atacant - rep del destino - màquina escanejada - els bits SYN+ACK, envia un bit RST (no és necessària una nova trama, ja que aquest bit s'envia automàticament a nivell de nucli) en lloc del ACK corresponent a un three-way handshake complet.

Els escanejos SYN són fàcilment detectables i poden ser bloquejats en qualsevol tallafocs. Existeix una variable d'aquesta tècnica denominada dumb scanning en la qual entra en joc una tercera màquina denominada “ximple” (pel poc tràfic que emet i rep), alguna cosa que pot ajudar al pirata a camuflar el seu origen real. No obstant això, el dumb scanning és més complicat que el SYN scanning, per

la qual cosa s'utilitza molt menys en la vida real. Al desembre de 1995 Christopher Klaus va proporcionar les pautes de certes tècniques d'escanejo que permetien a l'atacant eludir l'acció dels sistemes de detecció d'intrusos de l'època i a les quals va batejar com stealth scanning, actualment el significat del terme ha canviat, ja que el que Klaus va presentar es denomina avui dia half-open scanning, i per stealth scanning es coneix a una família de tècniques d'escanejo que compleixen alguna de les següents condicions:

4 Eludir tallafocs o llistes de control d'accés.

5 No ser registrades per sistemes de detecció d'intrusos, ni orientats a xarxa ni en el propi host escanejat.

6 Simular tráfico normal y real para no levantar sospechas ante un analizador de red.

Una de les tècniques que es troben dins de la família dels escanejos stealth és la coneguda com SYN+ACK. La idea és molt simple, i consisteix en una violació del three-way handshake, l'atacant, en lloc d'enviar en primer lloc una trama SYN, envia SYN+ACK. Si el port està obert simplement s'ignora, i si està tancat sap que no ha rebut prèviament un paquet SYN, per la qual cosa ho considera un error i envia una trama RST per finalitzar la connexió. Els escanejos basats en aquest mètode s'usen poc en l'actualitat, a causa de l'elevat nombre de falsos positius que poden generar: només hem de pensar en els múltiples motius que poden existir perquè un sistema no respongui davant una petició SYN+ACK, des de llistes de control d'accessos en els routers o tallafocs fins a simples timeouts. Una altra tècnica dins dels escanejos *tealth és la FI scanning, en aquest cas, l'atacant envia al seu objectiu una trama amb el bit FI activa, davant el que est respon amb un RST si el port està tancat, o simplement no respon en cas d'estar obert, com en el cas dels escanejos SYN+ACK aquest mètode pot proporcionar molts falsos positius, per la qual cosa tampoc s'utilitza molt avui dia. Un mètode d'escanejo una mica més complex és el ACK. L'atacant envia una trama amb aquest bit actiu, i si el port destino està obert és molt possible que o bé el camp TTL del paquet de tornada sigui menor que el de la resta de les trames RST rebudes, o que la grandària de finestra sigui major que zero, com podem veure, en aquest cas no n'hi ha prou amb analitzar el bit RST sinó també la capçalera IP del paquet resposta. Aquest mètode és difícil de registrar per part dels detectors d'intrusos, però es basa en el codi de xarxa de BSD, per la qual cosa és depenent de l'operatiu escanejat.

Per finalitzar amb la família de stealth scanning dir que hi ha dos mètodes oposats entre si però que es basen en una mateixa idea i proporcionen resultats similars, es tracta de XMAS i NULL. Els primers, també denominats escanejos

"arbre de nadal", es basen a enviar a l'objectiu trames amb tots els bits TCP (URG, ACK, PST, RST, SYN i FI) actius, si el port està obert el nucli del sistema operatiu eliminarà la trama, ja que evidentment la considera una violació del three-way handshake, però si està tancat retornarà un RST a l'atacant. Com abans, aquest mètode pot generar massa falsos positius, i a més només és aplicable contra màquines Unix a causa que està basat en el codi de xarxa de BSD. El mètode oposat al XMAS es denomina NULL scanning, i evidentment consisteix a enviar trames amb tots els bits TCP reseteados, el resultat és similar, no es retornarà cap resultat si el port està obert, i s'enviarà un RST si està tancat. Encara que en principi aquest mètode seria aplicable a qualsevol pila TCP/IP, la implementació incorrecta que fan alguns sistemes operatius (entre ells HP/UX o IRIX) d'aquesta, fa que en ocasions s'enviïn bits RST també des dels ports oberts, la qual cosa pot proporcionar massa falsos positius.

Una altra tècnica que no aquesta englobada en l'anterior classificació és els escaneos UDP, que al contrari de tots els comentats fins al moment utilitza aquest protocol, i no TCP, per determinar l'estat dels ports d'una màquina. En enviar un datagrama UDP a un port obert est no ofereix resposta alguna, però si està tancat retorna un missatge d'error ICMP: ICMP_PORT UNREACHABLE. Evidentment, aquests atacs són molt senzills de detectar i evitar tant en un sistema de detecció d'intrusos com en els nuclis d'alguns Unix, i per si això fos poc hem de recordar que UDP no és un protocol orientat a connexió (com l'és TCP), per la qual cosa la pèrdua de datagrames pot donar lloc a un elevat nombre de falsos positius.

2.4.4 Spoofing y escaneig de ports.

Per spoofing es coneix a la creació de trames TCP/IP utilitzant una adreça IP falsa, des del seu equip, un pirata simula la identitat d'una altra màquina de la xarxa per aconseguir accés a recursos d'un tercer sistema que ha establert algun tipus de confiança basada en el nom o l'adreça IP del host suplantat. I com els anells de confiança basats en aquestes característiques tan fàcilment falsificables són encara massa abundants, el spoofing segueix sent en l'actualitat un atac no trivial, però factible contra qualsevol tipus d'organització. En el spoofing entren en joc tres màquines: un atacant, un atacat, i un sistema suplantat que té certa relació amb l'atacat, perquè el pirata pugui aconseguir el seu objectiu necessita d'una banda establir una comunicació falsejada amb el seu objectiu, i per un altre evitar que

l'equip suplantat interfereixi en l'atac. Probablement això últim no li sigui molt difícil d'aconseguir, a pesar que existeixen múltiples formes de deixar fora de joc al sistema suplantat - almenys als ulls de l'atacat - que no són trivials (modificar rutes de xarxa, situar un filtrat de paquets entre tots dos sistemes...), el més fàcil en la majoria d'ocasions és simplement llançar una negació de servei contra el sistema en qüestió. Encara que en el punt següent parlarem amb més detall d'aquests atacs, no sol ser difícil "tombar", o almenys bloquejar parcialment, un sistema mitjà; si malgrat tot l'atacant no ho aconsegueix, simplement pot esperar al fet que desconnectin de la xarxa a la màquina a la qual desitja suplantar (per exemple, per qüestions de pur manteniment).

L'altre punt important de l'atac, la comunicació falsejada entre dos equips, no és tan immediat com l'anterior i és on resideix la principal dificultat del spoofing. En un escenari típic de l'atac, un pirata envia una trama SYN al seu objectiu indicant com a adreça origen la d'aquesta tercera màquina que està fora de servei i que manté algun tipus de relació de confiança amb l'atacada. El host objectiu respon amb un SYN+ACK a la tercera màquina, que simplement ho ignorarà per estar fos de servei (si no ho fes, la connexió es resetearía i l'atac no seria possible), i l'atacant enviarà ara una trama ACK al seu objectiu, també amb l'adreça origen de la tercera màquina. Perquè la connexió arribi a establir-se, aquesta última trama haurà d'enviar-se amb el nombre de seqüència adequat, el pirata ha de predir correctament aquest nombre, si no ho fa, la trama serà descartada, i si ho aconsegueix la connexió s'establirà i podrà començar a enviar dades al seu objectiu, generalment per tractar d'inserir una porta posterior que permeti una connexió normal entre les dues màquines.

Podem comprovar que el spoofing no és immediat, d'entrada, l'atacant ha de fer-se una idea de com són generats i incrementats els nombres de seqüència TCP, i una vegada que ho sàpiga ha d'aconseguir enganyar al seu objectiu utilitzant aquests nombres per establir la comunicació, com més robusta sigui aquesta generació per part de l'objectiu, més difícil ho tindrà el pirata per realitzar l'atac amb èxit. A més el spoofing és un atac cec, l'atacant no veu en cap moment les respostes que emet el seu objectiu, ja que aquestes van dirigides a la màquina que prèviament ha estat deshabilitada, per la qual cosa ha de pressuposar què està succeint a cada moment i respondre de forma adequada sobre la base d'aquestes suposicions.

Per evitar atacs de spoofing reeixits contra els nostres sistemes podem prendre diferents mesures preventives, en primer lloc, sembla evident que una gran ajuda és reforçar la seqüència de predicció de nombres de seqüència TCP. Una altra mesura

senzilla és eliminar les relacions de confiança basades en l'adreça IP o el nom de les màquines, substituint-les per relacions basades en claus criptogràfiques, el xifrat i el filtrat de les connexions que poden acceptar les nostres màquines també són unes mesures de seguretat importants de cara a evitar el spoofing.
Hi ha altres atacs de falsejament a part del comentat entre els quals cal destacar:

-DNS Spoofing: Aquest atac fa referència al falsejament d'una adreça IP davant una consulta de resolució de nom (això és, resoldre amb una adreça falsa un cert nom DNS), o viceversa (resoldre amb un nom fals una certa adreça IP). Això es pot aconseguir de diferents formes, des de modificant les entrades del servidor encarregat de resoldre una certa petició per falsejar les relacionis adreça-nom, fins a comprometent un servidor que infecti la memòria cau d'un altre (el que es coneix com DNS Poisoning); fins i tot sense accés a un servidor DNS real, un atacant pot enviar dades falsejades com a resposta a una petició de la seva víctima sense més que esbrinar els nombres de seqüència correctes.

-ARP Spoofing: L'atac denominat ARP Spoofing fa referència a la construcció de trames de sol·licitud i resposta ARP falsejades, de manera que en una xarxa local es pot forçar a una determinada màquina al fet que enviï els paquets a un host atacant en lloc de fer-ho a la seva destinació legítima. La idea és senzilla, i els efectes de l'atac poden ser molt negatius, des de negacions de servei fins a intercepció de dades.

-Web Spoofing: Aquest atac permet a un pirata visualitzar i modificar qualsevol pàgina Web que la seva víctima sol·liciti a través d'un navegador, incloent les connexions segures via SSL. Per a això, mitjançant codi maliciós un atacant crea una finestra del navegador corresponent, d'aparença inofensiva, en la màquina de la seva víctima, a partir d'aquí, encamina totes les pàgines dirigides a l'equip atacat, incloent les carregades en noves finestres del navegador, a través de la seva pròpia màquina, on són modificades perquè qualsevol esdeveniment generat pel client sigui registrat (això implica registrar qualsevol dada introduïda en un formulari, qualsevol clic en un enllaç, etc.).

2.5 Orientació dels atacs.

Hacker.: és una de les denominacions de major prestigi en el sentit del coneixement tecnològic, no obstant això els hackers més famosos són els qui van

cometre delictes informàtics. Per tant podria dir-se que existeixen dos tipus d'hackers, els que col·laboren en el creixement de la tecnologia i els que s'aprofiten dels seus coneixements per dur a terme operacions il·legals. D'altra banda, els crackers i script kiddies són en realitat els qui efectuen danys en les màquines. Un hacker investiga, tracta de solucionar problemes i és precisament un cracker, i en menor mesurada un script kidd, qui es dedica a ocasionar-los.

Virus.: els virus informàtics i cucs s'aprofiten de les vulnerabilitats de les aplicacions per infectar el PC i reproduir-se, sent indetectable a la visió de l'usuari fins que es duu a terme l'atac. Existeixen diferents tipus de virus, segons les seves finalitats, però les dues característiques que els uneixen són: reproduir-se i/o sobreviure, i complir les seves missions. La millor solució per protegir el PC dels virus és tenir instal·lat un bon antivirus i mantenir-ho actualitzat.

Hoax.: bàsicament, un Hoax és una falsedat, que moltes persones creuen i difonen, creada amb aquesta fi. La definició més estesa la trobem en l'àmbit del món antivirus, i que considera als Hoax com a missatges enviats en general mitjançant correu electrònic, encara que poden aparèixer moltes vegades en paper fotocopiat en l'ambient empresarial, en els quals s'avisa en to alarmant de l'existència de nous i potents virus, molt perillosos i destructius.

Aquests suposats virus en realitat no existeixen, o són arxius inofensius sobre els quals recau l'elecció dels creadors de l'Hoax. La finalitat de tal creació seria la de crear alarma entre els cibernautes i aconseguir la reexpedició massiva d'aquests missatges alarmistes. Llavors potser la definició més encertada seria aquella que contempli als Hoax com un missatge el contingut del qual està basat en mentides, enganys o falsedats, en ocasions relatives a falsos virus, creat per a la seva reexpedició massiva. Aquest missatge estaria creat bé per causar algun tipus de perjudici o bé per a diversió del/els creadors del mateix. L'objectiu d'aquests avisos alarmants és difícil d'establir, ja que no es coneixen els motius que impulsen a algú a crear un element perjudicial d'aquest tipus. Aquestes serien les motivacions:

1 Crear una "alarma social" entre els cibernautes. Se suposa que això resultaria divertit pel qui ha iniciat l'hoax.

2 Recopilar gran quantitat d'adreces de correu.

3 Difondre informació falsa en perjudici de terceres persones o organismes.

4 Incitar al receptor del missatge a causar danys en el seu propi ordinador.

5 Una mera competició a la recerca del major nombre de missatges.

6 La notorietat que atorgaria en el cercle del creador de l'hoax una gran difusió del mateix.

Spam.: és el rebut de correu electrònic no sol·licitat. El correu no desitjat és el major problema que enfronta avui Internet.

El spam és responsable de col·lapsar xarxes, provocar pèrdues milionàries i enfuriar a l'usuari casolà saturant les seves bústies.

Els qui fan spam justifiquen els seus actes dient que realitzen màrqueting electrònic, no obstant això no tenen en compte la situació límit a la qual s'ha arribat.

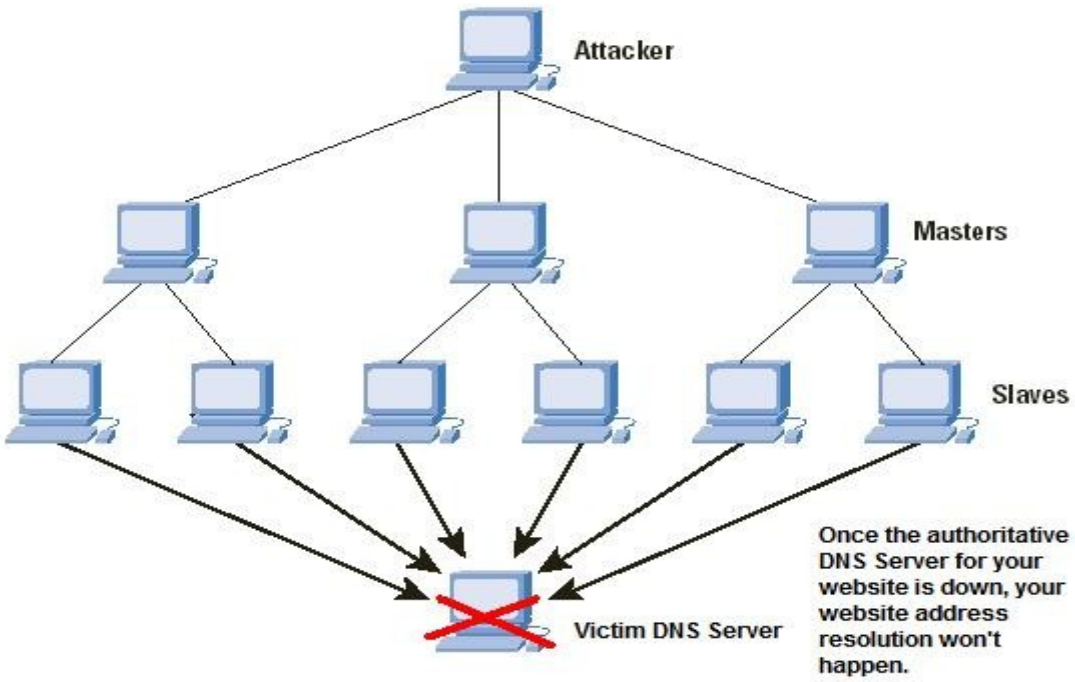
Dialers.: sense cap dubte, una de les més recents i impactants amenaces d'Internet. El que fa un dialer és connectar el nostre PC a Internet per mitjà d'un nombre més costós del normal.

El problema resideix que els responsables no sempre adverteixen de la instal·lació d'aquesta modalitat en el nostre equip, usualment mentre visitem una pàgina Web.

D'aquesta manera, l'usuari només adverteix el parany en rebre la seva factura telefònica. Els dialers afecten principalment als usuaris d'Espanya, on s'han pres mesures sobre aquest tema (denegar l'ús d'aquests nombres telefònics a usuaris que ho sol·licitin, i reduir els costos de trucada).

Els dialers no s'eliminen perquè una gran part dels llocs Web viuen d'això, i no està mal sempre que l'usuari sigui conscient de la modalitat que se li imposa per accedir al contingut d'una pàgina.

2.5.1 Atacs al sistema (Core Attack)



2.5.2 Atacs a la plataforma web (vulnerabilitat de plataformes d'e-commerce)

Durant els últims anys els servidors Web s'han convertit en una excel·lent font de diversió per a pirates, qualsevol empresa que es preï, des de les més petites a les grans multinacionals, té una pàgina Web en les quals almenys tracta de vendre la seva imatge corporativa. Si fa uns anys un pirata que volgués atacar a una empresa (i no a totes, ja que molt poques tenien representació a la xarxa) havia d'agenciar-les-hi per obtenir primer informació de la mateixa i després buscar errors de configuració més o menys comunes dels seus sistemes, avui dia li n'hi ha prou amb teclejar el nom del seu objectiu en un navegador i afegir l'afegitó .com darrere del mateix per contactar amb almenys una de les seves màquines, el seu servidor Web.

Els atacs a les pàgines Web d'una organització són gairebé sempre els més vistosos que la mateixa pot sofrir, en qüestió de minuts pirates de tot el món

s'assabenten de qualsevol problema a la pàgina Web principal d'una empresa més o menys gran pugui estar sofrint, i si es tracta d'una modificació de la mateixa fins i tot existeixen recopilatoris de pàgines hackeades. Per descomptat, la notícia de la modificació salta immediatament als mitjans, que gràcies a ella poden emplenar alguna capçalera sensacionalista sobre els pirates de la xarxa, i així s'aconsegueix que la imatge de l'empresa atacada caigui notablement i la del grup de pirates pugi entre la comunitat underground nacional o internacional.

La major part d'aquests atacs té èxit gràcies a una configuració incorrecta del servidor o a errors de disseny del mateix, si es tracta de grans empreses, els servidors Web solen ser bastant complexos (alta disponibilitat, balanceig de càrrega, sistemes propietaris d'actualització de continguts…) i difícils d'administrar correctament, mentre que si l'empresa és petita és molt possible que hagi triat un servidor Web simple en la seva instal·lació i administració però en el qual és gairebé impossible garantir una mínima seguretat. Sigui pel motiu que sigui, la qüestió és que cada dia és més senzill per a un pirata executar ordres de forma remota en una màquina, o almenys modificar continguts de forma no autoritzada, gràcies als servidors Web que un sistema pugui albergar.

Qualsevol analitzador de vulnerabilitats que puguem executar contra els nostres sistemes (nessus, ISS Security Scanner, NAI CyberCop Scanner…) és capaç de revelar informació que ens va a resultar útil a l'hora de reforçar la seguretat dels nostres servidors Web, fins i tot existeixen analitzadors que estan dissenyats per auditar únicament aquest servei, com whisker, el qual ens proporciona excessiva informació sobre la configuració del servidor(versió, mòduls, suport SSL…), i que l'eina ha obtingut alguns arxius i directoris que poden resultar interessants per a un atacant, en el cas dels CGI no té més que apropar-se a alguna base de dades de vulnerabilitats i introduir en el cercador corresponent el nom de l'arxiu per obtenir informació sobre els possibles problemes de seguretat que pugui presentar. El cas dels directoris és alguna cosa diferent, però típicament se sol tractar de noms habituals en els servidors que contenen informació que també pot resultar-li útil a un potencial atacant.

Com evitar aquests problemes de seguretat dels quals estem parlant? Una mesura elemental és eliminar del servidor qualsevol directori o CGI d'exemple que s'instal·li per defecte, encara que generalment els directoris (documentació, exemples…) no són especialment crítics, el cas dels CGIs és bastant alarmant, molts servidors incorporen programes que no són ni tan sols necessaris per al correcte

funcionament del programari, i que en certs casos obren enormes forats de seguretat, com l'accés al codi font d'alguns arxius, la lectura de fitxers fos del DocumentRoot, o fins i tot l'execució remota de comandos sota la identitat de l'usuari amb que s'executa el dimoni servidor.

Una altra mesura de seguretat bàsica és deshabilitar el Directory Indexing que per defecte molts servidors incorporen, la capacitat d'obtenir el llistat d'un directori quan no existeix un fitxer index.html o similar en el mateix, es tracta d'una mesura extremadament útil i sobretot senzilla d'implantar, ja que en molts casos un simple chmod -r sobre el directori en qüestió és suficient per evitar aquest problema. A primera vista aquesta mesura de protecció ens pot resultar curiosa, al cap i a l'últim, a priori tot el que hi hagi sota el Document Root del servidor ha de ser públic, ja que para això se situa aquí. Evidentment la teoria és una cosa i la pràctica altra molt diferent, entre els fitxers de qualsevol servidor no és estrany trobar des d'arxius de log fins a paquets tar amb el contingut de subdirectoris complets. Per descomptat, la millor defensa contra aquests atacs és evitar d'alguna forma la presència d'aquests arxius sota el Document Root, però en qualsevol cas això no és sempre possible, i si un atacant sap de la seva existència pot descarregar-los, obtenint en molts casos informació realment útil per atacar al servidor (com el codi de fitxers jsp, php, asp… o simplement rutes absolutes en la màquina), i una excel·lent forma de saber que un d'aquests fitxers està aquí és justament el Directory Indexing, per si això no queda del tot clar, no tenim més que anar a un cercador qualsevol i buscar la cadena Index of /admin, per posar un exemple senzill, per fer-nos una idea de la perillositat d'aquesterror de configuració.

A més, en qualsevol servidor Web és molt important l'usuari baix la identitat del qual s'executa el dimoni httpd, aquest usuari no ha de ser mai el root del sistema, però tampoc un usuari genèric com nobody, s'ha de tractar sempre d'un usuari dedicat i sense accés real al sistema. Per descomptat, les pàgines html (els fitxers plans, per entendre'ns) mai han de ser de la seva propietat, i molt menys aquest usuari ha de tenir permís d'escriptura sobre els mateixos, amb un accés de lectura (i execució, en cas de CGIs) és més que suficient en la majoria dels casos.

Hem de tenir en compte que si l'usuari que executa el servidor pot escriure a les pàgines Web, i un pirata aconsegueix executar ordres sota la identitat de dita usuària, podria modificar les pàgines Web sense cap problema (que no oblidem, és el que perseguirà la majoria d'atacants del nostre servidor Web).

Igual d'important que evitar aquests problemes és detectar quan algú tracta d'aprofitar-los intentant trencar la seguretat dels nostres servidors, per aconseguir-ho no tenim més que aplicar les tècniques de detecció d'intrusos que veurem més endavant.

Una característica important dels patrons de detecció d'atacs via Web és que no solen generar molts falsos positius, per la qual cosa la configuració de la base de dades inicial és ràpida i senzilla, almenys en comparació de la detecció de escanejos de ports o la de trames amb alguna característica especial en la seva capçalera.

El nombre d'atacs d'hackers a sistemes connectats a Internet està tenint un creixement exponencial en els últims temps. Així mateix, el nombre de serveis que l'Administració Pública proporciona als ciutadans a través d'Internet és cada vegada major, sent en conseqüència també major el risc d'atacs als Sistemes d'Informació de les entitats públiques. Un troià és un programa maliciós inserit en un PC sense consentiment del seu amo que permet el control d'aquest PC per part d'una persona no autoritzada, podent-se fins i tot considerar un tipus de virus, ja que el PC atacat es "infecta" amb ell. Té unes característiques pròpies que li confereixen un caràcter maliciós:

1 S'aprofita freqüentment de bugs i backdoors dels sistemes informàtics, com el Back Orifice o el BackDoor.

2 Només una de les dues parts del programa (un troià s'instal·la en tots dos PCs) té capacitat de controlar (client del troià) mentre que l'altra serveix de connexió amb el PC controlat (servidor del troià).

3 L'usuari del PC que actua com a servidor (el PC controlat) no té consciència o coneixement d'estar comunicat amb aquell altre PC. Ni tan sols és conscient d'haver instal·lat el troià en el seu PC.

4 El servidor del troià s'oculta intentant passar desapercebut per actuar clandestinament.

Atès que la infecció del nostre PC per part d'un troià és en realitat una instal·lació d'una aplicació, el nostre sistema explicarà a partir de llavors amb elements nous dins del nostre disc dur, i fins i tot de la memòria. La instal·lació d'un troià en un PC ve acompanyada de la creació de noves llibreries DLL, d'arxius executables, de noves entrades en el registre de Windows i de noves línies de comando en arxius tipus

win.ini, system.ini... Una altra forma una mica menys complicada de dur a terme aquestes comprovacions consistiria en la utilització d'un monitor de sistema que localitzi més fàcilment els nous arxius creats. També es podria usar el comando netstat (estat de la xarxa) del propi Windows. Per a això obriríem una finestra DUES en el nostre PC i teclejaríem "netstat –an", mostrant-se les connexions del nostre PC que s'estan duent a terme en aquest precís moment i ens fixaríem en si hi ha alguna que resulti sospitosa.

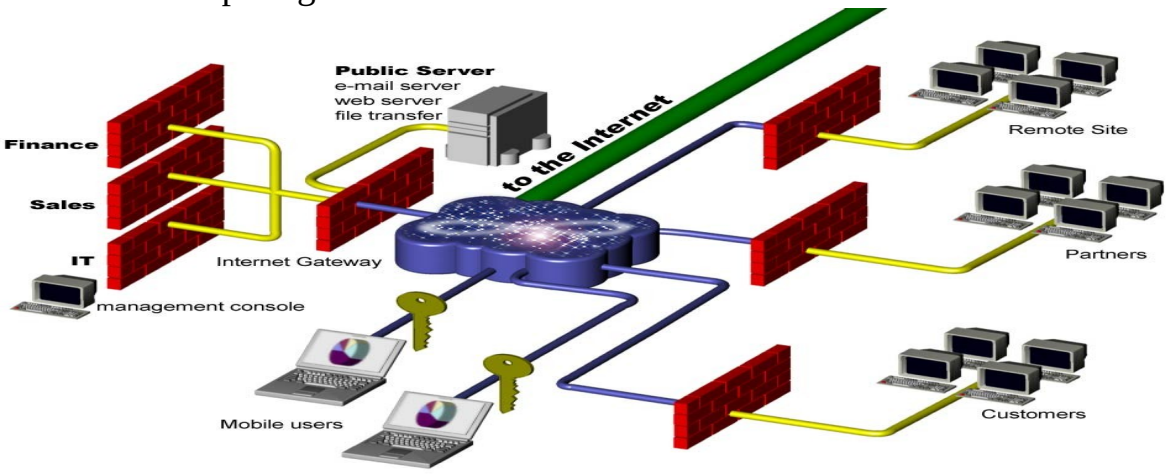
2.5.3 Atacs orientats a objectius BBDD.

Dins de les solucions tecnològiques que en l'actualitat estan disponibles per reforçar la seguretat d'una xarxa trobem els firewalls els quals són molt populars. Un firewall és un sistema encarregat del compliment de les polítiques de control d'accés a la xarxa, la qual cosa es fa a través de regles. Un firewall actua com a guàrdia perimetral d'una xarxa protegeix una xarxa d'atacs que provinguin de l'exterior d'aquesta. Però l'escenari es pot complicar de la següent forma:

1 Un atacant pot aconseguir passar el firewall, deixant la xarxa a la seva mercè.

2 Un firewall protegeix dels accessos no autoritzades cap a la xarxa interna, però no protegeix a les màquines situades a la xarxa perimetral com a servidors web, servidors de correu, servidors FTP, en altres paraules, a les bases funcionals d'Internet.

3 Un firewall no protegeix contra atacs des d'endins.



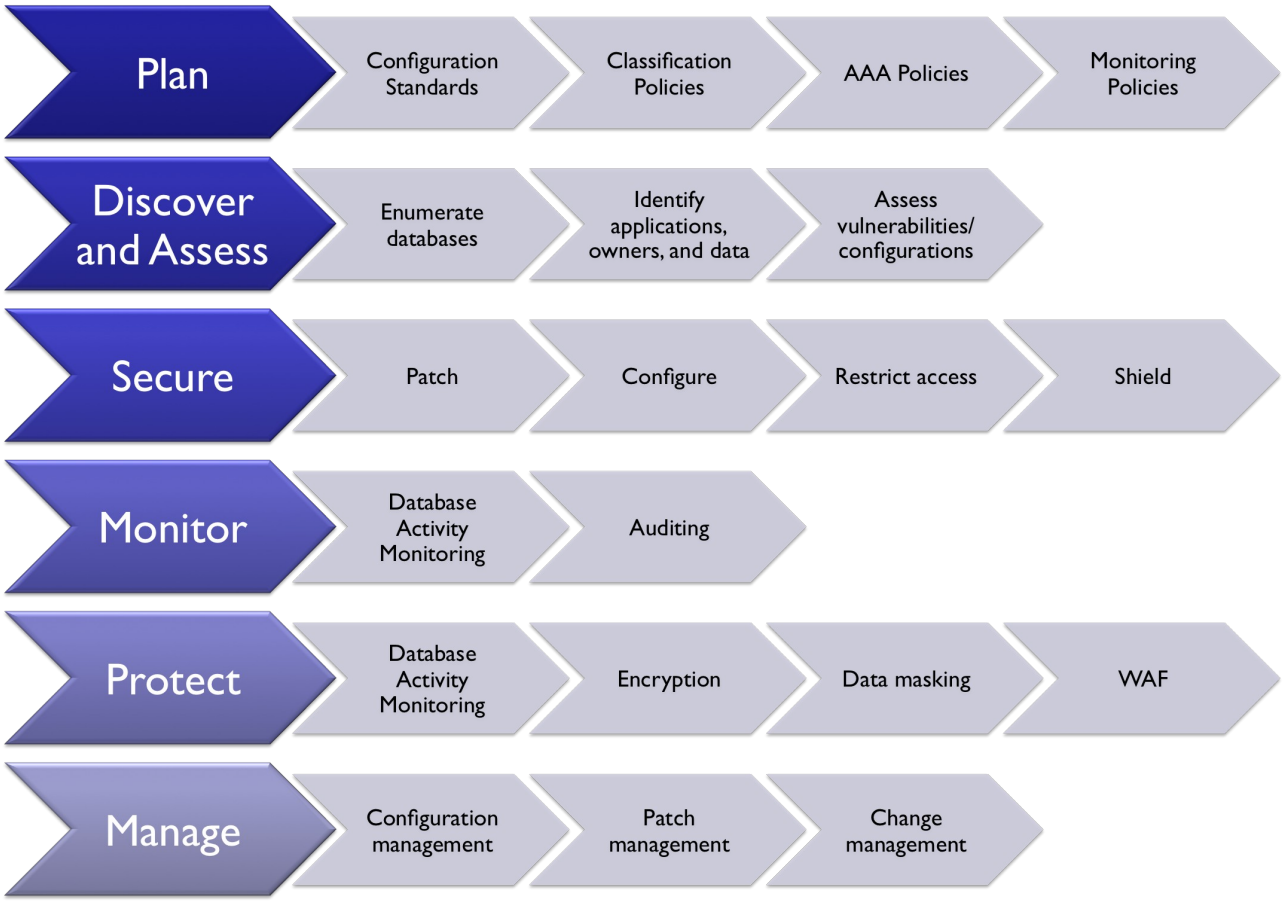
En aquests casos el que ens queda detectar l'atac o la intrusió al més aviat possible perquè causi el menor dany en el sistema. Abans de continuar anem a definir què s'entén normalment per intrusió. Normalment un intrús intenta:

4 Accedir a una determinada informació.

5 Manipular certa informació.

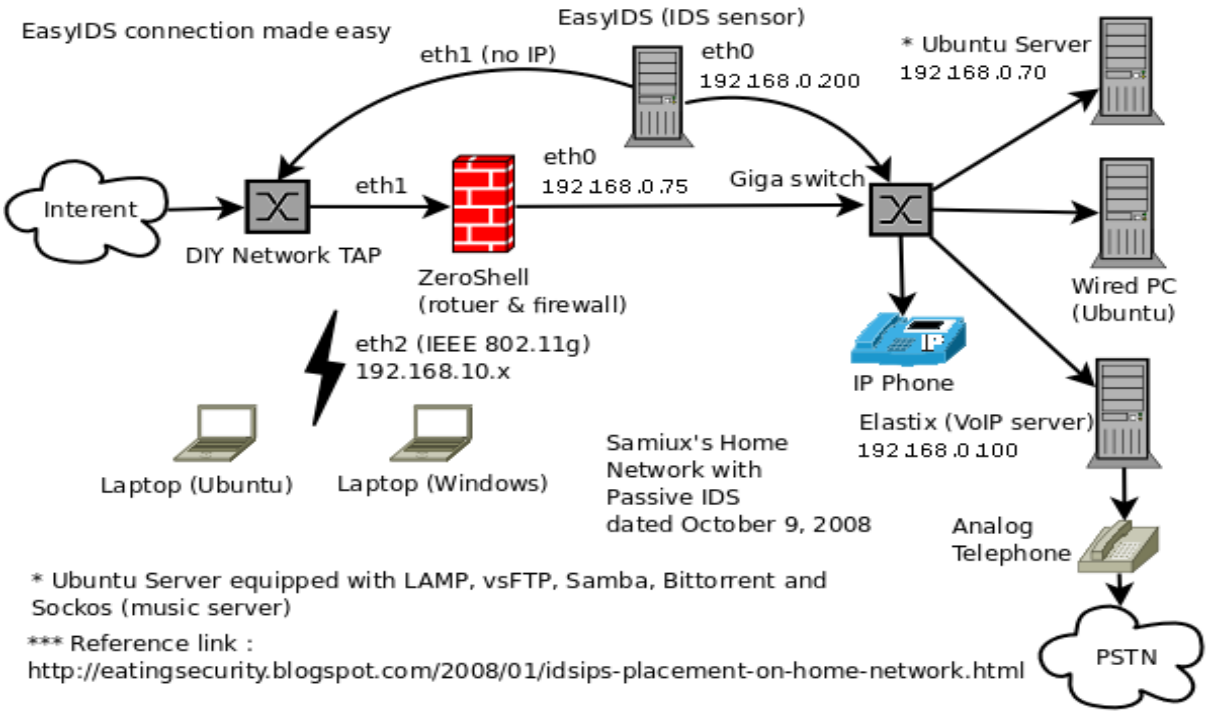
6 Fer que el sistema es no funcioni de forma segura o inutilitzar-ho.

Una intrusió és qualsevol conjunt d'accions que pot comprometre la integritat, confidencialitat o disponibilitat d'una informació o un recurs informàtic. Els intrusos poden utilitzar debilitats i bretxes en l'arquitectura dels sistemes i el coneixement intern del sistema operatiu per superar el procés normal d'autenticació.



https://securosis.com/assets/library/main/DatabaseSecurityProcessFramework.png

Mòdul III: SISTEMES IDS DE DETECCIÓ D'INTRUSOS. AUDITORIA DE SEGURETAT.



3.1 Arquitectura IDS per a Administradors.

Existeixen nombroses mesures de seguretat per protegir els recursos informàtics d'una empresa, però encara que se segueixin totes les recomanacions dels experts, no estarem lliures de possibles atacs amb èxit. Això es deu al fet que aconseguir un sistema virtualment invulnerable és summament costós, a més de que les mesures de control reduirien la productivitat de l'empresa. Cridarem intrusió a un conjunt d'accions que intenten comprometre la integritat, confidencialitat o disponibilitat d'un recurs, podem adonar-nos que una intrusió no té per què consistir en un accés no autoritzat a una màquina, també pot ser una negació de servei. Als sistemes utilitzats per detectar les intrusions o els intents d'intrusió se'ls denomina sistemes de detecció d'intrusions Intrusió Detection Systems, IDS) o, més habitualment sistemes de detecció d'intrusos, qualsevol mecanisme de seguretat amb aquest propòsit pot ser considerat un IDS, però generalment només s'aplica aquesta denominació als sistemes automàtics (programari o maquinari).

Una de les primeres coses que hauríem de plantejar-nos a l'hora de parlar de IDSs és si realment necessitem un d'ells en el nostre entorn de treball, al cap i a l'últim, hem de tenir ja un sistema de protecció perimetral basat en tallafocs, i per si el nostre firewall fallés, cada sistema hauria d'estar configurat d'una manera correcta, de manera que fins i tot sense tallafocs qualsevol màquina pogués seguir-se considerant relativament segura.

La resposta és, sens dubte, sí, hem d'esperar que en qualsevol moment algú aconsegueixi trencar la seguretat del nostre entorn informàtic, i per tant hem de ser capaços de detectar aquest problema tan aviat com sigui possible (fins i tot abans que es produeixi, quan el potencial atacant es limiti a provar sort contra les nostres màquines).

Cap sistema informàtic pot considerar-se completament segur, però fins i tot encara que ningú aconsegueixi violar les nostres polítiques de seguretat, els sistemes de detecció d'intrusos s'encarregarien de mostrar-nos tots els intents de multitud de pirates per penetrar en el nostre entorn, no deixant-nos caure en cap falsa sensació de seguretat, si som conscients que diàriament hi ha gent que tracta de trencar els nostres sistemes, no caurem en la temptació de pensar que les nostres màquines estan segures perquè ningú sap de la seva existència o perquè no són interessants per a un pirata.

Els sistemes de detecció d'intrusos no són precisament nous, el primer treball sobre aquesta matèria data de 1980, no obstant això, est és un dels camps més en auge des de fa ja uns anys dins de la seguretat informàtica. I no és estrany, la capacitat per detectar i respondre davant els intents d'atac contra els nostres sistemes és realment molt interessant. Durant aquests vint anys, centenars d'investigadors de tot el món han desenvolupat, amb major o menor èxit, sistemes de detecció de tot tipus, des de simples processadors de logs fins a complexos sistemes distribuïts, especialment vigents amb l'auge de les xarxes de computadors en els últims anys.

La detecció d'intrusos es pot detectar a partir de la caracterització anòmala del comportament i de l'ús que fan dels recursos del sistema. Aquest tipus de detecció pretén quantificar el comportament normal d'un usuari. Per a una correcta distinció cal tenir en compte les tres diferents possibilitats que existeixen en un atac, atenent a qui és el que ho duu a terme:

1 Penetració externa. Que es defineix com la intrusió que es duu a terme a partir un usuari o un sistema de computadors no autoritzat des d'una altra xarxa.

2 Penetracions internes. Són aquelles que duen a terme per usuaris interns que no estan autoritzats a l'accés.
3 Abús de recursos. Es defineix com l'abús que un usuari duu a terme sobre unes dades o recursos d'un sistema al que està autoritzat el seu accés.

La idea central d'aquest tipus de detecció és el fet que l'activitat intrusiva és un subconjunt de les activitats anòmales. Això pot semblar raonable pel fet que si algú aconsegueix entrar de forma il·legal en el sistema, no actuarà com un usuari normal. No obstant això en la majoria de les ocasions una activitat intrusiva resulta de l'agregat d'altres activitats individuals que per si soles no constitueixen un comportament intrusiu de cap tipus. Idealment el conjunt d'activitats anòmales és el mateix del conjunt d'activitats intrusives, de totes maneres això no sempre és així:

4 Intrusives però no anòmales. Se'ls denomina falsos negatius i en aquest cas l'activitat és intrusiva però com no és anòmala i no s'aconsegueix detectar-la. Es denominen falsos negatius perquè el sistema erròniament indica absència d'intrusió.

5 No intrusives però anòmales. Es denominen falsos positius i en aquest cas l'activitat és no intrusiva, però com és anòmala el sistema decideix que és intrusiva. Es denominen falsos positius, perquè el sistema erròniament indica l'existència d'intrusió.

6 Ni intrusiva ni anòmala. Són negatius veritables, l'activitat és no intrusiva i s'indica com a tal.

7 Intrusiva i anòmala. Es denominen positius veritables, l'activitat és intrusiva i és detectada.

Els primers no són desitjables, perquè donen una falsa sensació de seguretat del sistema i l'intrús en aquest cas pot operar lliurement en el sistema.

Els falsos positius es deuen minimitzar, en cas contrari el que pot passar és que s'ignorin els avisos del sistema de seguretat, fins i tot quan siguin encertats. Els detectors d'intrusions anòmales requereixen molta despesa computacional, perquè se segueixen normalment diverses mètriques per determinar quant s'allunya l'usuari del que es considera comportament normal.

3.1.1 Exploració de dades en temps real.

Aquests sistemes basen el seu funcionament en la recol·lecció i anàlisi d'informació de diferents fonts, que després utilitzen per determinar la possible existència d'un atac o penetració d'intrusos.

En cas que existeixi la suficient certesa de la detecció d'un incident, el IDS té com a funció principal alertar a l'administrador o personal de seguretat, perquè prengui accions sobre aquest tema. Altres implementacions més complexes són capaces d'anar més enllà de la notificació d'un possible atac, és a dir poden executar accions automàtiques que impedeixin el desenvolupament d'aquest.

Avui dia existeixen al mercat una bona quantitat de productes coneguts com IDS (Sistemes de Detecció d'Intrusos) o en anglès IDS (Intrusion Detection System).

3.1.2 Agents autònoms. Coordinació arquitectura IDS.

Els NIDS analitzen el tràfic de la xarxa completa, examinant els paquets individualment, comprenent totes les diferents opcions que poden coexistir dins d'un paquet de xarxa i detectant paquets armats maliciosament i dissenyats per no ser detectats pels tallafocs.

Poden buscar com és el programa en particular del servidor de Web al que s'està accedint i amb que opcions i produir alertes quan un atacant intenta explotar alguna fallada en aquest programa. Els NIDS tenen dos components:

-Un sensor: situat en un segment de la xarxa, la monitoritza a la recerca de tràfic sospitós.

-Una Consola: rep les alarmes del sensor o sensors i depenent de la configuració reacciona a les alarmes rebudes.

3.2 Models de detecció.

Existeixen diversos tipus de IDS, classificats segons el tipus de situació física, del tipus de detecció que posseeix o de la seva naturalesa i reacció quan detecta un possible atac.

Classificació per situació:

1 HIDS (HostIDS): un IDS vigilant un únic ordinador i per tant la seva interfície corre en manera no promíscua. L'avantatge és que la càrrega de processament és molt menor.
2 NIDS (NetworkIDS): un IDS basat en xarxa, detectant atacs a tot el segment de la xarxa. La seva interfície ha de funcionar en manera promíscua capturant així tot el tràfic de la xarxa.
3 DIDS (DistributedIDS): sistema basat en l'arquitectura client/servidor compost per una sèrie de NIDS (IDS de xarxes) que actuen com a sensors centralitzant la informació de possibles atacs en una unitat central que pot emmagatzemar o recuperar les dades d'una base de dades centralitzada.

L'avantatge és que en cada NIDS es pot fixar unes regles de control especialitzant-se para cada segment de xarxa i l'estructura habitual en xarxes VPN (Xarxes Privades Virtuals).

3.3 Característiques d'implantació d'un IDS.

Els principals avantatges del NIDS són:

-Detecten accessos no desitjats a la xarxa.
-No necessiten instal·lar programari addicional en els servidors en producció.
-Fàcil instal·lació i actualització per que s'executen en un sistema dedicat.

Com a principals desavantatges es troben:

-Examinen el tràfic de la xarxa en el segment en el qual es connecta, però no pot

detectar un atac en diferents segments de la xarxa. La solució més senzilla és col·locar diversos sensors.

-Poden generar tràfic a la xarxa.

-Atacs amb sessions encriptades són difícils de detectar.

En canvi, els HIDS analitzen el tràfic sobre un servidor o un PC, es preocupen del que està succeint en cada host i són capaços de detectar situacions com els intents fallits d'accés o modificacions en arxius considerats crítics. Els avantatges que aporta el HIDS són:

-Eina potent, registra comandos utilitzats, fitxers oberts,...

-Tendeix a tenir menor nombre de falsos-positius que els NIDS, entenent falsos-positius als paquets etiquetats com a possibles atacs quan no ho són.

-Menor risc en les respostes actives que els IDS de xarxa.

Els inconvenients són:

-Requereix instal·lació en la màquina local que es vol protegir, la qual cosa suposa una càrrega addicional per al sistema.

-Tendeixen a confiar en les capacitats de*auditoria i logging de la màquina en si.

Conclusions

Qualsevol atacant pot aconseguir, amb molta facilitat, i en un temps record, moltes de les eines d'atac que necessitarà. Si és un amateur, li bastarà amb aconseguir les aplicacions i començar a usarles. Si es parla d'un professional, seleccionarà entre les millors aplicacions, buscarà, fins i tot, aquelles de les quals es disposa del codi font, però, els uns i els altres, podran gaudir d'elles en un temps incomparablement menor del que necessitarien al món no cibernètic. Els mecanismes de seguretat es divideixen en tres grans grups: Prevenció, Detecció i Recuperació.

Els mecanismes de prevenció són aquells que augmenten la seguretat d'un sistema durant el funcionament normal d'aquest, prevenint l'ocurrència de violacions a la seguretat, per exemple, l'ús de xifrat en la transmissió de dades es pot considerar un mecanisme d'aquest tipus, ja que evita que un possible atacant escolti les connexions. Per mecanismes de detecció es coneix a aquells que s'utilitzen per detectar violacions de la seguretat o intents de violació, exemples d'aquests mecanismes són els programes d'auditoria com Tripwire. Finalment, els mecanismes de recuperació són aquells que s'apliquen quan una violació del sistema s'ha detectat, per retornar a aquest al seu funcionament correcte, exemples d'aquests mecanismes són la utilització de còpies de seguretat o el maquinari addicional. Dins d'aquest últim grup de mecanismes de seguretat trobem un subgrup denominat mecanismes d'anàlisis forense, que el seu objectiu no és simplement retornar al sistema a la seva manera de treball normal, sinó esbrinar l'abast de la violació, les activitats d'un intrús en el sistema, i la porta utilitzada per entrar, d'aquesta forma es prevenen atacs posteriors i es detecten atacs a altres sistemes de la nostra xarxa. Sembla clar que, encara que els tres tipus de mecanismes són importants per a la seguretat del sistema, s'ha d'emfatitzar en l'ús de mecanismes de prevenció i de detecció, la màxima popular "més val prevenir que guarir" es pot aplicar a la seguretat, per a seguretat Web, evitar un atac, detectar un intent de violació, o detectar una violació reeixida immediatament després que ocorri és molt més productiu i menys comprometedor per al sistema que restaurar l'estat després d'una penetració de la màquina. És més, si s'aconsegueix un sistema sense vulnerabilitats i que la seva política de seguretat s'implementés mitjançant mecanismes de prevenció d'una forma completa, no necessitaríem mecanismes de detecció o recuperació.

Yago Blanco Presas

Bibliografia

Bibliografia Avançada:

-Cariacedo Gallardo, Justo. Seguridad en Redes Telemáticas. McGraw Hill, 2004.

-Areitio, Javier. Seguridad de la Información. Redes, informática y sistemas de información. Paraninfo, 2008.

-HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. http://www.cert.org. Capítulo 12–Página 165

-DISA (Defense Information System Agency). http://www.disa.mil

-Inteco http://www.inteco.es/

-Agencia de Protección de Datos https://www.agpd.es/portalwebAGPD/index-ides-idphp.php

-RNormas UNE (NorWeb) http://www.upm.es/institucional/Biblioteca/NORWEB

-Schneier, Bruce. Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd ed., John Wiley & Sons, Inc., 1996

-Fúster, A.; De la Guía, D.; Hernández, L.; Montoya, F.; Muñoz, J. Técnicas Criptográficas de Protección de Datos. 2ª ed, Ra-Ma, 2000

-Caballero, Pino. Introducción a la Criptografía. Ra-Ma, Textos Universitarios, 1996.

-HOWARD, John D. Thesis. An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. http://www.cert.org. Capítulo 12–Página 168.

-Ramió Aguirre, Jorge. Seguridad Informática y Criptografía v 4.1 (texto guía de clases) Dpto. de Publicaciones E.U.I., 2006 (edición impresa). Libro electrónico gratuito disponible en la página Web del autor. Aplicaciones Criptográficas. Segunda Edición), Dpto. de Publicaciones EUI 1999.

-Menezes, Alfred; Oorsschof, Paul; Vanstone, Scott. Handbook of Applied Cryptography. CRC Press, 1977. Libro electrónico gratuito disponible en la página Web del autor

-Stallings, William. Cryptography and Network Security. Principles and Practice. Third ed.,

Prentice Hall International Editions, 2003.

-Pastor, José; Sarasa, Miguel Angel. Criptografía Digital. Colección Textos Docentes; Prensas Universitarias de Zaragoza, 1998.

-Red Temática Iberoamericana de Criptografía y Seguridad de la Información http://www.criptored.upm.es/

Bibliografia web i Fonts consultades:

http://www.openssl.org/docs/HOWTO/keys.txt

http://www.freebsd.org/doc/es/books/handbook/openssl.html

http://doc.ubuntu-es.org/HTTPD_Servidor_web_Apache2

http://www.vilecha.com/Hellguest/ssh_tuneles.asp

http://www.iespana.es/mundolinux/linux/unixsec/

http://www.porcupine.org/satan/

http://www.tenable.com/products/nessus

http://www.saintcorporation.com/

http://vulnerabilityteam.wordpress.com/tag/saint-network-vulnerability-scanner/

http://systemadmin.es/2009/09/tipos-de-tuneles-ssh

http://linux.byexamples.com/archives/238/ssh-reverse-tunneling/

http://articles.techrepublic.com.com/5100-10878_11-5779944.html

http://www.linux.ebre.cat/2009/11/apache-2-con-soporte-ssl.html

http://systemadmin.es/2009/09/tipos-de-tuneles-ssh

http://www.scribd.com/doc/39764542/Manual-Snort

http://informatica.uv.es/it3guia/AGR/apuntes/teoria/documentos/Certificados.pdf

http://www.noah.org/wiki/SSH_public_keys

http://es.wikipedia.org/wiki/Ataque_Man-in-the-middle

http://brsi.blogspot.com/2006/08/ataques-mitm.html

http://www.sans.org/reading_room/whitepapers/threats/address-resolution-protocol-spoofing-man-in-the-middle-attacks_474

http://es.wikipedia.org/wiki/Ataque_Man-in-the-middle

http://www.linuxfocus.org/Castellano/March2003/article282.shtml

http://www.microsoft.com/technet/itsolutions/network/nap/default.mspx

http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

http://www.oxid.it/downloads/apr-intro.swf

http://www.grc.com/nat/arp.htm

http://wiki.ethereal.com/CaptureSetup/Ethernet

http://www.sans.org/rr/whitepapers/threats/rss/474.php

Vídeos i contingut multimèdia:

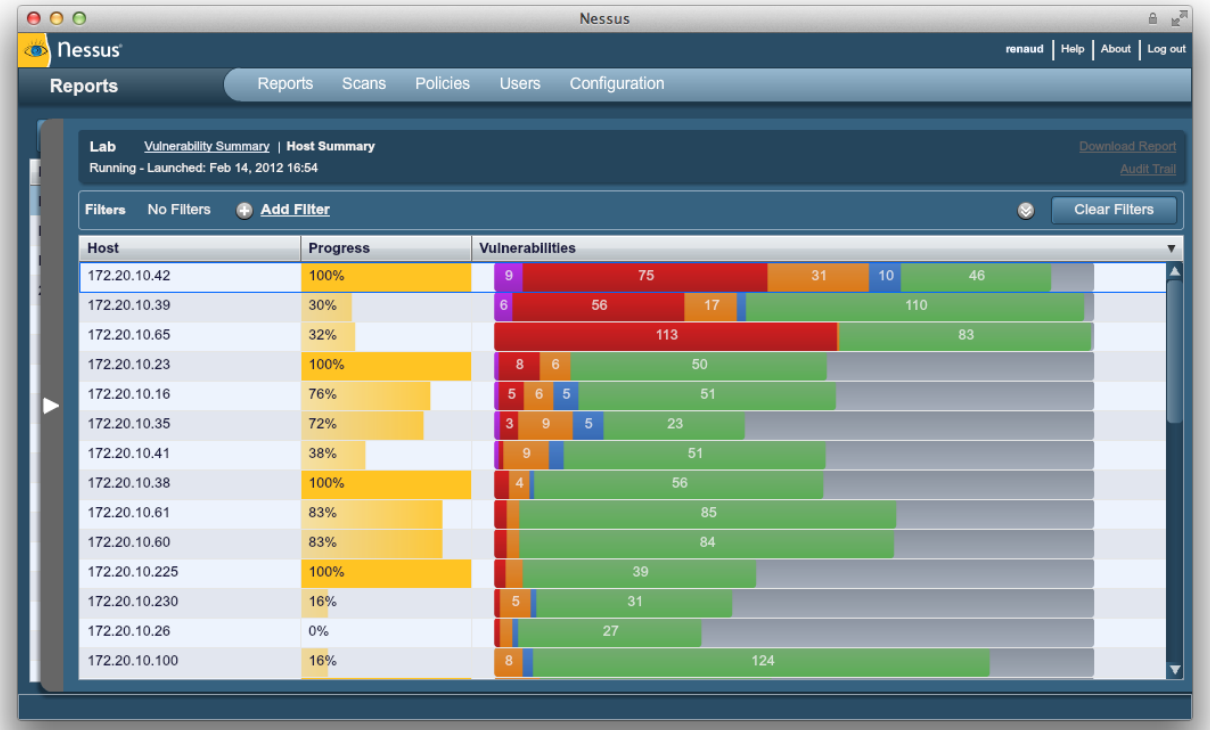
-Seguretat en LAN - Enverinament de ARP:
http://www.youtube.com/watch?v=gVGVKUGyaN8

-SATAN(Security Administrator Tool for Analyzing Networks):
http://www.youtube.com/watch?v=YGVUj8B6nbA

-Introduction To Using The Nessus Vulnerability Scanner:
http://www.youtube.com/watch?v=-7ThbeAMqkw

-Network Security Fundamentals:
http://www.youtube.com/watch?v=kcks1FLBVOI

ANNEX I: NESSUS, SATAN,SAINT i altres opcions.



[Nessus]

Nessus és un programa d'escaneig de vulnerabilitats en diversos sistemes operatius. El projecte Nessus va començar en 1998, quan Renaud Deraison va voler que la comunitat d'Internet tingués un escàner remot de seguretat que fos lliure. Nessus és una potent eina d'arquitectura Client – Servidor de seguretat informàtica o de xarxa, utilitzat principalment per analitzar les vulnerabilitats que es troben en equips objectius, servidors, dominis o en qualsevol dispositiu que compti amb una adreça IP i serveis informàtics instal·lats. Consisteix en un daemon (nessusd) que realitza l'escaneig en el sistema objectiu, i el client (nessus: basat en consola o gràfic) que mostra l'avanç i informa sobre l'estat dels escaneigs. Des de consola nessus pot ser programat per fer escaneigs programats amb cron.

En operació normal, nessus comença escanejant els ports amb nmap o amb el seu propi escanejador de ports per buscar ports oberts i després intentar diversos exploits per atacar-ho. Les proves de vulnerabilitat, disponibles com una llarga llista de plugins, són escrits en NASL (Nessus Attack Scripting Language, Llenguatge de Scripting d'Atac Nessus per les seves sigles en anglès), un llenguatge scripting optimitzat per a interaccions personalitzades en xarxes.

Algunes de les proves de vulnerabilitats de Nessus poden causar que els serveis o sistemes operatius es corrompin i caiguin. L'usuari pot evitar això desactivant "unsafe test" (proves no segures) abans d'escanejar.

Opcionalment, els resultats de l'escaneig poden ser exportats com a informes en diversos formats, com a text pla, XML, HTML, i LaTeX. Els resultats també poden ser guardats en una base de coneixement per a referència en futurs escaneigs de vulnerabilitats.

Com instal·lar Nessus en Linux: la forma en què funciona és analitzant els ports que es troben oberts i executant exploits (atacs) per descobrir la vulnerabilitat, i en molts o la majoria dels casos mostra una descripció detallada del forat de seguretat i com pot ser solucionat. Nessus funciona sobre la base d'una sèrie de plugins que són descarregats al moment de la instal·lació i pot prendre molt temps depenent de les velocitats d'internet amb què s'expliqui. La instal·lació d'aquesta eina és realment senzilla:

[1] El primer és descarregar el nessus des de la pàgina oficial i s'han d'acceptar els acords de llicència (Agree).

[2] Després sortirà una pantalla per seleccionar el sistema operatiu que tenim. En aquest cas s'escull Ubuntu 10 (32 bits). Han d'escollir molt bé la seva versió i guardar l'arxiu d'instal·lació en una ubicació que recordin fàcilment.

[3] Quan acabi la descàrrega n'hi ha prou amb executar el següent comando en una consola:

sudo dpkg -i /home/yagonet/Escritorio/Nessus-4.4.1-ubuntu1010_i386.deb

[4] Una vegada acabat el procés ja es té instal·lat el Nessus en Ubuntu. El següent és activar el Nessus, mitjançant el registre d'un compte a la pàgina oficial. Això no pren més d'un minut. El que cal fer és acceptar els termes de llicència, omplir els camps de Nom, Cognoms i Correu, i ja haurem finalitzat el procès.

[5] En revisar el nostre correu electrònic, arribarà el codi d'activació, seguit de diverses instruccions per activar-ho d'acord a la Distribució que tinguem en aquell moment. En aquest cas som usuaris Linux, així que mitjançant la següent comanda es registrarà el producte satisfactòriament:

sudo /opt/nessus/bin/nessus-fetch –register DF3A-9287-95C2-A4E0-643B *<-- EL REGISTRE CANVIA EN CADA ACTUALITZACIÓ*

[6] cada codi és únic i enregistrable una única vegada. En fer això, apareixerà un missatge que diu que l'activació ha sigut satisfactòria i que s'estan descarregant els últims plugins. (Aquest procés pot prendre diversos minuts, així que no és de preocupar-se si dura molt temps)

[7] El següent pas és crear l'usuari administrador amb el qual usarem el Nessus d'ara endavant. La forma de fer-ho és amb el següent codi:

sudo /opt/nessus/sbin/nessus-adduser

[8] I a continuació seguir els passos, escrivint el nom d'usuari, contrasenya, etc. Hauria de sortir alguna cosa com el següent:

sudoyagonet@cst:~$ sudo /opt/nessus/sbin/nessus-adduser
[sudo] password for yagonet:
Login : prueba
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc…) (y/n) [n]: y

User rules
———-
nessusd has a rules system which allows you to restrict the hosts
that prueba has the right to test. For instance, you may want
him to be able to scan his own host only.
Please see the nessus-adduser manual for the rules syntax
Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)
Login : prueba
Password : ******* ***
This user will have 'admin' privileges within the Nessus server
Rules :
Is that ok ? (y/n) [y] y
User added

[9] L'usuari Prova serà l'usuari administrador amb el que ingressarem a l'aplicació. Una vegada finalitzat tot el procés reiniciem el servei nessusd mitjançant la comanda.

sudo /etc/init.d/nessusd restart

[10] En reiniciar el servei satisfactòriament, obrim qualsevol navegador i entrem a la següent adreça https://localhost:8834/ (En la majoria dels casos es reconeix la connexió com "No Segura" pel que s'ha d'agregar l'excepció per permetre la navegació).

[11] S'ha de donar clic primer en Comprenc els riscos a "Agregar excepció". En donar clic a Confirmar excepció de seguretat, ja no es tindran problemes per tornar a entrar i poder usar el servei. Una vegada tornem a accedir sortirà la finestra que demana les dades de l'usuari, al que cridem prova que vam crear en una secció anterior juntament amb la seva contrasenya. S'ingressen per accedir al client del Nessus: (Molt Important! S'ha de tenir actualitzada la versió del Flaix Player, ja que és necessari perquè el Nessus funcioni correctament).

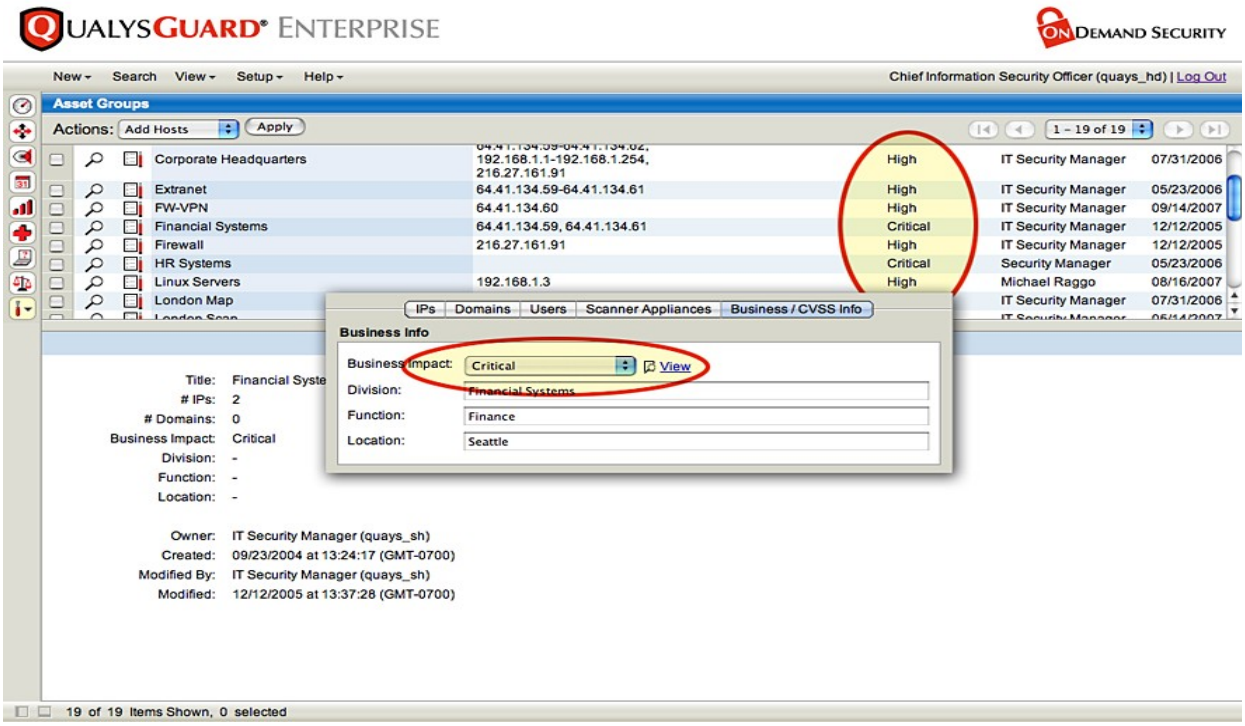
[12] En ingressar es poden veure diverses pestanyes en la part superior: Reports – Scans – Policies – Users. En Reports sortiran els reports de les anàlisis que estiguin en curs en el moment o els que ja han finalitzat. Entrant allí es veurà la llista d'anàlisi

i es podrà ingressar a qualsevol així no estiguin complets per anar revisant els resultats. En Scans, es podran agregar els escaneigs que es desitgi i controlar també el progrés de cadascun. Policies és molt important ja que permet definir mitjançant una sèrie de paràmetres la configuració de la política que usarem per determinada anàlisi. En Users simplement es llistaran els usuaris que hàgim creat per a l'administració del Nessus.

Exemple: aquest serà un senzillíssim exemple de com usar el Nessus, almenys perquè els que no són experts es vagin familiaritzant amb l'entorn i puguin fer diverses proves. En aquest cas tinc una màquina virtual amb la meva Linux Ubuntu 11.04, la qual té una adreça IP 10.0.2.15 (per esbrinar la ip faig servir la comanda ifconfig en un terminal), i vaig a analitzar el meu propi equip a la recerca de possibles vulnerabilitats.

Primer em dirigeixo a la pestanya de Policies per crear una nova política d'escaneig. Solament vaig a donar-li el nom i deixaré les configuracions que estan per defecte. Després en Scans vaig a agregar un de nou. Després d'uns 5 minuts analitzant l'equip es troben diverses vulnerabilitats de baix, mitjà i alt risc.

[SAINT]



SAINT Network Vulnerability Scanner (SAINTscanner® Vulnerability Assessment): aquest escàner de vulnerabilitat de xarxa es troba integrat amb un sistema per realitzar proves de penetració(pentest) permetent així a l'usuari explotar les vulnerabilitats oposades. SAINT descobreix les àrees de debilitat i recomana solucions per resoldre aquestes vulnerabilitats:

-Amb SAINT es poden identificar les vulnerabilitats en els dispositius de xarxa, sistemes operatius, aplicacions d'escriptori, aplicacions web, BBDD, etc.

- Detectar i corregir possibles deficiències en la seguretat de la seva xarxa abans que puguin ser aprofitades per intrusos.

- Mostra si la xarxa és compatible amb els estàndards de seguretat PCI; SAINT està certificat per la Indústria de Targetes de Pagament (PCI) del Consell de Normes de Seguretat com Approved Scanning Vendor.

- Suport per CVE, OSVDB, BID, IAVA, OVAL, SANS / FBI, la puntuació CVSS, ID de proveïdor.

- SAINT dóna suport al Programa d'Adopció OVAL com un escàner de vulnerabilitat, i proporciona les capacitats tant com a avaluador de la definició i característiques del Sistema Productor.

- Permet dissenyar i generar informes d'avaluació de la vulnerabilitat de forma ràpida i senzilla.

- SAINT és una solució que no requereix programari agent.

- Mostra si la seguretat de la xarxa està millorant amb el temps mitjançant l'informe d'anàlisi.

- Dóna l'opció de guardar les dades de vulnerabilitat a nivell local o de forma remota (les dades de vulnerabilitat no han de ser enviats a través d'Internet).

- Proporciona actualitzacions automàtiques de noves comprovacions de vulnerabilitats i exploits diàriament.

- Permet administrar i programar exploracions a través de les grans empreses amb la consola d'administració remota SAINTmanager.

- Permet agregar els seus propis controls personalitzats i signatures de vulnerabilitat.

- Realitza anàlisi de contingut de les dades (per exemple, targetes de crèdit o nombres de seguretat social) que no han de ser emmagatzemats en equips de sobretaula / servidors.

- Potents informes personalitzables. Permet construir informes personalitzats o utilitzar plantilles pre-configurades per a una gran varietat d'informes de nivell executiu.

- Permet administrar els recursos de manera més eficient. Conèixer el grau de la seva vulnerabilitat de la xarxa permet enfocar l'atenció i els recursos on més es necessiten.

- A causa que l'escàner s'integra amb el programari d'exploit, es pot començar la seva rehabilitació amb les vulnerabilitats crítiques.

- Anticipar i prevenir vulnerabilitats dels sistemes habituals.

- Revisar regulacions de la indústria, tals com PCI DSS, NERC, FISMA, SOX, GLBA i HIPAA.

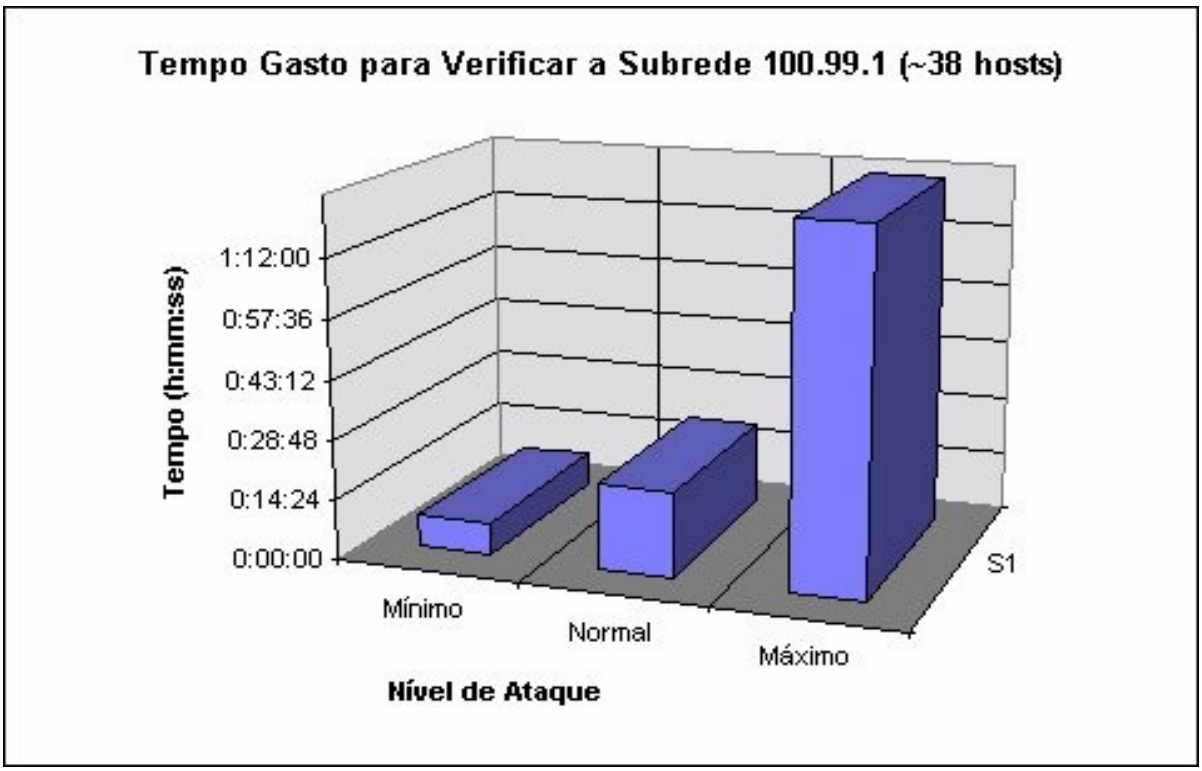
- Realitzar auditories de conformitat amb les polítiques definides pel CCFD, USGCB i DISA.

- Permet explotar vulnerabilitats oposades per l'escàner amb l'eina de proves de penetració integrada, SAINTexploit.

- Permet avaluar tant les avaluacions externes i internes.

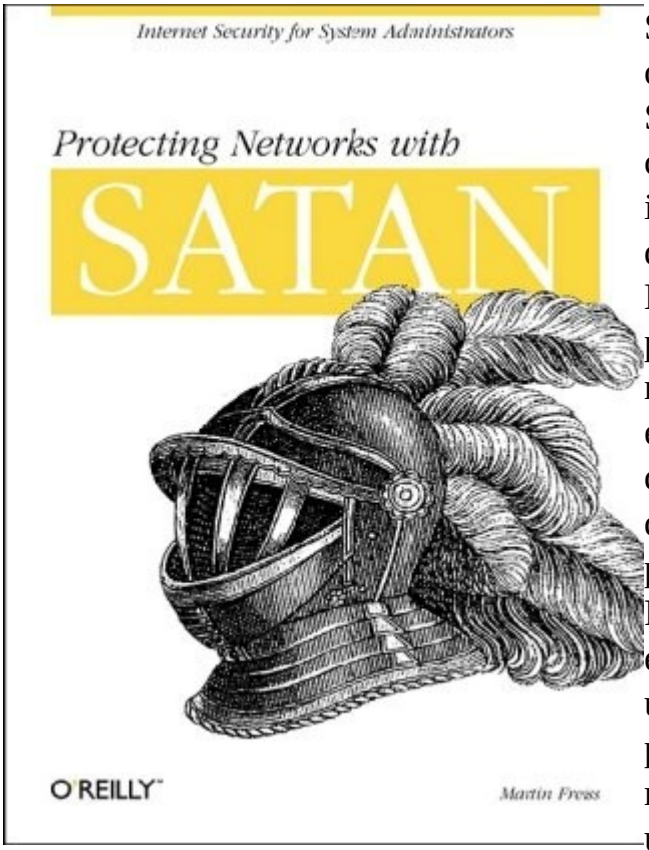
- Realitza autenticat i no autenticat d'anàlisi de vulnerabilitat de sistemes operatius, bases de dades i aplicacions Web.

- Permet explorar i explotar els objectius amb una adreça IPv4, IPv6, i l'adreça URL.



[SATAN]

SATAN (Eina d'Administrador de Seguretat per Analitzar Xarxes) és una eina de seguretat dissenyada per Donen Farmer i Wieste Venema que ajuden als administradors de sistemes, reconeixen diversos elements relacionats amb la xarxa, problemes de seguretat, en un món en el qual els sistemes informàtics són cada vegada més dependents de les xarxes. SATAN (the Security Administrator Tool for Analyzing Networks) és una eina de testeig que recol·lecta una varietat d'informació sobre hosts de xarxa i va ser considerada una de les millors en el seu moment. De fet, va ser el primer escàner amigable amb l'usuari: posseeix una interfície HTML completa amb formularis per ingressar objectius, taules per mostrar resultats i tutorials que apareixen quan s'ha trobat un forat de seguretat.



SATAN és una eina basada en UNIX, originalment dissenyat només per SunOS / Solaris i Irix, no obstant això és compatible amb altres versions d'UNIX, incloent una per Linix, permetent que qualsevol persona amb un PC i un compte Eslip / PPP pugui accedir a la informació proporcionada per SATAN, que normalment requereix root accés per a executar-se. És important tenir en compte que SATAN és una eina basada en UNIX que es pot configurar per escanejar pràcticament qualsevol tipus de la xarxa. Per exemple, un usuari de Macintosh que executa un paquet telnet que podria tenir un servidor ftp habilitat, la qual cosa permet a un usuari remot escriure o modificar arxius en la màquina local, o un usuari de PC amb un servidor de X Window sense control d'accés permès o un VMS estació de treball utilitzant NFS per exportar discos, sense cap restricció SATAN recapta la major informació possible sobre els serveis del sistema i de la xarxa, com els dits, NFS, NIS, ftp, rexd, etc Juntament amb això, SATAN també recull informació sobre errors de programari coneguts, malament o una mala configuració de xarxa utilitzada, serveis o configuracions de xarxa. Per a qualsevol vulnerabilitat que SATAN troba que proporciona informació limitada sobre com corregir el problema. SATAN pot provar individus, màquines o xarxes senceres de màquines.

SATAN va ser dissenyat per ajudar als administradors de sistemes a automatitzar el procés de testeig dels seus sistemes enfront de vulnerabilitats conegudes que poden ser explotades per la xarxa. SATAN es troba escrit majoritàriament en Perl i utilitza un navegador Web com Netscape, Mosaic o Lynx per proveir la interfície d'usuari. A més de presentar vulnerabilitats SATAN també recol·lecta grans quantitats d'informació general sobre la xarxa: que hosts estan connectats a subxarxes, que tipus de maquines són i que serveis proveeixen. SATAN va ser desenvolupat en 1993 per Donen Farmer i Wietse Venema, però ha estat discontinuada. Per a aquells ofesos pel nom, el paquet conté un programa anomenat repent, que canvia el nom SATAN a SANTA.

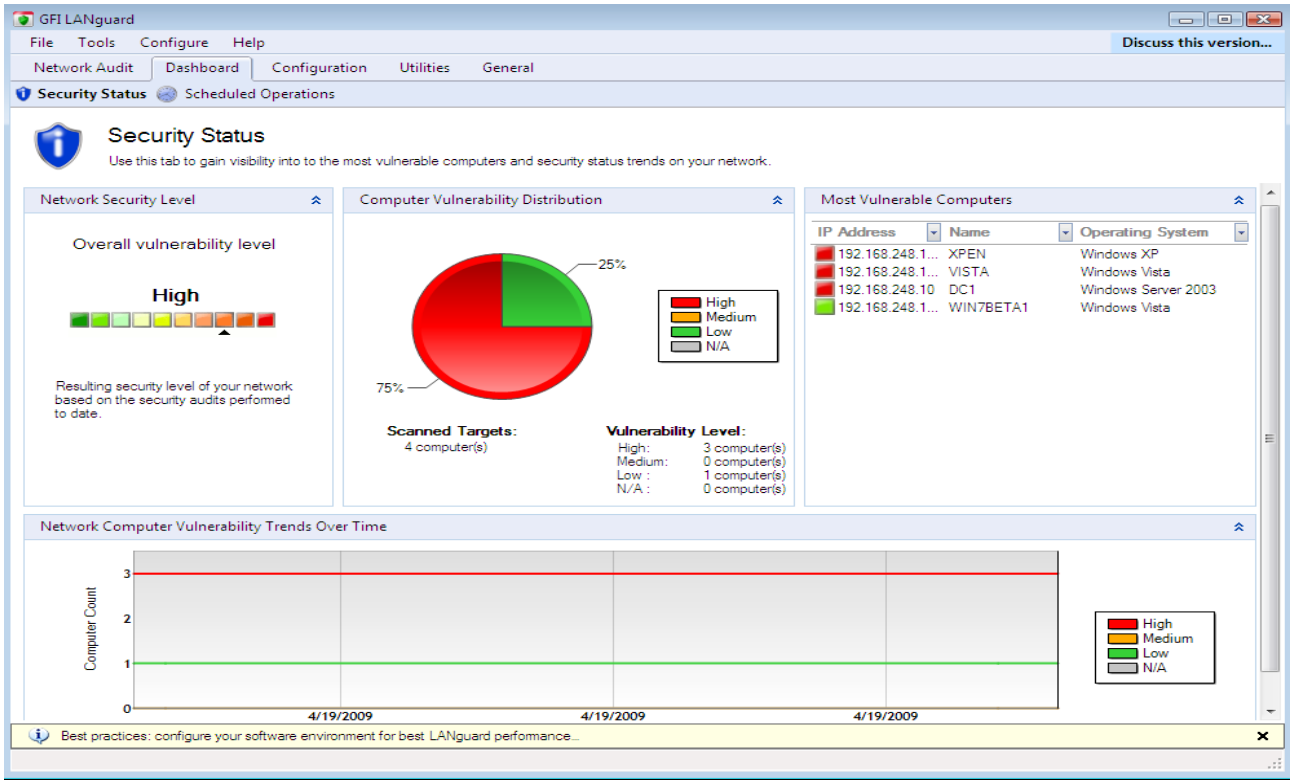
Per exemple, SATAN troba sovint els llocs que no han instal·lat una versió actualitzada del sendmail i per tant estan en risc fins i tot als hackers inexperts. La seva veritable força prové de la seva manera d'exploració. Basant-se en la informació recollida inicial per l'usuari i un conjunt de regles, SATAN examinarà les avingudes de la confiança i la dependència per cada host a la xarxa, explorant encara més qualsevol amfitrió secundari que troba, donant a l'administrador de la xarxa una bona imatge no només dels hosts / xarxes locals, sinó també la de qualsevol xarxa de prestació de serveis a la xarxa local. Això proporciona l'administrador d'una imatge molt completa de la seguretat de la xarxa. Tota la informació recollida per SATAN se li presenta a l'usuari a través d'una World Wide Web (com Netscape, Mosaic, etc) en un format fàcil de llegir i seguir. Fer SATAN extremadament fàcil d'usar. Llançat sense cost el 5 d'abril de 1995, SATAN va ser una calamarsada immediata de controvèrsia. A causa de la generalitzada disponibilitat de SATAN, la seva facilitat d'ús i el fet que pot escanejar xarxes estrangeres per a configuracions pobres i determinar què amfitrions tenen la confiança que els sistemes de les xarxes, molts temien que SATAN es convertís en l'eina d'elecció per als pirates informàtics.

[ALTRES OPCIONS]

-Nmap: és un escàner de port utilitzat per a l'exploració de la xarxa o la revisió de seguretat (open source)

-Acunetix Web Vulnerability Scanner: Aquest programari inclou un escàner de seguretat Web, una consola per a l'anàlisi d'informes i una base de dades per gestionar totes les plataformes principals del servidor web.

-GFI LANguard Network Security scanner: Aquesta solució inclou l'exploració de vulnerabilitats de xarxa i tambien serveix per realitzar auditories informàtiques de seguretat.



-Teneble Nessus 3: Compatible amb diversos tipus d'Unix, aquest producte executa més de 900 comprovacions de seguretat i suggereix solucions per als problemes oposats (open source)

-Retina Network Security Scanner: El seu distribuïdor és la signatura Eye Digital Security Inc. Afirmen que el seu escàner de vulnerabilitat descobreix tant les vulnerabilitats conegudes com les vulnerabilitats denominades "zero days". El producte també proporciona l'opció de realitzar anàlisis de riscos basats en la seguretat ajudant a l'empresa a executar i posar les millors practiques, ajuda a reforçar les polítiques i a manejar les auditories.

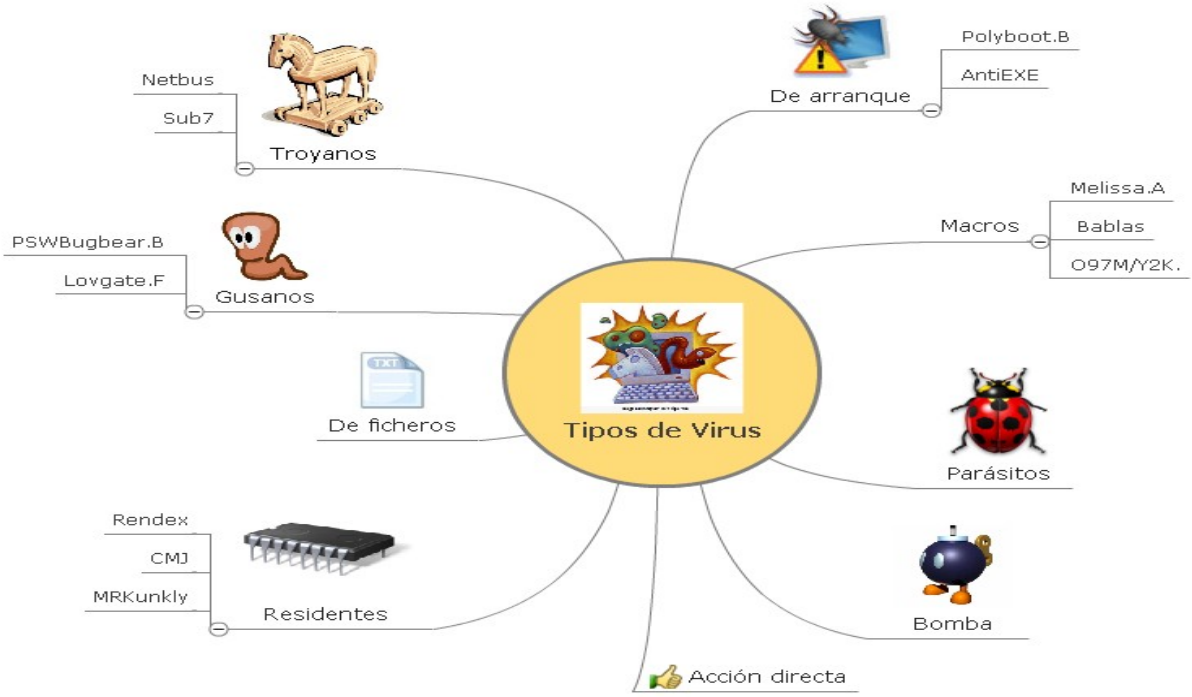
-WATCHFIRE RATIONAL APPSCAN: escàner d'IBM utilitzat per a aplicacions web.

-ISS Internet Scanner: escàner de vulnerabilitats de xarxa de la companyia IBM.

ANNEX II: Virus i antivirus.

Un virus és un petit programa capaç instal·lar-se en la computadora d'un usuari sense el seu coneixement o permís. Es diu que és un programa paràsit perquè ataca als arxius i es replica per continuar el seu esplai.

Alguns es limiten solament a replicar-se, mentre que uns altres poden produir seriosos danys als sistemes. Mai es pot assumir que un virus és inofensiu i deixar-ho surant en el sistema. Ells tenen diferents finalitats. Alguns només infecten, uns altres alteren dades, uns altres les eliminen, alguns només mostren missatges. Però la fi última de tots ells és el mateix: propagar-se.



Existeixen diferents tipus de virus:

Cucs. Són programes que es reprodueixen i no requereixen d'un amfitrió, perquè s' arrosseguen per tot el sistema sense necessitat d'un programa que els transporti. Els cucs es carreguen en la memòria i se situen en una determinada adreça, després es copien a un altre lloc i s'esborren del que ocupaven i així successivament. Esborren els programes o la informació que troben al seu pas per la memòria, causen

problemes d'operació o pèrdua de dades.

Virus de macros/codi font. S'adjunten als programes font dels usuaris i a les macros utilitzades per: processadors de paraules (Word, Works, WordPerfect), fulls de càlcul (Excell, Quattro, Lotus), etcètera.

Virus mutants. Són els que, en infectar, realitzen modificacions al seu codi, per evitar la seva detecció o eliminació (NATES o SATÁN, Miguel Angel, per esmentar alguns).

Bombes de temps. Són els programes ocults en la memòria del sistema, en els discos o en els arxius de programes executables amb tipus COM o EXE, que esperen una data o una hora determinada per explotar. Alguns d'aquests virus no són destructius i solament exhibeixen missatges en les pantalles al moment de l'explosió. Arribat el moment, s'activen quan s'executa el programa que els conté.

Cavalls de Troia. Són aquells que s'introdueixen al sistema sota una aparença totalment diferent a la del seu objectiu final; això és, que es presenten com a informació perduda o escombraries, sense cap sentit. Però al cap d'algun temps, i d'acord amb una indicació programada, desperten i comencen a executar-se i a mostrar les seves veritables intencions.

Autorreplicables. Són els virus que realitzen les funcions mes semblants als virus biològics, es autorreprodueixen i infecten els programes executables que es troben en el disc. S'activen en una data o hora programada o cada determinat temps, a partir de la seva última execució, o simplement en sentir que se'ls tracta de detectar. Un exemple d'aquests és el virus anomenat Divendres 13, que s'executa en aquesta data i s'esborra (juntament amb els programes infectats), per evitar que ho detectin.

Infectants de l'àrea de càrrega inicial. Infecten els disquets o el disc dur, s'allotgen immediatament a l'àrea de càrrega. Prenen el control quan s'encén la computadora i ho conserven tot el temps.

Infectants del sistema. S'introdueixen als programes del sistema, per exemple COMMAND.COM i uns altres que s'allotgen com a residents en memòria. Els comandos del sistema operatiu, com COPY, DIR o DEL, són programes que s'introdueixen en la memòria en carregar el sistema operatiu i és així com el virus

adquireix el control per infectar tot disc que s'introdueixi a la unitat amb la finalitat de copiar-ho o simplement per revisar les seves carpetes

Infectants de programes executables. Aquests són els virus més perillosos, perquè es disseminen fàcilment cap a qualsevol programa com a fulls de càlcul, jocs, processadors de paraules.

En funció de com es comporten, també podem fer la següent classificació de virus:

Programa: Infecten arxius executables com .com / .exe / .ovl / .drv / .sys / .bin

Boot: Infecten els sectors Boot Record, Master Boot, FAT i la taula de partició.

Múltiples: Infecten programes i sectors de boot.

Bios: Ataquen al Bios para des d'allí reescriure els discos durs.

Hoax: Es distribueixen per correu i l'única forma d'eliminar-los és l'ús del sentit comú. Sobre aquest tema, es tracta de virus que no existeixen i que s'utilitzen per aterrir als novençans especialment en Internet a pesar que els rumors ho mostren com alguna cosa molt seriós i, de vegades, la premsa especialitzada pren la informació. En general, com es va expressar, la difusió es fa per cadenes de correu amb terribles advertiments. En realitat l'únic virus és el missatge. A continuació es relacionen una sèrie de suposats virus, per la qual cosa és aconsellable ignorar els missatges que apareixen i no ajudar a replicar-los per continuar amb la cadena, perquè es van crear precisament per produir congestionamiento en Internet.

Els virus stealth (invisibles) enganyen als programari antivirus. Essencialment, un virus d'aquest tipus conserva informació sobre els arxius que ha infectat i després espera en memòria i intercepta qualsevol programa antivirus que busqui arxius modificats i li ofereix la informació antiga en lloc de la nova.

Els virus polimòrfics s'alteren només quan es dupliquen, de manera que el programari antivirus que busca comportaments específics no trobarà totes les aparicions dels virus; els que sobreviuen poden seguir duplicant-se.

La funció d'un programa antivirus és detectar, d'alguna manera, la presència d'un virus informàtic en una computadora. Aquest és l'aspecte més important d'un antivirus, independentment de les prestacions addicionals que pugui oferir, perquè el fet de detectar la possible presència d'un virus informàtic, detenir el treball i prendre les mesures necessàries, és suficient per eliminar un bon percentatge dels danys possibles. Addicionalment, un antivirus pot donar l'opció d'erradicar un virus informàtic d'una entitat infectada

Existeixen diferents tècniques per a la detecció dels virus informàtics.

Scanning o rastreig: Va ser la primera tècnica que es va popularitzar per a la detecció de virus informàtics, i que encara s'utilitza però cada vegada amb menys eficiència. Consisteix a revisar el codi de tots els arxius situats en la unitat d'emmagatzematge, fonamentalment els arxius executables, a la recerca de petites porcions de codi que puguin pertànyer a un virus informàtic.

La primera debilitat d'aquest sistema radica que en detectar-se un nou virus, aquest ha d'aïllar-se per l'usuari i enviar-se al fabricador d'antivirus, la solució sempre serà a posteriori: és necessari que un virus informàtic es dispersi considerablement perquè s'enviï als fabricants d'antivirus. Ells ho analitzaran, extrauran el tros de codi que ho identifica i ho inclouran en la propera versió del seu programa antivirus. Aquest procés pot demorar mesos a partir del moment en què el virus comença a tenir una gran dispersió, periode de temps en el qual pot causar greus danys sense que pugui identificar-se.

Un altre problema és que els sistemes antivirus han d'actualitzar-se periòdicament a causa de l'aparició de nous virus. No obstant això, aquesta tècnica permet identificar ràpidament la presència dels virus més coneguts i, en ser aquests els de major dispersió, possibilita un alt índex de solucions.

Comprovació de summa o CRC (Ciclyc Redundant Check): és un altre mètode de detecció de virus. Mitjançant una operació matemàtica que abasta a cada byte de l'arxiu, generen un nombre (de 16 o 32 bytes) per a cada arxiu. Una vegada obtingut aquest nombre, les possibilitats que una modificació de l'arxiu aconsegueixi el mateix nombre són molt poques. Per això, és un mètode tradicionalment molt utilitzat pels sistemes antivirus. En aquesta tècnica, es guarda, per a cada directori, un arxiu amb els CRC de cada arxiu i es comprova periòdicament o en executar cada

programa. Els programes de comprovació de suma, no obstant això, només poden detectar una infecció després que es produeixi. A més, els virus més moderns, per ocultar-se, busquen els fitxers que generen els programes antivirus amb aquests càlculs de grandària. Una vegada oposats, els esborren o modifiquen la seva informació.

Programes de vigilància: Ells detecten activitats que podrien realitzar-se típicament per un virus, com la sobreescritura de fitxers o el formateig del disc dur del sistema. En aquesta tècnica, s'estableixen capes per les quals ha de passar qualsevol ordre d'execució d'un programa. Dins de la closca d'integritat, s'efectua automàticament una comprovació de summa i, si es detecten programes infectats, no es permet que s'executin.

Cerca heurística: És una altra tècnica antivirus que evita la cerca de cadenes. Amb ella, es desencadella el programa i s'executa pas a pas, de vegades mitjançant la pròpia CPU. D'aquesta manera, el programa antivirus esbrina què fa exactament el programa en estudi i realitza les accions oportunes. En general, és una bona tècnica si s'implementa bé, encara que el defecte més important és la generació de falses alarmes, que no es té la certesa que un programa sigui un virus en funció del seu comportament. La majoria dels virus nous eviten directament la cerca heurística modificant els algorismes, fins que el programa antivirus no és capaç d'identificar-los.

Malgrat utilitzar aquestes quatre tècniques, cap programa pot assegurar la detecció del cent per cent dels virus.

La qualitat d'un programa antivirus no només es demostra pel nombre de virus que és capaç de detectar, sinó també pel nombre de falses alarmes que produeix, és a dir, quan el programa antivirus estima que ha localitzat un virus i en realitat es tracta d'un fitxer sa (fals positiu). Pot ocórrer que un fitxer presenti una combinació de bytes idèntica a la d'un virus, i el programa antivirus indicaria que ha detectat un virus i tractaria d'esborrar-ho o de modificar-ho.

L'expressió "quin és el millor antivirus", pot variar d'un usuari a un altre. És evident que per a un usuari inexpert el terme defineix gairebé amb seguretat al programari que és més fàcil d'instal·lar i utilitzar, alguna cosa totalment intranscendente per a usuaris experts, administradors de xarxes, etc.

No es pot afirmar que existeixi un sol sistema antivirus que presenti totes les característiques necessàries per a la protecció total de les computadores; alguns fallen en uns aspectes, uns altres tenen determinats problemes o manquen de certes facilitats. Les característiques essencials són les següents:

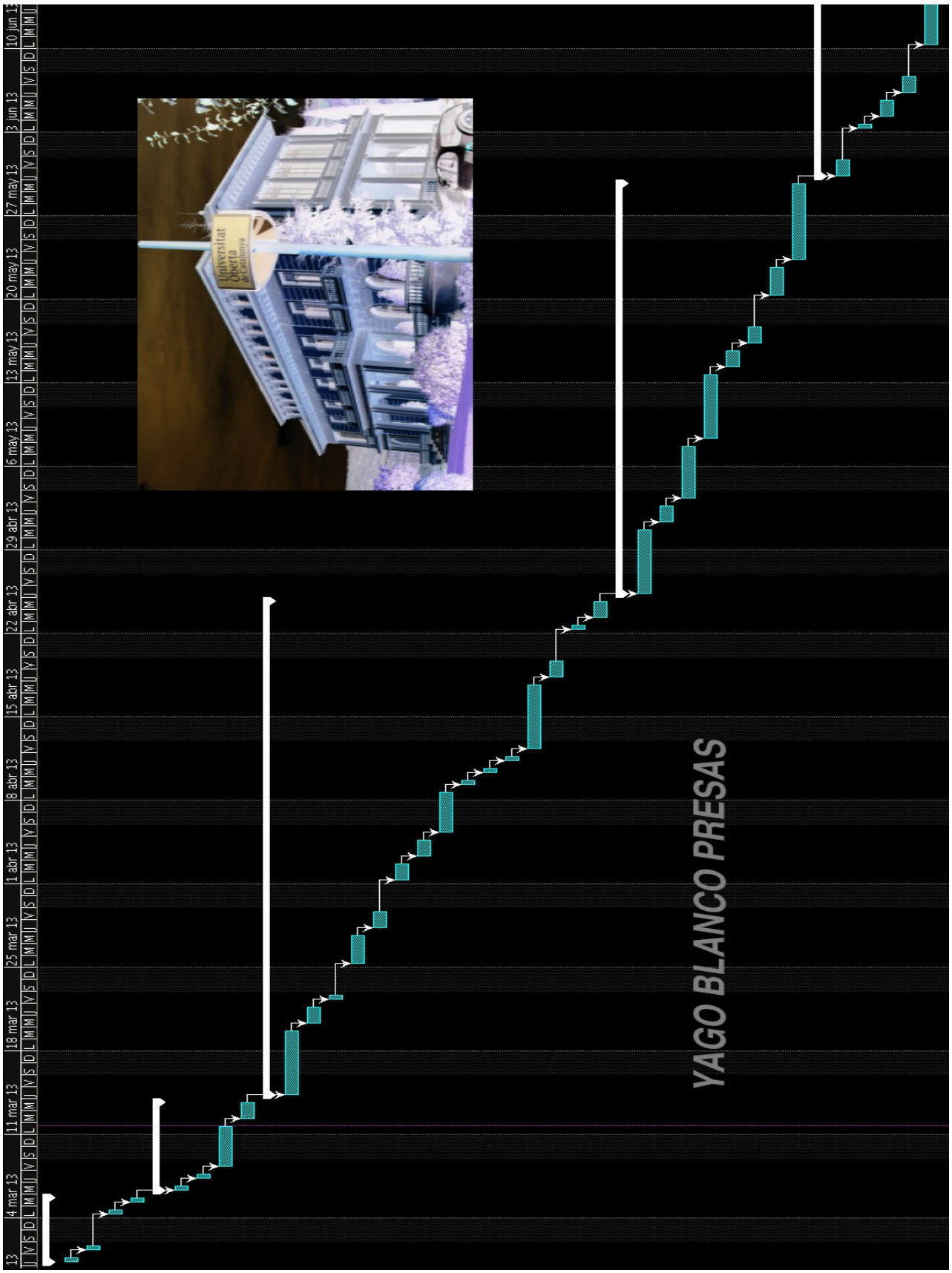
Gran capacitat de detecció i de reacció davant un nou virus.
Actualització sistemàtica.
Detecció mínima de falsos positius o falsos virus.
Respecte pel rendiment o acompliment normal dels equips.
Integració perfecta amb el programa de correu electrònic.
Alerta sobre una possible infecció per les diferents vies d'entrada (Internet, correu electrònic, xarxa o discos flexibles).
Gran capacitat de desinfecció.
Presència de diferents mètodes de detecció i anàlisi.
Revisió mèdica de l'arrencada i possibles canvis en el registre de les aplicacions.
Creació de discos d'emergència o de rescat.
Disposició d'un equip de suport tècnic capaç de respondre en un temps mínim (exemple 48 hores) per orientar a l'usuari en cas d'infecció.

Existeixen sistemes antivirus que tenen a més, la característica de treballar directament en xarxes LAN i WAN, així com en servidors proxy.

Davant la massiva proliferació, tant de virus com de productes dirigits al seu tractament, existeix la necessitat que algun organisme reconegut de caràcter internacional certifiqui els productes antivirus i asseguri el seu correcte rendiment. En un antivirus el més important és la detecció del virus i, a l'estudi de tal fi es dediquen associacions com la ICSA (International Computer Security Association) - anteriorment la NCSA - i la Checkmark. Ambdues segueixen procediments similars. En concret, perquè la ICSA certifiqui un producte antivirus, ha de ser capaç de detectar el 100 % dels virus inclosos en la Wildlist (llista de virus considerats en circulació) i, almenys, un 90 % de la Zoolist -una col·lecció de varis milers de virus no tan difosos. La certificació d'un producte es realitza quatre vegades a l'any, sense el coneixement del fabricador i amb una versió totalment comercial, amb el que s'assegura que la versió que se certifica és la que rep directament l'usuari i no una especialment preparada per a la prova.

ANNEX III: [Gantt- Openproj GNU]

Nombre	Duración	Inicio	Terminado	Predecesores
Preliminars a la realització del TFG i inici del projecte (Yago Blanc Preses - Grau Tecno Telecomunicacions)	4 days	**28/02/13 8:00**	**5/03/13 17:00**	
Planejament de la temàtica del TFG	1 day	28/02/13 8:00	28/02/13 17:00	
Revisió de la base Documental de la UOC. Cerca de Normativa actualitzada i exemples d'aplicació pràctica.	1 day	1/03/13 8:00	1/03/13 17:00	2
Motivació del projecte. Concretar àrees d'especialització en el TFG. Notificar al consultor l'àrea temàtica.	1 day	4/03/13 8:00	4/03/13 17:00	3
Esborrany "maqueta" inicial del projecte: "Polítiques de Seguretat Corporatives"	1 day	5/03/13 8:00	5/03/13 17:00	4
Pla de Treball (PAC 1)	6 days	**6/03/13 8:00**	**13/03/13 17:00**	
Divisió de tasques a realitzar.	1 day	6/03/13 8:00	6/03/13 17:00	5
Cronograma avançat amb OpenProj.	1 day	7/03/13 8:00	7/03/13 17:00	7
Pla de treball i modelització de desviacions possibles.	2 days	8/03/13 8:00	11/03/13 17:00	8
Realització de requeriments del projecte i índex preliminar.	2 days	12/03/13 8:00	13/03/13 17:00	9
Primer desenvolupament del TFG (PAC 2)	30 days?	**14/03/13 8:00**	**24/04/13 17:00**	
Recerca bibliogràfica avançada. Hemeroteca i accés a webs especialitzades.	4 days	14/03/13 8:00	19/03/13 17:00	10
Anàlisi de Disseny i Dimensionament de Models de Seguretat.	2 days	20/03/13 8:00	21/03/13 17:00	12
Aspectes Organitzatius i legals de la política de seguretat. Inici Documental.	1 day	22/03/13 8:00	22/03/13 17:00	13
La seguretat en entorns de comerç electrònic.	3 days	25/03/13 8:00	27/03/13 17:00	14
La seguretat en sistemes Open Source.	2 days	28/03/13 8:00	29/03/13 17:00	15
Documentació addicional i fonts d'empresa.	2 days	1/04/13 8:00	2/04/13 17:00	16
Models MITM, Spoofing i atacs DoS	2 days	3/04/13 8:00	4/04/13 17:00	17
Establiment de la topologia i infraestructura de xarxa. Normatives de seguretat.	2 days	5/04/13 8:00	8/04/13 17:00	18
Aspectes legals de la política de seguretat.	1 day	9/04/13 8:00	9/04/13 17:00	19
Aspectes lògics i de topologia. Documentació i Bibliografia relacionada.	1 day	10/04/13 8:00	10/04/13 17:00	20
Repercussió en els aspectes organitzatius i de recursos humans	1 day	11/04/13 8:00	11/04/13 17:00	21
Aspectes físics de les polítiques de seguretat de xarxa.	4 days	12/04/13 8:00	17/04/13 17:00	22
Desenvolupament expandit de l'apartat (1.5) sobre polítiques corporatives.	2 days	18/04/13 8:00	19/04/13 17:00	23
Elements bàsics de seguretat.	1 day?	22/04/13 8:00	22/04/13 17:00	24
ISO 17799	2 days	23/04/13 8:00	24/04/13 17:00	25
Segon desenvolupament del TFG (PAC 3)	25 days	**25/04/13 8:00**	**29/05/13 17:00**	
Aplicació a un supòsit de comerç electrònic. Plataforma PHP - Apache Server.	4 days	25/04/13 8:00	30/04/13 17:00	26
Tipificació i anàlisi dels atacs corporatius.	2 days	1/05/13 8:00	2/05/13 17:00	28
Atacs a la plataforma web (Vulnerabilitat de plataformes de comerç electrònic)	3 days	3/05/13 8:00	7/05/13 17:00	29
Webmin i SSL	4 days	8/05/13 8:00	13/05/13 17:00	30
Arquitectura IDS per Administradors.	2 days	14/05/13 8:00	15/05/13 17:00	31
Revisió dels annexos i les fonts de la informació (Primera Part)	2 days	16/05/13 8:00	17/05/13 17:00	32
Reflexió final sobre el projecte. Parametrització.	3 days	20/05/13 8:00	22/05/13 17:00	33
Revisió general de la solució proposada pel projecte (part final)	5 days	23/05/13 8:00	29/05/13 17:00	34
Memòria i Presentació final. Tribunal d'avaluació (TFG - UOC 2013)	12 days	**30/05/13 8:00**	**14/06/13 17:00**	
Maquetació i supervisió de l'ortografia de tot el projecte.	2 days	30/05/13 8:00	31/05/13 17:00	35
Revisió bibliogràfica i annexos (Part final avançada)	1 day	3/06/13 8:00	3/06/13 17:00	37
Desenvolupament final de la presentació virtual. Revisió del Lliurament final	2 days	4/06/13 8:00	5/06/13 17:00	38
Lliurament Final.	2 days	6/06/13 8:00	7/06/13 17:00	39
Tribunal Virtual i presentacions.	5 days	10/06/13 8:00	14/06/13 17:00	40


13
4 mar 13
11 mar 13
18 mar 13
25 mar 13
1 abr 13
8 abr 13
15 abr 13
22 abr 13
29 abr 13
6 may 13
13 may 13
20 may 13
27 may 13
3 jun 13
10 jun 13
Universitat Oberta de Catalunya
YAGO BLANCO PRESAS

GRAU TECNOLOGIES DE TELECOMUNICACIÓ 2013

Yago Blanco Presas