ENGINYERIA TÈCNICA DE TELECOMUNICACIONS

UOC Universitat Oberta de Catalunya

Memòria Final

Projecte fi de carrera

VULNERABILITATS EN XARXES WLAN
PROTOCOLS I MECANISMES DE PROTECCIÓ

José Luis Blasco de Gracia
Enginyeria Tècnica de Telecomunicacions (Telemàtica)
Universitat Oberta de Catalunya

Consultor: José López Vicario
Data: 10 de gener de 2016

Índex

Figures

Taules

Introducció del projecte

➢ Descripció

És evident que les tecnologies de la informació estan en constant desenvolupament. El naixement de la computadora, Internet i l'evolució dels sistemes de comunicacions han produït un canvi molt important en la societat, doncs han contribuït a millorar la nostra qualitat de vida facilitant l'accés a la informació i la comunicació entre persones d'arreu del mon. Si ens fixem en l'àmbit empresarial, internet ha estat clau en fomentar l'expansió dels negocis, i amb el naixement de les xarxes privades virtuals, una injecció de dinamisme, seguretat i eficiència que no té precedents. Són alguns exemples d'un univers en expansió.

Si el creixement de les xarxes i l'*Internet* mitjançant tecnologia cablejada ja fou un avanç revolucionari, va ser la implantació de la tecnologia sense fils el que va produir realment una transformació en els nostres hàbits d'accessibilitat i intercanvi d'informació. El domini de les comunicacions començava incloure el terme *mobilitat* com una de les seves virtuts principals. I és que intercanviar dades, accedir a internet o consultar el correu des d'un parc, un aeroport o pràcticament qualsevol lloc amb el nostre *smartphone*, *tablet* o ordinador portàtil fou veritablement surrealista.

Avui en dia les xarxes sense fils i més concretament les xarxes WLAN (Wireless LAN), ja formen part de la nostra vida, fins al punt en què és habitual trobar el logotip de la marca Wi-Fi en una plaça, un restaurant, un equip de música o la televisió.

Malauradament, com que l'intercanvi d'informació mitjançant la tecnologia Wi-Fi està forta i extensament implantada tant en l'àmbit domèstic com en el empresarial, la fa molt atractiva per als intrusos, els quals, trauran profit de qualsevol forat de seguretat existent. Un atac maliciós compromet la nostra privadesa, la pròpia informació o incús la seguretat informàtica d'una empresa. La facilitat que tenen els dispositius actuals per detectar xarxes Wi-Fi en un radi de 150 metres, ens porta a escenaris potencialment vulnerables per als atacants, la qual cosa exigeix solucions i mecanismes per protegir nostres dades.

Conscient d'aquesta situació, aquest treball s'endinsa en les xarxes WLAN amb l'objectiu principal d'exposar les seves vulnerabilitats i els mecanismes de protecció que s'implementen en la família d'estàndards IEEE 802.11. També estudia el funcionament d'algunes eines existents en el mercat que podrien incrementar la seguretat de la xarxa. La síntesi dels capítols és la següent:

El **capítol 1** ofereix una visió dels elements que integren les **xarxes locals sense fils** amb tecnologia WiFi, així com els diferents modes d'operació que poden adoptar segons la topologia implantada.

A continuació, el **capítol 2** tractarà principalment de **l'estàndard IEEE 802.11** com l'especificació que regula les normes de funcionament de les xarxes d'àrea local sense fils (WLAN).
També veurem que, donat les fallades de seguretat del protocol WEP implícit en aquesta especificació, naixerà el protocol *WPA* com a pont de transició cap a l'estàndard IEEE 802.11i, el qual, facilita l'ús de sistemes de xifrat com *AES*, autenticacions més robustes amb *WPA2* i la distribució de claus mitjançant el protocol *TKIP*. En aquest mateix capítol, veurem que la norma IEEE 802.1x i el protocol d'encapsulació *EAP*, ofereixen un pas més enllà en la identificació i autenticació d'usuaris abans d'accedir a la xarxa.

En el **capítol 3** s'analitzaran els diferents **tipus d'atacs** en aquest tipus de xarxes, com per exemple trencar llistes de control d'accés (ACL), atacs *Man in the middle* o atac *ARP poisoning*. També s'examinaran els **mecanismes de defensa** disponibles per minimitzar o evitar qualsevol intent d'intrusió.

Tot i que havent vist que existeixen algoritmes de xifratge i solucions a nivell de protocols per combatre possibles intrusions, el **capítol 4** presenta una sèrie de normes i **recomanacions generals a l'hora de protegir la xarxa**; ja sigui per a un usuari domèstic com per a un administrador d'empresa. En aquesta línia, també es determinaran aspectes importants a tenir en compte durant l'elaboració de les **polítiques de seguretat** que garanteixen un intercanvi de dades fiable.

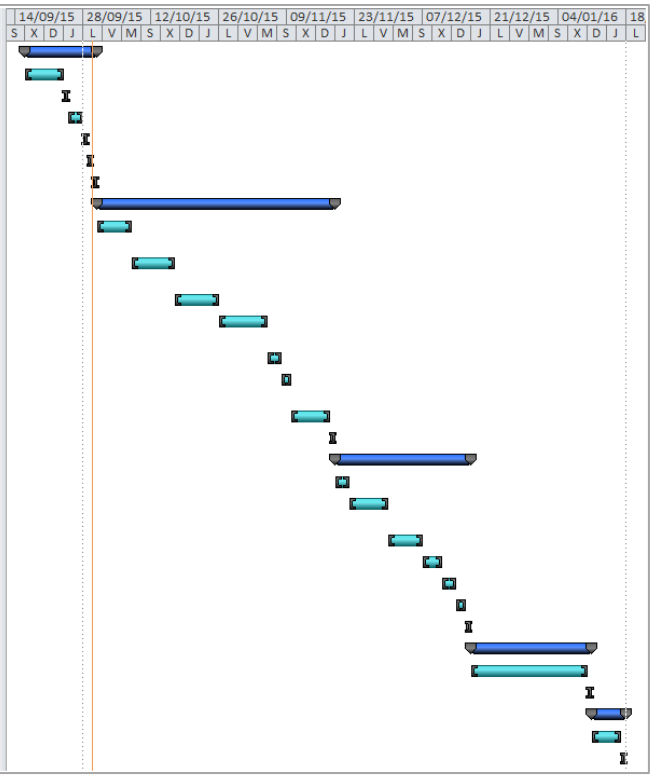
Ara bé, si no coneixem les nostres debilitats difícilment podrem establir un pla de prevenció i actuació davant possibles atacs. En aquest sentit, és necessari fer una "radiografia" de la nostra xarxa i detectar possibles esquerdes, doncs probablement seran la porta d'entrada dels intrusos. El **capítol 5** ens permetrà

conèixer què són les **eines d'escaneig i detecció de vulnerabilitats** en xarxes, com per exemple el programari *GFI LANguard*, el funcionament de qual s'estudiarà més a fons a l'annex 1.
Com que la seguretat de la xarxa es pot comprometre en qualsevol moment, també hem de tenir eines dissenyades per detectar i solucionar automàticament qualsevol intent d'intrusió. En aquest mateix capítol també es presentarà els sistemes de **prevenció d'intrusions (IPS)** i els sistemes de **detecció d'intrusions (IDS)** com els mecanismes de prevenció i defensa recomanats per als administradors de xarxa. Aquests sistemes estan dissenyats principalment per evitar accessos no autoritzats i manipulació de dades.

El software *Snort*, és un *sniffer* de paquets i detector d'intrusions que s'utilitzarà per entendre l'objectiu d'aquest tipus de detectors i aprendre a construir algunes regles de configuració. Per a aquesta tasca, es prepararà un escenari hipotètic mitjançant màquines virtuals on simularem el servidor d'una empresa de ventes per internet, l'IDS *Snort* i la xarxa interna d'administració. Es construiran regles personalitzades per alertar de cinc moviments sospitosos en la xarxa.

➢ Planificació

	Nom de la tasca	Durada	Inici	Fi
1	**PLANIFICACIÓ DEL TFC PAC1**	**11 días**	**mié 16/09/15**	**mié 30/09/15**
2	Decisió projecte i comunicació consultor	6 días	mié 16/09/15	mié 23/09/15
3	Anàlisi de les fites a realitzar	1 día	jue 24/09/15	jue 24/09/15
4	Elaboració del pla de treball	2 días	vie 25/09/15	dom 27/09/15
5	Realització del diagrama de Gantt	1 día	lun 28/09/15	lun 28/09/15
6	Elaboració document d'entrega PAC 1	1 día	mar 29/09/15	mar 29/09/15
7	Lliurament PAC 1	1 día	mié 30/09/15	mié 30/09/15
8	**ELABORACIÓ I LLIURAMENT PAC 2**	**35 días**	**jue 01/10/15**	**mié 18/11/15**
9	Estudi topologia i elements que integren les xarxes WLAN	5 días	jue 01/10/15	mié 07/10/15
10	Objectius i funcionament dels estàndards i protocols WLAN	7 días	jue 08/10/15	vie 16/10/15
11	Anàlisi dels riscos en xarxes Wi-Fi	7 días	sáb 17/10/15	dom 25/10/15
12	Estudi dels mecanismes de seguretat existents	8 días	lun 26/10/15	mié 04/11/15
13	Recomanacions per protegir xarxes Wi-Fi	3 días	jue 05/11/15	sáb 07/11/15
14	Consideracions a tenir en compte sobre les polítiques de seguretat	2 días	dom 08/11/15	lun 09/11/15
15	Elaboració document d'entrega PAC 2	6 días	mar 10/11/15	mar 17/11/15
16	Lliurament PAC 2	1 día	mié 18/11/15	mié 18/11/15
17	**ELABORACIÓ I LLIURAMENT PAC 3**	**20 días**	**jue 19/11/15**	**mié 16/12/15**
18	Recerca detectors de vulnerabilitats actuals	3 días	jue 19/11/15	sáb 21/11/15
19	Intal·lació i proves funcionals analitzador GFI Languard	7 días	dom 22/11/15	dom 29/11/15
20	Estudi funcionament i resultats obtinguts	6 días	lun 30/11/15	dom 06/12/15
21	Funcionament i objectius sistemes IDS i IPS	4 días	lun 07/12/15	jue 10/12/15
22	Escenaris i regles de filtratge IDS Snort	2 días	vie 11/12/15	dom 13/12/15
23	Elaboració document d'entrega PAC 3	2 días	lun 14/12/15	mar 15/12/15
24	Lliurament PAC 3	1 día	mié 16/12/15	mié 16/12/15
25	**MEMÒRIA FINAL**	**18 días**	**jue 17/12/15**	**dom 10/01/16**
26	Elaboració de la memòria	18 días	jue 17/12/15	sáb 09/01/16
27	Entrega de la memòria final	1 día	dom 10/01/16	dom 10/01/16
28	**PRESENTACIÓ DEL PROJECTE**	**6 días**	**lun 11/01/16**	**dom 17/01/16**
29	Elaboració de la presentació	6 días	lun 11/01/16	sáb 16/01/16
30	Entrega de la presentació	1 día	dom 17/01/16	dom 17/01/16



➢ Objectius

El treball està destinat, en general, a tots els usuaris que utilitzen la tecnologia sense fils per accedir a la xarxa. Tot i així, en alguns punts es treballen aspectes específics que poden estar orientats a empresaris i administradors de xarxes. Els objectius principals són els següents:

- Donar una **visió general del funcionament de les xarxes sense fils WLAN**, així com els tipus i elements que les integren. També es pretén demostrar que al ser una tecnologia molt estesa que utilitza l'aire com a medi de transmissió, la fa més vulnerable a atacs maliciosos que poden comprometre les nostres dades.
- **Presentar l'estàndard IEEE802.11** com l'especificació que regula les transmissions de dades en xarxes sense fils en els nivells de capa física i d'enllaç, però donada la falta d'eficàcia dels seus protocols, ha estat necessari crear els estàndard IEEE802.11i i el IEEE802.1x per donar suport a la implementació de mecanismes de seguretat més robustos i efectius.
- **Conèixer els riscos i amenaces** més comuns en aquest tipus de xarxes sense fils i comprendre la necessitat d'implantar solucions en els estàndards actuals.
- Oferir, tant a usuaris domèstics com a administradors de xarxes, un conjunt de **recomanacions** que s'haurien de tenir en compte quan es treballa amb xarxes WLAN.
- **Transmetre la importància de la prevenció** com a eina indispensable per minimitzar possibles atacs amb èxit i per tant, la necessitat de conèixer les vulnerabilitats que un atacant podria utilitzar per accedir a la nostra xarxa. Afortunadament existeixen al mercat programaris d'anàlisi dissenyats per detectar vulnerabilitats i corregir-les. S'utilitzarà l'escàner *GFI LanGuard* per comprendre com funcionen i què ens poden oferir.
- Mostrar els **Sistemes de Prevenció (IPS) i Detecció d'Intrusions (IDS)** com aliats dels administradors a l'hora d'aconseguir una vigilància permanent de la xarxa i a més, una ràpida resposta davant la detecció de moviments no autoritzats o manipulació de dades sospitoses. Amb l'IDS *Snort* s'aprendrà com es configuren les seves regles de filtratge davant els escenaris més habituals.

Capítol 1: Comunicacions a través de xarxes sense fils WLAN

Aquest capítol, situa les xarxes d'àrea local sense fils en un escenari on, la tecnologia *Wi-Fi,* es desenvolupa vertiginosament per arribar a consolidar-se com el mecanisme d'interconnexió entre dispositius amb mobilitat més utilitzat en àmbits privats, públics i empresarials.

Posteriorment, es determinaran els diferents modes d'operació que aquests tipus de xarxes adopten habitualment com a conseqüència de la topologia dissenyada, així com el funcionament de cada una d'elles en relació als elements que les integren.

Abans d'iniciar el primer punt, convé recordar que aquest treball no pretén aprofundir en les tècniques de modulació ni analitzar les característiques freqüencials associades als diferents canals d'ample de banda de les xarxes WLAN. L'objectiu principal és analitzar les amenaces de seguretat en la comunicació sense fils mitjançant la tecnologia WiFi i els possibles mecanismes pal·liatius. Per aquest motiu, considero que, abans d'examinar capítols posteriors, és important recordar el concepte de WLAN, conèixer els elements que la integren i les topologies que pot adoptar.

1.1 Conceptes bàsics d'una xarxa WLAN

WLAN (de l'anglès *Wireless Local Area Network*) significa xarxa d'àrea local sense fils. És un sistema de comunicació que permet la transmissió de dades entre dispositius mòbils utilitzant ones de radiofreqüència. Aquest tipus de comunicació, està àmpliament estesa per tot el món i regulada per la família d'estàndards **IEEE 802.11**. Des de l'any 1977, l'associació d'enginyers IEEE (*Institute of Electrical and Electronics Engineers*), designa diferents grups de treball per a desenvolupar els estàndards adients que donen suport al constant desenvolupament de les comunicacions WLAN.

Durant els primers anys de vida de la norma IEEE 802.11 va ser utilitzada pels fabricants d'equips informàtics de comunicació sense fils. Tanmateix, existien ambigüitats en alguns punts de la norma que deixaven la porta oberta a la interpretació, fet que es traduïa en problemes d'incompatibilitat entre dispositius de diferents fabricants. Per solucionar aquest inconvenient, l'empresa actualment anomenada *Wi-Fi Alliance* va desenvolupar una tecnologia coneguda popularment per la marca ***WiFi***, amb la qual, s'ha aconseguit compatibilitzar les comunicacions Ethernet sense fils i una homogeneïtzació dels productes.

La figura següent mostra el logotip de la marca comercial WiFi, amb la que l'empresa *Wi-Fi Alliance* certifica que els dispositius que porten aquesta tecnologia, compleixen les especificacions recollides en els estàndards 802.11, i per tant, vàlids per treballar en xarxes sense fils d'àrea local.

Logotip de la marca WiFi [1] Fig.1

1.1.1 Elements que integren una xarxa WLAN

Dintre d'una xarxa local sense fils destaquen els següents elements:

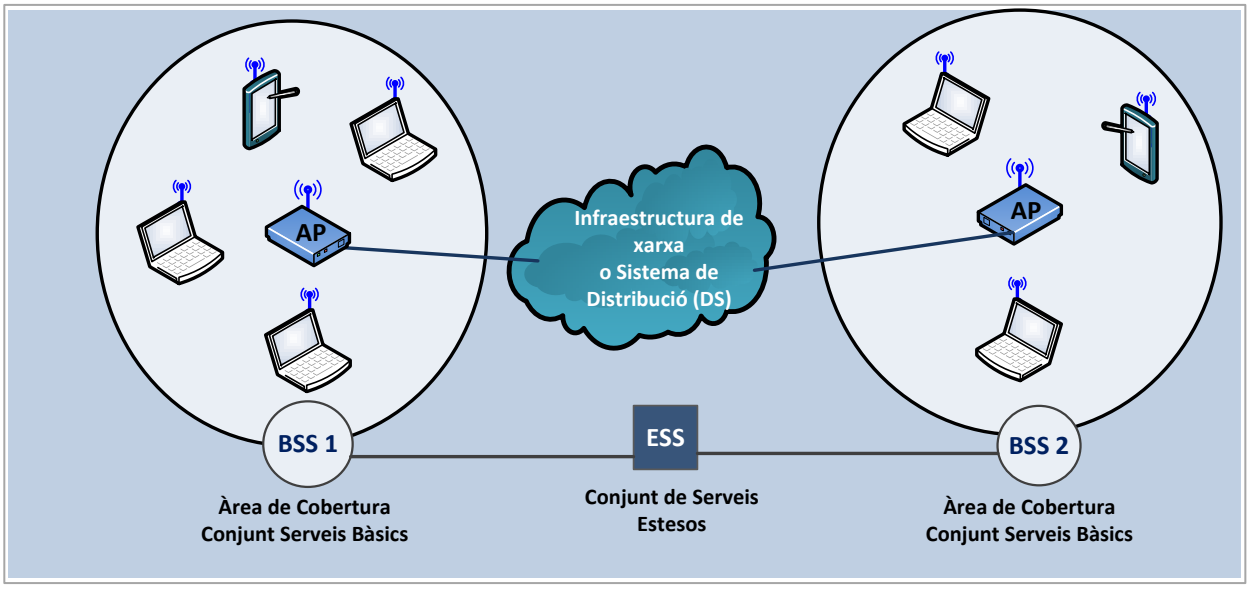
- Hosts sense fils
- Estacions base

Hosts sense fils: són dispositius que es connecten a una xarxa no cablejada i proveeixen o utilitzen serveis d'ella. Pot ser una computadora portàtil, una tauleta tàctil (*tablet*), un telèfon intel·ligent (*smartphone*) o un ordinador d'escriptori per exemple. Els hosts poden ser mòbils o no, i en general, tenen assignada una direcció IP per interconnectar-se amb altres equips.

Estació base (AP): coneguda en xarxes *WiFi* com a punt d'accés (en anglès: *Wireless Access Point* amb les sigles *WAP* o *AP*). La seva funció és enviar dades cap a un host que utilitza tecnologia sense fils i rebre els paquets d'informació que provenen d'un altra host associat amb aquest punt d'accés.

Les estacions base tenen un abast d'uns 150 metres en zones obertes, mentre que en llocs més grans com un aeroport, un campus universitari o un edifici, és necessari utilitzar diversos AP, formant cèl·lules solapades, que en el seu conjunt, donaran cobertura a tota un àrea pre-establerta. D'aquesta manera, els hosts client disposen d'una àmplia mobilitat sense talls perceptibles de comunicació (*roaming*).

La figura següent presenta una visió global dels elements comentats anteriorment, on el núvol representa la connexió dels AP amb la xarxa cablejada i els hosts sense fils dintre del radi de cobertura de cada punt d'accés.



Configuració típica de xarxes WLAN i elements integradors. Figura 2

Els equips actuals poden integrar la funcionalitat d'un encaminador, per tant, a més de tenir la responsabilitat de coordinar la transmissió dels múltiples hosts que té associats, actua de passarel·la entre la xarxa sense fils i la xarxa cablejada. Quan es diu que un equip està associat o vinculat a un punt d'accés, significa que el host es troba dins del radi de comunicació o àrea de cobertura i a més, utilitza l'estació base per intercanviar dades amb una infraestructura de xarxa de major grandària.

En relació als elements descrits anteriorment (hosts i punts d'accés), les xarxes Wi-Fi poden formar blocs o **cel·les de comunicació bàsiques** anomenades ***BSS*** (en anglès *Basic Service Set*). Una BSS té un àrea de cobertura dintre de la qual, tots els AP que pertanyin al BSS poden comunicar-se entre elles.

Tot i que una xarxa sense fils pot estar formada per una única cèl·lula, normalment s'utilitzen diverses cel·les, on els punts d'accés estan connectats a través d'un ***Sistema de Distribució*** (**DS**), generalment Ethernet i en alguns casos sense utilitzar cables.

La xarxa Wi-Fi completa, incloent les diferents cèl·lules *BSS*, els seus punts d'accés *AP* i el sistema de distribució *DS*, es pot considerar en capes superiors del model OSI com una **xarxa 802.11** clàssica, i es anomenada com un ***Conjunt Estès de Serveis*** (***ESS*** *en anglès Extended Service Set*). [2]

1.1.2 Topologies

La topologia d'una xarxa representa la disposició dels enllaços que connecten els seus nodes. Com que la interconnexió d'aquests nodes varia segons les necessitats, les xarxes poden adoptar formes diferents. La topologia d'una xarxa es pot descriure de dues formes: física o lògica.

La topologia física es refereix a la disposició del cablejat, antenes, ordinadors i altres dispositius de xarxa. Tanmateix, la topologia lògica fa referència a un nivell més abstracte, considerant la manera en què els hosts es comuniquen a través del medi. Les topologies de les xarxes WLAN, adopten els següents modes d'operació [2]:

- Infraestructura
- Ad-hoc
- Mesh

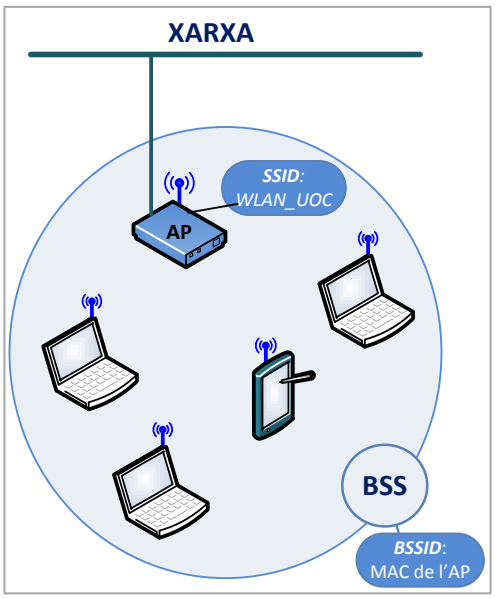
Infraestructura:
en aquest mode d'operació cada host es connecta a un punt d'accés a través d'un enllaç sense fils. La configuració formada pel punt d'accés (*AP*) i els hosts dintre de l'àrea de cobertura formen, tal i com s'ha comentat anteriorment, un conjunt de serveis bàsic (*BSS*), això és, una cèl·lula. Cada BSS s'identifica a través d'un identificador de 6 bytes anomenat **BSSID** (en anglès *Basic Service Set Identifier*) el qual es correspon amb l'adreça MAC del punt d'accés associat.

Donat que múltiples xarxes WLAN podrien compartir el mateix espai aeri, cada WLAN necessita un únic nom. Aquest nom, és l'identificador del conjunt de serveis de la xarxa anomenat **SSID** (en anglès *Service Set Identifier*). Així doncs, qualsevol host podrà veure els SSID de les xarxes disponibles, on l'administrador pot identificar-les amb un nom alfanumèric, per exemple WLAN_UOC, WLAN_estudiants, WLAN_visites...

Qualsevol usuari de WLAN, solament haurà de preocupar-se de seleccionar l'SSID de la llista que apareixerà en el seu dispositiu i establir connexió, introduint l'autenticació especificada segons el tipus de xarxa que a la que vol accedir.

Els paquets que circulen en una WLAN han d'arribar al destí correcte. L'SSID manté els paquets dintre de la WLAN que li correspon, inclús quan hi conviuen WLAN superposades.

La possibilitat d'existir diversos punts d'accés dintre de cada WLAN, implica necessàriament identificar cada AP i el seus clients o hosts associats. Aquest identificador és precisament el **BSSID**, portador de la MAC de l'AP associat i que està implícit en tots els paquets que viatgen a través de xarxes sense fils.

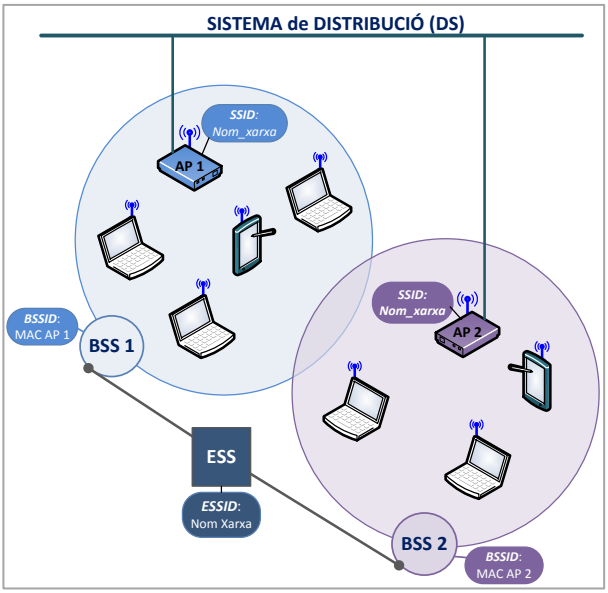


Representació del SSID i BSSID d'una WLAN Figura 3

Quan un host intenta unir-se a una cèl·lula, envia una sol·licitud de sondeig a cada canal. Aquesta sol·licitud, inclou l'SSID de l'AP de la cèl·lula i també el volum de tràfic que el seu adaptador de xarxa sense fils pot admetre. Cada punt d'accés, transmet una senyal en intervals regulars (10 vegades per segon aproximadament). Aquesta senyal, anomenada ***beacon frames***, proveeix informació del BSSID (adreça MAC), les característiques de l'AP i de manera predeterminada, el seu SSID.

En el moment en què es rep una sol·licitud de sondeig, el punt d'accés verifica el SSID i la sol·licitud del volum del tràfic implícita en la senyalització. Si l'SSID ofert coincideix amb el del punt d'accés, aquest envia una resposta amb dades de sincronització i informació sobre la seva càrrega de tràfic. D'aquesta manera, el host que rep la resposta, pot verificar la qualitat de la senyal que rep de l'AP i valorar la distància entre ells. Així doncs, a mesura que disminueix aquesta distància, s'incrementa la capacitat de transferència de dades.

A la figura 4 podem veure que en mode infraestructura també és possible vincular diversos AP junts, o més exactament, associar diversos BSS amb un sistema de distribució DS.



Associació de diversos BSS per formar un ESS Figura 4

Cada xarxa **ESS** s'identifica a través de l'**Identificador del Conjunt de Servei Estès** (***ESSID,*** *en anglès Extended Service Set Identifier*). Consta de 32 caràcters en format ASCII i representa el seu nom a la xarxa. És necessari conèixer l'ESSID de l'AP per poder formar part de la xarxa WLAN, és a dir, l'ESSID configurat al host ha de concordar amb el l'ESSID del punt d'accés. Es tracta doncs d'una primera mesura de seguretat bàsica.

Si un usuari itinerant es desplaça amb el seu host des d'un BSS a un altre sense sortir de l'espai que abasta l'ESS, el seu adaptador xarxa podrà canviar de punt d'accés, depenent de la qualitat de senyal que rebi dels diferents AP's.

L'objectiu és intercanviar informació sobre els hosts, i en cas necessari, transmetre dades des de dispositius mòbils. Aquesta característica que permet als hosts la possibilitat de moure's de manera "transparent" d'un punt d'accés a un altre s'anomena **itinerància**.

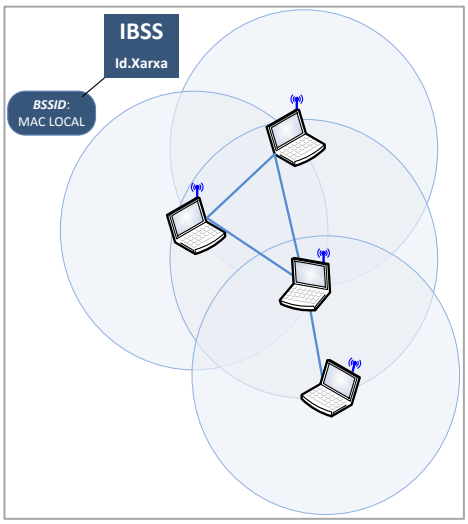
En alguns casos, hi pot haver diferents BSSID's en un punt d'accés per a cada WLAN configurada per a un radi de cobertura. Si per exemple tenim un AP que dona servei a dos radis de cobertura amb 32 xarxes WLAN configurades en cadascun, tindríem 64 BSSID's més el punt BSSID de l'AP.

Per donar cobertura als múltiples BSSID's, s'assignaria a cada AP un bloc únic de 64 adreces MAC. Cada radi de cobertura tindrà 32 adreces MAC i suporta fins a 32 noms de xarxa diferents (identificadors SSID), els quals, tindran assignats una adreça MAC com a identificació de serveis bàsics (BSSID).

Un aspecte important a tenir en compte és el risc de col·lisions durant transmissions simultànies de diversos dispositius. En comunicacions sense fils basades en IEEE 802.11 s'utilitza generalment el mecanisme ***CSMA/CA*** (*Carrier Sense Multiple Access with Collision Avoidance*), que significa accés múltiple amb escolta de portadora i evasió de col·lisions. Aquest algoritme, especifica que abans de que un equip transmeti informació, ha d'escoltar la xarxa per comprovar si ja existeix un altra dispositiu enviant dades. Si no és així, podrà transmetre, però si es detecta un altra host transmetent, haurà d'esperar un temps aleatori. Finalitzat aquest temps, tornarà a comprovar si el medi continua ocupat amb una altra transmissió.

El problema esdevé quan dos o més equips comproven a la vegada si el canal està lliure, i en cas afirmatiu, comencin a transmetre simultàniament. En qualsevol cas, aquesta situació haurà de ser solucionada per protocols superiors, com TCP, que al detectar pèrdues d'informació demanaran la retransmissió d'aquesta.

Ad-hoc: és un mode d'operació que adopten els dispositius integrats en una WLAN per un temps limitat, els quals, els hosts no estan connectats a través d'un punt d'accés (AP) a cap xarxa o sistema de distribució. Un exemple seria, tal i com es mostra a la figura 5, diversos usuaris amb un ordinador portàtil que desitgen intercanviar i compartir arxius a través del medi sense fils, prescindint de mitjans externs, com podria ser les memòries USB.



Esquema d'una xarxa *Ad-hoc* Figura 5

En el mode ad-hoc els hosts client sense fils es connecten entre sí per a formar una xarxa punt a punt, és a dir, una xarxa en la que cada equip actua com a client i com punt d'accés simultàniament.

La configuració que formen els hosts s'anomena **conjunt de servei bàsic independent** (***IBSS***). Així doncs, un IBSS és una xarxa sense fils que té almenys dos dispositius interconnectats sense utilitzar cap AP. El fet de no utilitzar cap punt d'accés, implica la inexistència de l'SSID com identificador i per aquest motiu, l'IBSS possibilita la creació d'una xarxa temporal que permet als usuaris presents en la mateixa sala puguin intercanviar dades i el BSSID és un valor MAC de 48 bits generat localment.

En una xarxa *ad-hoc*, el rang del BSS independent està determinat pel rang de cada host. Això significa que si dos hosts de la xarxa estan fora de rang un de l'altre, no podran comunicar-se, ni tan sols en cas de que puguin veure altres hosts. A diferència del mode infraestructura, el mode *ad-hoc* no té cap sistema de distribució que pugui enviar trames de dades des d'un host a un altre. Cada node, té la capacitat d'un encaminador. Per tant, es diu que un IBSS és una xarxa sense fils **restringida**.

Tanmateix, la comunicació a través d'estructures *ad-hoc* necessita algoritmes que suportin certa mobilitat en els hosts clients (xarxes *MANET*), amb limitacions d'ample de banda, memòria reduïda i situacions de tràfic dens. També hem de tenir en compte el nombre de salts que ha de recórrer la informació per arribar al host final. Com que cada node que transmet la informació és un salt, quants més salts es produeixin, més temps tardarà en arribar la informació a destí, incrementant la probabilitat de que arribi corrompuda.

Així doncs, és necessari comptar amb protocols que es responsabilitzin de trobar una ruta per a cada paquet i assegurar que aquest, es transmet pel camí adequat. Si es desitja un encaminament eficient, es necessiten protocols que ofereixin una senyalització mínima i un temps reduït de processament. A més, també interessa que no produeixin bucles, que permetin compartir decisions d'encaminament (distribuïts), i suportin enllaços unidireccionals amb mode *sleep* quan un dispositiu està inactiu.

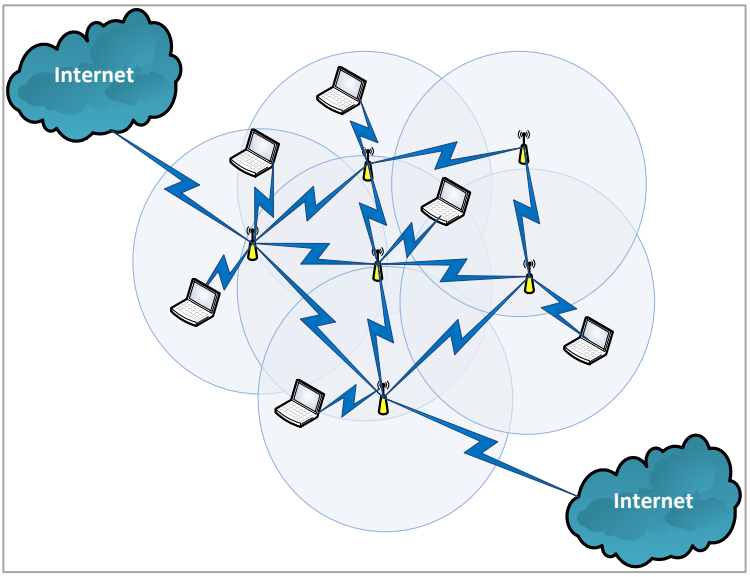
Existeixen diversos protocols que intenten cobrir les prestacions anteriors, dels quals comentaré els més utilitzats: ***AODV*** (*Ad-hoc On Demande Distance Vector*) i ***DSDV*** (*Destination Sequenced Distance Vector*).

- ***AODV*** és un protocol d'encaminament IP que permet als hosts descobrir i mantenir rutes vers a altres dispositius de la xarxa. És un protocol *reactiu*, doncs les rutes s'estableixen solament quan es necessiten, això és, quan un host origen vol transmetre dades a un host destí. La particularitat d'aquest protocol radica en les decisions d'encaminament, les quals es realitzen utilitzant vectors de distància, per exemple, distancies mesurades en els salts efectuats a tots els encaminadors disponibles. Els encaminadors, mantenen les distancies d'aquells destins amb els quals necessiten contactar o transmetre informació.

  Cada host disposa d'una taula d'encaminament amb les rutes i el destí, on cada entrada conté l'adreça del següent salt (dispositiu inclòs en la ruta prevista), un comptador de salts vers a destí i un nombre de seqüència de destinació amb el registre de temps (*timestam*p).
  Amb els nombres de seqüència, es determina si la ruta està actualitzada o no; quan més gran és aquest nombre més actualitzada està la ruta i si el nombre és molt baix, la ruta es descarta. D'aquesta manera, el protocol s'assegura de que no hi haurà bucles.

- ***DSDV*** és un protocol que pertany a la família d'algoritmes basats en vector de distància. El seu adreçament és de tipus *proactiu*, és a dir, localitza les rutes abans que siguin necessàries. Disposa d'una taula d'encaminament que indica el nombre de salts necessaris per arribar a destí i quin serà el salt successiu. L'actualització de les taules es produeix mitjançant l'intercanvi d'informació entre nodes pròxims i replicant els algoritmes de camí més curt i a menor cost. També s'etiqueta cada camí amb un nombre de seqüència, amb la particularitat de que si està identificada amb un nombre imparell, significa que aquell camí és inassolible, mentre que si és un nombre parell, el camí sí és assolible.[3]

Mesh: en les xarxes sense fils *Mesh* conflueixen les topologies descrites anteriorment; infraestructura i ad-hoc. S'anomenen també xarxes acoblades o xarxes de malla sense fils on existeixen almenys dos camins en cada node. La seva característica principal, radica en què possibilitat la connexió a la xarxa a dispositius que estan fora del rang de cobertura dels punts d'accés, però sempre que estiguin dintre del rang de cobertura d'alguna targeta de xarxa, la qual, ha d'estar directa o indirectament, dintre del radi de cobertura d'un AP.



Esquema d'una xarxa *Mesh* Figura 6

Les xarxes *Mesh*, permeten la comunicació entre targetes de xarxa independentment del punt d'accés. Això significa que els dispositius que actuen com a targeta de xarxa no poden enviar directament els seus paquets al punt d'accés, sinó que hauran de passar a través d'altres targetes de xarxa per arribar al destí. Una característica important és que les xarxes de malla són tolerants a fallades, ja que la caiguda d'un sol node no afecta a la resta de la xarxa.

La transmissió de la informació fins a destí, també s'ha de gestionar mitjançant un protocol dissenyat per a transmetre la informació amb un nombre mínim de salts o, que almenys, sigui suficientment eficient. Un dels protocols més coneguts per a aquesta tasca és ***OSLR*** *(Optimized Link-State Routing Protocol)*.

- ***OLSR*** és un protocol d'encaminament reactiu, així que no depèn exclusivament de l'intercanvi periòdic d'informació d'encaminament o càlcul de rutes. Quan es necessita una ruta, el host ha d'iniciar el procés de descobriment d'aquesta, per la qual cosa s'optimitzen els recursos evitant l'enviament de paquets innecessàriament. Està basat en la definició i ús d'alguns hosts de la xarxa que prenen el nom de MPR's (*Multipoint Relays*). Aquests MPR's, escollits per altres nodes veïns de la xarxa, es designen com a únics responsables de controlar els paquets de *broadcast* durant el procés de *flooding*. L'objectiu és reduir la sobrecàrrega de trames, evitant que cada host reenviï automàticament cada paquet que rep.

  OLSR està dissenyat per operar en mode distribuït, això significa que els hosts comparteixen les decisions d'encaminament i no depenen d'una entitat central. El re-ordenament de paquets típic en xarxes ad-hoc es porta a terme gràcies al nombre de seqüència diferent que porta cada paquet. Com que aquest protocol utilitza el re-enviament de paquets *per-node*, cada host utilitzarà la seva informació més recent per encaminar el paquet. [3]

Capítol 2: Estàndards i protocols utilitzats en WLAN

La facilitat d'instal·lació, baix cost, cobertura, mobilitat i senzilla ampliació són alguns factors que d'alguna manera han propiciat freqüents actualitzacions de l'estàndard per cobrir la creixent demanda i necessitats del mercat. Per tant, la tecnologia 802.11 és actualment la dominant en el sector WLAN.

Així doncs, aquest capítol donarà a conèixer els protocols i estàndards més importants desenvolupats per IEEE 802.11, donant un especial èmfasi en els estàndards **802.11i** i **802.11x** relacionats amb la seguretat, donat que les xarxes WLAN són, per sí mateixes, més insegures que les xarxes cablejades, ja que el medi físic per transmetre les dades és l'aire i a través de les ones electromagnètiques.

2.1 Estàndards WiFi: IEEE 802.11

WiFi es la marca comercial amb la que actualment s'identifiquen els productes WLAN que disposen de tecnologia desenvolupada amb les especificacions descrites en els estàndards **802.11**. Aquest model, fou desenvolupat per un grup de comerç que va adoptar el nom de "*WiFi Alliance*", format principalment per companyies com *3com, Aironet, Luncent* o *Nokia* i que responien originalment al nom oficial WECA (*Wireless Ethernet Compatibility Alliance*).

L'estàndard 802.11 es va presentar al juny de 1997 i es va caracteritzar per oferir velocitats de 1 i 2 Mbps, un sistema de xifrat senzill anomenat **WEP** (*Wired Equivalent Privacy*) i operar en la banda de freqüència de 2,4 Ghz. En dos anys, van aparèixer les variants 802.11a i 802.11b que oferien velocitats superiors de 54 i 11 Mbps respectivament. Tanmateix, no trigaren gaire en sorgir les debilitats a nivell de seguretat d'aquests estàndards, fet que va obligar a desenvolupar noves revisions i protocols. La figura 7 mostra un exemple del logotip que implementaria un dispositiu dotat de tecnologia WiFi i els estàndards que suporta.

Etiqueta WiFi amb tecnologies suportades [4] Figura 7

Avui en dia, la família 802.11 està formada per una gran nombre d'estàndards. A continuació es resumeixen els més rellevants. [5]

- **802.11:** estàndard que es va començar a desenvolupar a l'any 1970 per l'IEEE. No va ser fins a l'any 1977 en el qual es va aprovar la norma 802.11 com l'estàndard oficial per a tecnologies de xarxa sense fils. Permet la connexió sense fils de dispositius a través de punts d'accés i sota un àrea de cobertura de 100 metres aproximadament. La connexió es realitza mitjançant ones de Radi Freqüència. Originalment oferia una velocitat de transmissió de 1 o 2 Mbps en la banda de freqüència WiFi de 2,4 GHz. Aquesta norma es coneixerà popularment per la marca WiFi.
- **802.11a:** estàndard que fa servir els mateixos protocols que l'estàndard original i opera en la banda de 5GHz utilitzant 52 subportadores d'accés múltiple per divisió de freqüències ortogonals (*OFDM*). La velocitat màxima de 54 Mbps el converteix en un estàndard molt versàtil per a xarxes sense fils amb velocitat reals de 20 Mbps aproximadament. Disposa de 12 canals sense solapament: 8 per a la xarxa sense fils i 4 per a connexions punt a punt.
- **802.11b:** ofereix una velocitat màxima de transmissió de 11 Mbps i utilitza el mateix mètode d'accés definit a l'estàndard original *CSMA/CA* (accés múltiple amb escolta de portadora i evasió de col·lisions). Funciona a la banda de 2,4 GHz i la velocitat màxima de transmissió és de 5,9 Mbps sobre TCP i 7,9 Mbps sobre UDP.
- **802.11c:** defineix característiques de punts d'accés (AP) com a Bridges. És utilitzat per a la comunicació de dues xarxes diferents o de tipus diferents.
- **802.11e:** ofereix un estàndard sense fils per operar entre entorns públics, de negocis i usuaris residencials amb la capacitat de solucionar les necessitats de cada sector d'aplicació. És tracta d'un dels primers estàndards per a xarxes sense fils que permet treballar en entorns domèstics i empresarials, afegint característiques de qualitat de servei (*QoS*) i suport multimèdia.

- **802.11f:** facilita la compatibilitat de connexió entre punts d'accés. Utilitza el protocol *IAPP* que permet a un usuari itinerant canviar d'un punt d'accés a un altre sense importar els tipus de fabricants que utilitzen la infraestructura de xarxa. Aquesta funcionalitat es definia al capítol 1 com itinerància.
- **802.11g:** implementa un estàndard de modulació que utilitza la banda de 2,4 GHz i opera a una velocitat teòrica màxima de 54 Mbps amb un promig real de transferència de 22 Mbps. És compatible amb l'estàndard 802.11b i utilitza les mateixes freqüències.
- **802.11i:** estàndard dissenyat per resoldre vulnerabilitats en la seguretat de protocols utilitzats en l'autenticació i codificació. Aquest estàndard abasta els protocols 802.1x, TKIP (en anglès *Temporal Key Integrity Protocol*) i AES (*Advanced Encryption Standard*). Està implementat en el mecanisme WPA2 (*Wi-Fi Protected Access*). En capítols posteriors s'abordarà aquest estàndard i els seus protocols amb més detall, donada la seva importància en la millora de la seguretat en xarxes Wi-Fi.
- **802.11n:** dissenyat per millorar el rendiment de la xarxa ofert pels estàndards 802.11b i 802.11g, amb un increment important de la velocitat màxima de transmissió de 54 Mbps fins a un màxim de 600 Mbps, tot i que a la capa física es permetran 300 Mbps com a màxim. Gràcies a la implementació de la tecnologia MIMO (*Multiple Input – Multiple Output*) permet utilitzar diversos canals simultàniament per enviar i rebre dades mitjançant la incorporació de múltiples receptors i transmissors. A diferència de versions anteriors, pot treballar en dues bandes de freqüències: 2,4 GHz (utilitzada per 802.11b i 802.11g) i també amb 5 GHz (utilitzada per 802.11a).
- **802.11ac:** implementa notables millores respecte al 802.11n. Utilitza part dels estàndards 802.11a i n, amb la novetat de que pot subministrar una velocitat de transmissió superior a 1 Gbps en la banda de 5 GHz. Utilitza canals estesos de 80 i 160 MHz, el doble o quàdruple que 802.11n i a més, utilitza MIMO multi-usuari amb 5 a 8 sequències espacials, amb la modulació 256-QAM, el quàdruple també que l'estàndard 802.11n
- **802.1x :** norma que forma part de la família de protocols IEEE 802.1 i destinada a regular el control d'accés a la xarxa basada en ports. Permet l'autenticació de dispositius connectats a un port LAN, de manera que estableix una connexió punt a punt o commutant l'accés per aquest port si es detecta una falla en l'autenticació. S'utilitza en alguns punts d'accés sense fils tancats i es basa en el protocol d'autenticació extensible *EAP*.

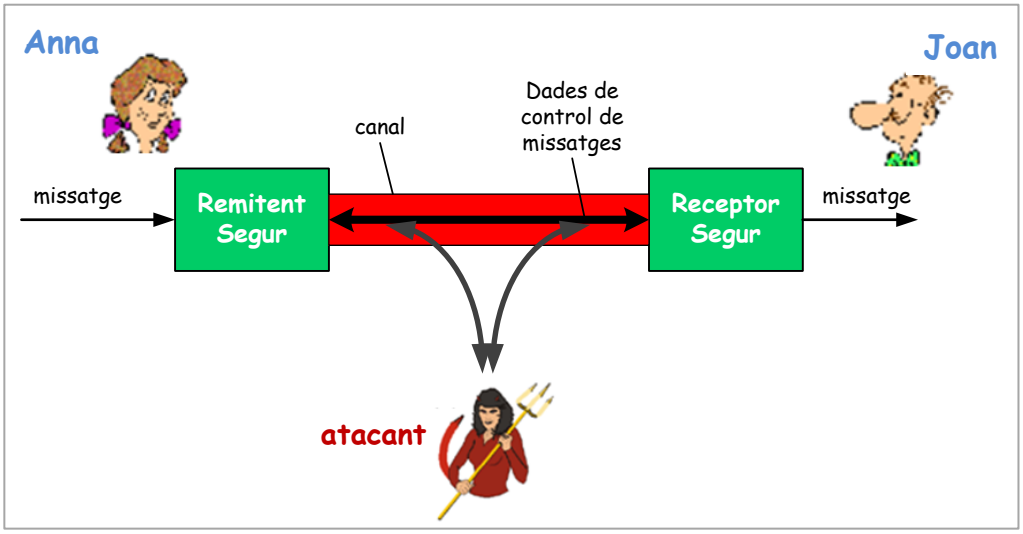
Acabem de veure una gran part dels estàndards que formen l'evolució del 802.11 que avalen la seva versatilitat i adaptació a les necessitats dels fabricants i consumidors. A continuació veurem amb més detall els estàndards 802.11i i 802.1x, els quals, ens ajudaran a entendre en el capítol 3, cóm han contribuït en millorar significativament la seguretat de les xarxes WLAN davant a les amenaces de possibles d'intrusos o atacants.

Però abans d'avançar en la descripció dels mecanismes de seguretat que implementa aquest nou estàndard, és important entendre què entenem i desitgem en una comunicació segura.

2.1.1 Una comunicació segura

Quan parlem de seguretat en un procés de comunicació entre dues entitats, ens estem referint a que la informació intercanviada entre, per exemple, dues persones Anna i Joan, no ha estat interceptada ni manipulada per un tercer. A més, Joan, el receptor, vol estar segur que el missatge rebut prové realment d'Anna, i aquesta, estaria més tranquil·la si tingués la certesa de que Joan és l'única persona que ha vist el missatge.

La comunicació a través de la xarxa pública comporta una sèrie de riscos que hem d'afrontar. Qualsevol intrús, a més de suplantar la identitat d'algun interlocutor, també pot tafanejar, modificar, afegir, esborrar el contingut dels missatges o inclús esborrar-los completament.



Esquema d'intrusió durant la comunicació mitjançant la tècnica *MitM* Figura 8

El primer mecanisme que ens ajuda a aconseguir una comunicació amb certes garanties de seguretat és el **xifrat** del missatge. Xifrar o encriptar un missatge significa utilitzar un algoritme d'encriptació amb una clau de xifrat que transforma el missatge en un text incomprensible. L'única manera de desxifrar el missatge serà mitjançant una **clau secreta** de desxifrat del algoritme. Si la clau o contrasenya de xifrat i desxifrat és la mateixa (compartida) es tracta de **criptografia simètrica**. Si les claus són diferents, estem parlant de **criptografia asimètrica**.

Tot i que el xifrat pot mantenir en secret el contingut d'un missatge i ens aporta **confidencialitat**, és necessari complementar-lo amb altres tècniques criptogràfiques per comunicar-se de forma segura i garantir, per exemple, la **integritat** i l'**autenticació** dels interlocutors, conceptes que es detallen a continuació:

- **Confidencialitat:** Solament l'emissor i el receptor podran comprendre el contingut dels missatges transmesos. Com que un missatge por ser interceptat per un tercer, és imprescindible que els missatges siguin xifrats, de manera que en el cas de que el missatge sigui interceptat, no pugi ser comprés per la persona maliciosa.

- **Integritat del missatge**: o autenticació del missatge. Inclús si l'emissor i el receptor són capaços de d'autenticar-se entre sí, voldran estar segurs de que el contingut del missatge no ha estat alterat per un tercer durant la transmissió.

- **Autenticació:** Durant el procés de comunicació, tant l'emissor com el receptor hauran de poder confirmar la identitat de l'altre. És a dir, Joan ha d'estar segur de que el missatge que ha rebut ha estat escrit realment per l'Anna, i el mateix passa a la inversa.

- **Seguretat operacional:** Evitar que organitzacions (empreses, universitats...) amb xarxes connectades a Internet, siguin compromeses per atacants des de la xarxa pública. Mecanismes pal·liatius: es disposa de tallafocs col·locats entre la xarxa de l'organització i la xarxa pública per controlar l'accés de paquets que provenen de d'Internet. A més, mitjançant un sistema de detecció d'intrusions, es realitza una inspecció profunda de cada paquet alertant als administradors de xarxa d'activitats sospitoses. Aquestes solucions les veurem amb més detall al capítol 6. [6]

Podem concloure que parlar d'una comunicació segura en xarxes, implica resoldre els aspectes descrits anteriorment, això és, **Autenticació**, **Confidencialitat** i **Integritat**, tot i que alguns autors també consideren la dimensió **Disponibilitat** (ACID). En aquest sentit, l'estàndard 802.11i implementa mecanismes que ajuden a aconseguir les dimensions abans indicades i que veurem a continuació.

2.1.2 L'Estàndard 802.11i

La norma original 802.11 proveïa un mecanisme de seguretat conegut col·lectivament pel nom de *privacitat equivalent a la del cable* (**WEP**, *Wired Equivalent Privacy*), amb el qual, proporcionava un nivell de seguretat similar al de les xarxes cablejades, utilitzant sistemes d'autenticació oberts o de clau compartida tan poc recomanables.

L'objectiu del protocol WEP era facilitar l'encriptació del tràfic entre punts d'accés i dispositius mòbils per compensar la falta de seguretat existent quan s'envia la informació per un medi compartit com és l'aire. Per tant, tots els AP's i dispositius Wi-Fi incloïen l'opció d'encriptar les transmissions amb el protocol d'encriptació WEP.

El seu funcionament es basa en establir una clau secreta en el punt d'accés compartida amb els clients WiFi. Amb aquesta clau, el simple algoritme criptogràfic **RC4** i un **Vector d'Inicialització** (IV), es realitza l'encriptació de les dades transmeses per radiofreqüència.

Tanmateix, amb la proliferació de les xarxes WiFi va començar a sorgir greus problemes de seguretat informàtica derivats de certes deficiències en els següents elements:

- Vector d'Inicialització (IV) massa curt amb 24 bits. Davant d'un gran volum de tràfic en xarxes WiFi es pot repetir amb certa freqüència.
- Existien dispositius amb targetes o USB molt simples, on el primer Vector d'Inicialització que generaven era zero i seguidament 1; i així successivament. Per tant, fàcil d'endevinar.
- Les claus utilitzades eren estàtiques i es devien canviar manualment. La modificació de les claus no era un procés fàcil per realitzar-lo freqüentment.
- Absència d'un control de seqüència de paquets. Això significa que diversos paquets d'una comunicació podien ser robats o modificats sense que ningú ho detectés.

Davant aquest panorama, no trigaren gaire en sortir múltiples aplicacions preparades per vulnerar la seguretat WEP, de manera que, segons la capacitat de l'atacant i la màquina utilitzada, podria desxifrar la clau WEP entre 15 minuts i un parell d'hores.

Conscients d'aquesta situació, l'IEEE va començar a treballar en la creació de protocols de seguretat més robustos. Els reptes que l'equip IEEE tenia que assolir es basaven en millorar el dèbil xifrat que oferia WEP i la problemàtica d'autenticar-se sense disposar de cap mecanisme de distribució de claus.

El primer repte al que *Wifi Alliance* s'enfrontava passava per implementar una solució funcional en els punts d'accés ja venuts a milers i milers d'usuaris. El segon desafiament, era la capacitat del hardware dels AP's, el qual ocupava el 90% dels recursos amb diverses funcions, així que qualsevol modificació en el protocol WEP no podia exigir demandes de recursos exigents.

Per tal motiu, l'equip d'enginyers IEEE van decidir desenvolupar dues solucions; una immediata de caire temporal que correspondria a una primera fase de l'estàndard 802.11i, basada en un nou protocol anomenat **TKIP** (*Temporal Key Integrity Protocol*) i conegut popularment pel nom **WPA** (*Wifi Protected Access*).

Tot i que es tractava realment d'un pedaç sobre l'algoritme RC4, les millores que WPA va oferir respecte a WPE són:

- El Vector d'Inicialització (IV) s'incrementa de 24 bits a 48.
- Implementació de la funció **MIC** (*Message Integrity Check*) per controlar la integritat dels missatges i detectar la possible manipulació de paquets.
- Reforç del mecanisme de generació de claus.

La segona solució, que ja seria definitiva, era una versió millorada de WPA, la qual van anomenar **WPA2** i es va incorporar en els nous punts d'accés (no en el els existents). WPA2 implementa un nivell de

seguretat més potent que WPA conegut pel nom de **CCMP** (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*). CCMP utilitza un dels algoritmes d'encriptació més potents i difícils de trencar: **AES** (*Advanced Encryption Standard*).

Com que aquest algoritme requeria un hardware més robust, els AP's anteriors al 2006 no van poder utilitzar WPA2 i a partir del Març d'aquell any, va ser un requisit obligatori per a tots els productes WiFi.

Les millores WPA2 respecte WPA són:

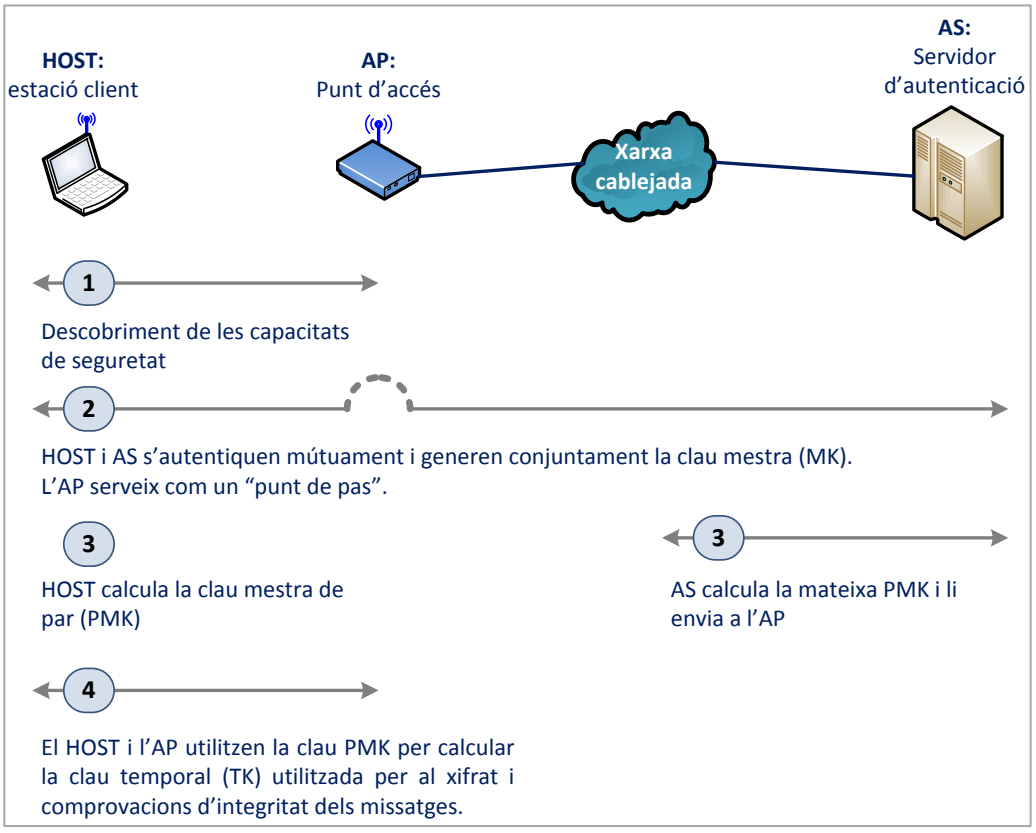
- Algoritme d'encriptació basat en AES
- Xifrat simètric de 128 bits
- Vector d'Inicialització (IV) de longitud 48 bits

Aquests canvis van obligar a modificar els paquets que utilitzaven les xarxes sense fils WiFi per transmetre la informació, de manera que els paquets de senyalització "*Beacons*", devien incloure les dades sobre el tipus d'encriptació (WEP, TKIP, CCMP) o sobre el tipus d'autenticació 802.1x utilitzat mitjançant la família de protocols EAP (LEAP, TLS, TTLS etc.), els quals s'estudiaran en aquest mateix capítol.

Podem concloure que l'estàndard **802.11i** es va adoptar finalment a l'any 2004 superant el nivell de seguretat que implementava la norma original 802.11. Les seves fortaleses es basen en mecanismes de xifrat més potents, sistemes d'autenticació ampliables i mecanismes de distribució de claus.

Mitjançant la figura 8, estudiarem en quatre fases, el mode d'operació de l'estàndard 802.11i en un marc gràfic, on a més del host client sense fils, es defineix un **Servidor d'Autenticació** (**AS**) amb el que l'AP pot comunicar-se.

Separar el servidor d'autenticació (AS) del punt d'accés, permet que un mateix servidor d'autenticació ofereixi servei a múltiples AP, centralitzant les decisions d'autenticació i accés en aquest únic servidor. D'aquesta manera, s'aconsegueix un baix nivell de cost i una disminució de la complexitat dels punts d'accés.



Fases del mode d'operació de l'estàndard 802.11i [6] Figura 9

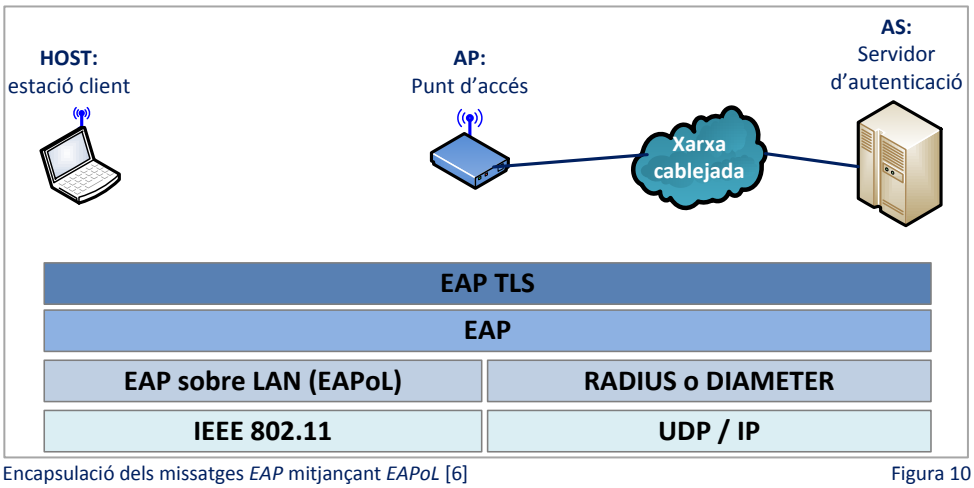
Aquestes quatre fases es descriuen a continuació:

① **Descobriment:**
En la fase de descobriment l'AP anuncia la seva presencia i els mecanismes d'autenticació i xifrat que pot proporcionar al host client sense fils. El host, sol·licita els mecanismes d'autenticació i xifrat que desitja. Tot i que el host i l'AP ja estan intercanviant missatges, el host encara no està autenticat i tampoc disposa de cap clau de xifrat, per tant, són necessaris alguns passos més abans de que el host client pugui comunicar-se amb un altre host remot a través del canal sense fils.

② **Autenticació mútua i generació de la clau mestra (*MK, Master Key*):**
L'autenticació té lloc entre el client sense fils i el servidor d'autenticació (AS). En aquesta fase, el punt d'accés actua bàsicament com un repetidor, reenviant els missatges entre el host i el servidor d'autenticació. El Protocol Ampliable d'Autenticació **EAP-TLS** (***Extensible Authentication Protocol-Transport Layer Security***) defineix els formats dels missatges terminal a terminal utilitzats en un mode d'interacció simple, això és, de tipus sol·licitud / resposta entre client i servidor d'autenticació.

Aquests missatges encapsulats, s'envien a través de l'enllaç sense fils 802.11 i seran desencapsulats en el punt d'accés, per tornar-los a encapsular novament mitjançant el protocol **RADIUS** (*Remote Access Dial In-Use Server*) o el recent estandarditzat **DIAMETER** que millora l'anterior. La finalitat d'aquests protocols és facilitar l'autenticació i autorització per a aplicacions d'accés a la xarxa o mobilitat IP, així com la transmissió de paquets sobre UDP/IP vers al servidor d'autenticació.
Amb els protocols EAP, el servidor d'autenticació pot seleccionar diverses formes per a portar a terme l'autenticació. Tot i que 802.11i no imposa un mètode concret, molt sovint s'utilitza l'esquema d'autenticació EAP-TLS, el qual fa servir tècniques de clau pública que inclouen xifrat i resums de missatges, amb la finalitat de permetre que el client i servidor d'autenticació, s'autentiquin mútuament entre sí i calcular una clau mestre (MK) que serà coneguda per les dues parts.

La figura 9, representa l'encapsulació dels missatges EAP utilitzant **EAPoL** (EAP sobre LAN implementat a l'estàndard IEEE 802.1x que veurem més endavant).



Encapsulació dels missatges *EAP* mitjançant *EAPoL* [6] Figura 10

Quan s'intenta la connexió amb un ISP (Proveïdor de Serveis d'Internet), s'envia una informació que generalment és un nom d'usuari i una contrasenya. L'important és que aquesta informació, es transfereix a un servidor RADIUS mitjançant el protocol ***PPP*** (*Point-to-Point Protocol*), el qual s'encarrega d'autenticar la connexió, xifrar la transmissió utilitzant el protocol d'encriptació *ECP* i finalment comprimir-la. El servidor RADIUS, comprova que la informació rebuda és correcta utilitzant esquemes d'autenticació, com per exemple EAP. Si és acceptat, els servidor autoritzarà l'accés al sistema i li assignarà recursos de xarxa, com una adreça IP, etc.

③ **Generació de la clau mestre de parell (*PMK, Pairwise Master Key*):**
La MK representa un secret compartit que solament coneixen el client i el servidor d'autenticació. A més, tots dos utilitzen la clau mestra de parell (PMK) per generar una segona clau. El servidor d'autenticació envia la PMK al punt d'accés, i com que el host i l'AP disposen d'una clau compartida s'autentiquen mútuament entre sí. (Recordem que el mecanisme de seguretat WEP implementat en la norma 802.11 ni tan sols contemplava la distribució de claus).

④ **Generació de la clau temporal (*TK, Temporal Key*):**
Amb la PMK, el client sense fils i l'AP ja poden generar les claus addicionals que s'utilitzaran per a la comunicació. La clau temporal TK es farà servir per realitzar el xifrat de les dades que s'enviaran a través de l'enllaç sense fils vers a un host remot arbitrari.

Així doncs, acabem de veure que l'estàndard 802.11i preveu diversos mecanismes que ajuden a incrementar la seguretat durant el procés de connexió i intercanvi de dades a través de la xarxa. Inclou una versió més potent del que ofereix WEP, amb un esquema de xifrat basat en AES (*Advanced Encryption Estandard*), el qual, és un dels algoritmes més segurs i més utilitzats avui en dia, amb una longitud de la clau que pot anar des de 128 bits fins a 256 bits.

Tal i com s'ha comentat en punts anteriors, la norma 802.11i també proporciona autenticació. Aquest procés es porta a terme gràcies al component d'autenticació 802.1x que ja s'havia provat en xarxes cablejades, i al 2004 es va adaptar finalment per a les xarxes sense fils WiFi.

2.1.3 L'Estàndard 802.1x

L'estàndard 802.1x és l'eix vertebrador de la seguretat WiFi. La seva participació en la norma 802.11i és clau per aconseguir una seguretat robusta, doncs introdueix una sèrie de modificacions importants en l'esquema WiFi que es detallen a continuació:

- autenticació dels usuaris abans de connectar-se a una xarxa sense fils WiFi.
- l'autenticació es realitza amb el protocol EAP mitjançant alguna de les seves versions com per exemple *EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP i EAP-TTLS*.
- autenticació mitjançant un servidor RADIUS (*Remote Authentication Dial-In User Service*) o més avançat anomenat DIAMETER.
- 802.1x autentica a l'usuari i no al dispositiu com podria ocórrer en el filtrat d'adreces MAC. Aquest procés és important, doncs impedeix l'accés a la xarxa encara que l'usuari autoritzat perdi o li sigui robat el seu dispositiu.
- El punt d'accés no autoritza l'accés a la xarxa sinó el servidor RADIUS o DIAMETER.
- El port de comunicació no s'obrirà per a permetre la connexió mentre que l'usuari no estigui autoritzat.

Els elements que intervenen en el sistema són:

1. **Sol·licitant:** és una aplicació "client" que facilita les credencials de l'usuari a l'autenticador (AP) per accedir a la xarxa.
2. **Autenticador:** dispositiu que rep la informació de l'usuari i la trasllada al servidor d'autenticació. S'ha vist anteriorment que aquesta funció recau en el punt d'accés.
3. **Servidor d'autenticació:** verifica les credencials dels usuaris amb la seva base de dades. Generalment és el servidor basat en el protocol RADIUS o DIAMETER. [7][8]

Capítol 3: Riscos i solucions en xarxes WiFi

Conceptes com amenaça, risc o intrús en el mon de les xarxes sense fils, poden passar desapercebuts, donada la facilitat amb la que els usuaris accedeixen a la xarxa i de la relativa dependència que tenim d'ella. És fàcil comprovar cóm els dispositius actuals estan orientats a la connexió quasi per defecte, amb aplicacions intuïtives que executen els processos de connexió entre host i punt d'accés de manera quasi transparent per a l'usuari, el qual, en la majoria dels casos, només haurà de acceptar la connexió seleccionada.

És difícil ser conscient d'un risc quan no percebem cap indici o no tenim la sensació de perill. Avui en dia ja és normal veure diverses persones en una plaça o un cafè amb els seus dispositius portàtils connectats a la xarxa gratuïta d'alguna institució, gran superfície o ajuntament. La comunicació va per l'aire, no es veu ni es percep res anormal.

Ara bé, què passaria si sabéssim per endavant que la vestimenta i el portàtil dels atacants és de color vermell i que a més, porten un trident tal com s'està representant en les figures?. Probablement, abans de connectar-nos a la xarxa, miraríem al voltant per intentar detectar visualment algun possible intrús i en conseqüència, prendre mesures preventives en cas de confirmar la seva existència.

En aquest sentit, el perill de vulnerabilitat en xarxes sense fils és superior si el comparem amb les xarxes cablejades. Si detectem una persona desconeguda, connectada a una xarxa cablejada a través d'un switch el qual està restringit al personal informàtic de la nostra empresa, probablement desviarà la nostra atenció. Però, aquesta mateixa persona, asseguda en la terrassa d'un restaurant i en el mateix edifici on s'ubica l'empresa en qüestió, podrà passar desapercebut robant informació sensible al departament de I+D.
Així doncs, aquest capítol tracta primerament de conèixer i alertar de les amenaces a les quals s'enfronten les xarxes WiFi, així com els mecanismes que utilitzen els intrusos per intentar aconseguir un atac amb èxit. Posteriorment, veurem que els protocols 802.11i i 802.1x són els pilars fonamentals de la seguretat Wi-Fi, però que encara que estan basats en protocols molt robusts tal i com havíem vist al capítol 2, presenten algunes vulnerabilitats a tenir en compte que posen en perill la privadesa de la informació.

3.1 Amenaces en comunicacions WiFi

Sabem que el fet d'utilitzar l'aire com a medi de transmissió de dades mitjançant la propagació d'ones de radi comporta una sèrie de riscos de seguretat a tenir molt en compte. Hem de pensar que les ones de radi surten fora del nostre edifici, empresa o institució, de manera que les dades queden exposades a possibles intrusos que podrien obtenir certa informació privada, dades sensibles d'una empresa o posar en perill la seva seguretat informàtica.

Ens enfrontem a vulnerabilitats implícites en les xarxes WiFi que no podem obviar i per tant, mereix la pena exemplificar alguns d'ells per demostrar d'una manera realista, que les amenaces presents en la comunicació *Wireless* formen part d'una estratègia perfectament elaborada per individus que, amb certs coneixements informàtics, treballen sigil·losament i en l'anonimat. Vegem alguns exemples:

Es podria perpetrar un atac per inserció amb el conegut ***Man-in-the-Middle*** representat esquemàticament com l'individu atacant de la figura 8 al punt 2.1.1, quan parlàvem de comunicació segura. Aquest usuari no autoritzat, podria llegir, inserir o modificar la informació intercanviada entre Anna i Joan sense generar cap tipus de sospita. Aquest procés és tan simple com implementar un accés il·legal més potent que capti els dispositius clients en comptes del punt d'accés legítim, interceptant així la xarxa sense fils.

També seria possible originar atacs amb interferències o ***jamming*** destinades a produir una denegació de servei (DoS), simplement introduint un dispositiu que emeti ones de radi a la mateixa freqüència que les ones utilitzades per les xarxes Wi-Fi. Existeixen dos tipus, un d'ells denominat ***spot***, el qual va adreçat a interferir una freqüència específica, mentre que si es tracta de afectar a diversos canals simultàniament estem davant d'una interferència de tipus ***barrage***.

Les víctimes d'aquests atacs són clients autoritzats que no es poden connectar a la xarxa, i en qualsevol cas, l'AP seguirà operant normalment. En el millor dels casos, solament podran establir connexió alguns clients que estiguin situats el suficientment a prop del dispositiu emissor. Ara bé, es necessita trobar la

freqüència adient per a que l'atac sigui efectiu i la potència suficientment elevada per suplantar la senyal original.

Una altra escenari susceptible de ser atacat és durant la comunicació amb la xarxa directament entre hosts sense fils, és a dir, sense passar per cap punt d'accés. Aquest fet facilita l'atac d'un intrús a qualsevol d'aquests hosts i com a resultat, problemes greus si el dispositiu atacat ofereix serveis TCP/IP o comparteix arxius per exemple. També existeix la possibilitat de duplicar les adreces IP o també les MAC dels hosts legítims, situació que podria provocar el **robatori d'informació** o **suplantacions d'identitats** per exemple.

Els punts d'accés també estan exposats a atacs de ***Força Bruta*** amb l'objectiu d'esbrinar les contrasenyes, així que una configuració incorrecta o l'elecció de dèbils mecanismes d'encriptació deixaria l'AP vulnerable i facilitaria als intrusos la seva irrupció a la xarxa per iniciar un procés d'intercepció d'informació de manera no autoritzada (***eavesdropping***).

Acabem de veure algunes hipotètiques situacions en les que les xarxes sense fils s'exposen constantment. A pesar d'aquest riscos i altres que es comentaran més endavant, hem vist que afortunadament l'estàndard 802.11i preveu solucions i mecanismes de seguretat per fer front a aquestes amenaces, però també descobrirem que malauradament, aquests mecanismes no sempre s'habiliten o simplement no s'exigeixen.

A continuació, veurem la facilitat en la que es poden detectar espais amb xarxes sense fils i les particularitats que tenen les anomenades *Xarxes Obertes*, caracteritzades per no tenir implementat cap sistema d'autenticació o xifrat.

Posteriorment, a través de la web ***wigle.net*** s'analitzarà i compararà el nivell de protecció d'un volum de xarxes sense fils detectades per simpatitzants arreu del món i a l'estat espanyol. Ens servirà per revelar estadísticament una proporció important de xarxes sense fils que no disposen de cap mecanisme de seguretat, o la que tenen habilitada, no és suficientment efectiva.

3.1.1 Detecció de xarxes sense fils

Avui en dia disposem de dispositius dotats de comunicació WiFi en la majoria d'ordinadors portàtils, telèfons intel·ligents o tauletes tàctils. De fet, són els equips que més s'utilitzen a l'hora de establir connexió a la xarxa amb mobilitat.

Qualsevol d'aquests dispositius detecten i mostren una llista de xarxes sense fils localitzades dintre del seu radi de cobertura, incloent l'SSID de cada xarxa, el nivell de potencia rebuda i el tipus de protecció que té habilitada. L'usuari només ha de seleccionar alguna xarxa de la llista i començarà el procés de connexió específic que haurà configurat l'administrador de la xarxa escollida.

Vegem doncs que detectar xarxes WiFi és senzill, de fet, existeix un mètode de detecció de xarxes sense fils mitjançant una persona en moviment, com per exemple amb un vehicle. Aquesta variant rep el nom en anglès de ***Wardriving*** i el procés és simple:

Un dispositiu portàtil dotat amb tecnologia WiFi i un software gratuït per detectar punts d'accés com *NetStumbler* o *Inssider* seria suficient per passejar-se per un carrer o centre de negocis i observar la quantitat sorprenent de xarxes existents. Posteriorment, amb l'ajuda d'un GPS, es marcaria la posició exacta de la senyal rebuda amb més potència o amb una antena direccional si es vol rebre el tràfic de la xarxa des d'una distància considerable.

Amb l'objectiu de posar de manifest la facilitat amb la que les xarxes WiFi son detectables i susceptibles d'un anàlisi posterior d'intencionalitat qüestionable, val la pena comentar un exemple conegut de fa pocs anys sobre *Wardriving* i pot ser "*Sniffing*". Em refereixo al vehicle utilitzat per la famosa i útil aplicació *Google Street View*.
Aquest vehicle, recorria els carrers múltiples ciutats per a prendre fotografies i elaborar mapes de situació visualment molt més atractius i reals. El problema va sorgir quan es va detectar que mentre el vehicle practicava *Wardriving* també es capturava el tràfic de les xarxes obertes sense fils. Es tractava d'un

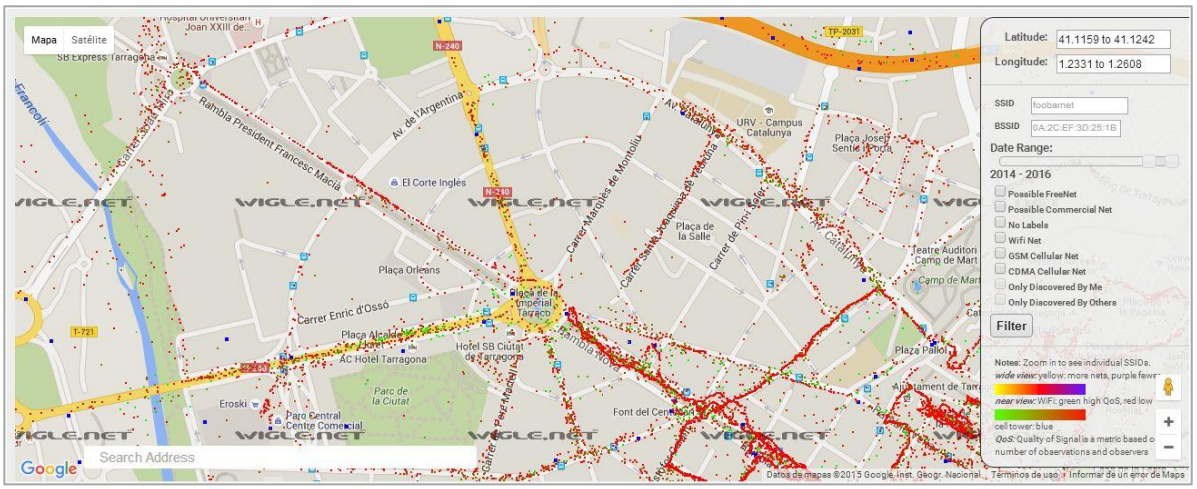
programa tipus "*sniffer*" que cada 5 segons recollia mostres de la xarxa WiFi de cada canal, obtenint informació com l'SSID, la posició GPS i les adreces MAC dels punts d'accés que treballaven en obert.

"*Ara està clar que s'han recollit erròniament dades de xarxes WiFi obertes, inclús encara que nosaltres mai hem utilitzat aquestes dades en cap producte Google*" va anunciar Alan Eustace responsable d'enginyeria i investigació de Google. [9]

Acabem de veure un exemple on les xarxes sense fils són originalment de domini públic en el moment en què utilitzen l'aire com a medi de transmissió i són vulnerables si no es protegeixen adientment.

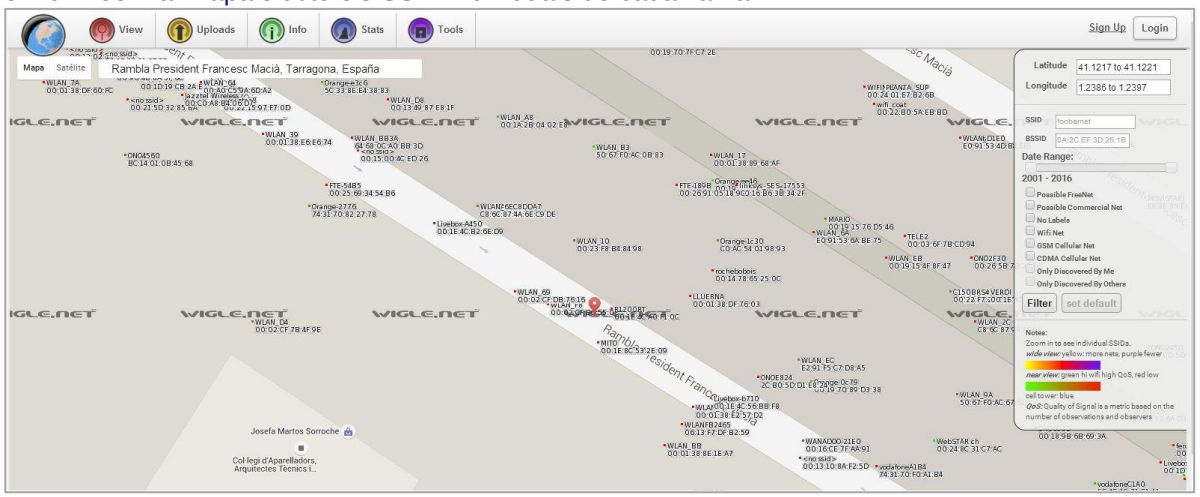
Tal i com s'havia anticipat a l'inici del capítol, es interesant visitar el portal *Wigle.net* on podem trobar informació sobre xarxes WiFi i antenes de telefonia mòbil de tot el planeta. Les seves dades, són enviades per seguidors que realitzen *Wardriving* amb els seus dispositius mòbils sense fils. D'aquesta web, surten dades que, tot i que són orientatives, no deixen de ser interessants.

La figura següent presenta una vista parcial de la ciutat de Tarragona on es pot comprovar la gran quantitat de punts vermells que representen xarxes WiFi disponibles amb baix QoS, mentre que els punts de color verd, disposen d'una qualitat de servei més elevada. Tot i que es tracta d'una part molt petita de la ciutat, és impressionant la quantitat de punts trobats. [10]



Plànol parcial de Tarragona amb AP's detectats mitjançant *Wardriving* [10] Figura 11

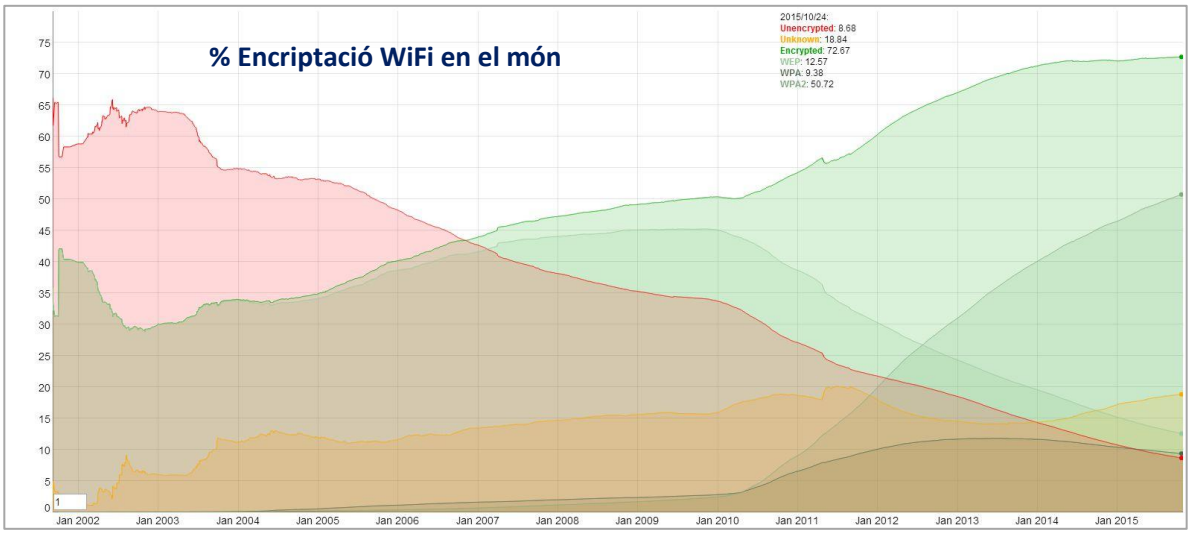
Si fem un zoom al mapa s'obté els SSID individuals de cada xarxa.



Plànol d'un carrer de Tarragona amb els SSID de les xarxes detectades.[10] Figura 12

Es torna a posar de manifest la facilitat en que les xarxes sense fils s'anuncien, són detectables i ofereixen informació a possibles atacants sense que molts usuaris tinguin la mínima sospita o coneixement.

A continuació analitzarem a nivell estadístic, l'evolució dels mecanismes de protecció utilitzats en les WLAN primerament a nivell mundial. Aquestes dades van des de l'any 2003 fins l'octubre de present any 2015.

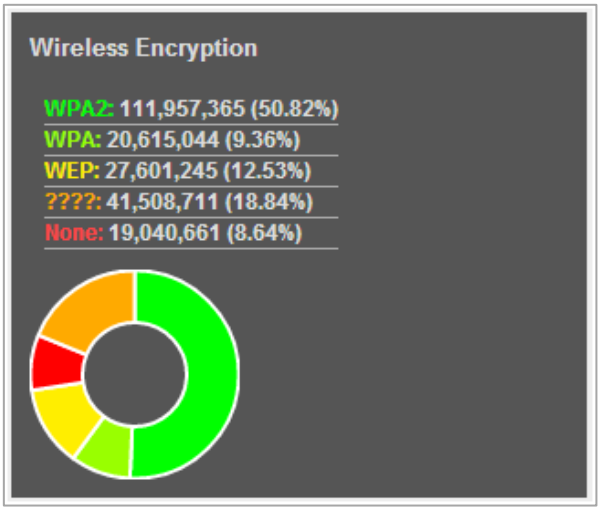


Gràfica d'evolució dels mecanismes d'encriptació en el món. [11] Figura 13

Al gràfic anterior, podem observar que afortunadament la tendència inicial de xarxes desprotegides a disminuït del 65% del total en el 2002, a un 8,68% de la actualitat, en detriment d'un augment significatiu de xarxes protegides amb algun tipus d'encriptació (72,67%) al 2015.

Tot i així, és significatiu que encara existeix un percentatge de 12,57% de xarxes desprotegides amb el dèbil protocol WEP. Pel que fa a WPA, tenim un 9,38% i amb WPA2 el 50,72%.

No oblidem que alguns percentatges, tot i que poden semblar relativament baixos, referencien la part corresponent del global mundial.



Distribució mundial per tipus d'encriptació. [11] Figura 14

Vegem ara les dades corresponents al territori espanyol i comunitats indicades a la taula inferior:

Country	Count
US	53,493,418
DE	8,856,744
GB	7,903,464
NL	6,051,799
CA	5,198,488
FR	3,372,666
JP	2,837,254
RU	2,499,390
AU	2,079,888
PL	1,939,365
ES	1,897,154
BE	1,679,765
SE	1,519,415
DK	1,491,799
IT	1,426,888
CH	1,150,361
NO	1,044,554
CN	1,036,809
BR	1,025,481
CZ	906,521
MX	799,855
AR	752,439
UA	729,554
KR	714,146

Region	Count
Catalunya	490,688
Madrid	251,532
Comunitat Valenciana	210,134
Andalucía	142,545
Illes Balears	95,971
Cataluu00f1a/Catalunya	68,606
Castilla y León	60,056
Galicia	51,442
Murcia	47,244
Navarra	47,062
Andalucu00eda	45,322
Aragón	44,510
La Rioja	37,700
Asturias	36,731
Cantabria	34,966
Canarias	29,364
Castilla-La Mancha	25,389
Castilla y Leu00f3n	18,839
Aragu00f3n	6,154
Extremadura	5,352
Euskadi	2,749
Islas Canarias	49
Ceuta	22
Principado de Asturias	3

Dades a Espanya

Encryption	Count
WPA	617,060
WEP	567,893
WPA	470,995
?	148,042
	93,164

Distribució del tipus d'encriptació al territori espanyol [11] Figura 15

Observem que de les 1.897.154 xarxes WiFi detectades 93.164 (4,9%) no tenen cap tipus de protecció habilitada. Només un **24,8%** de les xarxes totals treballen amb WPA2 i un 32,52% WPA. Però el realment preocupant és que existeixen quasi un **30%** de xarxes protegides amb el obsolet mecanisme de seguretat WEP.
Així doncs, tenint en compte les dades aproximades anteriors i sent optimistes, podem deduir que el 87,2% de les xarxes WiFi del territori espanyol té habilitada algun tipus de protecció, ja sigui WEP, WPA o WPA2, valors superiors si els comparem amb els que vam obtenir a nivell mundial (72,67%). Tanmateix, pel que fa a xarxes protegides amb WPA2 (24,8%) perdem la proporció en comparació al resultat mundial (50,72%).

Amb les xifres anteriors, podem deduir que els atacants disposen d'un ampli domini de xarxes totalment desprotegides o amb un sistema de protecció realment qüestionable. De la mateixa manera que nosaltres ho sabem, ells també ho saben, i a més, tenen medis i coneixements per aprofitar-se d'aquesta situació.

3.1.2 La inseguretat de les xarxes obertes

El mode de vida que la societat porta des de fa unes anys, reflecteix una necessitat constant de estar connectats d'alguna manera a Internet. Per donar un exemple, l'aplicació *WhatsApp* s'ha convertit en una eina de comunicació personal quasi imprescindible. Podem consultar *Facebook*, pujar fotografies a l'*Instagram*, *tuitejar* alguna cosa que hem vist i contestar missatges de correu de l'oficina des de qualsevol lloc.

Indicació de Zona WiFi [12] Figura 16

La majoria de vegades tot l'anterior es porta a terme mitjançant el telèfon mòbil, la tauleta i cada vegada més, els ordinadors portàtils.

En aquesta línia, és molt comú buscar xarxes WiFi publiques sense protecció amb contrasenyes que ens permeti la connexió a Internet d'una manera fàcil i econòmica. De fet, és molt habitual trobar cadenes de restauració amb WiFi gratuït per als seus clients, aeroports, estacions o llocs públics amb WiFi proporcionat pels ajuntaments.

El problema és que encara és habitual trobar xarxes sense fils sense cap tipus de protecció o amb protocol WEP i activat amb el SSID utilitzat per defecte. Per tant, les comunicacions entre terminals i els punts d'accés es transmeten en text pla, sense xifrar, i no es sol·licita cap dada per accedir a la xarxa.

Els únics elements amb els que podríem intentar incrementar la seguretat en aquests tipus de xarxes serien:

- Adreces MAC
- Adreces IP
- L'ESSID de la xarxa

Si es filtra l'accés a la xarxa solament en aquells terminals que tinguin una adreça MAC o IP determinada, o bloquegem l'enviament dels anuncis *Beacon Frames*, l'usuari haurà de conèixer per endavant el valor ESSID per connectar-se a la xarxa.

Amb les mesures anteriors però, es pretén limitar l'accés no autoritzat al sistema, però malauradament no impedeix que algú intercepti i espiï les comunicacions.

3.1.3 Els atacs dels intrusos

A continuació veurem cóm els intrusos poden evitar les mesures enumerades al punt anterior i entendre cóm funcionen els mecanismes que utilitzen per accedir a la xarxa de manera il·lícita, silenciosa i sense coneixement de la víctima.

- **Trencar les ACL** (*Acces Control Lists*) basades en MAC.

  Una primera mesura de seguretat implementada en les xarxes sense fils és el filtrat de les connexions per l'adreça MAC. Per a això es configura una llista d'adreces MAC en el punt d'accés indicant si aquestes adreces disposen d'accés permès o denegat. Ara bé, la seguretat que proporciona aquesta mesura és nul·la, donada la senzillesa que comporta modificar l'adreça MAC de la nostra targeta per una altra vàlida prèviament obtinguda mitjançant un simple *sniffer*. Tot i que una xarxa amb dues adreces MAC repetides pot ocasionar problemes, l'intrús ho pot solucionar realitzant un atac de tipus *DoS* precisament a la màquina que ha utilitzat per a apoderar-se de la seva MAC.

- **Atac de Denegació de Servei** (*DoS*).

  L'objectiu és impedir la comunicació entre un terminal i un punt d'accés. Per aconseguir-lo, l'atacant s'atribueix el paper de l'AP apropiant-se de la seva adreça MAC, la qual haurà obtingut fàcilment amb un *sniffer*. A continuació, li negarà la comunicació al host o terminals escollits mitjançant l'enviament continuat de notificacions de dissociació.

- **Descobrir ESSID ocults.**

  L'ocultació de l'ESSID d'una xarxa és un mètode utilitzat per augmentar la seva invisibilitat i augmentar així les possibilitats de ser detectada per un atacant. En quasi tots els punts d'accés porten implementar l'opció de deshabilitar l'enviament de l'ESSID en els paquets o desactivar els anuncis que els AP's envien constantment a la xarxa (*Beacon Frames*).

  Tanmateix està demostrat que aquest mecanisme no resulta del tot efectiu, doncs davant d'aquesta mesura, un atacant tindria dues opcions:

  1. Rastrejar la xarxa amb un *sniffer* durant un temps indeterminat a l'espera de detectar d'una nova connexió a la xarxa. L'objectiu és aconseguir l'ESSID present en les trames *PROVE REQUEST* del host client que es generen en absència dels *Beacon Frames* desactivats.

  2. Provocar la desconnexió d'un client mitjançant el mateix mètode descrit en l'atac DoS, però sense mantenir al client desconnectat.

- **Atac ARP Poisoning.**

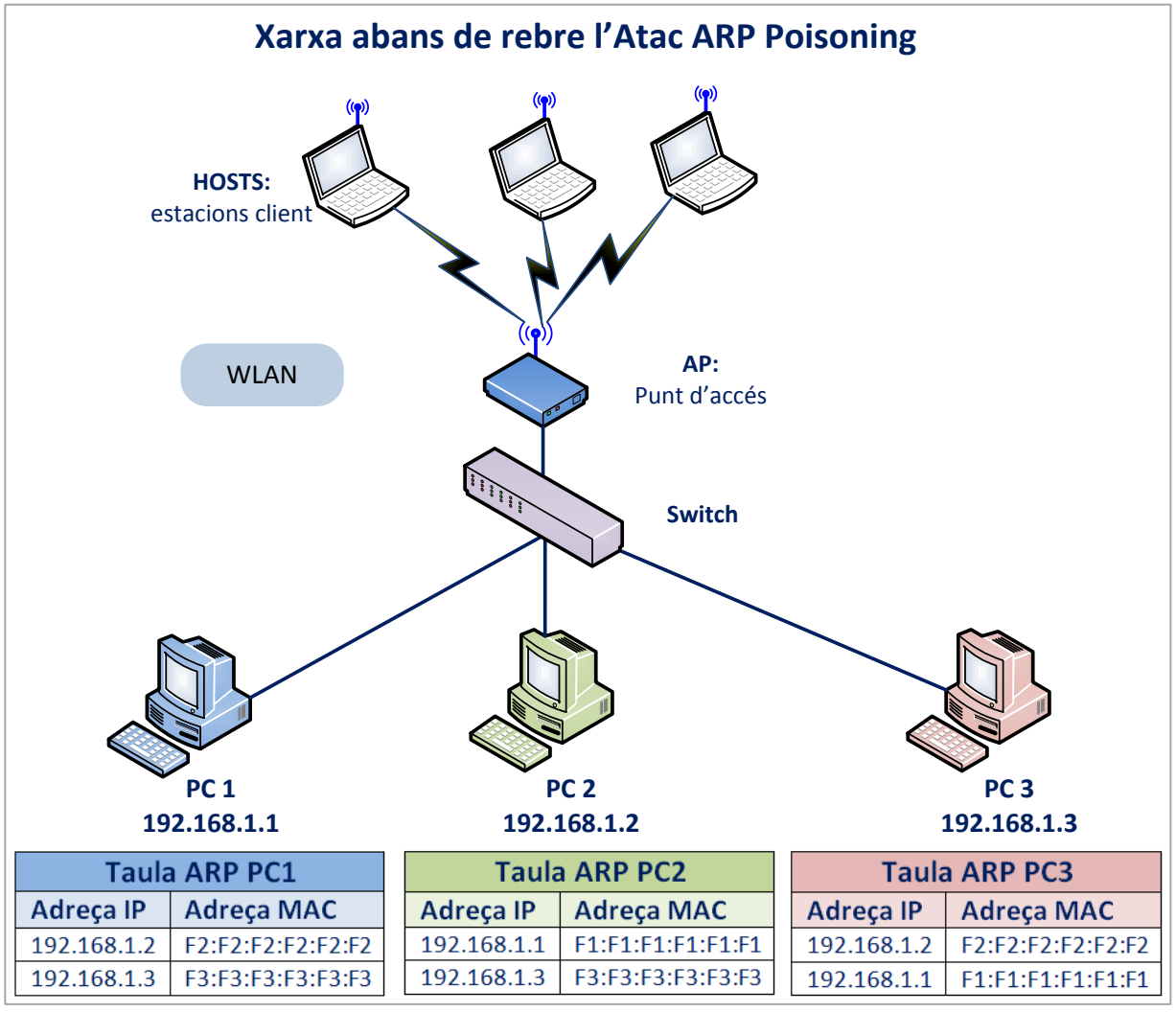
  El seu objectiu, al igual que l'atac Man in The Middle, és accedir al contingut de la comunicació entre dos terminals connectats mitjançant dispositius intel·ligents com per exemple un commutador (*switch*).

  Aquesta variant, altera la taula ARP (*Address Resolution Protocol*) que els equips de xarxa mantenen de manera *stateless,* això és, sense memòria d'estat. Recordem que la taula ARP d'un dispositiu equival a una memòria cau on s'emmagatzema la traducció d'adreces IP a adreces MAC realitzades pel protocol ARP.

  La figura 17 mostra la distribució típica d'una xarxa WLAN, on cada PC connectat al switch, implementa en la seva taula ARP les adreces IP i MAC dels altres PC's amb els que comparteix la xarxa. Les operacions que podria realitzar l'atacant es descriuen a continuació en dos passos:

  1. Enviar paquets *ARP REPLY* al PC 3 que contenen l'adreça IP del PC 1 però amb la MAC de l'atacant. Aquí és on es produeix el primer engany; doncs l'intrús aconsegueix modificar la taula ARP del PC 3.

  2. Realitzar la mateixa operació d'atac al PC 1 enviant-li informació falsa, la qual indica que l'adreça IP del PC 3, la té també la seva pròpia MAC. (Veure figura).



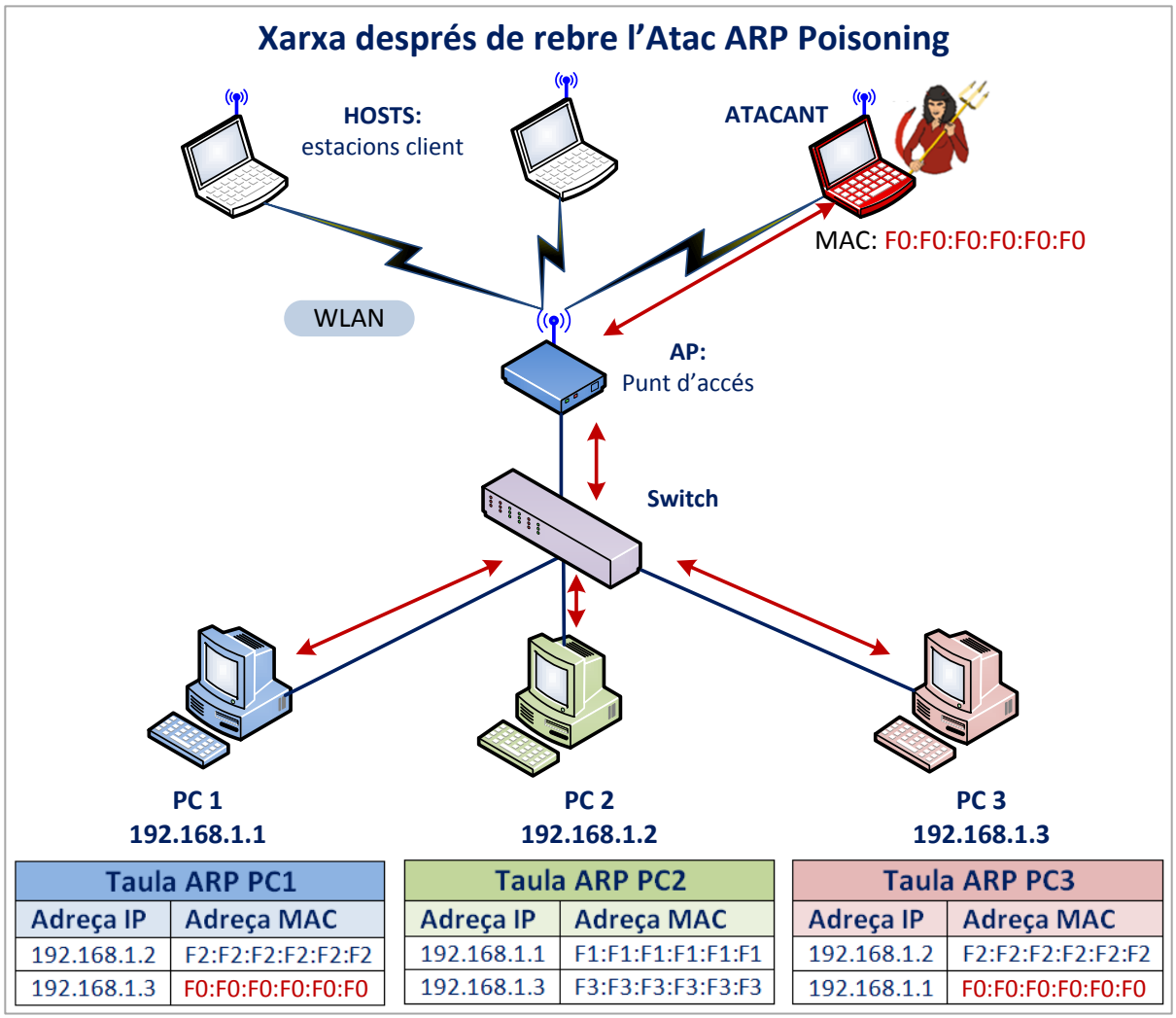
Taula ARP PC1	
Adreça IP	Adreça MAC
192.168.1.2	F2:F2:F2:F2:F2:F2
192.168.1.3	F3:F3:F3:F3:F3:F3

Taula ARP PC2	
Adreça IP	Adreça MAC
192.168.1.1	F1:F1:F1:F1:F1:F1
192.168.1.3	F3:F3:F3:F3:F3:F3

Taula ARP PC3	
Adreça IP	Adreça MAC
192.168.1.2	F2:F2:F2:F2:F2:F2
192.168.1.1	F1:F1:F1:F1:F1:F1

Esquema d'una xarxa WLAN abans de rebre un atac *ARP Poisoning* [13] Figura 17

L'esquema de la figura anterior, quedaria modificat després d'aquest atac de la següent manera:



Esquema de les taules ARP després de rebre un atac *ARP Poisoning.* [13] Figura 18

Com que el protocol ARP és *stateless* tal i com s'havia comentat abans, el PC1 i el PC3 actualitzen la seva taula d'acord a la informació que l'atacant ha enviat a la xarxa.

El switch i el punt d'accés formen part del mateix domini de broadcast, així que els paquets ARP circulen de la xarxa WLAN a la xarxa cablejada sense cap problema.

- **Atac Man in the Middle (*MitM*)**

Comentat anteriorment com un dels atacs típics de les xarxes sense fils, consisteix en que l'atacant es fa passar pel punt d'accés i actua com a tal , i al mateix temps, convenç a l'AP de que l'atacant és el host client.

Per aconseguir amb èxit aquest tipus d'atac, l'intrús necessita obtenir les següents dades amb l'ajuda d'un "*sniffer*".

1. L'ESSID de la xarxa (si està ocult utilitzarà el mètode descrit anteriorment)
2. L'adreça MAC del punt d'accés
3. L'adreça MAC del host víctima

Una vegada que l'intrús disposa de les dades anteriors, utilitzaria la mateixa metodologia que en l'atac de tipus DoS per trencar la connexió entre host client i l'AP. Posteriorment a aquesta ruptura, la targeta de xarxa del host client començarà a buscar un nou AP en altres canals, moment que

aprofitarà l'atacant per suplantar l'AP amb la seva MAC i ESSID en un canal diferent. Per a aquesta tasca l'atacant haurà de commutar la seva pròpia targeta a mode *master*.

Paral·lelament, l'atacant ha de suplantar la identitat del client amb l'AP real utilitzant l'adreça MAC del host client. D'aquesta manera, l'atacant pot col·locar-se entre els dos dispositius de forma transparent.

3.2 Mecanismes de seguretat

Durant l'estudi de l'estàndard 802.11 vam veure que per protegir les xarxes WiFi portava "de sèrie" el conegut i a la vegada poc efectiu protocol WEP. Tanmateix, va ser el responsable de forçar la revisió d'aquest estàndard per evolucionar finalment a altres més potents com els estàndards 802.11i i 802.1x, amb els quals, podem protegir la xarxa d'una manera més seriosa, això és, amb confidencialitat, integritat i autenticació.

En aquesta línia, també era necessari conèixer l'existència dels algoritmes WPA, WPA2 o la família de protocols EAP, per descobrir que treballant amb els estàndards 802.11i i 802.1x, formaven un front comú amb el que es podria donar una resposta efectiva a les amenaces que hem estudiat.

Però malauradament aquests mecanismes no són infal·libles. De la mateixa manera que estudiàvem el procés que portava a terme un atacant per transgredir la xarxa, ara veurem una mica més a fons el funcionament dels mecanismes de seguretat implementats en els estàndards anteriors, amb l'objectiu de comprendre no solament les seves fortaleses, sinó també les seves debilitats, que per descomptat, aprofiten els atacants.

3.2.1 Privacitat equivalent per cable (WEP)

Després d'analitzar els resultats obtinguts a l'apartat 3.1.1 i observar que un 30% de xarxes detectades a Espanya, encara utilitzen WEP com a mecanisme de seguretat, és obvi que el tema encara és prou important com per deixar-lo a banda.

Tal i com s'ha vist en el segon capítol WEP (*Wired Equivalent Privacy*) és un algoritme de seguretat que intentava oferir protecció a les xarxes sense fils i estava inclòs a la primera versió de l'estàndard IEEE 802.11. Posteriorment es va mantenir sense canvis en 802.11a i 802.11b per garantir la compatibilitat entre diferents fabricants.

Aquest sistema, utilitza l'algoritme RC4 per al xifrat de les claus que poden ser de 64 o 128 bits teòrics, tot i que en realitat són 40 o 104, ja que els 24 bits que falten s'utilitzen per al vector d'inicialització (IV). La seguretat que ofereix WEP, es basa en una clau secreta compartida per tots els usuaris que intervenen en la comunicació i es fa servir per xifrar les dades enviades. Tot i que no està establert així, la realitat és que els hosts i punts d'accés comparteixen la mateixa clau, fet que redueix el nivell de seguretat que pot oferir aquest mecanisme.

Per verificar la integritat s'aplica un algoritme de comprovació d'integritat (CRC-32) al text pla, de manera que s'obté un ICV o valor de comprovació d'integritat que és afegit al text xifrat. Així, el receptor del missatge pot verificar que la integritat d'aquest no ha estat alterada. El procés s'indica a continuació:

- **Generació de les claus**

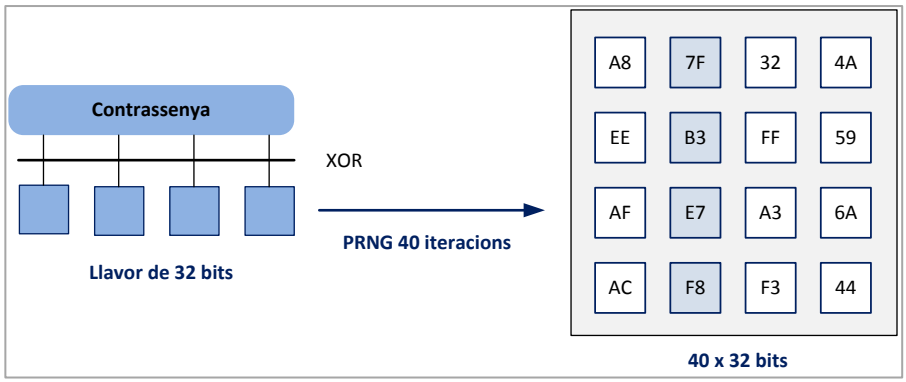
  Les claus, de 40 o 104 bits, es generen a partir d'una clau que pot ser generada automàticament o introduïda manualment. Aquesta clau, ha de ser coneguda per tots el comunicants. El problema és que normalment s'utilitzen claus molt senzilles i poc canviants. A partir d'aquesta clau, es generen 4 claus de 40 bits, de les quals s'utilitzarà una diferent cada vegada per realitzar el xifrat WEP. El procés per obtenir les claus a partir de la clau inicial, es basa en l'aplicació d'una operació XOR amb la cadena ASCII de la clau i de la qual s'obté una llavor de 32 bits. Per realitzar aquesta operació, es divideix la clau en grups de 4 bytes de la següent manera:

Clau d'exemple: "La clau WEP"

es divideix d'aquesta forma:

U O C _
C L A U
_ W E P

I de forma esquematitzada es pot representar a la figura següent:

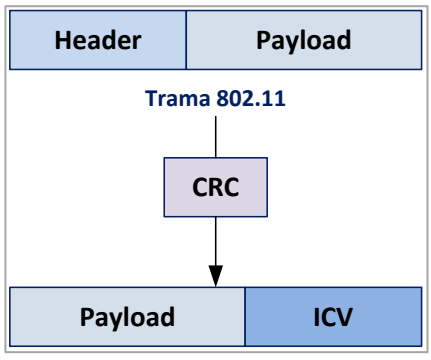


Esquema de la generació d'una clau WEP [13] Figura 19

S'executa l'operació XOR entre els elements de cada columna i d'aquesta manera obtenim la llavor de 32 bits. Aquesta llavor serà la que utilitzarà un generador de nombres pseudoaleatoris (**PRNG**) per generar 40 cadenes de 32 bits cadascuna. A partir d'un bit de cada una de les 40 cadenes, s'obtindran les 4 claus de 40 bits, i en cada cicle, una d'elles s'utilitzarà per realitzar el xifrat WEP.

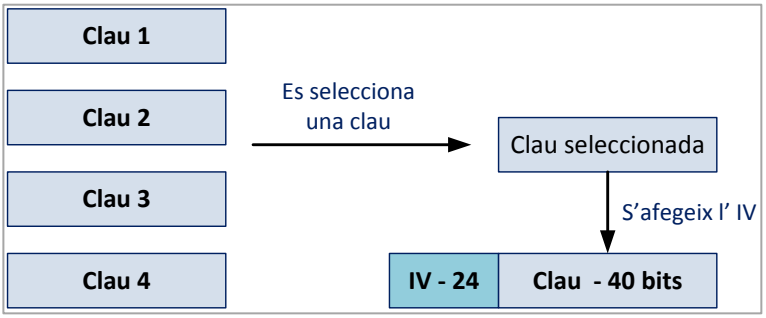
- **Xifrat**

  Obtingudes les claus, comença el procés per xifrar les trames, les quals, es componen bàsicament d'una capçalera (***Header***) i un contingut (***Payload***). Primerament es calcula el **CRC** (mecanisme de comprovació d'errors) del *payload* a xifrar. Recordem que, d'aquest procés, s'obtindrà el valor de verificació d'integritat (**ICV**: *Integrity Check Value*), el qual, s'afegirà al final de la trama xifrada, per a que el receptor pugui comprovar que no ha estat modificada.



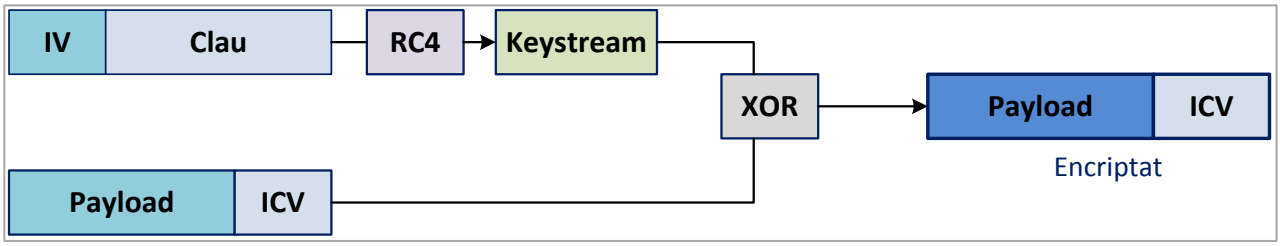
Creació de l'ICV durant el xifrat WEP Figura 20

Seguidament es selecciona una de les claus de 40 bits d'entre les 4 possibles i s'afegeix al Vector d'Inicialització al començament de la clau. El Vector d'Inicialització (IV), és un comptador que va canviant de valor a mesura que es generen trames, de manera que, quan s'afegeix a una clau, s'augmenta el número de "claus" possibles a utilitzar.



Implementació de l' IV a la clau seleccionada [13] Figura 21

Després es realitza el xifrat **RC4** al conjunt IV + clau per obtenir el *keystream* o fluxe de clau. Aquests *keystream*, s'utilitzarà per xifrar el conjunt *Payload* + ICV mitjançant una operació XOR.



Esquema d'obtenció del *Payload* encriptat. [13] Figura 22

Posteriorment, s'afegeix el conjunt [Payload Encriptat + ICV Encriptat] a la capçalera de la trama i a l'IV. S'obté finalment el paquet preparat per a ser enviat.

Paquet encriptat mitjançant WEP preparat per a ser enviat. [13] Figura 23

Acabem de veure el funcionament del mecanisme WEP alhora de construir un paquet d'informació encriptat. A continuació veurem un exemple d'atac a la seguretat WEP que posarà de manifest la seva ineficàcia i en conseqüència el risc que comporta el seu ús.

- Exemple d'atac al mecanisme WEP utilitzant l'Atac de força bruta:

Recordem que en criptografia, l'Atac de força bruta consisteix en recuperar la clau provant totes les combinacions possibles fins trobar aquella que permet l'accés.

Com que la llavor de 32 bits que s'utilitza amb el PRNG procedeix d'una contrasenya generalment formada per caràcters ASCII, podem deduir que el bit més alt de cada caràcter serà sempre zero doncs el rang de caràcters ASCII està comprès entre 00 i F7. Això és,

00 = 0000 0000
...
4F = 0100 0000
...
7F = 0111 1111

Per tant, si es realitza una operació XOR d'aquests bits, també és zero i les llavors solament es trobaran en el rang 00:00:00:00 fins a 7F:7F:7F:7F.

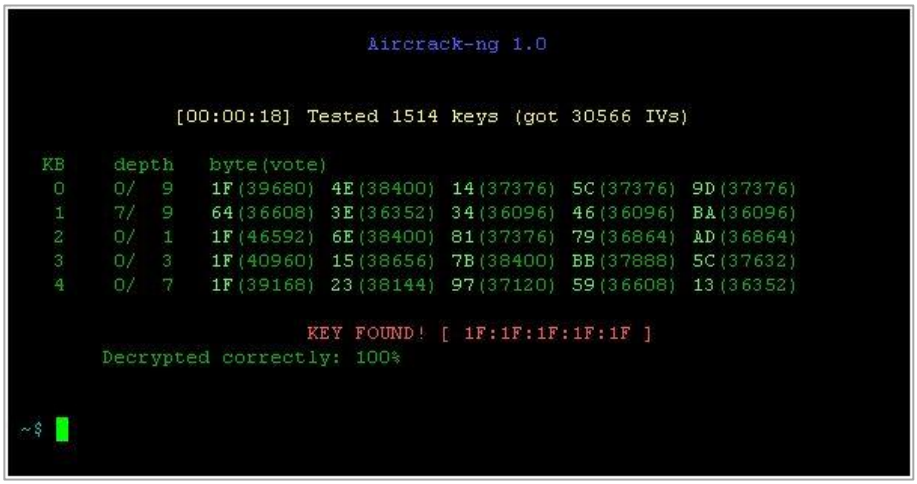
El problema és que el PRNG utilitzat és de tipus LGC (*Linear Congruential Generator*) i això comporta que els bits més baixos seran "menys aleatoris" que els bits més alts. En conseqüència, s'obté una longitud en

cada cicle de 2^{24} i per tant, solament les llavors que es trobin entre 00:00:00:00 i 00:FF:FF:FF produiran claus úniques.

Així doncs, les llavors només arribaran fins a 7F:7F:7F:7F i l'última que tindrà en compte el PRNG serà 00:FF:FF:FF. Al considerar aquest rang, l'entropia es redueix a 21 bits.
Amb aquesta informació, l'atacant redueix l'àmbit d'atac de força bruta considerablement i en conseqüència el temps necessari per produir totes les claus seqüencialment.

A més, també existeix la possibilitat d'utilitzar un diccionari per generar solament les llavors de les paraules o frases contingudes en el diccionari. Si la contrasenya utilitzada està al diccionari, l'atacant també aconseguiria reduir considerablement el temps dedicat per trobar-la.

A la figura inferior es mostra el resultat d'utilitzar l'eina anomenada *Aircrack*, la qual implementa les aplicacions necessàries per trobar fàcilment les claus WEP.



Trencament de clau mitjançant aplicació *Aircrack.* [14] Figura 24

Tot i que existeixen més atacs al mecanisme WEP, com per exemple *l'Atac Inductiu Arbaugh* o l'*Atac FMS*, el seu estudi queda fora de l'objectiu d'aquest treball, doncs el que s'intenta transmetre, és el risc que comporta utilitzar la seguretat WEP per protegir la xarxa i per tant gens recomanable.

3.2.2 Mecanismes WPA i WPA2

Els equips que emeten una senyal Wi-Fi, generalment permeten configurar a l'usuari o administrador de xarxa el protocol de seguretat amb el que es desitja transmetre, permetent així cobrir les dimensions de control d'accés, confidencialitat i en alguns casos autenticació. Quan al capítol 2 es parlava de l'estàndard 802.11i, van aparèixer els protocols WPA i WPA2 com elements de seguretat que van donar suport a la consolidació d'aquest estàndard.

Com a recordatori, WPA (Protecció d'Accés Wi-FI) és l'evolució directa de WEP i més robust. Fou dissenyat com a protocol d'autenticació per paliar les deficiències del xifrat WEP. Tot i que la seva longitud de clau es menor que la WEP, el seu mètode de xifrat és més sòlid i resistent.

Posteriorment es va desenvolupar l'estàndard de seguretat **WPA2** (Protecció d'Accés Wi-Fi versió 2). Aquest protocol ja es basava en el IEEE 802.11i i és considerat bastant segur per utilitzar l'algoritme AES, amb una resistencia a la seva ruptura bastant forta i complicada.

Per augmentar les prestacions de WPA2, es va desenvolupar la versió **WPA-PSK** (Protecció d'Accés amb Clau Pre-compartida). Aquesta opció de xifrat és de les més segures. Aquest mètode, es diferència de WPA2 en que existeix una clau compartida per tots els integrants de la xarxa prèviament a la comunicació, i des de que s'inicia la comunicació dels dispositius. La robustesa de la seguretat resideix precisament en el nivell de complexitat d'aquesta clau.

Podem diferenciar el tipus de protecció de la família WPA en dos grups principals:

- **WPA-Personal**: aquest mode, d'ús preferentment domèstic, permet implementar una infraestructura segura basada en WPA sense la necessitat d'utilitzar un servidor d'autenticació. Es basa en l'ús de la clau pre-compartida PSK comentada anteriorment i que s'emmagatzema en el punt d'accés i en els dispositius client. A diferència de WEP, no necessita la introducció de cap contrasenya de longitud pre-definida. El WPA permet a l'usuari introduir una frase de contrasenya. Posteriorment, un algoritme la converteix en PSK.

- **WPA-Enterprise**: és un mode que requereix la infraestructura d'autenticació 802.1x amb un servidor d'autenticació, (generalment un servidor RADIUS) i un punt d'accés. Destinat a xarxes empresarials.

Qualsevol d'aquests protocols de xifrat de dades i autenticació de xarxa, generalment es configuren en dos pasos:

1. Primerament es configura la clau en el punt d'accés i després en els dispositius que hauran d'utilitzar la xarxa. Més concretament, la configuració de l'AP es realitzarà generalment mitjançant una interfície web, posteriorment es configurarà la seguretat en els hosts sense fils i finalment s'escollirà el tipus de xifrat de seguretat desitjat.

   Per exemple, en WEP, (tot i que no és recomanable utilitzar aquest tipus de mecanisme), s'hauria d'escollir una clau de 5 o 13 caràcters, o bé, una clau de 10 o 26 dígits hexadecimals, depenent de si es vol una clau de 64 o 128 bits de longitud.
   En canvi, per a una clau de la família WPA, solament es necessita entre 8 i 63 caràcters o 64 digits hexadecimals.

2. En segon lloc, s'hauria de realitzar el mateix procediment en tots els dispositius que s'hagin de connectar a la xarxa, utilitzant exactament la mateixa configuració utilitzada en el punt d'accés.

Una de les millores que implementa WPA és, que a diferència de WEP, la clau compartida és eliminada. Per xifrar qualsevol paquet de dades en hosts clients i l'AP, s'utilitza un mecanisme de generació de clau dinàmica entre el host i l'AP. D'aquesta manera, per a cada sessió entre un dispositiu client i el punt d'accés, s'utilitza un parell de claus diferent als demés hosts, i com que aquest mecanisme és aleatori, els atacs que eren exitosos en WEP, aquí ja no resulten vàlids.

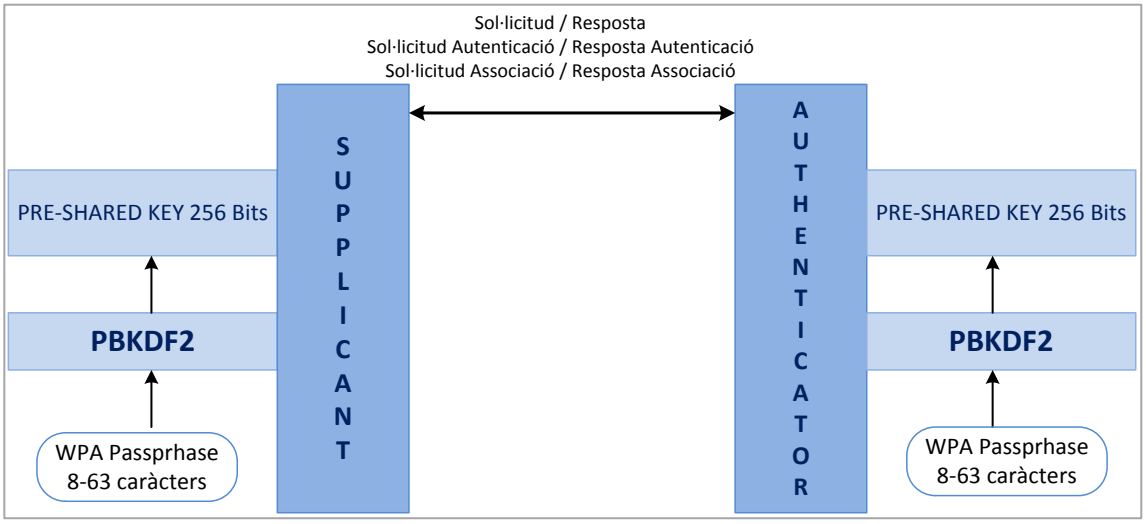
Ara bé, el realment interessant, és saber cóm es genera de manera dinàmica aquestes claus. Aquest procés, es porta a terme gràcies a l'algoritme **PBKDF2**, el qual permet la generació de la clau pre-compartida **PSK** (*Pre-Shared Key*) indicada anteriorment. Aquest algoritme, es basa en una clau d'entre 8 i 63 caràcters que s'estableix normalment en un AP amb protecció WPA i s'utilitza com a paràmetre per generar aleatòriament una nova PSK.

L'algoritme PBKDF2 implementa cinc paràmetres:

1. *Passphrase* (la clau de l'AP seleccionada pel administrador del router)
2. L'SSID
3. La longitud del SSID anterior
4. Nombre de vegades que el *passphrase* serà codificat (hashed) -> 4096
5. Longitud de la clau PSK (256)

Amb aquests paràmetres, l'algoritme genera una clau PSK de longitud 256 caràcters, la qual serà utilitzada per xifrar i desxifrar paquets de dades. Aquest mateix procediment es porta a terme tant en hosts clients (***Supplicant***) com en els punts d'accés (***Authenticator***).

Queda representat de manera esquemàtica a la figura següent:



Generació de Claus del mecanisme WPA-PSK [15] Figura 25

Fins a aquest punt solament tenim un parell de claus PSK que s'utilitzaran en el *Supplicant* i en l'*Authenticator*. A partir d'aquest moment, s'intercanviaran els paquets de dades entre les dues entitats utilitzant aquestes claus PSK. Aquest procés es coneix com ***4-Way Handshake*** i que es detalla a continuació en vuit passos:

1. L'Authenticator envia un missatge al supplicant amb un valor generat aleatòriament utilitzant la seva clau PSK, el qual, és simplement un valor arbitrari sense cap tipus de significat especial. Aquest missatge és conegut com ***Auhenticated nonce*** o simplement ***Anonce***.

2. Posteriorment, el supplicant rep el missatge i genera un altra missatge anomenat ***Snonce*** (Supplicant nonce), que és bàsicament del mateix tipus que el paquet Anonce rebut, però que conté un *nonce* diferent basat, en aquest cas, en un text arbitrari generat aleatòriament utilitzant la clau PSK del *supplicant*.

3. Amb la informació anterior, el supplicant crea el conegut ***PTK*** (*Pairwise Transient Key*). Aquest pas és precisament on radica la millora de WPA respecte a WEP; en la generació dinàmica de claus. Les PTK són les claus generades en cada paquet intercanviat entre el *supplicant* i l'*authenticator* utilitzant la clau PSK obtinguda al pas 1, de manera que finalment, obtenim les ***PMK*** (*Pairwise Master Key*). Així doncs, cada PMK és dinàmicament generada per les PSK del *supplicant* i l'*authenticator*.
4. La generació de la clau PTK és realitzada per la PMK, que utilitza una funció de generació aleatòria de claus PTK formada pels paràmetres:

    a. **PMK**, això és, la PSK generada pel *supplicant* i l'*authenticator* mitjançant l'algoritme PBKDF2.
    b. **Anonce**, el paquet generat per l'*authenticator* que conté un text aleatori xifrat amb la seva clau PSK.
    c. **Snonce**, el paquet generat pel *supplicant* que conté el text aleatori xifrat amb la seva clau PSK.
    d. **MAC de l'*authenticator***
    e. **MAC del *supplicant***

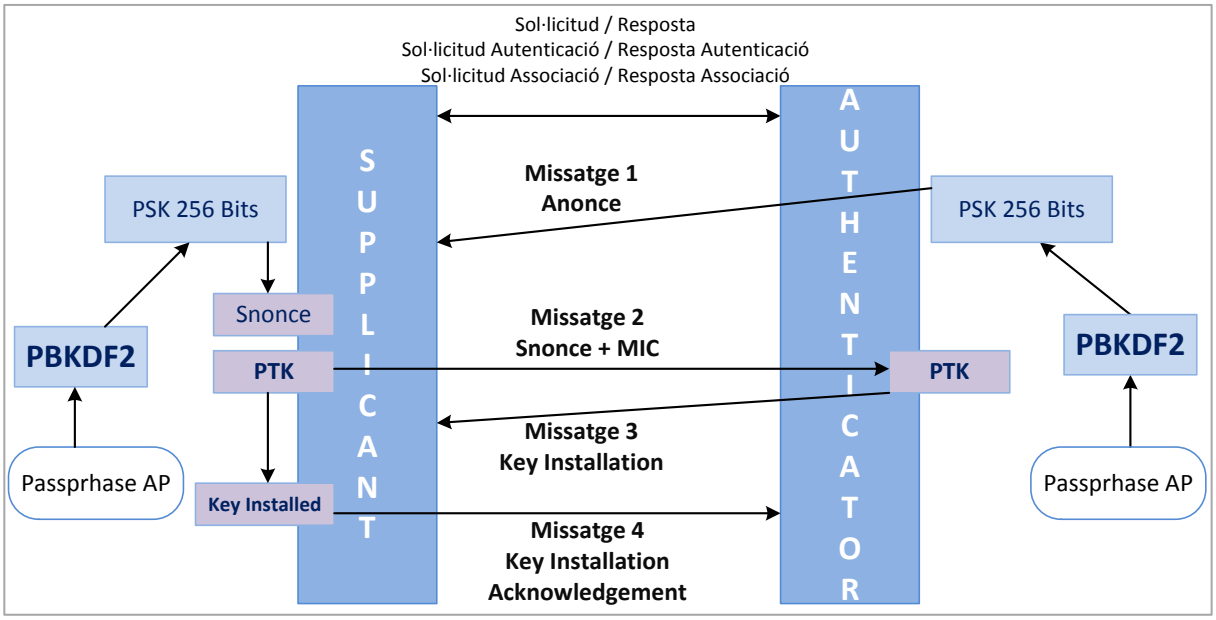
5. En aquest pas, el supplicant envia un paquet a l'*authenticator* amb el missatge Snonce i un camp ***MIC*** (Camp xifrat amb el mecanisme de xifrat *Michael*) que permet realitzar una verificació d'integritat i consistència del paquet. Aquest camp és generat pel supplicant utilitzant la PTK i la PMK.

6. Amb el paquet enviat al pas anterior pel *supplicant*, l'*authenticator* està en disposició de derivar la clau PTK, doncs coneix els camps necessaris per realitzar el càlcul, això és, el PMK (és el mateix per al *supplicant* i l'*authenticator*), l'Anonce, l'Snonce i les adreces MAC de l'*authenticator* i *supplicant*.

7. Quan l'*authenticator* genera la PTK amb els camps rebuts del paquet anterior (amb el camp Snonce), intenta generar el camp MIC, doncs compta amb la mateixa PTK i PSK que el *supplicant*. El MIC generat pel *authenticator* i el *supplicant* han de ser el mateix, en tal cas, envia un missatge al *supplicant* de tipus "**Key Installation**".
   Nota: si la verificació MIC falla perquè el valor calculat pel *authenticator* no coincideix amb el valor enviat pel *supplicant*, l'*authenticator* finalitza automàticament el procés enviant un paquet **DeAuthentication**.

8. Finalment, el *supplicant* envia a l'*authenticator* el missatge "**Key Install Acknowledgement**", com a confirmació de que en aquesta sessió d'intercanvi de paquets s'utilitzi la mateixa PTK generada en el client i l'AP. Aquest paquet, conté el camp "*Key ACK*" amb un valor de 0, indicant que és l'últim missatge enviat en el procés d'autenticació entre *supplicant* i l'*authenticator*.

Donat que tot el procés de lectura anterior respecte a l'autenticació entre *supplicant* i l'*authenticator* pot ser una mica dens, es representa esquemàticament en la següent figura:



Esquema d'autenticació entre *Supplicant* i *Authenticator* en WPA2 [15] Figura 26

Per regla general, els mètodes anteriorment descrits solucionen molts problemes de seguretat en termes de confidencialitat, integritat i autenticació, ja que són protocols que actúen a nivell d'enllaç i donen la possibilitat de treballar en xarxes sense fils equiparables a les xarxes cablejades.

Ara bé, dependre d'una clau compartida pot comportar un problema en el moment en què aquesta sigui coneguda (bé perque s'hagi difòs o perquè sigui coneguda per enginyeria social o adivinació). En aquest cas, les dimensions de seguretat anteriors deixaràn de ser segures.

Si tenim en compte que la longitud de la contrasenya WiFi determina el nivell de seguretat amb el que treballem, quina longitud és l'adequada?. Per donar una idea, podem dir que una contrasenya de 12 caràcters és segura i difícilment desxifrada amb el poder de còmput existent en les màquines comercials existents avui en dia, donat el temps exponencial necessari per *crackejar-la*.

Un *hash* WiFi tipus WPA, és el resultat de realitzar diverses operacions matemàtiques amb una contrasenya WiFi i que pot ser utilitzat per comprovar si la contrasenya és vàlida en un procés de cracking. Per intentar precisar una mica més el concepte de contrasenya més o menys segura, ens valdrem en l'equiparació d'un hash a una clau WiFi i realitzar les comparacions següents:

Una targeta gràfica potent d'ús domèstic proporciona un rendiment d'uns 350.000 *hashes* WPA o WPA2 per segon, és a dir, que és capaç de comprovar 350.000 contrasenyes en un segon. Un hardware FPGA comercial (dispositiu amb portes lògiques programable), pot aconseguir 1.750.000 *hashes* per segon.

Si la contrasenya és prou llarga i no està basada en paraules de diccionari o frases predictibles, serà impossible desxifrar la contrasenya WiFi, almenys en un temps prudencial.

D'una altra banda, també hem de tenir la següent consideració: si un atacant intercepta amb un *sniffer* WiFi el procés d'autenticació d'un usuari, (que s'anomenava *4 way handshake*), i aconsegueix *crackejar* la contrasenya o coneix la contrasenya WiFi, podria desxifrar el tràfic de qualsevol usuari connectat.

3.2.3 Autenticació amb 802.1x: els protocols EAP.

Recordem que l'estàndard 802.1x proporcionava el control d'accés a la xarxa basat en ports i el seu objectiu principal, és encapsular qualsevol protocol d'autenticació sobre els protocols de la capa d'enllaç de dades. En aquesta línia, 802.1x utilitza el protocol d'autenticació extensible (*EAP*) per autentificar a l'usuari de diverses maneres. Anem a veure cóm treballa l'estàndard 802.1x:

D'una banda tenim que l'IEEE 802.1.x defineix 3 entitats:

- El **sol·licitant** (*supplicant*), resideix en el host client
- L'**autenticador** (*authenticator*), que resideix en el punt d'accés
- El **servidor d'autenticació**, resident en un servidor AAA (*Authentication, Authorization & Accounting*) com el servidor RADIUS que s'ha vist anteriorment o també DIAMETER.

D'altra banda, el protocol EAP treballa amb quatre tipus de missatges:

- **Petició** (*Request Idetntity*), utilitzat per enviar missatges des de l'AP al host client.
- **Resposta** (*Identity Response*), utilitzat per enviar missatges de del host client a l'AP.
- **Èxit** (*Success*): emès pel AP i significa que l'accés està permès.
- **Fallada** (*Faillure*): enviat per l'AP al suplicant indicant que se li denega la connexió.

Una vegada es produeix l'associació, el procés d'autenticació és:

a) Enviament de l'*EAP-Request/Identity* des de l'autenticador al sol·licitant
b) El sol·licitant respon amb l'*EAP-Response/Identity* a l'autenticador, el qual li passa al Servidor d'Autenticació.
c) Es *tunelitza* el *Challenge/Response*. Si el resultat és afirmatiu, l'autenticador permetrà al sol·licitant l'accés a la xarxa, tot i que estarà condicionat a les directrius del Servidor d'Autenticació.

La filosofia de l'estàndard 802.1x, està basada en la denegació de qualsevol tràfic excepte el destinat al servidor d'autenticació mentre el client no s'autentiqui correctament. Per a aquesta tasca, l'autenticador crea un **port** per a cada client que defineix dos camins; un autoritzat i l'altra no. El primer camí estarà tancat fins que el servidor d'autenticació li comuniqui que el client té accés al camí autoritzat.

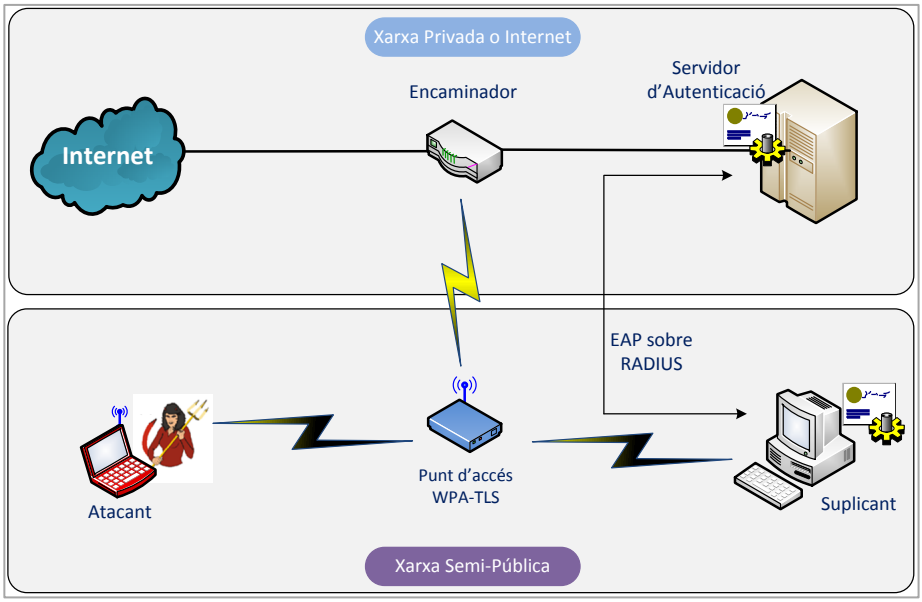
Així, quan el sol·licitant passa a estar actiu al medi, selecciona i s'associa a un punt d'accés. L'autenticador, que es localitza a l'AP, detecta la associació del host client i habilita un port per a ell, permetent únicament el tràfic 802.1x i la resta queda bloquejat.
El host client envia un missatge "*EAP Start*" i l'autenticador respon amb el missatge "*EAP Request Identity*" per obtenir la identitat del host client. Posteriorment es genera la resposta del sol·licitant "*EAP Response*" amb un identificador i l'autenticador ho reenvia vers al servidor d'autenticació.

A partir d'aquest moment, el sol·licitant i servidor d'autenticació es comuniquen directament, utilitzant un algoritme d'autenticació negociable. Si el servidor d'autenticació accepta l'autenticació, l'autenticador passa al port del host client a un estat autoritzat i el tràfic serà permès.

Els mètodes d'autenticació que veurem, *EAP-TLS, EAP-TTLS, PEAP* i *LEAP*, s'anomenen també protocols ***ULA*** (*Upper Layer Protocol*). Estan basats en el mètode d'infraestructura pública (***PKI***) i proporcionen un intercanvi d'autenticació entre host client i un servidor d'autenticació. Aquest procés es porta a terme mitjançant certificats digitals i per tant, és necessària l'existència d'una **Autoritat de Certificació** (CA), ja sigui empresarial o pública.

EAP-TLS
Necessita la possessió de certificats digitals per part del client i servidor d'autenticació. El procés d'autenticació, s'inicia amb l'enviament de la seva identificació (nom d'usuari) per part del sol·licitant vers als servidor d'autenticació. Posteriorment, el servidor envia el seu certificat al sol·licitant, que després de validar-lo, respon amb el seu propi.
Si el certificat del sol·licitant és vàlid, el servidor respon amb el nom d'usuari que havia rebut anteriorment i comença a generar la clau de xifrat, la qual, és enviada a l'AP pel servidor d'autenticació per a que s'iniciï la comunicació segura.

Tanmateix, en aquest procés existeixen algunes vulnerabilitats a tenir en compte. Per exemple, **en la fase d'identificació**, el host client envia el missatge *EAP-Identity* sense xifrar, permetent a un atacant veure la identitat del client que intenta connectar-se a la xarxa. De la mateixa manera, l'enviament de l'acceptació/denegació de la connexió es realitza sense xifrar, així que un possible atacant podria enviar aquest tipus de tràfic per a generar atacs de tipus DoS. La figura següent, mostra la infraestructura necessària per establir una xarxa basada en EAP-TLS amb un possible atacant.



Escenari d'una xarxa basada en el protocol EAP-TLS amb un possible atacant [16] Figura 27

Un altra inconvenient que comporta utilitzar EAP-TLS, és que, tant el servidor d'autenticació com els hosts clients, han de posseir el seu propi certificat digital i la distribució entre un gran nombre de clients, pot ser complicada i costosa.

PEAP (*Protected EAP*)
Per a corregir el problema anterior, es van crear **PEAP** (*Protected EAP*) que proporciona una autenticació basada en la contrasenya i solament el servidor d'autenticació necessitaria un certificat. Malauradament és vulnerable a l'atac *Man-in-the-middle*.

EAP-TTLS (*EAP-Tunneled TLS*)
És semblant al PEAP. Està implementat en alguns servidors RADIUS i en software dissenyat per a treballar amb xarxes sense fils 802.11. També és vulnerable a l'atac *Man-in-the-middle*.

LPEAP (*Lightweigh EAP*)
Protocol propietat de Cisco i dissenyat per oferir portabilitat entre diverses plataformes sense fils. La seva popularitat està justificada per haver estat el primer i l'únic mecanisme d'autenticació basat en contrasenya i amb cobertura a diferents clients segons els sistema operatiu.

El que es pretén amb aquests protocols és que, utilitzant el certificat del servidor prèviament validat, el host client pugui enviar les seves dades d'autenticació xifrades a través d'un túnel segur. A partir d'aquest moment, i posterior a la validació del sol·licitant per part del servidor, tots dos poden generar una clau de sessió.

3.2.4 Xarxes Privades Virtuals (VPN)

La comunicació a través d'una WiFi pública utilitzant una xarxa **VPN** (*Virtual Private Network*) garanteix que el tràfic generat es transmeti xifrat i dificulta a un possible intrús apoderar-se d'informació confidencial. Una VPN és una tecnologia de xarxa que s'utilitza per connectar un o més dispositius a una xarxa privada utilitzant Internet. Les empreses solen utilitzar una VPN per a que els seus empleats, des de els seus domicilis, hotels, etc. puguin accedir a recursos corporatius, que d'una altra manera, no seria possible.

La connexió de l'ordinador portàtil d'un empleat als recursos corporatius, és una funció específica d'una VPN. Per tant, és necessària una correcta implementació d'aquesta tecnologia per assegurar la confidencialitat i integritat de la informació. A continuació veurem alguns usos d'aquest tipus de xarxes i els seus protocols de xifrat.

A través d'una VPN circula informació privada i confidencial que, segons la intencionalitat d'un atacant, podria resultar molt perjudicial no solament per a un usuari particular, sinó també per a l'empresa. Aquest fet, s'agreuja encara més si l'empleat es connecta utilitzant una xarxa Wi-Fi pública sense cap tipus de protecció. Afortunadament, aquest problema es pot atenuar xifrant les dades que s'envien i es reben mitjançant els protocols següents:

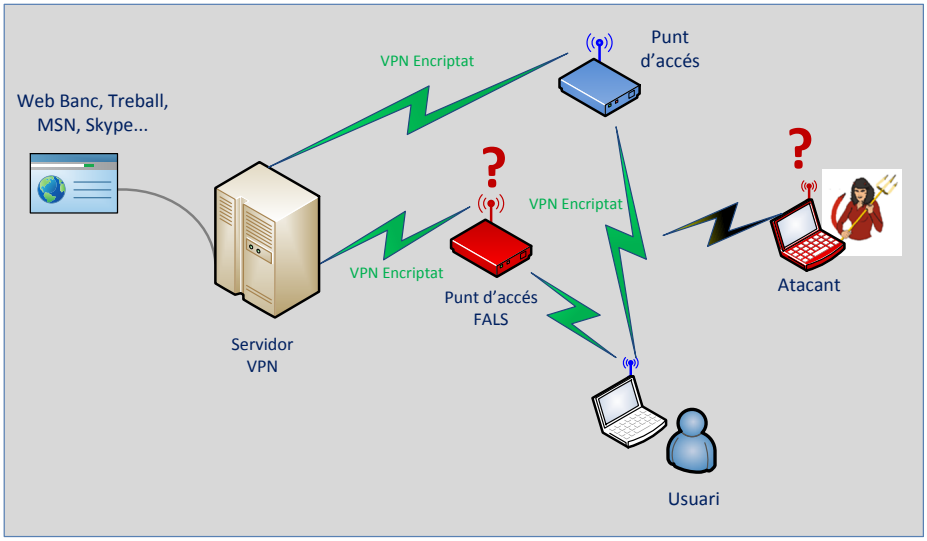
- **IPsec** (*Internet Protocol Security*): permet millorar la seguretat gràcies a algoritmes de xifrat potents i robustos, així com un sistema d'autenticació més exhaustiu. *IPsec* posseeix dos mètodes d'encriptat, mode de transport i mode túnel. Així mateix, suporta encriptat de 56 bits i 168 bits (triple DES).

- **PPTP/MPPE**: és una tecnologia desenvolupada per un consorci format per diverses empreses. Suporta diversos protocols VPN amb xifrat de 40 bits i 128 bits utilitzant el protocol *Microsoft Point Encryption*(MPPE). Ara bé, PPTP per sí sol no xifra la informació.

- **L2TP/IPsec** (L2TP sobre IPsec): tecnologia capaç de proveir el nivell de protecció d'IPsec sobre el protocol de túnel L2TP. Al igual que PPTP, L2TP no xifra la informació per sí mateix.

Així doncs, el xifrat de la informació que es transmet per una VPN es part de la seguretat que ofereix. Ara bé, és molt important que aquesta informació es mantingui íntegra en tot el seu recorregut. Per aconseguir aquest objectiu, *IPsec* utilitza un mecanisme dissenyat per detectar modificacions dintre d'un paquet i descartar-lo automàticament.

La figura inferior mostra l'escenari d'una xarxa basada en un servei VPN i un possible atacant on el tràfic entre el host de l'usuari i el servidor VPN està encriptat. Això significa que si l'atacant captura les dades durant qualsevol transmissió, no podrà esbrinar el seu contingut, degut a la encriptació que ofereix el servei VPN.



Xarxa VPN amb un atacant sense possibilitat de desxifrar la informació interceptada Figura 28

De la mateixa manera, l'AP fals (configurat per l'atacant), només veurà un conjunt de zeros i uns que no li aportarà cap informació. A més, l'intrús tampoc podrà realitzar un atac *Man-in-the-middle* contra la comunicació VPN de l'usuari degut a les proteccions existents en el protocol VPN.

Així doncs, protegir la confidencialitat i la integritat de la informació utilitzant una VPN és una bona mesura de seguretat per navegar en xarxes WiFi públiques i insegures, inclús si no es desitja accedir a cap recurs corporatiu.

3.2.5 Portals Captius

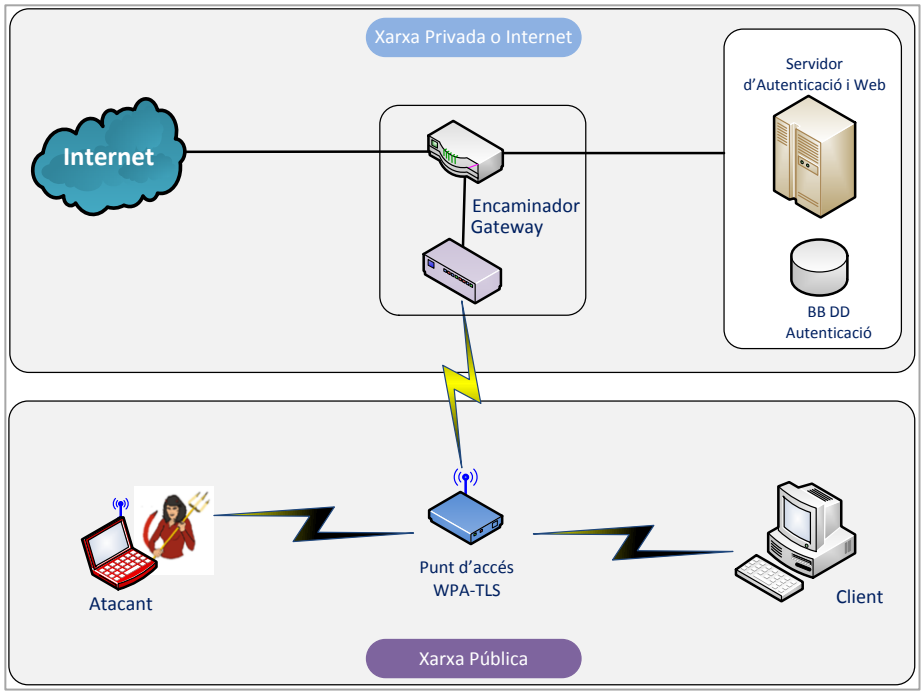
És un sistema creat per a permetre la validació d'usuaris en nodes sense fils. El seu ús proporciona connexió regulada als usuaris d'establiments públics, hotels, aeroports, etc. Es basa en un programa o un dispositiu informàtic integrat en una xarxa que vigila el tràfic http i força als usuaris, a pasar per una pàgina especial si volen navegar per internet.

Mitjançant un software, s'intercepta tot el tràfic http fins que l'usuari s'autentifica. El portal s'encarregarà de que la sessió caduqui després d'un temps determinat. També pot controlar l'ample de banda utilitzat per cada client.

En un sistema amb portal captiu, es defineixen dues parts ben diferenciades:

- **zona pública**: formada normalment per nodes sense fils que possibiliten la connexió de qualsevol terminal
- **zona privada:** accés normalment a Internet regulat per un sistema d'autenticació que impideix la naegació fins que l'usuari es valida.

A la figura inferior podem veure la infraestructura necessària per a un sistema de Portal Captiu:



Esquema d'un portal captiu amb possible atacant interceptant informació des d'AP [13] Figura 29

Un sistema de portals captius estan formats, en línies generals, d'una sèrie d'AP's connectats a un *Gateway*, un servidor web on resideix el portal i una base de dades on emmagatzemar els usuaris i el servei d'autenticació.

En el moment en què un usuari no autenticat decideix connectar-se a la zona privada, el *gateway* comprova si aquest usuari està autenticat.
Aquest procés està basat en la possessió de components lèxics (*token*) temporals gestionats per https. Si l'usuari no posseeix un *token* vàlid, el gateway adreça la connexió vers al portal on l'usuari haurà de ingressar un usuari i contrasenya vàlids per assignar-li un *token*. En el moment en què l'usuari disposi d'un *token* vàlid, el *gateway* permetrà la connexió a la zona privada.

Donades les característiques de la zona oberta dels sistemes que implanten aquest sistema de portals, està permesa l'associació amb el punt d'accés a qualsevol client, i el tràfic entre clients i l'AP, no està xifrat. Per tal motiu, un possible atacant podria capturar el tràfic de les connexions amb la zona privada.

D'una altra banda, també seria possible implementar atacs de tipus *spoofing* (simular una entitat distinta falsificant dades) o *hijacking* (robatori d'informació de manera il·legítima), a pesar de que el *token* que utilitza l'usuari legítim sigui vàlid.

Per acabar aquest capítol, s'ha elaborat la taula següent on es resumeix les amenaces en comunicacions WiFi que s'han vist i els impactes que aquestes poden produir. També s'indiquen les possibles solucions amb les seves vulnerabilitats.

Amenaces	Impactes	Possibles Solucions	Vulnerabilitats
Detecció i accés a la xarxa.	Localització de xarxes privades o empresarials per part d'atacants. Accés il·legítim a xarxes restringides per part d'usuaris no autoritzats. Informació potencialment compromesa.	a) Ocultació ESSID i evitar noms de xarxes relacionables amb identitats de particulars o de l'empresa. b) Filtrat de les connexions a la xarxa a través d'una llista amb les adreces *MAC* dels clients autoritzats (*ACL*)	a) L'ocultació del ESSID no evita la detecció de la xarxa. Els atacants aconsegueixen l'ESSID analitzant les trames *Probe Requests* mitjançant *sniffers*. b) Trencament de les *ACL* fàcilment. L'intrús s'apodera d'una adreça MAC vàlida amb un *sniffer* i se l'assigna a ell mateix.
Man-in-the-Middle (*MitM*)	Llegir, inserir, modificar informació de manera silenciosa i il·legítima.	Evitar accedir a xarxes públiques obertes. a) Establir comunicació a través de xarxes dotades amb mecanismes de xifrat; WEP, WPA, WPA-PSK b) Control d'accés a la xarxa amb autenticació 802.1x c) Efectuar comunicacions a través de xarxes VPN	a) La seguretat WEP és molt dèbil, amb claus fàcilment vulnerables a atacs de força bruta. b) Protocols d'autenticació vulnerables en la fase d'identificació del host client. (Per exemple WPA-TLS) c) Connexió a VPN's a través de xarxes obertes o sense xifrat
Jamming (interferències)	Denegació de servei a clients pròxims a l'atacant per interferències intencionades	Evitar xarxes públiques a l'aire lliure	
Atac *ARP Poisoning*	Atacant modifica taules ARP del client legítim interceptant la seva comunicació entre altres hosts.	Configuració de *gateways*, *firewalls* o commutadors intel·ligents amb l'opció de prevenció d'ARP *Spoofing* activada.	Configuració deficient des dispositius de xarxa o desconeixement de l'opció esmentada per part de l'administrador.

Amenaces	Impactes	Possibles Solucions	Vulnerabilitats
Phishing	Obtenció d'informació confidencial de forma enganyosa i fraudulenta	Evitar l'accés a enllaços procedents d'entitats desconegudes. Assegurar que s'està accedint a webs segures *https* i introduir manualment l'url sospitós en cas de dubte.	Actitud poc segura i excés de confiança per part de l'usuari. Atacants elaboren escenaris fraudulents que simulen situacions fàcilment creïbles o suplanten pàgines web aparentment segures.
Atac força bruta	Descobriment de contrasenyes i accés a la xarxa il·legítimament	Evitar xarxes amb mecanismes WEP. a) Navegar sota mecanismes de seguretat WPA, WPA-PSK o WPA-Enterprise dotats de contrasenyes segures i de longitud superior a 8 caràcters.	a) Contrasenyes poc segures, curtes, predicibles o accessibles.
Eavesdropping	Pèrdua de confidencialitat per "escoltar" secretament informació il·legítima sense arribar a modificar-la.	a) Realitzar comunicacions amb xarxes VPN i dades xifrades amb protocols IPsec per exemple. b) Utilitzar Portals Captius amb *tokens* exclusius d'accés a usuaris	a) Perill d'una deficient configuració de la xarxa VPN. Connexió a VPN's a través de xarxes obertes o sense xifrat de dades. b) Portals Captius amb associació client-AP sense xifrar, permet a l'atacant capturar el tràfic de les connexions a la zona privada. Són vulnerables a atacs *spoofing* o *hijacking*.

Resum dels atacs, impactes i solucions amb les seves possibles vulnerabilitats Taula 1

Capítol 4: Comunicacions WiFi més segures

Arribats a aquesta part del treball, disposem de la informació suficient per relacionar la seguretat en xarxes WiFi amb els estàndards 802.11i i 802.1x, i per tant, seria lògic que qualsevol administrador o tècnic de xarxes exigeixin instal·lacions amb dispositius capaços de treballar amb els mecanismes de seguretat més exigents que aquestes normes poden oferir.

De igual forma, s'ha vist que els usuaris de xarxes WiFi, haurien d'evitar connexions a punts d'accés de dubtosa procedència i exigir una comunicació amb un mínim de garanties que li permetin autenticar-se i mantenir la integritat i confidencialitat de les seves dades.

En qualsevol cas, a part de conèixer els mecanismes de seguretat que ens brinda la tecnologia en un dispositiu de comunicació, és imprescindible donar un pas més enllà a la nostra visió de seguretat, això és, com un conjunt d'actituds i hàbits que juguen un paper importantíssim alhora de consolidar un alt nivell de seguretat en una comunicació. És evident que no podem evitar l'atac d'algun intrús, però si que està en les nostres mans la possibilitat de dificultar els seus moviments per evitar que aquest atac acabi amb èxit.

A continuació, presentaré una sèrie de recomanacions que els administradors i usuaris d'una xarxa sense fils no solament haurien de practicar, sinó també fomentar, doncs es tracta d'un procés de seguretat global, que tal i com havia comentat anteriorment, comença en la sensibilització del propi usuari. Es veuran alguns consells importants que ajudaran als clients de xarxes WiFi, a configurar correctament el seu punt d'accés i el host de connexió per aconseguir una navegació segura i prevenir possibles atacs. També s'enumeraran algunes accions preventives destinades tant per a l'àmbit domèstic o personal com per a l'empresarial.

Posteriorment, i mitjançant un escàner WiFi des d'un edifici de la província de Tarragona, es mostraran un conjunt de punts d'accés detectats i s'analitzaran els mecanismes de seguretat que tenen activats, així com altres aspectes tècnics que ens donaran una idea dels mecanismes de seguretat que es configuren actualment.

Finalment es redactaran un conjunt d'indicacions que un administrador de xarxa hauria de tenir present a l'hora d'elaborar les polítiques de seguretat per prevenir intrusions.

4.1 Recomanacions generals per protegir la xarxa WiFi

A continuació veurem una sèrie de recomanacions tècniques i operatives que permetran comprendre els conceptes necessaris per protegir la xarxa WiFi i evitar, en la mesura possible, la seva vulneració per un intrús.

- **Estàndard WEP**
  Evitar que la seguretat de la nostra xarxa es fonamenti en el protocol WEP. Ja hem vist que utilitza un sistema de xifrat fàcil de trencar en pocs segons. Per tant, el seu ús no és recomanable donada la inseguretat que aporta i s'hauria de substituir per altres més robusts.

- **TKIP o AES CCMP**
  Al capítol 2 es va presentar a l'estàndard 802.11 el protocol WPA que utilitzava l'algoritme TKIP per realitzar la firma, mentre que WPA2 utilitza l'algoritme AES CCMP molt més robust i elimina fallades de seguretat dels anteriors. És aconsellable doncs, prescindir del suport TKIP, però si no és possible, es farà servir contrasenyes segures d'almenys 12 caràcters.

- **Nom de la xarxa WiFi**
  També hem estudiat que l'algoritme de xifrat WPA o WPA2 utilitza el nom de la xarxa WiFi (*SSID*) per generar la clau criptogràfica. Si volem evitar ser víctimes d'un atac de *cracking* mitjançant *taules rainbow* (trencament de contrasenyes xifrades amb una funció hash), s'ha d'evitar utilitzar una identificació de xarxa coneguda o amb el nom per defecte, per exemple WLAN_14. El més adequat és implementar un nom que no identifiqui l'empresa o usuari, per exemple WLAN_1F5JB.

- **Xarxa publicada**
  Sabem que la majoria de dispositius basats en tecnologia WiFi, pregunten periòdicament al seu voltant la llista de xarxes conegudes, sol·licitant aquesta informació a través de l'aire. Aquesta consulta es realitzava mitjançant l'enviament d'un paquet conegut com a *Probe Request*. Si un usuari configura incorrectament la xarxa WiFi i utilitza el nom de la xarxa com a contrasenya, qualsevol que estigui escoltant amb un escàner WiFi podrà veure la contrasenya de la xarxa sol·licitada a través del dispositiu de l'usuari.

- **Contrasenya d'administració**
  Normalment en l'àmbit domèstic, el punt d'accés WiFi té integrada la funcionalitat d'un encaminador per cable. Aquests dispositius poden estar configurats amb un nom d'usuari i una contrasenya d'administració remota, com per exemple *admin/admin*, *1234/ 1234* ..., i accessibles des d'Internet a través d'HTTP amb un navegador web. És important modificar la contrasenya d'administració per una altra alfanumèrica, i limitar l'accés al panel d'administració de l'encaminador des d'altres xarxes com Internet. Això evitarà que un atacant pugui obtenir la contrasenya WiFi aprofitant aquesta fallada de configuració i accedir al control de la nostra xarxa.

- **PIN WPS** (*Wireless Protected Setup*)
  També és molt habitual que els encaminadors WiFi incloguin el suport de la funcionalitat WPS per facilitar l'intercanvi de claus entre el punt d'accés i l'usuari sense la necessitat d'utilitzar la contrasenya WiFi. Aquest procés podria ser utilitzat maliciosament amb eines d'atac com *Reaver* o *Wpscrack*, de manera que l'intrús podria aconseguir la clau d'accés a la xarxa WiFi independentment de la seva longitud o complexitat. Per tant, seria recomanable inhabilitar la funcionalitat WPS si el dispositiu la té implementada.

- **Ocultació del SSID**
  Fa uns anys que els principals fabricants de punts d'accés permeten configurar la no emissió del nombre de les xarxes WiFi que publiquen. Però ocultar l'SSID només ofereix una capa de "Seguretat per ocultació", i en el moment en que existeix un firmware vulnerable o al menys un client que utilitza aquesta xarxa, el nom de la xarxa WiFi oculta es podria obtenir.

- **Intercepció de comunicacions**
  Si un intrús, intercepta amb un *sniffer* el procés d'autenticació d'un host client, (recordem que s'anomenava *4 way handshake*), i aconsegueix *crackejar* la contrasenya o, simplement la coneix, podria desxifrar el tràfic de qualsevol usuari legítim que es connecti a la xarxa. Per aquesta raó, WPA i WPA2 s'haurien d'utilitzar solament en entorns domèstics, ja que probablement la resta d'usuaris no van a espiar les comunicacions dels altres.

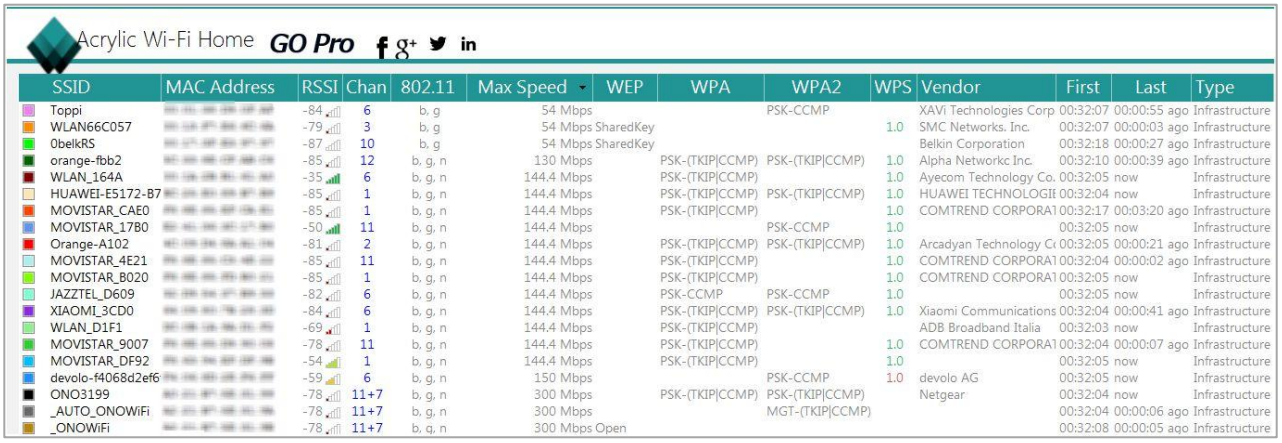
Després de veure les recomanacions tècniques anteriors, s'analitzarà i reflexionarà sobre la seguretat implementada en un conjunt real de xarxes WiFi que han estat detectades mitjançant l'aplicació *Acrylic*. Donat que aquestes xarxes són reals i han estat detectades a través d'un router sense fils d'un edifici del centre de Tarragona, he cregut convenient esborrar les adreces MAC.

Amb aquesta aplicació gratuïta, podem veure principalment l'SSID de les xarxes detectades, les adreces MAC, el nivell de potència rebuda (RSSI), estàndards suportats de la norma 802.11 (b,g,n), velocitat màxima i tipus de seguretat aplicada en (WEP, WPA o WPA2).

És interessant comprovar que la funcionalitat anteriorment comentada, WPS, està activada en tots els AP's (valor 1.0 en color verd) excepte un sol que està en color vermell. He de reconèixer que la meva pròpia xarxa la té activada.

També s'ha de dir que la versió d'Acrylic utilitzada és gratuïta, però existeix una altra versió més potent amb la que es podria esbrinar la contrasenya del encaminador d'accés. [17]

Vegem els resultats obtinguts:



SSID	MAC Address	RSSI	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Vendor	First	Last	Type
Toppi		-84	6	b, g	54 Mbps			PSK-CCMP		XAVi Technologies Corp	00:32:07	00:00:55 ago	Infrastructure
WLAN66C057		-79	3	b, g	54 Mbps	SharedKey			1.0	SMC Networks, Inc.	00:32:07	00:00:03 ago	Infrastructure
0belkRS		-87	10	b, g	54 Mbps	SharedKey				Belkin Corporation	00:32:18	00:00:27 ago	Infrastructure
orange-fbb2		-85	12	b, g, n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0	Alpha Networkc Inc.	00:32:10	00:00:39 ago	Infrastructure
WLAN_164A		-35	6	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)		1.0	Ayecom Technology Co.	00:32:05	now	Infrastructure
HUAWEI-E5172-B7		-85	1	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0	HUAWEI TECHNOLOGII	00:32:04	now	Infrastructure
MOVISTAR_CAE0		-85	1	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)		1.0	COMTREND CORPORA1	00:32:17	00:03:20 ago	Infrastructure
MOVISTAR_17B0		-50	11	b, g, n	144.4 Mbps			PSK-CCMP	1.0		00:32:05	now	Infrastructure
Orange-A102		-81	2	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0	Arcadyan Technology C	00:32:05	00:00:21 ago	Infrastructure
MOVISTAR_4E21		-85	11	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)		1.0	COMTREND CORPORA1	00:32:04	00:00:02 ago	Infrastructure
MOVISTAR_B020		-85	1	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)		1.0	COMTREND CORPORA1	00:32:05	now	Infrastructure
JAZZTEL_D609		-82	6	b, g, n	144.4 Mbps		PSK-CCMP	PSK-CCMP	1.0		00:32:05	now	Infrastructure
XIAOMI_3CD0		-84	6	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0	Xiaomi Communications	00:32:04	00:00:41 ago	Infrastructure
WLAN_D1F1		-69	1	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)			ADB Broadband Italia	00:32:03	now	Infrastructure
MOVISTAR_9007		-78	11	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)		1.0	COMTREND CORPORA1	00:32:04	00:00:07 ago	Infrastructure
MOVISTAR_DF92		-54	1	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)		1.0		00:32:05	now	Infrastructure
devolo-f4068d2ef6		-59	6	b, g, n	150 Mbps			PSK-CCMP	1.0	devolo AG	00:32:05	now	Infrastructure
ONO3199		-78	11+7	b, g, n	300 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)		Netgear	00:32:04	now	Infrastructure
_AUTO_ONOWiFi		-78	11+7	b, g, n	300 Mbps			MGT-(TKIP|CCMP)			00:32:04	00:00:06 ago	Infrastructure
_ONOWiFi		-78	11+7	b, g, n	300 Mbps	Open					00:32:08	00:00:05 ago	Infrastructure

Xarxes WiFi detectades mitjançant l'aplicació *Acrylic* Figura 30

Resulta interessant observar que un 35% de dispositius WiFi implementen mecanismes de tipus WPA, seguit de WPA2 amb un 50% i la resta, amb WEP o oberta un 15%. Podem veure que molt pocs dispositius prescindeixen del mecanisme TKIP, tal i com s'ha recomanat anteriorment.

Per acabar aquest punt, es presenta un quadre resum amb els problemes o errors més habituals en la seguretat WiFi en els entorns més típics on es produeixen, enumerant, per a cada problema, algunes recomanacions per solucionar-los, o almenys, intentar evitar-los.

Àmbits d'aplicació	Problema	Recomanacions resolutives
Privat / domèstic	Debilitat de la seguretat WiFi basada en WEP fàcilment desxifrable.	✓ Evitar la seguretat de la xarxa WiFi basada en el mecanisme WEP. ✓ Configurar dispositius d'accés preferiblement amb algoritmes WPA2. ✓ Implementar contrasenyes d'accés de 20 caràcters com a mínim.
General	Debilitat de la seguretat WiFi basada en WPA-TKIP poc robusta.	✓ Tot i que millora el xifrat WEP, no es recomana la seva utilització. ✓ Configurar els dispositius WiFi amb el tipus de xifrat WPA-AES. Utilitza algoritmes de xifratge molt robustos (*AES*).
General	Nom d'identificació de la xarxa predicible, conegut o per defecte que facilita l'atac *cracking* d'un intrús.	✓ Implementar noms de xarxes irrecognoscibles o no relacionables amb l'usuari o empresa.
General	Configurar la contrasenya de l'encaminador amb el nom de la xarxa es detectable per un intrús amb un *sniffer.*	✓ No utilitzar mai el nom de la xarxa com a contrasenya d'accés.
Privat / domèstic	Mantenir la contrasenya d'administració del encaminador per defecte.	✓ Modificar la contrasenya d'accés a la configuració de l'encaminador per una altre alfanumèrica.
General	Funcionalitat WPS activada facilita al intrús la clau d'accés a la xarxa WiFi.	✓ Deshabilitar l'opció WPS si el dispositiu la implementa.
General	Ocultar l'SSID de xarxa no la fa invisible a un atacant.	✓ Recomanable si el que es vol és únicament augmentar la seguretat de la xarxa per ocultació.
Empresarial	Intercepció de les comunicacions amb seguretat WPA / WPA2 durant el procés d'autenticació AP-client.	✓ Prescindir d'aquest mecanismes de seguretat. Utilitzar mètodes d'autenticació més robusts basats en *WPA-Enterprise* amb servidors *Radius* o IEEE 802.1x.

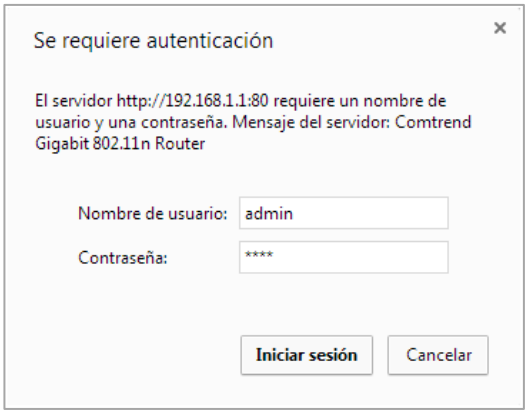
Problemes de seguretat WiFi i possibles solucions Taula 2

4.1.1 Configuració d'una xarxa WiFi segura

Al començament del capítol, es comentava que la seguretat d'una xarxa no es consolida únicament amb la utilització de dispositius que implementin mecanismes de seguretat molt robusts. La part tècnica s'ha de complementar amb l'actitud de l'usuari, el qual ha d'estar conscienciat de les amenaces existents en transmissions WiFi i actuar en conseqüència. En aquest sentit, hi han milions d'usuaris que es connecten a la xarxa des de la seva llar mitjançant un encaminador/AP WiFi, la configuració del qual acostuma a ser la que deixa l'instal·lador per defecte. Per aquest motiu, és molt important conèixer amb quina configuració de seguretat s'està treballant i modificar-la, si és necessari, per a aconseguir la màxima seguretat possible.

- **Configuració d'un encaminador privat o domèstic**

Una vegada establerta la xarxa sense fils, l'usuari ha de connectar-se a l'encaminador WiFi. Generalment és accessible a través del navegador introduint l'adreça de xarxa interna http://192.168.X.X. Apareixerà una pantalla semblant a la de la figura, en la que serà necessari autenticar-se:



Accés a un encaminador WiFi amb autenticació Figura 31

Una vegada introduïdes correctament les credencials, que generalment estan indicades al manual de l'encaminador, s'accedirà a un portal de configuració exemplificat a la figura 32.

Portal d'inici d'un encaminador WiFi Figura 32

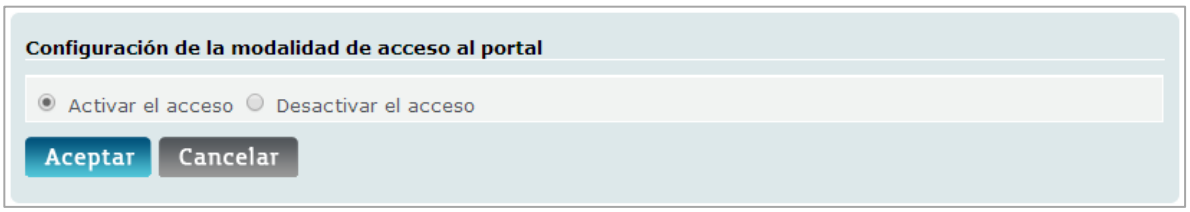
A continuació seguirem els següents passos:

1. **MODIFICAR LES CREDENCIALS D'ACCÉS AL PORTAL DE L'ENCAMINADOR**
   El primer pas és modificar la clau d'accés de configuració de l'encaminador. Pensem que una persona aliena podria conèixer aquestes dades per defecte, doncs tal i com s'ha comentat en punts anteriors, es localitzen en els manuals de la majoria de fabricants i per tant, a l'abast de tothom; per exemple són típiques (*1234/1234*, *admin/admin* etc.). Si un intrús introdueix aquestes credencials, és probable que accedeixi a la configuració de la nostra xarxa. Així doncs, és recomanable implementar una nova contrasenya alfanumèrica.

Captura de pantalla de configuració "Canvi de contrasenya" Figura 33

2. ACTIVAR L'ACCÉS AL PORTAL DE CONFIGURACIÓ AMB CREDENCIALS

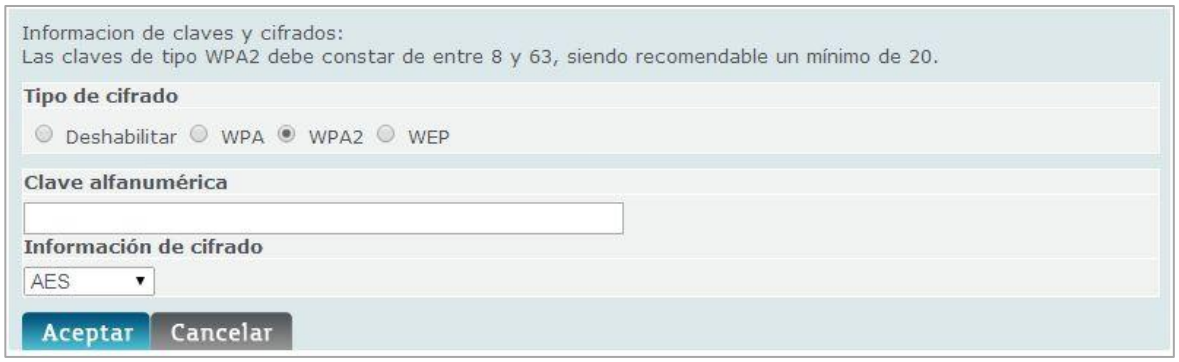
No oblidarem habilitar l'opció d'accés al portal de configuració de l'encaminador sota la sol·licitud de contrasenya.



Captura de pantalla de configuració "Accés al portal mitjançant contrasenya" Figura 34

3. CONFIGURACIÓ DEL TIPUS DE XIFRAT DE LA XARXA

Després d'haver vist els mecanismes de seguretat que ens ofereix actualment els l'estàndard 802.11i, no hauríem de dubtar a l'hora de seleccionar el màxim nivell de protecció que l'encaminador pugui suportar. En aquesta línia, és aconsellable configurar la xarxa per a que utilitzi el xifrat WPA2 amb encriptació AES. D'aquesta forma, les dades que circulen per la xarxa seran il·legibles per possibles tercers que estiguin escanejant informació. S'ha de tenir clar que WPA o WEP i TKIP són més insegurs i solament s'haurien d'habilitar en cas de no disposar d'una altra opció.



Captura de pantalla durant la configuració del tipus de xifrat de l'encaminador Figura 35

Després d'aplicar aquestes configuracions l'usuari haurà modificat radicalment la seguretat de la seva xarxa sense fils, minimitzant les probabilitats de que un intrús la vulneri amb fins maliciosos. Ara bé, a part del nivell de xifrat escollit i la protecció amb contrasenya, és convenient tenir en compte certes mesures de seguretat una mica més avançades que es poden aplicar en una xarxa WiFi. S'ha de dir també, que aquestes recomanacions poden estar limitades al model d'encaminador.

- **CONFIGURACIÓ DEL FIREWALL:** si l'encaminador ho permet, és possible definir quins serveis i ports poden estar disponibles per a l'accés extern a la xarxa.

Captura de pantalla de configuració de ports de l'encaminador Figura 36

- **ACCÉS AL ROUTER A TRAVÉS DE HTTPS:** també seria recomanable habilitar la configuració l'encaminador a través del protocol segur HTTPS, per evitar que un atacant intercepti la contrasenya d'accés a la configuració.

- **OCULTACIÓ DE L'SSID DE LA XARXA:** l'usuari hauria de modificar l'SSID per un nombre alfanumèric sense cap significat concret, de manera que no permeti relacionar aquest SSID amb l'usuari o ubicació per exemple. Ocultar la identificació de la xarxa, també és una opció comentada en apartats anteriors. Això donaria certa invisibilitat a l'hora de ser detectada per altres usuaris propers que busquin xarxes sense fils disponibles. En qualsevol cas, sabem que per a un atacant amb un mínim de recursos la detectaria igualment.

Captura de pantalla amb l'opció d'ocultat de l'SSID de l'encaminador seleccionada Figura 37

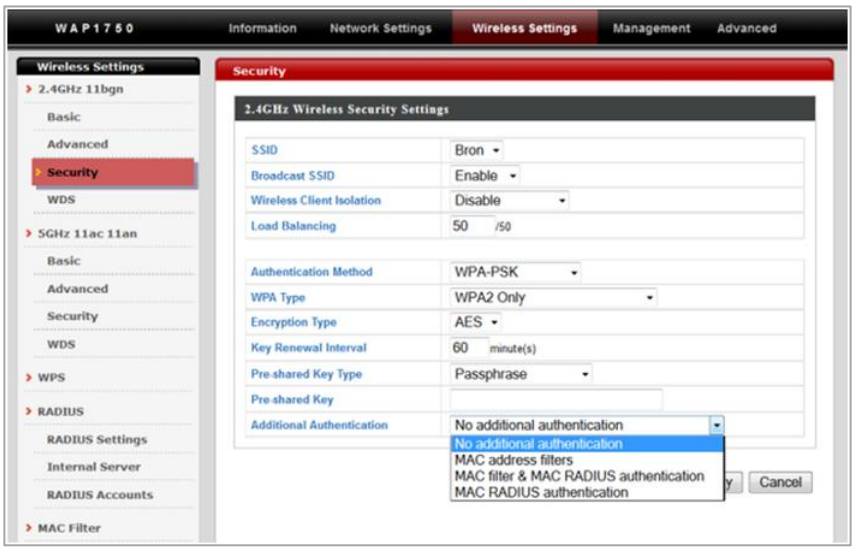
- **Configuració d'un encaminador empresarial**

A part de les configuracions esmentades anteriorment per a un encaminador domèstic, els encaminadors empresarials permeten algunes parametritzacions específiques i més avançades que les ofertes pels encaminadors domèstics.

L'accés a un encaminador o AP a través de la xarxa WiFi empresarial s'efectua generalment a través de l'adreça IP que el servidor DHCP de l'organització o l'administrador li hagi assignat. En qualsevol cas, si aquest és nou i l'hem de configurar, també es pot accedir directament amb una connexió *Ethernet* cablejada. Un exemple de configuració seria el següent:

- Mètode d'autenticació: *WPA-PSK*
- Tipus de *WPA*: *WPA2*
- Tipus d'encriptació: *AES*
- Freqüència de renovació de clau: 60 minuts.
- Tipus de *Pre-Shared-Key*: Introducció contrasenya (>12 caràcters alfanumèrics).
- *WPS*: Desactivar aquesta opció per ser vulnerable a atacs.
- Autenticació addicional: Podem combinar autenticació per filtrat MAC i/o RADIUS

L'administrador hauria de valorar el tipus d'autenticació addicional necessària. Per exemple, si es coneixen a priori, els dispositius *WiFi* clients que es connectaran a la xarxa, seria recomanable seleccionar l'opció de filtrat *MAC*, el qual, combinarà amb una autenticació *RADIUS* si necessita un increment addicional de seguretat.
Si es tracta de donar servei temporal a un gran nombre de clients, el filtratge *MAC* seria una opció poc recomanable.

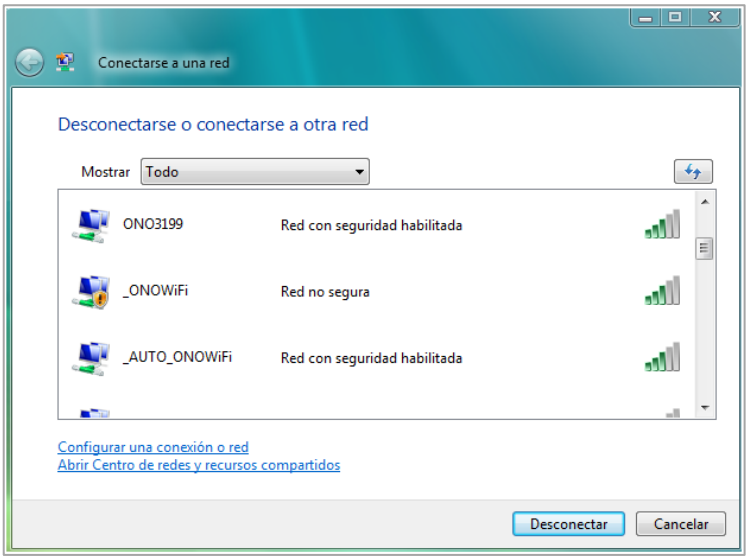


Captura de pantalla configuració de seguretat d'un encaminador empresarial [18] Figura 38

4.1.2 Navegar amb seguretat

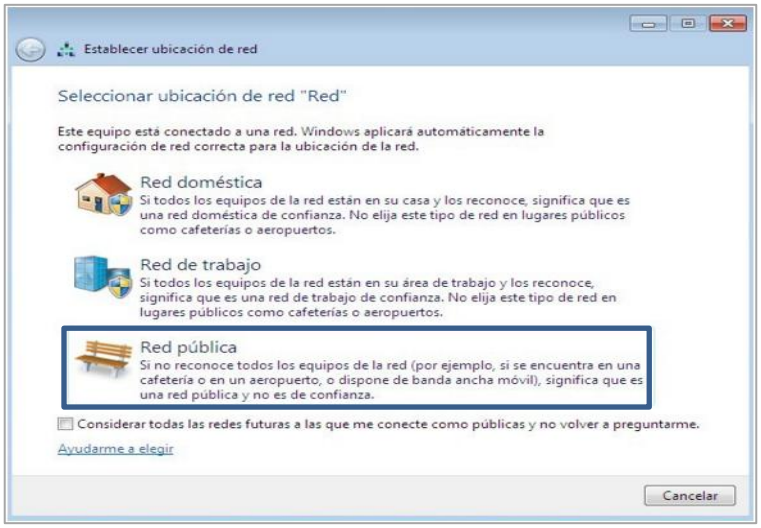
Acabem de veure un conjunt de suggeriments que ajuden a l'usuari d'una xarxa domèstica sense fils, a convertir-la més segura mitjançant la configuració del encaminador. Tanmateix, moltes vegades ens convertim en usuaris d'altres xarxes WiFi que no són de la nostra llar ni públiques, sinó xarxes privades de tercers, per exemple del treball o d'un amic. Tot i que són xarxes privades, l'usuari no coneix a les persones amb les que comparteix la xarxa ni les seves intencions, així que, s'han de prendre mesures **com si es tractés d'una xarxa pública**, tot i que es conegui i es confiï en l'administrador o propietari.

I aquí es torna a insistir en l'actitud i instint de seguretat pròpia de l'usuari; és important que cada vegada que l'usuari es connecti a Internet mitjançant WiFi, verifiqui si la connexió a la qual intenta accedir, disposa d'algun tipus de protecció. Per tant, és convenient observar si la xarxa està **protegida per una contrasenya** i posteriorment el tipus de xifrat que utilitza.



Connexió a xarxes WiFi amb seguretat habilitada Figura 39

- Recordem que una connexió WEP és molt més insegura que una xarxa WPA o WPA2.
- Abans de seleccionar una xarxa per establir connexió, podem veure si té habilitada la seguretat o per al contrari no és segura.



Connexió a xarxes WiFi públiques Figura 40

- Quan s'intenta la connexió a una xarxa WiFi, molts sistemes operatius o alguns *Firewall* pregunten si volem establir connexió amb una xarxa domèstica, corporativa o pública. Com a opció més preventiva és aconsellable seleccionar "*Xarxa pública*", amb la finalitat de que s'adoptin configuracions més restrictives de seguretat, especialment en relació a arxius compartits i accés al sistema.

D'una altra banda, si no podem evitar la navegació a través d'una WLAN insegura, és necessari utilitzar el protocol **HTTPS** (de l'anglès, *Hypertext Transfer Protocol Secure*). És un protocol de transferència de dades segur i per tant, tot el que es transmet a través d'aquest entorn, està xifrat per a que un tercer no llegeixi la informació enviada.

Connexió a través del protocol "*https*" [19] Figura 41

- Molts serveis web que requereixen contrasenyes com els bancs, correus electrònics, institucions públiques, seguretat social, xarxes socials etc. utilitzen aquest protocol de seguretat. Així doncs, és molt important assegurar-se que el camp *url* del lloc web al que s'accedeix, comença per "**https://**".

  En aquesta línia, és recomanable tenir activada aquesta opció en serveis com *Facebook*, *Twitter* o similars.

Existeixen extensions com "*HTTPS Everywhere*" per als navegadors *Mozzilla*, *Firefox* i *Google Chrome* que permeten activar aquesta funcionalitat automàticament.

Més informació: https://www.eff.org/https-everywhere

4.2 Polítiques de seguretat

Després de veure algunes recomanacions generals per accedir i navegar a través de xarxes *WiFi* de manera segura, també és important veure la seguretat des de la perspectiva d'un administrador de xarxa. La implementació d'una WLAN en una empresa, suposa adequar les seves polítiques de seguretat incloent un conjunt de consideracions per a mantenir la xarxa corporativa, en un marc de seguretat ben consolidat.

La taula següent, mostra un conjunt de recomanacions generals a tenir en compte a l'hora de confeccionar les polítiques de seguretat d'una empresa amb infraestructures WiFi, orientades a prevenir intrusions.

Objectius	Mesures
▪ Controlar l'abast de la xarxa WiFi per reduir al mínim possible la difusió d'ones fora de les instal·lacions.	➢ Estudi de cobertures i ubicacions dels punts d'accés per aconseguir difusions d'ones adaptades a les necessitats reals.
▪ Evitar l'accés a la configuració dels AP's o encaminadors de manera física o remota. ▪ Evitar accessos no autoritzats a la xarxa per intrusos que utilitzen contrasenyes per defecte i puguin modificar la configuració de seguretat de la xarxa.	➢ No deixar els AP's, encaminadors o commutadors de xarxa accessibles a qualsevol persona ➢ Ubicar els AP's en llocs d'accés relativament difícils, com per exemple sostres, falsos sostres, armaris amb panys. ➢ Modificar la contrasenya per defecte que permet l'accés i administració dels dispositius mencionats. ➢ Implementar una clau d'administrador segura.
▪ Permissivitat de connexió únicament a usuaris autoritzats als quals se'ls ha informat del nom de la xarxa de l'empresa o departament associat.	➢ Desactivar en els AP's la difusió de l'SSID de les WLAN.
▪ L'accés dels usuaris a la xarxa s'haurà de realitzar mitjançant contrasenyes segures i sota comunicacions xifrades.	➢ Configuració d'AP's per a que els clients accedeixin a la xarxa mitjançant les credencials requerides per l'administrador. ➢ Configuració dels AP's per treballar amb protocols de seguretat els més robustos possible, (per exemple WPA-PSK amb xifratge AES o WPA-Enterprise)
▪ Evitar contrasenyes d'accés a la xarxa de caràcter permanent.	➢ Establir un pla freqüencial de modificació de contrasenyes d'accés a les WLAN.
▪ Reduir les probabilitats d'èxit d'un atac, així com un possible ús fraudulent de la xarxa.	➢ Desconnectar l'alimentació elèctrica de l'AP o encaminador WiFi si no s'utilitza.
▪ Controlar els dispositius que accedeixen a la xarxa i denegació als no autoritzats.	➢ Crear una llista de control d'accés (ACL) únicament amb les adreces MAC dels dispositius que tindran autorització per accedir a la WLAN.
▪ Dificultar l'accés a la xarxa per part de tercers denegant-li una IP de manera automàtica. Cada dispositiu que intenti connectar a la xarxa haurà d'indicar una adreça IP, una màscara de subxarxa i l'adreça de l'encaminador (gateway) de manera aleatòria. Les probabilitats d'endevinar aquestes dades són quasi nul·les.	➢ Deshabilitar el DHCP (assignació dinàmica d'una IP al dispositiu client) i utilitzar IP's estàtiques. ➢ Modificar l'adreça IP que l'encaminador implementa per defecte (normalment és 192.168.0.1).
▪ Facilitar l'accés a les WLAN corporatives als empleats habituals mitjançant autenticació i un canal segur.	➢ Implementar el protocol 802.1x basat en certificats digitals que s'instal·len en els dispositius dels empleats, verificant la seva validesa cada vegada que el treballador intenta accedir a la xarxa. Així, els usuaris hi accedeixen autenticats i de forma segura, mitjançant un canal de comunicació segur proporcionat pels certificats.

Objectius i mesures d'aplicació per a una xarxa WiFi segura Taula 3

Capítol 5: Sistemes de Prevenció i Detecció d'Intrusions

Els recursos informàtics d'una organització és un patrimoni molt valuós. A part de donar suport a l'intercanvi d'informació entre les xarxes internes també facilita l'encaminament de dades vers a l'exterior, i en el seu conjunt, contribueix al bon funcionament de l'entitat empresarial. Una empresa amb la seva xarxa inutilitzada o amb informació sostreta, podria provocar un col·lapse en la seva activitat i esdevenir pèrdues importants no solament econòmiques, sinó també de clients decebuts per la vulneració de les seves dades personals.

La prevenció en aquest sentit és, en sí mateixa, una actitud segura i per tant, un pilar important a l'hora de lluitar contra atacs maliciosos vers la xarxa, ja sigui des de l'exterior com des de dins de la pròpia organització. Aquests atacs, generalment es produiran silenciosament i aprofitant fissures o deficiències de seguretat, les quals, els responsables de la xarxa hauran de localitzar. En aquesta línia, el primer pas serà realitzar una auditoria sobre tots els dispositius integrats en la xarxa per detectar possibles vulnerabilitats i eliminar-les. És aquí, on els escàners de vulnerabilitats tenen el protagonisme.

5.1 Escàners de vulnerabilitats

Són aplicacions que analitzen la nostra configuració de xarxa i executa un conjunt de tècniques d'atac, amb l'objectiu de detectar possibles deficiències de seguretat potencialment utilitzables per atacants. Tot i que són un bon complement dels sistemes de detecció instal·lats en una xarxa, solament poden detectar vulnerabilitats contingudes en la seva pròpia base de dades, les quals, es detectaran en els intervals en què s'executi l'escàner. Els escàners de vulnerabilitats generalment funcionen en tres etapes:

1. Extracció de mostres del conjunt d'atributs i elements que integren el sistema. Aquesta informació s'emmagatzema en un contenidor de dades segur.
2. Els resultats anteriors s'organitzen i comparen amb conjunts de dades de referència, com per exemple plantilles amb configuracions ideals o generada manualment. També pot ser una imatge de l'estat de la xarxa realitzada amb anterioritat.
3. Generació d'un informe de l'auditoria realitzada amb les diferències entre ambdós conjunts de dades.

S'ha de dir que aquestes tres etapes, es poden millorar utilitzant motors de comparació en paral·lel o fent servir mètodes criptogràfics per detectar possibles canvis en les màquines monitoritzades.
Els escàners de vulnerabilitats es poden diferenciar en **escàners basats en màquina** o **basats en xarxa**, segons la localització des de la qual s'obtenen les dades.

- **Escàners basats en màquina:** obtenen informació del sistema per detectar vulnerabilitats com comptes d'usuaris obertes per defecte, entrades d'usuari sospitoses o duplicades, errors en permisos de fitxers etc.

- **Escàners basats en xarxa:** utilitzen les connexions de xarxa establertes amb els objectius a analitzar per executar atacs de prova i registrar les respostes obtingudes. Aquestes proves poden ser de dos tipus: *proves d'explotació* i *mètodes d'inferència*.

    - *Proves d'explotació:* es programen atacs reals contra l'objectiu i es reben indicadors d'èxit o no. És una tècnica bastant agressiva sobre tot en atacs de denegació de servei.

    - *Mètodes d'inferència:* No s'exploten vulnerabilitats, sinó que el sistema busca indicis o evidències de que s'han realitzat atacs en la màquina analitzada. Aquest mètode és menys agressiu que l'anterior, tanmateix els resultats que ofereix són més inexactes.

Tot i que els escàners basat en xarxa realitzen proves d'atac i registren les respostes obtingudes, no s'han de confondre amb els analitzadors de sistemes de detecció d'intrusions, doncs aquests últims, no presenten una solució tan exhaustiva.

Alguns dels productes més utilitzats actualment com a escàner de vulnerabilitats basat en xarxa és *Nessus* o *GFI LanGuard*. Per a més informació `www.nessus.org` i `www.gfi.com`.

Tot i que els escàners de vulnerabilitats possibiliten l'anàlisi i correcció de possibles debilitats en el nostre sistema informàtic, no són infal·libles. Així que hem de ser capaços de detectar i neutralitzar moviments no autoritzats o la circulació de qualsevol tipus de tràfic maliciós. En aquest sentit, la instal·lació de sistemes de detecció i prevenció d'intrusions amb sensors distribuïts estratègicament per la xarxa, permetrà "escoltar" i analitzar en continu, tota la informació que circula per identificar possibles atacs. En cas de que l'atac es produeixi, el sistema reaccionarà activant els mecanismes de defensa estipulats i enviarà un informe a l'administrador.

A continuació, s'estudiaran els sistemes de prevenció (IPS) i detecció d'intrusions (IDS) primerament des d'una perspectiva teòrica. Posteriorment es realitzarà un cas pràctic, demostrant la utilitat d'un IDS/IPS com l'*Snort*, el qual treballarà sota unes regles personalitzades que s'implementaran prèviament.

5.2 Sistemes de Prevenció d'Intrusions (IPS)

IPS (Sistema de Prevenció d'Intrusions) és un programari dissenyat per analitzar, monitoritzar i bloquejar qualsevol intent d'atac abans de que pugui causar danys a la nostra xarxa. Aquest sistema es conegut pel nom de *tallafoc (Firewall)*.

Els IPS es classifiquen en dues categories:

- **Sistemes basats en màquina** (HIPS, *Host Based Intrusion Prevention Systems*), fan servir aplicacions que s'instal·len directament a la pròpia màquina que es vol protegir i que interactuen amb el sistema operatiu i els serveis que ofereix. Ens permet controlar atacs de Virus, *Spam*, *Spyware*, Cucs, Trojans, *Keyloggers*, *Rootkits*, atacs *DoS* i també els distribuïts *DDoS*. Un aplicatiu d'aquest tipus pot ser *BlackIce*.

- **Sistemes basats en xarxa** (NIPS, *Network Based Intrusion Prevention Systems*) són dispositius de xarxa que combinen filtratge de paquets i detecció dels sospitosos. Es recolzen com a mínim amb dues interfícies; una per monitoritzar la xarxa interna i una altre per a la externa. Un aplicatiu és *Tipping Point*, *IBM Proventia* o *NetworkIce*.

Els sistemes tallafoc, són un mecanisme de control d'accés sobre la capa de xarxa, de manera que separa la xarxa interna, on els equips són de confiança, dels equips potencialment hostils a l'exterior. Aquest control, consisteix en permetre o denegar el pas de comunicació d'una xarxa a una altra mitjançant el control dels protocols TCP/IP.

Les tecnologies més utilitzades a l'hora de construir un sistema tallafocs són:

1. **Encaminadors amb filtratge de paquets:** dispositiu que encamina el trànsit TCP/IP sota certes regles de filtratge prèviament configurades i que decideixen quins paquets es dirigeixen a través seu i quins són descartats (*iptables*).

2. **Passarel·les a nivell d'aplicació:** actua com a servidor intermediari (*proxy*). No encamina paquets a nivell de xarxa, sinó que treballa com a retransmissor a nivell d'aplicació. Així, els usuaris de la xarxa contactaran primer amb aquest servidor intermediari, el qual, estarà oferint un servei *proxy* associat a una més aplicacions.

3. **Passarel·les a nivell de circuit:** l'usuari ha d'establir primerament connexió amb el sistema tallafoc i aquest, establirà la connexió amb l'equip destí. El seu objectiu és determinar quines connexions estan permeses abans de bloquejar connexions destinades a l'exterior.

5.3 Sistemes de Detecció d'Intrusions (IDS)

La detecció d'intrusos és el procés d'identificació i resposta davant activitats malicioses o moviments sospitosos que s'observen vers a qualsevol equip o recurs d'una xarxa. Aquesta tasca és responsabilitat dels Sistemes de Detecció d'Intrusions (IDS), dissenyats per a detectar atacs i intrusions, localitzar i reportar tot tipus d'activitats malicioses i reaccionar davant l'atac de manera adient.

Un IDS, ha de complir els següents requeriments:

- Precisió: Capaç de diferenciar una acció legítima d'una altra deshonesta.
- Eficiència: Ha de minimitzar la taxa d'activitat maliciosa no detectada.
- Rendiment: Capaç d'arribar a realitzar una detecció en temps real abans de que la intrusió provoqui danys al sistema, això és, inferior a un minut.
- Escalabilitat: Preparat per gestionar el nombre d'esdeveniments necessari davant el creixement de la xarxa, tant en velocitat com en mida.
- Tolerant a fallades: Dissenyat per a mantenir el servei davant atacs produïts en diferents elements del sistema, incloent ell mateix.

Els elements necessaris per construir un IDS s'agrupen en quatre categories:

a) **Recol·lectors d'informació:** conegut com a sensor i responsable de recollir informació de les màquines monitoritzades pel IDS. Es poden implementar de tres maneres:

   1. *Sensors basats en equip*: analitzen i recullen informació d'esdeveniments succeïts a nivell de sistema operatiu, com per exemple, intents de connexió o crides al sistema.

   2. *Sensors basats en trànsit:* analitzen i recullen informació o esdeveniments succeïts a nivell de trànsit de xarxa, com per exemple anàlisi de capçaleres IP dels datagrames.

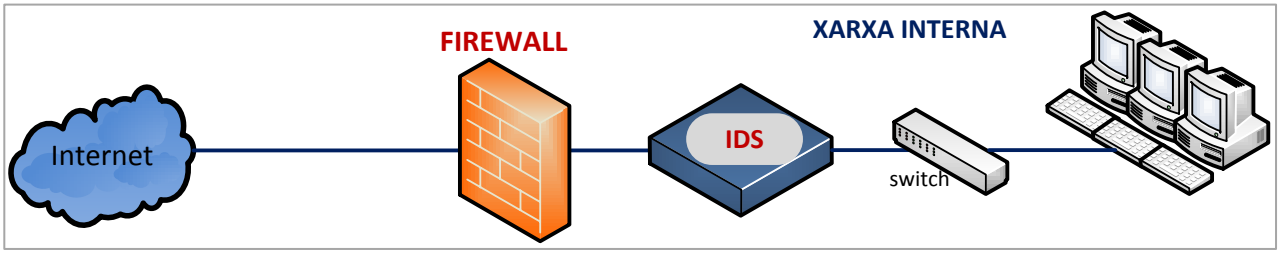
   3. *Sensors basats en aplicació:* reben informació d'aplicacions que s'estan executant.

b) **Processadors d'esdeveniments:** coneguts com analitzadors, formen el nucli central de l'IDS. Operen sobre la informació recollida pels sensors per poder associar-la amb possibles intrusions.

c) **Unitats de resposta:** inicien accions de resposta davant la detecció d'un atac o intrusió. Poden ser automàtiques (resposta activa) o requerir interacció humana (resposta passiva). També es divideixen en respostes basades en equip (bloqueig d'usuaris, finalització de processos etc.) i basades en xarxa, (tall d'intents de connexió, filtratge de connexions, etc.).

d) **Elements d'emmagatzematge:** necessaris per a emmagatzemar, durant dos o tres dies, la quantitat d'informació requerida segons el volum d'informació recollida pels sensors. Aquesta informació serà analitzada posteriorment pels processadors del sistema.

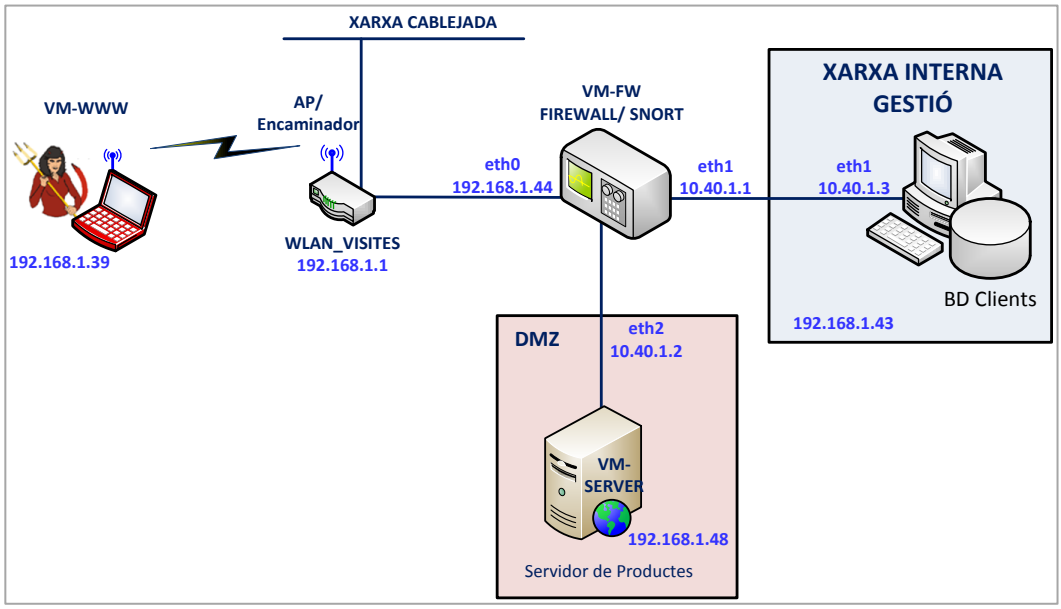
A l'esquema següent, podem veure un dibuix simplificat de la representació d'un Firewall i un IDS en la xarxa.



Esquema simplificat d'ubicació d'un Firewall (IPS) i un IDS Figura 42

5.4 Cas pràctic amb l'IDS *Snort*: regles i configuració

L'escenari representa una empresa de productes informàtics que té un servidor web amb el seu catàleg de productes. Disposa d'un sistema de seguretat deficient, a través del qual, aprofitarem per veure les eines bàsiques que fa servir l'atacant per analitzar la xarxa. Es detectaran moviments sospitosos pel detector d'intrusions *Snort*, utilitzat com a sensor basat en trànsit. L'escenari està format pels elements següents:



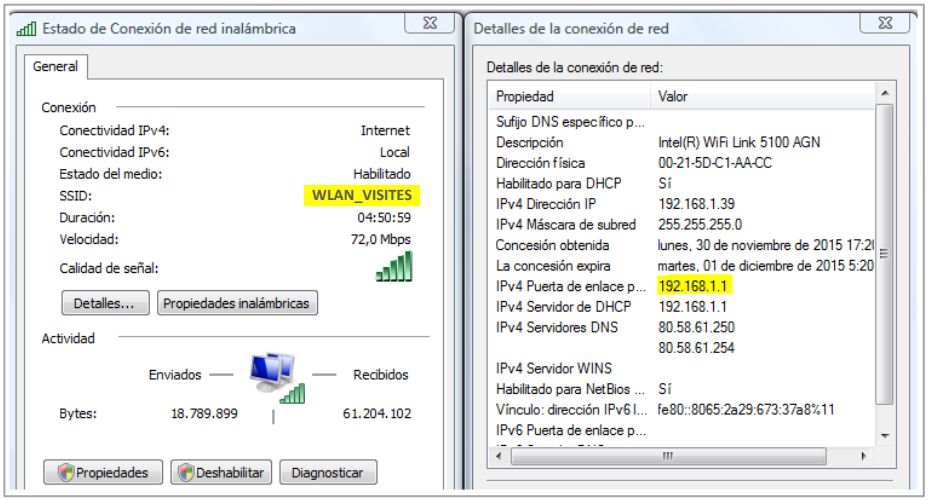
Escenari de simulació utilitzat per als diferents casos de prova Figura 43

- VM-WWW: Màquina virtual que simula el PC de l'**atacant.**
- VM-FW: Màquina virtual *Firewall* amb l'eina IDS ***Snort*** implementada. La configuració d'aquest tallafoc és deficient, per facilitar la demostració de detecció de l'eina ***Snort***. Per tant, la política per defecte és d'acceptar qualsevol connexió i les *Iptables* no estan configurades. Disposa de connexió a internet.
- VM-SERVER: Màquina virtual que simula un **servidor** de productes instalat en una DMZ i visitable des d'Internet. Gestionable des del PC de la xarxa interna.
- PC GESTIÓ: A través d'aquest PC es **gestiona** exclusivament el servidor web i la base de dades dels clients. Disposa de connectivitat a Internet per a usuaris autoritzats.
- AP/Router: Ofereix connectivitat WiFi a Internet o servidor de productes als comercials de diferents empreses subministradores. Per facilitar el servei, no està correctament configurat, doncs té visibilitat i accés sense cap tipus d'autenticació.

Es simularan cinc moviments sospitosos a la xarxa, els quals s'iniciaran a partir d'una prèvia exploració del sistema per part de l'atacant. Després d'iniciar l'IDS *Snort*, haurà de detectar els moviments generats i monitoritzar el missatges d'alerta corresponents mitjançant 5 regles implementades a l'arxiu *jlb.rules*. El procés de configuració d'aquestes regles s'especifica a l'Apèndix 2.

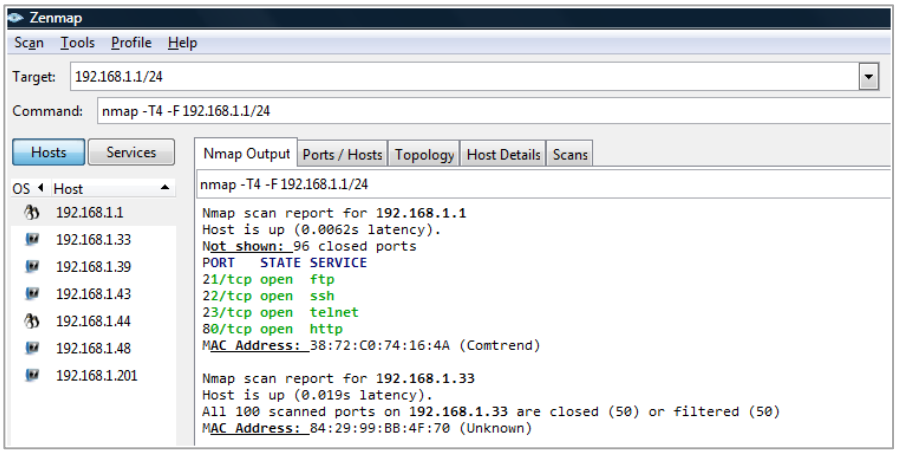
- Cas 1: Detecció de "*pings*" sospitosos
- Cas 2: Intent de connexions iniciades en qualsevol màquina cap a la xarxa de gestió interna.
- Cas 3: Connexió al servidor des de la xarxa de gestió per un port sospitós.
- Cas 4: Intent de connexió *tcp* no autoritzada i originada a la xarxa interna cap a Internet.
- Cas 5: Connexió *tcp* no autoritzada i originada al servidor de productes vers a Internet.

Exploració il·lícita de la xarxa empresarial: detecció de màquines i ports oberts.
Primerament l'atacant escanejarà la xarxa en busca d'un encaminador sense fils que li pugui reportar informació. L'SSID s'anuncia com WLAN_VISITES i per comoditat, aquesta empresa té l'AP amb el DHCP activat. Per tant, el PC atacant tindrà assignada una adreça IP tant aviat es connecti a la WLAN_VISITES. L'atacant només haurà de veure quina adreça té aquest encaminador WiFi i comprovar a través del seu PC, quina és la porta d'enllaç o *gateway* amb la que està connectat: en aquest exemple 192.168.1.1.



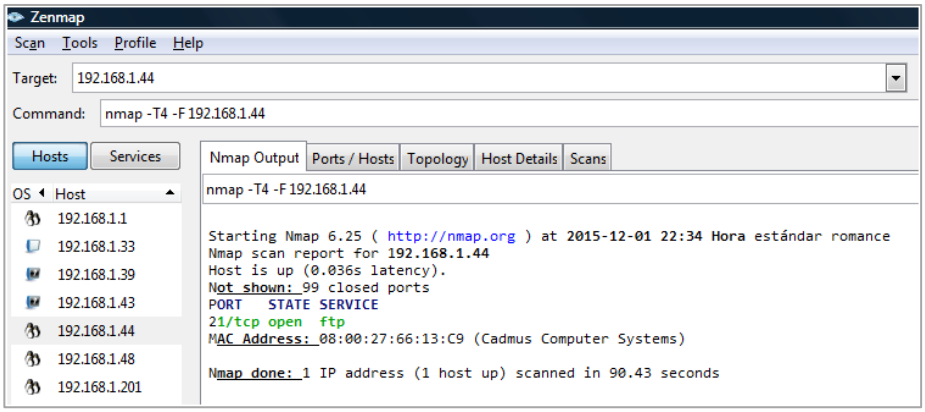
Detecció adreça de la porta d'enllaç d'encaminador WiFi Figura 44

A continuació, mitjançant una eina d'escaneig de ports, l'atacant intentarà veure totes les màquines que hi ha darrere del punt d'accés i els ports oberts amb els què hi podria accedir il·lícitament. En aquesta simulació s'utilitzarà *Zenmap* [20], que és una interfície gràfica de la versió oficial *nmap,* i amb la que l'intrús farà servir per rastrejar possibles ports oberts.
Amb la instrucció nmap –T4 –F 192.168.1.1/24 es detectaran tots els hosts que estan connectats al punt d'accés i també els ports oberts més comuns de cada host detectat.



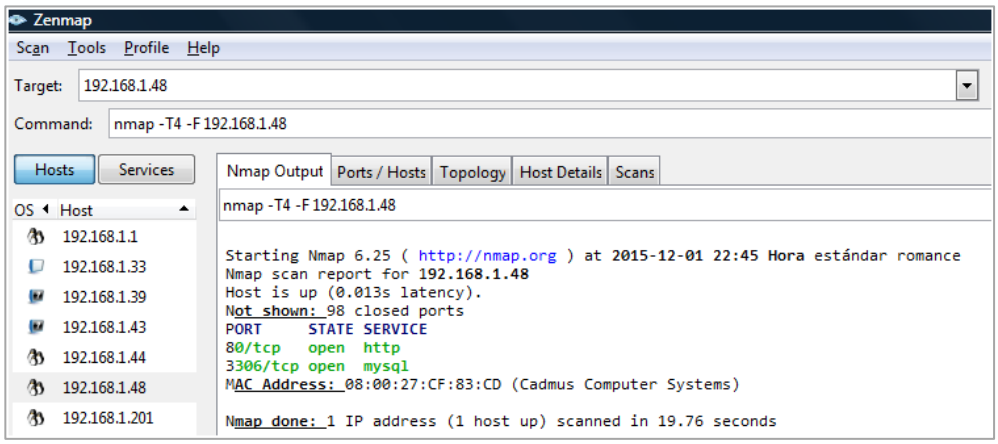
Detecció de ports oberts amb l'eina *Zenmap* Figura 45

En aquest cas, ens centrarem en la màquina detectada 192.168.1.44, que és precisament el Firewall de l'empresa i veurem que té el port *ftp* 21 obert utilitzat normalment per a la descàrrega d'arxius a l'equip. Pensem que un port obert sense cap tipus de control, és una entrada/sortida potencial per un atacant.



Detecció de ports oberts del *Firewall* amb l'eina *Zenmap* Figura 46

Després de analitzar cada host, l'atacant detectarà un servidor a l'adreça 192.168.1.48 i lògicament voldrà saber de què es tracta. Així que també escanejarà aquesta màquina, observant que té oberts el port 80 *HTTP* utilitzat pels navegadors web i el port 3306 *MySQL* per a bases de dades.



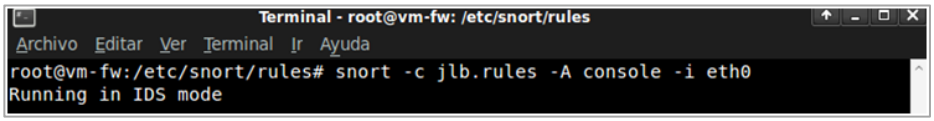
Detecció de ports oberts al servidor amb l'eina *Zenmap* Figura 47

Acabem de veure la possibilitat que té un atacant de detectar màquines i ports oberts, amb els quals utilitzarà per instal·lar *malware*, robar, manipular informació etc. Inclús podria accedir a la base de dades de la xarxa interna i obtenir informació sensible de l'empresa.

Generalment els processos d'exploració que genera una atacant en una xarxa són generalment bastant sorollosos. Però també existeixen instruccions en molts "*sniffers*" per silenciar aquests moviments i per tant, obliga als administradors a ser molt esquists a l'hora de configurar els detectors d'intrusions.

A continuació veurem que amb les regles configurades en el *Snort* detallades a l'Apèndix 2, podrem detectar aquest moviments sospitosos:

Primerament, posarem en marxa l'*Snort* per a que treballi segons les regles configurades amb l'opció `-c jlb.rules`.

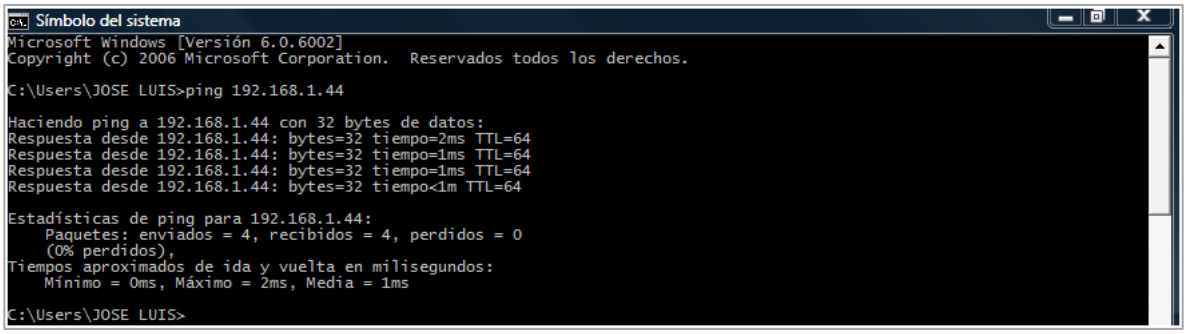


Execució de l'*Snort* condicionat a les regles de l'arxiu *jlb.rules* Figura 48

Tot i que veurem les alertes per la consola, quedaran emmagatzemades a la ruta `/var/log/snort`.

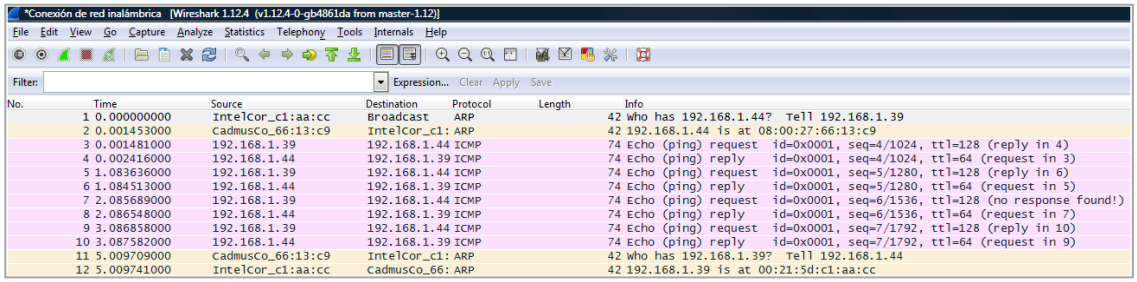
Cas 1: detecció de "*pings*" sospitosos

L'atacant podria fer un simple ping d'exploració per detectar el Firewall:



Ping des de la màquina de l'atacant vers al *Firewall* Figura 49

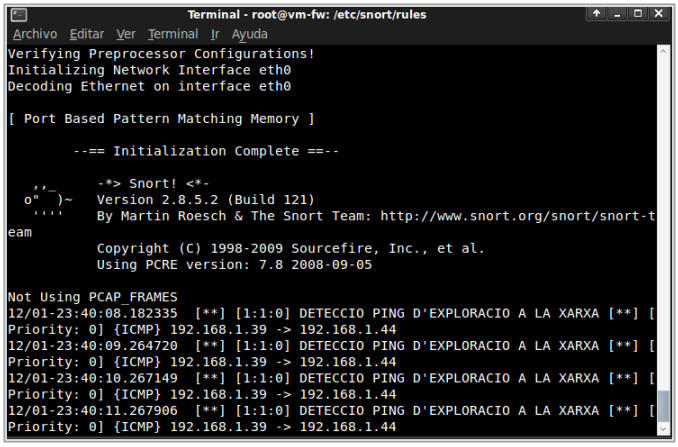
Podem veure amb l'analitzador de tràfic de la xarxa *Wireshark* [21] el ping enviat amb el protocol *ICMP* i la resposta de la màquina 192.168.1.44.



Captura del *ping* amb l'eina *Wireshark* Figura 50

No té per què haver "pings" a la xarxa, així que l'*Snort* ho detecta i ofereix l'alerta que s'havia configurat:

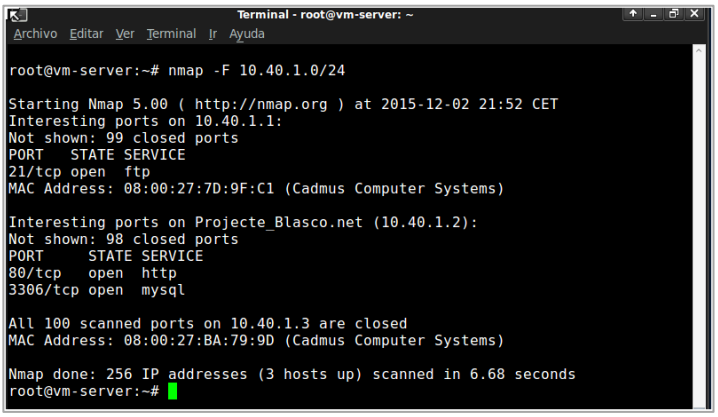
```
alert icmp any any -> any any (itype:8;sid:1;msg:"DETECCIÓ PING D'EXPLORACIÓ A LA XARXA";)
```



Alerta de l'*Snort* amb el "ping" detectat Figura 51

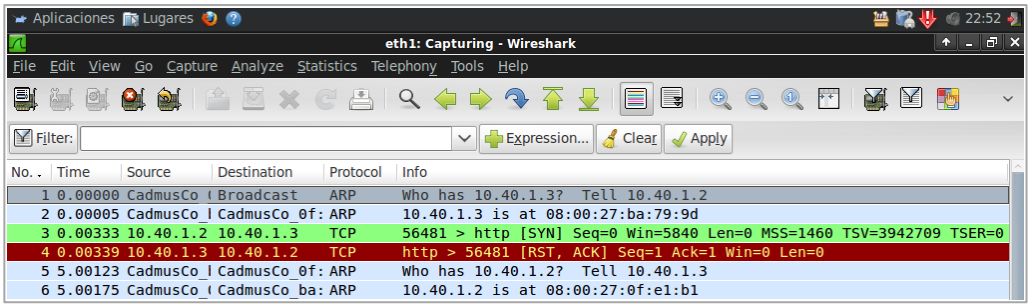
Cas 2: Intent de connexions iniciades en qualsevol màquina cap a la xarxa de gestió interna.

Si l'atacant tingués el control del servidor a través dels seus ports oberts o arribés físicament a aquest, podria intentar connexions amb la xarxa interna. Aquest moviment hauria de ser detectat pel detector d'intrusions, doncs, no podem permetre cap tipus de connexió iniciada al servidor cap a la xarxa interna. Solament s'hauria d'acceptar connexions iniciades a la xarxa interna pels ports 3306 exclusius per a gestionar bases de dades o al port 80 per connexions *http*.
Suposem que l'atacant, amb l'eina *nmap*, inicia un escaneig des del servidor instalat a la DMZ per veure quines màquines hi ha darrera d'ell. Podem veure que detecta el servidor *firewall* a l'adreça 10.40.1.1, el propi servidor, i finalment el PC de gestió a la IP 10.40.1.3 amb els ports tancats.



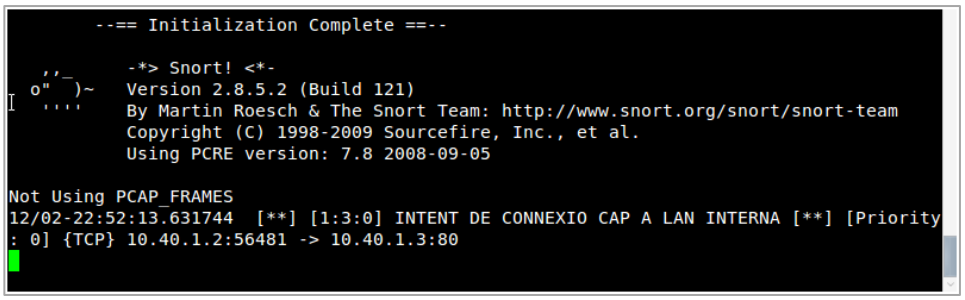
Detecció de màquines i ports oberts des de servidor DMZ Figura 52

Com que l'atacant ja coneix les adreces i ports de la xarxa interna, intenta establir una connexió *tcp* amb el PC de gestió.



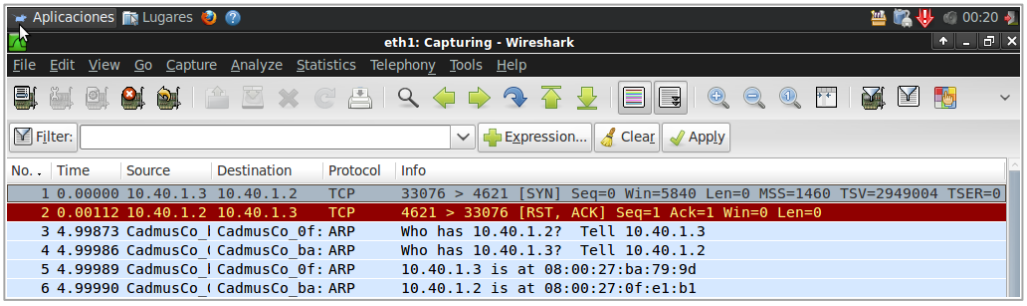
Captura de l'intent de connexió a la LAN interna amb l'eina *Wireshark* Figura 53

L'Snort, hauria de detectar qualsevol moviment iniciat al servidor i destinat a la xarxa interna amb la regla `alert tcp any any -> 10.40.1.0/24 any (flags:S;sid:2;msg:"INTENT DE CONNEXIÓ CAP A LAN INTERNA";)`



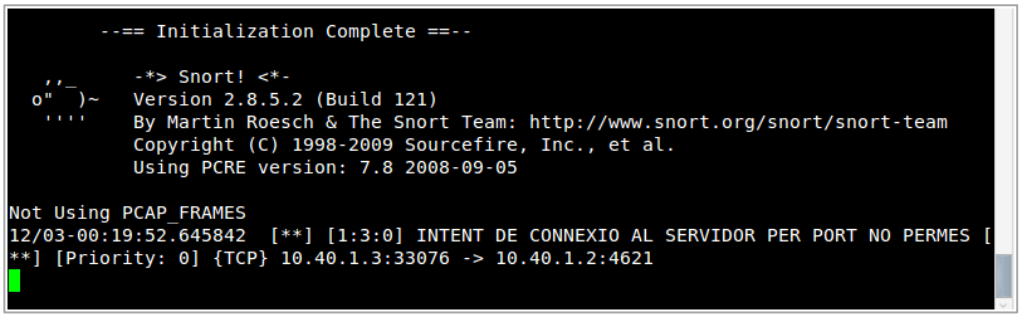
Alerta de l'*Snort* amb l'intent de connexió cap a LAN interna Figura 54

Cas 3: Connexió al servidor des de la xarxa de gestió per un port sospitós.
Un empleat del departament de gestió, intenta connectar amb el servidor per un port diferent al de base de dades (3306), possiblement amb intencions il·lícites.



Captura de l'intent de connexió des de xarxa LAN a servidor amb l'eina *Wireshark* Figura 55

Aquest tipus de connexió no està permès, l'IDS detectarà el moviment amb la regla creada:
`alert tcp 10.40.1.3 any -> 10.40.1.2 !3306 (flags:S;sid:3;msg:"INTENT DE CONNEXIÓ AL SERVIDOR PER UN PORT NO PERMÈS";)`

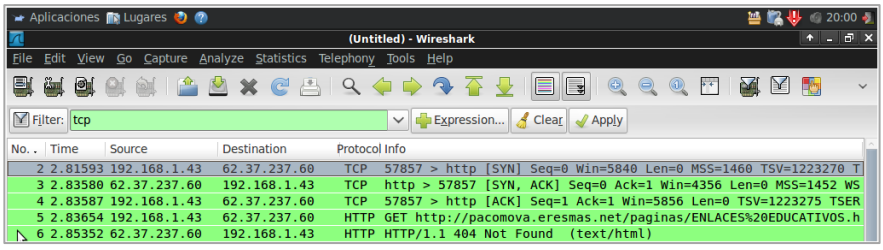


Alerta de l'*Snort* amb l'intent de connexió cap a servidor per un port no permès Figura 56

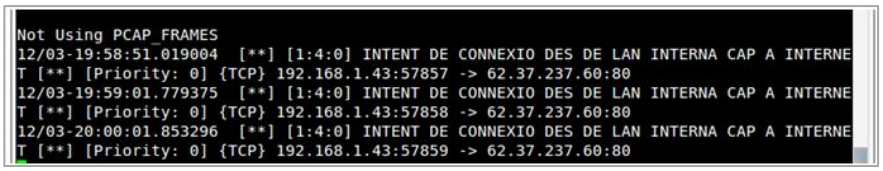
Cas 4: Intent de connexió *tcp* des de la xarxa interna cap a Internet.

Si aquest empleat fraudulent, intentés establir una connexió cap a Internet des de la LAN interna sense tenir els permisos adients, també seria detectat amb la regla següent:

```
alert tcp 192.168.1.43 any -> any any (flags:S;sid:4;msg:"INTENT DE CONNEXIÓ DES DE LAN INTERNA CAP A INTERNET";)
```



Captura de l'intent de connexió des de xarxa LAN vers a Internet amb l'eina *Wireshark* Figura 57

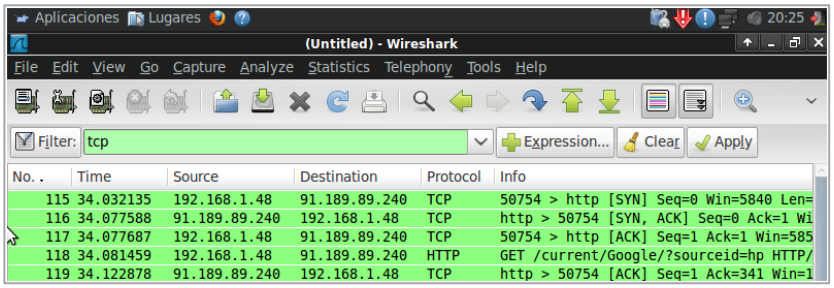


Alerta de l'*Snort* amb l'intent de connexió des de xarxa LAN vers a Internet Figura 58

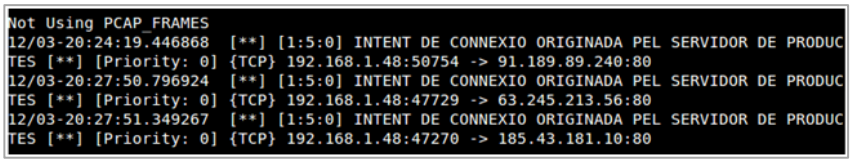
Cas 5: Connexió *tcp* originada al servidor de productes vers a Internet

Finalment, la detecció d'una connexió forçada en el servidor de productes vers a qualsevol màquina d'Internet es detectaria amb la regla *Snort* següent:

```
alert tcp 192.168.1.48 any -> any any (flags:S;sid:5;msg:"INTENT DE CONNEXIÓ ORIGINADA PEL SERVIDOR DE PRODUCTES";)
```



Captura de l'intent de connexió des de servidor vers a Internet amb l'eina *Wireshark*. Figura 59



Alerta de l'*Snort* amb l'intent de connexió des de servidor vers a Internet Figura 60

Acabem de veure alguns exemples de moviments sospitosos originats des de fora i des de dins de la xarxa, els quals, han estat detectats pel IDS Snort. Aquests moviments, començant per un simple "ping" fins a un escaneig més complet amb l'Nmap per exemple, inicien el que podíem anomenar un procés intrusiu, el qual, podria acabar amb un atac DoS, MitM o robatori d'informació sensible de l'organització.

Per evitar que això es produeixi, a part de disposar IPS/IDS, convindria limitar la visibilitat i abast de l'AP, establint l'accés a la xarxa mitjançant llistes d'accés (ACL). També s'hauria d'implementar un tallafocs, amb una política restrictiva de denegació per defecte i un encaminament d'IP's adient a les nostres necessitats. Finalment, establir mecanismes d'accés i control als recursos informàtics basats en nivells autenticació, limitant l'accés físic a dispositius informàtics amb els què es pugui obtenir informació sensible.

Capítol 6: Conclusions

Al igual que moltes persones de la meva generació, he tingut la sort de viure l'evolució de les TIC a una velocitat espectacular. Els primers ordinadors personals no solament eren poc eficients i amb poca memòria, sinó que també oferien una connectivitat lenta, amb configuracions manuals poc amigables per a tots aquells que no teníem coneixements d'informàtica. Afortunadament això és historia. Avui ja és normal veure als nostres fills que van a la biblioteca amb els ordinadors portàtils a la motxilla i *smartphones* a la butxaca. La veritat és que no són conscients del què tenen entre les mans, doncs han nascut amb la tecnologia "*plug&play*", orientada a la connectivitat, ràpida, fàcil, intuïtiva i automatitzada. Però el millor de tot; sense cables.

L'alta utilització dels telèfons intel·ligents (*smartphones*) i computadores portàtils ha impulsat la difusió de xarxes basades en tecnologia Wi-Fi a escala mundial, en àmbits domèstics, corporatius o espais públics. El concepte de mobilitat emmascara una dependència global, on la societat necessita estar "connectada" constantment, fins al punt de no concebre una universitat, hotel o centre comercial sense WiFi. Tanmateix, aquesta facilitat de comunicació i intercanvi de dades, allunya qualsevol intent de reflexió sobre la seguretat de la informació que viatja a través de l'aire, la qual, és visible per qualsevol intrús malintencionat. Així que, és absolutament necessari protegir-la.

Quan volem protecció per a les nostres dades significa que viatgi xifrada i a través de xarxes segures, les quals, hauran de tenir resolt aspectes com autenticació, confidencialitat i integritat. Afortunadament els estàndards 802.11i i 802.x ens ajuden a aconseguir-ho, aportant robusts algoritmes d'encriptació com WPA2-AES i amb la possibilitat d'incloure l'emissió de claus xifrades com per exemple WPA-PSK. L'accés a la xarxa mitjançant servidors d'autenticació (RADIUS) o a través de xarxes virtuals (VPN), reforcen considerablement el cercle de seguretat que protegeix la nostra informació a nivell empresarial.

Malauradament aquests mecanismes no són infal·libles. Les comunicacions amb tecnologia WiFi solen conviure en entorns potencialment hostils, degut principalment a la seva facilitat de detecció mitjançant eines a l'abast de tothom i la gran proliferació de les xarxes obertes, tant acceptades per la societat. Hem de ser conscients que generalment aquestes xarxes són poc segures, basades en dèbils mecanismes de xifrat com WEP o senzillament obertes, les quals, constitueixen un escenari ideal per als intrusos.

No hem de permetre que la xarxa monopolitzi el nivell de seguretat de les nostres transmissions, doncs una part d'aquesta responsabilitat ha de recaure en nosaltres mateixos. En aquest sentit, hem de seleccionar amb cura les xarxes a les quals ens connectem i aplicar en els nostres dispositius les configuracions més exigents de xifrat, desconfiar de les configuracions per defecte dels encaminadors i utilitzar sempre maquinari informàtic amb el sistema operatiu actualitzat i un antivirus instalat.

Pel que fa a l'àmbit empresarial, un bon punt de partida per consolidar una xarxa segura comença per la configuració dels AP's, els quals han de mantenir una visibilitat limitada, una connectivitat restrictiva i controlada, amb autenticació d'usuaris i potents algoritmes de xifrat. WPA-Enterprise és una bona opció en aquest sentit. No hem de perdre de vista que els atacants aprofiten forats de seguretat, així que haurem de detectar-los abans que ells. Els escàners de vulnerabilitats ens ajudaran a fer-ho; són els agents que auditaran la nostra xarxa per informar-nos de les esquerdes de seguretat detectades i possibles solucions.

Tot i així, no ens podem permetre baixar la guàrdia, per la qual cosa ens valdrem de sistemes de prevenció i detecció d'intrusions, amb els que monitoritzarem la xarxa en continu per detectar i evitar possibles atacs i a més, obtindrem alertes de moviments sospitosos o no autoritzats que s'originin tant des de fora, com des de dins de la nostra xarxa.

Amb les simulacions d'atacs i detecció mitjançant l'IDS *Snort*, s'ha demostrat la facilitat amb la que un atacant explora una xarxa, detecta les màquines que la integra i descobreix ports oberts. A partir d'aquí, la privadesa de la nostra informació queda seriosament compromesa. Les eines que s'han utilitzat són molt simples i a l'abast de qualsevol, així que, podem imaginar les accions que podria executar un intrús experimentat amb aplicacions sofisticades. Al nostre favor, sabem que amb l'ajuda d'un IDS configurat amb regles personalitzades, podríem ser alertats de moviments no autoritzats en la nostra xarxa.

Hem d'acceptar que no existeix una xarxa absolutament segura. Tanmateix, hem vist que afortunadament, sí existeixen eines i actituds, amb les quals, aconseguirem disminuir la probabilitat d'atacs amb èxit.

Capítol 7: Bibliografia

[1] https://es.wikipedia.org/wiki/Wifi
[2] http://es.ccm.net/contents/791-modos-de-funcionamiento-wifi-802-11-o-wi-fi
[3] http://bibing.us.es/proyectos/abreproy/11306/fichero/TEORIA%252F08+-+Capitulo+3.pdf
[4] http://www.comunicacionesinalambricashoy.com/wireless/802-11-ac-el-nuevo-estandar-wifi/802-11-ac-el-nuevo-standard-wifi/
[5] https://en.wikipedia.org/wiki/IEEE_802.11
[6] James F. Kurose – Keith W.Ross. *Computer Networking. A top-down approach.* Sixth edition. Edimburgh: Pearson, 2013. Cap.8.
[7] http://www.computerworld.com/article/2581074/mobile-wireless/how-802-1x-authentication-works.html
[8] http://www.networkworld.com/article/2216499/wireless/what-is-802-1x-.html
[9] http://www.trustedreviews.com/news/Google-Admits-Street-View-Cars-Stole-WiFi-Data
[10] https://wigle.net/
[11] https://wigle.net/stats
[12] http://www.pandasecurity.com/spain/mediacenter/consejos/redes-wifi-publicas-seguras/
[13] http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf/view
[14] https://encodingthecode.wordpress.com/2012/10/19/romper-clave-wep-en-linux-con-un-cliente-asociado/
[15] http://thehackerway.com/2012/05/04/wireless-hacking-conceptos-basicos-sobre-wpawpa2-parte-xiii/
[16] http://www.atc.uniovi.es/inf_med_gijon/3iccp/2006/trabajos/wifi/#eap
[17] https://www.acrylicwifi.com/
[18] http://www.redeszone.net/2015/08/20/como-configurar-el-ap-empresarial-edimax-wap1750-y-wap1200-con-wpa2-psk-y-cifrado-aes/
[19] http://www.registro-dominios.info/blog/75/
[20] http://recursostic.educacion.es/observatorio/web/fr/software/software-general/1050-zenmap?start=6
[21] http://www.wiresharktraining.com/

Altres fonts d'informació consultades:

- http://recursostic.educacion.es/observatorio/web/gl/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi
- http://windows.microsoft.com/es-es/windows/what-are-wireless-network-security-methods#1TC=windows-vista
- http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11i-security-wpa2-wep.php
- http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
- https://www.osi.es/es/actualidad/blog/2014/11/07/que-es-wps-pin-y-por-que-debes-desactivarlo
- Xavier Perramon Tornil. *Mecanismes de protecció.* PID 00187027 . Universitat Oberta de Catalunya.
- Joaquín Garcia Alfaro. *Mecanismes per a la detecció d'atacs i intrusions.* P07/05070/02626. UOC.
- James F. Kurose – Keith W.Ross. *Computer Networking. A top-down approach.* Sixth edition. Edimburgh: Pearson, 2013. Cap 6.

Annex 1 Escàner de vulnerabilitats GFI LanGuard

GFI LanGuard Network Security Scanner és una eina que permet als administradors realitzar una auditoria de seguretat de la xarxa. Crea informes que poden ser utilitzats per resoldre els problemes detectats i també és capaç de realitzar actualitzacions de seguretat i no seguretat de més de 60 aplicacions de tercers sota sistemes operatius com Microsoft ®, Mac ® i Linux ®.

http://languard.gfi.com/

Proporciona una imatge completa d'aplicacions instal·lades, hardware de la xarxa, dispositius mòbils que connecten a servidors Exchange, estat de les aplicacions de seguretat (antivirus, *anti-spam*, tallafocs, etc.), ports oberts i qualsevol recurs compartit o servei en execució en els equips que integren la xarxa.

Executa més de 60.000 avaluacions de vulnerabilitats en les xarxes especificades, incloent entorns virtuals, mòbils i dispositius de xarxa. També escaneja els sistemes operatius, entorns virtuals i aplicacions instal·lades mitjançant bases de dades de comprovació de vulnerabilitat com OVAL i SANS Top 20.

GFI LanGuard analitza l'estat de la seguretat de la xarxa i identifica els riscos, determina el grau d'exposició i indica la millor solució per evitar que la xarxa quedi compromesa.

A continuació veurem una demostració de la seva interfície gràfica instal·lada en un PC portàtil domèstic. Tot i que és una versió d'avaluació de 30 dies, podrem veure com treballa i un extracte de la informació que s'obté.

- **INSTAL·LACIÓ:** A la pàgina web http://www.gfi.com/home obtindrem l'instal·lador del programa d'avaluació per a 30 dies. És necessari registrar-se amb un mínim de dades; nom, cognoms, e-mail on enviaran nº llicència, i país.

Al iniciar l'executable introduirem les dades que ens demanin.

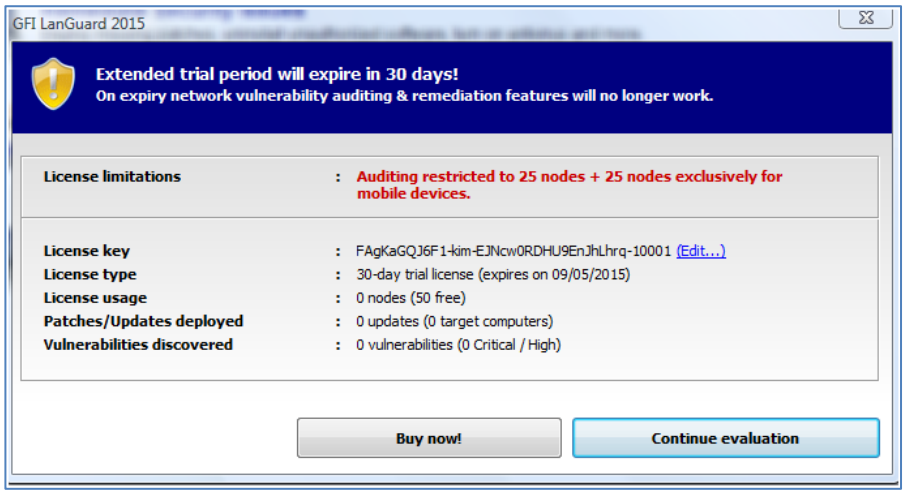
Durant la instal·lació de la aplicació, és necessari establir un usuari administrador amb una contrasenya. Aquesta contrasenya ha de ser inicialment la mateixa que l'administrador utilitza per accedir al sistema operatiu. En cas contrari, apareixerà l'avís de la figura.

Si optem per continuar sense contrasenya, les funcionalitats de GFI estaran limitades, com actualitzacions, operacions remotes i altres. En aquest cas s'introdueix la contrasenya d'inici sessió a Windows.

Seguidament ens indica la instal·lació dels components necessaris pel seu funcionament. Sobretot és molt important disposar d'una base de dades actualitzable per poder executar les tècniques d'atac més adients.

Finalment tenim el programa instal·lat i iniciant-se.

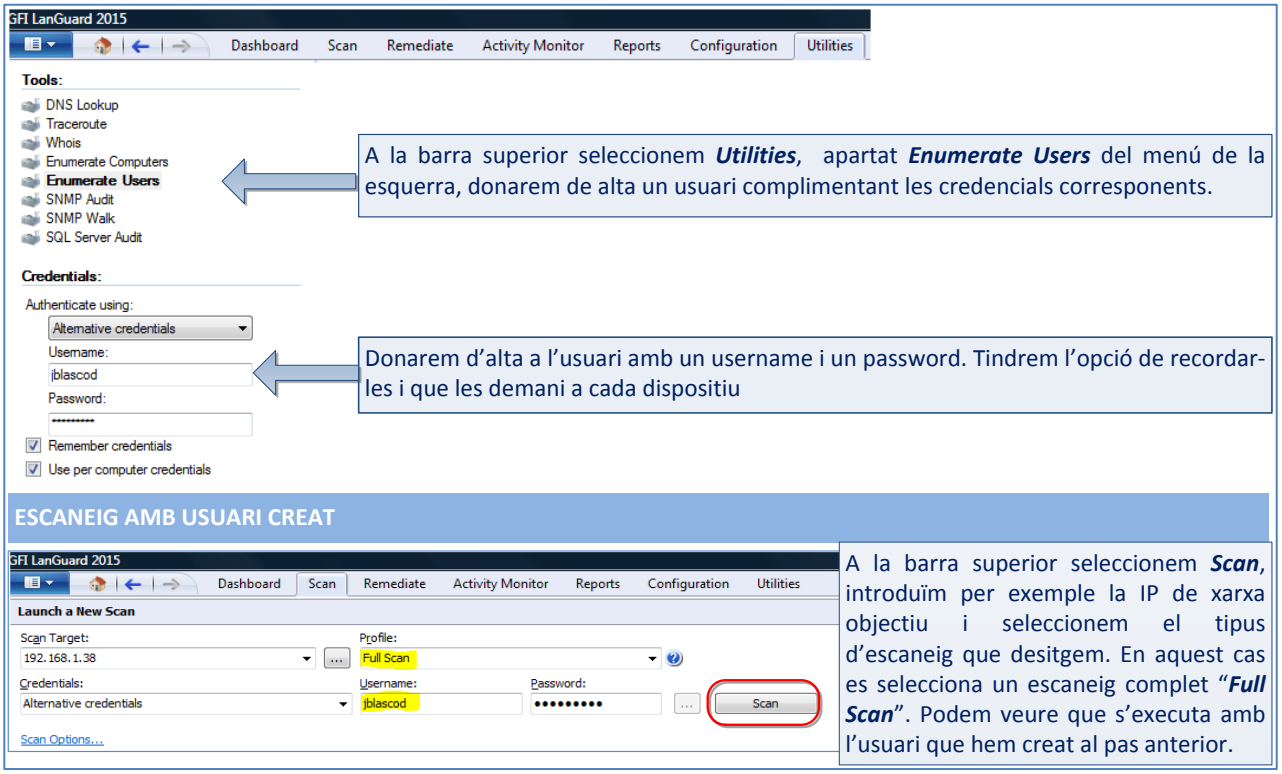
Ens avisa de que es tracta d'una versió de 30 dies amb la limitació dels nodes auditables.



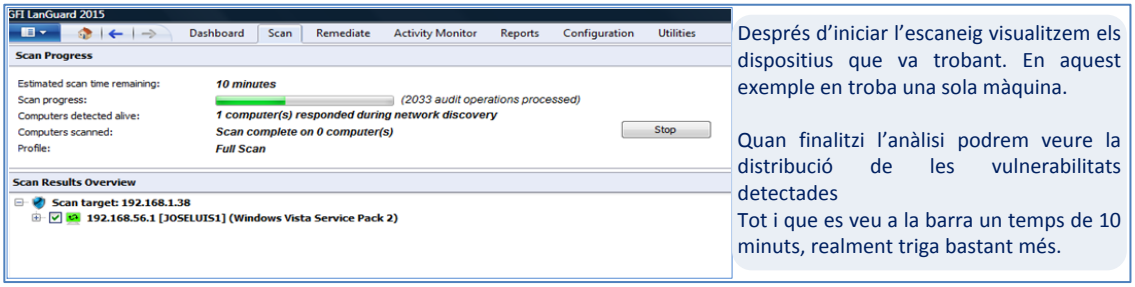
La pàgina d'inici ens mostra els 4 components principals que conformen l'aplicació.

Al menú superior *utilities* podem assignar diferents usuaris a dominis o grups de màquines. Cadascú amb les seves credencials.

A continuació, donarem d'alta a l'usuari *jblascod*. A l'exemple següent s'ha seleccionat l'opció amb recordatori de credencials requerida per a cada màquina. Es demanarà un escaneig complet sobre la IP 192.168.1.38.

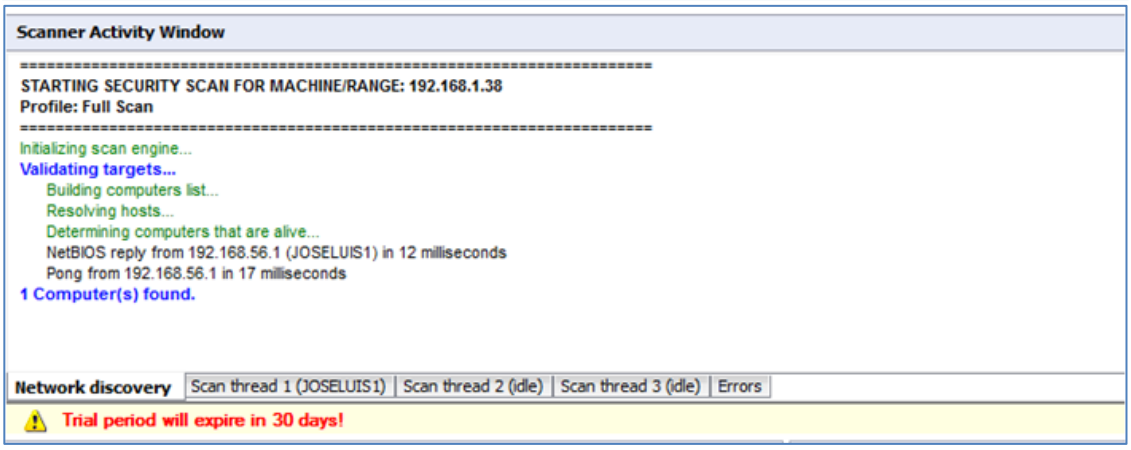


- **ESCANEIG DE LA XARXA:** Iniciem un escaneig inicial de la nostra xarxa per detectar tots els dispositius accessibles:



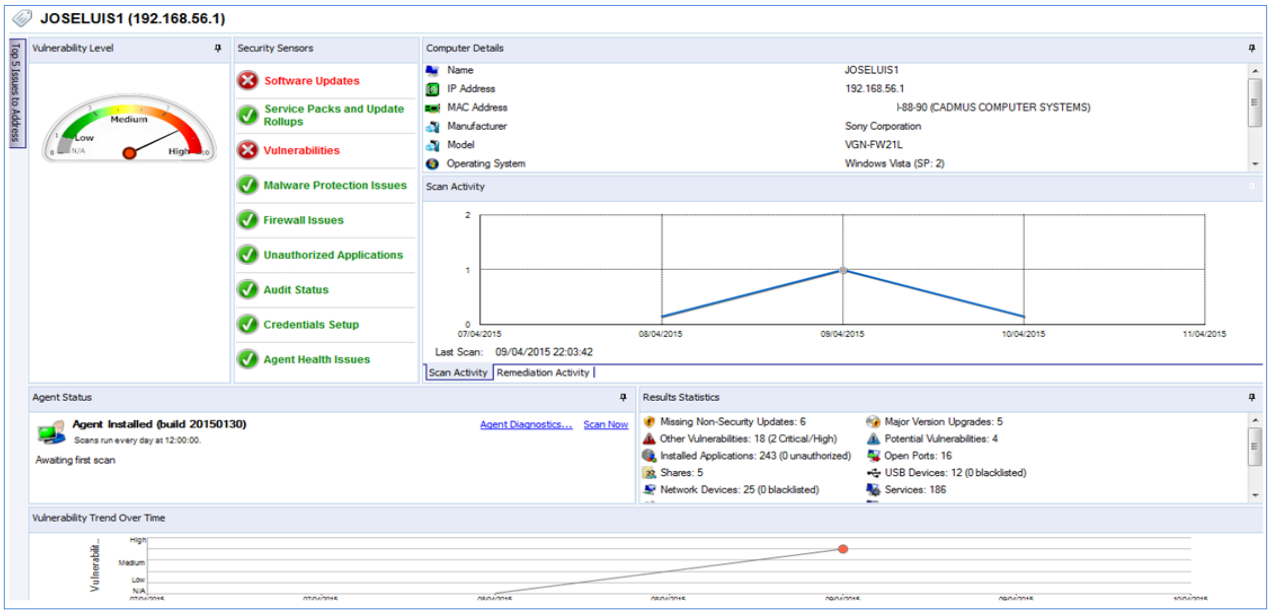
Després d'iniciar l'escaneig visualitzem els dispositius que va trobant. En aquest exemple en troba una sola màquina.

Quan finalitzi l'anàlisi podrem veure la distribució de les vulnerabilitats detectades
Tot i que es veu a la barra un temps de 10 minuts, realment triga bastant més.



- **RESULTATS OBTINGUTS:** Seleccionant a la barra superior *Dashboard* veurem l'anàlisi de vulnerabilitats. Podem observar que els sensors de seguretat avisen de dos problemes basats en actualitzacions de software (*Software Updates*) i diverses vulnerabilitats potencials (Vulnerabilities).

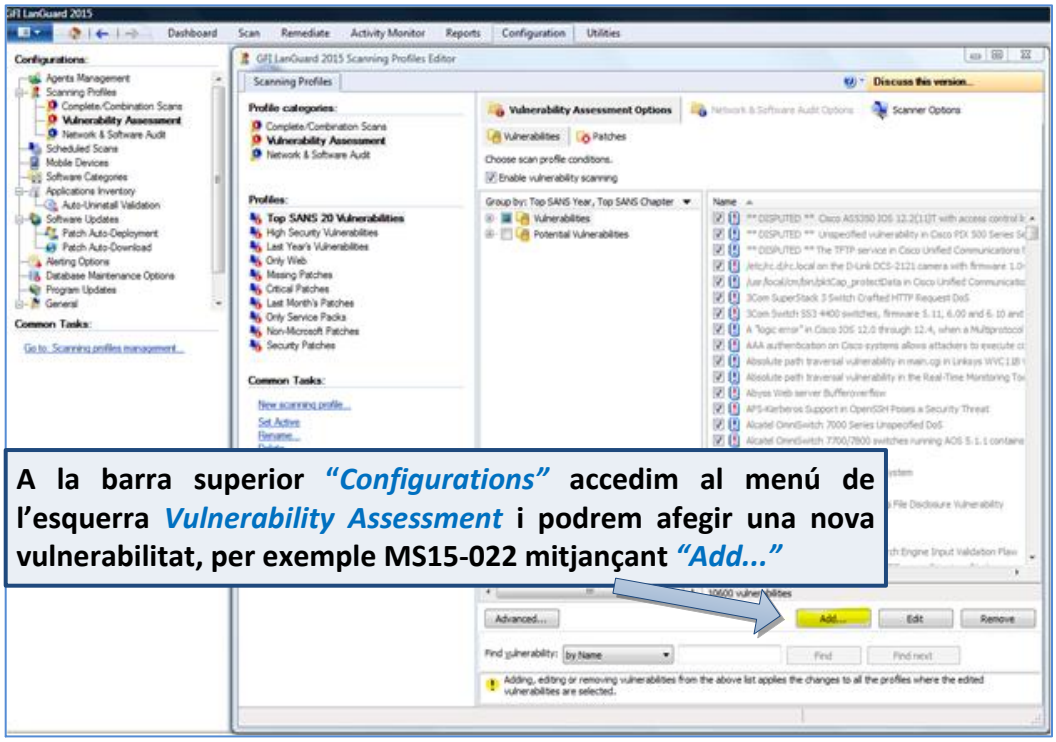
  També podrem tenir un històric del comportament de la xarxa analitzada, visualitzant ràpidament la seva evolució.
  És molt interessant la quantitat d'informació que l'analitzador arriba a extreure del nostre sistema, com per exemple, nom de la màquina, IP real, MAC i fabricant de la targeta de xarxa, fabricant del PC, model i versió del sistema operatiu.



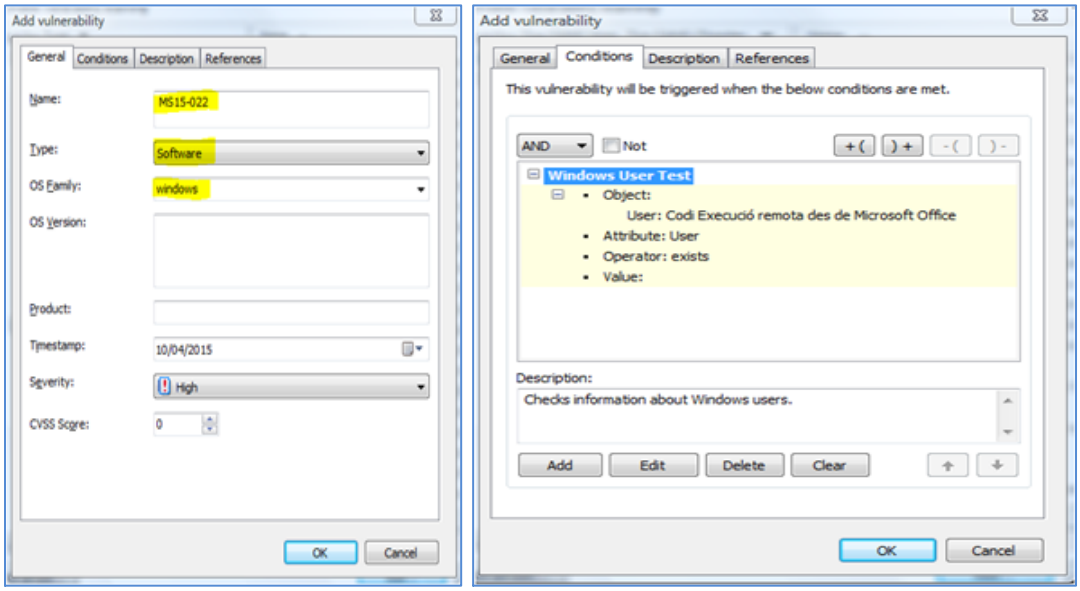
Ens podem fixar que ara, l'indicador de nivell de vulnerabilitat està a la zona vermella de perill.

❖ CONFIGURACIÓ D'UNA NOVA VULNERABILITAT:

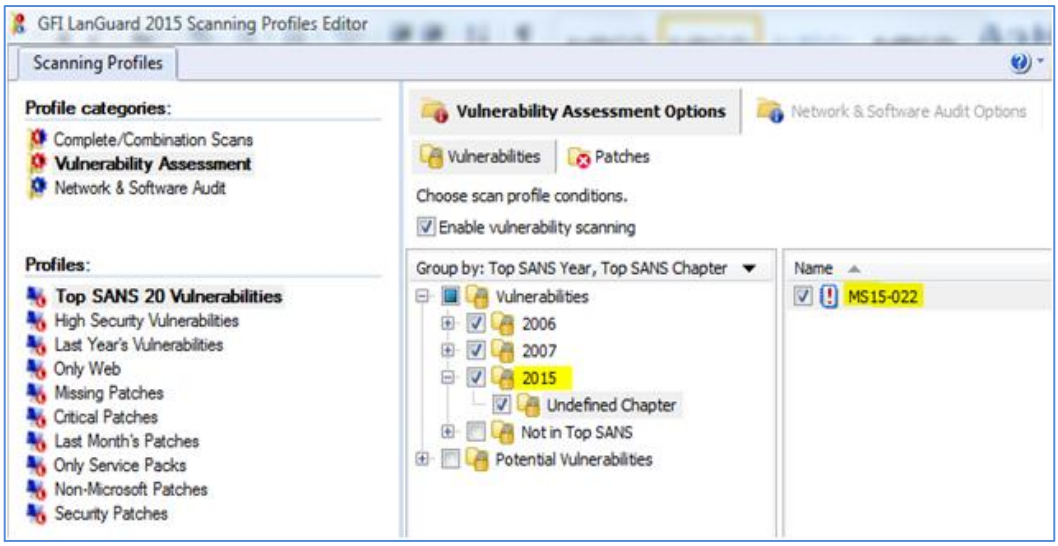
MS15-022 -Vulnerabilitat crítica en Microsoft Office d'execució remota. Aquesta vulnerabilitat d'exemple s'ha extreta de la web https://technet.microsoft.com/en-us/library/security/MS15-022.



Introduïm com a mínim el nom i tipus de vulnerabilitat, en aquest cas MS15-022, la data i la seva rellevància. Posteriorment continuem complimentant les dades sobre la descripció, atributs i condicions per a que s'activi l'avís d'aquesta vulnerabilitat.



Finalment comprovem que s'ha afegit la nova vulnerabilitat al directori de l'any 2015 amb el nom que hem introduït: MS15-022



A partir d'ara, qualsevol auditoria de vulnerabilitats que executi l'aplicació, tindrà en compte aquest tipus de vulnerabilitat introduïda manualment.

Acabem de veure una petita mostra del funcionament d'un escàner de vulnerabilitats, amb l'objectiu de complementar el concepte purament teòric vist al capítol 5, amb una visualització més gràfica de les grans prestacions que ofereix una aplicació d'aquestes característiques.

Annex 2 Instal·lació i configuració de l'Snort

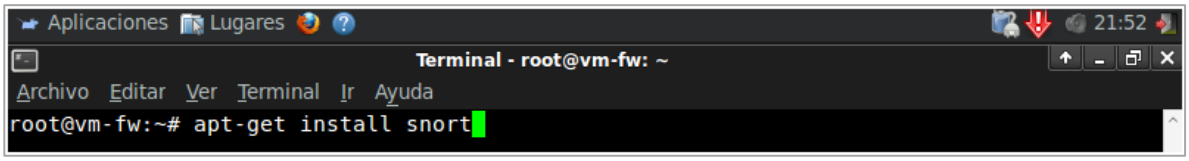
Snort és un dels principals IDS de lliure distribució que utilitza tècniques de detecció de firmes i anomalies. Pot funcionar com un *sniffer* de paquets o com un NIDS (sistema de detecció d'intrusos de la xarxa). També pot treballar com un sistema de prevenció d'intrusions implementant la funcionalitat *inline*.

El seu comportament és ràpid, flexible i altament configurable amb la possibilitat de permetre a l'usuari la creació de regles personalitzades. Podrem veure en aquest apèndix com es creen aquestes regles, les quals, correspondran a les utilitzades en els casos pràctics d'aquest treball, concretament al capítol 6.3.

És un sistema que pot ser integrat amb altres solucions de seguretat i prevenció d'atacs, amb la possibilitat d'augmentar les seves prestacions afegint nombrosos *plugins*.

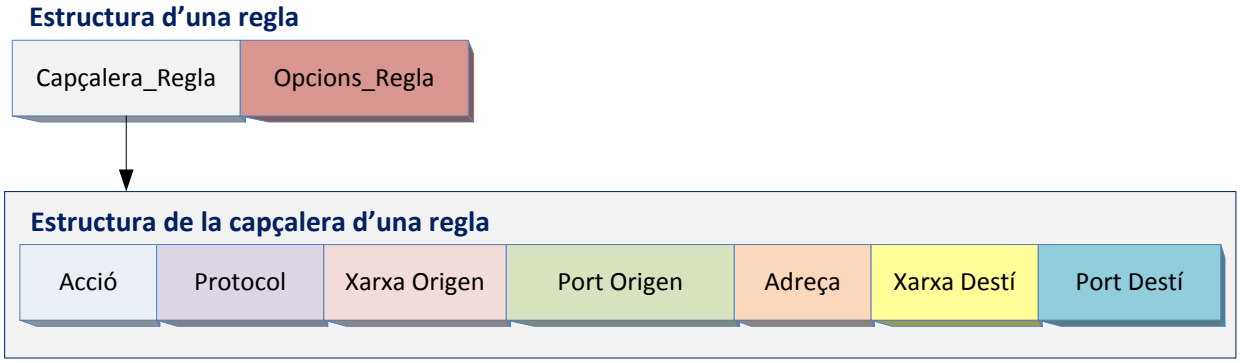
https://www.snort.org/

Amb la instrucció `apt-get install snort` iniciarem el procés d'instal·lació a la màquina virtual **vm-fw** facilitada per la UOC, la qual implementa el sistema operatiu *Linux Ubuntu* (32 bits). La versió que s'utilitza en aquest treball és la 2.8.5.2 (*Build* 121).



➢ Creació de regles personalitzades

El format general de les regles és el següent:



La capçalera permet establir l'origen i el destí de la comunicació. Sobre aquesta informació, *Snort* realitzarà una determinada acció.

En el nostre cas sempre serà una alerta. La capçalera conté alguns criteris per unir la regla amb el paquet i determinar l'acció que ha de prendre aquesta regla.

La seva estructura amb opcions és:

<acció> <protocol a controlar> < ip origen port origen> [->, <-, <>] *<ip destí> < port destí> <(referència: valor; sid: valor; msg: "missatge personalitzat"...;)>*

- **acció:** Permet indicar el tipus d'acció que s'ha de executar sobre el paquet analitzat. Els possibles valors són:
  - *alert*: Genera una alerta utilitzant el mètode d'alerta seleccionat i posteriorment comprova el paquet. Utilitzarem aquest tipus d'acció en les nostres simulacions.
  - *log*: Comprova el paquet.
  - pass: Ignora el paquet.
  - *activate*: Alerta i posteriorment activa una altra regla dinàmica.
  - *dynamic*: roman ociós fins que s'activa una regla, llavors actua com un inspector de regles.
- **protocol:** Permet establir el protocol de comunicacions que s'utilitzarà. Els possibles valors són TCP, UDP, IP i ICMP.
- **xarxa d'origen i xarxa destí:** determina l'origen i destí de la comunicació.
- **port origen i port destí:** permet establir els ports d'origen i destí de la comunicació. Accepta el numero de port o el rang de ports aplicat a la detecció de la xarxa que li precedeix.
- **adreça:** Indica el sentit de la comunicació. Les opcions possibles són "->", "<-" , "<>".

Seguidament a aquestes dades, s'implementaran les opcions de cada regla. A continuació, s'indiquen les més importants:

- **msg:** informa al motor d'alerta el missatge que ha de mostrar. Els caràcters especials de les regles com ":" i ";" han de col·locar-se dintre de l'opció *msg* amb el caràcter "\".
- **flow:** s'utilitza juntament amb els fluxos TCP per indicar que les regles haurien d'aplicar-se solament sobre certs tipus de tràfic.
- **content:** permet que l'*Snort* realitzi una recerca sensitiva per a un contingut específic del *payload* del paquet.
- **referent:** defineix un enllaç a sistemes d'identificació d'atacs externs.
- **classtype:** indica quin tipus d'atacs va intentar el paquet en qüestió. L'opció *classtype* utilitza els atacs classificats i definits a l'arxiu de configuració de l'*Snort* com *classification.config*.
- **sid:** en combinació amb l'opció *rev*, identifica una regla *Snort* relacionant l'ID de la regla individual amb la revisió de la regla.
- **itype:** prova el camp de tipus ICMP davant un valor específic.

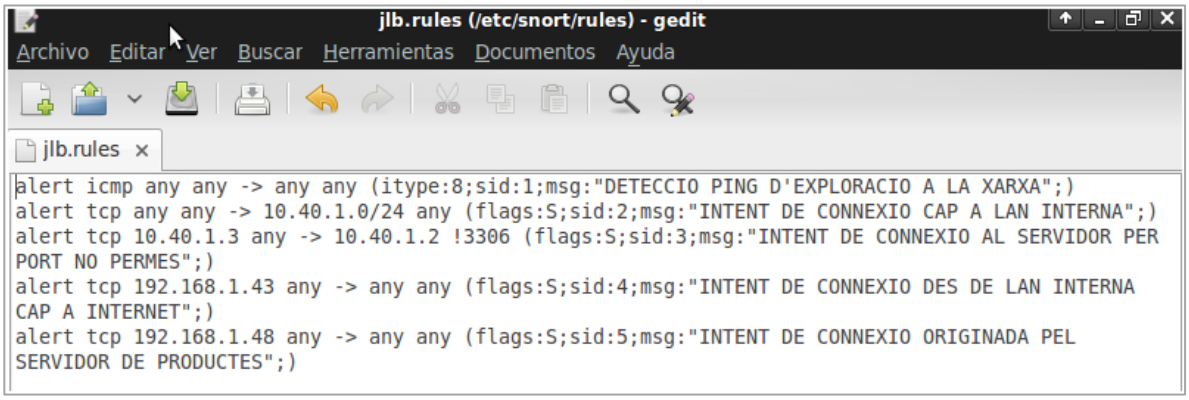
A la web *www.snort.org* trobarem tota la informació referent a la creació de regles i opcions de personalització, ja que és bastant extensa.

➢ Implementació de regles personalitzades

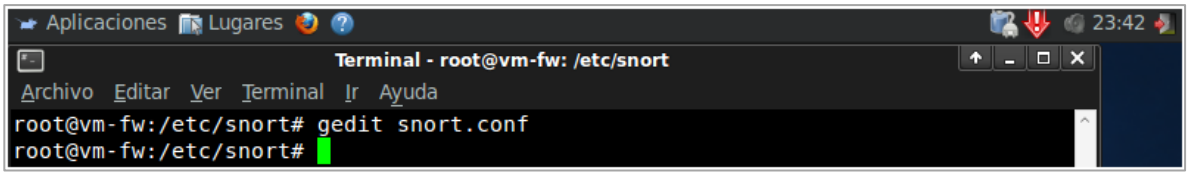
Al directori `/etc/snort/rules` trobarem els arxius amb extensió `.rules`, els quals, són fitxers on s'inclouen les regles amb les que *Snort* utilitzarà per detectar els tipus de moviments que pretenem capturar de la xarxa. A continuació, crearem el nostre propi fitxer de regles, el qual anomenaré **`jlb.rules`**.

Per donar cobertura a les 5 simulacions del capítol 6.3 es configuraran cinc regles:

- Detecció de "*pings*" sospitosos d'exploració a la xarxa des de qualsevol procedència i destí.
- Detecció d'intents de connexions des de qualsevol procedència vers a la LAN interna.
- Detecció d'intents de connexions al servidor de productes per ports no convencionals
- Detecció de connexions originades a la xarxa interna cap a internet.
- Detecció de connexió originada pel servidor de productes cap a qualsevol màquina

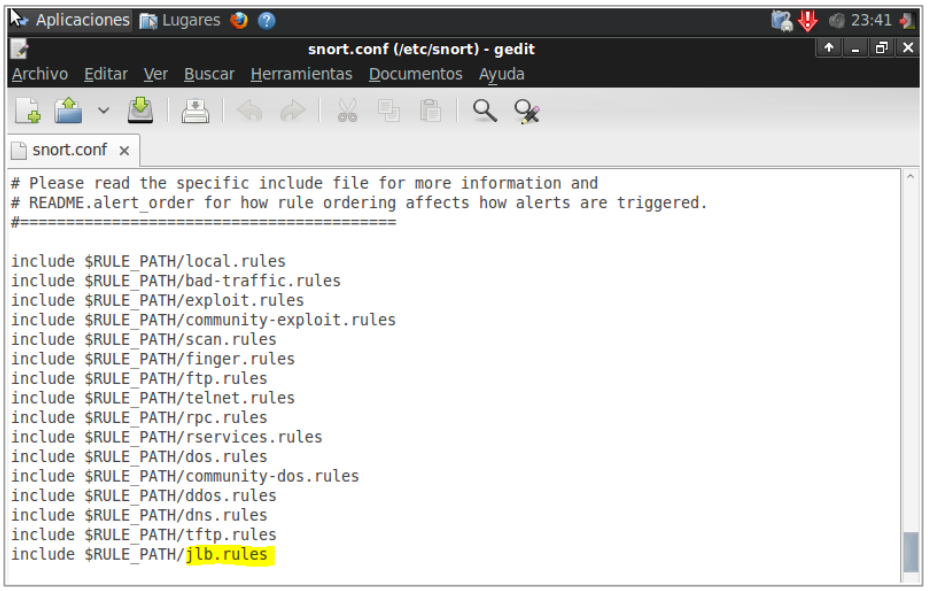


Per a que l'eina *Snort* pugui escanejar la xarxa tenint en compte les regles creades a `jlb.rules`, és necessari afegir aquest arxiu en la configuració de l'*Snort*, concretament a **`/etc/snort/snort.conf`**.



L'objectiu és que quan l'*Snort* s'executi, tingui en compte les regles imposades a l'arxiu `jlb.rules`.

A continuació es mostra l'arxiu de configuració *snort.conf*, on ja està inclòs el nostre arxiu personalitzat `jlb.rules` .



Finalment executem l'Snort amb la instrucció `snort -c jlb.rules -A console -i eth0.`

Amb la part de la instrucció (**`-c jlb.rules`**) especifiquem l'arxiu on es troben les cinc regles amb les quals ha de treballar, (`-A console`) indica mode d'alerta per consola i finalment amb (`-i eth0`) selecciona la escolta per la interfície *eth0* que en aquest cas, correspon a l'enllaç que comunica amb la xarxa externa.

L'Snort comença a escoltar la xarxa...