LANGATON LÄHIVERKKO JA TIETOTURVA

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Riihimäki, kevät 2018

Nico Hätönen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

RIIHIMÄKI
Tietotekniikka
Tietoliikennetekniikka

Tekijä Nico Hätönen **Vuosi** 2018

Työn nimi Langaton lähiverkko ja tietoturva

Työn ohjaaja Marko Grönfors

TIIVISTELMÄ

Opinnäyteyön tarkoituksena oli perehtyä 802.11-standardiin pohjautuvan langattoman lähiverkon toimintaan ja tutkia yleisimpien langattomiin lähiverkkoihin kohdistuvien hyökkäysten toimintaperiaatetta. Opinnäytetyössä käsitellään langattoman lähiverkon tietoturvaa kuluttajalaitteiston osalta ja opinnäytetyön sisällöstä on rajattu yritystason ratkaisut pois. Tästä huolimatta työssä esitelty teoria ja tietoturvauhat pätevät myös yritystason langattomiin lähiverkkoratkaisuihin. Aiheen opinnäytetyöhön valitsin oman kiinnostukseni pohjalta ja opinnäytetyö on kohdistettu tieto- ja tietoliikennetekniikan opiskelijoille.

Opinnäytetyössä käydään läpi langattomiin lähiverkkoihin liittyvää teoriaa ja historiaa näiden kehityksen alusta lähtien. Teoriaosuudessa on avattu yleisimpiä langattomaan lähiverkkoon kohdistuvia hyökkäyksiä ja niiden toimintaperiaatetta tarkemmin.

Opinnäytetyön käytännön osuudessa testataan useimpia työssä esiteltyjä hyökkäyksiä testiverkkoa kohden ja havainnoidaan vaikutuksia langattoman lähiverkon toimintaan sekä käyttäjien yhteyden laatuun. Testiympäristö koostui langattomasta reitittimestä, kahdesta kannettavasta tietokoneesta, älypuhelimesta ja ulkoisesta verkkokortista. Varsinaiseen tietoturvatestaukseen käytettiin Kali Linux -käyttöjärjestelmää ja tämän mukana tulleita tietoturvatestaustyökaluja.

Avainsanat WLAN, 802.11, salaukset, tietoturvatestaus

Sivut 31 s.

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Riihimäki
Degree programme in Information Technology
Networking technology

Author Nico Hätönen **Year** 2018

Subject of Bachelor's thesis WLAN and information security

Supervisor Marko Grönfors

ABSTRACT

The purpose of this thesis was to study the operation of 802.11-based wireless local area networks and examine their most common information security threats. The thesis focuses on information security of wireless local area network when using consumer equipment. Enterprise-level solutions have therefore been ruled out of the subject. Despite this, the theory presented applies to enterprise-level wireless local area network solutions as well. The subject for this thesis comes from my own interest in the wireless technology.

The thesis involves a thorough view of the theory of wireless local area networks and presents the development history of wireless local area networks from the beginning. The theoretical part of the thesis presents also principles of most common attacks against wireless local area networks in depth.

The practical part of the thesis focuses on the most common attacks against wireless local area networks and the direct effects of network performance from user point of view and the wireless network infrastructure itself. Equipment used for the testing involved a wireless router, two laptops, smartphone and an external network interface card. The penetration testing was done by using Kali Linux operating system and the toolkits for information security testing available for Kali.

Keywords WLAN, 802.11, cryptography, penetration testing

Pages 31 p.

TERMIT JA LYHENTEET

Suomi	English	Selite
alustusvektori	Initialization Vector (IV)	Satunnaisnumerosarja
ARP	Address Resolution Protocol	Tietoliikenneprotokolla, jolla selvitetään IP-osoitetta vastaava MAC-osoite.
ARS	Adaptive Rate Selection	Radioliikenteen virheentarkastus-menetelmä.
ASCII	American Standard Code for Information Interchange	Tietokonemerkistö, sisältää numerot 0-9 ja kirjaimet a-z, sekä erikoismerkkejä.
avain	key	Bittijono, jota käytetään salausal-goritmissä datan salaukseen ja purkamiseen.
avainvirta	keystream	Satunnaismerkkijono, jota käyte-tään datan salauksessa.
CCMP	Counter Mode CBC-MAC Protocol	Salausprotokolla
CRC	Cyclic Redundancy Check	Kehyksen eheydentarkastus-menetelmä
esineiden Internet	Internet of Things	Internetiin liittymisen mahdollis-taminen mille tahansa laitteelle.
Ethernet	Ethernet	Joukko lähiverkkotekniikoita.
FCS	Frame Check Sequence	Kehyksen virheentarkastusmene-telmä.
kehys	frame	Siirtoyhteyskerroksen tiedonsiirtoyksikkö.
MAC-osoite	Media Access Control Address	Verkkokortin yksilöivä osoite, pituudeltaan 12 heksadesimaalia eroteltuina kaksoispistein.

(MU)-MIMO	(Multiuser) Multiple Input Multiple Output	Useamman antennin samanaikaisen toiminnan mahdollistava tekniikka.
nelivaiheinen kättely	Four-way handshake	Prosessi, jossa luodaan salausavaimet ja todennetaan käyttäjä.
PBKDF2	Password-Based Key Derivation Function 2	Salauksissa käytetty avaimien johtamistapa.
RC4	Rivest Cipher 4	Salausalgoritmi, jonosalaaja
siltaus	bridging	Verkkotekniikka, jolla yhdistetään useampi lähiverkko.
todennus	authentication	Identiteetin tunnistus.

SISÄLLYS

1 JOHDANTO

Langaton tietoliikenne on yleistynyt rajusti viime vuosikymmenien aikana ja kasvusuunta on yhä ylöspäin. Langaton verkkoteknologia mahdollistaa kantoalueella olevien käyttäjien vaivattoman Internet-yhteyden käytön ilman fyysisten kaapelointien tuomaa rajoitetta. Langatonta verkkoteknologiaa hyödyntäen mahdollistetaan yhteys tietoverkkoon esimerkiksi tiloihin, joihin kaapeloinnin tai yhteyden toteuttaminen olisi muutoin vaikeaa.

Erilaisia langattomia laitteita voidaan liittää nykypäivänä tietoverkkoon ja esimerkiksi teollisuudessa langattomat mittausanturit ja etäluettavat laitteet hyödyntävät jo langattomia tietoliikenneyhteyksiä. Niin kutsuttu esineiden Internet on vahvasti nykypäivää. Langaton lähiverkko on myös käytössä useimmilla kuluttajilla langallisen yhteyden lisänä ja yritysmaailmassa langaton lähiverkko yhä enemmän muuttaa suuntaansa lisäarvopalvelusta vaatimukseksi. Langattomien lähiverkkojen mahdollistaessa yhteydettömän tiedonsiirron ilman fyysistä kaapelointia, on langattomaan tekniikkaan liittyvä tietoturva ollut oleellinen asia kehityksen alkumetreistä lähtien.

Opinnäytetyön teoriaosuudessa perehdytään langattoman lähiverkon historiaan ja toimintaan. Opinnäytetyössä esitellään eri tapoja, miten langattomassa lähiverkossa tapahtuvaa tiedonsiirtoa voidaan suojata, yleisimpiä hyökkäyksiä langattomia lähiverkkoja ja niiden käyttäjiä kohtaan sekä selvitetään miten hyökkäykset itsessään toimivat.

Käytännön osuudessa mallinnetaan teorian pohjalta hyökkäyksiä testiympäristöä vasten. Käytännön testeillä pyritään havainnoimaan hyökkäyksien välitöntä vaikutusta verkon toimintaan ja käyttäjien yhteyden laatuun nähden. Käytännön testeissä käytettiin Linux-pohjaista Kali-käyttöjärjestelmää ja tietoturvatestaamiseen soveltuvaa langatonta verkkokorttia.

2 LANGATTOMAT LÄHIVERKOT

Wireless Local Area Network eli WLAN on verkkoyhteyden langaton jakelumenetelmä radioaaltoja hyväksi käyttäen. Nykypäivänä työasemat voivat liittyä lähiverkkoon kiinteällä yhteydellä tai langattomasti ja useat julkiset tahot, muun muassa hotellit ja lentokentät tarjoavat maksutonta ja avointa WLANia asiakkailleen.

WLAN perustuu lähetin-vastaanotin periaatteeseen ja pohjautuu Institute of Electrical and Electronics Engineer-organisaation, eli IEEE:n hallinnoimaan 802.11-standardijoukkoon. WLAN tunnetaan myös kaupallisella nimellään Wi-Fi (Wireless Fidelity) joka on Wi-Fi Alliancen lanseeraama termi.

Tyypillinen langaton lähiverkko koostuu langattomasta reitittimestä tai tukiasemasta ja langattomista käyttäjistä. Langattomaan reitittimeen määritellään verkko ja käytettävä salaus. Tämän jälkeen verkkoon voidaan yhdistää langattoman verkkokortin omaavalla laitteella. Yhdistettäessä päätelaitteen

langaton verkkokortti ottaa yhteyttä tukiaseman radioantenniin sekä tarkastaa vaadittavat parametrit tähän liittyäkseen. Yhteyden onnistuneen muodostuksen jälkeen voidaan dataa lähettää ja vastaanottaa verkossa.

Tässä luvussa on käyty läpi historiaa ja tekniikkaa langattomaan tiedonsiirtoon liittyen ja pohjustetaan vaadittava teoria langattomien lähiverkkoihin kohdistuvien hyökkäysten avaamiseksi.

2.1 IEEE 802.11

Langattomien lähiverkon kehityskaaren katsotaan alkaneen vuonna 1997, jolloin IEEE spesifioi alkuperäisen 802.11 standardin. Alkuperäinen 802.11-standardi mahdollisti 2Mbit/s teoreettisen tiedonsiirron nopeuden ja standardi operoi 2,4GHz taajuusalueella. Julkaisuhetkenä langallisen Ethernet-yhteyden teoreettinen maksiminopeus oli 10Mbit/s, joten 802.11 tiedonsiirtonopeus ei tähän verrattuna ollut järin suuri.

2.1.1 IEEE 802.11b ja 802.11a

Standardit 802.11a ja 802.11b kehitettiin ja julkaistiin samaan aikaan IEEE:n toimesta vuonna 1999. 802.11b-standardia pidetään langattomien lähiverkkojen osalta läpimurtona ja standardin julkaisemisen jälkeen langattomat lähiverkot yleistyivät muun muassa lentokentillä sekä muissa julkisissa tiloissa, kuin myös yritysmaailmassa.

802.11b-standardi operoi 2,4GHz taajuusalueella ja mahdollistaa teoreettisen tiedonsiirron maksiminopeuden aina 11Mbit/s asti. Standardin mukana esiteltiin myös ARS-ominaisuus, joka mahdollisti tiedonsiirron nopeuden pudottamisen kanavalla esiintyvän radioliikenteen aiheuttaman häiriön mukaan, lisäämällä tiedonsiirron välille enemmän virheentarkastelua. Tällä ominaisuudella parannettiin huomattavasti langattoman yhteyden laatua ja käytettävyyttä. Käytettävän 2,4GHz taajuusalueen vuoksi kantoalue ja radioaaltojen läpäisykyky on 802.11a-standardia parempi.

802.11b-standardista poiketen 802.11a toimii 5GHz taajuudella ja teoreettinen tiedonsiirron maksiminopeus standardia käyttävillä verkkolaitteilla on 54Mbit/s.

802.11a-standardi ei missään vaiheessa langattomien lähiverkkojen kehityskulkua saavuttanut yhtä suurta suosiota kuin 802.11b. Johtuen standardin käyttämästä korkeammasta taajuudesta, langattoman lähiverkon peittoalue on pienempi ja radioaallot läpäisevät esineitä tehottomammin. Myös 802.11a-standardin kanssa yhteensopivien piirikorttien valmistaminen oli 802.11b:hen verrattuna huomattavasti kalliimpaa. (Poole n.d.)

2.1.2 IEEE 802.11g

802.11g-standardi julkaistiin vuonna 2003. 802.11-standardi toimii 2,4 GHz taajuudella ja mahdollistaa maksimitiedonsiirtonopeuden 54 Mbit/s

asti. Standardi toi mukanaan parannuksia aikaisempaan 802.11b:hen nähden ja standardista tuli lopulta yleisimmin käytetty. 802.11g on tänä päivänäkin vielä yleisesti käytössä.

802.11g-standardi on 802.11b-standardin kanssa kääntäen toiminnallinen, eli 802.11g-standardia tukevat verkkolaitteet pystyvät myös kommunikoimaan aikaisempaa 802.11b-standardia käyttävien laitteiden kanssa. Tämä muunnos aiheuttaa tosin tiedonsiirron nopeuden putoamisen, johtuen 802.11b-standardin hitaammasta maksimitiedonsiirtonopeudesta ja pidemmästä kaistanvarausajasta. (Poole n.d.)

2.1.3 IEEE 802.11n

IEEE julkaisi 802.11n-standardin vuonna 2009, tavoitteenaan vastata langallisen Ethernet-yhteyksien kovaa vauhtia kasvaviin tiedonsiirtonopeuksiin. Aikaisempia standardeja suuremman tiedonsiirtonopeuden mahdollistamiseksi, standardissa hyödynnetään MIMO-tekniikkaa. MIMO-tekniikka mahdollistaa useamman antennin käyttämisen tiedonsiirtoon. Enimmillään standardi tukee yhteensä neljää antennia ja mahdollistaa teoreettisen maksimitiedonsiirtonopeuden aina 600Mbit/s asti. 802.11n-standardia käyttäen pystytään myös yhdistämään kaksi tavallista, kaistanleveydeltään 20 MHz kanavaa, yhdeksi 40 MHz levyiseksi kanavaksi, joka nopeuttaa tiedonsiirtoa. Standardin maksiminopeuden saavuttaminen on kuitenkin käytännössä vaikeaa, sillä se vaatii sekä langattomalta tukiasemalta että langattomalta verkkoadapterilta neljä antennia ja johtuen kanavien yhdistämisestä, mahdollisimman häiriövapaan alueen. Standardi operoi 2,4 GHz taajuusalueella ja 5 GHz taajuusalueella.

Muiden ympäristön laitteiden, kuten esimerkiksi mikroaaltouunien tai läheisyydellä olevien toisten langattomien verkkojen aiheuttamista häiriöistä radioliikenteeseen, 802.11n-standardin verkkoja operoidaan yleensä yhdellä kaistanleveydeltään 20 MHz kanavalla. Tällöin tiedonsiirtonopeus standardissa on yhtä antennia ja yhtä kanavaa käyttäen 72Mbit/s. Nopeutta pystytään tosin tehokkaasti nostamaan lisäämällä antennien lukumäärää.

MIMO-tekniikan käyttöönotto standardissa lisää myös standardia käyttävien laitteiden virrankulutusta. Tätä ongelmaa varten standardissa on viransäästöominaisuus, joka kytkee MIMO-tekniikan pois päältä aina kun laitteen käyttöaste on alhainen.

802.11n-standardi on nykypäivänä yksi yleisimmin käytössä oleva. Standardi on taaksepäin yhteensopiva myös standardien 802.11a/b/g kanssa. (Poole n.d.)

2.1.4 IEEE 802.11ac

802.11ac-standardi on IEEE:n vuonna 2013 kehittämä 5 GHz taajuusalueella toimiva ensimmäinen gigabittiluokan langattoman lähiverkon standardi. 802.11ac-standardi pohjautuu aiempiin IEEE:n standardeihin, mutta

sisältää myös uusia ominaisuuksia. Standardien tukemien antennien lukumäärää on nostettu aiemman 802.11n-standardin neljästä antennista kahdeksaan antenniin. 802.11ac-standardissa kanavan kaistanleveys voi olla aiempien standardien 20 MHz ja 40 MHz lisäksi myös 80 MHz tai 160 MHz. Lisäksi standardi pystyy yhdistämään kaksi 80 MHz levyistä kanavaa.

Myös tässä standardissa käytetään MIMO-tekniikkaa ja uutena lisänä MU-MIMOa. MU-MIMO-tekniikkaa hyödyntäen pystyvät 802.11ac-standardia tukevat langattomat tukiasemat ohjaamaan dataa usealle käyttäjälle samanaikaisesti.

Uusien ominaisuuksien ansiosta 802.11ac-standardin teoreettinen tiedonsiirron maksiminopeus on 6,93Gbit/s. Standardi on myös taaksepäin yhteensopiva samalla taajuusalueella operoivien aikaisempien 802.11a- ja 802.11n-standardien kanssa. (Poole n.d.)

2.2 OSI-malli

OSI-malli (Open System Interconnect) on tietoliikennetekniikan malli, jota käytetään kuvaamaan, miten yksittäinen protokolla toimii tai miten data kokonaisuudessa liikkuu tietoverkossa. OSI-malli pitää sisällään seitsemän eri kerrosta. Data kulkee tietoverkossa lähettäjältä OSI-mallin hierarkian ylhäältä alas vastaanottajalle, joka purkaa datan päinvastaisessa järjestyksessä. Langaton lähiverkkotekniikka asettuu OSI-mallin toiselle ja ensimmäiselle tasolle.

Sovelluskerrokselle (Application layer) kuuluvat käyttäjäapplikaatiot, jotka esittävät verkosta vastaanotetun datan oikeassa muodossa loppukäyttäjälle.

Esityskerroksella (Presentation layer) suoritetaan datan konvertointi, esimerkiksi käyttäjän applikaatiota varten. Esitystasolle kuuluvat myös tyypillisesti datan salaus ja salauksen purku.

Istuntokerroksella (Session layer) avataan, ylläpidetään ja lopetetaan istuntoja verkossa.

Kuljetuskerroksella (Transport layer) tapahtuu yhteyksien avaus ja lopettaminen, tärkeimpinä protokollina TCP ja UDP. TCP:n ollessa yhteydellinen protokolla, suoritetaan kuljetustasolla myös virheentarkastelua. UDP-protokollan tapauksessa data lähetetään jatkuvasti ilman, että kohteelta varmistetaan datan olevan vastaanotettu.

Verkkokerroksella (Network layer) tapahtuu IP-osoitus ja liikenteen reititys eri verkkojen välillä. Verkkotason data on pakettimuodossa. Fyysisten ja loogisten osoitteiden yhteen liittäminen tehdään myös verkkokerroksella. Reitittimet sekä reitittämään kykenevät kytkimet operoivat tällä kerroksella.

Siirtoyhteyskerroksella (Data link layer) data on kehysmuodossa. Siirtoyhteyskerros vastaa datakehysten välityksestä laitteiden välillä fyysisen me-

dian yli. Verkon laitteiden fyysinen tunnistaminen tapahtuu myös siirtoyhteystasolla. Siirtoyhteyskerroksella tunnistetaan ja myös korjataan tiedonsiirron aikana tapahtuvia virheitä. Verkkokytkimet toimivat siirtoyhteyskerroksella.

Fyysisellä kerroksella (Physical layer) data on bittimuodossa. Fyysisellä tasolla on itse media, jonka yli datan siirto tapahtuu. (CCNA 200-120 Exam: The 7 Layer OSI Model n.d.)

OSI-mallin kerrokset ja kerroksilla toimivia yleisimpiä protokollia on esiteltynä kuvassa 1.

Nro.	Kerros	Protokollia
7	Application	HTTP, SMTP, FTP
6	Presentation	JPG,MPEG,GIF
5	Session	NetBIOS, PPTP, L2TP
4	Transport	TCP, UDP
3	Network	IPv4, IPv6, ICMP
2	Data link	Ethernet, 802.11, VLAN
1	Physical	Ethernet, token ring

Kuva 1. OSI-mallin seitsemän kerrosta ja kerroksilla toimivia tietoliikenneprotokollia.

2.3 802.11 kehykset

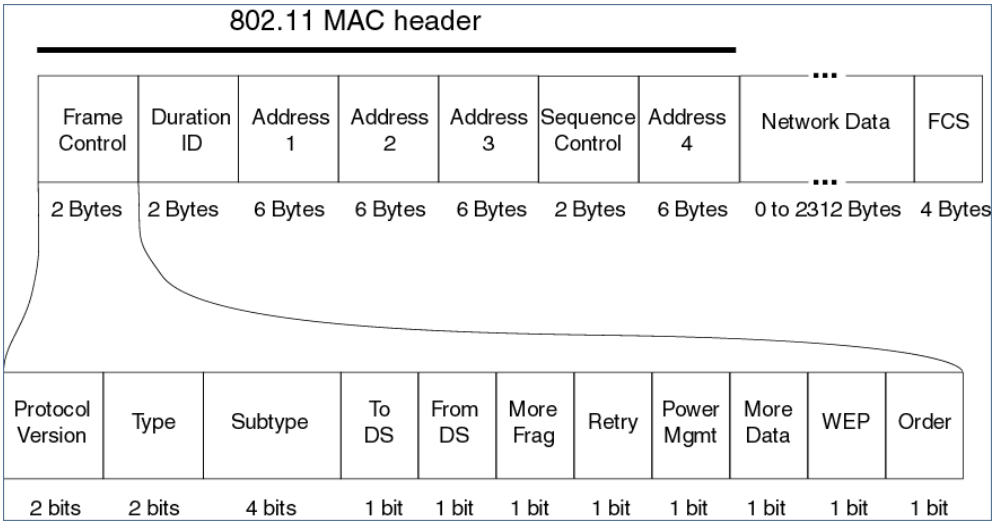
802.11-standardin eri kehystyyppejä on kolme - management, control ja data. Jokaisella näistä on myös useita eri alityyppejä, joita käytetään tiettyjen viestien lähettämiseen.

Management-tyypin kehyksiä käytetään esimerkiksi todentamiseen ja käyttäjän tunnistamiseen.

Control-tyypin kehyksillä hallitaan käyttäjien ja tukiasemien välisiä yhteyksiä, sekä verkossa tapahtuvaa tiedonsiirtoa.

Data-tyypin kehyksissä yleisimmin kulkee itse langattoman median yli lähetettävä data.

802.11-standardin kehysrakenne vaihtelee hieman kehyksen tyypistä ja alityypistä riippuen, mutta on tyypillisimmin alla olevan kuvan mukainen (Kuva 2).



Kuva 2. Langattoman kehyksen perusrakenne. (802.11 WLAN Packets and Protocols. n.d)

Jokainen kehys sisältää vähintään Frame Control- ja Duration ID -kentät, tiedon kehyksen vastaanottajan MAC-osoitteesta sekä kehyksen virheentarkastuskentän FCS.

Kehyksen kahden tavun kokoinen Frame Control -kenttä sisältää tietoa langattoman kehyksen tyypistä, käytetystä standardista, virranhallinnasta sekä tietoturvasta. Tarkemmin Frame Control -kenttä jakaantuu seuraavasti:

- Kehyksessä käytettävä 802.11-standardi (Protocol Version)
- Kehyksen tyyppi (Type)
- Kehyksen alityyppi (Subtype)
- Tieto siitä, onko kehys menossa hajautettuun järjestelmään vai poistumassa siitä. Käytössä vain datakehyksissä (To DS & From DS)
- Tieto siitä, lähetetäänkö kehys palasina ja seuraako kehyksen perässä lisää palasia (More Frag).
- Tieto siitä, onko kyseessä uudelleenlähetys vai ei (Retry)
- Dataa lähettävän aseman tila, aktiivinen vai virransäästötilassa (Power Mgmt)
- Tukiaseman lähettämä tieto virransäästötilassa olevalle asemalle, että kehyksen jälkeen seuraa lisää dataa (More Data)
- Tieto käytetäänkö kehyksen salaukseen WEP-protokollaa ja tuleeko kehys purkaa tämän mukaisesti (WEP)
- Datan prosessointijärjestys (Order)

Kehyksen Duration ID -kenttä on käytössä vain control-tyypin kehyksissä. ID-kenttää käytetään ainoastaan PS-POLL-alityypin kehyksissä kertomaan virransäästötilassa olevan aseman yhdistämistunnus tukiasemalle. Muiden alityyppien tapauksessa, Duration ID -kenttä kertoo ajan, jonka sisällä lähetetty kehys ja vastaanottokuittaus tulee tapahtua.

Osoitekenttien Address 1 – 4 -sisällöt riippuvat kehyksen tyypistä sekä siitä, minkälainen WLAN-ympäristö on käytössä. Kaikkia neljää osoitekenttää ei välttämättä käytetä ollenkaan.

- BSSID (Basic Service Set Identifier), tukiaseman MAC-osoite
- Kohdeosoite (DA), kehyksen lopullisen vastaanottajan MAC-osoite
- Lähdeosoite (SA), kehyksen alkuperäisen lähettäjän MAC-osoite
- Vastaanottimen osoite (RA), aseman MAC-osoite langattomassa verkossa, jolle kehys siirretään seuraavaksi
- Lähettimen osoite (TA), aseman MAC-osoite, joka on lähettänyt kehyksen eteenpäin

Kehyksen osoitetietojen järjestys ja sisältö määrätään Frame Control-kentän To DS & From DS -bittien mukaisesti. Kuvassa 3 on esitelty osoitekenttien tietueet.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

WLAN MAC, Address Field Contents

Kuva 3. Kehyksen osoitetiedot. (RF Wireless World. n.d)

Sequence Control -kentän tarkoituksena on ilmaista samaan kehykseen kuuluvien palasien järjestys ja tunnistaa mahdolliset uudelleenlähetykset.

Kehyksen varsinainen data kulkee Network Data -osiossa. FCS-osiossa tapahtuu kehyksen virheentarkastus. (How 802.11 Wireless Works 2003.)

2.4 Taajuusalueet ja kanavat

Langattomassa lähiverkossa tiedonsiirto tapahtuu kahdella eri taajuusalueella riippuen käytetystä standardista. Yleisimmin käytetty taajuusalue on 2,4GHz. Kyseinen taajuusalue pitää sisällään yhteensä 14 eri kaistanleveydeltään 22 MHz kanavaa jaoteltuina 5MHz:n välein. Käytössä olevien kanavien lukumäärä on maakohtainen ja esimerkiksi Suomessa on sovittu käytettävän kolmeatoista kanavaa. 2,4GHz taajuusalueella käytettävissä olevat kanavat ovat esiteltynä kuvassa 4.

Kanavien jaottelusta ja kaistanleveydestä johtuen osa kanavista menee päällekkäin ja lähekkäin olevilla kanavilla kommunikoivat laitteet aiheuttavat häiriöitä tiedonsiirtoon. Suositeltavaa on käyttää ei-päällekkäisiä kanavia, esimerkiksi kanavia 1, 6 ja 11, jotta häiriöiltä vältytään. (Poole n.d.)

Kanava	Pienin taajuus (MHz)	Keskitaajuus (MHz)	Suurin taajuus (MHz)
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

Kuva 4. Kuva 2,4GHz taajuusalueesta ja kanavista.

Toinen käytettävissä oleva taajuusalue on 5GHz, jota käyttää 802.11 standardeista a, n ja ac. Tarkemmin taajuusalue ulottuu noin 5180MHz aina 5825MHz asti. Kanavien kaistanleveys on 20MHz ja kyseinen taajuusalue sisältää kanavia yhteensä 24 kappaletta. Käytettävien kanavien lukumäärä on maakohtainen ja Suomessa käytössä on vain 19 kanavaa.

5GHz taajuusalue on häiriövapaampi kuin 2,4GHz, sillä useimmat häiriötä aiheuttavat elektroniikkalaitteet operoivat matalammilla taajuuksilla. Korkeampaa 5GHz taajuutta käyttäen pystytään myös nopeampaan tiedonsiirtoon, mutta 5GHz radioaallot eivät läpäise esineitä yhtä hyvin jonka takia signaalin kantama on lyhyempi. Suomessa käytössä olevat 5GHz taajuusalueen kanavat näkyvät kuvassa 5. (Poole n.d.)

taajuusalue (MHz)	numero	rajoitukset
5180 - 5200	36	vain sisätiloissa
5200 - 5220	40	vain sisätiloissa
5220 - 5240	44	vain sisätiloissa
5240 - 5260	48	vain sisätiloissa
5260 - 5280	52	vain sisätiloissa
5280 - 5300	56	vain sisätiloissa
5300 - 5320	60	vain sisätiloissa
5320 - 5340	64	vain sisätiloissa
5500 - 5520	100	
5520 - 5540	104	
5540 - 5560	108	
5560 - 5580	112	
5580 - 5600	116	
5600 - 5620	120	
5620 - 5640	124	
5640 - 5660	128	
5660 - 5680	132	
5680 - 5700	136	
5700 - 5720	140	

Kuva 5. Suomessa käytetyt 5GHz taajuusalueen kanavat. (Radiotaajuuskirja/langaton lähiverkko, 2015)

2.5 ESSID ja BSSID

ESSID eli Extended Service Set Identifier, on langattoman lähiverkon nimi. Usein puhutaan myös pelkästään SSID:stä. SSID on pituudeltaan maksimissaan 32 merkkiä ja se määritetään verkkoa luodessa. Tukiasemat mainostavat tarjoamiaan SSID:tä beacon-tyypin kehyksillä tasaisin väliajoin. Beacon on yksi management-kehyksien alityypeistä ja sisältää myös tietoa verkossa käytettävistä asetuksista, kuten tiedonsiirtonopeudesta ja kanavasta.

Laajemmissa WLAN-ympäristöissä sama SSID on yleensä käytössä usealla tukiasemalla ja tukiasemien yksilöimiseksi jokaisella tukiasemalla on oma BSSID (Basic Service Set Identifier). BSSID on tukiaseman radion MAC-osoite ja mikäli useampia SSID:tä käytetään, generoidaan jokaiselle SSID:lle tukiasemakohtainen BSSID tukiaseman radion MAC-osoitteen

pohjalta. (Understanding the Network Terms SSID, BSSID, and ESSID 2015.)

3 SUOJAUKSET JA YLEISIMMÄT HYÖKKÄYKSET

Langattoman lähiverkon yleistymisen ja kehityksen myötä on verkon tietoturvan varmistamiseksi kehitetty erilaisia tekniikoita salata verkossa tapahtuvaa tiedonsiirtoa ja itse verkkoon liittymistä. Langattoman lähiverkon tietoturvasta huolehtimalla rajoitetaan asiattomien käyttäjien pääsyä verkkoon ja verkon mahdollistamiin resursseihin sekä pyritään estämään verkossa tapahtuvan tiedonsiirron häiritsemistä.

Langattoman lähiverkkotekniikan ollessa käytössä jo vuodesta 1997 lähtien, on kehityskaaren aikana havaittu useita erinäisiä haavoittuvuuksia kehitettyjen salausten ja verkon toiminnallisuuden osalta, jotka vaarantavat eheän tiedonsiirron verkon yli ja mahdollistavat pahimmillaan asiattomien käyttäjien liittymisen langattomaan lähiverkkoon näitä tietoturva-aukkoja hyväksikäyttäen.

Tässä luvussa on käyty läpi yleisimpiä langattoman lähiverkon salauksia tarkemmin ja langattomaan lähiverkon heikkouksia, yleisimpiä hyökkäyksiä sekä niiden toimintaperiaatetta.

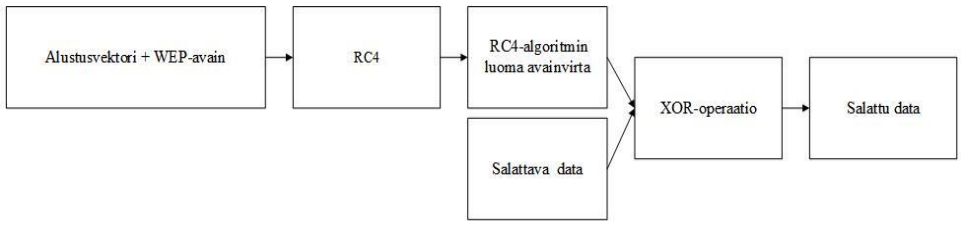
3.1 WEP

Wired Equivalent Privacy (WEP) on IEEE:n vuonna 1997 alkuperäisen 802.11-standardin mukana julkaistu tiedon salaamista ja käyttäjän todennusta varten kehitetty salausmenetelmä. WEP-salaus kehitettiin turvaamaan langattomia lähiverkkoja, jotta voitaisiin estää asiattomien käyttäjien liittyminen verkkoon ja suojata verkossa liikkuvaa dataa.

WEP on niin sanottu symmetrinen salaus, eli sekä vastaanottaja ja lähettäjä käyttävät aina samaa avainta datan salaukseen sekä purkamiseen. Myös verkkoon kirjautuminen tapahtuvaa samaa avainta käyttäen. WEP:ssä datakehyksen eheydentarkistuksesta vastaa CRC32-tarkistussummamenetelmä.

WEP-avaimen pituus oli alkuperäisessä standardissa 40 bittiä ja myöhemmin avaimen pituutta nostettiin turvallisuuden parantamiseksi 104 bittiin asti. WEP-avain voidaan määrittää heksadesimaalimuodossa tai ASCII-merkeillä.

Kuvassa 6 havainnollistetaan WEP-salauksen toimintaa. Datan salauksessa käytetään RC4-jonosalausmenetelmää ja satunnaisesti luotua 24 bitin mittaista alustusvektoria. RC4-algoritmi luo WEP-avaimen ja alustusvektorin pohjalta satunnaisen avainvirran, jolle tehdään vielä lopuksi salattavan viestin kanssa looginen XOR-operaatio. Lopuksi salatun datan eteen liitetään vielä salaukseen käytetty alustusvektori. Datakehyksen vastaanottaja purkaa WEP-salatun kehyksen käyttämällä tiedossa olevaa WEP-avainta ja alustusvektoria. (Wong 2003, 1 - 3)

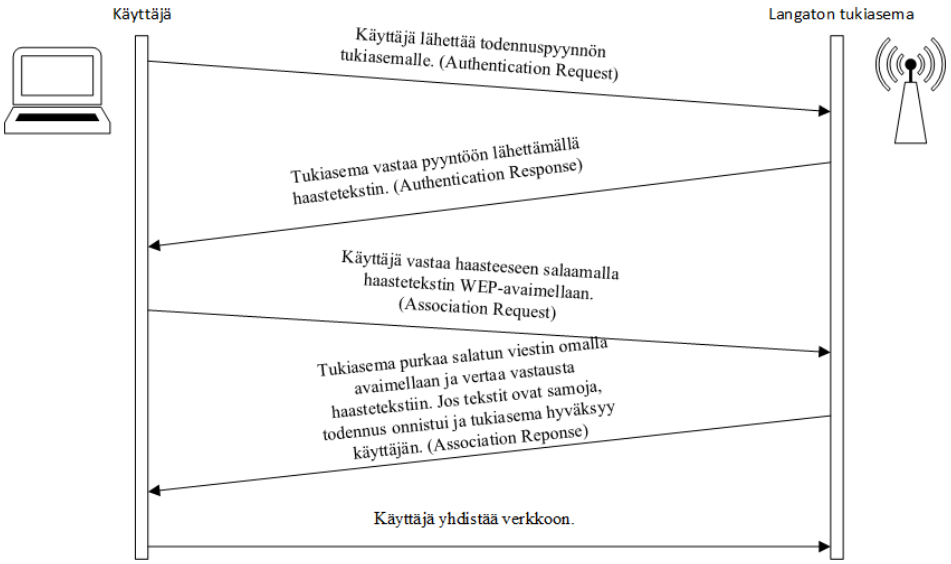


Kuva 6. WEP-salauksen toimintaperiaate.

3.1.1 Todennus WEP-suojattuun langattomaan lähiverkkoon

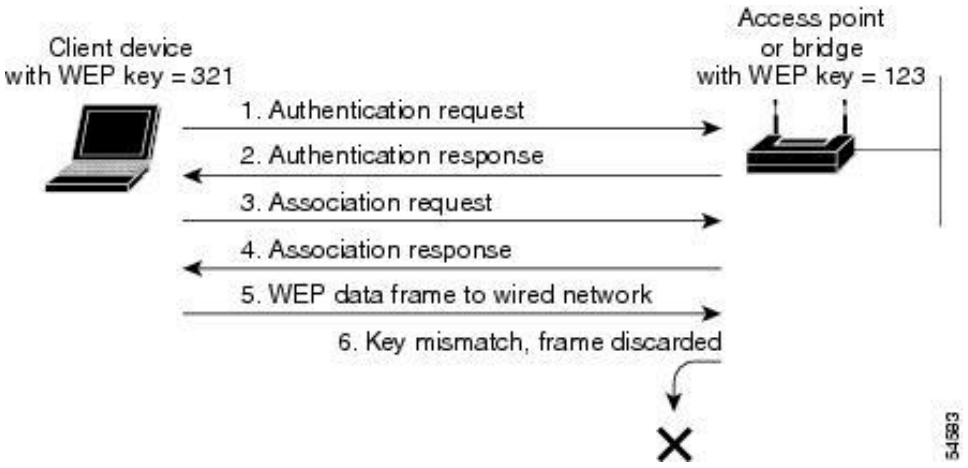
WEP-suojattuun langattomaan lähiverkkoon voidaan liittyä kahdella eri tavalla, joko haaste-vaste -todennuksen kautta tai avointa todennusta käyttäen.

Haaste-vaste -todennuksessa käyttäjä aloittaa todennuksen lähettämällä tukiasemalle todennuspyynnön. Tukiasema vastaa tähän pyyntöön lähettämällä haastetekstin, jonka käyttäjä salaa tiedossa olevalla WEP-avaimellaan. Käyttäjä lähettää salatun viestin tukiasemalle ja mikäli tukiasema pystyy WEP-avaimellaan purkamaan salatusta kehyksestä alkuperäisen haastetekstin, hyväksytään ja todennetaan käyttäjä verkkoon. (Kuva 7)



Kuva 7. Haaste-vaste -todennus WEP-suojatussa langattomassa lähiverkossa.

WEP-salauksen kanssa voidaan käyttää myös avointa todennusta, jolloin kuka tahansa langattomaan lähiverkkoon haluava voi todentaa ja yhdistää verkkoon, mutta ei pysty ilman oikeaa WEP-avainta kommunikoimaan verkossa (Kuva 8).



Kuva 8. Avoin todennus WEP-suojattuun langattomaan lähiverkkoon. Väärän WEP-avaimen tapauksessa, tukiasema tiputtaa kehykset. (Understanding Authentication Types 2018.)

3.1.2 WEP-salauksen haavoittuvuudet

WEP-salauksesta on paljastunut sen julkaisemisen jälkeen useita heikkouksia, eikä sen käyttö ole ollut suositeltavaa pitkään aikaan, mikäli käytössä olevat päätelaitteet tukevat uudempia 802.11-standardeja. WEP-salauksesta tekevät heikon WEP-avaimen symmetrisyys, muuttumattomuus, saman avaimen käyttö käyttäjien todentamiseen ja datan salaamiseen, salaukseen käytettävän alustusvektorin lyhyt pituus ja puutteellinen kehyksen eheydentarkistus.

Alustusvektorin kiinteän 24 bitin pituuden myötä mahdollisia erilaisia alustusvektoreita on olemassa yhteensä rajattu määrä, 16777215 kappaletta. Alustusvektori kulkee WEP-salatussa kehyksessä salaamattomana osiona ennen WEP-salattua dataa, ja koska alustusvektoria myös käytetään yhdessä WEP-avaimen kanssa salaamaan itse data, voi hyökkääjä tarpeeksi dataa kerättyään vertailla samaa alustusvektoria käyttäviä datakehyksiä ja selvittää WEP-avaimen näiden yhtäläisyyksien avulla. Tätä hyökkäystä kutsutaan liittyvä avain -hyökkäykseksi. Riippuen langattoman lähiverkon liikennemääristä, voi WEP-avaimen murtaminen viedä parhaimmillaan vain muutamia minuutteja. (Related-key attack 2015; Beaver & Davis 2005, 259 - 262)

3.2 WPA-TKIP

Wi-Fi Protected Access (WPA) on Wi-Fi Alliancen kehittämä ja vuonna 2003 julkaistu salaus. WEP-salauksessa ilmenneiden heikkouksien jälkeen, alkoi IEEE kehittelemään 802.11i-tietoturvastandardia, joka toisi mukanaan parannetun salauksen langattomille lähiverkoille. Samalla aikaa Wi-Fi Alliance vastasi tarpeeseen suojata langattomissa lähiverkoissa liikkuvaa informaatiota WEP-salausta paremmin kehittämällä WPA-salauksen, joka suunniteltiin toimimaan väliaikaisena salauksena ennen varsinaisen IEEE:n tietoturvastandardin julkaisua. WPA oli hyvä ratkaisu, koska se hyödynsi

myös datan salauksessa RC4-jonosalaajaa ja näin ollen mahdollisti käyttöönoton pelkän ohjelmistopäivityksen avulla.

WPA käyttää datan salaukseen Temporal Key Integration Protocol -nimistä salausta (TKIP) ja vahvempaa kehysten eheydentarkistusmenetelmää Message Integrity Checkiä (MIC). TKIP:ssä alustusvektorin pituus on tuplasti pidempi verrattuna WEP-salaukseen, eli 48 bittiä. TKIP pitää myös huolen siitä, ettei samaa salausavainta käytetä kuin yhdessä datakehyksessä. Uusien ominaisuuksien ansiosta WPA:n avulla voitiin data salata huomattavasti tehokkaammin kuin edeltäjässään WEP:ssä. (Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks 2003)

3.3 WPA2-CCMP

Vuonna 2004 Wi-Fi Alliance julkaisi Wi-Fi Protected Access 2 -salauksen (WPA2), jonka IEEE ratifioi samana vuonna 802.11i-standardiksi. Vuotta aikaisemmin julkaistun WPA:n ollessa vielä varsin tuore, oli WPA2:n käyttö alkuaikoina varsin vähäistä, mutta sittemmin WPA2:n käyttöaste on noussut vahvasti ja vuodesta 2006 edellytetään jokaiselta uudelta Wi-Fi-sertifioidulta langattomalta verkkolaitteelta WPA2-tukea. Tänä päivänä WPA2-suojaus on yleisin ja luotettavimmaksi todettu tekniikka langattomien lähiverkkojen suojaukseen.

WPA2 toi mukanaan edeltäjäänsä vahvemman datan salauksen CCMP-lohkosalaajan myötä, joka pohjautuu Advanced Encryption Standard -tietoturvastandardiin (AES). AES-salausalgoritmi on yleisesti tunnustettu hyvin vahvaksi. Myös WPA2:ssa käytetään kehysten eheydentarkastuksessa MIC:iä. (The State of Wi-Fi Security 2012)

3.3.1 Todennus WPA- ja WPA2-suojattuihin verkkoihin

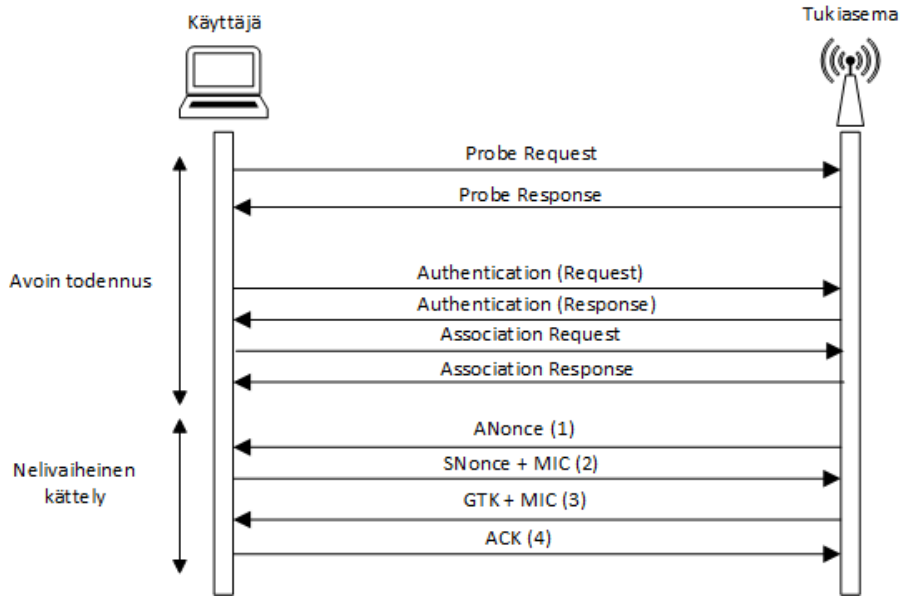
Käyttäjän todennus tapahtuu WPA- ja WPA2-suojatuissa verkoissa niin kutsutun neliosaisen kättelyn kautta (Kuva 9). Neliosainen kättely tehdään tukiaseman ja käyttäjän välillä ja aloitetaan, kun tukiasemaan yhdistävä käyttäjä on jo suorittanut avoimen todennuksen. Kättelyssä tukiasema ja todennettava käyttäjä luovat vaadittavat avaimet datan salaamiseen ja purkamiseen.

WPA- tai WPA2-salausta voidaan käyttää joko Personal- tai Enterprise-tilassa. Personal-tilan tapauksessa verkolle määrätään Pre-Shared Key (PSK), jonka pituus on kokonaisuudessaan 256 bittiä. PSK voidaan antaa joko 64 pituisena heksadesimaalina tai 8 – 63 pituisena ASCII-merkkeinä. Mikäli PSK annetaan ASCII-merkeillä, lasketaan annettujen ASCII-merkkien ja SSID:n pohjalta PSK käyttäen PBKDF2-menetelmää.

Avaimien luomiseen vaaditaan Pairwise Master Key (PMK), joka luodaan Personal-tilan tapauksessa PSK:n ja SSID-nimen pohjalta, Enterprise-tilan tapauksessa erillinen todennuspalvelin luo PMK:n ylimääräisen todennuksen päätteeksi, joka tapahtuu ennen nelivaiheisen kättelyn aloittamista.

Luotu PMK lähetetään todennuspalvelimelle tehdyn todennuksen jälkeen lopulta tukiasemalle. Nelivaiheisen kättelyn suorittamiseen käytetään Extensible Authentication Protocol over LAN-protokollaa (EAPOL).

1. Tukiasema aloittaa kättelyn lähettämällä todennettavalle käyttäjälle ANonce-viestin, joka on tämän luoma satunnaisnumerosarja. Saatuaan ANonce viestin tukiasemalta, käyttäjä luo PTK-avaimen (Pairwise Transient Key) PMK-avaimen, ANonce-numerosarjan ja muiden parametrien pohjalta. PTK-avain on voimassa niin pitkään, kun käyttäjä on yhdistäneenä langattomaan lähiverkkoon ja tätä käytetään tukiaseman sekä käyttäjän välisen datan salaamiseen tänä aikana.
2. Käyttäjä lähettää SNonce-viestin tukiasemalle, jossa taasen on käyttäjän oma satunnaisnumerosarja. Viestissä kulkee myös MIC-eheydentarkistusmenetelmän mukainen tarkistussumma.
3. Vastaanotettuaan viestin käyttäjältä, tukiasema tarkastaa vastaanotetun kehyksen eheyden ja luo samaan tapaan PTK-avaimen itselleen. Tukiasema generoi myös Group Master Keyn (GMK) PMK:n pohjalta, joka lähetetään kolmannessa viestissä käyttäjälle. GMK:ta käytetään broadcast-liikenteen salaukseen. Kolmannessa viestissä on mukana myös MIC-eheydentarkastus.
4. Käyttäjä tarkastaa kolmannen viestin eheyden ja mikäli virheitä ei ole tapahtunut, asennetaan luodut PTK- ja GTK -avaimet käyttöön salattua tiedonsiirtoa varten. Neljäs viesti on käyttäjän tukiasemalle lähettämä kuittaus siitä, että sekä käyttäjä ja tukiasema omaavat samat avaimet ja myös tukiasema voi asentaa nämä käyttöön. (IEEE 802.11i-2004 2018.)



Kuva 9. Täydellinen todennus ja yhdistäminen WPA/WPA2-suojattuun verkkoon SSID:n kysymisestä lähtien.

3.3.2 Heikkoudet WPA- ja WPA2-salauksissa

WPA-TKIP:n alkuperäinen tarkoitus oli toimia vain väliaikaisena ratkaisuna ennen WPA2:n kehittämistä ja TKIP-salauksesta on löydetty vuosien mittaan haavoittuvuuksia. Wi-Fi Alliance on todennut WPA-TKIP:n

vuonna 2015 vanhentuneeksi salausmenetelmäksi ja suosittelee sen käytön lopettamista. (Technical Note Removal of TKIP from Wi-Fi Devices 2015)

WPA ja myös WPA2 ovat haavoittuvaisia niin kutsulle sanakirjahyökkäykselle. Sanakirjahyökkäyksellä pyritään selvittämään langattoman lähiverkon PSK, jota käytetään neliosaisessa kättelyssä PTK-avaimen luontiin. Sanakirjahyökkäyksen toteuttaminen vaatii neliosaisen kättelyn taltioinnin, jonka jälkeen hyökkääjällä on kaikki vaadittavat parametrit PTK-avaimen luomiseen, lukuun ottamatta itse PSK:ta. Sanakirjahyökkäyksessä käytettävä ohjelmisto käy läpi sanalistaa ja käyttää listan sanoja muodostaakseen PSK:n ja tämän sekä nelivaiheisen kättelyssä taltioitujen parametrien avulla PTK-avaimen. Luodulle PTK-avaimelle lasketaan MIC-tarkistussumma ja tätä verrataan taltioidussa nelivaiheisessa kättelyssä nähtyyn tarkistussummaan. Mikäli summat täsmäävät, voidaan todeta avaimen muodostukseen käytetyn PSK:n olevan oikein. Hyökkäys vaatii paljon laskentatehoa ja onnistumisen todennäköisyys laskee, mitä monimutkaisempi PSK verkolle on määritetty käyttöön. (Understanding WPA/WPA2 Pre-Shared-Key Cracking 2015)

WPA2 AES-pohjaista salausta on pitkään pidetty murtumattomana, kunnes vuonna 2017 belgialaiset Mathy Vanhoef ja Frank Piessens julkaisivat tutkimuksensa, joka todisti haavoittuvuuden nelivaiheisessa kättelyssä. Tätä ennen WPA- ja WPA2-salauksiin liittyvät haavoittuvuudet olivat liittyneet enimmäkseen liian yksinkertaisiin PSK:hin, mihin sanakirjahyökkäyskin pohjautuu.

Vanhoefin ja Piessensin niin kutsuttu Key Reinstallation Attack (KRACK) aiheutti nimensä mukaisesti datan salaamiseen käytettävien avainten uudelleen asennuksen. Hyökkäyksessä nelivaiheisen kättelyn kolmas viesti lähetettiin uudelleen käyttäjälle, jonka myötä käyttäjä asensi jo aiemmin neuvotellut avaimet uudelleen ja resetoi alkuarvoihin parametrejä, joita käytettiin avaimien muodostukseen.

KRACK-hyökkäyksessä hyökkääjä asettuu ensin käyttäjän ja langattoman tukiaseman väliin ja estää käyttäjää lähettämistä nelivaiheisen kättelyn viimeistä viestiä tukiasemalle. Tästä syystä tukiasema olettaa, ettei kolmas viesti koskaan tullut perille ja lähettää tämän uudestaan. Kun nelivaiheinen kättely suoritetaan kokonaisuudessaan ensimmäisen kerran, lähettää käyttäjä viimeisen, neljännen viestin tukiasemalle salaamattomana. Mikäli luotuja avaimet asennetaan uudelleen, lähtee neljäs viesti käyttäjältä salattuna tukiasemalle. Hyökkääjä voi näin ollen taltioituaan salaamattoman neljännen viestin, salatun neljännen viestin avainten uudelleenasennuksen jälkeen sekä tietäessään avainten luontiin käytettyjen parametrien resetoituvan tiettyihin arvoihin verrata näiden yhtäläisyyksiä ja purkaa datapakettien salauksia.

Vanhoef ja Piessens havaitsivat tutkimuksessaan myös vakavan haavoittuvuuden Linux-pohjaisissa käyttöjärjestelmissä ja Android-mobiilikäyttöjärjestelmässä versiosta 6.0 eteenpäin, jolloin nelivaiheisessa kättelyssä luotujen avainten uudelleenasennuksen sijaan laite asensikin avaimet, joiden ar-

vona oli pelkkiä nollia. Tämän myötä hyökkääjä pystyi vaivattomasti purkamaan minkä tahansa datapaketin salauksen, kun salaukseen käytettävä avain oli tiedossa. Suurimmat laitevalmistajat ovat kuitenkin jo julkaisseet tietoturvapäivityksiä, jotka torjuvat KRACK-hyökkäyksen ja estävät avaimien uudelleenasennuksen. (Vanhoef & Piessens 2017)

3.4 WPS

Wi-Fi Protected Setup (WPS) on Wi-fi Alliancen vuonna 2007 julkaisema tekniikka, joka yksinkertaistaa uusien laitteiden liittämistä langattomaan lähiverkkoon. WPS:ää käyttämällä laitteita voidaan liittää langattomaan lähiverkkoon napinpainalluksella tai yleensä 8 numeron mittaista PIN-koodia käyttämällä, joten käyttäjän ei tarvitse muistaa mahdollisesti hyvin monimutkaiseksi määritettyä langattoman lähiverkon PSK:ta. WPS-ominaisuus on laajalti käytössä eri valmistajien langattomissa reitittimissä. (Wi-Fi CERTIFIED Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi Networks, 2014.)

WPS on todettu haavoittuvaiseksi ainakin PIN-koodikirjautumisen osalta. Tämä johtuu siitä, että PIN-koodi syötön epäonnistuessa langattoman reitittimen tai tukiaseman lähettämästä vastineesta on mahdollista päätellä, oliko PIN-koodin ensimmäinen puolisko oikein. Myös kehysvastine kertoo PIN-koodin viimeisen numeron, koska tätä käytetään tarkistussummana varsinaiselle PIN-koodille. Nämä kaksi seikkaa laskevat oleellisesti PIN-koodin arvaukseen vaadittavien yritysten lukumäärää. Huomioonotettavaa on myös se, etteivät useat verkkolaitevalmistajat ole kehittäneet turvamekanismia edellä mainittua haavoittuvuutta vastaan. (Allar 2011)

3.5 MAC-suodatus & piilotettu SSID

MAC-suodatuksella voidaan rajoittaa pääsyä langattomaan lähiverkkoon, sallimalla kirjautuminen ainoastaan erikseen asetetuilta MAC-osoitteilta. Yleisimmissä langattomissa reitittimissä ja tukiasemissa voidaan asettaa useampia sallittuja MAC-osoitteita ja useimmiten MAC-suodatusta käytetään yhdessä jonkin salauksen kanssa verkon tietoturvan parantamiseksi.

MAC-suodatus ei kuitenkaan yksinään riitä turvaamaan verkkoa, koska tämä on helposti kierrettävissä. MAC-suodatuksen ohittamiseen riittää, että taltioi verkossa liikkuvaa dataa jo kirjautuneilta käyttäjiltä ja poimii talteen jonkin käyttäjän MAC-osoitteen. Sallittu MAC-osoite asetetaan langattomalle verkkokortille käyttöön ja verkkoon voidaan tämän jälkeen kirjautua.

Langattoman lähiverkon SSID voidaan myös määrittää piilotetuksi. Asetuksen ollessa päällä, ei tukiasema lähetä beacon-kehyksiä ollenkaan, eikä tällöin mainosta verkon SSID:tä ympärilleen. Esimerkiksi Windows-käyttäjille tällainen verkko näkyy ”muuna verkkona” ja käyttäjän pitää ennen yhdistämistä syöttää SSID itse.

Piilotettu SSID paljastuu kuitenkin, kun käyttäjä aloittaa yhdistämisen verkkoon ja syöttää SSID:n. Tukiasema ja käyttäjä vaihtavat tällöin probe requset- ja probe response -kehyksiä. Kyseisissä kehyksissä SSID kulkee salaamattomana.

3.6 Palvelunestohyökkäys

Palvelunestohyökkäyksellä pyritään ruuhkauttamaan langaton lähiverkko, häiritsemään verkossa tapahtuvaa tiedonsiirtoa tai käyttäjien yhteydenlaatua. Langattoman lähiverkon osalta palvelunestohyökkäyksen toteutuksessa hyödynnetään tyypillisesti salaamattomia management-kehyksiä ja yhteydettömyyden vuoksi langattoman lähiverkon toimintaa pystytään häiritsemään verkon ulkopuolelta.

Tukiasemaan kohdistetussa palvelunestohyökkäyksessä pyritään lähettämään tukiasemalle niin paljon liikennettä, ettei tämä pysty liikennemäärää hallitsemaan. Pahimmillaan langaton tukiasema saattaa kaatua tai käynnistyä uudelleen liian kovan kuorman johdosta ja aiheuttaa kaikkien tukiasemaan yhdistäneiden laitteiden yhteyden menetyksen. Palvelunestohyökkäys voidaan kohdentaa myös yksittäiseen käyttäjään, jolloin yksittäinen käyttäjä pyritään tiputtamaan verkosta tai estämään tämän tiedonsiirto.

De-authentication -hyökkäyksessä hyökkääjä lähettää tukiasemalle kehyksiä, jotka pyytävät tukiasemaa unohtamaan tietyn käyttäjän todennuksen ja katkaisemaan yhteyden. De-authentication -kehysten jatkuva lähettäminen saa aikaan käyttäjän putoamisen verkosta, jonka jälkeen käyttäjä automaattisesti yrittää yhdistää uudestaan verkkoon. Hyökkäyksen onnistuessa ja hyökkääjän jatkaessa de-authentication-kehysten lähettämistä, ei käyttäjä pysty yhdistämään tänä aikana takaisin verkkoon.

De-authentication -hyökkäystä voidaan myös käyttää kaikkien langattoman lähiverkon käyttäjien yhteyden häiritsemiseen. Luomalla kehyksiä broadcast-lähetyksinä, jotka käyttävät lähettäjän MAC-osoitteena tukiaseman osoitetta, kohdistuu hyökkäys kaikille verkon käyttäjille. Tämä vaatii hyökkääjän verkkokortilta tosin lähetystehoa konkreettisen vaikutuksen saavuttamiseksi.

Todennuspyyntöhyökkäyksessä hyökkääjä lähettää langattomalle tukiasemalle authentication -kehyksiä käyttäen satunnaisia MAC-osoitteita lähettäjän osoitteena. Hyökkäyksen teho perustuu langattoman tukiaseman ylläpitämän yhteystaulun rajattuun muistiin. Tukiasema ylläpitää siihen yhdistäneiden laitteiden MAC-osoitetietoja erikseen varatussa yhteystaulussa ja hyökkääjä pyrkii täyttämään yhteystaulun täyteen satunnaisia MAC-osoitteita. Kun taulu lopulta täyttyy, eivät uudet verkkoon haluavat käyttäjät pysty yhdistämään tukiasemaan, vaan tukiasema hylkää todennuspyynnöt. (Compton 2007, 13-14)

Beacon-tulvituksella pyritään hankaloittamaan ja estämään käyttäjien kirjautumista langattomaan lähiverkkoon. Langattomat verkkokortit kuuntelevat käyttöjärjestelmästä riippuen oletuksena tukiasemien lähettämiä beacon-kehyksiä ollakseen tietoisia ympäristössä olevista verkoista.

Hyökkääjä lähettää useita beacon-kehyksiä tiheällä aikavälillä ja mainostaa näissä verkkoja, joita ei todellisuudessa ole olemassa. Käyttäjille nämä näkyvät samaan tapaan kuin muutkin langattomat lähiverkot, joihin käyttäjä voisi halutessaan kirjautua. Langattomien verkkokorttien kuunnellessa ja prosessoidessa beacon-kehyksiä, voi näiden jatkuva tulvittaminen aiheuttaa ongelmia käyttäjän laitteiston tai laiteajureiden kanssa.

3.7 Välimieshyökkäys

Välimieshyökkäyksessä hyökkääjä asettuu käyttäjän ja tukiaseman väliin, kaapaten näiden välisen liikenteen ja vaarantaen datan säilymisen eheänä. Hyökkäyksestä vaarallisen tekee se, että tavallinen käyttäjä ei todennäköisesti huomaa mitään eroa tiedonsiirron osalta, vaan olettaa kommunikoivansa suoraan tukiaseman kanssa. Langattoman lähiverkon tapauksessa välimieshyökkäyksissä hyödynnetään usein management-kehyksiä ja niiden toimintaperiaatetta.

Yksi yleisimmistä välimieshyökkäyksistä on honeypot-hyökkäys. Käyttäjien päätelaitteet tallentavat useimmissa tapauksissa muistiin langattomat lähiverkot sekä SSID:t, joihin ovat aiemmin olleet yhdistäneenä. Langattoman verkkokortin ollessa päällä, saatetaan näitä verkkoja hakea aktiivisesti probe request -kehyksillä. Hyökkääjä voi edellä mainittuja kehyksiä kuunnella ja tarjota käyttäjälle oman koneen kautta käyttäjän kyselemän SSID:n sekä pääsyn verkkoon.

Useimmat päätelaitteet myös valitsevat tukiaseman vahvemman radiosignaalin pohjalta. Honeypot-hyökkäys voidaan siis toteuttaa tarjoamalla käyttäjälle sama verkko, kuin missä tämä on jo yhdistäneenä, mutta paremmalla signaalilla. Käyttäjä voidaan pakottaa myös yhdistämään hyökkääjän luomaan tukiasemaan palvelunestohyökkäyksellä. (Schoeneck 2003, 5-9)

4 TIETOTURVAN TESTAAMINEN

Tietoturvatestaamisella pyritään testaamaan tietojärjestelmää ja arvioimaan järjestelmän tietoturvallisuutta oikeita hyökkäyksiä simuloiden. Testaamisen tavoitteena on kartoittaa järjestelmän tila, potentiaaliset riskitekijät ja varmistamaan, että järjestelmä toimii sillä tavalla, kuten se on alkuperäisesti määritetty toimimaan.

Langattoman lähiverkon osalta testaamisella arvioidaan sekä tunnistetaan verkkoon, salaukseen ja pääsyyn liittyviä uhkia ja riskejä. Lopullisena tavoitteena on parantaa langattoman lähiverkon tietoturvaa kerättyjen havaintojen pohjalta. Nykypäivänä Internetissä on tarjolla useita käyttöjärjestelmävaihtoehtoja ja ilmaisohjelmia, joilla langattoman lähiverkon tietoturvaa voidaan testata hyvinkin tehokkaasti.

4.1 Kali Linux

Kali Linux on Debian-pohjainen avoimen lähdekoodin käyttöjärjestelmä, joka on erityisesti tietoturvan testaamista varten suunniteltu. Kali Linux julkaistiin maaliskuussa 2013 ja sen ylläpidosta, rahoituksesta ja kehityksestä vastaa Mati Aharonin perustama Offensive Security-organisaatio. Kali Linuxin pääkehittäjinä tällä hetkellä Aharonin lisäksi ovat Devon Kearns ja Raphaël Hertzog. (About Kali Linux 2016.)

Kali Linux on uudelleen rakennettu Offensive Securityn aiemman, Ubuntuun pohjautuvan Backtrack-käyttöjärjestelmän päälle. Backtrackin käyttöjärjestelmäpäivitykset aiheuttivat usein yhteensopivuusongelmia kehittäjien luomien ohjelmistojen kanssa, joten Offensive Security päätti rakentaa kokonaan uuden käyttöjärjestelmän Debianiin pohjautuen vastatakseen yhteensopivuusongelmiin. (Kali Linux review and a brief history of the BackTrack pentesting distro 2013.)

Kali Linuxissa on esiasennettuna useita erilaisia ohjelmia eri palveluiden tietoturvan testaamiseen. Kali Linuxista löytyy laaja kirjo ohjelmistoja muun muassa web-applikaatioiden, tietokantojen ja tietoverkkojen tietoturvatestaamiseen. Kali Linux on tietoturva-alan ammattilaisten keskuudessa suosittu käyttöjärjestelmä monipuolisen ohjelmistotarjonnan vuoksi.

4.2 Langattoman verkkokortin tilat ja vaatimukset

Promiscuous-tila on langattoman tai tavallisen verkkokortin tila, joka mahdollistaa lähiverkossa liikkuvien datakehysten taltioinnin, kun laite on lähiverkkoon kuuluva. Normaalitilassa, kun verkkokortti vastaanottaa datakehyksen, se vertaa kehyksen MAC-osoitustietoja omaan MAC-osoitteeseen. Jos vastaanotettu kehys ei ole osoitettu kyseisen verkkokortin MAC-osoitteeseen, tai ei ole broadcast- tai multicast-kehys, verkkokortti pudottaa kehyksen. Promiscuous-tilaa käytettäessä verkkokortti kuitenkin pystyy kuuntelemaan ja prosessoimaan myös muille lähiverkon laitteille osoitettuja kehyksiä.

Jotta verkkoliikennettä voidaan kuunnella ja taltioida, pitää myös muiden verkkoon kuuluvien laitteiden verkkokortit olla promiscuous-tilassa. Lähiverkon ylläpitäjät voivatkin tehokkaasti etsiä verkon heikkoja kohtia ja analysoida verkkoliikennettä asettamalla verkkoon kuuluvien laitteiden verkkokortit promiscuous-tilaan. Promiscuous-tilaa hyödyntävät myös erilaiset verkkoliikenteen analysointiohjelmat.

Monitorointitilan etuna promiscuous-tilaan on yhteydettömyys. Toisin kuin promiscuous-tilassa, monitorointitilassa pystytään verkkoliikennettä taltioimaan verkon ulkopuolelta. Langattoman lähiverkon tietoturvaa testatessa tapahtuu testaus langattoman lähiverkon ulkopuolelta, joten tietoturvan testaamista varten tulee langattoman verkkokortin tukea monitorointitilaa. Monitorointitilassa langaton verkkokortti ei ota myöskään kantaa datakehyksen CRC-arvoon, jolla tarkistetaan kehyksen eheys. Taltioidut kehykset voivat siis olla korruptoituneita tiedonsiirron aikana. Monitorointitilaa kut-

sutaan usein myös raw monitor -tilaksi, koska tässä tilassa langaton verkkokortti vastaanottaa kaiken verkkoliikenteen eheydestä riippumatta. (Difference - Promiscuous vs. Monitor Mode Wireless Context 2008)

Langatonta verkkokorttia tietoturvatestausta varten valitessaan on suositeltavaa kiinnittää huomiota myös testausalustaan. Opinnäytetyössäni käytän tietoturvan testaamiseen Kali Linux-käyttöjärjestelmää, joten langattoman verkkokortin tulee myös olla yhteensopiva Kali Linuxin kanssa. Myös standardi tulee valita testattavan langattoman lähiverkon mukaan. 802.11n-standardin langaton verkkokortti on yleensä sopivin valinta, koska 802.11n-standardi on myös taaksepäin yhteensopiva aiempien standardien laitteiden kanssa, eikä näin ollen rajoita testausta.

4.3 Aircrack-ng

Aircrack-ng on langattomien lähiverkkojen tietoturvatestaamiseen tarkoitettu ohjelmistopaketti. Aircrack sisältää työkaluja muun muassa WLAN-salausten purkamiseen, palvelunestohyökkäysten toteuttamiseen, langattoman verkkoliikenteen taltioimiseen ja analysointiin sekä väärennettyjen kehysten lähettämiseen. Yleisimmin käytettyjä aircrack-ng:n mukana tulevia työkaluja ovat:

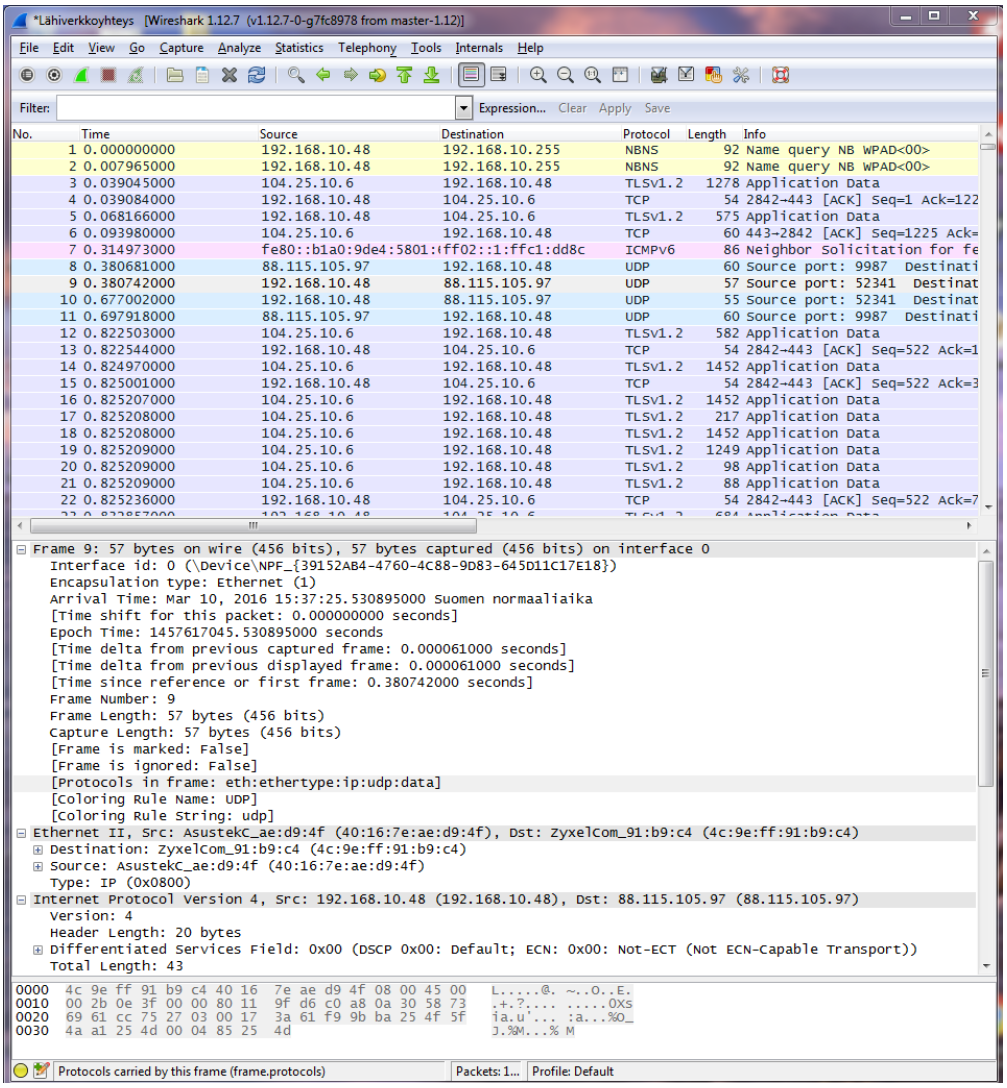
- airmon-ng, käytetään monitorointitilan käyttöönottoon ja kanavan valitsemiseen.
- aireplay-ng, käytetään luomaan halutun tyyppistä langatonta liikennettä ja toteuttamaan esimerkiksi palvelunestohyökkäyksiä.
- airbase-ng, käytetään väärennetyn tukiaseman luomiseen ja välimieshyökkäysten toteuttamiseen.
- aircrack-ng, käytetään WEP-avaimen murtamiseen ja sanakirjahyökkäyksien toteuttamiseen.

Aircrack-ng on saatavilla Linux- ja nykyään myös Windows-käyttöjärjestelmille. Aircrack-ng:n käyttäminen vaatii monitorointi-tilaan soveltuvan verkkokortin ja tukee yleisimpiä 802.11-standardeja alkupäästä lähtien. (Aircrack-ng 2018)

4.4 Wireshark

Wireshark on graafinen verkkoliikenteenhaistelija ja tietoliikenteessä laajasti käytetty. Wiresharkin kehitys alkoi Gerald Combsin toimesta vuonna 1998, jolloin Wireshark kulki työnimellä Ethereal. Sittemmin vuonna 2006 vaihtui Ethereal-työnimi Wiresharkiksi.

Wiresharkia käytetään muun muassa verkko-ongelmien havainnointiin ja analysointiin. Wireshark soveltuu myös langattoman verkkoliikenteen kuunteluun, edellyttäen, että käytössä on monitorointitilaa tukeva langaton verkkokortti. Wiresharkilla voidaan tutkia langattoman kehyksen eri osioita jopa yksittäisten bittien osalta. Wireshark on saatavilla Windows-ympäristöön sekä Linux-ympäristöön ja se on täysin maksuton. Kuvassa 10 näkymä Wiresharkin käyttöliittymästä.



Kuva 10. Wiresharkin käyttöliittymä ja taltiointi lähiverkkoliikenteestä.

5 KÄYTÄNNÖN TESTIT

Opinnäytetyön käytännön osuudessa testattiin teoriakappaleessa esiteltyjä yleisimpiä langattomiin lähiverkkoihin kohdistuvia hyökkäyksiä ja testiverkon tietoturvaa. Tietoturvatestauksen tavoitteena oli tutkia, miten haastavaa kyseisiä hyökkäyksiä on toteuttaa, miten yleisesti tunnetut hyökkäykset vaikuttavat langattoman lähiverkon toimintaan ja kuinka haavoittuvaisia langattomat lähiverkot ovat erilaisille hyökkäyksille.

Testausympäristö koostui seuraavista laitteista:

- kaksi kannettavaa tietokonetta (hyökkääjä sekä verkon käyttäjä)
- langaton reititin
- monitorointitilaa tukeva langaton verkkokortti
- tavallinen 802.11n-standardin langaton verkkokortti
- älypuhelin.

5.1 Esivalmistelut

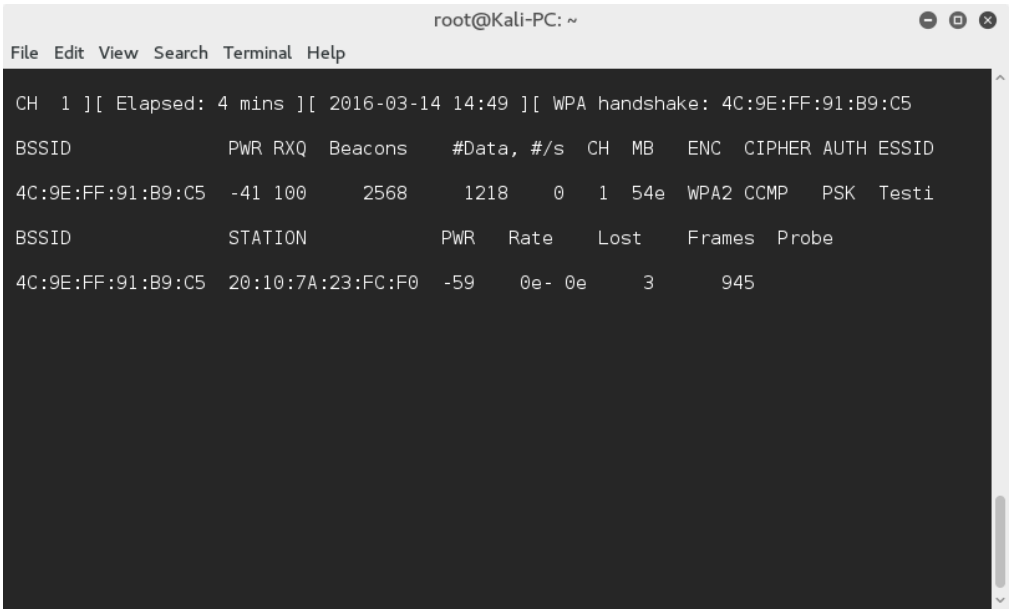
Ennen varsinaista testausta, kerättiin tietoa testiverkosta ja verkon laitteista Tarvittavan informaation kerääminen suoritettiin hyökkääjän koneelta käyttämällä airodump-työkalua. Tätä ennen langaton verkkokortti asetettiin monitorointitilaan.

```
airmon-ng start wlan1.
```

Airmon-ng vaihtaa verkkokortin nimeä, ja uutta nimeä käyttämällä käynnistettiin airodump.

```
airodump-ng start wlan1mon
```

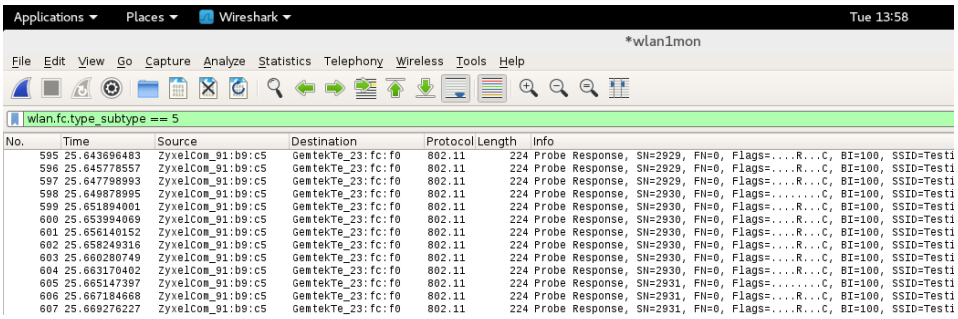
Airodump-ng:tä käyttämällä saatiin taltioitua langattoman reitittimen BSSID 4c:9e:ff:91:b9:c5 ja käyttäjän osoite 20:10:7a:23:fc:f0, sekä langattoman lähiverkon käyttämä kanava ja SSID. Kuvassa 11 näkymä airodump-työkalusta.



Kuva 11. Airodump-ng:n keräämä tieto verkosta.

5.2 Piilotettu SSID ja MAC suodatus

Testin suorittamista varten langattoman reitittimen asetuksista määritettiin SSID piilotetuksi. Tavoitteena oli selvittää piilotettu SSID ja tämä toteutettiin kaappaamalla testikäyttäjän kirjautuminen verkkoon. Testikäyttäjän kirjautuessa verkkoon, vaihtavat käyttäjä ja tukiasema probe request- ja probe response -kehyksiä, joissa ilmenee verkon SSID-tunnus. Tämä taltioitiin hyökkääjän koneelta kuuntelemalla verkkoliikennettä Wiresharkilla (Kuva 12).



Kuva 12. Wireshark-taltiointi WLAN-reitittimen lähettämistä probe response-kehyksistä.

Testissä todettiin piilotetun SSID:n olevan yksinään riittämätön suojausmenetelmä langattomalle lähiverkolle ja tämä on helposti kierrettävissä vapaasti saatavilla työkaluilla.

MAC-osoitesuodatuksen testausta varten WLAN-reititin on määritetty ennen testin aloittamista käyttämään suojauksenaan pelkkää MAC-suodatusta ja sille on sallittu ainoastaan testikäyttäjän MAC-osoite 20:10:7a:23:fc:f0.

MAC-osoite suodatuksen kiertäminen onnistui kuuntelemalla verkkoliikennettä langattoman reitittimen ja siihen yhdistäneiden käyttäjien välillä, käyttäen airodumpia.

Airodump asetettiin kuuntelemaan kanavaa 1, jolla testiverkko operoi.

```
airodump-ng –c 1 wlan1mon
```

Komennon antamisen jälkeen, huomaa airodump kanavalla olevan käyttäjän, joka on yhdistänyt Testi-verkkoon. Tästä saatiin poimittua talteen käyttäjän MAC-osoite.

MAC-osoite vaihdettiin hyökkääjän koneen langattomalle verkkokortille käyttöön macchanger-työkalulla.

```
macchanger –m 20:10:7A:23:FC:F0 wlan0
```

Vaihdoksen jälkeen, voidaan hyökkääjän koneelta yhdistää Testi-verkkoon.

```
iw wlan0 connect Testi
```

MAC-suodatuksen kiertäminen onnistui vaivattomasta ja testi todistaa MAC-suodatuksen olevan riittämätön yksinään verkon suojaamiseksi. Onkin suositeltavaa käyttää MAC-suodatusta yhdessä WPA2-salauksen kanssa tietoturvan tason nostamiseksi.

5.3 WEP-salauksen murtaminen

WEP-avaimen murtaminen suoritettiin liittyvä avain -hyökkäyksellä. Langaton reititin määritettiin käyttämään WEP-salausta ja satunnaisesti luotua 104-bitin mittaista WEP-avainta.

Käyttäjä kirjautui sisälle verkkoon, jonka jälkeen hyökkääjän koneelta asetettiin verkkokortti taltioimaan liikennettä ja tallentamaan salattu liikenne tekstitiedostoon.

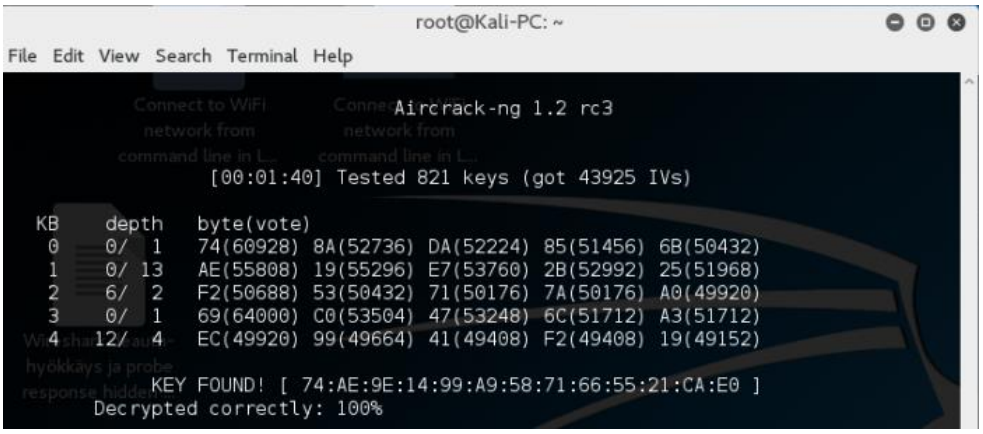
```
airodump-ng --bssid 4c:9e:ff:91:b9:c5 --channel 1 --write
demo2 wlan1mon
```

Liittyvä avain -hyökkäyksessä pyritään taltioimaan mahdollisimman paljon eri alustusvektoreilla salattuja WEP-kehyksiä ja purkamaan WEP-avain näiden yhtäläisyyksien pohjalta. Ainoastaan yhden käyttäjän ollessa kirjautuneena verkkoon, on verkon liikennemäärät varsin pienet. Tämän vuoksi hyökkäyksen nopeuttamiseksi käytettiin aireplay-työkalua, joka tunnistaa ARP-kyselyt verkossa sen ulkopuolelta ja monistaa näitä, käyttäen lähdeosoitteena verkossa olevan käyttäjän MAC-osoitetta.

```
aireplay-ng -3 -b 4C:9E:FF:91:B9:C5 -h 20:10:7A:23:FC:F0
```

Varsinainen avaimen purkaminen tiedostosta tapahtui aircrack-ng -työkalulla (Kuva 13).

```
aircrack-ng demo2.cap
```



Kuva 13. WEP-salauksen murtaminen aircrackillä.

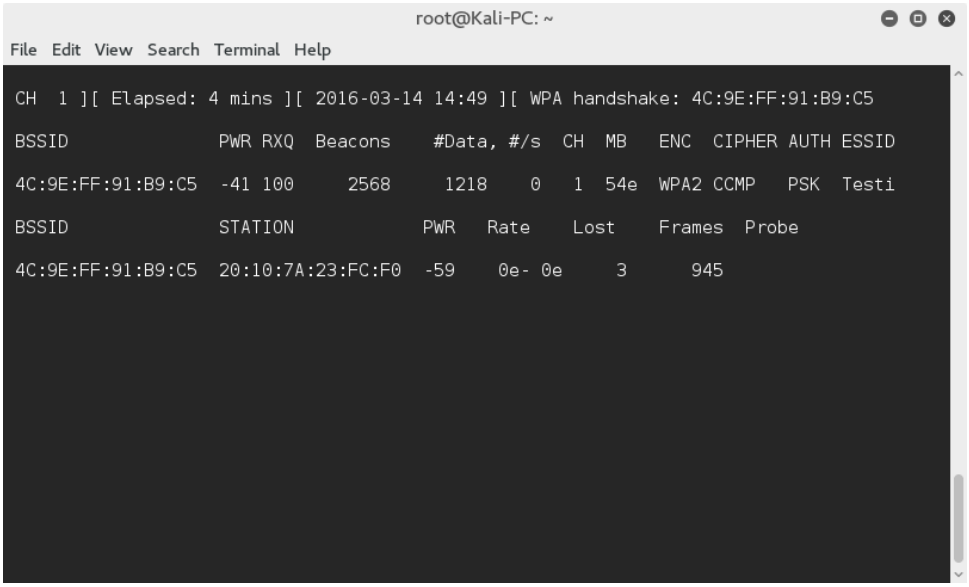
Testi todistaa WEP-salaukseen liittyvien haavoittuvuuksien olevan tosiasia. Testissä täysin satunnaisesti luotu WEP-avain murtui alle kahdessa minuutissa aireplay:n ja aircrackin avulla. Testi suoritettiin vielä toistamiseen uudella WEP-avaimella ja toisella kerralla WEP-avain murtui vielä hieman nopeammin.

5.4 WPA2-sanakirjahyökkäys

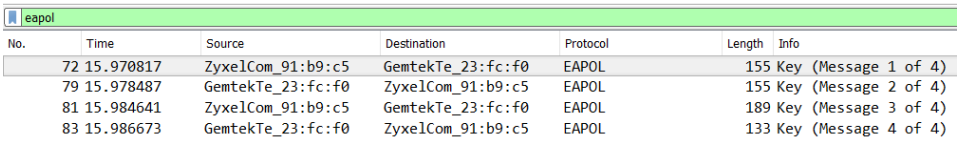
Ennen testauksen aloittamista määritettiin verkolle käyttöön WPA2-salaus ja tälle PSK. Hyökkääjän kone asetettiin kuuntelemaan langatonta reititintä ja tallentamaan kerätty liikenne tiedostoon.

```
airodump-ng --bssid 4C:9E:FF:91:B9:C5 --channel 1 --write
Capture wlan1mon
```

PSK:n selvittämiseksi vaaditaan käyttäjän kirjautuminen Testi-verkkoon ja neliosaisen kättelyn taltiointi (Kuva 14, Kuva 15).



Kuva 14. airodump ja neliosaisen kättelyn onnistunut taltiointi.

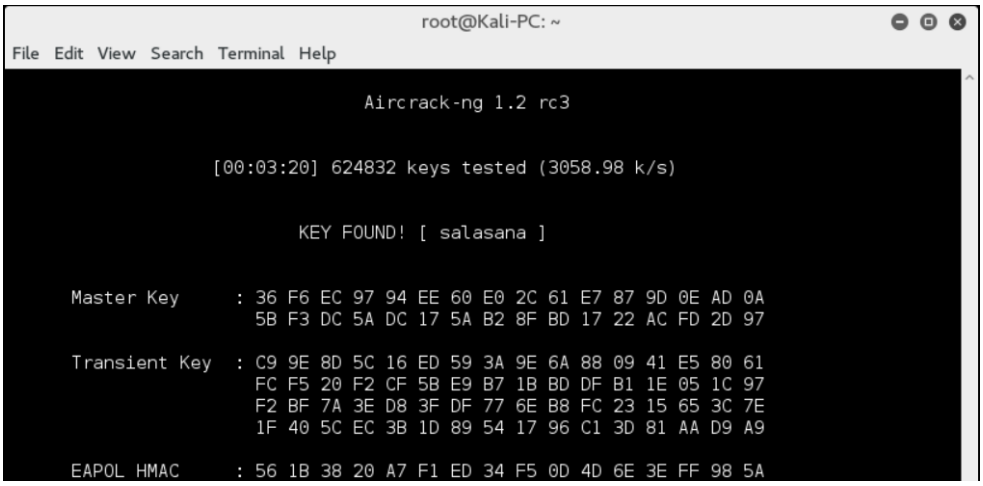


Kuva 15. Taltioitu kokonainen neliosainen kättely Wiresharkissa avattuna.

Sanakirjahyökkäyksen tapauksessa teho perustuu käytettävissä olevan sanalistan lukumäärään ja verkon salausavaimen kompleksisuuteen – mitä helpommin arvattavissa oleva avain ja mitä laajempi sanakirja, sen todennäköisempää on avaimen selvittäminen. Kalissa on asennettuna jo valmiiksi sanalistoja ja laajempia listoja on myös ladattavissa Internetistä. Tässä testissä käytettiin noin 1,2 miljoonan sanan listaa.

Sanakirjahyökkäys toteutettiin aircrackilla (Kuva 16).

```
aircrack-ng Capture-01.cap -w /usr/share/word-
lists/sqlmap.txt
```



Kuva 16. WPA2-avaimen purkaminen aircrackillä.

Aircrack sai varsin lyhyessä ajassa laskettua ja selvitettyä langattoman lähiverkon PSK:n. Testissä todistettiin yksinkertaisten salasanojen olevan varsin haavoittuvaisia sanakirjahyökkäyksille. Hyökkääjän ei tarvitse olla verkon välittömässä läheisyydessä kuin sen ajan, jotta saadaan yhden käyttäjän todennus taltioitua. Tämän jälkeen sanakirjahyökkäystä ja PSK:n selvitystä voidaan jatkaa kokonaan paikallisesti.

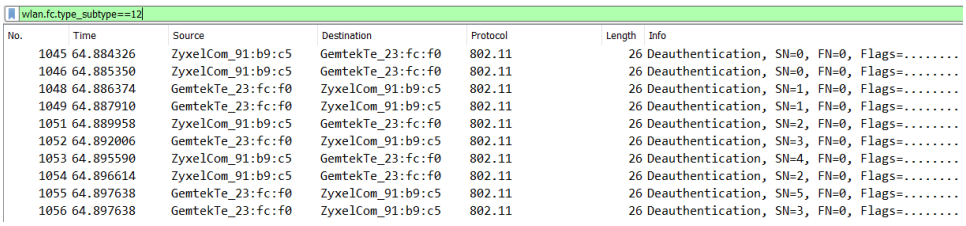
5.5 Palvelunestohyökkäykset

Teoriakappaleessa esitellyistä hyökkäyksistä testattiin käytännössä de-authentication-, todennuspyyntö- sekä beacon-tulvitus -hyökkäyksiä. Hyökkäyksiä kohdennettiin sekä verkon käyttäjään että langattomaan reitittimeen ja tavoitteena oli tutkia, mikä näiden vaikutus on langattoman lähiverkon käytettävyyteen ja toimintaan.

5.5.1 De-authentication -palvelunestohyökkäys

Hyökkäystä varten testikäyttäjä on jo valmiiksi kirjautuneena langattomaan verkkoon. Kyseinen hyökkäys kohdistettiin yksittäiseen verkon käyttäjään. Hyökkääjän koneelta lähetettiin aireplayllä de-authentication -kehyksiä sekä käyttäjälle että langattomalle reitittimelle samanaikaisesti, käyttäen näiden MAC-osoitteita kehysten osoitetiedoissa. Kyseiset kehykset kertovat langattomalle reitittimelle, että MAC-osoitteen omistava käyttäjä haluaa kirjautua ulos verkosta. Kuvassa 17 Wireshark-taltiointi liikenteestä hyökkäyksen ajalta.

```
aireplay-ng -0 0 -a 4C:9E:FF:91:B9:C5 -c 20:10:7A:23:FC:F0
wlan1mon
```



Kuva 17. Hyökkäyksen aikana taltioitu liikenne Wiresharkissa avattuna.

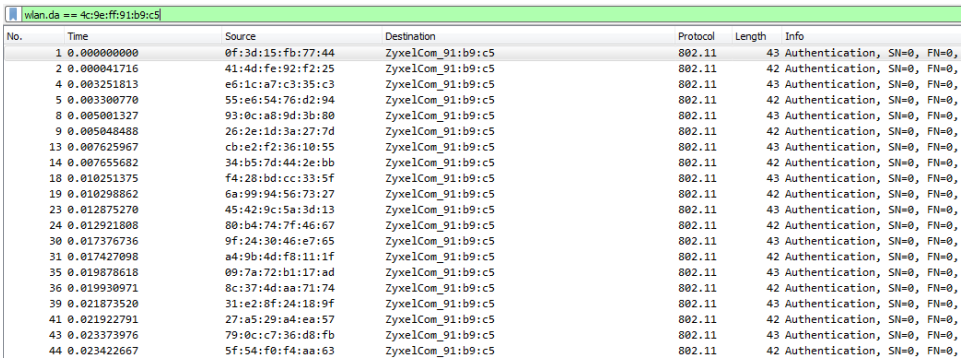
De-authentication -hyökkäys havaittiin testissä varsin tehokkaaksi. Verkon käyttäjä ei päässyt missään vaiheessa hyökkäyksen aikana takaisin verkkoon, vaan menetti yhteyden täysin.

5.5.2 Todennuspyyntöhyökkäys

Todennuspyyntöhyökkäys kohdistettiin langattomaan reitittimeen, tavoitteena tukiaseman ylikuormittaminen. Hyökkäyksen teho perustuu langattoman reitittimen suorituskyvyn rajallisuuteen – langattomalle reitittimelle lähetetään väärennettyjä authentication request -kehyksiä niin paljon, ettei se pysty niitä ajoissa käsittelemään eikä niihin vastaamaan.

Hyökkäys toteutettiin Kaliin saatavalla mkd3-työkalulla. mkd3 luo authentication-kehyksiä ja generoi satunnaisia MAC-osoitteita kehysten lähettäjiksi (Kuva 18).

```
mkd3 a -a 4C:9E:FF:91:B9:C5
```



Kuva 18. Kuvakaappaus Wiresharkista hyökkäyksen ajalta.

Hyökkäyksellä ei saavutettu haluttua lopputulosta (Kuva 19). Testin aikana verkkoon kirjautuneella käyttäjällä ei havaittu ongelmia langattoman yhteyden kanssa. Langaton reititin hylkäsi väärennetyt todennuspyynnöt ja reitittimellä todennäköisesti oli sisäänrakennettu suojaus lyhyen ajan sisällä tapahtuvia todennuspyyntöjä vastaan.

```
Connecting Client: 72:3F:1F:57:A5:84 to target AP: 4C:9E:FF:91:B9:C5
Connecting Client: 3A:78:EC:B4:BA:EB to target AP: 4C:9E:FF:91:B9:C5
AP 4C:9E:FF:91:B9:C5 seems to be INVULNERABLE!
Device is still responding with  6000 clients connected!
Connecting Client: 0D:0B:EF:43:BA:3C to target AP: 4C:9E:FF:91:B9:C5
Connecting Client: D4:55:8A:29:FB:17 to target AP: 4C:9E:FF:91:B9:C5
AP 4C:9E:FF:91:B9:C5 seems to be INVULNERABLE!
Device is still responding with  6500 clients connected!
Connecting Client: 87:6D:53:DD:13:0C to target AP: 4C:9E:FF:91:B9:C5
Connecting Client: 56:91:CF:30:CA:D8 to target AP: 4C:9E:FF:91:B9:C5
Connecting Client: 01:5A:7A:63:17:7C to target AP: 4C:9E:FF:91:B9:C5
AP 4C:9E:FF:91:B9:C5 seems to be INVULNERABLE!
Device is still responding with  7000 clients connected!
Connecting Client: 18:A7:0E:96:36:25 to target AP: 4C:9E:FF:91:B9:C5
Connecting Client: B6:4E:73:E6:CD:05 to target AP: 4C:9E:FF:91:B9:C5
AP 4C:9E:FF:91:B9:C5 seems to be INVULNERABLE!
Device is still responding with  7500 clients connected!
Connecting Client: 10:72:A4:FB:6B:A4 to target AP: 4C:9E:FF:91:B9:C5
Connecting Client: 3E:0F:AF:DB:AA:34 to target AP: 4C:9E:FF:91:B9:C5
AP 4C:9E:FF:91:B9:C5 seems to be INVULNERABLE!
Device is still responding with  8000 clients connected!
Connecting Client: 8F:39:43:23:B4:8B to target AP: 4C:9E:FF:91:B9:C5
Connecting Client: 66:7D:9D:34:0F:89 to target AP: 4C:9E:FF:91:B9:C5
Connecting Client: 09:17:BB:41:3B:A6 to target AP: 4C:9E:FF:91:B9:C5
AP 4C:9E:FF:91:B9:C5 seems to be INVULNERABLE!
Device is still responding with  8500 clients connected!
Connecting Client: 22:E1:AB:9C:50:4C to target AP: 4C:9E:FF:91:B9:C5
Packets sent:   8624 - Speed:  203 packets/sec
```

Kuva 19. Kuva hyökkäyksestä Kalin komentoriviltä.

5.6 Beacon-tulvitus

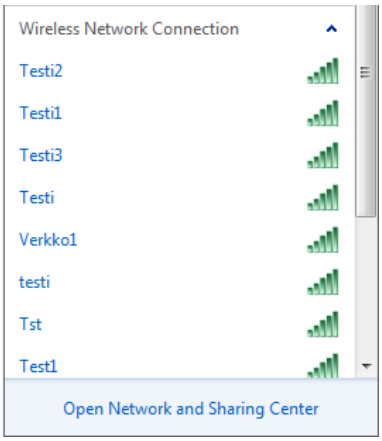
Testi toteutettiin Kalin mdk3 työkalulla. Tätä ennen oli luotuna lista ssid.txt, johon sisällytettiin SSID:t, joita halutaan hyökkääjän koneelta mainostaa beacon-kehyksillä. Hyökkäyksellä pyrittiin häiritsemään käyttäjän kirjautumista haluamaansa verkkoon.

Parametri a sisällyttää beacon-kehykseen WPA-CCMP tunnisteet. Parametrillä m, mdk3 lähettää kehykset satunnaisella MAC-osoitteella, sisällyttäen lähettäjän MAC-osoitteen satunnaisesti jonkin laitevalmistajan OUI-tunnisteen. Oletuksena mdk3 lähettää beaconeja 50ms välein. Kuvassa 20 nähdään, miltä liikenne näyttää Wiresharkissa ja kuvassa 21 on näkymä Windows-käyttäjän koneelta.

```
mdk3 wlan1mon b -f ssid.txt -a -m
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	LinksysG_25:cc:31	Broadcast	802.11	105	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Testi1
2	0.001150052	LinksysG_25:cc:31	Broadcast	802.11	106	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Testi1
4	0.016102340	Cisco_23:d0:f7	Broadcast	802.11	105	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Testi2
5	0.017246746	Cisco_23:d0:f7	Broadcast	802.11	106	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Testi2
6	0.032246784	Universa_b6:4a:83	Broadcast	802.11	105	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Testi3
7	0.033370836	Universa_b6:4a:83	Broadcast	802.11	106	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Testi3
8	0.048378901	3Com_b0:60:b3	Broadcast	802.11	104	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Testi
9	0.049526983	3Com_b0:60:b3	Broadcast	802.11	105	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Testi
	0.064514963	Cabletro_04:1a:5c	Broadcast	802.11	104	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Testi
	0.065666025	Cabletro_04:1a:5c	Broadcast	802.11	105	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Testi
	0.080687698	AmdPcnet_a3:da:52	Broadcast	802.11	104	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=T3sti
	0.081951211	AmdPcnet_a3:da:52	Broadcast	802.11	105	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=T3sti
	0.096899362	D-Link_5d:60:0e	Broadcast	802.11	104	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Te5ti
	0.098050092	D-Link_5d:60:0e	Broadcast	802.11	105	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Te5ti

Kuva 20. Wireshark-taltiointi liikenteestä. Beacon-kehysten lähettäjinä useita eri valmistajia.



Kuva 21. Käyttäjän kannettavan tietokoneen näkymä verkoista. Joukossa langattoman reitittimen mainostama oikea SSID ”Testi”.

Verkot testikäyttäjälle näkyivät WPA-suojattuina, kuin minä tahansa normaalina verkkona joihin voisi kirjautua. Käyttäjä voi valita haluamansa verkon ja kirjautua, mutta salasanan syötön jälkeen ei mitään tapahdu.

Beacon-tulvitus on muodoltaan häiritsevä hyökkäys, mutta testien aikana havaittiin myös käyttäjän koneen langattoman verkkokortin käyvän alhaalla muutamaan otteeseen. Beacon-tulvituksella voidaan aikaansaada ongelmia päätelaitteiden langattomien verkkokorttien kanssa, näiden joutuessa prosessoimaan tiheään tahtiin vastaanotettuja kehyksiä.

5.7 Honeypot-välimieshyökkäys

Testissä luotiin hyökkääjän koneelle honeypot-tukiasema, tavoitteena saada käyttäjä yhdistämään tähän automaattisesti. Testilaitteena käytettiin älypuhelinta, joka oli jo kerran kirjautunut salaamattomaan Testi-verkkoon ja tallentanut tämän muistiinsa. Langattomasta reitittimestä otettiin WLAN-toiminnallisuus kokonaan pois ja hyökkääjän kone kytkettiin reitittimeen Ethernet-kaapelilla.

Testin toteuttamista varten asennettiin Linuxin bridge-utils -paketti, joka mahdollistaa langallisen- ja langattoman verkkokortin siltaamisen. Honeypot-tukiaseman ja Testi-SSID:n luonti tapahtui airbase-työkalulla (Kuva 22).

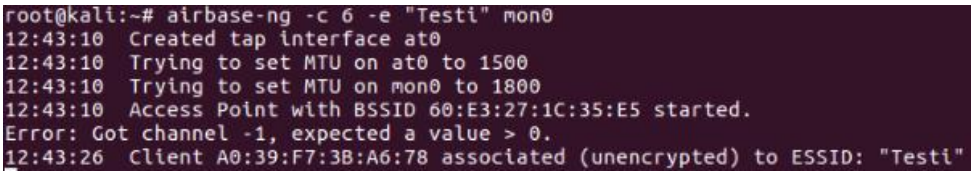
```
airbase-ng -e "Testi" -c 6 mon0
```

airbasen luoman at0-virtuaaliliitännän ja langallisen verkkokortin eth0 välille luotiin silta ja asetettiin Kali reitittämään liikenne langallista verkkokorttia käyttäen langattomalle reitittimelle. Lopuksi vielä otettiin käyttöön virtuaaliliitäntä at0 ja aiemmin luotu siltaus.

```
brctl addbr Silta
brctl addif Silta eth0
brctl addif Silta at0
echo 1 > /proc/sys/net/ipv4/ip_forward
route add default gateway 192.168.0.1
ifconfig at0 up
```

```
ifconfig Silta up
```

Puhelimesta asetettiin WLAN-toiminto päälle ja pian tämän jälkeen, puhelin havaitsi lähistöllä olevan Testi-verkon. Laitteen ollessa jo tallentanut Testi-nimisen verkon muistiin aiemmin, laite yhdisti verkkoon automaattisesti ilman, että verkkoa tuli valita itse. Puhelin sai IP-osoitteen langattomalta reitittimeltä hyökkääjän koneen välittämänä ja puhelimella oli täysi pääsy ulos Internetiin. Mikäli verkkoliikenteessä ei käytetä ylimääräistä salausta, kaikki liikenne voidaan nähdä salaamattomana hyökkääjän koneelta esimerkiksi Wiresharkin avulla.



Kuva 22. Älypuhelin yhdisti airbase-ng:n luomaa Testi-verkkoon.

Välimieshyökkäyksestä tekee vaarallisen se, ettei honeypot-tukiasemaan yhdistäminen näkynyt käyttäjälle mitenkään. Honeypot-välimieshyökkäystä voidaan potentiaalisesti hyödyntää ainakin kahdella tavalla:

- kuuntelemalla päätelaitteen lähettämiä probe request -kehyksiä, joilla laitteesta riippuen saatetaan aktiivisesti kysellä aiemmin tallennettuja verkkoja ympäristöstä
- tarjoamalla esimerkiksi jonkin yleisen paikan SSID-nimi honeypot-tukiaseman kautta, sillä olettamuksella, että jokin lähistöllä oleva päätelaite on aiemmin ollut tässä verkossa kirjautuneena ja tallentanut sen muistiin

6 YHTEENVETO

Tietoturva on hyvin tärkeässä roolissa langattomien lähiverkkojen osalta näiden yleistyessä koko ajan. Langattoman lähiverkon mahdollistaessa kenen tahansa liittymisen tietoverkkoon radiosignaalin kantaman alueella, on tärkeää huolehtia verkon suojauksesta ja verkon toimivuuden varmistamisesta. Historian aikana käytetyistä langattoman lähiverkon suojauksista on löytynyt useita eri haavoittuvuuksia ja myös luotetuimmaksi todettu WPA-salaus ei ole aukoton.

Opinnäytetyössä käytiin läpi langattomiin lähiverkkoihin kohdistuvia hyökkäyksiä. Opinnäytetyössä esitettiin useiden langattoman lähiverkon suojaamiseen tarkoitetun salauksen tai protokollan olevan haavoittuvaisia ulkopuoliselle hyökkääjälle.

Hyökkäyksien toteuttaminen ei itsessään vaatinut kovin suurta teknistä osaamista, vaan kaikki tarvittava tietous oli saatavilla alan kirjallisuudesta ja Internetistä käsin. Testeissä havaittiin eritoten palvelunestohyökkäysten olevan todella tehokkaita langatonta lähiverkkoa kohden ja näiden tehokkuutta voitaisiin vielä nostaa paremman laitteiston ja radion lähetystehon

avulla. Oli mielenkiintoista havaita, että verkon ulkopuolelta pystyttiin toteuttamaan konkreettisia verkon toimintaa haittaavia ja tietoturvan riskeeraavia hyökkäyksiä suurellakin onnistumistodennäköisyydellä.

Opinnäytetyön aihe mielenkiintoinen ja asiaan perehtyminen vei runsaasti aikaa. Oma tavoitteeni opinnäytetyönprosessin aikana oli oppia WLAN-tekniikasta ja tavoite kyllä täyttyi. Aika näyttää, miten langattoman lähiverkon tietoturva tulee kehittymään.

LÄHTEET

About Kali Linux. 2016. Offensive Security. Viitattu 16.2.2016.
https://www.kali.org/about-us/

Aircrack-ng. 2018. Viitattu 13.4.2018.
https://www.aircrack-ng.org/doku.php?id=Main

Allar, J. 27.11.2011. Vulnerability Note VU#723755 WiFi Protected Setup (WPS) PIN brute force vulnerability. Software Engineering Institute. Viitattu 12.3.2018.
https://www.kb.cert.org/vuls/id/723755

Beaver, K. & Davis, P. 2005. Hacking Wireless Networks For Dummies. Indianapolis, Indiana: Wiley Publishing Inc.

CCNA 200-120 Exam: The 7 Layer OSI Model. n.d. Certification Kits. Viitattu 11.4.2017.
https://www.certificationkits.com/osi-model/

Compton, S. 802.11 Denial of Service Attacks and Mitigation. 2007. SANS Institute InfoSec Reading Room. Viitattu 17.4.2018.
https://www.sans.org/reading-room/whitepapers/wireless/80211-denial-service-attacks-mitigation-2108

Difference - Promiscuous vs. Monitor Mode (Wireless Context). 2008. High on Wireless-blogi. Viitattu 8.2.2016.
http://lazysolutions.blogspot.ca/2008/10/difference-promiscuous-vs-monitor-mode.html

How 802.11 Wireless Works. 2003. Microsoft Technet. Viitattu 28.12.2017.
https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx

IEEE 802.11i-2004. 15.1.2018. Wikipedia. Viitattu 29.3.2018.
https://en.wikipedia.org/wiki/IEEE_802.11i-2004

Kali Linux review and a brief history of the BackTrack pentesting distro. Päivitetty 23.08.2013. Concise Courses- blogi. Viitattu 16.2.2016.
https://www.concise-courses.com/kali-linux-review-and-history/

Vanhoef, M & Piessens, F. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. 2018. Viitattu 2.4.2018.
https://papers.mathyvanhoef.com/ccs2017.pdf

Poole, Ian. n.d. IEEE 802.11n Standard. Adrio Communications. Viitattu 20.1.2016.
http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11n.php

Poole, I. n.d. IEEE 802.11b Standard. Adrio Communications. Viitattu 9.2.2016.

http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11b.php

Poole, I. n.d. IEEE 802.11ac Gigabit Wi-Fi. Adrio Communications. Viitattu 9.2.2016.
http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11ac-gigabit.php

Poole, Ian. n.d. Wi-Fi / WLAN Channels, Frequencies, Bands & Bandwidths. Adrio Communications. Viitattu 22.2.2018
http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php

Radiotaajuuskirja/langaton lähiverkko. 22.9.2015. Wikibooks. Kuva Suomessa käytetyistä 5GHz taajuusalueen kanavista. Viitattu 22.2.2018.
https://fi.wikibooks.org/wiki/Radiotaajuuskirja/langaton_l%C3%A4hiverkko

Related-key attack. 2016. Wikipedia. Viitattu 13.2.2016.
https://en.wikipedia.org/wiki/Related-key_attack

RF Wireless World. n.d. Kuva langattoman kehyksen osoitetiedoista. Viitattu 28.12.2017.
http://www.rfwireless-world.com/images/WLAN-MAC-Address-field-contents.jpg

Schoeneck, R. Wireless Honeypot. 2003. Global Information Assurance Certification. SANS Institute. Viitattu 26.4.2018.
https://www.giac.org/paper/gsec/2975/wireless-honeypot/104986

The State of Wi-Fi Security. 2012. Wi-Fi Alliance. Viitattu 29.3.2018
https://www.wi-fi.org/downloads-registered-guest/20120229_State_of_Wi-Fi_Security_09May2012_updated_cert.pdf/7600

Technical Note Removal of TKIP from Wi-Fi Devices. 2015. Wi-Fi Alliance. Viitattu 2.4.2018.
https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Alliance_Technical_Note_TKIP_v1.0.pdf

Understanding Authentication Types. 18.2.2018. Cisco. Viitattu 1.4.2018.
https://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-2_11_JA/configuration/guide/b12211sc/s11auth.html

Understanding WPA/WPA2 Pre-Shared-Key Cracking. 12/2015. A blog about security -blogi. Viitattu 2.4.2018.
https://www.ins1gn1a.com/understanding-wpa-psk-cracking/

Understanding the Network Terms SSID, BSSID, and ESSID. 12.02.2015. Juniper Networks. Viitattu 26.2.2018.
https://www.juniper.net/documentation/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-ssid-bssid-essid.html#jd0e71

Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi-networks. 4/2013. Wi-Fi Alliance. Viitattu 2.4.2018. http://www.ans-vb.com/Docs/Whitepaper_Wi-Fi_Security4-29-03.pdf
Wi-Fi CERTIFIED Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi Networks. 2014. Wi-Fi Alliance. Viitattu 12.3.2018. https://www.wi-fi.org/downloads-registered-guest/wp_Wi-Fi_CERTIFIED_Wi-Fi_Protected_Setup_20140409.pdf/7670

Wong, S. The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. 2003. SANS Institute InfoSec Reading Room. Viitattu 13.2.2016. https://www.sans.org/reading-room/whitepapers/wireless/evolution-wireless-security-80211-networks-wep-wpa-80211-standards-1109

802.11 WLAN Packets and Protocols. n.d. Savvius Inc. Kuva langattoman kehyksen rakenteesta. Viitattu 26.4.2017. https://www.savvius.com/resources/compendium/wireless_lan/wlan_packets