Kalle Havukainen

WLAN-salausmenetelmät ja tietoturva

Opinnäytetyö
Tietotekniikan koulutusohjelma

Huhtikuu 2010

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

KUVAILULEHTI

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Opinnäytetyön päivämäärä** **9.4.2010**
Tekijä(t) Kalle Havukainen	**Koulutusohjelma ja suuntautuminen** Tietotekniikan koulutusohjelma

Nimeke

WLAN-salausmenetelmät ja tietoturva

Tiivistelmä

Tämän työn tavoitteena oli selvittää, ovatko langattomien verkkojen salausmenetelmät turvallisia. Työssä tutustuttiin kevyesti myös eri antennityyppeihin. Testauksessa käytettiin Backtrack-ohjelmistoa. Linux-pohjaisena ohjelmistona se aiheutti työn edistymisessä pieniä ongelmia mutta ongelmiin löytyi ratkaisut. Työssä käytettiin hyökkäysmenetelmiä WEP – ja WPA-salauksia vastaan.

Lopputuloksena saatiin selville, että WEP-salaus on salausmenetelmänä riittämätön. WPA-salaus todettiin turvalliseksi, kunhan käytettiin riittävän pitkää – ja erikoismerkkejä sisältävää salasanaa. Työn avulla lukijalle tulee selväksi edellä mainittujen salausmenetelmien heikkouksia ja pystyy näiden tietojen perusteella valitsemaan turvallisen salausmenetelmän.

Asiasanat (avainsanat)

WLAN, WEP, WPA, BACKTRACK, TIETOTURVA

Sivumäärä	**Kieli**	**URN**
36	Suomi	

Huomautus (huomautukset liitteistä)

Ohjaavan opettajan nimi Martti Susitaival	**Opinnäytetyön toimeksiantaja**

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Date of the bachelor's thesis** 9.4.2010
Author(s) Kalle Havukainen	**Degree programme and option** Information and media technology

Name of the bachelor's thesis

WLAN-encryption methods and information security

Abstract

In this thesis I studied encryption methods for WLAN-networks. The main aim was to find if WEP and WPA- security methods are enough for securing a private network. For testing was used Linux-based Backtrack software.

It was used for running attacks against WEP and WPA-encrypted networks. Final result was that only WPA-encrypted networks are safe if those are used with a strong password.

Subject headings, (keywords)

WLAN, WEP, WPA, BACKTRACK, SECURITY

Pages	Language	URN
36	Finnish	

Remarks, notes on appendices

Tutor	Bachelor's thesis assigned by
Martti Susitaival	

SISÄLTÖ

LYHENTEET

1 JOHDANTO 1

2 802.11 STANDARDI 2

2.1 Langattoman lähiverkon edut 2

2.2 Nopeudet 3

2.2.1 802.11a 3

2.2.2 802.11b 4

2.2.3 802.11g 4

2.2.4 802.11n 4

2.3 Antennit ja niiden hyödyt 4

2.3.1 Suunta-antennit 5

2.3.2 Ympärisäteilevät antennit 6

2.3.3 Sektoriantennit 7

2.3.4 Lautasantennit 8

2.3.5 Tee-se-itse- antennit 9

2.3.6 Kantomatkat 11

3 LANGATTOMAN LÄHIVERKON SALAUSMENETELMÄT 12

3.1 WEP-salaus 12

3.2 WPA-salaus 13

3.3 WPA2-salaus 14

4 OMAT TESTAUKSET 14

4.1 Käytettävä laitteisto 15

4.2 Salauksenpurku ympäristö 16

4.2.1 Verkkojen etsintä ja tiedonkeräys 24

4.2.2 WEP-salauksen murtaminen 25

4.2.3 WPA-salauksen murtaminen 32

5 JOHTOPÄÄTÖKSET 35

LÄHTEET

LYHENTEET

AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
CCMP	Counter Mode/CBC-MAC Protocol
CRC	Cyclic Redundancy Check
EAP	Extensible Authentication Protocol
ICV	Integrity Check Vector
IEEE	Instiute of Electrical and Electronics Engineers
IV	Initialization Vector
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
Mbps	Megabits per second
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output
PEAP	Protected EAP
TKIP	Temporal Key Integrity Protocol
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 JOHDANTO

Langattomat lähiverkot ovat kasvattaneet suosiotaan siitä lähtien, kun kyseinen tekniikka julkaistiin. Johdoista eroon pääseminen ja niiden aiheuttamien kustannuksien säästäminen edesauttavat suosion kasvua. Langattomaan tekniikkaan siirtyminen tuo tullessaan myös uusia tietoturvariskejä, joita vastaan on kehitetty suojausmenetelmiä. Rikollisten menetelmät seuraavat tekniikan kehittymistä ja joissain tapauksissa ne ovat jopa edellä. Tästä syystä tietoturva-asioissa kannattaa pysyä ajan tasalla ja seurata alan kehitystä monista näkökulmista.

Mielenkiinto langattomien lähiverkkojen salausmenetelmiä kohtaan heräsi Cisco-WLAN(Wireless Local Area Network)-kurssilla. Siellä tuli tietoa joidenkin salausmenetelmien heikkouksista ja siitä, että osa on murrettavissa.

Tämän työn tarkoituksena on selvittää langattoman tiedonsiirron salausmenetelmien turvallisuutta. Työssä rakennetaan testiverkko, jonka avulla testataan internetistä löytyviä menetelmiä WEP(Wired Equivalent Privacy) - ja WPA-salauksia (Wi-Fi Protected Access) vastaan. Menetelmien toteuttamiseen käytän Linux-pohjaista Backtrack-ohjelmistoa. Samalla yritän luoda näkökulmaa siihen, onnistuuko salauksien murtaminen jokaiselta Matti Meikäläiseltä vai vaaditaanko enemmän kokemusta tietotekniikasta.

2 802.11 STANDARDI

Langattomien lähiverkkojen, eli WLAN:n synty sijoittuu 90-luvun loppupuolelle, kun IEEE (Instiute of Electrical and Electronics Engineers) julkaisi 802.11 standardin vuonna 1997. WLAN yhteydestä käytetään myös toista nimeä Wi-Fi:ä (Wireless Fidelity). Jotta WLAN-tekniikka olisi aikoinaan hyväksytty yleiseksi tiedonsiirtomenetelmäksi, piti varmistua siitä, että käytettävien laitteistojen - ja materiaalien kustannukset säilyisivät alhaisina. Tekniikan piti olla myös helposti integroitavissa silloisiin tiedonsiirtolaitteistoihin, kuten reitittimiin ja kytkimiin. Tästä syystä IEEE päätti kehittää 802.11 standardin, jonka kehittelemisessä oli mukana useiden laitevalmistajien edustajia. [1, s. 65], [2.]

WLAN-tekniikan nopeampaa yleistymistä haittasi puutteet määritellyissä standardeissa. Vaikka 802.11 standardiin oli määritelty tiedonsiirtotapahtumaan käytettäviä menetelmiä - ja asetuksia, silti ei voitu olla sataprosenttisen varmoja olisivatko eri valmistajien tuotteet keskenään yhteensopivia. Osa valmistajista lisäsi laitteisiinsa ominaisuuksia, jolla taattaisiin yhteensopivuus edellisiin laitteisiin. [1, s. 65.]

2.1 Langattoman lähiverkon edut

Tärkeimpinä langattomien lähiverkkojen etuina voidaan pitää liikkuvuutta, asentamisen nopeutta ja hyvää laajennettavuutta. Näistä edellä mainituista liikkuvuus on usein se tekijä, joka saa harkitsemaan langatonta lähiverkkoyhteyttä tavallisen lankaverkon sijaan. Nimensä mukaisesti langattoman lähiverkon luominen ei tarvitse erillistä kaapelointia, vaikka usein sitä käytetäänkin jo olemassa olevan langallisen lähiverkon laajentamiseen alueille, josta kaapeloinnit puuttuvat, kaapeleiden vetämiselle on esteitä tai halutaan säästää kaapelointikustannukset muihin tarkoituksiin. [1, s. 65–67.]

Mietittäessä langattoman lähiverkon rakentamista, tulee ottaa muutamia asioita huomioon. Ensimmäisenä tulee kartoittaa, riittääkö langattoman verkon kapasiteetti omiin käyttötarkoituksiin, sillä suurien tietomäärien siirtely useiden käyttäjien kesken tiputtaa verkon suorituskykyä merkittävästi.[1, s. 134–135.] Kuten Jaakko Pulkkisen insinöörityöstä [3] käy ilmi, päästään uusimmalla 802.11n [4] standardin laitteilla lähelle 100 Mbps kaapeliverkon tasoa ihanteellisissa olosuhteissa. Pulkkinen kuitenkin

muistuttaa, ettei 802.11n standardikaan tarjoa yhtä tasaista nopeutta kuin kaapeleilla toteutettu lähiverkko. Näistä voimme päätellä, että vielä on mentävä ajassa eteenpäin jokunen vuosi kunnes langattomien lähiverkkojen suorituskyky menevät langallisten verkkojen ohi.

2.2 Nopeudet

Kun otetaan puheeksi langattomien lähiverkkojen nopeudet, täytyy esiin nostaa muutamia seikkoja, jotka vaikuttavat asiaan. Langallisessa 100 Mbps:n lähiverkossa jokaiselle käyttäjälle on mahdollista tarjota 100 Mbps:n yhteys kytkimen avulla. Toisin on langattomassa lähiverkossa, jossa käytettävä kaistanleveys jaetaan kaikkien käyttäjien kesken. Tämä tarkoittaa sitä, että mitä enemmän käyttäjiä kyseiseen tukiasemaan on liitettynä, sitä pienempi on jokaiselle käyttäjälle jäävä kaistanleveys. Yksi keino lisätä kaistanlevyttä on asentaa rinnalle toinen tukiasema, jolle syötetään eri nimi ja radiokanava. Tämänlaisia tukiasemia on mahdollista asentaa rinnakkain kolme kappaletta. [5, s. 285.]

802.11 standardi julkaistiin vuonna 1997. Sen maksiminopeus oli 1 tai 2 Mbps ja se käyttää 2.4GHz taajuutta[2], [6.]

2.2.1 802.11a

Vuonna 1999 julkaistiin kaksi uutta standardia josta toinen oli 802.11a. Se käyttää 5GHz taajuutta ja sen maksiminopeus 54 Mbps, mutta pystyy säätämään nopeuden tarvittaessa 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps tai 6 Mbps nopeuksiin jos yhteydessä havaitaan heikentymistä . Käytännössä maksiminopeudella jäädään kuitenkin 30-35 Mbps tiedonsiirtonopeuteen.[2], [6.]

2.2.2 802.11b

Toinen vuonna 1999 julkaistusta standardista oli 802.11b. Sen käyttämä 2.4GHz taajuus aiheuttaa sen, ettei se ole yhteensopiva 802.11a standardin kanssa. 802.11b tukee 11 Mbps maksiminopeutta, mutta pystyy säätämään nopeuden 5.5 Mbps, 2 Mbps tai 1 Mbps jos yhteydessä havaitaan heikentymistä. Käytännössä 11 Mbps nopeudella jäädään noin 6 Mbps teoreettiseen nopeuteen.[2], [6.]

2.2.3 802.11g

Vuonna 2003 ilmestyi uusi standardi 802.11g, joka oli risteytys 802.11a:sta ja 802.11b:stä. Se käyttää 2.4GHz taajuutta ja on yhteensopiva vanhemman 802.11b:n kanssa. Uusilla menetelmillä saatiin 54 Mbps maksiminopeus, mutta käytännössä jäädään jopa 802.11a:n alapuolelle noin 20 Mbps tiedonsiirtonopeudella. Pienemmän taajuuden ansiosta kantama on parempi kuin 802.11a:lla.[6.]

2.2.4 802.11n

Tällä hetkellä uusin markkinoilla oleva standardi on 802.11n. Sille on luvattu jopa 600 Mbps nopeutta mutta kuten Jaakko Pulkkisen insinöörityöstä [3] käy ilmi, jäänee oikea nopeus 100–200 Mbps väliin. 802.11n standardin laitteet tukevat 5GHz sekä 2.4GHz taajuuksia, tästä johtuen se on yhteensopiva aiempien standardisoitujen laitteiden kanssa. 802.11n tukee MIMO (Multiple Input Multiple Output)-tekniikkaa, jonka avulla nopeudet saadaan suuremmiksi käyttämällä kahta antennia ja useampia kanavia samaan aikaan. MIMO-tekniikka käyttää hyväkseen monitie-etenemistä, jossa signaalien kimpoilut käytetään hyödyksi, kun yleensä niistä on vain haittaa.[4],[7.]

2.3 Antennit ja niiden hyödyt

WLAN-tekniikka käyttää tiedon siirtämiseen radioaaltoja. Radioaalloilla on kyky läpäistä esteitä, mutta erinäiset esteet aiheuttavat signaalin heikentymistä, eli vaimentumista. Riittävän toiminnan takaamiseksi tarvitaan tarpeeksi vahva signaali, jos laitteen oma antenni ei pysty vahvistamaan signaalia tarpeeksi, tulee yhdeksi

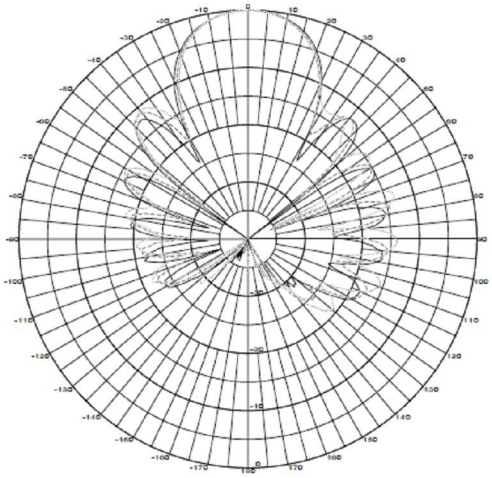
vaihtoehdoksi käyttää ulkoista antennia. Vahvistuksen ja vaimennuksen ilmoittamiseen käytetään desibelejä.[8], [9.]

Laitteen ulkopuolisella antennilla saavutetaan usein parempi vahvistus signaaleille. Antennit voidaan jakaa kahteen pääryhmään, suuntaaviin - ja ympärisäteileviin antenneihin. Näistä päätyypeistä löytyy useita erilaisia antennityyppejä ja antennityypin valinta riippuukin paljon käyttötarkoituksesta - ja paikasta. Antennien koosta voidaan yleisesti päätellä sen vahvistuskykyä, fyysisen koon kasvaessa usein myös sen tuoma vahvistus kasvaa. Otan seuraavaksi esittelyyn neljä eri antennityyppiä ja mainitsen olennaisia seikkoja kustakin tyypistä.[8], [9.]

2.3.1 Suunta-antennit

Kuvassa 1. olevaa suunta-antennia kutsutaan toiselta nimeltä myös Yagi-antenniksi. Jos verrataan suuntakuviota (kuva 2.) sektori - ja lautasantenniin, voidaan havaita sen sijoittuvan näiden puoleen väliin. Suuntakuvioissa on hyvä ottaa huomioon, että ne ovat kolmiulotteisia. Vahvistus onkin sektoriantennin kanssa samalla tasolla, mutta vähän kapeammassa kentässä, jonka seurauksena sillä saavutetaan vähän pidempi etäisyys.[8], [9], [10.]

KUVA 1. Suunta-antenni [10]

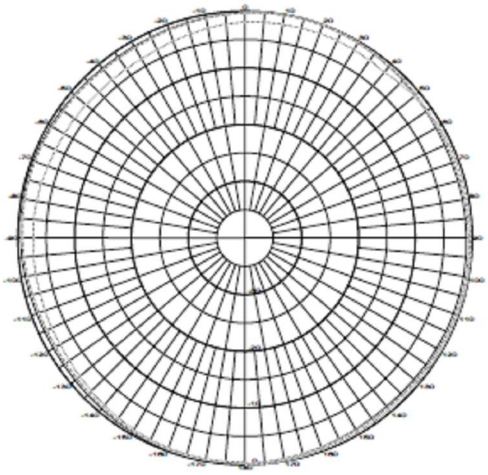


KUVA 2. Suunta-antennin suuntakuvio ylhäältä päin [10]

2.3.2 Ympärisäteilevät antennit

Ympärisäteilevän antennin vahvistus ja etäisyys eivät yllä suunta-antennien tasolle, mutta sen käyttötarkoituskin on toisenlaisessa ympäristössä. Ympärisäteilevä antenni soveltuu parhaiten tilanteeseen, missä se on mahdollista sijoittaa keskelle sitä ympäröiviä laitteita, joihin yhteys halutaan luoda. Kolmiulotteisessa suuntakuviossa kuvion muoto muistuttaa lähes palloa.[9], [10], [11.]

KUVA 3. Ympärisäteilevä antenni [11]

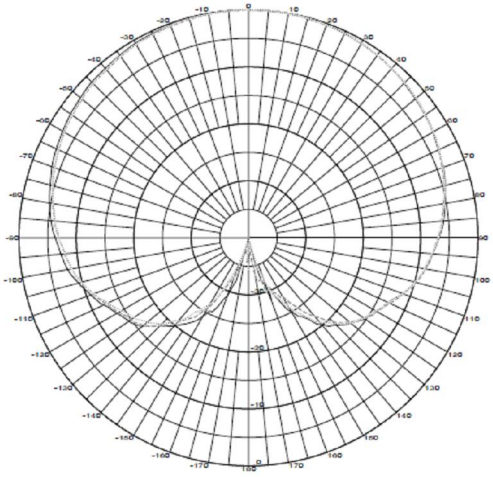


KUVA 4. Ympärisäteilevän antennin suuntakuvio ylhäältä päin [12]

2.3.3 Sektoriantennit

Sektoriantennin leveämpi suuntakuvio (kuva 6.) tekee siitä suunta-antennia paremman vaihtoehdon kohteisiin, missä tarvitaan hieman leveämpää peittoaluetta haluttuun suuntaan. Leveämpi peittoalue syö sen saavuttamaa maksimietäisyyttä, mutta siihen tarkoitukseen soveltuu paremmin lautasantenni, johon tutustumme seuraavaksi.[9], [10], [13.]

KUVA 5. Sektoriantenni [13]

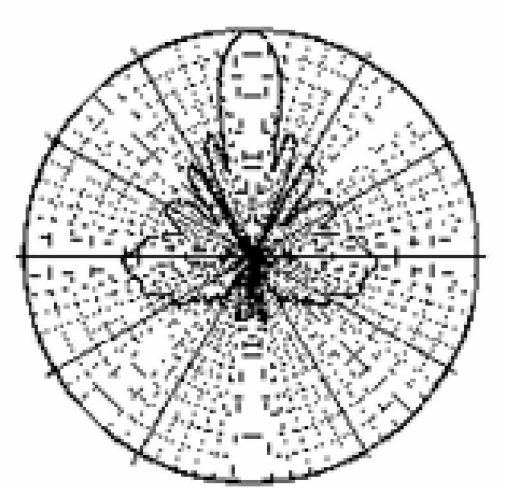


KUVA 6. Sektoriantennin suuntakuvio ylhäältä päin [14]

2.3.4 Lautasantennit

Pisintä etäisyyttä haettaessa on lautasantenni paras vaihtoehto signaalien lähettämiseen - ja vastaanottamiseen (kuva 7.). Suuntakuviosta (kuva 8.) nähdään, että lautasantennin luoma kapea peittoalue on tarkoitettu pitempien etäisyyksien saavuttamiseksi. Kapealla suuntakuviolla saavutetaan pisin etäisyys koska suurin osa vahvistukseen käytettävästä tehosta suuntautuu tuohon kapeaan, kiilamaiseen pisteeseen, eikä teho hajaannu ympäriinsä kuten esimerkiksi ympärisäteilevällä antennilla.[9], [10], [15.]

KUVA 7. Lautasantenni



KUVA 8. Lautasantennin suuntakuvio ylhäältä päin [16]

2.3.5 Tee-se-itse- antennit

Aikaisemmat kuvat eri antennityypeistä olivat kaupallisista antenneista. Itse tehdyt antennit ovat varmasti olleet radiotekniikan harrastajien - ja ammattilaisten tiedossa yleisesti. Internetin yleistyminen on kuitenkin levittänyt tätä tietotaitoa ripeään tahtiin. Jo muutamalla hakusanalla löytää internetin hakukoneesta linkkejä sivustoihin, joista löytyvät tarkat rakennusohjeet omatekoisille antenneille. Nostan esiin muutamia tee-se-itse-tekoisia, yleisesti käytettyjä antennityyppejä, joiden tekeminen onnistuu kätevästi kotonakin.

Yksinkertaisen ja halvan antennin saa itse tehtyä vaikka vanhasta kahvi - tai säilykepurkista (kuva 9.). Purkin halkaisijan tulisi olla noin 10 cm luokkaa. Paremman vahvistuksen saavuttamiseksi, tulisi purkin sisäpintojen olla mahdollisimman sileitä. Antennin rankentamiseen tarvitsee omaan verkkokorttiin sopivat liittimet ja sopivan pituisen matalahäviöisen välikaapelin, jotta kaapelin tuoma vaimennus olisi mahdollisimman pieni.[17.]

KUVA 9. Omatekoinen WLAN-antenni [18]

Yleistyviin USB-liittimillä (Universal Serial Bus) varustettuihin WLAN-sovittimiin on myös mahdollista käyttää aikaisemmin mainittua antenninrakennusohjetta. WLAN-sovitin tulee sijoittaa kuvassa 9 näkyvän liittimen kohdalle. Täysin tarkkaa kohtaa tai asentoa ei kuitenkaan pysty määrittelemään kokeilematta, sillä USB-liittimillä varustettujen WLAN-sovittimien rakenteet voivat erota toisistaan[19].

Lautasantenneista tutulla rakenteella voidaan valmistaa omatekoisia antenneja pitemmille etäisyyksille. Heijastinpinnaksi kelpaa usein laakeanmallinen esine, aina siivilöistä lampunvarjostimiin (kuva 10.). Kuvan 10 antennin rakentamisen ainoat työvaiheet ovat WLAN-sovittimen oikean etäisyyden - ja kohdan määrittely testaamalla, sekä itse WLAN-sovittimen kiinnitys heijastinpintaan.[20.]

KUVA 10. Omatekoinen USB-sovittimella varustettu WLAN-antenni [21]

2.3.6 Kantomatkat

Aikaisemmin mainituilla antenneilla saavutetaan merkittäviä parannuksia WLAN-sovittimien toimintaetäisyyksiin. Ei ole siis ihme, että nämä rakennusohjeet - ja mallit saavuttavat suosiotaan kaikkien WLAN-verkkoja käyttävien keskuudessa. Täytyy kuitenkin muistaa, että lakipykälillä on määrätty sallitut maksimilähetystehot.

Suunnattavilla antenneilla päästää parhaimmillaan useista kilometreistä jopa kymmenen kilometrin etäisyyksiin hyvissä olosuhteissa. Korkea sijainti ja esteetön näkyvyys kohteeseen luovat hyvät puitteet pitemmän yhteyden saavuttamiseksi. Signaalien etenemiseen vaikuttavat tekijät kuten puut, maaston muodot, rakennukset, mastot ja vallitseva säätila vaimentavat osaltaan lähtevää signaalia.[20], [22.]

Kotikonsteinkin saavutettavat pitemmät kantomatkat herättävät kysymyksen, onko WLAN-yhteys turvallinen peruskäyttäjän tiedonsiirtomenetelmä ja luulevatko syrjemmällä asuvat verkkonsa salauksen turhaksi.

3 LANGATTOMAN LÄHIVERKON SALAUSMENETELMÄT

Työn kannalta olennaisia salausmenetelmiä ovat WEP - ja WPA-salaus, sillä oman työn osuudessa tarkoitukseni on selvittää onko WEP-salaus salausmenetelmä niin heikko kun on maailmalla annettu ymmärtää. WPA-salausta pidetään riittävänä salausmenetelmänä useimmissa ympäristöissä. WPA-salauksen osalta keskityn selvittämään onko se salausmenetelmänä riittävä ja onko se mahdollista murtaa.

3.1 WEP-salaus

WEP oli ensimmäinen WLAN-salausmenetelmä, joka tuli 802.11-standardin mukana. Sen päätavoitteena oli tehdä WLAN-verkosta lankaverkon kaltainen turvallisuudeltaan, suunnittelijat saivat kuitenkin todeta epäonnistuneensa tässä yrityksessä.

WEP-salaus perustuu RC4-nimiseen salausalgoritmiin, jonka avulla luodaan salaus käyttäen joko 40 tai 104-bittisestä salausavainta ja 24-bittistä IV:tä eli alustusvektoria (Initialization Vector). Salausavain, alustus - ja tarkistusvektori yhdistetään ennen RC4-algoritmiin toimitusta, jonka tuloksena syntyy 64 tai 128-bittinen salaus. WEP:n heikkous salausmenetelmänä WLAN-verkoille perustuu juuri tähän 24-bittiseen alustusvektoriin, koska se liitetään salaamattomana salauksenmuodostusvaiheessa. [23, s. 213-214.]

Alustusvektori on määritelty liian pieneksi. Samaa alustusvektoria käytetään uudestaan lähetettäville datapaketeille. Tästä johtuen lähetettävien kehyksien salaus alkaa muistuttaa toisiaan liian nopeasti ja keräämällä tarpeeksi samaan alustusvektoriin perustuvia kehyksiä, voidaan salausavain selvittää. Suuri liikennöinti verkossa nopeuttaa avaimen selvittämistä, koska alustusvektorit alkavat toistumaan sitä nopeammin mitä enemmän dataa liikkuu. [23, s. 213-214.]

Myös bittien tarkistukseen käytettävä lineaarinen, 32-bittinen CRC-menetelmä (Cyclic Redundancy Check) epäonnistuu tehtävässään. Vaikka RC4-algoritmista saatu salaus sisältää tarkistusvektorin eli ICV:n (Integrity Check Vector) tiedon salattuna, ei tästä ole mitään hyötyä. CRC-menetelmä nimittäin mahdollistaa tietojen muuttamisen ilman ICV:n oikeellisuuteen vaikuttavia muutoksia. Muutokset aiheuttavat ennustettavan

muutoksen tarkistussummassa. Tämän opin avulla muutetuissa tiedoissa vain tiettyjen bittien arvoja muuttamalla, saadaan tarkistussumma täsmäämään, vaikkei salattua ICV:tä edes tiedetä. [23, s. 213-214.]

Käyttäjän todentamiseen eli autentikointiin on WEP:ssä kaksi mahdollisuutta, avoin (Open Authentication) ja jaettu-avain (Shared-Key Authentication). Käytettäessä avointa todentamista, hyväksyy tukiasema autentikoitumisen kaikilta liittyjiltä. Jaettu-avain metodilla täytyy vastaanottajan ja lähettäjän syöttää sama WEP-avain omiin kokoonpanoihinsa. Yleensä kyseessä on AP (Access Point) ja Client eli käyttäjän tietokone tai muu laite. [23, s. 129-136.]

3.2 WPA-salaus

WPA-salaus luotiin paikkaamaan WEP:ssä olevat puutteet ja tietoturva-aukot. Koska WPA perustuu osittain laitepohjaisiin WEP-algoritmeihin, täytyy sen peruselementit säilyä ennallaan, kuten alustusvektori, RC4-algoritmi ja tarkistussumma. Se käyttää edelleen WEP:stä löytyvää RC4-salausalgoritmia mutta rinnalle on lisätty muita uudistuksia. Yksi uudistuksista oli TKIP(Temporal Key Integrity Protocol), jonka tarkoitus on korjata WEP:ssä esiintyvä avaimien uudelleenkierrätys. TKIP luo jokaiselle paketille eri salausavaimen, lisäksi se sisältää pakettilaskurin, joka yhdessä MIC:n (Message Integrity Check) kanssa estää pakettien muokkaamisen - ja uudelleenlähettämisen. [23, s. 239-240.]

WPA-salauksen turvallisuutta voidaan parantaa käyttämällä erillisiä autentikointiservereitä(Radius server), joiden kautta yhdistyvät clientit tunnistetaan. Näitä menetelmiä on useita tarjolla, joista mainittakoon EAP(Extensible Authentication Protocol), PEAP(Protected EAP), LEAP(Lightweight Extensible Authentication Protocol) ja 802.11x. [23, s. 180-204.]

En aio perehtyä autentikointiservereiden saloihin tämän enempää, koska omassa työssäni ei ole tarkoitus käyttää niitä.

3.3 WPA2-salaus

Vuonna 2004 julkaistiin uusi 802.11i –standardiin perustuva WPA2-salausmenetelmä, se on nykyäänkin uusin salausmenetelmä WLAN-teknologiassa. Se vaatii laitteistolta laitepohjaisen tuen, joten siirtyessä WPA2-salaukseen voidaan joutua päivittämään laitteita uusiin. Suurimpana uudistuksena WPA:n käyttämä RC4-algoritmi korvattiin CCMP-protokollalla (Counter Mode/CBC-MAC Protocol), joka perustuu AES-standardiin(Advanced Encryption Standard). AES-standardin turvallisuudesta salausmenetelmänä kertoo sekin seikka, että se täyttää Yhdysvaltain hallituksen tietoturvavaatimukset. [24.]

AES mahdollistaa 128, 192 ja 256-bitin pituisten avaimien käyttämisen mutta WPA2 käyttää 802.11i-standardiin pohjautuen 128-bittistä salausta. AES-salausta vastaan ei ole tiedossa yhtään hyökkäysmenetelmää ja tutkimukset osoittavat, että sen purkamiseen tarvittaisiin 2^{120} operaatiota. [24.]

4 OMAT TESTAUKSET

Nyt olisi tarkoitus testata omilla laitteillani internetistä löytyviä menetelmiä salauksien purkamiseen. Oman haasteensa luo laitteiden yhteensopivuus saatavilla olevien ohjelmien kanssa. Usein vaaditaan muokatut laitteistoajurit, joilla laitteet saadaan toimimaan käytettävillä ohjelmilla oikein. Tästä huolimatta osa laitteista ei tue jotain ominaisuuksia mitä jokin toinen laite.

WEP – ja WPA-hyökkäyksissä käytetään seuraavia menetelmiä:

- Man in the middle
- Dictionary Brute Force

WEP-salauksen murtamiseen käytettävä hyökkäysmenetelmä perustuu niin sanottuun Man in the middle-hyökkäykseen. Tässä menetelmässä on tarkoitus seurata tukiaseman ja clientin välistä tiedonsiirtoa. Tiedonsiirrosta kaapataan viestejä, joita syötetään verkkoon uudelleen. Tukiasemaa huijataan luulemaan, että viestit tulevat lailliselta clientiltä. Omassa työssä menetelmällä kaapataan ARP-viestejä (Address Resolution Protocol), joita uudelleen syöttämällä alustusvektoreiden kaappausnopeus kasvaa

huomattavasti. Riittävä määrä kaapattuja alustusvektoreita mahdollistaa WEP-salauksen murtamisen.

WPA-hyökkäyksissä käytetään Dictionary Brute Force-menetelmää. Nimensä mukaan menetelmässä käytetään ”sanakirjaa” ja raakaa voimaa. Sanakirjalla tarkoitetaan tiedostoa, joka sisältää sanoja listattuna. Sanat voivat koostua etu – ja sukunimistä, paikannimistä, sanakirjoista otetuista sanoista ja niin edelleen. Hyökkäyksessä salasanaa verrataan tiedostosta löytyviin sanoihin. Tämän prosessin nopeuteen vaikuttaa tietokoneen prosessorin teho ja tiedoston sisältämien sanojen määrä.

4.1 Käytettävä laitteisto

Työssäni käytin A-LINK WNAP-tukiasemaa, Linksys WUSB600N WLAN-verkkokorttia sekä kahta tietokonetta ja PS3-pelikonsolia.

A-LINK WNAP-tukiasema tukee 802.11n/g/b-standardin laitteita, sekä salausmuotoina WEP, WPA ja WPA2-salauksia, joten se soveltuu työn toteuttamiseen hyvin. Lisäksi se tukee 3G-modeemien jakamista tukiasemasta löytyvän USB-portin kautta, näin saan käytössäni olevalla ”nettitikulla” internet-verkkoliikennettä aikaiseksi.
Salauksien purkamiseen käytän Linksys WUSB600N WLAN-verkkokorttia, joka toimii USB-väylässä. Laite tukee 802.11n/g/b-standardeja ja käyttää aikaisemmin mainittua MIMO-tekniikkaa. Laitteen ajureina käytetään normaalista poikkeavia, muokattuja ajureita, joista kerron myöhemmin lisää.

PS3-pelikonsolia tarvitsin WPA2 salauksen yhteydessä, koska oman kannettavan tietokoneeni WLAN-piiri ei tue WPA2 salausta. Näin sain liitettyä myös WPA2-salauksella olevan laitteen testiverkkoon.

KUVA 11. A-LINK WNAP ja Linksys WUSB600N

4.2 Salauksenpurku ympäristö

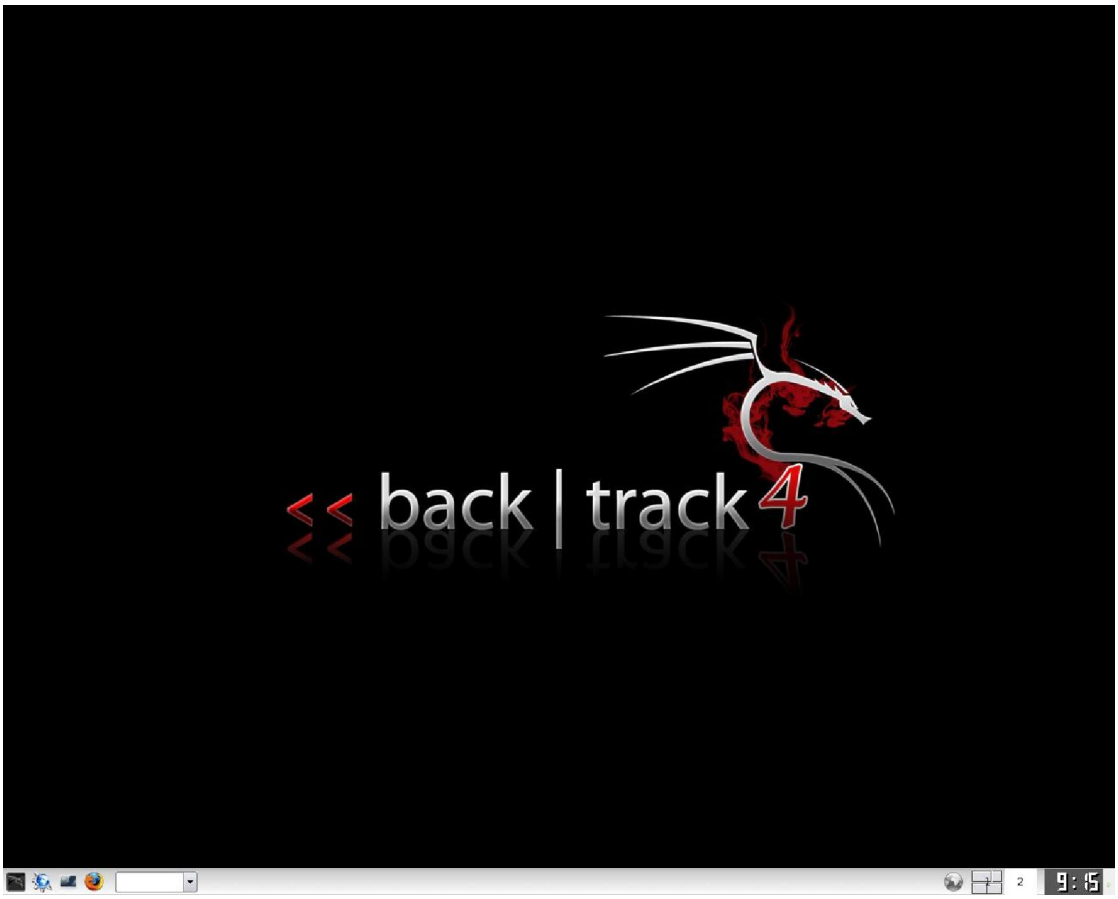
Tärkeimpänä elementtinä salauksenpurku ympäristössä tapahtuvassa testauksessa on Backtrack-ohjelmisto [25]. Se on Linuxia käyttävä ohjelmistokokonaisuus, joka sisältää valmiiksi asennetut tietoturva - ja testausohjelmistot. Näitä esiasennettuja ohjelmia löytyy yli 300 kappaletta. Ohjelmia löytyy muun muassa WLAN, VoIP (Voice over Internet Protocol) - ja Bluetooth-laitteistoille. Näiden ohjelmien avulla voidaan suorittaa hyökkäyksiä ja kartoittaa tietoturvan tasoa. Ohjelmistosta on varmasti apua tietoturva-asiantuntijoille ja muille tietoturvasta kiinnostuneille. Se sisältää myös muokatut ajurit monille laitteille valmiina, joten useissa tapauksissa säästytään ajureiden manuaaliselta asennukselta.

Backtrack-ohjelmiston ovat luoneet eri aloilta ja kansalaisuuksista koostuva työryhmä. Ohjelmiston kehittämiseen he käyttävät vapaa-aikaansa, sillä he haluavat ohjelmiston pysyvän ajan tasalla. Ohjelmistolle on kehitetty laajoja keskusteluryhmiä internetiin. Ongelmatilanteissa näistä on suuri apu käyttäjille ja luultavasti myös ohjelmiston kehittäjille, jotka voivat käyttää tietoja tulevissa julkaisuissa.

Backtrack-ohjelmistossa on tarkoitus suorittaa seuraavia toimenpiteitä:

- Ajureiden asentaminen WLAN-sovittimelle ja paketinsyötön testaus
- Verkkojen etsintä ja tiedonkeräys
- Hyökkäykset WEP-salattuun verkkoon
- Hyökkäykset WPA-salattuun verkkoon

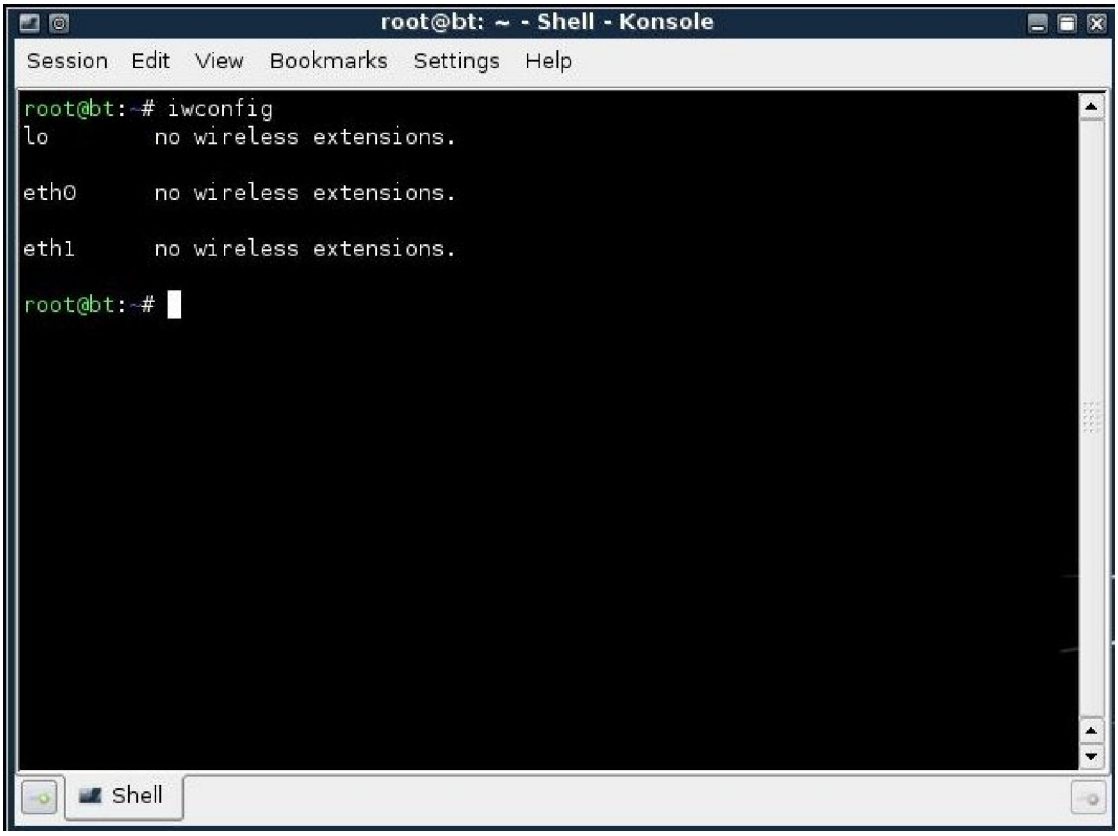
Oletuksena ohjelmisto käyttää käyttäjätunnuksena ”root” ja salasanana ”toor”. Työpöytänäkymän saa käyttöön kirjoittamalla ”startx” kirjautumisen jälkeen. Kuvassa 12 on Backtrack 4 Beta:n työpöytä käynnistyksen ja kirjautumisen jälkeen. Tästä lähtöpisteestä lähdetään suorittamaan toimenpiteitä testauksien toteuttamiseksi.



KUVA 12. Backtrack 4 Beta työpöytä

Ensimmäisenä on syytä tarkistaa onko Backtrack-ohjelmisto tunnistanut käytettävän WLAN-sovittimen automaattisesti vai joutuuko ajurit asentamaan itse. Tämä tapahtuu avaamalla shell eli kometokehoite-ikkuna, johon syötetään komento ”iwconfig”. WUSB600N-sovittimen pitäisi näkyä päätteellä ”ra0” koska se käyttää Ralink:n piiriä [26]. Backtrack ei kuitenkaan tunnistanut käytettävää WUSB600N-sovitinta vaan

joudun asentamaan ajurit manuaalisesti (kuva 13.). Käytettävien ajureiden täytyy kuitenkin olla yhteensopivia käyttöjärjestelmän kernel:n eli ytimen kanssa. Muutoin ajureiden asennuksessa tulee virheilmoituksia, jotka itse sain myös huomata käyttäessäni eri versioita ajureista. Seuraavaksi tarkastellaan vaiheita ajureiden asennuksesta.



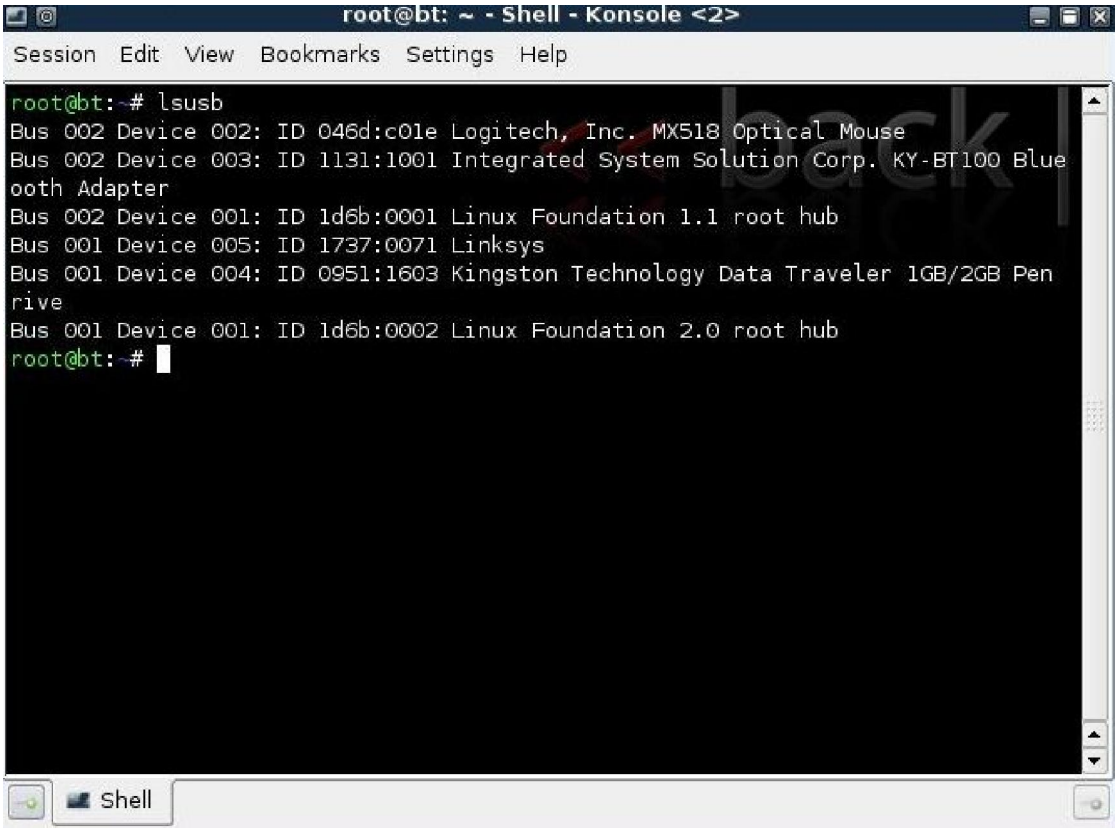
KUVA 13. WLAN-sovitin ei näy

Suorittamalla komento ”lsusb”, saadaan listattua koneeseen kytketyt USB-laitteet (kuva 14.). Kyseisestä listasta havaitaan Linksys-laite, joka tässä tapauksessa on kytketty WUSB600N-sovitin. Listasta otetaan talteen ID-kohdan jälkeinen numerosarja, koska sitä tarvitaan myöhemmässä vaiheessa.

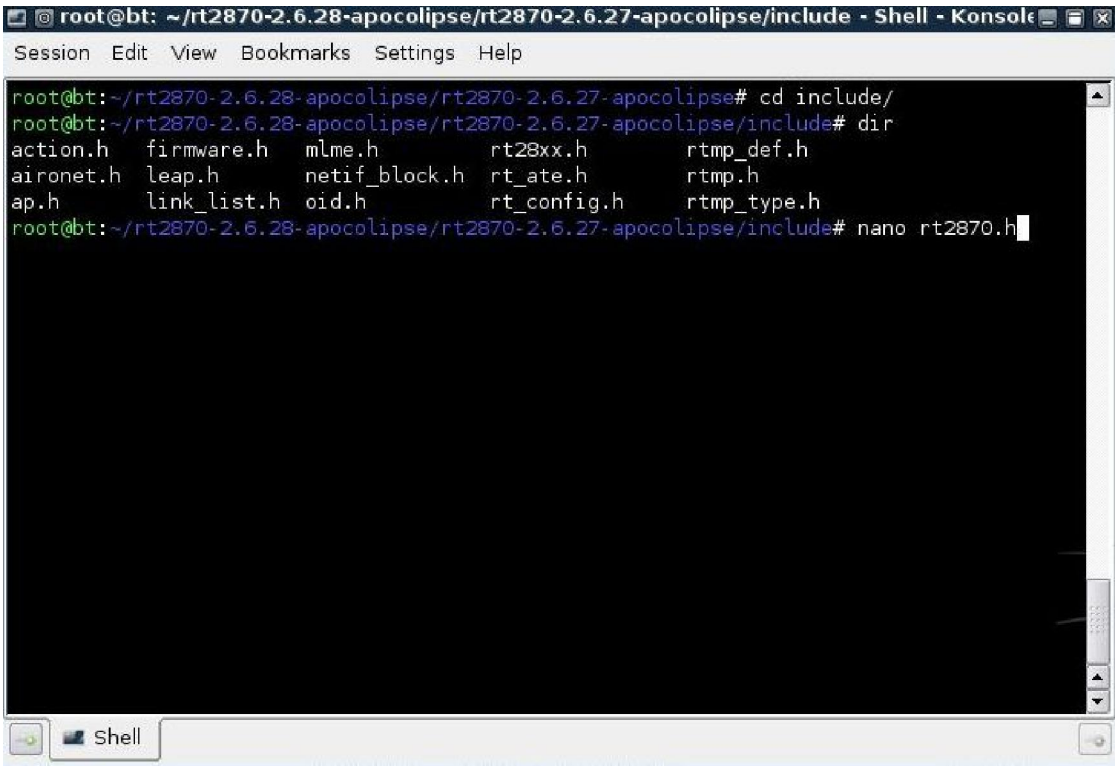
Seuraavaksi siirrytään asennettavien ajureiden include-kansioon, jossa avataan rt2870.h-tiedosto nano tekstieditorilla (kuva 15.). Kun nano-tekstieditori on käynnistynyt, selataan kohtaan ” #define RT2870_USB_DEVICES \” jonka alle lisätään rivi ”{USB_DEVICE(0x1737,0x0071)}, /* WUSB600N */ \”. Rivi sisältää juuri tämän talteen otetun ID-numerosarjan, joka selvitettiin aikaisemmin (kuva 16.). Lopuksi tallennetaan muutokset ja poistutaan nano-tekstieditorista.

Nyt kun ajurit on muokattu WUSB600N-sovittimelle sopivaksi, on aika suorittaa itse asennus. Ensin poistutaan include-kansiosta ja sitten syötetään ”make && make install” komento (kuva 17.). Nyt laiteajurit on asennettu rt2870sta-moduuliin, mutta moduuli täytyy ottaa vielä käyttöön, jotta lisätty laite saadaan toimintakuntoon. Tämä tapahtuu komennolla ”modprobe rt2870sta” (kuva 18.).

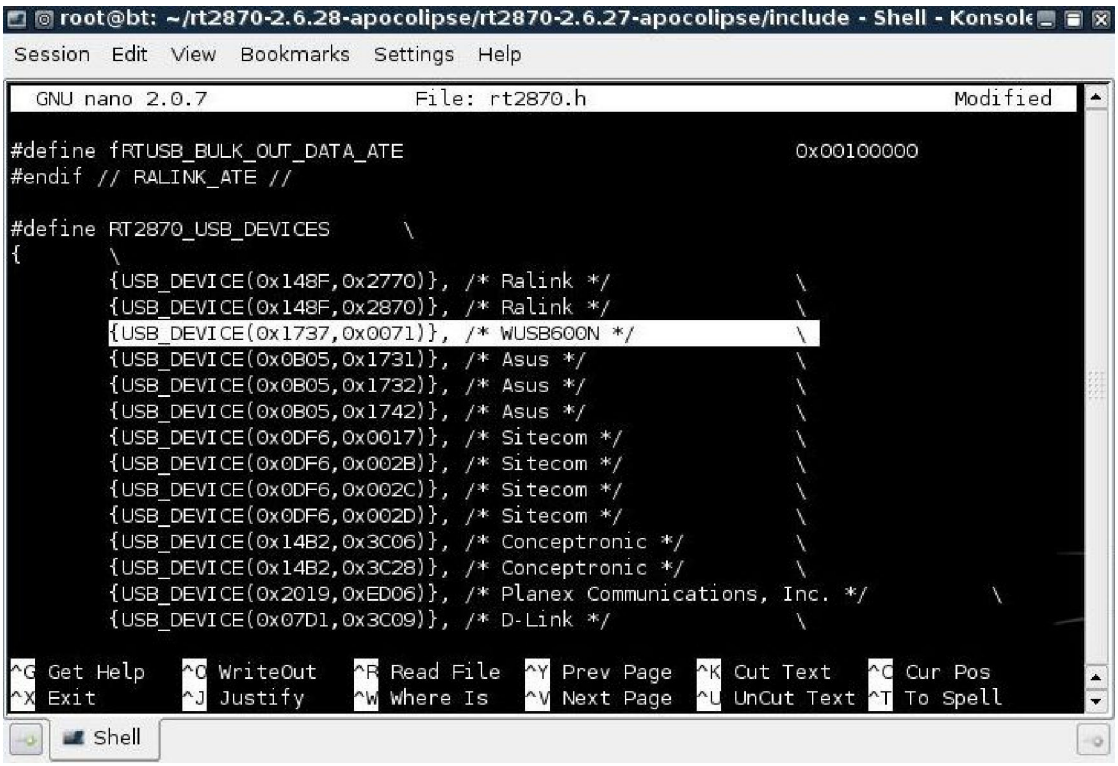
Nyt tarkistetaan tilanne uudestaan suorittamalla komento ”iwconfig” ja voidaan todeta että laite näkyy kyseisessä listassa (kuva 19.).



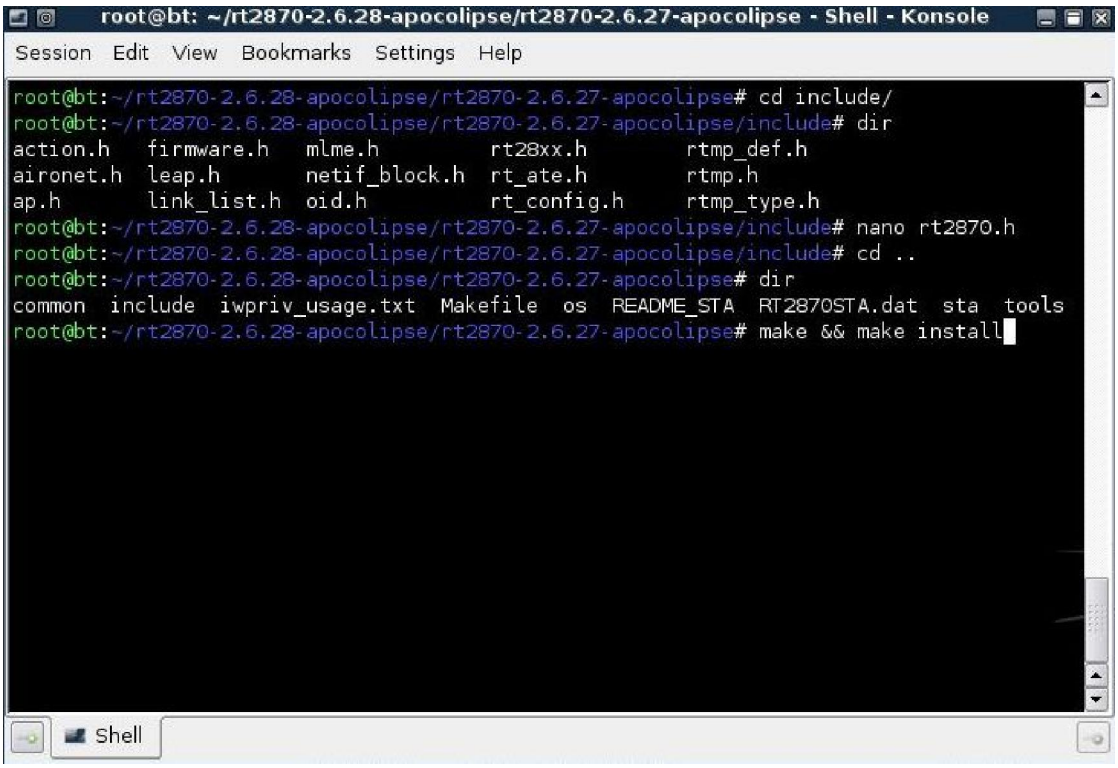
KUVA 14. USB-laitteet listattu



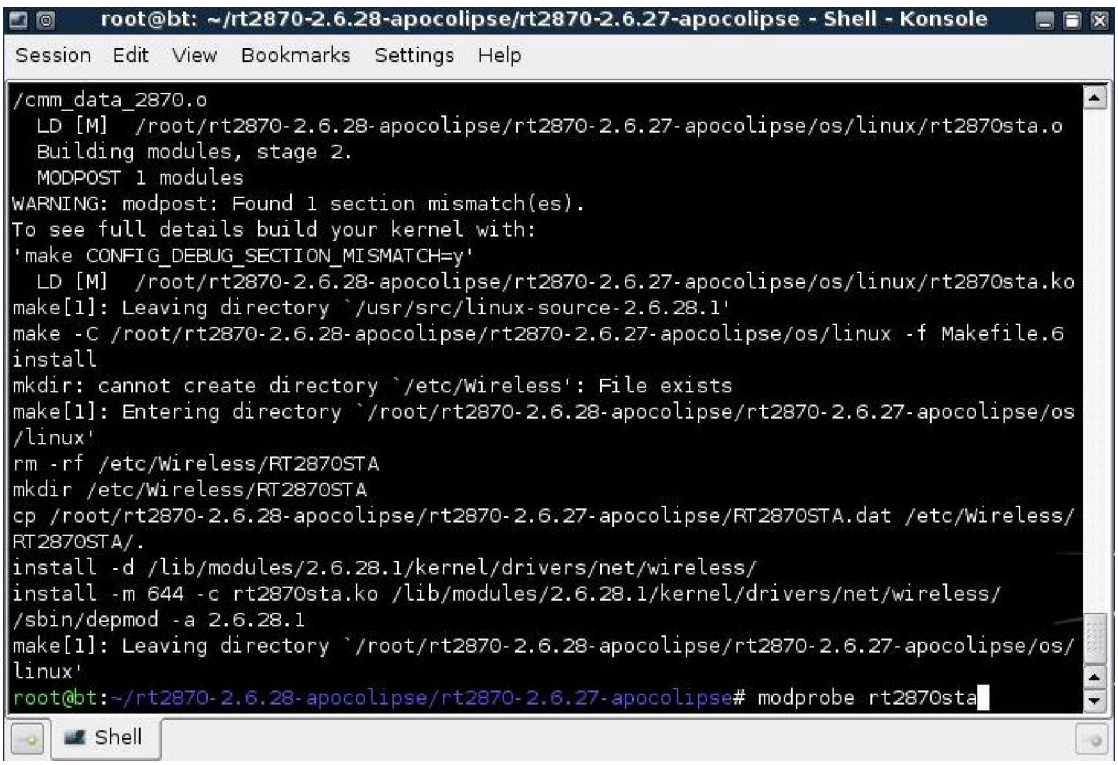
KUVA 15. Suoritetaan komento nano rt2870.h



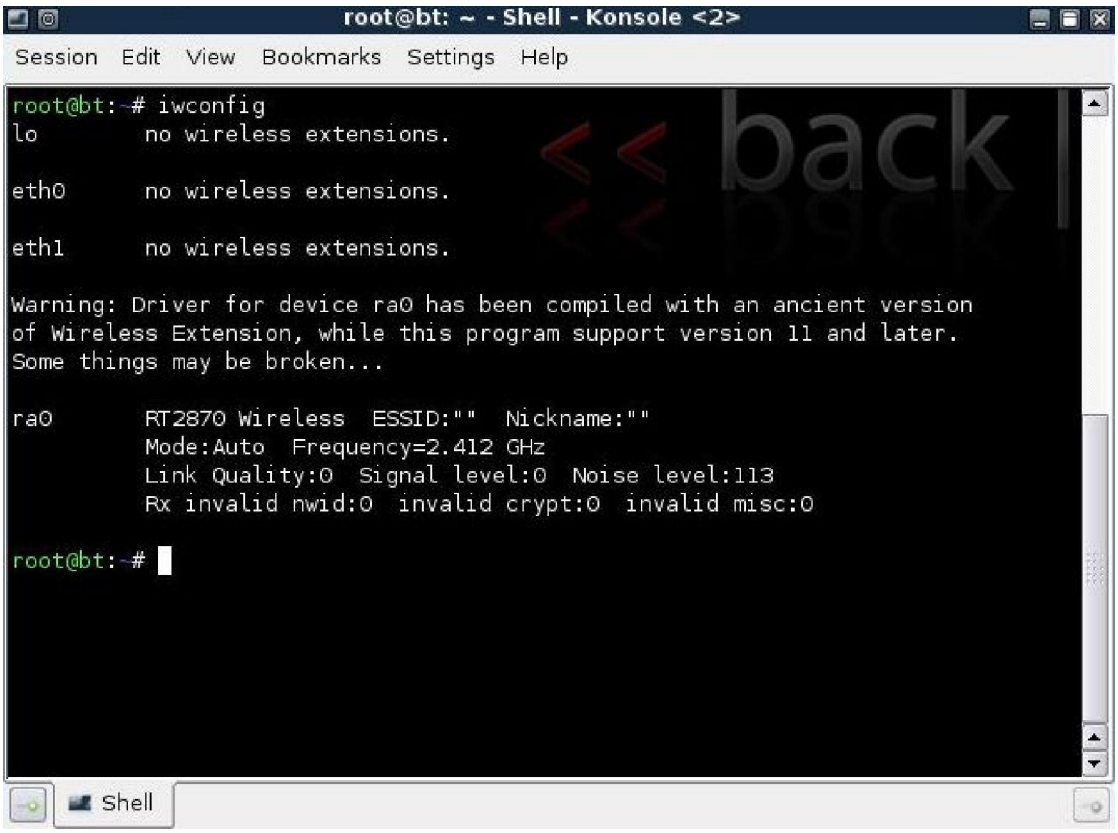
KUVA 16. WUSB600N-sovitin lisätty listaan



KUVA 17. Suoritetaan komento make && make install

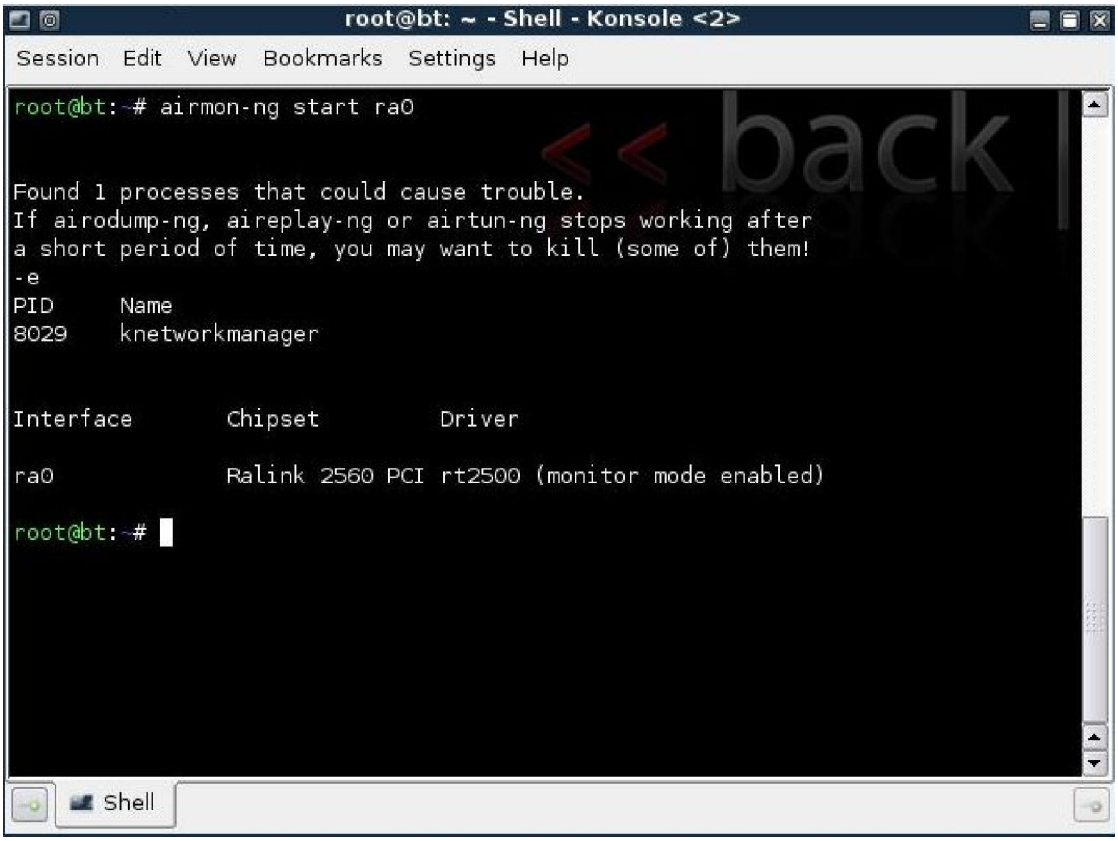


KUVA 18. Suoritetaan komento modprobe rt2870sta



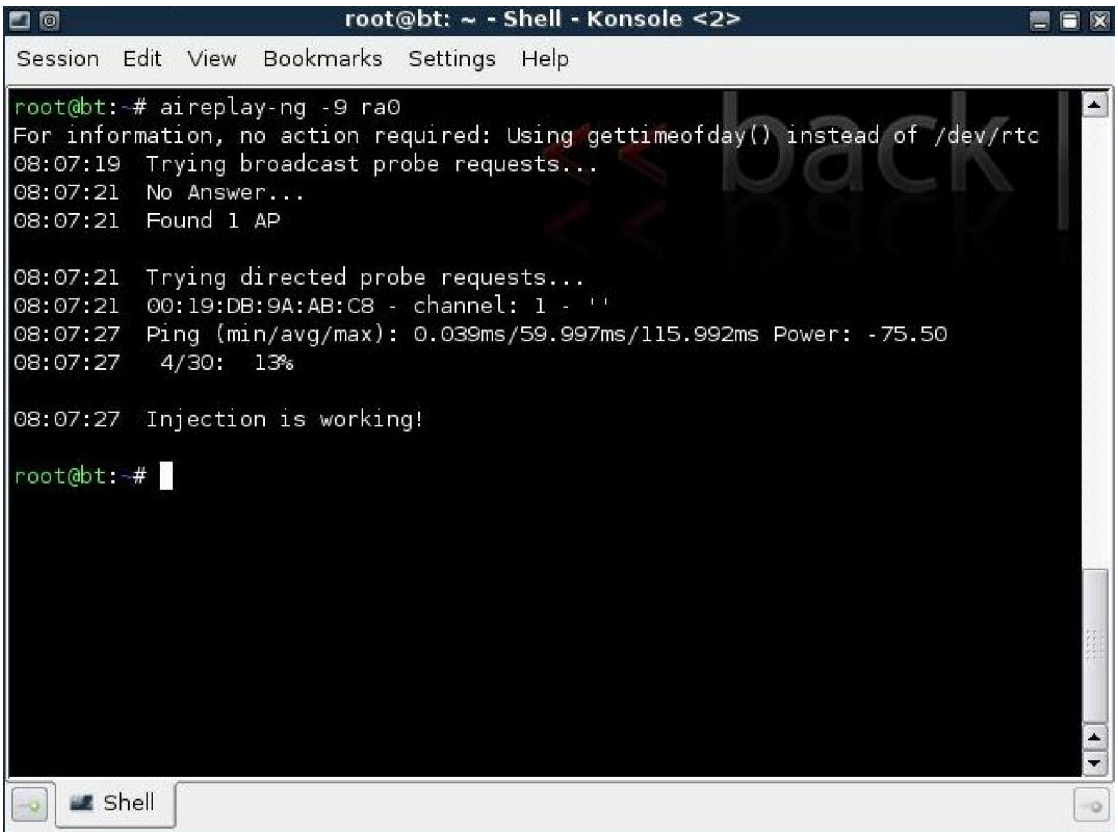
KUVA 19. WLAN-sovitin näkyy

Nyt on vuorossa toimenpide, jolla WLAN-sovitin saadaan niin kutsuttuun monitor-mode tilaan[27]. Tämä tila mahdollistaa pakettien kaappaamisen ilman assosioitumista AP:n kanssa. Tähän tilaan päästää syöttämällä komento ”airmon-ng start ra0” (kuva 20.) [28].



KUVA 20. WLAN-sovitin kytketty monitor-mode tilaan

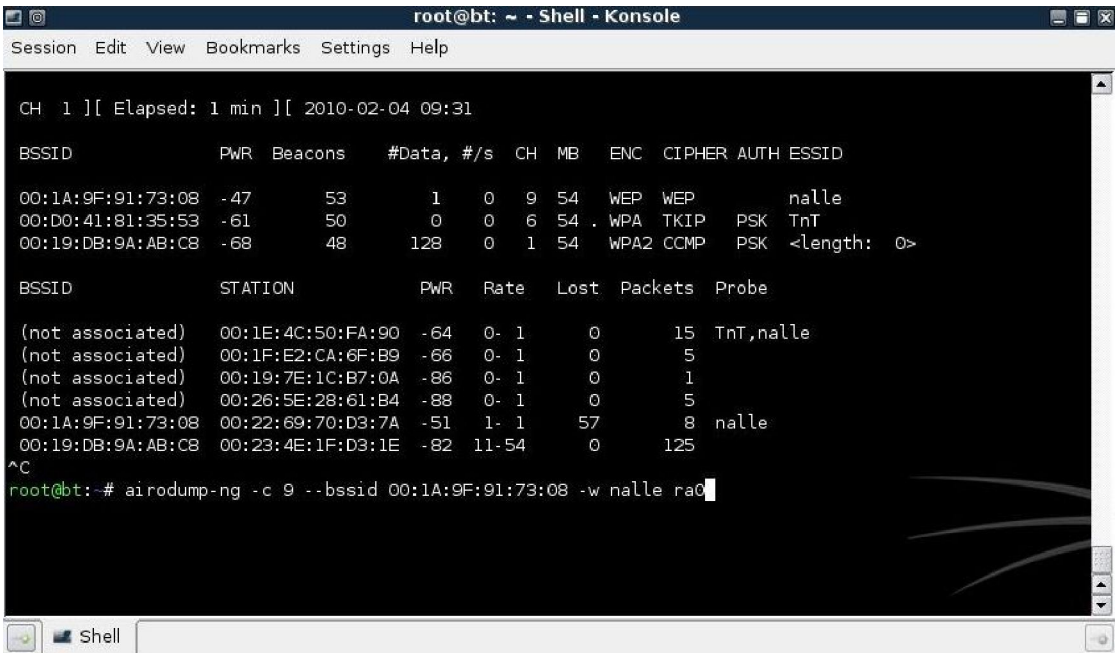
Tärkeimpinä ominaisuuksina muokatuissa ajureissa voidaan pitää, mahdollisuutta kytkeytyä monitor-mode tilaan, sekä syöttää paketteja verkkoon (Packet Injection). Aireplay-ng on Backtrack:n mukana tuleva ohjelma, jolla pystyy toteuttamaan monia hyökkäyksiä verkkoon[29]. Kuvassa 21 on syötetty komento ”aireplay-ng -9 ra0”, jolla käynnistetään automaattinen testaustoiminto paketinsyötön toimivuuden varmistamiseksi. Se etsii tukiaseman ja kokeilee pakettien lähettämistä. Kuvan tapauksessa vain neljä pakettia 30:stä saatiin syötettyä. Tämä kertoo liiasta välimatkasta tukiasemaan ja joissain tapauksissa myös liian lyhyestä välimatkasta. Testaustoiminnolla saatiin todettua, että ajurit tukevat paketinsyöttöä ja ne toimivat odotetulla tavalla. Nyt kun laitteisto on saatu toimintakuntoon, voidaan siirtyä WEP-salauksen murtamiseen.



KUVA 21. Packet Injection toimii

4.2.1 Verkkojen etsintä ja tiedonkeräys

Ensimmäisenä toimenpiteenä täytyy etsiä tukiasema ja aloittaa tiedonkeräys. Tähän tarkoitukseen Backtrack tarjoaa airodump-ng ohjelman[30]. Airodump-ng:tä voidaan käyttää, oli sitten kyseessä WEP - tai WPA-tyyppinen salaus. Airodump-ng saadaan käynnistettyä komennolla ”airodump-ng ra0”, jolloin kytketty WUSB600N-sovitin alkaa kerätä tietoja kaikista ympäriltä löytyvistä tukiasemista, kaikilta kanavilta. Normaalisti ei ole järkevää kerätä tietoa kuin valitulta tukiasemalta, näin turhan tallennetun datan määrä vähenee. Tällöin airodump-ng kannattaa käynnistää uudelleen tarkennetuilla komennoilla, kuten kuvassa 22 ollaan tekemässä. Kuvassa tietoa aletaan kerätä kanavalta 9, määritetyltä tukiaseman MAC-osoitteelta (Media Access Control) ja tallennettujen tiedostojen nimet määritellään alkaviksi nalle nimellä. Tämän jälkeen airodump-ng:n näkymässä näkyy vain tämä määritelty tukiasema ja mahdollisesti siihen yhdistyneet clientit. Airodump-ng näyttää myös paljon muutakin tietoa verkoista, joista WEP-salauksen kohdalla tärkeimpänä voidaan pitää ”#Data” arvoa. WEP-salauksessa tämä arvo kuvastaa kaapattujen IV-pakettien määrän.

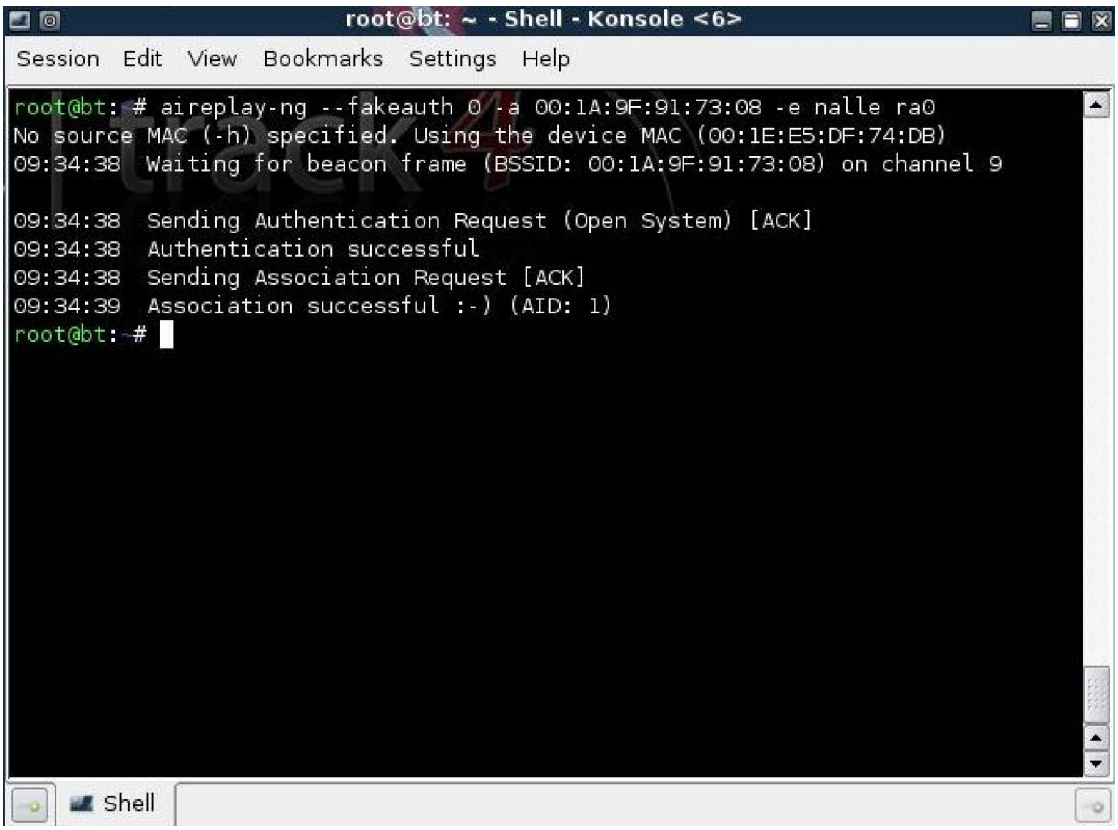


KUVA 22. Airodump-ng tarkennetaan kohteeseen

4.2.2 WEP-salauksen murtaminen

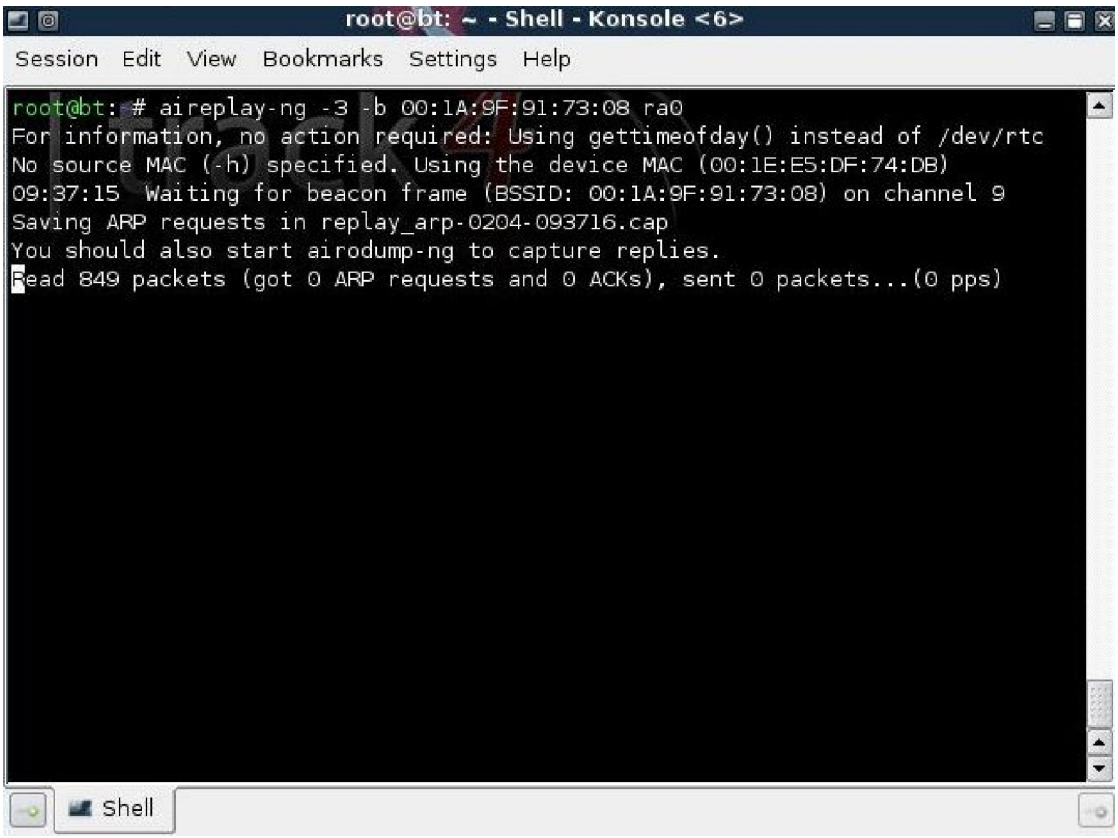
Ensimmäisessä tapauksessa 128-bittinen WEP-salaus on suoritettu avoimella autentikoinnilla (Open System Authentication), joka sallii kaikkien laitteiden assosioitumisen tukiasemaan. Tukiasemaa ei kuitenkaan pysty käyttämään ilman WEP-avainta mutta mahdollistaa pakettien syöttämisen verkkoon. Tässä ensimmäisessä tapauksessa tukiasemaan on yhdistynyt client.

Seuraavaksi suoritamme vale-autentikointi hyökkäyksen (Fake Authentication Attack), jolla oma WLAN-sovitin assosioidaan verkkoon nimeltä nalle (kuva 23.)[31]. Nyt kaapattavien IV-pakettien kasvua voidaan nopeuttaa erilaisilla hyökkäyksillä. Näin WEP-salauksen murtamiseen käytettävä aika lyhenee huomattavasti.

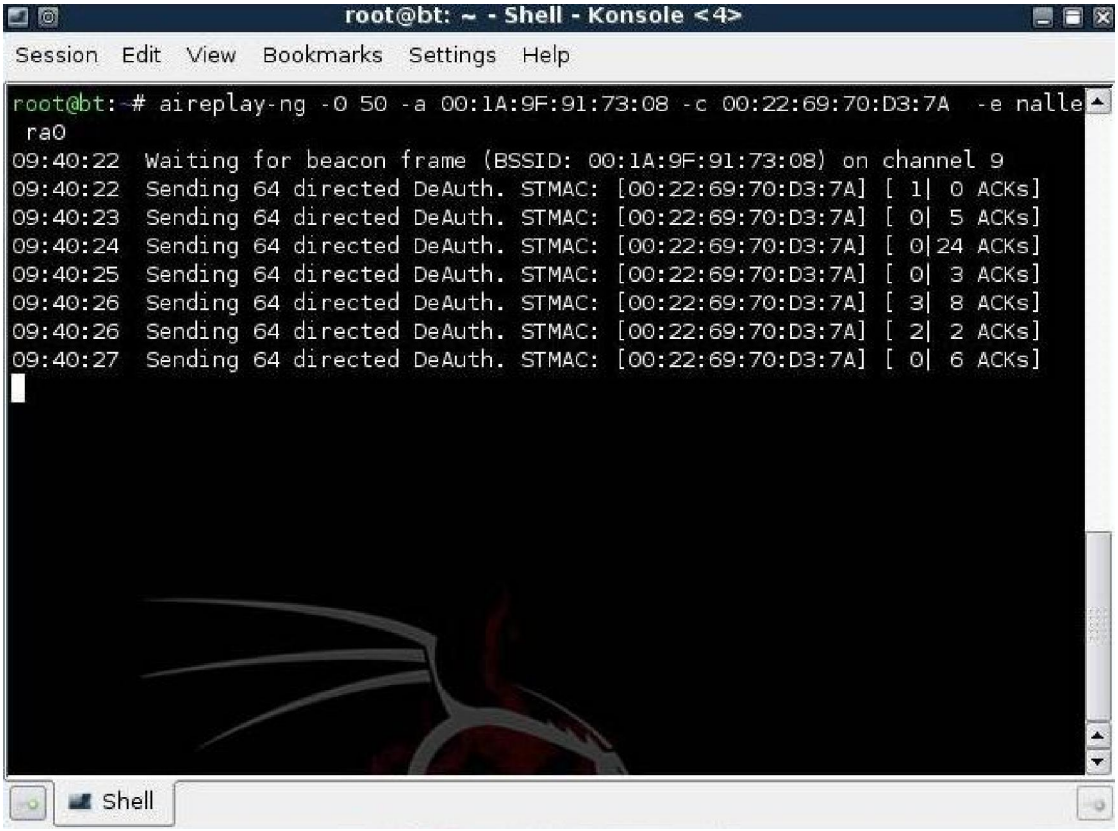


KUVA 23. Fake authentication suoritettu

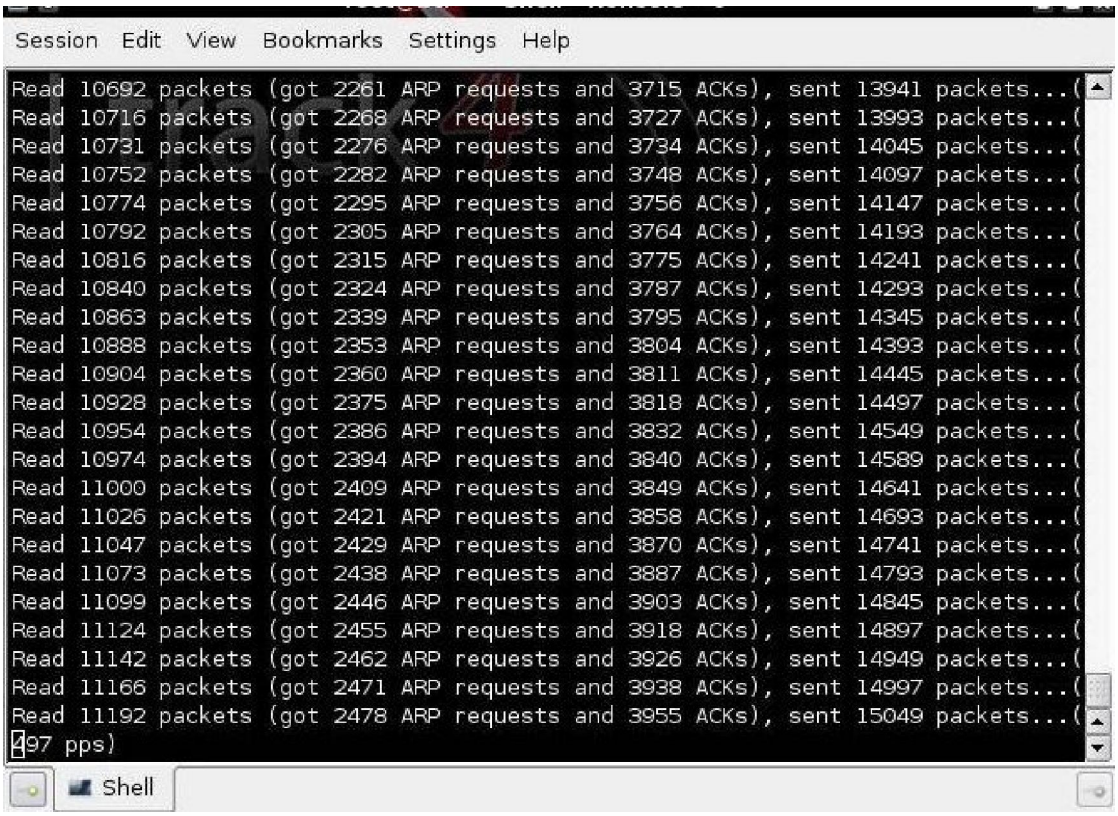
Nyt voimme käynnistää hyökkäyksen jossa ensin kaapataan ARP-viestejä tukiaseman ja clientin väliltä (kuva 24.)[32]. Tämän tapahtuman käynnistymiseen voi mennä jopa muutamia minuutteja, riippuen verkkoliikenteen määrästä tukiaseman ja clientin välillä. Tilannetta voi kuitenkin nopeuttaa suorittamalla toisessa shell:ssä deautentikointi-hyökkäyksen (Deauthetication Attack) tukiasemaan yhdistynyttä clienttiä vastaan[33]. Tällä hyökkäyksellä yhdistynyt client ”potkitaan” hetkeksi pois tukiasemalta, jonka jälkeen se yhdistää itsensä uudestaan tukiasemaan (kuva 25.). Kun ARP-viesti saadaan kaapattua, aletaan sitä syöttää uudelleen verkkoon (kuva 26.). Tämän seurauksena liikenne verkossa kasvaa, jolloin myös kaapattujen IV-pakettien määrä kasvaa huomattavasti nopeammin (kuva 27.).



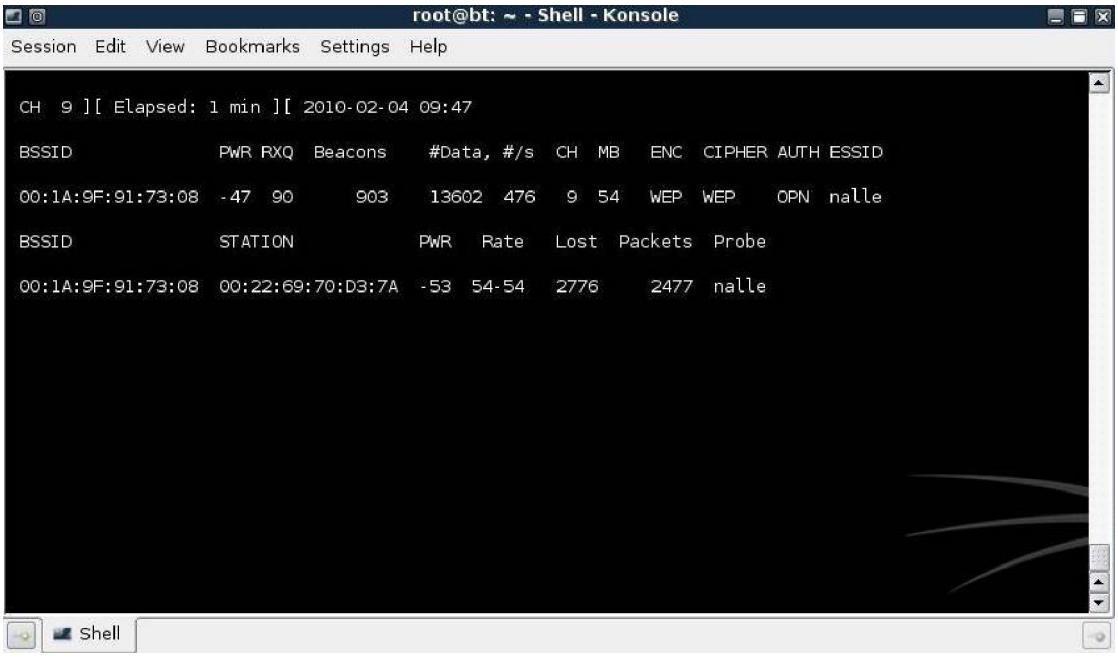
KUVA 24. Käynnistetään ARP-replay hyökkäys



KUVA 25. Aireplay-ng suorittaa deautentikointi-hyökkäystä

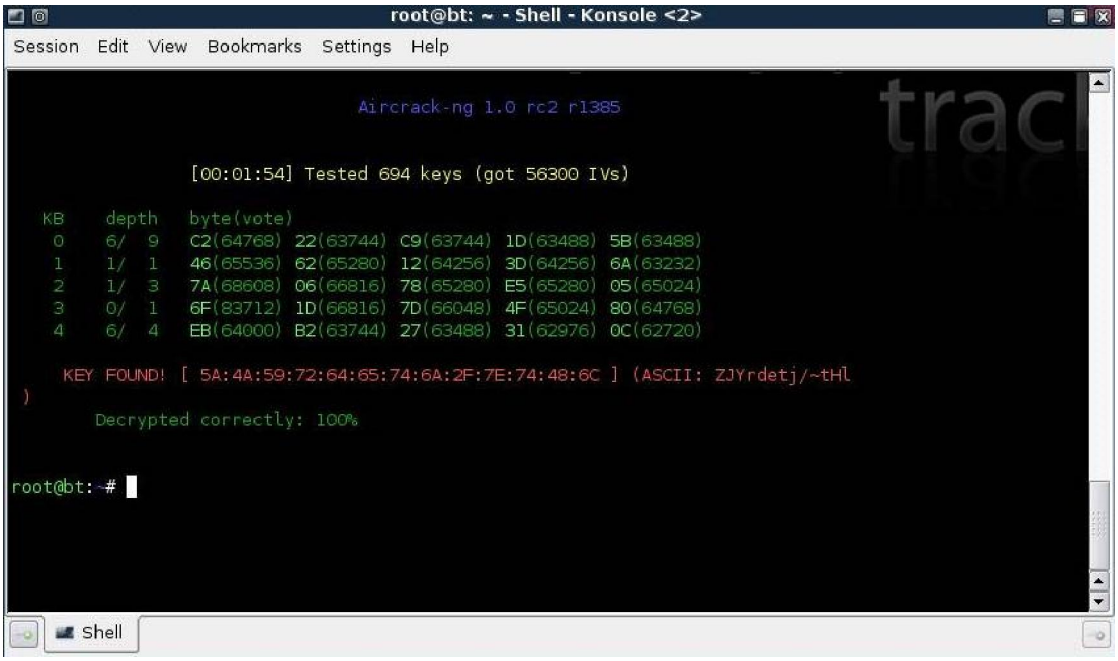


KUVA 26. ARP-viestejä lähetetään verkkoon



KUVA 27. IV-pakettien määrä kasvaa 476 pakettia sekunnissa

Nyt kun kaapattujen IV-pakettien määrä kasvaa jatkuvalla syötöllä, voidaan taustalle käynnistää aircrack-ng ohjelma selvittämään salausavainta[34]. Suorittamalla komento “aircrack-ng -0 -b 00:1A:9F:91:73:08 nalle-01.cap” alkaa aircrack-ng selvittää salausavainta cap-tiedostoon kerättyjen IV-pakettien avulla. Jos kaapattuja IV-paketteja ei ole tarpeeksi avaimen selvittämiseen, jää aircrack-ng odottamaan uutta yritystä kunnes IV-paketteja on kaapattu cap-tiedostoon 5000 kappaletta enemmän. Tätä jatkuu kunnes salausavain saadaan selvitettyä (kuva 28.). Suorittamissani testauksissa salausavain saatiin selville keskimäärin 3-5 minuutin kuluessa pakettien kaappaamisen aloittamisesta.

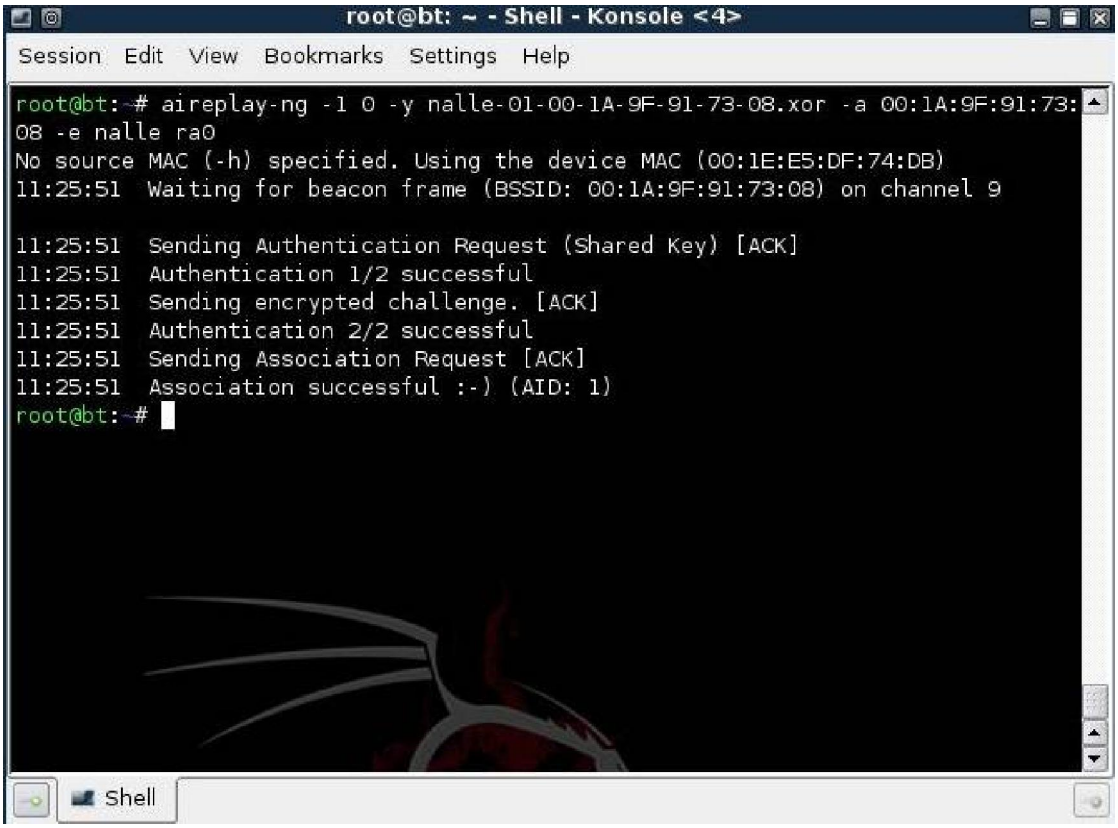


KUVA 28. Aircrack-ng on löytänyt salausavaimen

Ilman pakettisyöttöä, IV-pakettien kaappausnopeuteen vaikuttaa tukiaseman ja clientin välinen datansiirtomäärä. Jos verkossa ei liiku paljon dataa, saadaan IV-paketteja kerättyä harvakseltaan, vain muutamia silloin tällöin. Jo nettisivun avaamisen aiheuttama datansiirto kasvattaa kaappausnopeuden 100-200 paketin sekuntinopeuteen hetkellisesti. Tätä kestää vain siihen asti kunnes nettisivun sisältö on ladattu. Youtube:n käyttämisestä aiheutuva datasiirto antoi keskimäärin 30-70 kaappausnopeuden.

Tästä johtuen hitaasti liikennöivässä verkossa voi mennä aikaa 30 minuutista ylöspäin ennen kuin salausavain saadaan selville.

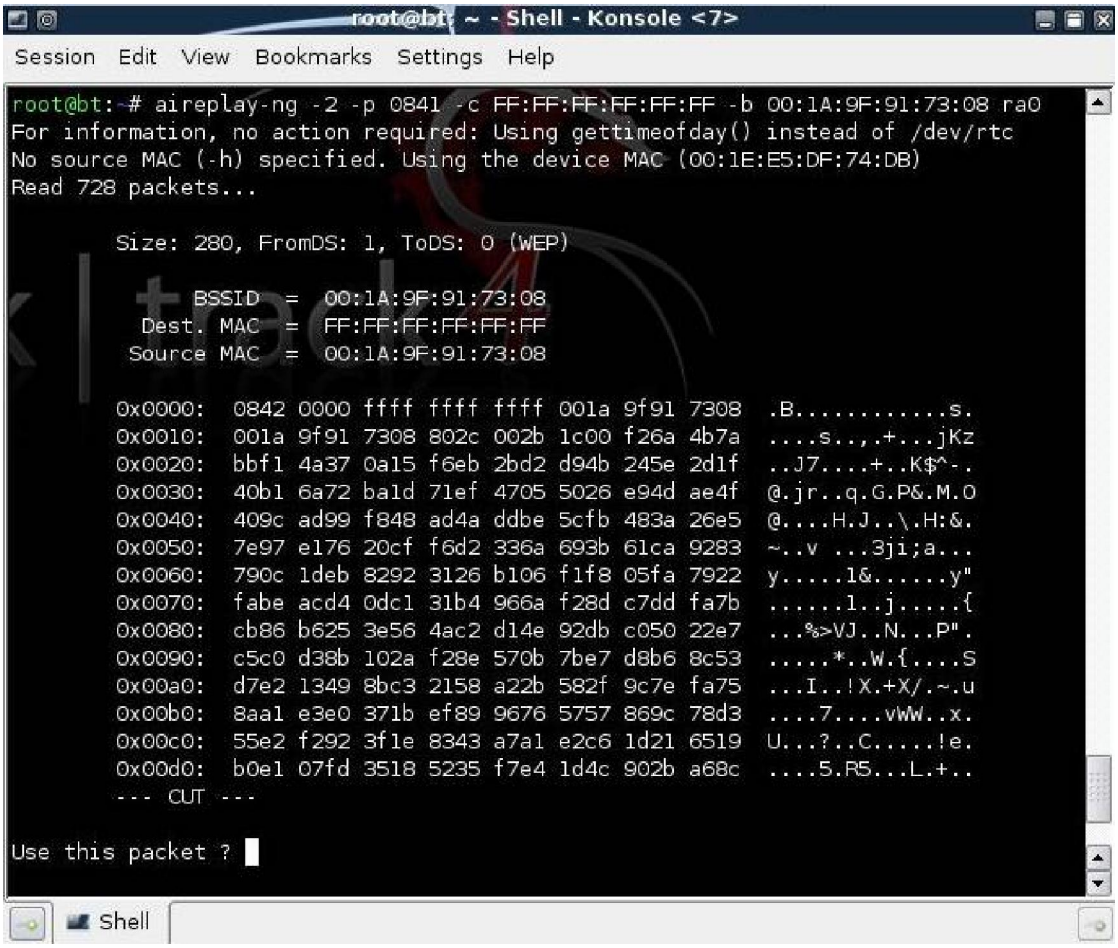
Kun autentikointi on suoritettu jaettu-avain menetelmällä (Shared Key Authentication), tarvitaan yhdistynyt client ja deautentikointi-hyökkäys sitä kohtaan. Tämän tuloksena saadaan xor-tiedosto, jota käytetään vale-autentikointi hyökkäyksessä (kuva 29.). Kun xor-tiedosto on saatu, päästään verkkoon käsiksi vaikka client poistuisi verkosta.



KUVA 29. Fake authentication (Shared Key Authentication) verkkoon

Nyt vuorossa on tilanne, jossa ei ole clienttiä yhdistyneenä, tästä syystä verkossa ei liiku dataa, jotta ARP-hyökkäys saataisiin toimimaan. Nyt joudutaan käyttämään toisenlaista hyökkäystä pakettien syöttämiseen. Tämä on nimeltään interaktiivinen pakettien uudelleensyöttö(Interactive Packet Replay) ja siitä on monta eri versiota (kuva 30.). Osa hyökkäyksistä vaatii vale-autentikoinnin ja osa ei. Minun tapauksessani vale-autentikointi tarvitaan. Koska tukiasema ei hyväksy mitä tahansa pakettia uudelleenlähetettäväksi, joudutaan hyökkäyksessä ottamaan tämä huomioon. Kun Frame Control Field määritellään hyökkäyksen yhteydessä, luulee tukiasema syötettyjen pakettien tulevan oikealta clientiltä. Tämän lisäksi kohde MAC-osoite täytyy muuttaa muotoon FF:FF:FF:FF:FF:FF, jotta tukiasema lähettää pakettia uudelleen ja samalla uuden IV:n. [35.]

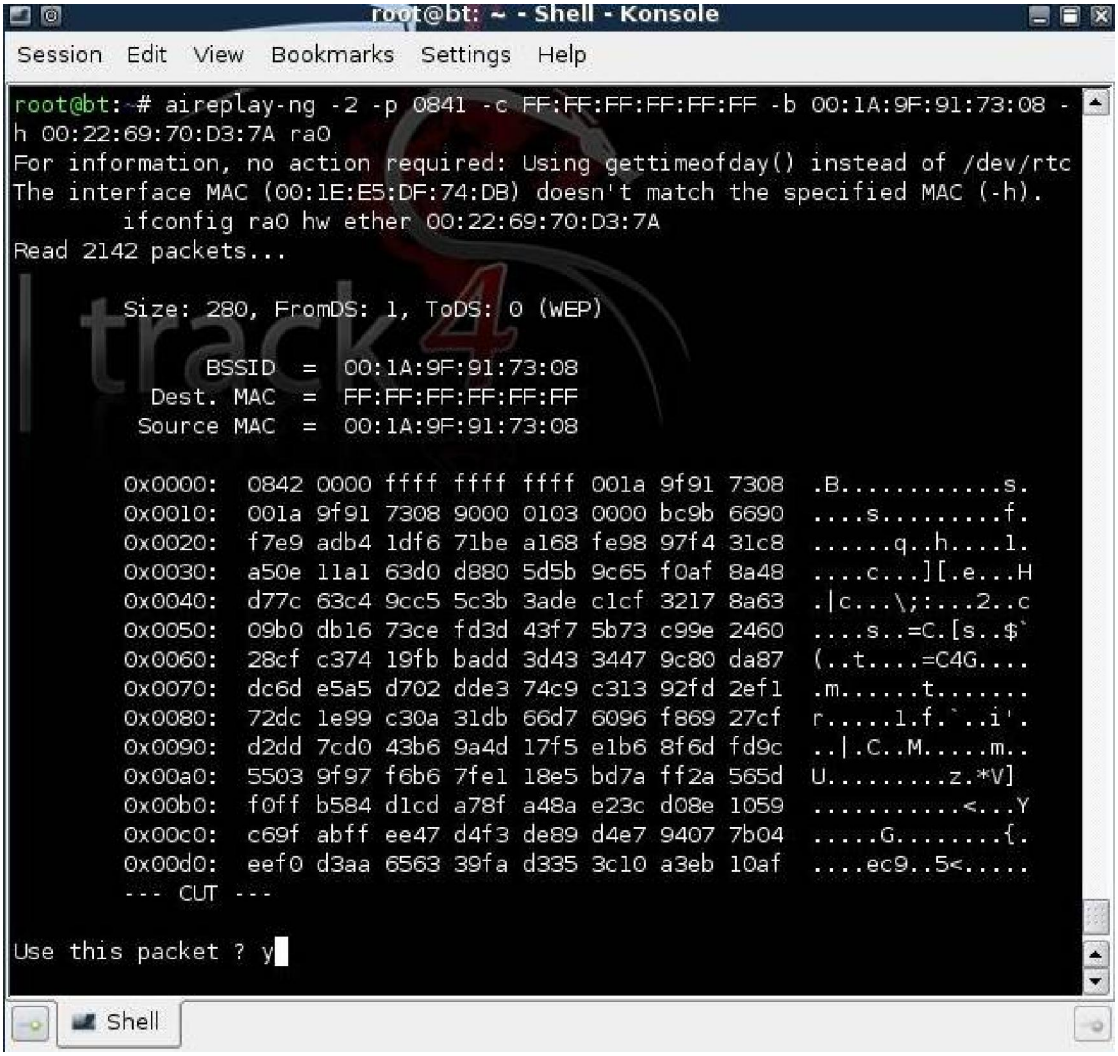
Kuvan 30 hyökkäyksessä on myös mahdollista määrittää kuinka isoja paketteja halutaan käyttää. Etuna on se, että pienillä paketeilla saavutetaan suurempi IV-pakettien kaappausnopeus. Tämä tapahtuu käyttämällä ”-m” ja ”-n” parametreja, joilla määritellään pienimmät - ja suurimmat paketit joita otetaan huomioon. [35.]



KUVA 30. Interactive Packet Replay

Kun tukiasemalle määritetään MAC-suodatus, hyväksyy se vain ennalta määriteltyjen MAC-osoitteiden kommunikoinnin verkossaan. Tällöin joudutaan joko väärentämään oman WLAN-sovittimen MAC-osoite tai syöttämään paketteja aireplay-ng:ssä, tiedossa olevalla clientin MAC-osoitteella.

Omalla WUSB600N-sovittimella MAC-osoitteen vaihtaminen ei onnistu, kyseessä on jokin ajuripohjainen ristiriita. Kun MAC-osoitetta yritetään vaihtaa, sovitin palauttaa aina tehdasasetukset. Tästä syystä ainoaksi vaihtoehdoksi jää autentikoituneen clientin MAC-osoitteen käyttäminen. Tämä lisätään aireplay-ng:n hyökkäykseen ”-h” parametrilla (kuva 31.).



KUVA 31. Interactive Packet Replay MAC-suodatuksen ollessa päällä

Kuvan 9.9 hyökkäysasetuksilla päästiin noin 130 paketin sekuntivauhtiin. Kun paketin koko määriteltiin pienemmäksi, kaapattiin paketteja jo yli 400 sekunnissa.

WEP-salauksen murtamiseen käytetyt menetelmät toimivat kiitettävästi eri salausasetuksilla. Tulosten perusteella voidaan sanoa, että erilaiset paketinsyöttöhyökkäykset tehostavat murtamista ja vähentävät siihen käytettävää aikaa huomattavasti. Sopivan hyökkäysmenetelmän valitsemisessa auttaa perehtyminen eri asetusten ja kokoonpanojen rajoituksiin.

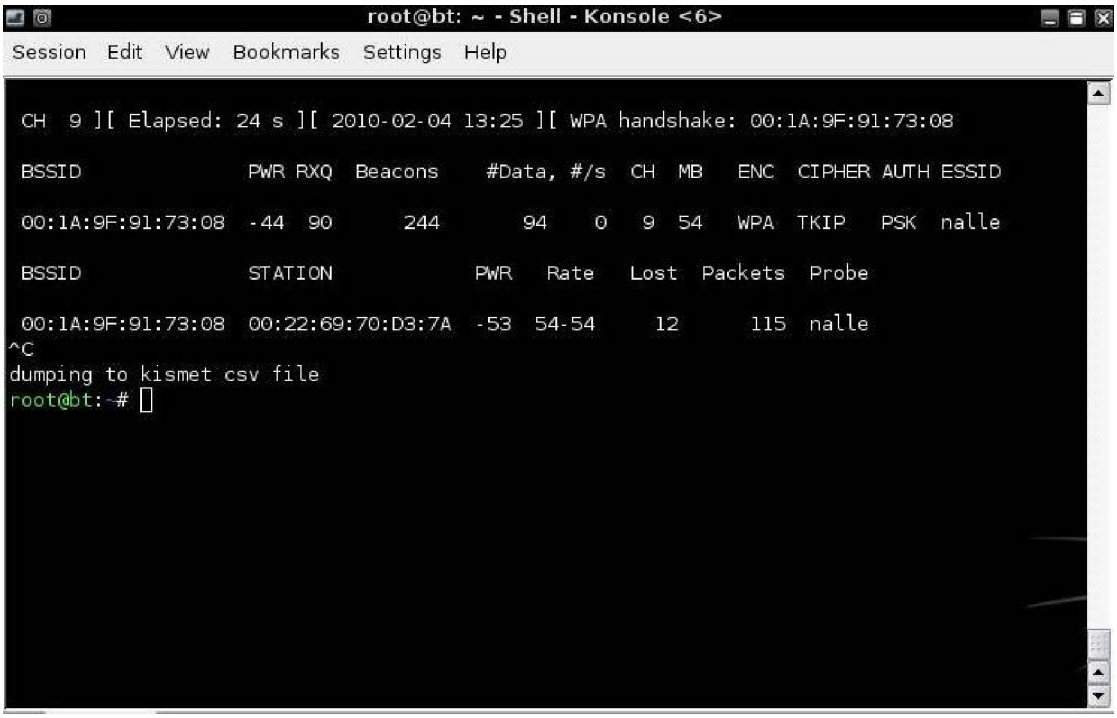
4.2.3 WPA-salauksen murtaminen

WPA-salauksen murtamisessa tarvitaan muutamia tekijöitä, jotta salaus on mahdollista murtaa. Näitä ovat yhdistynyt client ja heikko salasana. Heikolla salasanalla

tarkoitetaan tässä yhteydessä salasanaa, joka voi mahdollisesti löytyä internetistä löytyvistä salasanalistoista.

Kun tukiasemalle yhdistyvä client on luomassa yhteyttä tukiasemaan, käydään näiden välillä nelivaiheinen kättelytapahtuma (4-Way Handshake), jolla tarkistetaan liittyjän oikeellisuus. Salauksen murtamisessa tämän kättelytapahtuman kaappaaminen on ensimmäinen vaihe.
Airodump-ng pystyy kaappaamaan tämän kättelytapahtuman ja tallentamaan sen tiedostoon. Kättelytapahtuman kaappaamiseksi täytyy clientin olla yhdistynyt tukiasemaan tai liittyä verkkoon kun airodump-ng on käynnissä taustalla. Jos airodump-ng käynnistetään clientin liittymisen jälkeen, pitää clienttiä vastaan suorittaa deautentikointihyökkäys jotta kättelytapahtuma tapahtuisi uudelleen ja se saadaan kaapattua (kuva 32.).

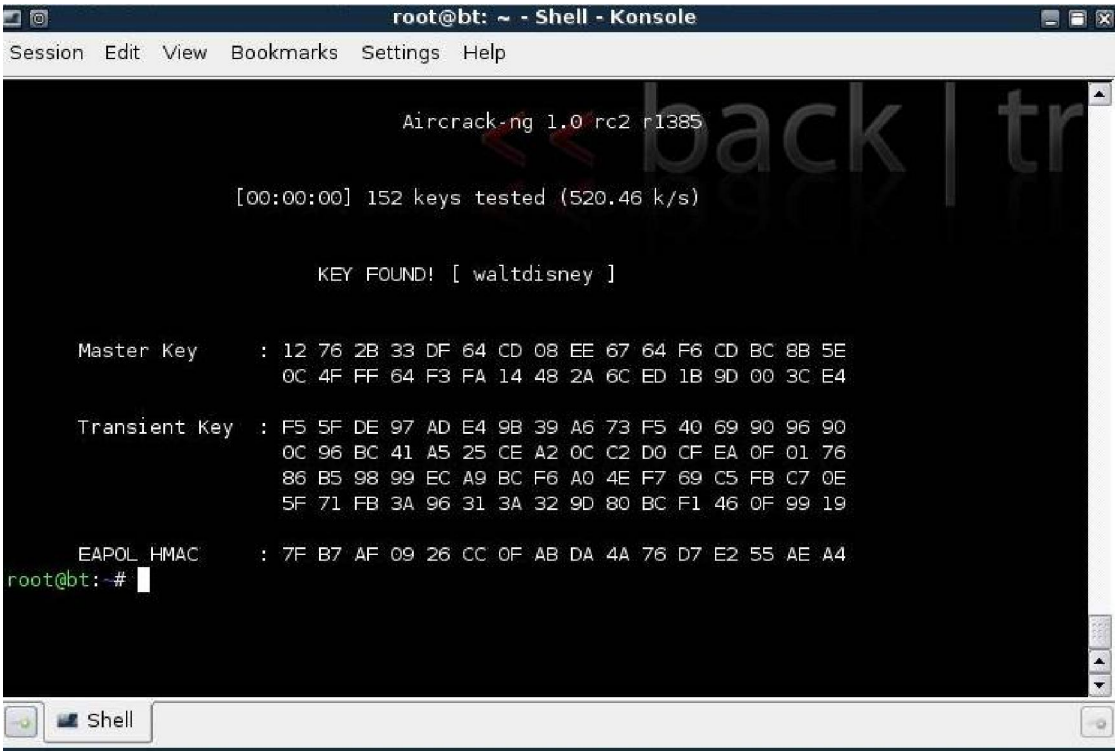
Testasin omalla laitteistollani niin WPA - ja WPA2-salauksia, niin TKIP kuin AES-protokollilla. Kaikilla asetuksilla tulos oli sama ja kättelytapahtuma saatiin kaapattua.



KUVA 32. 4-Way Handshake kaapattu WPA-TKIP verkosta

Airodump-ng tallentaa kättelytapahtuman cap-tiedostoon jota käytetään aircrack-ng:n yhteydessä salasanan selvittämiseksi. Olin tallentanut käytettävän salasanan famous-

nimiseen tekstitiedostoon, joka määritellään aircrack-ng:n salasanalistaksi. Komennolla ”aircrack-ng -0 -w famous.txt -b 00:1A:9F:91:73:08 nalle-01.cap” alkaa selvittää aircrack-ng salasanaa. Jos salasana löytyy listasta, tulee siitä ilmoitus ja aircrack-ng pysähtyy (kuva 33.). Kuvasta käy myös ilmi nopeus, jolla salasanoja käytiin läpi salasanalistasta.



KUVA 33. Aircrack-ng on löytänyt WPA-salasanan

WPA - ja WPA2-salauksia voidaan pitää turvallisina menetelminä WLAN-verkkojen salaamiseen. Vaikka niitä vastaan on olemassa hyökkäysmenetelmä, vaatii tämä onnea, jotta salasana löytyy salasanalistoista. Muodostamalla riittävän vahvan salasanan on tämä hyökkäysmenetelmä hyökkääjälle pelkkää ajanhukkaa. Omissa testitapauksissani salasanalistat olivat kooltaan pieniä ja niiden tarkoitus oli vaan demonstroida kuinka salasana tunnistetaan listasta. Salasanalistoja on kuitenkin saatavissa useiden gigatavujen kokoisina, joten niiden sisältämät salasanamäärät ovat aivan toista luokkaa.

5 JOHTOPÄÄTÖKSET

Työssäni tarkoitus oli tutkia langattoman tiedonsiirron salausmenetelmiä. Halusin myös infoa erilaisista menetelmistä kantomatkan pidentämiseksi langattomissa verkoissa. Päällimmäisenä ajatuksena työtä aloittaessa oli surullisen kuuluisan WEP-salauksen murtoyritykset. Tarkoituksena oli selvittää onko sen murtaminen niin helppoa kuin oli annettu ymmärtää. Lisäksi menetelmät WPA-salauksen murtoon nousivat esiin työn edetessä.

Kantomatkojen osalta tuli selväksi, että kotikonsteinkin tehdyt suuntaavat antennit mahdollistavat yllättävän pitkiä etäisyyksiä. Tästä syystä pitempikään välimatka ei estä hyökkääjää nuuskimasta langattomia verkkoja, kunhan olosuhteet ovat asialliset.

Omien testauksien aloittamisessa suurimmaksi haasteeksi osoittautui vähäinen Linux-kokemukseni. Tiettyjen perusteiden oppimiseen meni paljon aikaa ja monta valvottua yötä. Palaset kuitenkin loksahtivat paikalleen ja sain laitteiston toimimaan lähes odotetulla tavalla. Työssä oli alun perin tarkoitus tutustua myös Windows-ympäristössä tapahtuviin murtoyrityksiin. Tämän osuuden jätin kuitenkin pois, koska Windows-ympäristössä ei ole tarjolla samoja ominaisuuksia ja menetelmiä kuin Linux-ympäristössä.

Hyökkäysten suorittamisessa täytyi hahmottaa, mitä eri toimenpiteitä erilaiset tietoturva-asetukset aiheuttivat hyökkäysten kannalta. Joidenkin hyökkäyksissä olevien ongelmien ratkaisu onnistui vasta useiden epäonnistumisten jälkeen.

Työn kannalta merkittävästä WEP-salauksen turvallisuudesta tein omien testauksien avulla vahvan johtopäätöksen. Tiedot sen heikkouksista osoittautuivat oikeiksi ja pahimmillaan sen murtamiseen tarvitaan vain muutamia minuutteja. Se, mitä tulee hyökkäyksien suorittamisen helppouteen, jää kiinni käyttäjän taidoista - tai oppimishaluista. Kokeneelle Linux-käyttäjälle kynnys on hieman matalampi, jos laitteisto ei toimikkaan automaattisesti.

WPA-salauksien turvallisuudesta voidaan olla asiantuntijoiden kanssa samaa mieltä, käyttämällä riittävän vahvaa salausavainta on salaus käytännössä mahdoton murtaa. Käytännössä tämä tarkoittaa pitkiä, erikoismerkkejä sisältäviä salasanoja, joita ei löydy mistään internetistä löytyvistä salasanalistoista.

Tulevaisuus näyttää, kehitetäänkö näitä nykyisiä salausmenetelmiä vastaan tehokkaampia murtokeinoja vai säilyttävätkö ne asemansa turvallisina salausmenetelminä.

LÄHTEET

[1] Fuller Ron, Blankenship Tim. Building Cisco Wireless Lan. Rockland, MA: Syngress Publishing, Inc.2002

[2] Haanperä Ville, Sinisalo Tiina.2006. Langattomat lähiverkot seminaarityö. Verkkodokumentti. Lappeenrannan teknillinen yliopisto. http://www.it.lut.fi/kurssit/05–06/Ti5316800/seminaarit/WLAN.pdf Päivitetty 1.2.2006. Viitattu 7.3.2010.

[3] Pulkkinen, Jaakko. 2009. WLAN 802.11n-standardin suorituskyky. Metropolia Ammattikorkeakoulu. Verkkodokumentti. https://publications.theseus.fi/bitstream/handle/10024/3700/inssity_45.pdf ?sequence=1 Päivitetty 14.4.2009. Viitattu 7.3.2010.

[4] Cisco Systems, Inc. 802.11n: The Next Generation of Wireless Performance. Verkkodokumentti. Cisco Systems, Inc. http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/ps8382/prod_white_paper0900aecd806b8ce7.html Julkaisuaika tuntematon. Viitattu 7.3.2010.

[5] Thomas, Tom. Verkkojen Tietoturva. Helsinki: Edita. 2005.

[6] Broadband Wireless Exchange, Inc. 802.11g Wireless Internet Access. Verkkodokumentti. Broadband Wireless Exchange, Inc. http://www.bbwexchange.com/wireless_internet_access/802.11g_wireless_internet_access.asp Julkaisuaika tuntematon. Viitattu 7.3.2010.

[7] IPv6.com, Inc. 802.11n Wireless Standard. Verkkodokumentti. IPv6.com, Inc. http://www.ipv6.com/articles/wireless/80211n-Wireless.htm Julkaisuaika tuntematon. Viitattu 7.3.2010.

[8] Juutilainen, Matti. Radiotekniikan perusteet: Signaalit ja antennit. Verkkodokumentti. Lappeenrannan teknillinen yliopisto. http://www2.it.lut.fi/kurssit/06–07/Ti5312600/luentokalvot/luento02.pdf Julkaisuaika tuntematon. Viitattu 7.3.2010.

[9] Juutilainen Matti. Langaton lähiverkko. Verkkodokumentti. Lappeenrannan teknillinen yliopisto. http://www.it.lut.fi/kurssit/04-05/010651000/Luennot/1651_wlan.pdf Julkaisuaika tuntematon. Viitattu 7.3.2010.

[10] TELEX Communications, Inc. Technical Data 2.4GHz WLAN Yagi Antenna. Verkkodokumentti. TELEX Communications, Inc. http://www.wlanantennas.com/datasheets/wlan_antenna_2415.pdf Julkaisuaika kesäkuu 2002. Viitattu 7.3.2010.

[11] TELEX Communications, Inc. Telex Technical Data 2.4GHz WLAN Omnidirectional Antenna. Verkkodokumentti. TELEX Communications, Inc. http://www.wlanantennas.com/datasheets/telex_2439.pdf Julkaisuaika elokuu 2001. Viitattu 7.3.2010.

[12] TELEX Communications, Inc. 9.5 dBi Omni Azimuth Pattern. Verkkodokumentti. TELEX Communications, Inc. http://www.wlanantennas.com/datasheets/telex_2439_azimuth.pdf Julkaisuaika tuntematon. Viitattu 7.3.2010.

[13] TELEX Communications, Inc. Telex Technical Data WLAN / WISP 120 degree Sector Antenna. Verkkodokumentti. TELEX Communications, Inc. http://www.wlanantennas.com/datasheets/telex_sector_2443.pdf Julkaisuaika tammikuu 2003. Viitattu 7.3.2010.

[14] TELEX Communications, Inc. 12 dBi Directional Panel Azimuth Pattern. Verkkodokumentti. TELEX Communications, Inc. http://www.wlanantennas.com/datasheets/telex_2443_azimuth.pdf Julkaisuaika tuntematon. Viitattu 7.3.2010.

[15] TELEX Communications, Inc. Telex Technical Data 2.4GHz WLAN Directional Antenna. Verkkodokumentti. TELEX Communications, Inc. http://www.wlanantennas.com/datasheets/wlan_antenna_2440-24.pdf Julkaisuaika elokuu 2001. Viitattu 7.3.2010.

[16] TELEX Communications, Inc. Telex 2.4 GHz, 20 dBi, 24" Parabolic Dish Antenna Radiation Pattern. Verkkodokumentti. TELEX Communications, Inc. http://www.wlanantennas.com/product_info.php?cPath=21_24&products_id=42 Julkaisuaika tuntematon. Viitattu 7.3.2010.

[17] Palomäki, Martti. Wlan-antenni, Waveguide-tyyppiä. Verkkodokumentti. http://www.saunalahti.fi/elepal/antenni2.html#2B Päivitetty 29.2.2002. Viitattu 7.3.2010.

[18] Julkaisija tuntematon. Ant2_02.jpg. Kuva. http://www.saunalahti.fi/elepal/photos/ant2_02.jpg Julkaisuaika tuntematon. Viitattu 7.3.2010.

[19] RF Peep. 2007. Cantenna, directional antenna with gain. Verkkodokumentti. http://www.aircrack-ng.org/doku.php?id=cantenna_directional_antenna_with_gain Päivitetty 28.1.2007. Viitattu 7.3.2010.

[20] Swan, Stan. 2008. USB adaptors & DIY antenna = "Poor Man's WiFi" ?. Verkkodokumentti. http://www.usbwifi.orconhosting.net.nz/ Päivitetty 29.4.2008. Viitattu 7.3.2010.

[21] usbwifi.orconhosting.net.nz. dutchwif.jpg. Kuva. http://www.usbwifi.orconhosting.net.nz/dutchwif.jpg Julkaisuaika tuntematon. Viitattu 7.3.2010.

[22] Palomäki, Martti. 2001. Wlan-antennien testi. Verkkodokumentti. http://www.saunalahti.fi/elepal/antvert.html Päivitetty 20.9.2001. Viitattu 7.3.2010.

[23] Sankar Krishna, Sundaralingam Sri, Balinsky Andrew, Miller Darrin. Cisco Wireless LAN Security. Indianapolis, IN: Cisco Press. 2005.

[24] Wi-Fi Alliance.2005. Deploying Wi-Fi Protected Access (WPA) and (WPA2) in the Enterprise. Verkkodokumentti. Wi-Fi Alliance. http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf Julkaisuaika maaliskuu 2005. Viitattu 7.3.2010.

[25] BackTrack Linux.2010. Backtrack. Verkkodokumentti. BackTrack Linux. http://www.backtrack-linux.org/ Päivitetty 2010. Viitattu 7.3.2010.

[26] Ralink Technology, Corp. Ralink Corp. | Home. Verkkodokumentti. Ralink Technology, Corp. http://www.ralinktech.com/ Päivitetty 2009. Viitattu 7.3.2010.

[27] Wikipedia, the free encyclopedia. 2010. Monitor Mode. Verkkodokumentti. http://en.wikipedia.org/wiki/Monitor_mode Päivitetty 13.2.2010. Viitattu 7.3.2010.

[28] Darkaudax. 2010. Airmon-ng. Verkkodokumentti. Aircrack-ng.org. http://www.aircrack-ng.org/doku.php?id=airmon-ng/ Päivitetty 19.2.2010. Viitattu 7.3.2010.

[29] Darkaudax. 2010. Aireplay-ng. Verkkodokumentti. Aircrack-ng.org. http://www.aircrack-ng.org/doku.php?id=aireplay-ng/ Päivitetty 3.2.2010. Viitattu 7.3.2010.

[30] Mister_X. 2010. Airodump-ng. Verkkodokumentti. Aircrack-ng.org. http://www.aircrack-ng.org/doku.php?id=airodump-ng/ Päivitetty 7.3.2010. Viitattu 7.3.2010.

[31] Mister_X. 2010. Fake authentication. Verkkodokumentti. Aircrack-ng.org. http://aircrack-ng.org/doku.php?id=fake_authentication Päivitetty 14.3.2010. Viitattu 7.3.2010.

[32] Mister_X. 2010. ARP Request Replay Attack. Verkkodokumentti. Aircrack-ng.org. http://aircrack-ng.org/doku.php?id=arp-request_reinjection/ Päivitetty 6.3.2010. Viitattu 7.3.2010.

[33] Darkaudax. 2009. Deauthentication. Verkkodokumentti. Aircrack-ng.org. http://www.aircrack-ng.org/doku.php?id=deauthentication/ Päivitetty 26.9.2009. Viitattu 7.3.2010.

[34] Mister_X. 2010. Aircrack-ng. Verkkodokumentti. Aircrack-ng.org. http://aircrack-ng.org/doku.php?id=aircrack-ng/ Päivitetty 9.3.2010. Viitattu 7.3.2010.

[35] Mister_X. 2009. Interactive packet replay. Verkkodokumentti. Aircrack-ng.org. http://aircrack-ng.org/doku.php?id=interactive_packet_replay/ Päivitetty 1.6.2009. Viitattu 7.3.2010.