Ilkka Moilanen

IEEE 802.1 (WLAN) -verkkojen tietoturva

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Opinnäytetyö

10.5.2014

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Ilkka Moilanen IEEE 802.11 (WLAN) -verkkojen tietoturva 41 sivua 10.5.2014
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Kari Järvi

Tämän työn tarkoituksena on käydä läpi WLAN/Wi-Fi-verkkojen tietoturvaa ja tarkastella, miten turvallisia ovat avoimet WLAN-verkot tai WEP-, WPA / WPA2 + WPS -suojatut WLAN-verkot. Työssä käydään myös läpi WLAN-verkkojen tuomia uhkia tavalliselle käyttäjälle ja miten tällaisilta uhkilta voidaan suojautua.

Työssä on myös tarkoitus teorian lisäksi toteuttaa osa hyökkäyksistä, jotta saadaan parempi kuva siitä, miten tällaiset hyökkäykset oikeasti toimivat.

WEP-salaus osoittautui odotusten mukaisesti hyvin heikoksi eikä sitä tule käyttää missään olosuhteissa. WPA2-salauksessa ilmeni myös pahoja tietoturvariskejä, joista olisi syytä olla tietoinen. WPA2-salaus on kuitenkin turvallinen, mikäli välttää pahimmat sudenkuopat.

Langattomien verkkojen häiriöalttius on ehkä niiden huomattavin heikkous. Käytännössä yhdellä kannettavalla ja WLAN-kortilla voi estää kaiken langattoman verkkoliikenteen alueella.

Avoimet langattomat verkot osoittautuivat hyvinkin riskialtteiksi ja altistavat ”Man in the middle” -hyökkäykselle.

Avainsanat	IEEE 802.1, Wi-Fi, WLAN, langattomat verkot, tietoturva

Author(s) Title Number of Pages Date	Ilkka Moilanen Security of IEEE 802.11 (WLAN) Networks 41 pages 10 May 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Kari Järvi, Principal Lecturer

The purpose of the thesis was to go through WLAN / Wi-Fi networks security, and view how secure the networks really are. Wireless Network technologies discussed are: Open WLANs, WEP, WPA / WPA2 and WPS-protected WLANs. The thesis also goes through the WLAN threats from the perspective of regular users and teaches how to avoid the most common treats.

Real attacks were also carried out in the study in order to provide a better picture of how they actually function.

WEP-encryption turned out to be very weak, as expected, and should not be used under any circumstances. WPA2-encryption also revealed severe security risks that one would need to be aware of. WPA2-encryption is safe if the worst pitfalls are avoided.

The vulnerability of wireless networks is perhaps the most significant weakness. In practice, one laptop and the WLAN-card can block all wireless network traffic in the area.

Open wireless networks turned out to be very risky and vulnerable to "man in the middle" attacks.

Keywords	IEEE 802.1, Wi-Fi, WLAN, wireless networks, security

Sisällys

Lyhenteet

3G	Third generation on yleisnimitys kolmannen sukupolven matkapuhelintekniikoille.
4G	Fourth generation on yleisnimitys neljännen sukupolven matkapuhelintekniikoille.
ARP	Address Resolution Protocol on protokolla, jolla Ethernet-verkoissa selvitetään IP-osoitetta vastaava MAC-osoite.
AES	Advanced Encryption Standard on vahva lohkosalausmenetelmä.
ADSL	Asymmetric Digital Subscriber Line on verkkokytkintekniikka, jolla on mahdollista siirtää dataa tavallista puhelinlinjaa käyttäen.
DNS	Domain Name System on Internetin nimipalvelujärjestelmä.
Edge	Enhanced Data rates for GSM Evolution on matkapuhelinten pakettikytkentäiseen tiedonsiirtoon suunniteltu tekniikka.
HiperLAN	High Performance Radio Local Area Networks on nopea langaton lähiverkko.
HTTP	Hypertext Transfer Protocol on protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
HTTPS	Hypertext Transfer Protocol Secure on HTTP-protokollan ja SSL/TLS-protokollan yhdistelmä, jota käytetään tiedon suojattuun siirtoon.
IEEE	Institute of Electrical and Electronics Engineers (IEEE) on kansainvälinen tekniikan alan järjestö.
IV	Initialization Vector, alustusvektori on mielivaltainen binääriluku, jota voidaan käyttää salaisen avaimen kanssa tiedon salaamiseen.
MAC	Media Access Control on IEEE 802 -verkoissa verkon varaamisen ja itse liikennöinnin hoitava osajärjestelmä.
MIC	Message Integrity Check estää väärennettyjen pakettien hyväksynnän.
MS-CHAPv2	Microsoft Challenge-Handshake Authentication Protocol version 2 on todennusmenetelmä, joka tukee salasanaan perustuvaa käyttäjä- tai tietokonetodennusta.
PIN	Personal Identification Number on salasanana käytettävä luku, jolla voidaan tunnistautua järjestelmään.
PPTP	Point-to-Point Tunneling Protocol on VPN-tunnelointiprotokolla.
RC4	Ron's Code 4, tunnetaan myös nimellä Rivest Cipher 4, on symmetrinen jonosalaaja.

SSID	Service Set Identifier on langattoman lähiverkon verkkotunnus.
SSL	Secure Sockets Layer on salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.
TKIP	Temporal Key Integrity Protocol on langattomien lähiverkkojen tietoturvaprotokolla.
WLAN	Wireless Local Area Network on langaton lähiverkkotekniikka, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita.
Wi-Fi	Wireless Fidelity, Wi-Fi Alliancen tavaramerkki.
WEP	Wired Equivalent Privacy on ensimäinen langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä.
WPA	Wifi Protected Access on välivaiheen tietoturvatekniikka.
WPA2	Wifi Protected Access 2, tunnetaan myös nimellä IEEE 802.11i, on langattomien 802.11-verkkojen viimeisin tietoturvastandardi.
WPS	Wi-Fi Protected Setup on tekniikka, jonka tarkoituksena on helpottaa laitteiden liittämistä salattuihin langattomiin verkkoihin.
VPN	Virtual Private Network muodostaa yksityisen verkon julkisen verkon yli.

1 Johdanto

Tässä työssä käydään läpi Wi-Fi:n tai kansankielessä paremmin tunnetun WLAN-verkkojen tietoturvaa. Tarkoituksena on käydä läpi WLAN-verkkojen suojautumismenetelmiä kuten WEP- ja WPA/WPA2 -kryptauksia ja niihin kohdistuvia yleisimpiä hyökkäyksiä. Tarkoituksena on tuoda esiin eri suojausten mahdolliset heikkoudet ja menetelmät, joita käytetään näiden suojausten murtamiseen. Tämä antaa paremman ymmärryksen hyökkäyksistä ja antaa hyvän tietämyksen suojautua näiltä hyökkäyksiltä. Lopputuloksena pitäisi olla hyvä ymmärrys WLAN-verkkojen vahvuuksista ja heikkouksista.

Työssä käydään läpi myös asiakaspuolen hyökkäyksiä. Kun suurin osa WLAN-verkoista on rakennettu turvallisiksi, on suurin osa hyökkäyksistä vaihtanut kohdettaan verkossa vieraileviin asiakkaisiin. Tässä työssä on tarkoitus kartoittaa näitä hyökkäyksiä, jotta voidaan paremmin välttyä ja suojautua niiltä. Lopputuloksena pitäisi siis olla hyvä yleisymmärrys WLAN-verkkojen tietoturvasta ja erinäisistä riskeistä esimerkiksi avoimissa verkoissa.

2 Laitteistot ja ohjelmistot

Tässä työssä jouduttiin rakentamaan pieni laboratorioympäristö, jotta voitiin turvallisesti ja laillisesti testata erilaisia hyökkäysmenetelmiä omia laitteita ja verkossa olevia tietokoneita kohtaan. Laboratorioympäristön luomisella pyrittiin siihen, ettei vahingossa murrettaisi naapurin WLAN-yhteyttä tai aiheutettaisi muuta harmia. Laboratorioympäristön rakentaminen toi pieniä haasteita. Työssä käytettiin myös kannettavaa tietokonetta, johon oli asennettuna Windows 7 ja Kali Linux. Samoin käytettiin myös pöytätietokonetta, jossa Windows 7 -käyttöjärjestelmässä pyörii WMwaren alaisuudessa virtuaalinen Kali Linux. Kali Linuxin kanssa käytettiin myös USB-WLAN-modeemia TL-WN722N.

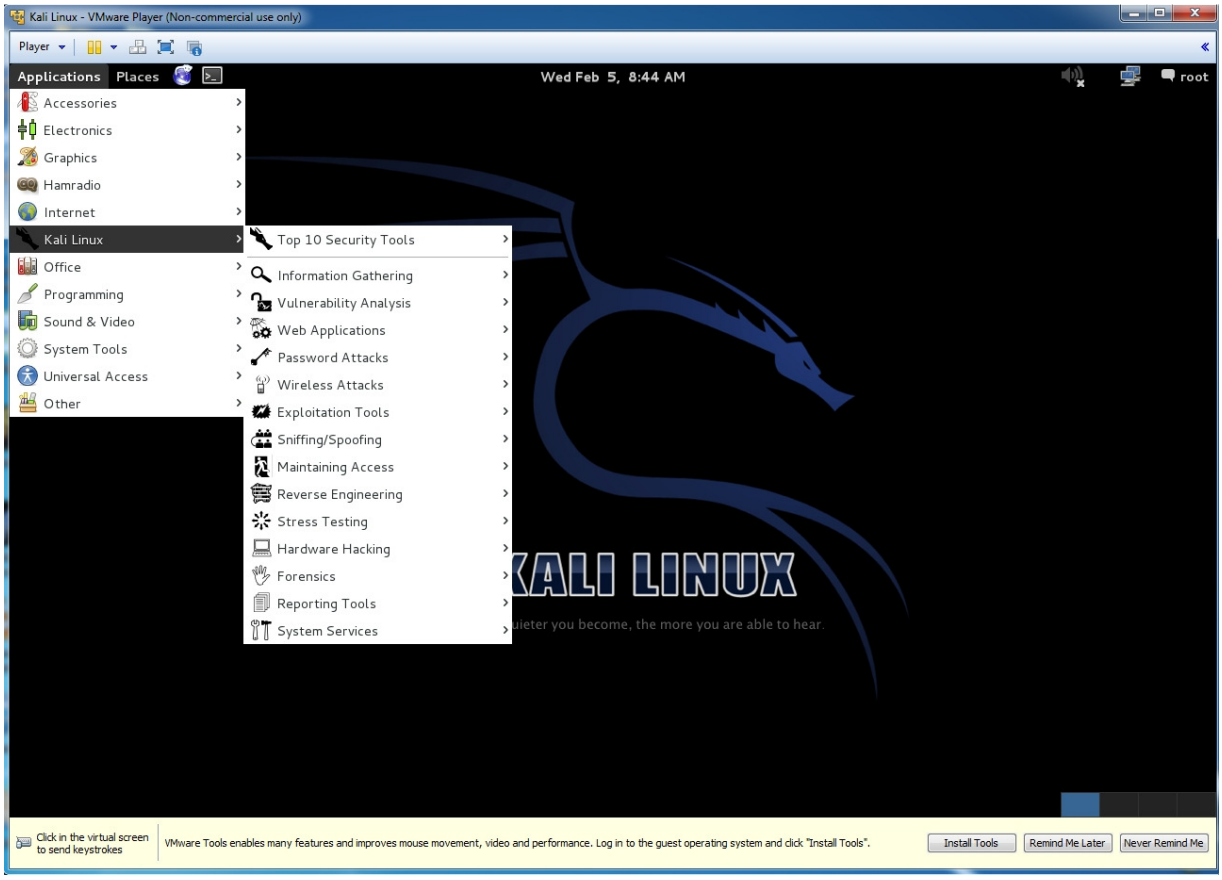
Tukiasemana ja reitittimenä laboratorioverkossa toimi D-Linkin Dir-655-reititin. Tarkoituksena oli käyttää tätä reititintä ja testata sitä vastaan erinäisiä hyökkäyksiä, kuten murtaa WEP- ja WPA + WPS -salaukset. Tällä hetkellä reitittimessä on 1.21 firmware, mikä on hiukan vanha, mutta ajaa asiansa demonstraatiossa paremmin.

2.1 Kali Linux

Kali Linux on käyttöjärjestelmä, joka on tehty suoraan penetraatiotestaukseen ja erinäisten haavoittuvuuksien löytämiseen. Kali Linux sisältää yli 300 erilaista työkalua, joilla voidaan testata tai murtaa verkkojen, palvelimien, tietokantojen, tietokoneiden jne. tietoturvaa. Kali Linuxia käyttääkin moni tietoturvallisuuden ammattilainen, koska se on kätevä työkalu juuri siihen, mihin se on suunniteltu eli tietoturva-aukkojen löytämiseen.

Tässä työssä ei perehdytä itse Kali Linuxin asennukseen, mutta myöhemmin tullaan käymään läpi jotain komentoja, jotka liittyvät itse hyökkäykseen tai langattoman verkon murtamiseen.

Kali Linuxin aikaisempi versio tunnettiin nimellä Back Track, ja se oli Ubuntu-pohjainen. Back Trackin tekijät päättivät kuitenkin uudistaa käyttöjärjestelmän kokonaan, ja näin syntyi Debian-pohjainen Kali Linux.



Kuva 1. Kali Linux.

2.2 Pineapple Mark V

Pineapple Mark V on pieni tukiasema, joka on alusta asti suunniteltu penetraatiotestaukseen. Laitetta käyttävät tietoturva-ammattilaiset, lainvalvojat, armeija ja hallituksen eri osastot. Laitteella on helppo havainnollistaa erinäisiä haavoittuvuuksia, kuten esimerkiksi ”Man in the middle” -hyökkäystä. [1.]

Pineapple Mark V on rakennettu siten, että sitä voidaan hallinnoida verkkosivujen kautta, joten laite itsessään ei tarvitse mitään ulkopuolisia asennuksia, vaan se toimii niin Windowsissa kuin Linuxissakin. Pineapple sisältää kaksi erillistä WLAN-verkkokorttia, jolloin laitteesta voi tehdä samaan aikaan tukiaseman sekä yhdistää sen toiseen tukiasemaan. Tämä mahdollistaa niin sanotut honeypot (hunajapurkki) -viritykset. Laite sisältää erinäisiä ohjelmia kuten ”*aircrack-ng, dsniff, easy-creds, ettercap, hping3, httptunnel, karma, kismet, macchanger, mdk3, ngrep, nmap, nodogsplash captive portal, privoxy, ptunnel, snort, sslsniff, sslstrip, ssltunnel, stunnel, tcpdump, tor, and reaver*.” [1.]

Laitteen tarkemmat tiedot:

- CPU: 400 MHz MIPS Atheros AR9331 SoC.
- Memory: 16 MB ROM, 64 MB DDR2 RAM
- Disk: Micro SD support up to 32 GB, FAT or EXT, 2 GB Included
- Mode Select: 5 DIP Switches - 2 System, 3 User configurable
- Wireless: Atheros AR9331 IEEE 802.11 b/g/n + Realtek RTL8187 IEEE 802.11 b/g
- Ports: (2) SMA Antenna, 10/100 Ethernet, USB 2.0, Micro SD, TTL Serial, Expansion Bus
- Power: DC in Variable 5-12v, ~1A, 5.5mm*2.1mm connector, International Power Supply
- Status Indicators: Power LED, Ethernet LED, Wireless 1 LED, Wireless 2 LED

Kuva 2. Pineapple Mark V. [1.]

3 Langattomat verkot

Langattomat verkot koostuvat joko yksityisistä verkoista, julkisista verkoista tai näiden välimuodoista kuten julkisista suljetuista langattomista verkoista. Langattomia verkkotyyppejä on paljon erilaisia kuten WLAN, 3G, 4G, Edge jne. Tässä työssä kuitenkin keskitytään pääosin WLAN-ratkaisuihin. WLAN on tällä hetkellä yleisin langaton verkkotyyppi, kun puhutaan julkisista avoimista verkoista. [2.]

Suljettu langaton verkko on yleensä verkko, joka on rajoitettu jollekin tietylle käyttäjäkunnalle. Tällaisen langattoman verkon voi löytää esim. hotellista, joka tarjoaa asiakkailleen mahdollisuuden käyttää langatonta verkkoa. [2.]

Avoimet langattomat verkot taas ovat vapaita kaikille ja niihin voi liittyä kuka tahansa alueella oleva. Tällaisia verkkoja voi löytää esimerkiksi internetkahviloista tai kirjastoista. Nämä verkot ovat yleisesti kaikkein turvattomimpia, koska verkkoon voi liittyä kuka tahansa, mikä on riski jo itsessään. Lisäksi avoimeen verkkoon liittyessä ei voi olla koskaan varma, että mihin on liittynyt. Tästä kerrotaan lisää luvussa 7. [2.]

3.1 IEEE 802.11

IEEE 802.11 on standardi, joka määrittää linkkikerroksen langatonta protokollaa ja sitä hallinnoi Institute of Electricial and Electronics Engineers (IEEE). Yleisesti myös mielletään 802.11 ja Wi-Fi samaksi asiaksi, vaikka ne eivät olekaan aivan samoja. Wi-Fi on 802.11-standardin osajoukko, jota hallinnoi Wi-Fi Alliance. Wi-Fi Alliance tehtiin siitä syystä, että IEEE 802.11 -standardi oli hyvin monimutkainen ja sen päivitettävyydestä vastasi komitea, joten se ei ollut kovin joustava vaihtoehto. [3.]

WiFi Alliancen tehtävä onkin vastata Wi-Fi-logoilla varustettujen laitteiden yhteensopivuudesta. WiFi Alliance myös mahdollistaa sen, että laitevalmistajat voivat tuoda laitteisiinsa ominaisuuksia, joita ei ole vielä vahvistettu IEEE:n toimesta. Tunnetuin näistä esimerkeistä on WPS (Wi-Fi protect access) -toiminto. [3.]

Ensimmäinen IEEE 802.11 -standardi julkaistiin vuonna 1997. Se oli nopeudeltaan vain 1 - 2 megabittiä sekunnissa (mikä todettiin nopeasti riittämättömäksi), joten sen syrjäytti nopeasti (kaksi vuotta myöhemmin) IEEE 802.11b, jonka nimellinen nopeus oli 11 megabittiä sekunnissa. Vuonna 1999 julkaistiin myös 802.11a, joka mahdollisti jopa 54 megabitin vauhdin. Tämä tekniikka käytti suurempaa taajuutta 5 GHz (vanhan 2,4 GHz:n sijasta). 802.11a jäi kuitenkin 802.11b:n jalkoihin, koska sen vaatima tekniikka oli kallista. Lisäksi korkeampi taajuus pienensi toiminta-aluetta. 802.11a ei myöskään ollut yhteensopiva 802.11b:n kanssa. [3.]

Vuonna 2003 julkaistiin 802.11g, joka yhdisti 802.11a:n ja 802.11b:n tekniikat. Se toimi myös 2, 4 GHz:n taajuudella ja oli yhteensopiva myös 802.11b:n kanssa. 802.11g onkin sittemmin syrjäyttänyt 802.11b:n. [3.]

Lisäominaisuuksien standardeina on tällä hetkellä 802.11e, 802.11f, 802.11d, 802.11h, 802.11i, 802.11s ja 802.11n. Näihin standardeihin en tässä työssä syvenny tarkemmin. [4.]

3.2 WLAN

> ”WLAN (lyhenne sanoista wireless local area network) on langaton lähiverkkotekniikka, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita. Useimmiten WLAN-termiä käytetään tarkoittamaan IEEE 802.11 -standardia, mutta myös ETSI:n HiperLAN-standardi on langaton lähiverkko. HiperLAN-standardin eri versiot eivät kuitenkaan ole yleistyneet, joten yleisessä kielenkäytössä termeillä WLAN, 802.11 ja Wi-Fi tarkoitetaan samaa asiaa, vaikka tarkkaan ottaen nämä termit eivät olekaan synonyymejä.” [5.]

WLAN:in käyttötarkoituksia ovat esimerkiksi langallisen internetyhteyden verkottaminen langattomaksi. Näin voidaan langallinen internetyhteys helposti jakaa suuremmalle alueelle ja useammalle laitteelle. Usein julkiset langattomat verkot ovat tällaisia. WLAN:ia voidaan myös käyttää langattoman sisäverkon luomiseen, joten aina ei kyse ole langallisen internetyhteyden verkottamisesta. [5.]

3.3 WLAN-verkon turvallisuus

Yksityinen suojattu WPA2 WLAN -verkko vahvalla salasanalla on turvallinen ratkaisu. Tällaista ratkaisua ei kuitenkaan aina ole saatavilla. Julkisen WLAN-verkon turvallisuudesta ei koskaan ole takeita. WLAN-verkon turvallisuus voidaan nähdä kahdesta suunnasta. Julkisen avoimen verkon omistaja voi joutua hankaluuksiin, jos joku verkonkäyttäjä käyttää verkkoa rikolliseen toimintaan. Tällöin verkon omistaja on ensimmäinen, jota aletaan rikoksesta epäillä. Toisesta suunnasta katsottuna taas julkinen verkko voi olla uhka siihen liittyneelle. Koskaan ei voi tietää kuka verkkoa salakuuntelee ja usein on vaikea edes tunnistaa, onko liittynyt oikeaan verkkoon. Verkon SSID-tunnus on kenen tahansa muokattavissa, joten jos verkon nimi on Starbucks, ei se vielä kerro, että kyseessä olisi oikeasti Starbucksin ilmainen verkko. [6.]

> ”On huomattava, että avoimeen WLAN-verkkoon voi kytkeytyä kuka tahansa ja että yhteyden kautta siirrettävä tietoliikenne on helposti kenen tahansa sivullisen kuunneltavissa ja tallennettavissa, jos käytettävät sovellukset eivät salakirjoita liikennettä. Avoin WLAN-yhteys ei siis tarjoa itse suojaa, mutta tietoliikenteen salakuuntelulta voi välttyä esimerkiksi käyttämällä vain sellaisia www-palveluja, jotka tarjoavat SSL-suojatun yhteyden.” [6.]

Avoimia langattomia verkkoja tulisi välttää aina. Valitettavasti se ei ole aina mahdollista ja siksi onkin tärkeää tietää vaaroista paremmin. SSL-suojatut verkkosivut estävät salakuuntelun, mutta vain jos käyttäjä itse kirjoittaa https:// -komennon kokonaisuudessaan osoiteriville. ”Man in the middle” -hyökkäyksissä hyökkääjä voi estää sslstrip-ohjelmalla sivun ohjautumisen ssl-suojatuksi. Jotkut sivustot eivät toimi ilman ssl-suojausta, mutta näissä tapauksissa hyökkääjä on muodostanut ssl-suojatun yhteyden sivustolle ja välittää uhrille suojaamattoman version. Tällöin uhrin ja hyökkääjän välinen yhteys on salaamaton. Mikäli aikoo käyttää avoimia langattomia verkkoja, on syytä aina käyttää myös VPN-tunnelointia.

4 WEP

WEP (Wired Equivalent Privacy) oli ensimmäinen 802.11-standardin langaton salausmenetelmä, jonka tarkoitus oli estää langattoman verkon salakuuntelu ja luvaton käyttö. WEP julkaistiin vuonna 1997 ja se oli liitetty 802.11b-standardiin. Tuohon aikaan Yhdysvalloissa oli kuitenkin paljon vientirajoitteita vahvoja kryptauksia kohtaan, mistä johtuen WEP luotiin käyttämään vain 40-bittistä avainta. Myöhemmin uusimpien standardien myötä avaimen kokoa on saatu kasvatetetuksi 64–128 bittiseksi. WEP-salaus kuitenkin todettiin myöhemmin riittämättömäksi ja nykypäivänä se on täysin turvaton ja sen murtamisessa ei mene kuin 5 minuuttia. [7.]

> ”WEP käyttää RSA Securityn RC4-salausalgoritmia, jonka toiminnassa on havaittu puutteita. WEP-salauksen haittana ovat myös lyhyet alustusvektorit (IV, Initialization Vector), jotka lähetetään salaamattomina jokaisen kehyksen parissa ensimmäisessä bitissä. Tietoliikennettä kuuntelemalla sekä siirrettävää dataa ja samankaltaisia alustusvektoreita seuraamalla voidaan laskea salattu avain eli murtaa verkon salaus. Siirrettävät datamäärät langattomassa verkossa vaikuttavat siihen, kuinka helposti ja nopeasti avain on murrettavissa.” [7.]

WEP-salauksen heikkoutena on siis RC4, jonka kanssa ei saisi koskaan käyttää identtisiä avaimia. IV kuitenkin käyttää vain 24 bittiä pitkiä avaimia, jolloin se jossain vaiheessa toistaa itseään antaen hyökkääjälle useamman paketin samalla IV:llä. Mikäli verkko on todella aktiivinen, niin tällainen tapahtuma saattoi tapahtua 5000 paketin jälkeen. Tämän myötä alkoi ilmestyä erilaisia työkaluja, joiden tarkoitus oli murtaa WEP-salaus. Ensimmäiset työkalut (Airsnort) vaativat 5–10 miljoonaa pakettia, jolloin hiljaisemman verkon murtamisessa kesti päiviä. Myöhemmin julkaistiin alkuperäinen Aircrack, joka vaati vain 200 000–500 000 pakettia 40–64-bittisellä salauksella ja miljoona pakettia 128-bittisellä salauksella. [8.]

Työkalujen kehityttyä IV:n tietoja pystyttiin tutkimaan entistä nopeammin ja tehokkaammin. Myös hyökkäystä saatiin lyhennetyksi ”ARP Replay” -hyökkäyksen ansiosta. ”ARP Replay attack” on metodi, jossa kryptattu ARP-paketti lähetetään takaisin tukiasemalle (kryptatun ARP-paketin tunnistaa sen uniikista koosta), joka vastaavasti lähettää uuden ARP-paketin uudella IV:llä. Tätä toistamalla saadaan nopeasti paljon IV:tä, joista osa on duplikaatteja tietyn ajan päästä. Tällä metodilla saatiin aikaisemmin tunteja ja jopa päiviä kestävä murto tehtyä jopa 10 minuutissa. [8.]

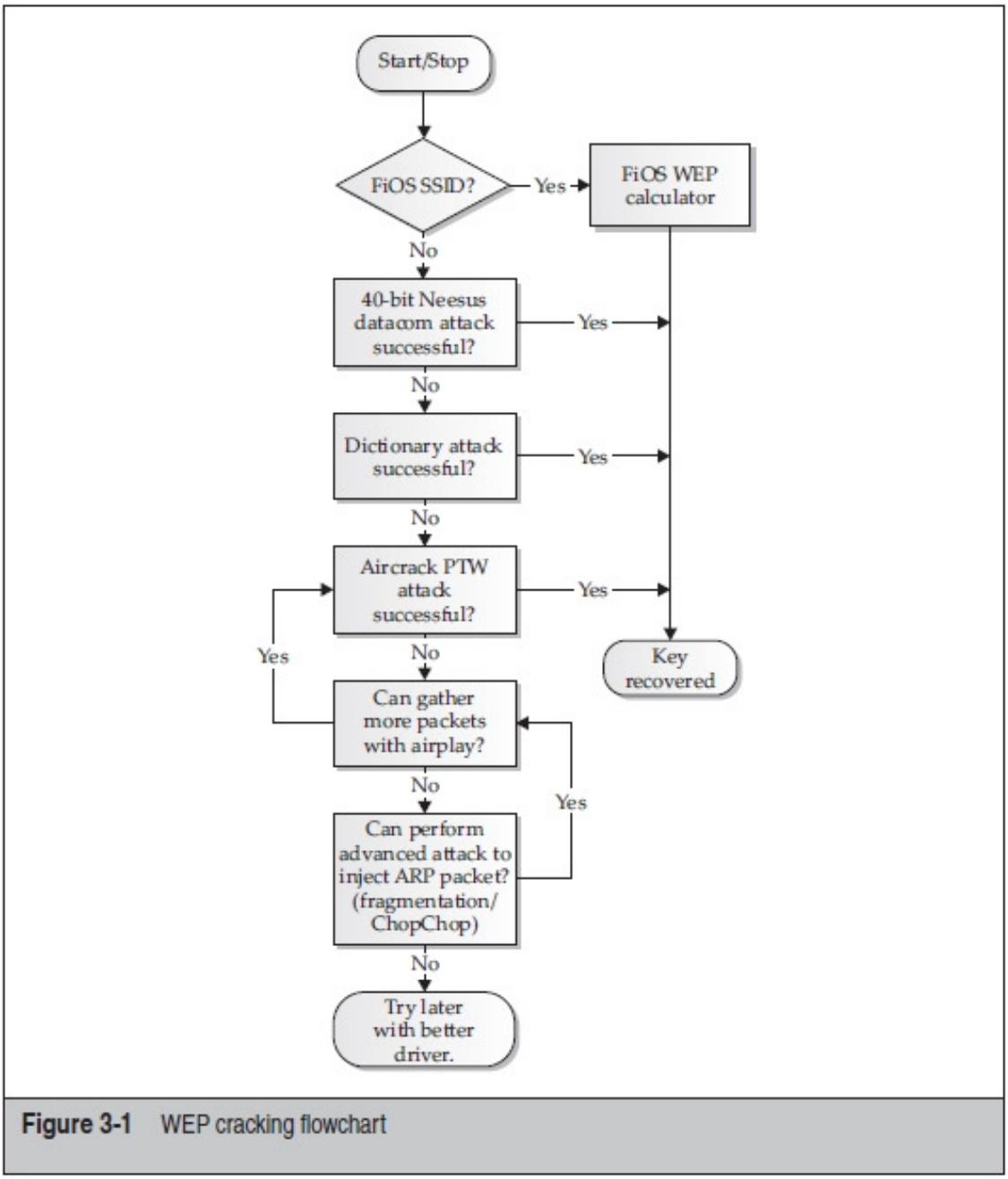
Lopullinen WEP-suojauksen tappaja oli Psychkine-Tews-Weinmann (PTW) -hyökkäys, joka tarvitsi ainoastaan 20 000 – 50 000 pakettia toimiakseen. Tämä yhdistettynä ARP-replay -hyökkäykseen lyhensi hyökkäyksen keston yhteen minuuttiin. Tämän myötä WEP-salausta ei voi enää edes kutsua salaukseksi. [8.]

WEP-salauksen riittämättömyyden tullessa ilmi IEEE julkaisi WPA-salauksen ja se onkin pikkuhiljaa syrjäyttänyt WEP:n. [8.]

> ”WEP (engl. Wired Equivalent Privacy) on IEEE:n 802.11-standardin ensimmäinen työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä. WEP-salauksen on tarkoitus suojata langatonta verkkoa salakuuntelulta ja estää valtuuttamattomilta käyttäjiltä pääsy verkkoon.
>
> WEP luottaa salaiseen avaimeen, josta alun perin tehtiin Yhdysvaltain tiukkojen salakirjoitukseen liittyvien vientimääräysten vuoksi vain 40-bittinen. Myöhemmin kehitettyjen 802.11b- ja 802.11g-suositusten myötä voidaan käyttää myös 64- tai 128-bittistä salaista avainta. Salainen avain hoitaa lähetettävien pakettien kryptaamisen ja pyrkii takaamaan siirrettävän tiedon eheyden” [7.]

4.1 WEP-salauksen murtaminen

Seuraavaksi tarkastellaan vähän tarkemmin, miten WEP-salaus käytännössä murtuu. Alla olevasta vuokaaviosta käy nopeasti ilmi prosessin kulku.



Kuva 3. WEP-salauksen murtamisen vuokaavio. [3]

FiOS SSID on helpoin tapa murtaa WEP-salaus. Valitettavasti se kuitenkin toimii vain FiOS-reittittimien kanssa, joita oli saatavilla Verizonin toimesta osassa Yhdysvaltojen osavaltioista. Käytännössä reitittimen WEP-avain oli sidoksissa reitittimen SSID:hen, jonka vuoksi WEP-avaimen selvittäminen kävi helpolla laskukaavalla. [3.]

4.2 Neesus Datacom attack

Neesus Datacom teki yhden ensimmäisistä algoritmeistä, jota käytettiin WEP-salauksessa. Neesus Datacom -algoritmi on paremmin tunnettu sitä vastaan tehdystä hyökkäyksestä, joka tunnettaan nimellä Newsham 21bit attack, joka sai nimensä sen löytäjän Tim Newshamin mukaan. Hyökkäys tuli kuuluisaksi, koska sen avulla pystyttiin pienentämään 40-bittinen avain vain 21-bittiseksi. Tämä taas mahdollisti erittäin nopean murtotavan. Neesus Datacom -algoritmissa on myös muita heikkouksia kuten se, että samankaltaiset sanat luovat saman WEP-avaimen. Esimerkiksi cat ja catt luovat saman WEP-avaimen. [3.]

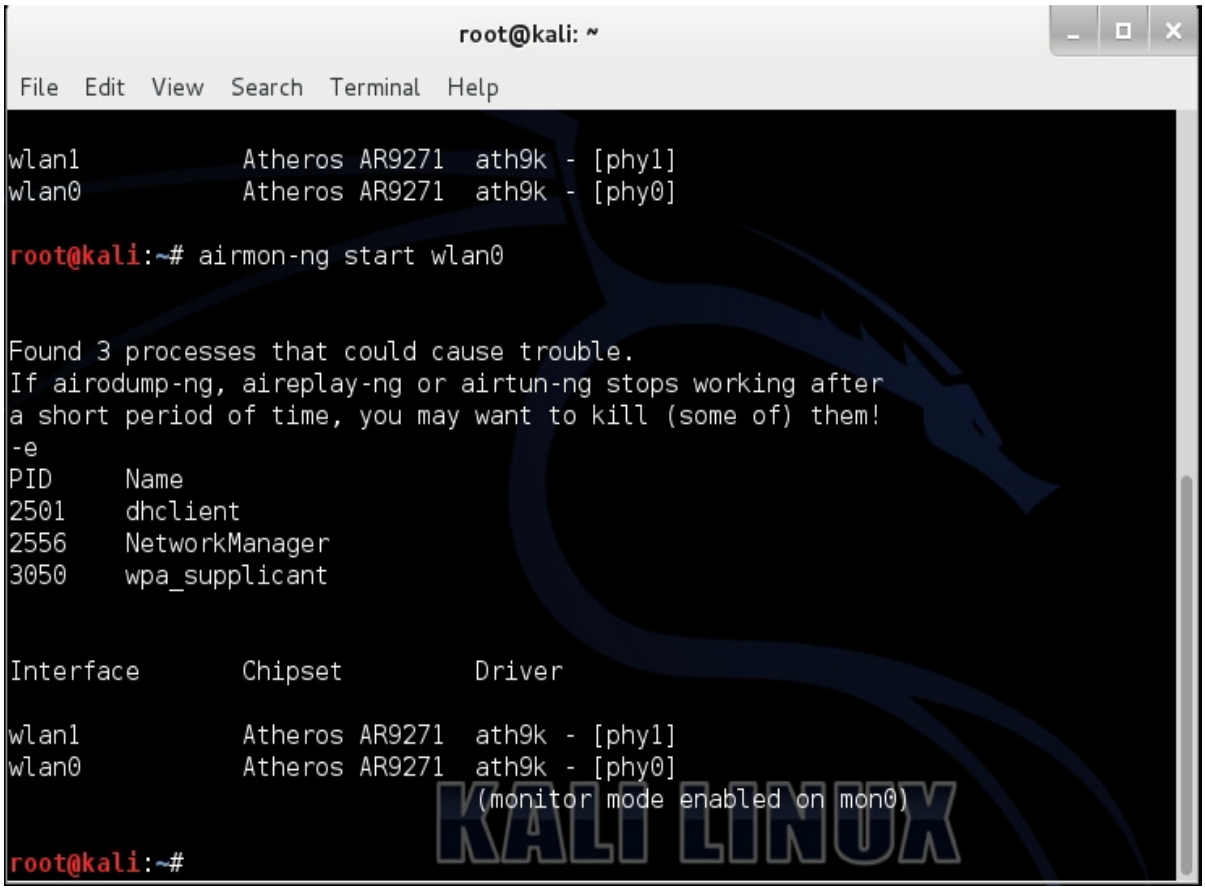
4.3 WEP-sanakirjahyökkäys

Sanakirjahyökkäys on lyhykäisyydessään hyökkäys, jossa käytetään ennakkoon tallennettuja sanoja eli ”Sanakirjaa” salasanan murtamiseen. Käytännössä sanakirja käydään läpi, ja mikäli salasana löytyy, sanakirjasta saadaan salasana murretuksi. Sanakirjahyökkäystä ei oikeastaan kukaan enää käytä WEP-salauksen murtamiseen. Tämä johtuu pitkälti siitä, että on muita parempia menetelmiä, joilla salaus saadaan murrettua minuuteissa. Sanakirjahyökkäys on laajemmin käytössä WPA-salauksen murtamisessa. Sitä käsitellään paremmin luvussa 5. [3.]

4.4 Aircrack PTW

Aircrack PTW on yleisin tapa, jolla WEP-salausta murretaan ja tarkemman kuvan saamiseksi murretaan WEP-salaus laboratorio-olosuhteissa Dir-655-reitittimestä. Tämä operaatio suoritetaan Kali Linuxilla, johon on kiinnitetty TL-WN722N -langaton usb-sovitin. Koneessa on myös kiinni toinenkin langaton usb-sovitin, joka käyttää samaa Atheros AR9271 -piiriä kuin TL-WN722N.

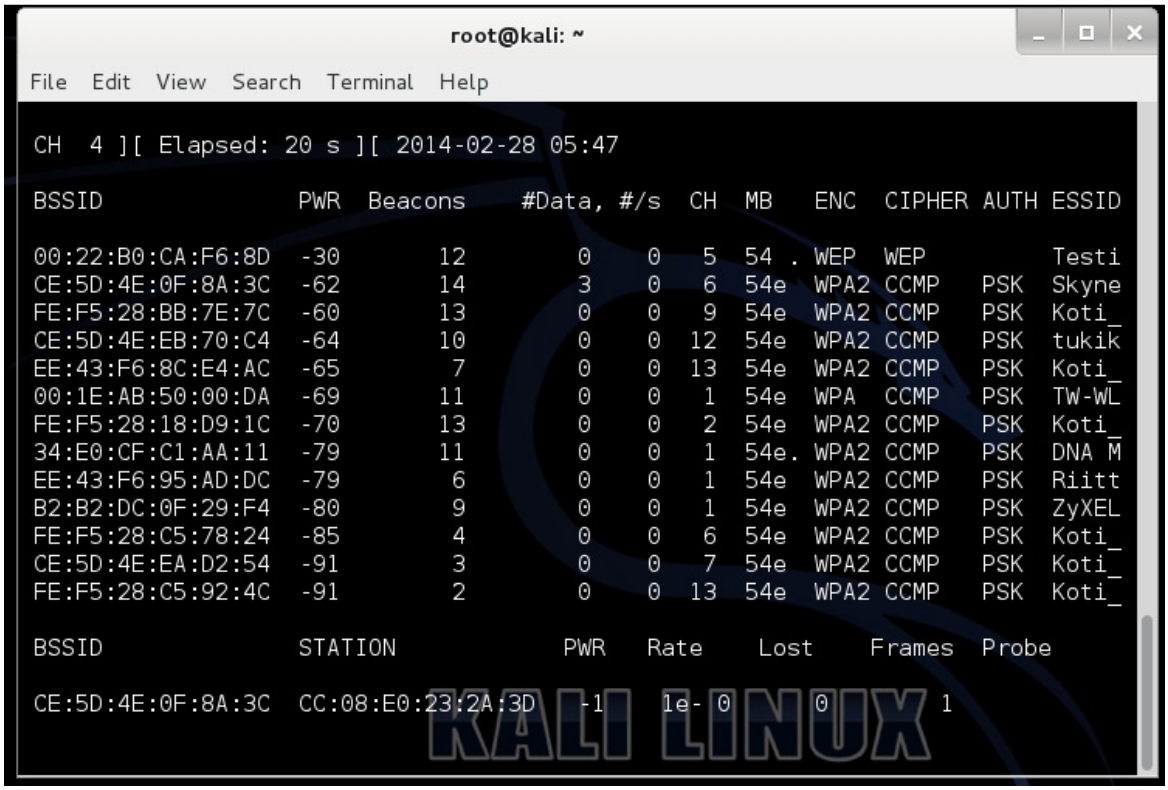
Ensimmäinen tehtävä Kali Linuxilla on tarkistaa, että langattomat USB-sovittimet löytyvät Linuxin alta. Tämä voidaan tehdä yksinkertaisesti vain ifconfig käskyllä tai paremminkin terminaali-ikkunassa pyynnöllä airmon-ng. Airmon-ng on tässä tapauksessa parempi, koska se on työkalu jota käytetään, ja mikäli se ei löydä langatonta adapteria, ei WEP-salauksen murtamisesta tule yhtään mitään.



Kuva 4. Langattoman sovittimen laittaminen monitorointitilaan.

Airmon-ng-komento paljastaa, että käytössä ovat langattomat sovittimet wlan1 ja wlan0. Kummatkin käyttävät Atheros AR9271 -piiriä. Tässä työssä valittiin kyseinen piiri tarkoituksella, koska se on erittäin hyvin yhteensopiva Linuxin kanssa.

Ensimmäinen vaihe WEP:n murtamisessa on laittaa jompikumpi langattomista sovittimista monitorointitilaan. Se onnistuu komennolla ”airmong-ng start wlan0”, jossa wlan0 on haluttu sovitin. Kuten kuvasta 4 näkyy, on monitorointimoodi asennettu mon0:laan, jota käytetäänkin tästä lähtien Wlan0:n sijasta. Kuvasta 4 käy myös ilmi, että taustalla on kolme prosessia, jotka voivat mahdollisesti haitata airodump-ng-, aireplay-ng- ja airtun-ng -ohjelmien toimintaa. Koska WEP-salauksen murtamiseen tarvitaan sekä airodump-ng:tä että Aireplay-ng:tä, on syytä ”tappaa” kaikki kolme taustalla olevaa prosessia. Tämä onnistuu kätevästi kill-komennolla. Huomioitavaa on, että mikäli tarvitsee jotakin tapettua prosessia myöhemmin, on se käynnistettävä käsin uudestaan päälle. Esimerkiksi network manager voi olla tällainen. Seuraava vaihe onkin tarkastella, mitä langattomia verkkoja ympäristöstä löytyy. Tämä onnistuu ”airodump-ng mon0” -käskyllä.

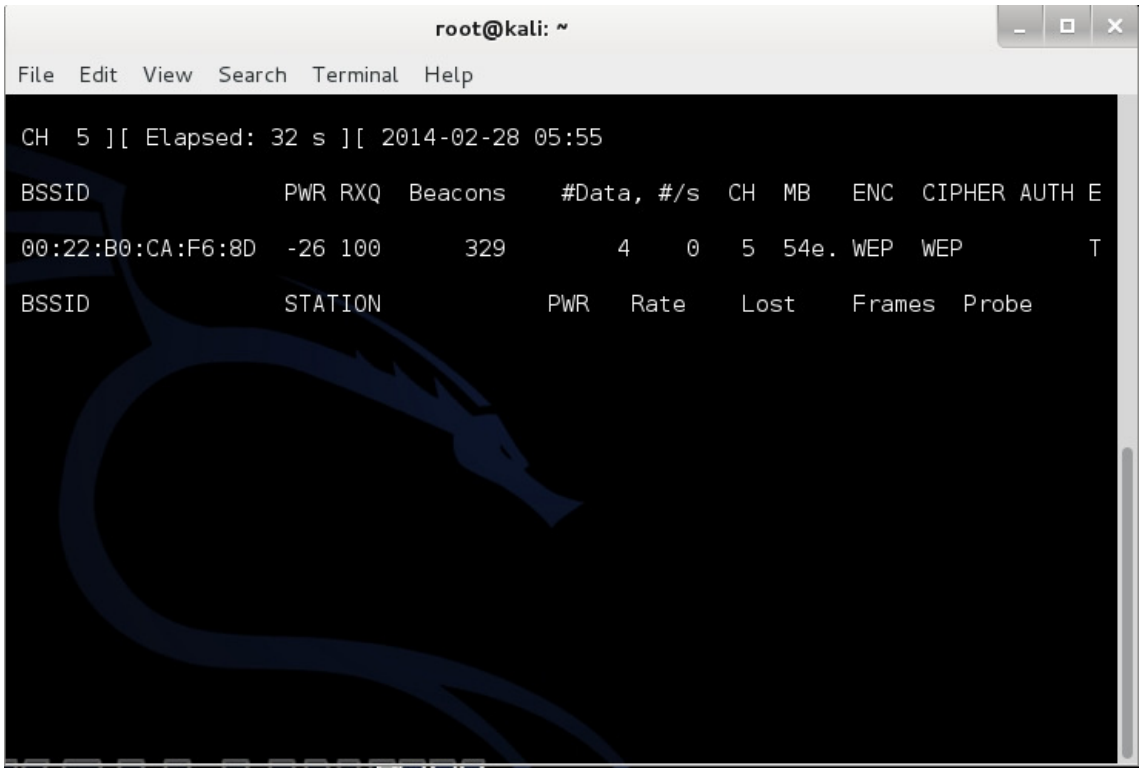


Kuva 5. Lista alueella sijaitsevista tukiasemista.

Käsky listaa lähettyvillä olevat tukiasemat. Tästä listasta tärkeimmät tiedot WEP-salauksen kannalta ovat BSSID, joka kertoo tukiaseman MAC-osoitteen ja PWR:n, joka kertoo signaalin voimakkuuden. Mitä suurempi luku sitä huonompi yhteys (-80 on huonompi kuin -30). CH kertoo, millä kanavalla tukiasema operoi. ENC:llä eli encryptillä saadaan selville, mitä salausta mikäkin tukiasema käyttää. ESSID on tukiaseman SSID, eli nimi.

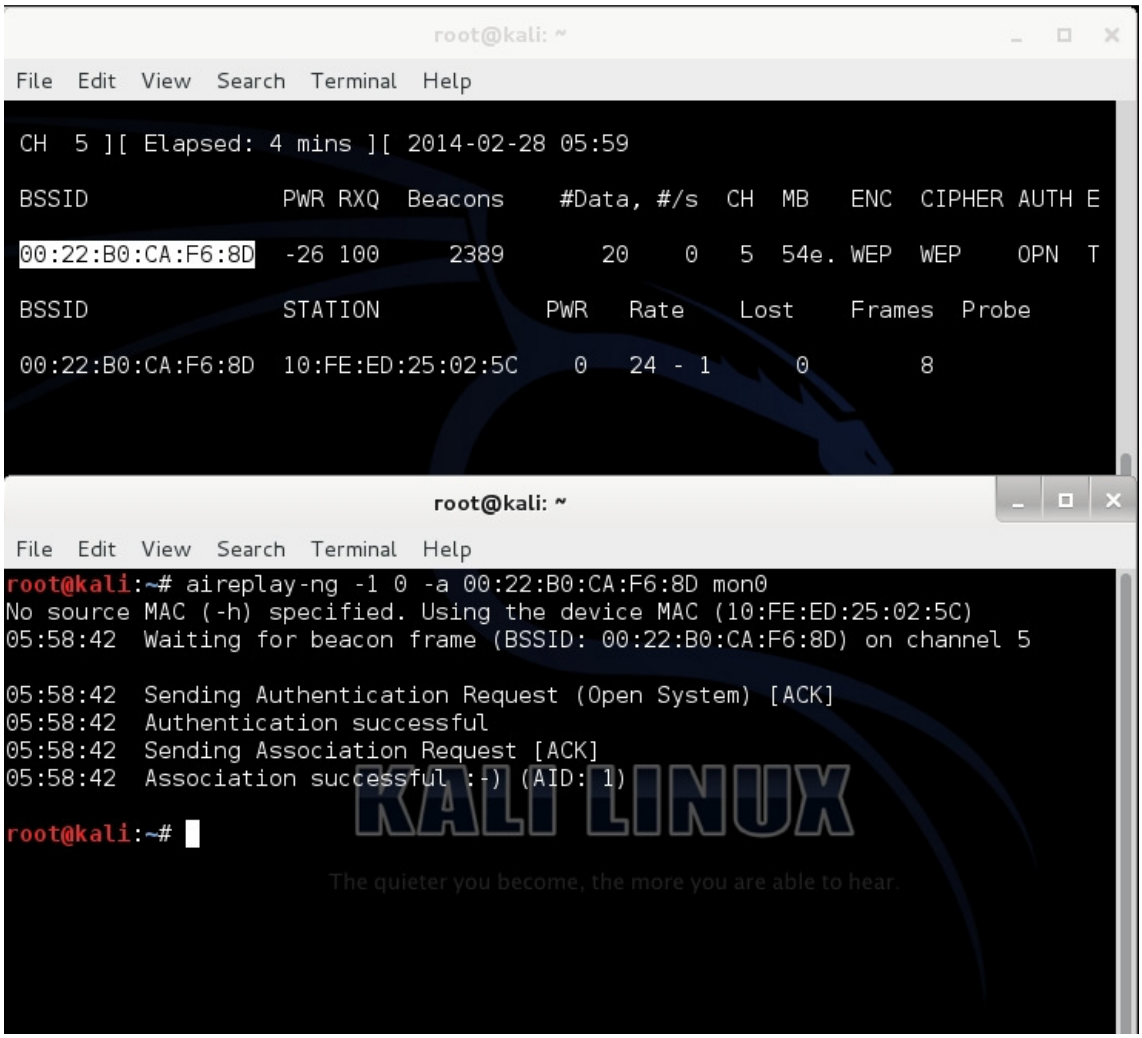
Kuvaa 5 katsomalla saadaan nopeasti selville, mikä on kohdetukiasema. Kyseessä on ylin vaihtoehto ja tässä tapauksessa ainoa tukiasema, joka käyttää WEP-salausta. Ilmeisesti Suomessa Sonera ja Elisa hoitavat hommansa ainakin ADSL-modeemien osalta asiallisesti. Kuitenkin nyt on siis tiedossa BSSID eli tukiaseman MAC-osoite ”00:22:B0:CA:F6:8D”, kanava ”5”, salausmuoto ”WEP” ja SSID ”Testiverkko” (jota ei tarvita tässä vaiheessa). Voidaan siirtyä eteenpäin eli monitoroimaan itse kohdetukiasemaa. Tämä onnistuu helposti kerätyillä tiedoilla sekä Airodump-ng-nimisellä ohjelmalla. Komennolla ”airodump-ng -c 5 -w testi -bssid 00:22:B0:CA:F6:8D mon0”, jossa -c kertoo, millä kanavalla kyseinen tukiasema toimii ja kuten edellisestä kuvasta 5 nähdään, on kanavan numero 5. -w tallentaa .cap-päätteisen tiedoston,

johon kerätään tarvittavat tiedot itse salasanan murtamista varten. Testi on tuon tiedoston nimi, ja kokonaisuudessaan se onkin testi-01.cap. -bssid on tukiaseman MAC-osoite ja mon0 on monitorointiasetuksille pistetty langaton sovitin.



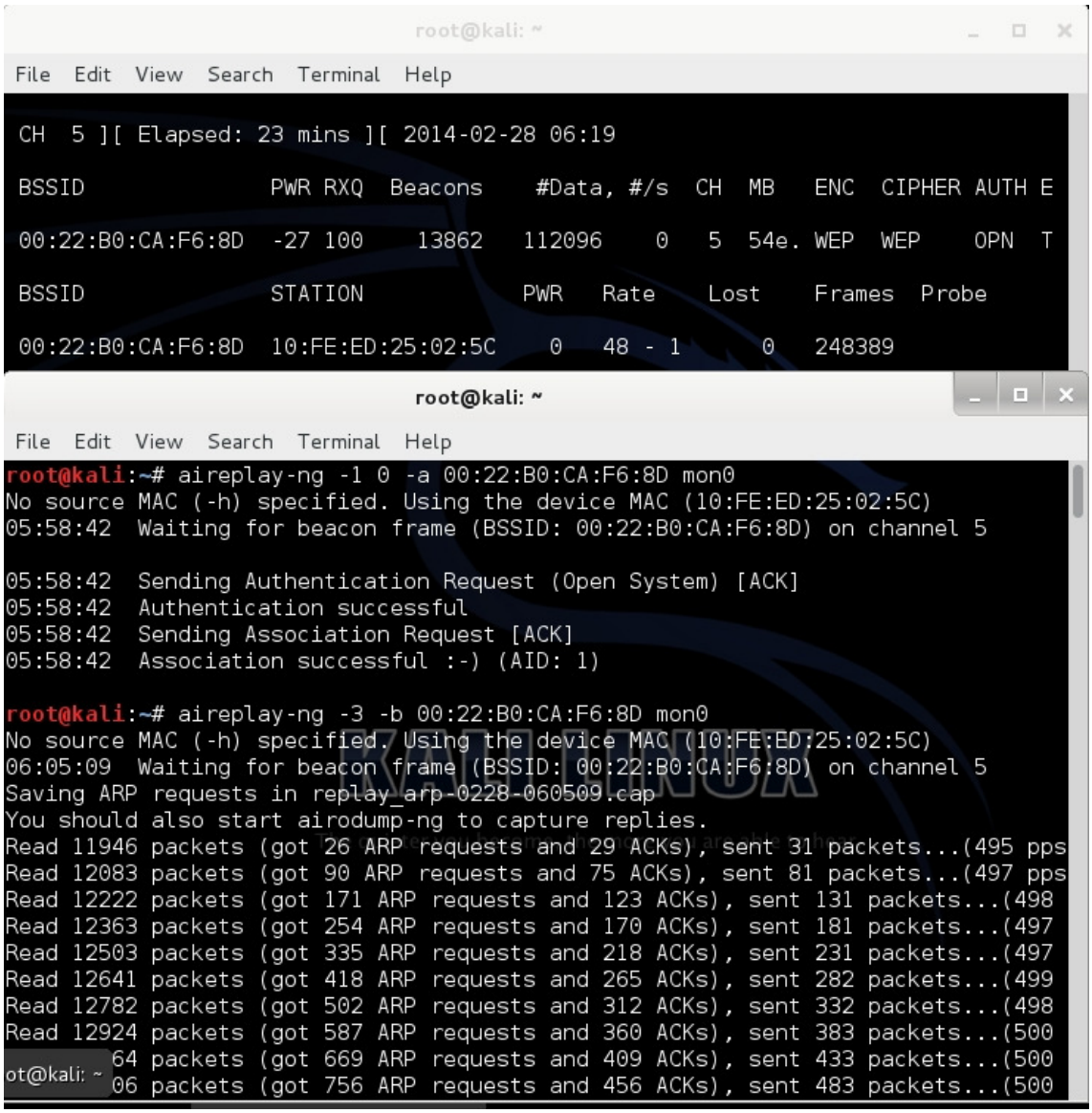
Kuva 6. Valitun tukiaseman monitorointi.

Komennon jälkeen päästään monitoroimaan itse tukiasemaa. Heti ensimmäisenä selviääkin, että itse laitteessa ei ole tällä hetkellä ketään kiinni. Tämä käy ilmi Station-kohdasta, jossa ei tällä hetkellä näy yhtään mitään. Mikäli tukiasema käyttäisi MAC-suodatusta, jouduttaisiin odottamaan sen aikaa, että joku yhdistäisi tukiasemaan. Tämän jälkeen voisi kopioida käyttäjän MAC-osoitteen. Tämä onnistuu Kali Linuxissa erittäin helposti, käytännössä komennolla ”ifconfig wlan0 down”, joka poistaa wlan0:n käytöstä siksi aikaa, että MAC-osoite saadaan vaihdetuksi. Itse Mac-osoitteen muuttaminen onnistuu helposti komennolla ”macchanger -m 00:11:22:33:44:55 wlan0”, jossa siis MAC-osoite voi olla käytännössä mikä tahansa. Tässä esimerkissä käytettiin 11:22:33:44:55-osoitetta. Huomioitavaa on, että mikäli MAC-osoite vaihdetaan, on sama operaatio syytä tehdä myös man0:lle.



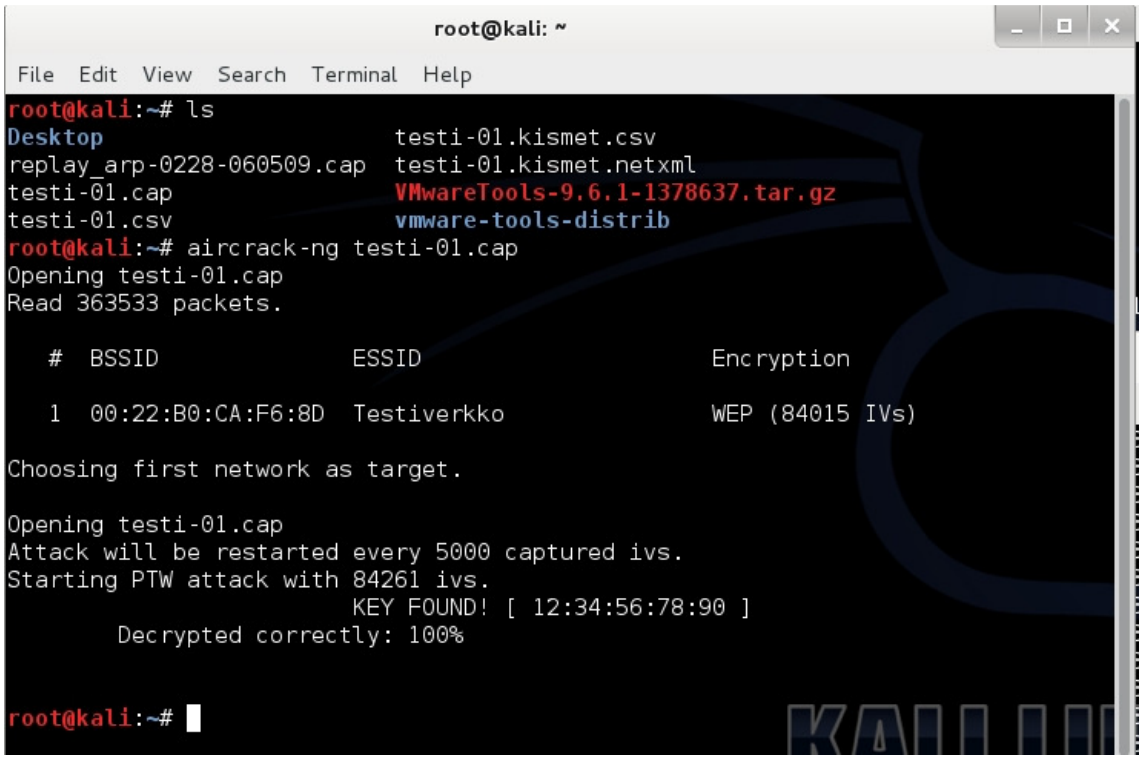
Kuva 7. Vale-todentaminen.

Koska tukiasemaan ei ollut liittynyt yhtään käyttäjää, on aika tehdä vale-todentaminen. Näin saadaan selville, onko tukiasemassa mahdollisesti MAC-osoitteen suodatus päällä. Tämä toiminto onnistuu helposti aireplay-ng-komennolla, tarkemmin ”aireplay-ng -1 0 -a 00:22:B0:CA:F6:8D mon0”, jossa ”-1” tarkoittaa vale-authentikointia ja ”0” viivettä. ”-a” on kohdetukiaseman MAC-osoite. Kuten kuvasta 7 käy ilmi, kaikki sujuu ongelmitta ja vale-todentaminen onnistuu. Huomioitavaa on, että station-kohtaan ilmestyy WLAN-modeemin MAC-osoite. Vale-authentikointi ei kuitenkaan luo yhtään ARP-pakettia. Myös datapaketteja tulee auttamattoman hitaasti, noin yksi joka viides sekunti. Onkin aika hiukan nopeuttaa operaatiota.



Kuva 8. ARP-hyökkäys.

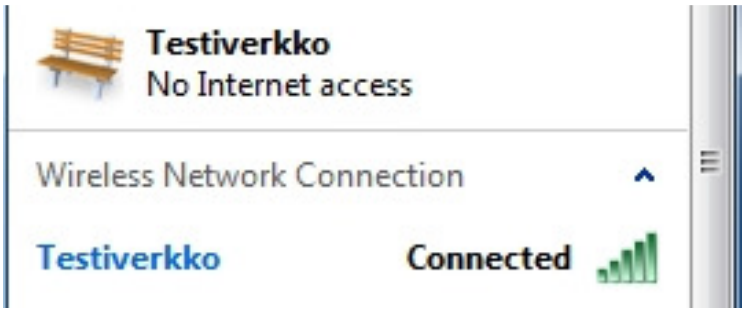
”Aireplay-ng -3 -b 00:22:B0:CA:F6:8D mon0” -komennolla saadaan hiukan vauhtia WEP-salauksen purkamiseen. Huomioitavaa kuitenkin on, että koska liikennettä ei ole aluksi hirveästi, joudutaan odottamaan 11964 pakettia ennen kuin saadaan ensimmäinen salattu ARP-paketti. ARP-paketin tunnistaa sen yksilöllisestä koosta. Ensimmäisen ARP-paketin jälkeen operaatio onkin melkein käytännössä ohi. Sen verran nopeasti datapaketteja alkaa kertyä. Kuten kuvasta 8 käy hyvin ilmi, niin saatu ARP-paketti lähetetään aina tukiasemalle takaisin. Tukiasema vastaa tähän pyyntöön aina uudella ARP-paketilla, jossa on uusi IV. Tällä edestakaisella ARP-pakettien lähettelyllä saadaan nopeasti kerättyä iso määrä iv:itä ja näistä voidaan sitten suorittaa itse avaimen murtaminen.



Kuva 9. WEP-salauksen murtaminen.

Aluksi on tietenkin löydettävä testi-tiedosto, joka luotiin aikaisemmassa vaiheessa ”-w testi” -komennolla. Helpoiten tiedoston löytää ”ls”-komennolla, joka listaa kotihakemistossa olevat tiedostot. Tässä tapauksessa tiedoston koko nimi on testi-01.cap. On aika avata tiedosto aircrack-ng-ohjelmaan komennolla ”aircrack-ng testi-01.cap” Tässä vaiheessa tiedostossa oli jo 84015 kpl ivs:iä, joten murtamisessa ei mennyt kahta sekuntia pidempään. Mikäli ivs:siä ei olisi ollut riittävästi, niin ohjelma ilmoittaisi epäonnistumisesta ja pyytäisi käyttäjää odottamaan hiukan kauemmin, jotta tarvittavia ivs:siä saataisiin kerättyä enemmän talteen.

Tässä tapauksessa kuitenkin avain löytyi, ja se ilmoitetaan heksadesimaalimuodossa. Varsinaista salasanaa ei siis näy, mutta tukiasemaan voi kirjautua käyttämällä avainta muodossa 1234567890. Eli ottamalla välistä ”:” -merkit pois. Huomioitavaa on, että WEP-oletussalasana on aivan hirveä. Jostain syystä WEP-salauksen päälle pistäminen antaa oletuksena avaimen 1234567890. Toisaalta WEP-salaus on muutenkin niin kehno, että tässä tapauksessa moisen oletussalasanan vielä kestää.



Kuva 10. Onnistunut murto.

Kuten kuvasta 10 näkyy, myös yhdistäminen kyseisellä salasanalla onnistui ongelmitta. Eli WEP-salaus on näin virallisesti murrettu.

5 WPA

WPA (Wi-Fi Protected Access) kehitettiin, kun huomattiin, että WEP-standardissa oli isoja puutteita, ja sen tietoturva oli murrettu. Luonnollisesti katseet kääntyivät IEEE:n puoleen, joka ilmoitti kehittävänsä 802.11i-standardin korvaamaan WEP:n. 802.11i-standardin kehityksessä kuitenkin kesti, ja se eteni hyvin hitaasti. Samaan aikaan langattomien laitteiden myynti tippui, koska WEP-ongelmaiset laitteet eivät olleet kovin haluttuja. Valmistajat alkoivat painostaa IEEE:tä ja muita standardin kehittäjiä julkaisemaan jotain, jolla WEP:in ongelmat saataisiin korjatuksi ja sitä myöten laitteiden myynti taas nousuun. Tästä johtuen WIFI Alliance päätti ottaa jo kehitetyn mutta keskeneräisen version IEEE 802.11i:stä ja lanseerata sen WPA:na. Näin ollen myöhemmät 802.11i-versiot olisivat jatkumoa WPA:lle. Myöhemmin kun 802.11i-versio valmistui, sen nimeksi annettiin WPA2. [10.]

WPA korjasi monia WEP:ssä ilmenneitä tietoturva-aukkoja ja toi samalla käyttäjätunnistuksen, joka suurimmalta osaltaan puuttui WEP-standardista. Yksi WPA:n parannuksista oli TKIP Eli Temporal Key Integrity Protocol, joka luo jokaiselle paketille oman uuden 128-bittisen avaimen. [11.] TKIP korjasi näin WEP:ssä olleen haavoittuvuuden, jossa samaa avainta käytettiin jokaisessa paketissa. TKIP käyttää RC4-salausta, jotta se olisi mahdollista päivittää vanhempiin WEP-laitteisiin. [10.]

WPA myös toi MIC:n eli Message Integrity Checkin (tunnetaan myös nimellä Michael), joka estää toistohyökkäykset korjaten näin ollen WEP:iä vaivanneen ARP replay -hyökkäyksen. WPA suunniteltiin alun perin niin, että se olisi mahdollista

päivittää WEP-salausta käyttäviin laitteisiin. WPA2 taas oli sen verran raskas, että sen päivittäminen vanhempiin laitteisiin firmware-päivityksellä ei ollut mahdollista. [12.]

Nykyisin WPA2 on syrjäyttänyt WPA:n, ja se onkin suositelluin langattoman verkon salausmuoto. WPA TKIP:stä on löytynyt myöhemmin tietoturva-aukkoja kuten Beck-Tews attack, joka mahdollistaa 7-15 datapaketin syöttämisen suojattuun verkkoon [13].

Mathy Vanhoef and Frank Piessens löysivät myös keinon, jolla WPA-TKIP-laite hyväksyy myös salaamatonta tietoa. [14.] Tästä johtuen onkin fiksua siirtyä suoraan WPA2- ja AES-salaukseen jos suinkin mahdollista.

Mikään edellisistä menetelmistä ei yleisen tiedon mukaan kuitenkaan palauta salasanaa tai murra itse laitetta siten, että murtautuja pääsisi käsiksi itse verkkoon samaan tapaan kuin verkon omistaja. Seuraavaksi käydään tarkemmin läpi, mitä erilaisia murtautumistapoja tunnetaan WPA- ja WPA2-verkkoihin.

5.1 Raaka laskenta

Raaka laskenta (engl. Brute force) on hyökkäystapa, jossa koitetaan kaikkia mahdollisia merkkiyhdistelmiä, kunnes haluttu salasana löytyy. Tämän tavan hyviä puolia on se, että salasanan murtuminen on varmaa tietyn ajanjakson kuluessa. Huonoja puolia taas on se, että tuo aikajana voi olla mitä tahansa 1 sekunnin ja miljoonan vuoden väliltä riippuen puhtaasti salasanan pituudesta ja isojen, pienten ja erikoismerkkien määrästä. [15.]

Raaka laskenta ei ole kovin käytännöllinen tapa murtaa WPA-salausta kotikonstein. Tämä johtuu puhtaasti siitä, että WPA-salaus käyttää vähintään 8 merkkiä, ja se voi olla jopa 63 merkkiä pitkä. Tämän lisäksi salasana hajakoodataan 4096 kertaa hash-1-menetelmällä. Joten sen murtaminen raa'alla laskentateholla on aikaa vievää. Lyhyesti, jos salasana olisi hajakoodattu vain kerran ja raa'alla laskennalla saataisiin tarkistettua yksi merkki sekunnissa. Kun se on hajakoodattu kerran, tarkoittaisi tämä sitä, että 4096-kertainen hajakoodaus veisi 4096 sekuntia saada sama tulos joka aikaisemmin saatiin sekunnissa. Moninkertainen hajakoodaus on luotu juuri hidastamaan Brute forcen hyödyllisyyttä. [15.]

Nykyiset näytönohjaimet ovat kuitenkin erittäin nopeita ja niitä on ahkerasti valjastettu erinäisiin laskentaoperaatioihin kuten Bitcoinien louhintaan ja salasanojen murtamiseen. Tässä työssä käytetyssä koneessa oleva Radeon 280x -näytönohjain murtaa noin 120–140 tuhatta merkkiä sekunnissa. Siis WPA-verkossa, joka käyttää 4096-kertaista hajakoodausta. Näin ollen mikäli salasanan pituus olisi 8 merkkiä ja kaikki 8 merkkiä olisivat pelkkiä pieniä kirjaimia, niin erilaisia yhdistelmiä olisi 26^8= 208 827 064 576 eli siis 208 miljardia erilaista yhdistelmää. Kun 208 miljardia jaetaan 140 tuhannella, saadaan loppusummaksi 1491621 sekuntia eli 414 tuntia, joka on pyöreästi 17 päivää.

Tämä osoittaa, että salasanan murtaminen Brute forcella yhdellä näytönohjaimella ei ole kovin kannattava operaatio. Varsinkin kun mukaan heitetään mahdolliset numerot ja isot kirjaimet. Mikäli omistaa 1000-näytönohjaimen murtokeskuksen, niin sitten brute force mahdollisesti on varteenotettava vaihtoehto. Silti merkkien lisääntyminen tekee siitä hyvin aikaa vievää puuhaa. Huomioitavaa on kuitenkin, että brute force on tehokas väline salasanojen murtamisessa. Se vain ei ole WPA-salauksen murtamisessa se tehokkain keino.

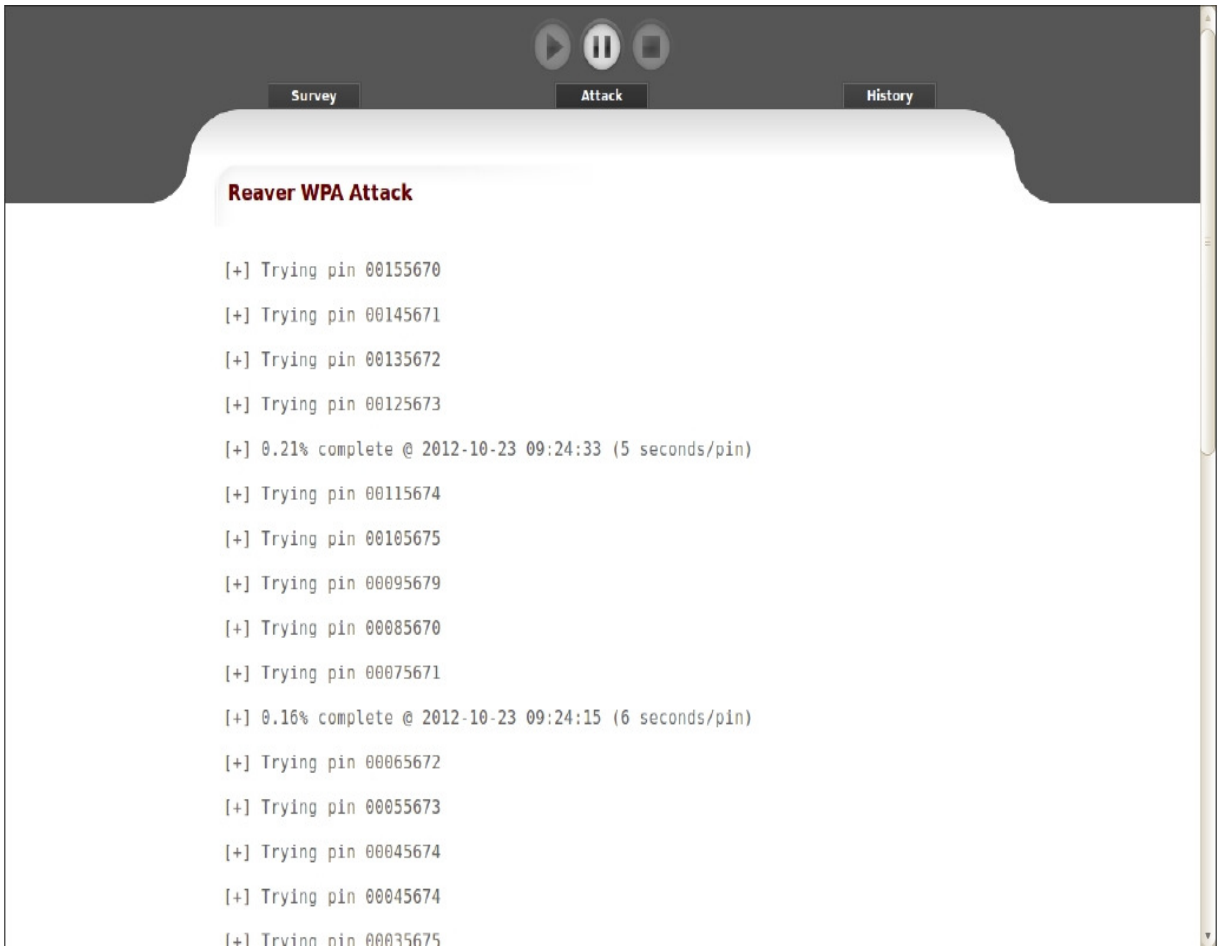
5.2 WPS

WPS Eli Wi-Fi Protected Setup on langaton standardi, joka mahdollistaa helpon yhdistämisen WPA-salattuun tukiasemaan. Tukiasemaan yhdistämiseen käytetään generoitua PIN-koodia. [16.]

> ” Wi-Fi Protected Setup (WPS) on tekniikka, jonka tarkoituksena on helpottaa laitteiden liittämistä salattuihin langattomiin verkkoihin. Eräs WPS-tekniikoista mahdollistaa WPA2-salauksessa (Wi-Fi Protected Access) käytetyn salalauseen siirron tukiasemasta päätelaitteeseen 8-numeroisella PIN-koodilla. WPS-tekniikka on käytössä useissa kotikäyttöön ja pieniin toimistoihin tarkoitetuissa langattomissa tukiasemissa.
>
> Tutkijat löysivät vuoden 2011 lopulla WPS-tekniikasta suunnitteluvirheen, joka mahdollistaa siinä käytetyn PIN-koodin arvaamisen 4 numeroa kerrallaan. Hyökkääjä voi virhettä hyväkseen käyttämällä ohittaa WPS-tekniikkaa käyttävän tukiaseman suojauksen pahimmillaan muutamassa tunnissa. WPS-suojauksen ohittamiseen on julkaistu automaattisesti toimivia työkaluja.” [17]

Käytännössä siis WPS PIN -koodin murtamiseen tarvitaan 11 000 yrityskertaa. On sanomattakin selvää, että jos WPA-salaus voidaan murtaa 11 000 yrityksellä, on kyseessä todella iso tietoturvariski. Paras tapa suojautua tältä haavoittuvuudelta on

yksinkertaisesti ottaa WPS pois päältä. Valitettavasti joissakin laitteissa WPS:n sulkeminen ei estä haavoittuvuuden käyttämistä. Haavoittuvuuden tultua julkisuuteen on sille jo generoitunut automaattisia työkaluja. Yksi näistä tunnetaan nimellä Reaver. [16.]



Kuva 11. Reaver murtamassa WPA-salausta. [16]

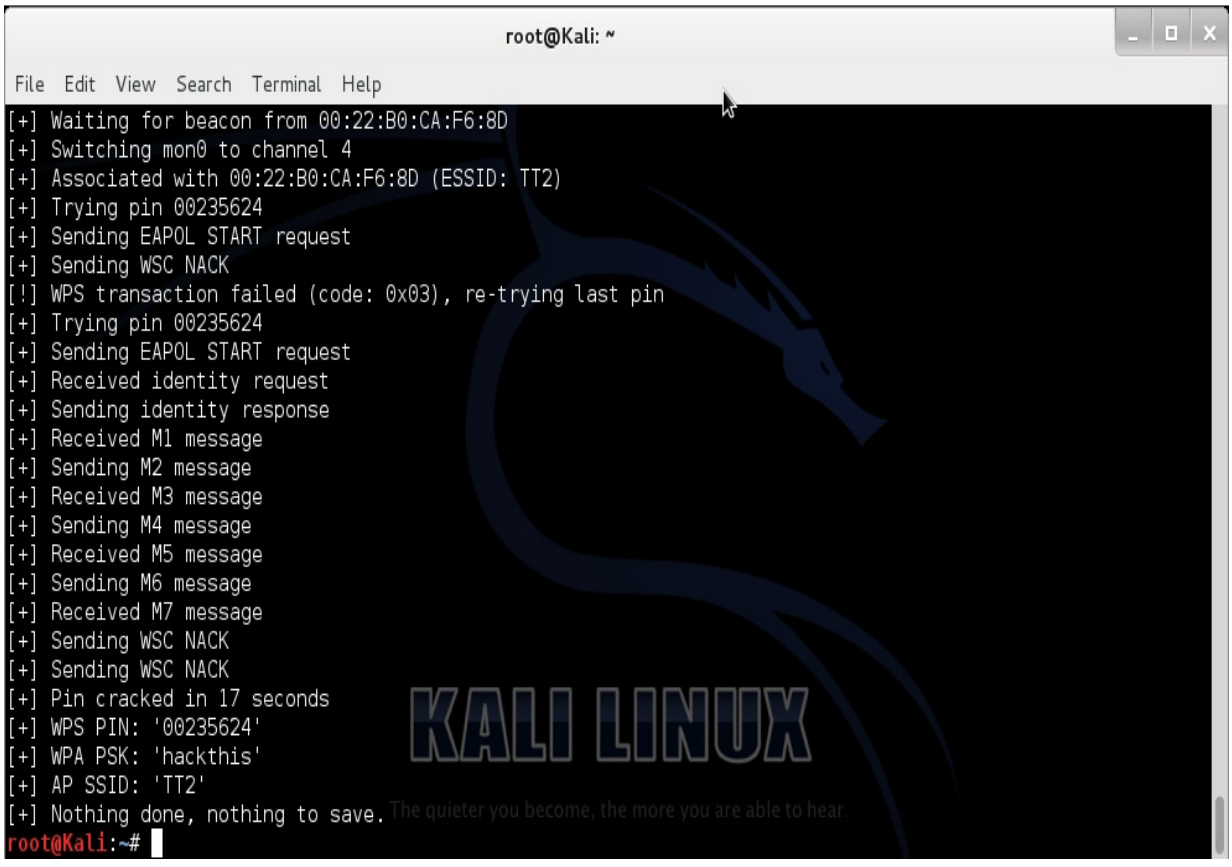
Rever pystyy murtamaan PIN-koodin ja sitä kautta salasanan keskimäärin 3-5 tunnissa. Kuvassa 11 on kuva Reaver Prosta, joka on saatavilla vain kaupallisesti. Sen sijaan Kali Linuxin mukana tulee vapaan lähdekoodin perustuva normaali Reaver-versio.

On selvää, että laitevalmistajat ovat alkaneet vastatoimiin tukkiakseen tämän kaltaisen tietoturva-aukon, ja monet firmware-päivitykset pyrkivätkin tekemään laitteista entistä turvallisempia. Valitettavasti monissa jo myydyissä laitteissa on kuitenkin WPS oletuksena päällä. Myöskään moni kotikäyttäjä ei osaa päivittää laitteiston firmwarea. Tästä johtuen tällä hetkellä on liikkeellä erittäin paljon tukiasemia, jotka ovat helposti

murrettavissa tällä menetelmällä. Erittäin vaarallisen tästä haavoittuvuudesta tekee se, että monet pienet ja suuremmatkin yritykset voivat luottaa langattoman verkon turvallisuuteen sokeasti.

Tästä on olemassa hyvä esimerkki kun TJX-yhtiön langaton WEP-verkko murrettiin ja miljoonien ihmisten luottokorttitiedot vuotivat rikollisille [18]. Samanlainen tapaus voi hyvinkin olla mahdollista, mikäli tukiasemassa on WPS-haavoittuvuus.

Tässä työssä koetettiin myös murtaa DIR-655-reititin, jossa oli WPA2-salaus ja WPS päällä. Operaatio näytti kohtalaisen mutkattomalta, mutta jostain syystä oma DIR-655-reititin kaatuili vähän väliä ja murto-operaatio kaatui lopullisesti 92 %:n kohdalla. Kuvasta 12 selviää, miltä lopullinen tulos näyttää, kun reititin on murrettu PIN-koodilla. Käytännössä kaikki näyttää kuten kuvassa 11 ennen kuin oikea PIN-koodi löytyy ja tulee kuvan 12 kaltainen tulos.



Kuva 12. Reaver mursi WPA-salauksen WPS:n avulla.

Kuvassa 12 on siis oikean PIN-koodin löydyttyä myös WPA-salasana. Operaatio on hyvin yksinkertainen suorittaa ja siksi onkin todella tärkeää päivittää reitittimen tai

tukiaseman firmware uusimpaan versioon ja ottaa WPS kokonaan pois käytöstä ellei sille ole erityistä tarvetta.

5.3 WPA-sanakirjahyökkäys

Sanakirjahyökkäyksestä eli Dictionary attackista olikin lyhyt maininta luvussa 4. Sanakirjahyökkäyksessä käytetään ennalta määrättyjä merkkijonoja, joita verrataan salasanaan, joka halutaan murtaa. Sanakirjahyökkäys on ehkä tehokkain tapa murtaa WPA-salaus, jos WPS-hyökkäys ei toimi. WPS-hyökkäys kuten yllä käytiin läpi, on toimiessaan erittäin tehokas. [3.]

Mikä sitten tekee sanakirjahyökkäyksestä niin tehokkaan? Lyhyesti tehokkaat näytönohjaimet ja internet. Verkosta saa helposti jopa miljardin sanan salasanalistoja. Tällainen lista voi sisältää esimerkiksi sadan kielen sanakirjat ja päälle satoja miljoonia vuotaneita salasanoja verkkosivuilta. Paras tai pahin osuus on, että nykyaikainen näytönohjain käy tämänkaltaisen listan läpi parissa tunnissa. Esimerkiksi tässä työssä käytetty näytönohjain kävi läpi raa'an laskennan testissä 140 tuhatta merkkiä sekunnissa. Salasanojen kohdalla sama näytönohjain koittaa 140 tuhatta salasanaa sekunnissa, joten miljardin salasanan koittamiseen menee aikaa noin 2 tuntia. Toimenpide on murskaavan nopea. [3.]

Koska teknologia on tehnyt sanakirjahyökkäyksestä erittäin tehokkaan ja nopean, on siihen alettu soveltaa myös osaksi raakaa laskentaa. Tätä menetelmää kutsutaan hybridiksi. Ihmisinä meillä on taipumus myös salasanojen suhteen valita merkityksellisiä sanoja kuten jalkapallo. Monet palvelut kuitenkin pyytävät nykyisin myös numeroita ja isoja kirjaimia. Tästä johtuen salasana jalkapallo onkin muuttunut muotoon Jalkapallo15. Tässä yhteydessä 15 voi hyvinkin olla esimerkiksi käyttäjän pelinumero. Heti huomataan, että salasana Jalkapallo15 sisältää 12 merkkiä, jossa on isoja kirjaimia, pieniä kirjaimia ja numeroita. Kyseisen salasanan murtaminen raa'alla laskennalla olisi miltei mahdotonta.

Sen sijaan jos otetaan sanakirja nimeltään ”sanakija.txt”, joka sisältää suomen kielen sanakirjan, jossa sanoja sanakirjassa olisi 200 000 [19]. Tällöin sana jalkapallo löytyisi sanakirjasta.

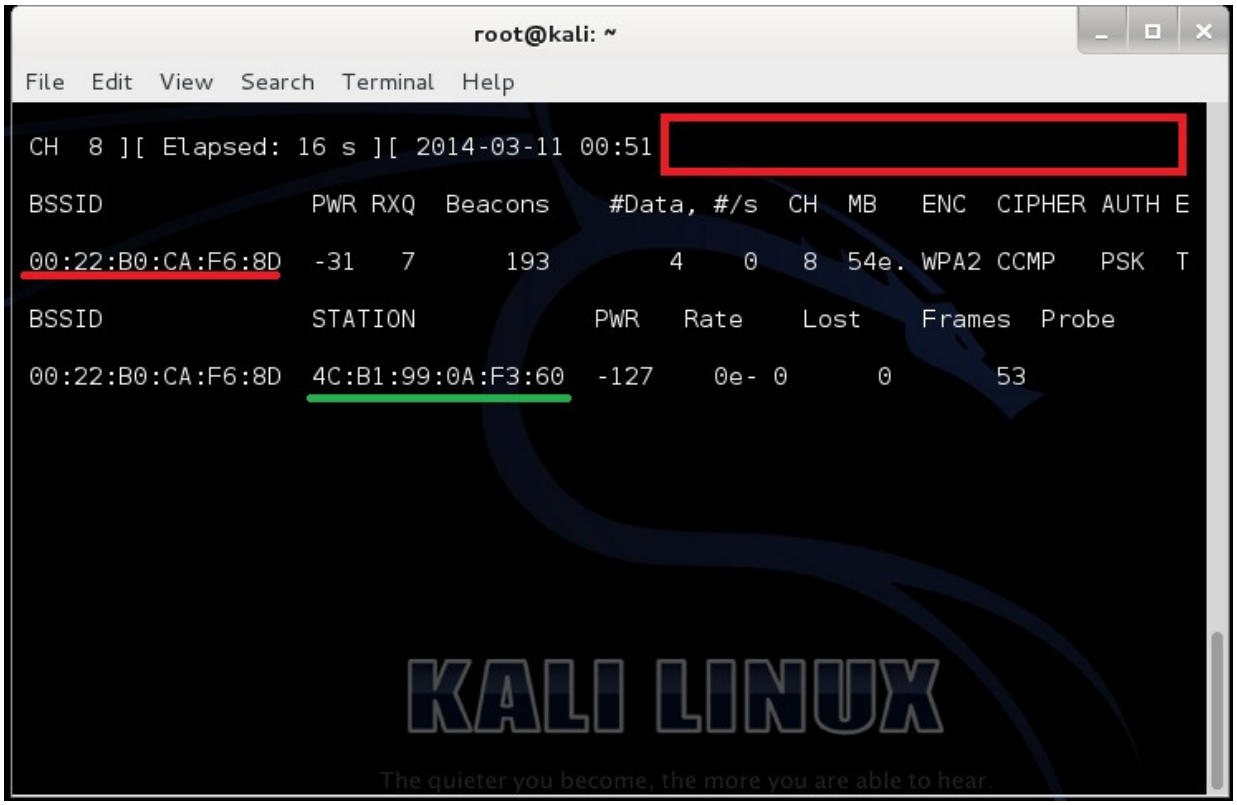
Seuraavaksi onkin aika luoda sääntöjä salasanan testaukseen. Paras ohjelma sanakirjan ja raa'an laskennan käyttämiseen on epäilemättä Oclhashcat. [20.] Oclhashcatilla voi erityisesti tehdä sääntöjä, joiden puitteessa sanakirja käydään läpi. Esimerkiksi voidaan tehdä sääntö, jolla yllämainittu sanakirja käydään läpi, mutta jokaisen sanan perään lisätään numerot 1-99. Tällöin sanakirja.txt käydään läpi 100 kertaa, ensin ilman numeroita ja sitten numeroiden 1-99 kanssa. Lisäksi jokainen sana voidaan myös käydä läpi ison alkukirjaimen kanssa. Tällöin voidaan nopeasti ajatella, että sanakirja.txt sisältää 400 000 sanaa. Eli jokaisen sanan kahdesti. Kun kaikki laitetaan yhteen, saadaan laskukaava 400 000 x 100 = 40 miljoonaa salasanaa. Tällaisen sanakirjan nykyaikainen näytönohjain käy läpi noin 5 minuutissa. Hyvin myös tiedetään, että tämän esimerkin Jalkapallo15 löytyy tuolta listalta.

Lopputulos on siis, että salasana, jonka raa'alla laskennalla olisi vienyt ikuisuuden murtaa, saatiin murretuksi viidessä minuutissa sanakirjan ja raa'an laskennan yhteistuloksella. Erityisesti tässä korostuu se, miten tärkeää on valita hyvä salasana.

Miten WPA2-salasanan murtaminen sitten tapahtuu ihan käytännössä. Tiedetään, että teoriassa käydään sanakirja läpi ja salasana joko murtuu tai ei murru. Mutta koska tässä työssä on tarkoitus oikeasti tarkastella lähemmin menetelmiä, niin yritetään murtaa DIR-655-reitittimen WPA-salaus sanakirjahyökkäyksellä.

Alkuasettelut ovat samat kuin WEP:n murtamisessa. Eli ensiksi on laitettava langaton verkkokortti monitorointitilaan kuten kuvasta 4 (sivu 12) käy hyvin ilmi. Tämän jälkeen toimitaan hyvin pitkälti samalla tavalla kuin WEP:n osalta eli katsotaan ympäriltä löytyvät langattomat tukiasemat ja valitaan niistä sitten se tukiasema, joka halutaan murtaa. Tässä tapauksessa tukiasema on sama kuin WEP-salausta murrettaessa ja tarkemman kuvauksen voi nähdä suoraan kuvasta 5 (sivu 13). WPA-salauksen murtaminen kuitenkin eroaa muilta osin WEP-salauksesta. Esimerkiksi WPA-salauksessa on kaapattava 4-suuntainen kättely. Tätä kättelyä ei ole WEP-salauksessa, koska WEP-salauksessa on hyvin alkeellinen todentaminen. WPA:ssa sen sijaan käytetään 4-suuntaista kättelyä, jotta voidaan luoda salattu väylä tukiaseman ja tietokoneen välille. Tämä kättely sisältää myös tukiaseman WPA-salasanan salakirjoitettuna, joten kättelyn kaappaaminen on tärkeää salasanan murtamisen kannalta. Kuten aikaisemmin WEP-salauksen kanssa, kerätyt tiedot halutaan tallentaa tiedostoon, jotta niitä voitaisiin käyttää myöhemmin. WEP-salauksen kohdalla kerättiin tietoa paketeista, mutta WPA-salauksen kohdalla tallennetaan

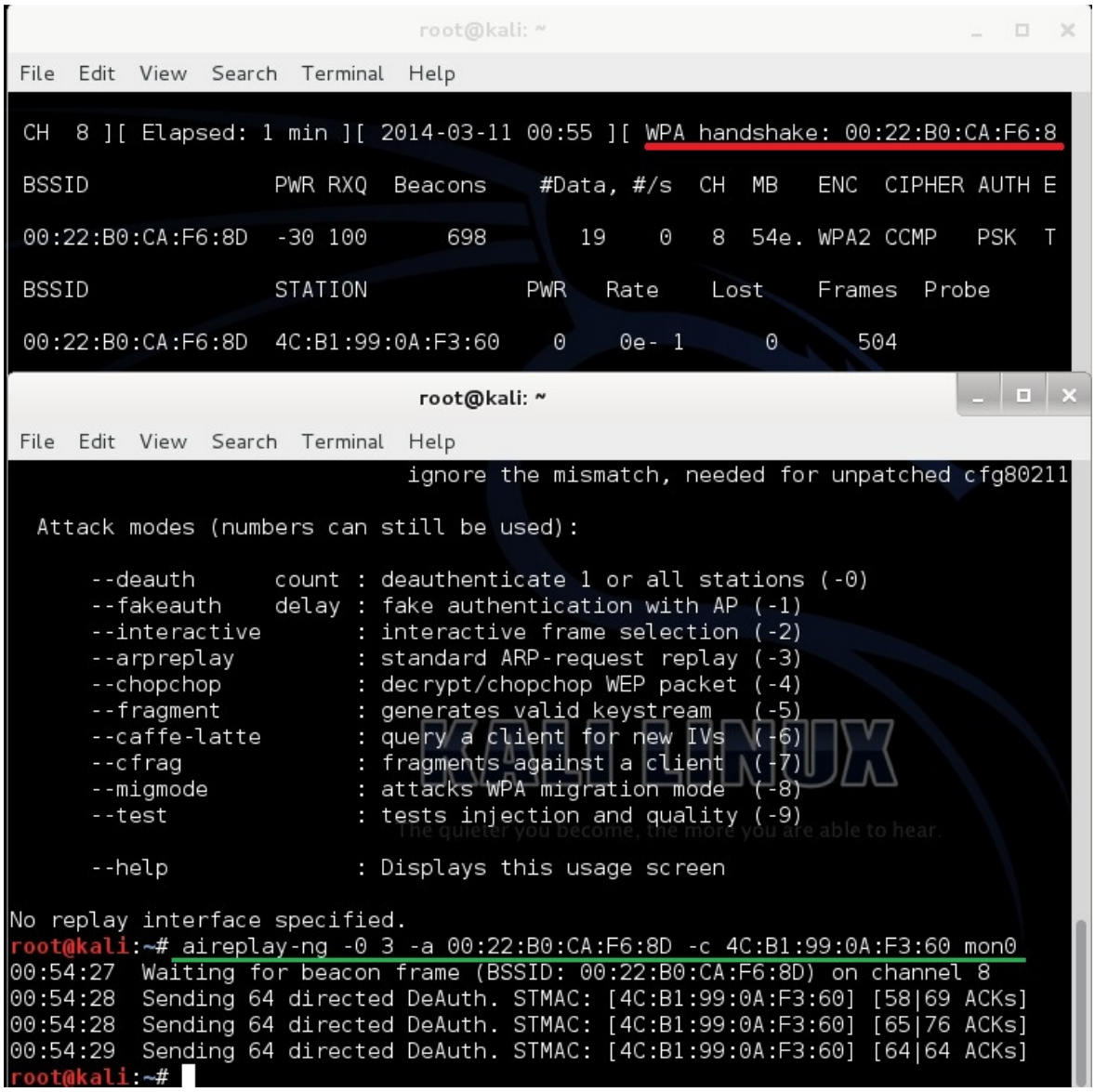
tarvittavat tiedot 4-suuntaisesta kättelystä. Tämä tallentaminen onnistuu samalla lailla kuin WEP:nkin tapauksessa komennolla ”airodump-ng -c 5 -w verkko -bssid 00:22:B0:CA:F6:8D mon0”, missä verkko on tiedoston nimi, johon tiedot kerätään. (Tiedoston nimi voi olla mikä tahansa).



Kuva 13. 4-way handshake.

Kuva 13 on suurin piirtein sama kuin kuva 6, kuitenkin sillä erotuksella, että tällä kerralla tukiasemaan on yhteydessä jo toinen laite. Tämä toinen laite on alleviivattu MAC-osoitteen vihreällä viivalla. Punaisella viivalla on tukiaseman MAC-osoite. Yllä oikealla näkyvä punainen laatikko osoittaa 4-suuntaisen kättelyn paikan, kun se on saatu kaapattua.

Tässä vaiheessa on kaksi tapaa edetä. Mikäli kukaan ei ole yhteydessä tukiasemaan, niin ei voi muuta kuin odottaa, että joku mahdollisesti liittyy kyseiseen tukiasemaan. Kun tämä yhdistäminen tapahtuu, niin samalla hetkellä saamme myös kaapatuksi 4-suuntaisen kättelyn. Toinen vaihtoehto on käyttää deauthentikointia. WLAN-tukiasemat ovat erittäin alttiita häirinnälle ja deauthentikoinnissa tukiasemalle lähetetään yhteyden katkaisupyyntö uhrin nimissä, jolloin tukiasema katkaisee yhteyden uhrin laitteeseen.



Kuva 14. Deauthentikointi

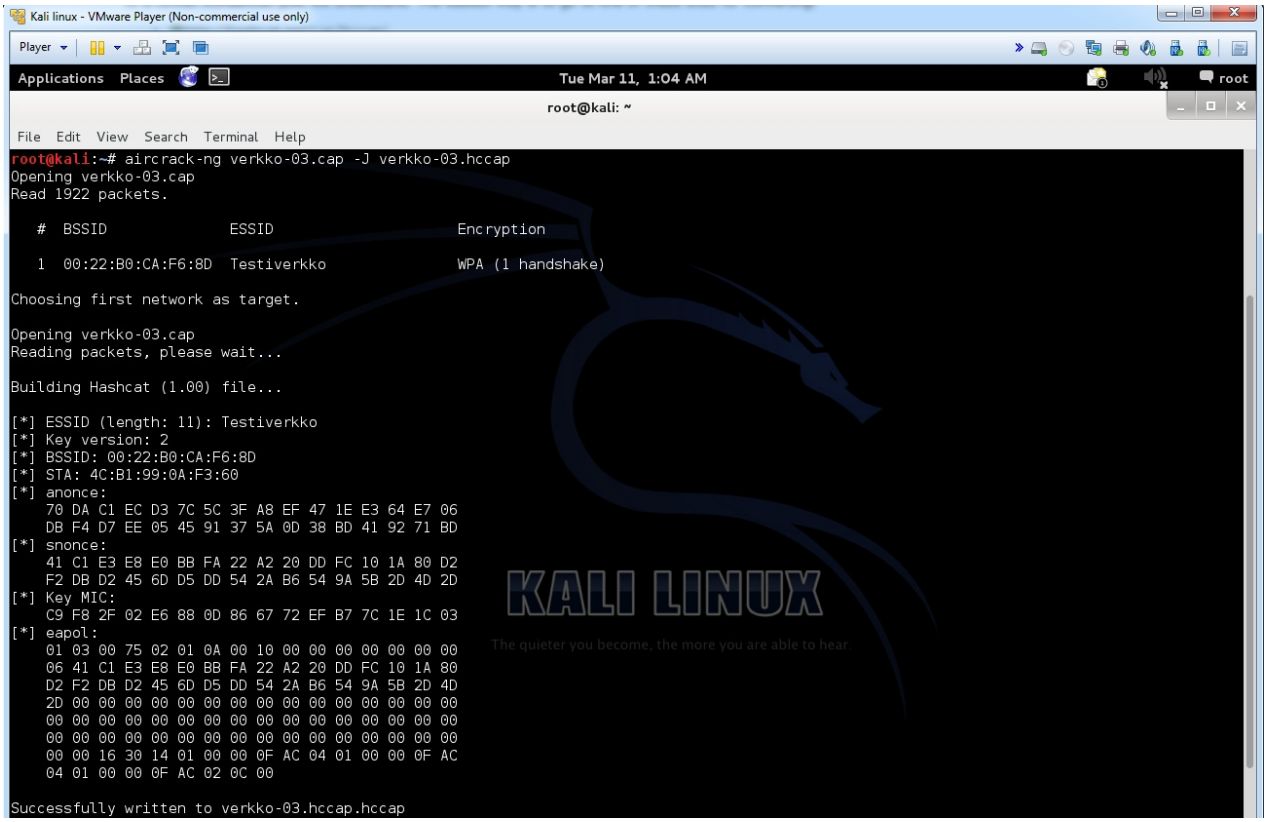
Kuvassa 14 suoritetaan deauthentikointi. Vihreällä alleviivatusta komennosta nähdään lyhyesti, että halutaan lähettää kolme kertaa deauthentikointi tukiasemalle 00:22:B0:CA:F6:8D laitteen 4C:B1:99:0A:F3:60 nimissä. Kun deauthentikaatio lähetetään, tukiasema katkaisee yhteyden laitteeseen 4C:B1:99:0A:F3:60. Laite vastaavasti koettaa yhdistää takaisin tukiasemaan heti, kun se huomaa, että yhteys on katkennut. Laitteen yhdistäessä takaisin tukiasemaan suoritetaan 4-suuntainen kättely uudestaan ja tässä kohtaa se saadaan napatuksi. Kuvan ylälaidassa näkyykin punaisella alleviivattuna, että WPA-handshake on saatu tallennetuksi.

Muuta tietoa ei oikeastaan tarvitakaan tukiasemalta ja voidaan täysin keskittyä itse salasanan murtamiseen. Kali Linuxissa itsessään on myös ohjelma, jolla onnistuu sekä

raa'alla laskentateholla murtaminen että salasanojen koittaminen sanakirjasta. Valitettavasti ohjelma on kuitenkin kohtalaisen hidas, koska se käyttää tietokoneen prosessoria tämän tehtävän suorittamiseen. Tämän kaltaiset tehtävät kannattaa kuitenkin suorittaa näytönohjaimella. Nopeus ero näytönohjaimen ja tietokoneen prosessin välillä on ällistyttävän suuri. Voidaan puhua jopa 100-kertaisista eroista. [21.]

Windowsin puolella paras ohjelma salasanojen murtamiseen on OclHashcat, kuten jo edellä onkin mainittu. Ensiksi joudutaan kuitenkin muuttamaan tallennettu tiedosto verkko.cap tiedostoksi verkko.hccap, jotta voidaan käyttää tiedostoa Oclhashcatissa.

Seuraavalta sivulta löytyy kuva 15 itse operaation suorittamisesta ja tietoa siitä, mitä operaatiossa tapahtuu ja mitä tiedosto sisältää.



Kuva 15. Tiedostomuunnos hccap-tiedostoksi.

Kuvasta selviää, mistä tukiasemasta on kyse eli Testiverkosta ja mikä salausmuoto on kyseessä eli WPA. Huomioitavaa on, että tiedoston muoto on verkko-03.cap, koska aikaisemmin oli jo käytetty samaa tiedostonimeä pariinkin otteeseen. Kaikki murtoyritykset eivät aina onnistu ensimmäisellä kerralla. Kuvasta 15 selviää myös

tiedostoon tallennetut salatut avaimet. Näistä avaimista yritetään murtaa WPA-verkon salasanan. Alhaalla myös lukee ilmoitus siitä, että muutostyö on tehty onnistuneesti.

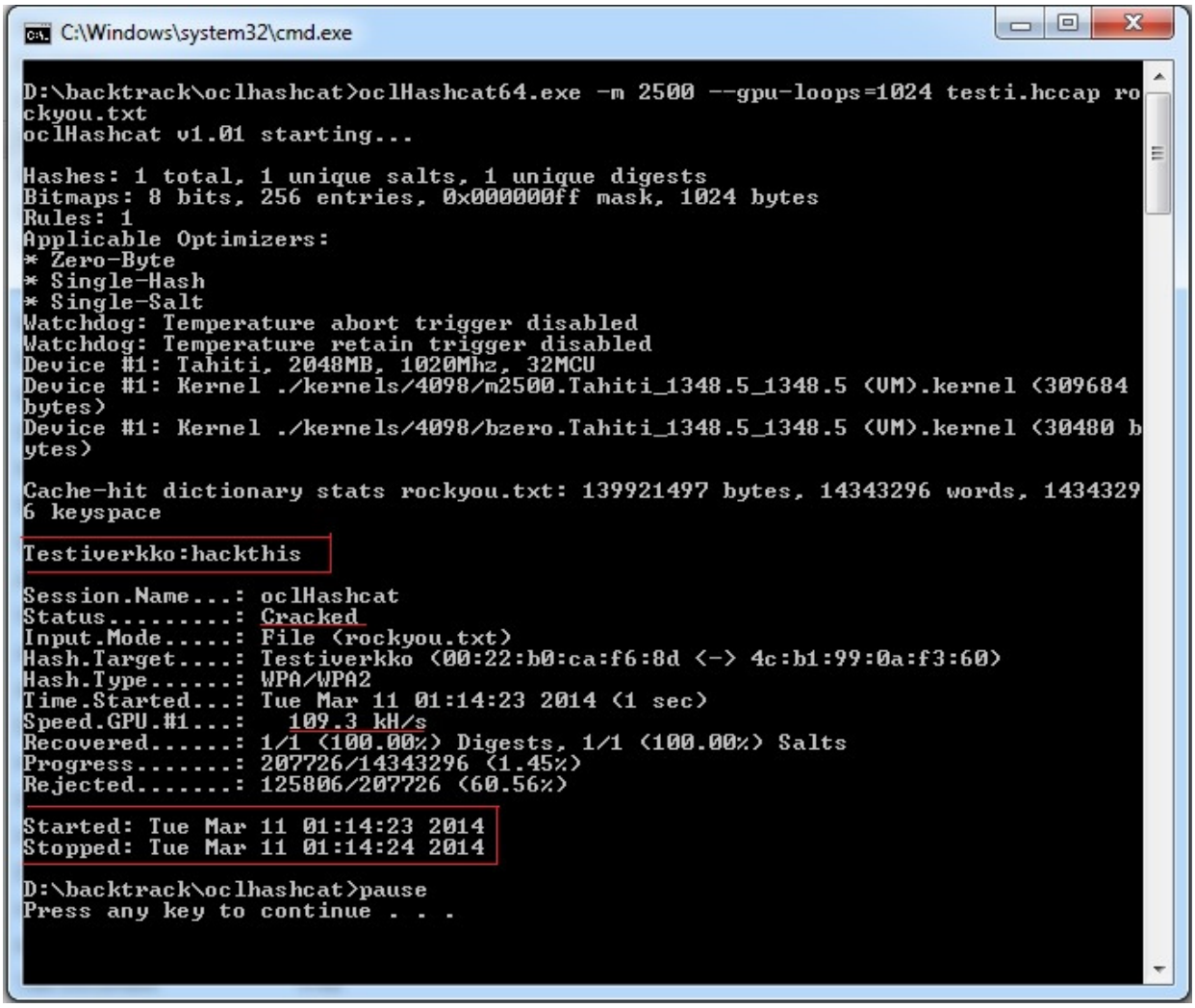
Tässä vaiheessa päästään varsinaisen salasanan murtamiseen Oclhashcat-ohjelmalla. Ohjelma on hyvin konsoliläheinen, ja kaikki suoritukset vaativatkin ohjelman ajamista erinäisillä käskyillä. Kaikkein helpointa on tehdä valmis bat-tiedosto, joka sisältää tärkeimmät parametrit. Myös verkko.hccp-tiedosto on syytä tallentaa samaan kansioon oclhashcat-ohjelman ja ajamiseen tehdyn bat-tiedoston kanssa.

Tässä vaiheessa tarvitaan myös itse sanakirjaa. Sanakirja voi olla käytännössä mikä tahansa tekstitiedosto, jossa vain on sanoja. Käytännössä itse testauksen kannalta ei ole väliä, onko sanoja tiedostossa yksi vai miljoona. Tässä työssä käytetään kuitenkin Kali Linuxin mukana tullutta Rockyou.txt-tiedostoa, joka sisältää noin 14,3 miljoonaa salasanaa. Rockyou.txt on kuuluisa nimenomaan siitä, että vuonna 2009 joku mursi rockyou.com-verkkosivuston ja varasti sieltä 30 miljoonan käyttäjän salasanat. Rockyou.txt on noiden varastettujen salasanojen lista. [22.]

Koska listassa on vain 14 miljoonaa salasanaa, voimme olettaa, että duplikaatit on poistettu. Rockyou.txt-salasanalista ei ole ihanteellinen juuri WPA-salasanan murtamisessa. Tämä johtuu lähinnä siitä, että WPA-salauksessa pienin salasana on kahdeksan merkkiä pitkä. Rockyou.txt-lista sisältää paljon salasanoja, jotka ovat pienempiä kuin kahdeksan merkkiä. Näin ollen aikaa kuuluu myös siihen, että salasanoja hylätään listasta, koska ne ovat liian lyhyitä.

Verkosta on myös saatavilla sanakirjalistoja, jotka on suunniteltu juuri WPA-salauksen murtamiseen. Salasanalistoja valitessa on myös hyvä huomioida alueelliset erot. Esimerkiksi Suomessa englanninkielinen sanakirja on oletettavasti paljon tehottomampi kuin esimerkiksi Yhdysvalloissa. Myös sanakirjalistan löytäminen suomenkielisillä sanoilla on huomattavasti haastavampaa kuin englanninkielisillä. Ei silti kuitenkaan kannata tuudittautua siihen turvallisuuden tunteeseen, että suomenkielisillä sanoilla olisi turvassa. Monet verkkosivut ovat vuotaneet salasanojaan ja niissä voi mahdollisesti olla myös monia suomenkielisiä salasanoja. Yksi hyvä esimerkki on Älypää-verkkosivujen salasanalista, joka julkaistiin verkossa. Se sisälsi noin 120 tuhannen suomalaisen salasanat.

Mutta palataanpa takaisin Oclhashacattiin. Seuraavalla sivulla on kuva 16 lopullisesta salasanan murtamisesta.



Kuva 16. WPA-salasanan murtaminen.

Kuvasta 16 nähdään heti, että verkon salasana on löytynyt. Tila on murrettu ja salasana hackthis on näkyvillä. Testiverkon salasana oli siis hackthis. Kuvasta myös huomataan, että murtoon meni aikaa yksi sekunti ja sinä aikana ehdittiin kokeilla noin 207726 salasanaa, joista hylättiin 60 %, eli 125806 kappaletta. Nämä salasanat oletettavasti olivat lyhyempiä kuin kahdeksan merkkiä. Murtonopeus oli noin satatuhatta sanaa sekunnissa. Tässä testissä nopeus jäi hiukan alhaisemmaksi, koska salasana löytyi käytännössä heti.

Yleisesti voidaan todeta, että WPA- ja erityisesti WPA2-salaus on erittäin toimiva, kunhan osaa välttää pahimmat ansakuopat. Lyhyesti WPS-järjestelmän

sammuttaminen, WPA2:n käyttäminen ja kunnollisen salasanan valitseminen ovat avaintekijät langattoman verkon turvallisuuteen. Myös tukiaseman firmwaren päivittäminen on suositeltavaa. Suurin riski WPA2-langattomalle verkolle on huono salasana. Onkin tärkeä tiedostaa, että Jalkapallo15 ei ole hyvä salasana, vaikka siinä onkin yli kahdeksan merkkiä ja numeroita.

6 Salasanat

Koska hyvä salasana on niin tärkeä osa hyvän langattoman verkon turvallisuutta, käydään seuraavaksi asiaa lyhyesti läpi. Tiedetään siis, että WPA2-verkon salasanan murtamiseen on käytössä pääosin vain pari menetelmää. Joko salasana murretaan raa'alla laskennalla, sanakirjalla tai näiden välimuodolla. Näistä menetelmistä voidaan raaka laskenta jättää nopeasti pois, mikäli salasana on yli 9 merkkiä. Sen sijaan sanakirja ja erityisesti hybridi (sanakirjan ja raa'an laskennan yhteistyö) ovat erittäin vaarallisia menetelmiä, mikäli salasana on heikko. Hybridi, kuten edellä mainittiin siis lisää laskennan tehon ennalta määrättyihin sanoihin. Tyyliin auto, auto1, auto2... auto67 jne. Tästä johtuen Jalkapallo15 ei ole hyvä salasana. [21.]

Minkälainen sitten on hyvä salasana? Hyvä salasana on esimerkiksi HevonenAutoLasi*10. Tällaisen salasanan murtaminen laskennalla on mahdotonta, ja hyvin todennäköisesti sitä ei myöskään sanakirjasta löydy. Tärkeää on myös, että samaa salasanaa ei myöskään käytä missään muualla. [21.]

Mikäli käyttää joka paikassa eri salasanaa, huomaakin nopeasti, että salasanoja kertyy sellainen määrä, että niitä kaikkia on miltei mahdotonta muistaa. Tähän ongelmaan on kehitetty pari erilaista menetelmää. Esimerkiksi salasanaholvi, jonne salasanat voi tallentaa ja holvin saa auki pääsalasanalla. Ongelma tietysti on, että jos pääsalasanan unohtaa, niin kaikki salasanat on menetetty, tai jos pääsalasana vuotaa, niin kaikki salasanat ovat vaarantuneet. [21.]

Omakohtainen menetelmäni on ollut kirjoittaa salasanat ylös pieneen kirjaan pöytälaatikkoon. Olen lisännyt tähän menetelmään pienen koodin, joka on vaikka tässä P9. Sanotaan, että sivuston A) Salasana on Pkissa9 ja sivuston B) salasana on Pkoira9. (Huom. Salasanat ovat huonoja ja ovat yksinkertaisia vain esimerkin vuoksi.) Nyt kirjoitan vihkoon, että salasana A on kissa ja salasana B on koira. Kukaan ei tiedä salaista koodiani, joka on P9, josta P tulee sanan eteen ja 9 sanan loppuun, joten jos

kirja varastetaan, ovat salasanat edelleen turvassa sen verran, että ehdin vaihtamaan ne joksikin muuksi.

Myöskään salasanan vuotaminen ei haittaa, koska jokainen salasana on käytössä vain yhdessä paikassa. Tietysti mikäli joku saa varastetuksi kirjani ja löytää koodini jostain, niin ollaan pulassa. Toisaalta ei siitä kaksivaiheisesta todennuksestakaan ole hyötyä, jos joku varastaa laitteen, jolla se tehdään. Kaksivaiheisesta todennuksesta sen verran, että sitä kannattaa aina ehdottomasti käyttää, mikäli se on mahdollista.

Kaksivaiheinen autentikaatio on esimerkiksi pankkikortti. Tällöin tarvitaan ensiksi kortti ja sen lisäksi PIN-koodi, jotta rahojen nosto onnistuu. Toinen esimerkki kaksivaiheisesta todennuksesta on nettipankin sisäänkirjautuminen, jossa tarvitaan salasanan lisäksi todennusavain pahvilappusesta, digitaalisesta laitteesta tai muusta vastaavasta. Monet verkkosivustot tarjoavat kaksivaiheista autentikointia, esimerkiksi Facebook, Twitter, Gmail jne. [21.]

7 Käyttäjäpuolen hyökkäykset

Yllä olevien testien perusteella voidaan sanoa, että hyvin suojattua WPA2-yhteyttä voidaan pitää turvallisena. Onkin aika siirtyä tutkimaan hyökkäyksiä ja vaaroja, jotka kohdistuvat tukiaseman sijasta niitä käyttäviin käyttäjiin. Usein kuulee paljon puhuttavan, että tukiasema ei välttämättä ole turvallinen tai, että tuntemattomaan tukiasemaan ei kannata yhdistää. Seuraavaksi onkin tarkoitus tutkia pikkuisen syvällisemmin, mitä tarkoittaa tuntematon tukiasema ja mitä vaaroja siihen sisältyy.

Selvennetään aluksi, että mikä on tuntematon avoin tukiasema. Tuntematon avoin tukiasema on mikä tahansa tukiasema, jota käyttäjä ei voi itse hallinnoida. Kaikki muut tukiasemat, jotka ovat avoimia ja jotka eivät ole käyttäjän hallinnassa, ovat riskialttiita.

Tärkeää on tietää, että tukiaseman nimen voi muuttaa hyvin helposti mistä tahansa tukiasemasta. Joten jos tukiaseman nimi on vaikka Osuuspankin WLAN, se ei vielä kerro varmuudella, että kyseessä on todellakin Osuuspankin WLAN! Kuka tahansa voi nimetä tukiasemansa Osuuspankin WLANiksi, mikäli näin tahtoo. Tämä on yksi niistä syistä, miksi tuntemattomat tukiasemat voivat olla niin vaarallisia.

Toinen syy, mikä tekee tuntemattomista tukiasemista niin vaarallisia, on se, että tukiasemat ovat erittäin herkkiä häirinnälle. Tästä olikin jo hyvä esimerkki edellä (WPA ja 4-suuntaisen kättelyn tiimoilta), jossa käytettiin deautentikaatiota. Deautentikaatiota lähettämällä jatkuvasti voi tehdä mistä tahansa tukiasemasta käyttökelvottomat. Hyökkääjä voi myös estää tällä tavalla useamman kuin yhden tukiaseman toiminnan. Pahimmassa tapauksessa yksi käyttäjä yhdellä tietokoneella voi estää koko kantoalueen langattomien verkkojen toiminnan. Pelkästään langattomien verkkojen käyttämisen estäminen on itsessään jo aika huolestuttava riski. Varsinkin kun sen voi tehdä kuka tahansa, millä tahansa kannettavalla ja kuinka monelle tukiasemalle tahansa.

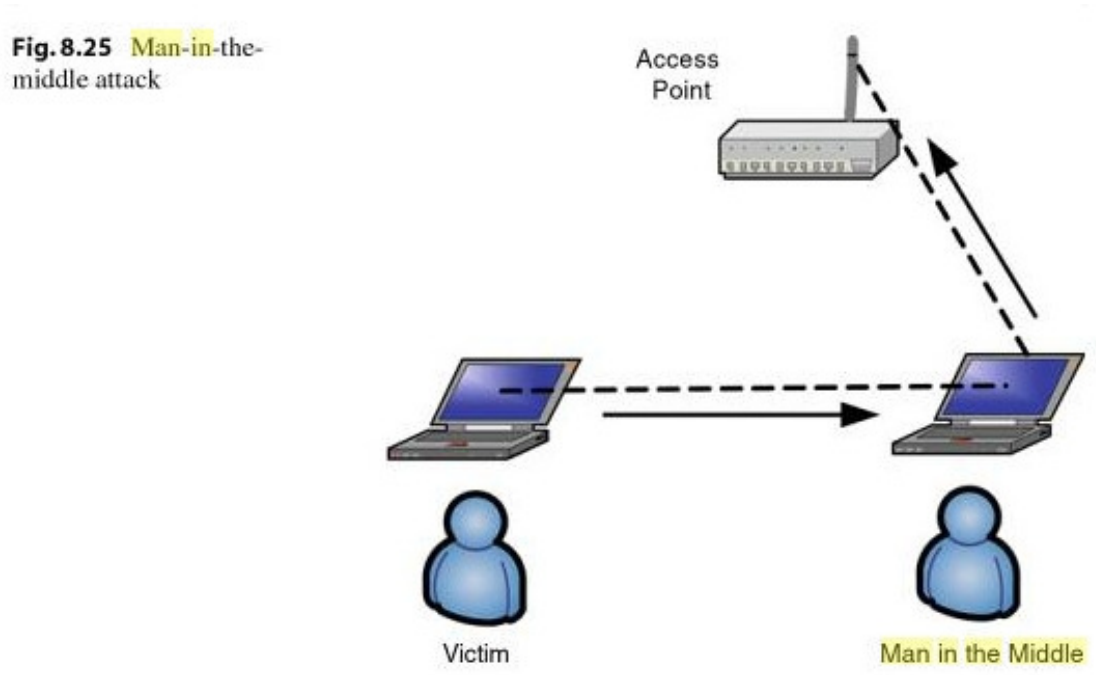
Mikä tästä sitten tekee käyttäjän kannalta vaarallisen, on se, että hyökkääjä voi estää kaikkien oikeiden tukiasemien toiminnan, jolloin ainoaksi toimivaksi vaihtoehdoksi jää hyökkääjän valitsema tukiasema. Toinen vaara on, että hyökkääjä voi koettaa pakottaa uhreja omaan tukiasemaansa deautentikoinnilla ja nimeämällä oman tukiasemansa täysin samannimiseksi kuin paikan virallinen tukiasema. Esimerkiksi samaksi kuin McDonaldsin tukiasema. Mikäli hyökkääjän tukiasemalla on vahvempi signaali, niin uhrit liittyvät hyökkääjän tukiasemaan. Tämä siksi, että langattomilla verkkokorteilla on tapana priorisoida vahvimman signaalin mukaan.

Yleensä hyökkääjän tukiasema on se, joka voittaa kilpailun. Tämä johtuu pitkälti siitä, että tukiasemien suurin sallittu lähetysvoimakkuus Suomessa on 20 dbm, joka on noin 100 mW. Tämä vaihtelee maakohtaisesti, ja yleisesti laitteet pystyvät lähettämään paljon suuremmallakin voimakkuudella, mutta ovat rajoitetut ohjelmallisesti lakien mukaisesti. Hyökkääjä sen sijaan voi vahvistaa lähetysvoimakkuutta vaikka 30 dbm:hen eli 1000 mWasti. (Mikäli käytössä oleva laite vain siihen voimakkuuteen teknisesti pystyy.) Tämä tietenkään ei ole laillista, mutta yleensä hyökkääjä ei muutenkaan niin paljoa välitä siitä, että mikä on laillista ja mikä ei. Hyökkääjän tukiasemalla voi siis olla jopa 10 kertaa voimakkaampi signaali kuin virallisella tukiasemalla.

7.1 Man in the middle

”Man in the middle” tarkoittaa lyhyesti sitä, että yhteyden välissä on kolmas osapuoli, joka salakuuntelee liikennettä. Mitä tämä sitten tarkoittaa avoimien tukiasemien osalta? Tietysti sitä, että jokainen avoin tukiasema voi altistaa tälle hyökkäykselle. Aina

kun yhdistää avoimeen tukiasemaan, johon itsellä ei ole hallintaa tai saati näköyhteyttä voi olla altistuneena man in the middle -hyökkäykselle. Tämän tyyppinen hyökkäys on todella helppo toteuttaa. Siihen ei tarvita muuta kuin kannettava ja ulkoinen usb-langaton modeemi. Esimerkiksi Kali Linuxilla voi tehdä usb-modeemista tukiaseman ja kuten minkä tahansa tukiaseman sen voi vielä nimetä haluamallaan tavalla. Yleisesti kannettavissa on myös langaton verkkokortti, jota voi tarvittaessa käyttää yhdistääkseen toiseen langattomaan verkkoon. Näin siis käyttäjät liittyvät hyökkääjän tukiasemaan, ja kaikki verkkoliikenne kulkee hyökkääjän tietokoneen kautta. Toinen vaihtoehto on käyttää toista verkkokorttia deautentikoimiseen ja pakottaa uhrit hyökkääjän tukiasemaan. Tämä usein vaatii myös nettitikun, jotta uhreille on mahdollista tarjota internetyhteys. Tämän jälkeen hyökkääjä voi salakuunnella kaikkea verkkoliikennettä ja kaapata salasanoja, luottokorttitietoja ja mahdollisesti muuta arkaluontoista tietoa.



Kuva 17. “Man in the middle” -hyökkäys. [22.]

Kuva 17 antaa paremman kuvan siitä, miltä man in the middle -hyökkäys näyttää. Uhrin on hyvin vaikea tunnistaa hyökkäystä, koska uhri ei käytännössä mitenkään näe, että välissä on joku, joka salakuuntelee yhteyttä. Tämä on yksi syy siihen, mikä tekee tästä hyökkäyksestä erittäin tehokkaan.

7.2 SSLStrip

Useimmat sivustot käyttävät nykyisin SSL-suojausta, joka suojaa osaltaan salakuuntelua vastaan. Kuitenkin ohjelmat kuten SSLStrip poistaa SSL-suojauksen. SSLstrip toimii siten, että hyökkääjän ja sivuston välinen yhteys on salattu mutta hyökkääjän ja uhrin välinen yhteys ei ole. Kuva 18 selventää hieman tätä.

Kuva 18. SSLStrip toiminnassa. [26]

Kuvassa 18 hyökkääjä on siis ”Man in the middle” -positiossa, jota käsiteltiin kohdassa 7.1.

Hyökkääjä saa kaikki mahdolliset salasanat, käyttäjätunnukset, luottokorttitiedot jne. Selkokielisinä, vaikka käyttäjä luulee, että sivusto käyttää automaattisesti https-suojausta. Hyvä tapa suojautua avoimissa langattomissa verkoissa on käyttää VPN-yhteyttä. VPN-yhteydestä kerrotaan lisää kohdassa 8. VPN.

7.3 Pineapple Mark V

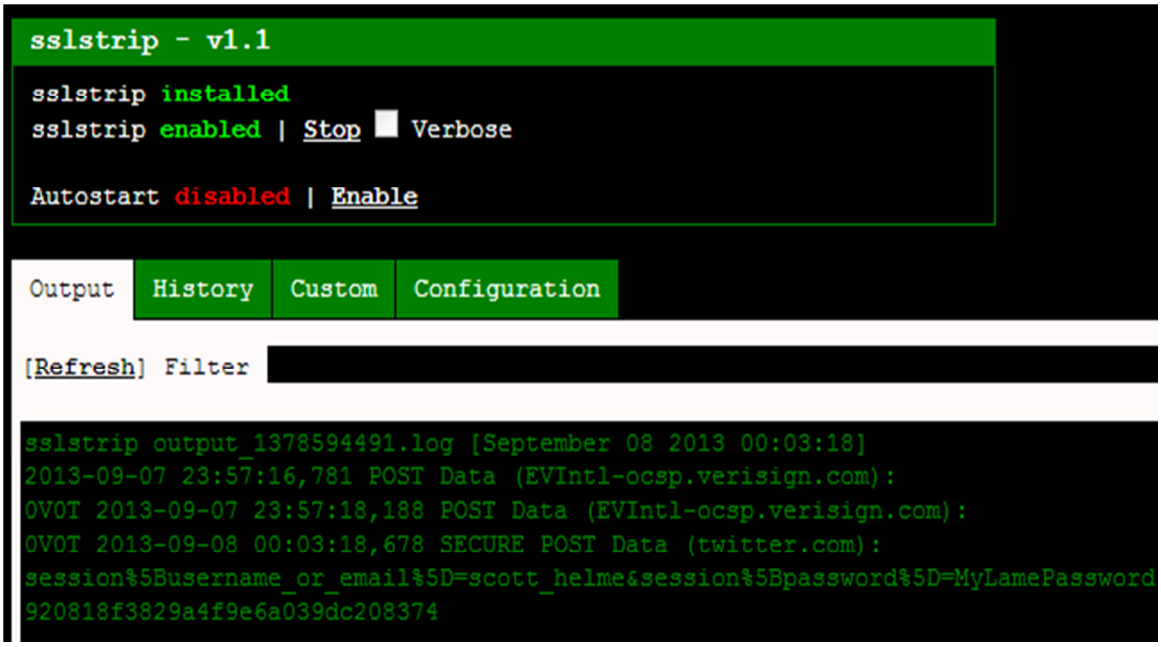
Miten helppoa tämä kaikki sitten loppujen lopuksi oikeasti on? Tässä kohtaa on hyvä mainita Pineapple Mark V, pieni laite, joka tekee kaiken oikeastaan automaattisesti, kun se on kerran asennettu. Mikä parasta, sen saa myös toimimaan akulla, joten sen voi heittää reppuun samalla kuin kiertelee ostoskeskuksessa.

Tässä laitteessa on kuitenkin yksi huomattava ero itse kannettavaan ja usb-modeemilla kalasteluun ja se on ohjelma nimeltä Karma. Karma tunnetaan myös nimellä yes-man. Tämä tulee siitä, että jokainen kannettava ja puhelin, jossa on langaton WLAN-yhteys, lähettävät kyselyitä tunnetuista tukiasemista. Yleisesti tukiasemat vastaavat näihin kyselyihin rehellisesti. Eli kun kannettava tietokone lähettää kyselyn, oletko lempikahvilani tukiasema, niin vastaus tulee rehellisesti, että en ole, tai mikäli kyseessä

on paikan X-tukiasema, niin vastaus on kyllä. Tällöin tietokone liittyy tukiasemaan automaattisesti. [24.]

Mitä Karma siis loppujen lopuksi tekee? Se yksinkertaisesti vastaa jokaiseen kyselyyn kyllä, mikä johtaa siihen, että se imaisee magneetin tapaan jokaisen langattoman laitteen sen kantoalueelta itseensä. [24.] Tämä tapahtuu kuitenkin vain, mikäli kyseiset laitteet eivät ole jo jossain langattomassa verkossa. Tämä toimii siis huonosti esimerkiksi kerrostalossa, mutta oletettavasti yllättävän tehokkaasti esimerkiksi kauppakeskuksessa. Mikäli tällaiseen laitteeseen tekee kloonisivustoja esimerkiksi Facebookista, Gmailista, Hotmailista ja sen ottaa kierrokselle kauppakeskukseen, jossa käy kymmeniä tuhansia ihmisiä päivittäin, on helppo ymmärtää laitteen vaarallisuus. Erityisesti kun nykypäivänä laitteen voi kytkeä nettitikulla verkkoon, jolloin uhrit eivät välttämättä huomaa käyttävänsä puhelimessa WLAN-verkkoa mobiilidatan sijasta. Useimmissa puhelimissa on vielä mahdollisesti päällä oletuksena WLAN-verkon käyttö mobiilidatan sijasta, jos se vain on saatavilla. Puhelimissa saattaa vielä olla oletuksena automaattinen sähköpostien haku tietyin väliajoin. Mikäli sähköpostit eivät tule salatusti, niin myös ne vuotavat laitteelle. Tämän tapaisen laitteen kalasteluilta on vaikea suojautua ja siksi pitääkin olla erittäin varovainen aina, kun annetaan arkaluontoista tietoa. VPN-suojaa kohtalaisen hyvin kannettavia, mutta puhelimissa se ei tiedettävästi kuitenkaan ole vielä tällä hetkellä yhtä kätevä suojautumismuoto. VPN:stä kerrotaan hiukan lisää luvussa 8.

Pineapple Mark V:n käyttöliittymä on hyvin yksinkertainen ja sitä hallinnoidaan pääosin verkkoliittymällä. Monet ohjelmista asentuvat suoraan yhdellä ainoalla hiiren napin painalluksella. Myös niiden päälle kytkeminen ja pois kytkeminen tapahtuu yhdestä napista. Laitteeseen saa yhdellä napin painalluksella asennetuksi SSLStrip-ohjelman, jota käsiteltiin luvussa 7.2 ja käytännössä kaikki verkkoliikenne, joka kulkee Pineapple-laitteen kautta, on monitoroitua. Laite tallentaa erityisesti kaiken POST-datan http-pyynnöistä, koska siellä ovat esimerkiksi käyttäjätiedot. [23.]



Kuva 19. Pineapple Mark V ja SSLStrip. [23]

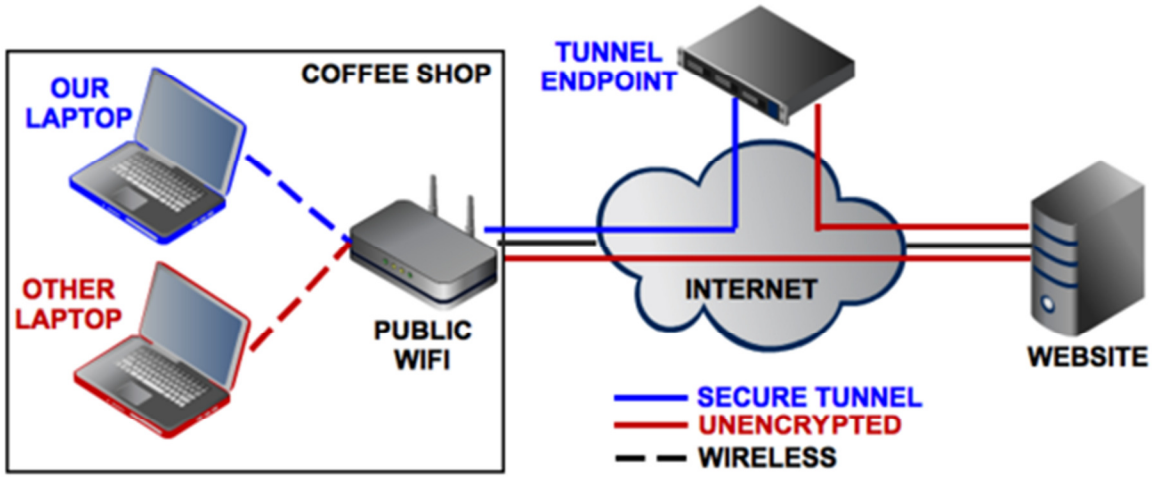
Kuva 19 on otettu Pineapple Mark V -laitteesta. Siitä näkee nopeasti, miten helppokäyttöinen Pineapple Mark V on. Kuvassa 19 SSLStrip on päällä, ja se tallentaa kaiken post-datan. Kuvasta 19 näkeekin, että Scott Helmen käyttäjätunnus ja salasana on tallentunut laitteeseen.

Pineapplen käyttö ei rajoitu pelkästään verkkoliikenteen monitorointiin vaan sillä voi myös pakottaa käyttäjät laitteen omistajan haluamalle verkkosivulle. Tällainen verkkosivu voi sisältää viruksia tai haitallista koodia. Mikäli tietokoneessa on jokin mahdollinen tietoturvaa heikentävä osio tai mahdollisesti jokin paikkaamaton tietoturva-aukko, niin hyökkääjä voi pahimmassa tapauksessa saada hallintaansa koko tietokoneen [25]. Hyökkääjä voi myös kloonata verkkosivuja ja huijata käyttäjää tällä tavoin luovuttamaan tietoa, mitä uhri ei välttämättä muuten luovuttaisi. Esimerkiksi mainittakoon verkkopankin sivut, jotka kysyvät varmistukseksi kolme seuraavaa pankki-avainta. Näillä roistot sitten voivat tyhjentää pankkitilin. [26.]

8 VPN

Julkisen avoimen verkon ollessa täysin turvaton on syytä käyttää jotakin salausmenetelmää. Yleisesti VPN (Virtual Private Network) on helppo ratkaisu suojata verkkoliikenne. VPN muodostaa suojatun tunnelin käyttäjän kannettavan ja VPN-serverin eli kohdekoneen välille. Näin kaikki verkkoliikenne, joka kulkee kannettavasta

suojaamattomasta verkosta internetin yli kohdekoneelle, on kryptattua. Ainoastaan tiedot, joita kohdekone hakee, kuten verkkosivut, eivät ole välttämättä kryptattuja. Tällä tosin ei ole niin suurta merkitystä. Mikäli esimerkiksi otat yhteyden VPN:llä kotikoneelle, on kotikoneen ja isp:n välinen verkko turvallinen. Ei siis haittaa vaikka tieto kotikoneen ja isp:n välillä kulkeekin ilman järeää salausta. Tärkeintä on, että tieto, joka kulkee julkisen langattoman verkon yli, on salattua. [27.] Kuva 20 selventää tilannetta hiukan.



Kuva 20. VPN:n toiminnan kuvaus julkisessa verkossa. [28]

Huomioitavaa on myös, että VPN PPTP (MS-CHAPv2) -yhteyden pystyy murtamaan helposti, joten syytä olisi käyttää parempaa VPN-protokollaa kuten OpenVPN:ää. [29] Tässä työssä ei käydä sen tarkemmin haavoittuvuutta läpi, koska se ei suoranaisesti aihepiiriin kuulu.

Toinen huomioitava asia on, että VPN-yhteyskään ei suojaa käyttäjää tietojen kalastelulta. Tietojen kalastelussa käyttäjä ohjataan hyökkääjän haluamalle verkkosivulle. Hyökkääjän ei siis tarvitse näissä tapauksissa nähdä verkkoliikennettä, vaan riittää, että käyttäjä itse syöttää esimerkiksi salasanansa hyökkääjän hallinnoimalle sivustolle. Siksi kirjautumiset olisi syytä jättää kokonaan tekemättä avoimissa langattomissa verkoissa. Myös dns-palvelin olisi syytä asettaa staattiseksi, jotta vältytään ”dns spoofing:ilta”. Dns spoofingissa huijataan käyttäjä kloonisivustolle. Esimerkiksi facebook.com ip -osoitteeksi voi olla host-tiedostossa annettu 127.0.0.1, mikä on hyökkääjän oma tietokone. Näin siis uhri hakee facebook.com-osoitteella sivuston hyökkääjän tietokoneelta ja mitä todennäköisimmin menettää käyttäjätunnustietonsa hyökkääjälle.

9 Päätelmät

Hyvin ja oikein suojattu langaton verkko WPA2-salauksella on kohtalaisen turvallinen vaihtoehto. Syytä on kuitenkin päivittää firmwarea ajoittain, jotta kaikki mahdolliset tietoturva-aukot tulevat säännöllisesti paikatuksi. Kuitenkin erityisesti WPS-haavoittuvuus osoittautui erittäin mittavaksi. Monet pienemmät yritykset voivat hyvinkin nojata WPA2-salaukseen ja mikäli WPS-toiminto on päällä ja tukiaseman firmware on jäänyt päivittämättä, voi tällä olla hyvinkin mittavia seurauksia. Tästä hyvä esimerkki oli luvussa 5.2 mainittu TJX-yrityksen tapaus, jossa WEP-verkko murrettiin ja tätä kautta päästiin käsiksi miljooniin luottokorttitietoihin. Tällainen tapaus voi hyvinkin olla mahdollista myös nykyisin.

WEP-salaus osoittautui odotusten mukaisesti hyvin heikoksi ja sitä ei tule käyttää missään olosuhteissa. Ainoa hyödyllinen käyttötarkoitus WEP-salaukselle tänä päivänä voisi olla käyttää sitä rikollisten metsästämiseen ja näiden käyttämien hyökkäystapojen tutkimiseen laboratorio-olosuhteissa. WEP-salaus on riittävän hyvä sikäli, että sinne ei voi mennä vahingossa. WEP-salaus on riittävä pitämään naapurin mummon poissa tukiasemasta tai kenet tahansa rehellisen käyttäjän.

Langattomien verkkojen häiriöalttius on niiden huomattavin heikkous. Käytännössä yhdellä kannettavalla ja WLAN-kortilla voi estää kaiken langattoman verkkoliikenteen alueella loputtoman ajanjakson ajan. Tämä perustuu ihan puhtaasti deautentikointi-pakettien lähettämiseen jokaiselle alueen tukiasemalla aina uudestaan ja uudestaan. Kyseessä on erittäin suuri heikkous juuri toiminnan saralla ja nykyaikana pitäisi olla parempia menetelmiä varmistaa verkon toimivuus. Käytännössä siis yritys, joka nojaa liian paljon langattoman verkon toimintaan on hyvin altis verkkoliikenteen häirinnälle. Pahimmassa tapauksessa koko verkkoliikenne voi olla lamautettuna ja tästä syntyvät kustannukset voivat olla mittavia. Mielestäni onkin siis tärkeä varmistaa, että yrityksen liiketoiminta voi jatkua ongelmitta myös silloin, kun langaton verkko on poissa käytöstä.

Työssä tuli myös erittäin hyvin ilmi hyvän salasanan merkitys. Käytännössä huono salasana on WPA2:n suurin heikkous heti WPS:n jälkeen. Hyvän salasanan merkitystä ei voida vähätellä etenkään yritysmaailmassa. Huono WPA2-salasana tai minkä tahansa elintärkeän palvelun salasana voi johtaa merkittäviin taloudellisiin tappioihin. Myös imagotappio voi olla hyvinkin merkittävä.

Myös käyttäjäpuolen hyökkäykset yllättivät. Suljetut tukiasemat vahvalla salauksella ja uusimmilla firmware-päivityksillä ovat turvallisia. Sen sijaan avoimet langattomat verkot ovat hyvinkin vaarallisia. Juuri verkkohäirintä ja langattoman verkon helppo nimeäminen osaltaan yllättivät lähinnä sillä, että ostoskeskuksen McDonaldsin WLAN-verkko ei välttämättä olekaan McDonaldsin WLAN-verkko. Kuinka moni verkkoa käyttävistä asiakkaista sitten edes ajattelee koko asiaa? Tuskin kovin moni, joten tällainen hyökkäys on erittäin helppo toteuttaa. Varsinkin kun ostoskeskuksissa liikkuu tuhansia ihmisiä, niin massoihin kohdistuvat hyökkäykset ovat erittäin vaarallisia. Niillä saadaan nopeasti erittäin paljon kerättyä tietoa kasaan. Esimerkiksi Facebook-salasanalla voidaan lähettää viruksia, jotka avaavat yhteyden käyttäjien kotikoneille. Myös onnistumisprosentti on suuri, koska kukapa ei avaisi tiedostoa, joka sattuu tulemaan parhaalta kaverilta? Sähköpostin salasanalla voidaan saada hyvinkin arkaluonteista asiaa selville. Myös monien paikkojen salasanojen resetointi onnistuu juuri sähköpostin avulla. Salakuuntelua voidaan hyvin ehkäistä esimerkiksi VPN-yhteyttä käyttämällä, mutta juuri tuon takia tämän tapaiset hyökkäykset kohdistuvat massoihin. Jos 100 henkilöä 1000 käyttää VPN:ää, niin jäljelle jää silti vielä 900 mahdollista uhria.

Erityisesti laitteet kuten Pineapple Mark V tekevät näistä hyökkäyksistä niin helppoja ja vaarallisia. Pineapplen Karma kerää automaattisesti kaikki laitteet alueelta, jotka ovat kykeneväisiä WLAN-yhteyteen ja joiden muistissa on jokin avoin langaton verkko. Koska suurin osa ihmisistä, jotka liikkuvat ostoskeskuksissa ei ole liittyneitä mihinkään langattomaan verkkoon, saa Pineapple nopeasti kerätyksi erittäin paljon laitteita itseensä. Luku 7.3 perustuu pitkälti Scott Helmen testeihin. Tämä johtui siitä, että tämän kaltaista laitetta ei ollut mahdollista testata laillisesti. Luvussa 7.3 läpikäyty operaatio olisi vaatinut paremmat laboratorio-olosuhteet, jotta sivulliset eivät päätyisi Pineapple-laitteen uhreiksi.

Koska suurin osa ihmisistä ei ole kovin teknisiä ja luottaa sokeasti tukiasemien nimiin ja turvallisuuteen voidaan sanoa, että käyttäjiin kohdistuvat hyökkäykset ovat erittäin vaarallisia ja niiden onnistumisprosentti on varmasti hyvinkin suuri. Tässä työssä ehkä suurimman yllätyksen toikin juuri avoimien tukiasemien vaarallisuus ja niiden väärinkäyttämisen helppous.

Kaiken kaikkiaan WLAN-verkkojen testaus oli kattava. Käyttäjäpuolen hyökkäysten testaamiseen olisi voinut käyttää enemmän aikaa, mutta WLAN-verkkojen tietoturvan

testaaminen ja tutkiminen vei suurimman osan ajasta. Lisäksi käyttäjäpuolen heikkouksien testaaminen on hiukan vaikeaa ilman, että syyllistyisi laittomuuksiin. Esimerkiksi Karmaa ei voinut kytkeä päälle kerrostalossa, koska mahdollisesti olisi saatu siihen osa naapurien laitteista ja tätä kautta olisi varmaan syyllistytty jo jonkin sortin väärinkäyttöön. Tämän takia käyttäjäpuolen hyökkäysten testaus jäi puhtaasti teoreettiseksi.

Lähteet

1 WiFi Pineapple Mark V Standard. HakShop. <https://hakshop.myshopify.com/products/wifi-pineapple>. Luettu 15.2.2014.

2 Langattomat verkot Suomessa. Wikipedia. <http://fi.wikipedia.org/wiki/Langattomat_verkot_Suomessa>. Luettu 21.2.2014.

3 Cache, J., Wright J. & Liu V. 2010. Hacking Exposed Wireless 2nd.

4 IEEE 802.11. Wikipedia. <http://fi.wikipedia.org/wiki/IEEE_802.11>. Luettu 20.3.2014.

5 WLAN. 2014. Wikipedia. <http://fi.wikipedia.org/wiki/WLAN>. Luettu 11.3.2014.

6 Ohje 2/2011 Langattomien verkkojen tietoturvasta. 2011. Verkkodokumentti. Viestintävirasto. <http://www.cert.fi/ohjeet/2011_23/ohje-2011-02.html>. Luettu 14.3.2014.

7 WEP. Wikipedia. <http://fi.wikipedia.org/wiki/WEP>. Luettu 27.3.2014.

8 Haines, Brad. 2010. Seven deadliest wireless technologies attack. Syngress Publishing, Inc.

9 Cracking WEP with Kali Linux tutorial (Verbal step by step). 2013. YouTube. <http://www.youtube.com/watch?v=RydsjNhUjdg>. Katsottu 18.2.2014.

10 Earle, Aaron E. 2005. Wireless security handbook. Auerbach Publications. S. 208

11 Praphul, C., Bensky, D., Bradley, T. and Hurley, C. 2011. Wireless Security: Know It All. Newnes. S. 650

12 Zhang, Y., Zheng, J. & Ma, M. 2008. Handbook of Research on Wireless Security. IGI Global. Nide 1, s. 762.

13 Temporal Key Integrity Protocol. Wikipedia. <http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#Beck-Tews_attack>.

14 Practical Verification of WPA-TKIP Vulnerabilities. Verkkodokumentti. <https://lirias.kuleuven.be/bitstream/123456789/401042/1/wpatkip.pdf>. Luettu 3.4.2014.

15 Shem, Mike. 2012. Hacking Web Apps: Detecting and Preventing Web Application Security Problems. Syngress Publishing, Inc. S. 157.

16 Beaver, Kevin. 2013. Hacking for dummies. John Wiley & Sons, Inc. 4th edition, s.170-171.

17 Tietoturva nyt! 2012. Viestintävirasto. <https://www.cert.fi/tietoturvanyt/2012/01/ttn201201041606.html>. Luettu 11.3.2014.

18 Hi-Tech Heist: How Hi-Tech Thieves Stole Millions Of Customer Financial Records. 2007. >http://www.cbsnews.com/news/hi-tech-heist/>. Luettu 19.3.2014.

19 Kysymykset: Montako sanaa on suomen kielessä? 2009. Helsingin kaupunginkirjasto. <http://www.kysy.fi/kysymys/montako-sanaa-suomen-kielessa>. Luettu 19.3.2014.

20 oclhashcat. 2014. <http://hashcat.net/oclhashcat/>. Luettu 21.3.2014.

21 Hakin9 magazine. 2013. Nro 04.

22 Brief Analysis of RockYou Passwords. 2012. Passcape Software. <http://www.passcape.com/index.php?section=blog&cmd=details&id=17>. Luettu 11.3.2014.

23 The WiFi Pineapple – Using Karma and SSLstrip to MiTM secure connections. 2013. Scott Helme. <https://scotthelme.co.uk/wifi-pineapple-karma-sslstrip/>. Luettu 11.4.2014.

24 How To: Use KARMA On the WiFi Pineapple Mk IV. 2013. YouTube. < http://www.youtube.com/watch?v=avJfT9JyiiM>. Katsottu 28.2.2014.

25 How To: WiFi Pineapple Captive Portal Setup (Evil Portal & NoDogSplash). 2013. YouTube. <http://www.youtube.com/watch?v=nw4bo4rXGgQ>. Katsottu 28.2.2014.

26 The WiFi Pineapple – Using Karma and DNSspoof to snag unsuspecting victims. 2013. Scott Helme. <https://scotthelme.co.uk/wifi-pineapple-karma-dnsspoof/>. Luettu 3.3.2014.

27 How (and why) to set up a VPN today. 2013. PCWord. <http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html>. Luettu 12.3.2014.

28 Divide and Conquer: Cracking MS-CHAPv2 with a 100% success rate. 2012. <https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/>. Luettu 17.3.2014.