LANGATTOMAN VERKON TIETOTURVA

Toni Lahtinen

Opinnäytetyö
Huhtikuu 2015
Tietotekniikka
Tietoliikennetekniikka

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

LAHTINEN, TONI:
Langattoman verkon tietoturva

Opinnäytetyö 30 sivua
Huhtikuu 2015

WLAN-verkot ovat yleistyneet viimeisen 15 vuoden aikana. Niitä on esimerkiksi yrityskäytössä sekä kotitalouksissa. Tässä opinnäytetyössä perehdytään langattoman verkon tekniikkaan, yleiseen tietoturvaan, ohjelmistoihin, muutamiin hyökkäyksiin sekä miten näitä hyökkäyksiä vastaan puolustaudutaan.

Langattomien verkkojen Wi-Fi-standardin kehitti IEEE (Institute of Electrical and Electronics Engineers). Ensimmäinen oli 802.11-standardi, jota kehitetään edelleen. Uusin versio on 802.11ac-standardi joka julkaistiin vuonna 2013. Ensimmäiset standardit toimivat joko 2,4 GHz:n tai 5 GHz:n taajuudella, mutta 802.11ac käyttää molempia. 802.11ac mahdollistaa maksimisiirtonopeuden 900 Mbit/s.

Tietoturva on tärkeä osa verkkoa. Avoimien verkkojen liikennettä ei ole salattu, joka altistaa käyttäjän vakavalle tietovarkaudelle. Kotikäytössä on tärkeää käyttää WPA2-salausta monimutkaisella salasanalla, jotta saavutetaan paras mahdollinen tietoturva.

Kali Linux on ammattilaisten käyttämä Linux-distro, joka tarjoaa yli 100 työkalua penetraatiotestaukseen. Yritysten on tärkeätä suorittaa verkontietoturvatestaus, jotta paikannetaan mahdolliset aukot. Huono tietoturva mahdollistaa tärkeiden tietojen menettämisen, joka puolestaan saattaa maksaa yritykselle miljoonia euroja. Kali Linux sisältää aircrack-ng-ohjelmiston, jolla voidaan testata langattoman verkon tietoturvaa. Aircrack-ng mahdollistaa datan kaappaamisen, salasanojen murron sekä datan injektoinnin liikenteeseen.

Työssä perehdytään mahdollisiin hyökkäyksiin. Mahdollisia hyökkäyksiä on suunnaton määrä, ja tästä johtuen työssä keskitytään niistä kolmeen. Man in the Middle –hyökkäys on näistä vaarallisin. Hyökkääjä sijoittautuu uhrin ja palvelimen väliin, jolloin kaikki data liikkuu hyökkääjän kautta. Tämä mahdollistaa datan kuuntelun ja sen muokkaamisen. Denial of Service –hyökkäys yrittää estää uhrin WLAN-verkon toimivuuden. Tämä tapahtuu kuormittamalla tukiasemaa eri pyynnöillä, esimerkiksi de-autentikointi-pyynnöllä. Rogue Access Point –hyökkäyksessä hyökkääjä toimittaa oman tukiasemansa kohteeseen ja yhdistää sen uhrin verkkoon, tai käyttää luvatonta tukiasemaa, jonka tietämätön työntekijä on asentanut.

Asiasanat: wi-fi, ieee 802.11, wlan, langaton verkko, tietoturva

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree programme in ICT Engineering
Telecommunications

LAHTINEN, TONI:
Security of Wireless Networks

Bachelor's thesis 30 pages
April 2015

Wireless networks have become more common in the last 15 years, for example they are used by corporations as well as households. In this bachelor's thesis we will focus on wireless technology, wireless network security, attacks and how to defend against these attacks.

Wi-Fi-standard was developed by IEEE (Institute of Electrical and Electronics Engineers). First version was the 802.11-standard, which is still being developed. Newest version is the 802.11ac-standard which was published in the year 2013. The first versions of 802.11-standards worked either on 2,4 GHz or 5 GHz frequencies, but the 802.11ac uses both. 802.11ac enables a maximum transfer rate of 900 Mbit/s.

Network security is very important. An open network doesn't encrypt the data which opens up the user for serious threats, data theft for example. Households should use WPA2-encryption with a complex password for the best security.

Kali Linux is a Linux-distribution used by professional penetration testers. It offers over a 100 tools for various uses from penetration testing to digital forensics. It is important for corporations to do penetration testing, so they can block the security holes. Bad network security enables the attacker to steal information which in turn could cause losses of millions of dollars for the company. Kali Linux offers the air-crack-ng-software suite, specifically made for testing the security of wireless networks. Aircrack-ng can capture data, break passwords and inject packets into the data traffic.

We will take a look at some possible attacks made against a wireless network. There are a huge amount of possible attacks, but we will take a look at three of them. Man in the Middle –attack is the most dangerous out of the three. The attacker places him/herself between the victim and the server. This causes him to be in control of all the data, which he can either listen to or modify it. Denial of Service –attack tries to block the victims Wi-Fi-network, making him unable to use it. This is done by loading the Access Point with for example de-authentication requests. Rogue Access Point –attack the attacker will bring his own AP and connect it into the corporations network or use an unauthorized AP, which has already been installed in the network, most commonly by an uninformed employee.

Key words: wi-fi, ieee 802.11, wlan, wireless network, security

SISÄLLYS

LYHENTEET JA TERMIT

AP	Access Point, langaton tukiasema
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol, salausprotokolla, korvaa TKIP:n, kuuluu 802.11i-standardiin
DoS	Denial of Service, palvelunestohyökkäys, jolla pyritään estämään palvelun (esim. Wi-Fi) käyttö
GPS	Global Positioning System, paikallistamisjärjestelmä
HTTP	Hypertext Transfer Protocol, tiedonsiirto protokolla
IEEE	Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö
IP	Internet Protocol, TCP/IP-mallin Internet-kerroksen protokolla
IV	Initialization Vector, alustusvektori, lähetetään aina paketin otsaketiedoissa salaamattomana, jotta vastaanottaja voi purkaa paketin sisällön
Linux	Käyttöjärjestelmä
MAC	Media Access Control, verkkokortin uniikki osoite
MIMO	Multiple-Input and Multiple-Output, moniantennitekniikka
MitM	Man in the Middle, tietoturvahyökkäys, jossa hyökkääjä asettuu kahden osapuolen välisen tietoliikenteen välittäjäksi ja halutessaan muuttaa viestien sisältöä
NIC	Network Interface Controller, verkkokortti
PSK	Pre-shared Key, tukiasemaan liittyessä käytettävä ennalta määritelty salasana
QAM	Quadrature Amplitude Modulation, modulointitekniikka
SSID	Service Set Identifier, langattoman tukiaseman verkkotunnus
TKIP	Temporal Key Integrity Protocol, tietoturvaprotokolla, kehitettiin WEP-protokollan tilalle salaamaan yhteydet
USB	Universal Serial Bus, sarjaväyläarkkitehtuuri
VOIP	Voice Over Internet Protocol, tekniikka, jossa ääni kuljetetaan IP:n kautta

WEP	Wired Equivalent Privacy, ensimmäinen laitteen ja tukiaseman tietoliikennettä suojaamaan kehitetty salausmenetelmä
WLAN	Wireless Local Area Network, langaton lähiverkko
WPA	Wi-Fi Protected Access, tietoturvatekniikka, joka kehitettiin WEP-salauksen ongelmien paljastuttua sen korvaajaksi
WPS	Wi-Fi Protected Setup, verkon tietoturvastandardi, tarkoituksena helpottaa laitteiden liittämistä salattuihin langattomiin verkkoihin

1 JOHDANTO

Langattomat verkot ovat yleistyneet viimeisten viidentoista vuoden aikana räjähdysmäisesti. Yritykset ja yksityishenkilöt ovat huomanneet sen tarjoamat edut, joita ovat muun muassa helppokäyttöisyys, hinta sekä liikkuvuus. Usein käyttäjiltä jää tietoturva huomioimatta, joka saattaa aiheuttaa mittavat taloudelliset sekä henkilökohtaiset vahingot.

Turvattomia langattomia verkkoja on käytetty esimerkiksi pankkiryöstöissä sekä varastettaessa valtion salaisuuksia. Tässä opinnäytetyössä esitellään langattoman verkon teknologiaa, tietoturvauhkia sekä ammattilaisten käyttämiä tietoturvan testaamiseen tarkoitettuja työkaluja.

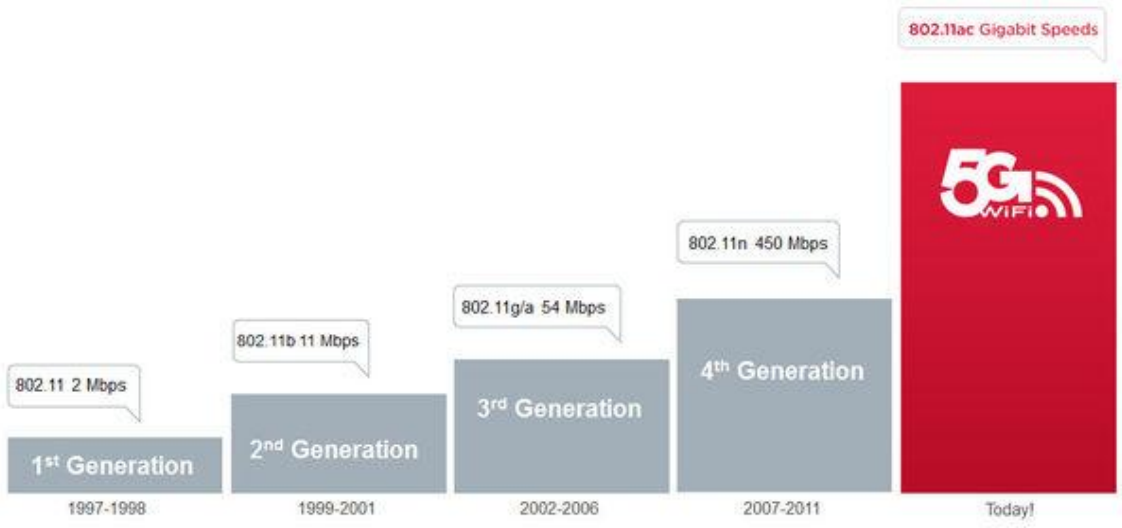
Työ aloitetaan langattomien verkkojen esittelyllä; mistä kaikki sai alkunsa ja kuinka teknologia on kehittynyt. Seuraavaksi otetaan katsaus yleisiin tietoturvastandardeihin sekä langattomaan verkon teknologiaan. Viimeisenä esitellään ammattilaisten käyttämät työkalut ja tarkastellaan, kuinka muutamia niistä käytetään.

2 LANGATTOMAT VERKOT

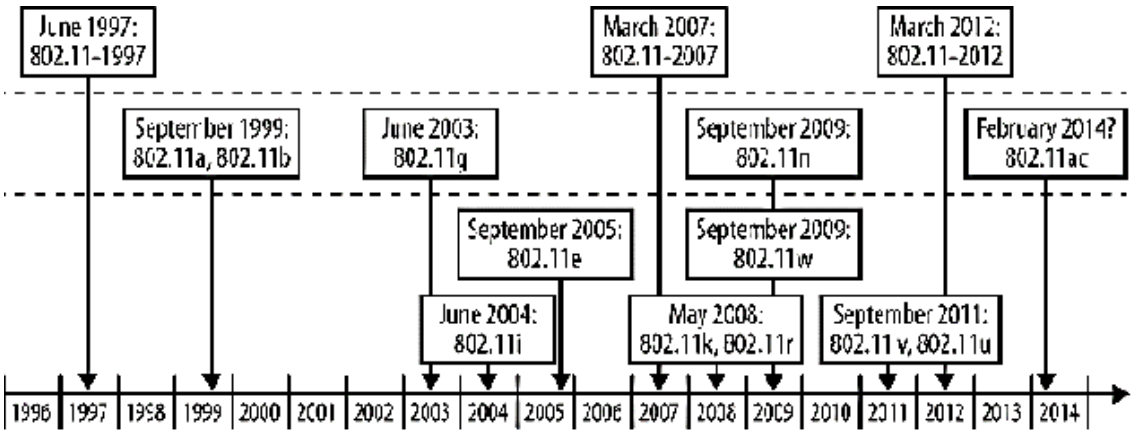
Langaton verkko tunnetaan myös WLAN:ina, joka tulee sanoista ”Wireless Local Area Network.” Kyseessä on teknologia, millä poistetaan tarve kaapelointiin, sen sijaan käytetään radioaaltoja, joilla yhdistetään laite haluttuun verkkoon.

2.1 Standardit

Ensimmäinen WLAN-standardi oli 802.11. Se toimii ainoastaan 2 Mbit/s:n siirtonopeudella, joka todettiin pian liian hitaaksi. Sitä kehitettiin edelleen, ja siitä syntyivät päivitetyt WLAN-standardit. Langattomat verkot käyttävät 2,4 GHz:n ja 5 GHz:n taajuusalueita. 2,4 GHz:n alue alkaa 2,4 GHz:sta ja päättyy 2,485 GHz:iin. Taajuusalueen leveys on siis 85 MHz. 5 GHz:n taajuusalue on lajiteltu kahteen kaistaan. Nämä ovat 5,15 – 5,35 GHz (200 MHz) ja 5,725 – 5,825 GHz (100 MHz).



KUVA 1. 802.11-standardien tiedonsiirtonopeudet (lifehacker.com)



KUVA 2. Wi-Fi-standardien julkaisut (802.11ac: A Survival Guide, chapter 1)

2.1.1 802.11b

IEEE julkaisi 802.11b-standardin vuonna 1999, jossa maksimitiedonsiirtonopeus oli 11 Mbit/s. 802.11b käyttää 2,4 GHz:n taajuusaluetta. Standardin etu on sen laaja kantama, joka saattaa olla jopa 100 metriä. Tämä vähentää tarvittavien tukiasemien määrää. [7.]

2.1.2 802.11a

802.11a julkaistiin samaan aikaan 802.11b:n kanssa. 802.11a käyttää 5 GHz:n taajuutta ja mahdollistaa tiedonsiirron nopeudella 54 Mbit/s. Korkeammasta taajuudesta johtuen 802.11a:n kantama on pienempi kuin b:llä. Signaali ei myöskään läpäise esteitä yhtä hyvin kuin alemman taajuuden 802.11b. Nämä ominaisuudet tekivät 802.11a:sta paremman yrityskäyttöön. [7.]

2.1.3 802.11g

Vuonna 2003 langattomissa laitteissa alettiin käyttää uutta standardia 802.11g, joka yritti yhdistää parhaat ominaisuudet 802.11a:sta sekä 802.11b:stä. 802.11g saavutti tiedonsiirtonopeuden 54 Mbit/s samaan aikaan käyttämällä 2,4 GHz:n taajuutta. [7.]

2.1.4 802.11n

Standardi 802.11n suunniteltiin parantamaan 802.11g-standardia entisestään. Sen tavoitteena oli parantaa tiedonsiirtonopeuksia huomattavasti. Tähän pyrittiin käyttämällä MIMO–teknologiaa. 802.11n-standardilla on mahdollista tavoittaa jopa 600 Mbit/s tiedonsiirtonopeus. MIMO–tekniikalla yhdistettiin kaksi 20 MHz:n kanavaa yhdeksi 40 MHz:n kanavaksi. Kaistanleveyden kasvaminen mahdollistaa suuremman tiedonsiirtonopeuden. [7.]

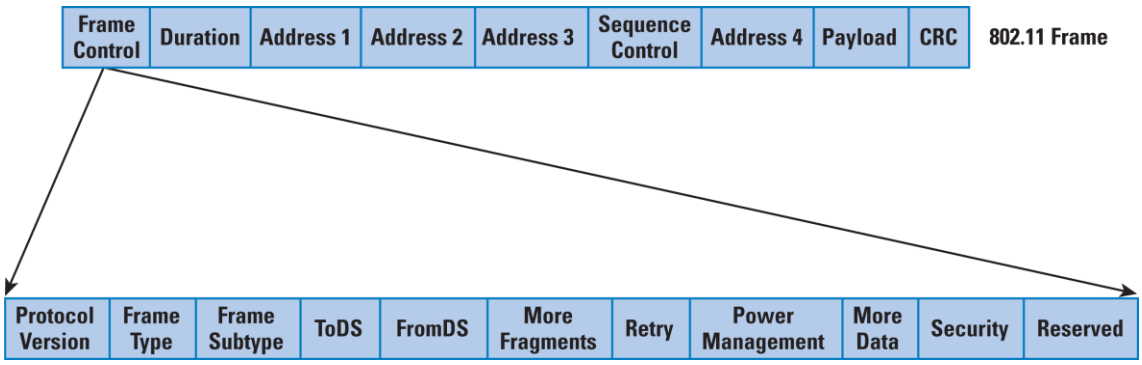
2.1.5 802.11ac

Uusin IEEE:n luoma Wi-Fi-standardi on 802.11ac. Se pyrkii suurempaan nopeuteen yhdistämällä useita kanavia, jolla saavutetaan 80 MHz:n sekä 160 MHz:n kaistanleveys. 802.11ac käyttää 256 QAM -modulaatiota (Quadrature Amplitude Modulation) kun 802.11n käytti 64 QAM -modulaatiota. Tällä saavutettiin 33 % kasvu maksimi-tiedonsiirtonopeudessa. 802.11ac käyttää myös 802.11n:n tapaan MIMO-tekniikkaa. [5.]

2.2 WLAN-kehykset

Langattomissa verkoissa laitteet kommunikoivat kehyksillä. Kuvassa 3 on esitetty WLAN-kehyksen rakenne. Kehyksen ohjauskenttä (Frame Control) on esitetty kuvan 3 alaosassa ja se koostuu kuvan mukaisesti useista kentistä. Tyyppi–kenttä (Frame Type) määrittää WLAN-kehyksen tyypin, jolle on kolme mahdollisuutta:

1. hallintakehys, jonka tehtävänä on ylläpitää yhteys AP:in (Access Point) ja langattoman laitteen välillä
2. ohjauskehys, helpottaa datakehyksen lähettämistä, järjestää kanavan, sisältää vain otsikkotietoja
3. datakehys, joka kuljettaa varsinaisen datan langattomassa verkossa. [1.]



KUVA 3. WLAN-kehys ylhäällä, Frame Control –kenttä alhaalla (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_11-4/114_wifi.html)

Frame Control –kenttä sisältää seuraavat ohjausbittikentät: [9.]

- Protocol Version: Määrittää protokollan version (2 bit)
- Frame Type: Hallinta-, ohjaus- tai data-kehys (2 bit)
- Frame Subtype: Frame Typen lisäksi erottelee, ilmaisemalla mihin kategoriaan sanoma kuuluu (4 bit)
- ToDS: Ilmoittaa, onko data matkalla tukiasemalle (1 bit)
- FromDS: Kertoo, onko data tulossa tukiasemalta (1 bit)
- More Fragments: On päällä, jos seuraavan kehyksen MSDU (MAC Service Data Unit) sisältää samoja fragmentteja (1 bit)
- Retry: On päällä, jos kehys on uusintalähetys (1 bit)
- Power Management: On päällä, jos laite menee virransäästötilaan kehyksen lähettämisen jälkeen (sammuttaa lähetin ominaisuuksia), tällöin AP puskuroi valmiiksi laitteen kehykset (1 bit)
- More Data: Päällä jos laite menee virransäästötilaan ja AP:lla on ainakin yksi puskuroitu kehys (1 bit)
- WEP/Security: Onko sanoma salattu. (1 bit)

3 TIETOTURVA

Langattomien verkkojen tietoturva on elintärkeää, koska viestisignaalit kulkevat ilmassa, ja ne ovat kaikkien tavoitettavissa alueella, jossa verkko toimii. Käyttäjien ja yritysten jotka käyttävät langattomia verkkoja, on oltava tietoisia mahdollisista ongelmista ja uhista. Tässä luvussa perehdytään yleisiin langattomien verkkojen suojauskeinoihin. Paras tietoturva langattomassa verkossa saavutetaan yhdistelemällä eri tekniikoita. [8.]

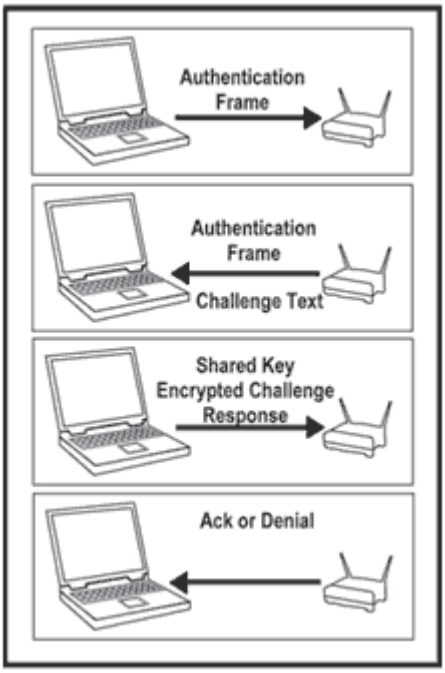
3.1 Piilotettu SSID

Yleisin keino, jolla verkkoa yritetään suojata, on käyttää piilotettua SSID:tä (Service Set Identifier). Normaalisti AP lähettää tiedon itsestään, mutta kun SSID on piilotettu, täytyy se tietää etukäteen, jotta verkkoon voi liittyä. Käytännössä hyökkääjän täytyy vain kuunnella verkkoliikennettä, ja heti kun yksikin laite liittyy AP:iin, saa hyökkääjä piilotetun SSID:n tietoonsa. Piilotettu SSID on hyvä alkukeino verkon puolustamiseen, mutta muitakin tietoturvakeinoja pitää käyttää. [4.]

3.2 WEP

WEP (Wired Equivalent Privacy) on IEEE:n luoma ensimmäinen 802.11-tietoturvaprotokolla. Kuvasta 4 nähdään WEP:n autentikaatiotapa:

1. Laite lähettää autentikaatiopyynnön AP:ille
2. AP vastaa lähettämällä salaamattoman viestin
3. Laite jatkaa vastaamalla AP:ille sen lähettämän viestin salattuna käyttämällä ennalta määritettyä salausavainta
4. AP purkaa laitteen lähettämän viestin ja vertaa sitä alkuperäiseen viestiin. Riippuen siitä, vastaako se alkuperäistä, AP joko hyväksyy laitteen verkkoon tai hylkää sen.



KUVA 4. WEP-kättely

WEP on tietoturvatasoltaan heikoin salaus, sen saa aina murrettua, oli salasana kuinka pitkä ja monimutkainen tahansa. Tämä johtuu protokollan suunnitteluvirheestä. WEP nimittäin lähettää IV:t (Initialization Vector) salaamattomina jokaisessa kehyksessä. Jos hyökkääjä kerää tarpeeksi IV:ta, voi salasanan murtaa. [3.]

3.3 WPA ja WPA2

WPA (Wi-Fi Protected Access) on tekniikka, joka kehitettiin WEP–salauksen murtamisen jälkeen sen korvaajaksi. WPA-tekniikka julkaistiin 2003 ja turvallisempi versio WPA2 vuonna 2004. WPA käyttää TKIP:ia (Temporal Key Integrity Protocol), jota myös WEP käyttää. Tämä protokolla on mahdollista murtaa ja sallii hyökkääjän injektoida JavaScriptiä uhrin liikenteeseen. WPA2 korvasi TKIP:lan CCMP:lla (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). CCMP on paljon turvallisempi TKIP:iin verrattuna ja se on uusi WPA2:n standardisuojaus. Peruskäyttäjän kannattaa huolehtia, että PSK on mahdollisimman monimutkainen, sillä WPA2:n ainut heikkous on huono salasana. [3.]

3.4 WPS

Wi-Fi Alliance esitteli WPS:in (Wi-Fi Protected Setup) vuonna 2006 helppona salausvaihtoehtona. Käyttäjän ei tarvitse muistaa pitkiä salasanoja. Suuressa osassa langattomia reitittimiä WPS on automaattisesti päällä. Reitittimissä oli PIN–koodi, joka käyttäjän piti syöttää halutessaan yhdistää verkkoon. Toinen vaihtoehto on ’Push button method’, jossa täytyy painaa reitittimen WPS–nappia sekä laitteen nappia, jotta yhteys muodostuu. [2.]

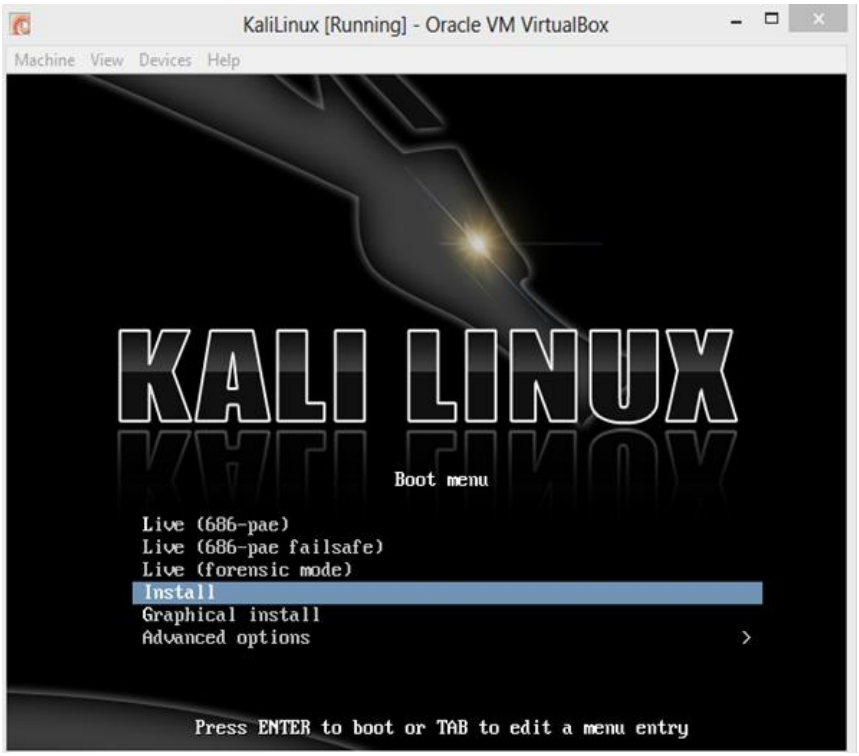
Vuonna 2011 paljastettiin, että WPS sisältää tietoturva-aukon. Oli mahdollista ’bruteforce’ –hyökkäyksellä saada WPS-PIN ja sitä kautta WPA/WPA2-PSK, josta seurasi täysi pääsy uhrin verkkoon. Tästä syystä käyttäjiä suositellaan poistamaan WPS käytöstä.

3.5 MAC–suodatin

MAC–osoite (Media Access Control) on jokaiseen verkkokorttiin kirjoitettu osoite, joka koostuu kuudesta kaksinumeroisesta heksadesimaaliluvusta. Jokaisella laitevalmistajalla on oma etuliitteensä MAC–osoitteessa, ja loppuosa sarjasta on satunnaisesti tehty. MAC–suodatus perustuu reitittimeen syötettävään listaan, johon lisätään sallitut MAC–osoitteet, joille halutaan antaa pääsy verkkoon. Hyökkääjän on kuitenkin mahdollista saada sallitun laitteen MAC–osoite ja vaihtaa se omalle laitteelleen, joten lisäturvatoimia tarvitaan, jos halutaan turvallinen verkko.

4 KALI LINUX

Kali Linuxin ovat kehittäneet Mati Aharoni sekä Devon Kearns, jotka työskentelevät Offensive Security:lle. Kali Linux on rakennettu Debianin pohjalle ja se on tarkoitettu verkkojen penetraatiotestaukseen sekä digitaalisen tutkintaan. Sen edeltäjänä toimi BackTrack Linux. Kalista on mahdollista asentaa kiintolevylle pysyvä käyttöjärjestelmä virtuaalisesti sekä USB–tikulle live-versio. USB–versiota voi muokata halutessaan niin, että sille tehdyt muutokset tallentuvat, muuten se palaa aina alkuperäiseen image–muotoon.

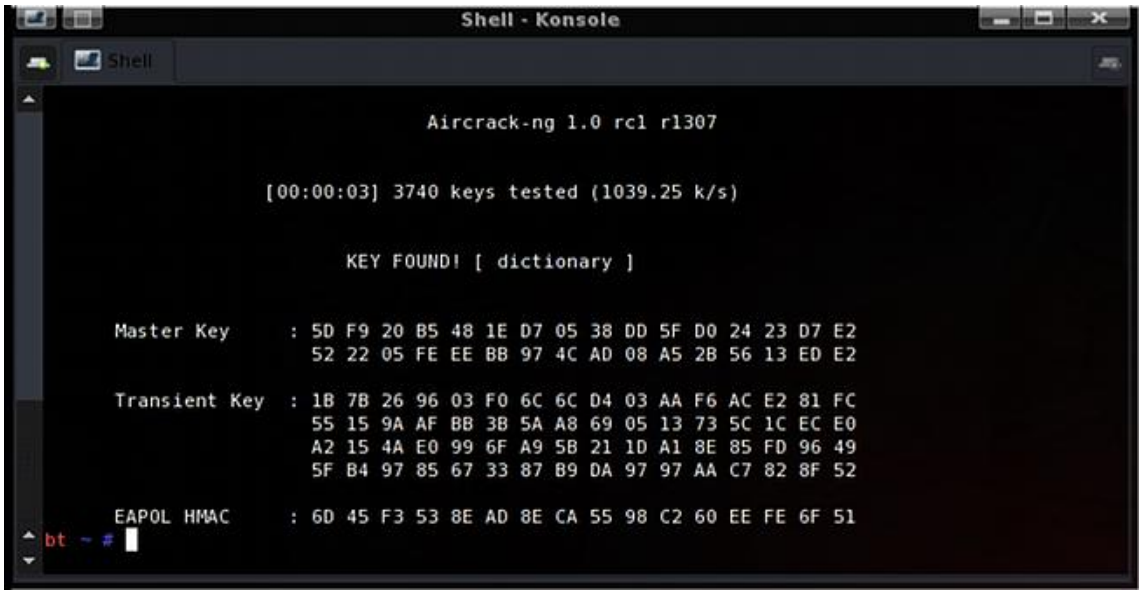


KUVA 5. Kali Linux -asennus (techwikasta.com)

Kali Linuxissa itsessään on automaattisesti yli 100 työkalua. Käyttäjän on mahdollista ladata niitä useita satoja lisää. Työkalut on kategorisoitu järkevästi. Sama työkalu löytyy useiden kategorioiden alta. Tässä kappaleessa esitellään suosituimpia sekä parhaita työkaluja, jotka Kali Linux sisältää.

4.1 Aircrack-ng

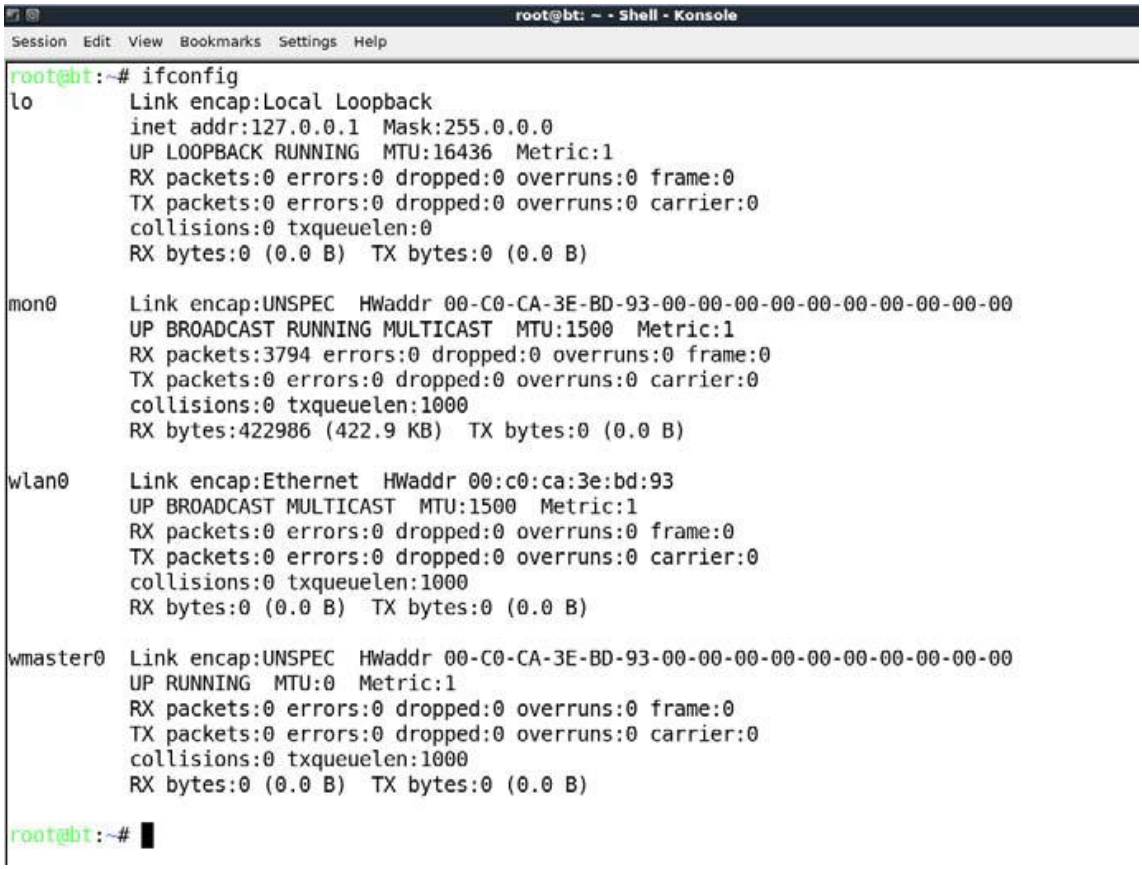
Aircrack-ng on 802.11–standardien WEP/WPA/WPA2-PSK–avainten murtamisohjelma. Tämä ohjelma pystyy murtamaan minkä tahansa WEP–avaimen, kunhan se saa tarpeeksi dataa (datan luomiseen käytetään aireplay-ng:tä). WPA/WPA2-PSK–avaimen voi murtaa käyttämällä salasanalistaa ja ’brute force’ -tekniikkaa, joka kokeilee listan jokaista salasanaa.



KUVA 6. Aircrack-ng on ratkaissut avaimen (http://null-byte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893/)

4.2 Airmon-ng

Tätä työkalua käytetään useissa hyökkäyksissä. Sillä laitetaan langaton verkkokortti monitorointimoodiin. Konsoliin kirjoitetaan ’ifconfig’, jolloin nähdään verkkorajapinnat. Langaton verkkokortti on yleensä wlan0, ellei laitteessa ole niitä useita, jolloin numerointi tapahtuu wlan0 – wlan99. Komento ’airmon-ng’ luo uuden rajapinnan mon0, jota käytetään langattomien pakettien haisteluun ilmasta. Tämä tarkoittaa sitä, että tällä työkalulla saadaan talteen kaikki data, mikä ilmassa liikkuu, alueen AP:it ja muut laitteet.

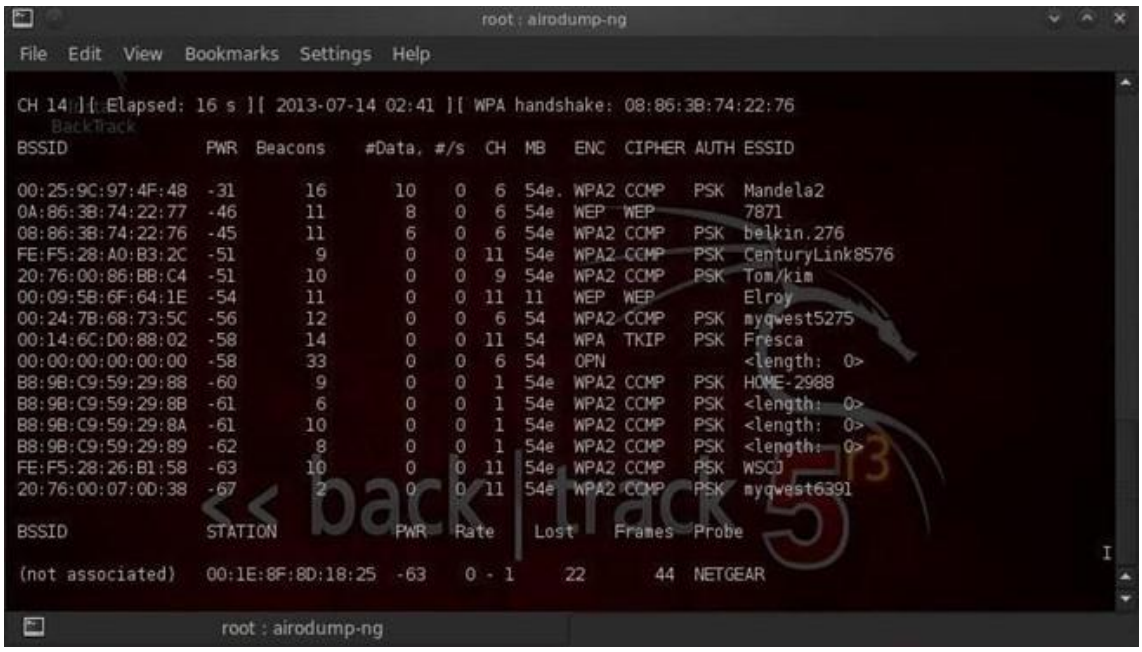


KUVA 7. Airmon-ng toiminnassa (http://null-byte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893/)

4.3 Airodump-ng

Airodump-ng haistelee ilmassa kulkevia 802.11–kehyksiä. Airodump-ng:tä käytetään keräämään lisää dataa, jotta voidaan käyttää aircrack-ng:tä löytämään oikea PSK. Tämä työkalu mahdollistaa myös AP:tien koordinaattien saannin, jos laitteessa on GPS–vastaanotin. Esimerkkikomento airodump-ng:llä: airodump-ng -c 8 --bssid 00:14:6C:7A:41:20 -w capture mon0.

- -c valitsee kanavan jota kuunnellaan
- -bssid parametrilla ilmoitetaan halutun AP:in MAC –osoite
- -w parametrilla valitaan mitä tallennetaan, tässä tapauksessa kaapatut paketit mon0 –rajapinnasta.



KUVA 8. Airodump-ng toiminnassa (http://null-byte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893/)

4.4 Aireplay-ng

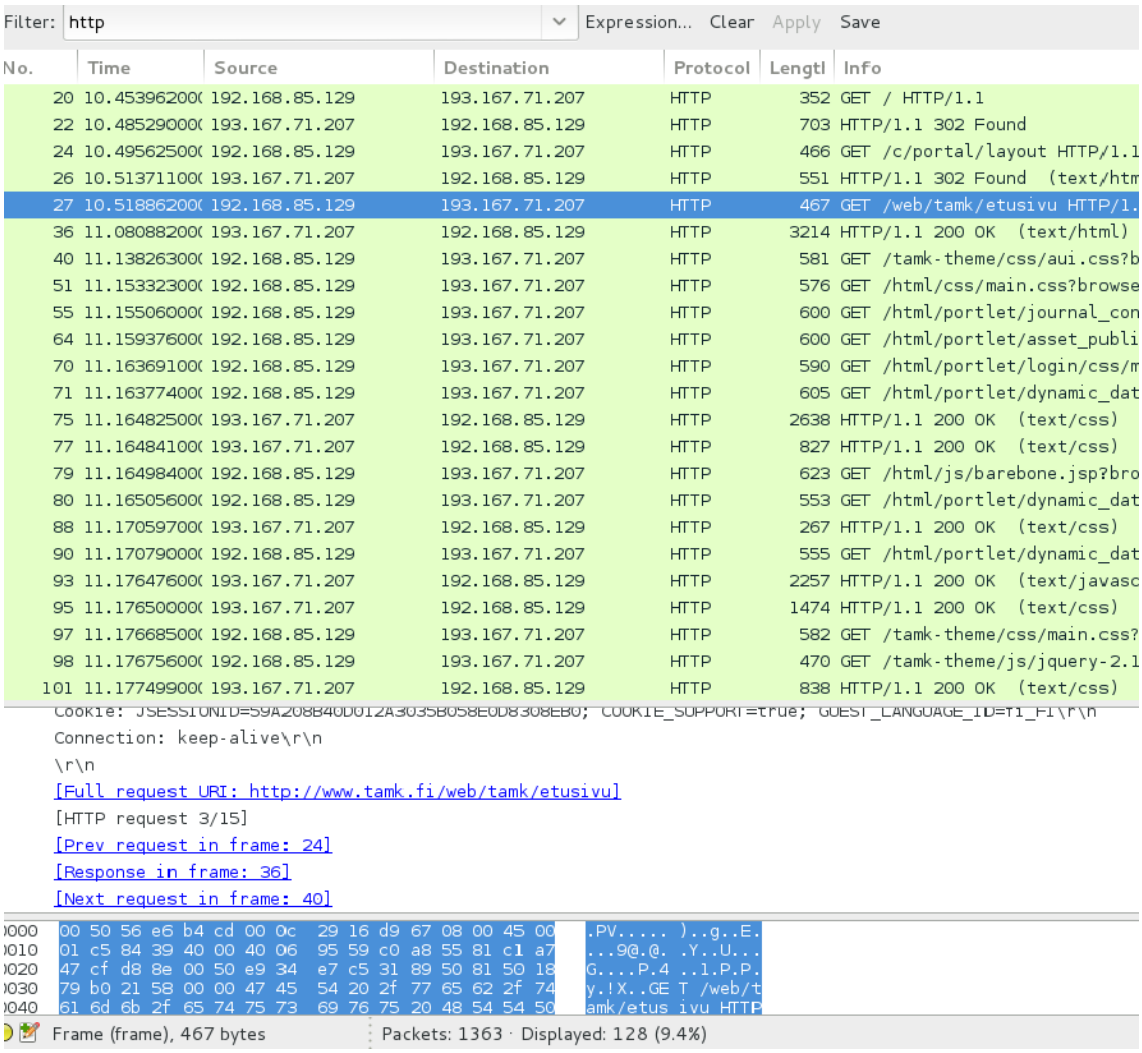
Aireplay-ng on työkalu, jolla injektoidaan kehyksiä tietoliikenteeseen. Sen päätoimenpide on luoda lisää liikennettä, joka kaapataan airmon-ng:llä. Tämän lisäliikenteen tarkoitus on saada lisää dataa, jotta voidaan käyttää aircrack-ng:tä murtamaan WEP- ja WPA-PSK-salasanoja. Tämä tapahtuu lähettämällä de-autentikointikomentoja, jotta saadaan WPA-handshake-dataa, josta salasana murretaan.

Tyypillinen komento jolla saadaan laite de-autentikoitumaan AP:in kanssa:
‘aireplay-ng -0 x -a 00:14:6C:7E:40:80 -c 00:0F:B5:AE:CE:9D wlan0.’ Komento jakaantuu eri parametreihin

- -0 määrittää de-autentikoinnin
- x määrittää montako de-autentikointipyyntöä lähetetään. Tarvitaan numeerinen arvo, esimerkiksi 100
- -a määrittää AP:in MAC-osoitteen
- -c määrittää MAC-osoitteen laitteelle, joka halutaan de-autentikoida.
- viimeisenä määritetään rajapinta, jota työkalu käyttää.

4.5 Wireshark

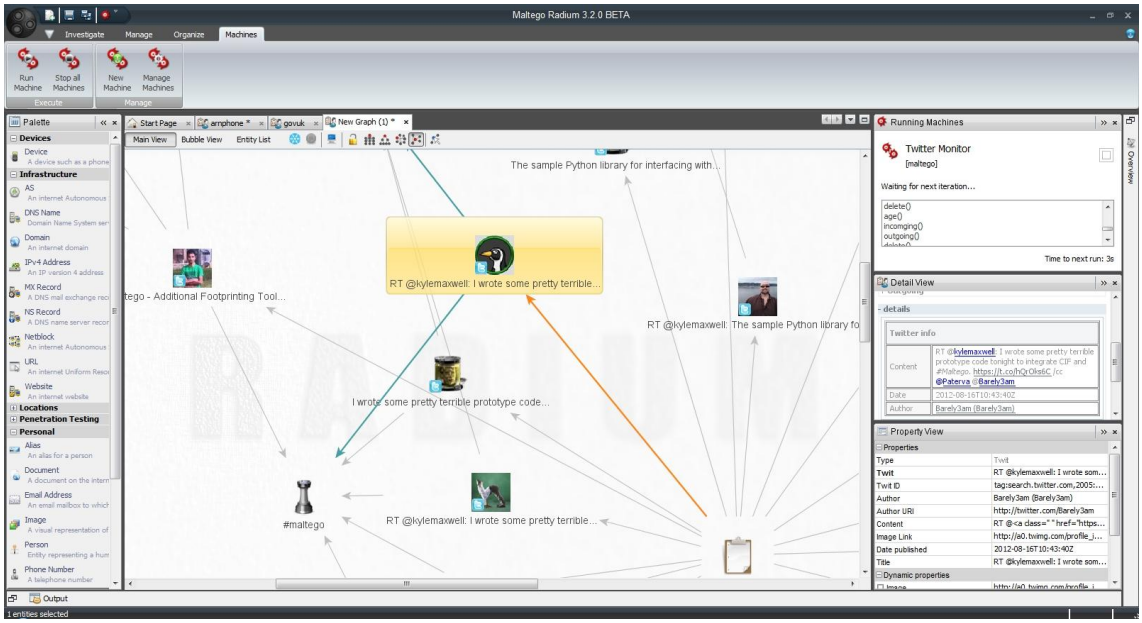
Wireshark on graafinen verkkoprotokollaanalysaattori, joka mahdollistaa verkossa liikkuvien pakettien tarkastelun. Sillä on mahdollista kuunnella kaikkea verkkoliikennettä, tai rajoittaa kuuntelu haluttuihin rajapintoihin, kuten wlan0–rajapintaan. Wiresharkilla on mahdollista avata protokollia, joka mahdollistaa esimerkiksi VoIP–puheluiden (Voice over Internet Protocol) audion muuttamisen.



KUVA 9. WireShark eth0–rajapinnan kuuntelu HTTP–protokolla filtterillä

4.6 Maltego

Maltego on informaation keräystyökalu. Murtautujat käyttävät sitä keräämään tietoa halutusta domainista/yrityksestä. Tällä työkalulla on mahdollista hahmottaa yrityksen infrastruktuuri ja saada internetistä tietoa yrityksen työntekijöistä. ”Social Engineering” hyötyy Maltegon kaltaisista työkaluista suuresti. Murtautuja voi Maltegon avulla saada selville yhtiön työntekijän henkilökohtaisen Twitter-tilin ja sitä kautta manipuloida työntekijää luovuttamaan tärkeitä tietoja.



KUVA 10. Maltego (www.paterva.com)

5 HYÖKKÄYKSIÄ

Langattomat verkot ovat alttiimpia hyökkäyksille kuin langalliset verkot. Kaapelilla toimivissa suljetuissa verkoissa hyökkääjän on täytynyt fyysisesti päästä käsiksi verkkoon, kun taas langattomissa verkoissa hyökkääjän täytyy vain olla lähellä mahdollisia tukiasemia. Hyökkääjä voi päästä käsiksi myös langalliseen verkkoon käyttämällä hyödyksi langatonta verkkoa. Nämä asiat täytyy pitää mielessä langatonta verkkoa suunniteltaessa. Tässä kappaleessa esitellään yleisiä langattomiin verkkoihin kohdistuvia hyökkäyksiä.

5.1 DoS – Denial of Service

DoS-hyökkäykset ovat yleistyneet huomattavasti vuosien varrella. Niitä käyttävät muun muassa valtiot sekä yksittäiset pahantahtoiset hyökkääjät. Jopa nuoret alasta kiinnostuneet ihmiset ovat päässeet otsikoihin kaataessaan pankkien verkkosivuja. DoS-hyökkäyksen tekemiseen on jaossa monia ilmaisia ohjelmia, jotka yleisimmin tarjoavat yhteyden botnettiin, jota käyttäjä voi hyödyntää vahingon aiheuttamisessa. Ilmaisten versioiden lisäksi on myös maksullisia, kovemman luokan ohjelmia joilla on hallussaan paljon laajempi botnet. [4.]

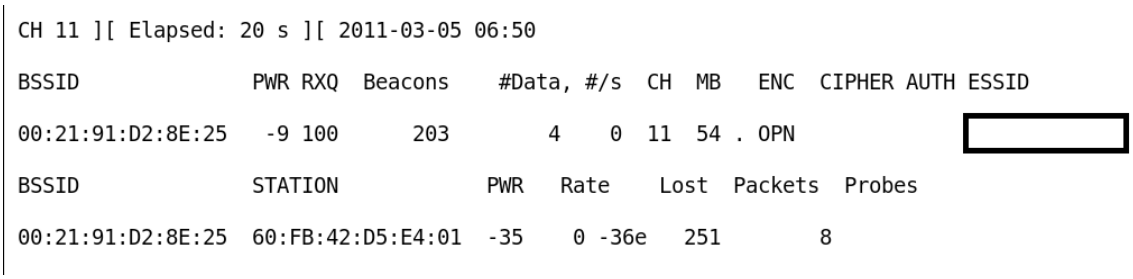
Langattomien verkkojen DoS-hyökkäykseen ei tarvita botnettiä. Sen voi toteuttaa muun muassa seuraavilla tavoilla: de-autentikaatio pakettien lähettämisellä, CTS-RTS-hyökkäyksellä (Clear To Send – Request To Send) ja signaalin häirinnällä.

Näillä yksinkertaisilla hyökkäyksillä jo yksi hyökkääjä voi aiheuttaa ongelmia langattoman verkon käyttäjille.

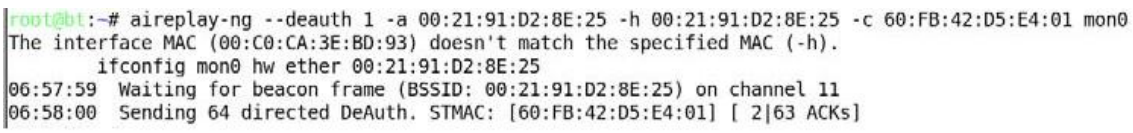
5.1.1 DoS-hyökkäyksen toteutus Kali Linuxilla

Seuraavassa on esimerkki, kuinka helposti DoS-hyökkäys onnistuu Kali Linuxin avulla.

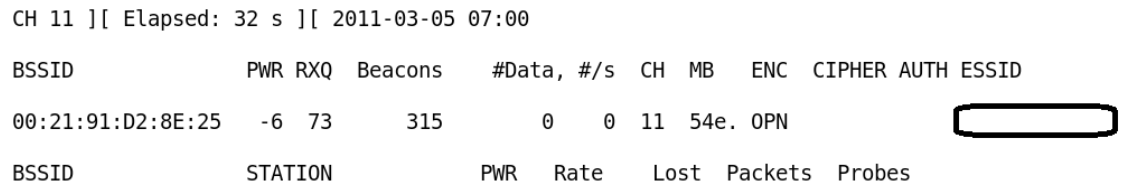
1. WLAN-verkkokortti laitetaan aluksi monitorointitilaan.
2. Odotetaan, kunnes haluttu AP tulee näkyviin (kuva 11).
3. Valitaan laite, jonka pääsy verkkoon halutaan estää.
4. Käytetään aireplay-ng-työkalua, jolla valitaan haluttu hyökkäys: de-autentikointi (kuva 12).
5. Määritetään kohdetukiasema MAC–osoitteen perusteella.
6. Määritetään haluttu uhri MAC–osoitteen perusteella.
7. Lähetetään de-autentikaatiopaketteja.
8. Todetaan, että uhri on menettänyt yhteyden AP:iin (kuva 13).



KUVA 11. Tiedonkeruu



KUVA 12. DoS-hyökkäys toteutettuna de-autentikointikomentoa käyttämällä



KUVA 13. DoS-hyökkäyksen jälkeen

5.1.2 DoS–hyökkäykseltä puolustautuminen

Yksinkertaisin tapa puolustautua DoS-hyökkäyksiä vastaan, on rajoittaa langattoman verkon kantamaa. Pienentämällä tukiaseman lähetystehoa signaalin kantama lyhenee. Radioaaltojen etenemistä voidaan vähentää sopivasti suunnatulla-antennilla.

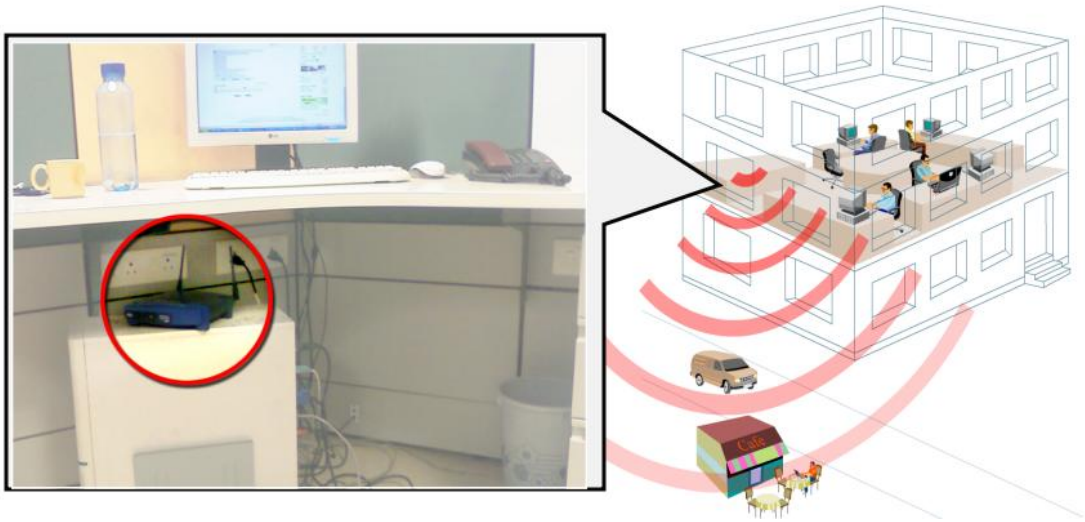
Mahdollista on myös käyttää radioaalloilta suojaavaa materiaalia ja asentaa sitä rakennuksen seinämiin. Näillä kaikilla toimenpiteillä saavutetaan se, että hyökkääjän on pakko olla fyysisesti samassa huoneessa tukiaseman kanssa jotta hyökkäys onnistuisi.

Verkkoa kannattaa seurata monitorointiohjelmilla, joilla havaitaan muun muassa liikenteen kasvu, tukiasemat ja niihin yhdistyneet laitteet. WIPS (Wireless intrusion-prevention system) on kattavin suoja DoS-hyökkäyksiä vastaan. WIPS koostuu sensoreista, palvelimesta sekä hallinta konsolista. WIPS yleensä havaitsee seuraavat asiat:

- Luvattomat MAC–osoitteet
- Luvattoman broadcast liikenteen
- Radiohäirinnän
- De-autentikaatio-hyökkäykset
- MitM-hyökkäykset
- DoS-hyökkäykset.

5.2 Rogue AP

Rogue Access Point on luvaton langaton tukiasema, joka on yleensä avoin ja salaukseton. Tämä langaton verkko on yhdistetty yrityksen langalliseen verkkoon, joka tarjoaa pääsyn yrityksen suojattuun verkkoon. Yleensä yrityksen tietämättömät työntekijät asentelevat luvattomia tukiasemia helpottaakseen omaa elämäänsä, mutta aiheuttavat vakavan tietoturvauhan yritykselle. Motivoituneelle hyökkääjälle ei myöskään tuota ongelmia saada oma luvaton tukiasemansa yrityksen sisälle. [4.]



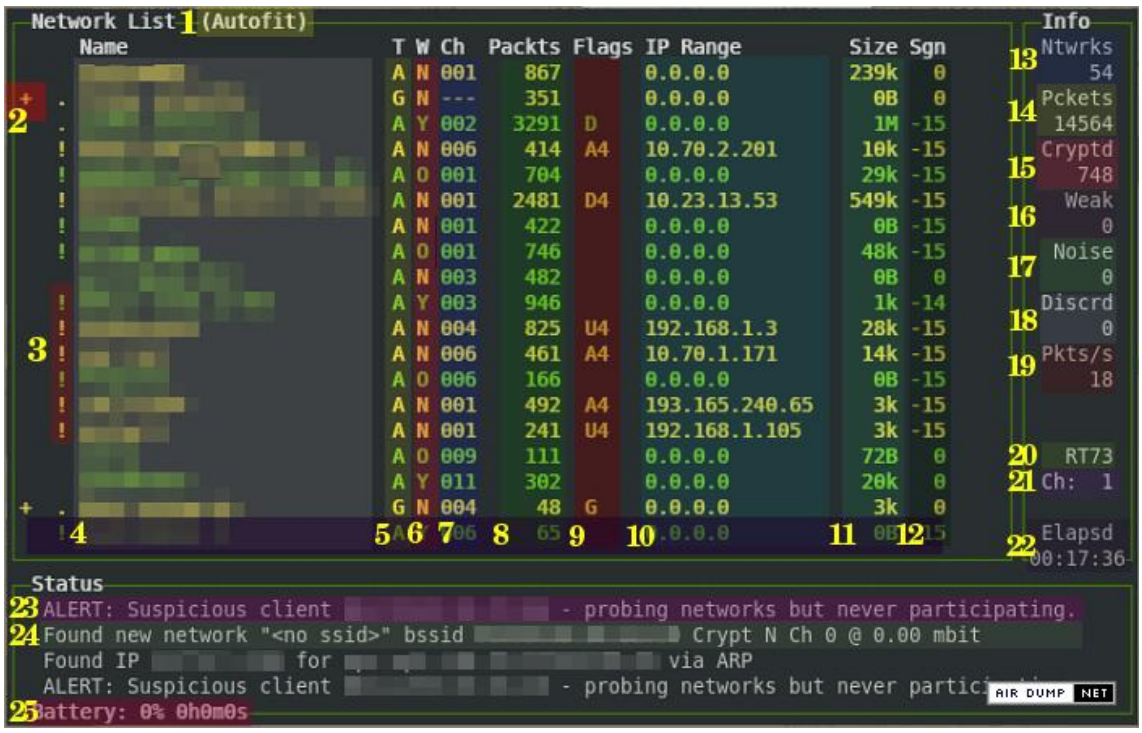
KUVA 14. Luvaton tukiasema (airtightnetworks.com)

5.2.1 Luvattomilta tukiasemilta suojautuminen

Luvattomien tukiasemien käyttöä on mahdotonta estää, mutta ne voidaan havaita. Kaikki tukiasemat on mahdollista löytää skannausohjelmistojen avulla. Järjestelmänvalvojan tehtäväksi jää eritellä luvalliset ja luvattomat tukiasemat. Nämä ohjelmistot eivät tosin skannaa kaikkia kanavia, esimerkiksi Yhdysvalloissa ei ole sallittua käyttää kanavaa 13. Hyökkääjä voi vaihtaa NIC:n ajurit eri maan ajureiksi, joka tällöin sallii hyökkääjän käyttää toisia kanavia. Vaihtoehtoisesti hyökkääjä voisi käyttää langatonta verkkokorttia, joka toimii 900 MHz:n taajuudella. Tätä taajuutta Wi-Fi-skannerit eivät yleisesti ota huomioon lainkaan.

Parhaiten hyökkääjät havaitaan käyttämällä sekä langallisen verkon puolelta tehtyjä skannauksia että langattomalta puolelta tehtyjä havaintoja. Näihin tarkoituksiin on tehty lukuisia ohjelmistoja. Hyvä aloituspiste on käyttää ilmaista Kismet–ohjelmistoa. Käyttäjät ovat luoneet Kismetille lukuisia plugineita, jotka parantavat ohjelmistoa entisestään ja tekee tunkeutujien havaitsemisesta helpompaa.

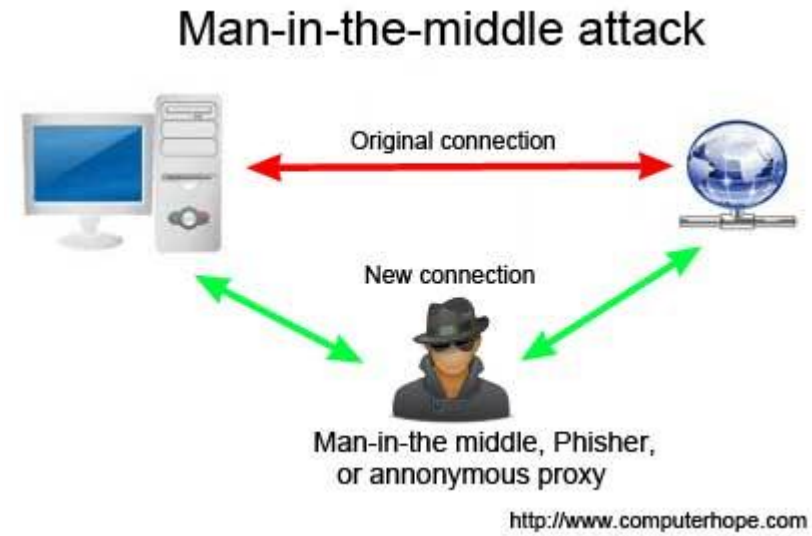
Kismet käyttää lukuisia tekniikoita skannatakseen kaikki tukiasemat alueelta. Mahdollista on myös käyttää GPS–korttia, jolloin Kismet myös paikantaa tukiasemat ja piirtää niiden sijainnin kartalle. Se myös laskee tukiaseman kantaman lähetystehon perusteella.



KUVA 15. Kismetin reaaliaikainen skannaus (http://airdump.cz/)

5.3 MitM – Man in the Middle

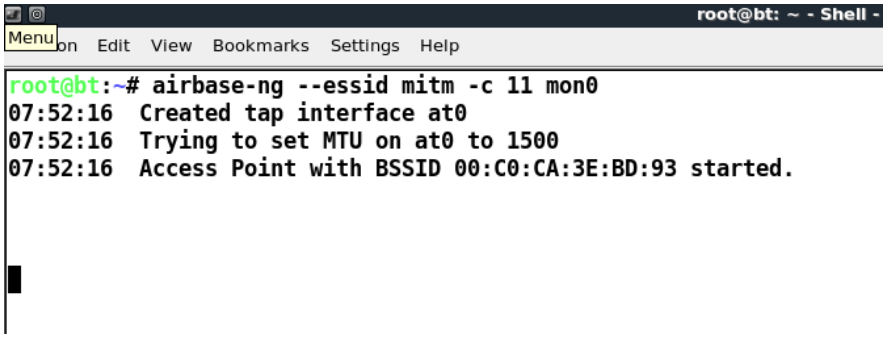
MitM–hyökkäyksessä hyökkääjä on uhrin ja esimerkiksi serverin välissä. Hyökkääjä välittää kaiken liikenteen. Liikennettä on mahdollista muokata myös pakettitasolla, tai vaihtoehtoisesti hyökkääjä voi injektoida omia pakettejaan. [4.]



KUVA 16. MitM (computerhope.com)

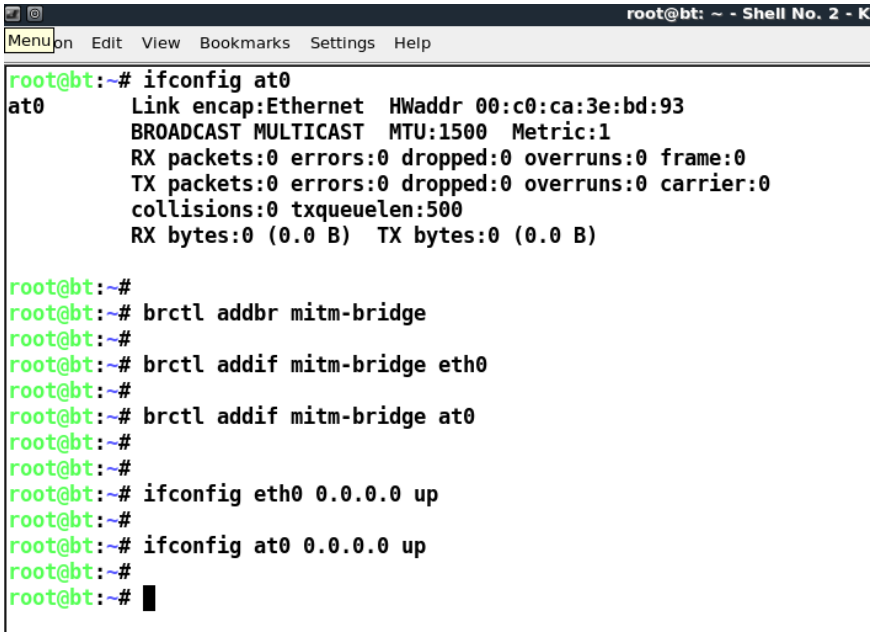
5.3.1 MitM-hyökkäyksen toteutus

Helpoin tapa toteuttaa MitM–hyökkäys on luoda oma tukiasema ja nimetä se halutun tukiaseman mukaan. Uhri voidaan saada liittymään luotuun tukiasemaan nostamalla signaalin tehoa voimakkaammaksi kuin alkuperäisen tukiaseman teho on. Luodaan Kali Linuxilla tukiasema ”mitm”, kuvassa 17 esitetty komento luo uuden rajapinnan at0, joka toimii ”mitm”-tukiasemana.



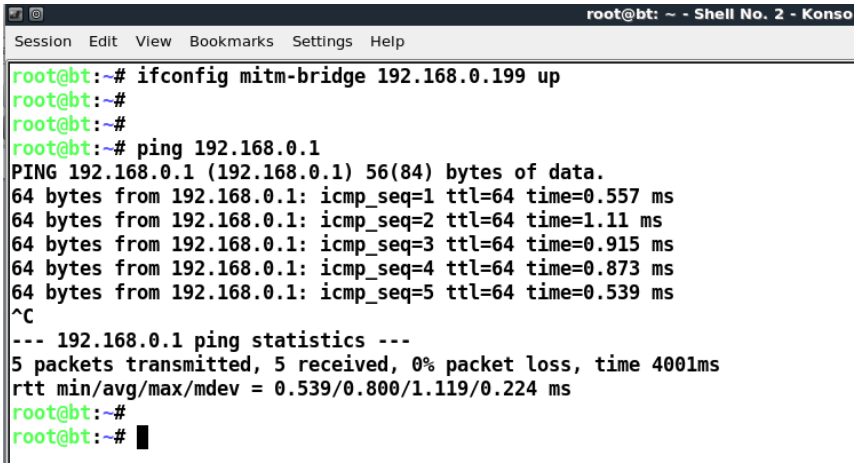
KUVA 17. Hyökkäävän tukiaseman ”mitm” luonti, jossa -essid määrittää tukiaseman nimen, -c määrittää kanavan ja viimeisenä määritetään haluttu rajapinta

Seuraavaksi täytyy yhdistää rajapinta at0 rajapintaan eth0 (langallinen verkko) kuten kuvassa 18.



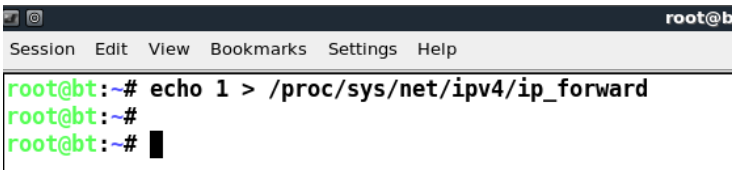
KUVA 18. Siltaus rajapintojen at0 – eth0 välillä

Määritetään sillatulle yhteydelle IP osoite ja testataan yhteyden toimivuus kuten kuvassa 19.



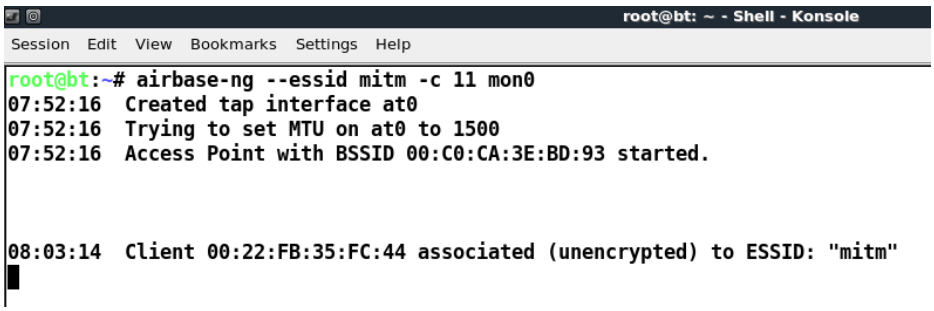
KUVA 19. IP-osoite sillatulle yhteydelle ja yhteyden testaus

Jotta tukiasema osaa lähettää paketit oikeaan paikkaan, täytyy käynnistää IP-reititys (kuva 20).



KUVA 20. IP-reitityksen käynnistäminen

Odotetaan, että uhri liittyy tukiasemaan (kuva 21). Wiresharkilla voidaan todeta, kuinka uhrin liityttyä tukiasemaan nähdään kaikki uhrin liikenne, koska tukiasema ”mitm” ohjaa liikennettä eteenpäin. Hyökkäyksen onnistumisen parantamiseksi hyökkääjät usein nostavat luodun tukiasemansa lähetystehoa jotta uhri varmemmin liittyy siihen alkuperäisen sijaan.



KUVA 21. Uhri liittyy verkkoon

6 POHDINTA

Langattomat verkot toimivat datan siirtoteinä ilmassa koko ajan. Niiden yleistyminen on avannut uusia tietoturvauhkia, sillä langattomissa verkoissa on ikävä kyllä paljon enemmän tietoturvariskejä kuin perinteisissä kaapeliverkoissa. On tärkeää kouluttaa ihmisiä langattomien verkkojen turvalliseen käyttöön.

Opinnäytetyön tavoitteena oli saada lisää tietoa langattomista verkoista, niiden tietoturvasta, sekä vahvistaa aiempaa tietämystä. Työhön kuului tiedonkeruuta, testilaboratorion rakentaminen, ohjelmistoasennuksia ja dokumentointia. Kieliopin kertaaminen osoittautui tärkeäksi osaksi dokumentaatio vaihetta. Tiedonkeruu vaiheessa löytyi uusi arvostus kirjoja kohtaan.

Työssä testilaboratorion rakentaminen oli mukava kertaus jo opituille taidoille. Tukiaseman konfigurointi sujui mallikkaasti aiempien tietojen pohjalta. Uhreina toimivat Windows 7 –käyttöjärjestelmällä varustettu virtuaalikone, sekä Metasploit-Linux, joka oli myös virtuaalinen. Kali Linuxista käytettiin sekä virtuaalista, että USB-tikulle asennettua versiota. Kodin tietoturva parani opinnäytetyön tekemisen myötä.

Aiempien kokemuksien myötä eniten tuli uutta tietoa langattoman verkon teknologiasta. TAMK:ssa oli aiemmin pidetty laboratorio kursseja, joista oli todella paljon hyötyä tämän uuden teorian oppimiseen. CCNA-kurssilla käytiin läpi langallisten verkkojen rakentamista ja reitittimien konfigurointia. Kurssi antoi hyvät lähtökohdat siirtyä langattomiin verkkoihin, ja helpotti hankitun tiedon ymmärtämistä.

Tietoturva on todella laaja ja mielenkiintoinen osa-alue tietotekniikkaa. TAMK:ssa järjestettiin yksi tietoturva kurssi, josta kipinä aiheeseen syntyi. Opinnäytetyöstä käy ilmi, kuinka suuria vahinkoja huono tietoturva aiheuttaa, ja kuinka pienillä muutoksilla nämä vahingot voidaan estää.

Tämän työn pohjalta on hyvä lähteä jatko-opiskelemaan aihetta. Seuraavia aiheita ovat uudet hyökkäykset, salauksen tarkempi tutkiminen, Wireshark-ohjelmiston parempi opettelu sekä tietoturvasertifikaatin suorittaminen.

LÄHTEET

1 Ramachandran V. 2011. BackTrack 5 Wireless Penetration Testing. Packt Publishing Ltd.

2 Buchanan C. 2014. Kali Linux CTF Blueprints. Packt Publishing Ltd.

3 Dieterle D. 2013. Basic Security Testing with Kali Linux.

4 Weidman G. 2014. Penetration Testing.

5 Gast M. 2013. 802.11ac: A Survival Guide.

6 Cisco. 802.11ac: The Fifth Generation of Wi-Fi Technical White Paper. Luettu 14.4.2015. http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.html

7 IEEE 802.11. Luettu 15.4.2015. http://en.wikipedia.org/wiki/IEEE_802.11

8 Geier, J. 2005. Langattomat verkot. Helsinki: IT Press.

9 Coleman, D. 2011. CWAP Certified Wireless Analysis Professional Official Study Guide: Exam PW0-270