jamk

Langattomien verkkojen tietoturva

Markus Oksanen

Opinnäytetyö,
Maaliskuu 2022
Tietojenkäsittely ja tietoliikenne, Insinööri (AMK)
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Oksanen Markus

Langattomien verkkojen tietoturva

Jyväskylä: Jyväskylän ammattikorkeakoulu. Maaliskuu 2022, 46 sivua.

Tietojenkäsittely ja tietoliikenne. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Langattomat tietoverkot ovat osa meistä lähes jokaisen päivittäistä arkea. Puhelimet, tietokoneen ja muut laitteet ovat kytkettyinä langattomaan verkkoon ja tietoa liikkuu siellä paljon. Jokaisen on syytä olla kiinnostunut omasta tietoturvastaan.

Perehdyttiin tietoturvallisuuteen tarkemmin avaamalla Wi-Fi-standardeja, erilaisia suojausmenetelmiä, sekä tutustumalla Rogue Access Pointin toimintaan, jolla toteutettiin myös pienimuotoinen hyökkäysdemo.

Tutkimusmenetelmänä oli työn aiheeseen hyvin soveltuva empiirinen tutkimus, joka koostuu mittaamisesta, konkreettisista havainnoista, sekä analysoinnista.

Rogue Access Pointin demonstraatio toteutettiin Raspberry Pi-pienoistietokoneella. Raspberry Pi:lle asennettiin Kali Linux-käyttöjärjestelmä, jossa käytettiin Wifipumpkin3-ohjelmistoa. Demonstraation eri vaiheet käytiin kohta kohdalta lävitse ja demonstraatiolla onnistuttiin osoittamaan kuinka käyttäjän kirjautumistiedot voivat joutua vääriin käsiin. Käytiin myös läpi keinoja suojautua tällaiselta hyökkäykseltä.

Avainsanat (asiasanat)

Tietoverkko, Tietoturva, Kyberturvallisuus, Tieto- ja viestintätekniikka, Demo

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Oksanen Markus

Security of wireless networks

Jyväskylä: JAMK University of Applied Sciences, March 2022, 46 pages.

Information and Communications. Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

Wireless networks are part of the daily lives of almost all of us. Phones, computers, and other devices are connected to wireless networks and a lot of data travels there. Everyone should be interested in their own information security.

We got to know more about information security by opening Wi-Fi standards, various security methods and by getting familiar with how Rogue Access Point operates. We also performed a small-scale attack demo with Rogue Access Point.

The research method was an empirical study as it suited the topic very well. It consists of measurement, concrete observations, and analysis.

The demonstration of the Rogue Access Point was conducted on a Raspberry Pi minicomputer. The Raspberry Pi was installed with the Kali Linux operating system, inside of which Wifipumpkin3 software was being used. The various steps of the demonstration were performed step by step and the demonstration succeeded in showing how the user's login information could fall into the wrong hands. Ways to protect against such an attack were also reviewed.

Keywords/tags (subjects)

Data network, Information security, Cybersecurity, Information and Communication Technology, Demo

Miscellaneous (Confidential information)

Sisältö

Lyhenteet

AP	Access Point
BSSID	Basic Service Set Identifier
CPU	Central Processing Unit
CSI	Camera Serial Interface
DSI	Digital Serial Interface
Gb/s	Gigabits per second
GHz	Gigahertz
GPIO	General Purpose Input/Output
HDMI	High-Definition Multimedia Interface
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISP	Internet Service Provider
MAC	Media Access Control
Mb/s	Megabits per second
MIMO	Multiple Input Multiple Output
RAM	Random Access Memory
SSH	Secure Shell (Protocol)
SSID	Service Set Identifier
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XRDP	Remote Desktop Protocol

1 Johdanto

Langattomat verkot ovat tulleet osaksi päivittäistä elämäämme kahden viime vuosikymmenen aikana. Yleisesti tunnettu nimi langattomille verkoille on Wi-Fi. Ensimmäinen Wi-Fi-standardi julkaistiin 1999. Siitä lähtien sen suosio on kasvanut nopeasti. Vuosikymmen sitten Wi-Fiä käyttivät pääasiassa kannettavat tietokoneet, sekä puhelimet. Tänä päivänä Wi-Fi on päivittäisessä käytössä tietokoneiden ja puhelimien lisäksi myös esimerkiksi tableteilla, televisioissa, pelikonsoleissa, kodin turvakameroissa, älylampuissa ja monissa muissa laitteissa. Tulevaisuudessa Wi-Fin läsnäolo jokapäiväisessä elämässä kasvaa entisestään, sillä Wi-Fiä käyttävien laitteiden tyyppi ja määrä jatkavat kasvuaan.

Wi-Fin korkean ja kasvavan läsnäolon vuoksi, niin arjessa kuin myös työelämässä, sen tietoturvan tärkeys kasvaa entisestään. Tietoturvaloukkausten vakavuus ja todennäköisyys ovat kasvaneet Wi-Fin läsnäolon kasvun myötä; mitä enemmän Wi-Fiä käyttäviä laitteita on, sitä enemmän on hyökkäysalttiita kohteita. Tietoturvaloukkausten seuraukset voivat olla hyvin vakavia, esimerkiksi tietovuoto tai rahavarojen menetys. Yksityinen käyttäjä voi esimerkiksi menettää hänelle tärkeän käyttäjätilin tiedot. Yrityksille tärkeän datan menettäminen voi johtaa siihen, että liiketoiminta estyy.

Riskien vakavuudesta huolimatta, monet Wi-Fi-laitteiden käyttäjät eivät välttämättä ole tietoisia niistä tai tavoista suojautua niiltä. On siis olemassa tarve kasvattaa käyttäjien tietoisuutta. Opinnäytetyö keskittyy kasvattamaan tietoturvariskien tietoisuutta:

- Tarjoamalla tietoa Wi-Fi-standardeista
- Tarjoamalla tietoa suojausmenetelmistä
- Demonstroimalla Rogue Access Pointin toimintaa esimerkkinä tietoturvauhasta, sekä
- Osoittamalla keinoja kuinka suojautua Rogue Access Pointilta.

2 Tutkimusasetelma

Työssä käsitellään langattomien verkkojen tietoturvaa, sekä esitetään Rogue Access Pointin toimintaa käytännössä demon muodossa. Tutkimusmenetelmäksi valikoitui työn aiheesta johtuen empiirinen tutkimus, joka koostuu kolmesta eri vaiheesta: mittaaminen, konkreettiset havainnot,

sekä analysointi. Aineisto kartutetaan tutkimalla ja demoamalla tapahtumaa. (Empiirinen tutkimus 2015.)

Työn aiheen ja luonteen pohjalta luotiin seuraavat kysymykset, joihin haettiin vastausta:

- Kuinka Rogue Access Point toimii?
- Kuinka Rogue Access Pointilta voi suojautua?
- Kuinka tukiaseman signaalin voimakkuus vaikuttaa langattoman verkon tietoturvaan?

Demo toteutetaan pienessä mittakaavassa käyttäen apuna Raspberry Pi:ta.

Raspberry Pi on pieni taskukokoinen tietokone, johon voidaan liittää kiinni näyttö, näppäimistö ja hiiri. Siihen saa kiinni muistikortin, johon voidaan asentaa käyttöjärjestelmä.

3 Tietoperusta

3.1 Mikä on Wi-Fi?

Wi-Fi on langaton verkkoprotokolla, jota laitteet käyttävät kommunikoidakseen ilman fyysisiä kaapeleita. Se on tuotteistettu termi, joka edustaa langatonta paikallista verkkoa (*Wireless Local Area Network* eli WLAN) perustuen 802.11 IEEE standardiin. (Uy 2021.)

Tavallisen käyttäjän näkökulmasta Wi-Fi on internet-yhteys langattomaan tiedonsiirtoon kykenevästä laitteesta, kuten puhelimesta, tabletista tai kannettavasta tietokoneesta. Useimmat modernit laitteet tukevat Wi-Fiä, jonka myötä ne voivat yhdistää verkkoon ja saada internet-yhteyden. (Uy 2021.)

3.2 IEEE-ammattiyhdistys

IEEE (*Institute of Electrical and Electronics Engineers*) on maailman suurin ammattiyhdistys, jonka tehtävänä on edistää innovaatiota ja teknologista huippuosaamista ihmiskunnan hyödyksi. IEEE:n tarkoituksena on palvella kaikkia sähkö-, elektroniikka- ja tietojenkäsittelyalojen ammattilaisia. IEEE on perustettu 1963 Yhdysvalloissa. (History of IEEE 2022.)

IEEE julkaisee lähes kolmanneksen maailman sähkötekniikan, tietojenkäsittelytieteen ja elektroniikan teknisestä kirjallisuudesta. (IEEE at a Glance 2021) IEEE ylläpitää aktiivista standardien kirjastoa, jotka määrittelevät useiden tuotteiden ja palveluiden toimivuutta, myös Wi-Fin.

3.3 Unicast, multicast ja broadcast -liikenne

Data liikkuu verkossa pakettien muodossa kolmen erilaisen menetelmän avulla. Unicast (täsmälähetys) tarkoittaa liikennettä yhdestä lähteestä yhdelle vastaanottajalle, sitä hyödyntävät esimerkiksi sähköpostiohjelmat. Multicast (ryhmälähetys) tarkoittaa liikennettä yhdestä lähteestä usealle vastaanottajalle ja sillä voidaan vähentää näin palvelimen kuormitusta. Broadcast (yleislähetys) puolestaan tarkoittaa liikennettä yhdestä lähteestä kaikille mahdollisille vastaanottajille, esimerkiksi suoratoistopalveluiden muodossa. (Nevase n.d.)

3.4 EAPoL-protokolla

EAPoL (*Extensible Authentication Protocol over LAN*) on tietoverkoissa käytetty protokolla, jota käytetään todennukseen asiakaslaitteen ja tukiaseman (*Access Point – AP*) välillä eli silloin kun asiakaslaite haluaa liittyä tukiasemaan. (EAPoL (Extensible Authentication Protocol over LAN) n.d.) EAPoL luotiin tukemaan vanhempaa EAP-protokollaa, joka oli alun perin luotu tiedonsiirtoon puhelinverkoissa. EAP ei sellaisenaan kykene siirtämään dataa lähiverkossa. EAP-viestit siis kapseloidaan EAPoL-viesteiksi. (EAPOL n.d.) Tunnistautuminen tapahtuu EAPoL-viestejä lähettämällä. EAPol-viestit koostuvat viidestä osasta:

- EAPoL Start
- EAPoL Key
- EAPoL Packet
- EAPoL Logoff
- EAPoL Encapsulated ASF Alert (EAPoL (Extensible Authentication Protocol over LAN) n.d.)

Asiakaslaite ei aluksi tiedä tukiaseman MAC-osoitetta, joten tunnistautuminen alkaa asiakaslaitteen lähettämällä EAPol *Start* -viestillä tukiasemalle. Tukiasema käyttää EAPoL *Key* -viestiä lähettääkseen kryptatut avaimet. (EAPoL (Extensible Authentication Protocol over LAN) n.d.) Avaimet tulee lähettää kryptattuna, jotta niitä ei voitaisi kaapata ja väärinkäyttää, esim. Rogue Access Pointia hyödyntäen.

EAPoL *Packet* -kehystä käytetään varsinaisten EAP-sanomien lähettämiseen. EAPoL *Packet* on yksinkertaisesti säiliö EAP-viestin kuljettamiseen lähiverkon yli, mikä oli EAPoL-protokollan alkuperäinen tavoite. EAPoL *Logoff* -viestillä asiakaslaite ilmaisee, että se haluaa katkaista yhteyden tukiasemaan. (EAPOL n.d.)

EAPoL *Encapsulated ASF Alert* -viestiä käytetään varoituksien lähettämiseen, esimerkiksi silloin, jos havaitaan luvattoman portin käyttö. Kyseessä on turvallisuusmekanismi. (EAPoL (Extensible Authentication Protocol over LAN) n.d.)

3.5 4-suuntainen kättely

4-suuntainen kättely (*4-Way Handshake*) on menettely, jossa vaihdetaan 4 viestiä tukiaseman (todentajan) ja asiakaslaitteen (pyynnön esittäjän) välillä salausavaimien luomiseksi. Saatuja salausavaimia voidaan käyttää langattoman laitteen kautta lähetettyjen tietojen salaamiseen. Erilaisia avaimia on useita:

- MSK (Master Session Key)
- GMK (Group Master Key)
- PTK (Pairwise Transient Key)
- GTK (Group Temporal Key)
- ANonce
- SNonce
- MIC (*Message Integrity Check*) (4-Way Handshake n.d.)

MSK-avain (*Master Session Key*) luodaan autentikointiprosessin yhteydessä, joka tapahtuu jo ennen varsinaista 4-suuntaista kättelyä. Autentikointiprosessin yhteydessä luodaan myös PSK (*Pre-Shared Key*). (4-Way Handshake n.d.) PSK on osa WPA2-salausmenetelmää. Salausmenetelmiä käsitellään lisää luvussa 3.9.

PTK:ta (*Pairwise Transient Key*) käytetään kaiken unicast-liikenteen salaamiseen asiakaslaitteen ja tukiaseman (*Access Point*) välillä. PTK on uniikki asiakaslaitteen ja tukiaseman välillä eli vain nämä kaksi laitetta käyttävät sitä. Mikäli uusi asiakaslaite liittyisi verkkoon, sen ja tukiaseman välille luotaisiin uusi, uniikki PTK. PTK:n luomiseksi asiakaslaite ja tukiasema tarvitsevat seuraavat tiedot:

molempien laitteiden MAC-osoitteet, ANonce-muuttujan, sekä SNonce-muuttujan. ANonce on tukiaseman luoma satunnaisluku avaimen luomista varten ja SNonce on samaan tapaan asiakaslaitteen luoma satunnaisluku. (4-Way Handshake n.d.)

GTK-avainta (*Group Temporal Key*) käytetään salaamaan kaikki multicast- ja broadcast-liikenne tukiaseman ja useiden asiakaslaitteiden välillä. GTK on avain, joka jaetaan kaikkien yhteen tukiasemaan liittyneiden asiakaslaitteiden kesken. Jokaisella tukiasemalla on oma GTK, joka jaetaan siihen liittyvien asiakaslaitteiden kesken. GMK:ta (*Group Master Key*) käytetään 4-suuntaisessa kättelyssä GTK:n luomiseen. (4-Way Handshake n.d.)

4-suuntaisen kättelyn alussa autentikointiprosessi on suoritettu ja PSK on tiedossa asiakaslaitteelle ja tukiasemalle. On tärkeää huomata, että PSK luodaan paikallisesti niin asiakaslaitteessa, kuin myös tukiasemassa. Näin ollen sitä ei koskaan välitetä sellaisenaan verkon välityksellä, mikä tarkoittaa, että sitä ei voi kaapata. Tämä menettely lisää verkon turvallisuutta. (4-Way Handshake n.d.)

Käydään seuraavaksi läpi 4-vaiheisen kättelyn vaiheet. Vaiheiden eteneminen on kuvattu kuviossa 1. Kättelyn ensimmäinen viesti etenee seuraavasti: AP lähettää EAPoL-viestin, joka sisältää ANoncen (satunnaisluku) asiakaslaitteelle. Tässä vaiheessa asiakaslaite on jo luonut SNoncen (oman satunnaislukunsa) itselleen. Tämä tarkoittaa, että asiakaslaitteella on kaikki tarvittava data PTK:n luomiseen:

- ANonce (vastaanotettu AP:lta ensimmäisessä viestissä)
- SNonce (asiakaslaite on luonut tämän itse)
- PSK (tiedossa molemmilla laitteilla autentikointiprosessin jälkeen)
- MAC Address of AP (on tiedossa, koska AP ja asiakaslaite ovat liittyneinä toisiinsa)
- MAC Address of client (on tiedossa, koska AP ja asiakaslaite ovat liittyneinä toisiinsa)

Asiakaslaite luo nyt PTK:n. (Dionicio 2018.)

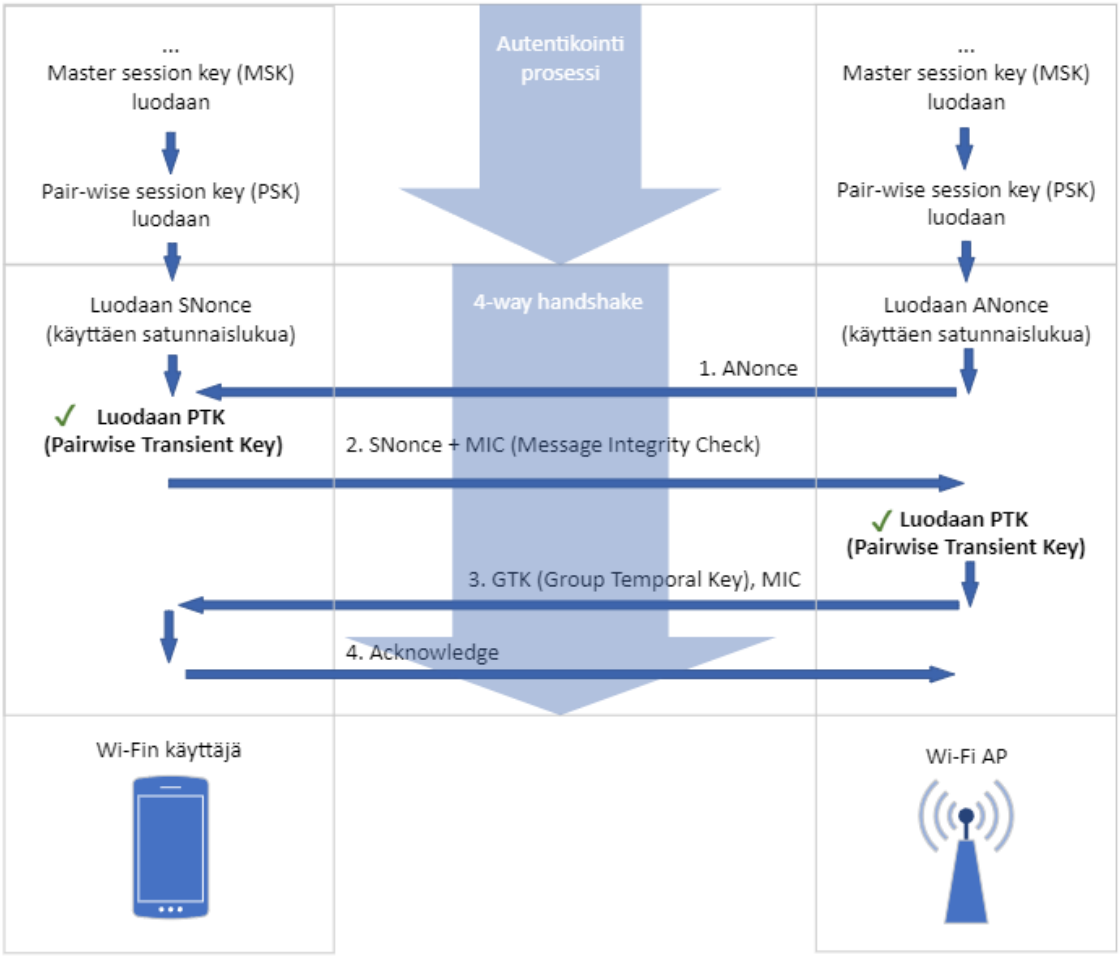
Kättelyn toisessa viestissä asiakaslaite lähettää EAPOL-viestin SNoncen (satunnaisluku) ja MIC:n kanssa AP:lle. Tässä vaiheessa AP:lla on kaikki tarvittava data PTK:n luomiseen, joten AP luo nyt PTK:n. (Dionicio 2018.) MIC (*Message Integrity Check*) on käytössä WEP-salauksen tehostamista

varten. (MIC (Message Integrity Check) n.d.) WEP-salausta käytetään langattomien verkkojen suojaamiseen ja sitä käsitellään lisää luvussa 3.9.

Kättelyn kolmannessa viestissä AP luo GTK:n. AP lähettää GTK:n ja MIC:n sisältävän EAPoL-viestin asiakaslaitteelle.

Kättelyn neljännessä vaiheessa asiakaslaite lähettää vahvistuksen AP:lle siitä, että avaimet on nyt asennettu.

4-suuntaisen kättelyn valmistuttua kaikki suojattu liikenne voi nyt kulkea. Kaikki unicast-liikenne suojataan käyttäen PTK:ta ja kaikki multicast-liikenne suojataan käyttäen GTK:ta, joka luotiin 4-suuntaisen kättelyn aikana. (4-Way Handshake n.d.)

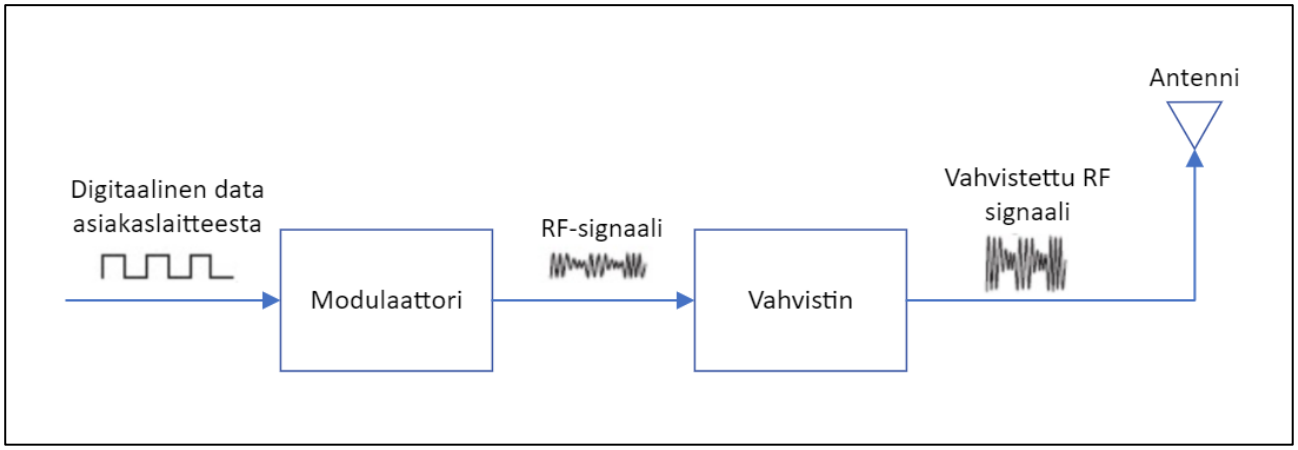


Kuvio 1. 4-vaiheinen kättely

3.6 Radiorajapinta

Yksi WLAN-verkolle oleellista komponenteista RF-lähetin-vastaanotin (*Radio Frequency transceiver*), joka koostuu lähettimestä ja vastaanottimesta. Lähetin lähettää radioaallon järjestelmän toisesta päästä ja vastaanotin vastaanottaa radioaallon järjestelmän toisesta päästä. Lähetin-vastaanotin koostuu yleensä laitteistosta, joka on jo osa langatonta asiakasradiolaitetta. (WiFi Networking: Radio Wave Basics 2017.)

Kuvio 2 esittää lähettimen peruskomponentit. Lähetyksessä tapahtuu modulaatio, joka muuntaa sähköiset, digitaaliset informaatiosignaalit (databitit) tietokoneen sisällä halutulla taajuudella radioaalloiksi, jotka etenevät ilmaväliaineen läpi. Vahvistin lisää radioaaltosignaalin amplitudia halutuun lähetystehoon ennen kuin se syötetään antenniin ja pääsee etenemään lähetysväliaineen läpi. Niin sanottu lähetysväliaine koostuu pääasiassa ilmasta, mutta kattaa myös esteet, kuten seinät, katot ja muut erilaiset rakenteet. (WiFi Networking: Radio Wave Basics 2017.)



Kuvio 2. Lähetin

3.7 Wi-Fi Alliance-järjestö

Wi-Fi Alliance on järjestö, joka edistää Wi-Fin maailmanlaajuista käyttöönottoa yhteistyössä yritysten kanssa. Järjestön tehtävänä on varmistaa, että kuluttajien Wi-Fi toimii toivotulla tavalla. Tähän pyritään kehittämällä testiohjelmistoja, sekä luomalla tiettyjä vaatimuksia Wi-Fi yhteyksille. (Who We Are 2022.)

Wi-Fi sertifikaatti (ks. kuvio 3) on kansainvälisesti tunnustettu hyväksyntämerkki laitteille, joka osoittaa, että laitteet ovat täyttäneet tietyt standardit yhteen toimivuuden, turvallisuuden, sekä sovelluskohtaisten protokollien osalta. (Certification 2022.)

Merkintä Wi-Fi sertifikaatista tarkoittaa, että laitetta on testattu useilla eri tavoilla sen yhteensopivuuden varmistamiseksi muiden Wi-Fi sertifioitujen laitteiden kanssa. (Certification 2022.)

Kuvio 3. Wi-Fi sertifioidun laitteen virallinen logo (Certification 2022.)

3.8 Wi-Fi standardit

Wi-Fi standardit saivat alkunsa vuonna 1999, IEEE:n määritellessä niistä ensimmäisen. Tästä lähtien standardeja on tullut useita lisää, jokaisen tuoden joitakin uusia ominaisuuksia mukanaan. Alla on listattuna taulukkoon erilaiset 802.11-standardit, sekä niiden julkaisuvuosi, taajuusalue ja maksiminopeus.

Standardi	Julkaisuvuosi	Taajuusalue	Maksiminopeus
802.11b	1999	2,4 (GHz)	11 (Mb/s)
802.11a	1999	5 (GHz)	54 (Mb/s)
802.11g	2003	2,4 (GHz)	54 (Mb/s)

802.11n	2009	2,4 (GHz) ja 5 (GHz)	600 (Mb/s)
802.11ac	2013	2,4 (GHz) ja 5 (GHz)	450–1300 (Mb/s)
802.11ad	2012	60 (GHz)	7 (Gb/s)
802.11ah	2017	863–868 (MHz)	78 (Mb/s)
802.11aj	2018	45 (GHz) ja 60 (GHz)	15 (Gb/s)
802.11ax	2019	2,4 (GHz) ja 5 (GHz)	10 (Gb/s)

802.11b-standardi tunnetaan myös nimellä *Wi-Fi 1*. (Mitchell 2021a.) Kyseessä on ensimmäinen, vuonna 1999 julkaistu, Wi-Fi-standardi. Mitchellin (2021a) mukaan sen teoreettinen maksiminopeus on 11 Mb/s, mutta todellisuudessa nopeus oli 2–3 Mb/s luokkaa. 802.11b:n käyttämä taajuusalue on 2,4 GHz.

802.11a-standardi, joka tunnetaan myös nimellä Wi-Fi 2, kehitettiin samaan aikaan 802.11b-standardin kanssa. 802.11a-standardi ei ollut yhtä suosittu kuin 802.11b ja se olikin kalliimpi ratkaisu ja lähinnä vain yritysten käytössä. 802.11a-standardin käyttämä taajuusalue on 5 GHz ja sen maksiminopeus on 54 Mb/s. (Mitchell 2021a.) Koska 802.11b ja 802.11a toimivat eri taajuusalueilla, ne eivät ole yhteensopivia keskenään.

Vuonna 2003 julkaistu 802.11g pyrkii yhdistämään 802.11a:n ja 802.11b:n parhaat puolet. Se käyttää 2,4 GHz taajuutta saavuttaakseen pidemmän kantaman ja sen maksiminopeus on 54 Mb/s. (IEEE 802.11g Wi-Fi n.d.) 802.11g-standardin etuna on, että se tukee kaikkia nykypäivänä käytössä olevia langattomia laitteita ja sen kustannukset ovat alhaiset. Huonona puolena on, että koko verkko hidastuu vastaamaan 802.11b-standardin laitteita, mikäli niitä on käytössä. 802.11g-standardi tunnetaan myös nimellä Wi-Fi 3. (Mitchell 2021a.)

802.11i-standardi julkaistiin vuonna 2004. Kyseessä oli hieman erilainen standardi, joka luotiin parantamaan langattomien verkkojen tietoturvaa. Se toi mukanaan parannuksia langattomaan todennukseen, salaukseen, avaintenhallintaan, sekä yksityiskohtaiseen suojaukseen. 802.11i-standardi parantaa WEP-menetelmää (ks. luku 3.9.1) ja kun se yhdistetään WPA2-menetelmän (ks. luku 3.9.3) kanssa, saadaan vahva suojaus aikaiseksi, joka sisältää myös AES-salauksen. (IEEE 802.11i n.d.)

802.11n-standardi julkaistiin vuonna 2009 ja se tunnetaan myös nimellä Wi-Fi 4. 802.11n-standardi suunniteltiin parantamaan 802.11g-standardin tukemaa kaistanleveyttä käyttämällä useita langattomia signaaleja ja antenneja, maksimissaan 4:aa. (Mitchell 2021a.) Tämä uusi tekniikka on nimeltään MIMO (*Multiple Input Multiple Output*) ja se mahdollisti merkittävästi suuremman datansiirron ilman suurempaa kaistanleveyttä tai lähetystehoa. (The evolution of Wi-Fi standards: a look at 802.11a/b/g/n/ac/ax n.d.). Myös Mitchell (2021a) toteaa 802.11n-standardin käyttävän MIMO-tekniikkaa. 802.11n-standardin tarjoama maksimi kaistanleveys on 600 Mb/s ja se toimii 2,4 GHz:n ja 5 GHz:n taajuusalueilla.

Vuonna 2013 markkinoille saapui 802.11n-standardin seuraaja, 802.11ac-standardi. 802.11ac-standardi tunnetaan myös nimellä Wi-Fi 5. 802.11ac-standardin maksiminopeus kasvoi huomattavasti edeltäjäänsä verrattuna ja on 1300 Mb/s. 802.11ac-standardi toimii 2,4GHz ja 5 GHz taajuusalueilla. (What Is 802.11ac? n.d.)

802.11ad-standardi julkaistiin vuonna 2012 ja sen erikoisuutena on, että se käyttää perinteisten 2,4 GHz:n ja 5 GHz:n taajuuksien sijaan 60 GHz:n taajuusaluetta. Se mahdollistaa näin ollen todella nopean tiedonsiirtonopeuden, jopa 7 Gb/s. (WiGig: IEEE 802.11ad 60GHz Microwave Wi-Fi n.d.) Vertailun vuoksi mainittakoon, että yksi gigabitti on 1000 megabittiä. Mitchellin (2021a) mukaan 802.11ad-standardin heikkoutena puolestaan on sen lyhyt kantama, maksimissaan noin 10 metriä päätelaitteesta.

Aust, Prasad ja Niemegeers (2012) kertovat, että 802.11ah-stadardi luotiin vastaamaan IoT:n (Internet of Things) nopeaa kehitystä ja kasvua. 802.11ah-standardi toimii alle 1GHz:n taajuuksilla, vaihtoehtona paljon käytetyille 2,4 GHz:n ja 5 GHz:n taajuuksille. Sen lisäksi, että 802.11ah-sta-

dardi toimii matalilla taajuuksilla, sen etuina ovat mm. hyvä käytettävyys myös ulkona, pitkä akunkesto, sekä virransäästöominaisuudet. (Aust, Psarad & Niemegeers 2012.) Mitchellin (2021a) mukaan 802.11ah-standardi hyväksyttiin toukokuussa 2017 IEEE:n toimesta.

Verrattain uusi, vuonna 2018 julkaistu, 802.11aj-standardi kehitettiin vastaamaan Kiinan tarpeita. Standardi tunnetaan myös nimellä *China Millimeter Wave*. 802.11aj-standardi määrittelee muutoksia jo olemassa olevaan 802.11ad-standardiin, mahdollistaen toiminnan Kiinan 59–64 GHz:n taajuusalueilla. 802.11aj-standardi pyrkii säilyttämään taaksepäin yhteensopivuuden 802.11ad-standardin kanssa, joka toimii 60 GHz:n taajuusalueella. (Shaw 2020.)

802.11ax-standardi hyväksyttiin käyttöön vuonna 2019 ja se tunnetaan myös nimellä Wi-Fi 6. Tämä standardi toimii 2,4 GHz:n ja 5 GHz:n taajuusalueilla ja sen maksiminopeus on 600 Mb/s. Wi-Fi 6:n uusia ominaisuuksia ovat parempi verkon suorituskyky, erityisesti silloin, kun verkkoon liitettyjä laitteita on useita, parempi kantama, parempi verkon tehokkuus, sekä liitettyjen laitteiden pienempi virrankulutus. (Näin Wi-Fi 6 toimii – Kaikki mitä sinun tarvitsee tietää 802.11ax:sta 2019.)

3.9 Salausmenetelmät

3.9.1 WEP-menetelmä

Wired Equivalent Privacy on vanha suojausmenetelmä vuodelta 1997, jota ei enää vuodesta 2004 eteenpäin olla virallisesti käytetty sen haavoittuvuuksien vuoksi. WEP salaa liikennettä käyttäen 64- tai 128-bittistä heksadesimaali avainta. Yksi ja sama avain suojasi kaikkea liikennettä. Nykypäivän mittareilla WEP ei ole riittävä suojausmenetelmä, eikä sitä tule käyttää. (WEP, WPA, WPA2 and WPA3: Differences and explanation 2022.)

3.9.2 WPA-menetelmä

WEP:n jälkeen otettiin käyttöön WPA eli *Wi-Fi Protected Access*, joka tuli markkinoille 2003. WPA oli samankaltainen WEP:n kanssa, mutta se tarjosi parannuksia suojausavainten käsittelyyn, sekä siihen kuinka käyttäjät tunnistettiin. WPA käytti myös 256-bittisiä avaimia, mikä oli huomattava parannus WEP:n nähden. (WEP, WPA, WPA2 and WPA3: Differences and explanation 2022.)

3.9.3 WPA2-menetelmä

Wi-Fi Protected Access 2 eli WPA2 on entisestään päivitetympi ja tietoturvallisempi versio WPA:sta. WPA2 on ollut käytössä kaikissa sertifioiduissa Wi-Fi laitteissa vuodesta 2006 alkaen. On suositeltavaa, että WPA2 salausta käytetään aina, kun vain mahdollista. (Mitchell 2021b.)

WPA2:n etuna on sen käyttämä AES-salaus (Advanced Encryption Standard). AES on lohkosalausmenetelmä, jossa salattu viesti pakataan 128 bitin kokoisiin lohkoihin ja salausavaimen koko voi olla joko 128, 192 tai 256-bittiä. (Advanced Encryption Standard (AES) 2021.)

3.9.4 WPA3-menetelmä

Wi-Fi Protected Access 3 on viimeisin langattomien verkkojen suojausmenetelmä ja se julkaistiin vuonna 2018. WPA3 pitää sisällään useita parannuksia, joihin kuuluu turvallisempi julkinen Wi-Fi, heikkojen salasanojen suojaus, sekä entistä helpompi käyttökokemus. (Fisher 2021.)

WPA3 eristää jokaisen istunnon salasanasuojauksella tehden datan keräämisestä ja hyväksi käyttämisestä myöhemmin mahdotonta hakkerointitarkoituksiin. WPA3 myös suojaa heikkoja salasanoja ylimääräisellä suojauksella, joka estää tehokkaasti brute-force-hyökkäyksen, jossa salasanoja yritetään arvata väkisin. (Security 2022.)

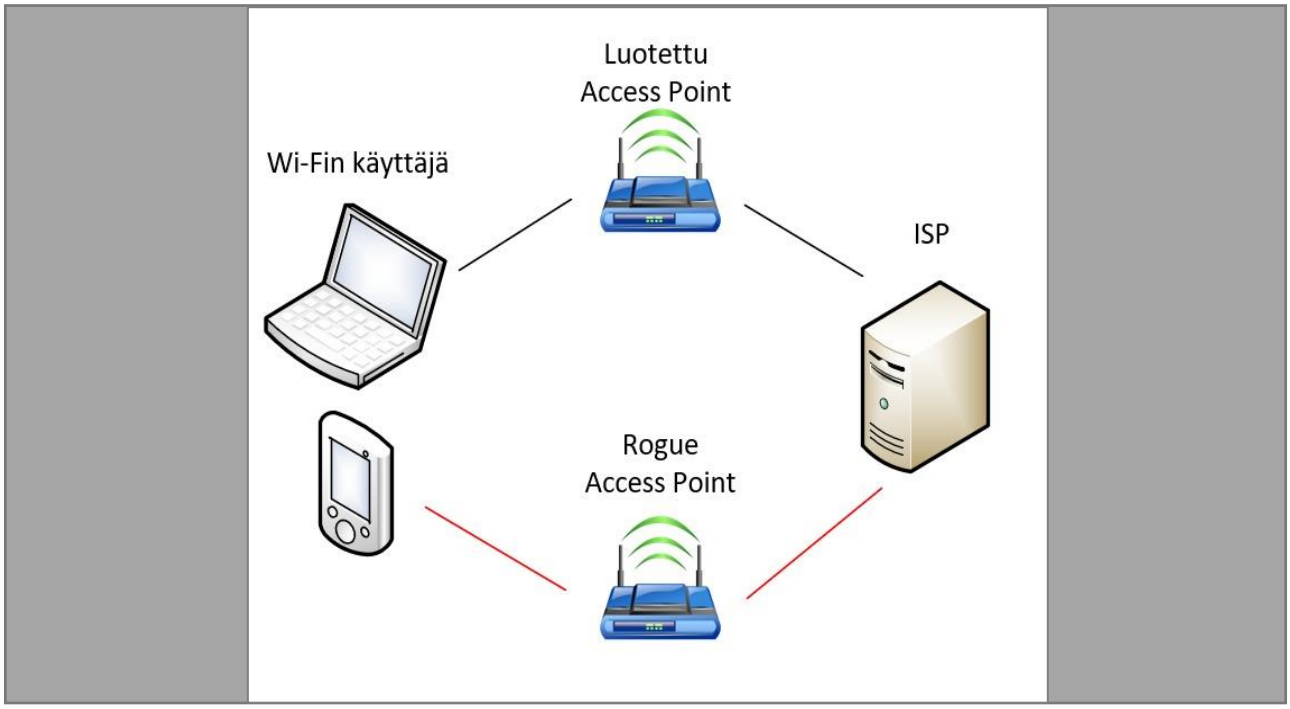
3.9.5 VPN eli virtuaalinen erillisverkko

Virtual Private Network eli virtuaalinen erillisverkko on tehokas tapa suojata oma yksityisyys nettiä käytettäessä. VPN toimii tunnelin tavoin internetyhteyden päällä. Sen sijaan, että laite yhdistäisi suoraan internetiin, se yhdistää VPN-palvelimeen. Tällöin verkkopalvelut näkevät, että kaikki liikenne kulkee VPN-palvelimen kautta ja oma IP-osoite ja sijainti pysyvät salassa. (What Is a VPN? - Virtual Private Network 2022.)

VPN yhteyden liikenne on aina kryptattua eli salattua, mutta on syytä ottaa huomioon, että ilmaista VPN-yhteyttä tulee välttää, sillä se on merkki vaarasta. VPN palvelinta, jonka kautta liikenne kulkee, ylläpitää aina joku taho.

3.10 Rogue Access Point -tukiasema

Rogue Access Point on verkkoon virallisesti kuulumaton tukiasema, joka ei ole verkon haltijan hallinnassa ja se pyrkii jäljittelemään luotettua tukiasemaa (ks. kuvio 4). (Understanding Rogue Access Points 2018.) Jokaisen verkon haltijan, sekä käyttäjän, tulisi tiedostaa Rogue Access Pointin vaarat.



Kuvio 4. Rogue Access Pointin toimintamalli

Shahin mukaan (n.d.) Rogue Access Pointilla voidaan suorittaa joko passiivinen tai aktiivinen datan kaappaus. Passiivisessa kaappauksessa Rogue Access Point lukee käyttäjän dataa, mutta ei voi muokata sitä. Tällöin esimerkiksi salasana syötettäessä http-sivulle, se voidaan lukea selkokielisenä. Tämän lisäksi Rogue Access Point pystyy helposti profiloimaan käyttäjää pitämällä kirjaa käyttäjän vierailemista sivustoista.

Aktiivisessa datan kaappauksessa Rogue Access Point kykenee myös muokkaamaan käyttäjän dataa. Se voi lukea käyttäjän antamaa dataa, muokata sitä haluamallaan tavalla ja lähettää sen eteenpäin. Näin ollen esimerkiksi maksua maksettaessa verkossa, Rogue Access Pointin haltija voi muokata maksun tulevaksi hänen tililleen. (Shah n.d.)

Ilmaiseen langattomaan verkkoon liityttäessä tulee olla tarkkana. Aktiivinen ja passiivinen hyökkäys ovat hyvin ehkäistävissä käyttämällä vain https-sivuja. Suojautumiskeinoja käsitellään lisää luvussa 6.

3.11 Kali Linux-käyttöjärjestelmä

Kali Linux on avoimen lähdekoodin käyttöjärjestelmä, joka pohjautuu Debian-käyttöjärjestelmään. Kali Linux on suunnattu käytettäväksi tietoturva-aukkojen penetraatiotestaukseen, takaisinmallinnukseen, sekä turvallisuuden ylläpitoon. Käyttöjärjestelmä sisältää useita satoja erilaisia työkaluja, joilla voidaan testata järjestelmän tietoturvallisuutta. (What is Kali Linux 2022.)

Kali Linuxin uniikin jakelun vuoksi sitä ei suositella uusille Linux-käyttäjille, eikä käytettäväksi tavallisena käyttöjärjestelmänä, web-suunnitteluun tai pelaamiseen. Kali Linuxin verkkopalvelut on oletuksena otettu pois käytöstä, jotta jakelun eheys voidaan varmistaa kaikissa tilanteissa. Myös bluetooth-palvelu on oletuksena pois käytöstä. (Should I Use Kali Linux 2022.) Linuxista on tarjolla useita erilaisia jakeluita, jotka soveltuvat paremmin perinteisiin tarkoituksiin.

4 Demon toteutus

4.1 Laitteisto

Demo toteutetaan käyttäen Raspberry Pi 3 Model B:ta, jossa on kiinni 16GB:n microSD-muistikortti. Muistikortille on ladattuna Kali Linux-käyttöjärjestelmä. Käyttöjärjestelmä on saatu ladattua muistikortille kytkemällä muistikortti oman tietokoneen muistikorttipaikkaan. Vaihtoehtoisesti olisi mahdollista käyttää esimerkiksi muistikortinlukijaa. Tämän lisäksi tarvitaan tavallinen USB-näppäimistö ja hiiri, sekä näyttö, johon Raspberry Pi kytketään HDMI-kaapelilla. Tarvitaan myös Ethernet kaapeli, jolla Raspberry Pi voidaan kytkeä verkkoon.

Raspberry Pi 3 Model B:n tekniset tiedot:

Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
1GB RAM
BCM43438 wireless LAN and Bluetooth Low Energy (BLE) on board
100 Base Ethernet
40-pin extended GPIO

4 USB 2 ports
4 Pole stereo output and composite video port
Full size HDMI
CSI camera port for connecting a Raspberry Pi camera
DSI display port for connecting a Raspberry Pi touchscreen display
Micro SD port for loading your operating system and storing data
Upgraded switched Micro USB power source up to 2.5A (Raspberry Pi 3 Model B. N.d.)

4.2 Ohjelmistot

Rogue Access Point on mahdollista toteuttaa useilla eri tavoilla. Tätä työtä varten työkaluksi valikoitui Wifipumpkin3, koska se on ilmainen ja se sisältää juuri tarvittavat työkalut demon toteutusta varten. Wifipumkin3:n etuihin kuuluvat mm. helppo käyttöliittymä, captiveflask (lisäosa, joka luo valheellisen kirjautumisikkunan), sekä automaattinen käyttäjätietojen haaliminen (uhrin ne syötettyä). (Wifipumpkin3 2022.)

Toinen hyvä vaihtoehto olisi ollut Wifi Pineapple, mutta tämä tuote on maksullinen. Hak5:n valmistama Wifi Pineapple on heti käyttövalmis tuote, jolla esim. yrityksen olisi mahdollista testata omaa tietoturvaansa. Laitetta markkinoidaankin juuri tähän käyttötarkoitukseen, mutta sitä olisi mahdollista käyttää myös pahoihin tarkoituksiin. Pitkälle tuotteistettu Wifi Pineapple on myös helppokäyttöinen työkalu ja sisältää helppokäyttöisen käyttöliittymän. Sen ominaisuuksiin kuuluu mm. patentoitu PineAP Suite, joka imitoi haluttua verkkoa mahdollistaen näin tietojen kalastelun. Tämän lisäksi Wifi Pineapple myös pyrkii tunnistamaan automaattisesti hyökkäykselle alttiita laitteita ja kohdistamaan hyökkäyksiä niihin. (Wifi Pineapple N.d.)

4.3 Asennusvaiheen kuvaus ja demon tavoitteet

Työ on luonnollista aloittaa keräämällä kaikki tarvittavat laitteet yhteen. Toteutukseen tarvitaan Raspberry Pi 3 Model B (myös uudempi versio 4 käy), microSD-muistikortti (16Gb muistia), USB-näppäimistö, USB-hiiri, sekä näyttö. Tarvitaan myös oma tietokone, jonka avulla voidaan ladata muistikortille Kali Linux -käyttöjärjestelmä, sekä myöhemmin muodostaa etäyhteys Raspberry Pi:hin. Käyttöjärjestelmän latausta varten tietokoneessa tulee olla muistikorttipaikka tai sitten vaihtoehtoisesti voidaan käyttää erillistä muistikortin lukijaa.

Kun Kali Linux-käyttöjärjestelmä on saatu ladattua muistikortille, se voidaan kytkeä kiinni Raspberry Pi:hin ja kytkeä siihen myös näppäimistö, näyttö ja hiiri. Ensimmäiseksi Kali Linuxille kirjauduttaessa, niin kuin myös esimerkiksi Windows -käyttöjärjestelmälle, on syytä luoda oma käyttäjätunnus, sekä asentaa uusimmat päivitykset.

Työn suorittaminen on luontevampaa, sekä se vastaan enemmän todellista tilannetta, kun SSH eli etäyhteys mahdollistetaan Raspberry Pi:lle. Näin laitetta voidaan hallita omalta tietokoneelta täysin etänä. Etäyhteys tulee mahdollistaa erillisillä komennoilla.

Demon tavoitteena on imitoida toista, olemassa olevaa verkkoa. Luomalla olemassa olevan verkon rinnalle samanniminen verkko, voidaan hämätä käyttäjää luulemaan, että kyseessä on aito verkko. Kuvitellaan esimerkiksi tilanne, jossa oppilaitoksessa on käytössä Wi-Fi-vierailijaverkko, joka vaatii käyttäjän kirjautumisen omia, olemassa olevia, käyttäjätunnuksia käyttäen. Kun luodaan varsinaisen verkon rinnalle samanniminen verkko, jossa kirjautumisikkuna näyttää samalta kuin varsinaisen verkon, käyttäjä syöttää tajuamattaan omat kirjautumistietonsa Rogue Access Pointin haltijan näkyville ja hän voi sen jälkeen käyttää niitä haluamallaan tavalla.

4.4 Asennus

Ensimmäiseksi asennetaan muistikortille Kali Linux-käyttöjärjestelmä. Kali Linuxin virallisilta sivuilta saa ARM-imagen, joka on suunnattu mikroprosessoreille eli se soveltuu juuri Raspberry Pi:lla käytettäväksi. Vaihtoehtoja olisivat esimerkiksi virtuaaliympäristöt ja puhelin. Mikäli tietokoneessa on paikka muistikortille, asennuksen voi suorittaa suoraan siihen. Tässä vaihtoehtona olisi myös esim. ulkoinen SD-kortin lukija.

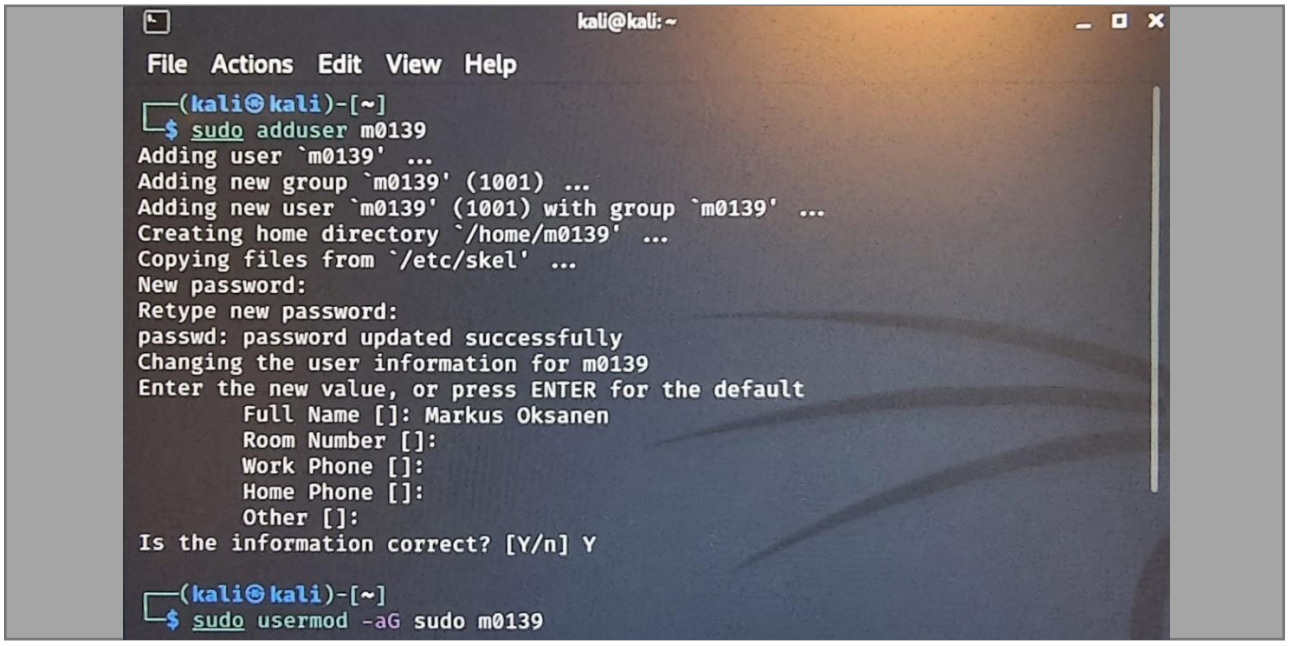
Kun Kali Linux on ladattu, voidaan muistikortti liittää Raspberry Pi:hin. Aluksi Raspberry Pi:hin täytyy kytkeä myös näyttö, näppäimistö ja hiiri, jotta voidaan laittaa sen asetukset kuntoon SSH-yhteyden muodostamista varten.

Rogue Access Point toteutetaan Wifipumpkin3 -työkalulla, joka voidaan asentaa seuraavaksi. Tässä vaiheessa työkalu on käyttövalmis.

Demon tavoitteena on imitoida käyttäjän kirjautumista jo olemassa olevaan vierasverkkoon, esim. oppilaitoksen salasanalla suojattuun langattomaan verkkoon. Yleisesti tällaiseen verkkoon kirjaudutaan omilla henkilökohtaisilla tunnuksilla. Mikäli käyttäjä kirjautuu näillä tunnuksilla luomaamme verkkoon, saamme heidän käyttäjätunnuksensa ja salasanansa näkyviin selkokielisenä.

Ensimmäisellä kirjautumiskerralla käyttöjärjestelmään pääsee sisään vakiokäyttäjätunnuksella ja salasanalla ”kali/kali”. Sisäänkirjautumisen jälkeen lisätään oma käyttäjä ”m0139” (ks. kuvio 5) ja muokataan käyttäjän ryhmää komennoilla:

sudo adduser m0139
sudo usermod -aG sudo m0139



Kuvio 5. Oman käyttäjän lisääminen Linux-käyttöjärjestelmään

Komento ”sudo adduser m0139” yksinkertaisesti lisää käyttäjän nimeltä ”m0139” järjestelmään. Komento ”sudo usermod -aG sudo m0139” lisää uuden käyttäjän järjestelmänvalvojien ryhmään. Parametri ”-a” lisää ryhmän ja ”-G” määrittää ryhmän.

Jotta järjestelmään voi muodostaa etäyhteyden, täytyy asentaa sen käyttöön tarkoitettu RDP-serveri. Tämä tapahtuu komennoilla:

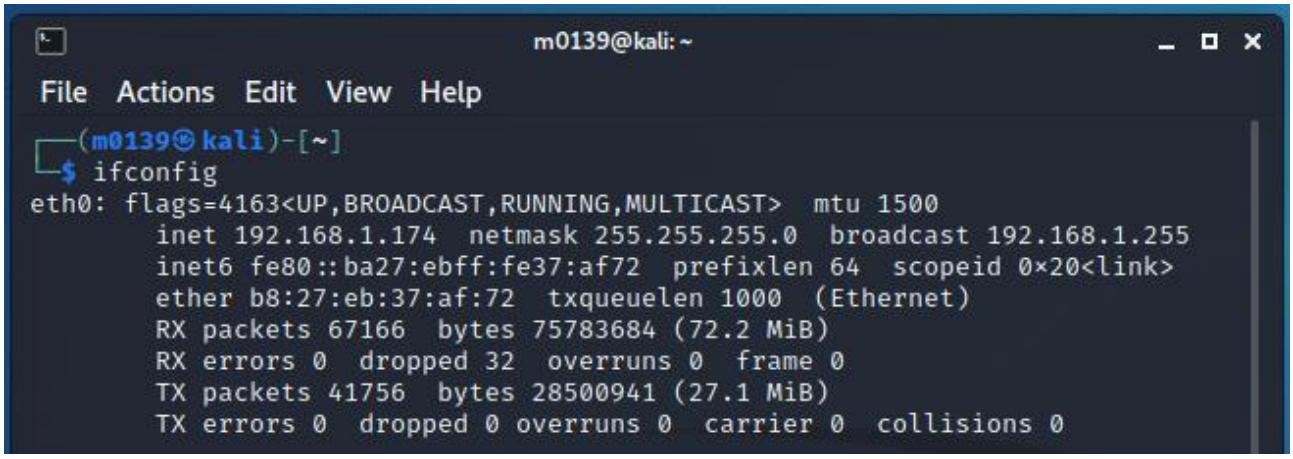
sudo apt-get update
sudo apt-get install xrdp
sudo systemctl start xrdp
sudo systemctl start xrdp-sesman

Ensimmäinen komento ”sudo apt-get update” asentaa järjestelmän uusimmat päivitykset. Komento ”sudo apt-get install xrdp” asentaa etäyhteyteen tarvittavan RDP-serverin. Seuraava komento ”sudo systemctl start xrdp” käynnistää XRDP-kantaserverin. Ja lopuksi komennolla ”sudo systemctl start xrdp-sesman” käynnistetään XRDP-serverin istunto manageri (session manager), joka hallitsee käyttäjien istuntoja todentamalla käyttäjän ja käynnistämällä sopivan XRDP serverin. (Enabling Remote Desktop and SSH access to Kali N.d)

Näiden komentojen syöttämisen myötä SSH-yhteyden muodostaminen on mahdollista. On kuitenkin käytännöllistä, että XRDP serveri käynnistyy aina Raspberry Pi:n käynnistyksen yhteydessä. Tätä varten tulee syöttää vielä komennot:

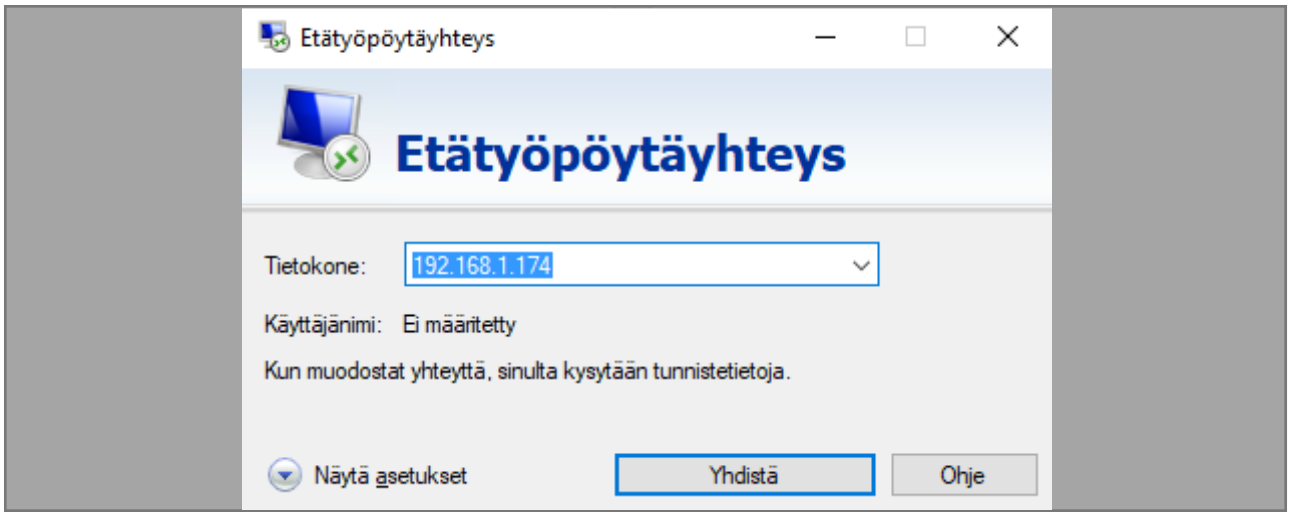
sudo systemctl enable xrdp
sudo systemctl enable xrdp-sesman

SSH-yhteyden muodostamiseen tarvitaan järjestelmän IP-osoite. Tämä saadaan selville syöttämällä komento ”ifconfig” (ks. kuvio 6). IP-osoitteeksi paljastuu 192.168.1.174.



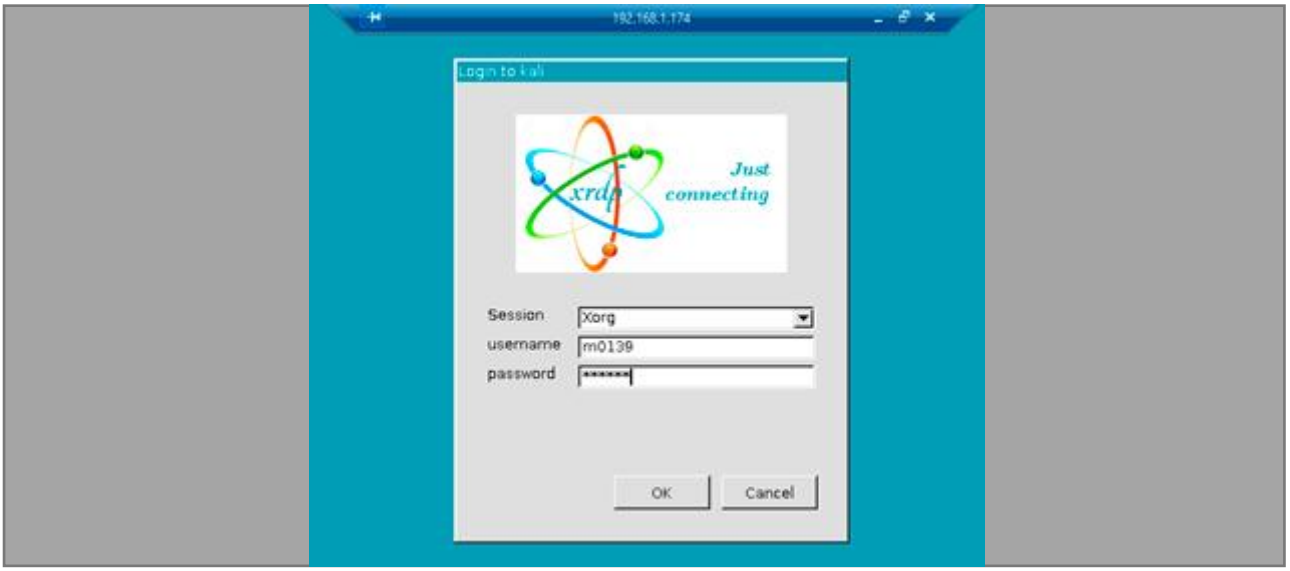
Kuvio 6. Oman IP-osoitteen tarkistaminen

SSH eli etäyhteyden muodostamiseen voidaan käyttää Windows-käyttöjärjestelmän omaa ”Etätyö-pöytäyhteys”-sovellusta (ks. kuvio 7).



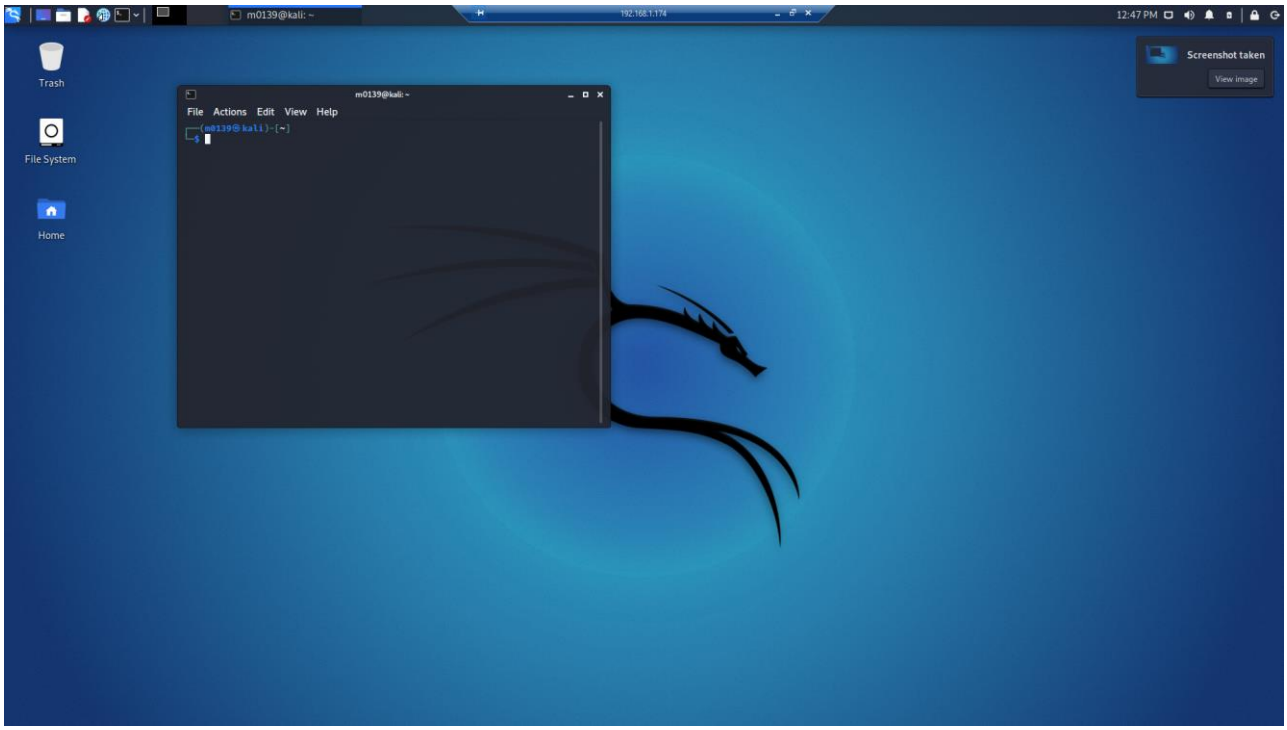
Kuvio 7. SSH-yhteyden muodostaminen

Yhdistämisen jälkeen eteen avautuu kirjautumisikkuna, johon syötetään aiemmin luodun uuden käyttäjän ”m0139” tiedot (ks. kuvio 8).



Kuvio 8. Linuxiin kirjautuminen SSH-yhteyden avulla

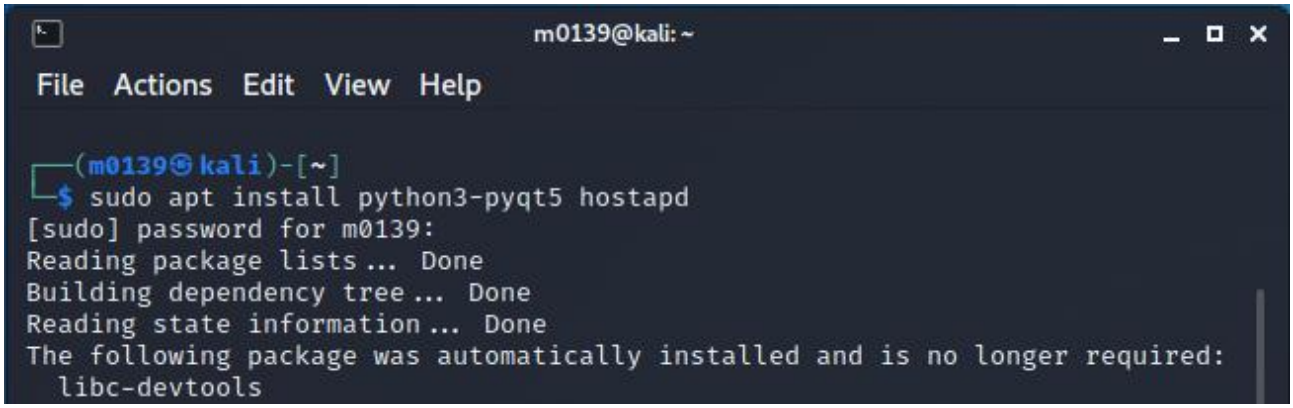
Nyt yhteys on muodostettu ja Kali Linuxin käyttö onnistuu täysin omalta koneelta (ks. kuvio 9) etäyhteydellä.



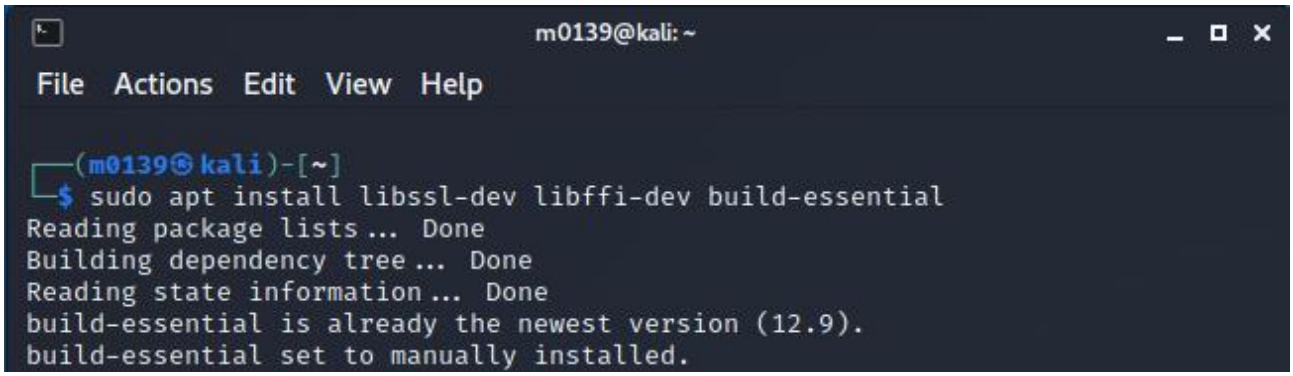
Kuvio 9. Onnistunut yhteyden muodostaminen

Demossa käytettävän Wifipumpkin3:n asennus aloitetaan (ks. kuviot 10 ja 11) komennoilla:

sudo apt install python3-pyqt5 hostapd
sudo apt install libssl-dev libffi-dev build-essential



Kuvio 10. Wifipumpkin3-ohjelman asennuksen aloitus

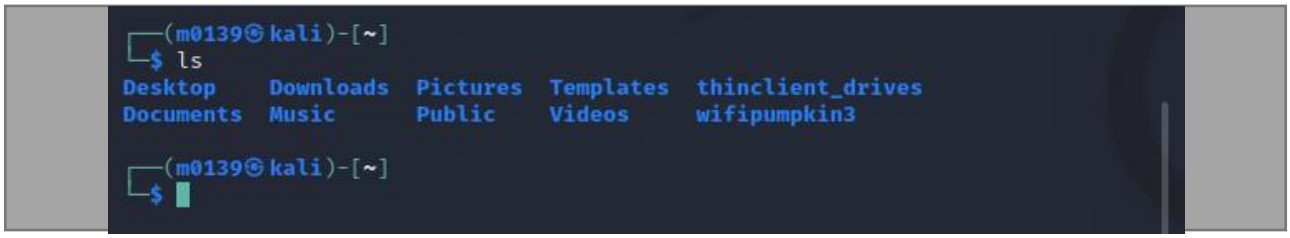


Kuvio 11. Wifipumpkin3-ohjelman asennuksen toinen vaihe

Komentojen jälkeen Wifipumpkin3 voidaan asentaa. Asennusta varten on olemassa valmis GitHub-repositorio, joka voidaan ladata komennolla:

git clone https://github.com/P0cL4bs/wifipumpkin3.git

Latauksen jälkeen tarkistetaan, että Wifipoumpkin3 löytyy hakemistosta komennolla ”ls” (ks. kuvio 12).



Kuvio 12. Wifipumpkin3-ohjelman tiedostosijainti

Wifipumpkin3 pitää vielä asentaa, joka tapahtuu komennoilla:

cd wifipumpkin3
sudo python3 setup.py install

Asennuksen jälkeen ohjelma käynnistetään komennolla (ks. kuvio 13):

sudo wifipumpkin3

Kuvio 13. Wifipumpkin3-ohjelma käynnissä

5 Demo

Wifipumpkin3:n ollessa käynnissä, voidaan aloittaa Rogue Access Pointin konfigurointi. Rogue AP:lle tulee asettaa wlan, verkon nimi (SSID) ja tämän lisäksi otetaan dns login pois käytöstä. Nämä tapahtuvat komennoilla:

set interface wlan0
set ssid testi
ignore pydns_server

Wifipumpkin3:n käytettävissä olevat moduulit saa näkyviin komennolla ”show” (ks. kuvio 14).

```
wp3 > set interface wlan0
wp3 > set ssid demo_m0139
wp3 > ignore pydns_server
wp3 > show

[*] Available Modules:
 ═══════════════════

 Name                      | Description
 ──────────────────────────+──────────────────────────────────────────────────
 misc.extra_captiveflask   | Extra customs captiveflask templates
 spoof.dns_spoof           | Perform a dns spoof with accesspoint attack
 wifi.wifideauth           | Sends deauthentication packets to a wifi network AP
 wifi.wifiscan             | Scan WiFi networks and detect devices


wp3 >
```

Kuvio 14. Wifipumpkin3-ohjelman moduulit

Aluksi käynnistetään Wifipumpkin3 komennolla:

start

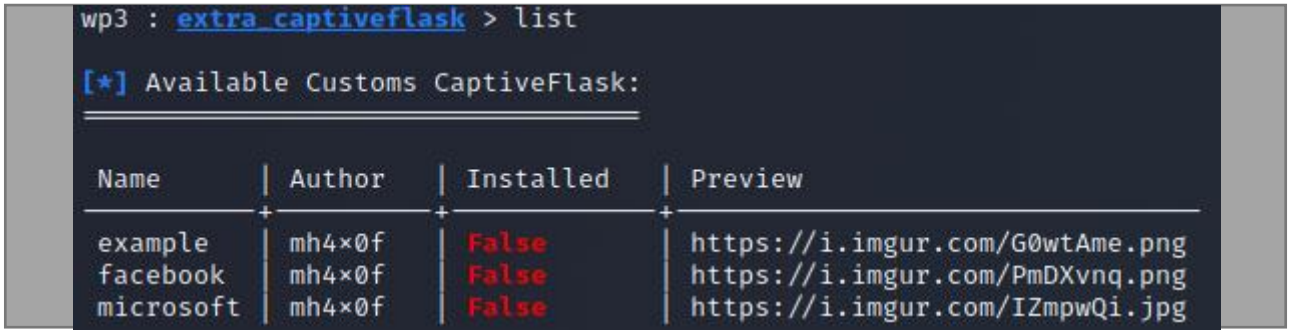
Demo toteutetaan käyttäen captiveflaskin sisäänrakennettuja pohjia, jotka saadaan käyttöön komennoilla:

use misc.extra_captiveflask
download

Asentamisen jälkeen voidaan tarkastella valmispohjia komennolla (ks. kuvio 15):

list

List-komento listaa kaikki käytössä olevat valmispohjat.



Kuvio 15. Wifipumpkin3-ohjelman captiveflask-valmispohjat

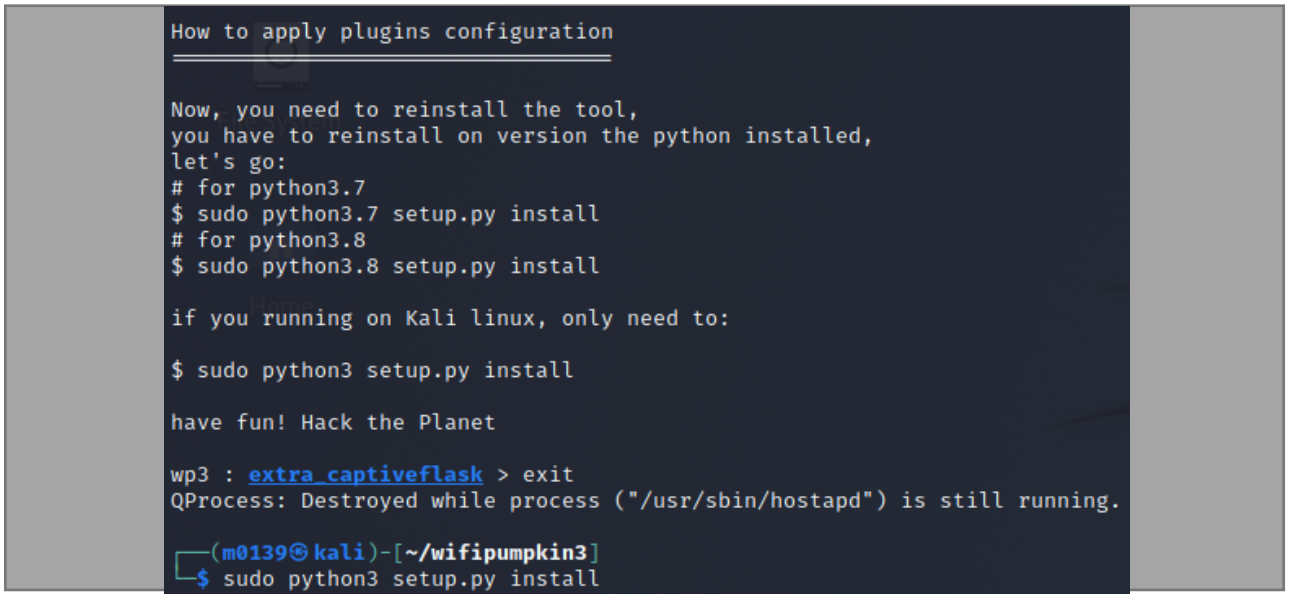
Valittavina on kolme eri vaihtoehtoa, joista kaikista on myös nähtävillä kuvat kirjautumissivun ulkoasusta. Tämän lisäksi olisi mahdollista myös luoda oma kirjautumissivu, niin halutessaan. Demossa käytetään ”example” vaihtoehtoa. Tämä voidaan asentaa käyttöön komennolla:

install example

Valmispohjan asennuksen jälkeen Wifipumpkin3-ohjelma tulee asentaa vielä uudelleen. Asennus tapahtuu samalla komennolla kuin aiemminkin eli (ks. kuvio 16):

sudo python3 setup.py install

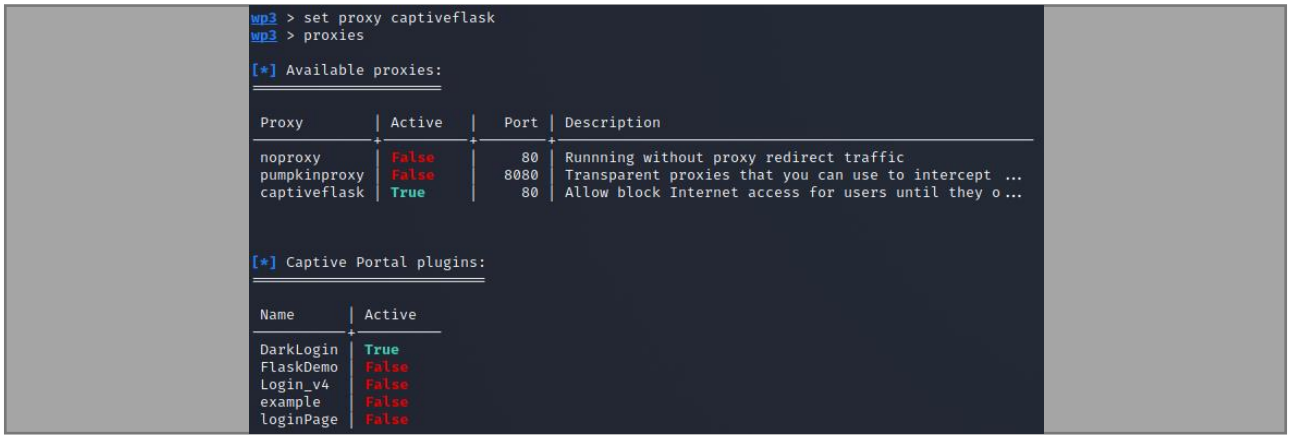
Uudelleenasennus kestää yhtä kauan kuin asennus ensimmäisellä kerralla.



Kuvio 16. Wifipumpkin3-ohjelman uudellenasennus

Wifipumpkin3-ohjelman uudelleenasennuksen jälkeen asetetaan vielä captiveflask proxy aktiiviseksi komennolla (ks. kuvio 17):

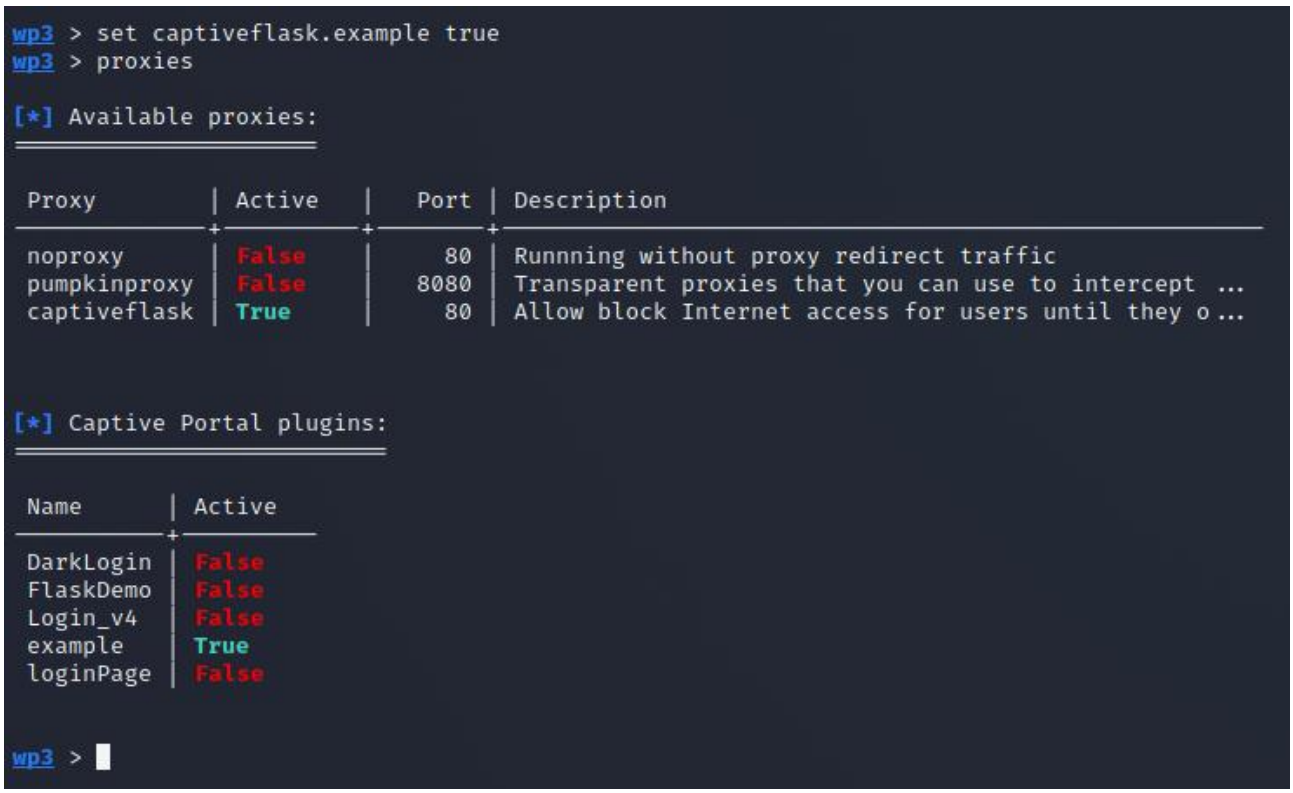
set proxy captiveflask



Kuvio 17. Captiveflask proxyn asettaminen aktiiviseksi

Kun captiveflask on aktiivinen, voidaan yksi sen valmiista käyttöliittymistä ottaa käyttöön. Tässä tapauksessa otetaan käyttöön ”example” niminen käyttöliittymä ja se tapahtuu komennolla (ks. kuvio 18):

set captiveflask.example true

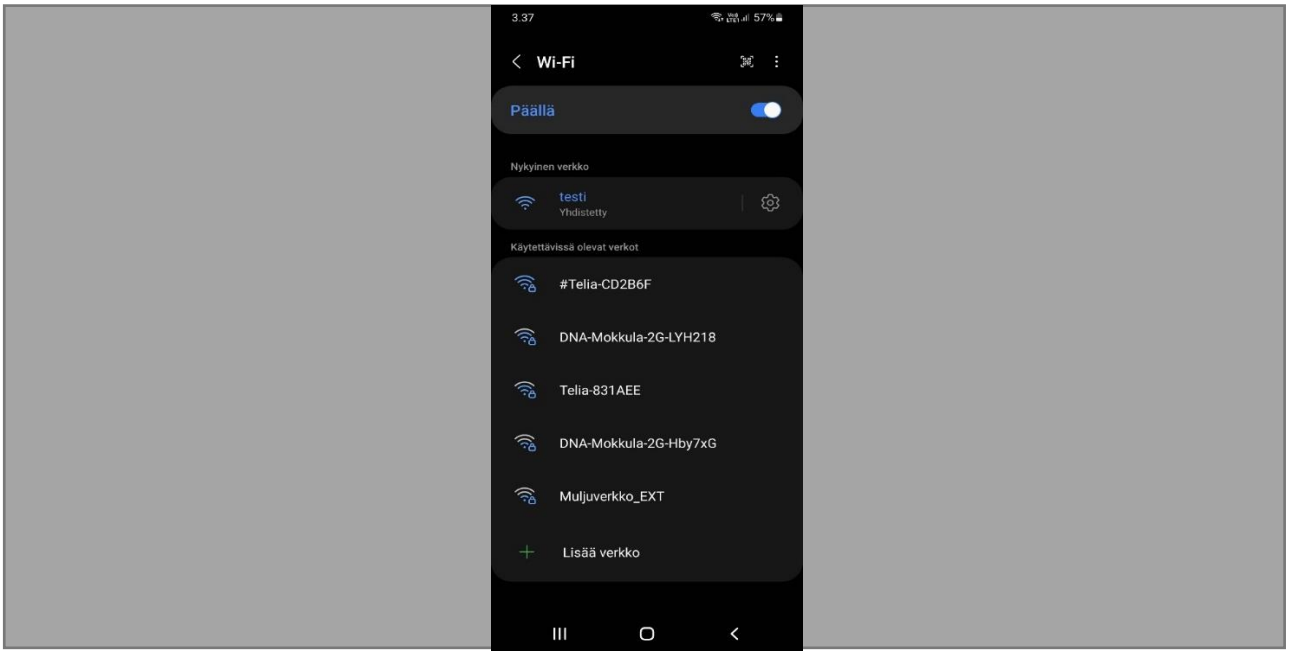


Kuvio 18. Captiveflaskin ”example” -käyttöliittymä käytössä

Rogue AP käynnistyy tämän jälkeen komennolla:

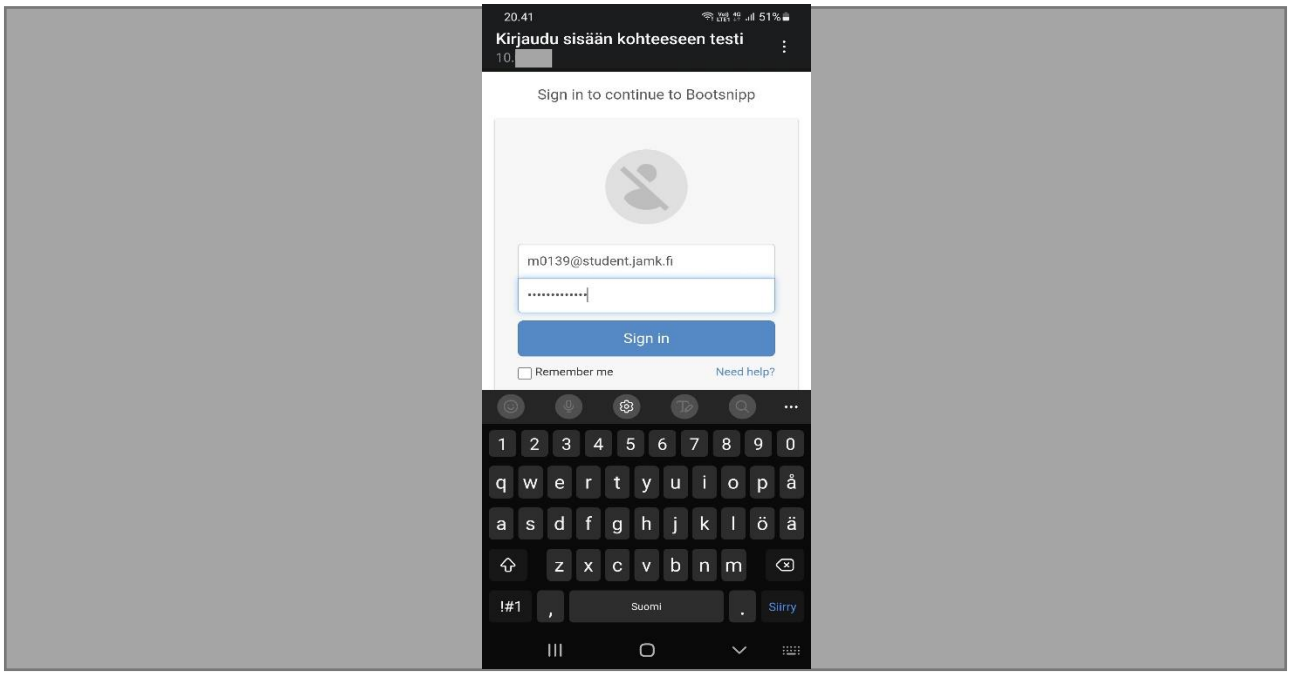
start

Kun Rogue AP on käynnissä, puhelin löytää luodun testiverkon, kuten minkä tahansa langattoman verkon ja siihen päästään yhdistämään (ks. kuvio 19).



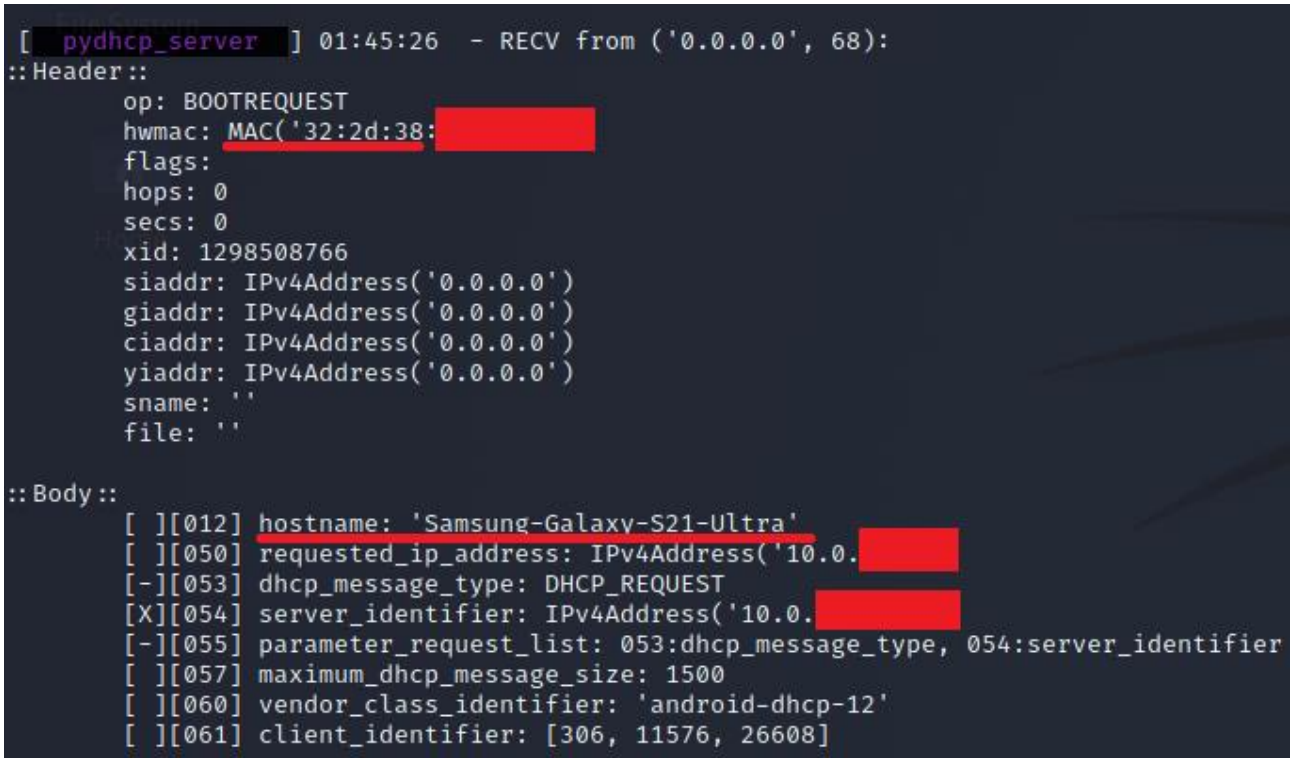
Kuvio 19. Testiverkko käytettävissä

Kirjautumista varten syötetään omat tunnukset samaan tapaan kuin oltaisiin kirjautumassa vieras-verkkoon (ks. kuvio 20).



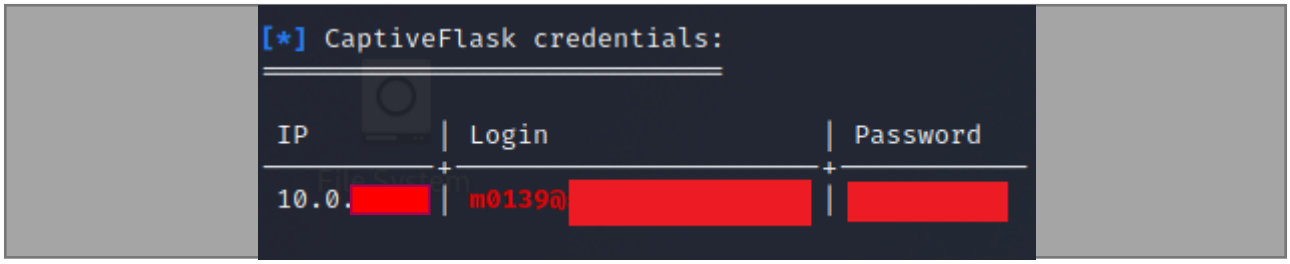
Kuvio 20. Testiverkon kirjautumisikkuna

Kun puhelimesta on kirjauduttu ”testi”-verkkoon ohjelma näyttää heti kirjautujan tiedot. Alla olevasta kuvasta nähdään laitteen MAC-osoite, sekä se että kirjautumiseen on käytetty Samsung Galaxy S21 Ultra-puhelinta (ks. kuvio 21).



Kuvio 21. Kaapatut tiedot

Tämän lisäksi nähdään myös käyttäjän kirjautumiseen käyttämä sähköpostiosoite, sekä salasana selkokielisenä (ks. kuvio 22).



Kuvio 22. Kaapattu sähköposti ja sen salasana

6 Tietoturvan kohentaminen

Jokaisen verkon käyttäjän, kuin myös verkon ylläpitäjän, on syytä tiedostaa Rogue AP:n vaarat. Valveutuneisuus ja maalaisjärjen käyttö ovatkin yksiä tärkeimmistä keinosta, kun puhutaan tietoturvan kohentamisesta. Verkon käyttäjän tulee olla tarkkana liityttäessä suojaamattomaan verkkoon. Luvussa 5 käytiin läpi, kuinka Rogue AP:n haltija voi määritellä verkolle haluamansa nimen eli SSID:n. Tästä syystä on syytä kiinnittää huomiota siihen, onko tarjolla enemmän kuin yksi samanniminen verkko, koska tällöin kyseessä voi olla Rogue AP.

Tukiaseman signaalin voimakkuus vaikuttaa myös turvallisuuteen. Päätelaite, esimerkiksi puhelin, listaa saatavilla olevia verkkoa niiden signaalin voimakkuuden perusteella. Päätelaite voi myös olla asetettu liittymään saatavilla olevaan verkkoon automaattisesti. Tästä syystä tukiaseman signaalin voimakkuutta kannattaa pyrkiä tehostamaan. Mikäli Rogue Access Pointin signaalin voimakkuus on parempi kuin varsinaisen tukiaseman, päätelaite voi pyrkiä yhdistämään siihen.

Käyttäjä voi kohentaa tietoturvaansa ottamalla automaattisen verkkoon yhdistämisen pois käytöstä esimerkiksi tietokoneelta tai puhelimesta. Tämän lisäksi Wi-Fi tai WLAN kannattaa kytkeä pois päältä silloin, kun sitä ei käytetä. Näitä vaihtoehtoja avataan tarkemmin luvussa 6.1.

Verkkoa hallinnoivan organisaation on tärkeää ylläpitää ajantasaista listaa laitteistaan, jotta Rogue AP:n voi helposti erottaa luotetusta tukiasemasta. Tukiaseman ylimääräiset portit ja palvelut kannattaa myös ottaa pois käytöstä. (Information Supplement: PCI DSS Wireless Guideline 2009). Käyttäjä voi suojata itseään vierailemalla vain suojatuilla HTTPS-sivustoilla, sekä käyttämällä VPN:ää. (Shah n.d.) Käyttäjän kannattaa siis tarkkailla vierailemansa sivuston osoiteriviä.

Rogue AP voidaan tunnistaa myös Wi-Fi-skannerin avulla, joka pystyy skannaamaan tukiasemille yksilöllisen BSSID-tunnuksen. Siinä missä tukiasemalla voi olla kaksi samanlaista SSID-tunnusta, BSSID-tunnus on aina yksilöllinen. Skannauksen jälkeen Rogue AP voidaan fyysisesti paikantaa seuraamalla vastaanotetun signaalin voimakkuutta. (Kaleem 2017.) BSSID on käytännössä laitteen MAC-osoite (Understanding the Network Terms SSID, BSSID, and ESSID 2018). Mikäli siis tunnetut laitteet on listattu, voidaan vieraan laitteen MAC-osoite tunnistaa helpommin ja nopeammin.

Verkon haltijan tulisi myös pystyttää asianmukaiset palomuurit suojaamaan verkkoa. On tärkeää käydä läpi palomuurin lokitiedostot läpi ja tarkistaa palomuuriin luodut säännöt riittävän usein. Oma tukiasema on myös syytä suojata niin, että ulkoiset käyttäjät eivät pääse siihen fyysisesti käsiksi. Tukiaseman voi esimerkiksi kiinnittää kattoon ja sen ympärille voi asentaa tukevan suojan. (Information Supplement: PCI DSS Wireless Guideline 2009.)

On tärkeää käydä läpi tukiaseman järjestelmänhaltijan asetukset. Usein tukiaseman oletusasetuksista löytyy heikkoja salasanoja, joita on helppo kalastella. Tukiaseman järjestelmänhaltijan oletuskäyttäjätunnus ja salasana saattavat olla esim. ”admin” ja ”11111”. (Information Supplement: PCI DSS Wireless Guideline 2009.) Tämä on luonnollisesti erittäin vakava tietoturvariski, mutta helposti vältettävissä vaihtamalla tunnukset ja käyttämällä vahvaa salasanaa.

Myös tukiaseman käyttämään suojausmenetelmään on syytä kiinnittää huomiota ja varmistaa, mikä suojausmenetelmä on oletuksena käytössä. On ehdottoman suositeltavaa käyttää vähintäänkin WPA2-salausmenetelmää. (Information Supplement: PCI DSS Wireless Guideline 2009.) Salausmenetelmiä käsiteltiin tarkemmin luvussa 3.9.

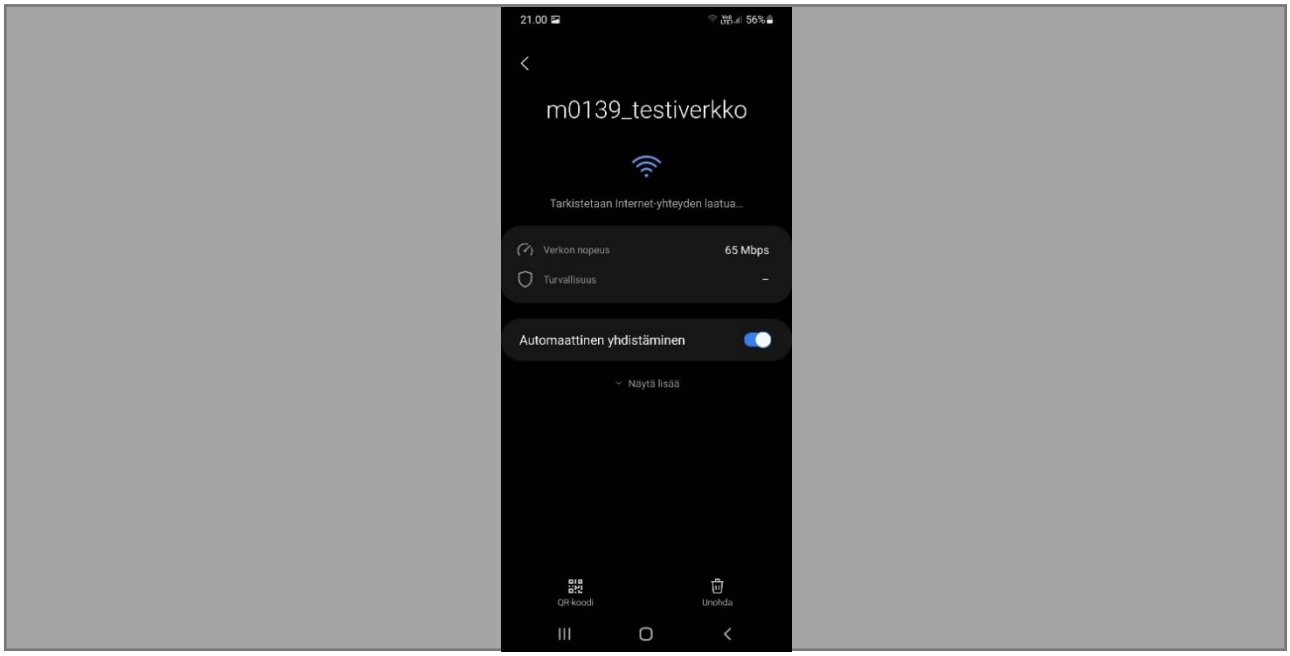
Samalla, kun käydään tukiaseman järjestelmänhaltijan asetukset, sekä tarkistetaan käytössä oleva suojausmenetelmä, on suositeltavaa myös vaihtaa SSID:n oletusnimi. Ei ole kuitenkaan suositeltavaa käyttää omaa organisaatiota mainostavaa tai helposti tunnistettavaa SSID:tä huomion välttämiseksi. Yksi vaihtoehto on olla mainostamatta langatonta verkkoa ollenkaan eli piilottaa SSID. SSID:n piilottaminen ei kuitenkaan ole suoranaisesti turvallisuusmekanismi, sillä kokeneempi käyttäjä voi saada sen silti selville. (Information Supplement: PCI DSS Wireless Guideline 2009.)

Myös Rutledge (2020) toteaa, että SSID:n piilottamisella on hyvät ja huonot puolet. Hyvänä puolena on, että potentiaalinen hyökkääjä ei välttämättä edes saa tietoonsa, että tällainen verkko on olemassa, koska se ei ole näkyvillä. Kokemattomampi hyökkääjä ei valitse kohteekseen tällaista verkkoa niin todennäköisesti kuin helpommin saatavilla olevaa. Huonona puolena taas on, että mikäli kyseessä on kokeneempi hyökkääjä, ei SSID:n piilottamisella ole juurikaan merkitystä, sillä verkko on siitä huolimatta löydettävissä. ”Täällä käytetään piilotettua verkkoa”-tyyppinen haaste saattaa houkutella kokeneempaa hyökkääjää. (Rutledge 2020.)

6.1 Tietoturvan kohentamisen demo

Selvittääksemme tarkemmin aiemmin luvussa 6 kuvattujen suojauskeinojen toimivuutta, testattiin niitä käytännössä demoamalla. Demo toteutettiin kotioloissa, mutta sitä olisi ollut mielenkiintoista testata laajemmassa mittakaavassa, esimerkiksi yrityksen toimitiloissa. Laitteina käytettiin Raspberry PI:ta, kodin reititintä, sekä omaa Android-puhelinta. Jotta demossa voitiin osoittaa käytännönläheisesti ja selkeästi laitteiden ja Rogue Access Pointin toimintaa, muokattiin ensin kodin reitittimen asetuksista kodin verkon nimi muotoon ”m0139_testiverkko”. Kodin verkkoni haltijana pääsen sen asetuksiin selaimen kautta. Tämän jälkeen otettiin Rogue Access Point jälleen käyttöön käyttämällä luvussa 5 esiteltyjä komentoja. Komennolla ”*set ssid m0139_testiverkko”* voitiin asettaa Rogue Access Pointille sama SSID kuin kodin verkolle, käytössä oli siis kaksi täysin samannimistä verkkoa. Tosielämän tilanteessa Rogue Access Pointin käyttäjä pyrkisi ensin saamaan tietoonsa halutun verkon nimen.

Kun Rogue Access Point oli toiminnassa, voitiin kokeilla liittyä molempiin saatavilla oleviin verkkoihin puhelimella. Kuviossa 23 puhelin on liittynyt Rogue Access Pointilla luotuun verkkoon.

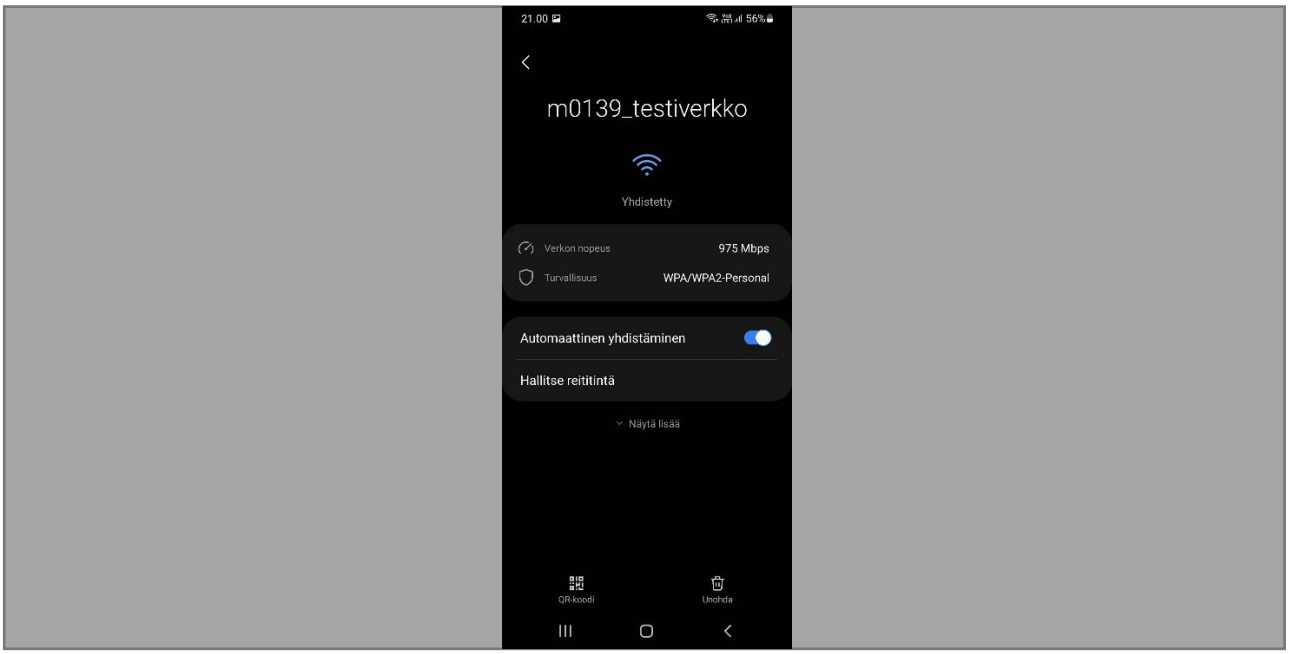


Kuvio 23. Rogue Access Pointin tietoja

Kuvasta voidaan havaita kaksi asiaa, ensinnäkin turvallisuustasoa eli salausmenetelmää ei ole määritelty ja toisekseen automaattinen yhdistäminen on käytössä. Salausmenetelmiä käsiteltiin tarkemmin luvussa 3.9. Käyttäjän kannattaa siis tarkastaa käyttämältään laitteelta, mikä on käytössä olevan verkon suojausmenetelmä ja pyrkiä välttämään verkon käyttöä, mikäli suojausmenetelmää ei ole. Tämä tieto on suhteellisen helppoa tarkistaa ja tapa siihen vaihtelee hieman laitteesta riippuen. Tässä demossa käytettiin Samsung puhelinta, jossa on Android-käyttöjärjestelmä. Asetuksen tarkistaminen onnistuu tällöin valitsemalla puhelimesta Asetukset, Yhteydet ja Wi-Fi. Tässä näkymässä voi tarkastella käytettävissä olevia verkkoja. Käytössä olevan verkon asetuksia voi tarkastella painamalla ”hammasrattaan”-kuvaketta, jolloin saa näkyviin Kuvion 23 mukaisen näkymän.

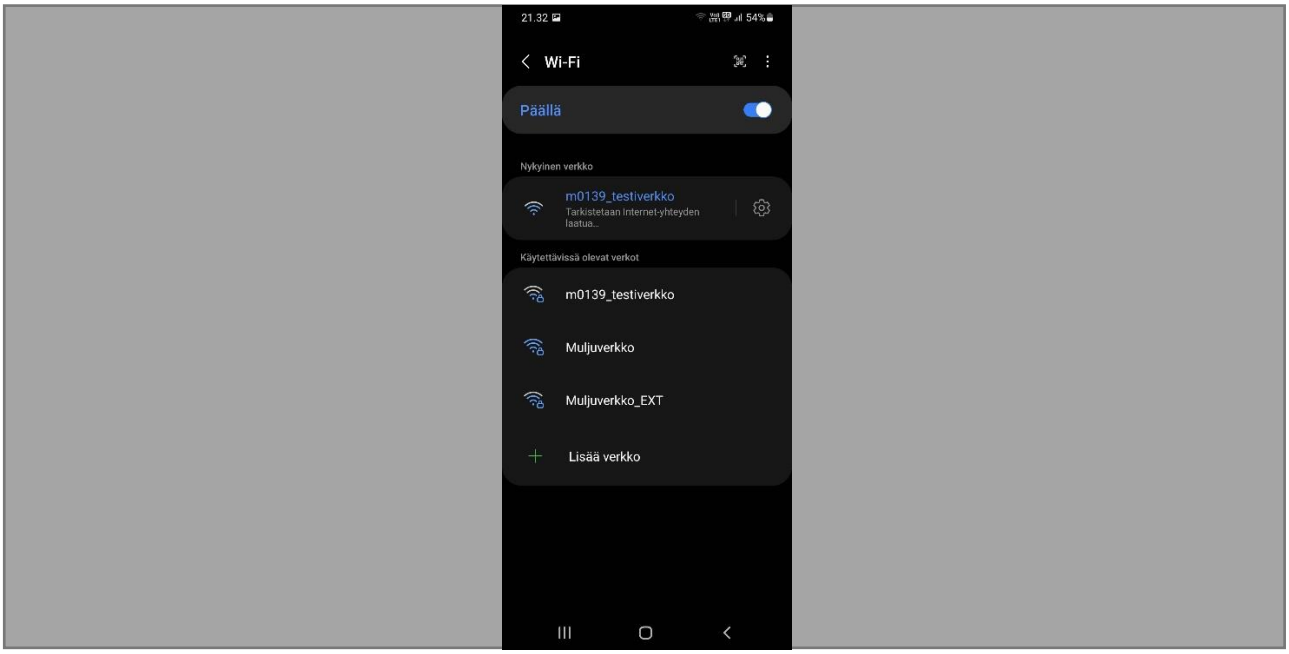
Automaattinen yhdistäminen kannattaa myös ottaa pois käytöstä, mikäli haluaa parantaa omaa tietoturvaansa. Asetus on usein oletuksena päällä. Tämä tarkoittaa, että laite pyrkii yhdistämään tähän verkkoon automaattisesti, kun se on sen kantaman sisällä. Jos asetuksen ottaa pois päältä, käyttäjän tulee valita saatavilla olevista verkoista manuaalisesti se, jota halutaan käyttää. Tämä osaltaan myös herättelee käyttäjää, mikäli hän huomaa kantaman sisällä olevan useampia samannimisiä verkkoja. Näin voidaan myös estää laitetta yhdistämästä tahtomattaan mahdolliseen Rogue Access Pointiin.

Kuviossa 24 nähdään puhelin liittyneenä kodin omaan verkkoon, joka on luotettu verkko. Verkon asetuksista nähdään, että suojauksena on käytössä WPA/WPA2-Personal, joka vastaa tämän hetken suosituksia. Kuviossa nähdään niin ikään, että automaattinen yhdistäminen on käytössä. Asetus kannattaa oman tietoturvan parantamiseksi ottaa pois käytöstä.



Kuvio 24. Access Pointin tietoja

Seuraavaksi testattiin signaalin voimakkuuden vaikutusta puhelimen käyttämään verkkoon. Myös automaattisen yhdistämisen asetus on tässä avainasemassa. Kuviossa 25 voidaan nähdä molemmat saatavilla olevat verkot. Kodin verkko on suojattu, jonka huomaa pienestä lukonkuvakkeesta signaalin voimakkuuden kuvakkeen päällä. Kun puhelimen Wi-Fin laittaa päälle, se pyrkii automaattisesti yhdistämään kodin verkkoon, joka on sille entuudestaan tuttu. Demoa varten kasvatettiin kodin reitittimen ja Rogue Access Pointin etäisyyttä toisistaan ja sijoitettiin kodin reititin hieman piiloon rakenteiden taakse. Metalliset, lasiset ja betoniset rakenteet heikentävät signaalin voimakkuutta. Kun puhelimen etäisyyttä kasvatettiin tarpeeksi tukiasemista, saatiin tulos, jossa Rogue Access Pointin signaali on voimakkaampi kuin kodin verkon signaali ja tämä käy ilmi kuviosta 25. Puhelimessa Wi-Fi oli päällä ja kun se vietiin riittävän kauaksi tukiasemista, yhteys katkesi kokonaan. Kun lähestyttiin tukiasemia, puhelin tuli aluksi Rogue Access Pointin tarjoamalle paremmalle kantamalle ja yhdisti siihen automaattisesti. Myös tämä voidaan havaita kuviosta 25. Näin voitiin todentaa, että Wi-Fi kannattaa kytkeä pois päältä silloin, kun sitä ei oikeasti tarvitse. Myös verkkoon automaattisesti yhdistäminen kannattaa kytkeä pois päältä.



Kuvio 25. Automaattinen yhdistäminen Rogue Access Pointiin

Vastaavanlaisesti kodin verkon signaalia voisi pyrkiä parantamaan sijoittamalla reititin paremmin niin, että se on mahdollisimman vähän rakenteiden takana. Signaalin voimakkuutta voisi myös parantaa erillisillä antenneilla, sekä vahvistimilla. Laitteisto ja sen ohjelmisto (firmware) kannattaa myös pitää ajan tasalla.

7 Pohdinta

Olemassa olevien tietoturvariskien vakavuudesta huolimatta, monet Wi-Fi-laitteiden käyttäjät eivät välttämättä ole tietoisia niistä tai tavoista suojautua niiltä. Työssä pyrittiin kasvattamaan Wi-Fin käyttäjien tietoisuutta ensin avaamalla syvällisemmin langattomien verkkojen teoriaa ja seuraavaksi tutkimuskysymysten avulla. Tutkimuskysymyksinä esitettiin kuinka Rogue Access Point toimii, kuinka Rogue Access Pointilta voi suojautua, sekä kuinka tukiaseman signaalin voimakkuus vaikuttaa langattoman verkon tietoturvaan? Näihin tutkimuskysymyksiin haettiin vastausta demonstroimalla Rogue Access Pointin toimintaa.

Työkaluksi Rogue Access Pointin demonstroimista varten valikoitui Raspberry Pi-pienoistietokone. Laitevalintaan vaikuttivat käytännön syyt, kuten se, että Raspberry Pi sattui olemaan helposti saatavilla ja siitä löytyvät myös tarvittavat ominaisuudet demonstraatiota varten. Tämän lisäksi, mikäli mietitään mahdollista tosielämän tilannetta, Raspberry Pi olisi periaatteessa helppo piilottaa pois näkyviltä pienen kokonsa vuoksi. Tämä tieto osaltaan kasvattaa tietoisuutta mahdollisesta uhasta.

Raspberry Pi:lle oli mahdollista asentaa Kali Linux-käyttöjärjestelmä, joka on suunnattu tietoturvan testaukseen ja siitä löytyy tarvittavia työkaluja harjoituksen toteutukseen. Tämän lisäksi käyttöjärjestelmä on ilmainen. Kali Linux myös toimii hyvin Raspberry Pi:lla, sillä sen järjestelmävaatimukset ovat melko alhaiset. Kali Linuxille asennettava Wifipumpkin3-ohjelma on niin ikään ilmainen ohjelma, joka on luotu Rogue Access Pointin testausta varten. Wifipumpkin3-ohjelmasta löytyy mm. captiveflask-liitännäinen, joka mahdollisti realistisen testiympäristön luomisen.

Varsinainen Rogue Access Point -hyökkäysdemo osoittaa, kuinka helposti varomattoman käyttäjän kirjautumistiedot ovat varastettavissa, mikäli hän käyttää niitä huomaamattaan Rogue Access Pointilla luotuun verkkoon kirjautumiseen. Mikäli käyttäjä ei tiedosta suojaamattomaan verkkoon liittymisen riskejä, hän on potentiaalisesti helppo kohde Rogue Access Point -hyökkäyksen toteuttajalle. Demon tulokset vahvistivat ajatusta siitä, että on tärkeää kasvattaa tietoisuutta langattomien verkkojen tietoturvaan liittyen.

Tietoturvan kohentamisen demolla voitiin osoittaa keinoja, kuinka suojautua Rogue Access Pointilta. Demo osoitti käytännössä, kuinka tukiaseman signaalin voimakkuus vaikuttaa asiakaslaitteen käyttämän verkon valintaan, mikäli yksi kuin useampi samanniminen verkko on saatavilla. Asiakaslaite listaa saatavilla olevat verkot niiden signaalin voimakkuuden perusteella. Tämän lisäksi voitiin osoittaa, että Wi-Fi kannattaa kytkeä pois päältä silloin, kun sitä ei tarvita. Myös automaattinen liittyminen verkkoon kannattaa kytkeä pois päältä. Tuloksina saatiin siis konkreettisia ja käyttökelpoisia keinoja oman tietoturvan kohentamista varten. Tulokset eivät kuitenkaan osoita kaikkia mahdollisia suojautumiskeinoja, eivätkä välttämättä edes niistä kaikkein parhaita mahdollisia, mutta ne antavat hyvän yleiskäsityksen.

Siinä missä tukiaseman signaalin voimakkuuden kasvattaminen vaatii potentiaalisesti rahallista panostusta, käyttäjiä voidaan opastaa olemassa olevista tietoturvariskeistä ja toimenpiteet, kuten automaattisen liittymisen ottaminen pois päältä, on suhteellisen helppoa saavuttaa.

Wireshark -ohjelmalla olisi mahdollista tarkastella tarkemmin 4-suuntaisen kättelyn vaiheita. Tätä yritettiinkin toteuttaa käytännössä, mutta ongelmaksi osoittautui sopivan verkkokortin puute. Tarkastelu vaatii Wirehark-ohjelman ”monitor-moden” käyttöä, joka puolestaan vaatisi sille sopivan, erillisen, verkkokortin.

Demonstraatiossa asioita testattiin hyvin pienessä mittakaavassa, joten on mahdollista, että suuremmassa mittakaavassa tulisi vastaan jotakin, mitä ei ole voitu pienemmässä mittakaavassa huomioida. Rogue Access Pointin käyttöönotosta todettiin, että “se on helppoa”, mutta tässä on hyvä huomioida, että käytössä oli yksi captiveflask-lisäosan valmispohjista. Siinä missä kyseinen valmispohja on neutraali, eikä välttämättä herätä huomiota, on todettava, että mikäli tositilanteessa pyrittäisiin täysin samankaltaisen kirjautumisikkunan käyttöön kuin varsinaisessa verkossa, se vaatisi jonkin verran lisätyötä ja osaamista.

Signaalin voimakkuuden vaikutuksia testattaessa voitiin todeta, että signaalin voimakkuudella on vaikutusta asiakaslaitteen valitsemaan verkkoon. Tämä demonstraatio ei kuitenkaan määritellyt tarkkoja raja-arvoja sille, kuinka suuri kynnys varsinaisen verkon ja Rogue AP:n signaalin voimakkuuksilla tulisi olla, jotta asiakaslaite liittyy Rogue Access Pointiin varsinaisen verkon sijaan. Työn loppuvaiheilla heräsi myös ajatus signaalin voimakkuuden vaikutuksen testaamisesta Windows-pohjaisella laitteella, mutta sopivan testilaitteen puutteen, sekä ajan loppumisen johdosta tämä ei ollut mahdollista.

Rogue Access Pointilla voidaan testata esimerkiksi yrityksen tietoturvaa, mutta sitä on mahdollista käyttää myös haitallisiin tarkoituksiin, kuten demosta käy ilmi. Tietojen kalastelu on sillä suhteellisen helppoa ja tarvittavat laitteet ja ohjelmistot ovat helposti saatavilla. Yritysten ja yksityisten henkilöiden kannattaa aina kiinnittää huomiota omaan tietoturvaansa. Usein tietoturvan heikoin lenkki on käyttäjä itse. Tarkkaavaisuus ja huolellisuus ovat erinomaisia suojautumiskeinoja myös Rogue Access Pointia vastaan. Käyttäjän on syytä olla varuillaan käytettäessä avointa verkkoa ja

esimerkiksi oman puhelimen Wi-Fi ominaisuus kannattaa kytkeä pois päältä silloin, kuin sitä ei tarvitse. Näin puhelin ei etsi jatkuvasti saatavilla olevaa verkkoa. Vierailtaessa verkkosivuilla kannattaa kiinnittää huomiota siihen, onko sivusto suojattu https:lla. Erityisesti yritysten tulee tehdä jatkuvaa työtä oman tietoturvansa varmistamiseen ja parantamiseen.

Rogue Access Point olisi mahdollista toteuttaa usealla eri tavalla. Myös sen toimintaa olisi mielenkiintoista testata laajemmassa mittakaavassa, esimerkiksi oppilaitoksella, mutta tästä pitäisi tietenkin sopia erikseen. Yksi vaihtoehto Rogue Access Pointin toteutukseen olisi ollut laajat ominaisuudet omaava, ”ammattikäyttöön” soveltuva, Wifi Pineapple, mutta sen käyttö ei ollut mahdollista maksullisuuden vuoksi. Näin ollen demon toteutukseen valittiin laitteiston osalta Raspberry Pi, joka palveli tässä tarkoituksessa oikein hyvin.

Yksi idea jatkokehitystä ajattelen voisi olla tarkastella signaalin voimakkuuden, sekä laitteiden sijoituksen vaikutuksia laajemmin. Signaalin voimakkuuden mahdollisia raja-arvoja voisi kokeilla määritellä tarkemmin. Myös Wiresharkin ”monitor-moden” tutkiminen siihen soveltuvilla laitteilla antaisi arvokasta lisätietoa aiheeseen liittyen.

Lähteet

4-Way Handshake. N.d. Artikkeli 4-suuntaisen kättelyn toiminnasta wifi-professionals.com -verkkosivulla. Viitattu 13.3.2022. https://www.wifi-professionals.com/2019/01/4-way-handshake

Advanced Encryption Standard (AES). 2021. Artikkeli AES-salauksen toimintaperiaatteesta GeeksforGeeksin verkkosivuilla. Viitattu 31.1.2022. https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

Aust, S., Prasad, V. & Niemegeers, I. 2012. IEEE 802.11ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi. Viitattu 28.2.2022. https://www.researchgate.net/publication/261200078_IEEE_80211ah_Advantages_in_standards_and_further_challenges_for_sub_1_GHz_Wi-Fi

Certification. 2022. Artikkeli Wi-Fi Alliancen sivuilla Wi-Fin sertifioinnista. Viitattu 16.2.2022. https://www.wi-fi.org/certification

Dionicio, R. 2018. Securing Your Network with the 4-Way Handshake. Artikkeli 4-suuntaisen kättelyn toiminnasta netbeez.net -verkkosivulla. Viitattu 13.3.2022. https://netbeez.net/blog/secure-network-4-way-handshake/

EAPoL (Extensible Authentication Protocol over LAN). N.d. Artikkeli EAPoL-protokollan toiminnasta ipcisco.com -verkkosivulla. Viitattu 13.3.2022. https://ipcisco.com/lesson/eapol-extensible-authentication-protocol-over-lan/

EAPOL. N.d. Artikkeli EAPoL-protokollan toimintaperiaatteesta etutorials.org -verkkosivulla. Viitattu 13.3.2022. http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+8.+Access+Control+IEEE+802.1X+EAP+and+RADIUS/EAPOL/

Empiirinen tutkimus. 2015. Jyväskylän avoimen yliopiston tietopankin sivusto empiirisestä tutkimuksesta. Muokattu. 23.05.2015. Viitattu 8.12.2021. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/empiirinen-tutkimus

Enabling Remote Desktop and SSH access to Kali. N.d. Artikkeli Kali Linuxin komennoista ja niiden toiminnasta Thedutchhackerin verkkosivuilla. Viitattu 8.1.2022. https://www.thedutch-hacker.com/enabling-remote-desktop-and-ssh-access-to-kali/

Fisher, T. 2021. What Is WPA3 Wi-Fi? Artikkeli WPA3-salauksesta Lifewiren -verkkosivuilla. Viitattu 31.1.2022. https://www.lifewire.com/what-is-wpa3-wi-fi-4845626

Getting started. 2020. Githubin artikkeli Wifipumpkin3:n toiminnasta. Viitattu 9.1.2022. https://wifipumpkin3.github.io/docs/getting-started

History of IEEE. 2022. Artikkeli IEEE:n alkutaipaleesta järjestön omilla verkkosivuilla. Viitattu 15.2.2022. https://www.ieee.org/about/ieee-history.html

IEEE 802.11i. N.d. 802.11i-standardin kuvaus technopedian verkkosivuilla. Viitattu 12.3.2022. https://www.techopedia.com/definition/16835/ieee-80211i

IEEE at a Glance. 2021. Artikkeli IEEE:n toiminnasta järjestön omilla verkkosivuilla. Viitattu 28.2.2022. https://www.ieee.org/about/at-a-glance.html

Information Supplement: PCI DSS Wireless Guideline. 2009. Dokumentaatio PCI SSC:n verkkosivuilla, joka on maksuliikenteen suojaukseen erikoistunut maailmanlaajuinen yritys. Viitattu 3.3.2022. https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

Kaleem, Z. 2017. How to Physically Locate a Rogue Access Point. Blogipostaus, jossa käsitellään Rogue AP:n paikantamiskeinoja. Viitattu 3.3.2022. https://www.accessagility.com/blog/locating-rogue-access-points

Mitchell, B. 2021a. 802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a. Artikkeli 802.11-stadardeista Lifewiren verkkosivuilla. Viitattu 28.2.2022. https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553#toc-80211ah

Mitchell, B. 2021b. WPA2 vs. WPA. Artikkeli WPA2 ja WPA salausten eroista Lifewiren verkkosivuilla. Viitattu 31.1.2022. https://www.lifewire.com/wpa2-vs-wpa-for-wireless-security-3971350

Nevase, V. N.d. A Practical Guide to Differentiate Unicast, Broadcast & Multicast. Blogipostaus unicastin, broadcastin ja multicasting eroista. Viitattu 12.3.2022. https://www.esds.co.in/blog/difference-between-unicast-broadcast-and-multicast/

Näin Wi-Fi 6 toimii – Kaikki mitä sinun tarvitsee tietää 802.11ax:sta. 2019. Artikkeli Wi-Fi 6:n toiminnasta io-tech.com-verkkosivuilla. Viitattu 28.2.2022. https://www.io-tech.fi/artikkelit/nain-wi-fi-6-toimii-kaikki-mita-sinun-tarvitsee-tietaa-802-11axsta/

Raspberry Pi 3 Model B. N.d. Raspberry Pi:n tekniset tiedot valmistajan sivuilla. Viitattu 29.1.2022. https://www.raspberrypi.com/products/raspberry-pi-3-model-b/

Rutledge, S. 2020. Should you hide your Wi-Fi SSID? Artikkeli verkon suojauksen keinoista Fractionalciso.com-verkkosivulla. Viitattu 3.3.2022. https://fractionalciso.com/should-you-hide-your-wi-fi-ssid/

Security. 2022. Artikkeli WPA3:n toiminnasta Wi-Fi Alliancen verkkosivuilla. Viitattu 31.1.2022. https://www.wi-fi.org/discover-wi-fi/security

Shah, A. N.d. Artikkeli Rogue Access Pointin toiminnasta khanacademyn-verkkosivuilla. Viitattu 2.3.2022. https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks

Shaw, K. 2020. 802.11x: Wi-Fi standards and speeds explained. Viitattu 28.2.2022. https://www.networkworld.com/article/3238664/80211x-wi-fi-standards-and-speeds-explained.html

Should I Use Kali Linux. 2022. Kali Linuxin ominaisuuksien läpikäynti Kalin omilla verkkosivuilla. Viitattu 2.1.2022. https://www.kali.org/docs/introduction/should-i-use-kali-linux/

The evolution of Wi-Fi standards: a look at 802.11a/b/g/n/ac/ax. N.d. Artikkeli Wi-Fi-standardien ominaisuuksista Actiontecin verkkosivuilla. Viitattu 27.2.2022. https://www.actiontec.com/wifi-help/evolution-wi-fi-standards-look-802-11abgnac/

Understanding Rogue Access Points. 2018. Artikkeli Rogue Access pointin toimintaperiaatteesta juniper.net-verkkosivustolla. Viitattu 1.2.2022. https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/topics/concept/wireless-rogue-ap.html

Understanding the Network Terms SSID, BSSID, and ESSID. 2018. Artikkeli tietoverkkojen termeistä Juniperin verkkosivuilla. Viitattu 3.3.2022. https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.7/topics/concept/wireless-ssid-bssid-essid.html

Uy, M. 2021. Lifewiren artikkeli Wi-Fin toiminnasta. Viitattu 5.12.2021. https://www.lifewire.com/what-is-wi-fi-2377430

WEP, WPA, WPA2 and WPA3: Differences and explanation. 2022. Artikkeli eri suojausmenetelmien eroista Kasperskyn verkkosivuilla. Viitattu 30.1.2022. https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa

What Is 802.11ac? N.d. Artikkeli Wi-Fi-standardin toiminnasta Cisco.comin-verkkosivuilla. Viitattu 27.2.2022. https://www.cisco.com/c/en/us/products/wireless/what-is-802-11ac.html

What Is a VPN? - Virtual Private Network. 2022. Artikkeli VPN:n toiminnasta Cisco.comin verkkosivuilla. Viitattu 1.2.2022. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

What is Kali Linux. 2022. Kuvaus Kali Linuxista Kalin omilla verkkosivuilla. Viitattu 1.2.2022. https://www.kali.org/docs/introduction/what-is-kali-linux/

Who We Are. 2022. Artikkeli Wi-Fi Alliancen sivuilla, joka kertoo heidän toiminnastaan. Viitattu 16.2.2022. https://www.wi-fi.org/who-we-are

WiFi Networking: Radio Wave Basics. 2017. Artikkeli radioaaltojen perusteista networkcomputing.com -verkkosivulla. Viitattu 17.3.2022. https://www.networkcomputing.com/wireless-infrastructure/wifi-networking-radio-wave-basics

Wifi Pineapple. N.d. Tuotteen kuvaus valmistajan sivuilla. Viitattu 30.1.2022. https://shop.hak5.org/products/wifi-pineapple

Wifipumpkin3. 2022. Wifipumpkin3:n ominaisuuksien läpikäynti github.com -verkkosivulla. Viitattu 30.1.2022. https://github.com/P0cL4bs/wifipumpkin3

WiGig: IEEE 802.11ad 60GHz Microwave Wi-Fi. N.d. Artikkeli 802.11ad-standardista Electronicsnotes.comin verkkosivuilla. Viitattu 27.2.2022. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ad-wigig-gigabit-microwave.php