jamk

Rogue Access Point -hyökkäysdemo

Topi Mällönen

Opinnäytetyö,
Syyskuu 2021
Tietojenkäsittely ja tietoliikenne, Insinööri (AMK)
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Mällönen Topi

Rogue Access Point -hyökkäysdemo

Jyväskylä: Jyväskylän ammattikorkeakoulu. **Syyskuu 2021**, 44 sivua.

Tietojenkäsittely ja tietoliikenne. Insinööri (AMK), tieto- ja viestintätekniikka. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Nykypäivänä n. 60 % maailman ihmisistä käyttää aktiivisesti internettiä ja kasvuvauhti on huima, 7 kertainen verrattuna maapallon väestönkasvuun. Internetin kehitys on tuonut myös mukanaan erilaisia tietoturvahyökkäyksiä ja uhkia. Tietoturvahyökkäyksien tekijöiden intressit voivat vaihdella yrityksen lamauttamisesta palvelunestohyökkäyksellä, arkaluontoisien tietojen kalasteluun.

CYBERDI-projektin toimeksiantona oli toteuttaa Rogue Access Point hyökkäys opetustarkoitukseen. Työn tavoitteina oli tutkia minkälaisella laitteistolla Rogue Access Point voidaan toteuttaa, vaatimuksina oli helppo liikuteltavuus ja tarvittavien tietojen kalastelu hyökkäyksellä.

Tutkimusmuotona oli empiirinen tutkimus. Empiirinen tutkimus perustuu mittaamiseen, konkreettisiin havaintoihin ja analysointiin.

Demonstraatio tehtiin kotiolosuhteissa Raspberry Pi pienois- tietokoneella, käyttöjärjestelmäksi valikoitui Kali Linux ja ohjelmistona käytettiin Wifipumpkin3. Demonstraatiossa käytiin läpi askel askeleelta käyttöjärjestelmän asennus, ohjelmiston asennus ja käyttö. Demonstraatio oli onnistunut, Rogue Access Point saatiin asennettua ja konfiguroitua käyttöä varten. Valetukiasemalla saatiin kerättyä langattomaan verkkoon liittyvältä MAC-osoite ja kirjautumisikkunan tiedot.

Toimeksiantajalle saatiin tutkimuksesta asennus- ja käyttöönotto-ohjeet, mitä vaaditaan toimivan Rogue Access Point hyökkäyksen toteutukseen laitteiston, käyttöjärjestelmän ja ohjelmiston osalta. Hyökkäys on mahdollista toteuttaa ohjeen pohjalta konkreettisesti pienillä muutoksilla.

Avainsanat (asiasanat)

Tietoverkko, Tietoturva, Kyberturvallisuus, Tieto- ja Viestintätekniikka, Demo, Demonstraatio

Muut tiedot (salassa pidettävät liitteet)

Liitteenä asennus- ja käyttöönotto-ohje, 12 sivua.

jamk

Description

Mällönen Topi

Rogue Access Point attack demo

Jyväskylä: JAMK University of Applied Sciences, September 2021, 44 pages.

Bachelor of Engineering, Information and Communication Technology, Bachelor's thesis.

Permission for web publication: yes

Language of publication: Finnish

Abstract

Nowadays approximately 60 percent world population uses actively internet and growth rate is wild, 7 times bigger than world population growth. Internet growth has brought us various Information security attacks and threats. Intruder's interest can be paralyzing company with DDOS attack to fishing delicate information.

CYBERDI-project assignment was execute Rogue Access Point attack for teaching purposes. Work goals was research which kind of hardware a Rogue Access Point can be implemented with. Requirements was easily movable hardware and gathering necessary information from attack.

Empirical study was research format, empirical study is based on measuring, concrete observation and analyzing.

Demonstration was made in home conditions with Raspberry Pi miniature computer, Kali Linux was selected operating system and used program was WifiPumpkin3. Installing operating system, program and usage was made step by step in demonstration. Demonstration was successful, Rogue Access Point was installed and configured correctly. MAC-address and signing box information was gathered from Rogue access point correctly.

Mandator got instruction and deployment guidelines from research, information about what it will need for setup Rogue Access point and how to implement Rogue Access Point Attack concrete with little chances.

Keywords/tags (subjects)

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

Miscellaneous (Confidential information)

Installation- and deployment instructions as attachment, 12 pages.

Sisältö

Lyhenteet ja käsitteet

BSSID= Langattoman tukiaseman MAC-osoite

COVID-19= Virus, joka alkoi leviämään 2019 vuoden loppupuolella, aiheuttaen pandemian

CSS= Tyylisivu, joka on kehitetty erityisesti verkkosivujen luontiin

Demo tai demoaminen= Demonstraatio

DNS= Nimipalvelujärjestelmä

HTML= Merkintäkieli, jota käytetään internet sivujen kirjoitukseen

HTTPS= Suojattu yhteys verkkosivulle, HTTP ja TLS/SSL protokollien yhdistelmä

Image tietotekniikassa= Valmis käyttöjärjestelmän kopio

ISP= Internet-palveluntarjoaja

MAC-osoite= Tietoteknisen laitteen verkkosovittimen yksilöivä osoite

Raspberry PI= Yhden piirilevyn tietokone

Rogue Access Point/ Rogue AP= Tukiasema, joka ei ole lähiverkon ylläpitäjien hallinnassa

SSID= langattoman lähiverkon verkkotunnus

VPN= virtuaalinen yksityinen verkko, suojattu yhteys

RSSI= Vastaanotetun signaalin vahvuus

1 Johdanto

Internetistä on kehittynyt maailmanlaajuinen tietoverkkojärjestelmä, mitä hyödyntää suurin osa maapallosta. Internetin kehitys on myös herättänyt rikollisten kiinnostuksen, miten sitä voisi hyödyntää rikolliseen toimintaan. Tämän johdosta tietoturvahyökkäykset ja uhat ovat kasvaneet.

Opinnäytetyössä käydään läpi tietoturvahyökkäyksen Rogue Access Point toiminnan, minkälaisella laitteella sen voi toteuttaa, käyttöjärjestelmän ja ohjelmiston vaatimukset. Rogue Access Pointtien tunnistaminen on haasteellista ja vaatii osaamista. Opinnäytetyössä käydään myös läpi tunnistamiseen liittyvät seikat.

Demossa käydään läpi käyttöjärjestelmän, ohjelmiston asennuksen ja miten ohjelmistoa käytetään. Kirjautumisikkuna luodaan ohjelmistoon kuuluvalla liitännäisellä, jossa on valmiita sapluunoita, joista käytämme facebook sapluunaa demonstrointi tarkoituksessa. Liitännäinen on täysin muokattavissa käyttötarpeen mukaan, kansiorakenne on kuvattuna demossa ja se on muokattavissa html/css kielillä.

2 Opinnäytetyön lähtökohdat

2.1 Toimeksiantaja

Opinnäytetyön toimeksiantaja on CYBERDI-projekti, jonka tarkoituksena on Kyberrikollisuuden torjuminen, tietoisuuden kasvattaminen ja yhteistyön vahvistaminen. CYBERDI-projekti on Jyväskylän ammattikorkeakoulun ja Poliisiammattikorkeakoulun yhteisprojekti, jonka rahoittaja on opetus- ja kulttuuriministeriö. Projektin toteutusaika on 10/2018 - 12/2021 ja projektipäällikkönä toimii Kirsi Heiskanen. (CYBERDI projektiesittely 2018.)

2.2 Toimeksianto ja tavoitteet

Toimeksianto kohdistui CYBERDI-projektin työpakettiin ”tietoisuuden kasvattaminen”. Opinnäytetyön toimeksiantona oli suunnitella Rogue Access Point, jolla lähdetään tutkimaan Jyväskylän ammattikorkeakoulun dynamon kampuksen vierailijoiden lähiverkkokäyttäytymistä. Rogue AP:n tulisi näyttää kampuksella aivan normaalilta vierailijaverkolta, jolloin saataisiin otantaa, kuinka moni ihminen liittyi kyseisen valetukiaseman kautta verkkoon. Vallitsevan tilanteen johdosta (COVID-19)

tutkimuksen toteutus kampuksella muodostui haasteelliseksi, koska otanta jäisi kapeaksi ja konkreettinen toteutus ei olisi eettistä tehdä paikan päällä, joten toteutus tapahtuu demon välityksellä, jolla demotaan kyseistä tapahtumaa.

Opinnäytetyöstä tehtiin asennus- ja käyttöönotto-ohjeet toimeksiantajalle, jota toimeksiantaja voi hyödyntää tulevaisuudessa opetuskäyttöön ja mahdollisesti toteuttaa konkreettinen tutkimus ohjeiden pohjalta.

2.3 Tutkimusmenetelmät

Tutkimusmenetelmänä on opinnäytetyössä empiirinen tutkimus. Empiirinen tutkimus perustuu kolmeen vaiheeseen: mittaaminen, konkreettiset havainnot ja analysointi. Pääaineisto saadaan tutkimalla aihetta konkreettisesti ja demoamalla tapahtumaa. (Empiirinen tutkimus 2015.)

Tutkimusta lähdettiin rajaamaan muutamalla tutkimuskysymyksellä. Kysymykset antavat hyvän kokonaiskuvan vierailijoiden lähiverkkokäyttäytymisestä ja valetukiaseman toimivuudesta.

Tutkimuskysymykset:

1. Miten Rogue Access Point toimii, käyttöönoton vaiheet, kuinka havaita ja välttää kyseinen hyökkäys.
2. Minkälaisilla laitteilla, käyttöjärjestelmällä ja ohjelmistolla Rogue Access Point voidaan toteuttaa.

2.4 Eettiset lähtökohdat

Rogue AP:n toteutus konkreettisesti kampuksella muodostui haasteelliseksi myös eettisyyden johdosta. Tulimme toimeksiantajan kanssa siihen tulokseen, että ei ole eettistä toteuttaa tutkimusta konkreettisesti kampuksella vallitsevan tilanteen johdosta.

Tutkimuksessa eettisyys on tärkeä osa tutkimusta, kun Rogue AP:lla hankitaan verkkoon liittyvältä tietoja. MAC-osoitteella voidaan yksilöidä verkkoon liittyvä, tällä vältytään, että sama ihminen liittyisi monta kertaa verkkoon ja luultaisiin, että verkkoon olisi liittynyt Rogue AP:n kautta eri henki-

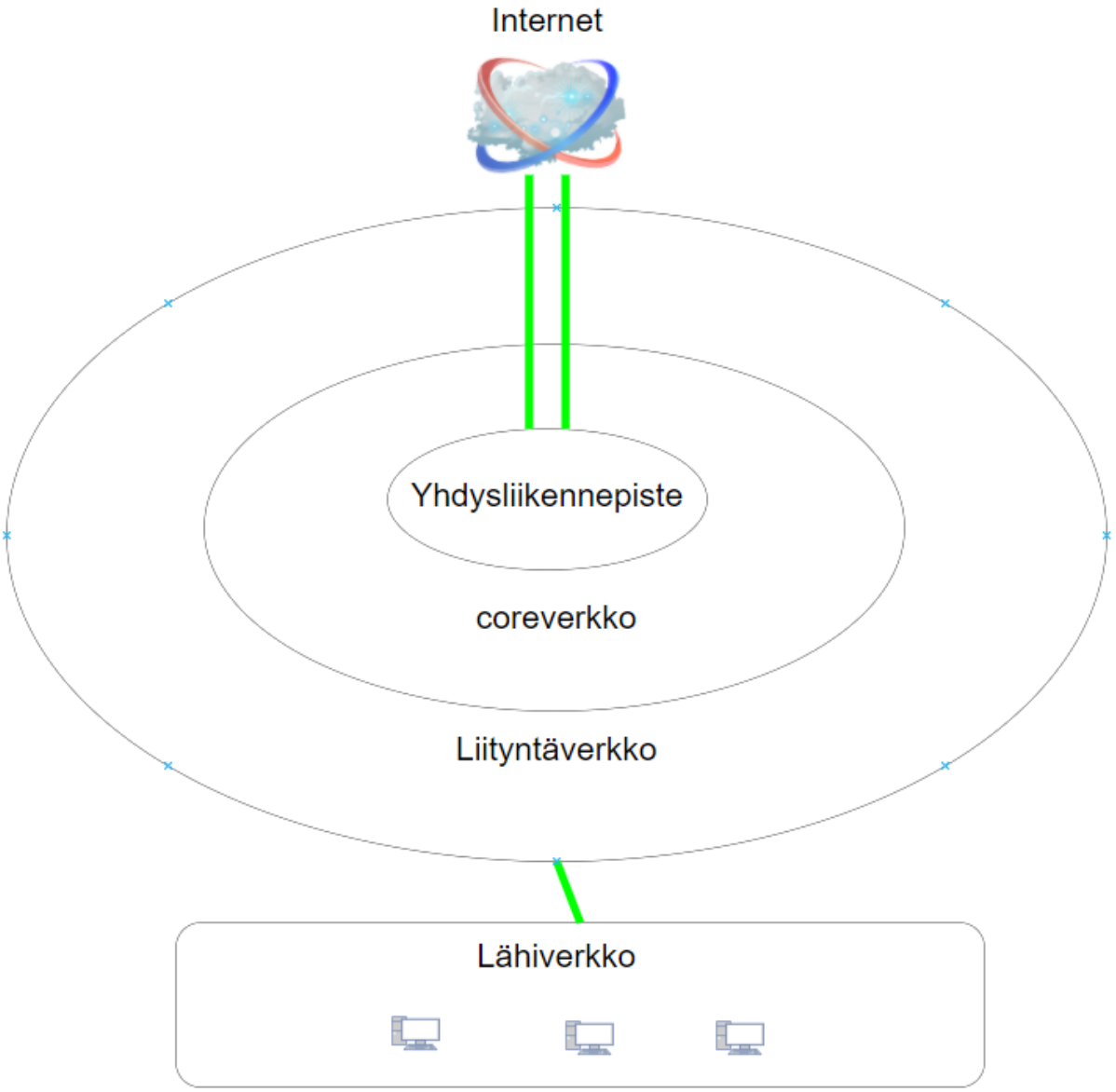
löitä. Opiskeluala kerätään tutkimuksessa, koska tällöin voidaan jakaa tutkittavat tutkinto-ohjelmittain ja vertailla mahdollisesti vaikuttaako tutkinto-ohjelma valetukiasemaan liittyviin ihmisiin. Demossa demonstroidaan Facebook kirjautumisikkunalla tätä tapahtumaa. Tutkimukselle muita relevantteja tietoja ei ole, joten näitä ei tulla keräämän eettisyyden takia. Lähiverkkoon liittyvän dataa ei lueta eikä tallenneta.

3 Tietoperusta

3.1 Internet

Maailmanlaajuisen internetin synty tapahtui vuonna 1989 englantilaisen tiedemiehen Tim Berners-Lee:n toimesta. Tämä historiallinen kohta muutti maailman, internet alkoi kasvamaan. Vuonna 2017 maailmassa oli 3.42 miljardia internetin käyttäjää. Nykypäivänä n. 60 % maailman ihmisistä käyttää aktiivisesti internettiä ja kasvuvauhti on huima, 7 kertainen verrattuna maapallon väestönkasvuun. (Roser, Ritchie & Ortiz-Ospina n.d.)

Internetin perusrakenne koostuu lähiverkoista, jotka yhdistyvät internettiin liityntäverkon kautta, liityntäverkosta liikenne kulkee coreverkkoon, josta liikenne menee yhdysliikennepisteen kautta Suomen ulkopuolelle. Yleisesti Liityntäverkon reitittimen linkit coreverkkoon ovat kahdennettuja, tämä takaa redundanttisen yhteyden internettiin. (Ks. kuvio 1)



Kuvio 1. Internetin perusrakenne.

Internetin kehitys on tuonut mukanaan myös haittapuolia, arkaluonteisia tietoja koitetaan hankkia erilaisilla tietoturvahyökkäyksillä ja internetistä riippuvaisia yrityksiä koitetaan häiritä. Tietoturvahyökkäyksillä voi olla moniakin erilaisia intressejä mm. rahallinen hyöty, politiikka tai sabotointi. (Threats to Information Security 2021.)

3.2 Rogue Access Point

3.2.1 Yleistä

Rogue Access Point on lähiverkkoon kuulumaton tukiasema, joka ei ole lähiverkon ylläpitäjien hallinnassa. Rogue AP on siis valetukiasema, jonka tarkoituksena on matkia lähiverkon langatonta verkkoa. (Wireless Rogue ap 2016.)

Rogue AP:n haltija voi olla yrityksen työntekijä, jonka tavoitteena on mahdollistaa rajoittamattoman ja valvomattoman internet-yhteyden. Haltija voi myös olla ulkopuolinen hyökkääjä, jonka tavoitteet ovat erilaiset. Ulkopuolisen hyökkääjän tavoitteina voi olla esimerkiksi palvelunestohyökkäys, tietojen kalastelu ja tietojen manipulointi. (Wireless Rogue ap 2016; Shah N.d.)

Rogue AP:t voi karkeasti jakaa 2 eri kategoriaan, passiiviseen ja aktiiviseen.

Passiivinen:

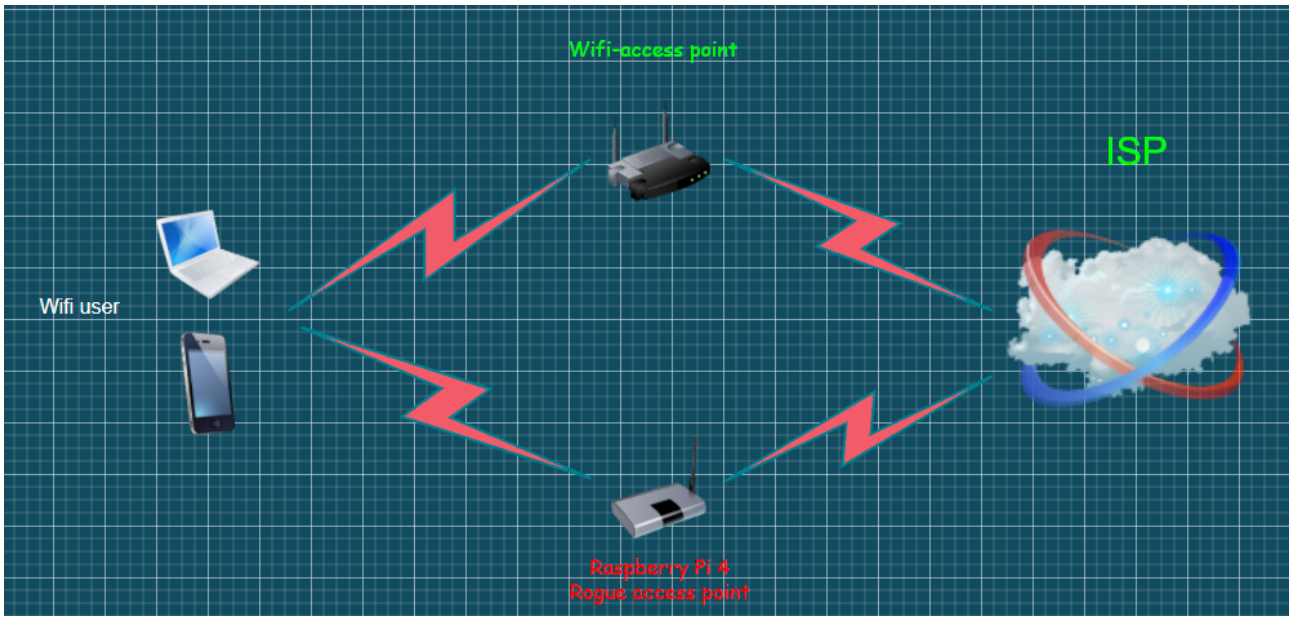
- Tallentaa kirjautumistiedot esimerkiksi http sivuille kirjautuessa tai jos käyttää kirjautumisikkunaa, kun henkilö liittyy tukiasemaan.
- MAC-osoitteen ja IP-osoitteen saaminen, kun henkilö liittyy tukiasemaan.
- Pystytään tarkkailemaan DNS pyyntöjä ja verkkosivuja millä henkilö vierailee.
- Ei pysty hallitsemaan dataa.

Aktiivinen:

Pystytään tekemään samat asiat kuin passiivisessa, lisäksi voidaan tarkastella dataa ja manipuloida sitä. Manipuloinnin jälkeen hyökkääjä voi uudelleen lähettää datan alkuperäiseen kohteeseen. (Shah N.d.)

Esimerkiksi Rogue AP:seen liittyvä aikoo tilata jotain verkkokaupasta, hyökkääjä tarkastelee dataa ja muuttaa osoitetiedot, näin ollen hyökkääjä saa paketin tulemaan haluamaan osoitteeseen.

Rogue AP:n ideana on matkia yrityksen tai julkisen rakennuksen langatonta verkkoa. Valetukiasemalle määritetään yleisesti sama SSID, muutamia poikkeuksia on, esimerkiksi jos matkittavan langattoman verkon käyttö on maksullista tai suojattu, voidaan luoda ”ilmainen” langaton verkko, joka houkuttelee käyttäjiä. (Ks. kuvio 2)



Kuvio 2. Rogue AP:n toimintamalli.

3.2.2 Rogue AP:n tunnistaminen ja välttäminen

Rogue AP:n tunnistamiseen tarvitaan Wifi-skanneri, jolla voidaan skannata tukiasemien yksilöllinen BSSID-tunnus. Tukiasemat jakavat samaa SSID-tunnusta, BSSID-tunnuksella nämä voidaan erottaa toisistaan. Skannauksen jälkeen pystymme etsimään Rogue AP:n fyysisesti seuraamalla vastaanotettua signaalin vahvuutta (RSSI) vaimennuksessa. (Kaleem 2017.)

Rogue AP:n tietojen kalastelulta voidaan välttyä suurimmaksi osaksi, käyttämällä VPN:ää ja vierailemalla ainoastaan HTTPS verkkosivuilla, koska VPN ja HTTPS verkkosivut käyttävät salausta (Shah n.d.).

3.3 Kali Linux

Kali Linux on ilmainen Debian pohjainen avoimen lähdekoodin käyttöjärjestelmä. Kali Linux kehitettiin 2013 BackTrack Linuxin korvaajaksi, joka vastaa täysin Debianin kehitysstandardeja. Kali:ssa on valmiina otettu pois käytöstä verkkopalvelut ja minimoitu kansiorakenteet, jotta tietoturva olisi parhaimmalla tasolla. Langattomien verkkojen tuki on myös todella laaja, joten Rogue AP:n toteutus on vaivatonta. (What is Kali Linux 2021.)

Kali Linuxin erot Ubuntuun verrattuna:

- Kali Linux on kehitetty tiettyä kohderyhmää ajatellen, tämän johdosta Kalin sovellukset ovat suurimmaksi osaksi penetraatiotestaukseen ja takaisinmallinnukseen tarkoitettuja. Ubuntu on suunniteltu enemmän niin sanotuille ”normaali” käyttäjille, sisältäen sähköpostisovelluksen, pelejä ja Word tekstinkäsittelyohjelman jne.
- Molemmat perustuvat avoimen lähdekoodin Debianiin.
- Käyttöliittymät eroavat jonkin verran toisistaan, Ubuntu on käyttäjäystävällinen, graafinen käyttöliittymä on valittavissa KDE ja GNOME:n välillä. Kali Linuxissa on ikkunanhallintaohjelma, joka tarjoaa komentoriviä käyttävälle loistavat puitteet. Kali Linuxin graafinen käyttöliittymä on aika rajoitettu käyttötarkoituksen takia.
- Kali Linux on kevyempi käyttöjärjestelmä, joten se toimii tietyissä sovelluksissa ja alustoilla nopeammin. (Kali Linux vs Ubuntu 2020.)

4 Toteutus

Rogue AP:n voi toteuttaa lukemattomilla eri tavoilla, tässä tutkimuksessa vaihtoehdoiksi muodostui tukiasema + tietokone ja Raspberry Pi. Toimeksiantajalta ei ollut mahdollista saada sopivaa tukiasemaa, joten käytännössä ainoaksi vaihtoehdoksi jää Raspberry PI. Raspberry PI:n päällä voidaan ajaa montaakin erilaista konfiguraatiota, jolla Rogue AP voidaan toteuttaa, myös Raspberry PI on helposti liikuteltavissa, joten se soveltuu Rogue AP:n toimintaan.

4.1 Laitteisto

Raspberry PI 4 Model B (2020)

Raspberry Pi:n 2020 vuoden malli (ks. kuvio 3), tästä mallista löytyy tarvittavat spesifikaatiot pyörittämään Rogue AP:ta. Sisäinen Wifi, riittävän tehokas prosessori, USB 3.0 ja Gigabit ethernet portti. (Raspberry Pi 4 N.d)

Mahdollinen liikuteltava 4G modeemi, LAN-yhteys tai toinen Wifi-adapteria, jolta saadaan verkkoyhteys laitteeseen, näin on mahdollista asentaa RPi käytännössä, minne vain. Tässä demossa käytämme LAN-yhteyttä havainnollistamaan tapahtumaa.

Kuvio 3. Raspberry PI 4 model B.

4.2 Käyttöjärjestelmä

Linux-pohjaisia käyttöjärjestelmiä vertaillessa, yksi käyttöjärjestelmä nousi muiden yläpuolelle. Kali Linux on juuri suunniteltu penetraatiotestaukseen, takaisinmallinnukseen, turvauhkien kartoitukseen ja esimerkiksi kyberhyökkäyksiin. Rogue AP:n voisi myös toteuttaa jollakin muulla Linux-pohjaisella käyttöjärjestelmällä mutta vaatisi jonkin verran konfigurointia turvallisuuden kannalta (verkkopalvelut ja kansiorakenteet).

4.3 Ohjelmistojen vertailu

4.3.1 Soveltuvat ohjelmistot

Vertaillessa erilaisia ohjelmistoja, jolla Rogue AP:n voisi toteuttaa, nousi muutama tutkimukselle soveltuva ohjelmisto:

-WifiPumpkin3

- Ilmainen
- Helppokäyttöinen käyttöliittymä
- Paljon erilaisia liitännäisiä, jota voi hyödyntää Rogue AP:n toiminnassa
- Captiveflask liitännäinen, kirjautumisikkunan luontiin.

-RogueOne

- Ilmainen
- Yksinkertainen Rogue AP:n toteutus
- Ei graafista käyttöliittymää

-Wifi-Pineapple

- Maksullinen (99$)
- Avaimet käteen paketti (sisältää reitittimen, ohjelmiston)
- Monipuoliset ominaisuudet
- Saatavuus

Ohjelmistoja vertaillessa, tuli nopeasti ilmi, että RogueOne ei sovellu minun tutkimukseeni, koska ohjelmistosta puuttuu monta ominaisuutta, mitä arvostan tässä tutkimustyössä. Wifi-Pineapple taas olisi soveltuva tutkimukseen, mutta maksullisuus ja saatavuus poistavat Wifi-Pineapplen valinnan. WifiPumpkin3 vaikuttaa kaikista pätevimmältä tähän tutkimustyöhön, ohjelmistosta löytyy tarvittavat ominaisuudet tutkimuksen suorittamiseen, graafinen käyttöliittymä on helppokäyttöinen ja ohjelmisto on ilmainen.

4.3.2 WifiPumpkin3

WifiPumpkin3 on niin sanottu ”end to end” ohjelmisto Rogue AP:n toteutukseen. WifiPumpkin3:n mukana tulee todella monta erilaista ominaisuutta mitä voidaan hyödyntää hyökkäyksessä.

muutamia ominaisuuksia:

- Langattoman verkon luonti
- Tietojen kalastelu clientin ja verkon väliltä
- Probe pyynnöt
- Kuvien tallennus lennosta
- DNS muunnokset
- Kirjautumistunnuksien monitorointi Asennettavissa Rasberry Pi:lle
- Helppo käyttöinen käyttöliittymä
- Monipuoliset liitännäiset
- Ilmainen
  (Githubin Wifi-Pumpkin tietosäilö 2020.)

4.4 Kirjautumisikkuna

Kirjautumisikkuna olisi tämän opinnäytetyön tärkein elementti, jos tämä opinnäytetyö toteutettaisiin konkreettisesti. Kirjautumisikkunan kuuluisi näyttää ”viralliselta”, koska valetukiasemaan liittyvä ei saa huomata mitään poikkeavaa normaaliin langattomaan yhteyteen verrattuna.

Wifipumpkin3 sisältää tähän tarkoitukseen täydellisen liitännäisen, nimeltään extra-captiveflask. Captiveflaskin idea on, kun valetukiasemaan liittyy henkilö, hänen tulee kirjautua ennen kuin voi

alkaa käyttämään internettiä, tietenkin näistä kirjautumistiedoista jää jäljet Raspberry PI:n käyttöliittymään. Captiveflaskissä on valmiita sapluunoita, joista käytän facebook sapluunaa demoamisen tarkoitukseen.

Captiveflaskiä voidaan muokata täydellisesti käyttäjän vaatimusten mukaan, Captiveflask on käytännössä vain kansiorakenne, jossa on html/css-tiedostoja (ks. kuvio 4).

```
exampleplugin/
├── preview.png
├── static
│   ├── css
│   │   ├── bootstrap.min.css
│   │   ├── main.css
│   │   ├── styles.css
│   │   └── util.css
│   └── js
│       ├── bootstrap.min.js
│       ├── jquery-1.11.1.min.js
│       └── main.js
└── templates
    ├── login.html
    └── login_successful.html

4 directories, 9 files
```

Kuvio 4. Captiveflask kansiorakenne (Extra-captiveflask 2020)

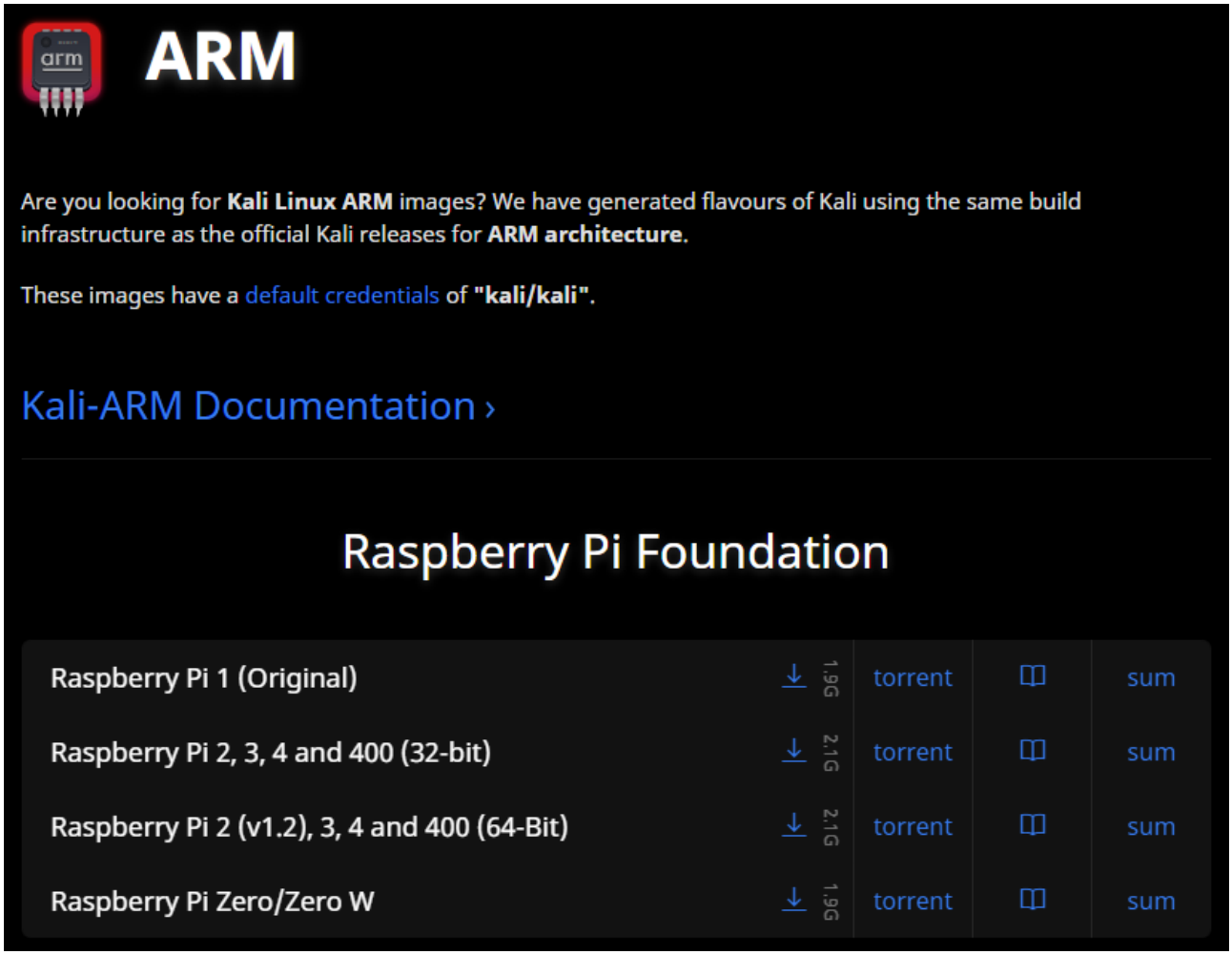
4.5 Käyttöjärjestelmän ja ohjelmiston asennus

Tässä luvussa käydään läpi asennusvaiheet käyttöjärjestelmän ja ohjelmiston osalta.

4.5.1 Käyttöjärjestelmä

Aloitetaan asentamalla Rasberry PI:lle Kali Linux käyttöjärjestelmän, Kalista löytyy ARM image, joka on tarkoitettu ajettavaksi microprosessoreille.

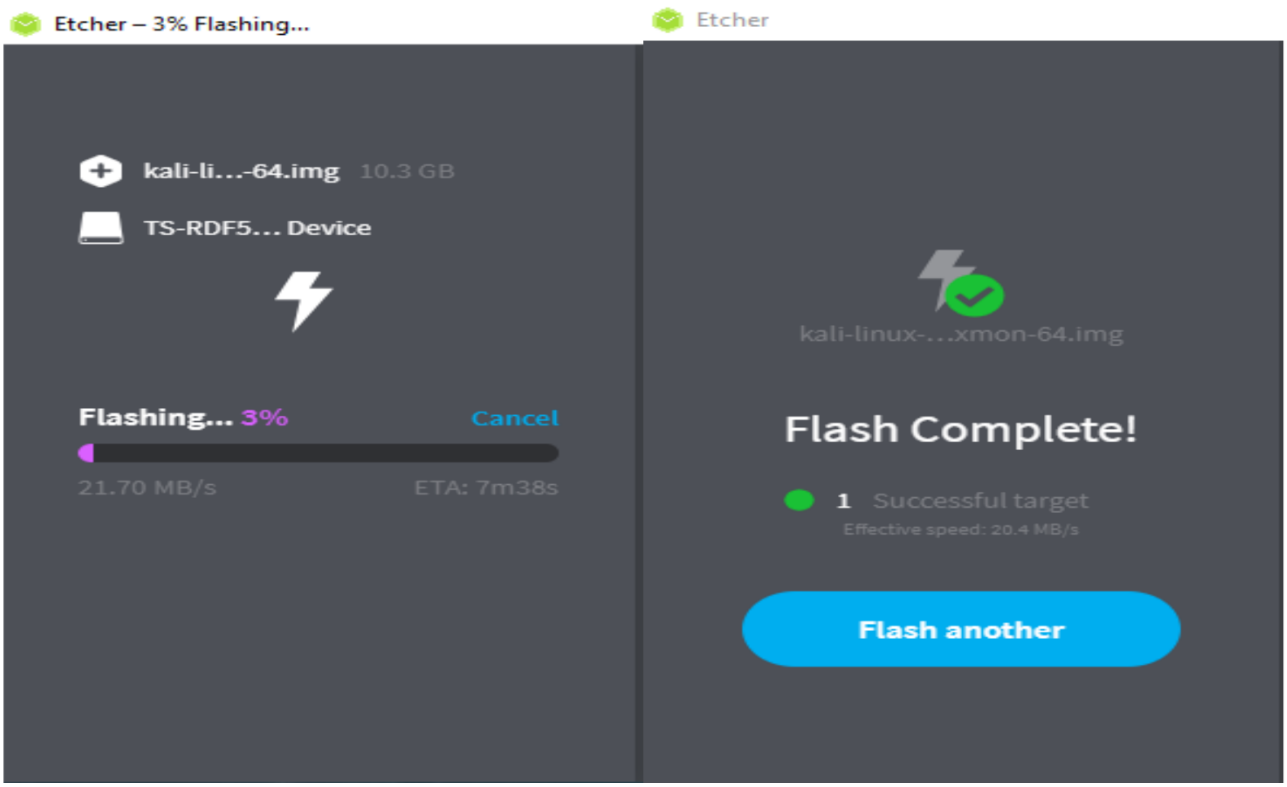
ARM image ladataan Kalin virallisilta sivuilta (ks. kuvio 5).



Kuvio 5. Kalin lataus viralliselta sivulta.

Latauksen jälkeen käyttöjärjestelmä pitäisi saada Raspberry PI:n muistikortille, tässä on muutama vaihtoehto, miten sen voi toteuttaa. Päätin käyttää ulkoista SD-kortin lukijaa ja BalenaEtcheriä, joka on tarkoitettu imagejen käyttöönottoon SD-korteille. Ohjelmiston voi ladata heidän viralliselta sivultaan.

Imagen käyttöönotto SD-kortille (ks. kuvio 6).



Kuvio 6. BalenaEtcher.

Tämän jälkeen käyttöjärjestelmä on valmis käytettäväksi, seuraavaksi laitamme asetukset kuntoon, jotta Raspberry PI:hin voidaan ottaa SSH-yhteys.

Lisätään käyttäjä nimeltä ”topi” ja muokataan käyttäjän ryhmää komennoilla:

sudo adduser topi
sudo usermod -aG sudo topi

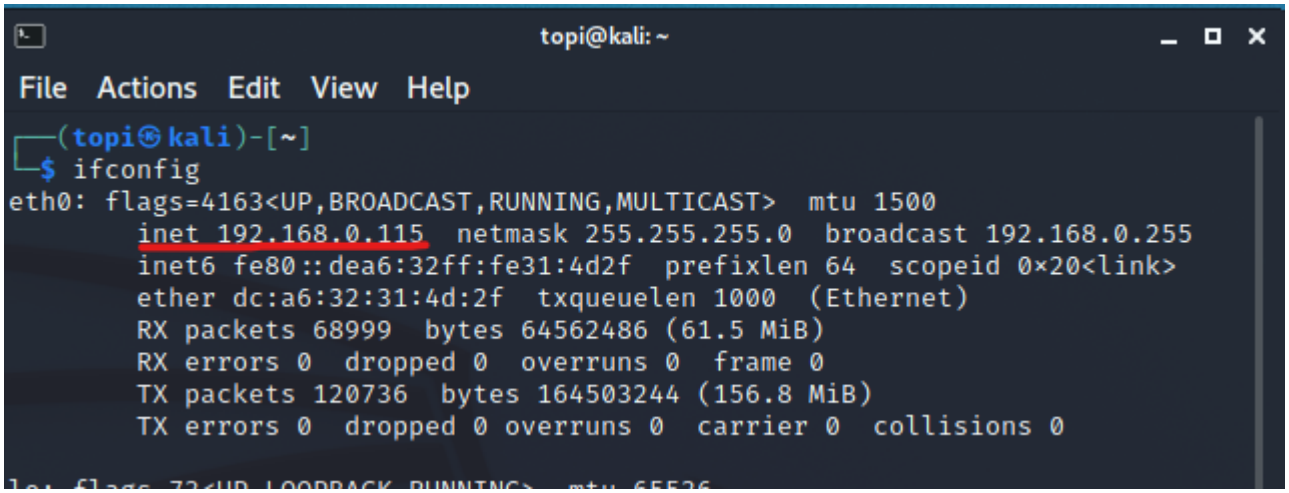
Remote desktopin käyttöön pitää ottaa käyttöön xrdp serveri komennoilla:

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

Komentojen jälkeen SSH-yhteys on mahdollistettu Rasberry PI:lle, jos kaikki toimii niin kuin pitää, voidaan asettaa xrdp serveri käynnistymään, kun Raspberry PI käynnistetään komennoilla:

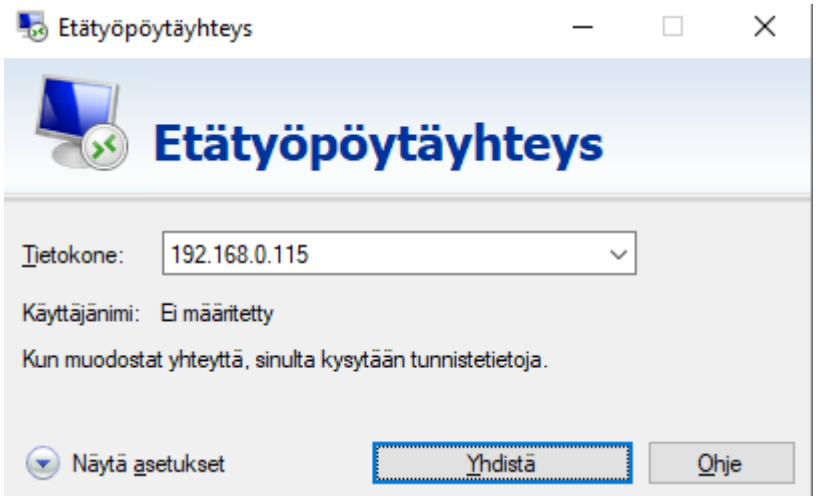
Sudo systemctl enable xrdp
Sudo systemctl enable xrdp-sesman

Seuraavaksi selvitetään Raspberry PI:n IP-osoite, jolla otetaan yhteys laitteeseen, komennolla ”ifconfig” saadaan verkkoadaptereiden osoitteet (ks. kuvio 7).



Kuvio 7. IP-osoitteen selvitys SSH-yhteyden muodostamiseen.

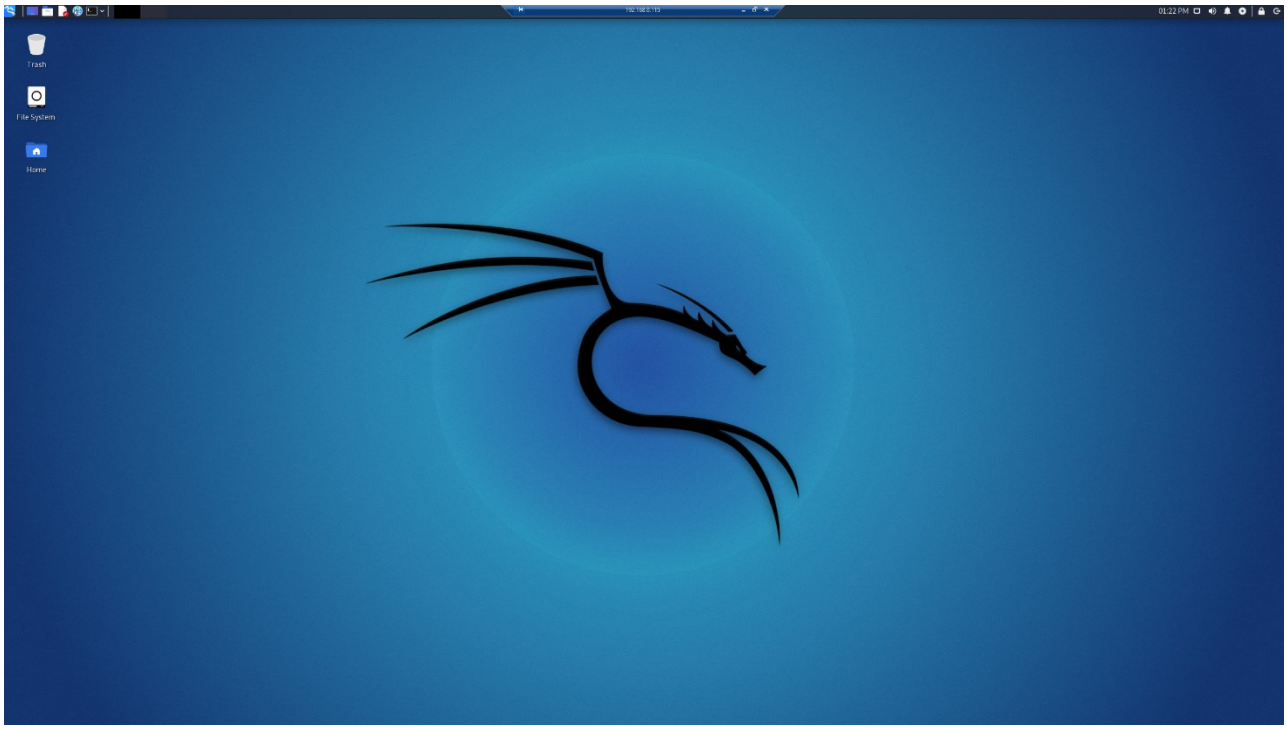
Seuraavaksi otamme yhteyden Windowsin omalla Remote desktop sovelluksella (ks. kuvio 8).



Kuvio 8. Remote desktop.

Kirjautumiseen käytetään aikaisemmin luomaamme käyttäjää.

Kun SSH-yhteys on muodostettu, pääsemme Raspberry PI:lle (ks. kuvio 9).



Kuvio 9. SSH-yhteys muodostettu.

4.5.2 Ohjelmisto

Aloitetaan Wifipumpkin3:sen asennuksen valmistelu.

Ensimmäiseksi asennamme muutaman tarvittavan paketin komennoilla:

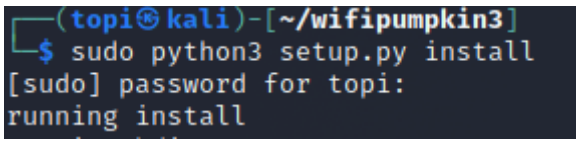
sudo apt install python3-pyqt5 hostapd
sudo apt install libssl-dev libffi-dev build-essential

Sitten voimme aloittaa itse Wifipumpkinin3 asennuksen, asennukselle löytyy suora Git-repositorio, jonka voimme ladata komennolla:

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

Repositorion latauksen jälkeen, menemme Wifipumpkin3:sen kansioon ja ajamme asennustiedoston (ks. kuvio 10) komennoilla:

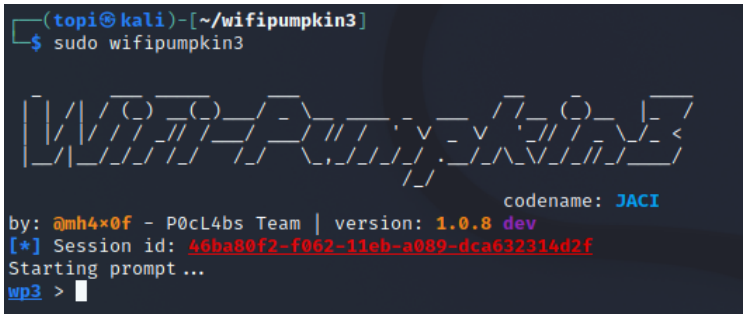
cd wifipumpkin3
Sudo python3 setup.py install



Kuvio 10. Asennuksen käynnistys.

Asennuksen jälkeen käynnistetään Wifipumpkin3 (ks. kuvio 11) komennolla:

Sudo wifipumpkin3



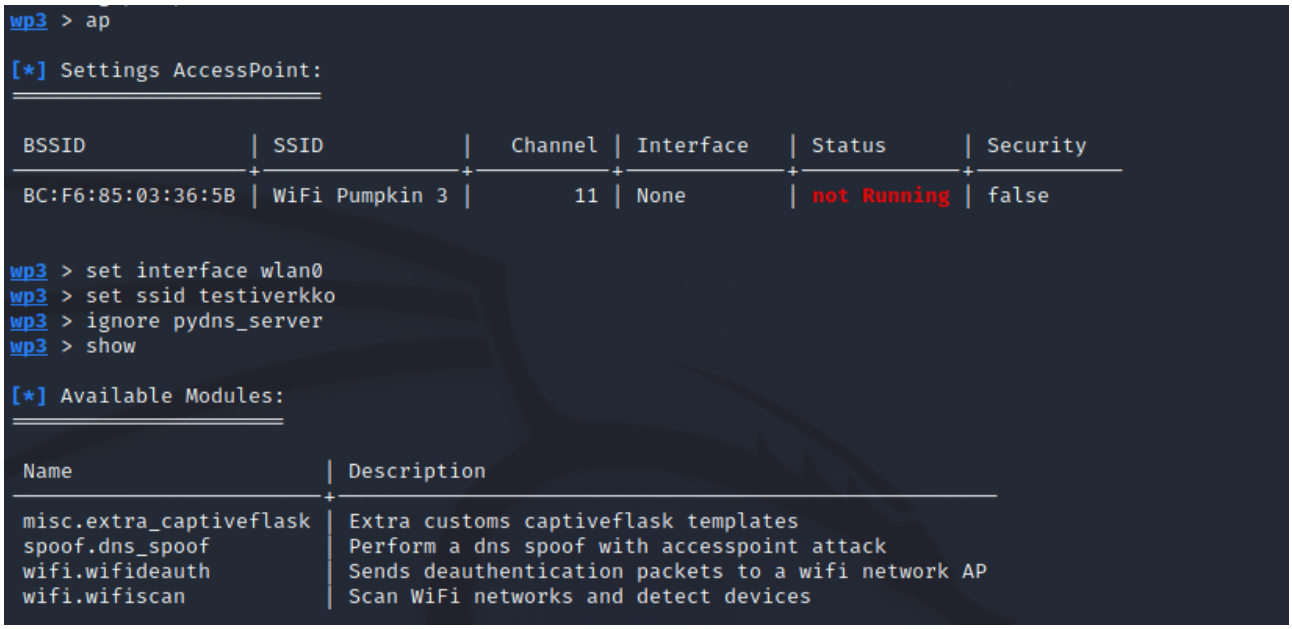
Kuvio 11. Käynnistetty ohjelma.

5 Demo

Aloitamme demoamisen, asetamme interface wlan0 käyttämään SSID ”testiverkko” ja otamme käytöstä pois DNS login komennoilla:

set interface wlan0
set ssid testiverkko
ignore pydns_server

Katsotaan ”show” komennolla moduulit, jota voimme käyttää. (ks. kuvio 12)



Kuvio 12. Interfacen asetukset.

Käytämme tässä demossa captiveflask valmiita sapluunoita, otamme käyttöön Captiveflaskin komennolla: ”set misc.extra_captiveflask”, ”Download” komennolla lataamme kaikki saatavilla olevat sapluunat (ks. kuvio 13)

```
wp3 : extra_captiveflask > download
[*] downloading templates on /tmp/master.zip
[+] extra captiveflask download successful.
[*] extracting files from zip archive
[*] extracted files on : /tmp/extra-captiveflask-master
```

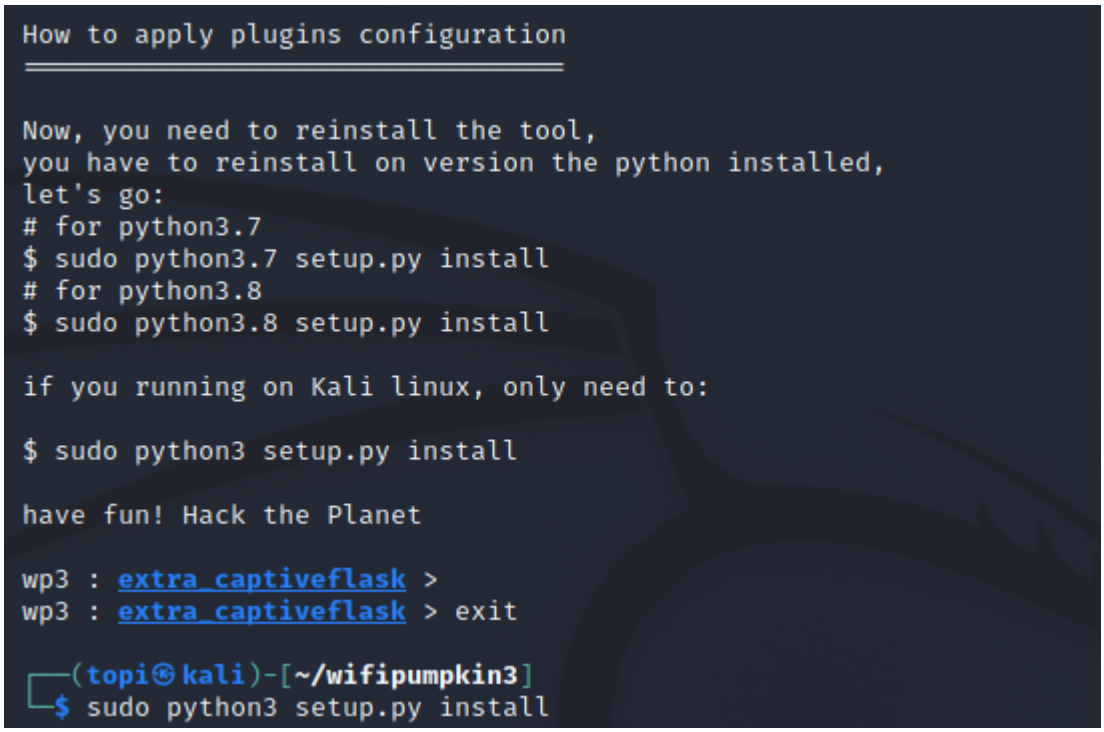
Kuvio 13. Sapluunoiden lataaminen.

”List” komennolla nähdään valmiita sapluunoita, tähän voisi myös tehdä itse sapluunan (kts. kappale 4.4), mutta tässä demossa käytämme ”facebook” sapluunaa. Asentamiseen käytämme komentoa ”install facebook” (ks. kuvio 14)

```
wp3 : extra_captiveflask > list

[*] Available Customs CaptiveFlask:
═══════════════════════════════════

 Name      | Author   | Installed   | Preview
-----------+----------+-------------+-----------------------------------
 example   | mh4x0f   | False       | https://i.imgur.com/G0wtAme.png
 facebook  | mh4x0f   | False       | https://i.imgur.com/PmDXvnq.png
 microsoft | mh4x0f   | False       | https://i.imgur.com/IZmpwQi.jpg

wp3 : extra_captiveflask > install facebook

[*] Install plugin:: facebook
═══════════════════════════════

[*] copy content file to wifipumpkin3/plugins/captiveflask/facebook.py
[*] copy content directory to config/templates/facebook
[*] plugin install sucessful
```

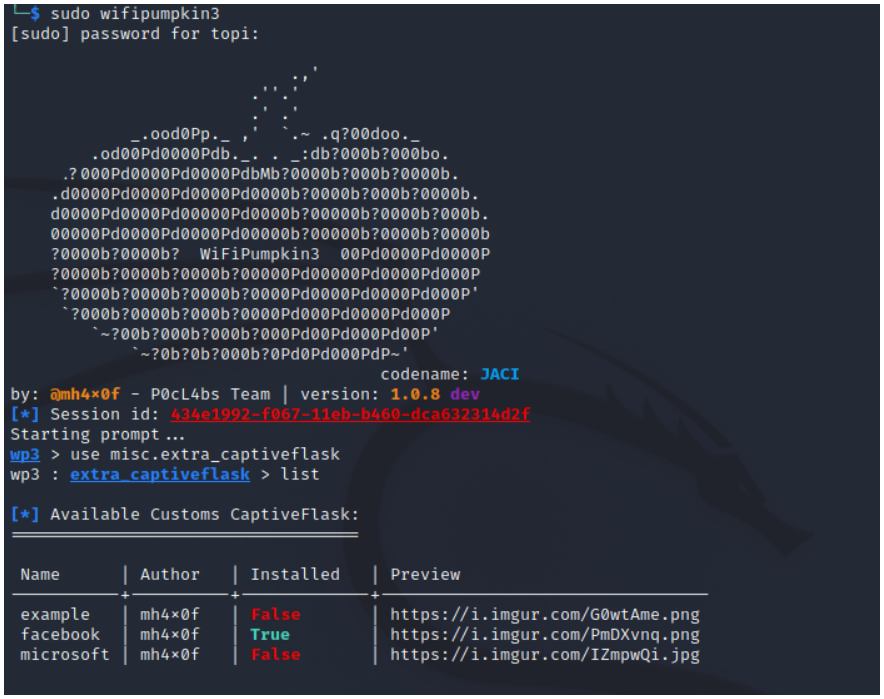
Kuvio 14. Sapluunat.

Sapluunan käyttöönottoon ohjelma osaa neuvoa suoraan mitä pitää tehdä, Kun käytämme Kali Linux käyttöjärjestelmää, proseduuri on selkeä, ”exit” komento ja ajetaan asennuskäsky uudestaan ”sudo python3 setup.py install” (ks. kuvio 15).

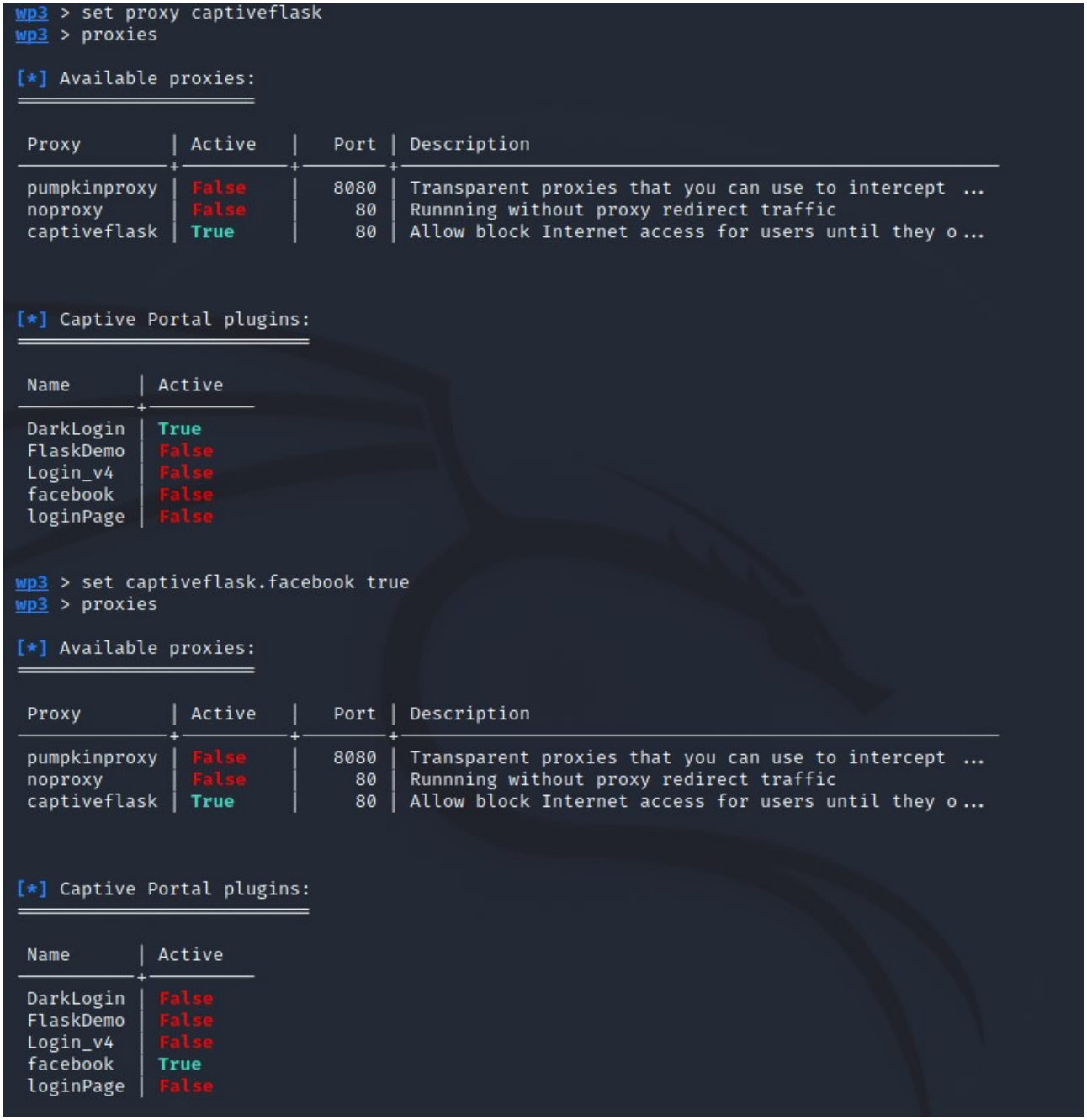


Kuvio 15. Sapluunan käyttöönotto.

Käynnistämme uudelleen ohjelmiston ja otamme käyttöön Captiveflaskin komennolla: ”use misc.extra_captiveflask”. ”List” komennolla katsomme, onko ”facebook” aktiivinen. (ks. kuvio 16)



Kuvio 16. Facebook sapluunan käyttöönotto.



Kuvio 17. Proxyn käyttöönotto.

Sitten voimmekin käynnistää Rogue AP:n, komennolla ”start” (ks. kuvio 18).

```
wp3 > start
[+] enable forwarding in iptables ...
[*] sharing internet connection with NAT ...
[*] settings for captive portal:
[*] allow FORWARD UDP DNS
[*] allow traffic to captive portal
[*] block all other traffic in access point
[*] redirecting HTTP traffic to captive portal
[+] starting hostpad pid: [173757]
wp3 > [+] hostapd is running
[*] starting pydhcp_server
[*] starting pydns_server
[+] starting captiveflask pid: [173762]
[*] starting sniffkin3 port: [80, 8080]
[+] sniffkin3 → kerberos   activated
[+] sniffkin3 → hexdump    activated
[+] sniffkin3 → emails     activated
[+] sniffkin3 → httpCap    activated
[+] sniffkin3 → ftp        activated
```

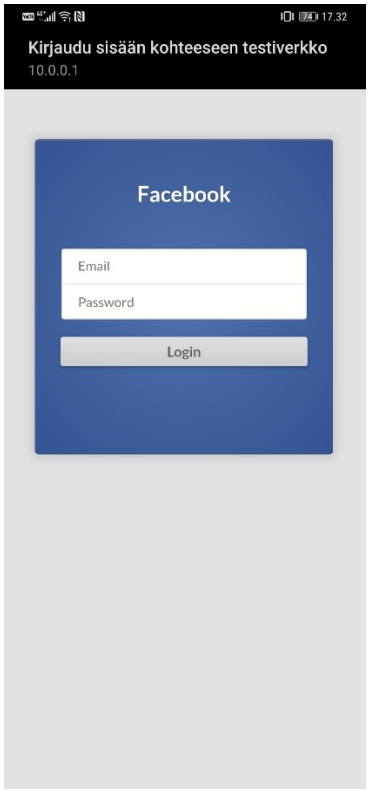
Kuvio 18. Rogue AP:n käynnistys.

Seuraavaksi demonstroidaan Rogue AP:seen yhdistyvää henkilöä.

Otamme yhteyden puhelimella Rogue AP:seen (ks. kuvio 19).

Kuvio 19. Yhdistäminen Rogue AP:seen.

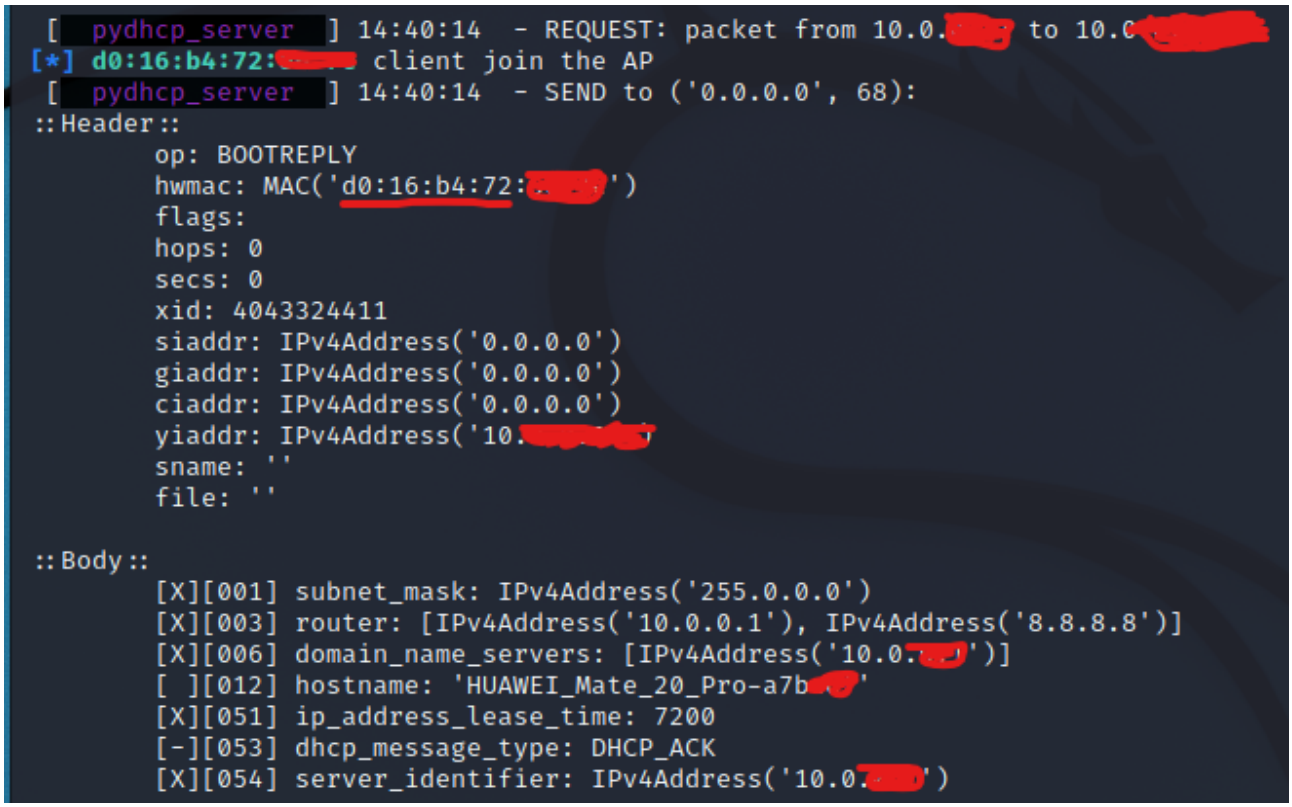
Kirjaudutaan Rogue AP:seen (ks. kuvio 20).



Kuvio 20. Kirjautumisikkuna.

Liittyessä Wifi-verkkoon, wifipumpkin3 tulostaa heti terminaaliin liittyjän tietoja (ks. kuvio 21).

Kuvasta näemme, että ”header” kohdassa, ”hwmac” lukee liittyjän laitteen MAC-osoite. Tulosteesta voidaan myös havaita ”body” kohdassa ”hostname”, joka tässä tapauksessa kertoo laitteen olevan Huawei Mate 20 Pro. (Ks. kuvio 21.)



Kuvio 21. Tietoja liittymisestä verkkoon.

Kirjautuessa, myös wifipumpkin3 tulostaa kirjautumistiedot (ks. kuvio 22).

Kuvio 22. Kirjautumisen tiedot.

6 Loppupohdinta

Opinnäytetyön toteutus konkreettisesti muodostui hankalaksi vallitsevan tilanteen (COVID-19) vuoksi. Tutkimuksen idea onnistuttiin hyvin välittämään demon välityksellä, demonstraatio vastaa lähes täydellisesti konkreettista tilannetta, miten hyökkäys toteutettiin, mitä laitteita se vaatii ja miten havaita hyökkäys. Haastavimmaksi osaksi muodostui, millä Rogue AP voidaan toteuttaa ja minkälaisella ohjelmistolla. Raspberry PI muodostui erinomaiseksi valinnaksi kokonsa puolesta, koska valetukiasema pitää sijoittaa hyökkäyksen kohteen lähelle. Raspberry PI:llä voidaan myös ajaa Kali Linuxin ARM versiota, joka on tarpeeksi kevyt käyttöjärjestelmä pyörittämään Rogue AP:ta. Ohjelmiston valinnassa Wifipumpkin3 tarjosi tarvittavat liitännäiset. Captiveflask liitännäisellä voitiin luoda kirjautumisikkuna, joka soveltuu loistavasti kouluympäristön hyökkäykseen, koska Rogue AP:hen liittyvä ei kyseenalaistaisi kirjautumista opiskelijaverkkoon.

Opinnäytetyö oli omasta mielestä onnistunut, sain tuotettua toimivan Rogue AP:n, jolla saatiin halutut tiedot langattomaan verkkoon liittyvältä. Toimeksiantajalle jäi opinnäytetyöstä asennus- ja käyttöönotto-ohje, joita toimeksiantaja voi hyödyntää tulevaisuudessa opetustarkoitukseen ja mahdolliseen konkreettiseen toteutukseen.

Lähteet

CYBERDI projektiesittely. 2018. JAMKin CYBERDI-projektin kotisivut. Viitattu 07.04.2021 https://www.jamk.fi/fi/Tutkimus-ja-kehitys/projektit/CYBERDI/Projektiesittely/

Empiirinen tutkimus. 2015. Jyväskylän avoimen yliopiston tietopankin sivusto empiirisestä tutkimuksesta. Muokattu. 23.05.2015. Viitattu. 07.04.2021. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/empiirinen-tutkimus

Extra-captiveflask. 2020. Githubin tietosäilö Extra-captiveflaskistä. Viitattu 6.9.2021. https://github.com/mh4x0f/extra-captiveflask

Kaleem, Z. 2017. Blogipostaus. How to physically locate a Rogue Access Point. Viitattu 8.9.2021. https://www.accessagility.com/blog/locating-rogue-access-points

Kali Linux vs Ubuntu. 2020. Educba:n vertailu artikkeli Kali Linux vs Ubuntu. Viitattu 5.9.2021. https://www.educba.com/kali-linux-vs-ubuntu/

Raspberry Pi 4. N.d. Raspberry pi:n kotisivuilla oleva malliesittely. Viitattu 4.9.2021. https://www.raspberrypi.org/products/raspberry-pi-4-model-b/

Roser, M. Ritchie, H & Ortiz-Ospina, E. N.d. Artikkeli internetin kasvusta. Ourworldindatan verkkojulkaisu. Viitattu 3.9.2021 https://ourworldindata.org/internet

Shah, A. N.d. Khan academyn artikkeli Rogue access pointeista. Viitattu 4.9.2021 https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks

Threats to Information Security. 2021. Geeksforgeeksin artikkeli tietoturvauhista. Viitattu. 4.9.2021. https://www.geeksforgeeks.org/threats-to-information-security/

What is Kali Linux. 2021. Kali Linuxin virallinen dokumentaatio, mikä on Kali Linux. Viitattu 5.9.2021 https://www.kali.org/docs/introduction/what-is-kali-linux/

Wireless Rogue ap. 2016. Juniperin dokumentti Rogue access pointista. Viitattu 4.9.2021 https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.1/topics/concept/wireless-rogue-ap.html

Liitteet

Liite 1. Asennus- ja käyttöönotto-ohje

Rogue Access Point asennus- ja käyttöönotto-ohjeet

Raspberry Pi, Kali Linux ja WifiPumpkin3

Tarvittavat laitteet:

Raspberry PI 4 tai uudempi

SD-kortti vähintään 4gb muistilla

SD-kortin lukija, käyttöjärjestelmän käyttöönottoon kortille.

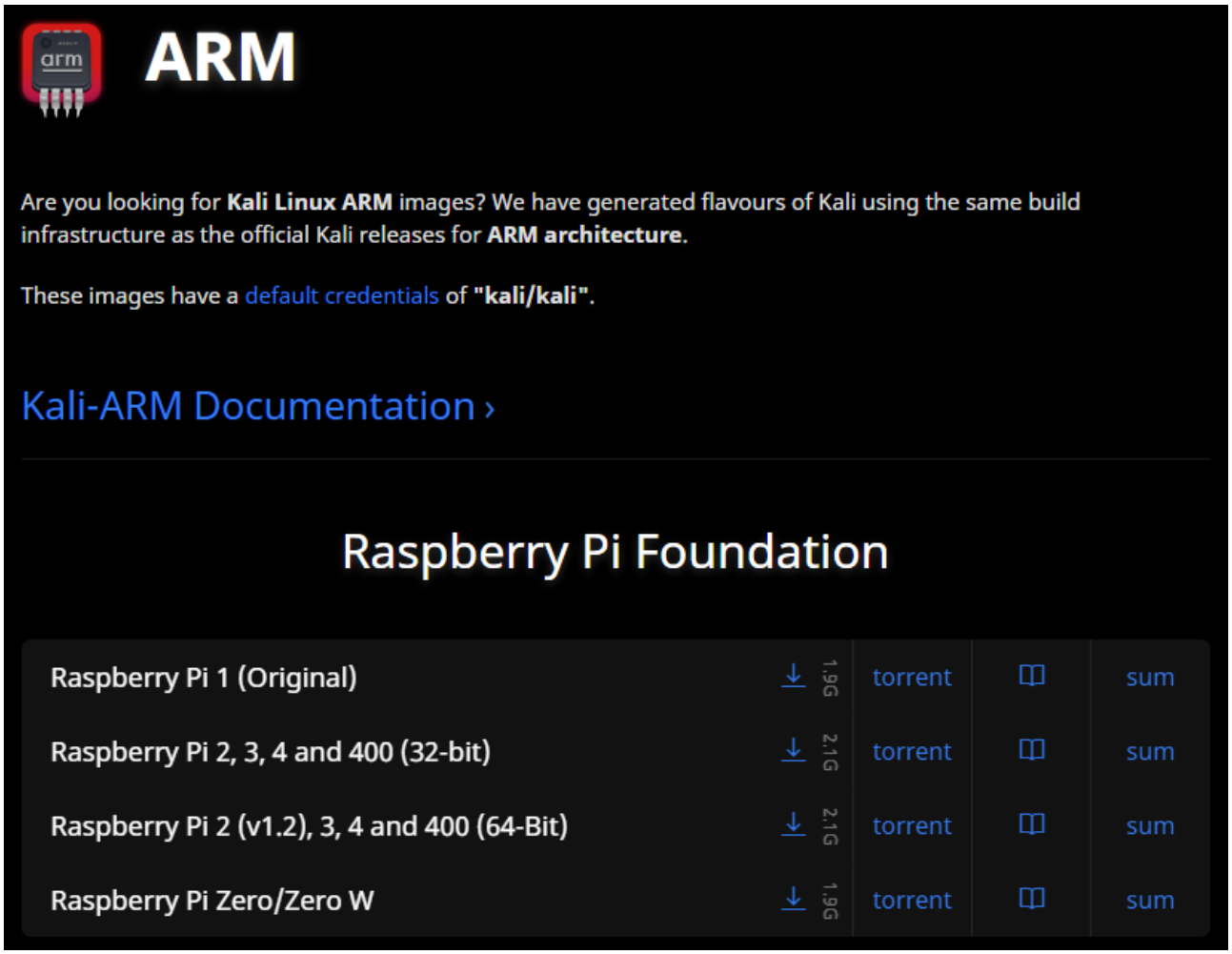
virtalähde tai verkkovirta

RJ45-piuha/ulkoinen wifi-adapteri/puhelin jolla jakaa internet-yhteys

Käyttöjärjestelmän asennus

Aloitamme lataamalla Kalin ARM imagen, kalin virallisilta sivuilta, käytämme 64-bittistä versiota.

Lataussivu: https://www.kali.org/get-kali/#kali-arm



Kuva 1. Kalin lataussivu.

Latauksen jälkeen, image pitäisi siirtää SD-kortille.

Kytke SD-kortin lukija koneeseen, tyhjennä muistikortti.

Imagen siirtämiseen voi käyttää esimerkiksi BalenaEtcheriä.

Lataussivu: https://www.balena.io/etcher/

Kun image on SD-kortilla, voidaan se laittaa takaisin Raspberry PI:hin, kytkeä Raspberry PI virtoihin ja verkkoon valitsemalla tavalla (RJ45 LAN-piuhalla, ulkoisella Wifi-adapterilla tai puhelimalla)

Kali Linuxiin voidaan kirjautua oletus tunnuksilla kali/kali.

Kali Linuxissa on oletuksena SSH-yhteyden muodostaminen pois päältä, joten se on laitettava päälle, jos haluaa ajaa Rogue AP:ta SSH-yhteyden kautta (helpottaa elämää kummasti).

Avaa komentorivi ja mahdollistetaan SSH-yhteys.

Lisätään käyttäjä:

sudo adduser topi

sudo usermod -aG sudo topi

Käyttäjän lisäyksessä voi täyttää muita yksityiskohtaisempia tietoja halutessaan, salasana pitää täyttää.

SSH-yhteyden muodostamiseen pitää ottaa käyttöön xrdp serveri komennoilla:

sudo apt-get update

sudo apt-get install xrdp

sudo systemctl start xrdp

sudo systemctl start xrdp-sesman

Tämän jälkeen voimme muodostaa SSH-yhteyden Raspberry PI:hin toiselta koneelta.

Selvitä Rasbperry PI:n IP-osoite, komentoriviltä komennolla:

ifconfig

Muodosta yhteys etätyöpöytä sovelluksella (remote dekstop) käyttäen aikaisemmin selvitettyä IP-osoitetta.

Käytä kirjautumiseen luomaasi tunnusta.

Ohjelmiston asennus

WifiPumpkin3 asennukseen tarvitsee tehdä muutamat valmistelut.

Asennamme tarvittavat paketit komennoilla:

sudo apt install python3-pyqt5 hostapd

sudo apt install libssl-dev libffi-dev build-essential

Sitten lataamme Git repositorion komennolla:

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

Repositorion latauksen jälkeen siirrymme asennuskansioon ja ajamme asennuskomennon:

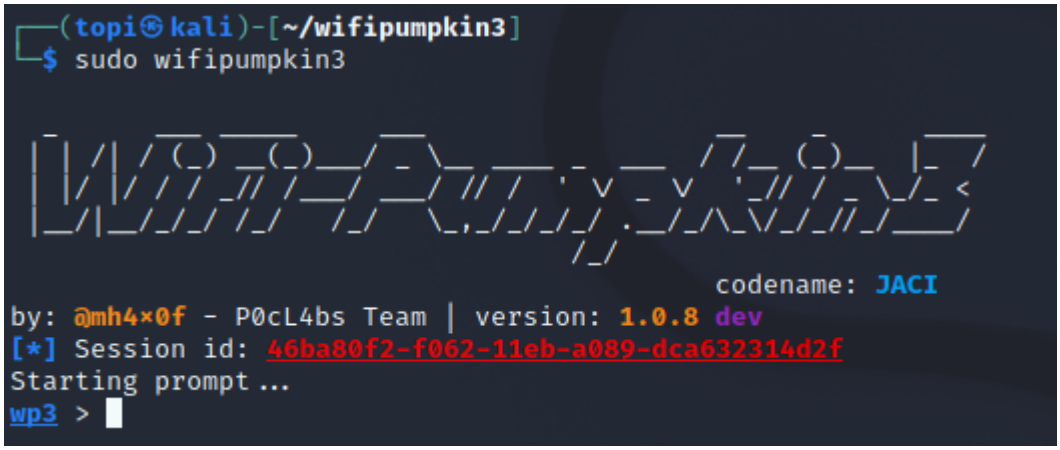
cd wifipumpkin3

sudo python3 setup.py install

Käynnistämme ohjelmiston komennolla:

sudo wifipumpkin3

Nyt pitäisi komentorivissä näyttää kuvan 2 mukaiselta.



Kuva 2. Wifipumpkin3 käynnistettynä.

Voimme aloittaa Rogue AP:n konfiguroinnin, Wlan0 on Raspberry PI:n sisäinen wlan-adapteri, jota käytämme Rogue AP:n mainostettavaan verkkoon.

Asetamme Rogue AP:lle wlanin, nimen ja otetaan dns loggaus pois käytöstä Komennoilla:

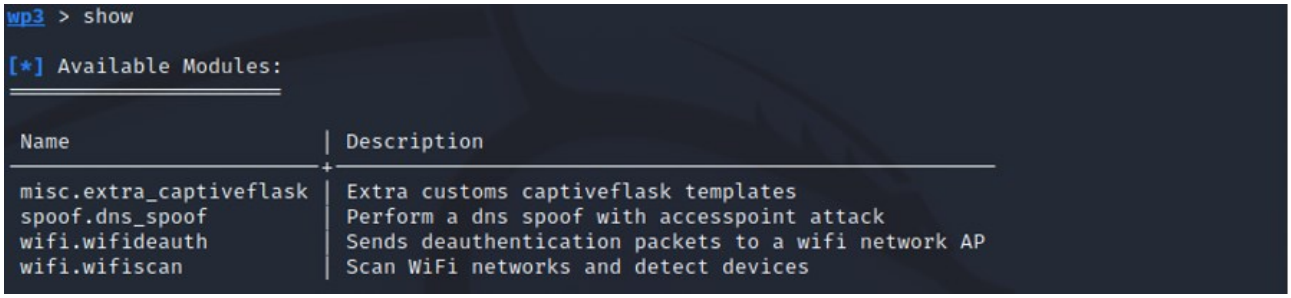
set interface wlan0

set ssid testiverkko

ignore pydns_server

Katsotaan saatavilla olevat moduulit komennolla:

show



Kuva 3. Moduulit

Käytämme Captiveflask moduulia kirjautumisikkunan luonnissa, lataamme olemassa olevat sapluunat komennoilla:

set misc.extra_captiveflask

download

Captiveflask on täysin kustomoitavissa hyökkäyksen kohteen mukaan, ohjeet löytyvät, github repositoriosta:

https://github.com/mh4x0f/extra-captiveflask

Tässä työohjeessa käymme läpi, miten ottaa käyttöön Captiveflask, työn tekijälle jää vapaat kädet muokata kirjautumisikkuna. Käytämme esimerkkinä ”facebook” sapluunaa.

Katsotaan seuraavaksi saatavilla olevat sapluunat komennolla:

list

```
wp3 : extra_captiveflask > list

[*] Available Customs CaptiveFlask:
═══════════════════════════════════

 Name      | Author   | Installed   | Preview
-----------+----------+-------------+-----------------------------------
 example   | mh4x0f   | False       | https://i.imgur.com/G0wtAme.png
 facebook  | mh4x0f   | False       | https://i.imgur.com/PmDXvnq.png
 microsoft | mh4x0f   | False       | https://i.imgur.com/IZmpwQi.jpg
```

Kuva 4. Valmiit sapluunat.

Sapluunan voi ottaa käyttöön komennolla:

install facebook

Ohjelmisto osaakin tässä vaiheessa neuvoa, että sapluunan käyttöönotto vaatii uudelleen asennusta, eli asennamme uudelleen WifiPumpkin3:sen komennoilla:

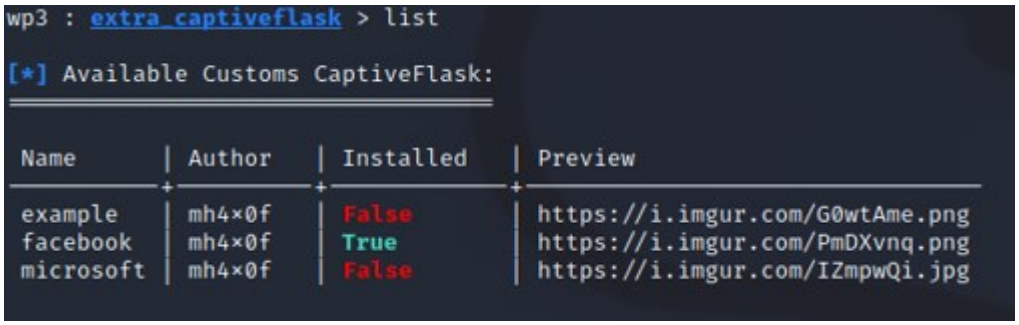
exit

sudo python3 setup.py install

Ohjelman käynnistyttyä, otamme Captiveflaskin aktiiviseksi ja katsomme että facebook on asennettu komennoilla:

use misc.extra_captiveflask

list



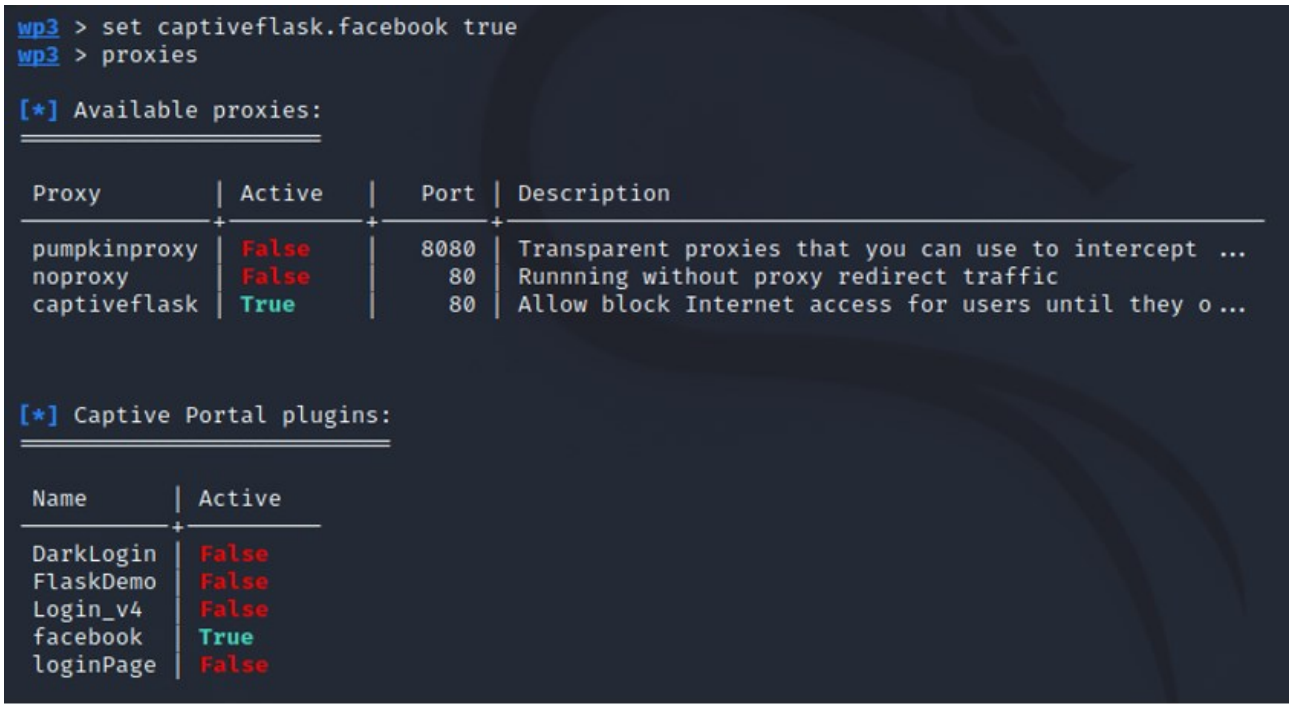
Kuva 5. Facebook asennettu.

Asetetaan Captiveflask proxyksi ja katsotaan että sapluuna on aktiivinen komennoilla:

set proxy captiveflask

set captiveflask.facebook true

proxies



Kuva 6. Proxyt.

Rogue AP on nyt konfiguroita ja valmis käynnistettäväksi komennolla:

start

Tämän jälkeen Rogue AP alkaa mainostaa luomaasi verkkoa ja keräämään kirjautustietoja ja liittyvien tietoja.

Komentoja mitä voidaan käyttää Wifipumpkin3 ohjelmistossa:

help = listaa saatavilla olevat komennot

clients = näyttää Rogue AP:seen yhdistetyt käyttäjät

ap = näyttää Rogue AP:n mainostettavan verkon tiedot

set = komento, jolla voidaan asettaa muuttujia

start = Rogue AP:n käynnistys

stop = lopettaa Rogue AP:n toiminnan

ignore = Viestien loggauksien poisto, voidaan poistaa liitännäisien logituksen

info = Voidaan hakea proxyistä ja liitännäisistä tietoa

jobs = Näyttää taustaprosessit

mode = näyttää saatavilla olevat langattoman yhteyden tilat

plugins = näyttää saatavilla olevat liitännäiset ja niiden tilan

proxies = näyttää saatavilla olevat proxyt ja niiden tilan

show = näyttää saatavilla olevat moduulit

dump = tulostaa tiedot Rogue AP:n clientista

update = päivittää Rogue AP:n git repositoriosta jos löytyy uusi versio