Anniina Peltola

Nmap-työkalun Python-laajentimen harjoitustyön kehittäminen tietoturva-kurssille

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

23.5.2024

Tiivistelmä

Tekijä:	Anniina Peltola
Otsikko:	Nmap-työkalun Python-laajentimen harjoitustyön kehittäminen tietoturvakurssille
Sivumäärä:	32 sivua + 1 liite
Aika:	23.5.2024
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Tietotekniikka
Ohjaajat:	Osaamisaluepäällikkö Janne Salonen

Insinöörityössä kehitettiin harjoitus Nmap scanning basics -tietoturvakurssille. Insinöörityö tehtiin Metropolia ammattikorkeakoululle. Kurssia järjestetään Metropolia ammattikorkeakoulun Moodle-alustalla. Tavoitteena oli kehittää harjoitus, jossa Windows-laitteella Kali Linux -jakelussa ajetaan Network Mapper -verkkoskannaustyökalua Python-laajentimella.

Aineistoa kerättiin monipuolisesti verkkoaineistosta ja e-kirjoista. Insinöörityössä kuvattiin Windows Subsystem for Linux -järjestelmän toimintaa sekä käyttöönottoa. Windows Subsystem for Linux mahdollistaa Linux-järjestelmän käytön Windowsissa. Linux-jakeluksi valittiin Kali Linux. Network Mapper -verkkoskannaustyökalu asennettiin Kali Linux -jakeluun. Python-tulkille haettiin Python-Nmap-laajennin, koska testattiin Network Mapper -verkkoskannausta Python-ohjelmointikielellä. Testauksissa Network Mapper -verkkoskannaukset kohdistettiin harjoitteluun tarkoitetulle verkkosivustolle.

Insinöörityön tuloksena kehitettiin harjoitus tietoturvakurssin opiskelijoille. Opiskelijat voivat harjoituksen avulla kokeilla Linux-järjestelmää Windowsissa sekä testata Network Mapper -työkalun käyttöä Python-laajentimella Kali Linux -jakelussa.

Avainsanat: Nmap, Python, WSL, Kali Linux

Abstract

Author:	Anniina Peltola
Title:	Developing an exercise for the Python extension of the Nmap tool for an information security course
Number of Pages:	32 pages + 1 appendice
Date:	23 May 2024
Degree:	Bachelor of Engineering
Degree Programme:	Information and Computer Technology
Professional Major:	Computer Technology
Supervisor:	Janne Salonen, Head of School (ICT)

In the engineering thesis an exercise was developed for the Nmap Scanning Basics information security course. The thesis was conducted for Metropolia University of Applied Sciences. The course is hosted on the Moodle platform of Metropolia university of applied sciences. The purpose was to develop an exercise in which the Network Mapper network scanning tool with a Python extension is run on a Windows machine in the Kali Linux distribution.

Data was collected from the various online sources and e-books. The engineering thesis described the functionality and installation of the Windows Subsystem for Linux program. Windows Subsystem for Linux enables the use of the Linux system in Windows. Kali Linux was chosen as the Linux distribution. The Network Mapper tool was installed on the Kali Linux distribution. The Python-Nmap extension was obtained for the Python interpreter as Nmap scanning was tested using the Python programming language. The Network Mapper scans were targeted at a website designated for training.

As a result of the engineering thesis, an exercise was developed for the students of the information security course. In the information security course, students can use the exercise to try out the Linux system in Windows and test the use of the Network Mapper tool with the Python extension in the Kali Linux distribution.

Keywords: Nmap, Python, WSL, Kali Linux

Sisällys

Lyhenteet

BASH: *Bourne Again Shell.* Linuxissa oletuksena oleva komentotulkki. Komentotulkin kautta käyttäjä antaa komennot, ja komentotulkki tulkitsee käyttäjän komennot.

GNU: *GNU's Not Unix.* Unixin pohjalta GNU-projektissa kehitetty käyttöjärjestelmä. Perustuu vapaisiin ohjelmistoihin. GNU-ohjelmistoja osana Linux-jakeluita nimitetään tavalla GNU/Linux.

IP: *Internet Protocol.* Tietoliikenteen perusprotokolla, jonka päälle rakennetaan muut protokollat.

NMAP: *Network Mapper.* Maksuton avoimen lähdekoodin verkkoskannaustyökalu.

TCP: *Transmission Control Protocol*. Tiedonsiirtoon yhteyssuuntautunut, yleinen ja luotettava tietoliikenneprotokolla.

UDP: *User Datagram Protocol.* Tiedonsiirtoon nopea ja yhteydetön, mutta hieman epäluotettava tietoliikenneprotokolla.

UNIX: Käyttöjärjestelmä. Yhdysvalloissa kehitetty monen käyttäjän järjestelmä. Yksi Unix-järjestelmän toteutus on Linux. Tavaramerkkinä on UNIX.

WSL: *Windows Subsystem for Linux*. Mahdollistaa Windowsin ja Linuxin yhtäaikaisen käytön Windowsissa. Antaa mahdollisuuden asentaa Linux -jakeluita ja käyttää Linux-ohjelmia Windowsissa.

1 Johdanto

Tämän insinöörityön tavoitteena oli kehittää harjoitus Metropolia ammattikorkeakoulun Nmap scanning basics -tietoturvakurssille. Tietoturvakurssia toteutetaan Metropolia ammattikorkeakoulun Moodle-alustalla. Harjoituksessa oli tarkoitus käyttää Linux- ja Windows-käyttöjärjestelmää samalla Windows-laitteella. Uusimmissa Windows-versioissa on alijärjestelmä Linuxille, minkä avulla molempia järjestelmiä voidaan yhtäaikaisesti käyttää Windowsissa. Lisäksi harjoituksessa oli tarkoitus testata verkkoskannausta Python-ohjelmointikielellä Network Mapper (Nmap) -työkalulla.

Windows ja Linux ovat tietokonemarkkinoiden hyvin tunnetut käyttöjärjestelmät. Windows on Microsoftin 1980-luvulla julkaisema käyttöjärjestelmä. Windows on hyvin suosittu kotikoneiden käyttöjärjestelmänä ja on useimmiten jo valmiiksi asennettuna uusissa kotiin ostettavissa tietokoneissa. (Microsoft 2024.)

Windows on maksullinen järjestelmä, josta on saatavilla erilaajuisia lisenssejä käyttäjien tarpeiden mukaan. Windows-nimi on lähtöisin käyttöjärjestelmälle tyypillisistä ikkunoista, joita voidaan näytöllä siirrellä. Windows-järjestelmää on päivitetty lukuisia kertoja vuosien varrella, ja siitä on tehty monia versioita. Uusin Windows-käyttöjärjestelmä Windows 11 julkaistiin vuonna 2021. Tässä työssä käytettiin Windows 10 -käyttöjärjestelmää. (Microsoft 2024.)

Windowsin helppokäyttöinen graafinen käyttöliittymä on laajalti tunnettu. Windows on järjestelmänä hyvin käyttäjäystävällinen. Sitä on helppo hallita eikä sillä useinkaan suoriteta tahattomasti mitään järjestelmän kannalta ratkaisevia toimenpiteitä. Windows on rajoitetumpi järjestelmä kuin Linux eikä esimerkiksi uusien turvallisuusominaisuuksien lisääminen olemassa olevaan Windows-ohjelmistoon ole yksinkertaista. (Awan & Khan 2022: 47–53.)

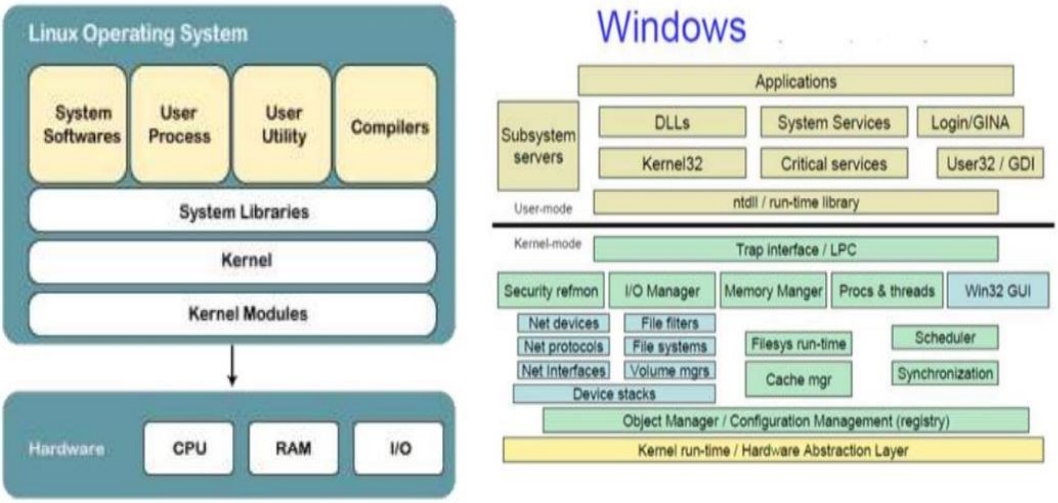
Linux on alun perin 1990-luvun alussa suomalaisen tietojenkäsittelytieteen opiskelijan, Linus Torvaldin, Helsingin yliopistossa kehittämä käyttöjärjestelmä. Käyttöjärjestelmä sai myöhemmin nimen Linux, joka tulee Linux-ytimestä. (Negus 2015: 6–8.)

Torvald kehitti Linuxin harrastemielessä omassa käyttöjärjestelmäprojektissaan. Nykyään siitä on tullut yksi maailman käytetyimmistä käyttöjärjestelmistä. Tänä päivänä muun muassa Google käyttää tuhansia Linux-palvelimia hakuteknologiansa pyörittämiseen. Myös Android-puhelimen käyttöjärjestelmä pohjautuu Linuxiin, vaikka tuskin monet älypuhelinten käyttäjät tätä tiedostavat. Kotitietokoneiden käyttöjärjestelmänä Linux ei ole kovin yleinen vaan näissä Windows on selvästi yleisempi käyttöjärjestelmä. (Negus 2015: 6–8.)

Linux on avoimen lähdekoodin käyttöjärjestelmä, joka toimii Linux-ytimellä. Linux on kustannustehokas ja turvallinen käyttöjärjestelmä. Linux-järjestelmällä on suuri muunneltavuus. Se on mukautettavissa käyttäjän tarpeisiin lähes rajattomilla mahdollisuuksilla. Linux ei ole riippuvainen graafisesta käyttöliittymästä, vaikka jakeluiden mukana yleensä tulee työpöytäympäristö. (Awan & Khan 2022: 47.)

Linuxia käytetään yleensä erilaisina ilmaisina jakelupaketteina. Jakeluihin on käyttötarkoituksen pohjalta sisällytetty asennuspaketti, ohjelmistoja, ohjelmakirjastoja sekä mahdollisuudet lisäohjelmien ja päivitysten asentamiseen. Yleensä jakelupaketit ovat kokonaisia käyttöjärjestelmiä. Ne voivat olla yksittäisten henkilöiden kokoamia tai kaupallisia kokonaisuuksia. Yksi käytetyimmistä Linux-jakeluista on Debian, joka tunnetaan erittäin vakaana järjestelmänä. Monet uudemmista jakeluista perustuvat Debianiin, kuten Ubuntu, Linux Mint, elementary OS, Zorin OS ja Kali Linux. (Negus 2015: 6–8.)

Linux- ja Windows-käyttöjärjestelmän arkkitehtuuria havainnollistetaan kuvassa 1. Kuvaa tarkastellessa havaitaan järjestelmien eroavan selvästi arkkitehtuuriltaan.

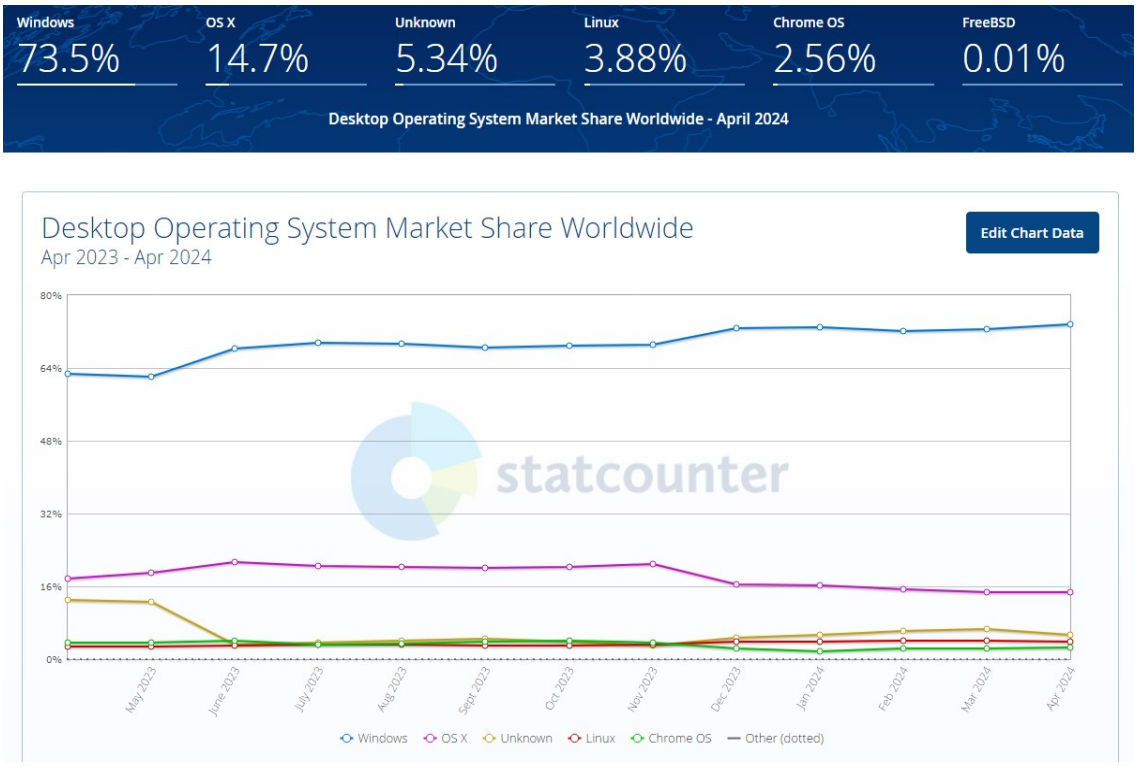


Kuva 1. Linux- ja Windows-käyttöjärjestelmän arkkitehtuuri (Awan & Khan 2022: 42).

StatCounter on vuonna 1999 Irlannissa perustettu analytiikkayhtiö, joka tarjoaa riippumatonta ja puolueetonta tilastointia maailmanlaajuisesti. Tilastot perustuvat verkkosivujen katselun analysointiin. Kuukaudessa analysoidaan maailmanlaajuisesti yli viisi miljardia sivunkatselua ja seurattavia sivustoja on yli 1,5 miljoonaa. StatCounter analysoi sivunkatselusta esimerkiksi käytetyn käyttöjärjestelmän, selaimen ja mahdollisen mobiililaitteen käytön. (StatCounter 2024a.)

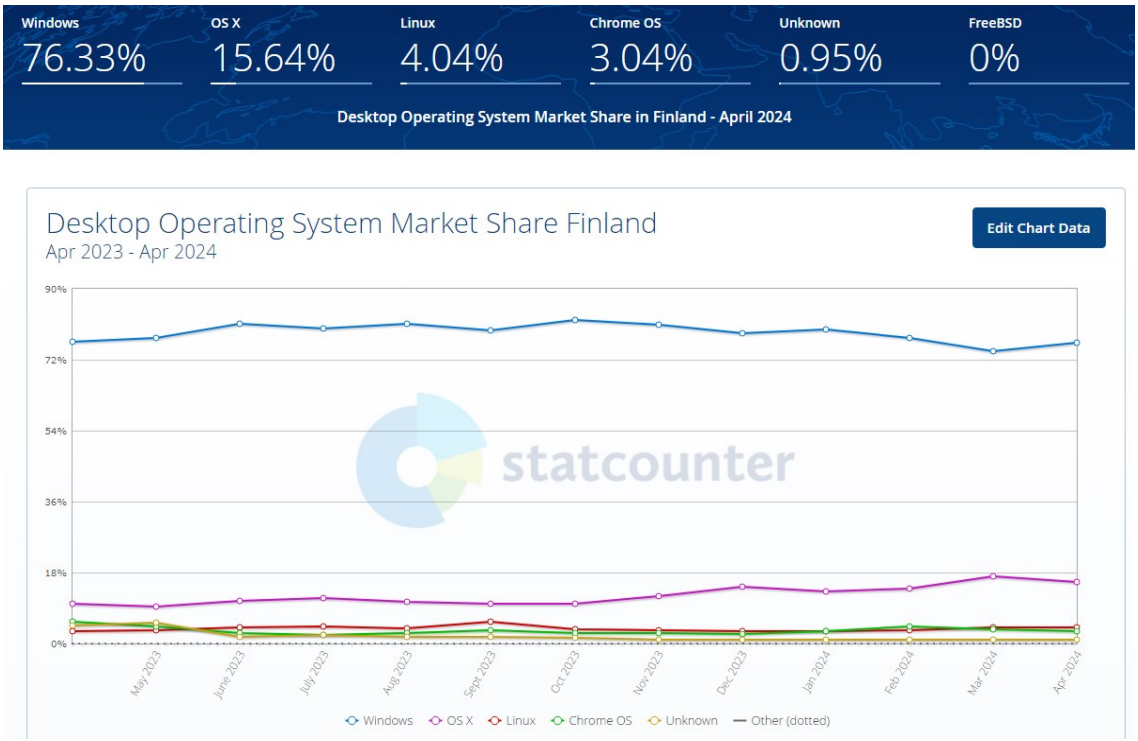
StatCounterin tilastot ovat yhden yrityksen dataan perustuvia, mutta todennäköisesti suuntaa antavia. StatCounterin sivustolta dataa pääsee tarkastelemaan haluamallaan aikavälillä. Kuvan 2 tilastossa on ajankohtaisia maailmanlaajuisia markkinaosuuksia eri käyttöjärjestelmien välillä.

Tietokoneiden käyttöjärjestelmänä Windows on yleisin. Huhtikuussa 2024 Windowsin markkinaosuus oli yli 70 prosenttia, kun taas Linuxin osuus oli vajaa neljä prosenttia. Windowsin jälkeen toiseksi yleisin on OS X -käyttöjärjestelmä, nykyisin nimeltään macOS-käyttöjärjestelmä. Se on Mac-tietokoneissa käytettävä Applen kehittämä Unix-käyttöjärjestelmä. OS X:n osuus markkinaosuudesta oli huhtikuussa noin 15 prosenttia. (StatCounter 2024c.)



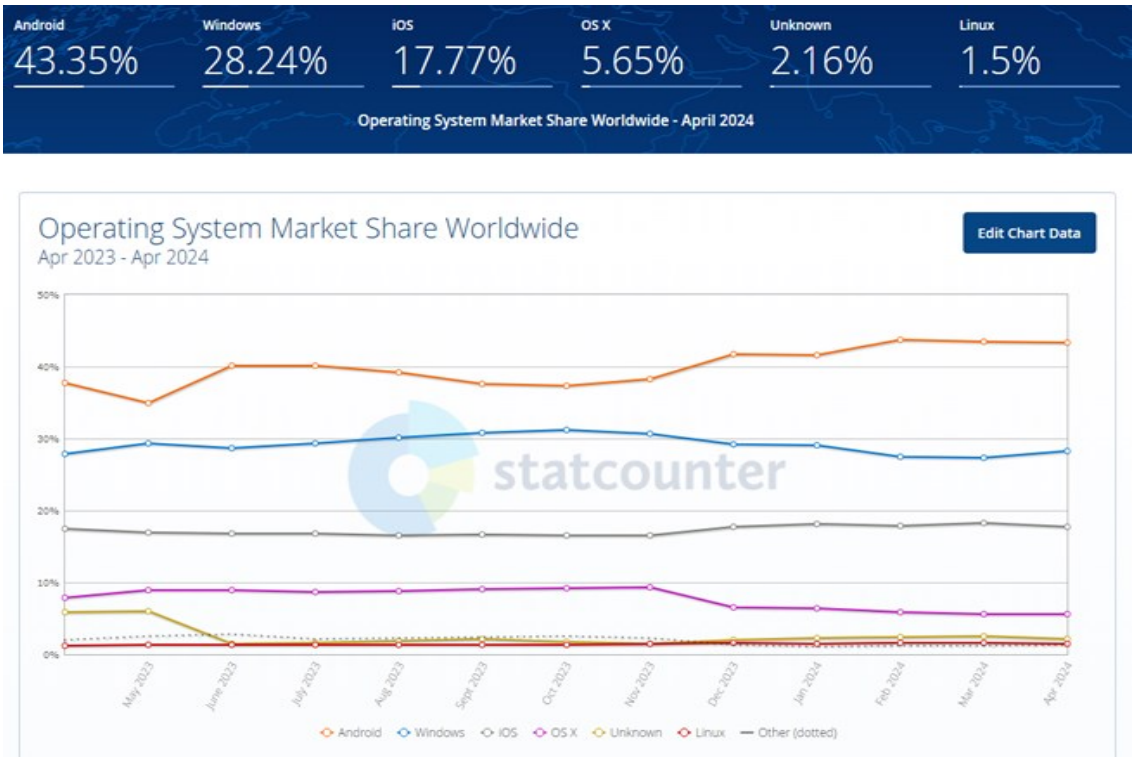
Kuva 2.Tietokoneiden käyttöjärjestelmien markkinaosuudet maailmanlaajuisesti viimeisen 12 kuukauden ajalta (StatCounter 2024c).

Kuvassa 3 on tilasto viimeisen 12 kuukauden ajalta tietokoneiden käyttöjärjestelmien markkinaosuuksista Suomessa. Suomessa markkinaosuudet näyttävät kahden käytetyimmän käyttöjärjestelmän osalta hyvin samanlaisilta kuin maailmanlaajuisestikin. (StatCounter 2024b.)



Kuva 3.Tietokoneiden käyttöjärjestelmien markkinaosuudet Suomessa viimeisen 12 kuukauden ajalta (StatCounter 2024b).

Kuvassa 4 vertaillaan markkinaosuuksia maailmanlaajuisesti kaikentyyppisten laitteiden osalta. Yleisin laitteiden käyttöjärjestelmä on Android 43 prosentin osuudella. Tätä todennäköisesti selittää Androidin käyttö yleisesti älypuhelinten käyttöjärjestelmänä. Toiseksi yleisin on Windows 28 prosentin markkinaosuudella. Linuxin käyttö jää markkinoiden perusteella puoleentoista prosenttiin. (StatCounter 2024d.)



Kuva 4.Kaikentyyppisten laitteiden käyttöjärjestelmien markkinaosuuksien vertailu viimeisen 12 kuukauden ajalta maailmanlaajuisesti (StatCounter 2024d).

Markkinoiden pohjalta tarkasteltuna käytetyin tietokoneiden käyttöjärjestelmä on Windows. Sen osuus on selvästi muita suurempi. Kova kilpailu eri järjestelmien kesken jatkuu todennäköisesti myös tulevaisuudessa. Linux- ja Windows-käyttöjärjestelmissä on omat etunsa ja haittansa kuten muissakin käyttöjärjestelmissä. Käyttäjän tarpeet määrittelevät sopivimman vaihtoehdon eikä kaikille markkinoiden suosituin ole välttämättä paras vaihtoehto. Yleensä järjestelmän menestymiseen vaikuttaa keskeisesti sen toiminnallisuus ja turvallisuus (Awan & Khan 2022: 53).

Network Mapper (Nmap) -työkalu on suosittu verkkoskannaustyökalu, jonka saa ladattua ilmaiseksi verkosta. Porttiskannaus on yksi yleinen verkkoskannauksen menetelmä. Nmap-työkalua voidaan hyödyntää säännöllisissä tietoturvatestauksissa. Tällöin verkon mahdolliset haavoittuvuudet löydetään ajoissa ja voidaan korjata. (Salmi 2021: 23–26.)

Verkkoskannauksella voidaan saada aikaan myös haittaa, jos tietoisesti etsitään jostakin kohteesta verkon haavoittuvuuksia ja aukkoja tietoturvassa. Verkkoskannaukseen tarkoitettuja ohjelmia on useita erilaisia. Ne ovat verkosta melko helposti kenen tahansa saatavilla. (Salmi 2021: 23–26.)

Päivittämättömät järjestelmät ovat erityisesti rikollisten kohteena. Verkon haavoittuvuuksia yritetään etsiä ennen kuin niitä ehditään korjata. Järjestelmälle ei kuitenkaan riitä pelkkien päivitysten tekeminen, vaan verkkoa tulisi tarkoin tutkia, jos löydetään pienikin haavoittuvuus. Haavoittuvuus on voinut olla jo pitkän aikaa, ja sitä on voitu hyväksikäyttää esimerkiksi tekemällä järjestelmään piilotettuja sisäänpääsyreittejä. (Kyberturvallisuuskeskus 2024.)

Ennen verkon tarkempaa tarkastelua on hyvä tiedostaa, että tällaisesta toiminnasta voi joutua rikosoikeudelliseen vastuuseen. Suomen rikoslaissa on erikseen tarkasti määritelty niin tietoliikenteen häiritsemisestä, tietojärjestelmään tunkeutumisesti kuin luvattomasta tietojen käsittelystä. Näistä saatetaan törkeimmissä tapauksissa tuomita vuosien vankeuteen. Sekä tietoliikenteen häirinnän että tietomurron kohdalla jo pelkkä yrityskin saattaa olla rangaistava teko. (Rikoslaki 1995.)

Tässä insinöörityössä tarkasteltiin Windows Subsystem for Linux -järjestelmää sekä Nmap -työkalua ja sen erilaisia skannausmenetelmiä. Lisäksi testattiin Nmap-työkalua Python-laajentimella tekemällä pienimuotoisesti verkkoskannausta.

2 Windows Subsystem for Linux (WSL)

2.1 Esittelyssä WSL

Windows Subsystem for Linux (WSL) on Windowsin alijärjestelmä, joka mahdollistaa Linux-ympäristön käyttämisen Windows-järjestelmässä ilman erillistä virtuaalikonetta tai kaksoiskäynnistystä. Sen avulla voidaan sujuvasti käyttää sekä Windowsia että Linuxia samanaikaisesti Windowsissa. (Microsoft 2023b.)

WSL:n avulla voidaan esimerkiksi käynnistää Windowsissa Linux-sovelluksia, ajaa BASH-komentosarjoja sekä Linux-komentorivisovelluksia, kuten työkaluja: vim ja emacs, kieliä: JavaScript, NodeJS, Python, C/C++, Ruby ja palveluita: SSHD, MySQL. WSL mahdollistaa erilaisten Linux-jakeluiden, kuten Ubuntun, Debianin ja Kalin, asentamisen ja suorittamisen Windowsissa. Jakeluiden myötä on mahdollista vastaanottaa myös automaattisia päivityksiä. Tässä insinöörityössä keskitytään Ubuntu- ja Kali-jakeluihin, jotka molemmat pohjautuvat tunnettuun ja vakaaseen Debian-jakeluun. (Microsoft 2023b.)

WSL:stä on käytössä kaksi erilaista arkkitehtuuria, WSL 1 vuodelta 2016 ja WSL 2 vuodelta 2020. WSL 2 on uudempi versio ja suorituskyvyltään paranneltu. WSL 1:ssä Linux-komennot käännetään Windowsille, mikä aiheuttaa toiminnallisia rajoituksia. WSL 2:ssa on täysimittainen Linux-ydin ja tekstipohjainen Linux-jakelu. (Microsoft 2023c.)

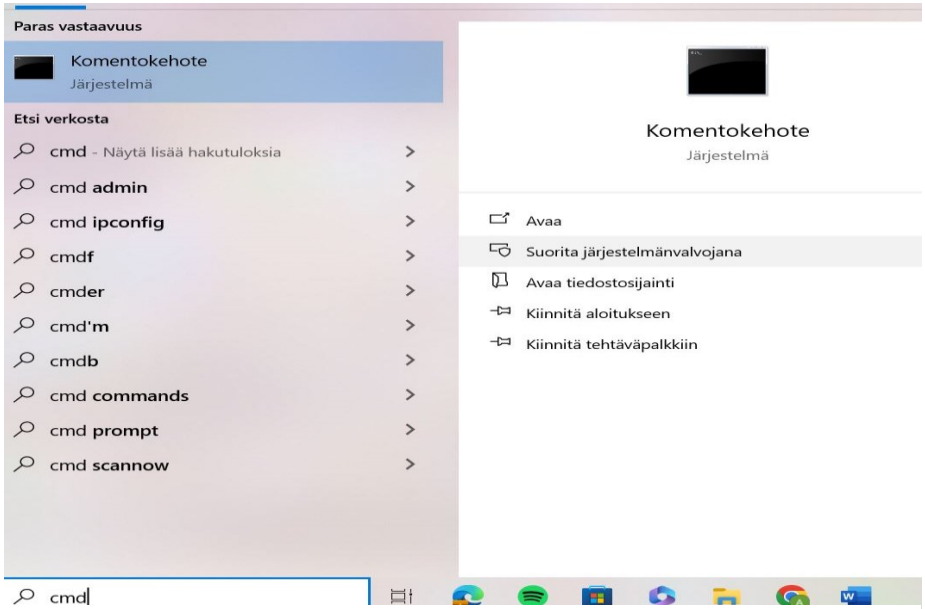
WSL 2 on yleensä oletuksena, kun asennetaan Linux-jakelu. Linux-jakelu toimii eristettynä omana osanaan WSL 2:n hallinnoimassa virtuaalikoneessa. WSL 1 ja WSL 2 ovat molemmat edelleen käytössä, ja niitä voidaan tarvittaessa ajaa myös rinnakkain. Näiden arkkitehtuurien välillä voidaan tehdä myös versiopäivityksiä toisesta toiseen. Tässä työssä hyödynnettävä arkkitehtuuri on WSL 2. (Microsoft 2023b.)

2.2 WSL käyttöönotto

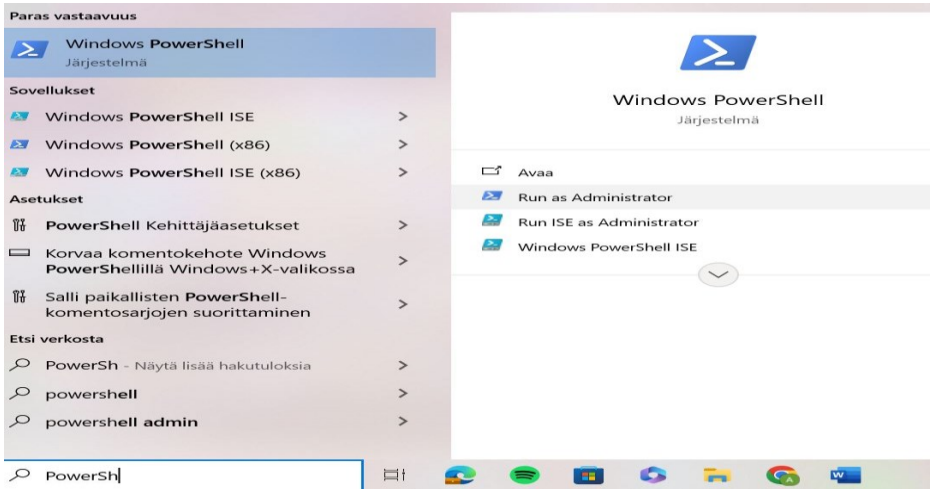
Windows Subsystem for Linux voidaan ottaa Windowsissa käyttöön monella eri tavalla. Tässä työssä Windows 10 -käyttöjärjestelmässä oleva WSL-alijärjestelmä asennettiin komentorivin avulla. Komento ottaa käyttöön ominaisuudet, jotka mahdollistavat WSL:n ajamisen sekä asentaa oletuksena GNU/Linux-käyttöjärjestelmän Ubuntu. WSL:n käyttöönotossa edetään eri tavalla, jos käytössä on vanhempi versio Windowsista kuin Windows 10 tai 11. (Microsoft 2023a.)

Oletuksena asentuva avoimen lähdekoodin Linux-järjestelmä Ubuntu pohjautuu Linuxin Debian-jakeluun. Ubuntussa on paljon peruskäyttöön soveltuvia ohjelmia, kuten esimerkiksi verkkoselain, sähköpostiohjelma ja tekstinkäsittelyohjelma. Lisää sovelluksia Ubuntuun, kuten muihinkin Linux-jakeluihin, voidaan asentaa helposti ohjelmapaketteina käyttäen komentoriviä tai paketinhallintaohjelmaa. (Ikonen ym. 2015: 8.)

WSL voidaan ottaa käyttöön esimerkiksi komentokehotteen (kuva 5) tai PowerShellin avulla (kuva 6). Molempien käyttö tehdään järjestelmävalvojan roolissa.



Kuva 5.Komentokehotteen avaaminen järjestelmänvalvojana.

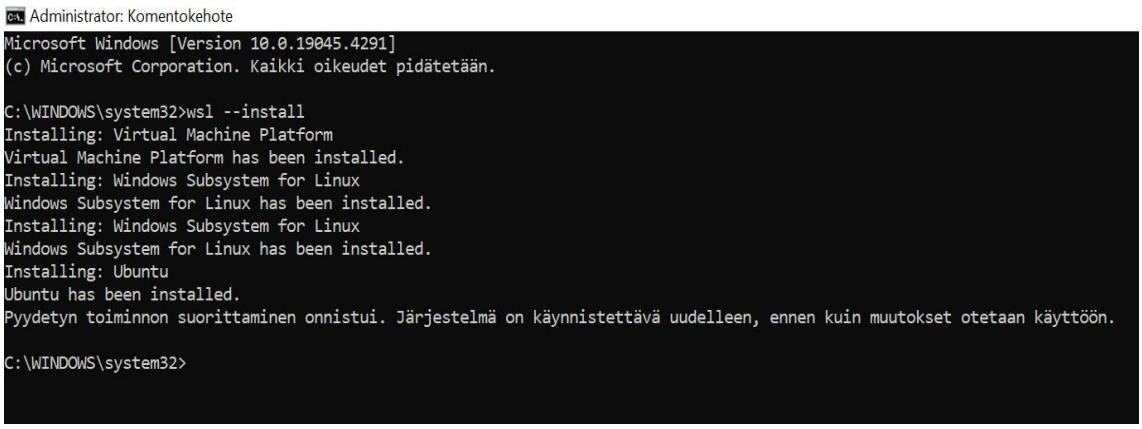


Kuva 6.PowerShellin avaaminen järjestelmänvalvojana.

Molemmissa vaihtoehdoissa WSL asennetaan komennolla (kuva 7):

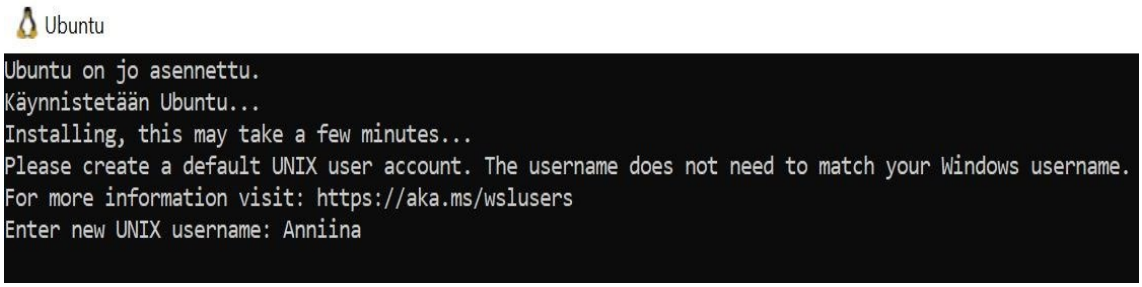
```
wsl --install
```

Annetun komennon jälkeen käynnistyi välittömästi WSL:n suorittamiseen tarvittavien ominaisuuksien sekä oletuksena Linux-pohjaisen Ubuntu-käyttöjärjestelmän lataus. Tietokone käynnistettiin uudelleen, kun Ubuntun lataus oli suoritettu. Ensimmäisellä käynnistyskerralla asennuksen jälkeen tietokoneen käynnistyminen kesti jonkin aikaa, koska asennetun Linux-jakelun tiedostoja purettiin ja tallennettiin sekä jakelu varsinaisesti asentui.



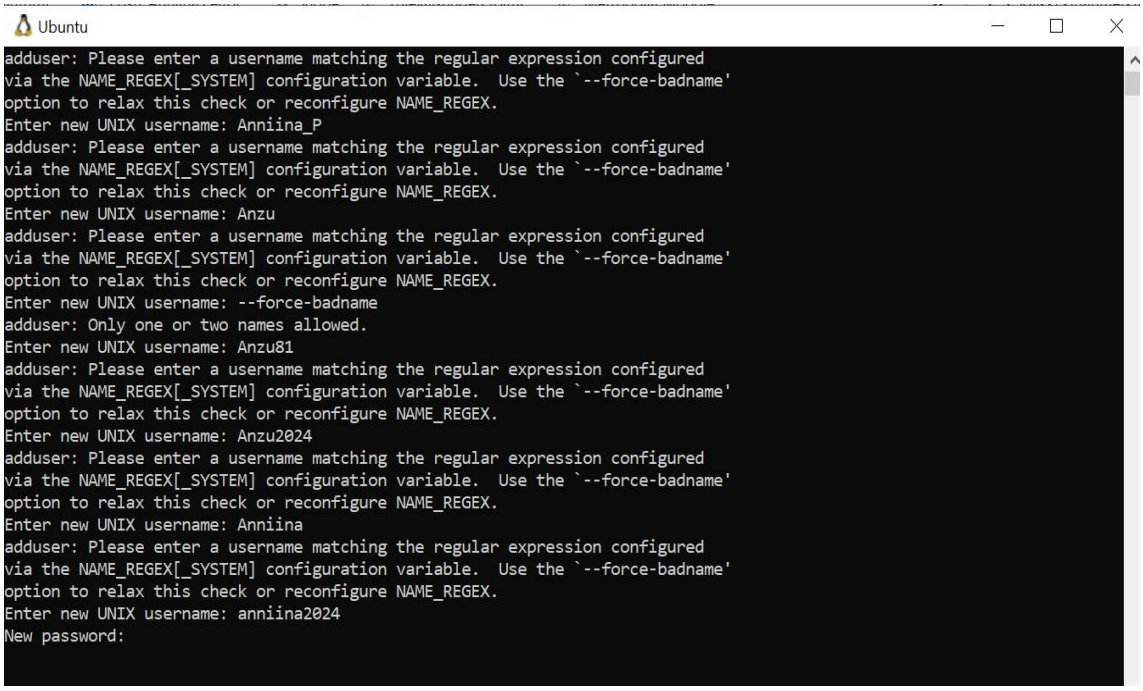
Kuva 7. Komentorivillä WSL:n asennus.

Tietokoneen uudelleenkäynnistyksen jälkeen komentorivi avautui. Linux-version tunnisti vasemmalle ylös ilmestyneestä pingviini-ikonista ja Ubuntu-nimestä. Järjestelmä pyysi valitsemaan UNIX-käyttäjänimen (kuva 8). Linux on tehty monen käyttäjän järjestelmäksi. Kaikilla käyttäjillä tulee olla alusta alkaen oma käyttäjätunnus, salasana ja kotihakemisto.



Kuva 8. Komentorivillä UNIX-käyttäjänimen valinta.

Kaikki käyttäjänimiehdotukset eivät olleet kelvollisia, jolloin saatiin kuvassa 9 näkyviä virheilmoituksia. Sopivan käyttäjänimen löydyttyä järjestelmä pyysi luomaan UNIX-salasanan. (Kuva 9.) Käyttäjätunnuksen ja salasanan luomisen jälkeen Ubuntu-järjestelmä oli valmis käytettäväksi.



Kuva 9. Komentorivillä virheilmoituksia käyttäjänimen valinnasta.

Ubuntu-järjestelmää voidaan ohjata komentoriviltä tai graafisen käyttöliittymän avulla. Komentorivillä Linux-järjestelmässä järjestelmävalvojan tilassa toimittaessa pitää komentoon lisätä teksti `sudo`. Turvallisuuden parantamiseksi kyseinen teksti vaaditaan kaikkiin järjestelmävalvojan käyttöä vaativiin toimintoihin. Jos toimitaan peruskäyttäjänä eikä ylläpidetä Linux-järjestelmää, `sudo`-tekstiä ei tarvita. `Sudo`-teksti komennon alussa antaa tilapäisesti käyttäjälle mahdollisimman laajat käyttöoikeudet. (Ikonen ym. 2015: 40.) Ubuntu-jakelu löytyy asennuksen jälkeen yleensä suoraan käynnistysvalikosta.

3 Network Mapper (Nmap)

Network Mapper (Nmap) on avoimen lähdekoodin verkkoskanneri, jolla on miljoonia käyttäjiä ympäri maailman. Nmap on ollut esillä tietokonemaailmaan sijoittuvissa elokuvissakin, kuten The Matrix Reloaded -elokuvassa. Nmap on ilmainen ohjelma, ja sitä voidaan käyttää useilla alustoilla, kuten Unix-, Windows- ja Mac OS -järjestelmissä. Nmap-työkalua voidaan käyttää myös graafisella käyttöliittymällä, Zenmap. (Lyon 2008: xxi.)

Nmap on tehokas työkalu ja suunniteltu skannaamaan suuria verkkoja nopealla tahdilla. Nmapia voidaan käyttää verkon tutkimiseen sekä tietoturvan tarkastamiseen. Sitä käytetään hyödyksi myös esimerkiksi verkon inventoinneissa, päivitysaikataulujen ylläpidossa ja palvelujen käytettävyyden valvonnassa. Nmap käyttää hyödyksi raakoja IP-paketteja, joiden avulla se saa selville kohdeverkosta mitä sovelluksia ja käyttöjärjestelmiä on käytössä tai millaisia pakettisuodattimia tai palomuureja käytetään. (Lyon 2008: xxi.)

Alkujaan Gordon Lyon julkaisi kehittämänsä Nmapin vuonna 1997, koska halusi tarjota tehokkaan ja yhden käyttöliittymän takana olevan joustavan toteutuksen monille erillisille porttiskannereille. Nykypäivänä siihen on lisätty paljon uusia ja erilaisia toiminnallisuuksia, kuten esimerkiksi etäkäyttöjärjestelmän tunnistus, IP ID -lepotilaskannaus ja nopea moniantenninen ping-skannaus. (Lyon 2008: xxi.)

Tietoliikenteen perustan muodostaa IP-protokolla. Sen päälle rakennetaan muut protokollat, joista yleisimpinä ovat TCP (Transmission Control Protocol) ja UDP (User Datagram Protocol). Yhteen rakentuneena IP:n kanssa niistä käytetään nimityksiä TCP/IP ja UDP/IP. TCP on yhteyssuuntautunut protokolla. Se muodostaa ja ylläpitää yhteyttä vastaanottajan ja lähettäjän välillä. TCP on luotettava protokolla, jolla tieto saapuu perille samanlaisena kuin se on lähtenyt. UDP on yhteydetön protokolla, jolla tiedonsiirto on nopeaa ja yksinkertaista, mutta tieto ei välttämättä siirtyessään pysy samanlaisena. (Williams 2024a.)

Tietoliikenneportit ovat verkossa olevia osoitteita tiettyihin palveluihin tai sovelluksiin. Portti ohjaa osoitteeseen tulevaa ja lähtevää tietoliikennettä. Portit ovat

numeroituna välille 0–65535 (Lyon 2008:4). Porttiskannaus on yksi Nmapin perustoiminnoista ja tapahtuu yleensä oletuksena, mutta se on myös ohitettavissa. Nmapin lähettämien pakettien ja niihin saatujen vastausten tai vastaamattomuuden avulla selvitetään kohdeverkossa olevien porttien tila. (Lyon 2008: 383–384.)

Porttiskannauksessa UDP- ja TCP-protokollaan perustuvat palvelut eroavat toisistaan. TCP-paketin vastaanotto kuitataan, ja jos kuittaus jää puuttumaan, se lähetetään uudelleen. UDP-paketteja ei kuitata vastaanotetuiksi. UDP-palveluiden porttiskannaus on näin ollen vaikeampaa. Vastausta skannaukseen ei siis välttämättä saada, vaikka portti olisi avoimena. (Salmi 2021: 23–26.)

Lähtökohtaisesti yhtä menetelmää voidaan käyttää skannauksessa kerrallaan, mutta UDP-skannaus (-sU) voidaan yhdistää mihin tahansa TCP-skannaustyyppiin. Nmapissa skannausmenetelmiä ovat esimerkiksi -sS (TCP SYN -skannaus), -sT (TCP Connect -skannaus) ja -sU (UDP-skannaus). (Lyon 2008: 385.)

Oletuksena Nmap suorittaa SYN-skannauksen (-sS), jossa tuhansia portteja skannataan hyvin nopeasti. SYN-skannauksella on mahdollista erotella luotettavasti porttien tiloja. SYN-skannauksessa ei avata täydellistä TCP-yhteyttä, joten se on melko huomaamaton. Jos käyttäjällä ei ole järjestelmävalvojan oikeuksia suorittaa skannausta, SYN-skannauksen tilalla tehdään Connect-skannaus (-sT). Connect-skannaus on tehottomampi kuin SYN-skannaus. Siinä hyödynnetään järjestelmäkutsuja, jotka muodostavat yhteyden avoimeen porttiin, toisin kuin SYN-skannauksessa. Connect-skannaus vie enemmän aikaa, ja se myös havaitaan todennäköisemmin kohteessa. (Lyon 2008: 385–386.)

Kaikilla Nmapin porttiskannausmenetelmillä voidaan määrittää, mitkä portit halutaan skannata ja onko järjestys satunnainen vai peräkkäinen. Oletuksena Nmap skannaa portit 1024:ään asti sekä tästä korkeammat, jotka on listattu skannattavalle protokollalle. (Lyon 2008: 389.)

Porttialueiden määrittelyllä (-p-) skannataan vain tietyt portit ja oletusarvo korvaantuu. Porttinumerot voidaan tällöin määrittää yksittäin tai eroteltuna alue väliviivalla, esimerkiksi 1–1023. (Lyon 2008: 389.)

Eri skannaustyypeillä saadaan tulokseksi hieman eri tavalla määriteltyjä porttien tiloja. Portit luokitellaan pääsääntöisesti avoimiin (*open*), suljettuihin (*closed*) ja suodatettuihin (*filtered*). Lisäksi Nmapin eri skannaustekniikoilla voidaan portteja luokitella myös seuraavasti: suodattamaton (*unfiltered*), avoin/suodatettu (*open/filtered*) sekä suljettu/suodatettu (*closed/filtered*). (Lyon 2008: 383–384.)

Avoin portti: Kohdeverkko hyväksyy aktiivisia TCP / UDP-yhteyksiä ja vastaa kutsuihin eli kuuntelee koko ajan verkon liikennettä. Avoimien porttien löytyminen on yleensä porttiskannauksessa tavoite, koska ne mahdollistavat murtautumisen kohdeverkkoon. Avoimia portteja voidaan suojata ulkopuolisilta tahoilta esimerkiksi palomuureilla, jolloin ei rajoiteta kohdeverkkoa luvallisesti käyttävien toimintaa. (Lyon 2008: 383–384.)

Suljettu portti: Kohdeverkko vastaanottaa pyyntöjä ja on saavutettavissa, mutta portti ei ole sillä hetkellä minkään sovelluksen käytettävissä eikä kuuntele verkon liikennettä. Suljetut portit saattavatkin seuraavalla porttiskannauskerralla olla aukinaisia. (Lyon 2008: 383–384.)

Suodatettu portti: Kohdeverkko ei vastaanota mitään eikä kuuntele verkon liikennettä. Portista ei skannauksella tunnisteta, onko se auki vai kiinni, koska se on suodatettuna. Suodatus estää tiedon kulkua. Se voidaan tehdä esimerkiksi palomuurin avulla. (Lyon 2008: 383–384.)

Suodattamaton portti: Perusskannauksella tunnistetaan, että portti on käytettävissä, mutta ei pystytä määrittelemään, onko portti suljettu vai avoin. (Lyon 2008: 383–384.)

Avoin/suodatettu: Perusskannauksella ei pystyä määrittämään, onko portti avoin vai suodatettu. Portti on skannauksen mukaan avoin, mutta siltä ei saada vastausta. (Lyon 2008: 383–384.)

Suljettu/suodatettu: Portista ei skannauksella pystytä määrittelemään, onko se suljettu vai suodatettu. (Lyon 2008: 383–384.)

Nmap-työkalulla voidaan tehdä paljon muitakin verkkoskannauksia kuin porttiskannauksia. Esimerkiksi version tunnistusta (-sV), käyttöjärjestelmän tunnistusta (-O), verkkoreittien etsintää (--traceroute) tai skriptausten skannausta (--script tai -sC). (Lyon 2008:13.)

Version tunnistuksessa Nmap yrittää auki olevista porteista tunnistaa, mitä palvelinohjelmistoa kohdejärjestelmässä käytetään. Käyttöjärjestelmän tunnistuksessa Nmap selvittää verkkostandardien eroja mittaamalla, mikä käyttöjärjestelmä kohdekoneessa on käynnissä. Erilaiset käyttöjärjestelmät toteuttavat verkkostandardeja eri tavalla. Verkkoreittien etsinnässä Nmap etsii verkkoreittejä isäntäkohteisiin. Skriptausten skannauksessa Nmap käyttää erityistä, verkon tiedonkeräämistä varten olevaa, skriptikokoelmaa saadakseen lisätietoa kohdejärjestelmistä. (Lyon 2008:13.)

Nmap-työkalun ei ole tarkoitus kaataa kohdeverkkoja, ja se esimerkiksi hidastaa toimintaansa, jotta ylikuormittumista ei tapahtuisi. Nmap lähettää aina IP-, TCP- ja UDP-otsikoilla asianmukaisia paketteja, mutta ne saattavat tulla vastaanottajalle yllättäen. Jos Nmapin skannauksen seurauksena kohdejärjestelmä kaatuu, on virhe yleensä kohdejärjestelmässä. Kaatunut järjestelmä on todennäköisesti ollut jo aiemmin epävakaa ja korjauksen tarpeessa. (Lyon 2008:19.)

4 Kali Linux

4.1 Esittelyssä Kali Linux

Kali Linux on Yhdysvaltalaisen Offensive Security Ltd:n kehittämä avoimen lähdekoodin Linux-jakelu. Kali pohjautuu suosittuun Linuxin Debian-jakeluun, kuten aiemmin käsitelty Ubuntu. Kali Linux on alun perin nimeltään BackTrack Linux. (Offensive Security Ltd. 2013.) BackTrack oli tietoturvaan keskittyvä käyttöjärjestelmä. Offensive Securityn Mati Aharoni ja Devon Kearns kehittivät järjestelmää ja kirjoittivat sen uudelleen, jolloin nimeksi tuli Kali Linux. Kali Linuxin ensimmäinen versio oli Kali 1.0.0. Versio julkaistiin maaliskuussa 2013. (Williams 2024b.) Kalin viralliselta sivustolta, *www.kali.org*, on saatavilla paljon lisätietoa jakelusta (Kali Linux 2024).

Kali Linuxin painopiste on tunkeutumistestauksessa ja tietoturva-auditoinneissa. Se on räätälöity erityisesti tietoturvatestaajille ja muille tietoturva-ammattilaisille. (Hertzog ym. 2017: 5.) Kali Linux on ainutlaatuinen alusta, koska sitä voidaan käyttää sekä tietoturvaloukkausten tekemiseen että estämiseen. Kali Linuxiin on esiasennettu valtava määrä työkaluja, jotka tekevät siitä monikäyttöisen alustan. (Williams 2024b.)

Kali Linuxin erilaisia verkkotyökaluja voidaan hyödyntää erityisesti tietoturvatestauksissa ja tutkimuksissa, kuten penetraatiotestauksessa ja digitaalisessa rikostutkinnassa. Kali Linux -alustalla toimivat esimerkiksi ohjelmat: Nmap, Hydra, Maltego, Responder, Sqlmap ja Wireshark. (Kali Linux 2024.)

Kali Linux on rolling-jakelu eli jatkuvasti päivittyvä jakelu. Saatavilla olevat työkalut on luokiteltu selkeästi toimintojen mukaan. Valikoista löytyy työkaluja esimerkiksi haavoittuvuusanalyysin, tietokanta-arviointiin, salasanahyökkäyksiin, langattomiin hyökkäyksiin sekä erilaisia raportointityökaluja. (Hertzog ym. 2017: 3–11.)

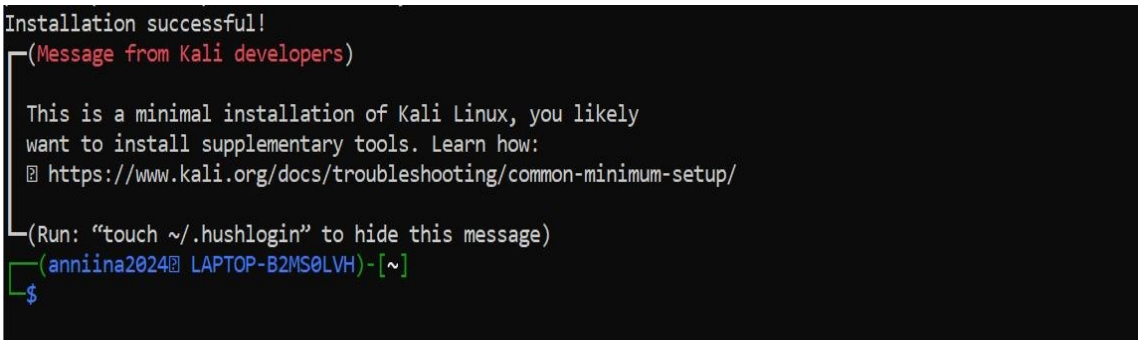
4.2 Kali Linuxin asennus

Kali Linux on saatavilla Windowsille esimerkiksi Microsoft Storesta virallisena WSL-jakeluna. Windows 10 -järjestelmän käyttäjät voivat ensin ottaa käyttöönsä WSL:n ja hakea sen jälkeen Microsoft Storesta Kalin. Asennus on helppoa ja yksinkertaista. (Offensive Security Ltd. 2018.)

Kali Linux -jakelussa voidaan käyttää monenlaisia työkaluja. Microsoft Storesta ladattava perusversio sisältää Kali Linux -alustan. Työkalut on ladattava erikseen komentorivin tai paketinhallintaohjelman avulla.

Microsoft Store löytyy yleensä Windowsista suoraan käynnistysvalikosta. Microsoft Storessa olevan hakukentän avulla voi helposti hakea ladattavissa olevia ohjelmia, kuten Kali Linuxin.

Kali Linux -jakelu ladattiin ja asennettiin suoraan Microsoft Storesta. Kali Linuxin asennuksen jälkeen luotiin jälleen UNIX-käyttäjätunnus ja -salasana, kuten Ubuntu-jakelussa. Kali Linuxin asennus oli valmis, kun sopiva käyttäjätunnus ja salasana oli luotu (kuva 10).

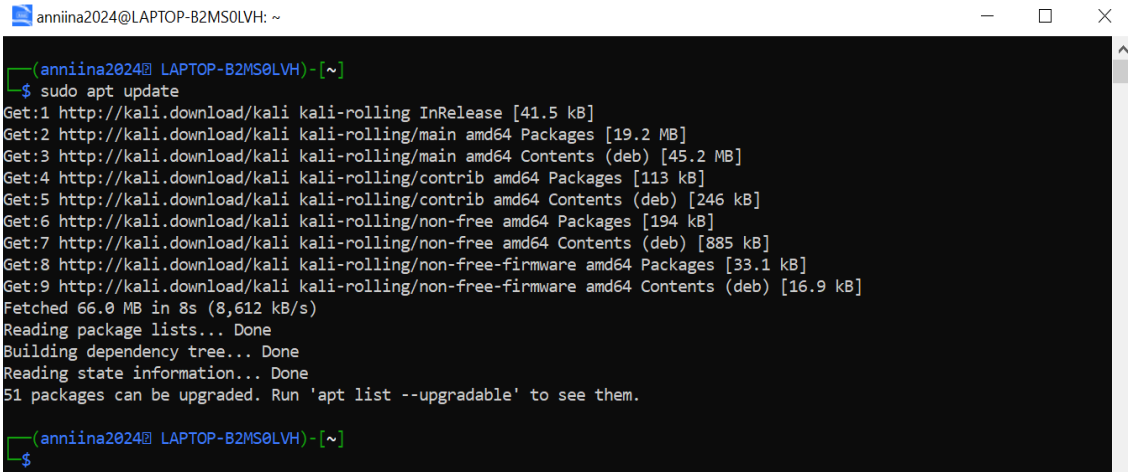


Kuva 10. Kali Linux -järjestelmän asennus valmis.

Kali Linux löytyi asennuksen jälkeen tietokoneen ohjelmavalikosta. Tämän jälkeen Kali Linux -jakeluun asennettiin ohjelmat ja sovellukset erillisten komentojen kautta. Ennen asennusta oli hyvä päivittää järjestelmäpakettien tiedot, jotta varmasti asennettiin uusimpia versioita (kuva 11).

Päivitys tehtiin komennolla:

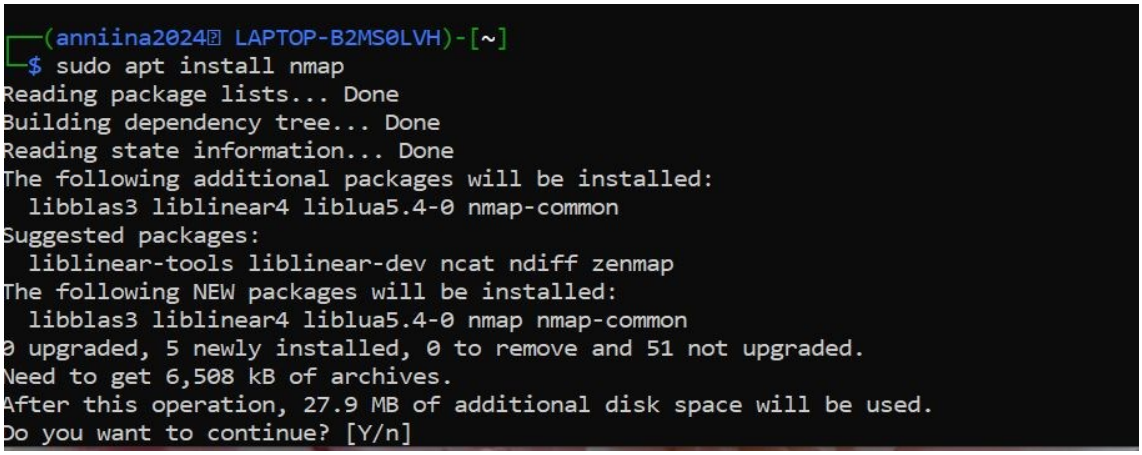
```
sudo apt update
```



Kuva 11. Komentorivillä Kali Linuxin järjestelmäpakettien päivitystä.

Kali Linux -jakeluun asennettiin Nmap, koska tarkoitus oli testata kyseistä verkkoskannaustyökalua. Kuvassa 12 asennettiin Nmap-työkalu Kali Linuxin komentorivillä komennolla:

```
sudo apt install nmap
```



Kuva 12. Komentorivillä Nmap-työkalun asennus Kali Linuxiin.

Asennuksen jälkeen tarkistettiin asennetun Nmap-version numero (kuva 13). Tämä tehtiin komennolla:

```
nmap --version
```

Kuva 13. Komentorivillä Nmap-version tarkistaminen.

4.3 Python-Nmap

Python on olio-ohjelmointikieli, jossa on selkeä ja yksinkertainen syntaksi. Python-kielellä on monipuolisia ominaisuuksia. Python-kieltä opitaan yleensä helposti, ja se soveltuu hyvin ensimmäiseksi ohjelmointikieleksi. Tietoliikenne- ja ylläpitosovelluksissa Python on paljon käytetty kieli. Python-kirjastot laajentavat sen ominaisuuksia ja lisäävät käyttötarkoituksia. Python-tulkki on vapaasti ladattavissa osoitteesta *www.python.org*. Tulkki on saatavissa kaikille yleisille käyttöjärjestelmille. (Rasila 2004:14.)

Python-kielellä on paljon erilaisia avoimen lähdekoodin kirjastoja, jotka laajentavat sen käyttämisen lähes kaikkeen. Tämä on kasvattanut Pythonin suosiota. Pythonin yksinkertainen syntaksi nopeuttaa sovellusten kehittämisessä. Python-kieli on integroitavissa eri ohjelmointikielille pohjautuviin järjestelmiin. (McFarland 2024.)

Python-Nmap on Python-kirjasto, jonka avulla voidaan käyttää Nmap-verkkoskanneria Python-ohjelmointikieltä hyödyntäen. Nmap on kirjoitettu alun perin C- ja LUA-ohjelmointikielille, mutta se voidaan integroida myös Python-kielelle. Python-kirjasto tukee Nmap-skriptien tulosteita. Tämä helpottaa Nmapin skannaustulosten käsittelyä sekä auttaa automatisoimaan skannausta ja raportointia. (PyPI 2024.)

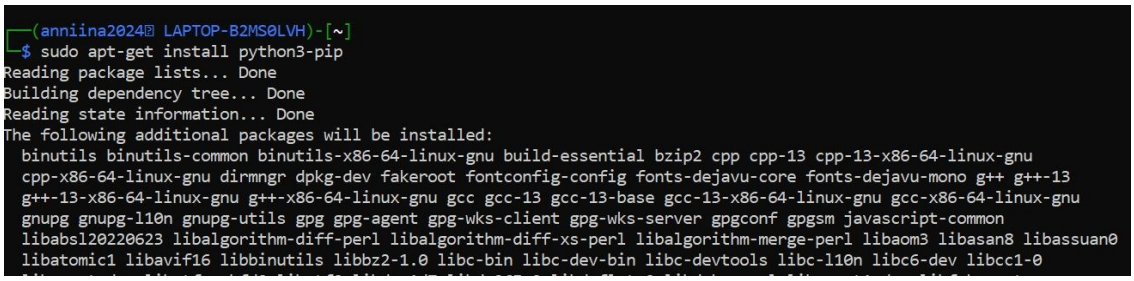
Python-Nmap on laajennus Nmap-verkkoskanneriin, joten Nmap-työkalu täytyy olla ensin asennettuna järjestelmään. Linux-jakeluista esimerkiksi Kali Linux mahdollistaa Nmapin käytön. Python-Nmapin viimeisin versio ja lataustiedostot löytyvät viralliselta Python-sivustolta, *pypi.org*. Sivustolta löytyvät myös ohjeistukset laajennusten latauksiin. (PyPI 2024.)

Python-Nmap asennetaan verkkosivuilta ladattavan tiedoston avulla tai paketinhallintaohjelmalla. Tässä harjoituksessa Python-Nmap-laajennin asennettiin paketinhallintaohjelma Pip3:n avulla. Pip3 on Python3:n virallinen paketinhallintaohjelma, jota ohjataan komennolla: `pip3`. Pip3:n avulla pystytään hallitsemaan ja asentamaan ohjelmistopaketteja, joita ei valmiiksi ole Pythonin standardikirjastossa. (Suhani 2021.) Ensin varmistettiin, että Kali Linuxissa on viimeisin Python3-versio komennolla:

```
sudo apt-get install python3
```

Tämän jälkeen asennettiin paketinhallintaohjelma Pip3 komennolla (kuva 14):

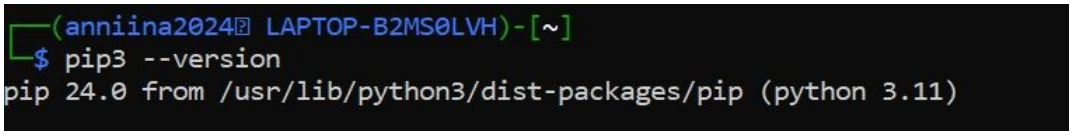
```
sudo apt-get install python3-pip
```



Kuva 14. Komentorivillä Pip3-paketinhallintaohjelman asennus.

Asennuksen jälkeen Pip3-versio tarkistettiin komennolla (kuva 15):

```
pip3 --version
```



Kuva 15. Komentorivillä Pip3-version tarkistaminen.

Kuvassa 16 Python-Nmap-laajentimen asennus Kali Linuxin komentorivillä. Python-Nmap asennettiin Pip3:n avulla komennolla:

```
pip3 install python-nmap
```

Kuva 16. Python-Nmap-laajentimen asennus Kali Linuxiin Pip3:n avulla.

Ohjelmien ja Python-laajentimen asennusten jälkeen Kali Linux -jakelussa voitiin suorittaa Python-koodilla Nmap-verkkoskannausta. Tämän jälkeen testattiin Nmapia sekä Python-Nmap-laajenninta Python-kielellä kirjoitetulla koodilla. Ennen lähdekoodin kirjoittamista on hyvä varmistaa, että käytettävissä on Pythonille sopiva tekstieditori. Tässä työssä käytettiin Visual Studio Code -tekstieditoria, joka on Microsoftin oma tuote. Ohjelma on ilmainen ja asennettavissa koneelle helposti Microsoft Storesta.

5 Nmapin testaus Python-laajentimella

Insinöörityössä kehitettiin harjoitus, jossa lopuksi testattiin Nmap-verkkoskannausta Python-kielellä kirjoitetulla lähdekoodilla. Verkkoskannaukset kohdistettiin sivustolle *http://scanme.Nmap.org/*, joka on luotu Nmap-työkalulle skannauksen harjoittelua varten. Näin toimittiin eettisesti oikealla tavalla, koska verkkoskannausta saa tehdä vain sivustoille, joihin on skannauslupa.

Lähdekoodi kirjoitettiin Python-kielelle sopivalla tekstieditorilla. Lähdekoodissa määriteltiin Nmap-työkalun verkkoskannausmenetelmät ja mihin skannaus kohdistettiin. Tässä työssä suoritettiin kaksi testiskannausta Nmap-työkalulla. Kummassakin skannaustestissä käytetyn Python-koodin kehittämisessä hyödynnettiin tekoälysovellusta (ChatGPT 2024).

Python-lähdekoodi tallennettiin tekstieditorilla Python-tiedostomuotoon (kuva 17). Tässä ensimmäisessä testissä tiedosto tallennettiin nimellä *Harjoitus*. Python-tiedoston tunnistaa päätteestä *.py*. Tämän jälkeen käynnistettiin Kali Linux-jakelun komentorivi.

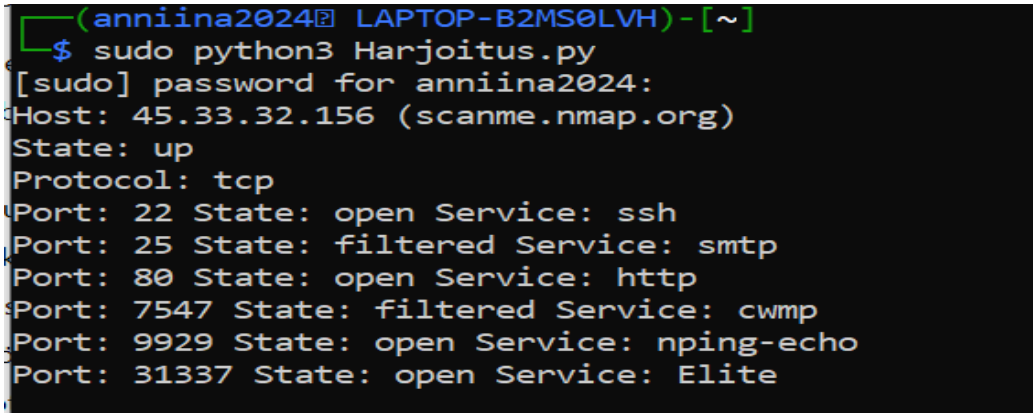
Kuva 17. Ensimmäisen skannaustestin lähdekoodi tekstieditorissa (ChatGPT 2024).

Tämän jälkeen käynnistettiin ensimmäinen testi, jossa suoritettiin Nmap-porttiskannaus. Python-tiedosto ajettiin Python-tulkin avulla Kali Linux-jakelussa. Python-tulkkiin oli aiemmin haettu laajennuksena Python-Nmap. Tietyissä skannausmenetelmissä komentorivillä pitää olla järjestelmävalvojan roolissa, jolloin komentoihin lisättiin alkuun teksti `sudo`.

Komentorivillä oli Python-tulkin käynnistyskomento sekä määriteltynä kohteena oleva Python-tiedosto. Kirjoitusasun täytyy olla täsmälleen sama kuin tallennuksessa, jotta tiedosto löytyy. Tiedoston tulee sijaita myös samassa hakemistossa, jossa ohjelmaa ajetaan. Yleensä se on Linux-järjestelmässä käyttäjän oma kotihakemisto. Ensimmäinen skannaustesti käynnistettiin komennolla (kuva 18):

```
sudo python3 Harjoitus.py
```

Ensimmäisessä testissä Nmap-työkalulla porttiskannattiin kaikki portit väliltä 1–65535. Tulokseksi saatiin listaus löydetyistä porteista sekä niiden tiloista. Kuvassa 18 on Nmap-porttiskannauksen tulos Kali Linuxin komentorivillä.



Kuva 18. Komentorivillä Nmap-skannauksen käynnistys ja ensimmäisen testin tulos.

Portit voivat olla avoimia (*open*), suljettuja (*closed*) tai suodatettuja (*filtered*). Skannaustuloksen perusteella kohdeverkosta löydettiin neljä avointa porttia: 22, 80, 9929 ja 31337 sekä kaksi suodatettua porttia: 25 ja 7547. Lisäksi porttien kohdalta tunnistettiin useita erilaisia palveluita.

Portti 22: palveluna oli SSH (*Secure Shell*) etäyhteyksiä varten. Portti oli avoinna, joten palvelin salli etäyhteydet Secure Shell -protokollan kautta.

Portti 25: palveluna oli SMTP (*Simple Mail Transfer Protocol*), jota käytetään sähköpostin lähetykseen. Portti oli suodatettuna, jolloin sähköpostin lähetysprotokolla oli käytössä ja tietoliikenne suojattiin esimerkiksi palomuurilla.

Portti 80: palveluna oli HTTP (*Hypertext Transfer Protocol*), jota käytetään web-palveluihin. Portti oli avoinna, joten web-palvelua käytettiin.

Portti 7547: palveluna oli CWMP (*CPE WAN Management Protocol*), jota käytetään laitteiden hallintaan. Portti oli suodatettu, jolloin laitteiden hallintaprotokollaa käytettiin, mutta liikennettä suodatettiin.

Portti 9929: palveluna oli Nping-echo, joka on Nmapin oma testipalvelu. Portti oli avoinna eli testipalvelua käytettiin.

Portti 31337: palveluna oli *Elite*, joka viittaa esimerkiksi testipalveluihin. Portti oli avoinna eli palvelua käytettiin.

Porttiskannauksella saatiin myös tietoja isännästä. Isäntä oli *scanme.nmap.org* ja IP-osoite 45.33.32.156. Tila (*state*) oli *up* eli kohde oli aktiivinen ja vastasi pyyntöihin. Protokollana oli TCP.

Toisessa skannaustestissä Nmap-työkalulla käytettiin erilaisia skannausmenetelmiä. Testin lähdekoodiin muutettiin skannausmenetelmiksi: *-O* (käyttöjärjestelmän tunnistus), *-sV* (version tunnistus), *-sC* (skriptiskannaus) ja *--traceroute* (verkkoreittien etsintä) (Lyon 2008: 13). Toisen skannaustestin lähdekoodi tallennettiin tiedostonimellä *Harjoitus_II*. Kuvassa 19 on toisen skannaustestin lähdekoodi tekstieditorissa.

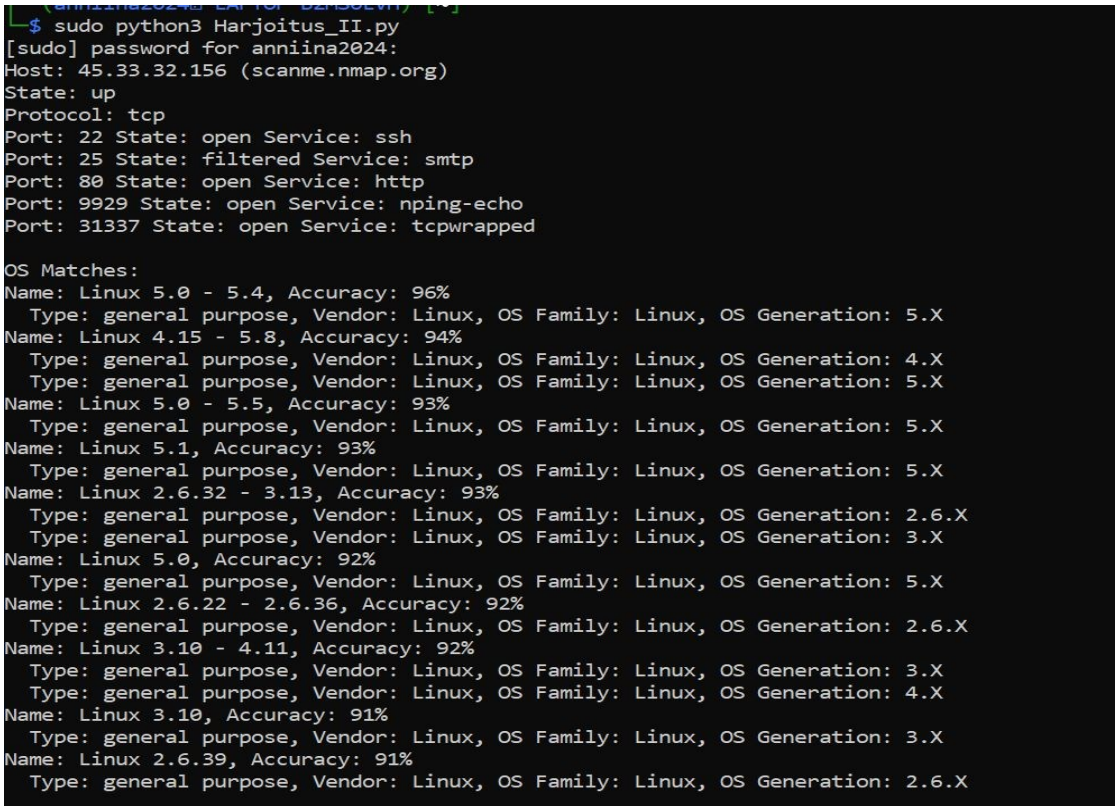
```
C: > Users > s2ape > Harjoitus_II.py > ...
import nmap

def nmap_scan(target_host):
    # Luodaan uusi muuttuja PortScanner-luokkaan
    nm = nmap.PortScanner()

    try:
        # Suoritetaan skannaus lisäargumenteilla
        nm.scan(target_host, arguments='-O -sV -sC --traceroute')

        # Tulostetaan skannauksen tulokset
        for host in nm.all_hosts():
            print("Host: %s (%s)" % (host, nm[host].hostname()))
            print("State:", nm[host].state())
            for proto in nm[host].all_protocols():
                print("Protocol:", proto)
                port_info = nm[host][proto]
                sorted_ports = sorted(port_info.keys())
                for port in sorted_ports:
                    print("Port:", port, "State:", port_info[port]['state'], "Service:", port_info[port]['name'])

            # Tulostetaan käyttöjärjestelmätiedot
            if 'osmatch' in nm[host]:
                print("\nOS Matches:")
                for osmatch in nm[host]['osmatch']:
                    print("Name: %s, Accuracy: %s%%" % (osmatch['name'], osmatch['accuracy']))
                    if 'osclass' in osmatch:
                        for osclass in osmatch['osclass']:
                            print("  Type: %s, Vendor: %s, OS Family: %s, OS Generation: %s" %
                                  (osclass['type'], osclass['vendor'], osclass['osfamily'], osclass['osgen']))

            # Tulostetaan skriptitulokset
            if 'hostscript' in nm[host]:
                print("\nHost Script Results:")
                for script in nm[host]['hostscript']:
                    print("Script ID: %s, Output: %s" % (script['id'], script['output']))

            # Tulostetaan traceroute-tiedot
            if 'traceroute' in nm[host]:
                print("\nTraceroute:")
                for hop in nm[host]['traceroute']['hop']:
                    print("Hop: %s, Address: %s" % (hop['ttl'], hop['ipaddr']))

    except Exception as e:
        print("An error occurred: ", e)

# Kutsutaan funktiota skannaamaan valittu kohde "scanme.nmap.org"
nmap_scan('scanme.nmap.org')
```

Kuva 19. Toisen skannaustestin lähdekoodi tekstieditorissa (ChatGPT 2024).

Toinen skannaustesti käynnistettiin komennolla:

```
sudo python3 Harjoitus_II.py
```

Kuvassa 20 on toisen verkkoskannaustestin tulos Kali Linuxin komentorivillä. Tuloksen perusteella Nmap-työkalu oli tehnyt porttien ja tilojen selvittämisen lisäksi isäntäkohteen käyttöjärjestelmän tunnistusta.



Kuva 20. Komentorivillä Nmap-skannauksen toisen testin tulos.

Nmap tunnisti kohteen mahdollisia käyttöjärjestelmävaihtoehtoja. Tunnistus ei ollut täysin tarkka, joten isännän käyttöjärjestelmän osalta määritettiin eri vaihtoehtoja sekä niiden tarkkuusprosentteja (*Accuracy*). Tuloksen perusteella suurimmalla todennäköisyydellä käyttöjärjestelmän versiona oli Linux 5.0–5.4.

Kehitetyssä harjoituksessa asennettiin Windowsiin Linux-jakelu Kali Linux sekä Kali Linuxiin työkalu Network Mapper. Kali Linuxiin asennettiin paketinhallintaohjelma ja Python-tulkin laajennus Python-Nmap, jotta Nmap-työkalua oli mahdollista ajaa Python-kielellä. Lopuksi Nmap-työkalulla tehtiin verkkoskannaustestejä. Tulosten perusteella onnistuttiin tavoitteen mukaisesti ajamaan Nmap-verkkoskanneria Python-kielellä. Kokonaisuutena saatiin kehitettyä käytännönläheinen harjoitus, jonka avulla tietoturvakurssin opiskelijat voivat testata Nmap-työkalun käyttöä Python-laajentimella Kali Linux -jakelussa. Lisäksi harjoituksessa tulee kokeiltua Linux-järjestelmän käyttöä Windowsissa.

6 Yhteenveto

Insinöörityössä kehitettiin harjoitus, jossa Nmap-verkkoskannaustyökalua ajettiin Python-laajentimella Kali Linux -jakelussa. Harjoituksessa käytettiin myös Linux-järjestelmää Windowsissa.

Insinöörityö kirjoitettiin etenemään kehitetyn harjoituksen mukaisesti. Harjoituksen tehtävänanto on liitteenä. Harjoituksessa otettiin Windowsissa käyttöön alijärjestelmä WSL. Tämän avulla pystyttiin käyttämään yhtäaikaisesti Linux- ja Windows-järjestelmiä. Harjoituksessa Linux-jakeluksi Nmap-työkalulle valittiin tietoturvakurssille hyvin soveltuva Kali Linux. Kali Linux -alustalle asennettiin Nmap-työkalu verkkoskannausta varten. Nmap on suunniteltu C- ja LUA-ohjelmointikielille, joten Pythonin käytön mahdollistamiseksi Kali Linux -jakeluun haettiin Python-tulkille laajennus Python-Nmap. Lopuksi kaikkien asennettujen ohjelmien ja Python-laajentimen toimivuutta testattiin tekemällä Python-kielellä verkkoskannausta Nmap-työkalulla.

Insinöörityön tekeminen sujui hyvin ja eteni aikataulussaan. Välillä oli haasteita, mutta työn tekeminen oli erittäin palkitsevaa. Työn aikana opin paljon uusia asioita, koska esimerkiksi Linux, Kali Linux, Python-kieli ja Nmap eivät olleet ennestään tuttuja. Työn edetessä opin ymmärtämään paremmin Linuxin ja Windowsin eroja ja mahdollisuuksia. Erityisesti Linux-käyttöjärjestelmä yllätti positiivisesti ja siihen oli mielenkiintoista perehtyä. Linuxin käyttäminen onnistui hyvin, vaikka graafista käyttöliittymää ei ollutkaan käytössä.

Työn luotettavuutta lisättiin käyttämällä aineistona mahdollisimman uutta ja ajankohtaista tietoa. Verkosta löydettyjä lähteitä arviointiin kriittisesti. Kaikkiin käytettyihin lähteisiin viitattiin asianmukaisesti. Työn luotettavuutta lisättiin myös kirjoittamalla mahdollisimman yksityiskohtaisesti työn eri vaiheista sekä käyttämällä paljon havainnollistavia kuvia. Työn luotettavuutta saattaa heikentää englanninkielisten lähteiden suuri osuus. Aineistoa jouduttiin kääntämään paljon ja käännösvirheitä on voinut tulla.

Työssä tehtiin harjoituksena verkkoskannausta, jossa toimittiin eettisesti oikealla tavalla. Kohdeverkkona käytettiin harjoitteluun tarkoitettua sivustoa, johon on lupa kohdistaa verkkoskannausta. Työssä tehdyt ohjeistukset on tarkoitettu vain harjoituskäyttöön. Kehitetyn harjoituksen tehtävänannossa muistutettiin, että verkkoskannausta saa tehdä vain luvallisiin kohteisiin.

Tietoturvaan liittyvät asiat ovat kiinnostavia ja tänä päivänä hyvinkin ajankohtaisia. Perehtyminen Nmap-verkkoskannerin laajoihin toimintamahdollisuuksiin oli antoisaa ja mielenkiintoista. Pohdin työn aikana paljon sitä, kuinka helposti verkosta on saatavilla erilaisia työkaluja, jos haluaa aiheuttaa toiselle harmia ja vahinkoa. Tietomurtouutisia kuulemme Suomestakin valitettavasti lähes viikoittain. Nmap-verkkoskanneria voidaan hyödyntää tietoturvan parantamiseen. Sen avulla voidaan esimerkiksi säännöllisesti etsiä tietoturva-aukkoja. Tällöin niitä ehditään korjata ennen kuin tiedot joutuvat vääriin käsiin.

Tässä insinöörityössä kehitettyä harjoitusta voisi tulevaisuudessa kehittää ja testata vaativampia Nmapin skannausmenetelmiä. Nmapin käyttöä voisi testata myös muilla Linux-jakeluilla. Mielenkiintoista olisi myös kehittää opiskelijoille harjoituksia, joissa vertaillaan Nmapin käyttämistä hyödyntäen sekä komentoriviä että graafista käyttöliittymää, Zenmap. Tässä työssä rajattiin pois Nmapin käyttö graafisen käyttöliittymän avulla. Tulosten laajemmasta tulkinnasta saisi kurssille myös lisää hyviä harjoituksia.

Insinöörityö toteutettiin suunnitellusti. Insinöörityön tuloksena kehitettiin käytännönläheinen harjoitus tietoturvakurssin opiskelijoille, jotka perehtyvät Nmap-verkkoskannerin toimintaan. Kehitetyssä harjoituksessa opiskelijat käyttävät Linux-järjestelmää Windowsissa sekä testaavat Nmap-työkalun käyttöä Python-laajentimella Kali Linux -jakelussa.

Lähteet

Awan, Muhammad & Khan, Kashaf. 2022. Linux vs. Windows: A Comparison of Two Widely Used Platforms. Journal of Computer Science and Technology Studies. Research article. Al-kindi center for research and development. 4(1): 41-54. <https://al-kindipublisher.com/index.php/jcsts/article/view/2763> Luettu 15.5.2024.

ChatGPT. 2024. Versio ChatGPT-3.5 Suomi. Hyödynnetty esimerkkikoodien tekemisessä Python-kielellä. <https://chatgpt.com/> Luettu 14.5.2024.

Hertzog, Raphael; O'Gorman, Jim & Aharoni, Mati. 2017. Kali Linux revealed. Mastering the Penetration Testing Distribution. E-kirja. <https://archive.org/details/KaliLinuxRevealed1stEdition/mode/2up?view=theater&q=kali.org>.Luettu 20.5.2024.

Ikonen, Annika; Hynninen Timo & Vanhala, Erno. 2015. Terminaali tutuksi, Linux ja komentorivin hallinta. Lappeenrannan teknillinen yliopisto. <https://lutpub.lut.fi/bitstream/handle/10024/104311/Linux-opas.pdf?sequence=2 > Luettu 15.5.24.

Kali Linux. 2024. Kali Linux, The most advanced Penetration Testing Distribution. Verkkoaineisto. <https://www.kali.org/>. Luettu 28.4.24.

Kyberturvallisuuskeskus. 2024. Tietomurrot - mitä ne ovat? Verkkoaineisto. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietomurrot-mita-ne-ovat>.13.5.2024. Luettu 20.5.2024.

Lyon, Gordon. 2008. Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning. E-kirja. Insecure.Com LLC, United States. Luettu 26.4.24.

McFarland, Alex. 2024. Pythonin kirjastot. 10 parasta Python-kirjastoa syvään oppimiseen. Unite.Ai. <https://www.unite.ai/fi/10-parasta-python-kirjastoa-syv%C3%A4%C3%A4n-oppimiseen/> 16.1.2024. Luettu 21.5.2024.

Microsoft. 2023a. How to install Linux on Windows with WSL. Verkkoaineisto. <https://learn.microsoft.com/en-us/windows/wsl/install>. 28.8.2023. Luettu 25.4.2024.

Microsoft. 2023b. What is the Windows Subsystem for Linux? Verkkoaineisto. <https://learn.microsoft.com/en-us/windows/wsl/about#what-is-wsl-2>. 29.22.2023. Luettu 25.4.24.

Microsoft. 2023c.Comparing WSL Versions. Verkkoaineisto. <https://learn.microsoft.com/en-us/windows/wsl/compare-versions.> Luettu 26.4.24.

Microsoft. 2024. Facts About Microsoft. Verkkoaineisto. < https://news.microsoft.com/facts-about-microsoft/> Luettu 25.4.24.

Negus, Christopher. 2015. Linux Bible. E-kirja. John Wiley & Sons. Incorporated. ProQuest Ebook Central.

Offensive Security Ltd. 2013. The Birth of Kali Linux. Verkkoaineisto. <https://www.kali.org/blog/kali-linux-1-0-0-release/>. Luettu 28.4.2024.

Offensive Security Ltd. 2018. Kali Linux in the Windows App Store. Verkkoaineisto. <https://www.kali.org/blog/kali-linux-in-the-windows-app-store/>. 5.3.2018. Luettu 29.4.24.

PyPI. 2024. Python-Nmap-sivusto. Verkkoaineisto. <https://pypi.org/project/python-Nmap/>. Luettu 2.5.2024.

Rasila, Antti. 2004. Ohjelmoinnin alkeita Python-kielellä. Matematiikkalehti Solmu 1/2004.14–19.<https://matematiikkalehtisolmu.fi/2004/1/solmu26.pdf>.Luettu 21.5.24.

Rikoslaki. 1995. 38 luku. Tieto- ja viestintärikoksista. 21.4.1995/578. <https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001>.Luettu 16.5.2024.

Salmi, Toni. 2021. Haavoittuvuusskannaukset osana organisaation tietoturvallisuuden kehittämistä. Diplomityö. Tampereen yliopisto. Trepo-tietokanta.

StatCounter. 2024a. Frequently Asked Questions. Verkkoaineisto. <https://gs.statcounter.com/faq#methodology>. Katsottu 16.5.2024.

StatCounter. 2024b. Desktop Operating System Market Share Finland. 4.2023–4.2024. Verkkoaineisto. <https://gs.statcounter.com/os-market-share/desktop/finland>. Katsottu 16.5.2024.

StatCounter. 2024c. Desktop Operating System Market Share Worldwide. 4.2023–4.2024. Verkkoaineisto. <https://gs.statcounter.com/os-market-share/desktop/worldwide>. Katsottu 16.5.2024.

StatCounter. 2024d. Operating System Market Share Worldwide. 4.2023–4.2024. Verkkoaineisto. <https://gs.statcounter.com/os-market-share>. Katsottu 16.5.2024.

Study tonight. 2024. Using the Nmap Port Scanner with Python. Verkkoaineisto. <https://www.studytonight.com/network-programming-in-python/integrating-port-scanner-with-Nmap>. Luettu 2.5.2024.

Suhani, S. 2021. How to install and use Pip3? ActiveState Software Inc. <https://www.activestate.com/resources/quick-reads/how-to-install-and-use-pip3/>27.7.2021. Luettu 14.5.2024.

Williams, Lawrence. 2024a. Erot TCP:n ja UDP:n välillä. Verkkoaineisto. <https://www.guru99.com/fi/differences-between-tcp-and-udp.html>. 22.4.2024. Luettu 20.5.2024

Williams, Lawrence. 2024b. Kali Linux Tutorial for Beginners: What is, How to Install & Use. Verkkoaineisto. <https://www.guru99.com/kali-linuxtutorial.html.> 13.4.2024. Luettu 20.5.2024.

Liite 1. Harjoituksen tehtävänanto

Harjoitustehtävä:

Network Mapper (Nmap) -työkalun käyttö Python-laajentimella.

Testataan Nmap-verkkoskannaustyökalua Python-ohjelmointikielellä Kali Linux -jakelussa.

Tietokoneessa käyttöjärjestelmänä Windows 10 tai uudempi. Tarvittavat asennukset: WSL, Kali Linux, Nmap ja Python-Nmap. Tarvittaessa asenna paketinhallinohjelma pip3. Lisäksi tarvitset Python-kielelle sopivan tekstieditorin.

1. Asenna komentorivin avulla Windowsin alijärjestelmä WSL. Oletuksena asentuu Linux-jakelu Ubuntu.

2. Asenna Microsoft Storesta Windowsiin Kali Linux -jakelu.

3. Kali Linuxin komentorivillä asenna Kaliin Nmap-työkalu. Muista tehdä ohjelmapakettien päivitys.

4. Asenna Kalin komentorivillä Python-tulkille laajennus Python-Nmap, jotta Nmap-työkalun käyttö mahdollistuu Python-kielellä.

   Tarvittaessa asenna paketinhallintaohjelma Pip3.

5. Käytä sopivaa tekstieditoria, esimerkiksi Visual Studio Code. Kirjoita verkkoskannauksesta Python-kielellä lähdekoodi, johon voit valita halutut skannausmenetelmät.

   Verkkoskannausta saa tehdä vain luvallisiin kohteisiin. Muista kohdistaa Nmap-skannaus harjoitussivustolle: *http://scanme.Nmap.org/*.

   Tehtävänannon lopussa on esimerkkikoodi, jolla voi myös testata asennetun Nmap-työkalun toimivuutta Python-kielellä.

6. Tallenna lähdekoodi Python-tiedostona.

7. Aja Nmap-työkalua Python-kielellä Kali Linux -jakelussa.

   Käynnistä ensin Kalin komentorivillä Python-tulkki ja kirjoita komentorivikoodiin tallennettu Python-tiedosto. Tiedoston tulee sijaita samassa hakemistossa, jossa ohjelmaa ajetaan. Ohjelma suorittaa verkkoskannauksen Nmap-työkalulla lähdekoodin mukaisesti.

8. Arvioi saatuja skannaustuloksia. Voit tehdä skannauksen uudelleen toistamalla kohdat 5–8.

   Esimerkkikoodi Nmap-työkalun testaamiseen:

```
import nmap

def nmap_scan(target_host):

    # Luodaan uusi muuttuja PortScanner luokkaan
```

```
    nm = nmap.PortScanner()

    # Suoritetaan valitulle kohteelle skannaus

    nm.scan(target_host, arguments='-p 1-65535')

    # Tulostetaan lopuksi skannauksen tulos

    for host in nm.all_hosts():

        print("Host: %s (%s)" % (host, nm[host].host-
name()))

        print("State:", nm[host].state())

        for proto in nm[host].all_protocols():

            print("Protocol:", proto)

            port_info = nm[host][proto]

            sorted_ports = sorted(port_info.keys())

            for port in sorted_ports:

                print("Port:", port, "State:",
port_info[port]['state'], "Service:",
port_info[port]['name'])

# Kutsutaan funktiota skannaamaan valittu kohde
"scanme.nmap.org"

nmap_scan('scanme.nmap.org')
```

(Lähdekoodin kehittämisessä hyödynnetty ChatGPT:tä)