

# **Tietoverkkojen nykytila-analyysi**

Alexi Manninen

Opinnäytetyö  
Lokakuu 2019  
Tekniikan ala  
Insinööri (AMK), Tieto- ja viestintätekniikka  
Kyberturvallisuus

Tekijä(t) Manninen, Aleksi	Julkaisun laji Opinnäytetyö, AMK	Päivämäärä Lokakuu 2019
	Sivumäärä 59	Julkaisun kieli Suomi
		Verkojulkaisulupa myönnetty: x
Työn nimi <b>Tietoverkkojen nykytila-analyysi</b>		
Tutkinto-ohjelma Tieto- ja viestintätekniikka		
Työn ohjaaja(t) Sampo Kotikoski, Petri Mutka		
Toimeksiantaja(t) TietoAkseli Oy		
Tiivistelmä <p>TietoAkseli Oy:n vauhdikkaan kasvun mukana tulleiden jatkuvien muutosten myötä haluttiin selvittää, onko yrityksen tietoverkko edelleen konfiguroitu asianmukaisella tavalla. Verkon nykytilan selvitys pohjautui yrityksen haluun tavoitella myöhemmin tulevaisuudessa ISO 27001-standardin sertifiointivalmiutta.</p> <p>Opinnäytetyön tavoitteena oli tunnistaa ja selvittää tietoverkoista löytyvät aktiivi- ja päätelaitteet sekä verkoissa avoimena olevat yleiset palvelut, portit ja protokollat. Samalla haluttiin selvittää, löytyykö TietoAkselin tietoverkoista yleisesti tiedossa olevia haavoittuvuuksia tai päivittämättömiä päätelaitteita.</p> <p>Opinnäytetyön teknistä toteutusta varten vertailtiin kolmea eri ohjelmistoa: Nessus, OpenVAS sekä Nexpose. Ohjelmistot valittiin toimeksiantajan määrittämien tavoitteiden perusteella. Vertailusta valikoitujen ohjelmistojen avulla TietoAkselin tietoverkkoon tehtiin erilaisia portti- ja verkkoskannauksia. Skannauksia suoritettiin sekä sisä- että ulkoverkosta.</p> <p>Opinnäytetyön lopputulokseksi saatiin kattava selvitys verkon nykytilasta ja sieltä löytyvistä kehityskohteista. Toimeksiantajan asettamiin tavoitteisiin löydettiin tilanteeseen sopeva tekninen ratkaisu, jota oli mahdollista hyödyntää myös myöhemmin muissa yrityksen toimipisteissä. Yrityksen tietoverkon nykytilasta saatiin tuotettua tärkeää reaaliaikaista tietoa.</p> <p>Toimeksiantajan tavoitteena on tulevaisuudessa suorittaa ISO/IEC 27001 -standardi. Opinnäytetyössä tehdyn tutkimuksen avulla toimeksiantaja sai ajantasaista tietoa yrityksen tietoverkosta sekä sen nykytilasta.</p>		
Avainsanat (asiasanat) Tietoverkot, Verkon skannaus, Porttiskannaus, Haavoittuvuus, Nessus		
Muut tiedot (Salassa pidettävät liitteet) Liitteet 4 ja 5 ovat salassa pidettäviä, ja ne on poistettu julkisesta työstä. Salassapidon perusteena on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24 §:n kohta 17: yrityksen liike- tai ammattisalaisuus. Salassapitoaika on viisi (5) vuotta. Salassapito päättyy 30.9.2024.		

Author(s) Manninen, Aleksi	Type of publication Bachelor's thesis	Date October 2019 Language of publication: Finnish
	Number of pages 59	Permission for web publication: x
Title of publication <b>Current state analysis of data networks</b>		
Degree programme Information and Communication Technology		
Supervisor(s) Kotikoski Sampo, Mutka Petri		
Assigned by TietoAkseli Oy		
Abstract  <p>TietoAkseli Oy has grown rapidly and the company has recently gone through significant changes. Due to these changes, the company wanted to investigate whether their network had been configured appropriately. The analysis of the current state of the network is based on TietoAkseli Oy's objective to reach the ISO 27001 standard in the future.</p> <p>The aim of the thesis was to identify and detect the devices connected to the network and to identify the services, ports and protocols that are open in the network. The study also aimed to find out whether there was any known vulnerability or endpoint device that was not up to date.</p> <p>For the technical part of the thesis three programs were compared: Nessus, OpenVAS and Nexpose. The programs were chosen based on the objectives of the target company. The two programs that were chosen were used to perform several different port and network scans. The scans were performed on both internal and external networks.</p> <p>The results of the thesis make up a comprehensive report of the current state of the network. The results also include the development targets identified through the research. The objectives set by the client company were reached and technical solutions for the discovered issues were found. The company was also able to implement these solutions later at their other branch locations. This research brought to light crucial information on the current state of the network at TietoAkseli Oy.</p>		
Keywords/tags (subjects) Data Network, Network Scanning, Port Scanning, Vulnerability, Nessus		
Miscellaneous (Confidential information) Annex 4 and 5 are confidential and is removed from the published thesis. Confidentially is based on the Act on the Openness of Government Activities 621/1999 24§, subsection 17, commercial and trade secrets of a business. This document is classified as confidential until September 30 <sup>th</sup> , 2024		

## Sisältö

<b>Lyhenteet .....</b>	<b>5</b>
<b>1 Lähtökohdat .....</b>	<b>6</b>
1.1 Toimeksiantaja .....	6
1.2 Toimeksianto .....	6
1.3 Opinnäytetyön tavoitteet.....	6
<b>2 Tutkimusmenetelmät .....</b>	<b>7</b>
2.1 Kvalitatiivinen tutkimus.....	7
2.2 Kvantitatiivinen tutkimus .....	7
2.3 Työssä käytetty menetelmä .....	8
2.4 Tutkimuskysymykset .....	8
<b>3 Yleistä tietoverkoista .....</b>	<b>9</b>
3.1 Ajankohtaisuus .....	9
3.2 Lähiverkko .....	9
3.3 Verkon hallinta .....	9
3.4 Verkon topologia .....	10
3.5 Laitetyypit.....	11
3.6 Päivitysten hallinta .....	11
3.7 Haavoittuvuus .....	12
3.8 Haavoittuvuuksien hallinta.....	13
3.9 Baselineing – Verkon suorituskyvyn määrittäminen.....	14
3.10 ISO/IEC 27001:2017 -Standardi.....	14
3.11 Katakri 2015.....	15
3.12 CIS Controls – parhaat käytänteet .....	16
3.13 Portti- ja verkon skannaustekniikat.....	18
<b>4 Kohteiden selvitys .....</b>	<b>20</b>
4.1 Tavoite .....	20
4.2 Rajaus .....	21
4.3 Kohteet .....	21
4.4 Vertailuun valitut ohjelmistot .....	22

	2
4.5 Vertailu .....	24
<b>5 Nykytilan analysointi .....</b>	<b>25</b>
5.1 Tietoverkon rakenne .....	25
5.2 Kohteiden tunnistus .....	26
5.3 Tietoverkon Baseline .....	27
<b>6 Tekninen toteutus .....</b>	<b>28</b>
6.1 Yleistä .....	28
6.2 OpenVAS.....	29
6.3 Nessus.....	36
<b>7 Tulosten tarkastelu.....</b>	<b>44</b>
7.1 Tutkimustulokset.....	44
7.2 Kehitysehdotukset.....	46
7.3 Haasteet .....	47
<b>8 Pohdinta.....</b>	<b>48</b>
<b>Lähteet .....</b>	<b>50</b>
<b>Liitteet.....</b>	<b>52</b>
Liite 1. Ulkoverkon skannauksen tulokset .....	52
Liite 2. Päätelaitteen skannauksen tulokset .....	53
Liite 3. Verkon segmentin skannauksen tulokset .....	54
Liite 4. Haavoittuvuudet (Salassa pidettävä) .....	55
Liite 5. Avoimet portit ja palvelut (Salassa pidettävä) .....	56

**Kuviot**

Kuvio 1. TCP, kolmivaiheinen kättely.....	19
Kuvio 2. SYN-skannaus.....	19
Kuvio 3. UPD-porttiskannaus.....	20
Kuvio 4. Toimipisteen verkon rakenne.....	22
Kuvio 5. Käytetyimmät palvelut.....	27
Kuvio 6. OpenVAS, asennus.....	29
Kuvio 7. OpenVAS, käyttöönotto.....	30
Kuvio 8. OpenVAS, etusivu.....	31
Kuvio 9. Ulkoverkosta suoritettu skannaus.....	32
Kuvio 10. Palomuurin loki.....	32
Kuvio 11. IPS-loki.....	33
Kuvio 12. Ulkoverkon skannauksen tulokset.....	33
Kuvio 13. Tunnusten luominen.....	34
Kuvio 14. Skannaus tunnusten avulla.....	34
Kuvio 15. Sisäverkon skannaus, yksittäinen päätelaite.....	35
Kuvio 16. Sisäverkon skannaus, verkon segmentti.....	35
Kuvio 17. Nessuksen aktivointi.....	36
Kuvio 18. Nessus asennettuna.....	37
Kuvio 19. Skannauspohjat.....	37
Kuvio 20. Skannaus ulkoverkosta.....	38
Kuvio 21. Palomuurin loki.....	39
Kuvio 22. IPS-loki.....	39
Kuvio 23. Ulkoverkon skannauksen tulokset.....	39
Kuvio 24. Skannaus päätelaitteelle.....	40
Kuvio 25. Päätelaitteen skannauksen tulokset.....	40
Kuvio 26. Skannaus käyttäjätunnuksilla.....	41
Kuvio 27. Käyttäjätunnusten lisääminen.....	41
Kuvio 28. Päätelaitteen skannauksen tulokset, käyttäjätunnuksilla.....	42
Kuvio 29. Verkon segmentin skannausasetukset.....	43

Kuvio 30. Verkon segmentin skannauksen tulokset, yksittäinen laite .....	43
Kuvio 31. Nessuksen tarjoamat korjausehdotukset .....	44

## **Taulukot**

Taulukko 1. CVSS-luokitus.....	13
Taulukko 2. Haavoittuvuusskannaus -ohjelmistojen vertailu .....	24
Taulukko 3. Liikkuneen datan määrä.....	28
Taulukko 4. Teknisen toteutuksen järjestys .....	29

## Lyhenteet

CIS = Center for Internet Security

CVE = Common Vulnerabilities and Exposures

CVSS = Common Vulnerability Scoring System

DHCP = Dynamic Host Configuration Protocol

DNS = Domain Name System

HTTP = Hypertext Transfer Protocol

HTTPS = Hypertext Transfer Protocol Secure

ICMP = Internet Control Message Protocol

IEC = International Electrotechnical Commission

IP = Internet Protocol

ISO = International Organization for Standardization

LAN = Local Area Network

SMTP = Simple Mail Transfer Protocol

SNMP = Simple Network Management Protocol

TCP = Transmission Control Protocol

UDP = User Datagram Protocol



# 1 Lähtökohdat

## 1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi TietoAkseli Oy. TietoAkseli Oy on osa TietoAkseli Yhtiöt Oy konsernia. TietoAkseli on suomalainen perheyritys, jolla on toimipisteitä Jyväskylässä, Helsingissä, Tampereella, Oulussa, Mikkelissä, Ikaalisissa ja Pieksämäellä. Yritys tarjoaa taloudellisen neuvonannon, tilintarkastuksen ja yritysjärjestelyjen osaamista. Vuonna 2018 yrityksen liikevaihto oli yli kahdeksan miljoonaa euroa ja henkilöstöä oli keskimäärin 130. Yritys on Suomen Taloushallintoliitto Ry:n valvoma, auktorisoitu tilitoimisto ja osa UHY International-yritysketjua. (Keskitettyä talouden osaamista kasvupolulle 2018.)

## 1.2 Toimeksianto

Opinnäytetyön toimeksianto pohjautui yrityksen haluun tavoitella tulevaisuudessa ISO 27001 -sertifiointivalmiutta. Yrityksen vauhdikkaan kasvun mukana tapahtuneiden jatkuvien muutosten myötä tietoverkkojen konfiguroinnin tulisi olla toteutettu asianmukaisella tavalla. Toimeksianto keskittyy tietoverkkojen nykytilan selvitykseen ulko- ja sisäverkon palveluiden sekä IP-osoitteiden pohjalta. Työn päätavoite oli varmistaa, että yrityksen verkoista löytyy vain sinne kuuluvia laitteita ja että niissä on käytössä vain tarvittavat ja halutut palvelut.

## 1.3 Opinnäytetyön tavoitteet

Työn tavoitteena oli selvittää ja tunnistaa TietoAkselin tietoverkkojen nykytila. Tietoverkon tärkeimpinä kohteina siellä toimivat aktiivi- ja päätelaitteet, verkoissa avoimena olevat yleiset palvelut, portit ja protokollat. Toimeksiantaja halusi myös selvittää, löytyykö TietoAkselin tietoverkoista tai niihin kuuluvista laitteista yleisesti tiedossa olevia haavoittuvuuksia tai päivittämättömiä päätelaitteita. Lopuksi selvityksen tuloksista tuli tehdä raportti, josta selviäisi tietoverkoista tehdyt havainnot ja niihin liittyvät kehittämisehdotukset.

Työssä mahdollisesti käytettävän ohjelmiston tuli olla avoimeen lähdekoodiin perustuva tai hinnaltaan yritykselle sopiva. Työn tavoitteena oli luoda toimeksiantajalle hyvä tilannekuva siitä, mitä laitteita, palveluita ja avoimia portteja verkoista löytyy. Lisäksi työ tarjoaa yritykselle kehitysehdotuksia verkon nykytilan parantamiseksi. Työn teoriaosuudessa käydään läpi eri teknisistä lähteistä koottua teoriaa liittyen haavoittuvuuksien sekä verkon hallintaa.

## 2 Tutkimusmenetelmät

### 2.1 Kvalitatiivinen tutkimus

Kvalitatiivisella eli laadullisella tutkimuksella tarkoitetaan tutkimusta, jonka tavoitteena on selvittää, mistä tutkittu ongelma johtuu tai mitkä eri tekijät ongelmaan vaikuttavat. Tutkimusta voidaan tehdä esimerkiksi havainnoinnin tai aiheen pohjalle aikaisemmin tuotettujen dokumenttien pohjalta. Kvalitatiivinen tutkimus sopii tilanteisiin, joissa tutkittavasta ilmiöstä halutaan saada selville siihen liittyvä kuvaus. (Kananen 2015, 70-71.)

### 2.2 Kvantitatiivinen tutkimus

Määrällinen eli kvantitatiivinen tutkimus tarkoittaa tutkimusta, jonka tavoitteena on tuottaa ja havainnollistaa luotettavaa ja perusteltua tietoa. Kvantitatiivista tutkimusta voidaan toteuttaa tekemällä tilastoja esimerkiksi kyselystä saatujen vastausten pohjalta. Kvantitatiivinen tutkimus vaatii tutkittavan ilmiön riittävän täsmentymisen tai tarkkuuden. Määrällinen tutkimus eroaa laadullisesta tarkasti määriteltyjen tulkintaohjeiden myötä. (Kananen 2015, 73.)

## 2.3 Työssä käytetty menetelmä

Opinnäytetyö toteutettiin kvalitatiivisena tutkimuksena, koska haluttiin saada varmuus siitä, miten toimeksiantajan asettamat tavoitteet tietoverkon nykytilasta voidaan selvittää ja ratkaista. Työssä otettiin kantaa sekä käytettiin erilaisia teknisiä ratkaisuja, joiden avulla toimeksiannon mukana tullessiin tutkimuskysymyksiin etsittiin vastausta. Työn teoriaosuus rakentuu useasta eri tietotekniikan alaan liittyvästä lähteestä kuten verkosta löytyvistä artikkeleista sekä julkaisuista.

Opinnäytetyössä tutkimusmuotona käytettiin Case-tutkimusta (tapaustudkimusta). Työn avulla haluttiin saada syvälinen ja laaja käsitys tutkittavasti aiheesta. Case-tutkimuksessa kohteena on usein yksittäinen tapaus. Kvalitatiivisen ja kvantitatiivisen tutkimusmenetelmän aineistonkeruuta ja sen analysointia voidaan käyttää Case-tutkimuksen tutkimusmenetelmänä. (Kananen 2015, 76.) Case-tutkimukseen liittyy lähestymistapojen eli tutkimusotteiden yhdistely (Kananen 2015, 358).

## 2.4 Tutkimuskysymykset

Opinnäytetyön tutkimuskysymyksiksi valittiin seuraavat:

- Miten selvittää ja tunnistaa TietoAkselin verkossa toimivat aktiivi- ja päätelaitteet sekä avoimena olevat palvelut, portit ja protokollat?
- Miten löytää TietoAkselin tietoverkoista yleisesti tiedossa olevia haavoittuvuuksia ja päivittämättömiä päätelaitteita?

Tutkimuskysymykset vastaavat suoraan opinnäytetyölle toimeksiantajan määrittämiä selvitettäviä tavoitteita. Samalla ne selkeyttävät tutkittavaa aihetta ja määrittävät mahdolliseen tekniseen toteutukseen valittuja ohjelmistoja ja niiltä vaadittavia ominaisuuksia. Opinnäytetyössä tutkittiin, löytyykö toimeksiantajan määrittämiin tavoitteisiin yhtä tai useampaa teknistä ratkaisua, jonka avulla löydettyistä epäkohdista ja puutteista olisi mahdollista koota selkeä raportti sekä niihin liittyvät kehitysehdotukset.

## 3 Yleistä tietoverkoista

### 3.1 Ajankohtaisuus

Ylen kesäkuussa 2019 julkaisemassa artikkelissa kerrotaan Lahden kaupungin tietoverkkoon kohdistuneesta hyökkäyksestä. Tietoverkkoon kohdistuneen hyökkäyksen takia Lahden kaupungin ja Päijät-Hämeen hyvinvointiyhtymän välinen verkkoyhteys jouduttiin katkaisemaan. Hyökkäyksen takia esimerkiksi potilaskertomusten tiedot sekä sähköiset reseptit eivät olleet käytössä. Tietoverkkoihin kohdistuneessa hyökkäyksessä yhden koneen saastuminen haittaohjelmalla johti sen leviämisen noin tuhanteen muuhun koneeseen. Artikkelissa korostettiin virusturvan, valvonnan sekä hyökkäystilanteessa tapahtuvan nopean reagoinnin tärkeyttä. Kyberhyökkäykset voivat aiheuttaa yrityksissä mittavia häiriöitä sekä lamauttaa yrityksen toiminnan hetkellisesti, minkä takia verkonvalvontaan sekä riskienhallintaan liittyvät seikat ovat tärkeä osa yrityksen toimintaa. (Heikkilä, Ahjopalo & Parkkinen 2019.)

### 3.2 Lähiverkko

Lähiverkko eli LAN (engl. Local Area Network) tarkoittaa tietyn rajatun alueen tietoliikenneverkkoa. Lähiverkko voi sisältää myös yrityksen sisäisen loogisen tietoverkon eri toimipisteiden välillä. Lähiverkkoon voi kuulua esimerkiksi kytkimiä, palomureja, reitittäjiä, työasemia ja palvelimia. Lähiverkko koostuu yleensä kahdesta tai useammasta toisilleen viestivistä laitteista. Isosta osasta lähiverkon toimintaa vastaavat siihen liitetyt palvelut, kuten DNS-nimipalvelu (Domain Name System). (Mikä on sisäverkko 2010.)

### 3.3 Verkon hallinta

Yrityksen sisäverkko ei siihen kuuluvien laitteiden näkökulmasta yleensä pysy kovin kauan samanlaisena, sillä muutoksia saattaa tapahtua useista kertoista viikossa tai jopa päivässä. Erilaiset laitteet liittyvät tai poistuvat työntekijöiden mukana yrityksen ver-

kon sisällä. Jokainen yrityksen verkossa oleva laite tulisi olla tiedossa sekä tarvittaessa yrityksen hallinnassa. Verkon toimintaa ja siihen liitettyjä laitteita tulisi valvoa ja seurata säännöllisesti tietoturvan näkökulmasta. Verkon hallintaa sekä valvontaa tulisi organisaatiossa hoitaa siihen määritetty henkilö. Käyttöoikeudet verkon hallintaa ja valvontaa toteuttavilla ovat vain niitä työtehtävissä tarvitsevilla henkilöillä (Verkon hallinta/valvonta 2010.)

Valvonnassa ja hallinnassa tulisi erityisesti huomioida seuraavat asiat:

- Hallittavat ja valvottavat laitteet on määritelty etukäteen.
- Toiminta, joka liittyy valvontaa ja hallintaan on erotettu loogisesti muusta verkosta
- Kuormitustilannetta seurataan mahdollisten ongelmien varalta.
- Hallinta ja valvonta suoritetaan laitteilta, jotka ovat fyysisesti erillään työasemista.
- Verkko tarkistetaan säännöllisesti ylläpitäjän toimesta.

## **SNMP**

SNMP-protokolla (Simple Network Management Protocol) on Sathyan (2010) mukaan yksi suosituimmista verkon hallintaprotokollista. Sen avulla voidaan hallinnoida useita eri verkon elementtejä, kuten reitittimiä tai työasemia. SNMP on yksi yksinkertaisimmista hallintaprotokollista, joka tunnistaa virhetilanteita SNMP TRAP -ominaisuuden avulla. Protokolla on helppo ottaa käyttöön hallituille laitteille. SNMP käyttää yhteydessä yhteydetöntä UDP-protokollaa. Protokollasta on kolme eri versiota: SNMPv1, SNMPv2 ja SNMPv3. Verkonhallinnassa SNMP koostuu yleensä aktiivi- tai päätelaitteille sijoitettavista agenteista sekä hallinta-asemasta. Hallinta-asema vastaanottaa dataa laitteilla sijaitsevilta agenteilta. (Sathyan 2019.)

### **3.4 Verkon topologia**

Fyysinen topologia antaa tarkan kuvan siitä, miten eri laitteet ovat fyysisesti kytkettyinä toisiinsa kaapeloinnin avulla. Looginen topologia tarkoittaa visuaalista esitystä, joka kertoo, miten eri laitteet ovat kytkettyinä toisiinsa. Looginen topologia ei välttämättä esitä suoraan, missä yksittäinen laite sijaitsee. Sen avulla kuitenkin nähdään, miten data liikkuu eri laitteiden välillä. Erilaisia verkkotopologioita ovat esimerkiksi

tähti- ja rengastopologia. Tarkasti tiedossa oleva sekä hyvin dokumentoitu verkon rakenne auttaa vikatilanteissa selvittämään, missä mahdollinen ongelmakohta saattaa sijaita. Tämän takia on tärkeää, että tehtäessä verkkoon muutoksia ne dokumentoidaan selkeästi. (Keary 2018.)

### 3.5 Laitetyypit

#### **Päätelaite**

Päätelaite tarkoittaa laitetta, joka kommunikoi edestakaisin muiden laitteiden kanssa siihen kytketyssä verkossa. Kommunikointi verkossa yleensä alkaa ja päättyy päätelaitteelta. Hyvä esimerkki päätelaitteesta on kannettava tietokone. (What is an endpoint 2019.)

#### **Aktiivilaite**

Olivieron ja Woorwardin (2014) mukaan verkon aktiivilaitteet liikuttavat, ohjaavat sekä vastaanottavat siellä kulkevaa dataa. Ne osallistuvat laitteiden väliseen kommunikointiin välittämällä ja vastaanottamalla elektronisia ja optisia signaaleja. Yleisimpiä aktiivilaitteita ovat kytkimet. Usean aktiivilaitteiden keskinäinen toiminta muodostaa yhtenäisemmän verkon. (Oliviero & Woodward 2014.)

### 3.6 Päivitysten hallinta

Verkossa olevien laitteiden turvallisuutta voidaan parantaa korjaamalla ohjelmistojen tai laitteiden toiminnallisia ongelmia tekemällä niihin päivityksiä. Päivitysten hallinnalla tarkoitetaan prosessia, jossa tunnistetaan, asennetaan ja varmistetaan uusimpien päivitysten saatavuus laitteille ja ohjelmistoille. Sillä voidaan estää jo olemassa olevien haavoittuvuuksien hyväksikäyttö IT-ympäristöissä. Se voi tuoda myös säästöjä ajan- sekä sovellustenhallintaan. Aktiivinen päivitysten hallinta vähentää tai voi jopa poistaa osan verkossa olevien laitteiden turvallisuusuhkista. Päivitysten hyötyihin lukeutuvat myös niiden mukana ohjelmistoihin tulevat uudet parannetut turvallisuusomaisuudet. (Bosworth, Kabay & Whyne 2014.)

### 3.7 Haavoittuvuus

Haavoittuvuus laitteistossa tai ohjelmassa tarkoittaa, että sen suunnittelussa tai koodissa voi olla virhe, johon kohdistuu mahdollisesti hyväksikäytettävä riski. Haavoittuvuus voi kohdistua esimerkiksi käyttöjärjestelmään, itse laitteistoon, sovellukseen tai verkkosovellukseen. Haavoittuvuudet voivat myös kohdistua yksittäisiin käytössä oleviin protokollisiin tai portteihin. Vain osa löydetyistä haavoittuvuuksista on korjattu päivityksillä. Uusia haavoittuvuuksia syntyy nopeasti uusien ohjelmiston ja laitteiden myötä. Haavoittuvuus voi pahimmillaan johtaa siihen kohdistettuun hyökkäykseen tai muuhun haitantekoon tietoverkossa. (Hibbert & Haber 2018.) Opinnäytetyössä haavoittuvuudet ja niiden käsittely rajattiin laitteistoista tai ohjelmista löytyviin haavoittuvuuksiin.

#### **Haavoittuvuus prosessissa**

Hodsonin (2019) mukaan organisaatiolla käytössä olevan teknologisen tietotaidon vahvuus muodostuu siellä käytössä olevien prosessien vahvuuden mukaan. Käytössä olevissa prosesseissa täytyy huomioida tarkista erilaisten laitteiden elinkaari. Organisaatiolla tulee olla tiedossa laitteiden sijainti sekä käyttäjä. Haavoittuvuus yrityksellä tai organisaatiolla käytössä olevassa prosessissa voi johtaa esimerkiksi lopettaneen työntekijän kadonneeseen päätelaitteeseen. (Hodson 2019.)

#### **CVE**

Common Vulnerabilities and Exposures (CVE) on lista yleisesti tunnetuille kyberturvallisuuden haavoittuvuuksille. CVE on perustettu 1999, kun useat eri kyberturvallisuuden toimijat viittasivat samoihin haavoittuvuuksiin eri tunnisteilla ja merkintätavat haluttiin yhtenäistää. Yhdelle haavoittuvuudelle voidaan kohdistaa yksi CVE, jonka avulla se yksilöidään. Työkalut ja palvelut voivat keskustella keskenään yhteisen merkintätavan avulla. CVE sisältää ID-numeron, lyhyen kuvauksen haavoittuvuudesta ja siihen liittyviä viitetietoja. Numero eli ID koostuu vuosiluvusta, joka kuvaa ajankohtaa, jolloin haavoittuvuus on löydetty, sekä yksilöllisestä juoksevasta luvusta. Juokseva luku alkaa aina uuden vuoden alkaessa alusta. (About CVE 2019.)

## CVSS

Common Vulnerability Scoring System (CVSS) on avoimen viitekehyksen järjestelmä, joka on julkaistu ensimmäisen kerran vuonna 2004. Järjestelmän on perustanut FIRST-organisaatio. CVSS-järjestelmästä on neljä eri versiota: v1, v2, v3 ja v3.1. Uusin versio on julkaistu kesäkuussa 2019. Järjestelmää käytetään ohjelmistoista ja laitteistoista löydettyjen haavoittuvuuksien vakavuuden arviointiin. Haavoittuvuuteen liitetyn CVSS-arvon tarkoituksena on kertoa käyttäjälle numeerinen arvo, jonka pohjalta haavoittuvuudesta aiheutuvat riskit ja sen vakavuus on mahdollista arvioida. Arvo haavoittuvuudelle annetaan väliltä 0.0 – 10.0. Taulukossa 1 on esitetty, miten CVSS-pisteet rajataan eri luokkiin. Pisteytyksessä otetaan huomioon hyökkäystapa, hyökkäyksen monimutkaisuus sekä tunnistautumisvaatimus. Pisteytykseen vaikuttaa myös haavoittuvuuden tuoma riski luottamuksellisuuteen, eheyteen tai saatavuuteen. (First 2019.)

Taulukko 1. CVSS-luokitus

Luokitus	CVSS-pisteet
Ei luokitusta	0.0
Matala	0.1 - 3.9
Keskitaso	4.0 - 6.9
Korkea	7.0 - 8.9
Kriittinen	9.0 - 10.0

### 3.8 Haavoittuvuuksien hallinta

Haavoittuvuuksien hallinnan tarkoituksena on minimoida riski, jonka haavoittuvuudet laitteistossa tai ohjelmissa tuovat mukanaan organisaatioihin. Päivitysten hallinta on yksi osa haavoittuvuuksien hallintaa. Haavoittuvuuksia havaittaessa täytyy olla tietoinen kohteen eli laitteen tai ohjelmiston kriittisyydestä organisaatiossa. Haavoittuvuuskanneri ei suoraan tiedä, kuinka tärkeä haavoittuvuuden sisältämä kohde on organisaatiolle. Kaksi tai useampi pieni haavoittuvuus voi johtaa yhdessä suurempaan haavoittuvuuteen, jotka toisiinsa yhdistämällä aiheuttavat suurempaa haittaa kuin alkuperäiset yksittäiset pienet haavoittuvuudet. Organisaation on hyvä kartoittaa valmiiksi toimenpiteitä, joita noudatetaan, kun järjestelmistä löydetään uusia haavoittuvuuksia. (Williams 2019.)



### 3.9 Baselineing – Verkon suorituskyvyn määrittäminen

Baseline tarkoittaa prosessia, jossa verkon suorituskykyä ja tilaa arvioidaan sekä mitataan säännöllisesti, jotta sitä voidaan verrata normaalitilasta poikkeavaan tilanteeseen. Samalla varmistetaan siitä, että organisaation verkko toimii suunnitellulla tavalla. Baseline-määrittämiseen tarvitaan tietoa verkon liikenteen määrästä, käytetyistä protokollista ja palveluista sekä esimerkiksi laitteiden rasituksen tilasta, kuten prosessorin suorituskyvyn määrästä.

Prosessin avulla saadaan selville verkossa olevien laitteiden ja sovellusten tila sekä tietoa verkon resursseista ja niiden riittävydestä. Kun raja-arvot verkon suorituskyvylle ja normaaliksi määritellylle tilalle on pystytty määrittämään, tulevien ongelmatilanteiden huomaaminen ja selvitys on helpompaa. Tekemällä verkon suorituskyvyn mittausta ja määrittämistä säännöllisesti voidaan käytössä olevista laitteista tai ohjelmistoista löytää ongelmia, jotka on mahdollista korjata ennen laite- tai ohjelmistorikojen. Verkon eri komponenttien vaihtumisen jälkeen vertaamalla verkon tilaa aikaisemmin määritettyyn Baselineen, muutokset tai ongelmat verkon tilassa on helpompi havaita. Raja-arvojen ja niihin liittyvien hälytysten tarkka määrittäminen voidaan selvittää Baselinein avulla. (Baseline Process Best Practices White Paper 2005.)

### 3.10 ISO/IEC 27001:2017 -Standardi

ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) yhdessä muodostavat maailmanlaajuiseen standardisointiin erikoistuneen järjestelmän. ISO/IEC 27001:2017 -standardissa esitellään tietoturvallisuuden liittyvää hallinjärjestelmänluomista, toteutusta, ylläpitämistä ja jatkuvaa parantamista. Hallintajärjestelmän tarkoitus on suojata tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Standardia voidaan käyttää sisäisten ja ulkoisten sidosryhmien organisaation kykyyn arvioida tietoturva-vaatimusten täyttämistä. (SFS-EN ISO/IEC 27701:2017 2017.)

### Soveltuvuus toimeksiintoon

Standardissa on esitettyä vaatimuksia, jotka soveltuivat samalla osaksi tämän opin- näytetyön toimeksiintoa. Standardissa olevat tietoturvakontrollit toimivat ohjeistuk- sina, joiden avulla voidaan hallita haavoittuvuuksien mukana tuomia vaikutuksia (SFS-EN ISO/IEC 27001:2017 2017):

- Teknisten haavoittuvuuksien hallinta – Teknisistä haavoittuvuuksista on han- kittava ajantasaista tietoa.
- Verkon hallinta – Verkkoja on hallittava ja valvottava.

### 3.11 Katakri 2015

Katakri eli kansallinen turvallisuusauditointikriteeristö on auditointityönkalu salassa pidettävän tiedon suojaamisen arviointiin. Se perustuu vaatimuksiin, jotka koskevat kansallisia säädöksiä ja velvoitteita. Kriteeristö ei aseta itsessään vaatimuksia, vaan se perustuu lainsäädäntöön ja kansainvälisiin tietoturvelvoitteisiin. Katakriassa esitetyt vaatimukset on jaettu kolmeen eri osa-alueeseen (Katakri 2015, 3):

1. Turvallisuusjohtaminen – Riittävä turvallisuusjohtamisen valmius ja kyvyk- kyys
2. Fyysinen turvallisuus – Fyysistä käyttöympäristöä koskevat turvallisuusvaati- mukset
3. Tekninen tietoturvallisuus – Tietojenkäsittely-ympäristölle asetetut turvalli- suusvaatimukset

Tekninen tietoturvallisuus on vielä jaettu tarkemmin neljään eri aihealueeseen: tieto- liikenneturvallisuus, tietojärjestelmäturvallisuus, tietoaineistoturvallisuus ja käyttö- turvallisuus (Katakri 2015, 3). Käyttöturvallisuudessa otetaan kantaa ohjelmistohaa- voittuvuuksien hallintaan. Vaatimuksessa kerrotaan, että koko tietojenkäsittely-ym- päristön elinkaaren ajalle toteutetaan menettelyt ohjelmistohaavoittuvuuksien hallit- semiseksi.

*Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannetta- vat tietokoneet ja vastaavat tarkastetaan (haavoittuvuusskannaus, CMDB, jne.) säännöllisesti aina merkittävien muutosten jälkeen päivitysmenettelyjen kor- jauskohteiden löytämiseksi (Katakri 2015, 64).*

### 3.12 CIS Controls – parhaat käytänteet

Center for Internet Security (CIS) Controls ovat joukon IT-alan ammattilaisten kehittämää kyberturvallisuuden parhaita suositeltuja käytänteitä. Sen kehittäjät tulevat useilta eri aloilta, kuten koulutus- ja hallinnolliselta-alalta. Käytänteet ovat jaettu kolmeen pääosioon: yleisiin, perustaviin ja organisaatioihin kohdistuviin osioihin. Yhteensä käytänteitä on 20 kappaletta, mutta työssä perehdytään niistä neljään. Valitut käytänteet soveltuvat opinnäytetyön toimeksiantoon. Käytänteiden päätarkoituksena on luoda ja edistää tietoturvaa julkisella sekä yksityisellä sektorilla. CIS-käytänteiden tarkoituksia ovat esimerkiksi seuraavat:

- Jakaa tietoa hyökkäyksistä ja hyökkääjistä, tunnistaa syyt ja jakaa tietoa niiden puolustautumiseen.
- Dokumentoida tapahtumia ja jakaa ratkaisuja ongelmiin.
- Jäljittää ja seurata uhkien kehittymistä.
- Tehdä käytänteistä säädelyjä ja toimivia kokonaisuuksia.
- Jakaa työkaluja ja ohjeita niiden käyttöön.
- Tunnistaa yleisiä ongelmia ja tarjota apua niiden ratkaisuun.

#### **CIS Control 1 – Laitteiden hallinta ja inventointi**

Käytänteen tarkoituksena on aktiivisesti hallita ja seurata organisaation omia laitteita verkossa, jotta vain sinne kuuluvat laitteet saavat pääsyn verkkoon. Sinne kuulumattomien ja ei-hallittujen laitteiden pääsy estetään. Verkosta löydettyjen tunnistamattomien laitteiden pääsy estetään. Käytäntö on tärkeä, sillä hyökkääjät skannaavat verkkoa ja organisaatioiden IP-osoite avaruuksia jatkuvasti. Hyökkääjät ovat erityisesti kiinnostuneita laitteista, jotka eivät jatkuvasti ole yrityksen verkossa, vaan niitä kuljetetaan esimerkiksi mukaan töihin. Kyseiset *Bring-Your-Own-Device* (BYOD) -laitteet voivat olla jäljessä yrityksen jakelemista päivityksistä ja näin ollen saattavat sisältää muita laitteita enemmän aukkoja tietoturvassa. Organisaation on tärkeää aktiivisesti skannata omaa verkkoaan sieltä löytyvien sinne kuulumattomien laitteiden varalta. (CIS Controls 2019, 8.)

**CIS Control 2 – Ohjelmistojen hallinta ja inventointi**

Käytännön tarkoituksena on aktiivisesti hallita kaikkia organisaation käyttämiä ohjelmistoja, jotta vain hallittuja ja tarkoituksenmukaisia ohjelmistoja voidaan asentaa ja suorittaa. Kaikki ei hallitut ja sallimattomat ohjelmistot pyritään estämään asentamasta tai suorittamasta. Hyökkääjät etsivät jatkuvasti ohjelmia, joiden käytössä olevasta versiosta löytyy haavoittuvuus hyödynnettäväksi. Organisaatioiden on tärkeää olla perillä siellä käytössä olevista ohjelmistoista, versioista sekä niihin saatavista päivityksistä. (CIS Controls 2019, 12.)

**CIS Control 3 – Jatkuva haavoittuvuuksien hallinta**

Käytännön tarkoituksena on jatkuvasti kerätä tietoa, arvioida ja tehdä toimenpiteitä liittyen haavoittuvuuksien tunnistamiseen ja hallintaan. Organisaation täytyy olla tietoinen ohjelmistojen päivityksistä, turvallisuusongelmista ja uhkista. Haavoittuvuuksien ymmärtäminen ja hallinta on muuttunut jatkuvaksi, aikaa ja resursseja kuluttavaksi toimenpiteeksi. Hyökkääjillä on käytössään sama tieto haavoittuvuuksista kuin organisaatioilla, joten uusien haavoittuvuuksien löytyessä he voivat hyödyntää löytynyttä ongelmaa, ennen kuin siihen tulee päivitys tai se korjataan. Organisaatiot, jotka eivät suorita haavoittuvuusskannausta ja aktiivisesti seuraa löytyneitä uhkia, ovat mahdollisesti suuremman uhkan kohteena. Haavoittuvuuden hallintaan voidaan toteuttaa esimerkiksi useilla eri haavoittuvuusskannaus-ohjelmistoilla. (CIS Controls 2019, 15.)

**CIS Control 9 – Porttien, protokollien ja palveluiden rajoitus ja hallinta**

Käytännön tarkoituksena on hallita jatkuvasti käytössä olevien porttien, protokollien ja palveluiden käyttöä ja samalla minimoida niiden käyttö vain tarvittavaan ja näin pienentää hyökkääjän mahdollisuuksia hyödyntää aukkoja tietoturvassa. Hyökkääjät etsivät verkossa olevia haavoittuvuuksia sisältäviä palveluita, joita voidaan hyödyntää etäkäytön avulla. Yleisiä kohteita ovat väärin tai puutteellisesti konfiguroidut web-, sähköposti- ja tiedostopalvelimet. Useat ohjelmistot asennuksen yhteydessä käynnistävät palvelun ja jättävät sen päälle ilman, että käyttäjä on siitä tietoinen. Käynnissä olevia palveluita ja portteja on mahdollista skannata ja koittaa käyttää myös hyväksi. Skannaustyökaluilla on mahdollista myös selvittää portissa toimivan protokollan versio ja palvelu, joka siellä toimii. (CIS Controls 2019, 34.)

### 3.13 Portti- ja verkon skannaustekniikat

#### **Porttiskannaus**

Viestintä verkossa laitteiden ja sovellusten välillä tapahtuu usein ennalta määritetyissä porteissa. Auki olevaa porttia on mahdollista kuunnella ja sen kautta kulkevaa liikennettä seurata. Porttiskannauksen tarkoituksena on selvittää, mitkä portit ovat auki ja käytössä skannattavassa järjestelmässä. Avoimia portteja voidaan siis käyttää myös haitallisessa tarkoituksessa. Tämän takia organisaation on hyvä tietää, mitkä portit ovat auki ja mitä palveluita kyseisissä porteissa toimii.

Esimerkiksi SMTP (Simple Mail Transfer Protocol) -protokolla, jota käytetään sähköpostin lähettämisessä, käyttää oletuksena porttia 25. Mitä vähemmän portteja ulospäin on auki, sitä vaikeampaa verkosta on saada tietoa ulos. Porttiskannaus lähettää kyselyn porttiin ja kertoo, saapuuko portista vastaus. Jos vastaus saapuu, portti voi mahdollisesti olla auki ja siellä toimivasta palvelusta voidaan saada tietoa. (Henry 2012.)

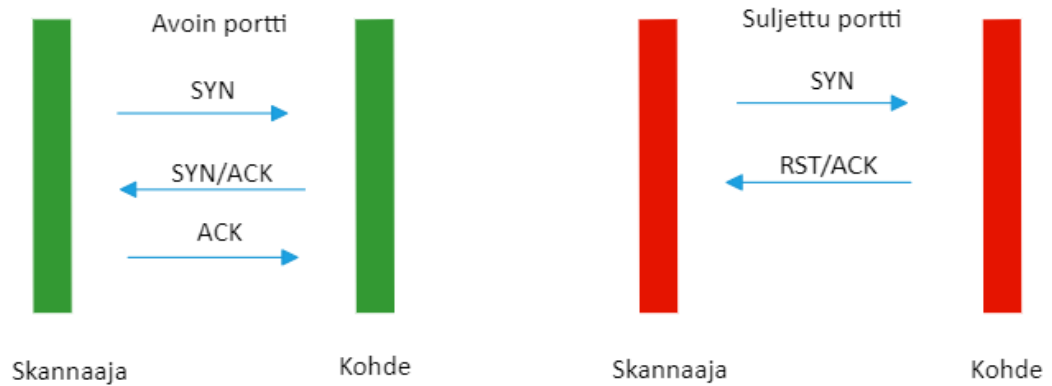
#### **ICMP / Ping Sweep**

ICMP (Internet Control Message Protocol) -protokollan avulla voidaan lähettää ping-kyselyä skannattavaan kohdeverkkoon. Verkossa olevat kohteet, joissa kyselyä ei ole erikseen estetty, vastaavat tähän. Tämä kysely paljastaa vastanneiden laitteiden olemassaolon ja niiden löytymisen kyseistä verkosta. Ping Sweep tarkoittaa ping-kyselyn automatisointia lähettämällä kyselyitä valmiiksi määritetyille IP-osoitealueelle. Tällä voidaan halutessaan välttää jokaisen yksittäisen verkossa olevan kohteen skannaus. (Henry 2012.)

#### **TCP-skannaus**

TCP (Transmission Control Protocol) -protokollan avulla voidaan yrittää muodostaa kolmivaiheinen kättely. Kättelyn avulla voidaan selvittää, onko skannauksen kohteena oleva portti auki. TCP-yhteydellä tehty porttiskannaus yrittää toistuvasti muodostaa yhteyttä kyseiseen porttiin. Ensiksi kyselyn tekijä lähettää SYN-pyyntöä. Portin ollessa auki se vastaa SYN/ACK. Lähettäjä vastaa vielä takaisin ACK ja yhteys laittei-

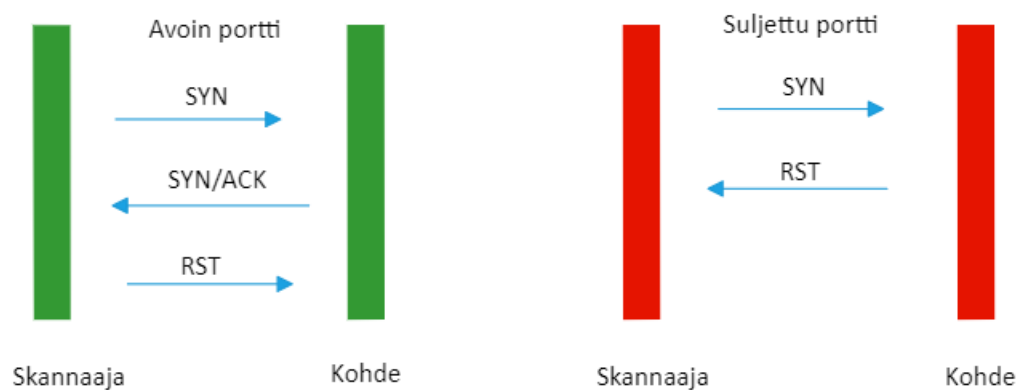
den välille muodostuu. SYN-pyyntöön voi tulla myös vastaus RST/ACK, mikä tarkoittaa, että kyseinen portti on suljettu tai se ei vastaa. Kuviossa 1 on esitettyä kolmivaiheinen kättely avoimen sekä suljetun portin osalta. (Henry 2012.)



Kuvio 1. TCP, kolmivaiheinen kättely

### SYN-skannaus

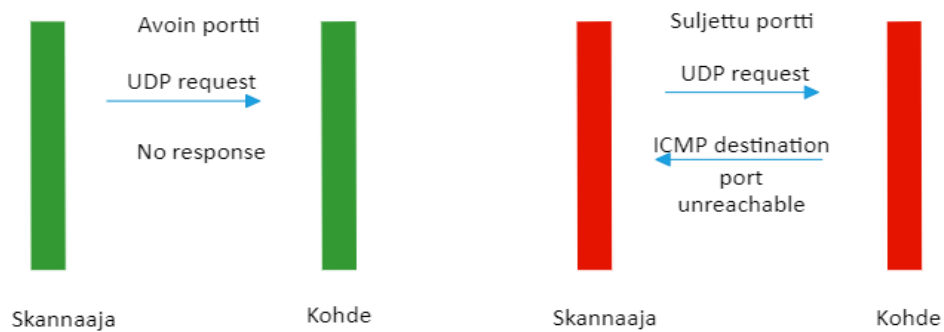
SYN-skannaus toimii samaan tapaan kuin TCP-skannauksessa tehty kolmivaiheinen kättely, mutta se suorittaa vain kaksi ensimmäistä vaihetta. SYN-skannaus lähettää ensiksi SYN-paketin kohteelle, josta tulee vastaus SYN/ACK, kun portti on auki ja käytössä. Tämän jälkeen kohteelle lähetetään ACK-paketin sijaan RST-paketti ja yhteys sulkeutuu. SYN-skannaus toimii nopeammin kuin normaali TCP-skannaus, koska lähetettyjä paketteja on vähemmän. Kuviossa 2 näkyy, miten tämä skannaus toimii. (Engbretson 2013.)



Kuvio 2. SYN-skannaus

## UDP-skannaus

UDP (User Datagram Protocol) -protokollan avulla voidaan myös havaita auki tai kiinni olevia portteja. UDP-skannauksen toiminta perustuu protokollan lähettämään UDP-pyyntöön. Jos pyyntöön tulee vastaus ”Port unreachable” tiedetään, että portti on kiinni. Kuviossa 3 näkyy, miten UDP-porttiskannaus toimii. Jos vastausta ei tule, portti saattaa olla auki, mutta se on voitu myös estää palomuurilta. (Henry 2012.)



Kuvio 3. UPD-porttiskannaus

## 4 Kohteiden selvitys

### 4.1 Tavoite

Yrityksen tietoverkon analysointiin sisältyi laitteiden tunnistaminen ja löytäminen verkosta. Löytyneistä laitteista haluttiin selvittää avoimet portit, porteissa toimivat palvelut ja palveluiden käyttämät protokollat. Tavoitteena oli myös löytää päivittä-mättömiä pääte- ja aktiivilaitteita ja yleisesti tiedossa olevia haavoittuvuuksia. Verkon laitteiden analysointi oli hyvä aloittaa ensiksi pienemmästä kohdealueesta, esimerkiksi yhdestä päätelaitteesta, minkä jälkeen oli helpompi ymmärtää, miten analysointia ja skannausta kannattaisi toteuttaa useammalle kohteelle.

## 4.2 Rajaus

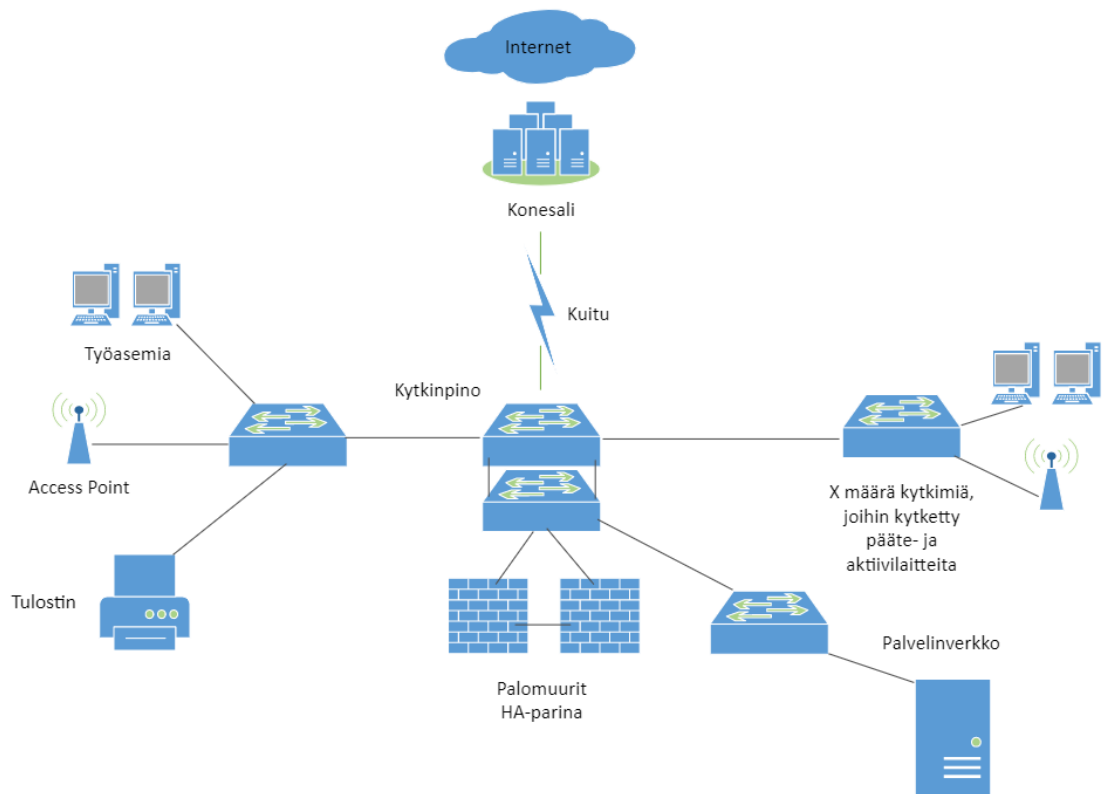
Tietoverkon analysointi rajattiin TietoAkselin Jyväskylän toimipisteeseen. Analysointiin liittyvä tekninen toteutus aloitettiin tekemällä ensimmäiseksi skannaus ulkoverkosta TietoAkselin ulkoverkon rajapintaan. Tämän jälkeen skannauksia suoritettiin sisäverkosta ensin yhteen sekä sen jälkeen useampaan sisäverkossa sijaitsevaan pääte- ja aktiivilaitteeseen. Opinnäytetyössä ei sen rajauksen kannalta käydä läpi jokaista toimipistettä. Jyväskylän toimipisteelle tehtävistä verkko- ja porttiskannauksen tuloksia voidaan hyödyntää tarpeellisin osin myöhemmin myös muille toimipisteille.

## 4.3 Kohteet

Ensimmäiseksi kohteeksi valittiin TietoAkselin Jyväskylän toimipisteen ulkoverkon IP-osoite. Ulkoverkosta tehtävä skannaus toteutettiin erillisen 4G-yhteyden avulla. Ulkoverkon skannauksella erillisestä verkosta pystyttiin samalla simuloimaan muiden tahojen tekemää skannausta.

Toiseksi tarkastelun kohteeksi valittiin yksi aktiivisessa työkäytössä oleva päätelaite, joka sijaitsee yrityksen työasemaverkossa. Päätelaitteelle ei tarvinnut tehdä mitään erillisiä valmisteluja, vaan skannaus suoritettiin siihen suoraan yrityksen sisäverkosta. Kolmas skannaus suoritettiin toimiston verkossa olevaan segmenttiin, jossa sijaitsi päätelaitteita, tulostimia, kytkimiä ja muita verkon laitteita. Toimeksiantaja oli teettännyt yrityksen verkkotopologiasta tuoreen kuvan, josta ilmenee miten käytössä olevat laitteet ovat kytkettyinä. Kuviosta 4 näkee, miten Jyväskylän toimipisteen toimistoverkko on toteutettu. Kuvio selittää toimipisteen verkon rakenteen pääpiirteittäin.





Kuvio 4. Toimipisteen verkon rakenne

#### 4.4 Vertailuun valitut ohjelmistot

Toimeksiannon mukaisten rajausten ja haluttujen ominaisuuksien täyttäviä ohjelmistoja löytyi verkosta useita kymmeniä kappaleita. Tärkeimpiä ominaisuuksia, mitä valitulta ohjelmistolta täytyi löytyä, olivat verkon ja porttien skannauksen suorittaminen, laitteiden löytäminen verkosta, päivitysten tunnistaminen ja tunnettujen haavoittuvuuksien löytäminen.

Näitä ominaisuuksia tukevia ohjelmistoja verkosta löytyi kattavasti, mutta erilliseen vertailuun valittiin OpenVAS, Nessus ja Nexpose. Jokainen valituista ohjelmistoista oli saanut positiivisia arvosteluja useilta verkosta löytyviltä eri sivustoilta. Ohjelmistojen välille suoritettiin ominaisuusvertailu, jonka tavoitteena oli saada tarkka käsitys siitä, mihin valitut ohjelmistot pystyvät ja voisiko niistä mahdollisesti olla hyötyä verkon tilan selvityksessä tai kehityksessä. Ohjelmistojen yhdistetty käyttö testauksessa tarkempien ja ajantasaisempien tulosten saamiseksi olisi myös mahdollista.

## OpenVAS

OpenVAS on ominaisuuksiltaan laaja haavoittuvuusskannauksen ja haavoittuvuuksien hallintaohjelmisto. Ohjelmisto tukee tunnistautumistestausta käyttäen ennakkoon sille annettuja tunnuksia sekä usean eri protokollan ja palvelun havaitsemista. Se on avoimeen lähdekoodiin perustuva, ilmainen ohjelmisto. Sen on kehittänyt joukko tietoturva-asiantuntijoita sekä aktiivinen yhteisö. OpenVAS käyttää automaattisesti päivittyvää sen yhteisön ylläpitävää haavoittuvuuskantaa. GNU-lisenssin (General Public License) alla olevan ilmaisen haavoittuvuuskannan aktiivinen päivitys lopetettiin 2017. Tarjolla on myös maksullinen versio, jonka kantaa päivitetään useammin ja joka tarjoaa käyttäjilleen erillisen tuen. Ohjelmistoa on mahdollista käyttää komentoriviltä tai web-käyttöliittymältä. (OpenVAS – Open Vulnerability Assessment System 2019)

## Nessus

Nessus on Tenable Network Securityn tuottama yksi suosituimmista haavoittuvuus työkaluista, sillä on yli kaksi miljoonaa latauskertaa. Ohjelmisto irtautui OpenVAS:sta vuonna 2005, kun sen lähdekoodi muuttui suljetuksi. Nessus tarjoaa vain kokeilu- tai maksullista versiota. Työkalu tunnistaa tunnettuja haavoittuvuuksia yli 45 000 kappaletta. Nessuksella voidaan käyttää myös valmiiksi tehtyjä pohjia tunnettujen haavoittuvuuksien havainnointiin.

Nessus luokittelee haavoittuvuudet viiteen eri kategoriaan: *Info*, *Low*, *Medium*, *High* ja *Critical*. Jossain tapauksissa haavoittuvuuksia voidaan kuvata myös *Mixed*-tyyppisenä, joka viittaa usean haavoittuvuuden sekoittumisen tai yhdistämisen toisiinsa. Luokittelu muodostuu haavoittuvuuden CVSSv2 -arvon mukaan. Nessuksen tuottamissa raporteissa haavoittuvuuksista annetaan myös CVSS Base -arvo sekä CVSS v3.0 -arvo. Verkon ja porttien skannaukseen tarkoitetuilla valmiilla pohjilla on mahdollista esimerkiksi testata konfiguraation toteutumista CIS-käytänteisiin perustuen. Käyttäjätunnusten avulla ohjelmistolla voidaan myös testata esimerkiksi kohteelta löytyvien sovellusten päivitysten ajantasaisuutta. (Nessus Professional 2019.)

## Nexpose

Rapid7 Nexpose on haavoittuvuustyökalu, jolla on ilmainen Community sekä maksulliset On-Premises ja InsightVM -versiot. Työkalu tunnistaa aktiiviset palvelut, portit ja kohteella toimivat sovellukset. Maksullisella versiolla voidaan kerätä tietoa, monitoroida ja analysoida verkkoa ja siihen liitettyjä laitteita. Työkalu tukee useita lisäosia ja se on yhdistettävissä Amazon:n ja VMware:n kanssa. Uhkia sisältävä kanta ja integroitava Metasploit antavat käyttäjälle tarkemman kuvan löytyneistä haavoittuvuuksista. Nexpose havaitsee uudet verkkoon liitetyt laitteet ja suorittaa niihin automaattisen skannauksen. Ohjelmisto tarjoaa myös valmiit kehitys ja parannusehdotukset liittyen verkosta löytyneisiin riskeihin ja haavoittuvuuksiin. (Nexpose 2019.)

## 4.5 Vertailu

Taulukkoon 2 tehtiin vertailu ohjelmistojen ominaisuuksista OpenVAS, Nessus ja Nexpose välille. Vertailussa otettiin kantaan yleisten ja toimeksiannossa määriteltyjen ominaisuuksien perusteella. Ominaisuudet valittiin käyttötarkoituksen ja tarpeen mukaan, sillä haluttiin selvittää, mikä ohjelmisto sopisi parhaiten opinnäytetyön tarpeisiin.

Taulukko 2. Haavoittuvuusskannaus -ohjelmistojen vertailu

	Nessus Professional	OpenVAS	Nexpose
Maksullinen	Kyllä	Ei	Kyllä
Tuetut käyttöjärjestelmät	Windows, Linux, MAC OS	Windows, Linux	Windows, Linux
Laitteiden löytäminen	Kyllä	Kyllä	Kyllä
Laitteiden merkitseminen	Ei	Kyllä	Kyllä
Verkon skannaus	Kyllä	Kyllä	Kyllä
Päivitystenhallinta	Ei	Ei	Kyllä
Web-skannaus	Kyllä	Kyllä	Ei
Haavoittuvuuksien löytäminen	Kyllä	Kyllä	Kyllä
Skannaustulosten vienti	PDF, HTML, CSV, Nessus DB	PDF, CSV, XLS, Docx	PDF, HTML, RTF, XML, XLS, CVS

Taulukon tulosten perusteella, jokainen ohjelmisto vaikutti pääperiaatteeltaan suhteellisen samanlaisesta. Nessus on tuotteista ladatuin. OpenVAS puolestaan tarjoaa myös ilmaisen version ja sen takia soveltuu toimeksiannon asettamiin tavoitteisiin hyvin. Sen ilmaisversion haavoittuvuuskanta ei kuitenkaan enää ole täysin ajantasainen. Nessus tarjosi seitsemän päivän kokeiluversion, jota oli myös mahdollista hyödyntää. Nexpose vaikutti myös lupaavalta työkalulta, vaikka se ei ollut ennestään

tuttu. Ominaisuuksien osalta se olisi myös mahdollisesti yksi hyvä ratkaisu työssä käytettäväksi haavoittuvuuskanneriksi. Jokaisen ohjelmiston avulla oli mahdollista tarkastella skannaustuloksia PDF-tiedostomuodossa, mikä helpottaa tulosten koostamista yhteen ja niiden selkeämpää tarkastelua ja analysointia.

Vertailun pohjalta ja toimeksiannon vaatimusten perusteella työssä käytettäviksi työkaluiksi valittiin Nessus ja OpenVAS. OpenVAS avulla skannauksia on mahdollista tehdä ilmaiseksi ja Nessus tarjosi seitsemän päivän kokeiluversion. Skannaustuloksista saisi tarkempaa dataa, jos kumpaakin työkalua käytettäisiin samalla tavalla. Työkalujen antamien tulosten pohjalta olisi myös mahdollista tehdä koottu raportti, josta selviäisi työkalujen antamat tulokset sekä niistä löytyvät erot. Jos Nessus vaikuttaisi huomattavasti paremmalta ja tarpeelliselta, olisi toimeksiantajalla mahdollisesti hyvät perustelut, ottaa se myös halutessaan pidempi aikaiseen käyttöön.

## **5 Nykytilan analysointi**

### **5.1 Tietoverkon rakenne**

Toimeksiantajan tietoverkon dokumentointi oli päivitetty etukäteen ajan tasalle opinnäytetyön aloituksen yhteydessä, myös verkossa olevia eri komponentteja oli vaihdettu sekä päivitetty. Verkkoon oli myös lähiaikoina lisätty useita aktiivi- ja päätelaitteita. Kaikki laitteet olivat dokumentoituina yrityksen omaan laitekantaan. Laitekannasta oli mahdollista tarkastella pääte- ja aktiivilaitteiden käyttöönoton päivämääriä ja yleistä tietoa laitteesta. Verkossa toimivien palveluiden tarkkaa määrää tai palveluiden tyyppiä ei ollut dokumentoitu uusiempien muutosten myötä. Tärkeimmät yleiset palvelut olivat kuitenkin etukäteen tiedossa.

Tietoverkko toimipisteellä koostuu verkko-operaattorin toimittamasta yhteydestä, useista eri aktiivilaitteista, työasemista, monitoimilaitteista ja muista verkon laitteista. Verkko oli jaettuna useisiin eri osiin laitteiden käyttötarkoituksen ja käyttäjäryhmän mukaisesti. Verkon hallintaa oli toteutettu useilla eri virtuaalilähiverkoilla

(engl. Virtual LAN). Käyttäjien pääsyä verkossa oli rajattu käyttäjän tarpeiden mukaan.

Verkossa olevien yleisten palveluiden, kuten DNS, DHCP sekä Active Directory lisäksi verkkoon oli asennettu esimerkiksi tiedostopalvelimella olevia levy- ja tiedostojakoja, tulostuspalveluita, Remote Desktop -palveluita ja virtualisointipalveluita. Avoimien palveluiden ja porttien määrä ei ollut etukäteen tarkalleen tiedossa. Palomuurille luoduista säännöistä sekä palomuurin lokista oli etukäteen mahdollista tarkistaa, mikä liikenne oli sallittua ja mikä oli estetty muurilla. Palomuurilta pystyttiin myös tarkastelemaan viikkotasolla sallitun ja estetyn liikenteen sekä käytettyjen palveluiden määrää.

## 5.2 Kohteiden tunnistus

Verkon laitteiden tunnistukseen liittyvä skannaus kohdistui pääasiallisesti verkosta löytyviin palveluihin ja portteihin sekä päätelaitteisiin ja niiden välisiin aktiivilaitteisiin. Yksi skannaus kohdistui ulkoverkosta tehtävään skannaukseen TietoAkselin ulkonverkon rajapintaan. Toinen skannauksen kohde oli yksittäinen sisäverkossa oleva kannettava tietokone. Yksittäisen laitteen skannaus antaisi hyvää pohjatietoa ennen isomman skannauksen suorittamista sisäverkkoon. Kolmas skannauksen kohde suoritettiin TietoAkselin toimistoverkosta etukäteen valittuun erilliseen verkon segmenttiin. Kyseisestä verkosta löytyvien laitteiden tarkka määrä ei ollut etukäteen tiedossa. Määrä vaihteli päivittäin työntekijöiden paikalla olon mukaan.

Ennen skannausta laitekannasta pystyttiin tarkistamaan, mitkä laitteet verkosta pitäisi löytyä. Skannauksen kohteeksi haluttiin kaikki kyseistä verkosta löytyvät laitteet. Etukäteen oli myös tiedossa, etteivät kaikki toimipisteen laitteet ole mahdollisesti kytkettynä verkkoon skannauksia suoritettaessa. Yrityksellä on pääasiallisesti käytössään Windows-käyttöjärjestelmän laitteita, myös muutama Linux ja Mac OS -laite. Kumpakin aikaisemmin valittua työkalua voitiin käyttää kaikkiin kolmeen eri tyyppiin skannaukseen.

### 5.3 Tietoverkon Baseline

Toimipisteen palomuurilta oli mahdollista tarkastella viikottasolla eniten käytettyjä palveluita, niiden käyttämiä portteja ja liikkuneen datan määrää. Myös eri sovellusten käyttöä ja niiden käyttämän datan määrää pystyttiin tarkastelemaan kuviosta 5 pystyttiin huomaamaan, että suurin käyttö oli kohdistunut portteihin 443, 445 ja 80. Palomuurilta saatavat raportit eivät kuitenkaan aina sisällä täysin tarkkaa tietoa, sillä jokaista palvelua ei ole etukäteen tarkasti tunnistettu.

TOP10 Services						
Total packets: 574 407 929						
Total traffic: 282.8 GB						
	Service Name	Protocol	Service Port	Packets	Traffic	%
1	[REDACTED]	TCP	443	207 385 761	103.0 GB	36.41 %
2	[REDACTED]	TCP	445	164 933 866	65.1 GB	23.01 %
3	[REDACTED]	TCP	80	45 080 349	42.6 GB	15.05 %
4	[REDACTED]	TCP	49155	42 168 119	26.5 GB	9.36 %
5	[REDACTED]	UDP	443	37 521 603	18.2 GB	6.44 %
6	[REDACTED]	TCP	389	21 553 920	11.1 GB	3.92 %
7	[REDACTED]	TCP	5020	8 462 589	6.5 GB	2.29 %
8	[REDACTED]	UDP	3410	8 341 489	2.1 GB	0.74 %
9	[REDACTED]	UDP	514	6 590 231	1.8 GB	0.65 %
10	[REDACTED]	TCP	9100	1 486 628	1.2 GB	0.41 %

Kuvio 5. Käytetyimmät palvelut

Palomuurin kautta liikkuneen datan määrä oli vaihdellut viikoittain huomattavia määriä. Ennen toimipisteen verkkoon tehtäviä skannauksia, käytettyjen palveluiden määrä oli kuitenkin tärkeä tiedostaa etukäteen, että skannausten jälkeen voidaan nähdä, kuinka paljon verkon skannaukset voivat mahdollisesti rasittaa toimipisteen eri verkon osia ja sieltä löytyviä laitteita. Taulukkoon 3 kerättiin viikoittain liikkuneen datan ja käsiteltyjen yhteyksien määrä. Ulkoverkosta tehtävä skannaus kohdistui palomuurille ja saattaa mahdollisesti rasittaa sitä.

Taulukko 3. Liikkuneen datan määrä

Päivämäärä	Liikkuneen datan määrä	Käsitellyt yhteydet
22.6.2019	280.3 GB	7 176 728
15.6.2019	443.0 GB	8 681 815
8.6.2019	328.2 GB	8 932 410
25.5.2019	357.4 GB	7 775 811
18.5.2019	410.1 GB	9 588 288
11.5.2019	460.2 GB	10 131 721

## 6 Tekninen toteutus

### 6.1 Yleistä

Tekninen osuus toteutettiin asentamalla ensiksi Kali Linuxille OpenVAS ja tekemällä sillä ensin skannaus toimipisteen ulkoverkon osoitteeseen. Tämän jälkeen skannaus suoritettiin satunnaiseen toimipisteellä sijaitsevaan päätelaitteeseen. Tämän päätelaitteen jälkeen skannaus suoritettiin yhteen toimipisteen verkosta löytyvään segmenttiin. Skannausten aikana löydetyt havainnot otettiin talteen myöhempää tarkastelua varten.

Toinen osuus koostui Tenablen Nessus -työkalulla tehtäviin skannauksiin. Skannaukset toteutettiin OpenVAS:lla tehtyjen skannausten tapaan, ensin ulkoverkosta tehtyyn skannaukseen ja sen jälkeen yksittäiseen työasemaan sekä lopuksi vielä yhteen verkon segmenttiin. Nessuksella oli myös mahdollista tehdä skannaus liittyen ohjelmiston päivitysten puuttumiseen. Löydetyt havainnot kerättiin talteen. Kummankin työkalun käytön jälkeen, syntyneitä tuloksia oli mahdollista verrata keskenään ja tehdä havaintoja niiden toiminnasta sekä ominaisuuksista. Taulukossa 4 näkyy teknisen toteutuksen järjestys.

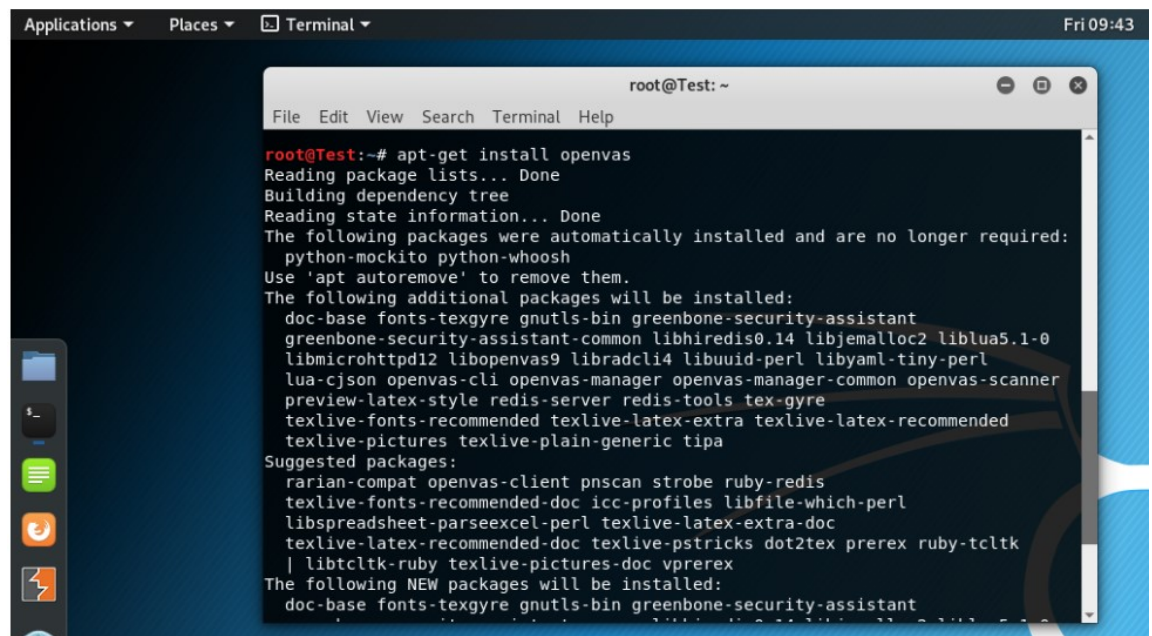
Taulukko 4. Teknisen toteutuksen järjestys

Ohjelmisto	Kohde
OpenVAS	Ulkoverkon julkinen IP-osoite
OpenVAS	Yksittäinen päätelaite
OpenVAS	Sisäverkon segmentti
Nessus	Ulkoverkon julkinen IP-osoite
Nessus	Yksittäinen päätelaite
Nessus	Sisäverkon segmentti

## 6.2 OpenVAS

### Asennus

OpenVAS asennusta varten yksittäiselle päätelaitteelle asennettiin Kali Linux 64-Bit versio 2019.2. OpenVAS olisi ollut myös mahdollista asentaa virtuaalikoneeksi, mutta opinnäytetyön kannalta se oli käytännöllisempi asentaa erilliseksi työasemaksi. Kalin uusimmasta versiosta työssä käytettävää skannaustyökalua ei löytynyt valmiina, joten se asennettiin erikseen. Kuviossa 6 näkyy OpenVAS asennus.



```

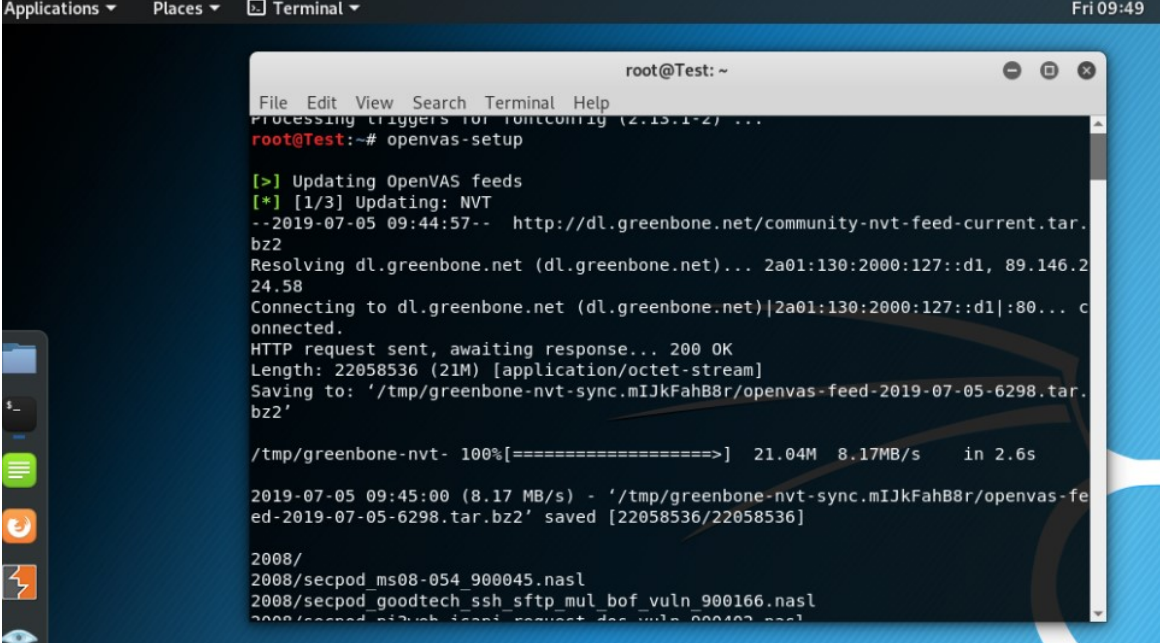
root@Test:~# apt-get install openvas
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  python-mockito python-whoosh
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  doc-base fonts-texgyre gnutls-bin greenbone-security-assistant
  greenbone-security-assistant-common libhiredis0.14 libjemalloc2 liblua5.1-0
  libmicrohttpd12 libopenvas9 libradcli4 libuuid-perl libyaml-tiny-perl
  lua-cjson openvas-cli openvas-manager openvas-manager-common openvas-scanner
  preview-latex-style redis-server redis-tools tex-gyre
  texlive-fonts-recommended texlive-latex-extra texlive-latex-recommended
  texlive-pictures texlive-plain-generic tipa
Suggested packages:
  rarian-compat openvas-client pncan strobe ruby-redis
  texlive-fonts-recommended-doc icc-profiles libfile-which-perl
  libspreadsheet-parseexcel-perl texlive-latex-extra-doc
  texlive-latex-recommended-doc texlive-pstricks dot2tex prerex ruby-tcltk
  | libtcltk-ruby texlive-pictures-doc vprerex
The following NEW packages will be installed:
  doc-base fonts-texgyre gnutls-bin greenbone-security-assistant

```

Kuvio 6. OpenVAS, asennus



Työkalu oli nopea ja yksinkertainen asentaa. Käyttöönotto tapahtui myös yhdellä erilisellä käskyllä. Käyttöönoton yhteydessä ohjelmiston haavoittuvuuskanta päivittyi hakemalla verkosta siihen uusimmat päivitykset. Kuviossa 7 näkyy, miten työkalun käyttöönotto tapahtui `apt-get install openvas` -käskyllä.



```

root@Test: ~
File Edit View Search Terminal Help
Processing triggers for fontconfig (2.13.1-2) ...
root@Test:~# openvas-setup

[>] Updating OpenVAS feeds
[*] [1/3] Updating: NVT
--2019-07-05 09:44:57-- http://dl.greenbone.net/community-nvt-feed-current.tar.
bz2
Resolving dl.greenbone.net (dl.greenbone.net)... 2a01:130:2000:127::d1, 89.146.2
24.58
Connecting to dl.greenbone.net (dl.greenbone.net)|2a01:130:2000:127::d1|:80... c
onnected.
HTTP request sent, awaiting response... 200 OK
Length: 22058536 (21M) [application/octet-stream]
Saving to: '/tmp/greenbone-nvt-sync.mIJkFahB8r/openvas-feed-2019-07-05-6298.tar.
bz2'

/tmp/greenbone-nvt- 100%[=====] 21.04M 8.17MB/s in 2.6s

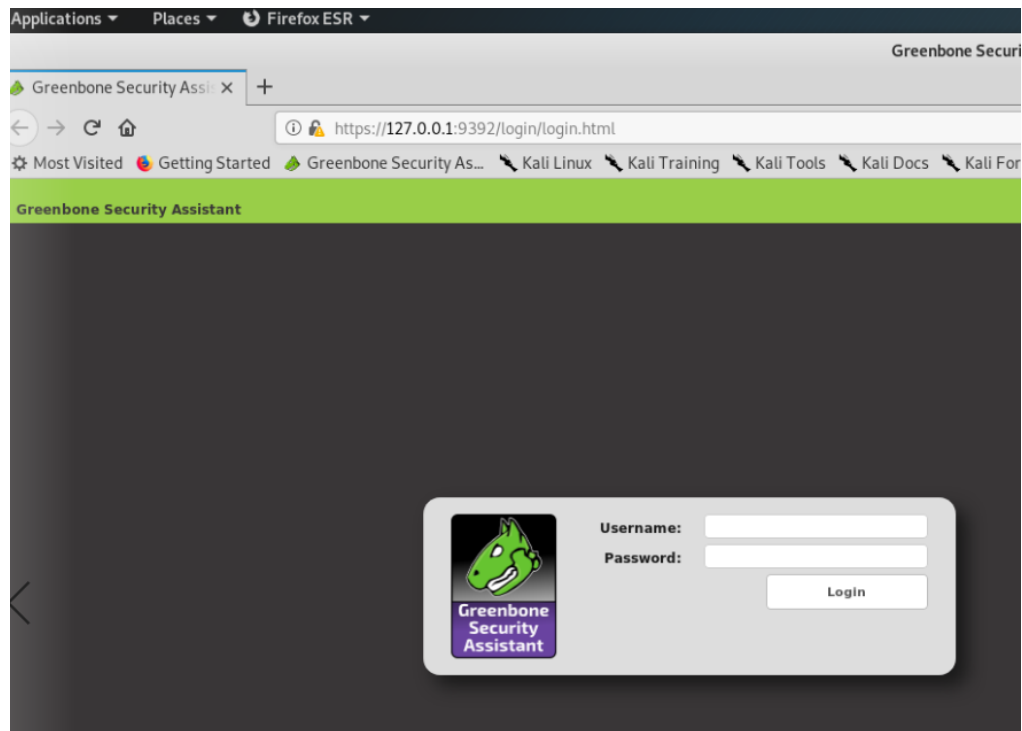
2019-07-05 09:45:00 (8.17 MB/s) - '/tmp/greenbone-nvt-sync.mIJkFahB8r/openvas-fe
ed-2019-07-05-6298.tar.bz2' saved [22058536/22058536]

2008/
2008/secpod_ms08-054_900045.nasl
2008/secpod_goodtech_ssh_sftp_mul_bof_vuln_900166.nasl
2008/secpod_nitish_feed_request_des_vuln_900103.nasl

```

Kuvio 7. OpenVAS, käyttöönotto

`Openvas-setup` -käskyn jälkeen työkalu latsi useita eri päivityksiä ja samalla loi käyttäjätunnuksen, jonka avulla kirjautuminen verkkosivulla tapahtui. Asennuksen jälkeen palvelua ei tarvinnut käynnistää erikseen, vaan sen oli käynnistynyt jo käyttöönoton ja asennuksen yhteydessä. Käyttöönoton valmistuttua selain yhdisti suoraan `localhost:n 127.0.0.1:9392` -osoitteeseen, josta kirjautuminen ohjelmistoon tapahtui. Kuvioista 8 näkee OpenVAS etusivun ensimmäisen kirjautumisen yhteydessä. Ensimmäisellä kerralla kirjautumiseen käytettiin tunnuksia, jotka käyttäjälle jaettiin asennuksen yhteydessä. Tämän jälkeen ohjelmiston käyttäjän kannattaa vaihtaa salasana.



Kuvio 8. OpenVAS, etusivu

Kirjautuminen OpenVAS:n onnistui asennuksen aikana jaetuilla tunnuksilla. Työkalun pystyi myös käynnistämään erillisellä *openvas-start* -komennolla komentoriviltä koneen sammuttamisen tai uudelleen käynnistytksen jälkeen. Asennus ja käyttöönotto sujuivat vaivattomasti ja skannaukset pystyttiin aloittamaan nopeasti ilman suurempia isompia ongelmia käyttöönotossa.

### Skannaus ulkoverkosta

Ennen ensimmäisen skannauksen aloittamista Kali Linux -pöytälaite liitettiin erilliseen 4G-verkkoon, minkä jälkeen sillä oli mahdollista tehdä skannausta ulkoverkosta. Toimipisteen ulkoverkon rajapinnan IP-osoite oli etukäteen tiedossa. Kuvio 9 näkyy OpenVAS:lla luotu ensimmäinen skannaustehtävä. Luotuun tehtävään ei annettu erillisiä tunnuksia, sillä haluttiin mallintaa ulkopuolisen tahon tekemää ns. Black Box -skannausta ilman, että kohteesta oli etukäteen tiedossa tunnuksia tai rajapinnassa toimivia palveluita sekä portteja.

Full and fast -konfiguraatio skannaa yleisesti käytössä olevia tunnettuja portteja noin 4480 kappaletta. Erilaisia konfiguraatioita oli useita, mutta valittu konfiguraatio oli

sopivin tähän tilanteeseen. Mahdollista olisi ollut myös valita esimerkiksi kaikkien tiedossa olevien porttien skannaus, mutta se ei olisi ollut ajallisesti järkevää tehdyn työn kannalta.

Kuvio 9. Ulkoverkosta suoritettu skannaus

Skannauksen alkaessa palomuurin loki otettiin seurantaan. Lokitapahtumista oli mahdollista nähdä, miten palomuri ja sen tunkeutumisen esto -toiminnot reagoisivat. Skannaus valmistui muutamassa minuutissa ja lokitapahtumia seuraamalla havaittiin, että muuri esti kaiken porttiskannaukseen liittyvän liikenteen. Kuviosta 10 ja kuviosta 11 näkyy kuvankaappaukset palomuurin ja Intrusion Prevention System (IPS) lokista.

12:03:22	Default DROP	TCP	85.76.51.112:45193	→ [redacted]
12:03:22	Default DROP	TCP	85.76.51.112:44878	→ [redacted]
12:03:22	Default DROP	TCP	85.76.51.112:49316	→ [redacted]

Kuvio 10. Palomuurin loki

```

2019:07:05-12:03:09 jkl-1 ulogd[27998]: id="2102" severity="info" sys="SecureNet" sub="ips" name="portscan detected" action="portscan"
2019:07:05-12:03:09 jkl-1 ulogd[27998]: id="2102" severity="info" sys="SecureNet" sub="ips" name="portscan detected" action="portscan"
2019:07:05-12:03:11 jkl-1 ulogd[27998]: id="2102" severity="info" sys="SecureNet" sub="ips" name="portscan detected" action="portscan"
2019:07:05-12:03:11 jkl-1 ulogd[27998]: id="2102" severity="info" sys="SecureNet" sub="ips" name="portscan detected" action="portscan"
2019:07:05-12:03:11 jkl-1 ulogd[27998]: id="2102" severity="info" sys="SecureNet" sub="ips" name="portscan detected" action="portscan"
2019:07:05-12:03:11 jkl-1 ulogd[27998]: id="2102" severity="info" sys="SecureNet" sub="ips" name="portscan detected" action="portscan"

```

## Kuvio 11. IPS-loki

OpenVAS-ohjelmisto ei saanut tuotettua erillisiä ulkoverkon skannaustuloksia, ainoastaan kaksi Log-tason merkintää, joissa mainittiin, ettei skannausta voitu suorittaa loppuun. Skannaus ei myöskään pystynyt tunnistamaan ulkoverkon osoitteesta löytyviä palveluita, siellä toimivaa käyttöjärjestelmää tai auki olevia portteja. Kuviosta 12 näkyy koonti tehdystä skannauksesta.

Task	Severity	Scan Results			
		High	Medium	Low	Log
External_Scan_JKL	0.0 (Log)	0	0	0	2

## Kuvio 12. Ulkoverkon skannauksen tulokset

### Skannaus päätelaitteelle

Ennen skannauksen aloittamista, Kali Linux liitettiin samaan verkkoon toisen päätelaitteen kanssa. Kone sai IP-osoitteen samasta verkosta, sekä *ping* -komennolla voitiin testata, että koneet vastasivat toistensa kyselyihin. Yhdelle yksittäiselle laitteelle tehtävässä skannauksessa oli mahdollista hyödyntää OpenVAS ominaisuutta, jossa skannaustyökalulle voidaan kertoa kohde koneen paikalliset tunnukset, jotta skannauksesta saadaan syvällisempi ja samalla saadaan tarkempia tuloksia. Tunnukset skannausta varten voidaan luoda erikseen New Credentials -toiminnon avulla. Alla olevassa kuviossa 13 näkyy tunnusten luominen skannausta varten.

Kuvio 13. Tunnusten luominen

Tunnusten lisäämisen jälkeen niitä oli mahdollista hyödyntää sisäverkkoon tehtävään skannaukseen päätelaitteelle. Tunnukset olivat yksittäisen koneen paikalliset tunnukset, joten niitä ei voitu hyödyntää kuin pelkästään kyseiselle laitteelle. Kuviossa 14 näkyy miten SSH- ja SMB-tunnukset olivat valittuna aikaisemmin tehtyihin Local Admin -tunnuksiin.

Kuvio 14. Skannaus tunnusten avulla

Skannaus tuotti vain yhden Medium-tason haavoittuvuuden ja 16 Log-tason merkintää. Kuviossa 15 näkyy skannauksen tulokset eriteltyinä. Löydetylle haavoittuvuudelle oli annettu CVSS -arvoksi 5.0 eli keskitason haavoittuvuus. Raportin tarkempi tutkiminen paljasti, että tuloksista löytyi myös yksi Low-tason merkintä, joka ei suoraan näkynyt tuloksen esikatselusta. Haavoittuvuuden CVSS -pisteet olivat 2.6.

Task	Severity	Scan Results			
		High	Medium	Low	Log
Internal_Scan_JKL_Credentials	5.0 (Medium)	0	1	0	16

Kuvio 15. Sisäverkon skannaus, yksittäinen päätelaite

### Skannaus sisäverkon segmenttiin

Kali Linux liitettiin toiseen verkon segmenttiin, jossa käyttäjiä oli päivän aikana noin 10 – 15. Skannaus tehtiin ilman tunnuksia, sillä verkosta löytyi useita laitteita. Verkosta löytyi vain sinne kuuluvia päätelaitteita, joissa havaittiin samat ongelmakohdat kuin aikaisemmin tehdystä yksittäisen laitteen skannauksessa. Kuviossa 16 näkyy sisäverkon segmentistä löytyneiden haavoittuvuuksien määrä.

Task	Severity	Scan Results			
		High	Medium	Low	Log
Internal_Scan_Jkl_Hr	5.0 (Medium)	0	10	1	104

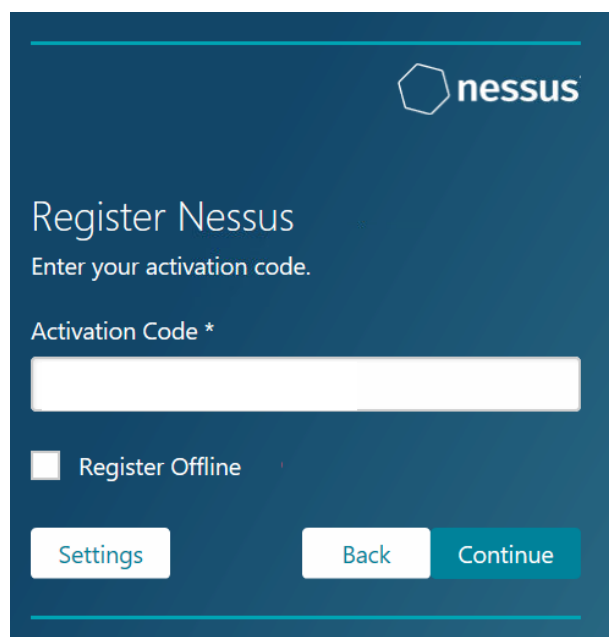
Kuvio 16. Sisäverkon skannaus, verkon segmentti

Medium-tason haavoittuvuus oli täysin sama 5.0 CVSS -arvoinen haavoittuvuus. Myös yksi Low-tason haavoittuvuus liittyen laitteilta löytyneisiin TCP-aikaleimoihin. Log-tason merkintöjä oli yhteensä 104 kappaletta. Yksittäisen koneen ja isomman koneiden ryhmän tulokset olivat lähes samat, vaikka toisessa käytettiin erillisiä tunnuksia.

## 6.3 Nessus

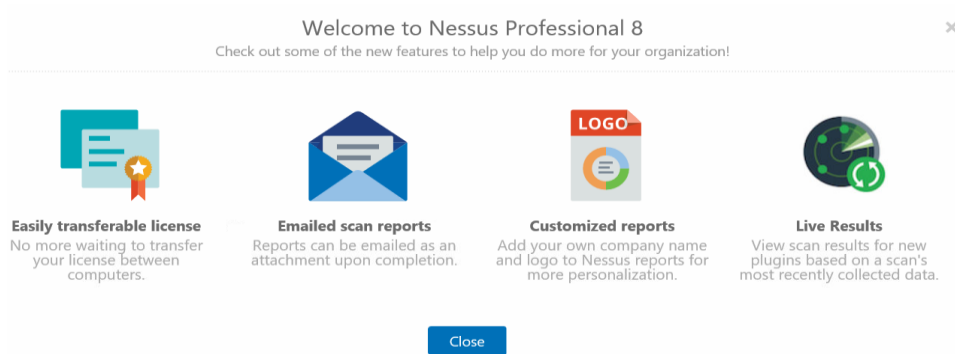
### Asennus

Ohjelmiston asennus tapahtui msi-paketin avulla lataamalla paketti Nessuksen sivuilta. Työssä käytettiin Windows 10 64-bittistä versiota paremman yhteensopivuuden takia. Ennen asennuksen aloittamista ohjelmisto vaati käyttäjän rekisteröinnin ja sähköpostiosoitteen. Sähköpostiin saapui Nessukselta erillinen linkki, jonka kautta aktivointikoodin sai ohjelmiston asennusta varten. Kuviossa 17 näkyy, miten asennuksen yhteydessä kysytään aikaisemmin saatua aktivointikoodia.



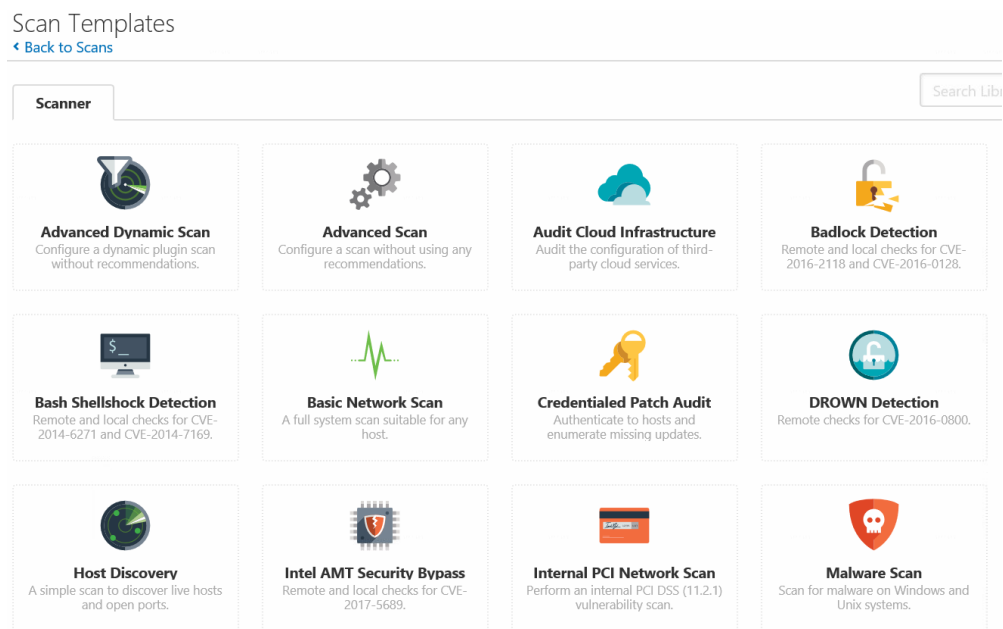
Kuvio 17. Nessuksen aktivointi

Aktivoinnin jälkeen ohjelmisto aloittaa asennuksen verkkoselaimen näkymässä. Ohjelmisto lataa uusimmat päivitykset ja mahdolliset puuttuvat lisäosat. Asennuksen suorittaminen onnistui suoraviivaisesti ja nopeasti. Samalla luotiin käyttäjätunnus palveluun. Asennuksen jälkeen selaimen <https://localhost:8834> -osoitteeseen avautui kuvion 18 mukainen näkymä ja ohjelmisto oli valmiina käytettäväksi. Ohjelmiston asennus hetkellä uusin versio oli 8.5.1. Ohjelmiston käynnistystä ja sammutusta pystyi hallitsemaan Windows-laitteilla palveluista (Services). Tenable Nessus näkyy erillisenä palveluna, jonka tilaa voidaan tarvittaessa muuttaa.



Kuvio 18. Nessus asennettuna

Nessus tarjoaa useita valmiita eri verkon ja laitteiden skannaukseen tarkoitettuja profiileja. Ohjelmiston Scan Templates -sivulta on mahdollista valita tilanteeseen sopivin vaihtoehto. Työssä käytettiin *Advanced Scan* -skannausprofiilia, sillä se soveltui parhaiten työn tavoitteisiin tehtäessä skannausta ensimmäistä kertaa. Toinen hyvä vaihtoehto olisi ollut *Advanced Dynamic Scan* -skannausprofiili, jonka avulla voidaan valita tarkemmin esimerkiksi mitä haavoittuvuuksia ei huomioida skannauksessa. Kuviossa 19 näkyy osa Nessuksen eri tarjoamista skannausvaihtoehdoista.



Kuvio 19. Skannauspohjat



## Skannaus ulkoverkosta

Windows 10 -pöytälaite liitettiin erilliseen 4G-verkkoon ja skannauksen kohteeksi asetettiin ulkoverkon rajapinnan IP-osoite. Skannauksen asetuksiin ei asetettu erillisiä tunnuksia, sillä haluttiin saada aikaan sama näkymä, joka muille skannauksia suorittaville tahoille näkyisi. Muihin perusasetuksiin ei ollut tarvetta tehdä muutoksia. Kuviossa 20 näkyy määritettynä yleiset asetukset ennen skannauksen aloitusta. Tallentamalla skannauksen asetukset Save -painikkeesta skannauksen profiiliin sekä asetukset pystyttiin tallentamaan.

The screenshot shows the 'General Settings' configuration page for a scan profile. The left sidebar contains a navigation menu with categories: BASIC (General, Schedule, Notifications), DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The main content area is titled 'General Settings' and includes the following fields:

- Name:** External\_Scan\_JKL
- Description:** Skannaus ulkoverkosta
- Folder:** My Scans
- Targets:** A text area containing a redacted IP address (represented by a black box).
- Upload Targets:** A button labeled 'Add File'.
- Post-Processing:** A checkbox for 'Live Results' which is currently unchecked. Below it is a note: 'Enabling this option will identify potential issues discovered by plugins added during updates without actively scanning targets.'

At the bottom of the window, there are two buttons: 'Save' and 'Cancel'.

Kuvio 20. Skannaus ulkoverkosta

Ulkoverkosta tehty skannaus jäi OpenVAS:n tapaan palomuurille kiinni. Kuvioissa 21 ja 22 näkyy esimerkkiä palomuriin ja IPS-lokiin jääneistä merkinnöistä. Eroina OpenVAS-skannauksiin, merkintöjä syntyi myös ICMP- ja UPD flood -havainnoista. Skannaus itsessään kesti aikaisempaa kauemmin. Skannattavien porttien määrä kyseisellä profiililla on oletuksena noin 4790 yleisesti käytössä olevaa porttia.

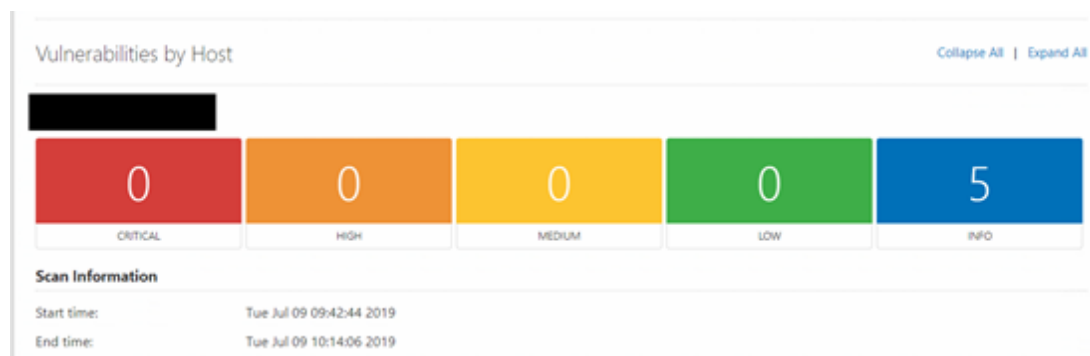
09:42:55	Default DROP	TCP	85.76.107.149:18977	→ [REDACTED]
09:42:55	Default DROP	TCP	85.76.107.149:13944	→ [REDACTED]
09:42:55	Default DROP	TCP	85.76.107.149:51724	→ [REDACTED]

Kuvio 21. Palomuurin loki

```
09:43:39 jkl-1 ulogd[27998]: id="2102" severity="info" sys="SecureNet" sub="ips" name="portscan detected" ;
09:43:39 jkl-1 ulogd[27998]: id="2103" severity="info" sys="SecureNet" sub="ips" name="SYN flood detected" ;
09:43:39 jkl-1 ulogd[27998]: id="2102" severity="info" sys="SecureNet" sub="ips" name="portscan detected" ;
09:43:40 jkl-1 ulogd[27998]: id="2103" severity="info" sys="SecureNet" sub="ips" name="SYN flood detected" ;
09:43:40 jkl-1 ulogd[27998]: id="2102" severity="info" sys="SecureNet" sub="ips" name="portscan detected" ;
```

Kuvio 22. IPS-loki

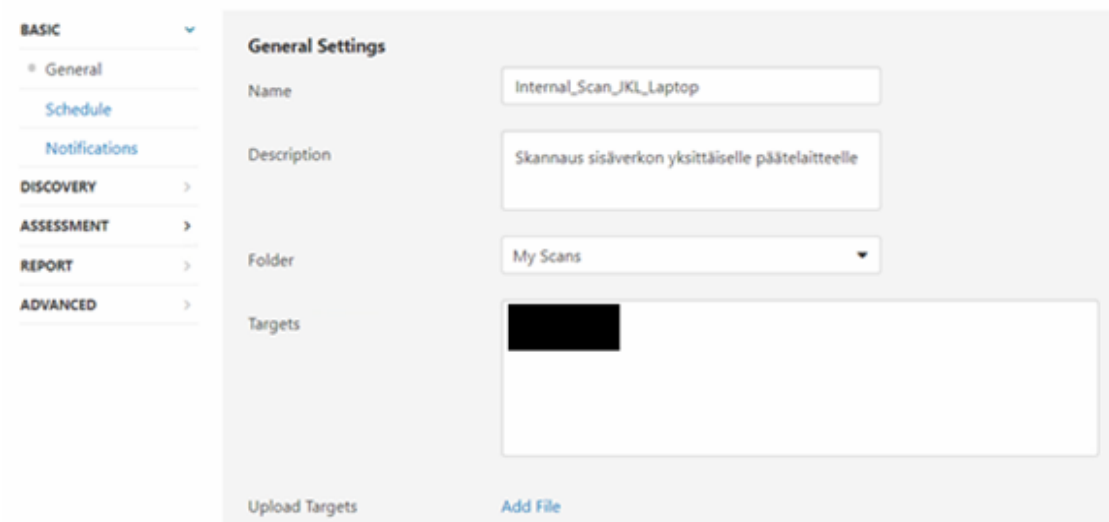
Skannauksen valmistuttua ohjelmisto antoi tulokseksi viisi Info-tason merkintää. Yhtäkään vakavampaa haavoittuvuutta tai puutetta ulkoverkon skannauksesta ei kyseisellä skannaustyyppillä ilmennyt. Info-tason merkinnöistä vain muutama oli työn kannalta oleellinen. Kuviossa 23 näkyy löydetty havainnot kootusti värikoodeihin.



Kuvio 23. Ulkoverkon skannauksen tulokset

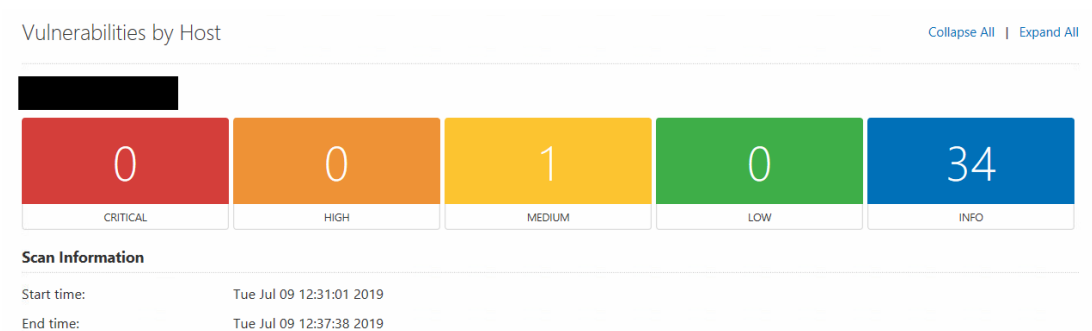
### Skannaus päätelaitteelle

Päätelaitteen skannausta varten Windows 10 -pöytälaite liitettiin takaisin toimipisteen sisäverkkoon. Samalla varmistettiin, että kohteena oleva päätelaite oli samassa verkossa ja koneilta sai yhteyden toisiinsa. Päätelaitteelle tehtävässä skannauksessa käytettiin samaa Advanced Scan -profiilia. Kuviossa 24 näkyy yleiset tiedot skannauksesta.



Kuvio 24. Skannaus päätelaitteelle

Skannauksen valmistuttua päätelaitteelta löytyi yhteensä 35 kappaletta haavoittuvuuksia, joista vain yksi oli Medium-tason haavoittuvuus. Haavoittuvuuden CVSS-pisteitys oli 5.3. Loput 34 kappaletta olivat Info-tason merkintöjä. Osa merkinnöistä ei ollut oleellisia opinnäytetyön kannalta. Suurin osa haavoittuvuuksista liittyi tiedostojakoihin ja erilaisiin oikeuksiin niiden ympärillä. Kuviossa 25 näkyy päätelaitteelta löydettyjen haavoittuvuuksien vakavuuden ja niihin liitetyt värikoodit.



Kuvio 25. Päätelaitteen skannauksen tulokset

## Skannaus käyttäjätunnusten avulla

Nessus:stä löytyvällä *Credentialed Patch Audit* -skannausprofiililla oli mahdollista selvittää käyttäjätunnusten avulla päätelaitteilta puuttuvia päivityksiä ohjelmistoista ja käyttöjärjestelmästä. Tätä skannausta varten Nessukseen piti määrittää erilliset paikalliset- tai domain-tunnukset. Kuvioissa 26 ja 27 näkyy skannauksen asetuksen sekä tunnusten määrittäminen. Tunnusten lisäämisen jälkeen skannaus voitiin aloittaa.

The screenshot shows the 'Settings' page in Nessus, specifically the 'Credentials' tab. The left sidebar has a menu with categories: BASIC (General, Schedule, Notifications), DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The main content area is titled 'General Settings' and contains the following fields:

- Name:** Internal\_Scan\_JKL\_Laptop\_Credentials
- Description:** Skannaus sisäverkon päätelaitteille käyttäjätunnusten avulla
- Folder:** My Scans
- Targets:** A large empty text area with a black redaction box at the top.

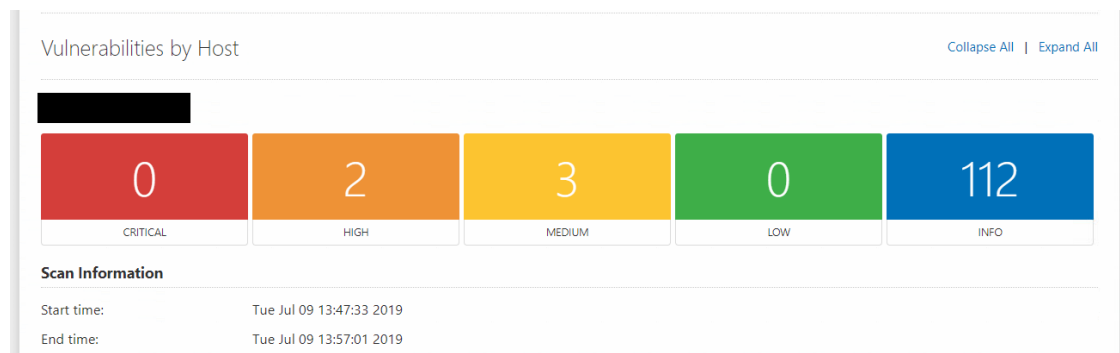
Kuvio 26. Skannaus käyttäjätunnuksilla

The screenshot shows the 'New Scan / Credentialed Patch Audit' page in Nessus, specifically the 'Credentials' tab. The left sidebar shows a list of categories: Host, Filter Credentials, SNMPv3 (1), SSH (∞), and Windows (∞). The main content area is titled 'Windows' and contains the following fields:

- Authentication method:** Password
- Username:** [Redacted]
- Password:** [Redacted]
- Domain:** [Empty]
- Global Credential Settings:**
  - Never send credentials in the clear

Kuvio 27. Käyttäjätunnusten lisääminen

Skannauksen avulla haavoittuvuuksia sekä yleisiä tietoja löytyi laitteesta huomattavasti enemmän kuin aikaisemmillä kerroilla käyttäjätunnusten ansiosta. Yhteensä haavoittuvuuksia löytyi 117 kappaletta, jotka Nessus rajasi 36 eri tyyppiin. Kaksi haavoittuvuudesta oli High -tasoa, kolme Medium -tasoa ja loput olivat Info -merkintöjä. High -tasojen CVSS -pisteet olivat 7.3 ja 7.2. Medium tasojen pisteet 6.5, 5.9 ja 5.0. Yhtä Medium-tason haavoittuvuudesta yhdisti neljä eri CVE -merkintää. Kuviossa 28 näkyy päätelaitteelta löydetyt haavoittuvuudet.



Kuvio 28. Päätelaitteen skannauksen tulokset, käyttäjätunnuksilla

### Skannaus sisäverkon segmenttiin

Windows 10 -pöytälaite siirrettiin samaan verkkoon, johon OpenVAS:lla suoritettu skannaus oli aikaisemmin tehty. Pöytälaite sai IP-osoitteen samasta verkosta ja skannaus pystyttiin suorittamaan käyttäen hyväksi aikaisemmin Nessukseen lisättyjä tunnuksia. Kuviossa 29 näkyvät tiedot skannauksesta. Kohteeksi pystyttiin määrittämään koko haluttu verkko käyttäen CIDR-notaatiota kertomaan skannattavan alueen koon.

**Settings** | Credentials | Compliance | Plugins

**BASIC** ▾

- General
- Schedule
- Notifications

**DISCOVERY** >

**ASSESSMENT** >

**REPORT** >

**ADVANCED** >

**General Settings**

Name: Internal\_Scan\_JKL\_Hr\_Credentials

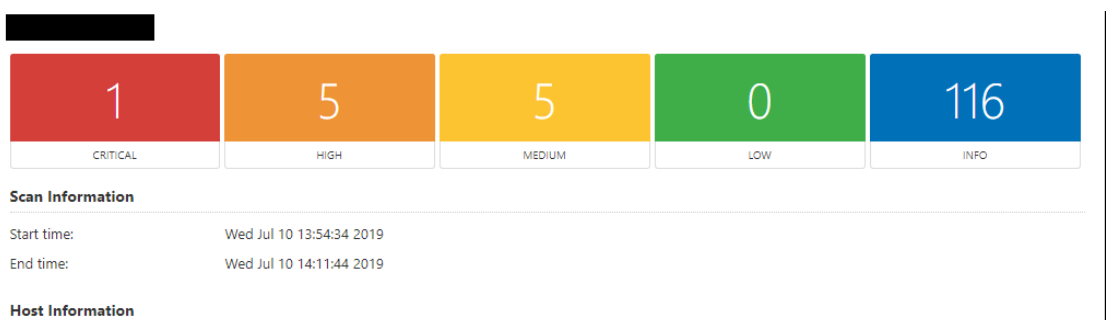
Description: Skannaus käyttäjätunnusten avulla

Folder: My Scans

Targets: [Redacted]

Kuvio 29. Verkon segmentin skannausasetukset

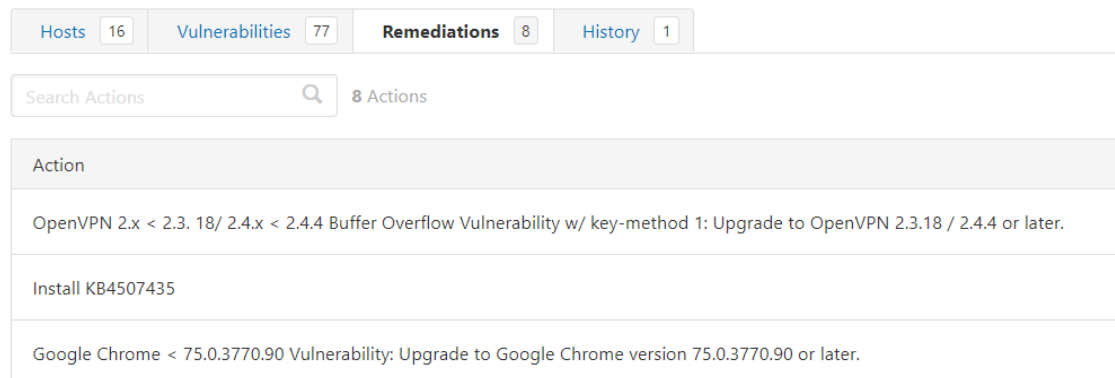
Skannauksen avulla kyseistä verkon osasta löytyi yhteensä 16 eri laitetta. Laitteista yksi oli aktiivilaite ja muut päätelaitteita. Erilaisia haavoittuvuuksia löytyi yhteensä 77 kappaletta. Info-tason merkintöjä löytyi yli 1600 kappaletta. Haavoittuvuuksista yksi oli kriittisen tason CVSS-arvoltaan 10.0. High-tason haavoittuvuuksia oli 10 kappaletta. Loput 66 kappaletta olivat Medium- ja Low-tason. Kuviossa 30 näkyy skannaus-tulokset yhdeltä yksittäiseltä päätelaitteelta.



Kuvio 30. Verkon segmentin skannauksen tulokset, yksittäinen laite

Aikaisempiin skannauksiin verrattuna tulokset poikkesivat määrällisesti huomattavan paljon verrattuna OpenVAS:lla tehtyihin skannauksiin. Nessus osasi suoraan tarjota

kahdeksan korjausehdotusta löydettyihin puutteisiin eri laitteille. Yksi ehdotus oli esimerkiksi asentaa yhdelle päätelaitteelle uusimmat Windows-turvallisuuspäivitykset muutamaan eri laitteeseen. Kuviossa 31 näkyy muutama esimerkki Nessuksen tarjoamista korjausehdotuksista. Skannausten yhteydessä olisi ollut mahdollista käyttää myös Live Results -toimintoa, joka tarjoaa tietoa uusista Nessukseen lisätyistä haavoittuvuuksista, ilman että samalaista skannausta tarvitsee heti ajaa uudelleen.



Kuvio 31. Nessuksen tarjoamat korjausehdotukset

## 7 Tulosten tarkastelu

### 7.1 Tutkimustulokset

Opinnäytetyön tulokseksi saatiin kattava määrä tietoa kohde organisaation toimipisteiden verkosta ja sieltä löytyvistä laitteista. Havaintoja syntyi useasta eri näkökulmasta ja kahdella eri ohjelmistolla. Kummatkin tekniseen toteutukseen valitut ohjelmat tuottivat työn kannalta oleellista tietoa yrityksen verkon ja laitteiden nykytilasta.

Kumpaakin eri tutkimuskysymykseen saatiin selkeä ja johdonmukainen vastaus työssä käytettyjen työkalujen avulla. Aktiivi- ja päätelaitteiden tunnistaminen ja selvitys onnistui sekä OpenVAS:lla, että Nessuksella. Kumpikin ohjelmisto tunnistasi verkon segmentistä sinne kuuluvat laitteet. Nessuksen avulla saatiin OpenVAS:a tarkemmin selville eri laitteiden käytössä olevat palvelut, portit ja protokollat. Käyttäjätunnusten

avulla Nessus tunnisti päätelaitteilta lähes kaikki niillä käytössä olleet yleisesti tunnetut palvelut ja ohjelmistot. Ohjelmisto löysi myös päivittämättömiä päätelaitteita. Kummallakin ohjelmistolla oli myös mahdollista selvittää ja löytää yleisesti tiedossa olevia haavoittuvuuksia. Nessus osasi myös yhdistää löydettyjä haavoittuvuuksia toisiinsa (Multiple Issues).

Teknisen toteutuksen jälkeen ohjelmistojen tuottamista raporteista oli mahdollista huomata merkittävä ero kahden eri ohjelmiston välillä. Yksi suurimmista eroista oli ulkoverkosta tehty skannaus. Nessus tunnisti sieltä yhden yksittäisen portin olevan auki. OpenVAS ei tätä porttia kuitenkaan saanut tunnistettua. Kummakin ohjelmiston avulla oli mahdollista tehdä skannauksia verkosta löytyviin laitteisiin käyttäjätunnusten avulla.

Nessuksella tämä skannaus onnistui helposti ja ohjelmisto pääsi käsiksi päätelaitteisiin ja sieltä löytyviin tiedosto- sekä levyjakoihin. OpenVAS tunnistautumisen ei toiminut, vaikka ohjelmistolle jaetut tunnukset olivat täysin identtiset Nessuksen tunnusten kanssa. Tunnukset syötettiin useassa eri muodossa. Raporttien sisältämä tieto vaihtelee ohjelmistojen välillä. OpenVAS tuotti Nessukseen verrattuna suppeamman raportin, joka ei ollut yhtä yksityiskohtainen kuin Nessus. Raporttien sisältö vaihteli myös esimerkiksi auki olevien porttien lukumäärässä sekä portin numerossa.

Tarkat skannauksista löydetty tulokset näkyvät opinnäytetyön liitteissä 1, 2 ja 3. Liitteet 1,2 ja 3 sisältävät tietoa skannatuista kohteista ja sieltä löytyneistä haavoittuvuuksista tai puutteista konfiguroinnissa. Haavoittuvuuden tai puutteen vakavuus on määritetty ohjelmiston käyttämän tason mukaan.

Ulkoverkon skannaus ei tuottanut lähes minkäänlaista rasitusta toimipisteen palomuurille. Palomuurin kuormitus pysyi prosentteina samassa luokassa mitä ns. normaalissa tilassa. Myöskään verkon yksittäiseen segmenttiin tehdyssä skannauksessa kytkimen tai päätelaitteiden toiminta ei hidastanut tai rasittunut. Päätelaitteille tehdyssä skannauksissa laitteiden toiminnassa ei ollut huomattavaa eroa, eikä sen käyttö hidastunut.



## 7.2 Kehitysehdotukset

Teknisen toteutuksen avulla OpenVAS:n ja Nessuksen tuottamista raporteista oli selkeää havaita tietoverkossa ja siellä olevissa laitteista löytyviä puutteita. Laitteilta löytyneet haavoittuvuudet liittyivät pääosin käytettävien ohjelmistojen vanhentuneisiin versioihin ja niistä löytyviin haavoittuvuuksiin. Liitteessä 4 on eritelty löydetty haavoittuvuuden kohde, kuvaus, CVE sekä korjausehdotus kyseiseen ongelma-kohtaan tai puutteeseen.

Liitteessä 5 on listattu avoimena sisäverkosta löytyneet portit. Porteille on ohjelmistojen (Nessus ja OpenVAS) avulla määritetty siellä toimivat protokolla, palvelu sekä palveluksen kuvaus. Suurin osa porteista on tarpeellisia ja ne liittyvät olennaista yrityksen käytössä oleviin ohjelmistoihin tai sen verkossa toimiviin palveluihin.

Tietoverkosta löytyneistä laitteista pystyttiin tekemään seuraavat havainnot:

- Ylimääräisten tarpeettomien porttien sulkimien
- Tärkeiden porttien liikenteen suojaaminen IP-filtteröinnillä
- Käytöstä poistuneiden tarpeettomien ohjelmien poistaminen päätelaitteilta
- Käytössä olevien vanhentuneiden ohjelmistoversioiden päivitys ajan tasalle
- Siirtyä pois ohjelmistoista, joihin ei ole enää tulossa päivityksiä

### **Jatkotoimenpiteet**

Opinnäytetyölle jatkokehityksen kannalta olisi hyvä tehdä tarpeelliset porttien ja siellä toimien palveluiden rajoitukset sekä liitteen 4 korjausehdotukset. Tämän jälkeen sisäverkkoon kannattaisi tehdä uudet portti- ja verkkoskannaukset samoilla skannausprofiileilla, jotta nähtäisiin, toimiiko skannausohjelmisto odotetulla tavalla sekä onko korjausehdotuksista ja ohjelmistojen päivityksestä ollut hyötyä. Samalla saataisiin selville, onko tietoverkosta löytyvistä laitteista ehtinyt paljastua uusia haavoittuvuuksia tai päivittämättömiä päätelaitteita.

Laitteiden päivityksen hallintaa pystyisi kehittämään automatisoimalla tietoverkon skannaukset tietylle aikavälille sekä tarkistamalla uusiempien päivitysten asentumisen päätelaitteille. Näin yritys saisi esimerkiksi muutaman kerran kuukaudessa tietoa ohjelmistojen ja laitteiden päivitysten ajantasaisuudesta.

### 7.3 Haasteet

Opinnäytetyön edetessä suurimmat vastaan tulleet haasteet löytyivät OpenVAS-ohjelmiston käytössä. Verkkoon tehtyihin skannauksiin liittyen OpenVAS ei onnistunut käyttämään sille annettuja erillisiä käyttäjätunnuksia niin, että ohjelmisto olisi päässyt käsiksi päätelaitteilla oleviin levy- ja tiedostojakoihin. Tunnuksia kokeiltiin useissa eri muodossa, ilman onnistumista.

Ulkoverkosta tehdyt skannaukset kummastakin ohjelmistosta jäivät kiinni palomuurille. Ulkoverkon rajapinnasta ei saatu tarkkaan tietoa, vaikka skannauksia suoritettiin eri profiileilla sekä asetuksilla. Skannauksen tulokset antoivat kuitenkin oikeaa ja tärkeää tietoa skannauksen kohteena olevasta ulkoverkon rajapinnasta.

Työkalujen käyttöönotto sujui ilman suurempia haasteita johtuen selkeistä ja suoraviivaisesta asennus- ja käyttöönotto-ohjeista. Ohjelmistojen suosion myötä verkosta löytyi helposti apua sekä esimerkkejä skannauksen tekemiseen. Haasteita olisi saatanut syntyä lisää, jos skannauksia olisi tehty kerrallaan suurempaan määrään aktiivitaipätelaitteita, sillä jo 15 laitteen skannauksesta tuotetun raportin pituus kasvaa nopeasti todella pitkäksi ja sen tulkinta hidastuu. Käyttäjätunnusten avulla tehtyjen skannauksien suoritus alusta loppuun vei runsaasti enemmän aikaa ja jos kerralla skannattavien laitteiden määrä kasvaa myös skannauksen käyttämä aika kasvaa huomattavasti.

## 8 Pohdinta

Opinnäytetyön tavoitteena oli selvittää ja tunnistaa Tietoakselin verkossa toimivat aktiivi- ja päätelaitteet sekä siellä avoimena olevat palvelut, portit ja protokollat. Toisena tavoitteena oli etsiä TietoAkselin tietoverkoista yleisesti tiedossa olevia haavoituvuuksia sekä päivittämättömiä päätelaitteita. Opinnäytetyön tutkimuskysymyksiin selvitettiin vastausta ensin vertailemalla kolmea eri teknistä ratkaisua keskenään. OpenVAS, Nessus ja Nexpose -ohjelmistoille suoritettiin vertailu teknisten ominaisuuksien sekä tutkimuskysymyksien asettamien tavoitteiden perusteella. Työssä käytetyiksi ohjelmistoiksi valittiin vertailun pohjalta OpenVAS ja Nessus. Ohjelmistot otettiin käyttöön ja niillä suoritettiin useita portti- ja verkkoskannauksia sekä sisä- että ulkoverkossa. Skannauksia saatiin tehtyä eri skannausprofiileilla, hyödyntäen myös päätelaitteissa toimivia paikallisia tunnuksia. Tunnusten avulla laitteista ja ohjelmistoista saatiin selville niistä puuttuvia päivityksiä sekä puutteellisia konfigurointeja.

Työssä käytetyn teorian, ISO/IEC 27001 -standardin, Katakri 2015:en, Vahti-ohjeiden sekä CIS-käytänteiden pohjalta saatiin luotettavaa tietoteknistä perustaa työn toteutukseen. Opinnäytetyössä käytetty teoria oli ajankohtaista sekä relevanttia tutkimuskysymyksiin nähden. Teoriaosuudessa käytettiin myös useaa englanninkielistä, teknistä lähdettä.

Opinnäytetyön alkuperäisen suunnitelman ja siihen liittyvien tarkkojen rajausten ansiosta työn teknisen toteutuksen -vaihe oli selkeä aikatauluttaa sekä suorittaa - teknisen vaiheen toteutus onnistui täysin sille varatun aikataulutetun suunnitelman mukaisesti. Nessus ja OpenVAS -ohjelmistojen avulla suoritettujen verkon skannaukset tuottivat yhdisteltäviä sekä vertailukelpoisia tuloksia, minkä ansiosta tietoverkosta saatiin yhteen ohjelmistoon verrattuna kattavampi määrä reaaliaikaista tietoa. Ulko-verkon skannauksessa haluttiin mallintaa verkon palveluiden ja porttien näkymää ulkopuolisen näkökulmasta. Palomuurien asianmukaisen toiminnan ansiosta skannaus tuotti vain niukasti tietoa. Tarvittaessa ulko-verkon skannauksia varten palomuurille olisi ollut mahdollista tehdä avauksia muurisääntöihin Nessus- ja OpenVAS-ohjelmiin liittyen.

Opinnäytetyölle olisi mahdollista tehdä jatkokehitystä liittyen verkon skannauksiin, tekemällä päätelaitteille muutoksia konfiguraatioon ja päivittämällä tarpeelliset ohjelmistot sekä sulkemalla tarpeettomat portit ja palvelut. Korjausten jälkeen skannaukset olisivat järkevää ajaa uudelleen ja sen jälkeen arvioida verkon tila. Verkon skannaukseen käytettävien Nessuksen ja OpenVAS:n tilalle olisi myös mahdollista kokeilla jotain toista ohjelmistoa. Näin verkosta saataisiin tietoa useammasta eri lähteestä. Jatkokehityksessä opinnäytetyössä tehdyt tietoverkon skannaukset olisi mahdollista tehdä samoilla konfiguraatioilla myös muihin yrityksen toimipisteisiin.

Opinnäytetyön tekemisen myötä pääsin syventämään opiskelun aikana saatua osaamista liittyen verkossa toimiviin laitteisiin sekä siellä toimiviin palveluihin ja portteihin. Omiksi kiinnostuksenkohteiksi nousi erityisesti ohjelmistojen tuottamien tulosten analysointi sekä tietoturvan kehitys yritys ympäristössä. Opinnäytetyöprosessissa erityisen antoisaa oli oman osaamisen haastaminen aidossa työympäristössä sekä mahdollisuus päästä työskentelemään itsenäisesti kiinnostavien aiheiden parissa.

## Lähteet

About CVE. 2019. About CVE. Mitren verkkosivut. Viitattu 4.7.2019.  
<https://cve.mitre.org/about/>

Baseline Process Best Practices White Paper. 2005 Cisco Baseline dokumentaatio. Muokattu 3.10.2005. Viitattu 17.6.2019.  
<https://www.cisco.com/c/en/us/support/docs/availability/high-availability/15112-HAS-baseline.html#what>.

Bosworth, S., Kabay, M. & Whyne, E. 2014. Computer Security Handbook, Sixth Edition. Chapter 40: Managing Software Patches and Vulnerabilities. 40.1 Introduction. Viitattu 9.5.2019  
<http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=63501>

CIS Controls V7.1. 2019. CIS -ohjeistus. Viitattu 11.6.2019.  
<https://www.cisecurity.org/cybersecurity-best-practices/>

First. 2019. Common Vulnerability Scoring System version 3.1: User Guide. Viitattu 4.7.2019. <https://www.first.org/cvss/user-guide>

Engebretson, P. 2013. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Chapter 3 – Scanning. Port Scanning. Viitattu 8.5.2019.  
<http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=56577>.

Heikkilä, M., Ahjopalo, J. & Parkkinen, S. 2019. Krp tutkii: Kyberhyökkäys Lahden verkkoon haittaa merkittävästi terveystalveta – sähköiset reseptit eivät toimi, verikokeissa ongelmia. Uutinen Ylen verkkosivuilla. Muokattu 14.6.2019. Viitattu 7.8.2019.  
<https://yle.fi/uutiset/3-10827423>

Henry, K. 2012. Penetration Testing: Protecting Networks and Systems. Chapter 4 - Active Reconnaissance and Enumeration. Port scanning. Viitattu 8.5.2019.  
<http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=47049>

Hibbert, B. & Haber, J. 2018. Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations. Chapter 2 – The Vulnerability Landscape. Vulnerabilities. Viitattu 8.5.2019.  
<http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=142606>

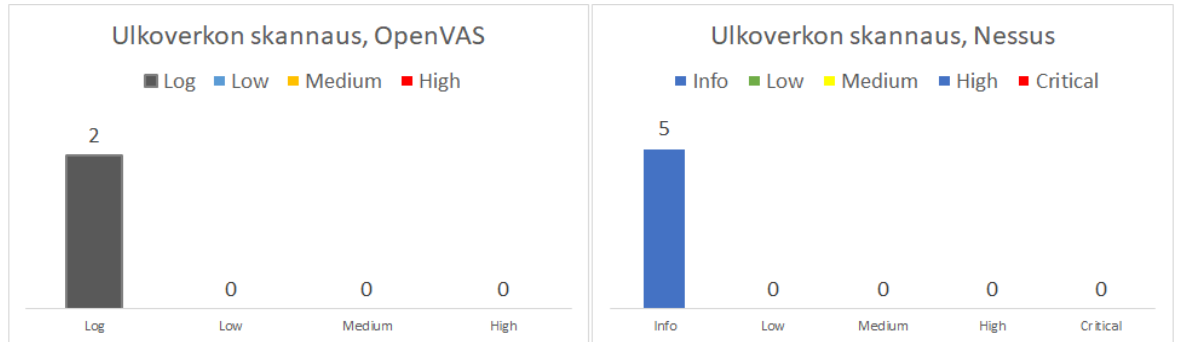
Hodson, Christopher. 2019. Cyber risk management: prioritize threats, identify vulnerabilities and apply controls. Chapter 8 – Vulnerabilities. Vulnerabilities in Process. Viitattu 26.8.2019.  
<http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=145391>.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas. Jyväskylän ammattikorkeakoulun julkaisu 202. Jyväskylä: Jyväskylän ammattikorkeakoulu.

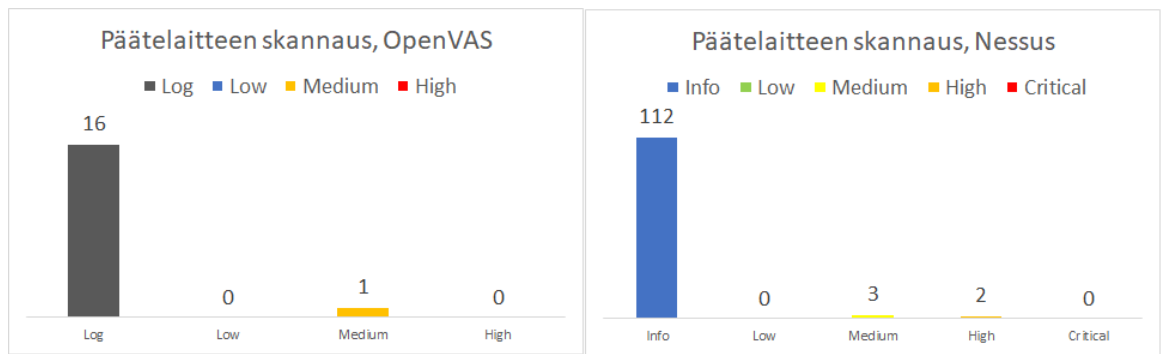
- Katakri 2015. 2015. Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 30.7.2019.  
[https://www.defmin.fi/files/3165/Katakri\\_2015\\_Tietoturvallisuuden\\_auditointityokalu\\_viranomaisille.pdf](https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf)
- Keary, T. 2018. Network Topology: 6 Network Topologies Explained & Compared. Comparitech-sivuton verkkojulkaisu. Päivitetty 21.11.2018. Viitattu 6.5.2019.  
<https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/>
- Keskitettyä talouden osaamista kasvupolulle. 2018. TietoAkselin kotisivut. Viitattu 6.5.2019. <https://www.tietoakseli.fi/yrittys/>
- Mikä on sisäverkko. 2010. Vahti-ohjeet. Muokattu 08.12.2010. Viitattu 6.5.2019  
<https://www.vahtiohje.fi/web/guest/2.-mika-on-sisaverkko.>
- Nessus. 2019. Nessus kotisivut. Viitattu 14.5.2019.  
<https://www.tenable.com/products/nessus/nessus-professional>
- Nexpose. 2019. Rapid7 kotisivut. Viitattu 13.5.2019.  
<https://www.rapid7.com/products/nexpose/>
- Olivier, A. & Woodward, B. 2014. Cabling: The Complete Guide to Copper and Fiber-Optic Networking, 5th Edition. Chapter 11 - Network Equipment. Network Connectivity Devices. Viitattu 8.5.2019.  
<http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=63486>
- OpenVAS. 2019. OpenVAS kotisivut. Viitattu 13.5.2019.  
<http://www.openvas.org/#about>
- Sathyan, Jithesh. 2010. Fundamentals of ems, nms and oss/bss. Chapter 14 - SNMP. Introduction. Viitattu 26.8.2019.  
[http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=36936.](http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=36936)
- SFS-ISO/IEC 27001:2017. 2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmä. Vaatimukset. Standardi. Suomen Standardisoimisliitto SFS.
- Verkon hallinta/valvonta. 2010. Vahti-ohjeet. Muokattu 08.12.2010. Viitattu 6.5.2019  
<https://www.vahtiohje.fi/web/guest/verkon-hallinta/valvonta.>
- Williams, J. 2019. Why Your Vulnerability Management Strategy is not Working – and What to do about It. Sans-organisaation julkaisema artikkeli. Viitattu 11.6.2019.  
<https://www.sans.org/reading-room/whitepapers/analyst/vulnerability-management-strategy-working-about-38938>
- What is an endpoint? 2019. Paloalton Cyperpedian julkaisu. Muokattu 2019. Viitattu 6.5.2019.  
<https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint.>

## Liitteet

### Liite 1. Ulkoverkon skannauksen tulokset

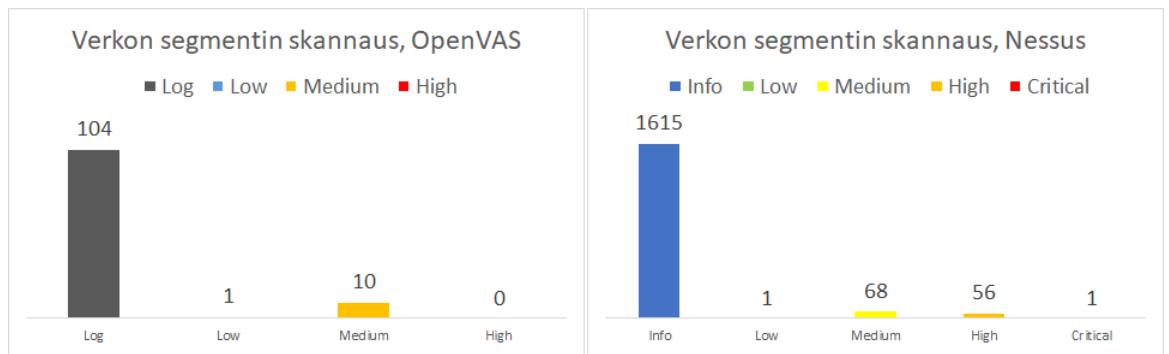


## Liite 2. Päätelaitteen skannauksen tulokset





## Liite 3. Verkon segmentin skannauksen tulokset



Liite 4. Haavoittuvuudet (Salassa pidettävä)

Liite 5. Avoimet portit ja palvelut (Salassa pidettävä)