LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Tietoverkkoturvallisuuskoulutuksen kehittäminen

Asseri Nieminen

Laurea-ammattikorkeakoulu

Tietoverkkoturvallisuuskoulutuksen kehittäminen

Asseri Nieminen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Huhtikuu, 2018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma
Tradenomi (AMK)

Asseri Nieminen

Tietoverkkoturvallisuuskoulutuksen kehittäminen

Vuosi 2018 Sivumäärä 39

Tämä opinnäytetyö kehitti tietoverkkoturvallisuuskoulutusta Laurea-ammattikorkeakoulun Network Security -opintojaksolle. Kehittäminen tapahtui luomalla harjoitteluun soveltuva laboratorio ja erilaisia harjoituksia. Opiskelijat suorittavat näitä harjoituksia syksyllä 2017 osana Network Security -opintojaksoa.

Opinnäytetyön teoreettinen viitekehys muodostui kyberturvallisuudesta, josta sitä rajattiin tietoverkkoturvallisuuteen ja vielä tarkemmin murtautumistestaukseen, jota Network Security -opintojakson teoriaosuus käsittelee.

Opinnäytetyö toteutettiin toimintatutkimuksena käyttäen laadullisia menetelmiä. Tutkimus selvitti laboratorioharjoitusten vaikutusta opiskelijoiden osaamisen kehittymiseen, luodun laboratorion käytettävyyttä, ja opiskelijoiden kokemuksia tällaisesta toiminnasta. Tiedonkeruumenetelminä käytettiin havainnointia, kyselyitä ja haastattelua. Tulokset olivat positiivisia: harjoituksilla oli oppimista edistävä vaikutus, laboratorio oli ratkaisuna toimiva ja opiskelijat kokivat toiminnan hyödyllisenä.

Opinnäytetyön tuotoksina syntynyttä virtuaalilaboratoriota ja harjoituksia voidaan käyttää sellaisenaan tulevilla Network Security -opintojaksoilla, sekä pienin muutoksin soveltaen myös muilla Laurea-ammattikorkeakoulun kyberturvallisuuden opintojaksoilla. Tulevaisuudessa opiskelijat voivat myös käyttää laboratoriota ja harjoituksia itsenäisesti, eikä niiden käytön tarvitse olla lähiopetukseen sidottua.

Asiasanat: Kyberturvallisuus, Laboratorio, Murtautumistestaus, Tietoverkkoturvallisuus

Laurea University of Applied Sciences
Degree Programme in Security Management
Bachelor's Thesis

Asseri Nieminen

Abstract

Developing Network Security Training

Year 2018 Pages 39

This thesis developed network security training at Laurea University of Applied Sciences. The thesis depicts the process of creating a suitable laboratory and various exercises. Students performed these exercises in the autumn 2017 as a part of the Network Security study unit.

The theoretical framework of this thesis covers cybersecurity, and the topic is confined to network security, and more specifically to ethical hacking, because it is a critical part of the theory covered in the study unit of Network Security.

The thesis was carried out as an operational study using qualitative methods. The study investigated the impact of the laboratory exercises on the development of students' knowledge, the usability of the created laboratory, and the students' experiences of such activities. The data collection methods used were observation, surveys, and interviews. The results were positive. The exercises had promoted learning, the laboratory was a working solution and the students felt the activity useful.

The virtual laboratory and exercises can be used in future Network Security study units and with slight modification, they can also be applied to other Laurea University of Applied Sciences' cyber security courses. In the future, students can also use the laboratory and the exercises independently, and their use does not need to be tied to classroom tuition.

Keywords: Cybersecurity, Laboratory, Network Security, Penetration Test

Sisällys

1 Johdanto

Opinnäytetyö kehittää tietoverkkoturvallisuuskoulutusta Network Security -opintojaksolla. Työn tilaajana toimii Laurea-ammattikorkeakoulu. Tietoverkkoturvallisuuskoulutuksen kehittäminen tapahtuu luomalla käytännön tietoverkkoturvallisuuden opiskeluun soveltuva laboratorio ja erilaisia harjoituksia.

Kyberturvallisuuden käytännön harjoittelu alkoi Laurea-ammattikorkeakoulussa Cybersecurity-opintojaksolla keväällä 2017. Opintojaksosta opiskelijoilta saatu palaute oli kannustavaa, joten tätä toimintaa haluttiin kehittää. Cybersecurity-opintojakson lopussa sovimme asiakkaan kanssa minun jatkavan alkanutta kehittämistyötä opinnäytetyön muodossa. Opinnäytetyölle sovittiin tavoitteiksi kyberturvallisuuskoulutuksen käytännön harjoittelun eteenpäin vieminen ja laboratorioharjoitusten vaikutuksen oppimiseen tutkiminen.

Opinnäytetyö toteutetaan toimintatutkimuksena. Toimintatutkimus koostuu kahdesta osasta, toiminnasta ja tutkimuksesta. Toiminta tässä opinnäytetyössä tarkoittaa laboratorion ja harjoitusten luomista ja ohjaamista opintojaksolla. Tutkimus toteutetaan laadullisena, käyttäen tiedonkeruumenetelminä oppimistilanteiden havainnointia, osaamistasoa mittaavia kyselyitä ja haastattelua. Työ etsii vastauksia kolmeen tutkimuskysymykseen:

1. Edistävätkö laboratorioharjoitukset opiskelijoiden osaamista?
2. Onko laboratorio toimiva?
3. Mitä mieltä opiskelijat ovat laboratorioharjoituksista?

Ensin työssä kuvataan teoreettista viitekehystä, jossa käsitellään kyberturvallisuutta ja sen koulutusta, josta aihetta tarkennetaan tietoverkkoturvallisuuteen ja lopulta murtautumistestaukseen. Tämän jälkeen esitellään opinnäytetyön toteutus kronologisessa järjestyksessä, käsitellen työn taustaa, luotuja harjoituksia ja laboratoriota.

Toteutuksen jälkeen kuvataan tutkimusasetelma, jossa käsitellään yleisesti laadullista- ja toimintatutkimusta sekä tiedonkeruumenetelmiä ja niiden käyttöä tutkimuksessa. Viimeisenä käsitellään tutkimuksen tulokset, johtopäätökset sekä pohdinta ja kehittämisehdotukset.

Käsitteet

Eettinen hakkeri	Henkilö joka murtautuu esimerkiksi tietoverkkoon tai -järjestelmään, tarkoituksenaan parantaa sen turvallisuutta. (Oriyano 2016, 9.)
Laboratorio	Opinnäytetytön tuotoksena syntynyt virtuaalisten tietokoneiden yhdistelmä, jossa suoritetaan laboratorioharjoituksia.
Laboratorioharjoitus	Opinnäytetytön tuotoksena syntynyt harjoitus, joka suoritetaan laboratoriossa.
Murtautumistestaus	Luvallinen, simuloitu hyökkäys esimerkiksi tietojärjestelmää tai -verkkoa kohtaan, jonka tarkoituksena on löytää ja korjata uhkia (Oriyano 2016, 11).
Tietoverkko	”Tietokoneiden ja niiden välisten tiedonsiirtoyhteyksien sekä näiden molempien avulla tarjottavien palvelujen yhdistelmä” (Vahtiohje 2008).

2 Teoreettinen viitekehys

Uutta tietoa tuotetaan tieteellisessä tutkimuksessa teorian avulla, johon viitataan tyypillisesti metodikirjallisuudessa teoreettisella viitekehyksellä. Tutkimuksen avulla on mahdollista uudistaa, rakentaa, selittää, purkaa ja täsmentää aikaisempaa teoriaa tai luoda uusia käsitteitä. Teoreettisen viitekehyksen ohella tutkimuksessa käytetään myös käsitteitä, jotka voivat olla konkreettisia tai teoreettisia. Konkreettisia käsitteitä ovat arkikieliset käsitteet, jotka muodostuvat havainnoista, kokemuksista ja kuvauksista. Teoreettiset käsitteet puolestaan ovat järjestelmällisen tutkimustyön tuloksia ja tämän vuoksi ne ovat yleisiä, eivätkä paikkaan tai aikaan sidottuja. Teoreettinen viitekehys ja käytettävät käsitteet tulee aina kuvata ja määritellä selkeästi ja täsmällisesti. Teoreettisen viitekehyksen ja käsitteiden tarkoituksena on luoda tutkimukselle kehys. Näin ne ensisijaisesti muodostavat näkökulman, joka muodostaa näkökulman josta tutkimusta tarkastellaan. (Vilkka 2015.)

2.1 Kyberturvallisuus

Kyberturvallisuus voidaan helposti sekoittaa tietoturvallisuuteen, tietoverkkoturvallisuuteen tai tietokoneturvallisuuteen, eikä näiden käsitteiden yhteneväisyyksistä tai eroavaisuuksista olla täysin yksimielisiä. Esimerkiksi tietoturvallisuudella yleensä tarkoitetaan tietoaineistojen, tietojärjestelmien ja palveluiden asianmukaista suojausta siten, että niiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit otetaan huomioon. Yleisesti kuitenkin kyberturvallisuutta pidetään edellä mainittuja laajempana kokonaisuutena ja ulottuvuutena, sillä kyberturvallisuus pyrkii turvaamaan koko sähköisen ja verkotetun yhteiskunnan. (Limnéll 2014, 4.)

Kyberturvallisuus on ilmiönä verrattain uusi ja käsitteen määrittely suomen kieleen on edelleen käynnissä. Sana kyber on johdettu kreikan kielen sanasta kybereo, joka tarkoittaa ohjata, opastaa ja hallita. Suomen kieleen se on otettu englannin kielen cyber-sanasta, jolla viitataan tietokoneiden kulttuuriin, informaatioteknologiaan ja virtuaaliseen todellisuuteen. (Limnéll 2014, 3.)

Standardointiorganisaatio ISO (International Organization for Standardization) määrittelee Guidelines For Cybersecurity -standardissa kyberturvallisuuden luottamuksellisuuden, eheyden ja saatavuuden turvaamiseksi kyberavaruudessa. Kyberavaruudella he puolestaan tarkoittavat monimutkaista ympäristöä, joka koostuu teknologisten laitteiden ja verkkojen vuorovaikutuksella yhdistyvistä ihmisistä, ohjelmistoista ja palveluista Internetissä. (ISO/IEC 27032 2012.)

Valtiovarainministeriön julkisen hallinnon digitaalisen turvallisuuden VAHTI-johtoryhmä vastaa julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta. (Valtiovarainmi-

nisteriö 2017). Heidän määritelmänsä mukaan kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan yhteiskunnalle tai organisaatiolle merkittävien ICT-toimintojen häiriöihin (Information and Communications Technology).

Kyber-käsitteen helppotajuisin määritelmä lienee jako fyysiseen ja digitaaliseen maailmaan. Fyysisellä maailmalla tarkoitetaan meitä ympäröivää atomeista koostuvaa konkreettista maailmaa. Digitaalinen maailma puolestaan koostuu biteistä, josta esimerkkinä on Internet, tietoverkot ja tietokoneen ohjelmistot. Kyberturvallisuus tarkoittaa siis digitaalisen maailman turvallisuutta. (Limnéll, Majewski & Salminen 2014, 12)

Kyberturvallisuuden rooli on viimevuosina noussut merkittävään asemaan. Elämme voimakkaasti digitalisoituneessa maailmassa, jonka johdosta fyysinen ja digitaalinen maailma ovat voimakkaasti nivoutuneet yhteen. Yhteiskunnat ovat äärimmäisen riippuvaisia esimerkiksi sähkön- ja energianjakelusta, rahoitusjärjestelmistä sekä elintarvikehuollosta, jotka kaikki toimivat bittien avulla. (Limnéll, ym. 2014, 13.) Esimerkiksi jo muutaman päivän mittainen laaja häiriö sähkönjakelussa voisi romahduttaa yhteiskuntarauhan täysin.

Kuten digitalisaation myötä muutkin asiat, myös rikollisuus on siirtynyt verkkoon. Poliisin määritelmän mukaan kyberrikollisuudella tarkoitetaan tietotekniikkaan tai tietoverkkoihin kohdistuvia, tai tietotekniikkaa ja tietoverkkoja hyväksi käyttäen tehtyjä rikoksia. Täten siihen liittyviä rikosnimikkeitä voivat olla esimerkiksi luvaton käyttö, yritysvakoilu, yrityssalaisuuden rikkominen, vaaran aiheuttaminen tietojenkäsittelylle, petos, tietoliikenteen ja tietojärjestelmän häirintä ja tietomurto. (Poliisi 2017.)

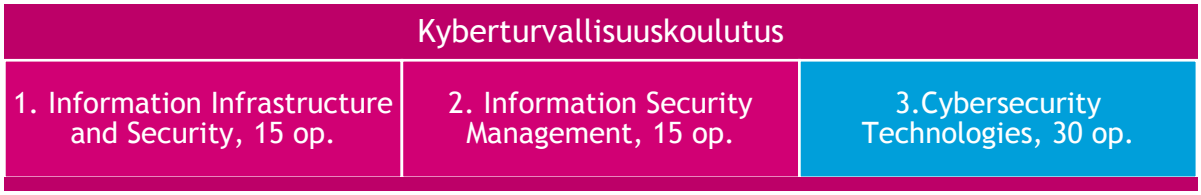
Europolin IOCTA 2017 -raportin mukaan kyberrikollisuus kasvaa ja kehittyy nopeammin kuin mikään muu rikosmuoto (Internet Organized Crime Threat Assessment 2017). Esimerkiksi haittaohjelmien kokonaismäärä on noussut vuodesta viimeisen viiden vuoden aikana yli 600 prosenttia (AV-Test Institute 2017). Kyberrikollisuuden laajuudesta kertoo myös se, että esimerkiksi Iso-Britanniassa kyberrikollisuus muodostaa jo yli puolet kaikesta rikollisuudesta, ja rahallisesti mitattuna sen arvioidaan olevan jopa globaalia huumekauppaakin suurempaa. (Cyber Security Assessment 2016; Fortune, 2015).

Useiden tutkimusten mukaan kyberturvallisuuden tilannetta pahentaa lähivuosina korostuvan työvoimapulan laajuus. Esimerkiksi ISACA:n (Information Systems Audit and Control Association) vuoden 2015 Global Cybersecurity Status -raportin mukaan, 86 % tietoturvapäälliköistä uskoo huomattavaan osaajapulan lähitulevaisuudessa. Vuonna 2016 toteutetussa globaalissa kyselytutkimuksessa havaittiin, että 46 % yrityksistä kokee osaajapulan jo tällä hetkellä ongelmana. Arvioiden mukaan osaajapula on vuoteen 2020 mennessä noin 1 – 1,5 miljoona henkilöä. (Cobb, 2017, 1-2.) Myöskään Suomessa ei ole riittävästi korkeatasoista kyberturvallisuusosaamista ja alan yritykset kokevat osaavan henkilöstön rekrytoinnin haasteellisena. (Lehto, ym. 2017, 71.)

2.2 Kyberturvallisuuskoulutus

Kansallisella tasolla Lehdon & Kähkösen (2015, 33) mukaan kyberturvallisuuskoulutus on korkeakouluissa jakautunut siten, että yliopistoissa korostuu kyberturvallisuuden tieteellinen tutkimus ja siihen perustuva opetus. Ammattikorkeakoulut puolestaan tuottavat käytännönläheistä ja työelämän tarpeita vastaavaa koulutusta.

Laurea-ammattikorkeakoulussa kyberturvallisuuskoulutusta on mahdollista saada Espoon Leppävaaran kampuksella. Kyberturvallisuuskoulutus on englannin kielistä koostuen kolmesta, yhteensä 60 opintopisteen suuruisesta moduulista. (Rathod 2017). Kyberturvallisuuskoulutuksen moodulit on esitetty kuviossa 1.



Kuvio 1 Kyberturvallisuuskoulutuksen moduulit (Rathod 2014, 1)

Kyberturvallisuuskoulutuksen moduulit lähestyvät kyberturvallisuutta eri näkökulmista, pyrkien muodostamaan syvää ja monimuotoista osaamista. Laurea-ammattikorkeakoulun kyberturvallisuuskoulutukseen kuuluu teoriaa, käytännön harjoituksia sekä erilaisia projektitöitä. (Rathod 2014, 1.)

Information Infrastructure and Security -moduulin tavoitteena on tuottaa opiskelijalle tietotaitoa, jonka avulla hän osaa parantaa tietoverkkojen turvallisuutta erilaisten suojausratkaisujen avulla. (Rathod 2014, 2.)

Information Security Management -moduulin tavoitteena on, että opiskelija ymmärtää, osaa suunnitella sekä implementoida tietoturvallisuuden hallinnan osaksi organisaation toimintaa. Tämä tarkoittaa esimerkiksi osaamista tietoturvallisuusstrategioista, tietoturvallisuuden riskien hallinnasta sekä erilaisten suunnitelmien luomisesta. (Rathod 2014, 2.)

Cybersecurity Technologies -moduulin tavoitteena on tutustuttaa opiskelija kybertoimintaympäristön riskeihin, uhkiin sekä haavoittuvuuksiin. Tavoitteena on, että opiskelija kykenee suojaamaan organisaation kybertoimintaympäristössä. (Rathod 2014, 3.)

Tämä opinnäytetyö käsittelee Cybersecurity Technologies -moduuliin kuuluvaa Network Security -opintojaksoa. Opintojakson teoriaosuus lähestyy tietoverkkoturvallisuutta eettisen hakkeroinnin, eli murtautumistestauksen näkökulmasta. Opintojakson opetukseen kuuluu teorian lisäksi reflektiopäiväkirjoja, osaamista mittaavia tenttejä, ohjausta ja nyt myös vapaaehtoisia laboratorioharjoituksia. Laboratorioharjoitusten tarkoituksena on mahdollistaa käytännön harjoittelu sekä pyrkiä helpottamaan teoriaosuudessa käsiteltävien aiheiden ymmärtämistä. Opiskelijoiden suoriutumista laboratorioharjoituksista ei arvioida, mutta heillä on mahdollisuus vaikuttaa koko opintojaksosta saamaansa arvosanaan suorittamalla laboratorioharjoituksia koskevan tentin.

Network Security -opintojakson teoriaosuus muodostuu osasta CEH-sertifikaatin (Certified Ethical Hacker) suorittamiseen tarkoitetusta materiaalista. CEH-Sertifikaatin tavoitteena on todentaa henkilön kyky ymmärtää ja tuntea järjestelmien heikkouksia ja kyetä korjaamaan ne (Oriyano, 2016, 1). Käytännössä sertifikaatti siis todentaa henkilön osaamista eettisestä hakkeroinnista ja erilaisten suojausratkaisujen toteuttamisesta.

Opintojakson teoriaosuus ei kuitenkaan käsitä kaikkia CEH-sertifikaatin 18 aihetta, vaan siihen on valittu lähinnä tietoverkkoturvallisuuden kannalta merkitykselliset aiheet. Opintojakson teoriaosuudessa käytetyt aiheet on kuvattu tarkemmin sivulla 16. Pois jätetyt aiheet ovat malware threats, sniffing, social engineering, denial-of-service, session hijacking, hacking webservers, hacking web applications, SQL injection sekä cloud computing. Näitä aiheita käsitellään tarkemmin muilla Laurea-ammattikorkeakoulun kyberturvallisuuden opintojaksoilla.

2.3 Tietoverkkoturvallisuus

Tietoverkkoturvallisuuden (engl. Network Security) tavoitteena on taata tiedon luottamuksellisuus, saatavuus ja eheys tiedonsiirrossa ja säilytyksessä. Tämä tarkoittaa, ettei luvaton käyttäjä voi lukea, estää pääsyä, eikä myöskään muokata tai väärentää tietoja. (Wang & Kissel 2015, 1-2).

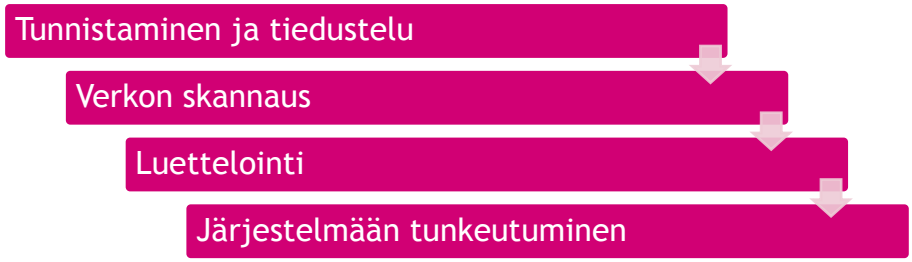
Tietoverkkoturvallisuus tarkoittaa siis käytännössä erilaisia strategioita ja toimenpiteitä, joilla turvataan ja varmistetaan tietoverkoissa ja -järjestelmissä liikkuva tieto. Tämä toteutetaan muun muassa erilaisilla laitteistoa (engl. hardware) ja ohjelmistoa (engl. software) koskevilla toimenpiteillä (Wang & Kissel 2015, 5).

2.4 Murtautumistestaus

Hakkeroinnilla terminä on yleensä negatiivinen konnotaatio ja termiä käytetään usein esimerkiksi tietomurroista uutisoitaessa. Todennäköisesti osin tämän takia, se tyypillisesti liitetään johonkin rikolliseen tai vähintäänkin arveluttavaan toimintaan. Hakkerit voidaan kuitenkin jakaa kolmeen tyyppiin heidän motiiviensa perusteella: mustahattu-, harmaahattu- ja valkohattuhakkereihin.

Mustahattuhakkerit (engl. black hat hacker) ovat tyypillisesti kyberrikollisia ja heidän motiivinsa liittyvät usein rahaan ja he murtautuvat järjestelmiin ilman lupaa. Harmaahattuhakkerit (engl. grey hat hacker) toimivat moraalisesti harmaalla alueella, saattaen esimerkiksi julkistaa löytämiään haavoittuvuuksia, tai toimia muuten edustamansa aatteen puolesta. Valkohattuhakkereiden (engl. white hat hacker) motiivina on turvallisuuden parantaminen. He saattavat käyttää samoja menetelmiä, kuin muutkin hakkerit, mutta ilman rikollista tarkoitusta. (Oriyano 2016, 8-9).

Murtautumistestaaja (valkohattu-hakkeri) käyttää siis työssään samoja keinoja, kuin esimerkiksi kyberrikollinenkin (mustahattu-hakkeri) voisi käyttää, mutta hänen motiivinsa ovat erilaiset.



Kuvio 2 Murtautumistestausprosessi (Oriyano 2016, 18).

Tyypillinen murtautumistestausprosessi, joka on kuvattu kuviossa 2, alkaa kohteen tunnistamisella ja tiedustelulla. Tässä vaiheessa kohteesta kerätään aktiivisesti ja passiivisesti tietoa. Aktiivinen tiedonkeruu on tiedonkeruun muoto, jossa ollaan kohteen kanssa vuorovaikutuksessa. Esimerkkejä aktiivisesta tiedonkeruusta voi olla niin sanottu käyttäjän manipulointi (engl. social engineering), jossa tarkoituksena on saada käyttäjä paljastamaan salaista tietoa. Passiivisessa tiedonkeruussa kohteen kanssa ei ole suoraa vuorovaikutusta. Esimerkkejä passiivisesta tiedonkeruusta voi olla verkkosivuilta ja sosiaalisesta mediasta kerättävä tieto. Tämän vaiheen tarkoituksena on luoda pohjaa prosessin myöhemmille vaiheille, muodostaen käsitystä kohteesta, jonka perusteella voidaan suunnitella myöhempien vaiheiden toteutus. Käytännössä tässä vaiheessa voidaan esimerkiksi selvittää IP-osoitteita tai kerätä kohteen henkilöstöstä tietoa. (Oriyano 2016 106, 161.)

Prosessin toinen vaihe on verkon skannaus (engl. Network Scanning). Tässä vaiheessa pääpaino on vuorovaikutuksessa kohteen kanssa ja tarkemman tiedon keräämisessä. Tämä voi tarkoittaa esimerkiksi aktiivisten järjestelmien ja näiden järjestelmien yksityiskohtien, kuten käytettyjen palveluiden tai avoimien porttien tunnistamista kohdeverkosta. Käytännössä tämä voi tarkoittaa verkon analysointia esimerkiksi ping-pakettien tai tietoliikenneporttiskannausten avulla. (Oriyano 2016, 161.)

Prosessin kolmas vaihe on luettelointi (engl. Enumeration). Vertauksena voidaan ajatella verkon skannauksen olevan kuin käytävällä sijaitsevien ovien lukituksen tarkistamista, siinä tutkitaan mitkä ovet ovat lukitsematta tai mistä ovesta voisi päästä sisään. Luetteloinnissa katsotaan, onko näiden tunkeutumisen mahdollistavien ovien takana jotakin mielenkiintoista. Käytännössä tässä vaiheessa voidaan etsiä järjestelmissä käytettäviä käyttäjätunnuksia, käyttäjäryhmiä ja salasanoja. (Oriyano 2016, 162.)

Prosessin viimeinen vaihe on järjestelmään tunkeutuminen aikaisempaa tietoa hyväksikäyttäen. Käytännössä tämä voi tarkoittaa salasanojen murtamista, käyttöoikeuksien manipulointia, erilaisten sovellusten käyttämistä, jälkien peittämistä tai murtautumisesta jääneiden todisteiden hävittämistä. (Oriyano 2016, 162.)

Murtautumistestauksen jälkeen asiakkaalle tyypillisesti raportoidaan havaitut turvallisuusuhat, esitetään riskiarvio niistä ja annetaan toimenpide-ehdotuksia niiden korjaamiseen.

3 Laboratorion ja harjoitusten toteutus

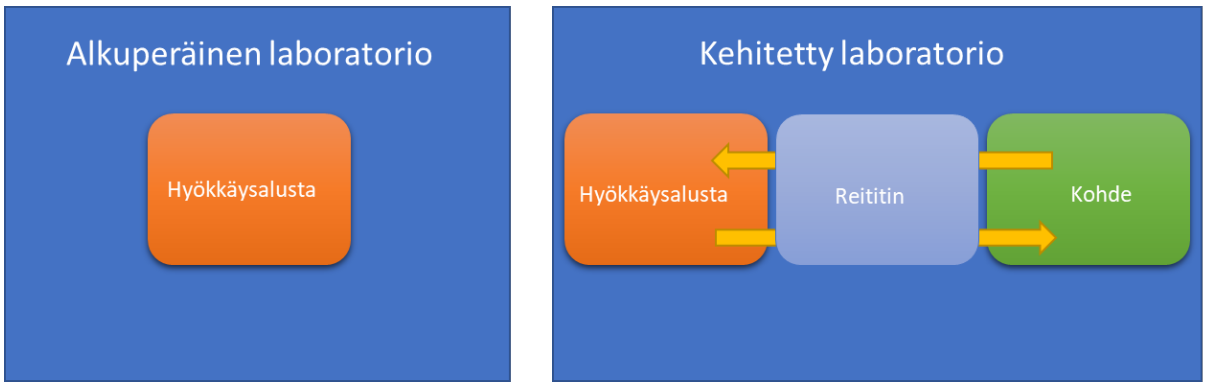
Ajatus tämän opinnäytetyön tekemisestä Laurea-ammattikorkeakoululle syntyi kevätlukukauden 2017 aikana, jolloin ohjasin laboratorioharjoituksia Cybersecurity-opintojaksolla. Kyseinen opintojakso toimi tämänkaltaisen koulutuksen pilottina, sillä aikaisemmin näitä käytännön kyberturvallisuusharjoituksia ei Laurea-ammattikorkeakoulussa ole ollut. Opintojaksosta opiskelijoilta saatu palaute oli positiivista, ja tämänkaltaista toimintaa nähtiin tarpeellisena viedä eteenpäin.

Cybersecurity-opintojakson harjoitukset käsittelivät kyber- ja tietoverkkoturvallisuutta. Opintojakson harjoitukset muodostuivat Juuso Myllylän ja Tomi Lindforsin opinnäytetyön, Laboratorioharjoituksia kyberturvallisuuden opiskelijoille (Myllyä & Lindfors 2017) tuotoksista. Opinnäytetyön lisäksi valmistelin muita harjoituksia, sillä opiskelijat suorittivat niitä nopealla tahdilla ja käytettävä materiaali uhkasi loppua opintojakson aikana kesken. Tämä opinnäytetyö jatkaa kehittämistyötä edellä mainitusta opinnäytetyöstä ja harjoituksista. Myllylän & Lidforsin luomassa mallissa harjoituksia suoritettiin virtualisoituna Kali Linux -käyttöjärjestelmässä. Malli oli hyvä ja sen ansiosta Laurea-ammattikorkeakoulun käytännön kyberturvallisuuskoulutus oli mahdollista aloittaa.

3.1 Laboratorio

Laboratorioharjoitusten kehittäminen edistyneemmiksi ja monipuoliseksi edellytti uuden laboratorion luomista, sillä Myllylän & Lindforsin mallissa ei ollut turvallista harjoitusmaalia, jota kohtaan harjoituksia suorittaa.

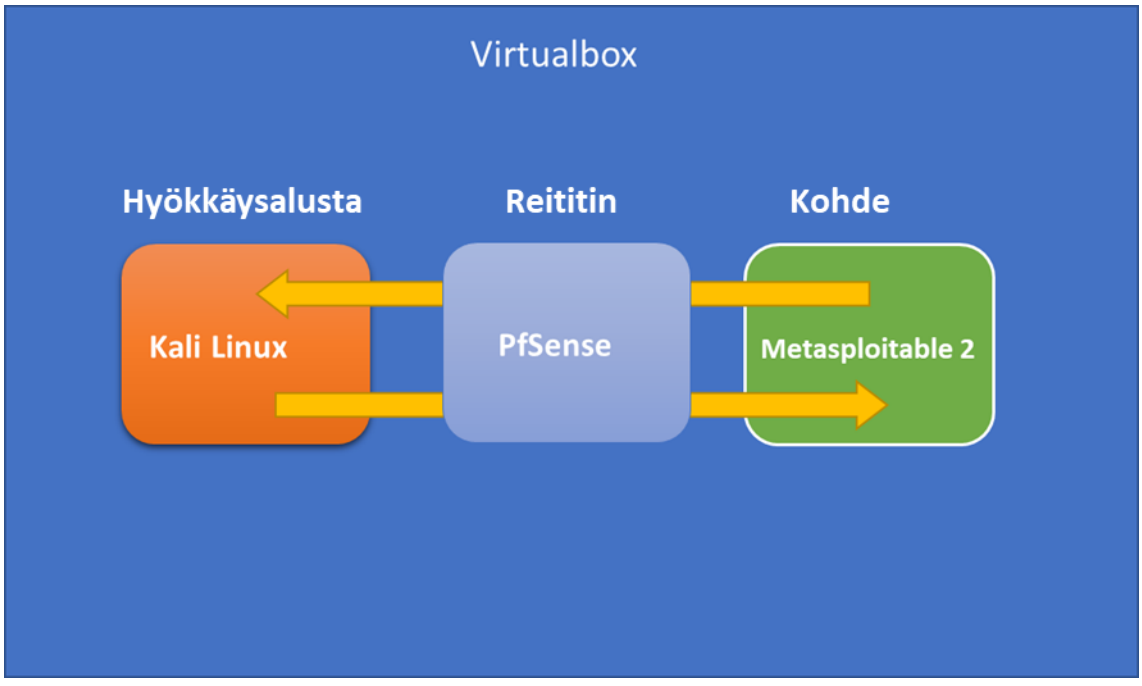
Uusi laboratorio syntyi kolmesta komponentista. Hyökkäysalustasta, kohteesta sekä reitittimestä, joka muodostaa verkkoyhteyden kahden edellä mainitun välille. Laboratorioiden erot on esitetty kuviossa 3.



Kuvio 3 Laboratoriot

Kuten Myllylän & Lindforsinkin mallissa, päätettiin laboratorio toteuttaa virtualisoinnilla. Virtualisoinnin avulla yksi fyysinen resurssi, kuten tietokone, voi toimia monena loogisena resurssina (Singh 2004). Käytännössä virtualisoinnilla voidaan siis luoda esimerkiksi tietokoneita tietokoneen sisälle. Virtualisointialustaksi valikoitui avoimen lähdekoodin ja maksuttomuutensa vuoksi Oraclen Virtualbox-ohjelma. Valintaan vaikutti myös siitä saatu kokemus kevään Cybersecurity-opintojaksolla. Virtualisoinnilla toteutettu laboratorio ei aiheuttanut asiakkaalle suoria kuluja, mutta epäsuorina kuluina voidaan pitää esimerkiksi käytetyn 009 IT -tilan laitteiden käyttöaikaa, joka oli pois muusta opetuksesta. Virtualisoituna toteutettuna laboratorio oli myös turvallinen, sillä se oli eristetty sen käyttämästä isäntätietokoneesta ja ulkopuolisesta verkosta.

Suunniteltujen laboratorioharjoitusten perusteella laboratorioon tarvittiin hyökkäysalusta ja kohde. Hyökkäysalusta oli opiskelijan harjoituksissa pääasiassa käyttämä käyttöjärjestelmä, jolla harjoitukset suoritettiin. Kohteen funktio oli toimia turvallisena harjoitusmaalina. Hyökkäysalustan ja kohteen välille tarvittiin myös verkkoyhteys, joka luotiin reitittimellä. Laboratorion tarkka rakenne on kuvattu alla kuviossa 4.



Kuvio 4 Laboratorion tarkka rakenne

Kali Linux -käyttöjärjestelmä toimi laboratorion hyökkäysalustana, jolla murtautumistestaus suoritettiin. Kali Linux on Debianiin perustuva, Linux-pohjainen jakelupaketti, jonka on luonut turvallisuusyritys Offensive Security Ltd. Se on suunniteltu erityisesti tekniseen rikostutkintaan sekä murtautumistestaukseen. (Offensive Security 2017).

Metasploitable 2 toimi laboratorioharjoitusten kohteena. Metasploitable 2 on tarkoituksella haavoittuvaiseksi luotu Ubuntu Linux -palvelin, jonka on luonut turvalliseksi kohteeksi murtautumistestauksen harjoittelemiseen Rapid 7 Inc. (Rapid 7 2017.)

PfSense on avoimeen lähdekoodiin perustuva, FreeBSD-pohjainen reititin ja palomuuri, jonka on luonut Rubicon Communications LLC (PfSense 2017). PfSensen funktio laboratoriossa on luoda verkko hyökkäysalustan ja kohteen välille.

3.2 Laboratorioharjoitukset

Laboratorion ja harjoitusten suunnittelu tapahtui heinä- ja elokuun aikana. Harjoitusten sisältö peilattiin Network Security -opintojakson teoriaosuutena käytettävästä Certfied Ethical Hacker -materiaalin murtautumistestausta käsittelevistä aiheista:

- Hacking & Penetration testing (suom. hakkerointi ja murtautumistestaus).
- Footprinting and reconnaissance (suom. tunnistaminen ja tiedustelu).
- Network Scanning (suom. verkon skannaus).
- Enumeration and Cryptography (suom. enumeraatio ja kryptografia).
- System Hacking (suom. järjestelmän hakkerointi).
- Hacking Wireless Networks (suom. langattomien verkkojen hakkerointi).
- Hacking Mobile Platforms (suom. mobiilialustojen hakkerointi).
- Evadings Intrusion Detection Systems, Firewalls and Honeypots (suom. tunkeutumisen havaitsemisjärjestelmän, palomuurin ja hunajapurkin ohittaminen).

Kaikkia edellä mainittuja aiheita ei kuitenkaan voitu lähiopetukseen varatun ajan, turvallisuuden ja opiskelijoiden osaamistason vuoksi käsitellä. Laboratorioharjoituksissa käsitellyt aiheet olivat hakkerointi ja murtautumistestaus, tunnistaminen ja tiedustelu, verkon skannaus, luettelointi ja kryptografia sekä järjestelmän hakkerointi. Esimerkkinä pois jätetyistä aiheista on langattomien verkkojen hakkerointi, jonka toteutus olisi voinut vaarantaa Laurea-ammattikorkeakoulun verkon toiminnan.

Syyskuun alussa suunnitelma esitettiin asiakkaalle, jonka palautteen perusteella sitä muokattiin opiskelijoiden osaamistasoon paremmin sopivaksi. Tässä vaiheessa sovimme myös viidestä erillisestä kerrasta, joissa harjoitusten ohjaus tapahtui. Ohjaus tapahtui osana Network Security -opintojaksoa, perjantai aamupäivisin Laurea-ammattikorkeakoulun Espoon kampuksen

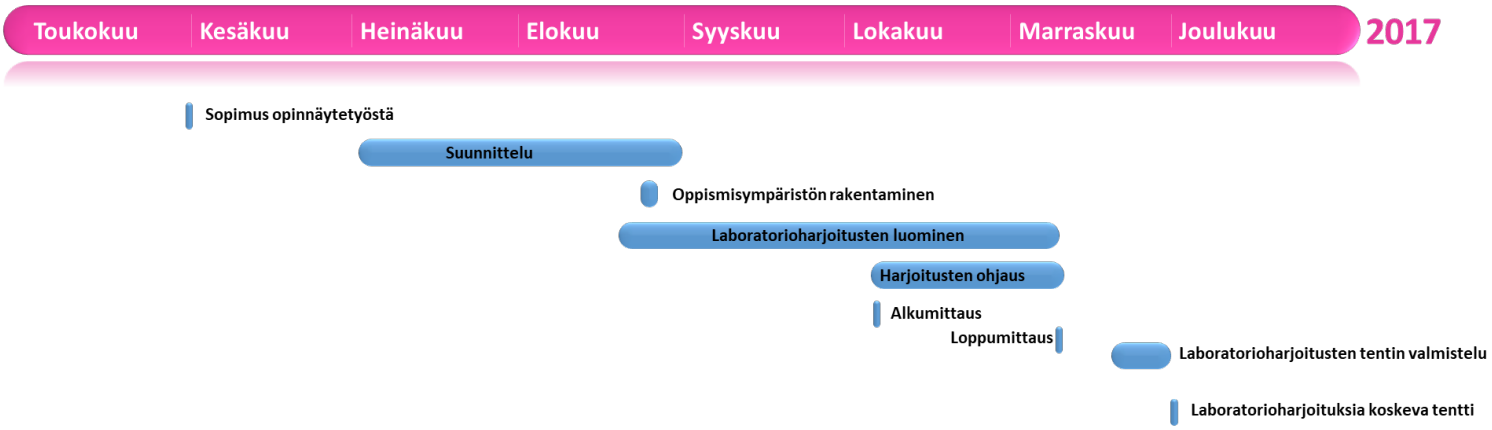
009 IT -tilassa. Ohjaukseen osallistuminen oli vapaaehtoista ja niihin osallistui kullakin kerralla noin seitsemän opiskelijaa. Yhden ohjauskerran kesto oli kaksi ja puoli tuntia.

Opintojaksoon kuului myös laboratorioharjoituksia koskeva tentti, joka ei kuitenkaan ollut osa tätä tutkimusta. Vapaaehtoisen tentin suorittamisella opiskelijoilla oli mahdollisuus vaikuttaa opintojaksosta saamaansa arvosanaan.

Kullekin ohjauskerralle suunnittelin oman moduulin käsiteltävien aihekokonaisuuksien mukaan. Moduuleita oli viisi ja niiden aiheet olivat:

- Laboratorion luominen (engl, Lab Setup)
- Tiedon kerääminen (engl. Information Gathering)
- Murtautumistestaus (engl. Penetration Test)
- Järjestelmän koventaminen (engl. Target Hardening)
- Kertaus (engl. Repetition).

Lopputuloksena harjoituksista muodostui noin 150-sivuinen opiskelumateriaali, joka sisältää vaihe vaiheelta etenevien ohjeiden lisäksi myös hieman teoriaa ja aiheiden taustoitusta. Harjoitukset on kuitenkin jätetty pois tästä opinnäytetyöstä, sillä Laurea-ammattikorkeakoulu haluaa korostaa eettisyyttä ja opiskelijoiden vastuuta niiden käytössä. Opinnäytetyön toteuttamisen prosessi on esitetty alla kuviossa 5 ja luotujen laboratorioharjoitusten sisällysluettelo kuviossa 6.

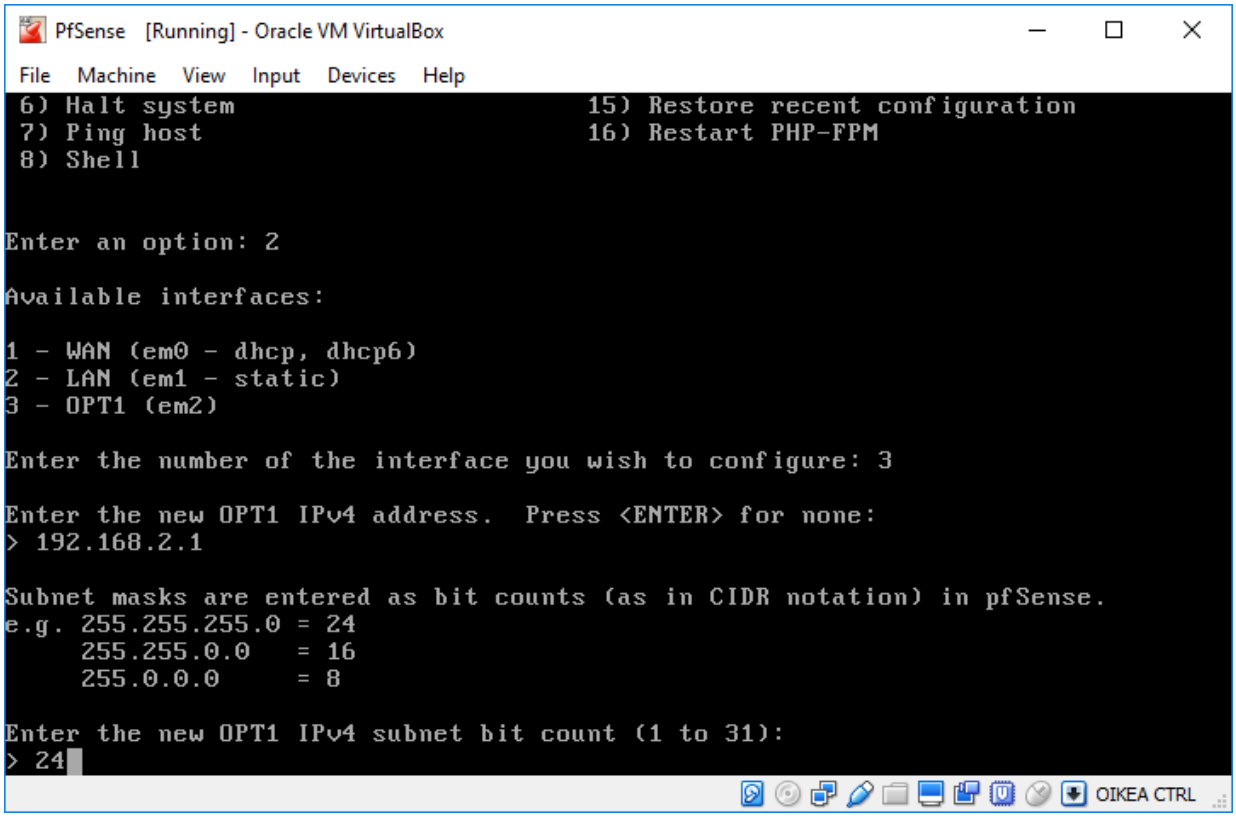


Kuvio 5 Gantt-kaavio opinnäytetyön aikataulusta

Kuvio 6 Luotujen harjoitusten sisällysluettelo

3.2.1 Laboratorion luominen

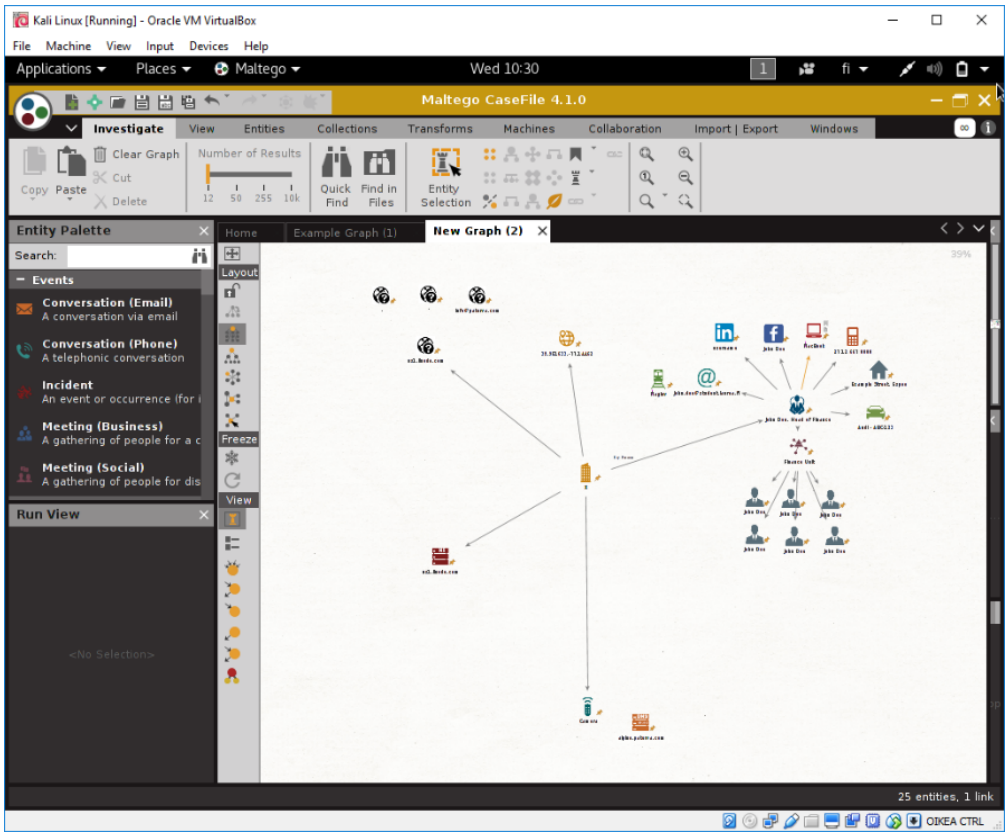
Laboratorion luominen -moduulissa opiskelija lataa verkosta Virtualbox-, Kali Linux-, Metasploitable 2- ja PfSense -tiedostot. Opiskelija asentaa Virtualbox-ohjelman ja luo lataamistaan tiedostoista kolme virtuaalitietokonetta. Opiskelija oppii näin asentamaan käyttöjärjestelmiä ja luomaan verkon näiden laitteiden välille. Laboratorion luotuaan hän tarkistaa sen verkon toimivuuden muun muassa ping-työkalun avulla. Moduulin viimeisessä vaiheessa hän tutustuu asentamiinsa käyttöjärjestelmiin ja harjoittelee niiden käyttämistä.



Kuvio 7 Verkkoasetusten luominen PfSense-reitittimeen

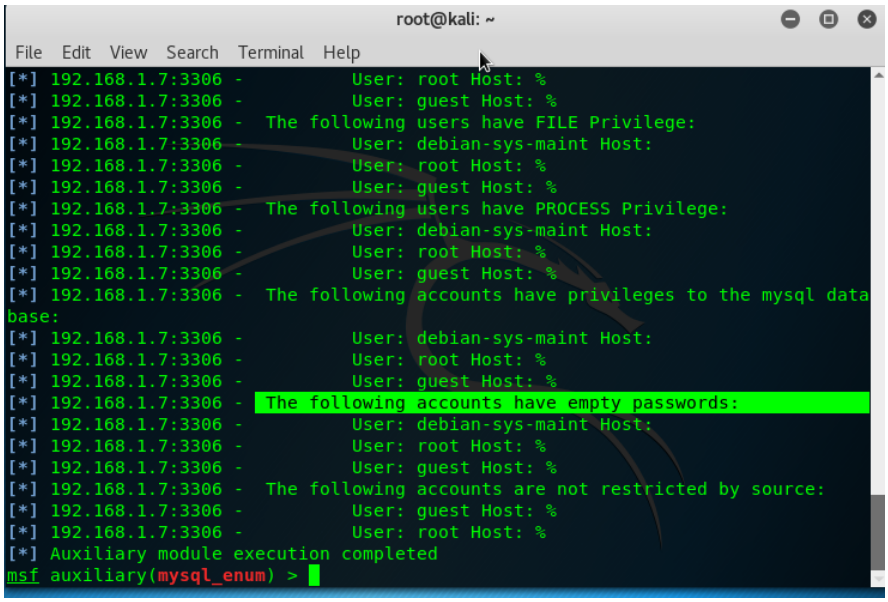
3.2.2 Tietojen kerääminen

Tietojen kerääminen -moduuli alkaa opiskelijan etsimällä itsestään tietoa käyttäen avointen lähteiden tiedustelua. Avointen lähteiden tiedustelulla (engl. Open Source Intelligence, OSINT) kerätään tietoa julkisista tai muutoin laillisesti saatavista lähteistä (Nurmi 2017, 12). Löytämänsä tiedot opiskelija esittää visuaalisesti Maltego-ohjelman avulla. Opiskelija etsii lisäksi Laurea-ammattikorkeakouluun liittyvää tietoa käyttäen muun muassa erilaisia komentoja ja ohjelmia. Kerättyään tarpeelliset tiedot, opiskelija arvioi niiden merkitystä turvallisuuden kannalta.



Kuvio 8 Kerättyjen tietojen esittäminen Maltego-ohjelmassa

Tämän jälkeen hän siirtyy Tietojen kerääminen -moduulin toiseen vaiheeseen. Opiskelija skannaa laboratorion suljettua kohdeverkkoa, tarkoituksenaan löytää sieltä aktiivisia järjestelmiä. Tarkoituksena on löytää sopivia kohteita, joiden kautta kohteeseen murtautuminen voisi onnistua. Opiskelija käyttää apunaan Nmap-ohjelmaa ja etsii sillä esimerkiksi avoimia tietoliikenneportteja. Tämän tietoliikenneportteihin kohdistuvan skannauksen tarkoituksena on pyrkiä havaitsemaan erilaisia avoinna olevia palveluita kohdeosoitteessa (Tiilikainen & Manner 2013, 3). Tämän jälkeen opiskelija kopioi kohdepalvelimelta verkkosivun ja tutustuu sen lähdekoodiin. Moduuliin viimeisessä vaiheessa opiskelija luetteloi MySQL-tietokannan tunnistaen sieltä esimerkiksi käyttäjätunnuksia ja niiden salaukseen liittyvää tietoa.



Kuvio 9 Tietokannan käyttäjätunnuksiin liittyvää tietoa

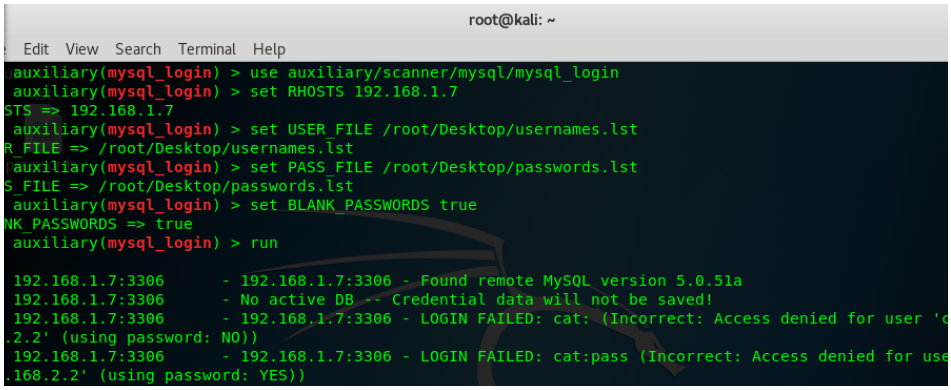
3.2.3 Murtautumistestaus

Murtautumistestaus-moduulissa opiskelijan tehtävänä on tunkeutua kohdejärjestelmään ja etsiä sieltä arvokasta tietoa. Opiskelija aloittaa harjoituksen tutustumalla Armitage-ohjelmaan. Tunnistettuaan verkosta aktiiviset järjestelmät Nmap-ohjelman avulla, hän suorittaa haavoittuvuusskannauksia, jonka jälkeen pyrkii käyttämään tunnistamiaan haavoittuvuuksia apunaan kohteeseen tunkeutumisessa.

Haavoittuvuudella tarkoitetaan alttiutta turvallisuutta uhkaaville tekijöille, esimerkiksi puutteita turvatoimissa sekä suojauksessa (Vahtiohje 2017). Esimerkkinä opiskelijan löytämästä haavoittuvuudesta on Ftp-palvelun (File Transfer Protocol)-haavoittuvuus. Kyseisen haavoittuvuuden avulla opiskelija saa etäyhteyden kohteeseen, pystyen käyttämään sitä komentorivin avulla. Saatuaan pääsyn kohteeseen, opiskelija etsii sieltä salatussa muodossa olevan salasanatiedoston. Opiskelija purkaa salaustiedot käyttämällä Johnny-ohjelmaa. Tämän jälkeen hän toistaa vastaavan kohteeseen tunkeutumisen käyttämällä Armitage-ohjelman graafisen käyttöliittymän sijasta komentoriviä Msfconsole-ohjelmalla.

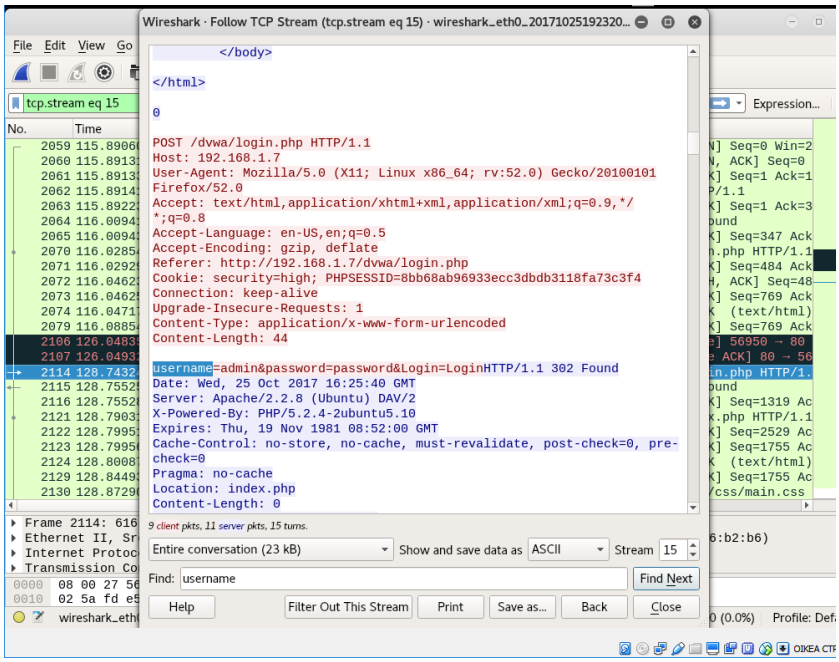
Murtautumistestaus-moduulin toisessa vaiheessa opiskelija tunkeutuu MySQL-tietokantaan käyttämällä apunaan aikaisemmin keräämäänsä tietoa. Opiskelija harjoittelee tietokannassa liikkumista ja etsii sieltä muun muassa kuvitteellisia maksukorttitietoja. Opiskelija harjoittelee MySQL-tietokantaan tunkeutumista myös väsytyshyökkäyksen (engl. Brute Force Attack)

avulla. Väsytyshyökkäyksessä opiskelija luo käyttäjätunnus- ja salasanalistat, joiden avulla ohjelma pyrkii löytämään oikean käyttäjätunnuksen ja salasanan kokeilemalla riittävän määrän tarvittavia yhdistelmiä.



Kuvio 10 Väsytyshyökkäys tietokantaan

Murtautumistestaus-moduulin toiseksi viimeisessä vaiheessa opiskelija kaappaa salaamattomana liikkuvaa tietoa laboratorion verkosta Wireshark-ohjelman avulla. Opiskelija käynnistää Wireshark-ohjelman pakettikaappauksen ja kirjautuu Metasploitable 2: IP-osoitteessa sijaitsevaan palveluun. Tämän jälkeen opiskelija palaa Wireshark-ohjelmaan ja etsii kaappaamansa, salaamattomina verkossa liikkuneet kirjautumistiedot.

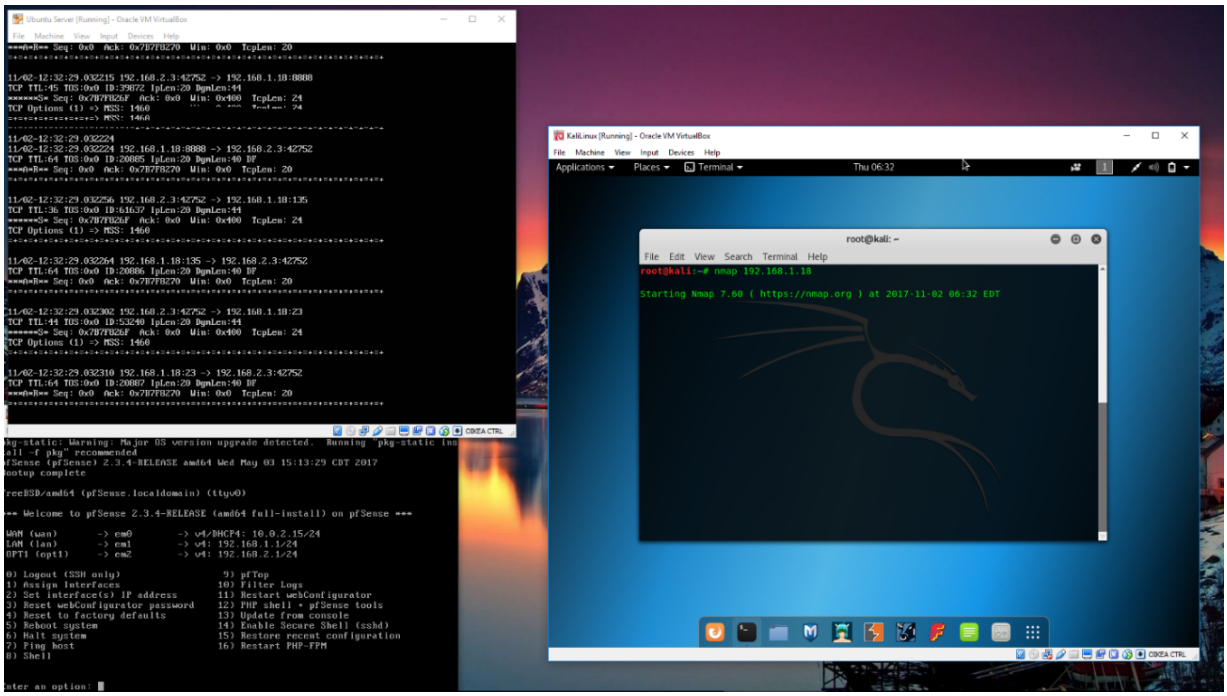


Kuvio 11 Salaamattoman tiedon kaappaaminen verkosta Wireshark-ohjelmalla.

Moduulin viimeisessä vaiheessa opiskelija nostaa Metasploitable 2 -järjestelmän rajoitetut käyttöoikeudet sisältävän käyttäjätunnuksen käyttöoikeudet niin sanotulle superuser-tasolle. Superuser on käyttöjärjestelmissä järjestelmänvalvojalle (engl. adminstrator) tarkoitettu käyttäjätunnus ja sillä on tyypillisesti peruskäyttäjää huomattavasti laajemmat käyttöoikeudet. Käyttöoikeuksien nostaminen tapahtuu käyttämällä erästä opiskelijan löytämistä haavoittuvuuksista.

3.2.4 Järjestelmän koventaminen

Järjestelmän koventaminen -moduulissa opiskelija oppii suojaamaan kohdejärjestelmän. Tämä tarkoittaa esimerkiksi hyökkäyspinta-alan kaventamista, järjestelmän päivitystä ja salasanojen vaihtamista. Hyökkäyspinta-alaa opiskelija kaventaa sulkemalla tarpeettomia tietoliikenneportteja. Koska Metasploitable 2 -järjestelmän päivittäminen on sen tarkoituksella haavoittuvaisen luoteen vuoksi estetty, korvaa hän sen Ubuntu Linux 16.04 -palvelimella. Opiskelija lataa palvelimen verkosta ja harjoittelee sen asentamista ja turvallista konfiguraatiota. Palvelimen asennettuaan hän asentaa ja konfiguroi Snort-tunkeutumisenhavaitsemisjärjestelmän, jonka avulla hän oppii tunnistamaan palvelimeen kohdistuvia tietoliikenneporttiskannauksi.



Kuvio 12 Tietoliikenneporttiskannauksen havaitseminen Snort-ohjelmalla

3.2.5 Kertaus

Kertaus-moduulissa opiskelija toistaa Murtautumistestaus-moduulin harjoituksia Järjestelmän koventaminen -moduulissa suojaamaansa järjestelmää vastaan.

4 Tutkimuksen toteutus

4.1 Laadullinen tutkimus

Laadullista tutkimusta käytetään ihmistieteissä määrällisen tutkimuksen lisäksi. Laadullinen tutkimus pyrkii ymmärtämään tutkittavaa ilmiötä. Laadullinen tutkimus eroaakin määrällisestä tutkimuksesta perustavanlaatuisesti siinä, ettei tutkimusaineiston koolla ole samanlaista merkitystä, eikä laadullisessa tutkimuksessa tehdä otoksia. Sen sijaan laadullisessa tutkimuksessa olennaista on tutkimusaineiston laatu, sillä tutkimus ei tavoittele ensisijaisesti yleistettävyyttä, kuten määrällinen tutkimus. Tutkittavien yksilöiden suuren määrän sijasta laadullinen tutkimus pyrkii tutkimaan pienempää joukkoa perusteellisemmin. Tämän vuoksi laadullisessa tutkimusmenetelmässä olennainen kysymys on, millaisella tutkimusaineistolla saadaan kattava kuvaus tutkimusongelmasta. Laadullisessa tutkimuksessa pyritään löytämään johtolankoja ja vihjeitä erilaisten aineistojen väliltä ja näiden avulla ratkaisemaan arvoituksia. Laadullisen tutkimuksen pätevyyttä ja yleistettävyyttä arvioi viimekädessä tutkimuksen lukija. Lukija perustaa arvionsa tutkimuksessa esitettyihin kuvausten, selostusten, selitysten, argumenttien ja väitteiden tarkkuuden ja vakuuttavuuden perusteella. Laadullisessa tutkimuksessa tarkka selostus tutkimuksen toteuttamisesta parantaa tutkimuksen luotettavuutta. Tutkimuksen validiutta voidaan parantaa yhdistämällä siinä kvalitatiivisia ja kvantitatiivisia elementtejä. (Hirsjärvi, Remes & Sajavaara 2010, 232-233; Vilkka 2015, 23-24).

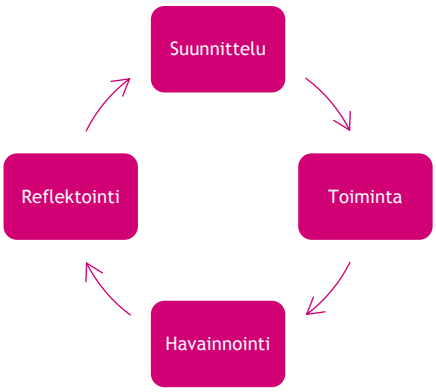
4.2 Toimintatutkimus

Tähän opinnäytetyöhön lähestymistavaksi valittiin toimintatutkimus, sillä se nähtiin tarkoituksenmukaisimmaksi lähestymistavaksi, johtuen tutkimuksen vahvasti käytäntöön suuntautuvasta kehittämistyöstä. Nimensä mukaisesti toimintatutkimus yhdistää toiminnan ja tutkimuksen. Toimintatutkimuksessa ei kuitenkaan ole kyse jokapäiväisestä työelämän kehittämisestä vaan sen lisäksi siihen kytkeytyy oleellisena osana tutkimuksellisuus. (Kananen 2014 9-11.) Toimintatutkimus on luonteeltaan osallistavaa, ja siinä pyritään ratkaisemaan käytännön ongelmia muutoksen avulla. Näin ollen se soveltuu hyvin kehittämistyön lähestymistavaksi. Toimintatutkimuksen tavoitteena on muutoksen lisäksi tuottaa uutta tietoa ja ymmärrystä ilmiöstä. Sille on ominaista ongelmakeskeisyys ja vahva käytäntöön suuntautuminen. (Ojasalo, Moilanen & Ritalahti 2014, 58.)

Toimintatutkimuksessa tuotetaan tietoa toiminnasta ja muutoksesta, jolloin vastataan kysymyksiin ”miten tutkittavat kohteet voivat muuttua?” tai ”mikseivät ne muutu?”. Toimintatutkimuksessa muutos voi siis joko tapahtua tai olla tapahtumatta. On myös mahdollista, että muutos on toisenlainen kuin aluksi suunniteltiin. Toimintatutkimuksen haaste on siinä, että se

on vahvasti tutkimuskohteeseen sidottu, jonka vuoksi muiden aikaisempia tutkimuksia ja tuloksia on vaikea hyödyntää. Lähtökohtiensa vuoksi, toimintatutkimus soveltuu erityisen hyvin tutkimukselliseen kehittämistyöhön ja kohteena voi olla mikä tahansa ihmiselämään liittyvä ilmiö. Toimintatutkimus ei ole kiinnostunut vain siitä, miten asiat ovat, vaan ennemminkin siitä, miten niiden tulisi olla. Koska toimintatutkimus pyrkii todellisuuden muuttamiseen, on se käytännön toiminnan ja teoreettisen tutkimuksen vuorovaikutusta. (Ojasalo ym. 2014, 58 – 60.)

Toimintatutkimus ei varsinaisesti ole oma tutkimusmenetelmä, vaan pikemminkin tutkimusstrategia, joka yhdistää erilaisia tutkimusmenetelmiä. Toimintatutkimus on prosessina syklinen, tyypillisesti koostuen suunnittelusta, toiminnasta, havainnoinnista sekä reflektoinnista. Toimintatutkimuksen prosessi on esitetty kuviossa 13. (Kananen 2014, 61.)



Kuvio 13 Toimintatutkimuksen prosessi (Kananen 2014, 61.)

Toimintatutkimus katsotaan yleensä laadulliseksi lähestymistavaksi, mutta siinä voidaan hyödyntää myös määrällisiä menetelmiä. Koska kyse on osallistavasta tutkimuksesta ja kehittämisestä, on myös valittavien menetelmien oltava osallistavia. Osallistavat menetelmät mahdollistavat pääsyn kohdeorganisaation hiljaiseen tietoon. Tutkimusaineisto on mahdollista kerätä muun muassa kyselyllä, haastattelulla ja havainnoimalla. Erityisesti havainnointia pidetään toimintatutkimuksessa tehokkaana tiedonkeruumenetelmänä. (Ojasalo ym. 2014, 67.)

4.3 Tiedonkeruumenetelmät

Kuten toimintatutkimuksissa yleisesti, niin myös tämä opinnäytetyö yhdistää laadullisia ja määrällisiä menetelmiä. Laadullisina menetelminä tutkimuksessa on opiskelijoiden havain-

nointi ja haastattelu, määrällisenä menetelmänä puolestaan käytetään kyselyjä, jotka mittaavat opiskelijoiden osaamisen alku- ja lopputasoa sekä kartoittavat heidän mielipiteitään tämän tyylisestä toiminnasta.

4.3.1 Havainnointi

Tiedonkeruumenetelmänä havainnointi ei ole tapahtuman satunnaista seuraamista, vaan sen systemaattista tarkkailua. Havainnoinnin avulla on mahdollista saada tietoa esimerkiksi siitä, miten ihmiset käyttäytyvät. Tiedonkeruumenetelmänä havainnointia voidaan käyttää itsenäisesti tai esimerkiksi haastattelun ja kyselytutkimuksen tukena. Havainnoinnilla on myös mahdollista täydentää kyselytutkimusta tai haastattelua. (Ojasalo ym. 2014, 116.)

Havainnointi soveltuu hyvin kehittämistehtäviin, kun tarkoituksena on tutkia yksilön toimintaa tai vuorovaikutusta muiden kanssa. Havainnoinnin avulla voidaan esimerkiksi selvittää mitä kohde tekee tai miten se toimii. Tiedonkeruumenetelmänä havainnoinnin on oltava mahdollisimman järjestelmällistä. Havainnoinnissa tulee ennakolta määritellä, millaisia asioita havainnoidaan, mihin havainnointi kohdistetaan ja tulokset tulee kirjata välittömästi tutkimuspäiväkirjaan. Havainnointi on joko strukturoitua tai strukturoimatonta. Strukturoimattomassa havainnoinnissa ongelma jäsennellään ennen havainnointia. Strukturoitua havainnointia käytetään silloin, kun halutaan mahdollisimman paljon ja monipuolista tietoa asiasta. Havainnointitekniikasta riippumatta, sille on määriteltävä tavoitteet ja päätettävä havainnoinnilta vaadittava tarkkuus. (Ojasalo ym. 2014, 116 – 118.)

Havainnoinnin tarkoituksena on kyetä muodostamaan havainnoitavasta asiasta looginen kokonaisuus ja löytämään punainen lanka sen taustalta. Havainnoimalla saatavien laadullisten tulosten analyysi syntyy kahdessa vaiheessa – pelkistämisessä ja tulkinnassa. Pelkistämisvaihe yhdistää havainnot, ja tulkintavaihe mahdollistaa pelkistettyjen havaintojen tulkinnan. (Ojasalo ym. 2014, 118.)

4.3.2 Haastattelu

Haastattelu tiedonkeruumenetelmänä eroaa tavallisesta keskustelusta siten, että haastateltava pyrkii ohjaamaan keskustelua aineiston keräämisen kannalta tarkoitukselliseen suuntaan. Haastattelu on käyttökelpoista esimerkiksi silloin, kun tutkimuksen tarkoituksena on tutkia jonkin ilmiön merkitystä osallistujille. (Ojasalo ym. 2014, 106 – 108.)

Haastattelumenetelmiä on erilaisia ja oikean menetelmän valinta tapahtuu sen perusteella, millaista ja miten tarkkaa tietoa sillä halutaan kerätä. Haastattelut tyypillisesti nauhoitetaan, jonka jälkeen ne litteroidaan, eli kirjoitetaan auki. Litteroinnin tarkkuus voi vaihdella tutkimuksen mukaan. Mikäli ollaan esimerkiksi kiinnostuneita vain vastausten sisällöstä, voidaan

litterointi toteuttaa yleiskielisenä, eikä sen tarvitse huomioida esimerkiksi haastateltavan äänenpainoja. (Ojasalo ym. 2014, 107.)

Tässä tutkimuksessa haastattelu toteutettiin avoimena haastatteluna vapaaehtoiseksi ilmoittautuneen opiskelijan kanssa. Haastattelu nauhoitettiin ja siinä käytiin läpi havainnoinnissa tunnistettuja, tutkimuksen kannalta olennaisia teemoja. Nämä tunnistetut teemat olivat: laboratorio ja laboratorioharjoitukset, opiskelijoiden suoriutuminen ja motivaatio sekä opiskelijoiden osaamisen kehittyminen. Vapaaehtoiseksi haastateltavaksi ilmoittui yksi opiskelija ja haastattelu kesti noin viisitoista minuuttia.

4.3.3 Kysely

Kysely on tutkimuksille hyvin tyypillinen tiedonkeruumenetelmä. Kyselyn etuna voidaan nähdä se, että sen avulla voidaan kerätä laajoja tutkimusaineistoja hyvin suurelta joukolta. Lisäksi se on nopea ja tehokas tiedonkeruumenetelmä. Kyselytutkimuksilla tyypillisesti saadaan numeerisia tuloksia, joita voidaan käsitellä esimerkiksi tilastollisesti. Kyselyn heikkoutena voidaan pitää sen tuottaman tiedon pinnallisuutta. On myös mahdotonta arvioida, miten vakavasti vastaajat ovat suhtautuneet tutkimukseen, miten he ovat tulkinneet vastausvaihtoehtoja tai miten tietoisia he ovat tutkittavasta aiheesta. ”Vakiotulkinnan mukaan kvantitatiivisilla menetelmillä saadaan pinnallista mutta luotettavaa tietoa ja kvalitatiivisilla menetelmillä syvällistä mutta huonosti yleistettävää tietoa.” (Ojasalo ym. 2014, 121-122.)

Vaikka kysely tyypillisesti mielletään määrälliseksi tiedonkeruumenetelmäksi, voidaan sitä käyttää myös laadullisena tiedonkeruumenetelmänä. Kyselyjä tehtiin kaksi kappaletta, jotka mittasivat opiskelijoiden osaamisen alku- ja lopputasoa. Lopputasomittauksen yhteydessä kartoitettiin lisäksi opiskelijoiden kokemuksia laboratorioharjoituksista ja laboratoriosta. Kyselytutkimuksiin osallistui molemmilla kerroilla seitsemän opiskelijaa. Opiskelijat vastasivat seitsemään heidän osaamistaan arvioivaan kysymykseen sekä lopputasomittauksessa myös seitsemään heidän kokemuksiaan kartoittavaan kysymykseen.

Kyselyissä oli osaamiseen liittyviä väitteitä, joihin vastattiin suljetulla neliportaisella Likertin asteikolla. Kysymykset ja vastausvaihtoehdot olivat englannin kielellä, mutta tässä opinnäytetyössä ne käsitellään suomen kielellä. Vastausvaihtoehdot olivat täysin samaa mieltä (engl. strongly agree), osin samaa mieltä (engl. agree), osin eri mieltä (engl. disagree) ja täysin eri mieltä (engl. strongly disagree). Kyselyissä käytetyt kysymykset on esitetty alla taulukossa 1.

Kysymys	Alku- ja loppumittaus	Opiskelijoiden kokemukset
1	Tiedän mitä tietoverkkoturvallisuus on käytännössä.	Suosittelisin näitä harjoituksia muille opiskelijoille.
2	Tiedän millainen on murtautumistestausprosessi.	Laboratorioharjoitukset lisäsivät kiinnostustani aiheitta kohtaan.
3	Tiedän miten järjestelmien turvallisuutta arvioidaan murtautumistestauksella.	Laboratorioharjoitusten vaikeustaso oli sopiva.
4	Tiedän miten järjestelmistä etsitään haavoittuvuuksia.	Laboratorioharjoitusten määrä oli sopiva.
5	Tiedän miten haavoittuvuuksia voidaan käyttää apuna kohteeseen tunkeutumisessa.	Suoritettuani kurssin, koen tietämykseni lisääntyneen aiheesta.
6	Tiedän miten verkosta tunnistetaan aktiivisia järjestelmiä, esimerkiksi Nmap-ohjelmalla.	Laboratorioharjoitusten ohjeet olivat selkeitä.
7	Tiedän miten järjestelmä suojataan palomuurin avulla, esimerkiksi Iptables-ohjelmalla.	Suosittelen käytettyjen laboratorioharjoitusten käyttämistä tulevilla opintojaksoilla

Taulukko 1 Käytetyt kysymykset

Kyselyllä saatavia tuloksia ei kuitenkaan käsitellä käyttämällä määrällisen tutkimuksen menetelmiä, vaan osana laadullista tutkimusta. Kyselyiden tarkoituksena on selvittää opiskelijoiden osaamistason muutosta ja heidän kokemuksiaan tällaisesta toiminnasta. Näin ollen tarkoituksena on ensisijaisesti nostaa tutkimuksen luotettavuutta ja vahvistaa havainnoimalla ja haastattelulla saatuja tuloksia.

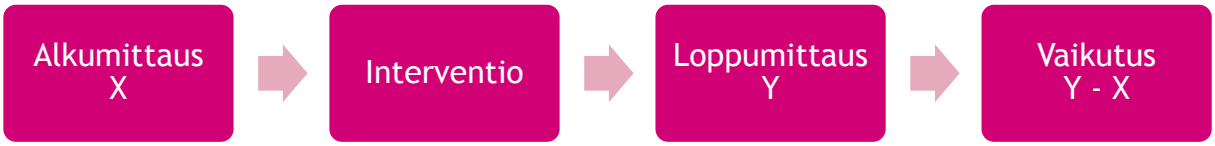
4.4 Aineiston analysointi

Analyysi tarkoittaa monimutkaisen ongelman pilkkomista pieniin, erillisiin osiin, jotka ratkaisemalla kokonaisongelma toivotaan pystyttävän ratkaisemaan. Laadullisen tutkimuksen analyysin tarkoituksena on esimerkiksi vastausten saaminen tutkimustehtävään, oleellisen aineiston erottaminen ja tutkimuksen luotettavuuden varmistaminen. Tyypillisesti laadullisen aineiston analyysi alkaa litteroimisella, eli tekstimuotoon purkamisella. Aineistoa luetaan ja reflektoidaan ja siitä pyritään ymmärtämään sen todellinen sisältö. Tämän jälkeen aineistoon yhdistetään muuta kerättyä aineistoa, jonka jälkeen sieltä etsitään tutkimusta kiinnostavia

asioita. Lopuksi aineisto alkaa pelkistymään, jonka jälkeen on mahdollista tehdä johtopäätöksiä. (Kananen 2014, 106.)

Aineisto kerätiin harjoituksiin osallistuneilta seitsemältä opiskelijalta. Suoralla havainnoinnilla ja avoimella haastattelemalla saatu aineisto litteroitiin, eli muutettiin tekstimuotoon. Litterointi toteutettiin propositiotasolla, eli kirjaamalla havaintojen ja haastattelun ydinsisältö ylös. Litteroinnin jälkeen aineisto on teemoiteltiin.

Teemoittelu on perusmenetelmä laadullisessa analyysissä. Teemoittelun avulla pyritään hahmottamaan eri aineistoja yhdistäviä aiheita, eli teemoja. Teemaksi voidaan hahmoittaa aiheita, jotka toistuvat aineistossa. Teemoittelu etenee niiden muodostamisesta kohti tarkempaa tarkastelua. (Kananen 2014, 108.) Teemoittelun jälkeen aineisto vedettiin yhteen ja sieltä etsittiin vastauksia tutkimuskysymyksiin. Tutkimuksen luotettavuutta pyrittiin parantamaan yhdistämällä toisiaan tukevia ja täydentäviä tiedonkeruumenetelmiä. Tiedonkeruumenetelmänä ei siis käytetty ainoastaan tutkijan tekemiä havaintoja, vaan näitä havaintoja vahvistettiin haastattelulla ja kyselyillä. Kyselyissä opiskelijoiden osaamistason muutosta alku- ja loppumittauksen välillä arvioitiin vertaamalla niitä keskenään, kuvion 14 osoittamalla tavalla.



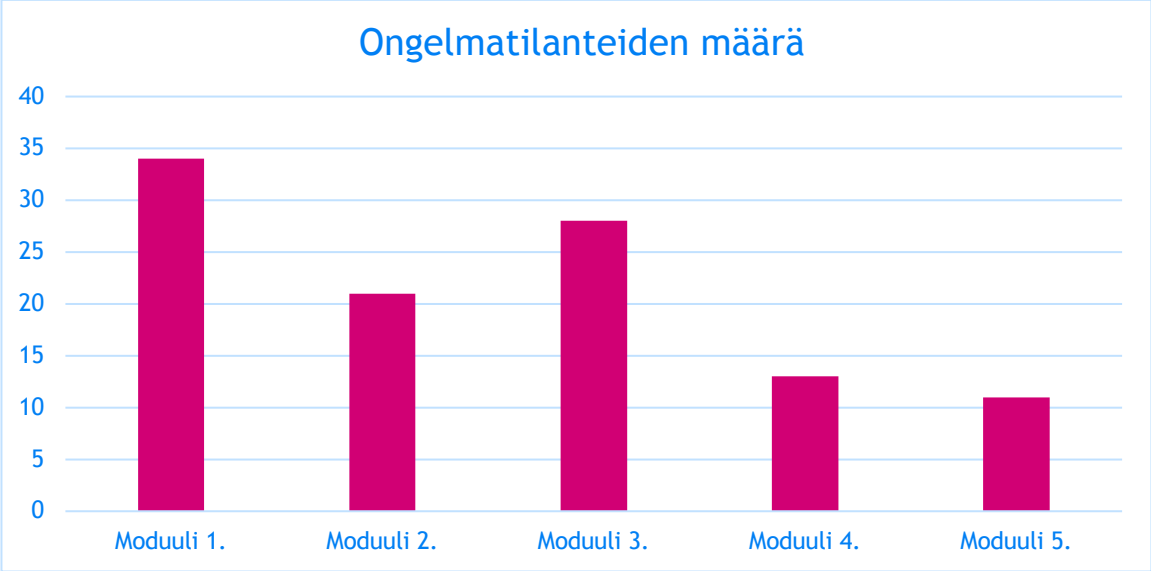
Kuvio 14 Toiminnan vaikutuksen toteaminen (Kananen 2014, 119)

5 Tulokset

5.1 Havainnointi

Tässä tutkimuksessa havainnointi tapahtui käyttämällä suoraa havainnointia. Suoralla havainnoinnilla tarkoitetaan tilannetta, jossa tutkija on tilanteessa läsnä ja seuraa sitä paikan päällä (Kananen 2014, 80). Havainnointi oli samanaikaisesti strukturoitua ja strukturoimatonta. Strukturoidussa havainnoinnissa päätettiin kirjata kunkin moduulin ongelmatilanteiden määrä, eli ne tilanteet, joissa opiskelija ei osannut ratkaista ongelmaa itsenäisesti ja tarvitsi tähän apua. Usein nämä liittyivät tilanteeseen, jota opiskelija ei hetken pohtimisen jälkeen osannut ratkaista itse. Esimerkkinä tällaisesta on tilanne, jossa verkko eri laitteiden välillä ei toiminut johtuen opiskelijan virheellisestä verkkokonfiguraatiosta. Strukturoimatonta havainnointia oli

kaikki muu ja se liittyi esimerkiksi opiskelijoiden suoriutumiseen ja motivaatioon. Ongelmatilanteiden määrä on esitetty kuviossa 15.



Kuvio 15 Ongelmatilanteiden määrä kappaleittain eri moduulien välillä.

Havainnoimalla oli mahdollista havaita opiskelijoiden osaamistason kehittymistä. Opiskelijoiden lähtötaso vaihteli opintojakson alussa. Muutamalla opiskelijalla aiheesta oli jonkinlaista kokemusta, mutta valtaosalle aihe oli uusi. Suurimmat vaikeudet opiskelijoiden suoriutumisessa liittyivät Linux-käyttöjärjestelmän ja erilaisten komentoriviin syötettävien komentojen käyttämiseen. Juuri näihin seikkoihin liittyi myös eniten ongelmatilanteita, eli tilanteita, joita opiskelija ei osannut ratkaista itse ja pyysi ohjaajalta apua. Havainnoinnin yhteydessä tutkimuspäiväkirjaan kirjattiin ongelmatilanteita kaikissa moduuleissa. Ongelmatilanteiden määrä oli suurin Laboratorion luominen -moduulissa (34 kappaletta) ja Murtautumistestaus-moduulissa (27 kappaletta). Opiskelijat kuitenkin selvästi kehittyivät, sillä he kykenivät Kertaus-moduulissa suoriutumaan Murtautumistestaus-moduulin harjoituksista hyvin itsenäisesti. Huomionarvoista on myös se, että harjoitusten suorittaminen Kertaus-moduulissa oli haastavampaa. Kertaus-moduulissa kirjattiin ongelmatilanteita 11 kappaletta. Ongelmatilanteiden määrän putoamisen lisäksi opiskelijoiden kehittymistä oli mahdollista nähdä havainnoimalla. Opiskelu muuttui loppua kohti itsenäisemmäksi, jolloin opiskelijat hakivat tietoa itse verkosta ja auttoivat toisiaan.

Laboratorio oli ratkaisuna toimiva ja siinä ei esiintynyt rakenteellisia ongelmia. Kaikki luodut harjoitukset oli mahdollista suorittaa laboratoriossa. Laboratorion luomisessa opiskelijoilla oli

kuitenkin pieniä haasteita, sillä esimerkiksi opiskelijoiden näppäinvirheet ja virheelliset konfiguraatiot estivät sen toimimisen. Tällaisen virheen paikantaminen ja korjaaminen veivät myös paljon aikaa. Tuntemattomasta syystä opiskelijat, jotka käyttivät omia Linux-käyttöjärjestelmällisiä laitteitaan, kokivat eniten verkko-ongelmia. Laboratorion käyttöä vaikeuttikin yleisesi lähinnä verkkoasetukset ja niiden säätäminen eri harjoitusten välillä. Verkkoasetuksia piti välillä muokata, sillä suljettuna ympäristönä laboratoriosta ei lähtökohtaisesti ollut yhteyttä Internetiin. Internet-yhteyttä tarvittiin esimerkiksi Snort-ohjelman latauksen yhteydessä.

5.2 Kysely

Opiskelijoiden osaamistasoa selvittävissä alku- ja loppumittauksissa havaittiin kehitystä kaikilla osa-alueilla. Eniten kehitystä tapahtui alueilla, joita käytettiin paljon. Alkumittaus toteutettiin ensimmäisellä laboratorioharjoitusten ohjauskerralla lokakuun alussa. Loppumittaus toteutettiin marraskuun lopussa laboratorioharjoituksia koskevan tentin jälkeen. Näihin mittauksiin osallistui molemmilla kerroilla seitsemän opiskelijaa ja he kaikki vastasivat niihin. Alku- ja loppumittausten tulokset on esitetty kuviossa 16. Opiskelijoiden osaamistason lisäksi kartoitettiin heidän kokemuksiaan tämän tyylisestä koulutuksesta. Opiskelijoiden kokemukset on esitetty kuviossa 17.

Kysymyksessä 1. alkumittauksessa ainoastaan yksi opiskelija oli osin samaa mieltä väitteen ”*tiedän mitä tietoverkkoturvallisuus on käytännössä*” kanssa. Loppumittauksessa osin samaa mieltä oli neljä ja täysin samaa mieltä väitteen kanssa kaksi opiskelijaa.

Kysymyksessä 2. alkumittauksessa kaksi opiskelijaa oli osin samaa mieltä väitteen ”*tiedän millainen on murtautumistestausprosessi*” kanssa. Opintojakson lopussa neljä opiskelijaa oli väitteen kanssa osin samaa mieltä ja kaksi täysin samaa mieltä.

Kysymyksessä 3. alkumittauksessa yksikään opiskelija ei ollut samaa mieltä väitteen ”*tiedän miten järjestelmien turvallisuutta testataan murtautumistestauksen avulla*” kanssa. Loppumittauksessa neljä oli osin samaa mieltä ja yksi täysin samaa mieltä.

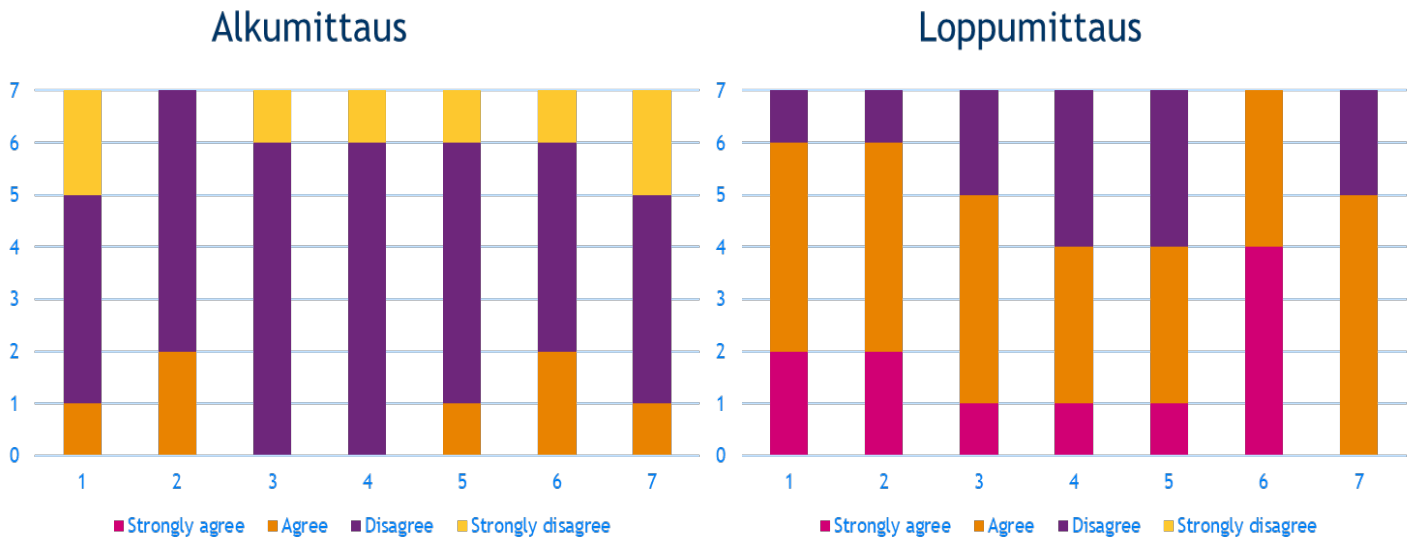
Kysymyksessä 4. alkumittauksessa yksikään opiskelija ei ollut samaa mieltä väitteen ”*tiedän miten järjestelmistä etsitään haavoittuvuuksia*” kanssa. Loppumittauksessa kolme opiskelijaa oli osin samaa mieltä ja yksin täysin samaa mieltä.

Kysymyksessä 5. alkumittauksessa yksi opiskelija oli osin samaa mieltä väitteen ”*tiedän miten haavoittuvuuksia voidaan käyttää apuna kohteeseen tunkeutumisessa*” kanssa. Loppumittauksessa kolme opiskelijaa oli osin samaa mieltä ja yksin täysin samaa mieltä väitteen kanssa.

Kysymyksessä 6. alkumittauksessa kaksi opiskelijaa oli osin samaa mieltä väitteen ”*tiedän miten verkosta tunnistetaan aktiivisia järjestelmiä, esimerkiksi Nmap-ohjelman avulla*” kanssa.

Loppumittauksessa väitteen kanssa oli osin samaa mieltä kolme ja täysin samaa mieltä neljä henkilöä.

Kysymyksessä 7. alkumittauksessa yksi opiskelija oli osin samaa mieltä väitteen ”*tiedän miten järjestelmä suojataan palomuurin avulla, esimerkiksi Iptables-ohjelmalla.*” Loppumittauksessa väitteen kanssa oli osin samaa mieltä viisi opiskelijaa.



Kuvio 16 Alku- ja loppumittausten tulokset

Opiskelijoiden kokemuksia kartoittavassa kyselyssä kysymykseen ”minkä arvosanan antaisit laboratorioharjoituksille” piti niitä kaksi opiskelijaa niitä erinomaisina. Erittäin hyvinä niitä piti kaksi ja hyvinä kolme opiskelijaa. Kukaan opiskelija ei kokenut harjoituksia menettelevíksi eikä surkeiksi.

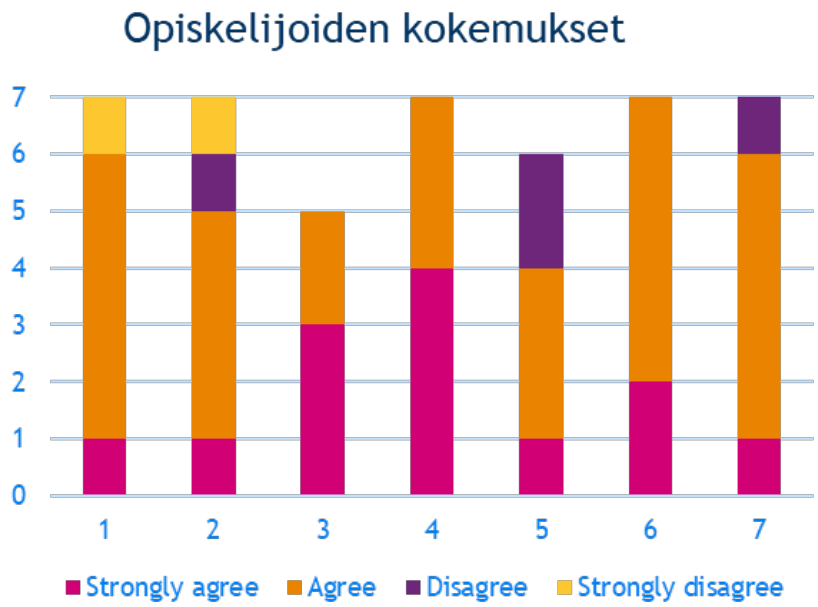
1. Kysymyksessä väitteen ”*suosittelisin näitä laboratorioharjoituksia muille opiskelijoille*” kanssa osin samaa mieltä oli viisi ja täysin samaa mieltä yksi opiskelija.

2. Kysymyksessä väitteen ”*Laboratorioharjoitukset lisäsivät kiinnostustani aihetta kohtaan*” kanssa oli osin samaa mieltä viisi ja täysin samaa mieltä yksi opiskelija.

Kysymyksissä 3, 4 ja 6, kaikki vastanneet opiskelijat olivat ainakin osin samaa mieltä siitä, että laboratorioharjoitusten ohjeistukset olivat selkeitä, sekä laboratorioharjoitustenharjoitusten määrä ja vaikeustaso olivat sopivia. Kaikki eivät vastanneet kysymyksiin 3 ja 5.

5. Kysymyksessä väitteen ”*suoritettuani kurssin, koen tietämykseni lisääntyneen aiheesta*” kanssa osin samaa mieltä oli kolme ja täysin samaa mieltä yksi opiskelija.

7. Kysymyksessä kysyttäessä ”*suosittelen näiden ohjeiden käyttämistä tulevilla opintojaksoilla*”, viisi oli osin samaa mieltä ja yksi täysin samaa mieltä.



Kuvio 17 Opiskelijoiden kokemukset.

5.3 Haastattelu

Haastattelu toteutettiin puhelimitse vapaaehtoiseksi ilmoittautuneen opiskelijan kanssa 12.12.2017. Haastateltava koki laboratorion hyvänä eikä hänellä esiintynyt merkittäviä ongelmia sen käytössä. Hän koki laboratorion luomisen työlääksi, mutta ei merkittävällä tavalla vaikeaksi. Hän kertoi erityisesti verkkoasetusten vaihtelemisen harjoitusten välillä aiheuttaneen hämmennystä, koska hän ei ymmärtänyt miksi niin tehtiin. Haastateltava kokisi valmiiksi luodun ympäristön helpompana. (Haastattelu 2017.)

Haastateltava koki suoriutuneensa harjoituksista kahden ensimmäisen moduulin jälkeen hyvin jälkeen hyvin. Vaikeinta hänen mielestään oli uusien Linux-käyttöjärjestelmien käyttäminen ja niihin liittyvät ongelmat. Komentorivin käyttämistä hän ei pitänyt kovinkaan vaikeana, sillä ohjeet olivat selkeät ja ne etenivät vaihe vaiheelta. Kuvattaessa tuloksia ongelmatilanteiden määrästä, haastateltava yhtyi niihin, kokien ensimmäisen ja kolmannen moduulin vaikeimmiksi ja mainitsi kaksi viimeisintä helpoimmiksi. Kysyttäessä miksi näin on, hän arveli labora-

torion tutuksi tulemisen ja harjoitusten päämäärän selviämisen helpottaneen hänen suoriutumistaan. Hän piti harjoituksia mielenkiintoisina ja oli niitä kohtaan motivoitunut erityisesti ammattinsa puolesta. Hän piti lähiopetuksessa tapahtuvia laboratorioharjoituksia hyvinä, sillä hän koki erityisesti aluksi tarvitsevansa niihin paljon apua. (Haastattelu 2017.)

Haastateltava koki laboratorioharjoitusten vaikuttaneen hänen oppimiseensa selkiyttämällä opintojaksolla muuten käsiteltävää teoriaosuutta, siihen liittyviä käsitteitä sekä sitä, miten asiat liittyvät toisiinsa. Tällä hän tarkoitti kertomansa mukaan sitä, että oli helpompaa hahmottaa isoa kuvaa ja esimerkiksi sitä, miten tiedon kerääminen liittyy myöhempään murtautumisvaiheeseen. (Haastattelu 2017.)

6 Johtopäätökset

Opinnäytetyössä etsittiin vastauksia kolmeen kysymykseen:

1. Edistävätkö laboratorioharjoitukset opiskelijoiden osaamista?
2. Onko laboratorio toimiva?
3. Mitä mieltä opiskelijat ovat laboratorioharjoituksista?

Laboratorioharjoitukset edistivät opiskelijoiden osaamista. Tätä tukee tulokset alku- ja loppumittausten välillä, ongelmatilanteiden määrässä ja haastateltavan kokemuksissa. Alku- ja loppumittauksissa havaittiin kaikilla osa-alueilla selkeää kehitystä opiskelijoiden osaamisen tasossa. Eniten osaaminen kehittyi osa-alueilla, joita käytettiin paljon. Esimerkkinä tästä aktiivisten järjestelmien tunnistamista Nmap-ohjelmalla koskeva kysymys, jossa kaikki vastaajat olivat vähintään osin samaa mieltä. Johtopäätöstä opiskelijoiden osaamisen kehittymisestä tukee myös se, että ongelmatilanteiden määrä väheni loppua kohden, vaikka vastaavasti harjoitusten vaikeustaso nousi. Lisäksi haastateltava mainitsi harjoitusten selkiyttäneen myös opintojakson teoriaosuutta.

Laboratorio oli kokonaisuutena toimiva ja kaikki luodut harjoitukset oli mahdollista suorittaa sen avulla. Laboratorion luominen oli kuitenkin haastavaa, jota tukee tulos ongelmatilanteiden määrässä, sillä se oli Laboratorion luominen -moduulissa suurin. Myös laboratorion asetusten vaihtaminen kesken harjoituksia aiheutti hämmennystä ja erilaisia ongelmia. Lisäksi haastateltava kertoi kokeneensa sen työläänä.

Kokonaisuutena opiskelijat kokivat laboratorioharjoitukset hyvinä ja mielekkäinä. Tätä tutkittiin kyselyn avulla. Harjoitusten määrää ja vaikeustasoa selvittäviin kysymyksiin kaikki vastanneet vastasivat olevansa vähintään samaa mieltä siitä, että ne ovat sopivia. Lisäksi lähes kaikki suosittelisivat harjoituksia muille opiskelijoille sekä käyttäisivät nyt luotuja harjoituksia tulevilla opintojaksoilla.

7 Pohdinta ja kehittämisehdotukset

Tutkimusta voi kritisoida siitä, ettei opintojakson teoriaosuuden vaikutusta voida poissulkea opiskelijoiden osaamista mittaavista kyselyistä. Jälkikäteen tarkasteltuna myös käytetyt kysymykset voisivat olla tarkempia ja niitä voisi olla määrällisesti enemmän. Lisäksi haastateltavaksi ilmoittautui seitsemästä opiskelijasta ainoastaan yksi vapaaehtoinen, joten haastattelulla saadut tulokset perustuvat ainoastaan hänen mielipiteisiinsä. Vaikka tutkimus ei ole täydellinen, voidaan sillä mielestäni perustella tämänkaltaisen toiminnan tärkeys ja jatkuvuus osana Laurea-ammattikorkeakoulun kyberturvallisuuskoulutusta.

Opinnäytetyössä kehitetty malli oli hyvä ja sillä oli positiivinen vaikutus opiskelijoiden osaamiseen. Mielestäni näistä syistä tätä toimintaa tulee kehittää jatkossakin ja viedä myös muille opintojaksoille. Koska Laurea-ammattikorkeakoulun kyberturvallisuusopetus tapahtuu pääosin verkko-opintoina, voidaan myös tämä käytännön harjoittelu toteuttaa ilman lähiopetusta kahdella tapaa:

Ensimmäisessä mallissa opiskelija luo laboratorion omalle tietokoneelleen ja suorittaa harjoituksia itsenäisesti. Tämän mallin ongelmana on kuitenkin se, että laboratorion virtualisointi edellyttää käytetyltä laitteelta tiettyjä vähimmäistehovaatimuksia, johon kaikilla opiskelijoilla ei välttämättä ole mahdollisuutta. Esimerkiksi puhtaasti opiskelukäyttöön tarkoitetut, alimman hintaluokan kannettavat tietokoneet eivät välttämättä tätä vähimmäistehovaatimusta täytä.

Toisessa mallissa laboratorio toteutetaan Microsoft Azure -pilvipalvelussa. Myös tässä mallissa opiskelijat suorittaisivat harjoituksia omilla laitteillaan. Tämä käytännössä poistaisi opiskelijan käyttämältä laitteelta vaaditun vähimmäistehovaatimuksen, sillä opiskelijat suorittaisivat harjoituksia käyttämällä pilvipalvelun resursseja. Ongelmana tässä mallissa on kuitenkin se, ettei kohteina toimivia virtuaalitietokoneita, kuten Metasploitable 2:ta voida Azureen suoraan asentaa. Laboratorio voidaan kuitenkin toteuttaa käyttämällä Nested Virtualization -tekniikkaa, joka on mahdollista toteuttaa tällä hetkellä Windows Server 2016 -käyttöjärjestelmällä. Nested Virtualization mahdollistaa virtuaalitietokoneiden luomisen Azuressa toimivan virtuaalitietokoneen sisään. (Fan, 2017.) Azuren käyttöehdot ja siihen sovellettava lainsäädäntö saattavat kuitenkin aiheuttaa rajoituksia.

Käytännön harjoittelu voidaan jatkossakin toteuttaa lähiopetuksessa suoraan käyttämällä nyt luotua laboratoriota. Laboratorio ja harjoitukset soveltuvat sellaisenaan tuleville Network Security -opintojaksoille. Tämän lisäksi nyt luotu laboratorio soveltuu myös sellaisenaan esimerkiksi Enterprise Applications Security -opintojaksolle, sillä Metasploitable 2 -järjestelmä mahdollistaa myös verkkosovellusten (engl. web application) murtautumistestauksen.

Kaikissa edellä esitetyissä malleissa laboratorio olisi hyvä tarjota valmiina kokonaisuutena. Tämä voidaan toteuttaa Virtualbox-ohjelmassa käyttämällä valmiiksi konfiguroituja virtuaalikovalevyjä, joiden asentaminen helpoittaa laboratorion luomista merkittävästi.

Kokonaisuutena opinnäytetyö oli onnistunut kokemus. Haasteita aiheutti tutkijan henkilökohtaisista syistä tiukentunut valmistumisaikataulu, jonka vuoksi opinnäytetyö tuli saada pääosin valmiiksi vuoden 2017 aikana. Lisäksi harjoitusten luominen, ohjaaminen ja niitä koskevan tentin valmistelu osoittautuivat arvioitua työläämmiksi ja haastavammiksi. Opinnäytetyö kuitenkin pysyi sekä tutkijan että asiakkaan aikataulussa. Opinnäytetyö oli myös opettavainen kokemus. Erityisesti osaamista kertyi teknisestä tietoverkkoturvallisuudesta, virtualisoinnista ja kouluttamisesta. Työ myös toteutettiin hyvin tiiviissä työelämäyhteistyössä ratkaisten oikeita ja tärkeitä ongelmia. Lisäksi asiakas oli lopputulokseen tyytyväinen.

Lähteet

Painetut

Gobb, S. 2016. Mind this gap: criminal hacking and the global cybersecurity skills shortage, a critical analysis. Virusbulletin 2016.

Hirsjärvi, S., Remes, P., Sajavaara, P. 2010. Tutki ja kirjoita. 16. painos. Helsinki: Tammi.

Kananen, J. 2014. Toimintatutkimus kehittämistutkimuksen muotona: miten kirjoitan toimintatutkimuksen opinnäytetyönä? Helsinki: Suomen yliopistopaino.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston kanslia 2017.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docenco

Limnéll, J. 2014. Kyber rantautui Suomeen. Helsinki: Aalto-yliopisto

Myllyä J. & Lindfors, T. Laboratorioharjoituksia kyberturvallisuuden opiskelijoille. 2017. Espoo: Laurea-ammattikorkeakoulu.

Nurmi, P. 2017. Avointen lähteiden Internet-tiedustelu. Helsinki: Aalto-yliopisto.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro

Oriyano, S-P. 2016. Certified Ethical Hacker Version 9. New Yersey: John Wiley & Sons

Rathod, P. 2014. Information and Cybersecurity Education. Espoo: Laurea-ammattikorkeakoulu

Tiilikainen, S. & Manner, J. 2013. Suomen automaatioverkkojen haavoittuvuus. Helsinki: Aalto-yliopisto

Vilkka, H. Tutki ja kehitä. 2015. 4. painos. Jyväskylä: PS-kustannus

Wang, J. & Kissel, Z. 2015. Introduction to Network Security. New Yersey: John Wiley & Sons

Sähköiset

AV-Test Institute. 2017. Total Malware.
https://www.av-test.org/en/statistics/malware/

Dethlefs, R. 2015. How cyber attacks became profitable. Viitattu 21.12.2017
http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/

Europol. 2017. Internet Organized Crime Threat Assessment. Viitattu 3.1.2017
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

ISO/IEC. 2012. Guidelines for cybersecurity. Viitattu 4.1.2017

https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Joy, F. 2017. Nested Virtualization in Azure. Viitattu 5.1.2017
https://azure.microsoft.com/en-us/blog/nested-virtualization-in-azure/

Laurea-ammattikorkeakoulu. 2017. Organisaatio. Viitattu 13.11.2017
https://www.laurea.fi/laurea/laurea-organisaationa/organisaatio

National Crime Agency. 2016. Cyber Crime Assessment. Viitattu 28.12.2017
http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

Offensive security. 2017. Kali Linux Viitattu 12.11.2017
https://www.kali.org/releases/kali-linux-2017-3-release/

Rapid 7. 2017. Metasploitable 2. Viitattu 12.11.2017
https://metasploit.help.rapid7.com/v1.1/docs/metasploitable-2

PfSense. 2017. Firewall. Viitattu 12.11.2017
https://www.pfsense.org/about-pfsense/features.html

Poliisi. 2017. Kyberrikollisuus. Viitattu 3.1.2017
http://www.poliisi.fi/rikokset/kyberrikollisuus

Signh, A. 2004. An Introduction to Virtualization. Viitattu 4.1.2017
http://www.kernelthread.com/publications/virtualization/

Vahtiohje. 2008. Valtionhallinnon tietoturvasanasto: haavoittuvuus. Viitattu 22.12.2017
https://www.vahtiohje.fi/web/guest/maaritelmat-h

Vahtiohje. 2008. Valtionhallinnon tietoturvasanasto: tietoverkko. Viitattu 4.11.2017
https://www.vahtiohje.fi/web/guest/maaritelmat-t

Valtiovarainministeriö. 2017. VAHTI-toiminta. Viitattu 28.12.2017
http://vm.fi/vahti

Julkaisemattomat

Opiskelijan haastattelu 12.12.2017. Viitattu 13.12.2017

Kuviot

Taulukot