Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Heimo Merilehto

# Kyberturvallisuuden oppimisympäristö ammatilliseen koulutukseen

Metropolia Ammattikorkeakoulu

Insinööri AMK

Tieto- ja viestintätekniikka

Insinöörityö

13.4.2019

| | |
|---|---|
| Tekijä<br>Otsikko<br><br>Sivumäärä<br>Aika | Heimo Merilehto<br>Kyberturvallisuuden oppimisympäristö ammatilliseen koulutukseen<br><br>33 sivua<br>13.4.2019 |
| Tutkinto | Insinööri AMK |
| Tutkinto-ohjelma | Tieto- ja viestintätekniikka |
| Ammatillinen pääaine | Tietoliikennetekniikka |
| Ohjaaja | Lehtori Kimmo Sauren |

Insinöörityössä hahmoteltiin ammattikoulussa opiskeleville ICT-asentajille sopiva oppimisympäristö kyberturvallisuuden opiskeluun. Työssä testattiin VirtuaBox-virtualisointiympäristön sopivuutta harjoitusympäristöksi. Testauksessa selvisi, että VirtualBox-virtualisointijärjestelmä on varsin sopiva ympäristö harjoitusten tekemiseen. VirtualBox-järjestelmän asentaminen on selväpiirteinen ja se on ilmainen ympäristö, ja mahdollistaa sen, että opiskelijat voivat asentaa myös kotikoneeseensa vastaavan ympäristön.

Työssä perehdyttiin myös lainsäädäntöön ja etsittiin esimerkkejä tapahtuneista kyberturvarikoksista ja niistä saaduista rangaistuksista, jotta opiskelijat ymmärtäisivät paremmin esitettyjen ohjelmien ja hyökkäystekniikoiden vaarallisuuden, jos niitä käytetään väärin.

Tiedustelutyökaluista selvitettiin Kali Linuxin ja sen työkalujen, kuten Wiresharkin ja Zenmap-porttiskannerin, käyttö esimerkkien avulla. Hyvien esimerkkiratkaisujen rakentaminen on avainasemassa opetuksessa. Toimivien hyökkäysten dokumentoiminen vie runsaasti aikaa, mutta on tarpeellista opiskelijoiden onnistumiskokemusten aikaansaamiseksi.
Myös puolustusmenetelmiä koottiin työhön esimerkinomaisesti.

Insinöörityön tavoitteena oli selvittää sopiva oppimisympäristö ammattikoulun kyberturvallisuuden opetukseen, ja sellainen ympäristö löydettiin ja testattiin toimivaksi. Virtualbox-ympäristöä ja testattuja harjoituksia voidaan jatkossa käyttää opetusalustana ammattikoulun opetuksessa.

| | |
|---|---|
| Avainsanat | Kyberturva, Wirehark, Virtualbox, Kali Linux, Google-hacking |

| | |
|---|---|
| Author<br>Title<br><br>Number of Pages<br>Date | Heimo Merilehto<br>Cybersecurity learning environment to Vocational school<br><br>33 pages<br>14 Apr. 2019 |
| Degree | Bachelor of Engineering |
| Degree Programme | Information and Communication Technology |
| Professional Major | Telecommunication |
| Instructor | Kimmo Sauren, Senior Lecturer |

The purpose of this study was to find out what kind of learning environment is suitable to study cyber security in vocational school. While doing this report, I found out that the best environment to do cyber security exams is a software called VirtualBox. VirtualBox is a free open source software, so students can install it onto their own computers and practice exams at home.I also examined the Finnish law in this study. Young students might try these operators in business environment too, which is why it is important to teach them what they can or can not do. There are some examples of cyber security crimes that have happened before and what kind of sentences the hackers got from those crimes. With examples, I explained the detailed function of some forensic tools. These tools were Wireshark forensic tool and Zenmap portscanner tool. As a result, I can say that it takes a lot of time to make detailed instructions for the students on how to make a working attack, but it is important for their learning experience. Also some security-defense examples are introduced in this report. The goal of engineering work was to find out a suitable learning environment for cybersecurity. The VirtualBox environment was suitable for that. In the future the tested labs and VirtualBox environment can be used as a platform for teaching cybesecurity at the vocational school.

| | |
|---|---|
| Keywords | cybersecurity |

**Sisällys**

## Tunkeutumismenetelmiä ja sanastoa

Haitallisen liitetiedoston sisältävät sähköpostit: yleisin tapa levittää haittaohjelma [1].

Tietojenkalastelu: valheellisena tahona esiintymällä pyritään saamaan luottamuksellista tietoa [1].

Kohdistettu tietojenkalastelu: vastaa tietojenkalastelua, mutta on suunnattu vain tietyille vastaanottajille [1].

Exploit kit: selaimen tai sen liitännäisten haavoittuvuuksia hyödyntävä verkkosivulla toimiva haitallinen ohjelmisto, joka tartuttaa verkkosivulla vierailevaan tietokoneeseen jonkin haittaohjelman [1].

Lateraalileviäminen: Hyökkääjä levittäytyy sisäverkossa muihin koneisiin ja pyrkii hankkimaan admin-tunnukset. Alkutartunnan jälkeinen vaihe. [1.]

Ohjelmistohaavoittuvuudet: Ohjelmistohaavoittuvuuksien hyödyntäminen on tyypillinen keino tartuttaa haittaohjelma tai esimerkiksi kasvattaa käyttöoikeuksia uhrin tietokoneessa. ”Remote code execution” ja ”priviledge escalation” ovat molemmat pahoja. Myös SQL-injektiot kuuluvat tähän. [1.]

Huijauslaskut: esimerkiksi toimitusjohtajan nimissä lähetettävä valelasku [1].

Watering hole -sivustot: uhri houkutellaan viattomalta näyttävälle verkkosivulle, jossa uhrin tietokoneeseen tartutetaan haittaohjelma selaimen haavoittuvuuden avulla [1].

Water carrier -menetelmä: esimerkiksi laitteen firmware- tai muuta ohjelmistopäivitystä on peukaloitu sisältämään haittaohjelma [1].

Reitittimien haittaohjelmat: yrityksen reunareitittimen haltuunotto ja sen käyttö jalansijana lateraalileviämisessä ja tietoliikenteen salakuuntelussa [1].

Hybridiuhkat: eri menetelmien yhdistely, kuten esimerkiksi sähköverkon sabotaasin yhteydessä tehtävä palvelunestohyökkäys ja tietojen tuhoaminen [1].

Pääsy sisäverkkoon: huomaamaton pääsy yrityksen sisäverkkoon esimerkiksi alihankkijoiden tai työntekijöiden käyttöön tarkoitetun VPN-yhteyden avulla [1].

BGP -hijacking: teleyritysten välisen reitityksen peukaloinnin avulla tehtävä IP-osoitteiden haltuunotto ja väärinkäyttö [1].

USB- ja muiden medioiden käyttö: Siirrettävien medioiden avulla voidaan päästä verkosta eristettyihin järjestelmiin kiinni. Esimerkiksi BadUSB-haavoittuvuus ei edellytä autorun toimintoa. [1.]

Metasploit framework: työkalu tiedustelu- ja hyökkäystoimintaan.

Armitage: graafinen käyttöliittymä Armitage-työkaluun.

0-day exploit: haavoittuvuus, johon ei ole suojausta.

Ransomware: kiristysohjelma.

Eettinen hakkerointi: etsitään laillisesti tietoturva-aukkoja yritysten tietojärjestelmistä.

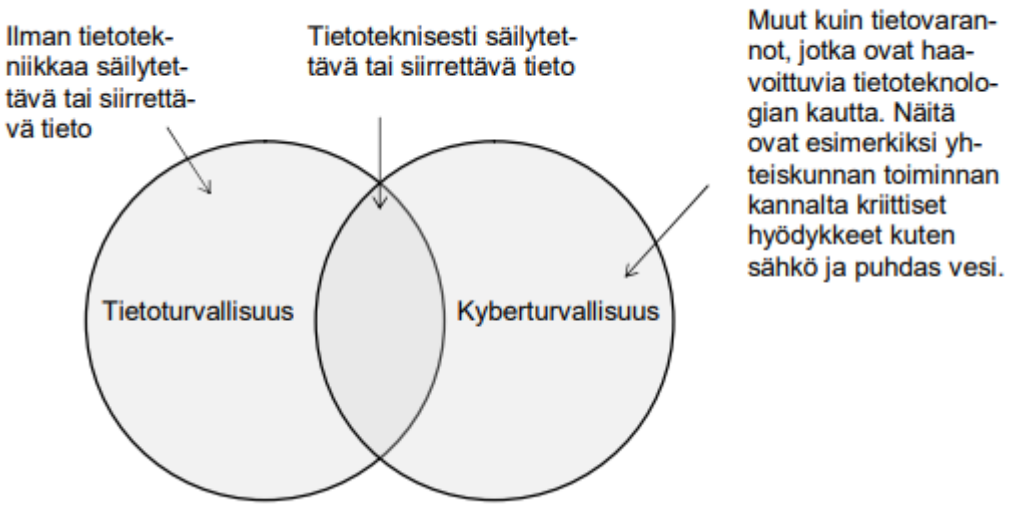
Payload: ohjelma koodi, joka suoritetaan kohdekoneessa onnistuneen hyökkäyksen jälkeen.

Exploit: ohjelmakoodi, joka käyttää hyväkseen tunnettua tai tuntematonta haavoittuvuutta suorittaakseen payload-ohjelman kohdekoneessa.

# 1 Johdanto

Nykyaikainen yhteiskunta perustuu digitaalisiin järjestelmiin. Järjestelmiä ohjataan tietoverkkojen kautta. Tämän vuoksi esimerkiksi tietoverkkojen suojaus on oleellinen osa yhteiskunnan infrastruktuurin suojaamista. Voidaan vain kuvitella, mitä tapahtuu, jos kyberhyökkäys kohdentuu seuraaviin kriittisiin yhteiskunnan toimintoihin: sähkönjakeluun, tietoliikenteeseen, kemianteollisuuteen, vesihuoltoon tai taloussektoriin. [2.] Myös teollisuus on hyvin haavoittuvainen mahdollisille kyberhyökkäyksille. Teollisuuden erilaiset automaatiojärjestelmät ja anturijärjestelmät voivat olla hyökkääjien kohteena ja muodostavat huonolla suojauksella todellisen uhan yrityksen toiminnalle.

Kansallisessa keskustelussa termi ”kyberturvallisuus” on 2010-luvulla tullut aiemmin käytetyn termin ”tietoturvallisuus” rinnalle. Määritelmällisesti nämä kuitenkin ovat hieman eri asioita. Tarkasti ottaen kyberturvallisuus voidaan ajatella pelkkää tietoturvallisuutta laajempana käsitteenä, joka kattaa tietojen ja niitä käsittelevien laitteiden lisäksi myös niitä käsittelevät ja niihin luottavat ihmiset aina yhteiskunnan etuun ja kriittiseen infrastruktuuriin saakka. [3.] Kuvasta 1 ilmenevät tietoturvan ja kyberturvan suhteet.




Kuva 1:Tietoturvallisuuden ja kyberturvallisuuden suhde [4, muokattu].

Tässä Insinöörityössä on tarkoitus selvittää kyberturvallisuuden opettamista ammatillisessa koulutuksessa sekä löytää ja testata sopiva oppimisympäristö kyberturvallisuuden opettamiseen.

## 2 Kyberturvallisuuden huomioiminen ICT-asentajan opetussuunnitelmassa

Ammattikoulusta valmistuvat ICT-asentajat sijoittuvat työelämässä tehtäviin, joissa asennetaan esimerkiksi tietoliikennelaitteita, antureita, ohjausjärjestelmiä ja hälytysjärjestelmiä. On tärkeää, että opiskelijalle muodostuu oikea näkemys tarvittavista suojaustoimista, joilla voidaan minimoida ulkopuolisten tahojen pääsy digitaalisiin järjestelmiin. Opiskelun aikana on hyvä harjoitella suojatussa järjestelmässä tapahtuvaa hyökkäystä ja sen analysointia sekä tietysti puolustautumista niin tietoturva- kuin kyberturvauhkia vastaan. Lisäksi täytyy käydä läpi lainsäädäntöä, jotta opiskelijat ymmärtävät, mitä ei saa tehdä ja millaiset oikeudelliset seuraamukset vääränlaisesta nettikäyttäytymisestä saattaa tulla.

ICT-asentajan opetussuunnitelmassa, joka pohjautuu vuonna 2009 julkaistuun tieto- ja tietoliikenteen opetussuunnitelmaan, ei varsinaisesti käsitellä ollenkaan kyberturvallisuutta. Kahdessa opintokokonaisuudessa kyberturvallisuutta sivutaan osana laitteiden ja palveliminen tietoturvaa.

Tietokone- ja tietoliikenneasennukset –opintokokonaisuudessa, jonka laajuus on 30 osaamispistettä, sitä sivutaan arvioinnin kohdassa ”ohjelmistot ja tietoturva”. Hyvän (H2) ammattitaidon vaatimuksena on, että opiskelija osaa ohjelmien asentamisen ja käyttöönoton sekä yksittäiskoneessa että lähiverkossa ottaen huomioon tietoturvan. Kiitettävän (K3) ammattitaidon vaatimuksena on, että opiskelija osaa asennusten automatisoinnin, tietoturvan sekä yksittäiskoneessa että lähiverkossa. [5.]

Palvelinjärjestelmät ja projektityöskentely nimisessä opintokokonaisuudessa, jonka laajuus on 30 osaamispistettä, sivutaan aihealuetta kohdassa ”Palvelimen tietoturvallisuus”. Tyydyttävän (T1) tason aihealueessa saavuttaa, kun hahmottaa palvelinjärjestelmiin

kohdistuvat tietoturvauhat. Hyvän (H2) tason vaatimuksena on, että osaa asentaa palvelimeen perustietoturvaohjelmistot, ja kiitettävän (K3) vaatimuksena on se, että opiskelija hallitsee tietoturvan kokonaisuutena ja osaa tarvittavien ohjelmistojen asennuksen sekä hallitsee niiden käytön. [5.]

Kuten aikaisemmin todettiin, kyberturvallisuuden kouluttaminen on tärkeää. Uudessa, vuoden 2020 elokuussa käyttöönotettavassa opetussuunnitelmassa kyberturvallisuuden opetukseen on kiinnitetty erityisesti huomiota ja siihen ollaan rakentamassa 30 osaamispisteen laajuista opintokokonaisuutta. Valtioneuvoston Selvitys- ja tutkimustoimikunta esitti vuonna 2016 raportissaan ”Kyberosaaminen Suomessa - Nykytila ja tiekartta tulevaisuuteen” seuraavaa:

> ”Kyberturvallisuuden koulutusta on tarpeen järjestää eri tasoilla ja erilaisilla painotuksilla alkaen tietoturvan kansalaistaidoista aina erikoistuneeseen korkeakoulutukseen asti. Kansalaistaitojen varmistamiseksi voidaan perustaa kyberajokortti, joka tarjoaisi perusymmärryksen henkilökohtaisesta kyberturvallisuudesta. Läpäisevyysperiaatteen mukaisesti kyberturvallisuustietoutta pitäisi integroida myös muiden alojen koulutukseen. Kyberturvallisuusalalla on tärkeää, että on saatavilla myös riittävän operatiivisen osaamisen omaavia ammattilaisia. Siksi esimerkiksi liikkeenjohdon, hallinnon tai IT-alan osaajat tarvitsevat myös kyberturvallisuusosaamista. Samanaikaisesti on tärkeää turvata erikoistumiseen tähtäävä koulutus. Tätä varten tarvitaan uusia toisen ja kolmannen asteen oppimisrakenteita ja koulutussuunnitelmia.” [3.]

Kyberturvallisuuden opettaminen tulisi järjestää niin, että ensin pohdittaisiin kokonaisvaltaisesti käsitettä ”kyberturvallisuus”. Tämän jälkeen kerrattaisiin tietoliikenteestä perusprotokollien toimintaperiaatteet. Seuraavaksi olisi syytä käydä aiheeseen liittyvä lainsäädäntö läpi, jotta opiskelijat ymmärtäisivät, että väärin käyttäytymisestä voi joutua jopa vankeuteen. Tämän jälkeen jokainen opiskelija rakentaisi laboratorioympäristöön oman erillisen virtuaalisoidun harjoitusympäristön, jossa hän pääsisi harjoittelemaan sekä hyökkäystä että tämän jälkeen järjestelmän puolustusta.

# 3 Kyberrikoksia määrittelevä lainsäädäntö

Kyberturvallisuuden testausta ja hyökkäyksiä estetään lainsäädännön avulla. Suomen rikoslain lukujen 34 (Yleisvaaralliset rikokset), 35 (Vahingonteko) ja 38 (Tieto- ja viestintärikokset) lainsäädäntö on tarkoitettu suojelemaan kansalaisia, yhteiskuntaa ja yrityksiä luvattomalta järjestelmiin tunkeutumiselta.

> ”Tietoverkkorikoksista valtaosa tutkitaan paikallispoliisissa. Kaikissa poliisilaitoksissa toimii digitaalisen todistusaineiston käsittelyyn ja analysoimiseen erikoistuneita yksiköitä. Keskusrikospoliisissa toimii maaliskuussa 2015 perustettu tietoverkkorikosten esitutkintaan erikoistunut yksikkö, Kyberrikostorjuntakeskus, jossa tutkitaan pääasiallisesti tietoverkkoympäristössä tehtyjä laajempia kansainvälisiä rikoskokonaisuuksia.” [6.]

Rikoslain luvut käydään tarkasti opiskelijoiden kanssa lävitse, ennen kuin varsinaisesti aloitetaan ensimmäistäkään harjoitusta. Lain ja rangaistusten tunteminen auttaa opiskelijoita pysymään lain oikealla puolella, ja samalla paneudutaan niin sanottujen valkohattuhakkereiden eettisiin sääntöihin, joissa noudatetaan lakia.

## 3.1 Laittomat koodinpurkuohjelmistot ja -laitteet

Rikoslain yleisvaaralliset rikokset -luvun 34, pykälät 9a ja 9b käsitelevät vaaran aiheuttamista tietojenkäsittelylle sekä tietoverkkorikosvälineen hallussapitoa. Nämä käsittävät sellaisia asioita kuin laitteet, ohjelmat tai ohjeet, joilla voidaan vahingoittaa tietojärjestelmiä, murtaa tai purkaa salasanoja, suojauksia ja pääsykoodeja. Näiden tuotteiden valmistaminen, maahantuonti ja levittäminen on tuomittavaa ja saattaa johtaa enimmillään kahteen vuoteen vankeutta. Hallussapidosta voidaan tuomita vankeuteen enintään kuudeksi kuukaudeksi. [7.]

## 3.2 Datavahingonteko

Rikoslain Vahingonteot-luvun (luku 35) pykälät 3a, 3b ja 3c käsittelevät datavahingontekoa. Asiasisältönä tässä luvussa on datan hävittäminen, turmeleminen, kätkeminen, va-

hingoittaminen, muuttaminen tai saattaminen käyttökelvottomaksi sekä salaa tietovälineelle tallennettu tieto. Tuomiot vaihtelevat sakosta aina kahden vuoden vankeustuomioon saakka. Erityisen törkeästä teosta, jolloin toiminta on osana rikollisjärjestön toimintaa tai se kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaa energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon tai muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon, tuomio on vähintään neljä kuukautta ja enintään viisi vuotta vankeutta. [7.]

### 3.3 Tiedon salassapito

Rikoslain luvussa 38 pykälät 1−2 käsittelevät tiedon salassapitoa. Tietoa tai seikkaa, joka lain tai asetuksen mukaan on määritelty salassa pidettäväksi ja jonka henkilö on saanut tietoonsa asemansa tai tehtävää suorittaessaan, ei saa paljastaa tai käyttää omaksi tai toisen hyödyksi. Tuomio voi vaihdella sakosta enintään yhden vuoden vankeuteen. [7.]

Pykälät 3−4 käsittelevät viestintäsalaisuuden loukkaamista. Tämä käsittää niin kirjesalaisuuden kuin sähköisen viestin eri keinoin avaamista tai suojauksen murtamista. Tuomio voi vaihdella sakosta aina kahden vuoden vankeusrangaistukseen saakka. Erityisen törkeissä tapauksissa, esimerkiksi jos rikoksentekijä toimii teleyrityksen palveluksessa ja tekee törkeän viestintäsalaisuuden loukkauksen, voi tuomio olla kolme vuotta vankeutta. [7.]

Pykälät 5, 6 ja 7a käsittelevät tietoliikenteen häirintää. Häirinnällä tarkoitetaan posti-, tele- ja radioliikenteen häirintää ilkivaltaisessa tarkoituksessa joko lähettämällä häiritseviä viestejä tai muuten estämällä posti-, tele- tai radioliikennettä. Tuomio häirinnästä voi olla sakkotuomio tai kahden vuoden vankeustuomio. Mikäli häirintä on ollut erityisen törkeää tai se on kohdistunut julkispalveluihin, joilla turvataan ihmishenkiä tai henkilö on ollut teletoimintaa, kaapelilähetystoimintaa tai yleisradiotoimintaa harjoittavan yrityksen palveluksessa tai häirintä on ollut osana rikollisjärjestötoimintaa, enimmäisrangaistus voi olla viisi vuotta vankeutta. [7.]

Pykälä 7c käsittelee törkeää tietojärjestelmän häirintää, jossa aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa tietojärjestelmille. Rangaistus vaihtelee neljästä kuukaudesta aina viiteen vuoteen vankeutta. [7.]

Pykälät 8 ja 8a käsittelevät tietomurtoa. Murtautuja käyttää hänelle kuulumatonta käyttäjätunnusta tai turvajärjestelyn muuten murtaen tunkeutuu tietojärjestelmään. Rangaistus on sakko tai enimmillään kahden vuoden vankeus. Mikäli tietomurto tehdään osana järjestäytynyttä rikollisuutta, voi rangaistus olla enimmillään kolme vuotta vankeutta. Myös datan katselu teknisen erikoislaitteen tai turvajärjestelyt ohittaen vilpillisessä mielessä on rangaistavaa. [7.]

Pykälä 8b käsittelee purkujärjestelmärikosta. Siinä käsitellään suojatun palvelun tarjoajan oikeuksia vahingontekijöitä vastaan. Purkamiseen tarkoitettuja laitteita ei saa tuoda maahan, myydä, vuokrata tai valmistaa eikä asentaa tai huoltaa. Rangaistus on enintään yksi vuosi vankeutta. [7.]

Pykälä 9 käsittelee henkilörekisteririkosta. Rikokseen voi syyllistyä joko tahallaan tai käsittelemällä törkeän huolimattomasti henkilötietoja vastoin henkilötietolain käyttötarkoitussidonnaisuutta, estämällä rekisteröityä henkilöä käyttämästä hänelle kuuluvaa tarkastusoikeutta tai siirtämällä tietoja Euroopan unionin ulkopuolelle. Rangaistus on sakko tai vankeutta enintään yksi vuosi. [7.]

Pykälä 9a käsittelee identiteettivarkautta, jossa käytetään oikeudettomasti toisen henkilötietoja tai tunnistetietoja erehdyttämään kolmatta osapuolta ja siten aiheutetaan taloudellista vahinkoa tai haittaa sille, jota tieto koskee. Rangaistus on sakko. [7.]

### 3.4 Esimerkkejä tietomurtorangaistuksista

Tärkeää on lainsäädännön läpikäymisen jälkeen konkreettisin rikostuomioesimerkein tuoda eläväsi opiskelijoille selväksi, että rikos ei kannata. Seuraavaan on poimittu muutamia aiheeseen liittyviä artikkeleita sanomalehdistä.

> ”17-vuotias suomalaispoika tuomittiin Espoossa yli 50 000 palvelimen murtamisesta. Espoon käräjäoikeus tuomitsi nimimerkkiä Ryan käyttäneen teinipojan kahden vuoden ehdolliseen vankeuteen 50 700 palvelimen murtamisesta. Oikeuden asiakirjojen mukaan hänen uhreihinsa lukeutui esimerkiksi Harvardin yliopisto sekä teknologiayliopisto MIT. Tietomurroissa muun muassa kaapattiin sähköposteja, estettiin liikennettä verkkosivustoille ja varastettiin luottokorttitietoja. Ehdollisen vankeuden lisäksi "Ryanin" tietokone takavarikoitiin ja hänet määrättiin palauttamaan noin 6 600 euron edestä omaisuutta, jonka hän oli rikoksillaan hankkinut”. [8.]

”Naisen Facebook-profiilia muuttanut mies on tuomittu hovioikeudessa tietomurrosta ja kunnianloukkauksesta 20 päiväsakon rangaistukseen sekä korvaamaan naiselle kärsimyksestä 300 euroa, kertoo uutispalvelu Edilex. Oikeus totesi, että mies oli oikeudettomasti ja hänelle kuulumatonta käyttäjätunnusta käyttäen tunkeutunut naisen Facebook-tilille. Oikeus tulkitsi Facebook-tilin tietojärjestelmäksi, jossa sähköisesti käsitellään, varastoidaan ja siirretään tietoja”. [9.]

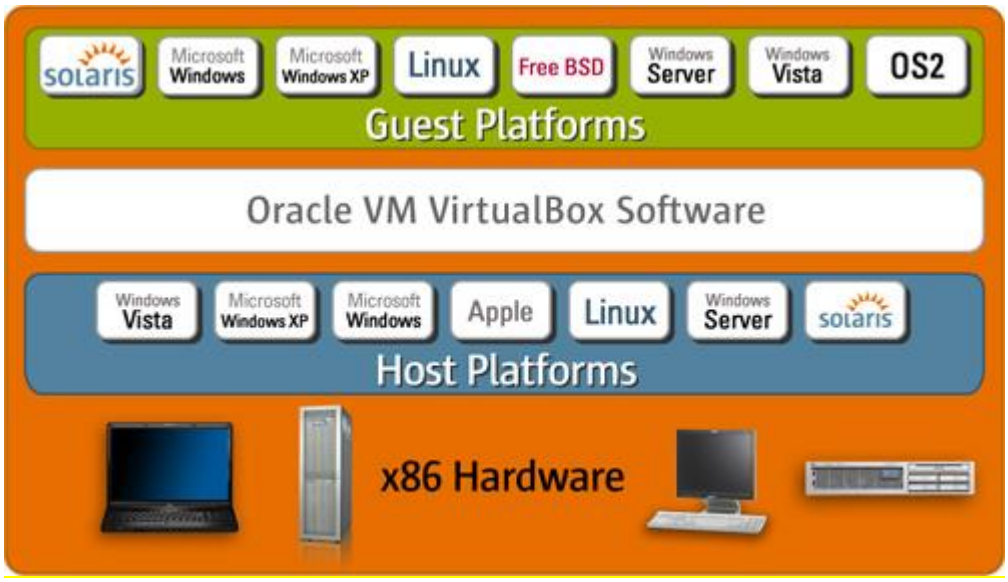
”OP:n rahaliikenteen katkaisusta nettislangilla kirjoitetun viestin lähettäjäksi epäillään tekoaikaan 17-vuotiasta miestä. Nykyisin 20-vuotiasta miestä pidetään päätekijänä laajassa pankkeihin ja mediaan kohdistuneessa hyökkäyssarjassa. Hänen epäillään tehneen hyökkäyksiä myös Nordeaa, Danske Bankia, Aktiaa ja mediayhtiöitä vastaan. Mies on myöntänyt ison osan palvelunestohyökkäyksistä, mutta kiistää syyllistyneensä kiristykseen. Myös hänen ystävänsä on osasyytettynä useissa teoissa. Syyttäjä vaatii pääepäillylle enimmillään kolmen vuoden ehdotonta vankeusrangaistusta. Pankki vaatii häneltä yli 450 000 euron korvauksia”. [10.]

# 4 Oppimisympäristön valinta

Oppimisympäristön valintaan vaikuttaa monta asiaa. Tärkein asia mielestäni on se, että opiskelijat voivat turvallisesti harjoitella esimerkiksi hyökkäysprosesseja. Tällainen ympäristö saadaan luomalla muista käyttäjistä riippumaton virtuaaliympäristö, josta hyökkäykset eivät karkaa reaaliympäristöön ja aiheuta haittaa muille verkon käyttäjille.

## 4.1 Oppimisympäristönä VirtualBox

VirtualBox virtualisointijärjestelmä on Oraclen kehittämä Type 2 -luokan virtualisointiympäristö, joka vaatii toimiakseen isäntäkäyttöjärjestelmän. Isäntäkäyttöjärjestelmäksi sopii laaja valikoima käyttöjärjestelmiä: Windows-työaseman käyttöjärjestelmät, Windows server -käyttöjärjestelmät, Linuxin eri jakeluversiot, Applen OS-käyttöjärjestelmät ja Solaris-käyttöjärjestelmä. Virtuaalikoneiksi voidaan myös asentaa laaja valikoima erilaisia käyttöjärjestelmiä, kuten esimerkiksi MS-DOS käyttöjärjestelmä. Kuvasta 2 ilmenevät VirtualBox-ympäristössä toimivat käyttöjärjestelmät.




Kuva 2: VirtualBOX -ympäristö [11].

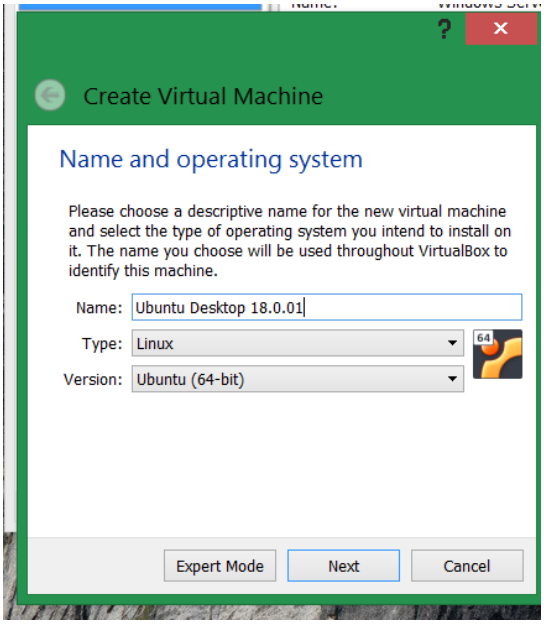
VirtualBox järjestelmän valintaa kouluympäristöön puoltaa myös se, että Virtuabox ei vaadi ns ” laitteistotason” virtualisointia. Suorittimen ei tarvitse tukea Intel VTx- tai AMD-V-virtualisointiominaisuutta. Tämä mahdollistaa vanhemmankin konekannan käytön harjoituksissa.

Virtualisoinnin hyötyjä ovat muun muassa seuraavat asiat: Voidaan ajaa useita käyttöjärjestelmiä samanaikaisesti yhden tietokonelaitteiston sisällä ja suorittaa eri käyttöjärjestelmille kirjoitettuja sovelluksia. Voidaan asentaa valmiiksi esiasennettuja sovelluspaketteja virtuaalikoneisiin (esimerkiksi sähköpostipalvelin), voidaan testimielessä konfiguroida asennuksia ja niin sanotun ”snapshots”-toiminnon avulla palauttaa järjestelmä alkutilaan.

## 4.2 VirtualBox-ympäristön asentaminen

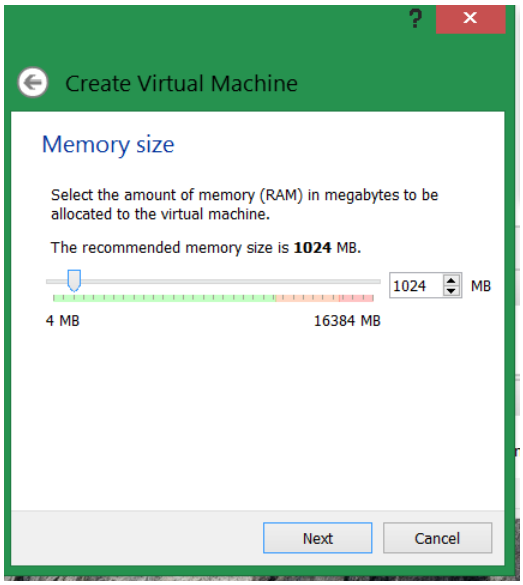
VirtualBox-järjestelmä asennetaan seuraavasti: Ladataan ensin VirtualBox.org-sivustolta omalle käyttöjärjestelmälle sopiva versio. Lataamisen jälkeen asennus käynnistetään kuten muukin, esimerkiksi Windowsin päälle asennettavien ohjelmien asennus. Asennuksen lopuksi voidaan valita, että asennus luo pikakuvakkeen työpöydälle.

Uusi virtuaalikone lisätään VirtualBox-ympäristöön seuraavasti: Valitaan ”NEW” VirtualBoxin hallintaikkunasta. Kohtaan ”type” valitaan käyttöjärjestelmän tyyppi, joka on tässä tapauksessa Linux. VirtualBox-järjestelmään on ohjelmoitu kuhunkin käyttöjärjestelmätyyppiin soveltuvia virtuaalikoneasetuksia. Lisäksi tulee valita, onko asennettava järjestelmä 32-bittinen vai 64-bittinen. ”Name” -kenttään kannattaa kirjoittaa käyttöjärjestelmän jakeluversio sekä sen version numero, joka asennaa. Tämä helpottaa oikean virtuaalikoneen käynnistystä harjoitusympäristössä. Kuvassa 3 on esitetty hyvä nimeämisjärjestelmä.



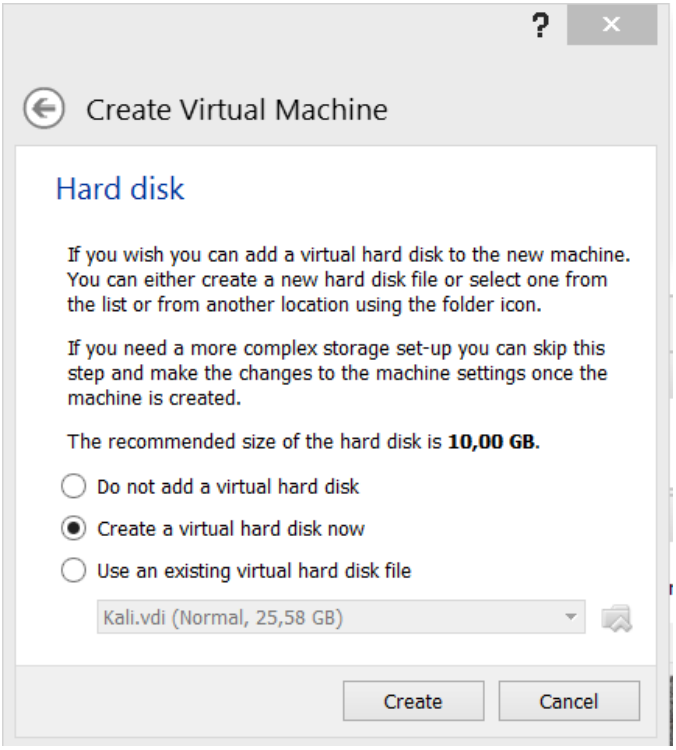

Kuva 3: 64-bittisen Ubuntu -käyttöjärjestelmän asennus.

Asennuksen seuraavassa vaiheessa varataan virtualisoidulle käyttöjärjestelmälle sopiva määrä keskusmuistia. Mitä enemmän virtuaalikoneille voidaan määritellä keskusmuistia, sitä paremmin ne toimivat. Tulee kuitenkin huomioida koneen muistirajoitukset, sillä silloin kun virtuaalikone on käynnistetty, se varaa käyttöönsä tässä kohdassa määritellyn muistikapasiteetin. Kuvassa 4 ilmenevät virtuaalikoneen muistinsäätömahdollisuudet.



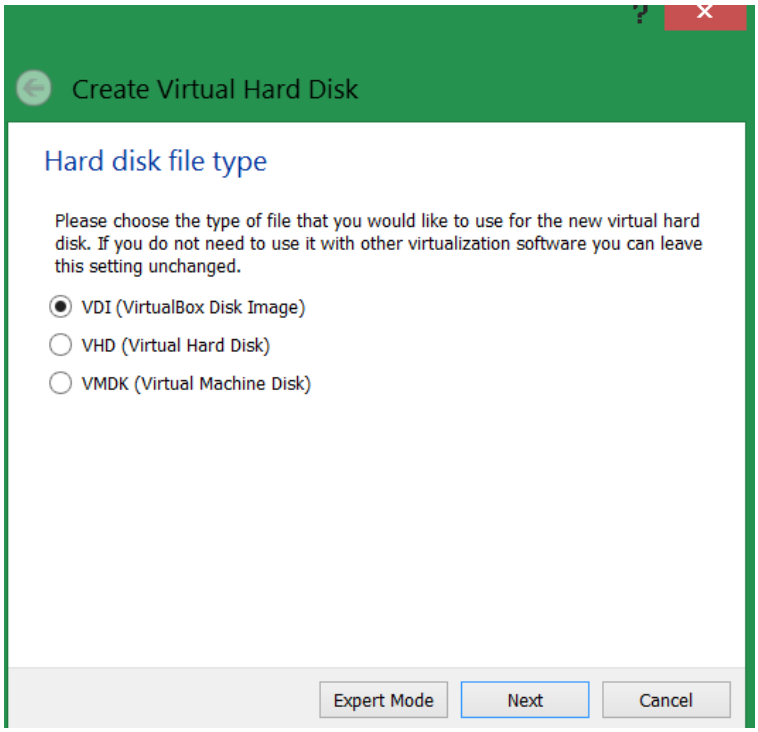

Kuva 4:Virtuaalikoneen muistinmääritys.

Tämän jälkeen luodaan virtuaalikonetta varten kiintolevy, jonka oletuskoko 10 GB on sopiva asenettavalle LINUX-käyttöjärjestelmälle. Kuvassa 5 esitetään virtuaalikoneen kiintolevyn määrittelyvaihtoehto.



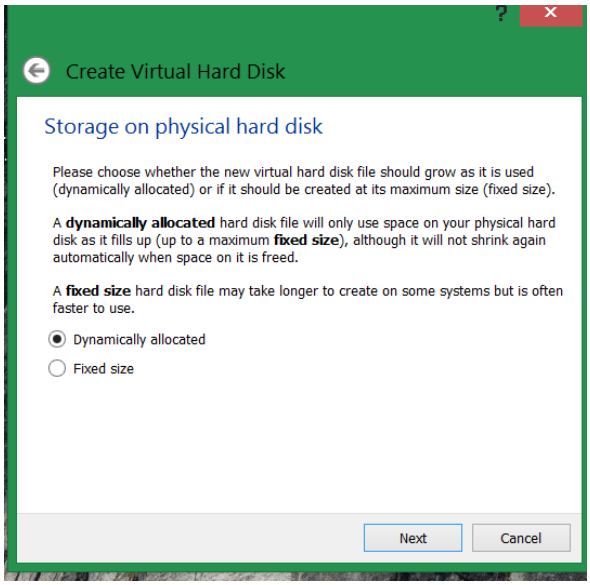

Kuva 5: Virtuaalikoneen virtuaalikiintolevyn tyypin määrittely.

Virtuaalikiintolevyn tyypiksi valitaan VDI (Virtual Disk Image), joka on VirtualBox -järjestelmän täysin tukema levyjärjestelmä. VirtualBox tukee myös VMDK-formaattia, jota käyttää esimerkiksi VMware, sekä Micrsosoftin käyttämää VHD-formaattia. Paras valinta virtuaalikoneen kiintolevyn valinnaksi esitetään kuvassa 6.



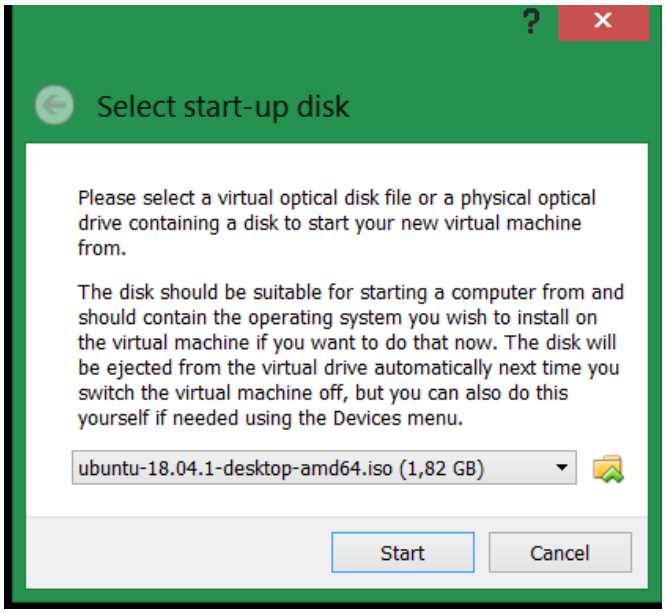

Kuva 6: Asennuksessa valitaan virtuaalikiintolevyn asennustyypiksi VDI.

Asennuksen seuraavassa vaiheessa valitaan kiintolevyn tyyppi, jota asennuksessa käytetään. Käytännöllisin valinta on ottaa dynaamisesti laajeneva kiintolevytyyppi. Tällöin kiintolevytilaa kasvatetaan sitä mukaa, kuin tarvetta ilmenee. Kuvassa 7 asennusta varten valitaan Dynamically allocated -valinta.



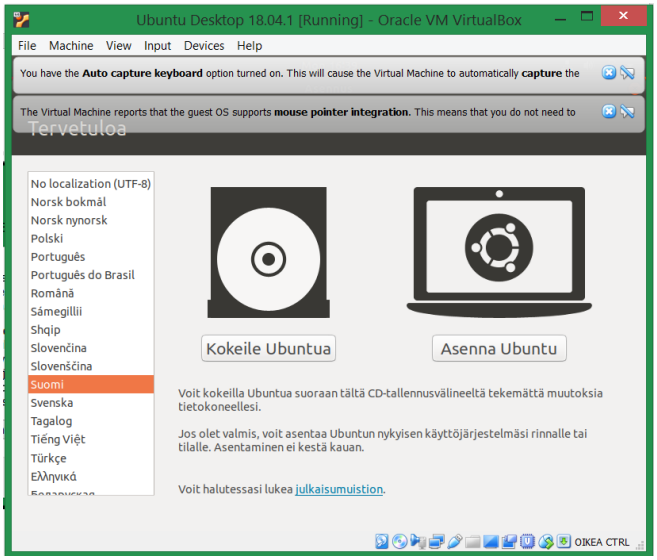

Kuva 7: Asennuksessa valitaan dynaamisesti laajeneva kiintolevy.

Seuraavaksi valitaan paikka, josta Ubuntu Desktop -järjestelmä asennetaan ja aloitetaan Ubuntun asennus. Kuvassa 8 selataan asennusta varten oikea .iso-tiedosto ja valitaan se asennusta varten.




Kuva 8: Etsitään Selaa -toiminnolla oikea .iso-asennustiedosto.

Kuvassa 9 aloitetaan suomenkielisen Ubuntun asennus.




Kuva 9: Aloitetaan Ubuntu-käyttöjärjestelmän asennus.

## 5 Penetraatiotestaus

Termi ”penetraatio” tarkoittaa läpäisyä tai tunkeutumista. Tietojärjestelmistä puhuttaessa termi tarkoittaa tietomurtoa suojattuun tietojärjestelmään. Testauksen tarkoituksena on löytää haavoittuvuuksia eikä niinkään testata, voidaanko niitä käyttää hyväksi.

Penetraatiotestaukseen liittyvät yleensä keskustelut kohdeyrityksen asiantuntijoiden kanssa. Haastattelujen tarkoituksena on saada kokonaiskuva yrityksen verkosta, ja kokonaiskuvan synnyttyä voidaan suunnitella verkkoskannaus. Verkon skannauksella tutkitaan potentiaaliset hyökkäyskohteet, porttiskannauksella tutkitaan ja etsitään järjestelmän avoimet portit ja haavoittuvuusskannauksella etsitään kohdejärjestelmästä tunnettuja haavoittuvuuksia. [12; 13.]

Penetraatiotestaukseen ja tutkimukseen käytetään Kali Linux -ohjelmistoa. Sen valinta oppilaitosympäristöön on perusteltua ohjelman ilmaisuuden ja monipuolisuuden vuoksi. Siitä löytyvät niin eettiseen hakkerointiin käytettävät työkalut kuin asioiden tutkimiseen liittyvät työkalut. Lisäksi siinä on valmiiksi konfiguroitu virtuaalikone oppilaitokseen valitulle VirtuaBox-ympäristölle. [14.]

Kali Linux asennetaan lataamalla VirtualBox-ympäristöön tarkoitettu Image OFFENSSIVE Security yrityksen verkkosivuilta ja tuomalla se sen jälkeen VirtualBox-ympäristöön. Samasta paikasta löytyvät valmiit kuvat myös VM-Warelle tarkoitettuun ympäristöön.

Kali Linuxissa on noin 600 erilaista työkalua, joilla voidaan monella eri tavavalla testata järjestelmiä. Työkalut on ryhmitelty seuraaviin aihekokonaisuuksiin: informaation kerääminen (Information Gathering), haavoittumisen analysointi (Vulnerability Analysis), langattoman verkon kautta tapahtuvat hyökkäykset (Wireless Attacks), web-sovellukset (Web Applications), haittaohjelmatyökalut (Exploitation Tools), tutkintatyökalut (Forensics Tools), käytettävyystestit ( Stress testing), nuuskinta- ja huijaustyökalut (Sniffing and Spoofing), salasanahyökkäykset (Password Attacks), takaisinmallintaminen (Reverse Engineering), yhteyden ylläpitotyökalut (Maintaining Access), kovohakkerointi (Hardware Hacking) ja raportointityökalut ( Reporting Tools). [15.] Luvussa 6 tutustutaan muutamaan työkaluun syvemmin.

# 6 Tiedustelu

Tiedustelulla pyritään selvittämään yrityksestä tai yksilöstä tietoja yleisten tietolähteiden kautta niin, että kohde ei välttämättä edes tiedä olevansa informaatiovaikuttamisen kohteena. Tähän kategoriaan voidaan luokitella esim. ”pishing”, jolla kalastellaan salasanoja, sosiaalinen vaikuttaminen, jossa lyöttäydytään seuraan ja kysellään esimerkiksi yritykseen liittyviä asioita tai työpaikan ulkopuolella olevassa ravintolassa kuunnellaan salaa ihmisten keskusteluja. Yrityksen tietojärjestelmistä voidaan ottaa selvää esimerkiksi porttiskannereiden avulla tai sitten ”Google Hacking” -menetelmällä. Lisäksi on muitakin menetelmiä.

## 6.1 Google Hacking

”Google hacking” -menetelmä perustuu Google-hakukoneen ominaisuuksiin löytää haavoittuvuuksia Internetistä. Haavoittuvuuksia on kahdentyyppisiä: ohjelmistohaavoittu-

vuuksia ja väärin konfiguroituja sovelluksia ja järjestelmiä. ”Google Hacking” -menetelmän etuna on se, että hakukoneet keräävät tietoa järjestelmistä koko ajan eikä niitä pidetä vaarallisina eli ne eivät hälytä järjestelmän ylläpitäjää. Esimerkiksi ”Google cache” -toiminnon avulla voi saada kohteista vanhempaa tietoa. Google tallentaa aina koko tiedoston omalle palvelimelleen. Hyökkääjä voi käyttää hakukonetta hyväkseen tutkiakseen kohteen arkaluontoisia tietoja ottamatta edes yhteyttä kohteen palvelimeen. [16.] ”Google Hacking” -tietokannassa on taulukossa 1 näkyvien aihealueiden valmiita kyselyjä.

Taulukko 1. Googlen hakkerointikyselyt [17].

| | |
|---|---|
| **Footholds** (79)Examples of queries that can help an attacker gain a foothold into a web server | **Web Server Detection** (113)<br>These links demonstrate Googles awesome ability to profile web servers. |
| **Sensitive Directories** (180)<br>Googles collection of web sites sharing sensitive directories. The files contained in here will vary from sensitive to über-secret! | **Files Containing Usernames** (21)<br>These files contain usernames, but no passwords... Still, Google finding usernames on a web site. |
| **Vulnerable Files** (62)<br>HUNDREDS of vulnerable files that Google can find on websites. | **Files Containing Passwords** (279)<br>PASSWORDS!!! Google found PASSWORDS! |
| **Vulnerable Servers** (94)<br>These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section. | **Sensitive Online Shopping Info** (11)<br>Examples of queries that can reveal online shopping infomation like customer data, suppliers, orders, credit card numbers, credit card info, etc |

| | |
|---|---|
| **Error Messages** (100)<br><br>Really verbose error messages that say WAY too much! | **Files Containing Juicy Info** (565)<br><br>No usernames or passwords, but interesting stuff none the less. |
| **Network or Vulnerability Data** (87)<br><br>These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... All sorts of fun stuff! | **Pages Containing Login Portals** (510)<br><br>These are login pages for various services. Consider them the front door of a websites more sensitive functions |
| **Various Online Devices** (393)<br><br>This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google. | **Advisories and Vulnerabilities** (2019)<br><br>These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific. |

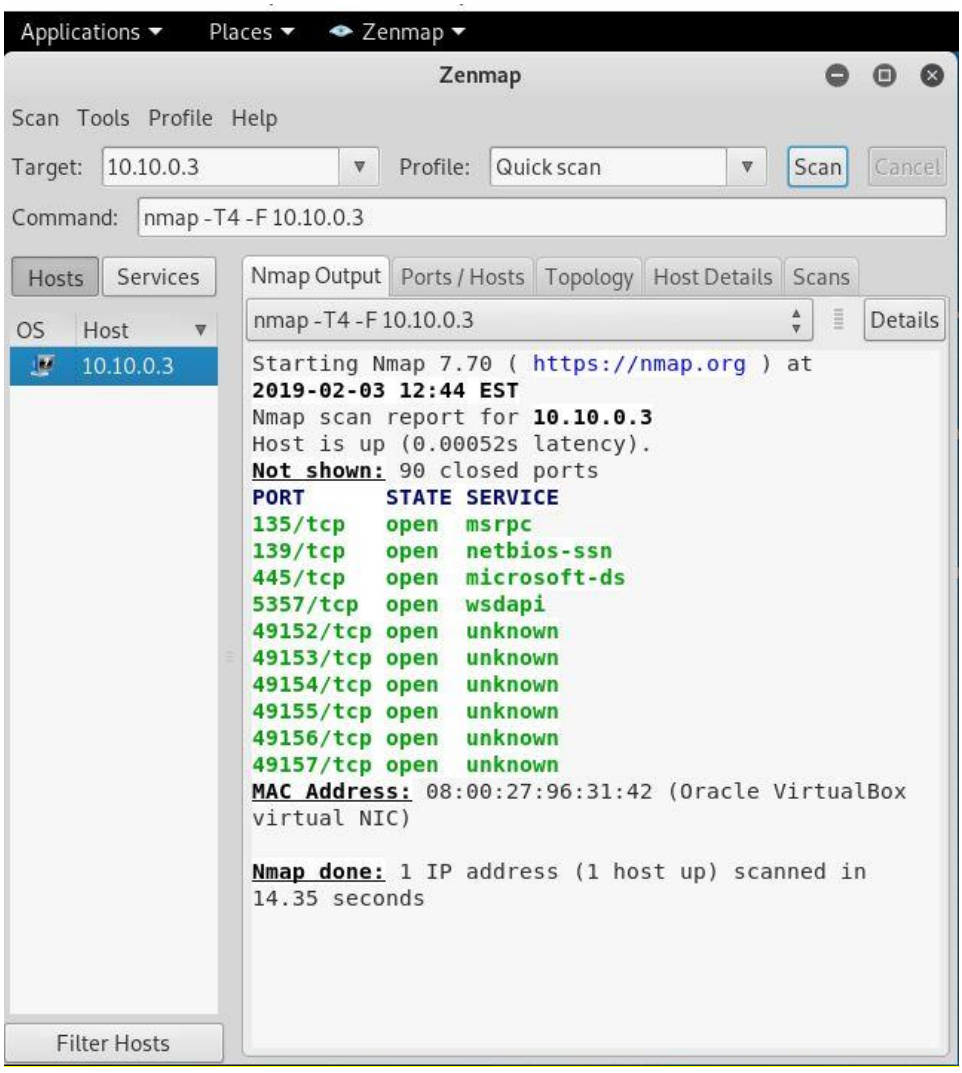
## 6.2 Porttiskannaus

Erityisiasiantuntija Antti Kurittu kirjoittaa Tietomurtojen ennaltaehkäisy, havaitseminen ja tutkinta -artikkelissaan seuraavasti:

> ”Porttiskannaus on toimenpide, jonka avulla pyritään selvittämään tietojärjestelmän eri tietoliikenneporteissa toimivia ohjelmia ja käyttöjärjestelmiä sekä niiden haavoittuvuutta. Tavanomaisesti porttiskannaus suoritetaan käyttäen hyväksi tätä varten laadittua ohjelmaa, joka voi - käytetystä ohjelmasta riippuen - esimerkiksi palauttaa raportin skannauksen kohteena olevasta koneesta, sen tietoliikenneporteista, ohjelmistoista ja niiden tiedetyistä tietoturva-aukoista. Porttiskannausohjelmaa voidaan käyttää luvallisessa tarkoituksessa esimerkiksi tietojärjestelmän turvallisuusjärjestelyjen selvittämiseen. Porttiskannausohjelmalla on näin ollen mahdollista järjestelmällisesti selvittää tietojärjestelmän mahdollisia aukkoja ja sen heikkoja kohtia. Toimenpiteen avulla kyetään saamaan tietoja, jotka mahdollista-

vat myös luvattoman pääsyn kohteena olevaan järjestelmään. Ohjelmaa käyttämällä hankitun tiedon avulla voidaan siten laissa tarkoitetuin tavoin murtaa tietojärjestelmän turvajärjestely. Kuten lain esitöissä todetaan jo se, että yrittää hankkia tällaisen luvattoman pääsyn järjestelmään mahdollistavan tiedon, on rangaistavaa, jos se tehdään tarkoituksella oikeudettomasti tunkeutua tietojärjestelmään". [18.]

Porttiskannaus tehdään Kali Linuxin mukana tulevalla Zenmap-ohjelmalla seuraavasti: kytketään W7-koneelta Firewall-toiminto pois päältä. Tämän jälkeen asetetaan kohdekoneen IP-osoite ja saadaan kuvan 10 mukaisesti näkymään avoimet portit.




Kuva 10: Onnistunut porttiskannaus Zemap-ohjelmistolla.

### 6.3 Wireshark

Wireshark-ohjelma on oiva työkalu tutkia verkossa liikkuvaa dataa. Se mahdollistaa datapakettien analysoinnin Wireshak-ohjelman sisällä. Datapakettien liikenne kaapataan Wireshark-ohjelman muistiin, minkä jälkeen se voidaan ryhmitellä protokollatasolla erilaisiin lohkoihin.Wiresharkin toimintaperiaate on seuraava: Se kaappaa datan verkkoliitännästä, ja sen jälkeen kaapattu data pilkotaan ymmärrettäviksi kehyksiksi tai paketeiksi, joilla on alku ja loppu. Tämän jälkeen Wireshark-ohjelma tulkitsee datan ja tuo esille niin, että siitä ilmenevät osoitteet, protokollat ja tietosisältö. Data voidaan tulkita heti tai tallentaa myöhempää tulkintaa varten tai sitä voidaan jakaa muille. Lisäksi Wiresharkissa on ”promiscuous mode” -asetus, jolla ohjelma saadaan jäljittämään myös langattoman verkon liikennettä. [19.]

Wireshark on parhaimmillaan silloin, kun etsitään jonkin ongelman syytä bittitasolla tai selvitetään laitteiden välistä protokollaa tai tietovirtaa [19].

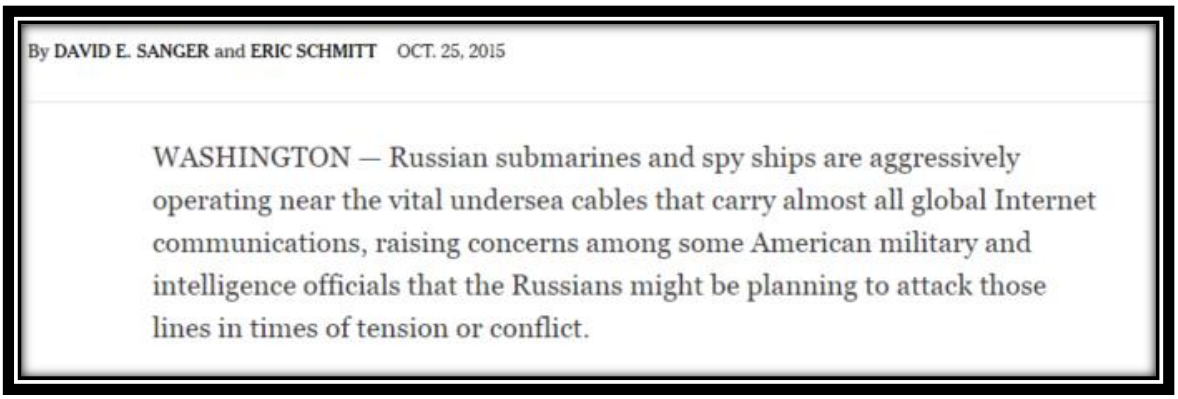
## 7 Hyökkäykset tietoverkon kautta

Tietoverkon kautta tehdään hyökkäyksiä eri tavoilla, ja niissä hyödynnetään tietoliikenteen OSI-mallin eli Open Systems Interconnectionin eri kerrosten tiedonsiirtoprotokollia ja niiden ominaisuuksia. Tällöin puhutaan Ethernet-kehyksistä, ARP-protokollasta, IP-protokollasta, TCP-protokolasta ja UDP-protokollasta. Kuvassa 11 on esitelty OSI-mallin 7 kerrosta ja kerroksilla vaikuttavat protokollat. ARP-protokolla on siirtokerroksen protokolla.


Kuva 11: OSI-mallin 7 kerrosta [20].

## 7.1 Fyysisen kerroksen hyökkäys

Fyysisen kerroksen hyökkäyksiin kuuluvat esimerkiksi kaapelit ja valokuidut sekä radioaallot. Fyysisen kerroksen hyökkäyksissä voidaan kaapeli irrottaa tai haaroittaa ja välistä voidaan siepata dataa. Valokuiduista voidaan esimerkiksi kuunnella merikaapeleissa kulkevaa dataa, jos kalusto on riittävän järeää. Kuvassa 12 kerrotaan sukellusveneillä tapahtuvasta hakkeroinnista.



By DAVID E. SANGER and ERIC SCHMITT OCT. 25, 2015

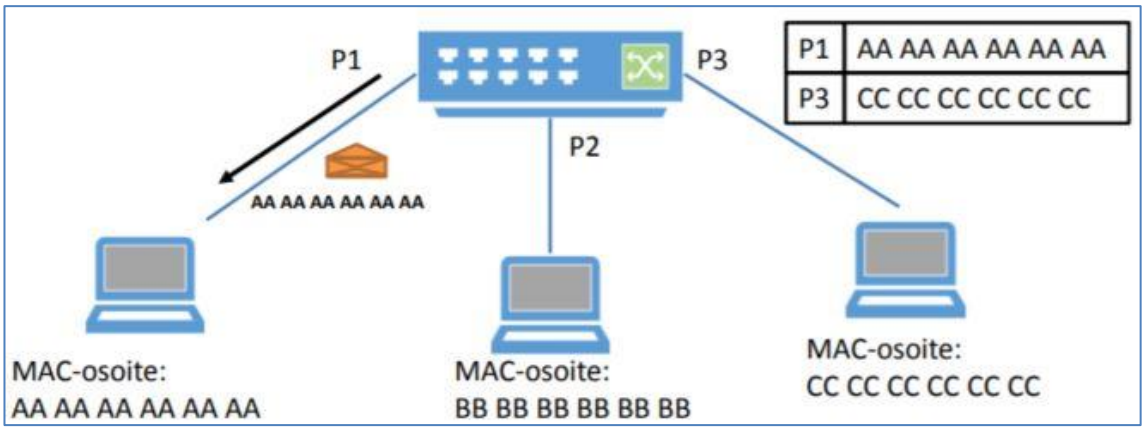
WASHINGTON — Russian submarines and spy ships are aggressively operating near the vital undersea cables that carry almost all global Internet communications, raising concerns among some American military and intelligence officials that the Russians might be planning to attack those lines in times of tension or conflict.

Kuva 12: New York Times -sanomalehden artikkeli sukellusveneellä tapahtuvasta salakuuntelusta [21].

Langattomassa verkossa tiedot siirtyvät radioaaltojen välityksellä tietyn kantavuusalueen sisällä. Adapteri muuntaa sähköiset signaalit radioaalloiksi, joita käyttäjät lähettävät tai vastaanottavat. Tämän uuden tekniikan heikkous ovat juuri radioaallot, jotka leviävät kaikkialle kantavuusalueella. Usein ne ulottuvat yrityksen toimitilojen ulkopuolelle. Kuka tahansa yrityksen läheisyydessä väijyvä hakkeri voi siepata radioaallot. Hakkeri tarvitsee vain tavallisen kannettavan tietokoneen, jossa on langattoman verkon kortti sekä vapaita verkkoja hakeva ohjelmisto. [22.]

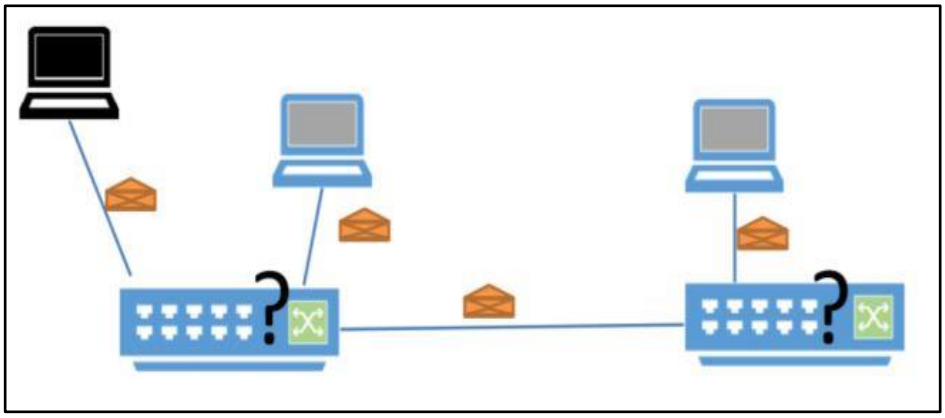
## 7.2 Siirtoyhteyskerroksen hyökkäys

Siirtoyhteyskerroksen hyökkäyksessä päätelaite selvittää ARP-protokollan avulla tarvitsemansa kohdelaitteen MAC-osoitteen. Tieto tallennetaan kytkimen osoitetauluun, jonka periaatekaavio on esitetty kuvassa 13.




Kuva 13: Kytkimen osoitetaulu [23].

Hyökkääjä lähettää verkkoon sekunnissa tuhansia kehyksiä, joissa on satunainen lähde -osoite. Tällöin kytkinten MAC -taulut täyttyvät ja lähettävät kaikesta liikenteestä kopion kaikkialle. Tästä seuraa se, että hyökkääjälle päätyy kopio kaikesta kahden tietokoneen välisestä liikenteestä, kuten kuvassa 15 on esitetty. Käyttämällä sopivaa paketinpurkuohjelmistoa, esimerkiksi Wireshark-ohjelmistoa, pystyy hyökkääjä saamaan selville arkaluontoista tietoa. Tällaisesta hyökkäysmenetelmästä käytetään nimitystä Tulvitus (MAC Flooding). [23; 24.]



Kuva 14: Tulvitus -hyökkäys.[24.]

## 7.3 Verkkokerroksen hyökkäysmenetelmät

Verkkokerroksen hyökkäysmenetelmänä voidaan käyttää esimerkiksi ICMP-tulvaa. Tällöin liikenne muodostuu ICMP-paketeista, kuten ping-komennon ”echo request” tai ”echo reply”-viesteistä. Esimerkiksi Smurf-hyökkäys toteutetaan lähettämällä väärennetyllä lähdeosoitteella varustettuja ICMP-paketteja verkon broadcast-osoitteeseen, jolloin kaikki kyseisen verkon laitteet saavat kyselyn ja mahdolliset vastaukset menevät väärennettyyn hyökkäyksen kohteena olevaan osoitteeseen. Kohteen kannalta paketit näyttävät tulevan eri osoitteista, jolloin hyökkäyksen torjuminen IP-osoitteen perusteella ei onnistu. Hyökkääjän osoitetta paketeissa ei näy. [25.]

## 7.4 Kuljetuskerroksen hyökkäykset

> ”Kuljetuskerroksen hyökkäykset pyrkivät kuluttumaan kaiken palvelimen saatavissa olevan kaistan tai käyttämään hyväksi heikkouksia kuljetuskerroksen protokollissa. Nämä vaativat paljon resursseja hyökkääjältä, joten näitä kutsutaan myös volyymipohjaisiksi hyökkäyksiksi”. [26.]

Yksi esimerkki on TCP SYN-Flood -hyökkäys. Siinä käytetään hyväksi TCP-protokollan kolmivaihekättelyä. Kättelyn toimintaperiaate on seuraava: yhteyden muodostava kone lähettää SYN-viestin palvelimelle, palvelin kuittaa saamansa pyynnön SYN-ACK-viestillä, ja tämän jälkeen yhteyden pyytäjä vastaa ACK-viestillä, että yhteys on muodostunut. SYN-Flood-hyökkäyksessä hyökkääjä lähettää väärennetyllä IP-osoitteella paljon SYN-paketteja kohdepalvelimelle. Palvelin ei tiedä olevansa hyökkäyksen kohteena ja

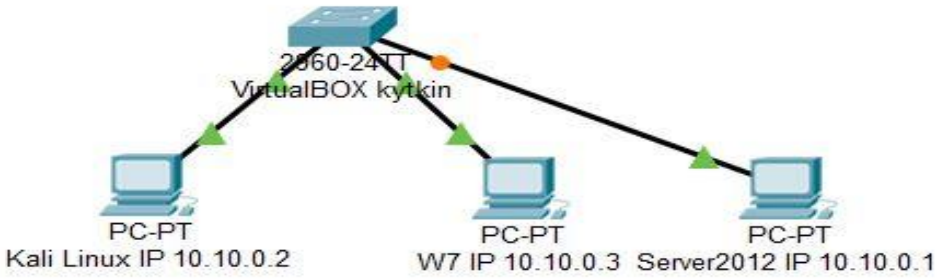
lähettää SYN –ACK-vastauksia olemattomille IP-osoitteille, mutta ei saa takaisin kuittauksia. Tämä aiheuttaa sen, että palvelimelle jää paljon avonaisia portteja odottamaan ACK-kuittauksia, joita ei lopulta saavukaan. Jossain vaiheessa porttitaulussa tapahtuu ylivuoto, ja palvelin joko kaatuu tai toimii väärin. [27.]

# 8 Tietomurtohyökkäyksen anatomia

Lähtökohtaisesti hakkeri pääsee sisään järjestelmään, jos hänellä on riittävä motivaatio ja riittävästi aikaa. Yleensä kaikki hyökkäykset noudattavat tuttua kaavaa, joissa hyökkääjä saa jotenkin muuntamansa exe-koodin ujutettua järjestelmän sisään esimerkiksi Word-tekstinkäsittelyohjelman liitetiedoston, selaimen tai näppäimistön avulla ja sen jälkeen käyttäjän suorittamaan exe-koodin. Tämän jälkeen murtautuja siirtää koodin johonkin muuhun prosessiin ja käyttäjän on vaikea löytää sitä enää järjestelmästä.

## 8.1 Hyökkäysympäristön rakentaminen

Parhaiten hyökkäystä päästään kokeilemaan virtualisoidussa oppimisympäristössä. Siinä VirtualBOX-ympäristöön asennetaan Kali Linux-kone, josta hyökkäykset tapahtuvat ja hyökkäyksen kohdekoneiksi Windows7-työasemakone ja Windows Server2012-palvelinkone. Kuvaan 15 on piirretty havainnekuva oppimisympäristöstä ja virtuaalikoneiden IP-asetuksista.




Kuva 15: Oppimisympäristön koneiden IP-osoitteiden määritykset.

Toteutetaan hyökkäys Kali Linux -koneelta Windows7-koneelle. Hyökkäys toteutetaan rakentamalla kohde koneeseen (W7) kuorma msfvenom työkalun avulla. Kuvassa 16 nähdään tarvittavat parametrit.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.0.2 LPORT=4
4444 -e x86/shikata_ga_nai -i 1 -f exe -o meterpreter.exe
```

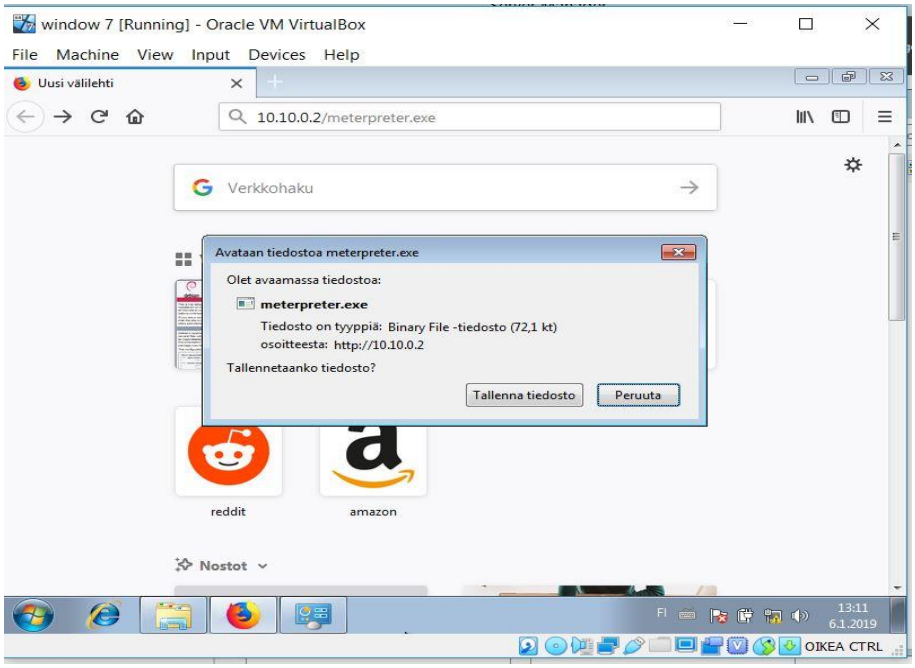
Kuva 16:Hyökkäyskuorman rakentaminen.

Saastutettu tiedosto meterpreter.exe siirretään hakemistoon /var/www/html, josta se voidaan siirtää W7-koneeseen. Kuvassa 17 on esitetty kuorman siirto oikeaan hakemistoon.

```
root@kali:~# cp meterpreter.exe /var/www/html
root@kali:~# cd /var/www/html
root@kali:/var/www/html# ls -la
total 100
drwxr-xr-x 2 root root  4096 Jan  5 18:07 .
drwxr-xr-x 3 root root  4096 Oct 26 04:40 ..
-rw-r--r-- 1 root root 10701 Oct 16 11:56 index.html
-rw-r--r-- 1 root root   612 Oct 16 11:53 index.nginx-debian.html
-rw-r--r-- 1 root root 73802 Jan  5 18:07 meterpreter.exe
root@kali:/var/www/html#
```

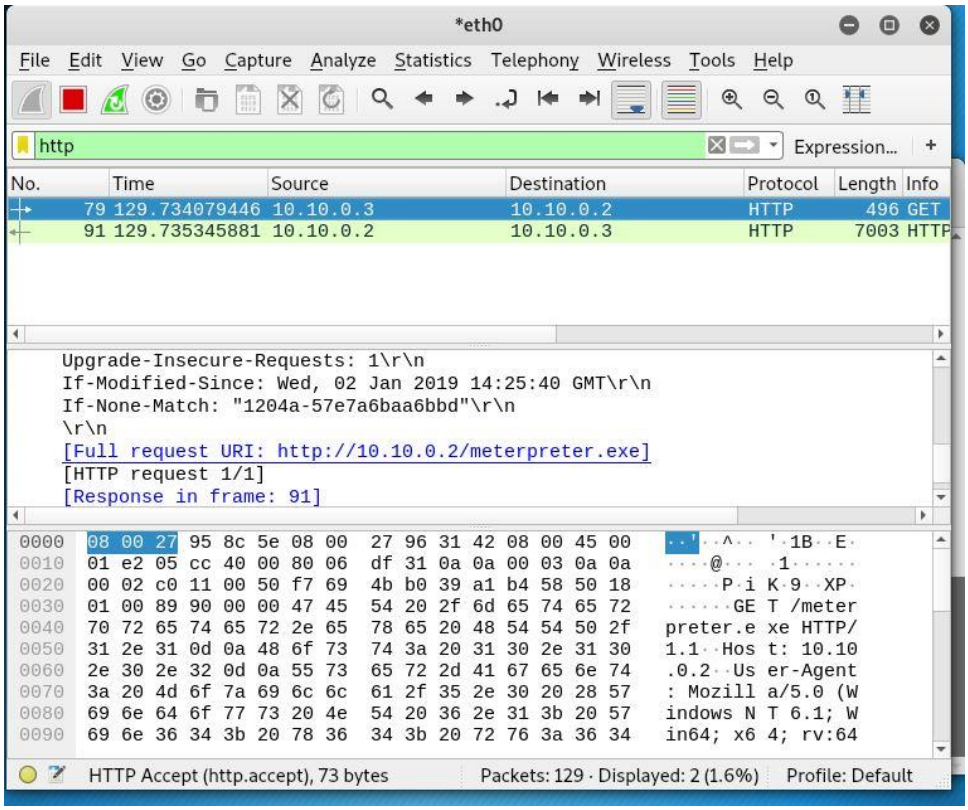
Kuva 17: Hyökkäyskuorman siirto hakemistoon /var/www/html.

Tartutettu meterpreter.exe-tiedosto siirretään W7-koneeseen http-protokollan avulla. Siirtotoiminto esitellään kuvassa 18.



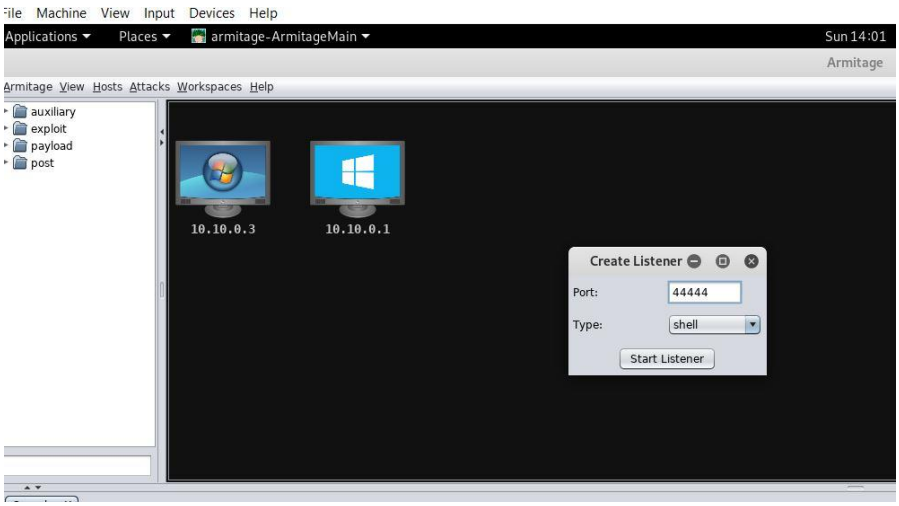

Kuva 18: Hyökkäyskuorman siirto kohdekoneeseen.

Wireshark-ohjelman avulla seurataan samalla tietoliikennettä. Kuvassa 19 voidaan nähdä, että W7-kone (10.10.0.3) hakee GET-komennolla meterpreter.exe-tiedoston Kali Linux -koneelta (10.10.0.2).



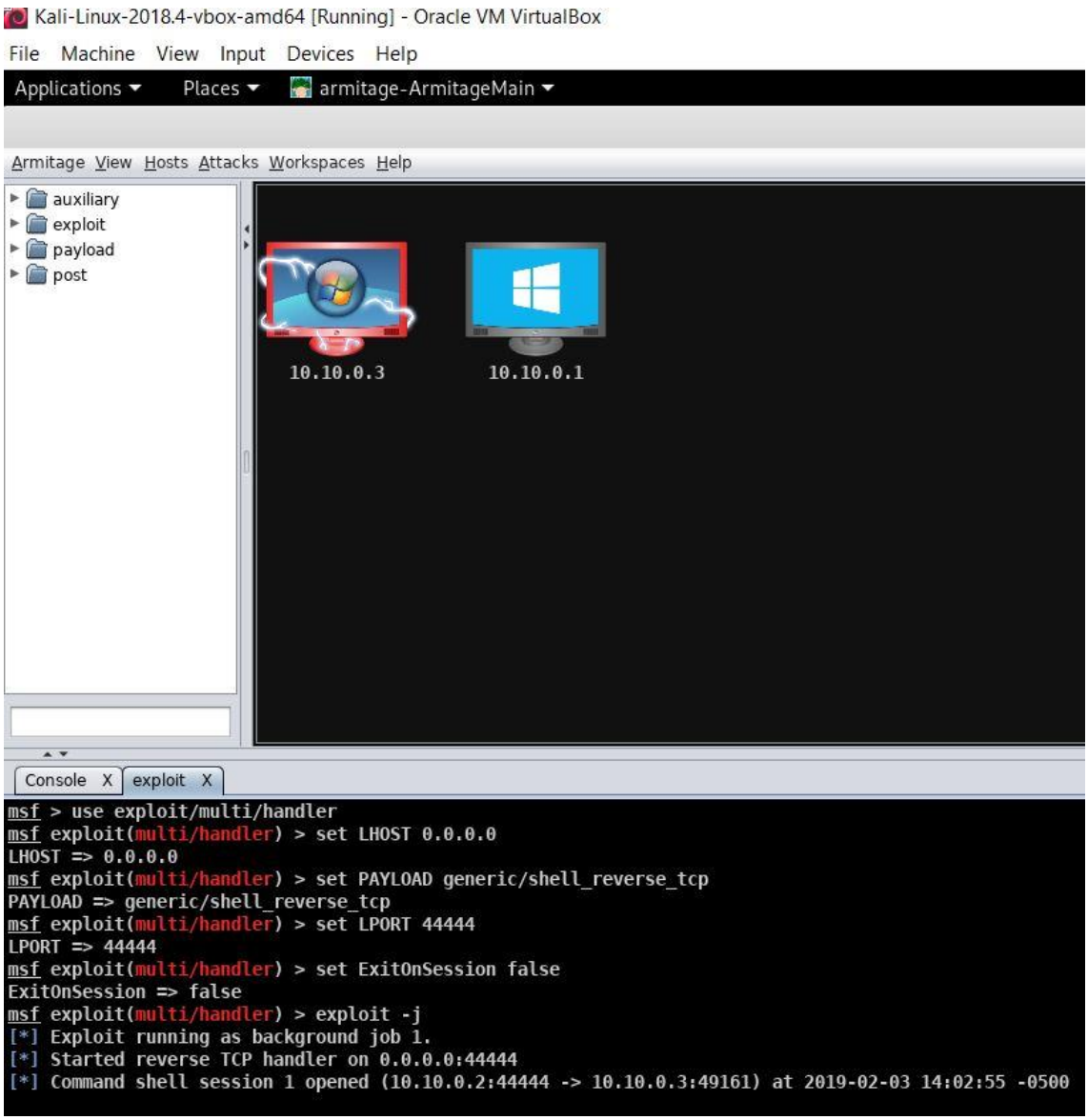

Kuva 19: Wireshark-ohjelmalla tutkitaan hyökkäyskuorman siirto.

Armitage-sovellus käynnistetään perusasetuksilla. Tämän jälkeen käynnistetään Armitage listener ja muistetaan antaa kuormaa rakennettaessa annettu porttimäärittely (port 44444). Tämä kaikki ilmenee kuvassa 20.




Kuva 20: Armitage listenerin käynnistys.

Sen jälkeen käynnistetään W7-koneella kuorma ja Kali Linux -koneen näytöllä nähdään, että W7-kone muuttuu punaiseksi eli se on saatu hallintaan kuvassa 21.




Kuva 21: Kohdekone otettu hallintaan.

## 9 Kyberpuolustus

Yrityksen kyberpuolustuksen rakentamisen lähtökohtana on, että täytyy ensin kartoittaa yrityksen tärkein suojattava kohde. Tämän jälkeen voidaan erilaisin teknisin ja koulutuksellisin keinoin huolehtia siitä, että suojattava kohde pysyy varjeltuna niin yritysvakoilun

kuin muunlaisen hyökkäysuhan vaikutuksilta. On kuitenkin muistettava, että kun rakennetaan suojamuuria hyökkäyksiä ja uhkia vastaan, on pidettävä huoli myös siitä, että tieto on kuitenkin sitä tarvitsevien henkilöiden ja järjestelmien saatavilla helposti. Tietoturvan tarkoituksena ei ole tietoturva itseisarvona, vaan tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistaminen eli CIA-malli. Tähän tavoitteeseen päästäkseen yrityksen on luotava kyberstrategia, johon kuuluu henkilöstön kouluttaminen, tilojen sisäänpääsyjen valvonta ja laitesijoittelu, tietokonelaitteiden tietoturvan määrittelyt, ohjelmistojen tietoturvan määrittelyt sekä järjestelmien vaatimat varmistukset ja palauttamiset. Lisäksi erittäin tärkeä asia on hyökkäyksen havaitseminen ja hyökkäyksen jälkeinen toipuminen.

Seuraavaksi käsitellään yrityksen kyberturvan parantamiseen liittyviä asioita. Itse olen nostanut ykkösprioriteetille henkilöstön koulutustarpeet. Priorisoinnissa useasti lähdetään siitä, että laitetaan palomuurit ja päivitykset kuntoon ja sen jälkeen kerrotaan henkilöstölle, miten yrityksen mielestä eri tilanteissa tulisi toimia. Oma prioriteettini koulutukseen ja sen korostamiseen juontaa siitä, että toimin opettajana. Pidän tärkeänä, että henkilökunta sitoutetaan koulutuksen kautta kyberturvaan jo rakentamisvaiheessa. Koulutuksen aikana henkilökunnalta saattaa tulla hyviä ehdotuksia kyberturvan parantamiseksi, ja ne saadaan lisättyä suoraan yrityksen kyberstrategiaan.

Henkilöstön kouluttaminen

Henkilöstön kouluttaminen on ensiarvoisen tärkeää kyberstrategian onnistumiseksi. Monissa tutkimuksissa on todettu, että henkilöstö on yrityksen heikoin lenkki kyberstrategian onnistumisen kannalta. Koulutettavia asioita on esimerkiksi salasanakäytänteet. Tärkeää on perustella hyvin se, että monimuotoisen ja riittävän pitkän salasanan käyttäminen on tarpeellista. Lisäksi on tärkeää kouluttaa koko henkilöstö havannoimaan ja puuttumaan yrityksen tiloissa liikkuvien ulkopuolisten henkilöiden tarpeellisuuteen ja siihen, millä asioilla he liikkuvat. Tähän tulisi olla selkeät käytännöt, kuten esimerkiksi vierailijakortit. Tässäkin on tärkeää korostaa, että hakkerit eivät kaihda minkäänlaisia keinoja päästäkseen yrityksen tietojärjestelmiin sisäkautta. Lisäksi on tarpeen kouluttaa henkilöstö tunnistamaan erilaiset huijausmenetelmät, jotka saatavat tulla sähköpostin tai median kautta puhumattakaan talon ulkopuolella erilaisissa sosiaalisissa tilanteissa yrityksen asioista puhumisesta. Tietokoneiden ohjelmistojen päivityskäytänteiden tuntemi-

nen on saatettava koko henkilöstön tietoisuuteen ja jälleen korostettava siihen vaikuttavia syitä eli sitä, miten se vähentää tietokoneiden tietoturvariskiä ja mahdollisuutta tulla saastutetuksi.

Työasemien suojaaminen

Monilta tietoturvaongelmilta vältytään, kun suunnitellaan työasemakoneiden konfiguraatiot niin, että ne vastaavat yrityksen tarpeita. Useasti toimittajien käyttämät oletuskonfiguraatiot eivät ota huomioon yrityksen omia tietoturvavaatimuksia vaan ne ovat painottuneet esimerkiksi saamaan koneesta parempaa suorituskykyä. [28.]

Tärkeimpinä asioina on otettava huomioon, että tietokoneiden ohjelmistopäivitykset suoritetaan ajallaan ja että koneisiin on asennettu vain tarvittavat ohjelmistot. Lisäksi koneiden tietojen varmistus- ja varmistusten palautusmenetelmien tulee olla testattu. Hyvä on suunnitella myös käytöstä poistettavien laitteiden tietojen tuhoamismenetelmät. [28.]

Palvelintietokoneiden suojaaminen

Asennetaan uusimmat käyttöjärjestelmäversiot ja asennetaan vain tarpeelliset palvelut. Ylimääräiset palvelut poistetaan. Lisäksi asennetaan palvelintietokoneet lukittuun tilaan, jonne vain tarpeellisilla henkilöillä on kulkuoikeus. Määritellään palvelimen varmistusten ajankohta ja palautustoiminnot sekä testataan ne. Lisäksi suunnitellaan palvelinohjelmistojen päivitysten ajankohta ja käyttöönotto. [28.]

Käyttöoikeudet

Määritellään käyttäjät sopiviin ryhmiin ja suunnitellaan ryhmille käyttöoikeudet palveluihin ja resursseihin GPO:n kautta. Käyttöoikeuksina määritellään salasanan pituudet, voimassaoloajat ja monimuotoisuus. Lisäksi voidaan estää kaikilta esimerkiksi USB-muistitikkujen käyttö. Sen sijaan voidaan käyttää SD-muistikortteja ja muistikortin lukijaa. [29.]

Virukset ja muut haittaohjelmat

Asennetaan virustorjuntaohjelmat ja päivitetään niitä säännöllisesti. Kiinnitetään erikoisesti huomioita palvelinkoneisiin. Asennetaan sähköpostisuotimet kuntoon, että ne hylkäävät epäilyttävät liitetiedostot, kuten EXE ja Javascript. [29.]

Määritetään selaimet käyttämään aina HTTPS-protokollaa ja otetaan Java sekä ActiveX pois päältä. Lisäksi estetään sekä Flashin että Silverlightin käyttö. [29.]

Poistetaan toimistotuotteilta käytöstä tarpeettomat ominaisuudet, kuten esimerkiksi multimediaominaisuudet.

Etäkäyttö

VPN-ratkaisuilla saadaan käyttäjille rakennuttua tietoturvallinen työskentelymahdollisus kotoa. Kannettavien koneiden käyttäjille kannattaa korostaa, että konetta ei saa jättää näkyviin esimerkiksi auton takapenkille tai hotellihuoneeseen. Hotellihuoneessakin kannattaa käyttää lukittavaa reppua.

Palomuuri

Palomuurijärjestelmä kannattaa hankkia ja toteuttaa siihen palomuurin pakettisuodatus. Lisäksi palomuuriin kannattaa asentaa loki- ja hälytysjärjestelmä. Palomuurijärjestelmä pitää olla testattuna ennen käyttöönottoa. [28.]

Tunkeutumisen havaitsemisen ja reagoinnin toimintamallit

Henkilöiden, jotka vastaavat yrityksen tietojärjestelmistä ja verkoista, on oltava valmistautuneita etsimään vihjeitä tietoturvamurroista ja reagoimaan niihin. Hyvä valmistautuminen antaa yritykselle valmiudet nopeasti havaita tunkeutuminen ja reagoida siihen sekä aloittaa nopeasti toipuminen normaalitilanteeseen.

Tärkeää on, että kerätään lokilistoja ja seurataan niitä. Lisäksi verkkotoimintoja ja järjestelmätoimintoja täytyy valvoa ja tutkia. On syytä myös skannata verkkoa luvattomista laitteista ja luvattomasta fyysisestä resurssien käytöstä. Myös tiedostoissa ja hakemistoissa tapahtuneet odottamattomat muutokset ovat signaali tietomurrosta. [28.]

Tunkeutumisiin reagointi

Mikään torjuntamenetelmä ei välttämättä pysty täysin ehkäisemään tunkeutumista, ja sitä varten on tärkeää, että on suunniteltu etukäteen toimintamalli ja vastuut, kuka tekee ja mitä tekee siinä vaiheessa, kun tunkeutuminen havaitaan.

Ensi vaiheessa pyritään estämään tunkeutujan eteneminen järjestelmässä eli pysäyttämään hyökkäys. Seuraavaksi selvitetään, missä laajuudessa tunkeutuminen on tapahtunut ja mihin tietoihin tunkeutuja on päässyt käsiksi. Tärkeää on myös selvittää hyökkäyksen kulku ja dokumentoida mahdollista rikostutkintaa varten kaikki lokit ja tiedot, joita hyökkäyksestä saadaan selville. Tämän jälkeen tukitaan mahdolliset tietoturva-aukot ja palautetaan varmistusten kautta tiedot järjestelmään ja pyritään aloittamaan järjestelmän normaali käyttö. [28.]

## 10 Johtopäätökset

Kyberturvallisuus on aihealueena erittäin laaja, ja helposti opetuksessakin saatetaan lähteä rönsyilemään asiasta toiseen. Tärkeintä olisi kuitenkin perusopetuksessa keskittyä kaikista oleellisimpiin asioihin, jotta koko opetusryhmä saisi onnistumisen kokemuksia ja oppisi sekä tietoturvan että laajempana kokonaisuutena kyberturvan keskeiset asiat. Tämä tarkoittaa osittain myös sitä, että täytyy olla muutama tarkkaan valittu harjoitustehtävä, joiden ohjeistus on laadittu siten, että aihealueesta vähitenkin kiinnostuneet opiskelijat saavat peruskäsityksen hyökkäyksen rakentamisesta ja sitä kautta ymmärtävät puolustuksen tärkeyden. Paremmille ja asiasta enemmän kiinnostuneille opiskelijoille on tarjottava mahdollisuuksia syventää taitojaan ja mahdollisesti myös löytää kyberturvallisuuteen liittyviä alan harjoittelupaikkoja yrityksistä.

Insinöörintyön päätarkoitus oli kartoittaa sopiva oppimisympäristö kyberturvallisuuden opetukseen, ja sellainen löydettiin. Toinen keskeinen tavoite oli kehittää ja testata muutama hyökkäysmenetelmä, joiden avulla oppilaat voisivat harjoitella kyberhyökkäystä. Hyökkäysten testaaminen ja dokumentoiminen oli kuitenkin yllättävän vaativaa, joten lopputuloksena päättötyöhön saatiin yksi dokumentoitu hyökkäys. Oppimisympäristön rakentaminen ja hyökkäyksen testaaminen on jo kerran toteutettu ammattioppilaitoksen kolmannen vuosikurssin opiskelijoille. Opiskelijoiden palaute oli myönteinen.

## Lähteet


1 Viitaila, Mikko. 2016.Miksi kyberturvallisuus on tärkeää? Ajankohtaiset uhat ja niiltä suojautuminen. Verkkoaineisto. < https://koulutus.fcg.fi/Portals/2/Viitaila_Mikko_VAHTI_kuntien_kyberturvallisuuskiertue_VM_n_kanssa__Miksi_kyberturvallisuus_on_t%C3%A4rke%C3%A4%C3%A4.pdf?ver=2016-11-10-081827-830>. 13.10.2016. Luettu 20.2.2019.

2 Yhteiskunnan Turvallisuusstrategia. Valtioneuvoston periaatepäätös. 2010. Verkkoaineisto. Puolustusministeriö. < https://turvallisuuskomitea.fi/wp-content/uploads/2015/10/yts_2010_fi_nettiin.pdf>. 16.12.2010. Luettu 20.1.2019.

3 Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen. 2016. Verkkoaineisto. Valtioneuvosto. < https://tietokayttoon.fi/documents/10616/2009122/9_Kyberosaaminen+Suomessa.pdf/29c8f675-0790-4c2f-91c2-69187b34b37e?version=1.0>. Luettu 18.2.2019.

4 Von Solms, R. & van Niekerk, J. 2013. From information security to cyber security. Verkkoaineisto. Computers & Security. <http://dx.doi.org/10.1016/j.cose.2013.04.004>. Luettu 20.2.2019.

5 Tieto ja tietoliikennetekniikan perustutkinto. 2014. Verkkoaineisto. Opetushallitus. <https://eperusteet.opintopolku.fi/eperusteet-service/api/dokumentit/2336794>. 4.11.2014. Luettu 18.2.2019.

6 Kyberrikollisuutta torjutaan yhteistyöllä. Verkkoaineisto. Sisäministeriö. <https://intermin.fi/poliisiasiat/kyberrikollisuus/kyberrikollisuuden-torjunta>. Luettu 20.1.2019.

7 Laki Tieto- ja Viestintärikoksista. 1995. 578/21.4.1995

8 Tuomio 50 000 Tietomurrosta; Suomalaisteinille ehdollista vankeutta. 2015. Verkkoaineisto. Iltasanomat < > 8.7.2015. Luettu 20.1.2019.

9 Facebook-jäynällä voi olla vakava seuraus-Todellinen esimerkki Suomesta. 2015. Verkkoaineisto. Uusisuomi. <https://www.uusisuomi.fi/kotimaa/110119-facebook-jaynalla-voi-olla-nainkin-vakava-seuraus> 4.9.2015. Luettu 20.1.2019.

10 Osuuspankki vaatii hakkerilta lähes puolta miljoonaa euroa – 17-vuotias perusteli hyökkäystään testaamisella. 2017. Verkkoaineisto. MTV Uutiset <https://www.mtvuutiset.fi/artikkeli/osuuspankki-vaatii-hakkerilta-lahes-puolta-miljoonaa-euroa-17-vuotias-perusteli-hyokkaystaan-testaamisella/6620090#gs.HdfuKEgK> 16.10.2017. Luettu 20.1.2019.

11 Oracle Virtualbox FAQ-Frequently Asked Questions.2019. Verkkoaineisto. H2S Media. <https://www.how2shout.com/what-is/oracle-virtualbox-faq.html> 20.2.2019. Luettu 22.2.2019.

12 Long, J. 2005. Google Hacking for Penetration Testers. Rockland: Syngress Publishing.

13 Penetraatiotestaus. Verkkoaineisto. Secmeter. <http://www.secmeter.com/penetraatiotestaus.html>. Luettu 3.2.2019.

14 Vähämaa, Aleksi. 2016. Verkkoaineisto. Tietoviikko. <https://www.tivi.fi/Kaikki_uutiset/kali-on-eettisen-hakkerin-linux-paketti-6586455>. 28.2.2016. Luettu19.10.2018.

15 Kali Linux Tools. Verkkoaineisto. Offensive Security. <https://tools.kali.org/tools-listing>. Luettu 24.2.2019.

16 Rouse, Margaret. Google hacking (Google scanning or Enginen hacking). Verkkoaineisto. <https://searchsecurity.techtarget.com/definition/Google-hacking>. Luettu 3.11.2018.

17 Google Hackining Database. Verkkoaineisto. Exploit Database. <https://www.exploit-db.com/google-hacking-database>. Luettu 9.3.2019.

18 Kurittu, Antti. Tietomurtojen ennaltaehkäisy, havaitseminen ja tutkinta. Verkkoaineisto. <https://teknologiateollisuus.fi/sites/default/files/kurittu_viestintavirasto.pdf>. Luettu 3.2.2019.

19 Bullock, J. & Paker J. 2017. Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework. Indianapolis: John Wiley & Sons.

20 OSI –malli. Verkkoaineisto. Wikipedia. <https://fi.wikipedia.org/wiki/OSI-malli>. Luettu 18.2.2019.

21 Sanger, E. David & Schmitt, Eric. 2015.Russian Ship Near Cables Are Too Close for U.S. Comfort. Verkkoaineisto. The New York Times. <https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html>. 26.10.2015. Luettu 18.2.1019.

22 Varo langattoman verkon vaaroja. Verkkoaineisto. Symantec Suomi. <http://www.symantec.com/region/fi/resources/wireless.html>. Luettu 18.2.2019.

23 Pätynen, Erik. 2018.Tietoverkkojen kyberturvallisuus. Luentomoniste. Metropolia Ammattikorkeakoulu.

24 MAC Flooding. 2018. Verkkoaineisto. Wikipedia. <https://en.wikipedia.org/wiki/MAC_flooding>. 10.1.2018. Luettu 21.2.2019.

25 Palvelunestohyökkäysten tekniikkaa puolustajille. 2016. Verkkoaineisto. Viestintävirasto. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_liite_1_Palvelunestohyokkaysten_tekniikkaa_puolustajille.pdf>. 29.4.2016. Luettu 9.3.2019.

26 Jääskelä, Jari. 2017. Sovelluskerroksen palvelunestohyökkäyksien toteuttaminen ja torjunta. Insinöörityö. Centria Ammattikorkeakoulu. Theseus-tietokanta.

27 Imperva. 2019. TCP SYN Flood. What is a Syn Flood Attack. Verkkoaineisto. <https://www.incapsula.com/ddos/attack-glossary/syn-flood.html>. Luettu 21.2.2019.

28 Allen, Julia H. 2002. CERT Verkkotietoturvan hallinta. Helsinki. Edita Prima Oy.

29 Niemelä, Jarno. 2018. Puolustava kyberturvallisuus. Luentomoniste. Metropolia Ammattikorkeakoulu.