LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Laboratorioharjoituksia kyberturvallisuuden opiskelijoille

Lindfors, Tomi & Myllylä, Juuso

2017 Laurea

Laurea-ammattikorkeakoulu

Laboratorioharjoituksia kyberturvallisuuden opiskelijoille

Lindfors, Tomi & Myllylä, Juuso
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Maaliskuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutusohjelma
IT-Tradenomi

Tomi Lindfors, Juuso Myllylä

Laboratorioharjoituksia kyberturvallisuuden opiskelijoille

Vuosi 2017 Sivumäärä 41

Ammattikorkeakouluissa järjestetään nykyään useita virtuaalisia opintojaksoja, joissa ei ole lähiopetusta. Tällöin opiskelija saattaa kokea oppineensa opintojaksolla käsitellyt aiheet vain pinnallisella tasolla, sillä hän ei pysty soveltamaan taitojaan käytännössä. Tämä voi aiheuttaa opiskelijassa turhautumista etenkin, jos hän kokee aiheen mielenkiintoiseksi. Tämän opinnäytetyön tavoitteena onkin ratkaista tämä ongelma luomalla käytännön harjoituksia kyberturvallisuudesta kiinnostuneille opiskelijoille, jotta he voivat syventää oppimisprosessiaan soveltamalla opittuja teoriataitoja käytännön harjoituksissa. Tällöin opiskelijat saattavat myös löytää itselleen mahdollisen urapolun kyberturvallisuuden parista, sillä näiden harjoitusten avulla opiskelijat tutustuvat yleisimpiin kyberturvallisuuteen liittyviin työkaluihin ja ohjelmistoihin.

Opinnäytetyön kehittämistehtävä oli luoda Laurea-ammattikorkeakoulun Leppävaaran kampuksella järjestettävään Network Security –opintojaksolle harjoituskokonaisuuksia, jotta opiskelijoille olisi mahdollista tarjota myös käytännön harjoituksia tukemaan heidän oppimisprosessia. Opinnäytetyöprosessin alussa ei ollut lainkaan käytännön harjoituksia, joita opiskelijat olisivat voineet tehdä.

Kehitystyö pohjautui suurin osin oman tiedon ja osaamisen soveltamiseen sekä tutkimukseen, koska lopputulos muodostui yksi aihealue kerrallaan inkrementaalisen toimintamallin mukaisesti. Tämän kehittämismenetelmän avulla prosessissa edettiin loogisesti sekä nopeasti. Kehittämistyötä kehitettiin myös tiiviissä yhteistyössä työelämän edustajan kanssa, sillä tahdoimme pitää tapaamisia viikoittain varmistaaksemme parhaan mahdollisen lopputuloksen. Tämän ansiosta pystyimme korjaamaan kaikki mahdolliset ongelmatilanteet hyvissä ajoin ja saavutimme toivotut tavoitteet.

Opinnäytetyön lopputuloksena on viisi käytännön harjoituskokonaisuutta, ohjeistukset, raportti sekä laboratorioympäristö. Harjoituksissa opiskelijat tutustuvat lukuisiin ohjelmistoihin sekä Linux käyttöjärjestelmän työkaluihin. Raportista luotiin kaksi eri versiota, pelkkä pohja opiskelijoille ja ohjaajille luotiin versio, josta löytyy oikeat vastaukset. Keräsimme myös listan mahdollisista jatkokehitysehdotuksista käytännön harjoitusten parantamiseen. Tärkeimpiä kehitysehdotuksia tulevaisuutta varten ovat esimerkiksi uusien ja haastavien harjoitusten luominen sekä laboratorioympäristön kasvattaminen suurempiin opetustiloihin.

Asiasanat: kyberturvallisuus, inkrementaalinen kehitys, tietoturva, virtuaalinen ympäristö

Laurea University of Applied Sciences
Degree in Business Information Technology
Bachelor's degree

Abstract

Tomi Lindfors, Juuso Myllylä

Hands-on exercises for cybersecurity students

Year 2017 Pages 41

In today's college courses, virtual study units have grown to be more popular than ever, due to their flexibility for both students and teachers. It is also common for the virtual courses not to have any classroom teaching. As the virtual study units focus heavily on theory, students may feel disappointed, if they can't apply their skills in practice at all. This is even a more serious problem, if the student finds the subject interesting. The goal for this thesis is to solve the problem by creating hands-on exercises for cybersecurity students, so they can apply their theoretical knowledge in practice. This way more students may find a new career path with cybersecurity, since the exercises include common practices for cybersecurity professionals.

The development project was to create a set of exercises with instructions for a virtual study unit to help students deepen their knowledge on cybersecurity. In the beginning of the thesis process, there weren't any exercises that the students could use to gain a more practical approach to fully understand what they have learned in theory when completing the virtual study unit.

Developing the exercises, lab environment and instructions was largely based on applying our own knowledge on the subject. Research was also a large part of the development, since we used the incremental model to create the exercises. The incremental model helped us reach our goals quickly and easily. During the development process, we also had many meetings with Laurea's representative to ensure the best possible outcome for the exercises and instructions. By having many meetings during the process, we were able to prevent any big issues from manifesting.

After the development process, we created a working hands-on lab environment for the Leppävaara campus. We also created five cybersecurity exercises and instructions on how to complete them. A separate installation guide for the virtual environment was also made to help students simulate the same environment in their own homes. We also made a report for the students to fill, since the exercises are included in the evaluation process. Based on the created report, we filled it with the correct answers to help the teachers to evaluate the answers provided by the students. We also compiled a suggestions list for the future to improve the exercises. The most notable suggestions were to create more exercises in general and to make them more challenging.

Keywords: cybersecurity, incremental lifecycle, information security, virtual machine

Sisällys

Käsitteet ja lyhenteet

Penetraatiotestaus	Tietoturvahaavoittuvuuksien kartoittamista kohteen verkosta ja käytänteistä
Oracle VirtualBox	Virtuaaliympäristön alusta, jossa Kali Linux käyttöjärjestelmää suoritetaan harjoitusten aikana
Distribuutio	Linux käyttöjärjestelmän versio. Kali Linux on yksi Linux käyttöjärjestelmän lukuisista distribuutioista
ICMP	Internet Control Message Protocol, jota käytetään viestien välittämiseen koneiden välillä. ICMP–protokollaa käytetään Ping ja Traceroute työkaluissa.
TCP	Transmission Control Protocol luo yhteyksiä koneiden välille, jotka ovat yhteydessä Internetiin
UDP	User Datagram Protocol mahdollistaa tiedostojen siirron yhteydettömästi laitteiden välillä
Nmap	Nmap on Kali Linux käyttöjärjestelmässä toimiva ohjelmisto, jonka avulla on mahdollista skannata verkkoja.
SHA	Secure Hash Algorithm on yksi kryptografisista tiivistefunktioista.
Salausalgoritmi	Algoritmi, jonka avulla salausjärjestelmä muuttaa tiedon tai viestin salatuksi.
Footprinting	Hakkeroinnin toimintatapa, jossa pyritään selvittämään kohteesta tietoja, kuten käyttöjärjestelmä.
Cleartext	Salauksen purkamisen jälkeen luettavissa oleva teksti. Esimerkkinä 1ad99cbe9e425d4f19c53a29d4f12597 on MD5 salausalgoritmilla salattu teksti, jonka cleartext on kissa.
Root-käyttäjä	Linux käyttöjärjestelmän oletusjärjestelmänvalvojakäyttäjätili
Unix	Laitteistosta riippumaton käyttöjärjestelmäperhe, johon kuuluu esimerkiksi Applen Mac OS X.
Otaverkko	Pääkaupunkiseudun korkeakoulujen verkkopalvelin.

1 Johdanto

Korkeakouluissa opiskelijat osallistuvat opintojensa aikana useille opintojaksoille, joiden toteutus on täysin virtuaalinen. Tällöin opetus on pääsääntöisesti teoriapainotteista, eikä oppimiskokemus välttämättä ole niin käytännön läheistä kuin opiskelijat haluavat. Pyrimme kehittämään tähän ongelmaan ratkaisun luomalla kyberturvallisuuteen liittyviä käytännön harjoituksia, joissa opiskelijat oppivat hyödyntämään jo teoriassa oppimiaan taitoja fyysisessä ympäristössä. Harjoitukset pohjautuvat Network Security-opintojaksolla käytyihin aihekokonaisuuksiin, joihin lukeutuvat muun muassa salasanojen murtaminen ja verkossa tapahtuvan liikenteen analysointi.

Opinnäytetyön aihe pohjautuu kasvavaan tarpeeseen kouluttaa lisää kyberturvallisuuden asiantuntijoita, sillä tietoturvariskit ovat yleistymässä kiihtyvään tahtiin. (O'Hara 2017.) Näiden harjoitusten avulla pyrimme esittelemään kyberturvallisuudesta kiinnostuneille opiskelijoille käytännön lähestymistapaa tietoturvamaailmaan. Aihe syntyi myös tarpeesta tutkia kuinka käytännön harjoituksia voidaan luoda hyödyntämällä jo olemassa olevia resursseja, sillä Laurea-ammattikorkeakoulun Leppävaaran kampuksella ei ole vielä käytössä kyberturvallisuuteen liittyviä käytännön harjoituksia. Opiskelijat ovat myös antaneet palautetta, että toivovat juurikin Network Security-opintojaksolle käytännön harjoituksia päästäkseen kokeilemaan oppimiaan asioita myös käytännön tasolla. Opiskelijoita ajatellen harjoituskokonaisuudet tullaan toteuttamaan siten, että harjoitukset voidaan tehdä joko koululla fyysisessä oppimisympäristössä ohjatusti tai opiskelijan kotona itsenäisesti.

Harjoitusten suunnittelussa on myös huomioitava pedagoginen lähestymistapa, sillä harjoitukset tulevat olemaan osa Network Security opintojaksoa ja täten ne ovat myös arvioitavia suorituksia. Arviointiperustaksi valitsimme penetraatiotestausraportin, jota kirjoitetaan läpi opintojakson. Tämä helpottaa opettajien arviointia, sillä kaikilla on samanlainen raportti. Raportissa jokaisesta harjoituksesta kirjoitetaan omat työvaiheet, työkalut mitä käytettiin sekä selitetään omin sanoin valikoitujen komentojen ja ohjelmistojen toimivuutta. Toinen pedagoginen näkökulma on ohjeiden tekeminen jokaiseen harjoitukseen. Ohjeet tulee toteuttaa mahdollisimman selkeästi, jotta opiskelijoilla on selkeä käsitys mitä harjoituksen aikana tulee käydä läpi.

Opinnäytetyössä keskitytään myös etiikan näkökulmaan, sillä kaikki harjoitukset liittyvät eettiseen hakkerointiin. Eettinen hakkerointi tarkoittaa hakkeroimista hyvin periaattein, jolloin samoja työtapoja käytetään esimerkiksi yrityksen tietoturvahaavoittuvuuksien kartoittamiseen. Tämän takia on tärkeää painottaa hyviä käytäntöjä ja eettistä ajattelua, sillä samoilla työtavoilla on mahdollista myös haavoittaa kohdetta tahattomasti tai tahallisesti. Resurssien suojaaminen on myös tärkeä eettinen näkökulma. Tämän takia kaikki harjoitukset toteutetaan virtuaaliympäristössä, jotta koulun tai opiskelijoiden tietokoneet

eivät vahingoitu millään tavalla. Pyrimme myös harjoituksissa huolehtimaan erityisesti siitä, että yksikään toimenpide ei aiheuta vahinkoa kohteelle, jota tutkitaan harjoitusten aikana. (SearchSecurity 2016.)

Työn tilaajana toimii Laurea-ammattikorkeakoulu ja yhteistyökumppanina Network Security – opintojakson opettaja. Työ suoritetaan tiiviissä yhteistyössä, jotta saamme luotua parhaimman mahdollisen lopputuloksen.

2 Tavoite, menetelmät sekä tutkimuksen rakenne

Tässä kappaleessa käsitellään opinnäytetyön tavoitteita sekä menetelmiä. Tavoitteissa selvitämme päätavoitetta, oppimisympäristön tavoitetta sekä dokumentoinnin tavoitetta. Menetelmän osalta tarkastelemme valitsemaamme kehittämismenetelmää ja sen soveltuvuutta käyttötarkoitukseen. Kuvaamme myös tutkimuksemme rakenteen sekä miten sovelsimme kehittämismenetelmää opinnäytetyöprosessin aikana.

2.1 Tavoitteet

Opinnäytetyön tavoitteena on suunnitella ja luoda yksinkertaisesti toteutettava tehtävä- ja harjoituskokonaisuus, joka on myös skaalautuvassa muodossa. Tavoitteena on pystyä toteuttamaan nämä kaikki harjoitukset jo olemassa olevilla resursseilla välttäen ylimääräisten kustannusten ja hankintojen määrää. Muita tavoitteita on luoda raporttipohja sekä ohjeistus harjoituksia varten.

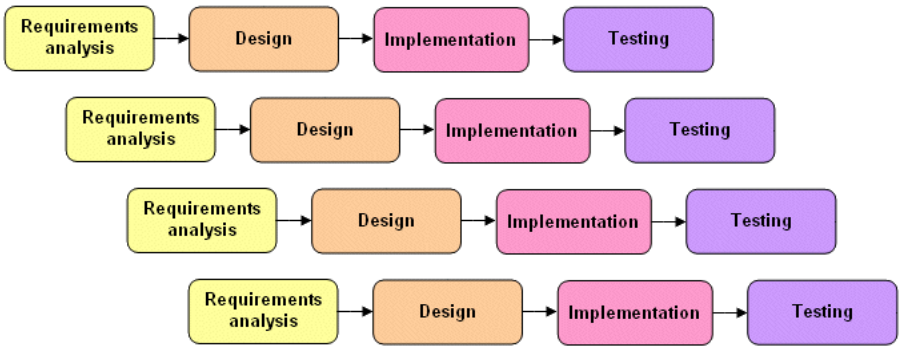
Oppimisympäristön tavoitteena on saada harjoitukset toteutettua koulussa tai vaihtoehtoisesti opiskelijan omalla tietokoneella. Kouluympäristössä tavoitteena on asentaa kaikki tarvittavat ohjelmistot tietokoneille, jotta käytännön harjoitukset voidaan aloittaa mahdollisimman vaivattomasti. Opiskelijan ympäristön tavoitteena on luoda ohjeet siihen, kuinka opiskelija asentaa itselleen virtuaalisen käyttöalustan ja kuinka hän saa asennettua kaikki samalla tavalla kuin koulun ympäristössä. Tarjoamalla mahdollisuuden suorittaa harjoitukset koulun lisäksi myös kotona takaa sen, että kaikilla on mahdollisuus osallistua käytännön harjoitusten tekemiseen.

Harjoitusraportin tavoitteena on luoda yhtenäinen pohja, johon kaikki opiskelijat kirjaavat työvaiheitaan ja täten muodostetaan arvioitava perusta harjoituksille. Raportin toisena tavoitteena on luoda raporttipohjasta mahdollisimman selkeä, jotta samaa raporttipohjaa voidaan muokata tarvittaessa myös muille opintojaksoille. Kolmas tavoite raporttipohjalle asetetaan selkeyden, muokattavuuden ja yksinkertaisuuden näkökulmasta, sillä näiden tavoitteiden avulla pyritään saavuttamaan skaalautuvuutta raporttipohjan näkökulmasta.

Ohjeistusten tavoitteena on luoda selkeät ja ymmärrettävät ohjeet, sillä opiskelijat tulevat suorittamaan kaikki harjoitukset kirjoittamiemme ohjeiden perusteella. Tällöin ohjeita luotaessa on oltava varmoja niiden toimivuudesta sekä selkeydestä. Ohjeistukset luodaan jokaiselle harjoitukselle sekä myös virtuaaliympäristön luomiselle. Erityisesti virtuaaliympäristön ohjeistuksen tulee olla täysin luotettava, sillä asennusprosessi ei välttämättä onnistu noudattamatta ohjeita.

2.2 Kehittämismenetelmä

Opinnäytetyön kehittämismenetelmänä toimii inkrementaalinen malli, joka soveltuu erinomaisesti kehittämistehtäviin jotka tehdään tietyssä järjestyksessä. Inkrementaalisessa mallissa kehittämisen aikana tehdään useita eri kehityssyklejä, jotka lisäävät toiminnallisuutta aina edellisen syklin päälle. (ISTQB 2017.) Tämä menetelmä soveltuu erityisen hyvin kehittämistehtäviin, jossa luodaan suurempia kokonaisuuksia tyhjästä.



Kuvio 1: Inkrementaalinen toteutusmalli (TechnologyUK.)

Menetelmä soveltui mainiosti kehittämistehtäväämme, sillä työ suoritettiin sykleittäin. Kehittämissyklimme olivat vaatimusmäärittelyn tekeminen, laboratorioympäristön luominen, harjoitusten suunnittelu ja luominen, dokumentaation luominen sekä testaus. Syklit tuli toteuttaa juuri tässä järjestyksessä, sillä edellisen syklin tietoja ja toimia tarvittiin aina seuraavan syklin toteuttamiseen.

Käytimme myös benchmarking-tutkimusmenetelmää valitessamme sopivaa käyttöjärjestelmää käytännön harjoitusten suorittamista varten. Benchmarking-tutkimusmenetelmässä kahta eri asiaa verrataan keskenään määriteltyjen ominaisuuksien kannalta. Tämä tutkimusmenetelmä sopi siis erinomaisesti kahden eri käyttöjärjestelmän ominaisuuksien vertailussa. (BusinessDictionary 2017.)

2.3 Tutkimuksen rakenne

Noudattamalla inkrementaalista kehittämismallia, loimme kehittämistyöllemme sovelletun inkrementaalisen mallin, jonka mukaan koko opinnäytetyöprosessi etenee. Alla olevasta kuviosta käy ilmi miten inkrementaalinen malli soveltuu käytännön harjoitusten tekemiseen.

Kuvio 2: Käytännön laboratorioharjoitusten luomisprosessi

Tämän rakenteen avulla on mahdollista suunnitella ja luoda harjoituskokonaisuuksia, sillä kehittämistyö noudattaa täysin yllä kuvattua prosessia. Tällä rakenteella on myös mahdollista luoda samankaltaisia harjoituksia muille opintojaksoille.

3 Opintojakson kuvaus

Network Security-opintojakso on Laurea-ammattikorkeakoulun järjestämä kyberturvallisuuteen perustuva opintokokonaisuus. Opintojakson sisältö koostuu kahdeksasta moduulista, joiden aikana opiskelija oppii monipuolisesti kyberturvallisuuteen liittyviä asioita ja aina moduulin päättyessä myös reflektoi oppimiaan aihekokonaisuuksia.

Opintojakso perustuu Certified Ethical Hacker-sertifikaattiin, jonka myöntäjänä toimii International Council of Electronic Commerce Consultants. Sertifikaatin pääsisältönä on todentaa henkilön kyvyt ymmärtää ja tuntea järjestelmien heikkoudet ja haavoittuvuudet ja käyttää vain hyviä aikeita näiden ongelmien korjaamiseen. (EC-Council 2017.)

Tällä hetkellä Network Security-opintojakso koostuu neljästä eri osa-alueesta. Näitä osa-alueista ensimmäinen on virtuaalinen oppimisympäristö. Virtuaalisessa oppimisympäristössä opiskelijat perehtyvät Certified Ethical Hacker-sertifikaatin mukaisiin aihealueisiin opetusvideoiden ja testien avulla. Virtuaalisessa oppimisympäristössä on kahdeksan eri moduulia, joiden rakenne muodostuu ensin käymällä läpi tietyn aihealueen, sen jälkeen kuinka aihealueen heikkouksia on mahdollista hyödyntää ja lopuksi kuinka heikkouksia voidaan vahvistaa. Tämä luo opiskelijalle selkeän käsityksen aihealueeseen liittyvistä uhista ja haavoittuvuuksista sekä kuinka näihin uhkiin on mahdollista valmistautua ja puolustautua. Esimerkiksi moduuli Hacking Wireless Networks sisältää ensin tietoa langattomista verkoista, niiden salauksista, hyökkäyksistä, havaitsemista, työkaluista ja vastatoimista.

Toisena kokonaisuutena opintojaksolla hyödynnetään reflektiopäiväkirjoja. Reflektiopäiväkirjojen tarkoituksena on saada opiskelija ymmärtämään ja sisäistämään oppimaansa kirjoittamalla aiheesta omin sanoin. Reflektiotehtävien tehtävänannot asettavat opiskelijan havainnollisesti tietoturva-asiantuntijan asemaan ja hänen on omin sanoin kuvailtava mitä hän tekisi tietyissä tilanteissa äskettäin oppimansa perusteella. Esimerkkinä reflektiotehtävästä opiskelijan tulee kertoa omin sanoin kuinka hän toimisi pankissa työskentelevänä tietoturvapäällikkönä parantaakseen järjestelmien yleistä turvallisuutta. Reflektiopäiväkirjat ovat myös tällä hetkellä ainoa käytännönläheinen tapa soveltaa opittua teoriaa. Tämän takia on tärkeää saada luotua myös käytännön harjoituksia tukemaan oppimista.

Kolmannen kokonaisuuden muodostavat kaksi koetta, jotka kummatkin kattavat neljä moduulia sisälleen. Kokeet ovat pakollisia suorituksia reflektiopäiväkirjojen sekä virtuaaliympäristön videoiden ja testien lisäksi. Kokeissa on useita monivalintakysymyksiä, joihin opiskelija vastaa aiemmin oppimansa perusteella. Koekysymykset painottuvat enemmän tarkkaan tekniseen tietoon, sillä tietoturva-alalla on tärkeää osata erottaa samankaltaiset asiat toisistaan. Esimerkkinä koekysymyksestä voidaan pitää tehtävää, jossa opiskelijan on kyettävä valitsemaan kuinka monta bittiä käytetään tietyn salausalgoritmin suojauksessa.

Neljäs kokonaisuus on vapaaehtoiset lähiopetustapahtumat, joita opintojakson ohjaajat järjestävät useasti koko opintojakson ajan. Lähiopetuksessa opiskelijat voivat perehtyä tarkemmin heille hankaliin asioihin ohjaajien avustuksella, jotta mikään aihealue ei jää epäselväksi. Näihin tapahtumiin voi osallistua kuka tahansa opiskelija, joka kokee tarvetta saada henkilökohtaista ohjausta liittyen opintojaksolla käytyihin aiheisiin. Lähiopetuksen tarjoaminen on hyvä keino luoda lisäarvoa oppimisprosessiin.

Viides kokonaisuus Network Security opintojaksolla tulee olemaan käytännön harjoitukset, joissa opiskelijat pystyvät hyödyntämään kaikkien näiden neljän edellisen kokonaisuuden

ymmärrystä suorittaessaan käytännön harjoituksia. Koemme tämän viidennen kokonaisuuden lisäämisen opintojaksolle tarjoavan lähes täydellisen oppimiskokonaisuuden, sillä ensin opiskelijoille tarjotaan kattava tietoperusta aiheesta, jonka jälkeen he pystyvät soveltamaan teoreettista osaamistaan käytännön harjoitteissa. Käytännön harjoitusten jälkeen opiskelijat pystyvät reflektoimaan kaikkea oppimaansa omin sanoin, jolloin he ovat saaneet kattavaa tietoa ja osaamista käsitellystä aihekokonaisuudesta.

4 Vaatimusmäärittely

Tässä kappaleessa luomme vaatimukset käytännön harjoitusten toteuttamiselle. Otamme huomioon myös ohjaajan sekä oppilaan näkökulmat. Näiden vaatimusmäärittelyjen avulla mahdollistamme selkeät vaatimukset harjoitusten suorittamisesta kolmesta eri perspektiivistä. Laitteiston kannalta keskitymme harjoitusten kunnolliseen toimintaan, ohjaajan näkökulmasta laboratorioiden onnistuneeseen ohjaukseen ja oppilaan perspektiivissä keskitymme enimmäkseen ohjeistukseen.

4.1 Laitteiston vaatimusmäärittely

Jotta käytännön harjoituksia voidaan toteuttaa, tietokoneen tulee täyttää tietyt vaatimukset virtuaaliympäristön suorittamiseen. Virtuaaliympäristö ei vaadi tehokasta tietokonetta, joten kaikki opiskelijat pystyvät suorittamaan harjoitukset hieman vanhemmillakin tietokoneilla. Virtuaaliympäristön luomiseen käytämme Oraclen VirtualBoxia, joka itsessään on kevyt ohjelma. (VirtualBox 2017.)

Laitteiston vaatimusmäärittely:

- Vähintään 512 megabittiä RAM muistia
- Vähintään 40 gigabittiä tallennustilaa
- Tuettu käyttöjärjestelmä (Windows, Mac OS X, useita Linux julkaisuja)
- Tuettu vieraskäyttöjärjestelmä (Windows, Mac OS X, useita Linux julkaisuja)
- Toimiva internet yhteys

Mikäli nämä ehdot täyttyvät, on virtuaaliympäristön luominen mahdollista ja yksinkertaista ohjeita noudattaen. On kuitenkin äärimmäisen tärkeää että asennusohjeita noudatetaan tarkasti, sillä virtuaaliympäristö ei välttämättä toimi niin kuin pitää, mikäli jotkin asetukset eivät ole päällä. Kehitimme tähän tarkoitukseen yksityiskohtaiset ohjeet kuinka valitsemamme käyttöjärjestelmä tulee asentaa. Käytimme myös runsaasti kuvia ohjeiden noudattamisen helpottamiseksi.

4.2 Ohjaajan näkökulma

Käytännön harjoitusten näkökulmasta ohjaajan rooli keskittyy pääosin virtuaaliympäristön toteuttamiseen, opiskelijoiden ohjaamiseen sekä raporttien arvioimiseen. Ohjaajan osalta tärkein tehtävä on tukea opiskelijoita laboratorioharjoitusten aikana sekä hänen on kyettävä korjaamaan yleisimpiä mahdollisia vikoja.

Ohjaajan on kyettävä käyttämään virtuaaliympäristöä luontevasti sekä pystyttävä vastaamaan kysymyksiin ja ongelmatilanteisiin asiantuntevalla taidolla, mikäli opiskelijoilla on ongelmia näiden kanssa. Näihin asioihin ohjaaja pystyy valmistautumaan perehtymällä virtuaaliympäristöön huolellisesti sekä opiskelemalla virtuaaliympäristön asennusohjetta. Ohjaajan tulee myös osata käyttää Linux käyttöjärjestelmiä luontevasti, jotta hän pystyy tehokkaasti tunnistamaan mahdolliset ongelmat ja neuvoa opiskelijoita, kuinka nämä ongelmat tulee korjata. Myös aiempi kokemus virtuaaliympäristöistä katsotaan hyödylliseksi.

Raportteja arvioidessa ohjaaja käyttää omaa harkintakykyään arvioidessaan tehtäviä, jossa ei ole tiettyä oikeaa vastausta. Hänen on myös kyettävä ymmärtämään opiskelijan ajatteluprosessi arvioidessaan raporttia. Raportit arvioidaan kuitenkin samankaltaisesti kuin kaikki muutkin raportit, joten näissä tehtävissä ei ole mitään erikoista verrattuna muihin tyypillisiin raporttien arviointeihin.

4.3 Opiskelijan näkökulma

Opiskelijan roolista käytännön harjoitusten näkökulma keskittyy haluun oppia, ohjeiden noudattamiseen sekä eettiseen toimintaan. Ohjeiden noudattaminen on myös tärkeää, sillä kaikki harjoitukset vaativat tarkkuutta ja ohjeiden noudattamatta jättäminen saattaa aiheuttaa ongelmatilanteita tehtäviä suorittaessa. Eettisesti toimiminen tarkoittaa opittujen taitojen käyttämistä vain hyviin tarkoituksiin sekä myös laitteiston turvalliseen käyttöön. (ComputerHope 2017.)

Opiskelijan on myös osoitettava kiinnostusta ja innokkuutta suorittamaan harjoituksia, sillä harjoitukset voivat vaikuttaa epämotivoituneen opiskelijan silmin työläiltä ja turhilta. Tämä näkökulma koskee kaikkia opiskelijoita kaikissa aiheissa, sillä hyvällä motivaatiolla ja kiinnostuksella opetuksesta saa paljon enemmän hyötyä. Harjoitusten tekeminen vaatii myös hieman sitoutumista, sillä opiskelijalta odotetaan innokkaan osallistumisen lisäksi myös raportointia tehdyistä töistä.

Kyky ja halukkuus noudattaa ohjeita on myös ehdottoman tärkeää, sillä suurin osa komennoista tulee syöttää terminaaliin juuri kuten ohjeistuksessa ne on esitetty. Opiskelijat ovat toki täysin vapaita tutkimaan eri komentoja omalla ajallaan, mutta tehtäviä tehdessä

tulee noudattaa annettuja ohjeita. Suurin syy tähän on se, että tehtävää ei välttämättä pysty suorittamaan kunnolla mikäli opiskelija on koettanut soveltaa ohjeita oman mielensä mukaan.

Etiikan perspektiivi korostuu etenkin harjoituksista opittujen tietojen ja taitojen soveltamisesta vain eettistä tarkastelua kestäviin toimiin. Eettistä hakkerointia ja tavallista hakkerointia erottavat vain tavoitteet, jota toiminnalla pyritään saavuttamaan. (ResearchPedia 2014.) Toinen eettinen seikka on etenkin koulun tarjoamien laitteiden käyttäminen vain niihin tarkoitettuihin tehtäviin. Tämä tarkoittaa jälleen ohjeiden noudattamista. Koulun laitteita ei myöskään saa käyttää omiin tarkoituksiin laboratorioympäristössä.

5 Suunnittelu

Inkrementaalisen kehittämismenetelmän mukaisesti edellisen syklin tulee olla tehtynä ennen seuraavaan vaiheeseen siirtymistä. Täten suunnittelua varten tarvitaan ensin vaatimusmäärittely, joka käytiin läpi edellisessä kappaleessa. Vaatimusmäärittelyn avulla on mahdollista luoda suunnitelma, jonka mukaan harjoitukset toteutetaan. (ISTQB 2017.)

Suunnitellessa harjoituksia keskityimme harjoitusten toteutustapaan, sopivan käyttöjärjestelmän valintaan, harjoitusten ympäristöön, pedagogiikkaan ja eettiseen näkökulmaan. Koimme näiden olevan tärkeimmät aihealueet harjoituksia suunnitellessa ja täten pyrimme luomaan mahdollisimman tarkan kartoituksen näistä aiheista.

5.1 Toteutustapa

Laboratoriot on mahdollista toteuttaa kahdella eri tavalla. Ensimmäinen toteutustapa on tulla koululle suorittamaan harjoituksia ohjatussa ympäristössä. Toinen vaihtoehto on suorittaa samat harjoitukset omalla tietokoneella, sillä virtuaalisen ympäristön avulla on mahdollista simuloida täysin identtinen ympäristö kuin koululla. Näiden kahden eri toteutustavan avulla on mahdollista tarjota jokaiselle opiskelijalle ajasta ja paikasta riippumaton tapa suorittaa harjoituksia. Toinen hyvä puoli tässä tavassa on myös se, että tietokonepaikkoja on rajattu määrä koululla ja kaikki opiskelijat eivät mahdu samaan aikaan samaan tilaan. Virtuaalinen ympäristö myös minimoi kaikki muutokset käytettäviin tietokoneisiin, sillä Kali Linux käyttöjärjestelmää ei asenneta kovalevylle lainkaan, vaan käytetään käyttöjärjestelmän ”live” tilaa.

Toteutustapa on kuitenkin sama, sillä harjoitusten yhteydessä on kirjoitettava raporttia joka muodostaa arviointipohjan opintojakson opettajille. Lisäksi ohjeistus katsotaan opintojakson työtilasta.

5.2 Käyttöjärjestelmän valinta

Harjoituksiin parhaiten soveltuvaa käyttöjärjestelmää valitessamme vertasimme Kali Linux sekä Windows käyttöjärjestelmiä benchmarking-tutkimusmenetelmän avulla. Vertailumme jälkeen huomasimme Kali Linux käyttöjärjestelmän olevan paljon monipuolisempi ja paremmin soveltuva käyttöjärjestelmä käytännön harjoitusten suorittamiseen. Asetimme benchmarking-tutkimukseemme viiden käytännön harjoituksen oleellisimmat ohjelmistot ja työkalut ja tarkastimme löytyvätkö nämä samat ominaisuudet valmiiksi asennettuina kummassakin käyttöjärjestelmässä. Alla olevasta taulukosta käy ilmi benchmarking vertailun tulokset.

Työkalu tai ohjelmisto	Kali Linux	Windows
Aktiiviseen ja passiiviseen tiedusteluun soveltuvat työkalut	Kyllä	Kyllä
Sisäänrakennetut verkkojen skannaus työkalut	Kyllä	Ei
Verkossa tapahtuvan liikenteen analysointi	Kyllä	Ei
Tunkeutumisen tunnistamiseen soveltuva ohjelmisto	Kyllä	Ei
Salasanojen salauksen purkamisohjelmisto	Kyllä	Ei

Taulukko 1: Windows ja Kali Linux käyttöjärjestelmien benchmarking tulokset

Windows käyttöjärjestelmän heikkoudet näkyivät eniten sisäänrakennettujen työkalujen ja nopeasti saatavilla olevien ohjelmistojen puutteessa.
Windows soveltuu paremmin harjoituksiin, joissa keskitytään esimerkiksi yrityksen verkon rakentamiseen ja sen suojaamiseen. Kali Linux käyttöjärjestelmän käyttötarkoitus korostuikin eniten juuri näiden sisäänrakennettujen työkalujen ja esiasennettujen ohjelmistojen saatavuudessa, sillä harjoituksia tehdessä opiskelijan ei pidä käyttää aikaa ohjelmistojen tai työkalujen asentamiseen.
Kali Linux valikoitui käyttöjärjestelmäksemme sisäänrakennettujen ominaisuuksien takia. Toinen hyvä ominaisuus on myös se, että käyttöjärjestelmä on ilmainen eikä siitä synny koululle ylimääräisiä kustannuksia. Näiden kahden seikan vuoksi päätimme sivuuttaa Windows käyttöjärjestelmän käytännön harjoituksia varten.

Linux on avoimen lähdekoodin käyttöjärjestelmä, josta on tarjolla useita eri jakeluversioita eli distribuutioita. Näistä versioista suurin osa on ilmaisia ja vapaasti muokattavissa. Linux

käyttöjärjestelmän jakeluversioille on myös tarjolla laaja valikoima useita erilaisia työkaluja ja ohjelmistoja. (Linux.fi 2017.) Myös Android –mobiilikäyttöjärjestelmien ytimet pohjautuvat Linux käyttöjärjestelmään. (Hoffman 2014.)

Tällä hetkellä eniten penetraatiotestaukseen käytettävä käyttöjärjestelmä on Debianiin perustuva Kali Linux. Kali Linux on avoimen lähdekoodin käyttöjärjestelmä, jota ylläpitää Offensive Security-niminen tietoturvayritys. Offensive Security toimii myös ylläpitäjänä suositussa Exploit Databasessa, josta hakkerit pystyvät hakemaan erilaisia tunnettuja heikkouksia kohteisiinsa. Kali Linux tunnetaan erityisesti laajasta tietoturva- ja penetraatiotestauksessa käytettävien työkalujen tarjonnastaan. Näihin työkaluihin sisältyy esimerkiksi verkkojen skannaustyökaluja. Kali Linux käyttöjärjestelmään on myös mahdollista asentaa ohjelmistoja, joita ei ole valmiiksi sisällytetty jakelupakettiin. (Kali Linux 2017.)

Koimme, että käytännön harjoitusten osalta on käytännöllisintä kaikkien ohjelmistojen valmiiksi asentaminen tietokoneille ja niiden olevan valmiina käytännön harjoituksia varten. Tähän tarkoitukseen Kali Linux soveltuu täydellisesti. Toisin kuin Windows käyttöjärjestelmässä, Kali Linux käyttöjärjestelmässä on jo kaikki työkalut valmiina ja sen käyttäminen labrotatoriokäyttöjärjestelmänä olisi mielestämme optimaalisinta. Linux käyttöjärjestelmissä on myös erittäin hyvänä ominaisuutena niiden keveys verrattuna Windows käyttöjärjestelmään, jolloin laboratorion koneilta ei vaadita yhtä paljon laitevaatimuksia, kuin Windows koneilta. Suurena etuna Kali Linux käyttöjärjestelmässä on myös mahdollisuus suorittaa se live-tilassa, jolloin käyttöjärjestelmää ei asenneta laitteen kovalevylle.

5.3 Pedagogiikka

Laboratorioharjoituksia suunnitellessa halusimme myös kiinnittää huomiota opiskelijan oppimisprosessiin, jotta harjoituksia ei tehdä pelkästään suorittamisen takia lisäpisteiden toivossa. Pyrimme parantamaan oppimiskokemusta luomalla erillisen raportin, johon opiskelijat kirjaavat tulosten lisäksi myös omin sanoin selitettyjä toimintoja. Muita keinoja parantaa oppimiskokemusta ovat myös opiskelijan ohjaus ohjaajan toimesta sekä harjoitusten ohjeistuksiin perehtyminen.

Raportin tärkeimmät kohdat ovat erityisesti tehtävät, jossa opiskelijan tulee kyetä selittämään omin sanoin suoritetun komennon tarkoitus. Verkkojen skannaus-harjoituksessa opiskelijan tulee selittää omin sanoin kuinka host-komento löytää verkkosivun www-osoitteen perusteella IP-osoitteen. Tämä estää opiskelijan vain suorittamasta tehtävän ja siirtymällä seuraavaan, sillä hänen tulee etsiä tietoa host-komennosta ja samalla hän myös oppii ymmärtämään mitä komennon takana tapahtuu.

Käytännön harjoituksia tehdessä kouluympäristössä opiskelijoiden oppimista tukee harjoitusten ohjaaja. Hänen tehtävänään on varmistaa laboratorioiden tekninen sujuminen sekä opiskelijoiden neuvominen tehtävien suorittamisessa. Ohjaajan rooli korostuu etenkin niiden oppilaiden auttamisessa, joilla ei ole aikaisempaa kokemusta Linux käyttöjärjestelmästä. Monilla oppilailla ei ole välttämättä käsitystä siitä, että suuri osa harjoituksissa käytettävistä työkaluista suoritetaan terminaalista ja täten niillä ei ole graafista käyttöliittymää. Mikäli opiskelija on käyttänyt pääsääntöisesti Windows käyttöjärjestelmää, tämä voi aiheuttaa aluksi hämmennystä. Ohjaajan on tällöin tärkeää osata neuvoa ja selittää terminaalin eri toimintoja sekä tarkoituksia, jotta opiskelijat eivät menetä motivaatiotaan tehdessään tehtäviä.

Ohjeistus tukee myös pedagogisesti opiskelijan oppimista, sillä ohjeistuksen myötä jokainen opiskelija pystyy suorittamaan harjoitukset onnistuneesti. Ohjeita tehdessämme keskityimme ensisijaisesti ohjeiden yksinkertaisuuteen, sillä tahdoimme luoda harjoituksista mahdollisimman lähestyttäviä. Tarkoituksena oli myös sisällyttää Linux käyttöjärjestelmän perustoimintoja tehtävien ohelle, jotta opiskelijat saavat perustason käyttökokemusta myös itse käyttöjärjestelmästä.

5.4 Eettinen näkökulma

Harjoituskokonaisuuksia suunnitellessamme tahdoimme myös huomioida eettisen hakkeroinnin perusteet, sillä Network Security-opintojakson keskeisenä pääteemana on eettinen hakkerointi. Hakkeroinnissa on tyypillisesti kolme eri käyttäjäryhmää, jotka jakautuvat valkohattuihin, harmaahattuihin ja mustahattuihin. (Hoffman 2013.)

Valkohatut ovat eettisiä hakkereita, jotka kartoittavat kohteen haavoittuvuuksia ja raportoivat niistä suoraan yritykselle sekä myös antavat parannusehdotuksia näiden haavoittuvuuksien korjaamiseen. (Technopedia 2017.) Laatimamme harjoitukset pohjautuvat valkohattuhakkerointiin, sillä ne ovat käyttötarkoitukseltaan suunniteltu simuloimaan eettisen hakkerin yksinkertaisimpia työtehtäviä.

Harmaahatut ovat hakkereita, jotka toimivat jokseenkin kyseenalaisesti. Harmaahatut eivät pyri aiheuttamaan vahinkoa tai harmia kohteelleen, mutta he saattavat julkistaa käyttämiään haavoittuvuuksia, jolloin mustahattuhakkerit saattavat käyttää näitä haavoittuvuuksia omiin pahaluontoisiin käyttötarkoituksiin. Harmaahattuhakkereita voidaan kuvailla aktivisteina, jotka tuovat haavoittuvuuksia julki oman aatteensa takia. (Technopedia 2017.)

Mustahatut ovat hakkereita, jotka etsivät aktiivisesti haavoittuvuuksia yritysten verkoista ja pyrkivät hyötymään näistä tyypillisesti rahallisessa muodossa. Mustahattuja voidaankin kutsua

valkohattujen vastakohdaksi, sillä eettisten hakkereiden tehtävänä on estää hakkereiden pääsy yrityksen verkkoon. (Technopedia 2017.)

Hakkeroinnin määritelmät ovat selkeitä ja eri hakkerityypit ovat hyvin eroteltavissa. Kuitenkin kaikki nämä kolme hakkerityyppiä käyttävät lähes samoja ohjelmistoja ja työkaluja omiin käyttötarkoituksiinsa. Tämän takia on tärkeää käsitellä yleisimmät hakkerityypit ja heidän päämääränsä, jotta opiskelijat ymmärtävät miksi näitä harjoituksia tehdään ja mihin käyttötarkoituksiin ne valmistavat opiskelijan. Myös opiskelijoiden raportti kuvastaa valkohattuhakkerointia, sillä eettisesti toimivat hakkerit dokumentoivat työvaiheitaan ja käyttämiään työkaluja luodakseen toiminnastaan mahdollisimman läpinäkyvää ja luotettavaa. (Johansen 2015.)

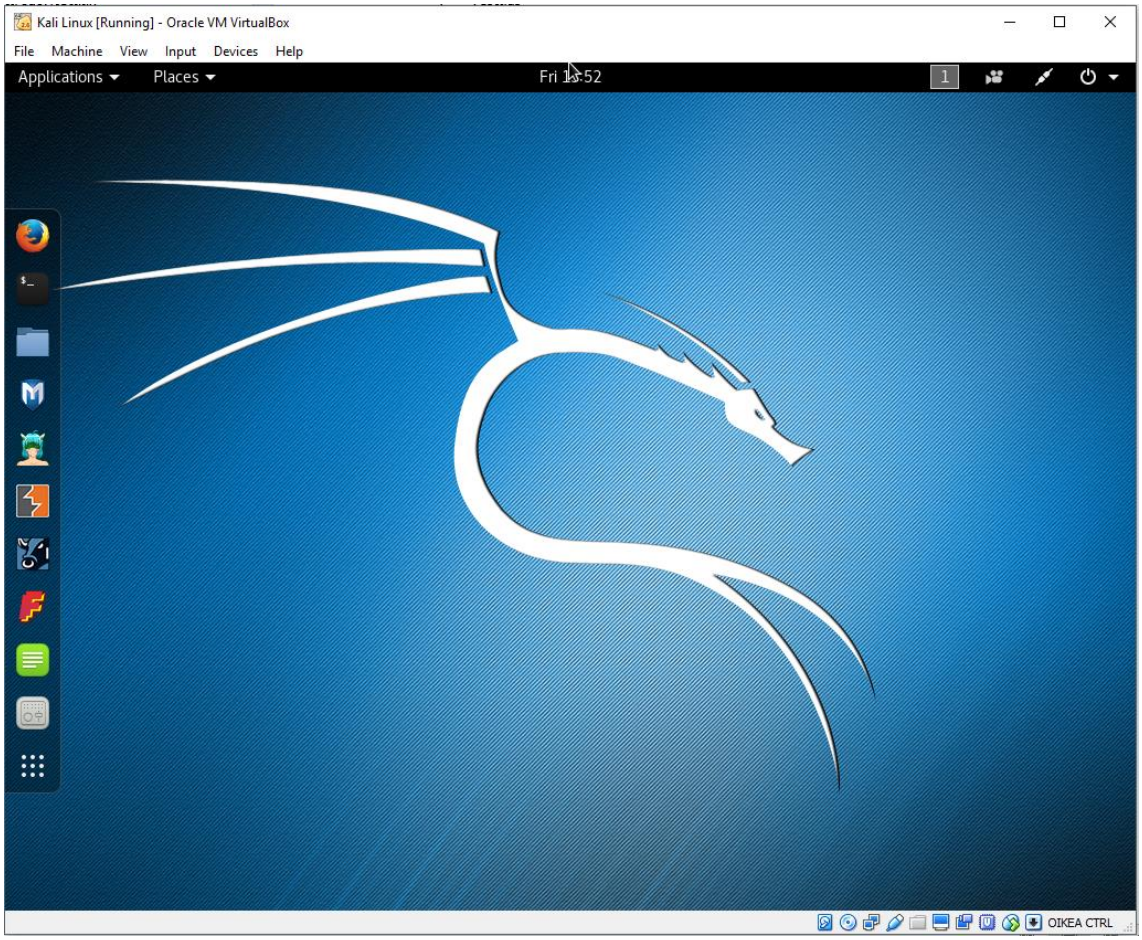
6 Toteutus

Inkrementaalisen kehittämismenetelmän mukaisesti toteutussykli vaatii ensin vaatimusmäärittelyn mukaisen suunnitelman, jotta toteutusvaihe sujuu ongelmitta. Toteutusvaiheessa keskitymme kuvaamaan luomisprosessia, jonka kävimme läpi käytännön harjoituksia luodessa. Harjoitusten luomisprosessissa hyödynnettiin myös inkrementaalista kehittämismenetelmää, jolloin harjoitusten rakenne syntyi tietyssä järjestyksessä. (ISTQB 2017.)

6.1 Oppimisympäristö

Käytännön harjoitusten ympäristönä toimii Linux käyttöjärjestelmän Kali distribuutio, jota suoritetaan virtuaaliympäristössä Oraclen VirtualBox sovelluksen avulla. Kali Linux käyttöjärjestelmää ei VirtualBox sovelluksen takia tarvitse asentaa lainkaan isäntäkoneen varsinaiselle kovalevylle, vaan asennusprosessin aikana luodaan virtuaalinen kovalevy joka toimii virtuaalikäyttöjärjestelmän kovalevynä. Virtuaalinen kovalevy on hyvin samantapainen kuin normaali fyysinen kovalevy, ainoana erona on juurikin laitteiston simuloiminen virtuaaliympäristössä. (Technopedia 2017.)

Kali Linux suoritetaan myös live-tilassa, jolloin käyttöjärjestelmä asennetaan suoraan virtuaalikovalevylle ilman erillisiä määrityksiä asennuksen aikana. Live-tila myös tarkoittaa sitä, että käyttöjärjestelmän joutuu asentamaan aina uudelleen kun harjoituksia suoritetaan. Tämän asennuksen aikana virtuaalinen käyttöjärjestelmä asettaa oletusasetukset käyttöjärjestelmälle ja käyttäjä joutuu vain odottamaan nopean asennusprosessin valmistumista. Live-tilan suurin hyöty on sen turvallisuudessa, sillä isäntätietokone ei koe mitään muutoksia. Tämä on erityisen hyödyllistä etenkin koulun ympäristössä, sillä koulun omat laitteet pysyvät turvassa haitallisilta muutoksilta. (Kali Linux Official Documentation 2017.)

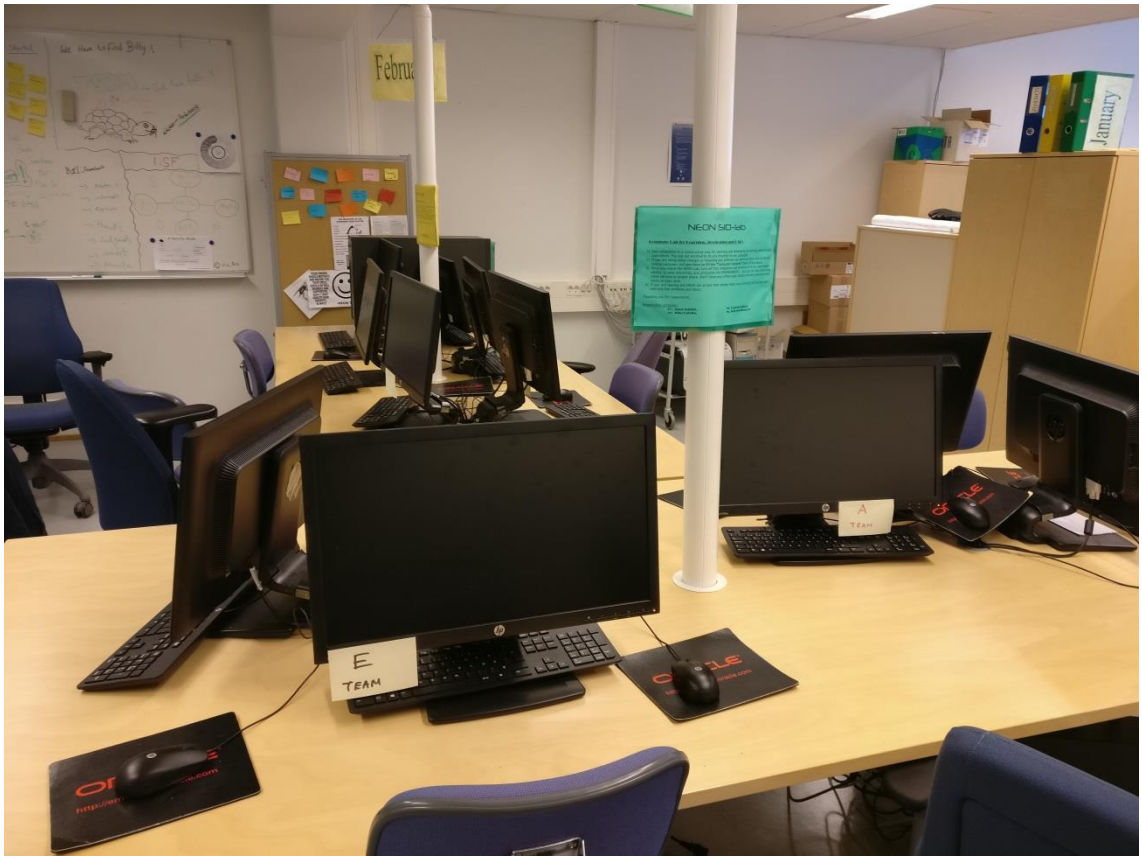


Kuvio 3: Kali Linux virtuaaliympäristössä.

Virtuaaliympäristön käyttäminen ei myöskään eroa normaalin käyttöjärjestelmän käytöstä mitenkään, vaan kaikki ominaisuudet ovat yhtälailla saatavilla kuin fyysisessäkin käyttöjärjestelmässä. (Rouse 2016.) Live-tilan vuoksi käyttöjärjestelmän näppäimistön syöttötavan joutuu asettamaan suomeksi joka kerran, kun virtuaaliympäristö käynnistetään uudelleen. Tämä on myös mahdollista korjata luomalla näköislevykuva, jossa käyttöjärjestelmän syöttökieleksi on asetettu suomi.

Virtuaalisen ympäristön lisäksi on myös olemassa fyysinen ympäristö, jossa opiskelijat pystyvät suorittamaan käytännön harjoituksia. Ensimmäinen ympäristö sijaitsee Laurea-ammattikorkeakoulun Leppävaaran kampuksen tiloissa, josta löytyy noin kymmenen tietokonetta laboratorioharjoituksia varten. Ympäristön soveltuvuus harjoitusten tekoon on erittäin käytännöllinen, sillä nämä tietokoneet eivät ole yhteydessä Otaverkkoon kuten muut korkeakoululla olevat tietokoneet. Tämän vuoksi harjoitukset eivät aiheuta rasitusta tai muita ongelmia koulun omalle verkolle. Laboratorioympäristön tietokoneet eivät myöskään ole keskitetysti hallinnoituja, joten tietokoneille on mahdollista asentaa omia ohjelmia. Näiden seikkojen avulla laboratorioympäristö oli mahdollista rakentaa toimimaan

vaatimusmäärittelyn mukaisesti. Tulevaisuudessa on myös mahdollista laajentaa koulun fyysistä ympäristöä, sillä Leppävaaran kampuksella on toinenkin opetustila, josta löytyy noin kolmekymmentä samankaltaista tietokonetta jotka soveltuvat harjoitusten tekemiseen.



Kuvio 4: Leppävaaran kampuksen laboratorioympäristö

Toinen ympäristö on opiskelijan itse luoma harjoitusympäristö, johon hän lataa ja asentaa tarvittavat ohjelmistot hyödyntäen luomaamme ohjeistusta. Ohjeistuksen avulla opiskelija saa käyttöönsä identtisen oppimisympäristön, joka vastaa koulun oppimisympäristöä. Opiskelijan oman ympäristön tarkoitus on tarjota mahdollisuus niille opiskelijoille, jotka eivät välttämättä pääse tulemaan koululle suorittamaan harjoituksia. Koulun ympäristössä on myös rajattu määrä tietokoneita, joten kaikki opiskelijat eivät välttämättä edes mahdu samanaikaisesti suorittamaan harjoituksia.

Näiden kahden ympäristön avulla jokainen Network Security-opintojaksolle osallistuva opiskelija pystyy suorittamaan käytännön laboratorioharjoitukset joko koulussa tai kotona. Koulun ympäristössä opiskelijalle tarjotaan ohjausta ja neuvontaa opetustilanteessa, kun taas kotiympäristössä opiskelijalla on vapaus tehdä harjoituksia oman aikataulun mukaisesti.

6.2 Harjoitukset

Inkrementaalisen mallin mukaisesti harjoituksia varten on luotava ensin laboratorioympäristö, joka käsiteltiin edellisessä kappaleessa. (ISTQB 2017.) Harjoituksien tekeminen perustui Hands-on Information Security Lab Manual teokseen, (Whitman, Mattord & Green, 2014) johon luomamme harjoitukset perustuvat. Harjoitukset valikoitiin käymällä läpi Network Security-opintojakson eri moduulit ja näiden tietojen perusteella valitsimme soveltuvat tehtävät kirjasta. Network Security opintojaksolla on kahdeksan eri moduulia ja saimme sovellettua viittä moduulia vastaamaan kirjan harjoituksia. Alla olevasta listasta käy ilmi valikoidut harjoitukset ja niiden sijainti liitteissä.

- Tietojen kerääminen kohteesta (liite 2)
- Verkon haavoittuvuuksien kartoittaminen (liite 3)
- Salausten purkaminen (liite 4)
- Verkkoliikenteen analysointi (liite 5)
- Tunkeutumisen tunnistamisjärjestelmät (liite 6)

Harjoituksia tehdessämme pyrimme luomaan harjoitukset ensin noudattaen Hands-On Information Security Lab Manualin esimerkkitehtäviä. Ongelmia kohdatessamme pyrimme soveltamaan omaa osaamistamme, jotta lopullinen harjoitus muistuttaa mahdollisimman paljon kirjan esimerkkiharjoituksia. Suurimmat ongelmatilanteet syntyivät vanhentuneista ohjelmistoista sekä käyttöjärjestelmän omista puutteista. Kirjassa kuvatut harjoitukset ovat vuodelta 2014 ja niissä on käytetty Linux käyttöjärjestelmän Fedora distribuutiota, joka on eri distribuutio kuin harjoituksissa käytetty distribuutio. Jokainen harjoitus käytiin tarkasti läpi ja ongelmatilanteiden ilmetessä kirjasimme ylös ratkaisut ohjeistuksia varten. Kun olimme saaneet kaikki harjoitukset tehtyä ja muokattua soveltumaan omiin käyttötarkoituksiimme, ryhdyimme dokumentoimaan harjoituksia. Halusimme myös sisällyttää harjoituksiin pohtimistehtäviä, jolloin opiskelijan tulee kuvata omin sanoin tiettyjen toimintojen toimintaperiaate. Tällöin oppimisprosessi syvenee ja opiskelija saa suuremman ymmärryksen eri työkaluista ja ohjelmistoista, joita hän käyttää harjoitusten aikana.

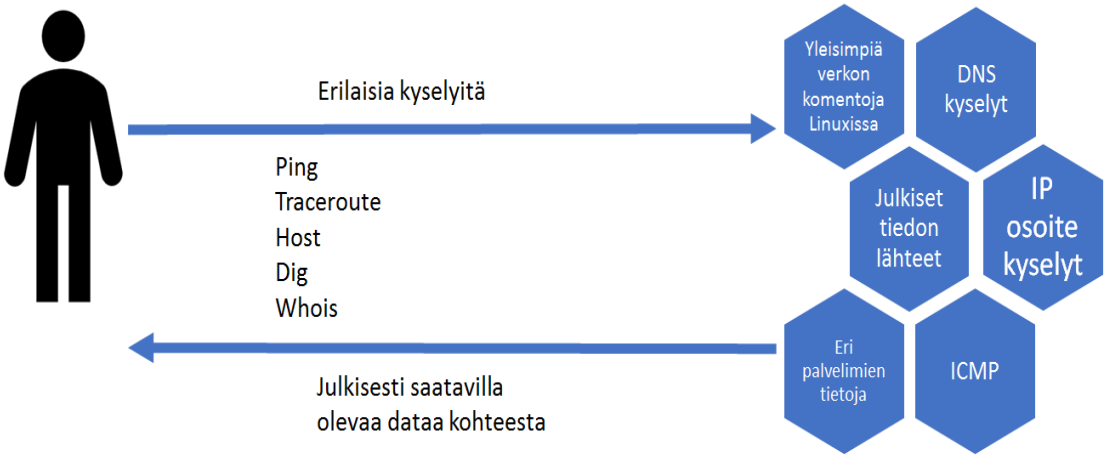
Tässä kappaleessa käymme läpi tarkemmin jokaisen harjoituksen, käsitteet sekä harjoituksissa käytettävät työkalut. Kappaleisiin sisältyy myös yleistä tietoa Network Security-opintojakson moduulien sisällöistä, joita voi käyttää tietoperustana uusien harjoitusten luomiseen tulevaisuudessa. Moduulien teoriasisältö on tiivistetty siten, että uusien harjoitusten suunnittelun ideointi on mahdollisimman helppoa. Kappaleet rakentuvat pohjustamalla lukijalle ensin tietoperusta aiheesta ja lopuksi esitämme harjoituksemme päämäärän.

Harjoitusten päämääränä on pyrkiä simuloimaan penetraatiotestauksen viittä eri vaihetta, joihin kuuluvat tiedustelu, skannaaminen, järjestelmään pääsy, järjestelmässä pysyminen sekä jälkien peittäminen. Kehittämiemme harjoitusten tarkoituksena onkin tutustuttaa opiskelijat käyttämään yleisimpiä kyberturvallisuuteen liittyviä työkaluja sekä ohjelmistoja. Harjoitusten avulla opiskelijat sisäistävät penetraatiotestauksen viisi eri vaihetta sekä oppivat ymmärtämään, miksi nämä työvaiheet toteutetaan juuri tässä järjestyksessä.

6.2.1 Tiedon kerääminen kohteesta

Penetraatiotestauksen ensimmäinen vaihe on tiedon kerääminen kohteesta, jonka aikana penetraatiotestausta suorittava henkilö pyrkii keräämään mahdollisimman paljon hyödyllistä tietoa kohteesta käyttäen hyväkseen esimerkiksi hakukoneita tai sosiaalista mediaa. Tiedon kerääminen on tavallisesti penetraatiotestauksen pisin vaihe, sillä kerätyillä tiedoilla pohjustetaan kohteeseen suunniteltavaa hyökkäystä. (Olzak 2008.)

Alla olevasta kuviosta käy ilmi, mitä opiskelijan tulee tehdä saadakseen kerättyä tietoa kohteesta. Opiskelija aloittaa tiedon keräämisen suorittamalla erilaisia kyselyitä käyttäen eri työkaluja ja näiden avulla hän saa tuloksena esimerkiksi verkon IP-osoitteita sekä tietoja palvelimesta.



Kuvio 5: Tiedonkeruuprosessi käyttäen eri työkaluja käytännön harjoituksessa

Aloitettaessa kohdeorganisaatioon tunkeutumista, ensimmäisenä vaiheena on tiedon kerääminen kohteesta. Ensimmäinen osa tätä tiedon keräämistä on footprinting, jossa hyökkääjä pyrkii tunnistamaan organisaation verkon, toisin sanoen jalanjäljen. Tähän jalanjälkeen kuuluu muun muassa organisaation verkkoja, verkko-osoitteita sekä henkilöitä, jotka käyttävät kyseisiä laitteita. Tiedon keräämiseen käytetään monia työkaluja ja tietolähteitä, kuten hakukoneita ja sosiaalista mediaa. Tiedon keräämisessä voidaan käyttää

hyväksi myös käyttäjän manipulointia (engl. social engineering), jossa henkilö esimerkiksi tekeytyy toiseksi kohdeorganisaation työntekijäksi ja pyrkii saamaan tietoja toiselta työntekijältä. Työntekijää voidaan yrittää myös kiristää luovuttamaan tietoja tai viemään muistitikun työpaikan koneeseen, jolloin hyökkääjä pystyy saastuttamaan kohteen verkon. (Whitman, Mattord & Green 2014, 16.)

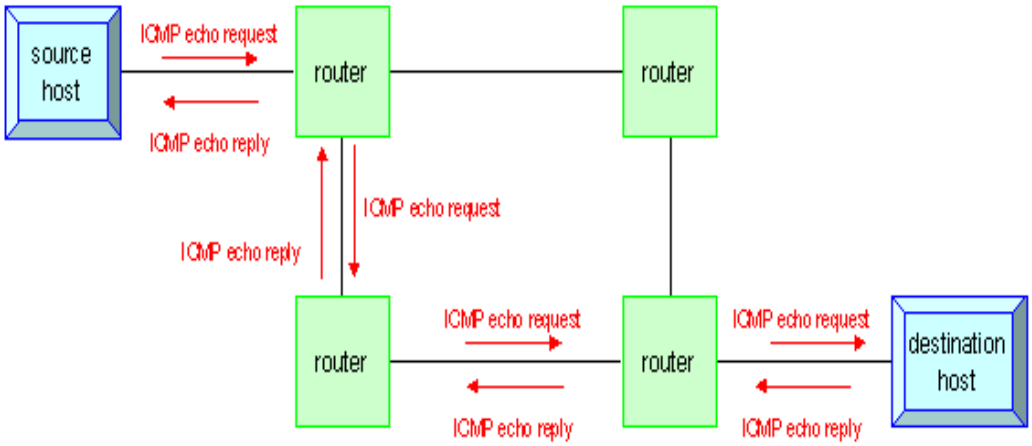
Toisena vaiheena on tiedustelu (engl. reconnaissance), jossa kohdeorganisaatiosta pyritään keräämään tietoja joko verkkoselaimen tai verkkotiedustelutyökalujen avulla. Verkkoselaimella suoritetusta tiedustelusta käytetään nimeä passiivinen tiedustelu (engl. passive reconnaissance), joka tarkoittaa huomaamatonta tietojen keräämistä. Verkkotiedustelutyökaluilla tehty tiedustelu on aktiivista tiedustelua (engl. active reconnaissance), jolla tarkoitetaan vaihetta jossa kohdejärjestelmää skannataan erilaisilla toimintatavoilla. (TutorialsPoint 2017.)

Web-tiedustelussa tietoa kerätään verkkoselainten avulla. Web-tiedustelussa käytetään hyväksi verkkosivujen lähdekoodia, jota voi lukea minkä tahansa verkkoselaimen avulla. Tähän on myös käytössä työkaluja kuten Blighty Designin Sam Spade, jolla lähdekoodin selaamista saa tehostettua. On myös mahdollista, että hyökkääjä lataa verkkosivun lähdekoodin ja tekee siitä muunnellun kopion mahdollista hyökkäystä varten. Lähdekoodista on mahdollista saada usein paljon erilaisia hyödyllisiä tietoja, kuten nimiä, osoitteita tai eri palvelimien nimiä. Lähdekoodista on myös mahdollista löytää tärkeitä tietoja kuten ylläpitäjän nimi, joita pystytään myöhemmin käyttämään käyttäjän manipulointiyrityksissä. Web-tiedustelua pidetään yhtenä yksinkertaisempana ja tehokkaimpana keinona kerätä tietoa, sillä se ei vaadi välttämättä erityisiä työkaluja selaimen lisäksi ja web-tiedustelusta saatu tieto voi olla erittäin hyödyllistä hyökkäykselle. (Whitman, Mattord & Green 2014, 16.)

Verkkotiedustelusta puhuttaessa tarkoitetaan laajaa kirjoa tekniikoita ja tapoja, joilla kohdeorganisaation verkon kokoa ja laajuutta voidaan kartoittaa internet työkalujen avulla. Yleisimmin tähän tarkoitukseen käytetään Ping- ja Traceroute- työkaluja. Nämä työkalut ovat saatavissa niin Linux- kuin Windows käyttöjärjestelmissä jo valmiiksi asennettuina. Näitä työkaluja käytetään Windows käyttöjärjestelmän komentokehotteesta ja Linux käyttöjärjestelmän terminaalista. (Whitman, Mattord & Green 2014, 19.)

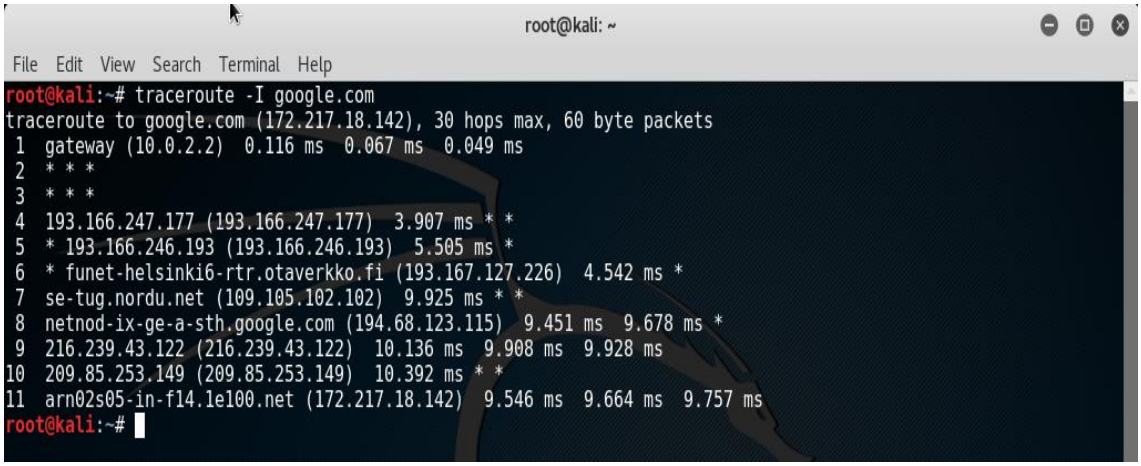
Ping-työkalu paketoi TCP/IP paketin, jonka se lähettää ennalta määritettyyn osoitteeseen. Ping-työkalua käytetään selvittämään vastaako kyseinen laite Internetissä kutsuihin. Selvitys tapahtuu lähettämällä ICMP pyyntöjä ja odottamalla vastauksia. Ping-työkalu toimii kolmannessa tasossa OSI-verkkomallissa ja on hyödyllinen juurikin laitteen yhteyksien toiminnan selvittämisessä. Ping-työkalu toimii yleensä internetin ylikin ja kertoo myös kuinka

pitkään pakettien toimittamisessa ja vastaanottamisessa kesti. (Whitman, Mattord, Green, 2014, 19.)



Kuvio 6: Ping-työkalun toimintakaava (St. Michael College 2017.)

Traceroute-työkalu on toinen yleinen menetelmä, jolla käyttäjä saa tarkkaa tietoa siitä, mitä kautta lähetetty paketti kulkee kohdeosoitteeseen. Traceroute-työkalun avulla lähettäjä saa selville paketin kuljetun matkan sekä kaikki osoitteet, joiden kautta paketti kulki osoitteeseen. Traceroute-työkalun avulla myös verkon rakenteen ymmärtäminen helpottuu huomattavasti. Traceroute-työkalu toimii lähettämällä paketin kohteeseen, jonka TTL (Time to live) eli elinaika on 1. Kun paketti saapuu ensimmäiseen kohteeseen, joka voi esimerkiksi olla reititin, palauttaa kohdelaite paketin takaisin, sillä sen elinaika on jo loppunut. Tämän jälkeen lähetetään paketti jonka elinaika on 2, jolloin seuraava osoite edellisen jälkeen vastaa samalla tavalla kuin ensimmäinenkin. Pakettien lähettäminen jatkuu niin kauan, kunnes viimeinen kohde on saavutettu. Kun paketti palaa takaisin lähettäjälle, Traceroute-työkalu saa siltä ICMP-virheviestin. Näiden virheviestien avulla Traceroute-työkalun on mahdollista laskea ja jäljittää reitti lähettäjän ja vastaanottajan välillä. (Whitman, Mattord & Green 2014, 20.)



Kuvio 7: Traceroute-työkalu toiminnassa harjoituksessa.

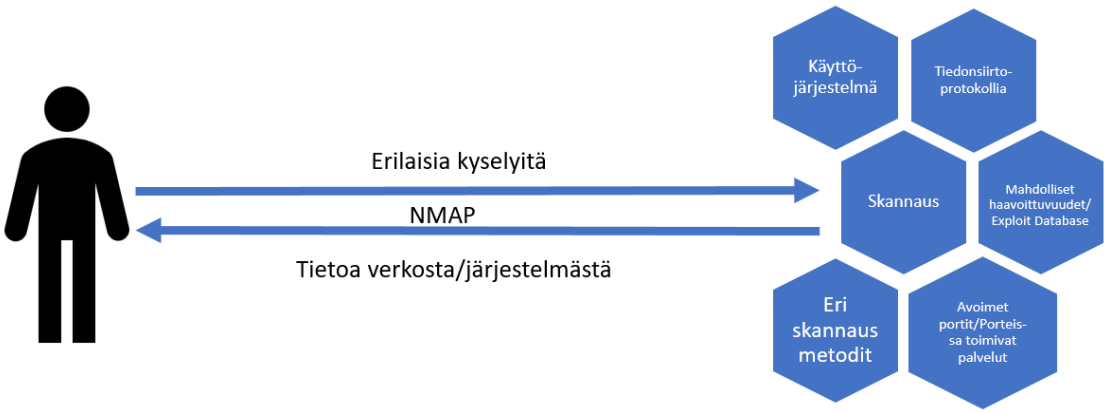
Tietojen kerääminen kohteesta kappaleen harjoituksessa sovelletaan kaikkia yllämainittuja tekniikoita ja toimintoja tietojen keräämistä varten. Näiden tekniikoiden ja työkalujen avulla opiskelija pystyy selvittämään kohteestaan paljon tärkeää tietoa, jotka voivat auttaa häntä esimerkiksi penetraatiotestausta tehdessään. Koska tiedot löytyvät julkisesti, ne eivät aseta kohdeyritystä vaaraan.

Harjoituksen päämääränä on kerätä tietoa kohteesta käyttäen julkisesti saatavilla olevia lähteitä. Opiskelija pyrkii ohjeistuksen avulla selvittämään esimerkiksi nimi- ja osoitetietoja, IP-osoitteita sekä hyödyntämään Ping- ja Traceroute-työkaluja selvittääkseen kuinka kaukana fyysisesti kohdeyritys sijaitsee ja mitä reittiä hänen tiedustelunsa kulkevat. Opiskelijan saadessa tämän moduulin harjoituksen tehtyä, hän on päässyt käsittelemään käytännön harjoitusten avulla yleisimpiä tiedonkeruu työkaluja ja menetelmiä. Näiden avulla opiskelija oppii myös ymmärtämään Linux käyttöjärjestelmän terminaalin käyttämistä sekä hän myös näkee kuinka tietoja on helppo kerätä yksinkertaisilla komennoilla.

6.2.2 Verkkojen haavoittuvuuksien kartoitus

Penetraatiotestauksen toisena vaiheena on kohteen haavoittuvuuksien kartoittaminen, jonka aikana testausta suorittava henkilö skannaa kohteen verkkoa löytääkseen haavoittuvuuksia. Skannausvaiheessa hyökkääjä pyrkii selvittämään esimerkiksi kohteen avoimet portit ja kuinka hän pystyy hyödyntämään verkossa olevia resursseja hyökkäystä suunnitellessa. (Corey 2015.)

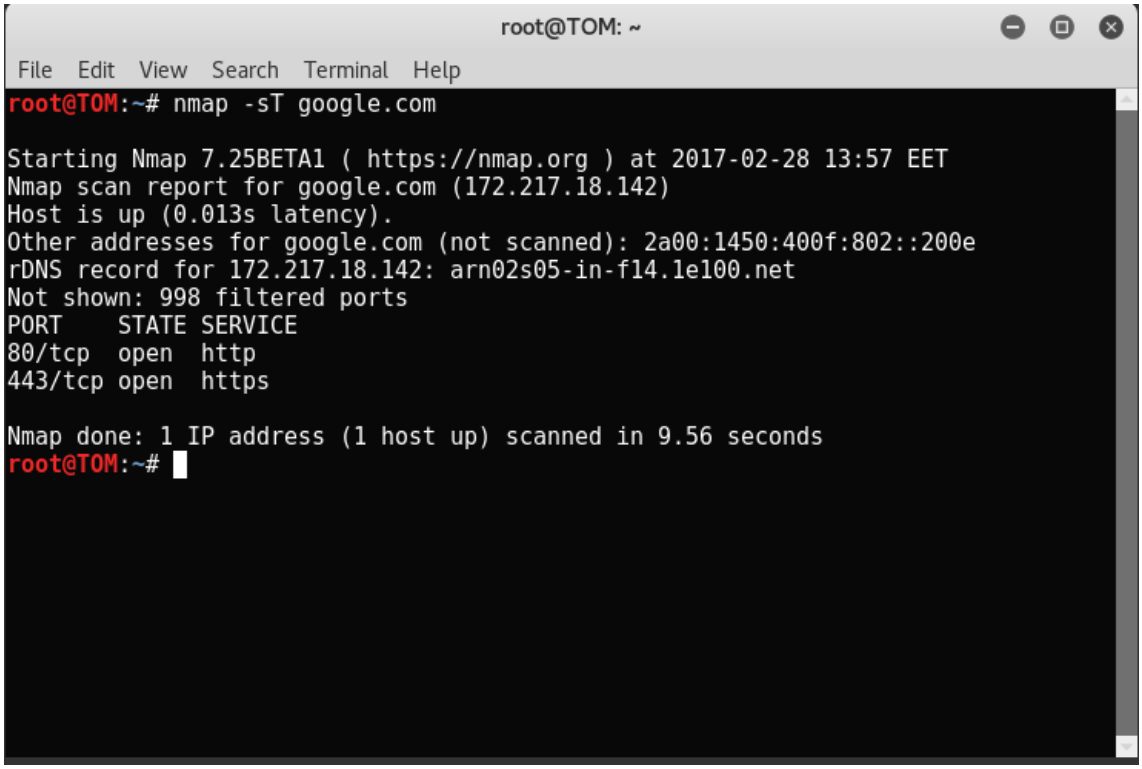
Alla olevassa kuviossa on kuvattu, kuinka opiskelija kartoittaa verkkojen haavoittuvuuksia käytännön harjoituksessa. Opiskelija tekee useita erilaisia kyselyitä käyttäen Nmap-ohjelmistoa ja lopputuloksena opiskelija saa tietoa esimerkiksi avoimista porteista sekä mahdollisesti kohteen käyttöjärjestelmästä.



Kuvio 8: Haavoittuvuuksien kartoittamisen prosessi harjoituksessa käyttäen Nmap –ohjelmistoa

Kun edellisessä vaiheessa on kerättyä tietoa kohdeorganisaatiosta, siirrytään keräämään tietoa kohteen verkosta. Tätä vaihetta kutsutaan nimellä verkkojen skannaaminen ja listaaminen (engl. network scanning & enumeration). Skannausvaiheessa kohdeorganisaation laitteista ja verkosta pyritään selvittämään mahdollisimman paljon tietoja, joiden avulla kohteeseen hyökkääminen helpottuu. Näitä tietoja kerätään seuraamalla verkon liikennettä tai lähettämällä omia paketteja ja seuraamalle niiden tuomia tuloksia. Kun kohdelaite tai kohdeverkko on skannattu ja sen ylläpitäjä tunnistettu, seuraa listaamisvaihe. Listaamisessa pyritään selvittämään, mitä mahdollisia resursseja on mahdollista hyväksikäyttää hyökkäyksessä. Näiden tekniikoiden käyttäminen yhdessä on erittäin tehokasta verkkoihin tunkeutuessa. Aluksi verkko skannataan ja selvitetään onko kohdelaitteita tms. verkossa. Tämän jälkeen mahdolliset kohdelaitteet luetteloidaan ja selvitetään mitä resursseja on saatavilla. (Whitman, Mattord & Green, 2014, 20-21.)

Skannausvaiheeseen käytettäviä työkaluja on tarjolla lukuisia eri vaihtoehtoja. Näillä työkaluilla tehtävät skannaukset saattavat antaa erittäin tarkkoja tietoja kuten käyttöjärjestelmän, avoinna olevat portit sekä palvelut tai yleisesti listata verkossa aktiivisena olevia laitteita. Skannaus saattaa myös kertoa mitä laitteet tekevät organisaatiossa ja minkälaisia rooleja niillä saattaa olla. On tärkeää myös ymmärtää minkälaisessa verkkoympäristössä skannausta tehdään, jotta pystytään käyttämään tilanteeseen parhaiten soveltuvia työkaluja. Esimerkiksi mikäli tarkoituksena on kerätä tietoa tietyistä porteista kuten UDP-protokollasta (User Datagram Protocol), voi siihen olla käytössä tehokkaampi ohjelma, joka on suunniteltu juuri UDP-porttien skannaamiseen. Työkalupakissa tulee olla myös ohjelmistoja, joilla laajempi ja yleistasoisempi skannaus onnistuu. Monissa ohjelmissa, kuten Nmap-ohjelmistossa, nämä kummatkin vaihtoehdot ovat saatavilla. (Whitman, Mattord & Green, 2014, 20.)



Kuvio 9: Nmap-ohjelmistolla skannatut avoimet portit

Listaaminen on prosessi, jossa verkossa olevia resursseja tunnistetaan. Näitä resursseja käytetään verkon sisälle pääsemiseen. Yleisesti ottaen jokaiseen käytössä olevaan resurssiin päästään käsiksi tietyn portin kautta, jota kyseinen protokolla käyttää. (TechnoPedia 2017.) Listaustyökalujen avulla käydään läpi mahdollisten avointen porttien alueet ja yritetään löytää mahdollisimman paljon tietoa resurssista, jota kyseinen avoin portti tarjoaa. Näiden työkalujen käyttö on myös hyödyllistä verkkojen ylläpitäjille, sillä niiden avulla voi joustavasti seurata, mitä resursseja verkossa on käytössä. Osa näistä resursseista on tarpeellisia organisaation toiminnoille, mutta joukossa saattaa myös olla resursseja, jotka ovat jääneet verkkoon ylläpidon tietämättä ja aiheuttavat näin tietoturvauhan. Näin saattaa käydä esimerkiksi tiettyjen käyttöjärjestelmien kanssa, sekä mahdollisesti taitamattomien työntekijöiden johdosta. (Whitman, Mattord & Green, 2014. 20)

Verkkojen skannaaminen & listaaminen moduulin harjoituksissa opiskelija oppii hyödyntämään yllämainittuja prosesseja kartoittaakseen kohdeverkosta löytyviä resursseja. Näiden opittujen taitojen avulla opiskelija pystyy esimerkiksi näkemään omassa kotiverkossaan olevat laitteet. Skannausta tehdessään opiskelija myös näkee omasta verkostaan avoinna olevat portit ja pystyy tämän tiedon avulla sulkemaan ne, parantaen verkkonsa tietoturvaa.

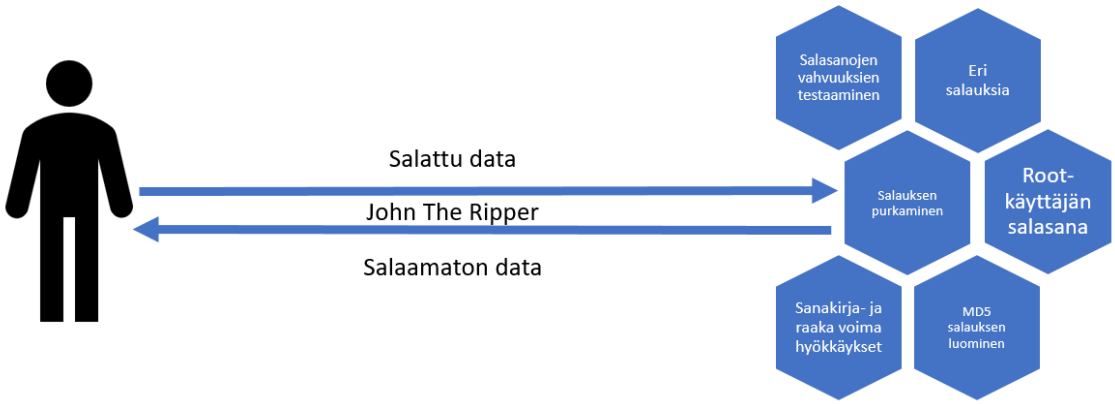
Harjoituksessa opiskelija käyttää Nmapin terminaaliversiota, jolloin hänen tietotaitonsa Linux käyttöjärjestelmästä ja terminaalin käytöstä kasvaa jälleen. Nmap-ohjelmasta on myös

tarjolla käyttöliittymä versio nimeltä Zenmap. Valitsimme terminaaliversion Nmap-ohjelmistosta harjoitusta varten, koska tahdomme opiskelijoiden oppivan käyttämään Linux käyttöjärjestelmän terminaalia. Tämän harjoituksen jälkeen opiskelija pystyy kartoittamaan verkosta löytyvät resurssit käyttämällä skannaustyökaluja.

6.2.3 Salausten purkaminen

Penetraatiotestauksen kolmannessa vaiheessa tavoitteena on järjestelmään tunkeutuminen hyödyntämällä aiemmista vaiheista saatua tietoa. Yhtenä keinona päästä käsiksi järjestelmiin on murtaa järjestelmän salasana. (Nullbyte 2016.) Järjestelmien hakkeroinnissa on kyse yleisimmin salasanojen tai muiden suojausten purkamisesta, jolloin hyökkääjän tarkoituksena on päästä kohdejärjestelmään sisään esimerkiksi murretun salasanan avulla. Salasanat ovat kuitenkin hankalia murtaa ja niiden suojana toimivat erinäiset salausalgoritmit.

Alla olevasta kuviosta käy ilmi, kuinka opiskelija pystyy purkamaan salatun datan salaamattomaan muotoon käyttäen John The Ripper-työkalua. Käytännön harjoituksessa opiskelija purkaa MD5-hajautusalgoritmilla salatun sanan sekä myös murtaa Kali Linux käyttöjärjestelmän root-käyttäjän salasanan.



Kuvio 10: Salausten purkamisen prosessi käytännön harjoituksessa

MD5 on 128-bittinen salausalgoritmi tyyppi, joka tunnetaan kryptograafisena hajautusalgoritminä. MD5-hajautusalgoritmi tuottaa hajautusarvon heksadesimaalisessa 32 merkkisessä muodossa. Kahden eri ajankohtana laskettujen MD5-hajautusarvojen vertailusta selviää, onko tiedostoa mahdollisesti muutettu siirron aikana. Mikäli tiedostoa on muokattu millä tahansa tavalla, hajautusarvo on eri kuin alkuperäisessä. Tällöin vertaamalla uutta ja vanhaa hajautusarvoa on mahdollista nähdä, onko suojattua tietoa muutettu. (Linux.fi 2017.)

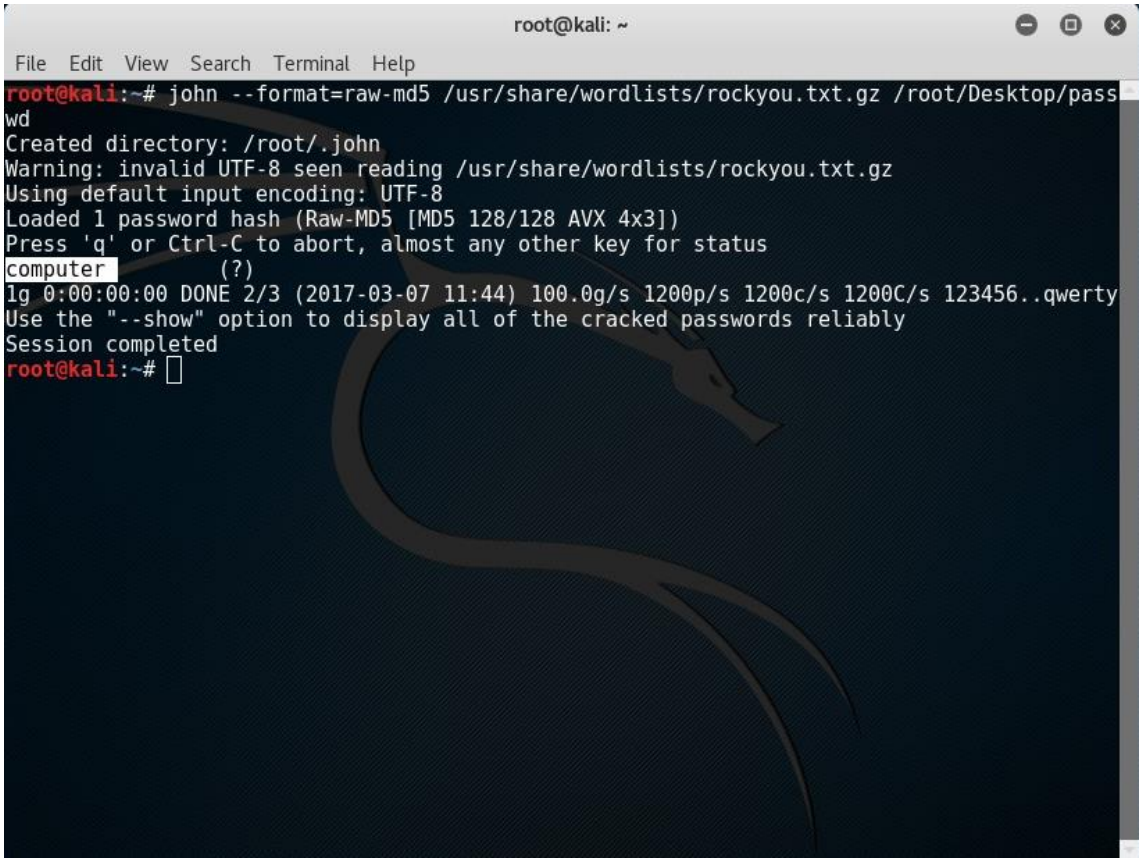
Muiden hajautusalgoritmien kehittämisten johdosta asiantuntijat ovat huomanneet MD5 hajautusalgoritmissa useita vakavia turvallisuusriskejä. MD5-hajautusalgoritmi ei ole suojattu törmäyksiltä. Törmäyksellä tarkoitetaan tilannetta, jossa kaksi MD5-hajautusarvoa on hyvin samankaltaisia tai täsmälleen samat. Toimiakseen oikein jokaisen MD5-hajautusarvon tulee

olla ainutlaatuinen. Käytetyimmille tunnistusprotokollille on tärkeää, että toiminnallisuus säilyy hyvänä. Tästä johtuen MD5-hajautusalgoritmi on usein korvattu esimerkiksi SHA-1-salausalgoritmilla. (Technopedia 2017.)

Tietoturva-ammattilaiset kutsuvat MD5- ja muita hajautusalgoritmeja nimellä viestin yhteenveto (engl. message digest). Tällä tarkoitetaan hajautusarvon tiivistävän alkuperäisen arvon ja palauttavan korvaavan arvon, joka on täysin erilainen kuin alkuperäinen arvo. Hajautusarvoja käytetään kyberturvallisuudessa sekä tietokantojen tehostamisessa esimerkiksi hakujen ja tiedonhallinnan yhteydessä korvaamaan arvoja, jotta haut nopeutuvat. (Technopedia 2017.)

John The Ripper-työkalu on Openwall nimisen tietoturvayrityksen tekemä avoimeen lähdekoodiin perustuva ilmainen salasanojen purkuohjelmisto. John the Ripper-työkalu on yksi tunnetuimmista ja käytetyimmistä salasanan purkuohjelmistoja ja käyttötarkoitukset soveltuvat niin aloitteleville kuin kokeneillekin käyttäjille. (Shankdar 2016.) John The Ripper-työkalun pääkäyttötarkoituksena on havaita heikkoja Unix-salasanoja. John the Ripper-työkalu pystyy purkamaan monia, usein Unixissa käytettyjä salasanojen hajautusarvoja kuten MD5- ja SHA215-hajautusalgoritmeja. Salasanojen purkuohjelmasta on olemassa myös yhteisön parantelema versio, jolla myös Windows käyttöjärjestelmän LM-hajautusarvot pystytään purkamaan sekä muita hieman vähemmän käytettyjä salaustyyppejä. John The Ripper-työkalusta on tarjolla myös maksullinen ammattilaisversio, joka toimii enemmän kaupallisena tuotteena. Ammattilaisversiota on helpompi käyttää ja sitä tarjotaan valmiissa paketeissa tietyille käyttöjärjestelmille, kuten Linux käyttöjärjestelmälle ja Mac OS X:lle. (Openwall 2017.)

Raaka voima (engl. brute force) tarkoittaa kyberturvallisuuden kontekstissa hyökkäystä, jossa käytetään järjestelmän laskentatehoa suorittamaan salasanan murtoyritystä. Hyökkäyksessä tietokone yrittää selvittää salasanan laskemalla mahdollisia merkkiyhdistelmiä ja kokeilemalla niitä yksitellen, kunnes oikea löytyy. Salasanan murtamisen yrittäminen vaatii tietokoneelta paljon resursseja, mutta nykyään moderneilla tietokoneilla raa’an voiman salasanan murtamista pidetään tehokkaana salauksen purkukeinona. Raa’an voiman hyökkäyksessä tärkeintä on ymmärtää, että lopulta tietokone onnistuu selvittämään salasanan huolimatta sen monimutkaisuudesta tai pituudesta. Tästä johtuen salasanojen monimutkaisuuteen tulee panostaa huolellisesti. Pitkissä ja monimutkaisissa sanoissa, joissa on useita erikoismerkkejä sekä numeroita voi kulua aikaa muutamista minuuteista jopa kuukausiin purkamisessa. Yksinkertaiset sanat, kuten esimerkiksi ”kissa” purkautuu muutamassa sekunnissa. (Oulun seudun ammattiopisto 2017.)



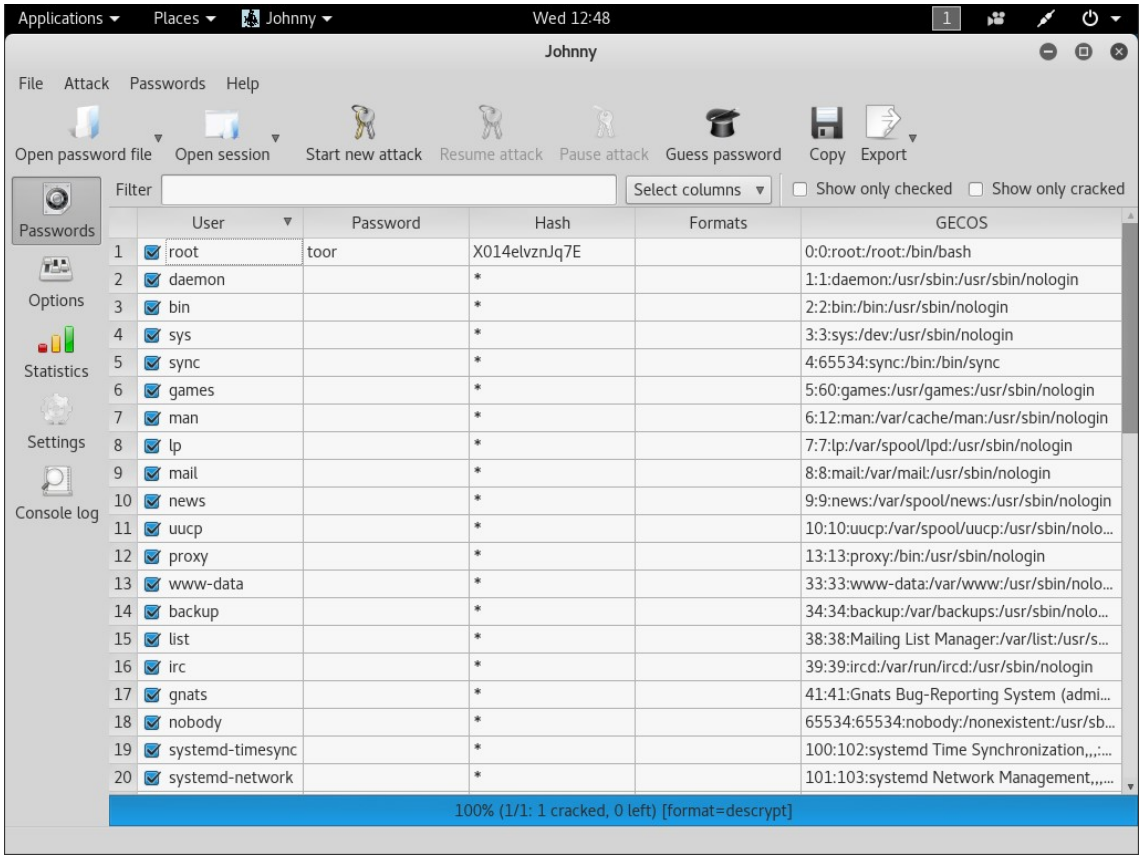
Kuvio 11: John The Ripper-työkalu murtamassa MD5-hajautusalgoritmilla suojattua salasanaa harjoituksessa

Sanakirjahyökkäys (engl. dictionary attack) tarkoittaa hyökkäystä, jossa salasanan murtamiseen käytetään valmista sanalistaa. Sanalistoja hyödyntäen salasananpurkuohjelma aloittaa murtamisen kokeilemalla sanalistassa olevia sanoja salasanakenttään yksitellen. Sanalistoja löytyy runsaasti internetistä, jolloin niitä ei tarvitse luoda itse. Listat ovat kuitenkin pääsääntöisesti kokoelma englanniksi olevia sanoja, joten kaikki salasanalistat eivät toimi suoraan suomeksi kirjoitettuihin salasanoihin. (Oulun seudun ammattiopisto 2017.)

Sanakirjahyökkäystä voi suorittaa monilla eri tavoin. Ensimmäisenä salasanaa voi suoraan kokeilla purkaa käyttämällä sanalistaa. Seuraavaksi on mahdollista kokeilla sanoja esimerkiksi takaperin tai isoilla ja pienillä kirjaimilla sekä erikoismerkeillä. Sanakirjahyökkäyksen avulla voi päätellä, ettei salasanan saa koskaan olla pelkkä yksittäinen sana, joka löytyy esimerkiksi sanakirjasta. Salasanan tulee olla mahdollisimman pitkä ja pyrkiä yhdistelemään erikoismerkkejä. (Oulun seudun ammattiopisto 2017.)

Salausten purkaminen kappaleen harjoituksissa käytetään edellä mainittuja käsitteitä osana salasanojen purkamista. Ensimmäisessä harjoituksessa opiskelija purkaa MD5-salausalgoritmilla suojatun avaimen John The Ripper-salasananpurkuohjelman avulla. John the Ripper-työkalulla suoritetaan kummatkin edellä mainitut raa’an voiman sekä sanalista

hyökkäykset. Raa'an voiman hyökkäyksessä opiskelija purkaa MD5-hajautusarvon. Salattu merkkijono saadaan joko opettajalta valmiina tai tehdään itse esimerkiksi internetistä löytyvillä MD5-salaustyökaluilla. Sanakirjahyökkäyksessä etsitään Linux käyttöjärjestelmän oma käyttäjä ja salasanatiedosto, joka on valmiiksi salattu Kali Linux käyttöjärjestelmässä SHA-512 salausalgoritmilla. Tämän jälkeen opiskelija käyttää John The Ripper-työkalua selvittääkseen salatun pääkäyttäjän salasanan.



Kuvio 12: John The Ripper-työkalun Johnny-niminen käyttöliittymäversio toiminnassa harjoituksessa.

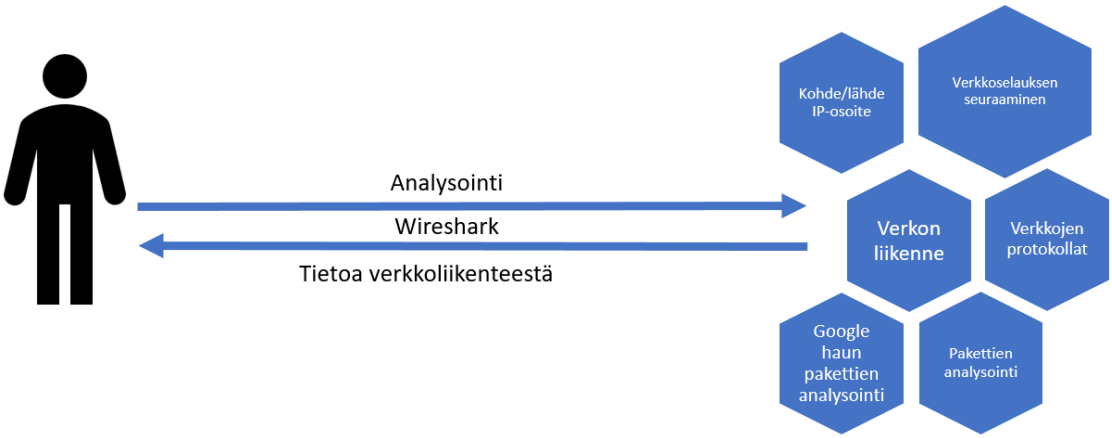
Harjoitusten tarkoituksena on tutustuttaa opiskelija eri salausalgoritmeihin sekä näyttää kuinka salasanoja on mahdollista purkaa. Opiskelija myös oppii monimutkaisten salasanojen tärkeyden, sillä yksinkertaiset salasanat murretaan harjoituksissa nopeasti. Näiden tietojen avulla opiskelija pystyy esimerkiksi tarkastamaan käyttämiensä salasanojen turvallisuuden käyttämällä John The Ripper-työkalua.

6.2.4 Verkkoliikenteen analysointi

Penetraatiotestauksen neljäs vaihe on järjestelmässä pysyminen, jolloin hyökkääjä pyrkii pysymään kohdejärjestelmän sisällä niin kauan, että saavuttaa tavoitteensa. Hyökkääjä voi

esimerkiksi verkkoliikennettä seuraamalla tutkia, onko häntä vielä huomattu. Tämän vaiheen aikana hyökkääjä yleisesti asentaa haitallisia sovelluksia kohdejärjestelmään. (Logisek 2016.)

Alla olevasta kuviosta käy ilmi, kuinka opiskelija analysoi verkkoliikennettä käytännön harjoituksessa käyttäen Wireshark-ohjelmistoa apunaan. Harjoituksen aikana opiskelija analysoi useita eri paketteja, jotka ovat syntyneet verkkoliikenteen seurannan aikana. Näiden pakettien avulla opiskelija pystyy esimerkiksi selvittämään pakettien lähde- ja kohde- IP-osoitteet.

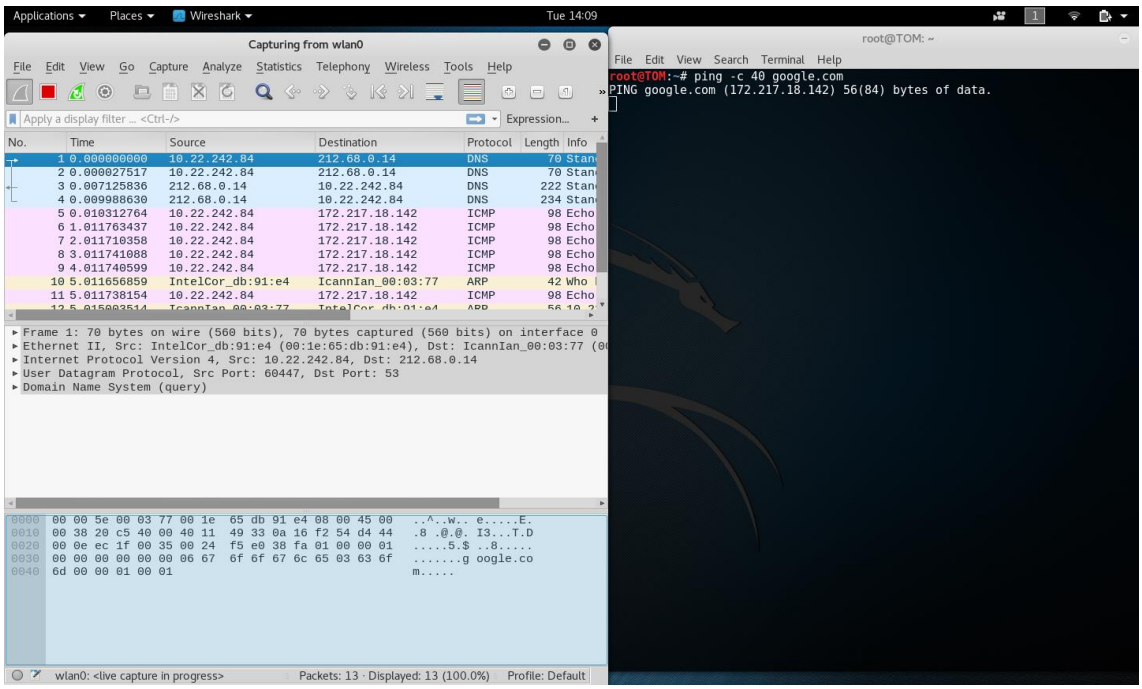


Kuvio 13: Verkkoliikenteen analysoinnin prosessi käytännön harjoituksessa Wireshark-ohjelmiston avulla

Verkon liikenteen analysointi (engl. network traffic analysis) tarkoittaa hyökkäystä tai puolustusta, jossa seurataan järjestelmän sisällä tapahtuvan kommunikoinnin kaavoja ja liikkeitä. Liikenteen analysoinnin päämääränä on saada tietää kuka kommunikoi kenen kanssa, miksi ja kuinka kauan. Verkon liikenteen analysoinnin avulla saatetaan saada tietoa, jota ei muilla menetelmillä ole mahdollista saada selville. (Whitman, Mattord & Green, 2014. 37)

Analyysin aikana järjestelmän sisällä lähetettyjä viestejä kaapataan ja seurataan, jotta niistä saadaan muodostettua kommunikointikaavoja. Itse analysointia on mahdollista tehdä, vaikka viestit ovatkin salattuja. Pääsääntöisesti mitä enemmän viestejä saadaan kaapattua ja seurattua, sitä enemmän verkon liikenteestä voi kerätä tietoa. Myös pakettien koko, jotka liikkuvat järjestelmien sisällä kertovat paljon hyödyllistä tietoa analysointia varten. Hyökkääjä voi tunnistaa pakettien koosta esimerkiksi tiedostojen siirtotapahtumia, vaikka paketit ovatkin salattuja. Hyökkääjän ei tarvitse nähdä pakettien sisältöä saadakseen hyödynnettyä analyysista muodostunutta tietoa. Hyökkääjän nähdessä monia pienikokoisia paketteja liikkuvan isäntäkoneiden välillä tasaisin väliajoin hän pystyy tunnistamaan, että kyseessä on interaktiivinen tilanne ja jokainen paketti vastaa yhtä näppäimistön painallusta. Suuria paketteja lähetettäessä pitkän aikavälin aikana on tästä mahdollista havaita, että verkossa joku vastaanottaa ja lähettää tiedostoja. Näistä paketeista voi myös yleensä

tunnistaa lähettäjän sekä vastaanottajan. Vaikka nämä tiedot eivät yksinään tuokaan hakkereille pääsyä kohdejärjestelmään, taitava hakkeri kykenee hyödyntämään analyysin aikana kerättyjä tietoja pyrkiessään läpäisemään järjestelmän turvamekanismit. Hyökkääjät käyttävät usein liikenteen analysointia yhdessä muiden hyökkäyskeinojen kanssa. Verkon liikenteen analysointi on kuitenkin kaikkein hyödyllisintä suorittaa tiedustelun yhteydessä, jolloin pyritään löytämään haavoittuvaisia isäntäkoneita tai kartoittamaan verkkoa. (Northcutt 2017.)



Kuvio 14: Wireshark-ohjelma analysoimassa verkon liikennettä harjoituksessa.

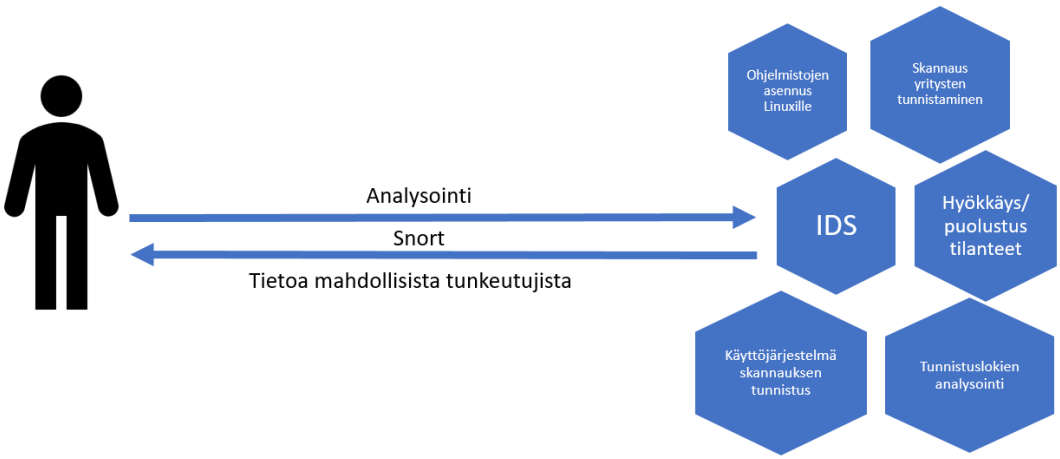
Verkon liikenteen analysointi-harjoituksessa opiskelija tutustuu verkon analysointiin Wireshark-ohjelman kanssa, jolla hän analysoi erityyppisiä liikkeitä verkossa. Harjoituksen tavoitteena on tutustuttaa opiskelija käyttämään Wireshark-ohjelmaa sekä ymmärtämään, miten verkossa tapahtuvaa liikennettä on mahdollista analysoida. Yllämainittujen toimintatapojen tarkoitus myös korostuu opiskelijan analysoidessa eri paketteja ja niiden ominaisuuksia.

Harjoituksessa opiskelija oppii tunnistamaan verkossaan liikkuvia paketteja, niiden lähettäjiä ja vastaanottajia sekä paketteja analysoidessa opiskelija saa syvemmän ymmärryksen eri protokollista ja yleisimmistä sisällöistä, kuten otsikoiden bittipituudesta sekä paketin elinajasta (engl. time to live).

6.2.5 Tunkeutumisen tunnistamisjärjestelmä

Penetraatiotestauksen viimeisessä vaiheessa hyökkääjä pyrkii peittämään jälkensä mahdollisimman huolellisesti, jotta hän ei jätä itsestään jälkiä hyökkäyksen jälkeiseen analyysiin. Tunkeutumisen tunnistamisjärjestelmillä on mahdollista havaita verkossa toimivia tunkeilijoita ja hyökkääjät pyrkivätkin välttämään näitä tunnistamisjärjestelmiä. (Certified Ethical Hacker 2011.)

Alla olevasta kuviosta käy ilmi tunkeutumisen tunnistamisjärjestelmä kappaleen käytännön harjoituksen prosessi, jossa opiskelija pyrkii tunnistamaan mahdolliset skannausyritykset omassa verkossaan käyttäen apunaan Snort-ohjelmistoa. Harjoituksen aikana opiskelija pystyy tunnistamaan mahdollisen hyökkääjän IP-osoitteen ja voi tarvittaessa estää kaiken liikenteen siitä osoitteesta.



Kuvio 15: Tunkeutumisen tunnistamisjärjestelmä harjoituksen prosessi

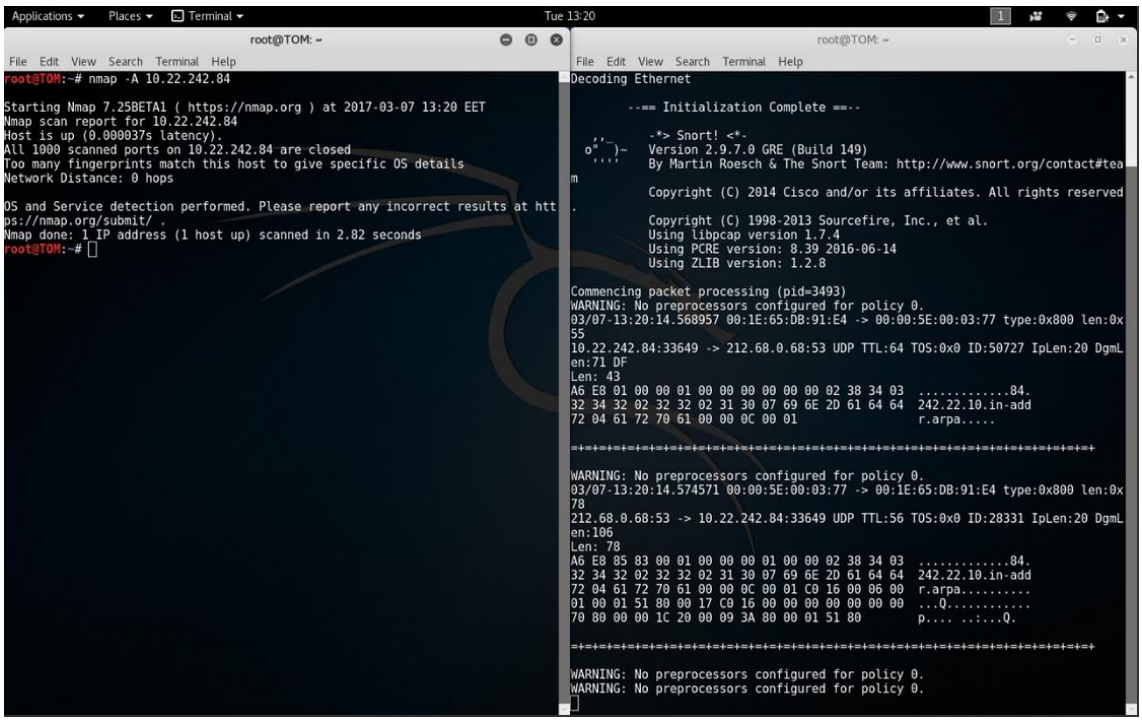
Tunkeutumisen tunnistamisjärjestelmä (engl. Intrusion Detection System), on järjestelmä tai laite jolla pyritään tunnistamaan hyökkääjä, joka yrittää päästä organisaation verkkoon sisään. Tämänkaltaisia erilaisia järjestelmiä on olemassa paljon, tunnetuin esimerkki tunkeutumisen tunnistamisjärjestelmä on Snort-ohjelma. Erilaisia ratkaisuja ovat muun muassa eri virustentorjuntaohjelmistot, kuten Symantec nimisen tietoturvayrityksen Norton-virustentorjuntaohjelma tai koko verkkoa monitoroivia ohjelmistoja. Nämä ohjelmistot toimivat usein esimerkiksi tapahtumalokeja seuraamalla ja analysoivat verkon liikennettä poikkeuksilta, jotka viittaavat mahdolliseen hyökkäykseen tai luvattomaan tunkeutumiseen. Tunkeutumisen tunnistamisjärjestelmät voidaan luokitella kahteen yläluokkaan, isäntään pohjautuvaan tunkeutumisen tunnistamisjärjestelmään (engl. Host Based Intrusion Detection System) eli konekohtaiseen ratkaisuun ja verkkoon pohjautuvaan tunkeutumisen tunnistamisjärjestelmään (engl. Network Based Intrusion Detection System) eli verkkopohjaiseen ratkaisuun. (Berge, Ernst & Young 2017.)

Vaikka palomuurit ja tunkeutumisen tunnistamisjärjestelmät liittyvät verkkojen turvallisuuteen, ne ovat helppo samankaltaisuuksistaan huolimatta eri kokonaisuudet. Molemmat ratkaisut pyrkivät suojaamaan verkkoja erilaisilta hyökkäyksiltä. Palomuuri eroaa tunkeutumisen tunnistamisjärjestelmästä pyrkimällä pysäyttämään hyökkäykset jo ennen kuin ne ovat päässeet verkkoon rajoittamalla pääsyä verkkoihin ulkopuolelta. Palomuurit eivät havaitse hyökkäyksiä verkon sisältä, vaan ne pyrkivät havaitsemaan hyökkäykset verkon ulkopuolelta.
Tunkeutumisen tunnistamisjärjestelmä pyrkii havaitsemaan tunkeutumisen vasta kun se on tapahtunut ja lähettämään ilmoituksen siitä verkon ylläpitäjälle. Tunkeutumisen tunnistamisjärjestelmä toimii seuraamalla verkon tapahtumalokeja sekä liikennettä ja vertaamalla niitä tunnettuihin kaavoihin ja heuristiikkoihin, joita yleisimmät hyökkäykset käyttävät. Usein tunkeutumisen tunnistamisjärjestelmät saatetaan sekoittaa myös tunkeutumisen estojärjestelmiin (engl. Intrusion Prevention System), joka katkaisee yhteyksiä mahdollisen hyökkäyksen sattuessa. Tunkeutumisen estojärjestelmä on sovelluskerroksessa toimiva palomuurin ominaisuus. (Whitman, Mattord & Green, 2014, 36.)

Isäntään pohjautuva tunkeutumisen tunnistamisjärjestelmää toimii analysoimalla ja seuraamalla koneen sisällä tapahtuvia muutoksia. Isäntään pohjautuvat tunkeutumisen tunnistamisjärjestelmien seuraamat tapahtumat liittyvät yleensä ohjelmistojen resurssien käytön seuraamiseen. Esimerkkitilanteessa selainohjelmisto saattaa yllättäen alkaa muokkaamaan järjestelmän tietokantoja, jolloin järjestelmä huomaa muutokset tietokannassa ja ilmoittaa tapahtuneesta järjestelmän ylläpitäjälle. Isäntään pohjautuva tunkeutumisen tunnistamisjärjestelmä myös seuraa eri järjestelmän tiloja kuten tiedostojärjestelmiä, muistia ja eri tapahtumalokitiedostoja ja pyrkii varmistamaan ettei niitä ole muutettu. Isäntään pohjautuviin tunkeutumisen tunnistamisjärjestelmäohjelmiin kuuluu esimerkiksi Windows-käyttöjärjestelmän GFI LANguard SIM-ohjelmisto, joka varmistaa että järjestelmän tiedostoja ei ole muutettu, lisätty tai poistettu. GFI LANguard myös skannaa järjestelmät tiedostot. GFI-ohjelmisto toimii tallentamalla skannatuista tiedostoista MD5-tarkisteen, johon se vertaa tasaisin väliajoin järjestelmän tiedostoja. Mikäli eroavaisuuksia löytyy, ne lähetetään järjestelmänvalvojalle ilmoituksena ja eroavaisuuksista luodaan tapahtumalokitiedosto. (Whitman, Mattord & Green, 2014, 31.)

Verkkoon pohjautuva tunkeutumisen tunnistamisjärjestelmä toimii käyttämällä verkkosegmenttien seuraamista datalähteinä. Verkkoon pohjautuvat tunkeutumisen tunnistamisjärjestelmät toimivat siten, että verkkokortti asetetaan seurantatilaan jossa se kerää kaiken tiedon liikenteestä, joka tapahtuu sen verkkosegmentissä. Verkkoon pohjautuvat tunkeutumisen tunnistamisjärjestelmät seuraavat verkossa liikkuvia paketteja kun ne ohittavat sen sensoreita. Sensorit pystyvät havaitsemaan vain paketteja jotka liikkuvat siinä verkon osassa, johon sensorit on asetettu. Paketit näkyvät vain mikäli niillä on yksi

ennalta määritellyistä allekirjoituksista. Allekirjoituksista on kolme eri tyyppiä ja niihin kuuluvat portti-, teksti- ja puskuriallekirjoitukset. Tekstikirjoitukset näyttävät mahdollisen tekstin, mikä merkitsee mahdollista hyökkäystä. Porttiallekirjoitukset seuraavat hakkereiden hyökkäyksissä yleisesti käytettyjä portteja kuten portteja 23 (Telnet), 21/20 (FTP) sekä 143 (IMAP). Puskuriallekirjoituksissa sensorit seuraavat puskureissa esiintyviä vaarallisia tai epäloogisia yhdistelmiä. Tämän kaltaiset yhdistelmät voivat jopa aiheuttaa tietokoneen toiminnan pysähtymistä äärimmäisissä tapauksissa. (Northcutt 2017.)



Kuvio 16: Snort-ohjelmisto havaitsee verkossa tapahtuvaa skannausta.

Tunkeutumisen tunnistamisjärjestelmä moduulin harjoituksessa opiskelija käyttää yllämainittua Snort-ohjelmaa tunnistaakseen omassa verkossa tapahtuvaa liikennettä. Snort on verkkoon pohjautuva tunkeutumisen tunnistamisjärjestelmä, jolla on mahdollista seurata verkkoon kohdistuvia hyökkäyksiä ja skannauksia. Harjoituksessa opiskelija asentaa Snort-ohjelmiston ja käyttää Snort-ohjelmistoa tunnistamaan hyökkääjän tekemän skannauksen omaan verkkoon. Täten opiskelija oppii asentamaan ohjelmistoja Linux käyttöjärjestelmälle, sekä oppii ymmärtämään tunkeutumisen tunnistamisjärjestelmien toiminnan pääperiaatteen.

Harjoituksen jälkeen opiskelijalla on hyvä yleistietämys tunkeutumisen tunnistamisjärjestelmistä ja osaa soveltaa näitä järjestelmiä esimerkiksi omaan verkkoonsa tunkeutujien tunnistamiseen. Opiskelija oppii myös harjoituksen aikana Linux käyttöjärjestelmän käyttämistä, sillä Snort-ohjelmisto asennetaan terminaalin kautta käyttöjärjestelmään harjoituksen alussa.

6.3 Dokumentointi

Inkrementaalisen mallin mukaisesti seuraava vaihe on luoda harjoitusten dokumentaatio. (ISQTB 2017.) Dokumentaation luomiseen tulee löytyä toimiva virtuaaliympäristö sekä harjoitukset. Näiden vaatimusten täytyttyä pystyimme luomaan ohjeistuksen virtuaaliympäristön rakentamiseen, tehtävien tekemiseen sekä raportin, johon kirjataan ylös harjoitusten tulokset.

Tehtävien ohjeistus luotiin suorittamalla harjoitukset uudelleen, jolloin jokainen työvaihe kirjattiin ylös mahdollisimman selkeästi. Ohjeistusten tekeminen oli harjoitusten kannalta tärkein osa, sillä opiskelijoilla ei ole suoraa pääsyä Hands-On Information Security Lab Manual teokseen, josta löytyy samantapaiset ohjeet. Ohjeistuksia tehtäessä yksi tärkeä seikka oli myös niiden ymmärrettävyys. Ohjeistuksessa pyrimme kuvaamaan pelkästään tarvittavat toiminnot, jotta opiskelijat eivät hämmenny ylimääräisestä tiedosta. Harjoitusten ohjeistukset löytyvät liitteistä.

Raportti kirjoitettiin ohjeiden jälkeen, jolloin kiinnitimme erityistä huomiota siihen, että jokainen ohjeissa mainittu tehtävä löytyy raportista mahdollisimman selvästi. Raportista tulee myös arvioitava kokonaisuus opintojaksolle, joten kehitimme myös opintojakson ohjaajille raportin josta näkyy kaikki vastaukset tehtäviin. Tällöin ohjaajien työtaakka vähenee, sillä he näkevät tehtävien oikeat vastaukset suoraan omasta kopiostaan raportista. Raportissa on myös useita tehtäviä, joissa opiskelijat kertovat omin sanoin vastauksia eri kysymyksiin. Raportti löytyy liitteistä.

7 Testaus

Inkrementaalisen kehittämismenetelmän mukaisesti viimeinen sykli on käytettävyystestaaminen. Jatkuva testaaminen tapahtui koko kehittämistyönajan. (ISQTB 2017.) Käytännön harjoituksia testattaessa suoritimme kaksi erillistä testausta, ensimmäisessä testissä teimme itse harjoitukset ja toisessa testissä pyysimme toisia opiskelijoita tekemään harjoitukset kehittämiemme ohjeiden avulla. Testauksen tärkein osuus oli toisilla opiskelijoilla teetetty lyhyt käytettävyystestaus, sillä halusimme tietää kuinka harjoitukset onnistuvat pelkästään ohjeistuksen avulla.

7.1 Itsearviointi

Oma testimme suoritettiin hyvin pian harjoitusten luomisten jälkeen, sillä halusimme varmistaa vielä kertaalleen harjoitusten toimivuuden. Oman testauksemme tarkoitus oli tarkistaa ohjeiden validiteetti, jotta kaikki tehtävät onnistuvat näiden ohjeistusten avulla. Testauksemme osoittautui ensisilmäyksellä onnistuneeksi, sillä ohjeiden avulla tehtävät oli mahdollista suorittaa tehokkaasti. Koimme kuitenkin, että oma testimme ei riitä ohjeiden

tarkastukseen ja täten halusimme suorittaa saman testin muiden opiskelijoiden avulla. Tekemämme testi erosi jatkuvasta testaamisesta siten, että teimme kaikki harjoitukset yhtenä kokonaisuutena emmekä keskittyneet mihinkään tiettyihin kohtiin kuten jatkuvassa testaamisessa olemme tehneet.

7.2 Käytettävyystestaus

Pyysimme kahta opiskelijaa suorittamaan luomamme harjoitukset Leppävaaran kampuksen laboratorioympäristössä, jotta voimme varmistua harjoitusten toimivuudesta. Aikarajoitusten vuoksi emme pystyneet suorittamaan kattavaa käytettävyystestausta, vaan pyrimme vain selvittämään palautteen perusteella tehtävien toimivuuden.

Testin aikana opiskelijapari suoritti kaikki tehtävät lukemalla tehtävänannon ohjeista. Testin ollessa lyhyt ja yksinkertainen, keskityimme vain ohjeiden validiteettiin. Testin aikana huomasimme useiden asioiden olevan jokseenkin epäselviä ohjeissa ja tällöin jouduimme neuvomaan kyseistä opiskelijaparia, jotta he pystyivät suorittamaan tehtävät loppuun. Nämä ongelmakohdat olivat ainoita asioita, joissa neuvoimme koehenkilöitä. Tarkoituksenamme oli simuloida testin aikana tilannetta, jossa opiskelija suorittaa yksin kotonaan harjoituksia ilman ohjaajan tukea.

Testauksen aikana saimme kerättyä seuraavat tulokset, jotka tullaan ottamaan käyttöön ohjeiden korjaamisen aikana. Koimme saaneemme suurta hyötyä näistä opiskelijaparin tekemistä huomautuksista ja omista havainnoistamme, sillä pystyimme annetun palautteen perusteella muokkaamaan ohjeistusta vastaamaan paremmin tehtävänantoa.

Tärkeimmät tulokset opiskelijaparin tekemästä testistä:

- Monet asiat tulee ilmaista selkeämmin. (Esimerkiksi tuleeko url-osoitteen eteen www. etuliite vai ei.)
- Voidaanko isäntäkäyttöjärjestelmää hyödyntää, mikäli virtuaaliympäristöstä ei saa tarpeeksi tietoa? (Eräässä tehtävässä Linux ei löydä tietyllä komennolla mitään, Windows käyttöjärjestelmän komentokehotteessa sama tehtävä onnistuu eri komennoilla.)
- Yhdessä moduulissa ei ole montaa tehtävää. (Tämän moduulin tehtävissä opiskelijan tulee asentaa Snort-ohjelmisto Linux käyttöjärjestelmän terminaalia käyttäen ja tehdä muutama tehtävä tällä ohjelmalla.)
- Joistakin tehtävistä ei koettu olevan hyötyä. (Yllämainitun moduulin kohdalla opiskelija tutustuu Snort-ohjelmiston säännöksiin, jotka olivat opiskelijoiden mielestä jokseenkin turhia ja vaikeasti ymmärrettäviä nähtynä moduulin muihin tehtäviin.)

- Ohjeistuksesta puuttui kohtia, jotka tulee lisätä ohjeistukseen. (Yhdessä tehtävässä ei ole selkeää mainintaa, että ohjelman palkkeja tulee venyttää näkyvyyden parantamiseksi.)
- Jotkin Linux käyttöjärjestelmän toiminnot antavat samat tulokset eri komennoilla. (Tässä tulee selvittää kaikkien komentojen tarpeellisuus ja hyöty tehtävään nähden.)
- Tehtävät tulee numeroida paremmin, sillä ohjeet ovat pitkiä. (Joissakin ohjeissa ei ole asetettu selkeitä tehtävänumeroita helpottamaan opiskelijan etenemistä harjoituksissa)

Näiden tutkimustulosten perusteella pystyimme muokkaamaan ohjeistusta selkeämmäksi, sillä emme kyenneet oman testimme aikana havaitsemaan näitä ongelmia. Koimme tämän lyhyen testin antaneen meille paljon arvokasta tietoa, sillä pystyimme kehittämään ohjeistuksestamme huomattavasti paremman ja selkeämmän saatujen tulosten perusteella. Testauksen ja tulosten analysoinnin jälkeen kehitimme uuden version kaikista ohjeista.

8 Johtopäätökset ja kehittämisehdotukset

Harjoitukset, ohjeistukset sekä raportti luotiin Network Security-opintojaksolle, joka toteutetaan seuraavan kerran lukukausilla 2017-2018. Tähän mennessä käytännön harjoitusten laboratorioympäristön tulee olla täydessä toiminnassa, perustuen tekemäämme suunnittelu- ja luomistyöhön. Laajemmin ajateltuna tulevaisuudessa on myös mahdollista rakentaa samankaltaisia harjoituksia muille virtuaalisille opintojaksoille, joissa ei ole käytännön harjoituksia lainkaan.

Opinnäytetyöprosessin aikana kehittämämme käytännön harjoitukset, ohjeistukset ja raportti on mahdollista ottaa käyttöön toisille opintojaksoille lähinnä muokkaamalla vain aihesisältöä. Tästä esimerkkinä toimii Salausten purkaminen -kappaleen harjoitus, jonka loimme ilman Hands-On Information Security Lab Manual–teosta, soveltaen omaa osaamistamme. Harjoitus luotiin perehtymällä moduulin eri aiheisiin, joista valittiin mielenkiintoisin ja hyödyllisin aihe. Tämän jälkeen moduulista saaduilla tiedoilla oli mahdollista löytää sopiva ohjelmisto harjoituksen luomiseen. Kun ohjelmisto ja aihe ovat löytyneet harjoitusta varten, tulee enää luoda jokseenkin samanlainen harjoitus kuin virtuaalisessa oppimisympäristössä on käsitelty aiheesta. Tällä prosessilla oli mahdollista luoda skaalautuva toimintamalli, jotta luomamme harjoitukset voivat toimia pohjana muiden opintojaksojen käytännön harjoitusten luomiselle.

Kehittämisehdotuksia kerääntyi useita koko opinnäytetyöprosessin aikana liittyen harjoitusten suunnitteluun, toteuttamiseen sekä ympäristöön. Kehittämisehdotusten suuri määrä pohjautuu virtuaaliympäristön lukemattomiin mahdollisuuksiin, sillä vain luovuus on rajana harjoituksia suunnitellessa. Uskomme seuraavien kehittämisehdotuksia parantavan hands-on harjoitusten käyttökokemusta vielä paremmaksi kuin mitä se tällä hetkellä on.

- Harjoitusten tekeminen / toistaminen eri käyttöjärjestelmillä. Virtuaaliympäristössä on mahdollista pitää useita eri käyttöjärjestelmiä samaan aikaan päällä.
- Ympäristön skaalautuvuus toisiin opetustiloihin. Opinnäytetyöprosessin aikana käytännön harjoituksia varten oli käytössä vain yksi pienehkö opetustila.
- Syvemmät ja monipuolisemmat harjoitukset, sillä aikarajoitteiden vuoksi harjoitusten määrä ja haastavuus jäivät toivottua pienemmäksi.
- Erillinen harjoituksia varten tehty verkko, jolloin harjoituksia tehtäessä on mahdollista simuloida hyökkäys- ja puolustusskenaariot kunnolla.
- Opetusvideo esimerkkisuorituksesta harjoituksessa, jolloin opiskelijat pystyvät näkemään yhden vaihtoehdon harjoituksen suorittamiseen
- Levykuvan luominen ennen harjoitusten alkamista, jotta opiskelijat saavat täysin päivitetyn ja valmiiksi asennetun Kali Linux käyttöjärjestelmän suoraan käyttöönsä eivätkä tällöin joudu itse asentamaan ohjelmistoja tai päivittämään käyttöjärjestelmää. Levykuvaa ei luoda opinnäyteprosessin aikana, sillä alkukeväästä 2017 tehty levykuva on auttamattoman vanha syksyllä 2017.
- Harjoitusvastaavan hankkiminen tai palkkaaminen ohjaamaan harjoituksia laboratorioympäristöön vähentää opintojakson opettajien työtaakkaa.
- Pilvipalveluiden soveltaminen harjoitusten suorittamiseen mahdollistaa vielä dynaamisemman ympäristön.
- Raportin mahdollinen korvaaminen opintojakson työtilassa olevilla monivalintakysymyksillä vähentää opintojakson ohjaajien työtaakkaa

Näiden kehittämisehdotusten avulla harjoituksista pystytään kehittämään hyvin kattavia ja tarvittaessa myös haastavia, jolloin opiskelijat saavat vielä enemmän arvoa tästä oppimisprosessista. Tärkeimmät kehityskohteet ovat ehdottomasti suuremman käytännön laboratorioympäristön rakentaminen sekä käytännön harjoituksia varten luotava tietoverkko. Jo näillä kahdella harjoitusten syvyys kasvaa moninkertaiseksi, sillä syvempien ja monipuolisempien harjoitusten luominen on myös yksinkertaisempaa.

Suuremman oppimisympäristön luominen mahdollistaa useamman opiskelijan pääsyn ohjattuun oppimistapahtumaan, jolloin harjoitukset ovat helpompia suorittaa. Suuremmassa oppimisympäristössä opiskelijat pystyvät myös kunnolla toteuttamaan hyökkääjän ja puolustajan roolia, jolloin harjoituksista tulee paljon realistisempia. Ennen suuremman oppimisympäristön luomista tulee kuitenkin selvittää esimerkiksi kyselyn avulla opiskelijoiden halukkuus osallistua ohjattuun oppimistapahtumaan tiettynä aikana Leppävaaran kampuksen opetustiloissa. Ympäristön luominen on kuitenkin jokseenkin aikaa vievä prosessi ja sitä ei ole mielekästä luoda, mikäli halukkaita osallistujia ei löydy tarpeeksi.

Harjoituksia varten luotavan tietoverkon tulee muistuttaa oikeaa verkkoa, jolloin opiskelijat pystyvät suorittamaan penetraatiotestausta lähes oikeaan verkkoon. Opinnäytetyöprosessin aikana laboratorion verkko oli tavallinen verkkoympäristö, joka oli vain internet käyttöä varten. Käytännön harjoituksia varten luotavassa verkossa pääpaino on eri laitteissa, joita opiskelijat pystyvät itse etsimään ja listaamaan käyttäen erinäisiä ohjelmistoja ja työkaluja. Tällöin opiskelijoilla on tietty IP-osoite, jota he voivat aina käyttää harjoituksia tehdessä. Tämän erillisen verkon avulla harjoitukset voidaan suunnitella paljon syvemmiksi ja monipuolisemmiksi, sillä tämä verkko mahdollistaa laitteiden skannauksen. Opinnäytetyöprosessin aikana sen hetkisessä verkossa ei ollut erillisiä laitteita, joita olisi ollut mahdollista tutkia. Tulevaisuudessa mikäli verkko rakennetaan, siihen on hyvä sisällyttää esimerkiksi tulostimia, reitittimiä sekä web-kameroita harjoituksia varten.

Lähteet

Painetut lähteet

Whitman, M., Mattord, H. & Green, A. 2014. Hands-On Information Security Lab Manual. Boston, MA:

Sähköiset lähteet

Berge, Ernst & Young. 2017. IDFAQ: What is Intrusion Detection? Viitattu maaliskuu 2017. https://www.sans.org/security-resources/idfaq/what-is-intrusion-detection/1/1

BusinessDictionary, Benchmarking. Viitattu maaliskuu 2017. http://www.businessdictionary.com/definition/benchmarking.html

Certified Ethical Hacker. 2011. The Phases of Ethical Hacking. Viitattu maaliskuu 2017. http://certifiedethicalhackerceh.blogspot.fi/2011/08/phases-of-ethical-hacking.html

ComputerHope, Ethical Hacking. Viitattu maaliskuu 2017. http://www.computerhope.com/jargon/e/ethihack.htm

Corey, R. 2015. Summarizing The Five Phases of Penetration Testing. Viitattu maaliskuu 2017. https://www.cybrary.it/2015/05/summarizing-the-five-phases-of-penetration-testing/

EC-Council, Certified Ethical Hacking Certification. Viitattu maaliskuu 2017. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Hoffman, C. 2013. Hacker Hat Colors Explained: Black Hats, White Hats and Grey Hats. Viitattu maaliskuu 2017. https://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

Hoffman, C. 2014. Android is Based on Linux, But What Does That Mean? Viitattu maaliskuu 2017. https://www.howtogeek.com/189036/android-is-based-on-linux-but-what-does-that-mean/

ISTQB, What is Incremental model- advantages, disadvantages and when to use it? Viitattu helmikuu 2017. http://istqbexamcertification.com/what-is-incremental-model-advantages-disadvantages-and-when-to-use-it/

Johansen, R. 2015. Ethical Hacking Code of Ethics: Security, Risk & Issues. Viitattu maaliskuu 2017 http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues

Kali Linux Official Documentation, Making a Kali Bootable USB Drive. Viitattu helmikuu 2017. http://docs.kali.org/downloading/kali-linux-live-usb-install

Kali Linux Official Documentation, Should I Use Kali Linux? Viitattu helmikuu 2017. http://docs.kali.org/introduction/should-i-use-kali-linux

Kali Linux, About Us. Viitattu helmikuu 2017. https://www.kali.org/about-us/

Kishore, A. 2015. How To Scan Your Network for Devices and Open Ports. Viitattu helmikuu 2017. http://www.online-tech-tips.com/software-reviews/free-advanced-network-ip-and-port-scanner-security-tool/

Linux.fi, 2017. Jakelu. Viitattu maaliskuu 2017. https://www.linux.fi/wiki/Jakelu

Linux.fi. MD5. Viitattu maaliskuu 2017. https://www.linux.fi/wiki/MD5

Logisek. 2016. 5 Phases of Penetration Testing. Viitattu maaliskuu 2017. https://securityblog.gr/3423/5-phases-of-penetration-testing/

Northcutt, S. IDFAQ: What is network based Intrusion Detection? Viitattu maaliskuu 2017. https://www.sans.org/security-resources/idfaq/what-is-network-based-intrusion-detection/2/3

Northcutt, S. Security Laboratory: Methods of Attack Series, Traffic Analysis. Viitattu helmikuu 2017. http://www.sans.edu/cyber-research/security-laboratory/article/traffic-analysis

NullByte. 2016. The Five Phases of Hacking. Viitattu maaliskuu 2017. https://null-byte.wonderhowto.com/how-to/five-phases-hacking-0167990/

O'Hara, K. The Future of Cybersecurity Jobs. Viitattu maaliskuu 2017. https://www.monster.com/career-advice/article/future-of-cybersecurity-jobs

Olzak, T. 2008. The five phases of a succesful network penetration. Viitattu maaliskuu 2017. http://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/

Openwall, John the Ripper password cracker. Viitattu maaliskuu 2017. http://www.openwall.com/john/

Oracle VirtualBox. End-user documentation. Viitattu helmikuu 2017. https://www.virtualbox.org/wiki/End-user_documentation

Oulun seudun ammattiopisto, Murtotekniikat. Viitattu maaliskuu 2017. http://www.okol.org/verkkokurssit/datanomi/tietojarjestelmien_kehittaminen/tietoturvajarjestelmat/internetin_tietoturva/murtotekniikat.htm

ResearchPedia, 2014. Difference between Ethical Hacking and Non Ethical Hacking. Viitattu maaliskuu 2017. http://researchpedia.info/difference-between-ethical-hacking-and-non-ethical-hacking/

Rouse, M. 2016. Definition: Ethical hacker. Viitattu helmikuu 2017. http://searchsecurity.techtarget.com/definition/ethical-hacker

Rouse, M. 2016. Definition: Virtual Machine (VM). Viitattu maaliskuu 2017. http://searchservervirtualization.techtarget.com/definition/virtual-machine

Shankdar, P. 2016. 10 Most Popular Password Cracking Tools. Viitattu maaliskuu 2017. http://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref

Technopedia, Black Hat Hacker. Viitattu maaliskuu 2017. https://www.techopedia.com/definition/26342/black-hat-hacker

TechnoPedia, Definition – What does Network Enumeration mean? Viitattu helmikuu 2017. https://www.techopedia.com/definition/25405/network-enumeration

Technopedia, Gray Hat Hacker. Viitattu maaliskuu 2017. https://www.techopedia.com/definition/15450/gray-hat-hacker

Technopedia, MD5. Viitattu 2017. https://www.techopedia.com/definition/4022/md5

Technopedia, White Hat Hacker. Viitattu maaliskuu 2017. techhttps://www.techopedia.com/definition/10349/white-hat-hacker

Technopedia, Virtual Disk Image (VDI). Viitattu helmikuu 2017.
https://www.techopedia.com/definition/10933/virtual-disk-image-vdi

Kuviot

Taulukot

Liitteet

Liite 1: Virtuaaliympäristön asennusohjeet

Setting up Linux Kali to run on VirtualBox

Software used for this guide:

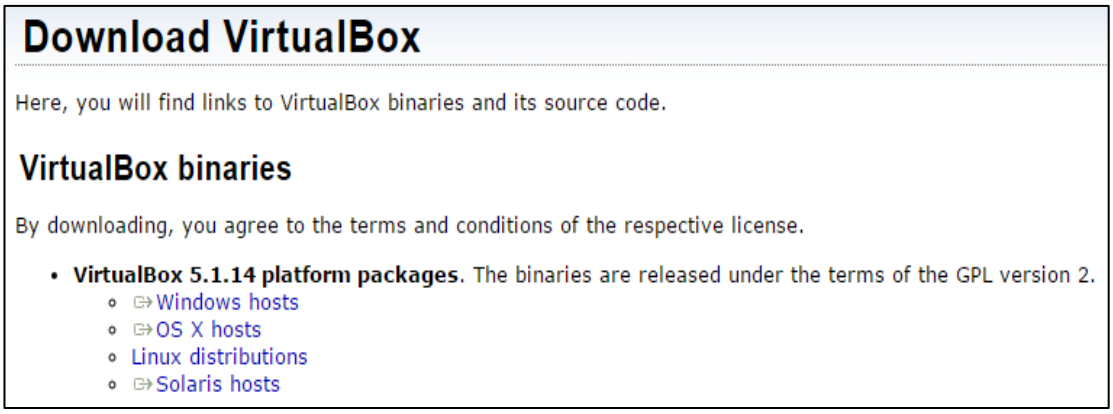
VirtualBox 5.1.14 for Windows
Kali Linux 64 bit VBox Version 2016.2

In order to properly install Linux Kali to run on Oracle's VirtualBox, you need to follow these instructions carefully.
In order to run a virtual operating system on your computer, you must meet the following requirements:

- At least 512MB of RAM
- At least 40GB of hard drive space
- A supported host operating system (Windows, Mac OS X, Most widely used Linux distributions)
- A supported guest operating system (Windows, Mac OS X, Most widely used Linux distributions)
- A working internet connection.

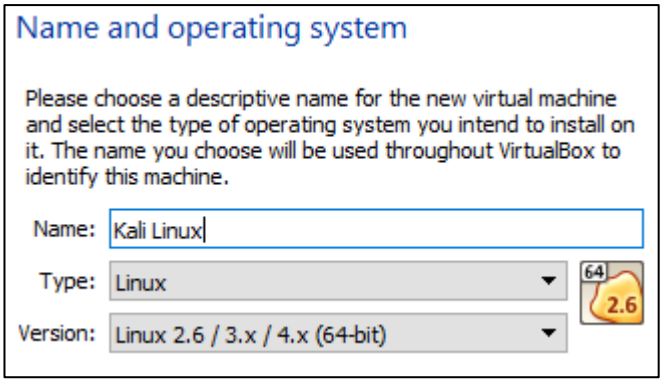
1. To get started, you must first download the virtualbox .ISO image from Kali Linux's website. https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/ From there, you must choose the Kali Linux VirtualBox images tab and select 64-bit .ISO(not light version) and download it. This will take quite some time depending on your connection speed. In the meantime, you can start setting up the Oracle VirtualBox. Remember to save the .ISO somewhere you can easily locate it.

2. Setting up the VirtualBox. Firstly, open your browser and navigate to (https://www.virtualbox.org/downloads). From there, you must choose the corresponding VirtualBox to match your host operating system.



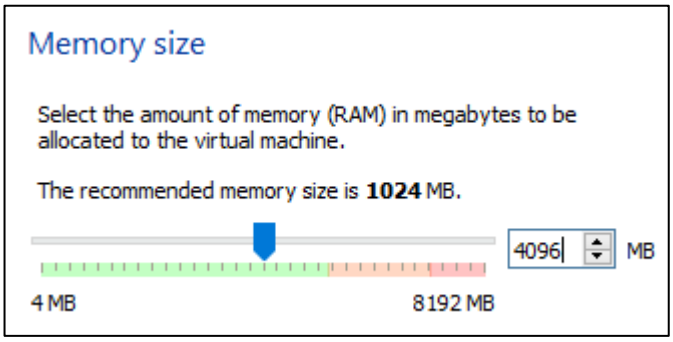
3. After choosing your operating system, an executable file will be downloaded. Follow the installation wizard and make sure that during the installation you choose register file associations (should be on by default). There will be a warning of resetting and disconnecting the network connection temporarily so make sure to save any work done on browsers or other programs that require internet connection before proceeding. After that, click install and you can start the VirtualBox after the installation wizard has finished.

4. Now that the VirtualBox is running, we can start configuring the Linux Kali operating system to run in virtual environment. First, you must choose New from the upper-left corner. You can now name your operating system. Choose the following options.

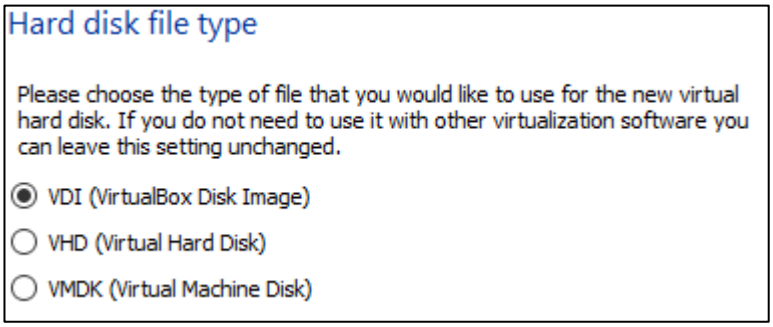


DISCLAIMER! If you don't see the 64-bit version on the dropdown menu, you must enable virtualization from your BIOS settings. BIOS can be opened by pressing either F1, F2, F10, Esc or Delete. This however varies with every model of the motherboard, so you might need to do this multiple times to access BIOS. Once in BIOS, you must navigate to (usually) advanced BIOS settings and switch virtualization ON if it is off. Refer to the manufacturer's manual if you are having troubles locating the BIOS or the virtualization settings.

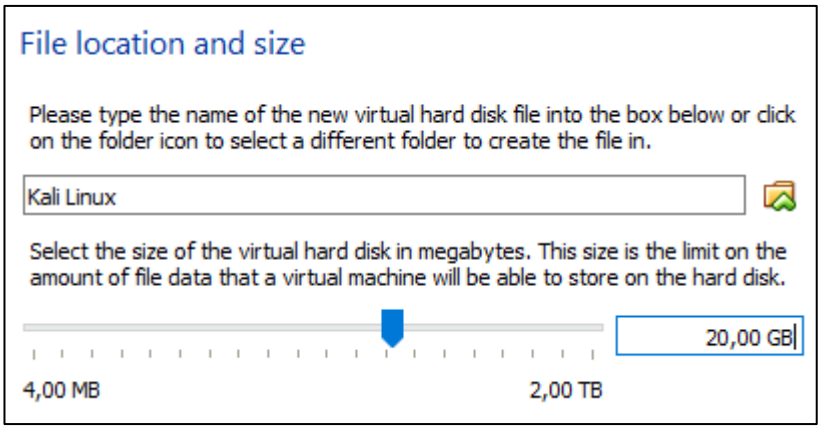
5. The next step is to allocate RAM for the virtual operating system to function. The minimum amount is 512 megabytes, however the more allocated RAM equals better performance. The recommend amount of RAM to run Kali Linux is 2 gigabytes. However, if possible use 4 gigabytes.



6. Creating virtual hard disk. The next step in configuring the virtual Kali Linux is to create a virtual hard disk drive. From the wizard choose Create virtual hard disk now. The recommended size is at least 8 gigabytes, however we are going to allocate 20 gigabytes just to be sure. When asked which hard disk file type you want to choose, choose VDI (VirtualBox Disk Image).

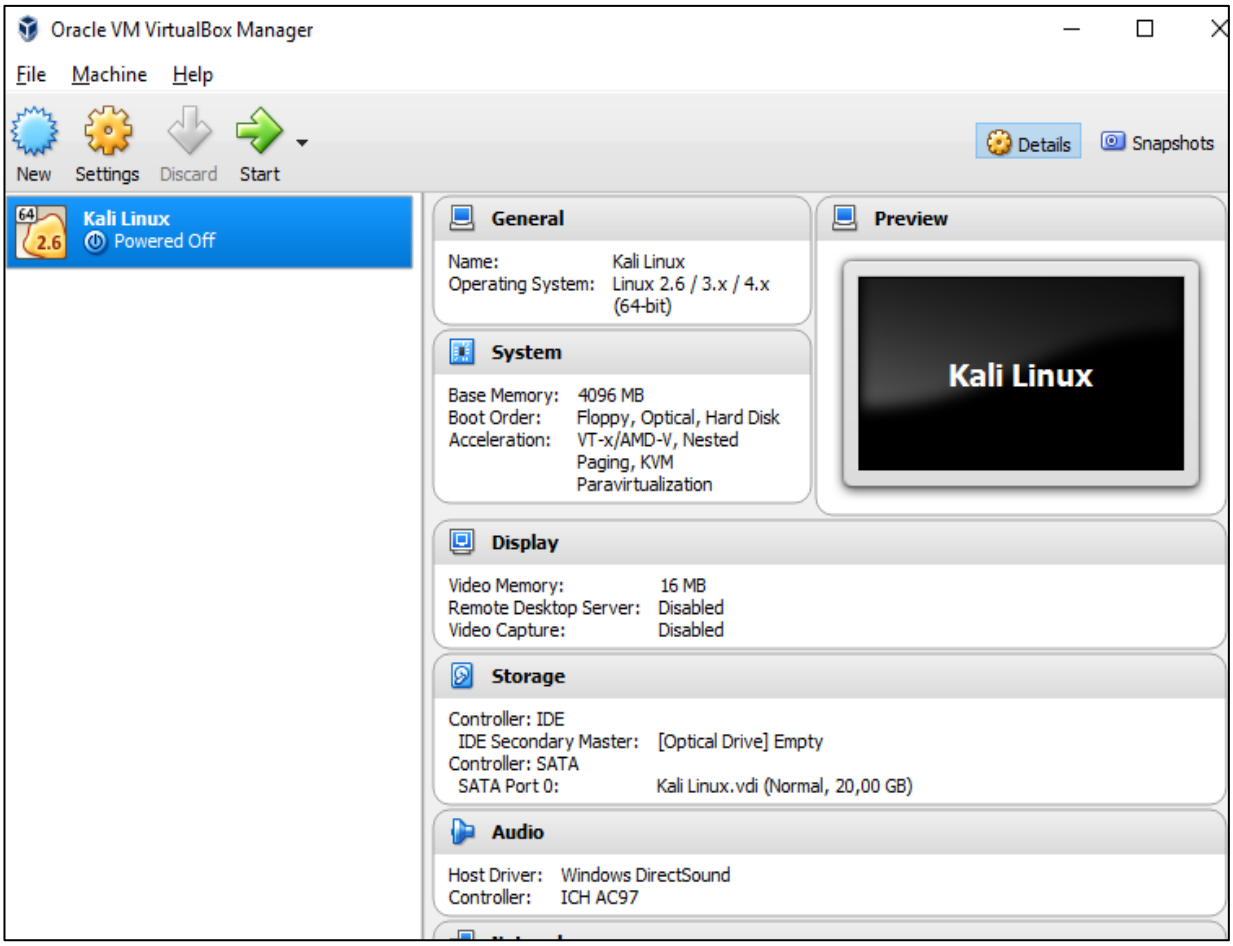


The next step is to determine the storage on physical hard disk. Choose Dynamically allocated to prevent any issues with storage space. After this we configure the total storage space allocated to the virtual Kali Linux.

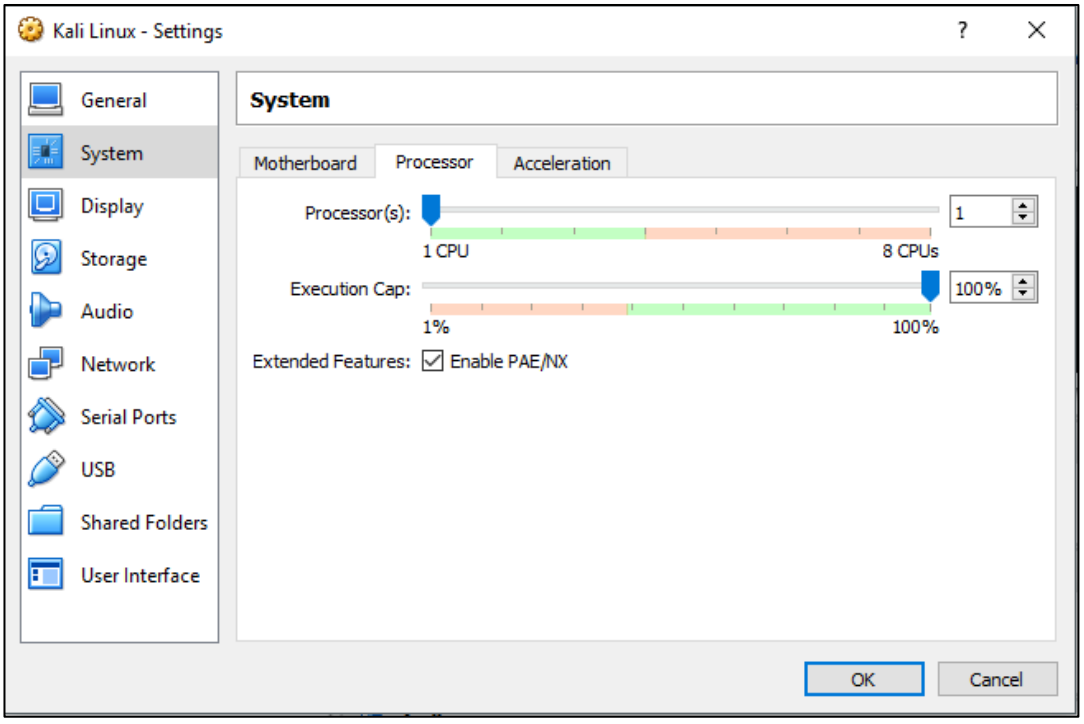


After clicking create, we have successfully configured the installation. The next step is to adjust the settings and upload the Kali Linux .ISO that was downloaded earlier.

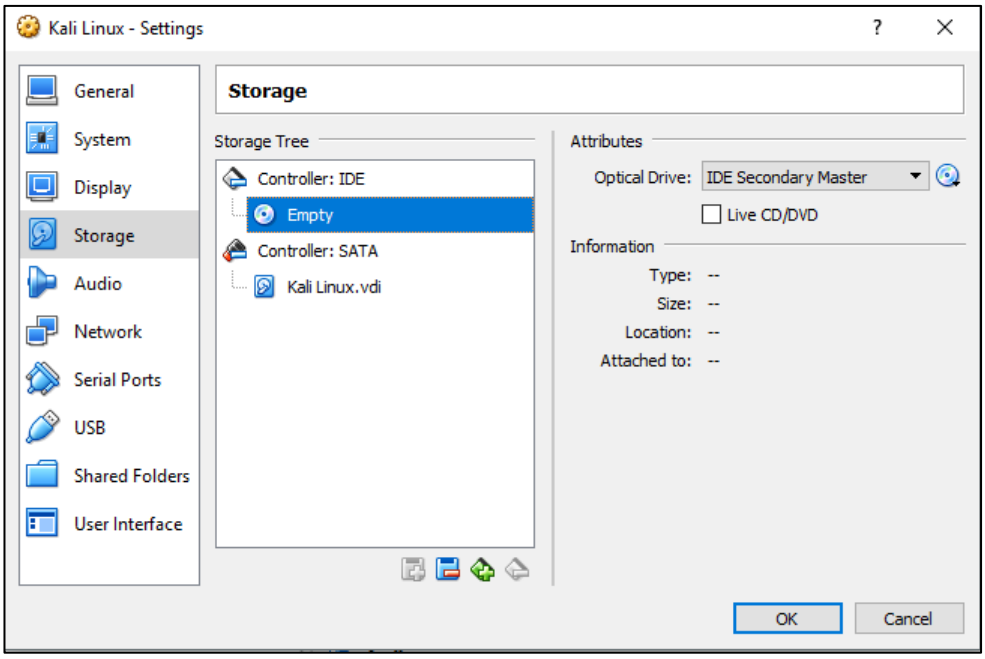
7. If done correctly, you should see a similar screen after the installation.



8. Adjusting the system settings. First press System on the right side (below General and above Display). Then open the processor from the top and click: Enable PAE/NX.

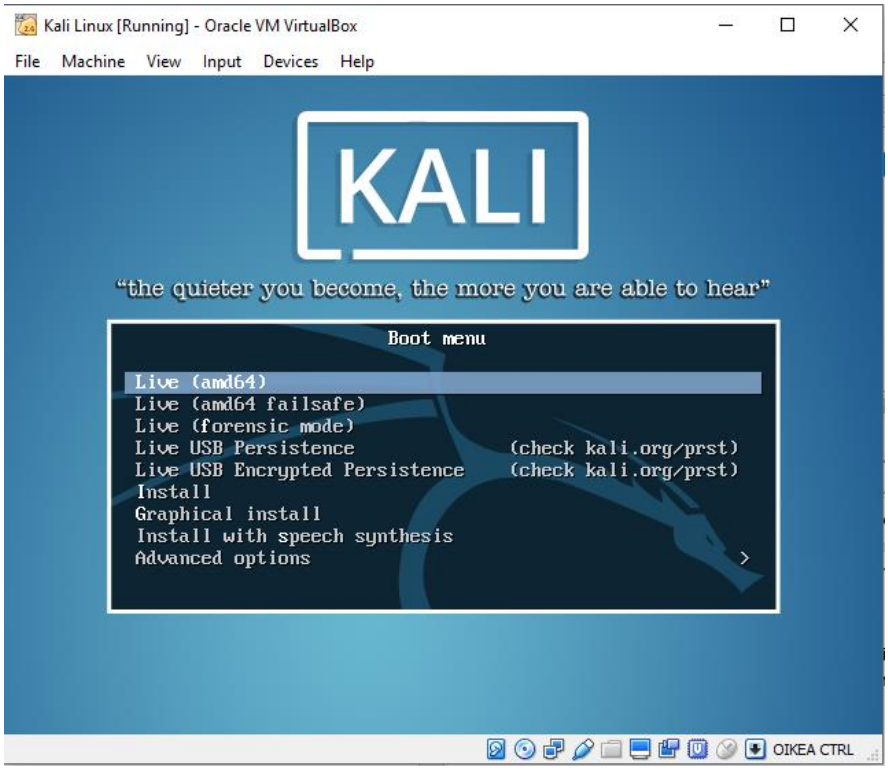


9. The last setting to configure before being able to use Kali Linux on VirtualBox is to upload the Kali Linux .ISO file to the virtual hard disk. To do this, click on Storage on the main page. Refer to the picture below:



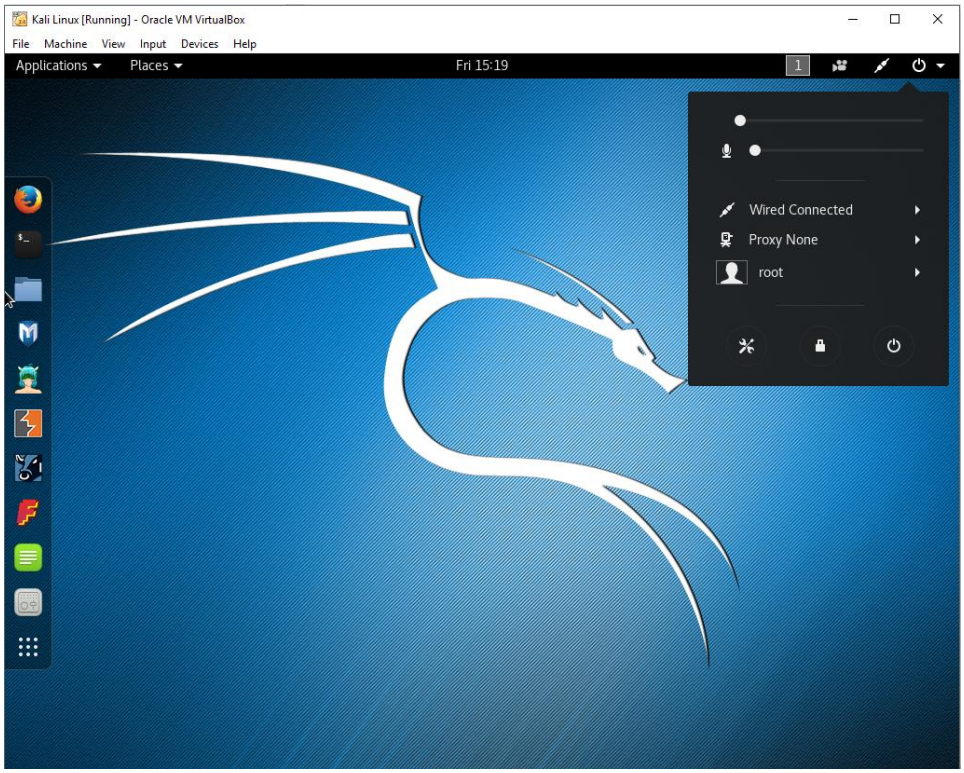
Click on the CD image next to the IDE Secondary Master text to open a menu to choose virtual optical disk file. Now you need to locate the .ISO file you downloaded at the beginning. After you found it, click on it and press open. After that, click OK. Now you can start the operating system! Click on the big green arrow on the upper left corner to start the virtual operating system.

10. The Operating System configuration. DO THIS EVERY TIME YOU RUN THE VIRTUAL OPERATING SYSTEM! After starting the operating system, a window opens to choose the installation for the Linux Kali operating system. We will be using the live (amd64) version every time when working on the hands-on labs. Press enter to access the live mode of the operating system. After this the operating system begins to load, so allow it to run for a moment.



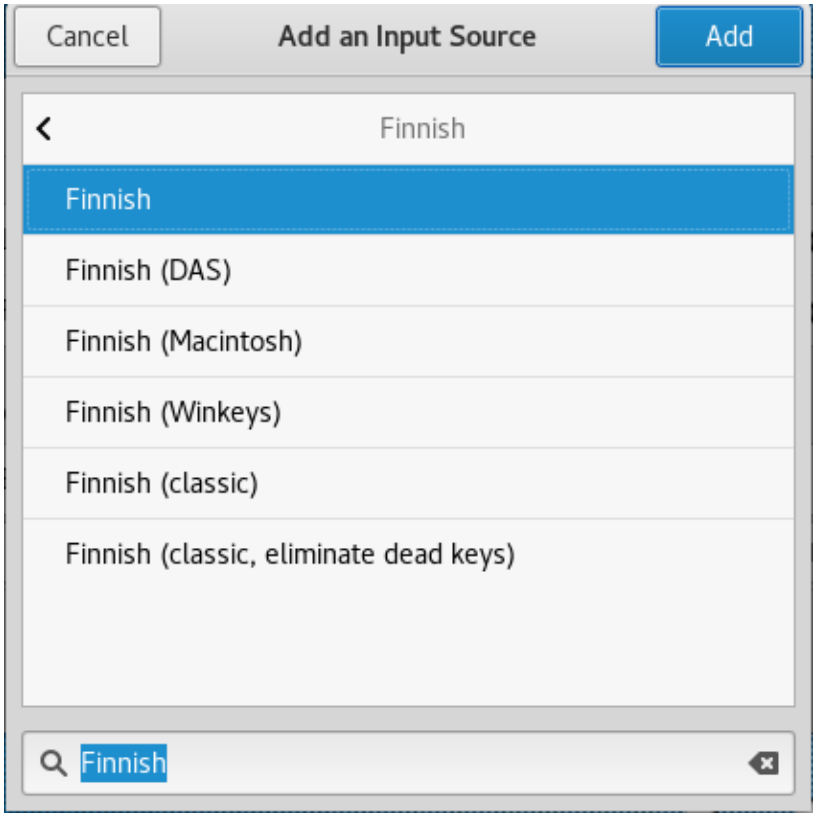
The next step is to configure the keyboard settings since the default keyboard settings is based on the United States keyboard layout.

Now that the desktop is loaded and ready to go, click on the icon next to the power button icon to open the settings. Now click the bottom left corner just below the picture next to root text.

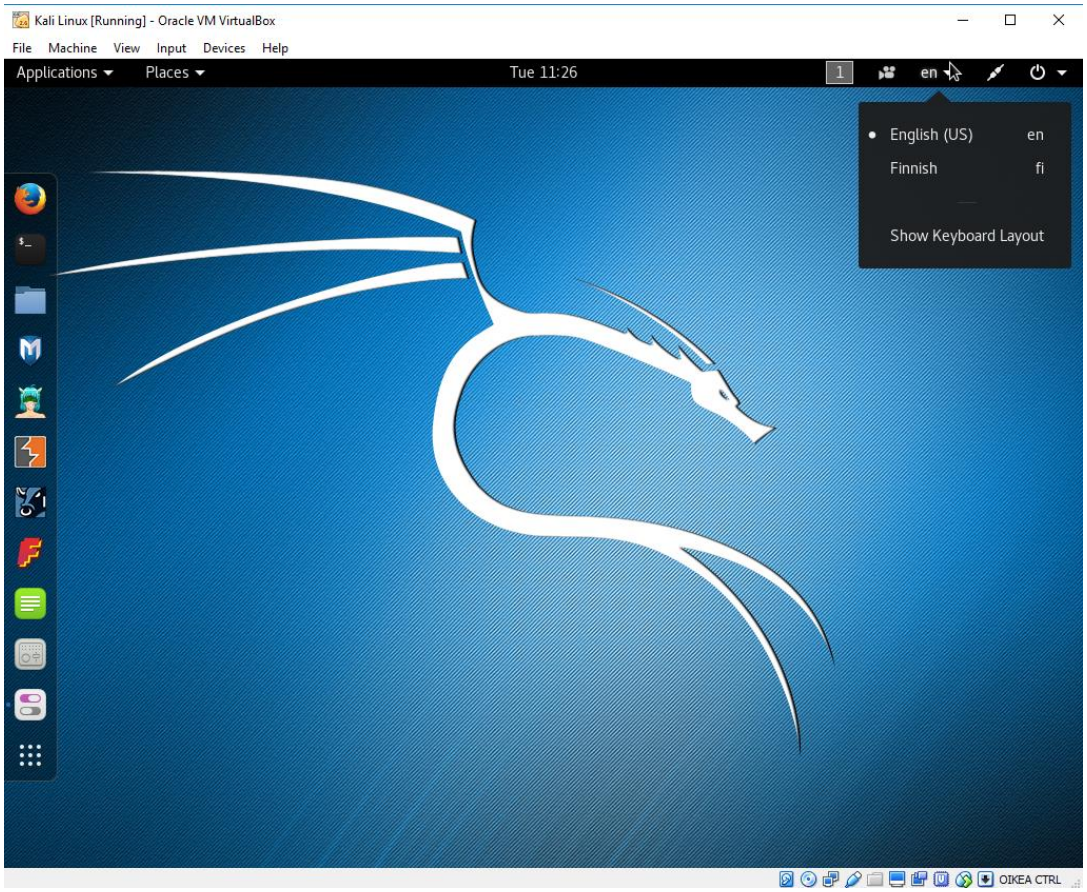


At the settings menu, choose Region & Language, and then click on the plus sign on Input Sources.

Next, click on the three dots in the bottom. Now you can type the desired language you want to work with. This doesn't change the language, only the keyboard input. So for example, we are going to choose Finnish. This makes using the terminal easier, since the special characters are located differently on the American keyboard in comparison to the Finnish.



After clicking Add, we finally choose the input language from the desktop.



11. Now you are ready to start working on the tasks! Remember to do the entire Step 10 every time you open the operating system, since the operating system settings do not get saved anywhere due to it being run in live mode!

Liite 2: Tietojen kerääminen kohteesta kappaleen ohjeistus

Footprinting & Reconnaissance

Software used for this exercise:

WHOIS 2.0
DiG 9.10.3-P4-Debian
host 9.10.3-P4-Debian
Modern Traceroute for Linux, version 2.1.0
Ping iputils-140519 Linux

1. General Network Information Using the Linux Command Line

You are a hacker trying to gain access to a large corporation to steal their information, your goal is to gather information about the target company from publicly accessible sources. To achieve this, you are going to use Linux terminal commands to find out information about the target company.

To begin this exercise, open the Linux terminal. The target company in this exercise is Google.

After you have opened the console, type in:

- whois google.com

Search the results for a plain google.com server. Now write the following information to the separate report:

- Registrar for the domain
- Primary and secondary name servers
- Administrative Contact name, address and phone number
- Technical Contact name, address and phone number

Explain what the other results of whois (google.com.pe etc) are?
How can you benefit from knowing this information when planning an attack?

2. Inverse mapping

To begin inverse mapping, you need to find out the target company's IP address. Type in:

- host google.com

and write down the IP address to the separate report.
How does the HOST command get the IP address?

3. DNS Interrogation

The next step is to find out IP addresses and information about different services tied to an address.

- host-t soa <IP address>

Write down soa information to separate document.
Explain what these numbers stand for.

The third command to find information about the target system is to use the command:

- dig google.com

How does the dig command differ from the host command?

The fourth command to find information about the mail servers is to use the command:

- host-t mx google.com

Write down all of your findings to the separate report.

4. Ping command

To get familiar with the Ping command, type in the command:

- man Ping

This will open the manual for the Ping command and you will be able to see all the different variations of the Ping tool. Familiarize yourself with the Ping manual.
To use Ping on footprinting, type in:

- Ping <IP address>

To stop the Ping command, press CTRL + C. After running the Ping scan, type the minimum, maximum, average and mdev return times to the separate report.

How does the Ping scan work? Explain in your own words.
What does mdev stand for?

5. Traceroute

Another useful way to gather information about the target is to use the Traceroute command to see the ”journey” of your Ping command from your console to the target console. To do this, simply type in:

- Traceroute google.com

You will notice that you see the amount of hops but not any information.
Why does the simple Traceroute command give only asterisks as a response?
To fix this, use the command:

- Traceroute-I google.com

Write down how many hops did it take to reach the target to the separate report. Also write down any other useful information about the Traceroute.
What information does the Traceroute –I command give us about the target system?

Liite 3: Verkon haavoittuvuuksien kartoittaminen kappaleen ohjeistus

Network Scanning & Enumeration

Software used for this exercise:

NMAP 7.40 for Linux

You are a network admin trying to find possible security flaws in your network and your goal is to perform various scans using the nMap tool. The goal is to get familiar with the nmap tool and find out how you can use it to perform penetration testing and as a network admin. The target for this exercise is Google. You can find out Google's IP address by using the host command. To begin this exercise, you need to open the Linux terminal.

1. Active Stack Fingerprinting and Enumeration with Nmap

1) The first step to start scanning with nmap is to find out how many systems respond to your first scan. To do this, type in:

- nmap-sP <IP address>

Write down how many systems responded to the scan on the separate report.

2) Now that you have found out how many systems are active, you can examine them more closely by using the command:

- nmap-sT <IP address>

Write down information about the ports on the separate report.
What information does-sT tell us about the ports?

3) Go to Exploit database https://www.exploit-db.com/ and try to find some exploits related to these open ports you just found using the search. Try searching for example with: https, http or telnet etc.. Write them down on the separate report. Try to find exploits, that are in metasploit library. These have the author marked as metasploit.

4) The next step is to perform a SYN stealth scan. Do this by typing:

- nmap-sS <IP address>

command on the terminal. Write about the difference between the SYN stealth scan and the-sT scan on the separate report.

5) After these scans, you are going to list the UDP ports available. You can do this by using the command:

- nmap-sU <IP address>

Write down the UDP ports that were available to the separate report.

2. Timing scans

1) Next you are going to perform scans with timing enabled on them. To do this, type in:

- nmap-sT-T normal <IP Address>

Write down what does normal signify in the scan and how long it took to complete the scan.

2) Now try the same scan with another timing. Type in:

- nmap-sT-T polite <IP Address>

Write to the separate report about how long it took to complete the scan and what does the polite timing mean. Disclaimer! If the scan doesn't complete within 10 minutes, cancel out and write down why this scan takes so long to complete.

3) Now finally, write down what you have learned about nmap, it's uses and how you could use nmap to perform penetration testing. Also write down how you could use this information as an attacker or as a defender.

Liite 4: Salausten purkaminen kappaleen ohjeistus

System Hacking

Software used for this exercise:

John The Ripper 1.8.0 for Linux

1) Decrypting MD5 hash

You have managed to capture a package through network traffic analysis which included a MD5 hashed password and your goal is to decrypt hashes and to crack a password. To do this, you will be using the password cracking tool called John The Ripper. Find out what MD5 is and write down answer on the separate report.

1) To open John The Ripper, navigate to applications-> password attacks-> and choose the program called john. This opens up a terminal with John The Ripper and you can see different functions for the program above.

2) For the first exercise, download the passw file from Optima and save it to desktop. The passw file contains a MD5 hashed password, which you need to encrypt using John The Ripper.

3) The first step is to locate the wordfile, which John The Ripper uses for decrypting hashes. This makes the decryption process much faster, because without the wordlist, John The Ripper would try to brute force the hash and that would take a very long time to complete. To locate the wordlist, use the following command:

- locate rockyou.txt

After you have found the word list, write down the location to the separate report.

4) The second step is to decrypt the MD5 hash in the text file that you downloaded earlier. To encrypt it with the word list, use the following command:

- john--format=raw-md5 /usr/share/wordlists/rockyou.txt.gz /root/Desktop/passw

5) After typing in the command, press enter and try to find the decrypted password.

Write down the decrypted password to the separate report. Also write in your own word why this decryption was so fast.

2) Decrypting root user password

1) You gained to access to an unlocked laptop and you want to get the user password in the case that user locks it up. This requires you to use Johnny, which is the GUI version of John The Ripper. Your goal is to crack the root user's password by unshadowing the password file and the shadow file. To do this, open up the terminal and write the following command:

- unshadow /etc/passwd /etc/shadow > mypasswd.txt

This command creates a clear text file, which has the hashed password for the root user. You can open the file by going to the Files folder and opening the mypasswd.txt file. You will notice that you can't really tell anything just by looking at this file.

Write down what does a shadow file contains in a separate report.

2) The next step is to open this file with Johnny. Navigate to applications-> password attacks and choose Johnny instead of john. Now you can see the graphical user interface of John the ripper.

3) The next step is to load the mypasswd.txt file to Johnny. Do this by choosing Open password file-> Open password file (PASSWD format) and select the mypasswd.txt file.

Click open and now you can see all the different users etc.

Simply press Start new attack and John The Ripper will crack the root users password.

4) Write down to the separate report the cracked password: Also write down why is it preferred to use wordlists with John The Ripper to crack hashes and passwords? Also think of ethical uses for John The Ripper.

Liite 5: Verkkoliikenteen analysointi kappaleen ohjeistus

Network Traffic Analysis

Software used for this exercise:

Ping iputils-140519 Linux

Wireshark 2.2.5 for Linux

1. Introduction to Wireshark

1) You are still trying to access the same organization you want to steal information from, but this time you're going to use network traffic analysis tools to try to find information which might be useful for you. You are going to use Wireshark for analyzing task. To complete this exercise, you need to navigate to Applications, then Sniffing & Spoofing and select Wireshark. Alternatively, you can also open the terminal and type Wireshark to open the application. There will be an error screen stating that Wireshark should be run as an unprivileged user, just click OK and proceed.

2) On the main page, go to the Capture menu and click options.

Choose the eth0 capture interface and click start. Now you have started to capture network traffic.

Open up the web browser and navigate to a few different sites to generate traffic for analysis purposes.

Once you have done that, click on the red square to stop the capturing process. Now you can see that Wireshark has captured loads of packets that can be analyzed.

3) Pick any packet you want from the list and explore the data gathered to get a glimpse of what information can be intercepted from doing network traffic analysis with Wireshark.

Drag down the bars so that the window with the packet information is larger. Remember to close web browser between all tasks so that it doesn't interfere with the traffic analysis.

This module’s task is to gather specific information from basic functions, such as from a Ping command and web browsing.

What do you see in Wireshark, after scanning your web browsing?

2. Capturing Ping packets

1) The first task is to analyze traffic from the Ping scan. Do this by starting a new capture on Wireshark (click file, then close and choose to continue without saving to start from a clean slate), then typing:

- Ping-c 40 google.com

Let this run for a few seconds, then stop the Ping and after that stop the traffic capture from Wireshark.

2) Now choose the first packet that says it's an echo (Ping) request and start to analyze it further. To do this, click on the packet, then choose Ethernet II from the middle window and expand it by clicking on the arrow. Also expand any other arrows.

Write down destination ipv6, source ipv6, capture length and packet protocol.

3. Capturing google.com ip address

1) The next task is to start a new capture from Wireshark and find out the IP address for google.com from using the search engines search function.

To do this, start a new capture and do a google search with the terms "Network Security". Only start the scan a moment before you are ready to press enter and start the search.

After this, you can close the capture by pressing the red square on Wireshark. Your job is now to find Google's IP from the captured packets! You can find the ip from a TCP packet. Write down your findings on the separate report.

2) Your final task is to analyze the same packets from the Google search task, so don't erase your latest capture! Otherwise you need to do it again. Now choose DNS packet you want and write down information about the Internet Protocol Version, header length, Time to live, source address and the destination address. Write these to the separate report.

Why would the information in this packet be useful to a hacker or useful to you as a network admin as you are monitoring for hacking attempts.

Liite 6: Tunkeutumisen tunnistamisjärjestelmät kappaleen ohjeistus

Intrusion Detection Systems

Software used for this exercise:
Snort version: 2.9.7.0 GRE (Build 149) for Linux
Ping iputils-140519 Linux

You have gained a hot tip that your competitor is jealous of your work and might be trying to steal it by hacking your systems. You must use your intrusion detection system to try to detect possible scanning attempts. Now you will familiarize yourself with Snort and how to install applications in Linux. To begin this exercise, you need to install Snort via the console. This can be done by following the instructions below.

1) Installing Snort

1) Open up terminal as a root user and type in:

- apt-get update

This command updates the repositories in Linux.

2) After the update has finished, type in:

- apt-get install snort

This command installs Snort on your system. When prompted do you wish to continue, press Y and enter after that. When asked for the address range for the local network, change the 16 subnet to 24 subnet.

Write down to the report why you had to change the address range subnet. After this, press enter to continue the installation.

3) To open Snort, type in the following command:

- snort-c /etc/snort/snort.conf-l /var/log/snort

After you notice that the installation is complete and you don't see root@kali text at the bottom of the terminal, you can close that terminal window and open up a new one. Now you need to verify that Snort has been installed properly by opening up a new terminal and typing in:

- snort--version

You should see that Snort is installed properly if you can see the version number of the current build in the terminal.

4) The next step is to download the ruleset for snort. Do this by typing in:

- wget https://www.snort.org/rules/community

After the ruleset has been downloaded, you can start using Snort.

Write about your installation process, did you find it easy or was it difficult?

2) Detecting scanning attempts with Snort

Now that Snort has been installed and the ruleset has been added, you can now begin the exercise. You will act as an attacker and as a defender on this exercise.

1) The first step to do is to find out your own IP address. This can be done by typing to the console:

- ifconfig

Write down your IP address to the separate report.

2) Next you open Snort to start monitoring the traffic. Do this by typing:

- snort-dev-i eth0

Now Snort is active and ready to go. Leave this terminal open and return to it after you have completed the attack.

3) Open up a new console and start attacking yourself. Type in:

- nmap-A <Your own IP address> (exclude the <> from the query)

Now open up the previous terminal where you ran Snort. After the nmap scan has completed, you will notice that Snort detected this scan and lots of information has come up to the screen. Stop the Snort scan by pressing CTRL + C. Now scroll up to see the scan and write down to the separate report about how Snort signifies the source and destination addresses on the defenders console?

4) Now that you have successfully used Snort, write in your own words how you could use Snort to detect any suspicious activity in your network. Also write about your installation process, did you find it easy or was it difficult?

Liite 7: Ohjaajan versio harjoitusraportista

Laurea-ammattikorkeakoulu

Network Security report example answers

Student's name and student number
Study program, Study unit number
Month, 201X

Footprinting & reconnaissance

1. General Network Information Using the Linux Command Line

Target address	Google.com
Registrar for the domain	Mark Monitor inc.
Primary name server	Ns1.google.com
Secondary name server	Ns2.google.com
Administrative Contact name	DNS admin
Administrative address	1600 amphitheater parkway, mountain view, California
Administrative phone number	+1. 650 623 4000
Technical contact name	DNS admin
Technical address	2400 E. Bay shore parkway, mountain view California
Technical phone number	+1. 650 33 00 100
How can you benefit from knowing this information when planning an attack?	To plan a social engineering attempt for example.
Explain what the other results of whois (google.com.pe etc) are?	Different servers for different countrires.

2. Inverse mapping

Target address	Google.com
IPv4 address	172.217.18.142
IPv6 address	2A00:1450:400F:802::200E
How does the HOST command get the IP address?	It uses DNS to translate information between IP address and domain names.

3. DNS interrogation

SOA name server	ns1.otaverkko.fi
SOA admin address	hostmaster.otaverkko.fi
Series of numbers at the end of SOA result	2017021002 10800 3600 604800 86400
Explain what these numbers stand for.	Timestamp that changes whenever you update your domain. The number of seconds before the zone should be refreshed. The number of seconds before a failed refresh should be retried. The upper limit in seconds before a zone is considered no longer authoritative. The negative result TTL (for example, how long a resolver should consider a negative result for a subdomain to be valid before retrying).
Dig domain name	google.com
Dig Name server:	ns1.google.com 216.239.32.10 ns4.google.com 216.239.38.10 ns3.google.com 216.239.36.10 ns2.google.com 216.239.34.10
How does the Dig command work?	It gets its information by querying dns name servers for information about host addresses, mail exchanges, name servers, and related information.
Mail servers corresponding to the DNS addresses:	google.com mail is handled by 30 alt2.aspmx.l.google.com. google.com mail is handled by 10 aspmx.l.google.com. google.com mail is handled by 50 alt4.aspmx.l.google.com. google.com mail is handled by 40 alt3.aspmx.l.google.com. google.com mail is handled by 20 alt1.aspmx.l.google.com

4. Ping

Target address	google.com
Min Ping	9.870 ms
Average Ping	10.566 ms
Max Ping	11.426 ms
mdev	0.553 ms
How does the Ping scan work? Explain in your own words.	It sends a packet to the target destination and then waits for its return and calculates spent time.
What does mdev stand for?	Average of how far each Ping RTT is from each other.

5. Traceroute

Target address	google.com
Amount of hops with Traceroute <Target>	30
Amount of hops with Traceroute –I <Target>	11
Why does the simple Traceroute command give only asterisks as a response?	Firewall is blocking ICMP requests?
What information does the Traceroute –I command give us about the target system?	For example, it shows how many points like routers are between target and you. It also shows how long it took to reach these points.

Network scanning & Enumeration

1. Active Stack Fingerprinting and Enumeration with Nmap

1) Target address	google.com
How many systems responded	1
What does-sP stand for in Nmap	Ping scan
2) What information does-sT tell us about the ports?	Open ports and services that are ran at them.
What does-sT stand for in Nmap:	Tcp connection scans.
3) Exploits that you found.	WinaXe 7.7 FTP Client- Remote Buffer Overflow (Metasploit)
4) Why might there be a difference between –sT and –sS commands?	sS is faster since it doesn't require full tcp connection, but it requires sufficient priviliges to run.
5) What UDP ports were available in your scanning:	All 1000 of the scanned ports were open

2. Timing scans

1) Explain what the normal state stands for.	It is an interval of how of then the scans take place.
2) How long did it take to complete the scan?	4,46s
3) How do you think this information might be useful to an attacker?	You can use the found information about the open ports, to try to find exploits to use as a way to take over the target system.
How about as a defender?	You can try to identify security threats of open ports in your network.
What have you learned about Nmap, its uses and how it is used to perform a penetration testing?	It's a powerful and flexible program for scanning ports. It can be used both as a defender and as an attacker.

Network traffic analysis

1. Introduction to Wireshark

1) Target address	google.com
2) What does capturing eth0 mean?	Capturing eth0 means capturing network traffic through Ethernet card.
What do you see in Wireshark, after scanning your web browsing?	Different network traffic packets containing information and their protocols

2. Capturing Ping packets

2) Destination IPv6	52:54:00:12:35:02
Source IPv6	08:00:27:D4:D0:A8
Capture length	98
Packet protocol	ICMP

3. Capturing google.com ip address

1) Google.com IPv4 address	172.217.18.142
2) Internet Protocol Version	IPV4
Header Length	20 bytes
TTL	64
Source address	10.0.2.15
Destination address	192.168.16.1
Why would the information in this packet be useful to a hacker or useful to you as a network admin as you are monitoring for hacking attempts.	You can use the source address to block further DDOS attacks as defender. As attacker you might find these addresses useful for example identifying more targets on the target network.

Intrusion detection system

1. Installing Snort

2) Why did you need to change the address range?	To make it correspond to the current network type.
4) Did you have any problems with the installation process?	no

2. Detecting scanning attempts with Snort

3) How does Snort signify the source and destination addresses on the defenders console?	Snort signifies these by showing the source address first and showing the destination address next to it on the right side.
4) How you can benefit from using Snort to detect suspicious activity on your network?	You can accurately monitor your network traffic for suspicious activity. You can block the traffic from that IP address and prevent further attacks.

System hacking

1. Decrypting MD5 hash

1) What is a MD5?	MD5 is an algorithm that is used to verify data integrity through creation of a 128-bit message.
5) Decrypted password	computer
5) Why was this decryption so fast?	Because the encrypted word was not very complicated.

2. Decrypting root user password

1) What does shadow file contain?	Shadow file stores actual password in encrypted form for user account with additional properties related to user password.
4) Cracked password	toor
4) Why is it preferred to use wordlists with John The Ripper to crack hashes and passwords??	Wordlists make the decryption process faster, otherwise john the ripper would try to brute force the password.
4)Ethical uses for John The Ripper	Test how secure your current password is.

Liite 8: Harjoitusraportti

Laurea-ammattikorkeakoulu

Network Security report

Student’s name and student number

Study program, Study unit number
Month, 201X

Footprinting & reconnaissance

1. General Network Information Using the Linux Command Line

Target address	
Registrar for the domain	
Primary name server	
Secondary name server	
Administrative Contact name	
Administrative address	
Administrative phone number	
Technical contact name	
Technical address	
Technical phone number	
How can you benefit from knowing this information when planning an attack?	
Explain what the other results of whois (google.com.pe etc) are?	

2. Inverse mapping

Target address	
IPv4 address	
IPv6 address	
How does the HOST command get the IP address?	

3. DNS interrogation

SOA name server	
SOA admin address	
Series of numbers at the end of SOA result	
Explain what these numbers stand for.	
Dig domain name	
Dig Name server:	
How does the Dig command work?	
Mail servers corresponding to the DNS addresses:	

4. Ping

Target address	
Min Ping	
Average Ping	
Max Ping	
mdev	
How does the Ping scan work? Explain in your own words.	
What does mdev stand for?	

5. Traceroute

Target address	
Amount of hops with Traceroute <Target>	
Amount of hops with Traceroute –I <Target>	
Why does the simple Traceroute command give only asterisks as a response?	
What information does the Traceroute –I command give us about the target system?	

Network scanning & Enumeration

1. Active Stack Fingerprinting and Enumeration with Nmap

1) Target address	
How many systems responded	
What does-sP stand for in Nmap	
2) What information does-sT tell us about the ports?	
What does-sT stand for in Nmap:	
3) Exploits that you found.	
4) Why might there be a difference between –sT and –sS commands?	
5) What UDP ports were available in your scanning:	

2. Timing scans

1) Explain what the normal state stands for.	
2) How long did it take to complete the scan?	
3) How do you think this information might be useful to an attacker?	
How about as a defender?	
What have you learned about Nmap, its uses and how it is used to perform a penetration testing?	

Network traffic analysis

1. Introduction to Wireshark

1) Target address	
2) What does capturing eth0 mean?	
What do you see in Wireshark, after scanning your web browsing?	

2. Capturing Ping packets

2) Destination IPv6	
Source IPv6	
Capture length	
Packet protocol	

3. Capturing google.com ip address

1) Google.com IPv4 address	
2) Internet Protocol Version	
Header Length	
TTL	
Source address	
Destination address	
Why would the information in this packet be useful to a hacker or useful to you as a network admin as you are monitoring for hacking attempts.	

Intrusion detection system

1. Installing Snort

2) Why did you need to change the address range?	
4) Did you have any problems with the installation process?	

2. Detecting scanning attempts with Snort

3) How does Snort signify the source and destination addresses on the defenders console?	
4) How you can benefit from using Snort to detect suspicious activity on your network?	

System hacking

1. Decrypting MD5 hash

1) What is a MD5?	
5) Decrypted password	
5) Why was this decryption so fast?	

2. Decrypting root user password

1) What does shadow file contain?	
4) Cracked password	
4) Why is it preferred to use wordlists with John The Ripper to crack hashes and passwords??	
4)Ethical uses for John The Ripper	