Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

Kevät 2014

Saku Lindroos

MURTAUTUMISTESTAUS-YMPÄRISTÖN RAKENTAMINEN OPETUSKÄYTTÖÖN

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

2014 | 54 sivua

Ohjaaja Esko Vainikka

Saku Lindroos

MURTAUTUMISTESTAUSYMPÄRISTÖN RAKENTAMINEN OPETUSKÄYTTÖÖN

Tämän opinnäytetyön tavoitteena on murtautumistestausympäristön rakentaminen opetuskäyttöön Turun ammattikorkeakoulun Lemminkäisenkadun toimipisteelle. Ympäristö on tarkoitettu toimipisteen tietoturvaopintojakson laboratorio-osuutta varten. Työssä käsitellään myös murtautumistestaukseen liittyvää teoriaa sekä eettisyyttä. Ympäristö on toteutettu käyttäen VMwaren virtualisointiohjelmistoja.

Työn teoriaosuus käsittelee itse murtautumistestausta ja sen eettisyyttä. Kappaleissa käsitellään muun muassa hakkeroinnin ja murtautumistestauksen eroja, testauksen eri tyyppejä sekä Penetration testing execution -standardin määrittelemiä vaiheita.

Käytännön osuudessa käsitellään opetusympäristön luomisessa käytettyjä ohjelmistoja, ympäristön toteutuksen aikana syntyneitä ongelmia, ympäristön virtuaalikoneita sekä niiden välistä verkkoa. Lopussa annetaan myös esimerkki ympäristön käytöstä suorittamalla yksi opintojaksolla tehdyistä laboratoriotehtävistä.

Lopputuloksena työssä on ympäristö, johon voitiin ottaa etäyhteys ja tehdä erilaisia murtautumistestaukseen liittyviä laboratoriotehtäviä siten, että ympäristöstä ei pääse haitallista liikennettä toimipisteen laboratorioverkkoon. Työn liitteinä ovat muun muassa opintojaksolle tehdyt laboratoriotehtävät.

ASIASANAT:

Murtautumistestaus, Hakkerointi, Virtualisointi, VMware

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

2014 | 54 pages

Instructor Esko Vainikka

Saku Lindroos

CREATING A PENETRATION TESTING LEARNING ENVIRONMENT

The objective of the present bachelor's thesis is to create a penetration testing learning environment for Turku University of Applied Sciences. The thesis also discusses the basics and ethics of penetration testing. The environment, which is implemented by using VMware virtualization software, can be used to teach the basics of penetration testing safely.

The theoretical part of the thesis discusses the differences between hacking and penetration testing, the ethics and the different styles of penetration testing as well as and about the standards of penetration testing.

The empirical part of the thesis discusses information about the virtualization software solutions used in implementing the environment, the problems that occurred during the process, the virtual machines in the environment and the network between them. At the end of the thesis, an example of the usage of the environment is introduced.

The result of the thesis is a working environment for teaching the basics of penetration testing safely. The environment was used successfully in the laboratory part of the information security course at Turku University of Applied Sciences in the autumn of 2013.

KEYWORDS:

Penetration testing, Hacking, Virtualization, VMware

SISÄLTÖ

1 JOHDANTO **6**

1.1 Murtautumistestaus osana tietoturvaa 6

1.2 Työn tausta 7

1.3 Työn rajaus ja tutkimusote 8

2 MURTAUTUMISTESTAUS **9**

2.1 Murtautumistestaajan ja hakkerin ero 9

2.2 Hakkerien kolme hattua 11

3 TESTAUKSEN TYYPIT JA VAIHEET **12**

3.1 Testaustyypit 12

3.2 Penetration testing execution standard 13

3.3 PTES-standardin vaiheet 13

4 OPPIMISYMPÄRISTÖ YLEISESTI **18**

5 OPPIMISYMPÄRISTÖN TOTEUTUS **21**

5.1 Oppimisympäristön ensimmäinen versio 22

5.2 Oppimisympäristön uusi rakenne 23

5.3 Oppimisympäristön hallinta 23

5.4 Virtuaalisten ESXi-palvelinten luonti 24

6 OPPIMISYMPÄRISTÖN VIRTUAALIKONEET **26**

6.1 Virtualisoidut ESXi-palvelimet 26

6.2 Kali Linux 26

6.3 pfSense 27

6.4 Kohdekoneet 27

6.5 Virtuaalikoneiden välinen verkko ja verkkoasetukset 28

7 OPPIMISYMPÄRISTÖN KÄYTTÖ **30**

7.1 Ympäristöön kirjautuminen 30

7.2 Opiskelijoiden oikeudet ympäristössä 31

7.3 Esimerkki ympäristön käytöstä 31

8 PARANNUSEHDOTUKSIA JÄRJESTELMÄÄN **35**

9 YHTEENVETO **36**

LÄHTEET **37**

LIITTEET

Liite 1. Opiskelijaympäristön verkkokuva.
Liite 2. Kirjautumisjärjestys.
Liite 3. Virtuaalikoneille annetut resurssit.
Liite 4. Opintojaksolle tehdyt laboratoriotehtävät.

KUVAT

Kuva 1. ESXin verkkoasetukset. 24
Kuva 2. PfSense verkkoasetukset. 29
Kuva 3. Kali Linux -verkkoasetukset. 29
Kuva 4. Esimerkki kirjautumisesta. 30
Kuva 5. Zenmap skannauksen tulos. 32
Kuva 6. Metasploit konsolinäkymä. 33
Kuva 7. Exploitille annettut parametrit. 34

1 JOHDANTO

Opinnäytetyön tavoitteena on rakentaa oppimisympäristö Turun ammattikorkeakoulun Lemminkäisenkadun toimipisteen tietoturvaopintojakson laboratorio-osuutta varten. Ympäristössä on tarkoitus opettaa murtautumistestauksen perusteita. Ympäristö on rakennettu käyttäen VMwaren eri ohjelmistoja.

Työssä käydään läpi murtautumistestauksen ja hakkeroinnin eroja sekä murtautumistestauksen eri tyyppejä ja vaiheita. Myöhemmissä luvuissa kerrotaan opetusympäristön rakentamisen eri vaiheista sekä pyritään selventämään sitä, miten ympäristö toimii ja mitä se sisältää.

1.1 Murtautumistestaus osana tietoturvaa

Nykyinen yhteiskunta on erittäin riippuvainen erilaisista tietoverkoista ja järjestelmistä. Tähän infrastruktuuriin kohdistuu joka päivä vakavia tietoturvauhkia, jotka vaikuttavat niin yksityisten ihmisten kuin yritystenkin toimintaan. Tällaisia uhkia aiheuttavat suurimmaksi osaksi erilaiset verkkorikolliset, joiden tavoitteena on tehdä rahaa tavalla tai toisella. Oma lukunsa erikseen ovat haktivistit, joiden tavoitteena on saada jollekin, esimerkiksi poliittisesti tärkeälle asialle huomiota. Eräs uhka on myös viime aikoina paljon puhetta herättänyt eri valtioiden suorittaman verkkovakoilun paljastuminen.

Vaikka yksi osa sodankäynnin taitoa on tuntea vihollisensa taktiikat ja toimintatavat, on myös tärkeää tuntea itsensä yhtä hyvin kuin vihollisensa. Tämä pätee myös nykytilanteessa, jossa organisaatioiden ja yksityishenkilöiden on puolustauduttava erilaisia tietoturvauhkia vastaan.

Tässä vaiheessa murtautumistestaus astuu mukaan kuvaan. Murtautumistestauksen tavoitteena on simuloida tilannetta, jossa joku ulkopuolinen taho hyökkää esimerkiksi yrityksen verkkoa tai verkkopalveluja

vastaan. Testauksen tulosten perusteella voidaan saada selville sellaisia aukkoja yrityksen tietoturvassa, joita ei muuten huomattaisi ja joita jokin pahantahtoinen taho voisi käyttää yritystä vastaan.

Murtautumistestauksesta käytetään myös termiä eettinen hakkerointi. Testauksessa käytetään usein hyvin samoja tapoja ja ohjelmistoja, joita hakkeritkin käyttäisivät. Eettisen hakkerin ja hakkerin ero onkin siinä, että eettinen hakkeri toimii aina jonkin toimeksiantajan luvalla ja pyrkii toiminnallaan parantamaan tietoturvaa. Hakkeri taas toimii yleensä jonkin pahaa tahtovan tahon palkkaamana ja pyrkii viemään yrityksiltä esimerkiksi käyttäjätietoja tai muuten aiheuttamaan tuhoa kohteelleen.

Hakkereiden käyttämien keinojen opettaminen saattaa ymmärrettävästi herättää monia eettisiä kysymyksiä. Opetetaanko esimerkiksi opiskelijoita tekemään verkkorikoksia tai muuta laitonta? Murtautumistestauksen tarkoituksena ei ole opettaa ketään verkkorikolliseksi. Tarkoituksena on antaa kuva siitä, mitä mahdollinen hyökkääjä tekisi ja auttaa ihmisiä ymmärtämään, mitä tapahtuu, kun jokin taho päättää hyökätä ja tätä kautta auttaa parantamaan esimerkiksi yritysten tietoturvakontrolleja.

1.2 Työn tausta

Opinnäytetyö sai alkunsa työharjoittelusta, jota minulle tarjottiin Turun ammattikorkeakoulun Lemminkäisenkadun toimipisteestä sen jälkeen, kun en löytänyt Turun lähialueilta paikkaa, jossa saisin työskennellä tietoturvan parissa. Harjoittelu syntyi tarpeesta saada toimipisteelle ympäristö, jossa voidaan turvallisesti opettaa syksyn 2013 tietoturvaopintojaksolla murtautumistestausta.

Itse harjoittelu eteni siten, että rakensin ympäristön, jossa opettelin kesä- ja heinäkuussa 2013 murtautumistestauksen perusteet. Tämä antoi käsityksen siitä, millaiseen tarkoitukseen ympäristö tulisi rakentaa ja mitä sen tulisi sisältää.

Tarkoituksena oli siis rakentaa murtautumistestausympäristö tietoturvaopintojakson laboratorio-osuutta varten. Ympäristössä tulee pystyä

turvallisesti opettamaan ja kokeilemaan erilaisia murtautumistestausmenetelmiä sekä ohjelmien käyttöä. Ympäristöstä ei saa päästä toimipisteen laboratorioverkkoon haitallista liikennettä tai sitä kautta ei pidä pystyä aiheuttamaan vahinkoa toimipisteen verkkolaitteille. Tämä tarkoittaa sitä, että ympäristö ei saa olla yhteydessä internetiin.

Järjestelmän suunnitteluun annettiin hyvin vapaat kädet. Muita vaatimuksia ei asetettu kuin että ympäristö on valmis ja toimii, kun opintojakso alkaa ja että sen avulla ei pysty vahingossa tai tahallaan aiheuttamaan vahinkoa järjestelmän ulkopuoliselle verkkoliikenteelle tai laitteille. Ensimmäiset ideat ympäristöstä olivat hyvin yksinkertaisia, mutta ne hylättiin jo ennen kuin niitä kokeiltiin käytännössä. Yksi ensimmäisistä suunnitelmista oli asentaa kohdekoneet virtuaalipalvelimelle siten, että hyökkäävät koneet sijaitsisivat laboratorioluokan fyysisillä tietokoneilla, mutta koko ajatus hylättiin hyvinkin nopeasti, sillä mitään liikennettä ympäristöstä ei saanut päästää ulos.

1.3 Työn rajaus ja tutkimusote

Työ on rajattu siten, että työssä ei käydä läpi esimerkiksi virtuaalikoneiden ja palvelinten asennuksia askel askeleelta, koska tällaisia opinnäytetöitä sekä ohjeita on olemassa ennestään. Työssä ei puhuta virtualisoinnin teoriasta eli lukijalta odotetaan vähintään perustason ymmärrystä virtualisoinnin periaatteista.

Työn teoriaosuus taas on rajattu niin, että siinä pyritään antamaan lukijalle yleiskuva murtautumistestauksen perusteista, eettisyydestä sekä testauksen eri tyypeistä ja vaiheista.

Työ on luonteeltaan konstruktiivinen tutkimus, johon on sovellettu toimintatutkimuksellista lähestymistapaa toimivan lopputuloksen aikaan saamiseksi.

2 MURTAUTUMISTESTAUS

Murtautumistestauksella on monta eri nimeä, joilla kuitenkin tarkoitetaan lähes samaa asiaa: pen testing, hakkerointi, eettinen hakkerointi tai white hat hacking. Murtautumistestauksessa tavoitteena on simuloida tapoja, joita mahdollinen hyökkääjä voi käyttää yrittäessään murtautua yrityksen verkkoon ja tietojärjestelmiin.

Murtautumistestaus voidaan myös määritellä lailliseksi ja luvalliseksi toiminnaksi, jonka avulla yritetään paikallistaa ja hyväksikäyttää vikoja tavoitteena tehdä järjestelmistä turvallisempia (Engebretson 2011, 1). Onnistunut murtautumistestaus päättyy siten, että testaaja on onnistunut osoittamaan, että haavoittuvuuksia on löytynyt ja niiden takia voi yritykselle koitua vahinkoa ellei asioiden korjaamiseksi tehdä jotain (Allen 2012, 9).

Yrityksissä panostetaan miljoonia erilaisiin tietoturvaratkaisuihin, jotta ne säästyisivät erilaisilta tietomurroilta ja että yritysten kriittiset tiedot pysyisivät salassa. Murtautumistestaus on yksi parhaista tavoista testata yrityksen tietojärjestelmien turvallisuutta ja havaita mahdollisia vikoja tai haavoittuvuuksia. Suomessa murtautumistestauksia suorittaa esimerkiksi Nixu. Murtautumistestaajan tavoitteena on siis luvallisesti yrittää tunkeutua yrityksen järjestelmiin ja löytää vikoja, joita mahdollinen hyökkääjä voisi hyödyntää yritystä vastaan.

2.1 Murtautumistestaajan ja hakkerin ero

Murtautumistestaajaa voidaan kutsua niin sanotuksi eettiseksi hakkeriksi. Sana hakkeri kuitenkin yhdistetään helposti rikolliseen tai laittomaan toimintaan, joten on tärkeää hieman selventää asiaa. CEH eli Certified Ethical Hacker lähestyy asiaa seuraavasti. Esimerkiksi poliisi joutuu opettelemaan rikollisten käyttämää sanastoa ja tapoja soluttautuessaan rikollisten joukkoon ja jopa tekemään lähes rikollisia asioita rikollisten kiinni saamiseksi. Eettistä hakkerointia voidaan ajatella samalla tavoin. Tietoverkon haavoittuvuuksien ja vikojen löytämiseksi

on ajateltava kuin verkkorikollinen ja käytettävä samoja tapoja kuin verkkorikolliset saattaisivat käyttää. (Walker 2011, 5.)

CEH määrittelee hakkerin ja eettisen hakkerin eron seuraavasti. Eettinen hakkeri on henkilö, joka käyttää samoja työkaluja ja tapoja, joita verkkorikollinen käyttää. Mutta eettinen hakkeri tekee kaiken työnantajan valvonnassa ja asiakkaan luvalla, tarkoituksenaan auttaa suojamaan verkkoa tai tietojärjestelmää.

Hakkeri tai verkkorikollinen taas käyttää samoja työkaluja ja tapoja esimerkiksi maksua vastaan jollekin, joka haluaa tehdä tuhoa tai viedä tietoja yrityksen tai hallitusten tietoverkoista. Nykyään hakkerointia käytetään myös aktivismin yhtenä keinona. Tällaisen ”haktivismin” tarkoituksena on saada huomiota esimerkiksi jollekin poliittisesti tärkeälle asialle. (Walker 2011, 5.)

Eettinen hakkeri siis toimii jonkun yrityksen alaisena ja haluaa olla parantamassa yritysten tietojärjestelmien ja verkkojen turvallisuutta, kun taas hakkeri toimii omillaan tai jonkun palkkaamana ja pyrkii aiheuttamaan tuhoa. (Walker 2011, 5.)

Myös verkkomaailmassa harjoitetaan siis aktivismia. Näiden ”haktivistien” tavoitteena on kaataa verkkosivuja tai palvelimia, luoda viruksia ja vain luoda epäjärjestystä verkossa tavoitteenaan tuoda esille esimerkiksi poliittisesti tärkeitä asioita ja näin saada aikaan muutosta asioihin. Yleensä haktivistit suorittavat Denial of Service -hyökkäyksiä, joiden tarkoituksena on estää pääsy johonkin palveluun kuormittamalla sitä liiallisella liikenteellä. Usein haktivistit yrittävät varastaa eri verkkopalveluista esimerkiksi käyttäjätietoja, kuten käyttäjätunnuksia ja salasanoja.

Haktivismi on lisääntynyt huomattavasti viime vuosina esimerkiksi Lähi-idän kriisin ja Pohjois-Amerikan talouskriisien myötä. Esimerkkejä haktivismista on monia, kuten vuonna 2011 tapahtunut Anonymous-ryhmän hyökkäykset MasterCardia ja maksuvälitysyhtiö PayPalia vastaan. Yhtiöt joutuivat kohteeksi, koska ne kieltäytyivät välittämästä maksuja arkaluontoisia tietoja verkkoon vuotavalle Wikileaks-sivustolle. Vaikka haktivismi pohjimmiltaan voidaan ajatella

eettiseksi toiminnaksi, tehdään sitä silti rikollisin menetelmin ja luvatta, jolloin se voidaan kategorisoida myös hakkeroinniksi. (Kanninen 2011.)

2.2 Hakkerien kolme hattua

Edellä mainittujen tapausten lisäksi IT-maailmassa hakkereita jaotellaan eri väristen ”hattujen” mukaan. Näiden hattujen avulla pyritään kuvaamaan sitä, onko hakkeri hyvä, paha vai jotain siltä väliltä.

- **White hats** eli valkohatut ovat hyviä, siis eettisiä hakkereita, jotka toimivat jonkin yrityksen palkkaamina ja pyrkivät toiminnallaan parantamaan yritysten tietoturvaa. White hat -hakkerien oletetaan toimivan vain laillisissa puitteissa eivätkä he käytä taitojaan väärin.
- **Black hats** eli mustahatut määritellään pahoiksi hakkereiksi, jotka käyttävät taitojaan joko rikolliseen toimintaan tai omaksi hyödykseen. Black hat-hakkerien tavoitteena on viedä tai tuhota tietoa ja esimerkiksi estää pääsy järjestelmään kohdistamalla siihen Denial of Service (DoS) -hyökkäys, jonka aikana esimerkiksi verkkopalvelimelle otetaan mahdollisimman monta yhtäaikaista yhteyttä, jolloin palvelin menee tukkoon tai pahimmassa tapauksessa kaatuu kokonaan.
- **Grey hats** eli harmaahatut. Grey hat -hakkerit ovat - kuten värikin kertoo - jostain valko- ja mustahattu-hakkerien välistä. Grey hat -hakkeriksi voidaan kategorisoida henkilöt, jotka lähinnä omasta mielenkiinnostaan kokeilevat hakkerointityökaluja tai sellaiset henkilöt, jotka kokevat vastuukseen paljastaa aukkoja yritysten järjestelmissä ilman yritysten lupaa. Tällaisissa tapauksissa tosin on myös kyse rikollisesta toiminnasta. Joissain tapauksissa myös haktivistit voitaisiin sisällyttää tähän ryhmään. (Walker 2011, 6.)

3 TESTAUKSEN TYYPIT JA VAIHEET

3.1 Testaustyypit

Walker (2011, 11) määrittelee CEH-teoksessaan murtautumistestaukselle kolme eri tyyppiä. Testaus voidaan toteuttaa kahdesta erilaisesta lähtökohdasta. Ensimmäinen tapa on käydä asiakasyrityksen kanssa tarkasti läpi yrityksen tietojärjestelmät sekä verkko. Tällaisessa tapauksessa voidaan jättää testauksen tiedonkeruuvaihe väliin, jolloin testaus nopeutuu. Toisessa mallissa testaajalle ei ole annettu mitään tietoja yrityksen verkoista tai tietojärjestelmistä. Tällöin testaaja joutuu itse luomaan kuvan kohteen verkosta. (Walker 2011, 11.)

Jälkimmäinen tapaus simuloi paremmin reaalimaailman tilannetta, jossa joku ulkopuolinen hyökkääjä yrittää päästä esimerkiksi yrityksen verkkoon käsiksi. Tämä tapa tosin vie enemmän aikaa kuin ensimmäinen vaihtoehto.

CEH:n mukaan kolme testaustyyppiä ovat White box, Black box ja Grey box.

- **White box** -mallissa testaajalle on saatettu antaa käyttöön esimerkiksi yrityksen verkkokaavio, yrityksessä käytettävät käyttöjärjestelmät, ip-osoitealueet tai yrityksessä käytettävät sovellukset ja niiden versiot.
- **Black box -**mallissa testaajalle ei ole annettu mitään tietoja yrityksen verkoista tai organisaatiosta ylipäänsä, vaan tarkoitus on simuloida reaalimaailman tilannetta, jossa organisaatiota vastaan yritetään hyökätä ulkoa päin.
- **Grey box -**malli pyrkii olemaan jossain kahden edellä mainitun välissä. Ero tulee siitä, että mallissa testaajalle annetaan rajallisesti tietoja yrityksestä. Tällä tavalla pystytään simuloimaan tilanne, jossa mahdollinen hyökkääjä kuuluukin jo yrityksen organisaatioon ja hänellä on pääsy osaan yrityksen verkosta. (Walker 2011, 11.)

3.2 Penetration testing execution standard

Murtautumistestaukselle on määritelty erilaisia standardeja ja toimintamalleja, esimerkiksi tässä luvussa käsiteltävä PTES-standardi (PTES 2012), NISTin Special Publication 800–115 Technical Guide to Information Security Testing and Assessment (NIST 2008) ja ISECOMin OSSTMM eli Open Source Security Testing Methodology Manual (OSSTMM 2010).

Kaikki edellä mainitut käsittelevät murtautumistestauksen prosessia ja antavat kukin oman näkemyksensä testauksen eri vaiheista ja suorittamisesta. Näistä kaikista PTES on kuitenkin malliltaan selkein ja johdonmukaisin. (Vainikka 2014.)

PTES-standardi jakaa testauksen seitsemään eri vaiheeseen. Vaiheet käydään läpi tässä järjestyksessä, ellei kyseessä ole White box -mallin mukaan suoritettava testaus, jolloin voidaan siirtyä suoraan riskianalyysin tekemiseen.

1. Pre-engament Interactions (Määrittely)
2. Intelligence Gathering (Tiedonkeruu)
3. Threat Modelling (Riskianalyysi)
4. Vulnerability Analysis (Haavoittuvuuksien kartoittaminen)
5. Exploitation (Hyökkäys)
6. Post Exploitation (Jälkihyökkäys)
7. Reporting (Raportointi).

3.3 PTES-standardin vaiheet

Määrittely

Määrittelyvaiheessa sovitaan asiakkaan kanssa, mitä testauksella halutaan saavuttaa ja asetetaan rajat sille, mikä on sallittua testauksen aikana. Lisäksi selvitetään, millaisia hyökkäyksiä voidaan käyttää, voidaanko esimerkiksi salasanoja kalastaa social engineering -tekniikoilla, onko virusten käyttö sallittua, tarvitaanko lupaa palvelun tarjoajalta suorittaa testausta verkossa tai

missä osassa asiakkaan verkkoa testausta saa tehdä. Tässä vaiheessa on myös hyvä keskustella asiakkaan kanssa, mitä hän odottaa testaukselta ja mitä testauksen aikana tulee tapahtumaan. On myös määriteltävä, testataanko esimerkiksi yrityksen fyysistä vai langatonta verkkoa, jotain verkkosovellusta tai yrityksen fyysistä tietoturvaa. Tässä työvaiheessa myös yleensä tehdään asiakkaan kanssa jonkinlainen sopimus testaamisesta ja miten siitä raportoidaan. (Kennedy ym. 2011, 2.)

Tiedonkeruu

Tiedonkeruuvaiheessa on tarkoituksena kerätä kaikki mahdollinen tieto kohteesta. Tietoa yrityksestä voidaan kerätä esimerkiksi sosiaalisten medioiden kautta tai käyttämällä Google Hacking -tapoja. Tiedonkeruun tarkoituksena on saada kuva yrityksen organisaatiosta. Kerätyn informaation avulla voidaan saada tietoa siitä, mitä kautta yrityksen tietoverkkoihin tai järjestelmiin voidaan päästä käsiksi.

Tiedonkeruun aikana on tarkoitus saada selville seuraavia asioita:

- Millaisia palomuurijärjestelmiä verkossa mahdollisesti on?
- Mitä verkkolaitteita verkossa on?
- Mitä käyttöjärjestelmiä yrityksessä käytetään?
- Mitkä ovat palvelinten ip-osoitteet?
- Onko verkkoa jaettu aliverkkoihin?
- Mitä portteja on mahdollisesti suljettu tai mitkä vastaavasti ovat avoinna?

Tässä vaiheessa käytettäviä työkaluja voivat olla esimerkiksi niin sanotut snifferit, jotka keräävät verkossa liikkuvia paketteja, portti- ja verkkoskannerit, perinteiset verkkokomennot kuten ping tai whois ja OS fingerprinting, jonka avulla saadaan käytössä olevat käyttöjärjestelmät selville. Testauksen kohteena olevan verkon kartoittamisesta käytetään asiaa hyvin kuvaavaa englanninkielistä termiä footprinting. (PTES 2012.)

Riskianalyysi

Tarkoituksena on edellisten vaiheiden perusteella luoda riskianalyysi, jonka tavoitteena on kartoittaa yritykselle tärkeimpiä kohteita, jotka ovat alttiita hyökkäyksille. Tarkoituksena on myös selvittää, millaisia hyökkäyksiä yritystä vastaan on mahdollista tehdä ja mitä kautta yritystä vastaan voitaisiin mahdollisesti hyökätä. (Kennedy ym. 2011, 3.)

Haavoittuvuuksien kartoittaminen

Haavoittuvuuksien kartoittamisen tarkoituksena on löytää mahdolliset haavoittuvuudet, joita vastaan hyökätä. Haavoittuvuuksia voivat olla esimerkiksi päivittämättömät ohjelmat, väärin konfiguroidut asetukset tai ohjelmistot tai vaihtoehtoisesti käyttöjärjestelmissä itsessään saattaa olla virheitä, joiden kautta hyökkääminen on mahdollista.

Tässä vaiheessa apuna voidaan käyttää esimerkiksi internetistä löytyviä haavoittuvuustietokantoja tai haavoittuvuuksien etsintään tarkoitettuja skannereita, kuten Nessus tai Nexpose. Täytyy myös muistaa, että koska testaaja pyrkii toimimaan kuten mahdollinen hyökkääjä, kaikki liikkeet verkossa tulee tehdä mahdollisimman huomaamattomasti. Koska palomuuri ja muut vastaavat järjestelmät huomaavat, mikäli verkossa tapahtuu outoa liikennettä, kannattaa skannaukset tehdä esimerkiksi siten, että skannaa vain pienen osan verkkoa kerrallaan. (Kennedy ym. 2011, 3; PTES 2012.)

Hyökkäys

Hyökkäysvaiheessa hyökkääjä keskittyy tunkeutumaan kohteen järjestelmiin ja testaajalla pitää myös olla selvillä verkon heikoimmat kohdat, joita vastaan on mahdollista hyökätä. Hyökkäykset tulee suorittaa vasta, kun on täysin varma, että hyökkäys tulee onnistumaan, sillä verkossa olevat palomuurit tai

antivirusjärjestelmät saattavat huomata hyökkäykset. Tämän takia hyökkäykset tulee suorittaa mahdollisimman harkitusti. (Kennedy ym. 2011, 3.)

Mikäli testauksen aikana pystytään kiertämään edellä mainitut järjestelmät, on testaus onnistunut. Juuri se, miten järjestelmät kierrettiin, on sellaista informaatiota, mitä testauksella pyritään saamaan selville. Näiden tietojen perusteella yrityksen järjestelmiä voidaan kehittää turvallisemmiksi (PTES 2012). Jos hyökkäys ei kuitenkaan onnistu, kertoo se siitä, että asiakkaan tietoturvan perusasiat ovat kunnossa. Mutta täytyy kuitenkin muistaa, että asiantuntijoiden mukaan rajattomilla resursseilla varustettu hyökkääjä pystyy tunkeutumaan mihin tahansa järjestelmään. Eli aukotonta tietoturvaa ei ole olemassa.

Jälkihyökkäys

Jälkihyökkäysvaiheeseen siirrytään, kun jokin laite on onnistuttu saamaan haltuun jonkin haavoittuvuuden avulla. Tämän jälkeen on arvioitava koneen ”arvoa” ja varmistettava, että yhteys koneeseen on pysyvä myöhempää käyttöä varten. Koneen arvo voidaan määritellä sen perusteella, mitä tietoa tai dataa kone sisältää ja voidaanko sen kautta tunkeutua syvemmälle organisaation järjestelmiin. Myös mahdollisen datan kerääminen haltuun saadulta koneelta kuuluu tähän jälkihyökkäykseen. Aineistoa kerätään ikään kuin todisteeksi asiakkaalle siitä, että hyökkäys on onnistunut. Lisäksi siitä voidaan löytää informaatiota, joka auttaa testaajaa hyökkäämään syvemmälle organisaation verkkoon. Jälkihyökkäyksen aikana on oltava varovainen ja vältettävä huomatuksi tulemista.

Tämän vaiheen aikana on kartoitettava muita mahdollisia kohteita, jotka mahdollisesti voidaan saastuttaa tai muuten saada haltuun jo kaapatun laitteen avulla. Testauksen jälkeen on koneelta viety data ja tiedostot raportoitava, palautettava tai tuhottava yrityksen kanssa sovittujen tapojen mukaan. (Kennedy ym. 2011, 3; PTES 2012.)

Raportointi

Raportointi päättää ja kokoaa yhteen koko murtautumistestausprosessin. Raportissa kerrotaan, mitä on tehty, kuinka on tehty ja tärkeimpänä, mitä korjattavia haavoittuvuuksia testauksen aikana on mahdollisesti löydetty. Raportissa on toki myös mainittava, mikäli mitään haavoittuvuuksia ei löydetty. Raportoinnin aikana on mahdollista kertoa löydöksistä organisaatiolle ja antaa neuvoja, millaisia joko teknisiä tai fyysisiä muutoksia on tehtävä turvallisuuden korjaamiseksi tai missä asioissa toimintaa voitaisiin parantaa.

On myös tärkeää kertoa, mitä mahdollisesti tapahtuu mikäli havaittuja puutteita tai vikoja ei korjata. PTES-standardi selostaa tarkasti, mitä mahdollisen raportin tulisi sisältää, joten sen sisältöä ei käydä tässä tarkemmin läpi. (Kennedy ym. 2011, 4; PTES 2012.)

4 OPPIMISYMPÄRISTÖ YLEISESTI

Järjestelmä koostuu kahdesta palvelimesta, joille kummallekin on asennettu VMware ESXi 5.1 -virtualisointiohjelmisto. Toiselle palvelimista on virtualisoitu kolme ja toiselle kaksi ESXi 5.1 -virtuaalipalvelinta. Järjestelmä on jaettu kahdelle palvelimme kuorman tasaamiseksi. Toinen palvelimista on omistettu kokonaan tälle ympäristölle ja toisella toimii myös muita toimipisteen laboratorioverkkoon ja kursseihin liittyviä koneita.

Neljässä viidestä virtualisoidusta ESXi-palvelimesta sijaitsee viisi opiskelijaympäristöä ja yhdellä kolme opiskelijaympäristöä sekä opettajalle varattu ympäristö. Opiskelijaympäristöjen määrä perustuu toimipisteen laboratorioluokan tietokoneiden määrään.

Kukin opiskelijaympäristö koostuu kuudesta virtuaalikoneesta, neljästä kohdekoneesta, joina toimivat Windows 7- ja Windows XP service pack 2 -järjestelmät sekä kaksi murtautumistestaukseen rakennettua haavoittuvaista Linux-järjestelmää, Kioptrix ja Metasploitable 2. Hyökkäävänä koneena käytetään murtautumistestaukseen rakennettua Linux-käyttöjärjestelmää nimeltä Kali Linux. Virtuaalikoneiden välistä liikennettä välittää Linux-pohjainen palomuuri pfSense (liite1).

Ympäristön kohdekoneet on valittu erilaisten testausten perusteella sekä opintojakson tarpeiden mukaan. Hyökkääväksi koneeksi testattiin myös Back Track R3 - käyttöjärjestelmää, mutta sitä testattaessa huomattiin, että käyttöjärjestelmän päivittämisen jälkeen suurin osa tarvittavista ohjelmista ei enää toiminut, jonka jälkeen päätettiin ottaa käyttöön Back Trackin tilalle kehitetty Kali Linux. pfSense valittiin siksi, että se on ilmainen, se voi toimia myös reitittimenä ja sen avulla voidaan opetella myös palomuurin peruskäyttöä opintojaksolla.

Ympäristöön kirjautuminen tapahtuu VMware vSphere Clientilla, jolla otetaan yhteys ESXi-palvelimeen sen ip-osoitteella sekä käyttäjätunnuksella ja

salasanalla. Käyttäjätunnus sekä ip-osoite määräytyvät sen mukaan, mitä laboratorio-luokan tietokonetta opiskelija käyttää (liite 2).

Ympäristön alusta

Ympäristön rakentaminen aloitettiin, kun Turun AMK:n Lemminkäisenkadun toimipisteen laboratorioverkon korjaus oli saatu valmiiksi elokuussa 2013. Tässä vaiheessa ei tiedetty muuta kuin, että ympäristöä varten on varattu yksi palvelin ja se rakennettaisiin VMwaren ohjelmistoilla. VMwaren ohjelmistot valittiin siksi, että niitä käytetään toimipisteessä opetustarkoituksiin. Itse olin opiskellut käyttämään VMwaren tuotteita, jolloin ympäristön rakentaminen sujui nopeammin, kuin jos olisi lähdetty etsimään esimerkiksi avoimen lähdekoodin ratkaisuja ja opeteltu niiden käyttöä. Jälkimmäisessä tapauksessa aikataulu olisi venynyt ja ympäristöä ei olisi saatu valmiiksi ajoissa ennen opintojakson alkua.

Kun laboratorioverkon korjaukset olivat valmiit, asennettiin palvelin paikoilleen ja tarkastettiin sen toiminta. Tämän jälkeen asennettiin palvelimelle käyttöjärjestelmäksi ESXi 5.1-virtualisointiohjelmisto, jonka päälle koko ympäristö lopulta toteutettiin.

Toteutuksessa käytetyt VMware ohjelmistot ovat VMware ESXi 5.1, VMware vSphere Client ja VMware vCenter Server.

VMware ESXi 5.1

ESXi on käyttöjärjestelmäriippumaton virtuaalikonemanageri eli hypervisor, joka mahdollistaa usean järjestelmän suorittamisen yhdeltä alustalta samaan aikaan. ESXi-järjestelmään asennettavat virtuaalikoneet käyttävät isäntäpalvelimen resursseja. Palvelimeen otetaan etäyhteys VMware vSphere Clientilla. ESXi-palvelinta on mahdollista hallita myös web-käyttöliittymällä sekä ssh-Clientilla kuten esimerkiksi PuTTYlla. ESXi-palvelimien hallintaan ja ylläpitoon voidaan käyttää myös VMware vCenteriä. Palvelimelle asennettavat koneet käyttäytyvät aivan niin kuin tavalliset tietokoneet. (Rouse 2013.)

VMware vSphere Client

vSphere Client on Windows –ohjelma, jolla otetaan etäyhteys ESXi-palvelimeen tai Virtual Center-palvelimeen. vSphere Clientia ei ole tällä hetkellä saatavana Linux käyttöjärjestelmille, mutta VMwaren mukaan se on kehitteillä myös Linux-pohjaisille järjestelmille, vaikka julkaisun ajankohdasta ei ole tietoa. vSphere Clientin asennusmedia voidaan ladata joko VMwaren omilta sivuilta tai omalta ESXi-palvelimelta. (Bipin 2012.)

VMware vCenter Server

vCenter on virtuaaliympäristöjen keskitettyyn hallintaan käytettävä sovellus. vCenter toimii välityspalvelimena siihen lisättyjen ESXi-palvelinten ja virtuaalikoneiden välillä. vCenteriä ei välttämättä tarvitse pienemmissä virtuaaliympäristöissä, joissa on vain muutamia palvelimia ja virtuaalikoneita, mutta tässä tapauksessa se on välttämätön virtuaalikoneiden ja palvelinten suurehkon määrän takia. vCenter voidaan asentaa joko Windows palvelimelle tai asentaa omana virtuaalikoneenaan jollekin virtuaaliympäristön palvelimelle. Kun palvelin on asennettu ja sille on annettu ip-osoite, siihen voidaan ottaa yhteys vSphere Clientilla, jolloin siihen voidaan lisätä ESXi-palvelimia.

Itse palvelimen hallintaan käytetään verkkokäyttöliittymää. vCenter helpottaa palvelinten hallintaa sekä mahdollistaa virtuaalikoneiden kopioimisen, virtuaalikoneiden siirtämisen ESXi-palvelinten välillä ja ajastettujen tehtävien luomisen. Se parantaa myös hälytysten ja tapahtumien hallintaa. (Davis 2010.)

5 OPPIMISYMPÄRISTÖN TOTEUTUS

Kun isäntäpalvelin oli saatu valmiiksi ja sille asennettua VMware ESXi 5.1, saattoi varsinainen ympäristön luonti alkaa. Tässä vaiheessa oli jo selvää, että jokaista toimipisteen laboratorioluokan tietokonetta kohden tultaisiin luomaan oma opiskelijaympäristö, jossa kaikki testaaminen tulisi tapahtumaan. Myös opintojakson tuleva sisältö oli suunniteltu, joten se antoi osaltaan suuntaa sille, mitä ympäristön tulisi sisältää ja mitä siellä pitäisi olla mahdollista tehdä.

Ensimmäistä versiota toteutettaessa suurimmiksi ongelmiksi muodostuivat, miten virtuaalikoneiden välinen verkko tulisi rakentaa ja miten virtuaalikoneiden asentaminen ja kopioiminen tultaisiin hoitamaan. Koska virtuaalikoneet eivät saisi olla yhteydessä toimipisteen laboratorioverkkoon ja VMware ESXi ei tarjonnut mahdollisuutta luoda tähän tarkoitukseen sopivaa verkkoa, oli keksittävä jokin muu keino välittää liikennettä koneiden välillä. Niinikään virtuaalikoneiden kopioiminen ei onnistunut suoraan VMware ESXi -palvelimella.

Koska opintojakson suunnitelmiin kuului myös palomuurin perusteiden opiskelu, päätettiin verkkoliikenteen ohjaamiseen käyttää palomuuria. Eri palomuuriratkaisujen vertailun jälkeen päädyttiin käyttämään ilmaista Linux-pohjaista pfSense palomuuria. pfSense päätettiin ottaa käyttöön siksi, että sitä käytettiin usein murtautumistestausta käsittelevässä kirjallisuudessa esimerkkinä. Myös omien testausten perusteella se osoittautui parhaaksi ratkaisuksi ominaisuuksiensa perusteella ja se oli valmiiksi käytössä toimipisteen laboratorioverkossa osoittaen näin myös toimivuutensa.

Virtuaalikoneiden kopioimiseen ja hallinnan helpottamiseksi löydettiin VMwaren tarjoama palvelu vCenter Server, joka mahdollistaa esimerkiksi koneiden suoran kopioimisen palvelimelta toiselle. Testauksen kohteeksi valikoidut koneet Windows 7, Windows XP Service Pack 2, Metasploitable 2 ja Kioptrix olivat hyvin luonnollisia valintoja. Kukin järjestelmä tarjosi mahdollisuuksia monenlaiseen testaukseen ja sopivat hyvin opintojakson sisältöön. Jokaisen

käytöstä murtautumistestauksen kohteena löytyi paljon esimerkkejä sekä kirjallisuutta, joten niiden käyttöönotto opintojaksolle oli lähes itsestäänselvyys ja kaikki sopivat opintojakson suunnitelmiin hyvin.

5.1 Oppimisympäristön ensimmäinen versio

Ensimmäinen versio ympäristöstä valmistui syyskuussa 2013 sopivasti ennen tietoturvaopintojakson alkua. Tässä vaiheessa järjestelmä koostui yhdestä ESXi-palvelimesta, jolle oli asennettu jokaista laboratorioluokan konetta kohden yksi opiskelijaympäristö, joka sisälsi tarvittavat virtuaalikoneet. Tässä vaiheessa opiskelijaympäristöjen verkko oli myös yksinkertaisempi. Kaikki virtuaalikoneet olivat yhdessä ja samassa pfSensen VLANissa eli ne toimivat kaikki samassa aliverkossa.

Kirjautuminen tapahtui vielä opiskelijoiden omilla laboratorioverkon tunnuksilla. Kun opiskelijat alkoivat yksitellen kirjautua ja avata konsolinäkymiä virtuaalikoneille huomattiin, että järjestelmä alkoi hidastua ja lopulta kirjautumaan ei päässyt kuin muutama opiskelija.

Asiaa tutkittaessa huomattiin, että ESXi-palvelimella on vain rajattu määrä muistia, jota se käyttää etäyhteyksiin. Kun muisti on kokonaan käytetty, palvelin hidastuu ja siihen ei enää pysty luomaan yhteyksiä ennen kuin osa jo avatuista yhteyksistä on suljettu. Tämä vika olisi voitu helposti havaita, kun ympäristöä ensimmäisiä kertoja testattiin ennen opintojakson alkua, mutta testattaessa ei huomattu ottaa tarpeeksi montaa yhteyttä samanaikaisesti palvelimelle.

Tämä vika toi ensimmäisen kerran esille havainnon, että VMwaren ESXi ei ehkä ole paras mahdollinen järjestelmä kyseiseen tarkoitukseen. Koska vaihtoehtoja ei ollut tässä vaiheessa opintojakson aikataulusta johtuen eikä aikaa ollut vaihtaa toiseen järjestelmään, niin VMwaren tuotteilla päätettiin jatkaa ja yrittää kiertää järjestelmän ongelma.

5.2 Oppimisympäristön uusi rakenne

Edellisessä luvussa mainitun vian takia jouduttiin koko testausympäristön alustan rakennetta miettimään uudelleen. Opiskelijaympäristöjen jakaminen suoraan kahdelle fyysiselle ESXi-palvelimelle ei olisi auttanut, sillä ei ollut mitään varmuutta siitä, että niiden muistin määrä olisi riittänyt tarpeeksi monen etäyhteyden käyttämiseen.

Pohdinnan jälkeen päätettiin järjestelmä jakaa kahdelle fyysiselle ESXi-palvelimelle ja luoda viisi virtuaalista ESXi-palvelinta, jotta muisti etäyhteyksiä varten varmasti riittäisi. Neljälle virtualisoidusta ESXi-palvelimesta sijoitettiin kullekin viisi opiskelijaympäristöä ja yhdelle sijoitettiin kolme opiskelijaympäristöä sekä ympäristö opettajaa varten. Kukin ympäristöistä sisältää samat virtuaalikoneet kuin edellä on mainittu ja niiden välistä liikennettä välittää pfSense-palomuuri.

5.3 Oppimisympäristön hallinta

Koska ympäristön palvelinten sekä virtuaalikoneiden määrä on huomattavan suuri, piti järjestelmän ylläpidon sekä toteutuksen helpottamiseksi keksiä ratkaisu: VMware tarjoaa suurten virtuaaliympäristöjen hallintaan vCenter Server välityspalvelimen. Palvelimen asennus on yksinkertaista ja siihen löytyy internetistä hyviä ja selkeitä ohjeita.

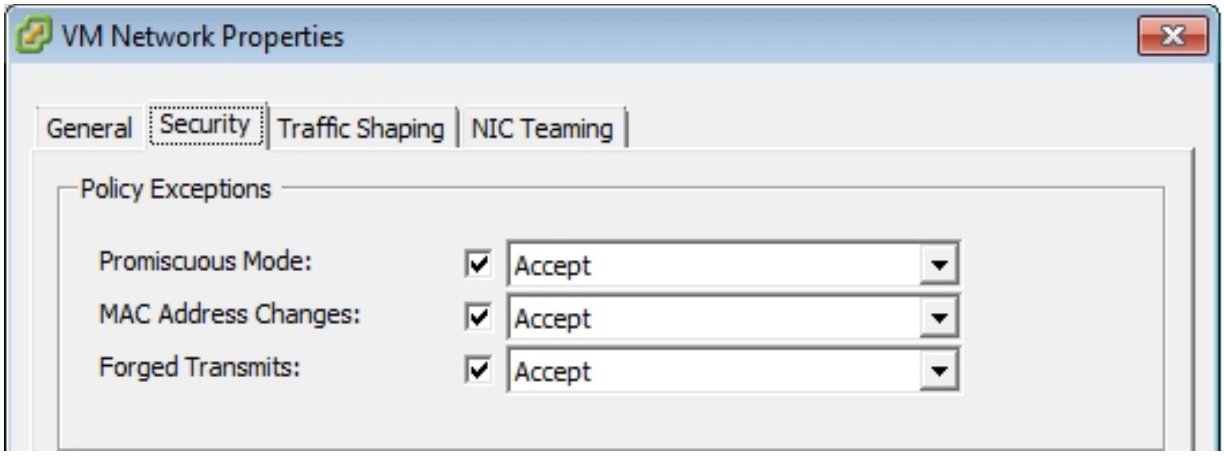
Ensimmäisenä ladataan valmis vCenter virtuaalikone VMwaren sivuilta, minkä jälkeen kone voidaan avata siltä ESXi-palvelimelta, jolle se halutaan asentaa. Tässä tapauksessa se asennettiin toiselle fyysisistä ESXi-palvelimista. Kun virtuaalikone avataan ensimmäisen kerran, pyytää se yhdistämään palvelimen verkkokäyttöliittymään internet-selaimella, jolloin ohjattu asetusten asettaminen alkaa. Kun asetukset kuten ip-osoite, pääkäyttäjän salasana, aika ja päivä ja muut vastaavat perusasetukset on asetettu, palvelin on käynnistettävä uudelleen, minkä jälkeen siihen voidaan ottaa etäyhteys vSphere Clientilla.

Kun yhteys palvelimeen on saatu lisättyä, voidaan siihen lisätä verkossa toimivat ESXi-palvelimet, jolloin kaikki palvelinten sisällä jo toimivat virtuaalikoneet tulevat myös näkyviin. Palvelimia voidaan tämän jälkeen hallita keskitetysti ottamalla yhteys vain yhteen palvelimeen monen sijasta.

vCenter tarjoaa myös paremmat mahdollisuudet koneiden liikuttamiseen ESXi-palvelinten välillä sekä mahdollistaa niiden kopioimisen palvelimelta toiselle. Tässä tapauksessa tämä nopeuttaa järjestelmän toteutuksen etenemistä sekä ylläpitoa. vCenterin asennuksen jälkeen voitiin aloittaa ympäristön uudelleen kokoaminen. Ensimmäisenä luotiin virtuaaliset ESXi-palvelimet ja tämän jälkeen kopioitiin virtuaalikoneet opiskelijaympäristöihin.

5.4 Virtuaalisten ESXi-palvelinten luonti

Kun virtuaalisten ESXi-palvelimien luonti aloitettiin, huomattiin että virtuaalisen ESXi-palvelimen luominen fyysisen ESXi-palvelimen päälle ei ollutkaan niin yksinkertaista kuin aiemmin oli ajateltu. Ennen virtuaalikoneen luontia täytyy fyysisen ESXi-palvelimen verkkoasetuksista asettaa vSwitch promiscuous -tilaan (kuva 1), joka sallii verkkoliikenteen kulkemisen fyysisen palvelimen kautta virtualisoidulle ESXi-palvelimelle sekä sieltä ulospäin.



Kuva 1. ESXin verkkoasetukset.

Kun virtuaalinen ESXi on asennettu ja sen perusasetukset kunnossa, sillä ei vielä sellaisenaan pysty käynnistämään asennettuja virtuaalikoneita vaan sen asetuksia täytyy muuttaa. Nämä muutokset voi myös tehdä suoraan virtuaalikoneen .vmx-tiedostoon:

- Sammuta virtualisoitu ESXi-palvelin.
- Valitse Edit Settings.
- Valitse Options-välilehti.
- Selaa Advanced / General / Configuration Parameters.
- Valitse lisää rivi.
- Lisää name-kohtaan teksti *monitor_control.restrict_backdoor.*
- Lisää value-kohtaan teksti *TRUE.*

Näiden muutosten jälkeen virtualisoidulle ESXi-palvelimelle voidaan asentaa ja siltä voidaan ajaa virtuaalikoneita. (Gray 2009.)

6 OPPIMISYMPÄRISTÖN VIRTUAALIKONEET

Ympäristössä on siis neljällä viidestä virtualisoidusta ESXi-palvelimesta jokaisella yhteensä 30 virtuaalikonetta ja viimeisellä yhteensä 24 virtuaalikonetta. Yhteensä koko ympäristössä on siis 150 virtuaalikonetta, kun mukaan lasketaan myös kaikki viisi virtualisoitua ESXi-palvelinta sekä VMware vCenter -palvelin. Opiskelijaympäristöjen koneet käyttävät virtualisoitujen ESXi-palvelinten resursseja, kun taas virtualisoidut ESXi-palvelimet käyttävät fyysisten isäntäpalvelinten resursseja kuten myös vCenter Server. Oppimisympäristön virtuaalikoneille jaetut resurssit on esitetty liitteessä 3.

6.1 Virtualisoidut ESXi-palvelimet

Jokaiselle virtualisoidulle ESXi-palvelimelle on annettu oma osansa isäntäpalvelimen resursseja, joita virtualisoitu ESXi-palvelin jakaa siihen asennetuille virtuaalikoneille. Kullekin virtualisoiduille ESXi-palvelimille on annettu seuraavanlaiset resurssit

- 16 Gigatavua RAM-muistia
- 2 prosessoria, joilla kummallakin 4 ydintä
- Kaksi kiintolevyä, joissa yhteensä 450 Gigatavua vapaata tilaa
- 1 verkkokortti.

6.2 Kali Linux

Kali Linux toimii ympäristössä hyökkäävänä koneena. Kali Linux on Offensive Securityn kehittämä Debian käyttöjärjestelmän pohjalle rakennettu ilmainen murtautumistestaukseen tarkoitettu käyttöjärjestelmä. Käyttöjärjestelmän edeltäjä on myös Linux-pohjainen Back Track. Järjestelmä on rakennettu yksinomaan murtautumistestaustarkoituksiin ja sisältää vakiona yli 300 erilaista murtautumistestaukseen tarvittavaa työvälinettä ja ohjelmistoa, näistä esimerkeinä nmap - verkkoskanneri, Hydra online -salasanacrackeri, John

offline -salasanacrackeri, aircrack-ng langattomien verkkojen testaukseen, Metasploit framework, Burbsuite verkkosovellusten testaukseen sekä Wireshark-verkkoprotokolla-analysaattori. (Bajpai 2013.)

6.3 pfSense

pfSense on Linux-pohjainen avoimen lähdekoodin palomuuri sekä reititin, joka perustuu FreeBSD-käyttöjärjestelmään. Järjestelmän kehitys on aloitettu vuonna 2004, pfSensen versio 1.0 on julkaistu vuonna 2006 ja viimeisin versio 2.1 julkaistiin 15. syyskuuta 2013. pfSenseä voidaan käyttää palomuurina, reitittimenä, langattoman verkon tukipisteenä, DHCP-palvelimena, DNS-palvelimena tai VPN-päätepisteenä. Tässä tapauksessa PfSense valittiin juuri palomuuri- ja reititinominaisuuksiensa takia. (PfSense.org 2014; PfSense 2014.)

6.4 Kohdekoneet

Windows 7

Windows 7:n valinta yhdeksi kohdekoneeksi oli hyvin luonnollinen ja itsestään selvä, sillä se on yksi maailman käytetyimmistä käyttöjärjestelmistä ja monelle tuttu, joten sen käyttö testauksen kohteena on varmasti monelle mielenkiintoista ja opettavaa. Kone on konfiguroitu siten, että sen palomuuri on asetettu pois päältä, jotta erilaisten haavoittuvuuksien kokeileminen olisi mahdollista, käyttöjärjestelmää ei ole päivitetty ja siihen on myös konfiguroitu huolimattomasti FTP-palvelin päälle, jotta kohteesta saataisiin entistä haavoittuvaisempi.

Windows XP Service Pack 2

Windows XP valittiin yhdeksi kohteeksi lähinnä sen perusteella, että sitä käytettiin jo aiemmalla tietoturvaopintojaksolla murtautumistestauksen

kohteena. Virtuaalikone oli jo valmiiksi tehtynä, joten se oli helppo ottaa käyttöön ympäristöön. Koneen asetuksia on konfiguroitu hyvin samoilla tavoilla kuin Windows 7-koneen asetuksia. Koneen palomuuri on asetettu pois päältä sekä koneelle on asetettu FTP-palvelin päälle samoin kuin web-palvelin, jotta järjestelmästä saadaan mahdollisimman haavoittuva.

Metasploitable 2

Metasploitable 2 on tarkoituksella haavoittuvaiseksi luotu Linux-käyttöjärjestelmä. Virtuaalikone on suoraan ladattavissa internetistä, minkä jälkeen se voidaan avata ja käyttää sitä testaamiseen. (Metasploit unleashed 2014.)

Kioptrix level 1

Kioptrix on Metasploitablen tapaan tarkoituksella haavoittuvaiseksi rakennettu Linux-käyttöjärjestelmä. Kioptrixista on saatavilla yhteensä neljä eri versiota, joista jokainen on toistaan hieman haastavampi. Virtuaalikoneet voidaan ladata valmiina suoraan internetistä, minkä jälkeen ne voidaan avata virtuaalisointiohjelmistolla. (Kioptrix blog 2014.)

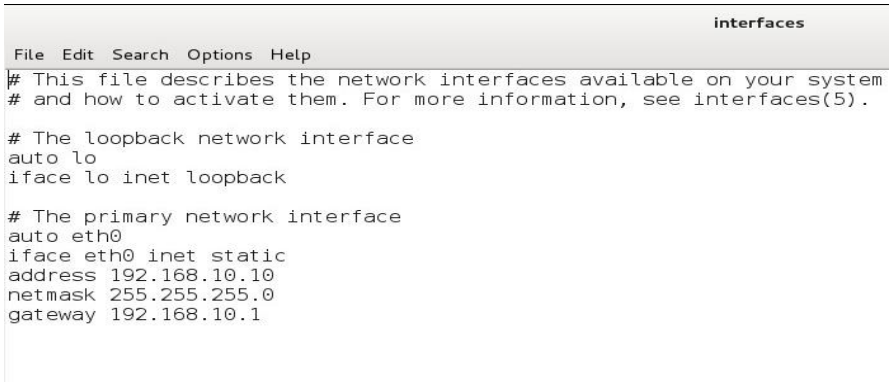
6.5 Virtuaalikoneiden välinen verkko ja verkkoasetukset

Virtuaalikoneiden välinen verkko oli yksi suurimmista ongelmista työn alkuvaiheessa, sillä VMware ESXi ei tarjoa mahdollisuutta Host-only-tyylisen verkon luomiseen. Tämä taas tässä tapauksessa oli ainut vaihtoehto, koska piti saada jokaiselle oppilaalle oma ympäristönsä ja liikennettä ei saanut päästää testausympäristön ulkopuolelle. Opiskelijaympäristöissä on siis jokaisessa oma verkko, jolloin vain sen ympäristön koneet pystyvät kommunikoimaan keskenään.

pfSense-palomuurissa on asetettu DHCP-palvelin päälle ja se jakaa osoitteita kohdekoneille. Palomuurin säännöt on asetettu siten, että se sallii kaiken liikenteen muurin läpi. Palomuurille on annettu kaksi verkkokorttia, joista toiseen on yhdistetty kohdekoneet ja toiseen Kali Linux (kuva 2).

Kuva 2. PfSensen verkkoasetukset.

Kali Linuxin verkkoasetuksia on muutettu siten, että sille on annettu staattinen ip-osoite, jotta se pystyy kommunikoimaan kohteena olevien koneiden kanssa palomuurin läpi (kuva 3). Windows-koneisiin on asetettu staattiset ip-osoitteet, jolloin ne eivät pääse vaihtumaan ja ne ovat jokaisessa opiskelijaympäristössä samat. Linux-kohdekoneet ovat valmiiksi konfiguroituja ja asennettuja virtuaalikoneita, joten niiden ip-osoitteet on asetettu staattisiksi pfSensen DHCP-asetusten kautta.

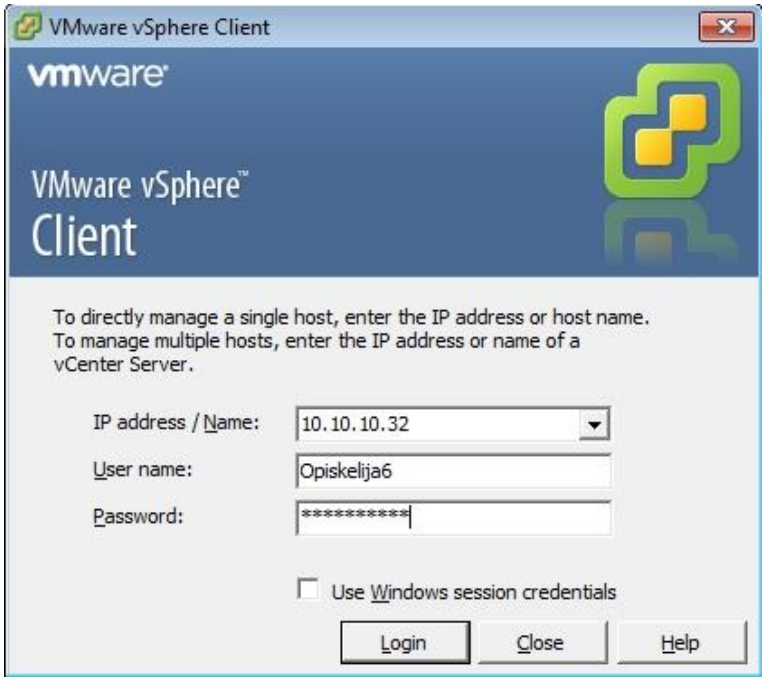


Kuva 3. Kali Linux -verkkoasetukset.

7 OPPIMISYMPÄRISTÖN KÄYTTÖ

7.1 Ympäristöön kirjautuminen

Ympäristöön kirjautuminen tapahtuu ottamalla etäyhteys ESXi-palvelimeen: opiskelijat siis eivät ota yhteyttä vCenter-palvelimeen vaan virtuaalisoituihin ESXi-palvelimiin (kuva 4). Se, mihin palvelimeen ja millä käyttäjätunnuksella opiskelija kirjautuu, määräytyy sen mukaan, millä laboratorioluokan tietokoneella tämä istuu (kuva kirjautumisjärjestyksestä liitteessä 2). Oppilaille luotiin yhteiset tunnukset, koska VMwaren järjestelmät eivät anna mahdollisuutta esimerkiksi Active Directory -tunnusten tehokkaaseen hyödyntämiseen, jolloin tunnusten ylläpito olisi todella vaivalloista. Kun opiskelija on kirjautunut, näkee hän vain oman ympäristönsä koneet.



Kuva 4. Esimerkki kirjautumisesta.

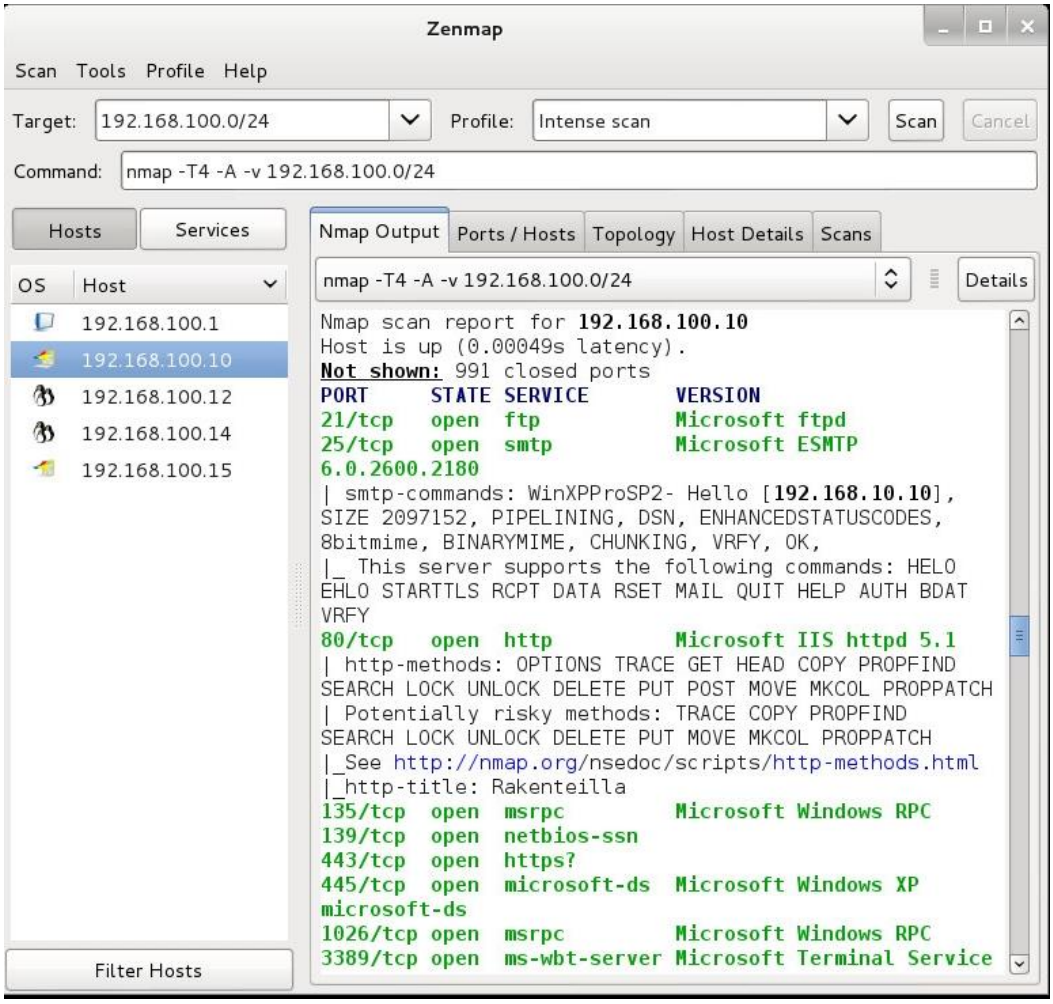
7.2 Opiskelijoiden oikeudet ympäristössä

Opiskelijoiden oikeuksia on rajoitettu siten, että heillä on oikeudet vain avata ja sulkea virtuaalikoneita. Oppilaat eivät pysty tekemään muutoksia virtuaalikoneiden resursseihin. He pystyvät kuitenkin toimimaan virtuaalikoneiden sisällä vapaasti ja tekemään muutoksia niihin, jolloin on tärkeää muistuttaa opiskelijoita siitä, että ympäristö tulee käytön jälkeen siistiä ja jättää entiselleen, jotta seuraavan käyttäjän on helppo aloittaa ympäristön käyttö.

7.3 Esimerkki ympäristön käytöstä

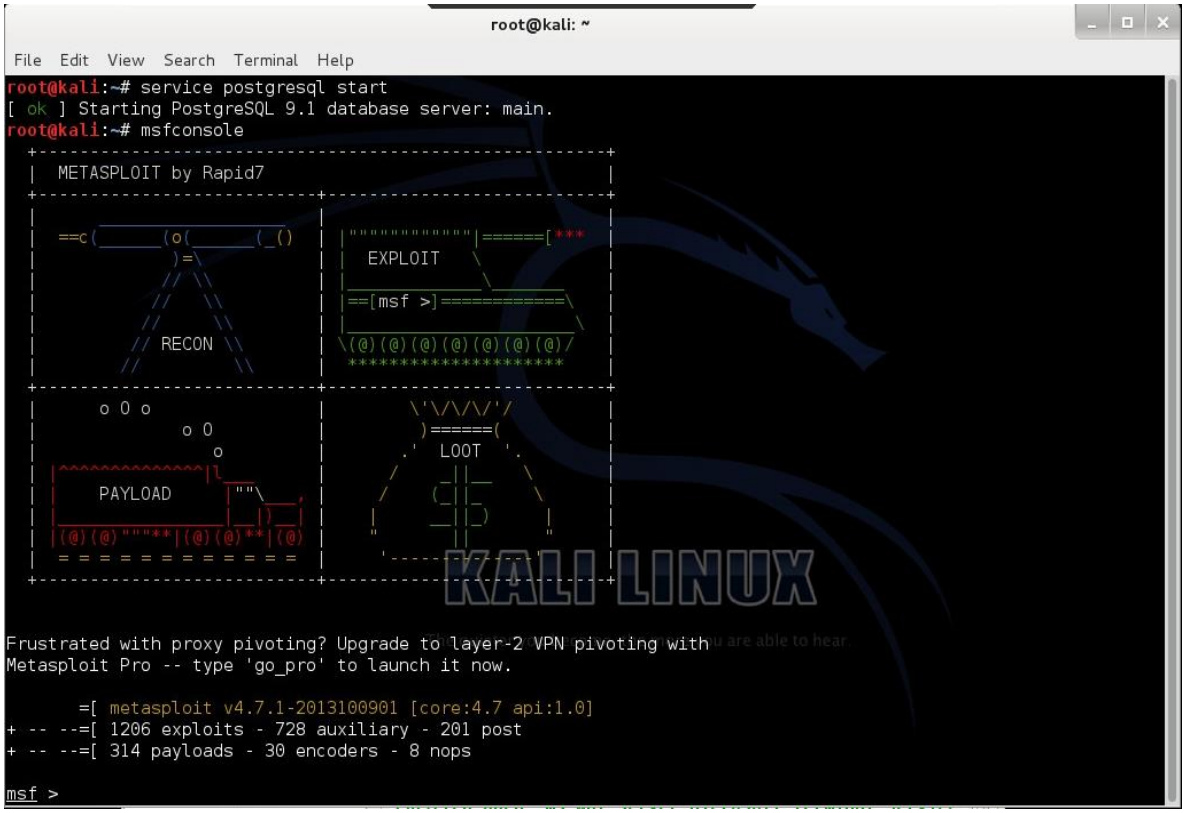
Tässä luvussa käytetään esimerkkinä yhtä tietoturvaopintojaksolla tehdyistä laboratoriotehtävistä. Kaikki tehtävät on esitetty liitteessä 4. Tehtävän tarkoituksena on käyttää Windows XP:n haavoittuvuutta hyväksi siten, että se avaa etäyhteyden hyökkääjän koneeseen, jolloin hyökkääjä voi esimerkiksi asentaa kohdekoneelle haittaohjelmia tai viedä sieltä tiedostoja.

Ensimmäiseksi kirjaudutaan sisään ympäristöön, avataan Kali Linux-virtuaalikone ja skannataan verkkoympäristö ja avoimet portit käyttäen nmap-tai zenmap-sovellusta (kuva 5). Skannauksen jälkeen tiedetään kohdekoneen ip-osoite sekä kohteessa olevat avoimet portit. Näiden tietojen avulla voidaan siirtyä seuraavaan vaiheeseen eli itse hyökkäämiseen.



Kuva 5. Zenmap-skannauksen tulos.

Tehtävässä käsketään käyttää Metasploit frameworkia hyökkäyksessä. Metasploitista on myös luotu graafinen käyttöliittymä nimeltään Armitage, mutta tehtävässä käsketään käyttämään tekstipohjaista versiota, joten käytetään sitä. Ennen kuin voidaan käynnistää Metasploit, on sen tietokanta käynnistettävä komennolla ”service postgresql start”. Itse Metasploit käynnistetään komennolla ”msfconsole”(kuva 6).



Kuva 6. Metasploit konsolinäkymä.

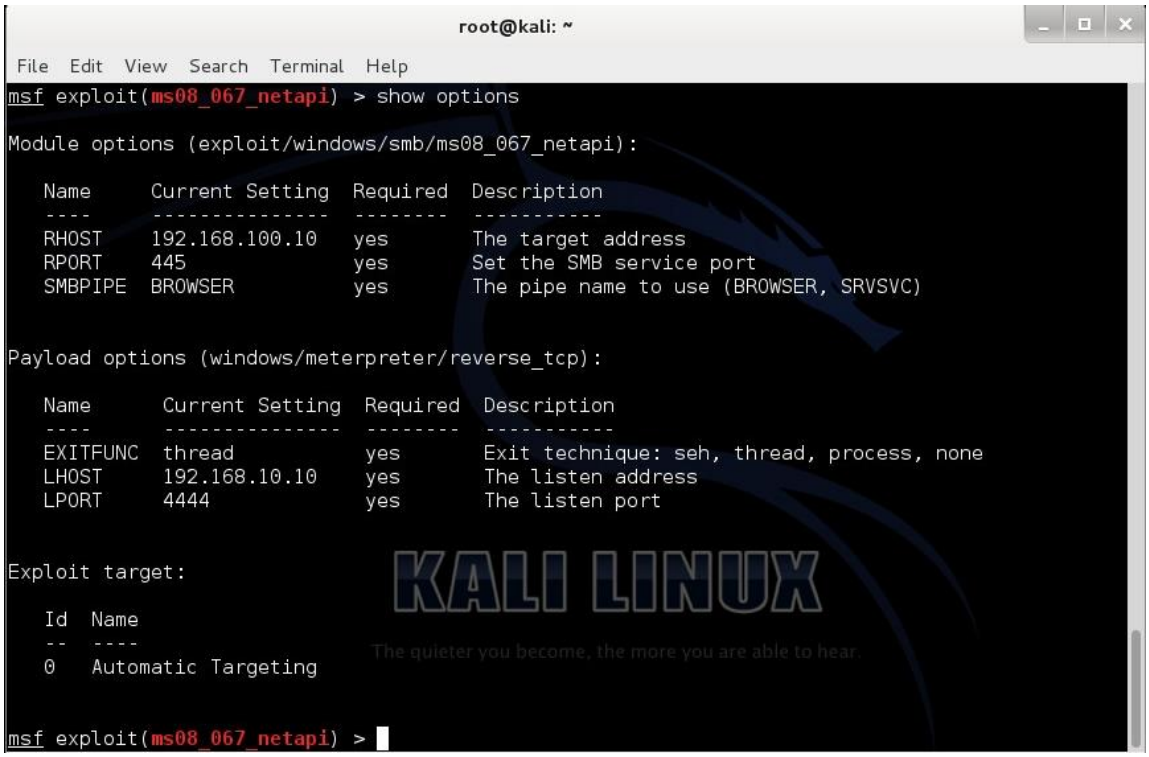
Tehtävässä oppilasta pyydetään etsimään internetistä ohjeita Metasploitin käytöstä ja selvittämään tunnettuja haavoittuvuuksia, joita tehtävässä voitaisiin käyttää hyödyksi.

Tässä tapauksessa tiedetään, mitä ollaan tekemässä, joten seuraavaksi valitaan käytettävä exploit. Tiedossa on, että exploit ms08_067_netapi toimii, joten ohjelmalle täytyy antaa komento ”use exploit/windows/smb/ms08_067_netapi”, jolloin exploit otetaan käyttöön.

Seuraavaksi ohjelmalle on annettava payload eli se, mitä haavoittuvuudesta viedään sisälle kohdekoneeseen. Tässä tapauksessa halutaan, että ohjelma avaa kohdekoneelta meterpreter-session, jolloin kohdekone on hyökkääjän hallussa. Payload asetetaan komennolla ”set PAYLOAD windows/meterpreter/reverce_tcp”.

Tämän jälkeen ohjelmalle on annettava vielä hyökkäävän koneen ip-osoite, jolloin ohjelma osaa yhdistää meterpreter-session takaisin hyökkääjälle. Samoin

on annettava tietysti kohdekoneen ip-osoite, jotta ohjelma osaa hyökätä oikeaan paikkaan. Ip-osoitteet asetetaan komennoilla ”set LHOST hyökkäävän koneen osoite ” ja ”set RHOST kohdekoneen ip-osoite” (kuva 7).



Kuva 7. Exploitille annetut parametrit.

Tämän jälkeen ohjelmalle annetaan komento ”exploit”, minkä jälkeen ohjelma käynnistää hyökkäyksen. Mikäli hyökkäys on onnistunut, avaa ohjelma meterpreter-session, jolloin kohde on hyökkääjän käytettävissä. Tämän jälkeen voidaan esimerkiksi ottaa kuvakaappaus kohdekoneesta, tallentaa näppäinten painallukset, ladata tiedostoja tai viedä tiedostoja kohdekoneelle.

Tehtävässä käsketään avata etätyöpöytä-sessio kohdekoneelle. Meterpreterissä on skripti, joka mahdollistaa etätyöpöytäyhteyden ottamisen kohdekoneelle. Skriptin ajamiseksi annetaan komento ”run getgui –e”. Kun skripti on ajanut itsensä, pitäisi etätyöpöytäyhteyden ottamisen onnistua konsolikomennolla ”rdekstop ip-osoite, johon halutaan yhdistää”. Kun etätyöpöytäyhteys on luotu onnistuneesti, tehtävä päättyy.

8 PARANNUSEHDOTUKSIA JÄRJESTELMÄÄN

Kuten aikaisemmin on mainittu, oppimisympäristön rakenne on todella monimutkainen ja hankala. Kun nyt katsoo taaksepäin ympäristön rakentamista, olisi sen suunnitteluun ja testaukseen voinut käyttää enemmän aikaa ja vaivaa sekä tutkia muitakin virtualisointiohjelmistoja.

VMware-järjestelmien monet puutteet ja viat tekivät ajoittain rakentamisesta todella haastavaa. VMwaren lisenssien määrä ympäristössä on huomattavan suuri, koska jokainen ESXi ja vCenter tarvitsevat omansa. Ympäristön ylläpidettävyys on todella kehno ja muutosten tekeminen vaatii paljon aikaa ja työtä.

Opiskelijoiden kirjautumiseen voisi yrittää luoda paremman tavan esimerkiksi laboratorioverkon Active Directory-tunnuksilla. Ympäristöjen reititys on vikaherkkää, koska reititystä hoitaa pelkästään palomuuri, joten sitä tulisi parantaa.

Ympäristön rakentamista jollain muilla virtualisointijärjestelmillä voitaisiin tutkia, jotta saataisiin selville, toisiko jokin toinen järjestelmä helpotusta lisenssi- ja ylläpito-ongelmiin. Ympäristöön voisi esimerkiksi asentaa palvelimia testauksen kohteeksi pelkkien yksittäisten järjestelmien sijasta.

Testausympäristöjen verkkoa voitaisiin monimutkaistaa siten, että verkossa olisi esimerkiksi palvelimia ja useampia palomuureja ja vain kaksi itse kohdetta. Tällaisista verkoista on esimerkkejä murtautumistestausta käsittelevässä kirjallisuudessa useampiakin. Verkon muuttaminen lisäisi todennäköisesti vaihtelevuutta ja johdonmukaisuutta opintojaksollekin.

Ympäristössä ei harjoiteta tällä hetkellä minkäänlaista verkkosovellusten tai -sivujen testaamista, joka on kuitenkin yksi tärkeä osa murtautumistestausta. Tähän pitäisi myös keksiä jokin ratkaisu, samoin langattomien verkkojen testaamiseksi tulisi kehittää jokin parempi ratkaisu.

9 YHTEENVETO

Opinnäytetyön tavoitteena oli toteuttaa opetus- ja oppimisympäristö toimipisteen tietoturvaopintojakson laboratorio–osuuteen sekä kertoa murtautumistestauksen perusteista. Työ painottuu kuitenkin suurimmaksi osaksi käytännön osuuteen, jossa kerrotaan muun muassa murtautumistestausympäristön rakenteesta, verkosta sekä virtuaalikoneista.

Työ oli alkujaan haastava, koska itselläni ei ollut mitään tietoa murtautumistestauksesta tai vastaavien virtuaaliympäristöjen toteuttamisesta. Ongelmia järjestelmää luodessa tuli vastaan lähes päivittäin. Ongelmia muodostui niin VMwaren ohjelmistojen, laitteiston kuin ympäristön verkon kanssa.

Ympäristössä on edelleen paljon vikoja, joita olisi voitu korjata jo opintojakson aikana ja pystyttäisiin edelleen korjaamaan. Täytyy ottaa huomioon myös se, että tällaisia järjestelmiä ei ilmeisesti ole kovin monia rakennettu, ainakaan kokonaan virtualisoituna.

Rakentamassani järjestelmässä siis on joitain vikoja, jotka vaatisivat korjausta ja uudelleen konfigurointia, mutta monista vioistaan huolimatta sillä saatiin opintojakso vietyä läpi ilman suurempia ongelmia ja se täytti näin tehtävänsä. Kokonaisuutena työ oli todella opettava kokemus.

Työn kautta pääsin tutustumaan tietoturvaan syvemmin ja sain samalla itse opetella murtautumistestausta sekä virtualisointia. Työtä tehdessäni sain varmistuksen myös sille, että haluan jatkossa olla tekemisissä tietoturvan kanssa ja saada myös uran siltä alueelta.

Vaikka ympäristöä ei tällaisenaan säilytettäisikään, olen silti tyytyväinen ja ylpeä siitä, että sain sen kaikista ongelmista ja vioista huolimatta rakennettua siihen pisteeseen, että sitä voitiin käyttää opettamiseen ja tiedon levittämiseen tietoturvan ja murtautumistestauksen tärkeydestä.

LÄHTEET

Allen, L. 2012, Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide. Birginham, Packt Publishing Ltd.

Bajpai, P. 2013. InDepth Review of the Kali Linux: A Hackser's Bliss. Pentest Magazine Extra: Kali Linux 2.

Bipin. 2012. Difference between vSphere, ESXI and Vcenter. Viitattu 17.2.2014 http://www.mustbegeek.com/difference-between-vSphere-ESXi-and-vcenter/.

Davis, D. 2010. What is VMware vCenter Server. Viitattu 17.2.2014 http://searchvmware.techtarget.com/What-is-VMware-vCenter-Server.

Engebretson, P. 2011, The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. New York, Syngress.

Gray, E. 2009. Vcritical 18.5. VMware ESX 4 can even virtualize itselft. Viitattu 20.2.2014 http://www.vcritical.com/2009/05/vmware-esx-4-can-even-virtualize-itself/.

Kanninen, T. 2011. Haktivismi räjähti käsiin "Haluavat nolata ja vaikuttaa. It-viikko. Viitattu 3.3.2014. http://www.itviikko.fi/tietoturva/2011/06/16/haktivismi-rajahti-kasiin---haluavat-nolata-ja-vaikuttaa/20118514/7.

Kennedy, D; O'Gorman, J; Kears, D & Aharoni, M. 2011, Metasploit: The Penetration Tester's Guide. San Francisco, No starch Press, Inc.

Kioptrix blog 2014. Test-page. Viitattu 21.2.2014. http://www.kioptrix.com/blog/test-page/.

Metasploit unleashed. Metasploitable. 2014. Viitattu 21.2.2014. http://www.offensive-security.com/metasploit-unleashed/Metasploitable.

NIST 2008. Technical Guide to Information Security Testing and Assessment. Viitattu 3.3.2014. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

OSSTMM 2010. Open Source Security Testing Methodology Manual. Viitattu 3.3.2014. http://www.isecom.org/research/osstmm.html.

PfSense.org 2014. About pfSense. Viitattu 20.2.2014 https://www.pfSense.org/about-pfSense/index.html.

PTES 2012. Penetration testing execution standard. Viitattu 5.3.2014. http://www.pentest-standard.org.

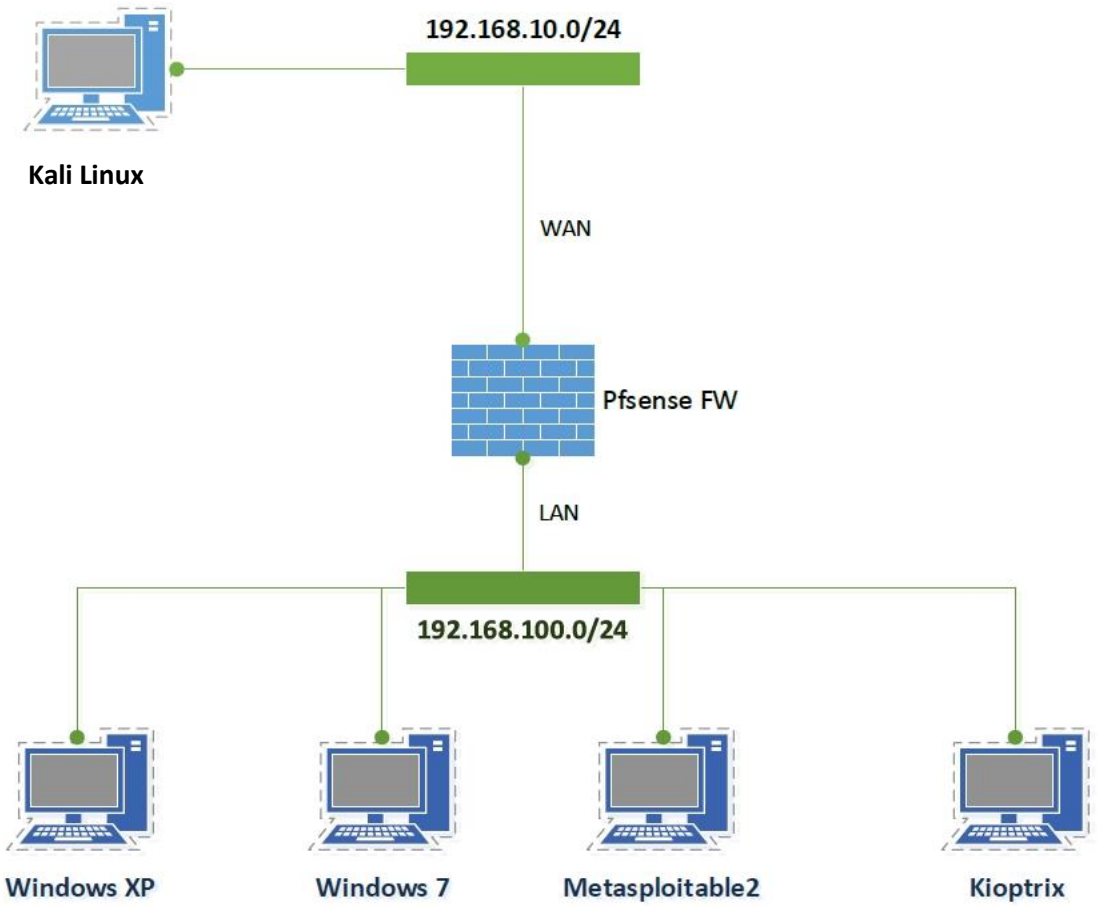
Rouse, M. 2013. Definition Vmware ESXI. Viitattu 17.2.2014 http://searchvmware.techtarget.com/definition/VMware-ESXi.

Vainikka, E. 2014. Murtautumistestaus – mitä se tarkoittaa ja miksi sitä tarvitaan. Teoksessa Paavola, J. (toim.) Näkökulmia tietoturvaan 2. Ajatuksia tietoturvasta. Turku: Turun Ammattikorkeakoulu, 16-26.

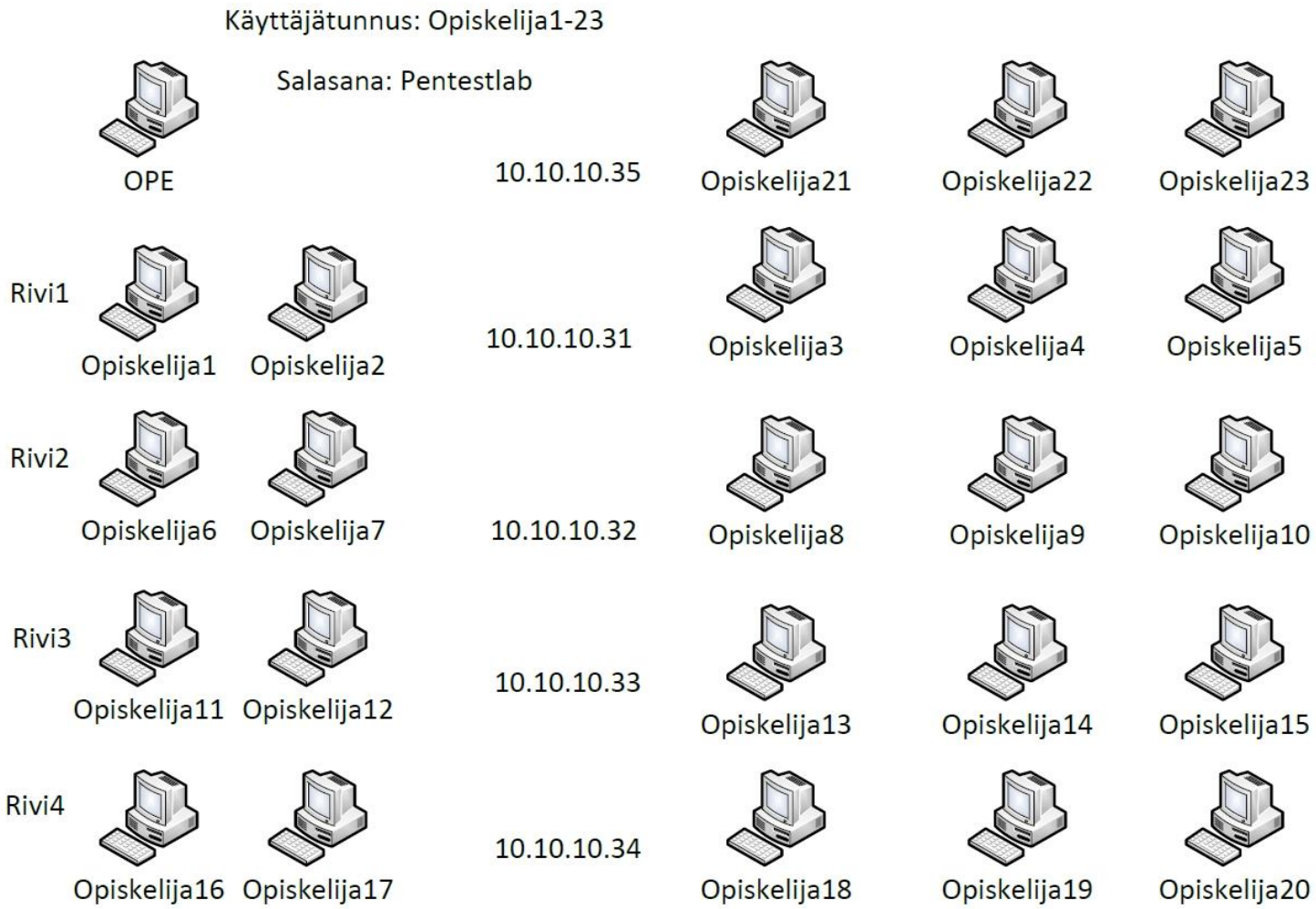
Walker, W. 2011, CEH Certified Ethical Hacker All-in-One Exam Guide. New York, McGraw-Hill.

Wikipedia pfSense. 2014. Wikipedia. Viitattu 20.2.2014. http://en.wikipedia.org/wiki/PfSense

Opiskelijaympäristön verkkokuva



Kirjautumisjärjestys



Virtuaalikoneille annetut resurssit

	RAM-muisti	Prosessoriytimien määrä	Kiintolevy tilaa	Verkkokorttien määrä
Kali Linux	1 Gigatavua	2	30 Gigatavua	1
pfSense	256 Megatavua	1	2 Gigatavua	2
Windows 7	2 Gigatavua	2	25 Gigatavua	1
Windows XP	256 Megatavua	1	8 Gigatavua	1
Metasploitable 2	512 Megatavua	1	8 Gigatavua	1
Kioptrix	64 Megatavua	1	3 Gigatavua	1

Opintojaksolle tehdyt laboratoriotehtävät

Lab work 1

1. Log in the environment by using VMware vSphere Client and your credentials
   - Your username is 8 characters long; the 1st character is the 1st letter from your First Name, and the other characters are the letters from your Family Name starting from the beginning (lower case letters)
   - Your password is your student number

2. Check what kind of working environment you have (it is located in a virtualized environment). Turn on the virtual machines if needed

3. Find out what kind of meaning the systems in your environment might have (e.g. use the web and the names of the systems)

4. Familiarize yourself with Kali Linux and look at its tools (e.g. use Kali Linux's web page and the suitable virtual machine) and walk around the toolset. Try to recognize how the toolset is organized

Note! The username for Kali Linux is root and the password is toor!

Note! You can also check the content of BackTrack 5 R3 toolset but we don't use that distribution.

5. What is the TCP/IP address of your Kali Linux virtual machine? Find it out from your Kali Linux system!
6. Check what are the TCP/IP addresses of the machines in your working environment (e.g. use nmap or zenmap or some other suitable tool)

Note! The TCP/IP addresses are in the range 192.168.100.10 - 20

7. Perhaps the teacher/assistant will show some example of how to use tools

Lab work 2

1. Check what kind of working environment you have (it is located in a virtualized environment). Turn on the virtual machines if needed.

2. What is the TCP/IP address of your Kali Linux virtual machine? Find it out from your Kali Linux system!

Note! The username for Kali Linux is root and the password is toor!

3. Check what are the TCP/IP addresses of the machines in your working environment (e.g. use nmap or zenmap or some other suitable tool).

4. nmap/zenmap
   - Familiarize yourself with different nmap options by using zenmap and nmap. nmap's web page (www.nmap.org) might also be useful (especially the page http://nmap.org/data/nmap.usage.txt).
   - Conduct different types of scanning in your working environment

5. Ettercap
   - Look for information about the tool ettercap and clarify to yourself its purpose

6. Wireshark
   - Familiarize yourself with Wireshark network sniffer by using it. Scan the network traffic between your Kali Linux virtual machine and a suitable target system (e.g. some web page in the internet). Try to understand the results of the scanning.
   - Wireshark's web page (www.wireshark.org) can be a quite useful place to visit.

Lab work 3

Note: We use only Kali Linux in this lab!

1. The teacher will show some examples of the usage of Wireshark network sniffer

2. Scan your working environment by using nmap or zenmap. Save the result of your scanning

3. The teacher assistant will present the features and the usage of Pfsense firewall

4. Log-in your Pfsense virtual machine and get yourself familiar with it (username = admin, password = PentestAdmin)

5. Adjust the firewall rules for the LAN interface so that some of the ports previously open will be closed **(Note: Do not touch the rules of the WAN interface!)**

6. Scan your working environment again (save the result again with different name than previously)

7. Compare the results so that you can verify that your firewall rules are working

8. **Before you finish your working remember to restore the original firewall rules!**

Lab work 4

1. Scan your working environment by using nmap/zenmap and save the scanning result (remember where you saved that)

2. Create the following firewall rules into your Pfsense firewall's **LAN interface** it (username = admin, password = PentestAdmin)
   - Block all other network traffic into your Kioptrix and Metasploitable 2 machines except traffic to TCP port 80
   - Block all network traffic into your Windows 7 machine
   - Allow all network traffic into and from your Windows XP machine

3. Check that your firewall rules are working by using again nmap/zenmap and compare the scanning result with the previous (task 1) one

4. Familiarize yourself with the usage of Armitage and try to exploit the vulnerabilities of Windows XP machine

Before you finish your working remember to restore the original firewall rules!

Lab work 5

Password attacks

In this week's laboratory work you are **not allowed** to use the Windows machines on the environment everything must be done via network connection. If you have any troubles ask Google or teacher to help.

1. Use Hydra in your Kali Linux machine to initiate a dictionary attack against Windows XP machine and gain it's admin accounts password

    - Use the password list **rockyou.txt** located at /usr/share/wordlists/
    - How can you tell which port and service to use?

2. Do the same to your Windows 7 machine but this time you must use Hydras graphical interface xHydra

    - How can you test that the password works if you don't have access to the physical computer?

3. When you have found out the passwords use an appropriate application to establish a connection to the windows XP and 7 machines and try to find some interesting files and download then to your computer

4. When you have found and downloaded a file try to open it and see what it contains!

Lab work 6

Exploiting windows XP SP2

In this week's laboratory work you learn how to use metasploit framework to exploit windows XP and how to use meterpreter to control the exploited machine.

1. Start your Kali Linux and Windows XP virtual machines if they are not already running.

2. Search internet for guides, tips etc. about how to use metasploit framework and meterpreter if you have never used them before. You also need to find known exploit to use against windows XP

3. When you have studied your findings use metasploit framework to exploit your windows XP virtual machine (use the command line NOT Armitage)
   - Remember to start metasploits database before you start working with metasploit! (metasploit uses postgresql)
   - Use payload that opens a meterpreter connection
   - Make sure that you have set your options right. You can see the options the exploit and payload needs by using the command "show options"

4. When you have exploited the windows XP machines vulnerability and have a meterpreter session open use a meterpreter script to enable remote desktop connections to your windows XP machine.
   - Use internet to find out the script and its commands!

5. Open a remote desktop connection to your windows XP machine.
   - Open a new terminal window and use command rdesktop <ip address>
   - Use the account and password you found in last week's laboratory work.

6. When you have tested that you are able to connect to your windows Xp machine use the meterpreter scripts command to clean your tracks

Lab work 7

Scanning with Nessus and using the information to exploit Metasploitable2

In this week's laboratory you learn how to use Nessus vulnerability scanner to search information and vulnerabilities in your network environment.

1. First you need to start Nessus services in kali Linux with command "service nessusd start"
    - Command starts Nessus server in your local machine

2. Next you need to use iceweasel to connect to the Nessus user interface.
    - The address is https://localhost:8834
    - Username and password "opiskelija/opiskelija"

3. When you have logged in launch a scan against your Metasploitable 2 machine
    - Use the "internal network scan" template in your scan
    - You need to know your Metasploitable 2 virtual machines ip address!

4. When your scan is ready use the information you have gained to exploit and gain access to your Metasploitable machine
    - Use command line version of metasploit for exploiting!
    - Can you find some other way besides exploiting for gaining access to the metasploit machine?

5. When you are done delete your scan results from Nessus!

Lab work 8

Social engineering toolkit

In this week's laboratory work you learn to use the Social engineering toolkit. You need to create a website that has malicious code embedded in it. All the things done in SET can also be done in metasploit framework. The toolkit just makes things a bit simpler.

1. Start your SET from Applications -> Kali Linux -> Exploitation tools -> Social engineering toolkit

2. When you have started SET take some time to look up information and guides from internet about how use SET

3. When you feel that you are ready try to make a fake website that contains some malicious code that establishes a meterpreter session to your victim machine in this case windows XP.

   - Tip: use metasploit browser exploit method, use a web template and metasploit browser autopwn

4. When you have created the web site login to your windows XP machine (password sysadmin1) and use IE to navigate to your website you just created and see if you have a meterpreter session open in metasploit.

5. If you have time left try to do the same as above but this time use msfconsole.

Lab work 9

This week we start penetration testing wireless networks. We start our testing with the most basic authentication methods. First task is to find out a hidden ssid (the wireless networks "name"). Today's second task is fool wireless access points mac address filter by spoofing an allowed mac address.

1. Start Kali Linux in your **local machine with VMware workstation**

   - You may have to download the virtual machine from our network storage

2. Make sure that you have your Wireless LAN Adapter connected to your virtual machine

   - Use either command iwconfig or ifconfig. You should see a wireless network interface.
   - If you don't see a network interface use command **ifconfig wlan0 up**

3. Next we need to set our network adapter in monitor mode with command **airmon-ng start wlan0 (or wlan1)**
   - After this you should see network interface called mon0

4. Now start Wireshark and select mon0 interface. What kind of traffic you can see?

   - You should see a buffalo device that doesn't show ssid in its broadcast packets and lots packets that were are not interested in

5. Next we need to start monitoring wireless connections in our area. For this we use tool named airodump-ng

   - When you have started the program let it scan for a minute then stop it with ctrl+c

6. You should see an open wireless network with no ssid, that's our target.

   - We need to start sniffing the traffic in our target network. For this we need to use **airodump-ng.**
   - You need to know the wireless access points mac address and channel. You also need to set name for the capture file
   - Use - -help to find out the commands and options

7. When you have started the sniffer we need to send deauthentication packets to the network so all the connected clients disconnect and re-connect back to the access point. For this we use **aireplay-ng**. You can use aireplay-ng - -help command to see what options you need.

8. After this you can use wireshark to open the capture file we created in stage 6. When you go through the packets you should see the deauthentication packets and most important the packets that shows the ssid

9. Now when you have found out the ssid try connect to the access point

MAC spoofing

1. First we need to see if there are any clients connected to the access point so we can spoof its mac address. So we need to use airodump-ng to see if there are any clients connected to the access point and what its mac-address is.

2. When you see the client connected to the access point we need to copy its mac address and spoof it whit a tool called macchanger

   - Before we can spoof the address we have to stop our wireless interface with command **ifconfig wlan0 down**
   - Now we can change our wireless interfaces mac address with **macchanger**. Use macchanger --help to find out the right options

3. Now use command **ifconfig wlan0 up** and try to connect to the access point.

4. After you are done with this week's work delete the capture files you have created and use command **service networking restart** to reset all network settings

Lab work 10

Last week we started testing with wireless networks and bypassed two basic wlan authentication methods. Today we crack open WEP and WPA2 –PSK

Cracking WEP encryption

1. Start Kali Linux in your **local machine with VMware workstation**
   - You may have to download the virtual machine from our network storage (ip- address \\10.100.0.100\)

2. Make sure that you have your Wireless LAN Adapter connected to your virtual machine
   - Use either command iwconfig or ifconfig. You should see a wireless network interface.
   - Sometimes you need to disconnect and connect your wireless adapter from your virtual machine to get it working right

3. Next we need to put our network adapter in monitor mode with command **airmon-ng start** '**wlan interface**'
   - After this you should see network interface called mon0

4. Next we need to start monitoring wireless connections in our area. For this we use tool named **airodump-ng**

5. You should see a wireless network named **Pentest_Wep**.
   - We need to start sniffing and capturing traffic in the wireless network
   - You need to know the wireless access points mac address and channel. You also need to set name for the capture file
   - Use - -help to find out the commands and options

6. To crack the wep encryption we need to capture about 5000 or more packets from the target. We can capture some arp packets and send them back to the network to generate all the traffic we need
   - To generate traffic you have to use aireplay's "standard ARP-request replay" module
   - You need to know the access point's mac-address also you should see a client connected to the access point we also need to spoof that.

7. When you have sent enough packets you can stop airodump and aireplay with ctrl+c

8. Now you can try to crack the encryption with command **“aircrack-ng yourcapturefile.cap”**

Cracking wpa2-psk using dictionary attack

1. Set your wlan interface to monitor mode if you already haven’t

2. Use airodump-ng to monitor wireless networks. You should see a network called **Pentest_WPA2**. We need to **capture** packets going in and out of this networks to crack the password

3. When you monitor the network you should see a client connected to it. We have to force client to disconnect and reconnect or wait for someone to connect to the network.
   - To get client to disconnect from the network you have to send deauthentication packets to the network using **aireplay-ng.** Use command **aireplay-ng - -help** to see the commands

4. After you have sent the deauthentication packets you can stop your airodump capture.
   - After you have sent the packets airodump should indicate in the top right cornet that it has captured a **WPA handshake** packet

5. Now we can start our cracking proses.
   - You may have to unzip the password file called “rockyou.txt”. Go to **usr/share/wordlists/** and see if you have to unzip the file first. Use command **gzip –d** to unzip the file.

6. Now when you have unzipped the password file we can use aircrack to crack the password file.
   - Use command **aircrack-ng ‘yourcapturefile’ -w /usr/share/wordlists/rockyou.txt** and see if you are able to crack the password

Lab work 11

In the past two weeks we have tested and cracked the most basic authentication methods and passwords for wireless networks. Now it's time to test if we have learned anything.

1. Start virtual machine called **Wlan_kali** in your **local machine with VMware workstation**
   - You may have to download the virtual machine from our network storage (address \\10.100.0.100)

2. When you have gotten your wireless adapter working in your virtual machine you should see a wireless network named **Pentest-WPA2**

3. Teacher has set up a wireless network but has forgotten the password and if there were any other authentication methods configured.
   - Your task is to find out the password and test if there is any other authentication methods configured
   - The task is over after you have successfully connected to the network

Lab work 12

Exploiting Windows 7 and privilege escalation

For our last task we are exploiting windows 7 through vulnerability in Mozilla Firefox and try raising our user privileges so that we are the “root” user and can enable remote desktop connections to our target machine.

1. Login to our test environment with vSphere client (the login instructions can be found in optima)

2. Make sure that your kali Linux and our target machine **Windows 7** are powered up

3. So our todays target is **Windows 7**. To get a meterpreter connection to our target we must use metasploit

4. Search the internet for metasploit module called **Mozilla Firefox Bootstrapped Add-on** and research information about how it works and how to use it

5. When you have studied the module open metasploit and configure it correctly so that you have a webserver running in your kali Linux

6. When you have configured the module open your windows 7 machine (password q2wertyu) and use Firefox to connect to your server and install the add-on the browser asks you to install

7. You should get a meterpreter connection after you have agreed to install the add-on

8. When you have a meterpreter connection open to your target use command **getsystem** to escalate your user privileges. After that use command **getuid** to make sure you are SYSTEM user

9. After that run meterpreter script **getgui** to enable remote desktop connections on our target machine. If the script runs successfully you should be able to open a remote desktop connections to your target

10. You can test this by opening a new terminal and by using command rdesktop (win7 ip address)