LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

# Microsoft Azuren soveltuvuus kyberturvallisuuden harjoitteluympäristönä

Purhonen, Teemu

2017 Laurea

Laurea-ammattikorkeakoulu
LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

# Microsoft Azuren soveltuvuus kyberturvallisuuden harjoitteluympäristönä

Teemu Purhonen
Tietojenkäsittely
Opinnäytetyö
Toukokuu, 2017

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Tietojenkäsittely koulutusohjelma
Tradenomi

Teemu Purhonen

**Microsoft Azuren soveltuvuus kyberturvallisuuden harjoitteluympäristönä**

Vuosi 2017 Sivumäärä 43

Laurea-ammattikorkeakoululla on suunnitteilla integroida käytännön harjoituksia kyberturvallisuutta käsitteleville kursseille. Tämän opinnäytetyön tavoitteena on testata Microsoft Azuren soveltuvuutta harjoitusympäristöksi ammattikorkeakoulun opiskelijoille. Toimeksiantajana on Laurea-ammattikorkeakoulu, mutta viime kädessä tästä työstä on eniten hyötyä opiskelijoille.

Ensimmäiseksi luon Azureen valmiin ympäristön ja testaan sitä neljällä kyberturvallisuutta käsittelevällä harjoituksella. Luon ensimmäisen testiversion harjoituksesta mahdollisimman nopeasti, minkä jälkeen sitä voidaan tarpeen mukaan muokata testauksesta saadun tuloksen perusteella.

Konfiguroin Azureen neljä virtuaalitietokonetta. Virtuaalitietokoneiden käyttöjärjestelminä on Windows Server 2012 R2 ja Windows Server 2008 R2 SP1. Yksi tietokoneista on alusta, jossa harjoitukset tehdään ja muut ovat harjoituksen kohteena.

Azure sopii tähän tarkoitukseen todella hyvin. Se on hyvin monipuolinen ympäristö, joka tarjoaa lukuisia eri vaihtoehtoja harjoitusten kohteeksi ja hyökkäyksien alustaksi. Opiskelijan näkökulmasta ympäristön käyttöönotto käy nopeasti ja helposti.

Jotta Azure kannattaa ottaa käyttöön Laurea-ammattikorkeakoulussa, on sitä mielestäni syytä testata lisää. Rakentamalla Azureen kokonaisen IT-infrastruktuurin harjoituksen kohteeksi, mikä simuloi oikeaa yritystä, Laurea voi saada paremman hyödyn Azuresta.

Asiasanat: Azure, kyberturvallisuus, Laurea, pilvipalvelu

**Laurea University of Applied Sciences** **Abstract**
Degree Programme in Bachelor of Business Administrator
Bachelor's Thesis

Teemu Purhonen

**Microsoft Azures suitability for practise environment in cybersecurity**

Year 2017 Pages 43

Laurea University of Applied Sciences are planning to integrate practical exercises into cybersecurity courses. The purpose of this thesis is to test the suitability of Microsoft Azure as a training environment for students. The commissioner is Laurea University of Applied Sciences but ultimately this is most beneficial for students.

First I will create an environment in Azure and test it with four cybersecurity exercises.
I will create the first test version of the exercise as soon as possible after which it can be modified as necessary, based on the results of test.

I configure four virtual machines to Azure. The operating systems for the virtual machines are Windows Server 2012 R2 and Windows Server 2008 R2 SP1. One of the virtual machines is the computer that is used to perform the exercise, and other machines are targets.

Azure suits well for this purpose. It is a very versatile environment that offers a wide variety of options for practise targets and platforms where attacks can be operated. From the perspective of the student, the access to the environment is quick and easy.

To Azure to be used at the Laurea University of Applied Sciences, I think it should be tested more. By building a legitimate IT infrastructure, which simulates life business to Azure, Laurea can get better benefit from it.

Keywords: Azure, cybersecurity, Laurea, cloud computing

Sisällys

Käsitteet ja lyhenteet

| | |
|---|---|
| Domain | Ryhmä tietokoneita ja laitteita, mitkä ovat määritelty samoilla säännöillä ja asetuksilla |
| HDD | Kiintolevy jota käytetään tietokoneen massamuistina, mihin tallennetaan ohjelmat ja tiedostot |
| Linux | Linus Torvaldsin kehittämä avoimen lähdekoodin käyttöliittymä tietokonelaitteille |
| Mac OS | Applen kehittämä käyttöliittymä |
| Optima | Virtuaalinen oppimisympäristö, joka toimii verkkoselaimella |
| Oracle VM VirtualBox | Käyttöjärjestelmien virtualisointiin tarkoitettu ohjelma |
| Palvelin | Tietokone joka suorittaa palvelinohjelmistoa ja tarjoaa palveluita muille saman verkon tietokoneille |
| Penetraatiotestaus | Järjestelmän testausta tietoturva-aukkojen varalta |
| Pilvipalvelu | Tietokonejärjestelmä tai -ohjelmiston fyysiset laitteet on ulkoistettu ja ne ovat käytössä Internetin kautta |
| Remote Desktop Protocol | Protokolla joka määrittelee yhteyden toiselta tietokoneelta toiseen tietokoneeseen |
| Ryhmäkäytänne | Hallinnoidaan samaan verkkoon kuuluvien tietokoneiden ja käyttäjien asetuksia |
| SSD | Tietokoneen massamuisti, jossa ei ole liikkuvia osia |
| SQL tietokanta | Tietokanta joka on rakennettu IBM:n kehittämällä kyselykielellä |
| Topologia | Tietokoneverkon perusrakenne, joka kuvaa miten tietokoneet ja laitteet ovat kytkettynä toisiinsa |
| Virtuaalitietokone | Tietokone joka on emulointi tietokonejärjestelmästä tai tietokone jota käytetään oman tietokoneen käyttöjärjestelmän sisällä |

# 1 Johdanto

Laurea Leppävaarassa on mahdollista suorittaa useita opintojaksoja, jotka käsittelevät tietoturvaa ja kyberturvallisuutta. Opintojaksot Systems Security, Enterprise Application Security ja Network Security käsittelevät kyberturvallisuutta ja valmentavat opiskelijoita alan ammattilaisiksi. Opintojaksot ovat suunniteltu niin, että kurssin suorittaneilla olisi valmiudet suorittavat sertifikaatit SCCP – System Security Certified Practitioner ja CEH – Certified Ethical Hacking. Molemmat sertifikaateista ovat arvostettuja tietoturva-alalla. Opintojaksojen toteutus on täysin virtuaalinen. Opintojaksojen materiaali koostuu verkossa olevista videoista ja opiskelijoiden itse keräämästä materiaalista.

Virtuaaliopiskelu muodostaa suurimman osan koko opintojakson materiaalista. Yhden oppitunnin suorittaminen kestää yleensä noin kaksi tuntia. Verkko-oppitunteihin on sisällytetty muutamia tehtäviä, jotka ovat yleensä monivalintakysymyksiä. Verkko-oppituntien läpipääsyyn vaaditaan, että opiskelija katsoo kaikki videot ja vastaa kaikkiin kysymyksiin. Opiskeluun sisältyy myös omaa pohdintaa. Opiskelijat kirjoittavat tuntien aiheista oppimispäiväkirjaan.

Oppituntien aiheet saattavat olla usein hyvinkin teknisiä ja videoissa kerrotaan muun muassa, miten hakkeri toteuttaa hyökkäyksensä tai miten suoritetaan yrityksen penetraatiotestaus. Opintojaksoilla opiskelijat eivät ole kuitenkaan itse päässeet toteuttamaan kursseilla opittuja asioita. Monet opiskelijat, kuten minä itsekkin, ovat toivoneet kurssin lopussa, että olisivat halunneet kokeilla videoissa opetettuja taitoja käytännössä, eivätkä vain katsoa niistä videoita.

## 1.1 Tavoite

Aikaisemmin mainituista opintojaksoista Network Security on opintojakso, jossa tullaan ensimmäisenä kokeilemaan käytännön harjoituksia. Opintojakso Network Securityn yhtenä tavoitteena on, että opintojaksolle osallistuvilla opiskelijoilla on hyvät valmiudet kehittävät itseään suorittamalla asioita käytännössä ja täten heillä olisi hyvät valmiudet kehittyä tietoturvallisuuden ammattilaisiksi.

Harjoituksien avulla oppilaat saavat yhden oppimiskeinon lisää, kun he pääsevät itse kokeilemaan tekniikoita, joista opetusvideoissa puhutaan. Tämän opinnäytetyön tarkoituksena on tutkia, miten Microsoftin julkinen pilvipalvelu Microsoft Azure soveltuu kyberturvallisuuden oppimisympäristöksi opiskelijoille.

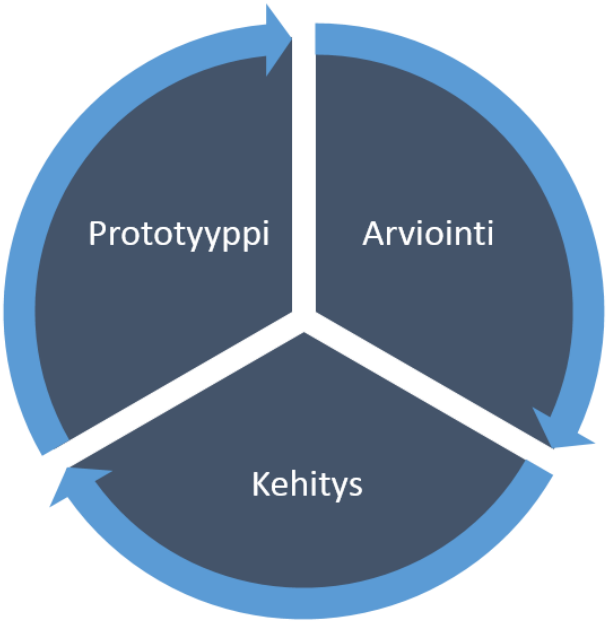
Testaan Azurea luomalla sinne testiympäristön, joka mahdollistaa neljän kyberturvallisuuteen liittyvän harjoituksen toteuttamisen. Harjoituksien luomisen lisäksi kerron yleisesti mikä Azure on ja analysoin sen soveltuvuutta tähän tarkoitukseen yleisellä tasolla sekä erikseen jokaisen harjoituksen kohdalla. Luomalla testiympäristö Azureen saadaan hyvä kuva Azuren toiminnasta ja mahdollisuuksista.

# 2 Tutkimusmenetelmä

Tässä opinnäytetyössä tutkimusmenetelmänä on käytetty menetelmää The rapid prototyping process. Tutkimusmenetelmän ideana on saada aikaan mahdollisimman nopeasti ensimmäinen raakaversio työstä, vaikka versio olisikin todella alkeellinen. Etu tämänkaltaisessa menetelmässä on se, että saadaan mahdollisimman nopeasti ensimmäinen palaute asiakkaalta. Tämän nopeasti saadun palautteen perusteella työn skaalaa voidaan tarvittaessa tarkentaa tai jopa täysin muuttaa. (Cerejo 2010)

## 2.1 Tutkimuksen rakenne

Tutkimusmenetelmässä on kolme vaihetta, jotka toistuvat. Nämä vaiheet ovat prototyyppi, arviointi ja kehitys. Ensimmäisessä vaiheessa suunnitellaan prototyyppi eli koekappale tai mallityyppi aiheesta. Arviointi -vaiheessa koekappaletta testataan ja kehitys -vaiheessa koekappaletta kehitetään arvioinnista saadun palautteen perusteella. Tämän jälkeen tehdään uusi koekappale. Tämä kolmen vaiheen kierto jatkuu niin kauan, kunnes kaikki osapuolet ovat tyytyväisiä koekappaleeseen.



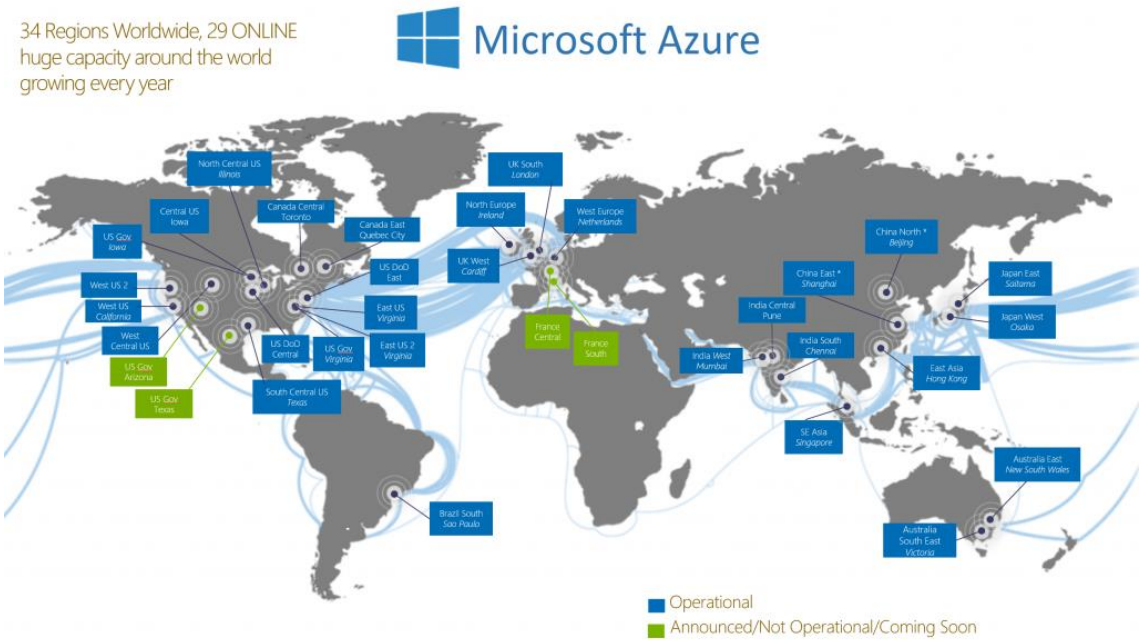

Kuvio 1: The rapid prototyping process (Cerejo 2010)

# 3 Microsoft Azure

Microsoft ilmoitti vuonna 2008 julkaisevansa pilvilaskenta -palvelun nimeltä Windows Azure ja se julkaistiin kaksi vuotta myöhemmin vuonna 2010. Myöhemmin vuonna 2014 palvelun nimeksi vaihdettiin Microsoft Azure. Azurea voidaan käyttää virtuaalipalvelinten alustana ja kehitysalustana. (Chappel 2008; Martin 2014)

## 3.1 Tietokeskukset

Microsoft Azure sisältää ison kokoelman eri palveluita, joita IT -alan ammattilaiset ja kehittäjät voivat käyttää työssään. Pilvipalvelut pyörivät Microsoftin hallinnoimissa tietokeskuksissa ympäri maailmaa. Azure mahdollistaa hyvin paljon eri vaihtoehtoja eri tarpeille tarjonnan monipuolisuuden ja hinnoittelupolitiikkansa ansiosta. (Poppelgaard 2017)




Kuvio 2: Azuren tietokeskukset (Poppelgaard 2017)

## 3.2 Palvelumuodot

Microsoft Azure tarjoaa käyttäjilleen SaaS (software as a service), PaaS (platform as a service) ja IaaS (infrastructure as a service) palveluita. Microsoft Azure -käyttäjä voi luoda muun muassa virtuaalitietokoneita ja SQL -tietokantoja. Eri virtuaalitietokoneita Azuressa on lukuisia. Perinteisiä Windows palvelimia on esimerkiksi Windows Server 2008 R2 SP1, Windows Server 2012 R2 ja Windows Server 2016 Datacenter. Azure tarjoaa myös lukuisia eri Linux -palvelimia, esimerkiksi Ubuntu Server 16.04 LTS ja SQL Server vNext on Red Hat.

### 3.2.1 SaaS

Perinteisesti sovelluksia on hankittu lisenssipohjaisesti. Software as a service tarkoittaa, että sovellus hankitaan palveluna. Tässä tapauksessa sovellusta ei edes asenneta laitteelle vaan se on käytössä palveluntarjoajan ylläpitämällä palvelimella. Käyttäjällä ei ole tässä mitään vastuuta siitä, toimiiko palvelu vai ei. Kaikki vastuu on palveluntarjoajalla. (Mikä on Saas?)

### 3.2.2 PaaS

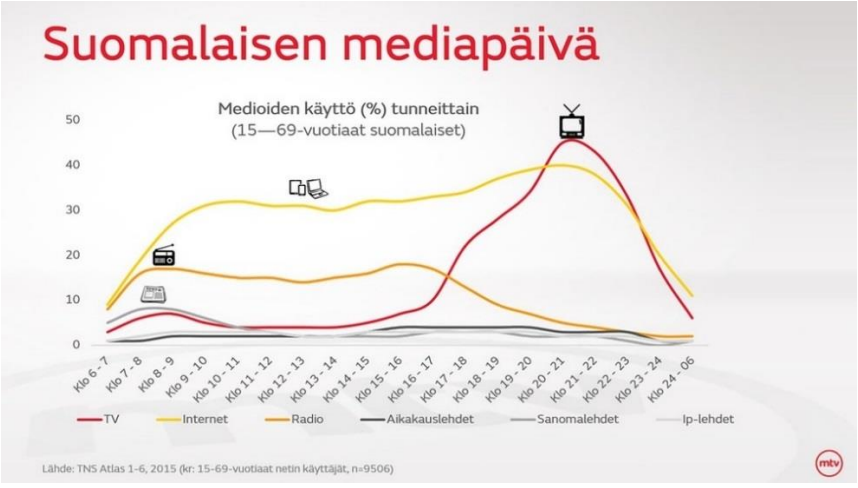
Platform as a service tarjoaa valmiin kehitys ja käyttöönottoympäristön. PaaS voi olla esimerkiksi yksi pilveen asennettu virtuaalitietokone, jota voi verrata kaupasta ostettuun normaaliin kannettavaan tietokoneeseen. Toisaalta PaaS voi olla myös täysin valmiiksi asennettu ja konfiguroitu virtuaalitietokone, mihin on asennettu kaikki mahdolliset sovellukset ja lisäosat, joilla yritys voi suorittaa toisen yrityksen penetraatiotestauksen. (Ahonen 2014)

### 3.2.3 IaaS

Infrastructure as a service tarjoaa valmiin laskentainfrastruktuurin asiakkaalle pilvipalveluna. Infrastruktuurin tarjoajan vastuulle kuuluvat palvelimet, tietoverkko, palomuuri ja tietokeskukset. (What is IaaS? 2017)

## 3.3 Hinnoittelu

Azuressa käyttäjä maksaa vain siitä, mitä hän käyttää. Yhtäkään Azuren tuotetta tai palvelua ei voi ostaa kerralla, vaan kaikesta maksetaan käytön mukaan (€/tunti). Tämä mahdollistaa esimerkiksi sen, että pienet yritykset voivat ajaa palvelimensa ja nettisivunsa alas esimerkiksi yön ajaksi alentaakseen kuluja. Yöllä kävijöitä on yleensä harvemmin kuin päivällä, joten sillä ei ole suurta vaikutusta yrityksen liiketoimintaan tai sen asiakkaisiin. (Azure pricing 2017; Tutkittu: Fagerström 2015)




Kuvio 3: Suomalaisen mediapäivä (Fagerström 2015)

Hinnoittelun ansiosta Azure sopii hyvin myös oppilaitoksille. Oppilaitoksilla harvoin on tarvetta pitää palveluita jatkuvasti yllä, koska esimerkiksi Laurea-ammattikorkeakoulussa tunnit sijoittuvat kello 09:00 ja kello 15:00 välille. Azuressa on myös ominaisuus, jolla virtuaalitietokoneelle voi luoda tarkat ajat, milloin se menee itsestään päälle ja sammuttaa itsensä.

### 3.4 Saatavuuskokoelmat

Microsoft markkinoi Azurea globaalina, luotettavana ja hybridinä pilvipalveluna, jota se todella on. Microsoftin, kuten kaikkien tietojärjestelmiä tuottavien yritysten, pitää välillä päivittää ja huoltaa järjestelmäänsä. Tämä saattaa vaikuttaa käyttäjän virtuaalitietokoneeseen tai muuhun palveluun.

Azuren palvelutasosopimuksen mukaan käyttäjän palvelu voi olla alhaalla 0,05%:n ajan kuukaudesta eli noin 45 minuuttia ennen kuin Microsoftin tarvitsee hyvittää sitä taloudellisesti. Jos käyttäjä kuitenkin luo palveluilleen ”Availability setin”, palvelutasosopimuksen mukaan, palvelu saa olla alhaalla vain 0,01%:n ajan eli noin yhdeksän minuuttia kuukaudessa. Eli jos käyttäjällä on useita virtuaalitietokoneita, hän voi luoda niille tämän saatavuuskokoelman, jolloin Microsoftin huollon tai päivityksen yhteydessä, tähän yhteen kokoelmaan kuuluvat virtuaalitietokoneet eivät voi kaikki olla alhaalla yhtä aikaa. Mikäli palvelu on kuukauden sisällä alhaalla enemmän kuin yhdeksän minuuttia, Microsoft on taloudellisesti velvollinen korvaamaan alhaalla olevan palvelun aiheuttamat seuraukset. (Foulds, Squillace, Wang & Zemault 2017; Smith 2015)

## 4 Azure oppimisympäristönä

Microsoft Azureen pystyy halutessaan rakentamaan täysiverisen IT-infrastruktuurin, jolla melkein mikä tahansa yritys pärjää. Kokonainen konesali kaikkine eri palvelimineen voidaan korvata Microsoftin pilvipalvelulla. Tässä työssä ei kuitenkaan ole tarkoituksena luoda isoa kokonaisuutta. Tässä harjoitustyössä samaan verkkoon on pystyttävä luomaan muutamia virtuaalitietokoneita, joiden on pystyttävä kommunikoimaan keskenään ja virtuaalitietokoneeseen tulee pystyä asentamaan muiden kuin Microsoftin omia sovelluksia.

Azure harjoitteluympäristönä mahdollistaa sen, että oppilaiden ei tarvitse itse asentaa mitään kolmannen osapuolen sovelluksia omalle tietokoneelleen. Kaikki on heti valmiina opiskelijaa varten ja hänen tarvitsee vain suorittaa annettu tehtävä. Luomalla itse oman ympäristön opintojakson ohjaajat voivat tarvittaessa myös rajoittaa opiskelijoiden oikeuksia virtuaaliympäristössä esimerkiksi hallitsemalla ryhmäkäytänteitä.

## 4.1 Oppimisympäristön eristäminen

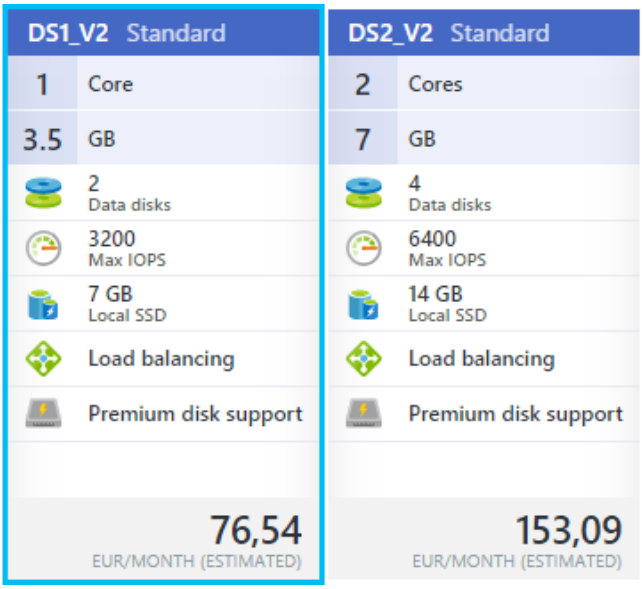
Pilvipalveluna Azure mahdollistaa sen, että harjoitushyökkäys voidaan toteuttaa ilman sitä vaaraa, että laki olisi esteenä. Osa harjoituksista voi olla vähintäänkin epäeettisiä tai jopa laittomia. Suorittamalla harjoitushyökkäyksen oikeaan kohteeseen opiskelija saattaisi rikkoa tietämättään lakia ja pahimmassa tapauksessa joutua enintään kahdeksi vuodeksi vankilaan. Hyökkäyksellään hän saattaisi aiheuttaa ainakin jonkinlaista haittaa kohteeseen. Pelkkä tietomurron yritys on rangaistavaa. (Rikoslaki 2015).

Azure ympäristönä mahdollistaa sen, että aktiivisen hyökkäyksen kohteena on toinen virtuaalitietokone. Virtuaaliympäristö mahdollistaa myös sen, että opiskelija voi vapaasti kokeilla ja testata, eikä mahdollisista seurauksista ei ole haittaa kenellekään. Virtuaalitietokoneen voi aina palauttaa, jos siitä on luotu varmuuskopio tai sen voi luoda melko vaivattomasti uudestaan. Kaikki mitä tehdään virtuaalitietokoneelle, jää virtuaalitietokoneelle. Esimerkiksi mikään mahdollinen virus tai mato ei pääse virtuaalitietokoneesta käyttäjän omalle tietokoneelle.

## 4.2 Oppimisympäristön tekninen kuvaus

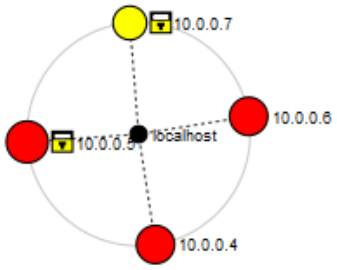
Suurin osa harjoituksista on pakko tehdä Windows -ympäristössä, koska niihin harjoituksiin tarvittavat sovellukset eivät ole saatavilla Linuxille tai Mac OS:lle. Tämän takia tarkoituksena oli luoda virtuaalitietokone tavallisella Windows 7 käyttöjärjestelmällä. Tämä ei kuitenkaan ollut mahdollista Laurean ympäristössä. Laurealla on käytössään ennakkoon maksettu Enterprise Agreement -tilaus, johon ei ole mahdollista luoda virtuaalitietokonetta tavallisella Windows käyttöjärjestelmällä. (Vanala 2017)

Lähellä Windows 7 työpöytäversiota on Windows Server 2012 R2. Tutkimusta varten tarvitaan kaksi virtuaalitietokonetta, joilla harjoitukset tehdään. Molemmissa virtuaalitietokoneissa ovat Windows Server 2012 R2:n, johon päätin valita SSD:n HDD:n sijaan, koska SSD käsittelee tietoa paljon nopeammin kuin HDD. Valitsin aluksi konfiguraatioksi DS2_V2:n, mutta päädyin kaksi kertaa halvempaan DS1_V2 konfiguraatioon. Harjoitusten suorittamiseen ei tarvita niin paljoa suoritustehoa kuin mitä DS2_V2 antaa.




Kuvio 4: DS1_V2 ja DS2_V2

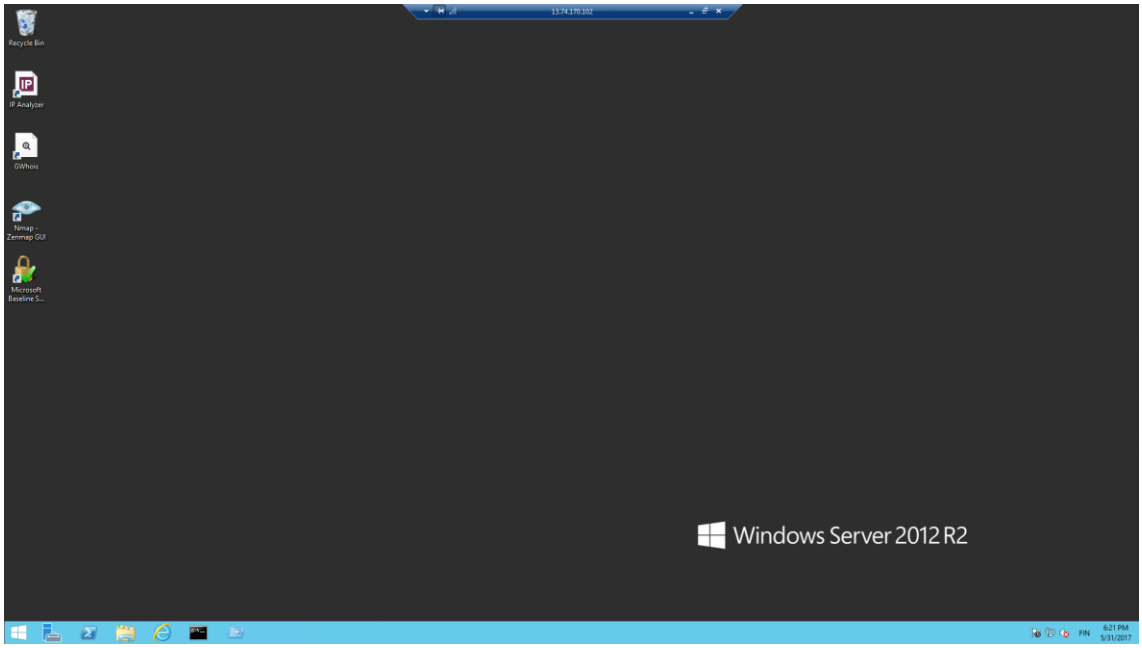
Lähes kaikissa harjoituksissa kohteena on jokin toinen tietokone. Tämän takia loin samaan verkkoon kaksi muuta virtuaalitietokonetta, joita voidaan käyttää harjoitusten kohteena§. Toinen kohdevirtuaalitietokoneista on Windows Server 2008 R2 SP1 ja toinen on Windows Server 2012 R2. Valitsin molempiin muistiksi HDD:n, koska kummallakaan tietokoneella opiskelijan ei ole tarkoitus aktiivisesti tehdä mitään, jolloin hitaampi muisti riittää.




Kuvio 5: Testiympäristön topologia

Tutkimukseen valituissa harjoituksissa käytetään muutamaa eri sovellusta. Nämä sovellukset ovat Nmap, josta käytetään sen graafista käyttöliittymää nimeltä Zenmap GUI versio 7.4, Microsoft Base Security Analyzer versio 2.3 ja Windows Firewall. Windowsin palomuuria lukuun ottamatta muut sovellukset oli ladattava niiden omilta nettisivuilta, koska niitä ei ollut val-

miiksi asennettuina. Azuresta sovelluksia ei myöskään voinut asentaa virtuaalitetokoneen konfiguraation yhteydessä. Loin myös pikakuvakkeet sovelluksista työpöydälle, mikä helpottaa ja nopeuttaa harjoitusten aloittamista.




Kuvio 6: Virtuaalitietokoneen työpöytä

## 4.3 Oppimisympäristön käyttöönotto

Remote Desktop Protocol -tiedosto mahdollistaa opiskelijan näkökulmasta hyvin vaivattoman pääsyn virtuaalitietokoneelle, koska hän voi tehdä sen omalta tietokoneelta. Opiskelijan tarvitsee ladata vain noin yhden kilotavun kokoinen RDP -tiedosto sieltä, mihin opintojakson opettajat ovat sen ladanneet. Tiedosto voidaan ladata esimerkiksi Optimasta tai muusta vastaavasta opiskelijoille tarkoitetusta Intra -sivustosta.

Remote Desktop Protocol eli etätyöpöytä -protokolla määrittelee yhteyden toiselta tietokoneelta toiseen tietokoneeseen. Azuresta ladattava Remote Desktop Protocol -tiedosto on keino ottaa yhteys virtuaalitietokoneeseen. Omaan tietokoneeseen ladatulla RDP -tiedostolla on virtuaalitetokoneen sen hetkinen julkinen IP -osoite tiedossa, jonka avulla virtuaalitietokoneeseen saa yhteyden. Tämän takia virtuaalitietokoneen julkiseksi IP -osoitteeksi tuli valita staattinen osoite dynaamisen osoitteen sijaan.

Jos valitsee virtuaalitietokoneen IP -osoitteen dynaamiseksi, kohtaa sen ongelman, että virtuaalitietokoneen uudelleenkäynnistyksen jälkeen, edellisen käynnistyksen yhteydessä luotu

RDP -tiedosto ei enää yhdistä virtuaalitietokoneeseen. Tämä hankaloittaa ympäristön käyttöönottoa, koska jokaisen uudelleenkäynnistyksen jälkeen tulisi lähettää opiskelijoille uusin RDP -tiedosto. Valitsemalla staattinen julkinen IP -osoite vältetään kyseinen ongelma, koska IP -osoite ei enää muutu uudelleenkäynnistyksen yhteydessä.

Ainoa asia, mikä pitää ottaa huomioon RDP -tiedoston käytössä on, että jos opiskelijan tietokoneessa ei ole Windows -käyttöliittymää, hän tarvitsee tiedoston avaamiseen kolmannen osapuolen sovelluksen tai hän joutuu käyttämään koulun tietokonetta. Linuxille on olemassa sovellus nimeltään Remmina ja Mac OS:n käyttäjät voivat ladata Microsoftin Remote Desktop -applikaation App Storesta. Molemmat sovellukset ovat ilmaisia.

### 4.4 Oppimisympäristön rajoitukset

Lähtökohtana on, että opiskelijalla pitää olla järjestelmänvalvojan oikeudet virtuaalitietokoneelle, koska tavallisilla käyttäjillä ei ole oikeutta ottaa etäyhteyttä mihinkään tietokoneeseen. Lisäksi Microsoftin käyttöehtojen johdosta oletusasetuksena on, että yhdelle tietokoneelle voi ottaa etäyhteyden vain kaksi järjestelmänvalvojaa samaan aikaan. Tämä tarkoittaa sitä, että koulun täytyy luoda useita eri virtuaalitietokoneita opiskelijoille. Vaihtoehtona on myös asettaa opiskelijoille tarkat vuorot, milloin heillä on aikaa suorittaa tehtävä. Tämä kuitenkin rajoittaa hieman sitä vapautta, jonka Azure tarjoaa. (Remote desktop for administration 2017)

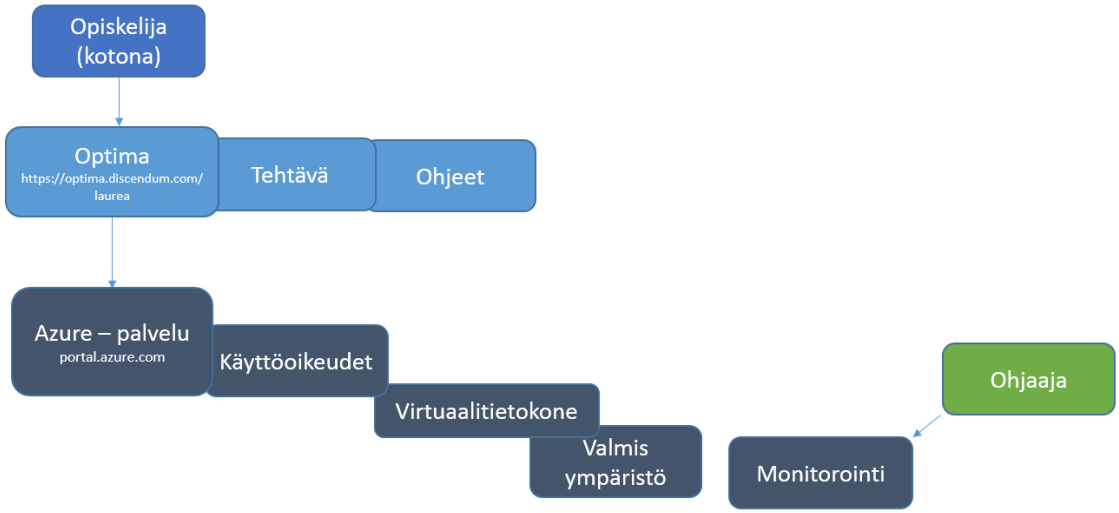
Toinen mahdollisuus on antaa tavallisille käyttäjille oikeus ottaa etäyhteys tietokoneeseen. Tätä varten täytyy kuitenkin muokata ryhmäkäytänteitä. En pystynyt tätä kuitenkaan testaamaan, koska ryhmäkäytänteitä muokatakseen virtuaalitietokoneelle pitää olla kirjautuneena domain -tunnuksella eikä paikallisella tunnuksella. Minun testiympäristöni on eristetty Laurean domainista, eikä minun testiympäristööni ollut mahdollista rakentaa omaa domainia.

Jos peruskäyttäjille annetaan oikeus ottaa etäyhteys virtuaalitietokoneeseen, jokaiselle opiskelijalle täytyy luoda oma käyttäjätunnus ja käyttäjätunnukselle on annettava oikeus ottaa etäyhteys ryhmäkäytänteiden kautta. Tässä tapauksessa virtuaalitietokoneen täytyy olla paljon tehokkaampi, koska koneella voi olla monta käyttäjää samaan aikaan. Azuressa on ominaisuus, että se nostaa virtuaalitietokoneen tehoa ylöspäin, jos sen suorituskyky alkaa laskea määrätyn ajan verran. Tähän kuitenkin tarvitaan joko Azuren automaatiotili, joka on hinnoiteltu erikseen. Toinen vaihtoehto on käyttää maksullista kolmannen osapuolen ohjelmaa nimeltä VMpower.

# 5 Laboratorioharjoitukset

Tätä opinnäytetyötä varten olen kerännyt harjoituksia, jotka sopivat opintojakso Network Security:n teemaan. Harjoituksien ideat on kerätty kirjasta Hands-On Information Security Lab Manual, Fourth edition. Kirjan on kirjoittanut Michael Whitman, Herbert Mattord ja Andrew Green. (Green, Mattord & Whitman 2014, 1)

Ymmärtääkseen hakkerin aikeet ja estääkseen ne, opiskelijoiden on opittava ajattelemaan samalla tavalla. Miten henkilö voi osata puolustaa itseään tai tässä tapauksessa tietojärjestelmää, jos hän ei osaa tai vähintään ymmärrä, mitä vastapuoli aikoo tai yrittää tehdä. Harjoituksien tarkoituksena on, että opiskelija pääsee itse kokeilemaan ja harjoittelemaan hyökkäystä tietojärjestelmään.




Kuvio 7: Harjoituksen mahdollinen kulku

## 5.1 Footprinting

Ennen kuin itse hyökkäys voi alkaa, on tiedettävä kaikki mahdollinen kohteesta. ”Footprinting” eli tiedustelu on ensimmäinen askel, kun halutaan tunkeutua vieraaseen järjestelmään. Tiedustelun tarkoituksena on kerätä tietoa kohteen IT-infrastruktuurista. Tähän kuuluu muun muassa palvelimien fyysinen sijainti, IP -osoiteavaruus, sähköpostiosoitteet ja puhelinnumerot. Jo pelkällä puhelinnumerolla ja soittamalla yritykseen hyökkääjä voi saada paljon aikaan: käyttämällä hyväksi sosiaalisia taitojaan ja saaden niiden avulla haltuunsa kohteen kriittistä informaatiota. (Green, Mattord, & Whitman 2014, 16)

Tiedustelussa tietoa on osattava etsiä oikeista paikoista. Keinoja on monia, mutta yleensä tiedustelu ei ole tunkeilevaa. Tässä vaiheessa hyökkääjä ei vielä yritä päästä sisälle järjestelmään. Valtava määrä hyödyllistä tietoa on aina löydettävissä yrityksen omilta sivuilta, mutta

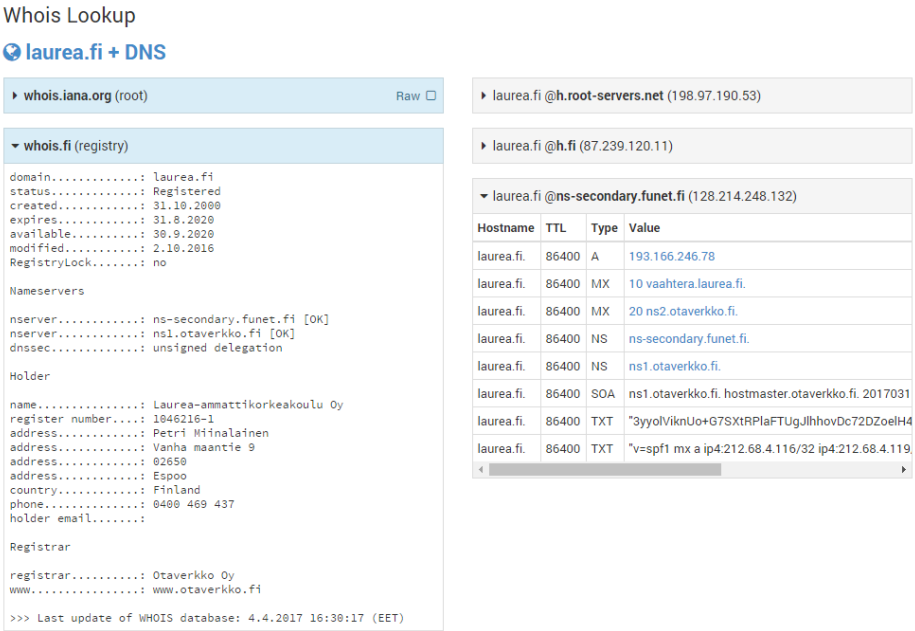
Internet tarjoaa myös paljon hyviä työkaluja siihen. Harjoituksessa käytämme työkalua WHOIS.

### 5.1.1 WHOIS

WHOIS is on ilmainen hakupalvelu, joka kehitettiin alun perin yksittäisiä henkilöitä ja organisaatioita varten. Sen avulla pystytään tarkistamaan, onko haluttu Domain-nimi käytössä vai ei. Tässä on kuitenkin varjopuoli. Hakkeri voi WHOIS -työkalun avulla kerätä paljon tietoa kohteestaan ja kerätä itselleen tärkeää tietoa esimerkiksi IP-osoiteavaruus, palvelimen sijainti ja sen ylläpitäjä. Tämä tieto helpottaa hyökkäystä kohteeseen. Hieman kokeneempi käyttäjä voi tehdä WHOIS -kyselyjä Windowsin komentotulkin avulla tai käyttämällä kolmansien osapuolien valmistamia sovelluksia, mutta Internetistä kuka tahansa voi löytää nettisivuja, jotka tekevät saman asian nopeammin, helpommin ja yleensä myös paremmin.

### 5.1.2 Tiedustelu käyttäen WHOIS -työkaluja

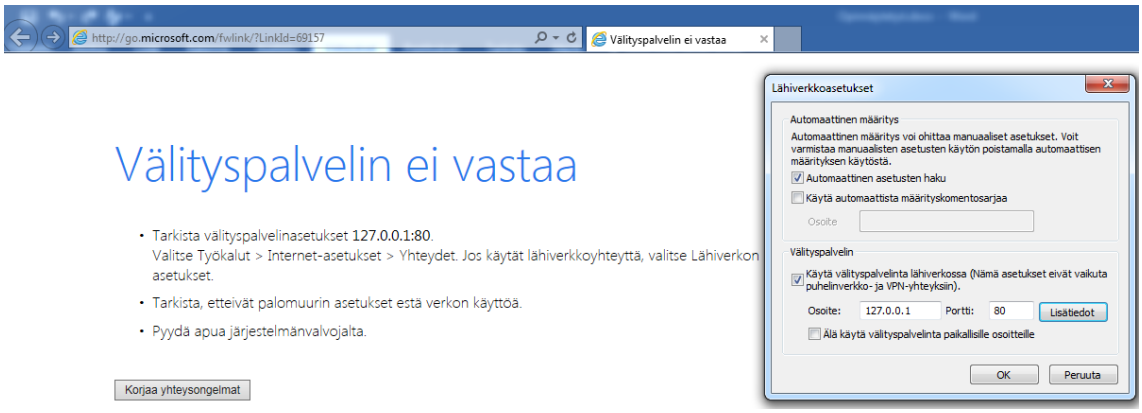
Tätä harjoitusta varten minun ei tarvinnut asentaa kolmansien osapuolien sovelluksia, koska voimme käyttää tähän tarkoitukseen perustettuja nettisivuja. Windows server 2012:n valmiiksi asennettu Internet Explorer 11 sopi tarkoitukseen hyvin. Harjoitusta varten loin palvelimen työpöydälle kaksi pikalinkkiä, mitkä vievät harjoituksen kannalta oleelliselle nettisivulle suoraan. Tämän harjoituksen suorittamiseen tarvitaan kahta eri nettisivua. Nettisivut ovat https://gwhois.org/ ja https://ipalyzer.com/. Tutkimustyöni perusteella nämä nettisivut antoivat oleellisimman tiedon helposti luettavassa muodossa.




Kuvio 8: Whois -kyselyn tulos

Tämän harjoituksen suorittamiseen ei välttämättä tarvita Microsoft Azuren kaltaista pilviympäristöä. Informaatio, jota WHOIS -sivustot tarjoavat, ovat julkista tietoa ja niihin käsiksi pääsemiseen ei vaadita keinoja, jotka voitaisiin luokitella laittomiksi. Tämän perusteella opiskelija voisi tehdä täysin saman harjoituksen samalla vaivalla myös omalla tietokoneellaan. Tällöin koulu säästäisi resursseja.

Ohjaajan itse luodussa ympäristössä on kuitenkin etunsa. Ohjaaja voi halutessaan estää pääsyn kaikille muille nettisivuille. Tämän voi tehdä esimerkiksi Internet Explorerin paikallisen verkon asetuksista käyttämällä välityspalvelimena osoitetta 127.0.0.1 ja lisäämällä poikkeussääntöihin ne nettisivut, joihin opiskelijoiden tarvitsee päästä. Tämän jälkeen voidaan ryhmäkäytänteillä poistaa Internet -asetuksista ”yhteydet” -välilehti tavallisilta käyttäjiltä, sekä estää pääsy muokkaamaan ryhmäkäytänteitä.




Kuvio 9: Välityspalvelin 127.0.0.1

### 5.1.3 Arvio Azuresta

Opintojakson ensimmäinen harjoitus on hyvä suorittaa Azuressa, koska siinä ympäristö tulee nopeasti tutuksi opiskelijalle, esimerkiksi virtuaalitietokoneen käyttöönotto, kirjautuminen ja yleisesti etäyhteyden ottaminen toiseen tietokoneeseen. Pitää kuitenkin ottaa huomioon, että Azureen luotu harjoitusympäristö on hieman erilainen kuin mitä opiskelijoilla on omalla koneellaan. Osa opiskelijoista saattaa käyttää Linux -käyttöjärjestelmää, mikä Linux -jakelusta riippuen saattaa olla hyvin erilainen Windowsiin verrattuna.

Vaikka järjestelmää olisi testattu todella paljon ja perusteellisesti, on aina mahdollisuus, että jokin ei mene suunnitellusti. Koska harjoituksen voi suorittaa myös omalla tietokoneella, opintojakson ohjaajien tekemät mahdolliset virheet ympäristön käyttöönotossa eivät vaikuta suuresti opiskelijoihin. Mikäli opiskelija kohtaa ongelman liittyen yhteyden ottamiseen, voi hän kertoa siitä opettajalle. Opiskelijan ei kuitenkaan tarvitse odottaa, että ongelma korjataan, vaan hän voi tehdä harjoituksen omalla tietokoneella.

## 5.2 Haavoittuvuuksien tunnistaminen

Verkon skannaaminen ja haavoittuvuuksien tunnistaminen ovat jokaisen järjestelmänvalvojan yksi tärkeimpiä tehtäviä. Järjestelmänvalvojan on pystyttävä huomaamaan kaikki poikkeukset omassa ympäristössään ja korjaamaan ne. Verkon skannaamiseen ja haavoittuvuuksien tunnistamiseen on olemassa monia hyviä työkaluja kuten Nessus, Wireshark ja Microsoft Baseline Security Analyzer (MBSA). Tässä harjoituksessa käytetään Microsoftin MBSA:ta.

### 5.2.1 MBSA

Microsoft Baseline Security Analyzer on työkalu, jolla käyttäjä voi helposti tarkistaa yleisellä tasolla verkon tilan. MBSA:n avulla järjestelmänvalvoja voi skannata ja analysoida sekä paikallisia tietokoneita, että myös etänä olevia. Skannauksen tuloksen perusteella järjestelmänvalvoja näkee, tarvitseeko järjestelmään ajaa uusia tietoturvapäivityksiä tai muuttaa epäkohtia joistakin asetuksista tai kokoonpanoista.

### 5.2.2 Haavoittuvuuksien löytäminen MBSA:lla

Harjoitusta varten virtuaalitietokoneelle piti asentaa MBSA, koska sitä ei oltu sisäänrakennettu osaksi Windows Server 2012 järjestelmää. Harjoitusta varten piti myös asentaa kaksi muuta virtuaalitietokonetta skannauksen kohteiksi. Toinen virtuaalitietokoneista on Windows Server 2012- ja toinen Windows Server 2008 -käyttöjärjestelmä. Toisen virtuaalitietokoneista annoin olla lähes muuttamattomana, mutta toiseen virtuaalitietokoneeseen loin muutamia huomiota vaativia kohtia: otin vieraskäyttäjän käyttöön, loin kaksi uutta käyttäjää joista toisella on heikko salasana, mikä ei vanhene koskaan ja toisella käyttäjällä ei ole salasanaa ollenkaan. Lisäksi otin Windowsin automaattiset päivitykset pois käytöstä.

**Windows Scan Results**

**Administrative Vulnerabilities**

| Score | Issue | Result |
|---|---|---|
| | Local Account Password Test | Some user accounts (2 of 4) have blank or simple passwords, or could not be analyzed. What was scanned Result details How to correct this |
| | Guest Account | The Guest account is not disabled on this computer. What was scanned How to correct this |
| | Automatic Updates | The Automatic Updates feature is disabled on this computer. What was scanned How to correct this |
| | Password Expiration | Some user accounts (3 of 4) have non-expiring passwords. What was scanned Result details How to correct this |
| | Incomplete Updates | No incomplete software update installations were found. What was scanned |
| | Windows Firewall | This check was skipped because it cannot be done remotely. |
| | File System | All hard drives (2) are using the NTFS file system. What was scanned Result details |
| | Autologon | Autologon is not configured on this computer. What was scanned |
| | Restrict Anonymous | Computer is properly restricting anonymous access. What was scanned |
| | Administrators | No more than 2 Administrators were found on this computer. What was scanned Result details |

Kuvio 10: Skannauksen tulos

### 5.2.3 Arvio Azuresta

Harjoituksen voi tässäkin tapauksessa suorittaa ilman Azurea tai muuta pilvilaskentapalvelua, koska MBSA:lla voi skannata myös omaa tietokonetta. MBSA on myös todella kevyt sovellus ja se on tuettu kaikissa Windows käyttöjärjestelmissä Windows XP:stä lähtien. Lisäksi se vie myös todella vähän tilaa (alle kaksi megatavua) tietokoneen kovalevyltä tai SSD:ltä, joten tilan puutteesta kukaan ei jätä sitä asentamatta.

On kuitenkin mahdollista, että osa oppilaista ei ole halukas asentamaan omalle tietokoneelle sovelluksia, joita he eivät yhden kerran jälkeen käytä tai he eivät halua hyväksyä sovelluksen valmistajien käyttöoehtoja. Osa opiskelijoista saattaa myös käyttää Linuxia, jolle MBSA:ta ei voi asentaa. (Korhonen 2016)

Tämän harjoituksen mutkattomaan suoritukseen Azure on loppuen lopuksi todella hyvä ympäristö. Pelkästään se, että opiskelijoilla on heti tarvittavat työkalut suorittaakseen harjoitus mutkattomasti, on jo suuri helpotus oppilaalle ja säästää aikaa ja voimia itse oppimiseen ja harjoituksen suorittamiseen. Tämän kaltaiseen harjoitukseen ei kuitenkaan riitä, että opiskelijalle tarjotaan hieman pintapuolista kokemusta jostakin tietoturva-alan sovelluksesta. Pitää myös olla kohde, johon sitä voi kokeilla. Tähän Azure sopii todella hyvin. Kohdetta ei tarvitse lähteä etsimään oikeasta maailmasta, vaan se voidaan rakentaa koulun toimesta.

## 5.3 Porttien skannaus

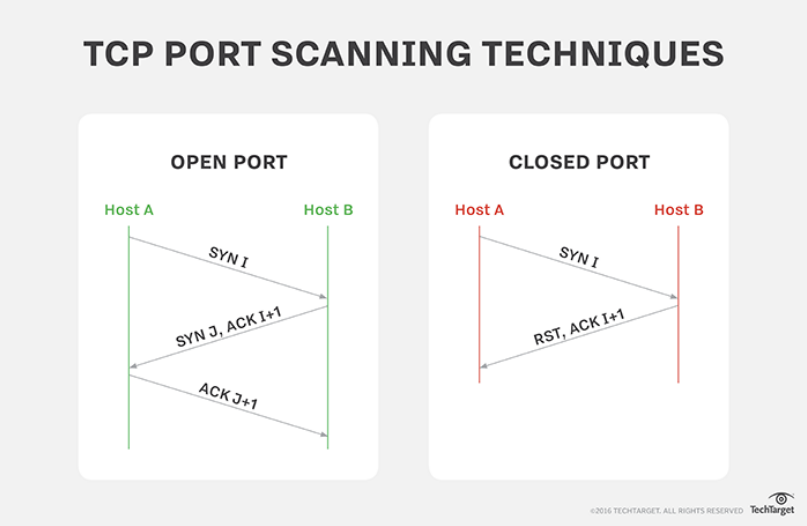
Portit tietokoneella ovat verrattavissa esimerkiksi kerrostalojen postilaatikoihin. Tiettyyn postilaatikkoon menevät vain tietyn henkilön toimitukset. Portit määrittelevät saman asian, mutta vain sovelluksille ja palveluille. Esimerkiksi https -protokolla käyttää porttia 443 ja http -protokolla porttia 80.

Porttien skannaus on oleellinen osa verkkohyökkäystä. Skannaamalla verkoston portteja, hyökkääjä voi saada selville, mitkä portit ovat avoimena. Avoimien porttien kautta hyökkääjä voi saada yhteyden verkkoon ja siihen kuuluviin tietokoneisiin.

Samalla kun skannataan portteja, monet siihen tarkoitetut sovellukset saavat yleensä selville myös paljon enemmän. Esimerkiksi Nmap saa selville kohteen käyttöliittymän ja mihin ryhmään tietokone kuuluu. Useita saman verkon IP -osoitteita skannaamalla saadaan tietoa myös verkon topologiasta.

### 5.3.1 Nmap

Nmap eli Network Mapper (Suomeksi verkon kartoittaja) on ilmainen ja avoimen lähdekoodin työkalu, jolla kuka tahansa voi skannata ja tutkia tietoverkkoja. Nmap on suosittu monien verkon- ja järjestelmänvalvojien keskuudessa. Se on erittäin joustava työkalu, koska se käyttää useita eri keinoja skannatakseen kohdetta. Näitä ovat muun muassa TCP connect, TCP SYN ja TCP FIN. (Nmap)

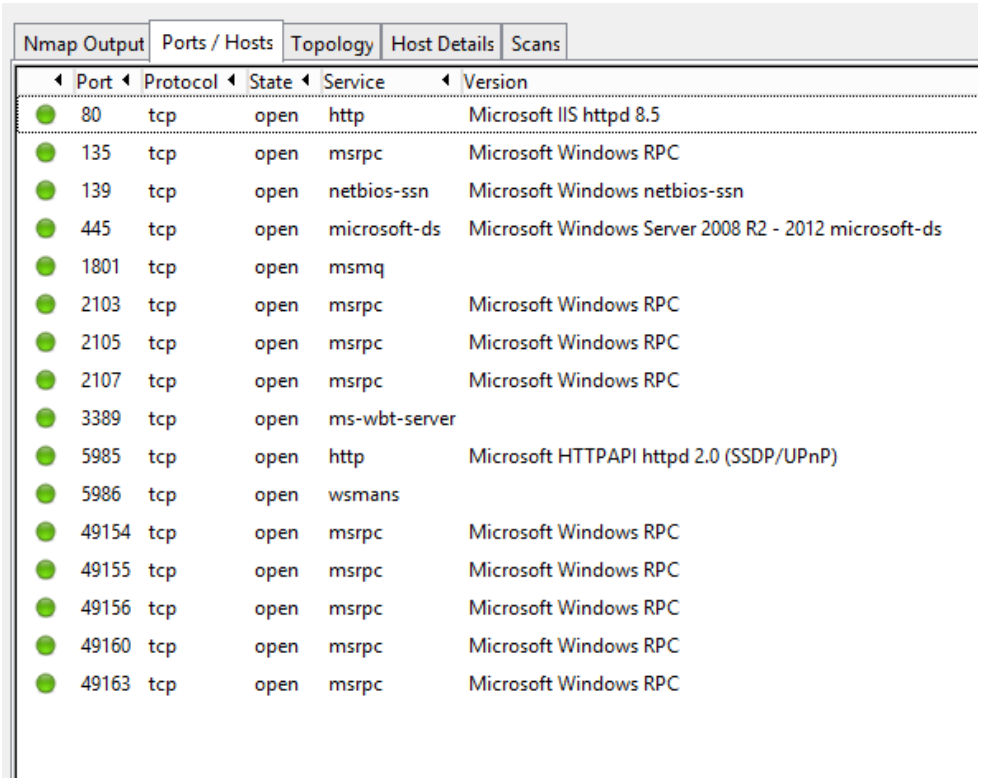



Kuvio 11: TCP porttiskannaus (Gont 2016)

Nmap kykenee myös arvaamaan kohteen käyttöjärjestelmän ja sen version. Nmappiin on julkaistu Zenmap GUI, joka on graafinen käyttöliittymä Nmapille. Zenmap GUI on erittäin helppokäyttöinen ja se on myös monialustainen eli sen saa asennettua Linuxille, Windowsille ja Mac OS:lle.

### 5.3.2 Skannaus Zenmapilla

Harjoitusta varten asensin Zenmap GUI:n Windows Server 2012:lle ja määritin kohteiksi kaksi virtuaalitietokonetta. Kohteita voi olla myös paljon enemmän, koska Zenmapilla voi skannata tuhansia koneita yhdellä kertaa. Tätä harjoitusta varten kaksi kohdetta riittää hyvin. Käytin tähän harjoitukseen samoja virtuaalitietokoneita kuin edellisessä harjoituksessa.




| Port | Protocol | State | Service | Version |
|---|---|---|---|---|
| 80 | tcp | open | http | Microsoft IIS httpd 8.5 |
| 135 | tcp | open | msrpc | Microsoft Windows RPC |
| 139 | tcp | open | netbios-ssn | Microsoft Windows netbios-ssn |
| 445 | tcp | open | microsoft-ds | Microsoft Windows Server 2008 R2 - 2012 microsoft-ds |
| 1801 | tcp | open | msmq | |
| 2103 | tcp | open | msrpc | Microsoft Windows RPC |
| 2105 | tcp | open | msrpc | Microsoft Windows RPC |
| 2107 | tcp | open | msrpc | Microsoft Windows RPC |
| 3389 | tcp | open | ms-wbt-server | |
| 5985 | tcp | open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |
| 5986 | tcp | open | wsmans | |
| 49154 | tcp | open | msrpc | Microsoft Windows RPC |
| 49155 | tcp | open | msrpc | Microsoft Windows RPC |
| 49156 | tcp | open | msrpc | Microsoft Windows RPC |
| 49160 | tcp | open | msrpc | Microsoft Windows RPC |
| 49163 | tcp | open | msrpc | Microsoft Windows RPC |

Kuvio 12: Kohteen avoimet portit

### 5.3.3 Arvio Azuresta

Tämän harjoituksen ennakkovaatimukset ovat täysin samat kuin harjoituksessa, jossa etsittiin haavoittuvuuksia käyttäen MBSA:ta. Tämän johdosta opiskelija voi osittain suorittaa tämänkin harjoituksen omalla tietokoneellaan ja omassa henkilökohtaisessa verkossa. Kuitenkin kuten edellisissä harjoituksissa, tässäkin tapauksessa Azure antaa edun: opiskelija saa harjoituksen kohteeksi ympäristön, joka ei ole tietoturvallinen tai on tavallisesta poikkeava.

## 5.4 Windowsin Palomuuri

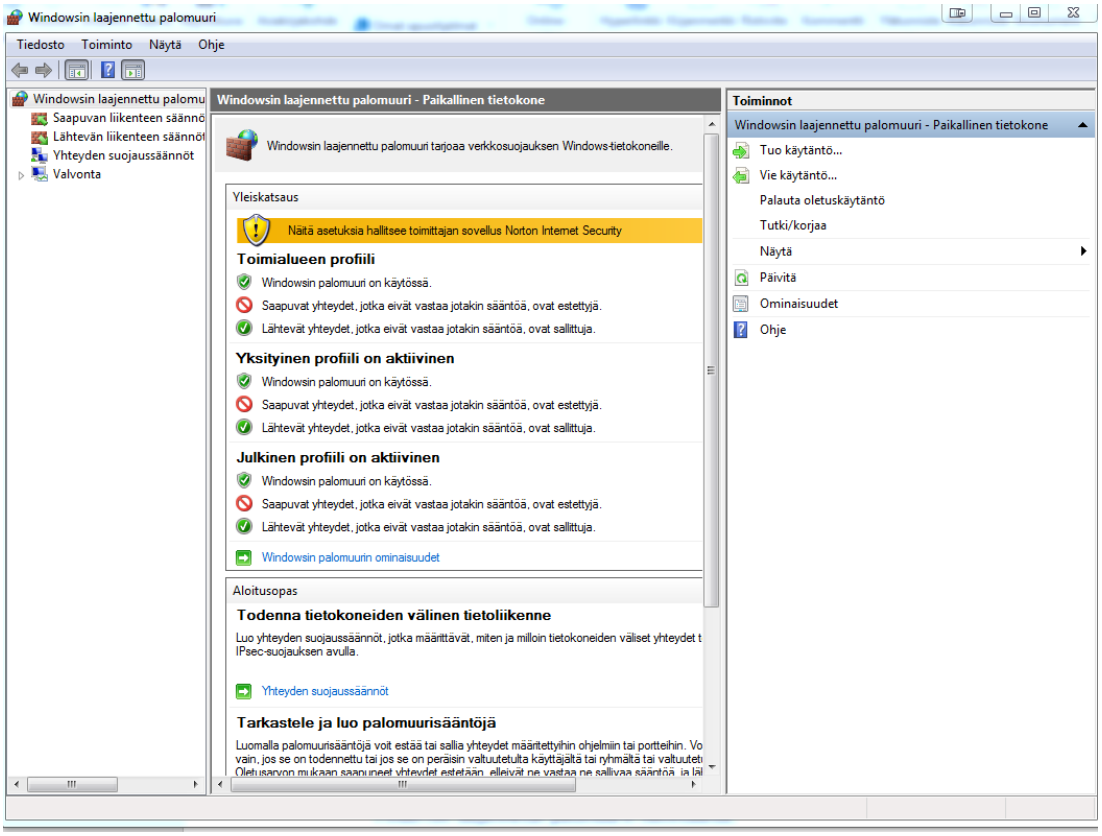
Windowsin palomuuri on Microsoftin kehittämä ja luoma palomuuri Windows käyttöjärjestelmille. Windowsin palomuurilla voidaan suodattaa tietokoneesta lähtevää ja tietokoneeseen saapuvaa dataa. Jos tietokone on kytkettynä internettiin, on tietämys palomuurista erittäin tärkeää.

### 5.4.1 Windowsin palomuurin konfiguraatio

Koska Windowsin palomuuri ja Windowsin laajennettu palomuuri kuuluvat sellaisenaan Windowsiin, ei harjoitusta varten tarvitse tehdä ylimääräisiä toimenpiteitä. Tämä tarkoittaa taas sitä, että opiskelija voi periaatteessa suorittaa harjoituksen myös kotonaan omalta tietokoneeltaan. Edellytyksenä on kuitenkin, että opiskelijalla on myös Windowsin käyttöliittymä ja joka on Windows XP tai uudempi. Linuxilla tai Mac OS:llä harjoitus ei onnistu.

### 5.4.2 Arvio Azuresta

Tähän harjoitukseen Azure ei oikeastaan tarjoa muuta kuin puhtaan ympäristön, johon ei ole asennettu mitään ylimääräistä sekä sen, että Windowsin palomuurin asetukset ovat oletusasetuksilla. Opiskelijan mahdolliset omat asetukset ja tietokoneelle asennetut kolmannen osapuolen virustorjuntaohjelmat saattaisivat vaikuttaa harjoituksen kulkuun.




Kuvio 13: Norton ja Windowsin palomuuri

Harjoituksen pystyy kuitenkin suorittamaan hyvin ottamalla tietokoneen irti verkosta. Kun tietokone on otettu pois verkosta, on turvallista ottaa virustorjuntaohjelma pois päältä ja sen jälkeen voi muokata ongelmitta Windowsin palomuurin asetuksia.

# 6 Yhteenveto Azuresta

Azure sopii kyberturvallisuuden oppimisympäristöksi hyvin. Se on kaikin puolin hyvin monipuolinen suuren tarjonnan ansiosta. Azuren kautta voi ylläpitää myös verkkosivuja. Sen käyttöönotto on helppoa ja perusymmärrys pilvipalveluista riittää Azuren käyttämiseen. Hallinnointi on vaivatonta, koska ylläpitäjä pääsee käsiksi kaikkiin virtuaalitietokoneisiin yhden portaalin kautta. Portaalin kautta voi lisätä, hallinnoida, monitoroida, päivittää ja poistaa virtuaalitietokoneita. Monitorointi on hyvä ominaisuus tämänkaltaisessa ympäristössä, jossa seurataan milloin virtuaalitietokoneella on aktiivisuutta. Opintojakson ohjaaja näkee tämän avulla, onko opiskelija tehnyt virtuaalitietokoneella jotain.

Ympäristön käyttöönoton ottoon vaikuttaa käyttäjän oma käyttöjärjestelmä. Virtuaalitietokoneelle kirjaudutaan lataamalla Azuresta RDP -tiedosto ja avaamalla se. Jos käyttäjän omassa tietokoneessa ei ole Windows -käyttöjärjestelmää, hän tarvitsee kolmannen osapuolen ohjelmiston avatakseen RDP -tiedoston.

Harjoitukset joita käytin Azuren testaamiseen, eivät tuoneet läheskään koko Azuren mahdollista potentiaalia esille. Pystyin toteuttamaan kaikki harjoitukset ainakin osittain paikallisesti. Käytin sovelluksia omalla tietokoneella ja otin kohteeksi myös oman tietokoneen. Ainoa ero Azureen tässä oli, että en voinut luoda haavoittuvaa ympäristöä. Samantyyliset harjoitukset voitaisiin myös toteuttaa pyörittämällä paikallisesti Linuxia Oraclen Virtual Boxin kautta, mikä antaa sen mahdollisuuden, että ympäristö voi olla haavoittuvainen. Jälkimmäiset vaihtoehdot olisivat täysin ilmaisia. Testiympäristöni yhden virtuaalitietokoneen hinta kuukaudessa on arviolta noin 80 euroa kuukaudessa. Hinta voi todellisuudessa olla alle puolet siitä, koska Azuren arvion mukaan virtuaalitietokone olisi koko ajan päällä. Mielestäni tämä ei ole liian korkea hinta, koska Azure mahdollistaa kuitenkin paljon enemmän vaihtoehtoja harjoitusten kohteiksi.

## 6.1 Jatkokehitys

Azureen voidaan rakentaa yrityksen koko infrastruktuuri kaikkine eri komponentteineen, johon voi kuulua muun muassa SQL -tietokannat, sähköpostipalvelimet ja verkkosivut. Oppilaitoksen on mahdollista rakentaa opiskelijoille erittäin laaja ja monipuolinen kohde, jota vastaan he voivat harjoitella tietoturvakursseilla opittuja taitoja. Tässä on kuitenkin otettava

huomioon Azuren mahdollinen oma penetraatiotestauspolitiikka. Jatkokehityksessä on otettava selvää, kuinka haavoittuvan ympäristön rakentaminen on mahdollista tai sallittua.

Vaikka Laurea tekee paljon yhteistyötä yritysmaailman kanssa ja harjoituksen kohteeksi on mahdollista saada oikea yritys, siihen liittyy aina lisähuomioitavaa, mikä ei liity itse harjoitukseen. Näitä voivat olla muun muassa salassapitosopimukset, tarkat ehdot ja säännöstelyt siitä, mitä saadaan tehdä ja milloin saadaan tehdä. Azure mahdollistaa paljon vapautta.

Lähteet

Ahonen, T. Mikä ihmeen PaaS. Viitattu 2.4.2017. http://www.cybercom.com/fi/Suomi/Yritys/Blogit/Blogit/Mika-ihmeen-PaaS/

Gont, F. 2016. Tips to understanding different TCP port-scanning techniques. Viitattu 30.4.2017. http://searchnetworking.techtarget.com/tip/Tips-to-understand-different-TCP-port-scanning-techniques

Cerejo, L. 2010. Design better and faster with rapid prototyping. Viitattu 5.2.2017 https://www.smashingmagazine.com/2010/06/design-better-faster-with-rapid-prototyping/#comments

Chappel, D. 2010. Introducing the Windows Azure platform. Viitattu 13.2.2017. http://www.davidchappell.com/writing/white_papers/Introducing_the_Windows_Azure_Platform,_v1.4--Chappell.pdf

Fagerström, K. Tutkittu: Näin suomalaiset käyttävät mediaa 2015. Viitattu 25.3.2017. http://www.mtv.fi/spotti/tutkittua/kuluttajat/artikkeli/tutkittu-suomalaisten-median-kaytto-vuonna-2015/5598232

Foulds, I., Squillace, R., Wang, L. & Zemault, C. 2017. Azure availability sets guidelines for Windows VM. Viitattu 20.3.2017. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/infrastructure-availability-sets-guidelines

Green, A., Mattord, H. & Whitman, M. 2014. Hands-on information security lab manual. Boston: Course Technology.

Korhonen, S. Opiskelija ei pääse kurssille, koska vastustaa Microsoft-ehtoja – "periaattellisia vainoharhoja löytyy". Viitattu 13.5.2017. http://www.tivi.fi/Kaikki_uutiset/opiskelija-ei-paase-kurssille-koska-vastustaa-microsoft-ehtoja-periaatteellisia-vainoharhoja-loytyy-6580271

Martin, S. 2014. Upcoming name change for Windows Azure. Viitattu 13.2.2017. https://azure.microsoft.com/en-us/blog/upcoming-name-change-for-windows-azure/

Microsoft. Azure pricing. Viitattu 25.3.2017. https://azure.microsoft.com/en-us/pricing/

Microsoft. Remote desktop for administration. Viitattu 12.4.2017. https://technet.microsoft.com/en-us/library/cc770759(v=ws.11).aspx

Microsoft. What is IaaS. Viitattu 2.4.2017. https://azure.microsoft.com/en-us/overview/what-is-iaas/

Nmap. Introduction. Viitattu 20.4.2017. https://nmap.org/

Poppelgaard, T. Citrix XenApp Essentials – Microsoft Azure. Viitattu 13.5.2017. https://www.poppelgaard.com/citrix-xenapp-essentials-microsoft-azure

Rikoslaki 2015/368. Viitattu 3.4.2017. http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Smith, R. 2015. Understanding Azure Availability sets. Viitattu 20.3.2017. https://www.petri.com/understanding-azure-availability-sets

Vanala, S. Atk-Asiantuntijan haastattelu sähköpostin välityksellä 12.4.2017.

Web-opas. Mikä on SaaS?. Viitattu 2.4.2017. http://www.webopas.net/saas.html

Kuviot

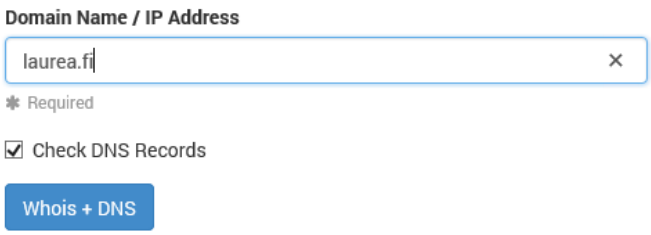
Liitteet

Liite 1: Lab exercises

**Assignment 1: Gwhois**

Open shortcut GWhois from desktop. This shortcut will open Internet Explorer and web site https://gwhois.org/


Write your targets Domain name or IP address to the field below in example and press “Whois + DNS” to perform the lookup:




Write down everything useful that malicious facets could use to do harm or any other malicious activities. Write down at least IP address, registrar and holders information and explain why would malicious facet would want to get hold on to this information.

What other important and relevant information did you collect and why?

After performing lookup for one domain repeat the same lookup for another domain. You can also do the second lookup using different Whois tool and compare them.

**Assignment 2: IP Analyzer**

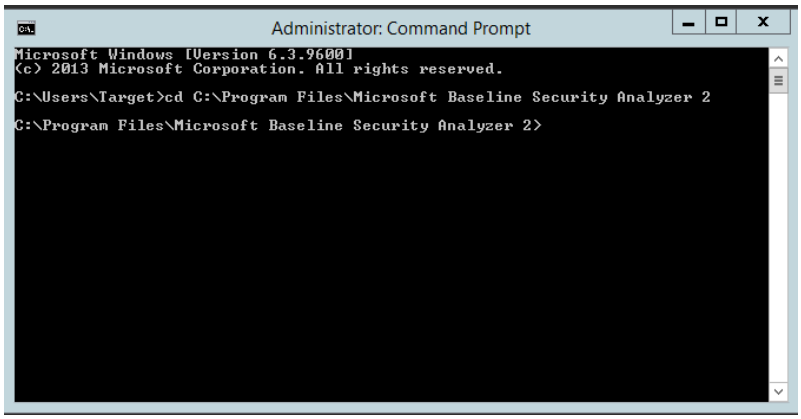
Open shortcut IP analyzer from desktop. This shortcut will open Internet Explorer and web site https://www.ipalyzer.com/


Now that you have your targets IP address use it to get more information about your target.

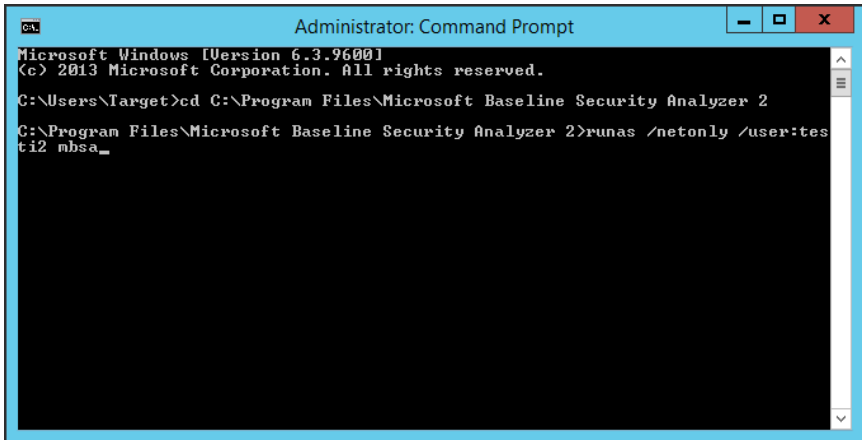

Write down all the information you could find and explain how you could use that information against that domain.

## Assignment 3: Finding vulnerabilities from network with MBSA

Open Command prompt
Go to location where MBSA is installed using change directory command
(“cd C:\Program Files\Microsoft Baseline Security Analyzer 2”)

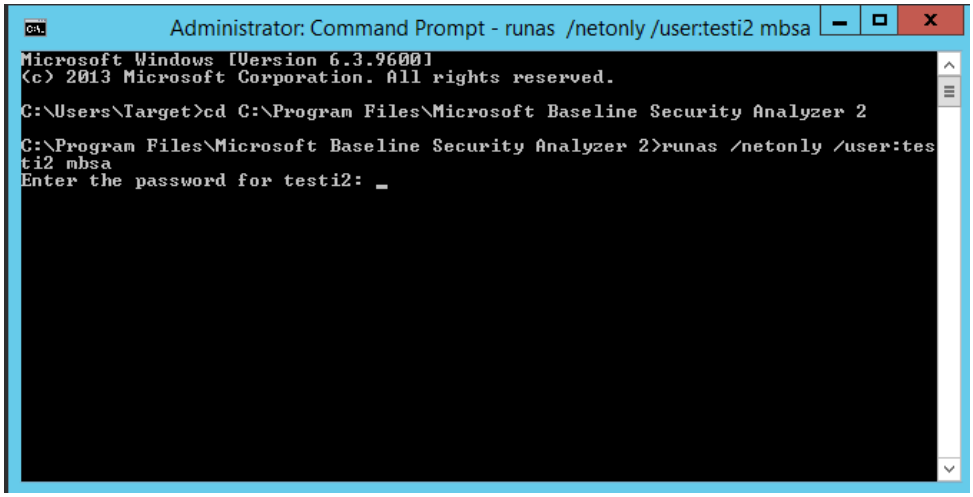



Open MBSA using following command: “runas /netonly /user:testi2 mbsa” and press Enter.

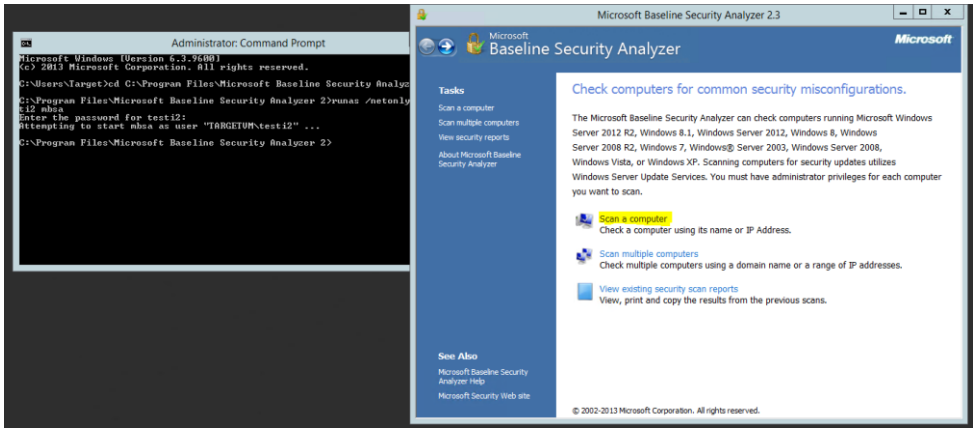



Type in password: Oppariteemu123

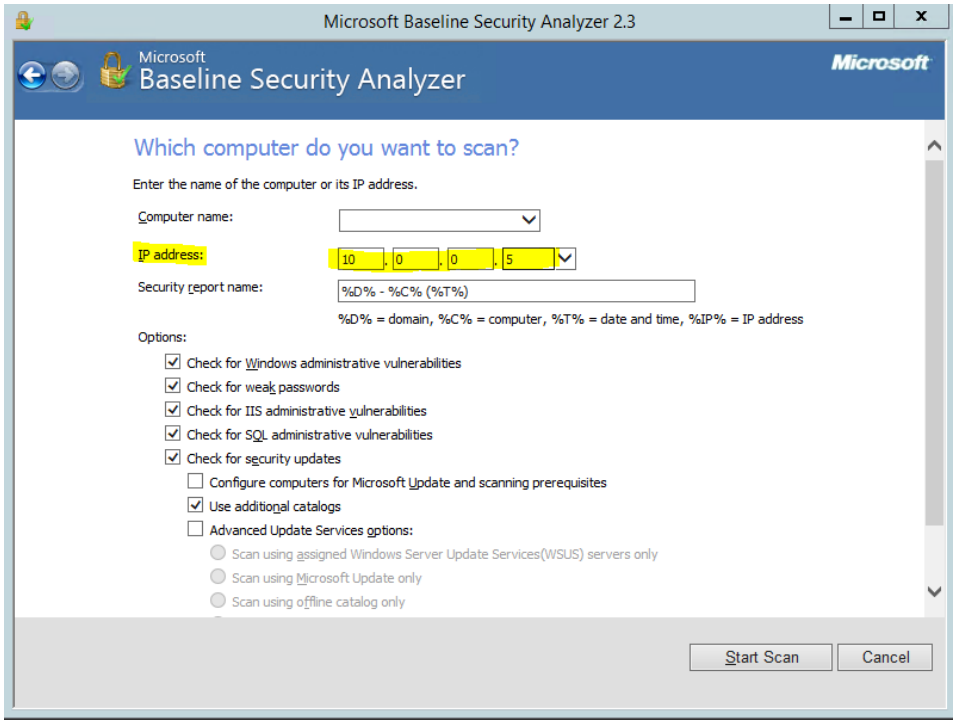
After pressing Enter MBSA will open.



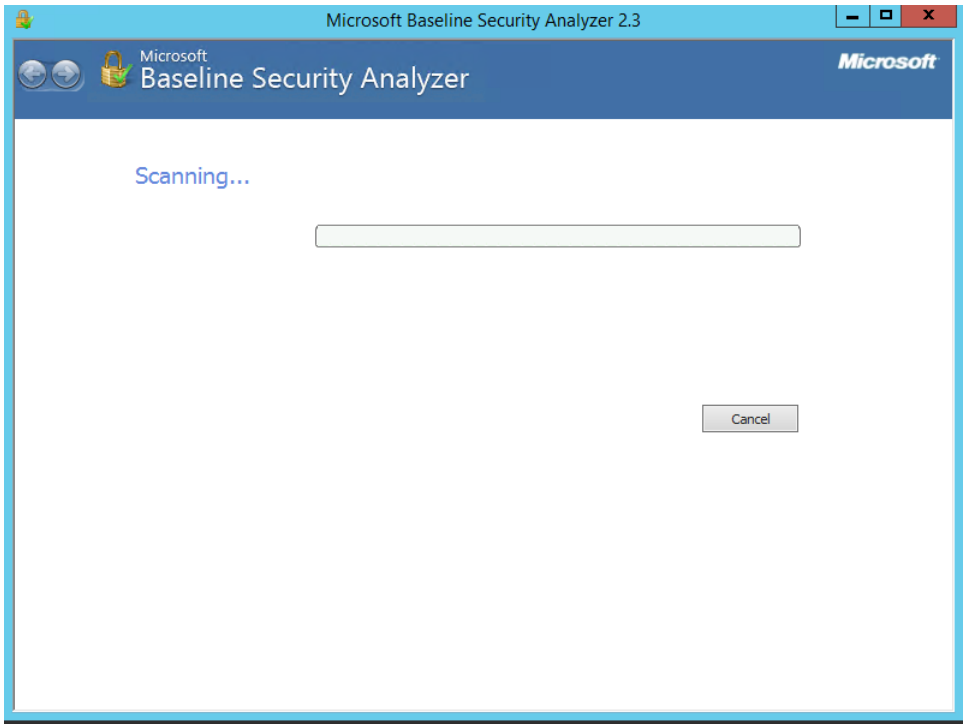

Choose option Scan a computer.




Scan computer by typing in its IP address (10.0.0.5).




Wait for the scan to be completed




Write down what kind of problems and vulnerabilities MBSA found and explain why they are vulnerabilities and try to find the solutions to them.

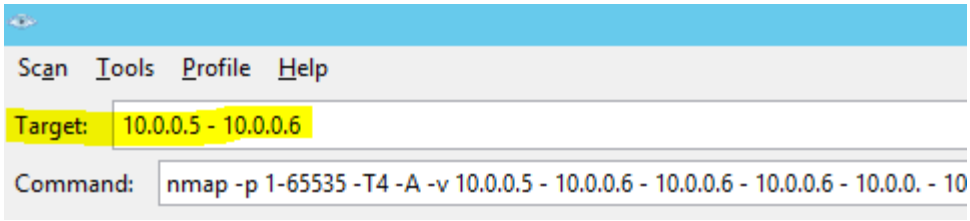
After that perform the same steps but use IP 10.0.0.6
Username in this case is Meta.

**Assignment 4: Port scanning using Zenmap**

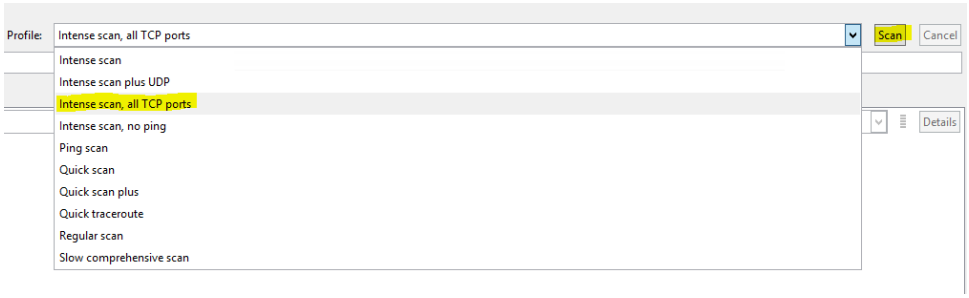
Open Nmap – Zenmap GUI from desktop.


Choose your target.

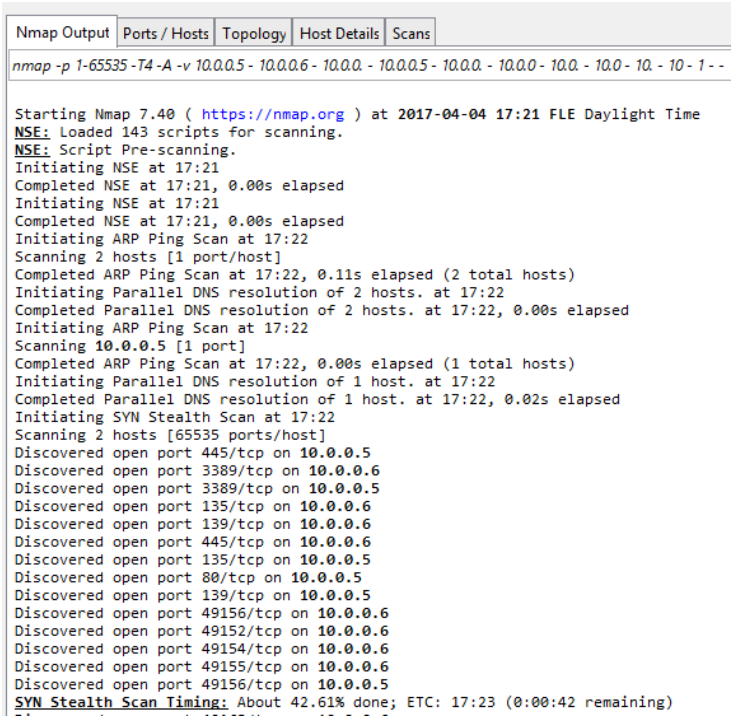
In this case, they are IP addresses 10.0.0.5 and 10.0.0.6.




From profile choose “Intense scan, all TCP ports” and then press “scan”.




Nmap is now scanning targets TCP ports.



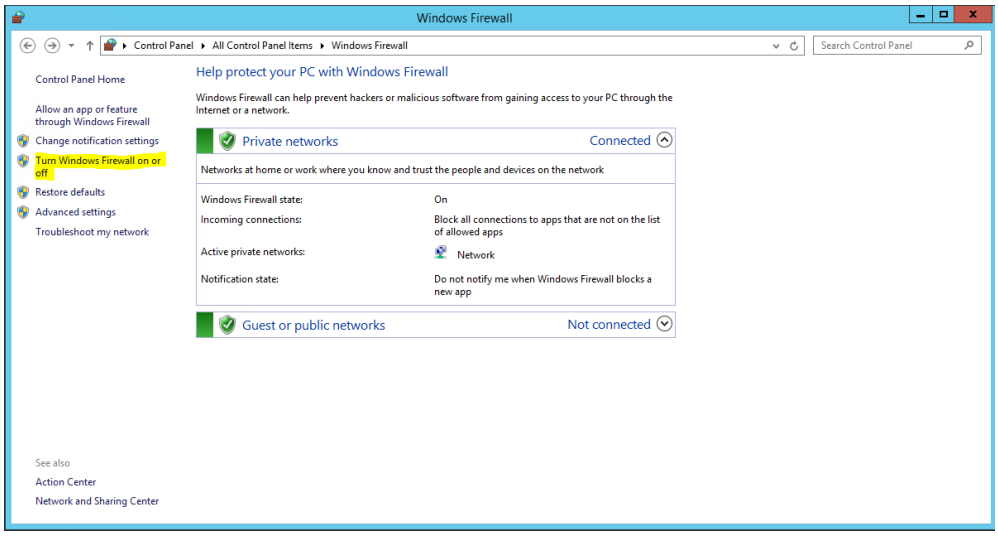

When the scan has finished list all open ports and what services or applications are running on them.

Are there any ports that shouldn't be open?
And if there is explain why they should be closed.

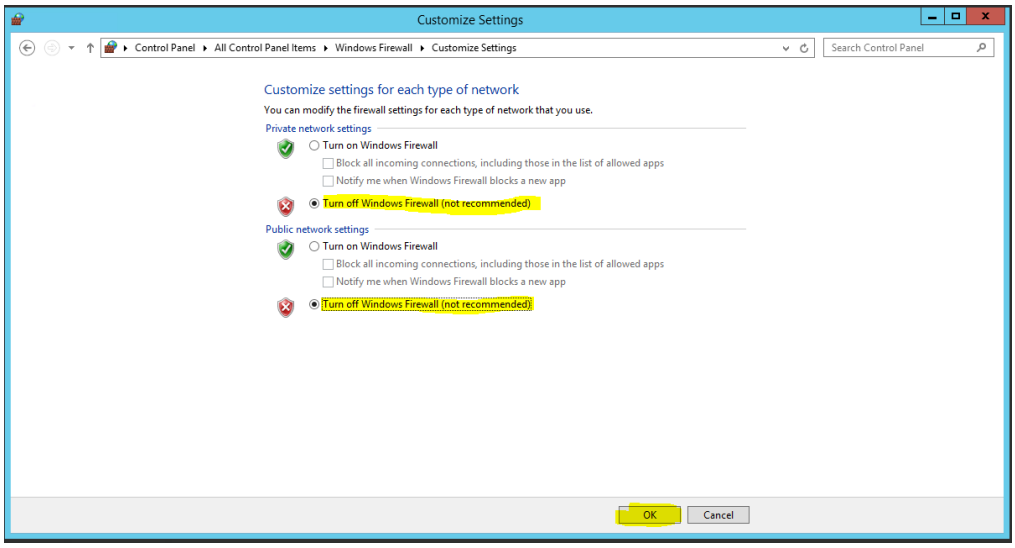
## Assignment 5: Configuring Windows Firewall

Open Windows Firewall by going to Control Panel\All Control Panel Items\Windows Firewall.

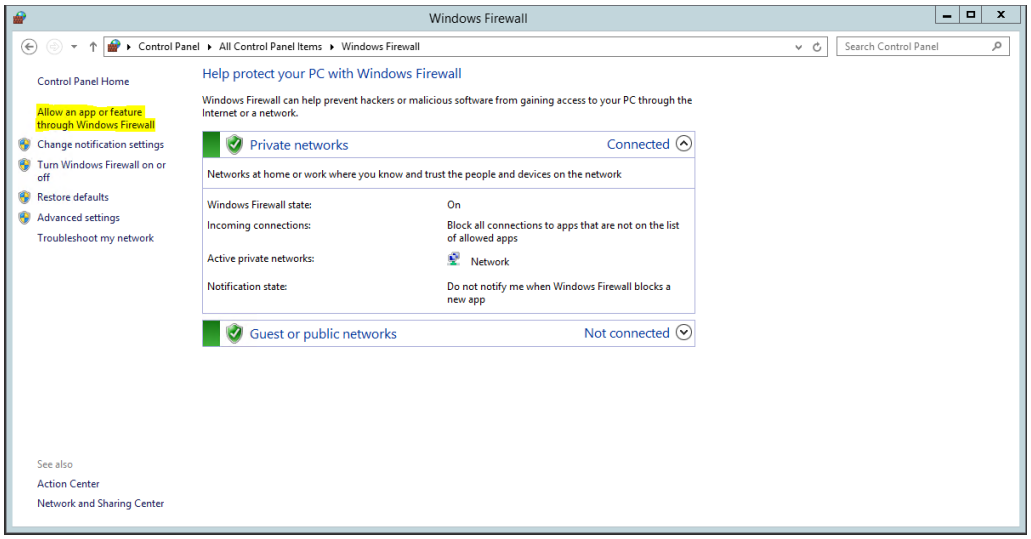
You can completely turn off Windows Firewall from the left panel.



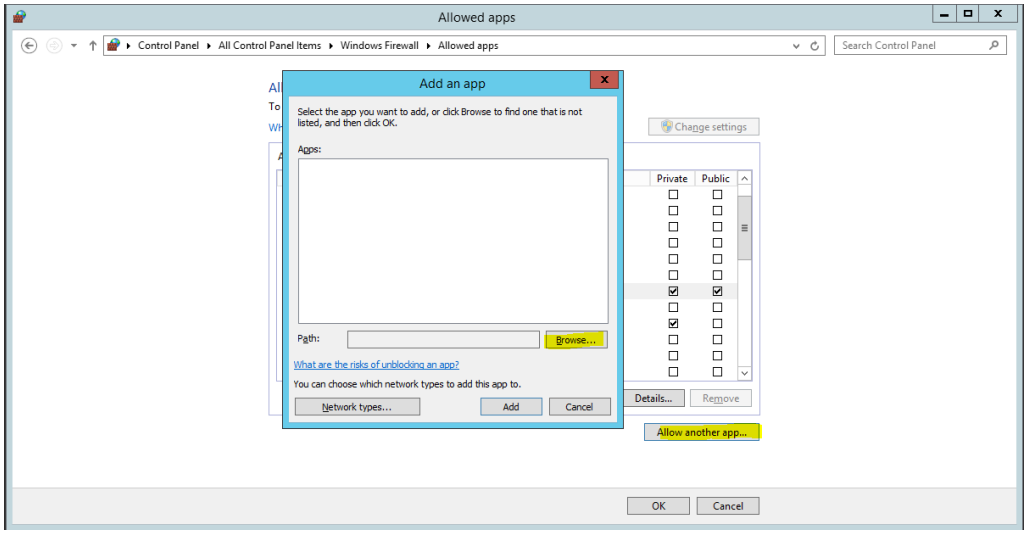
Check both “Turn off Windows Firewall” boxes and press OK.



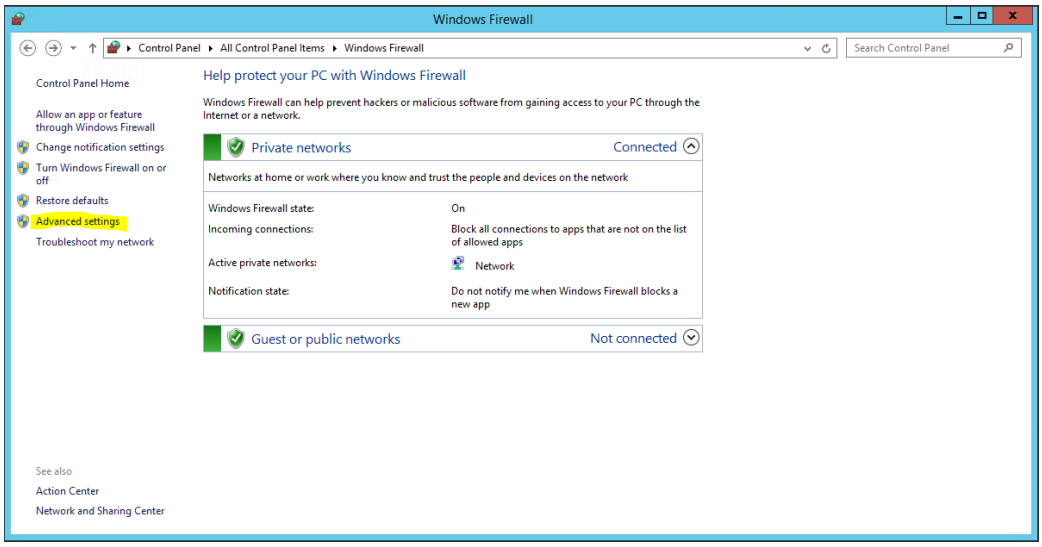

Allow only certain application or feature through Windows Firewall from the left panel.




You can give specific app an access by clicking “Allow another app” and then click “Browse”.



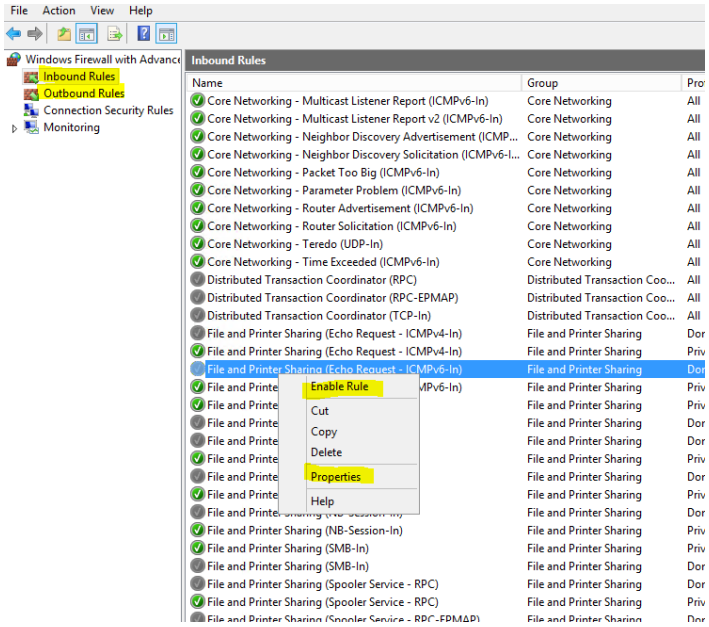

Open Advanced settings from left panel.




Going through inbound and outbound rules you can see what rules are enabled and what rules are disabled. When right clicking a rule, you can enable/disable the rule or click properties to find more information about the rule. You can also see what ports and protocols they are using.

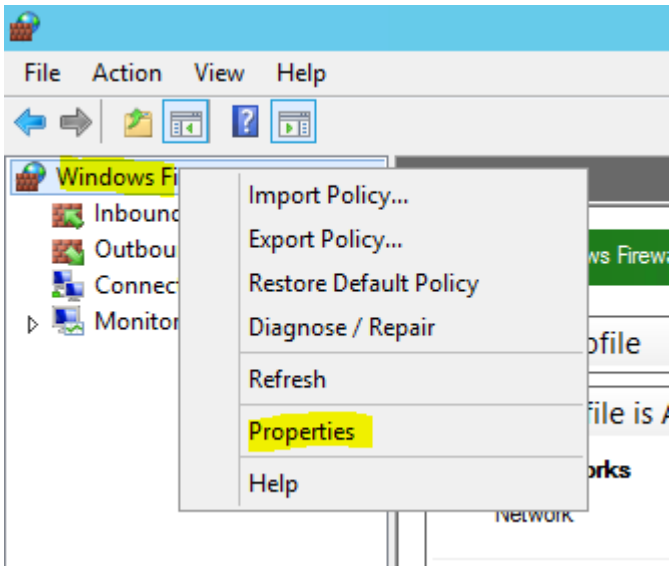
Explain what is the difference with outbound rules and inbound rules.

Explain why some rules are enabled and some are disabled.



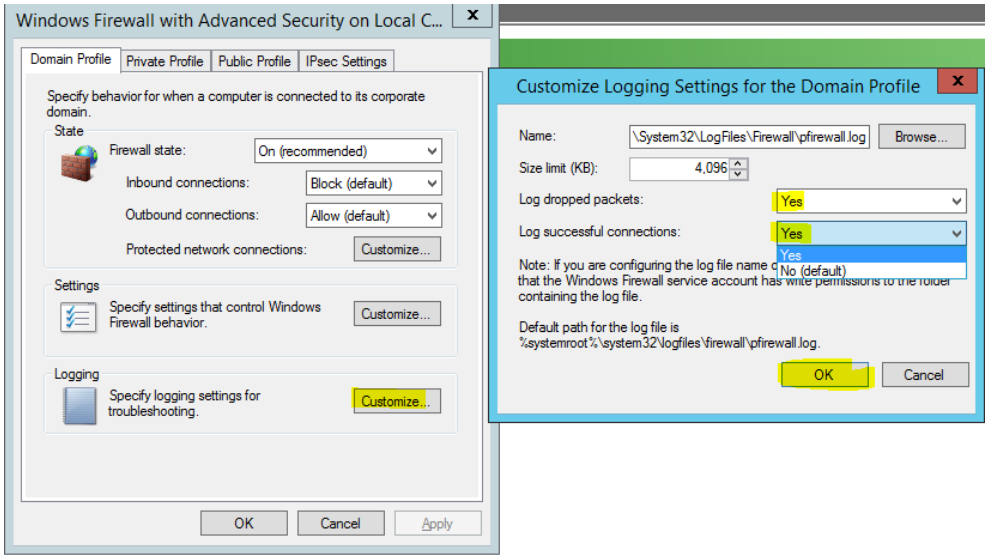

Enable logging.

Right click “Windows Firewall with advanced settings” and click “properties”.

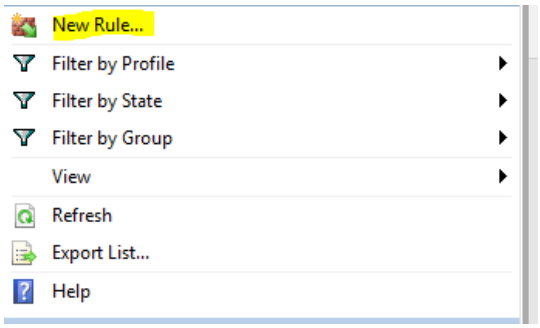


Click “Customize” in logging section and choose option “Yes” on “Log dropped packets”, “Log successful connections” and then press “OK”

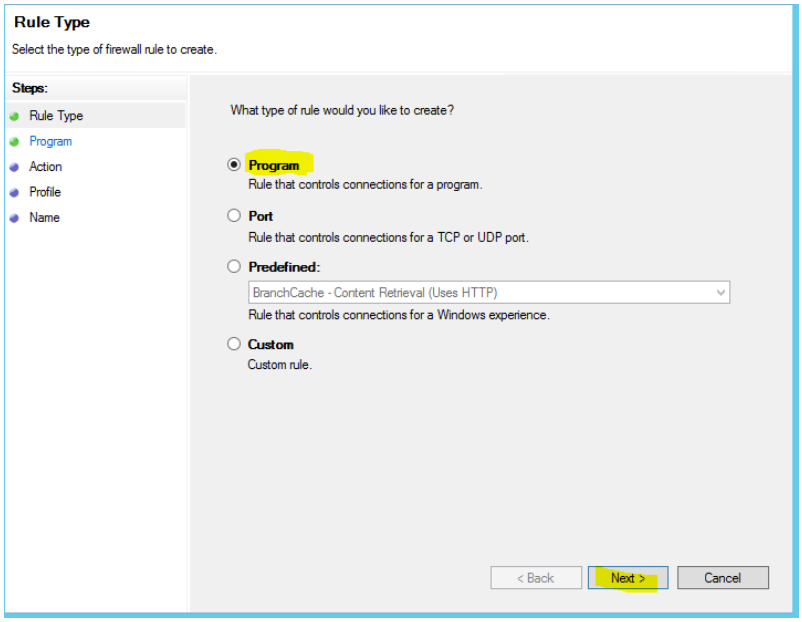
Repeat the same steps on “Private Profile” and “Public Profile”.




Now make a rule that blocks Internet Explorer having access to Internet.
Explain what kind of rule you must make (Inbound or Outbound).
After that choose “New rule” from left right panel after clicking “Inbound rules” or “Outbound rules”

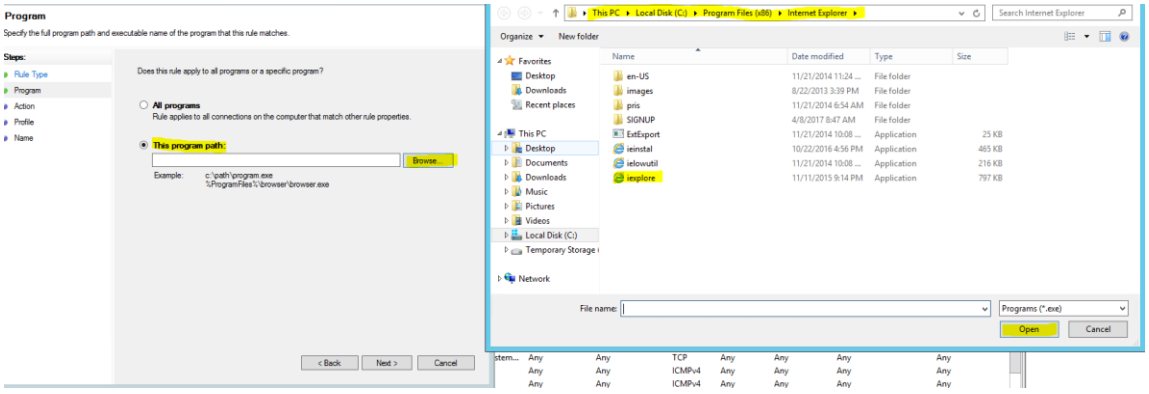



Choose “Program” and click “Next”.

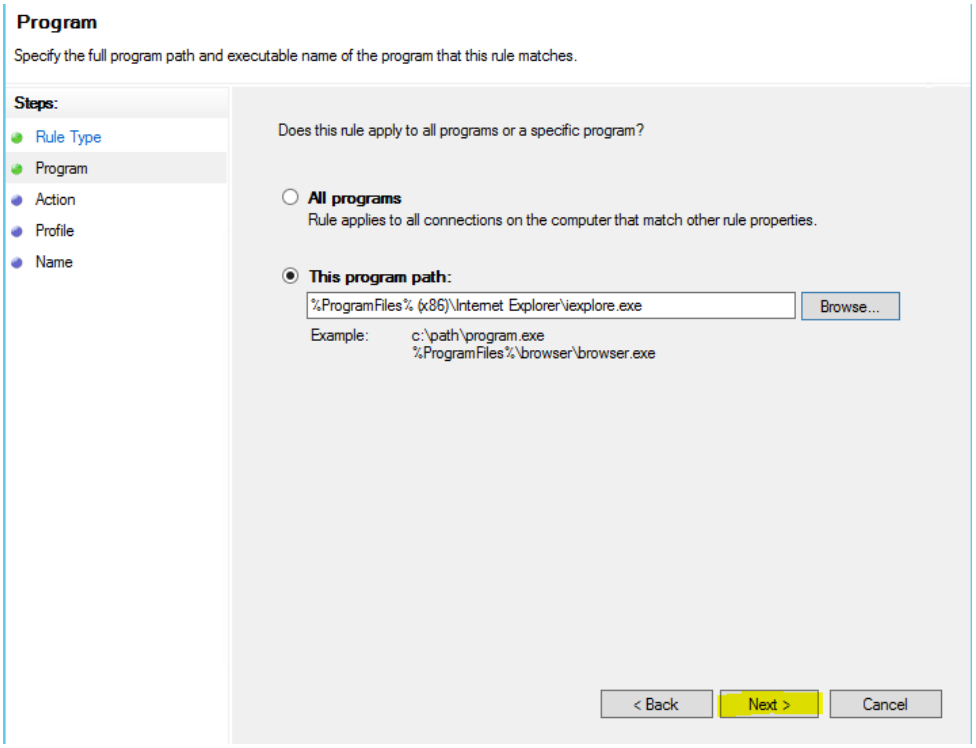



Choose “This program path” and click “Browse”.

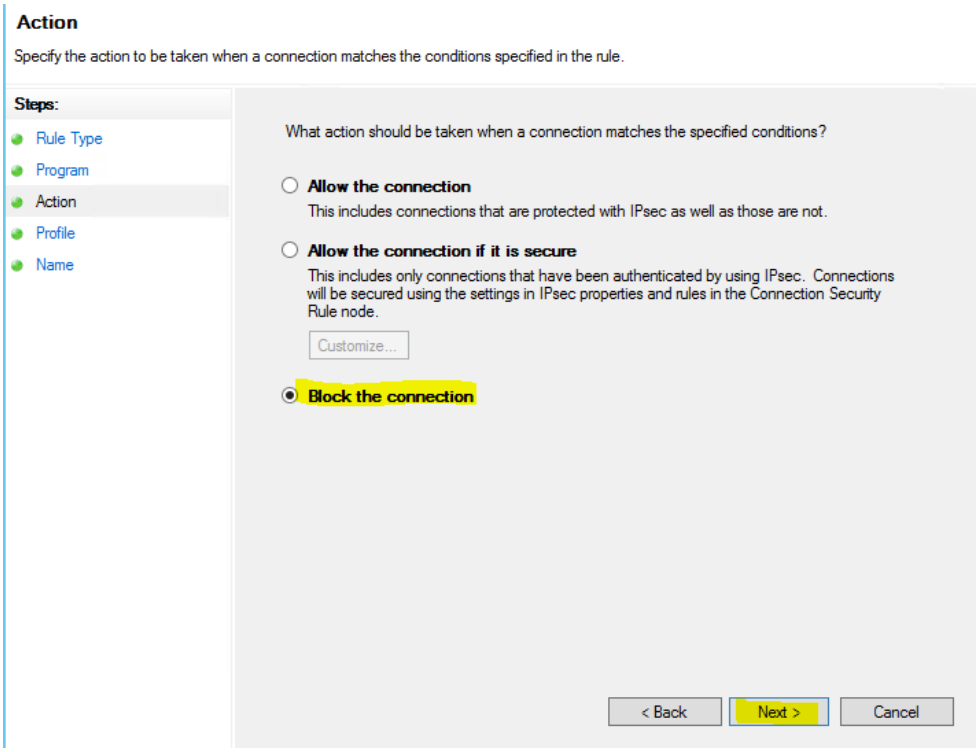
Navigate where Internet Explorer is installed on PC and choose it and click “Open”.



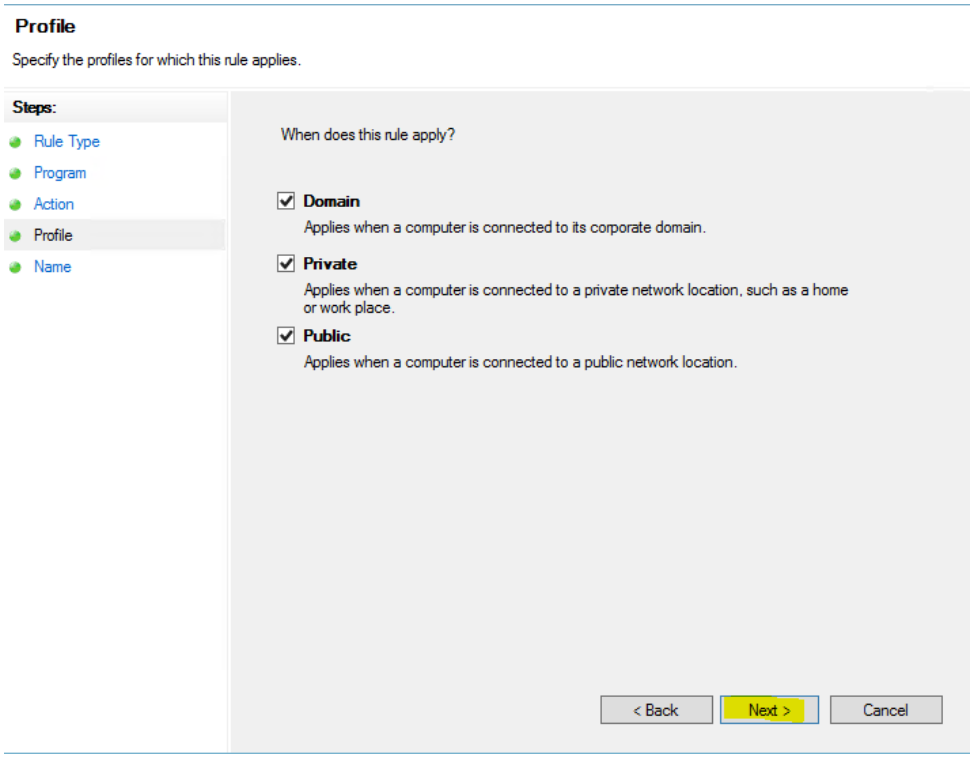

Then click “Next”.



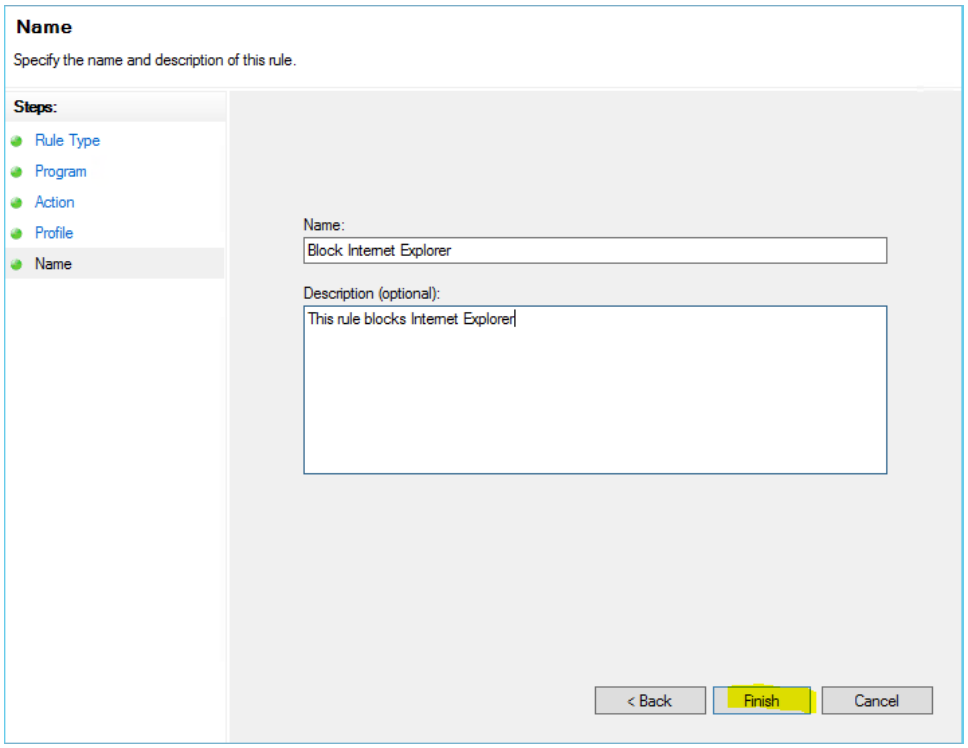

Choose “Block the connection” and click “Next”.




Keep all boxes checked and click “Next”.




Name the rule and then click “Finish” (Description is optional but recommended).




Open Internet Explorer and verify that the rule applies.

Open the Firewall log file and explain the results.

(Type the default path file in file explorer: %systemroot%\system32\logfiles\firewall\)

With Windows Firewall with Advanced Security you can open and close TCP/UDP ports.
You can try to close some open ports that you found with Nmap on previous lab.
You can also block specific IP addresses.
Block the IP address which you found on Footprinting lab and try to ping that.
Check the logs again.