jamk.fi

Tietoturvahaasteen suunnittelu ja toteutus

Case: Taitaja2020

Aku Karttunen

Opinnäytetyö
Huhtikuu 2020
Tekniikan ala
Insinööri (AMK), Tieto- ja viestintätekniikka
Kyberturvallisuus

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Karttunen Aku	Opinnäytetyö, AMK	Huhtikuu 2020
	Sivumäärä 85	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Tietoturvahaasteen suunnittelu ja toteutus

Case: Taitaja2020

Tutkinto-ohjelma

Insinööri (AMK) tieto- ja viestintätekniikka

Työn ohjaaja(t)

Jari Hautamäki, Sampo Kotikoski, Juha Piispanen

Toimeksiantaja(t)

JYVSECTEC/JAMK, Karo Saharinen

Tiivistelmä

Taitaja-kisat ovat vuosittainen tapahtuma, jolla mitataan ammattikoululaisten osaamista eri osa-alueilla ja aloilla. Tehtävänä oli suunnitella Taitaja2020-kisojen finaaliin tietoturva-tehtävä tietokoneet ja -verkot kategoriaan.

Tutkimuksen tavoitteena oli selvittää ammattikoululaisten kykyä havainnoida tietoturva-poikkeamia ja tutkia, toimiiko CTF-harjoitukset kiinnostavana tapana tutustua tietoturvail-miöihin.

Tutkimus toteutettiin kehittämistutkimuksena hyödyntäen kvalitatiivisten ja kvantitatiivi-sen tutkimuksen metodeja. Haasteeseen osallistuvien kilpailijoiden suorituksia analysoitiin suoritusajan, pistekeskiarvon, mediaanin ja kilpailijoiden pisteskaalan perusteella. Kilpaili-joille toteutettiin myös palautekysely finaalitehtävästä. Palautekyselyn perusteella arvioi-tiin harjoituksen kiinnostavuutta ja hyödyllisyyttä tietoturvataitojen suhteen.

Tietoturvahaasteeseen osallistuneet kilpailijat eivät juurikaan onnistuneet havaitsemaan haasteessa olleita tietoturvapoikkeamia. Testihenkilönä toiminut AMK-opiskelija kykeni ha-vaitsemaan selkeästi paremmin haasteessa ilmenneet tietoturvapoikkeamat. Kaikki tieto-turvahaasteeseen osallistuneet kuitenkin kokivat harjoituksen kiinnostavana tapana lähes-tyä tietoturvailmiöitä. Kaikki osallistujat kokivat saaneensa paremman käsityksen harjoituk-sessa ilmenneistä tietoturvailmiöistä.

Tietoturvahaasteet toimivat kiinnostavana ja haastavana tapana lähestyä tietoturvaa. Tie-toturvahaasteiden koetaan myös parantavan käsitystä tietoturvailmiöistä. Kilpailijoiden kyky havaita tietoturvapoikkeamia riippuu kilpailijan taustasta.

Avainsanat (asiasanat)

CTF, Tietoturva, Tietoturvahaaste, Taitajakisat, Kyberturvallisuus

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Karttunen Aku	Bachelor's thesis	April 2020
		Language of publication: Finnish
	Number of pages 85	Permission for web publication: Yes

Title of publication

Designing and creating CTF challenge

Case: Taitaja2020

Degree programme

Information and Communications Technology

Supervisor(s)

Jari Hautamäki, Sampo Kotikoski, Juha Piispanen

Assigned by

JYVSECTEC/JAMK, Karo Saharinen

Abstract

Taitaja2020 skill competition is an annual event that measures the skills of vocational school students in different areas of expertise.

The task was to design an information security themed challenge for the Computers and Networks category of the Taitaja2020 final. The aim of the study was to study the finalists' skills and abilities in detecting security breaches as well also study whether the finalists find the CTF exercise an interesting way to familiarize themselves with the areas of cyber security.

The research was carried out as a development study both qualitative and quantitative research methods. The performances of the competitors were analyzed quantitively based on the performance time, average score and median between the competitors and a score scale between the competitors. The results of the competitors were then compared to the score of a bachelor's student to give the results a reference point. A feedback survey was also issued for the competitors about the exercise's usefulness and how the exercise has improved their skills.

Competitors participating in the security challenge were hardly able to detect the security breaches in the challenge. The bachelor's student was able to detect the security breaches occurring in the challenge significantly better. All participants found the exercise an interesting way to approach cyber security and felt that the exercise increased their skills.

CTF exercises serve as an interesting way to approach cyber security. CTF exercises also improved the competitor's skills. The ability of the competitors to detect the security breaches depends on the competitor's background.

Keywords/tags (subjects)

CTF, Information security, Cyber security challenge, Taitaja competition, Cyber Security

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenteet

AD	Active Directory
AD DS	Active Directory Domain Services
C2	Command and Control
CCDC	Collegiate Cyber Defense Competition
CIFS	Common Internet File System
CIS	Competition Information System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
KDC	Key Distribution Center
LAN	Local Area Network
MIT	Massachusetts Institute of Technology
NSS	Name Service Switch
PAM	Pluggable Authentication Module
RAM	Random Access Memory
RPC	Remote Procedure Calls
SMB	Server Message Block
SSO	Single-sign on
SSH	Secure Shell
TGT	Ticket-granting ticket
UAC	User Account Control
VPN	Virtual Private Network
WAN	Wide Area Network

1 Johdanto

1.1 Työn taustat

Opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa ammattiin opiskelevien Taitaja2020-kisoihin finaalitehtävä tietoturvamoduuliin tietokoneet ja -verkot kategoriaan. Taitajakisat ovat vuosittain järjestettävä ammatilliseen perustutkintoon opiskelevien nuorten SM-kisat (Taitaja-tapahtuma n.d.). Opinnäytetyössä suunniteltiin ja toteutettiin tietoturvahaaste virtuaaliympäristönä, jolla pyrittiin vastaamaan mahdollisimman hyvin tieto- ja tietoliikennetekniikan pt. opetussuunnitelmassa esitettyjä osaamisvaatimuksia. Tietoturvapoikkeamiksi on valittu mahdollisimman realistisia ja ajankohtaisia ilmiöitä, joita kyseisiin järjestelmiin voisi kohdistua. Vastaavia opinnäytetöitä ei ole aiemmin tehty. Tietoturvahaasteessa myös painotettiin tietoturvapoikkeamien havainnointia. Useimmat tietoturvahaasteet on suunniteltu hyökkääjän näkökulmasta, joten näkökulma tietoturvahaasteen suunnitteluun on myös uusi. Tärkeimpänä tutkimustavoitteena opinnäytetyöllä olikin kartoittaa ammattiin opiskelevien nuorten osaamista ja havainnointikykyä tietoturvapoikkeamien parissa.

Teoriaosuudessa käydään läpi keskeisimmät tekniikat harjoituksen osalta, sekä myös harjoituksessa esiintyvät tietoturvailmiöt. Työssä pyrittiin suunnittelemaan sopivan haastava tietoturvahaaste ammattiin opiskeleville, joka vastaisi mahdollisimman hyvin todenmukaista tilannetta. Haasteessa ei ole tarkoituksena pyrkiä estämään tietoturvapoikkeamaa vaan pyrkiä havainnoimaan tietoturvapoikkeamaa ja saada kilpailijat ymmärtämään kyseisiä tietoturvailmiöitä. Haasteessa on pyritty asettamaan tehtäväpisteet, siten että ne kuvastaisivat mahdollisimman hyvin IT-tukihenkilön työtehtäviä ja osaamistasoa. Haasteen virtuaaliympäristöä on rajattu ja kuvattu pienen yrityksen olennaisimmat sisäiset palvelut ja ulkoiset palvelut, kuten toimialueen hakemistopalvelut ja verkkosivut.

Toimeksiantaja

Toimeksiantajana työlle toimi Jyväskylän ammattikorkeakoulun (JAMK) IT-instituutin lehtori Karo Saharinen. IT-instituutti on osa JAMKin teknologiayksikköä. JAMKin teknologiayksikössä opiskelee noin 2700 opiskelijaa. Teknologiayksikössä työskentelee noin 170 työntekijää koulutuksen, palveluliiketoiminnan ja TKI-toiminnan parissa. Tieto- ja viestintätekniikan tutkinto-ohjelma on saanut kansainvälisen EUR-ACE Bachelor -laatuleiman. (Teknologiayksikkö n.d.)

Taitajakisat

Taitajakisa on vuosittain järjestettävä ammattitaidon SM-kilpailut ammattiin opiskeleville nuorille. Vuoden 2020 semifinaaleihin osallistui tammikuussa valtakunnallisesti lähes 1500 kilpailijaa. Näistä 1500 kilpailijasta noin 350 kilpailijaa kilpailee Taitaja2020-finaalissa Jyväskylässä 11.-14.5.2020. Taitaja2020-tapahtumaan odotetaan saapuvan noin 40 000 kävijää. (Taitaja2020 2020.)

Kategoriaan 205 Tietokoneet ja -verkot osallistuu kahdeksan kilpailijaa. Kategoriat koostuvat useista eri tehtävistä ja tehtävien suorittamiseen on varattu aikaa keskimäärin 4 tuntia. Tehtävien arvioinnissa käytetään CIS-järjestelmää. CIS eli Competition Information System on Hämeenlinnan ammattikorkeakoulussa kehitetty pistelaskujärjestelmä, joka on myös ollut käytössä kansainvälisissä kilpailuissa (Vaahtera 2014.). Suunnitellussa tietoturvahaasteessa käytetään määrällistä arviointia.

Kisailijoiden lähtökohdat

Opetushallituksen määräyksessä tieto- ja tietoliikennetekniikan perustutkinnosta tietokone- ja tietoliikenneasennukset osiossa määritellään ammattitaitovaatimuksiksi monia asioita. Opiskelijan tulee muun muassa osata ottaa käyttöön tietokoneen suojaus- ja lisäominaisuudet, hallita asennusten automatisoinnin, tietoturvan sekä varmennukset. Opiskelijan tulee myös osata paikallistaa ja korjata laitteisto- ja ohjelmisto-ongelmia. (OPH M:84/011/2014, 65.)

Ammattikoululaisten tulisi siis ainakin ammattitaitovaatimusten perusteella olla jokseenkin perehtyneitä tietoturvaan sekä pystyvän paikallistamaan ohjelmisto- ja lait-

teisto-ongelmia. Opetushallituksen määräyksessä ei listata selkeitä osaamisvaatimuksia juuri tietoturvan suhteen. Opiskelijalta ei siis sovi odottaa kovin syvällistä osaamista. Voidaan kuitenkin olettaa, että opiskelijat ymmärtävät perustietoturvailmiöt, kuten haittaohjelmat ja niiden perusperiaatteet.

1.2 Tutkimuskysymykset ja -menetelmät

Tutkimuksessa käytettiin kehittämistutkimuksen menetelmiä. Tarkoituksena oli suunnitella tietoturvahaaste virtuaaliympäristönä. Virtuaaliympäristöllä mitattiin kilpailijoiden taitoja ja tietämystä tietoturvan ja tietoturvailmiöiden suhteen. Virtuaaliympäristöä oli tarkoitus käyttää Taitaja2020-kisoissa. Taitaja2020-kisoista kertyi aineistoa tutkimukseen. Aineistoa analysoitiin kvantitatiivisesti sekä kvalitatiivisesti. Keskeisinä tutkimuskysymyksinä työssä olivat:

Mikä on kilpailijoiden taso havainnoida tietoturvapoikkeamia suljetussa ympäristössä?

Toimiiko CTF-harjoitus kiinnostavana tapana tutustua ja tutkia tietoturvapoikkeamia ja parantavatko ne käsitystä tietoturvapoikkeamista?

Lisäksi tutkimuskysymyksiä täydentävät seuraavat alakysymykset:

Kykenevätkö kilpailijat asettamaan harjoituksen tapahtumat aikajärjestykseen?

Kokevatko kilpailijat tietoturvaopetuksen koulussa riittäväksi?

Tutkimuskysymyksiin vastattiin analysoimalla tietoturvahaasteeseen osallistuneiden kilpailijoiden tuloksia. Kilpailijoille toteutettiin myös palautekysely, jonka avulla saatiin vastauksia tutkimuskysymyksiin. Tuloksia analysoitiin kokonaisvaltaisesti ja tehtäväkohtaisesti. Saatuja tutkimustuloksia tuettiin aiemmilla tutkimustuloksilla. Tutkimuskysymyksiin saatiin myös vertailukohta AMK-opiskelijan suorituksesta. AMK-opiskelija toimi tietoturvahaasteen testihenkilönä, jonka avulla kartoitettiin mahdollisia ongelmakohtia tietoturvahaasteessa.

Kehittämistutkimus

Kehittämistutkimus pyrkii tuottamaan toimivia käytännön ratkaisuja. Kehittämistutkimuksessa yhdistyy kehittäminen ja tutkimus syklisessä prosessissa. Kehittämistutkimus koostuu useista eri tutkimusmenetelmistä, joita käytetään riippuen tutkimusongelmasta ja kehittämiskohteesta. Kehittämistutkimus on monimenetelmäinen tutkimustapa, jossa yhdistyy tarpeen mukaan laadulliset ja määrälliset tutkimusmetodit. (Kananen 2015, 33–34.)

Kvantitatiivinen tutkimus

Kvantitatiivista tutkimusta kutsutaan myös määrälliseksi tutkimukseksi tai tilastolliseksi tutkimukseksi. Kvantitatiivisen tutkimuksen avulla selvitetään lukumääriin ja prosenttiosuuksiin liittyviä kysymyksiä. Tutkimuksessa onkin tärkeää ottaa huomioon otannan suuruus ja sen edustavuus. Aineistonkeruussa käytetään yleensä standardoituja tutkimuslomakkeita valmiine vastausvaihtoehtoineen. Asioita kuvataan numeeristen suureiden avulla ja tuloksia havainnollistetaan yleensä erilaisin kuvioiden ja taulukoiden avulla. Kvantitatiivisen tutkimuksen yhteydessä usein tutkitaan myös asioiden välisiä riippuvuuksia. Kvantitatiivisen tutkimuksen avulla saadaan yleensä kartoitettua olemassa oleva tilanne. (Heikkilä 2014, 15.)

Työssä tutkittiin harjoituksen suorittavien kesken, mikä on kilpailijan suoritusaika, pistekeskiarvo, mediaani ja mille skaalalle osanottajien pisteet levittäytyvät. Yksittäisillä tehtäväpisteiden tai flagien sijoittamisella taas pyrittiin kartoittamaan osaamistilannetta erilaisten tietoturvapoikkeamien havainnoinnin suhteen.

Kvalitatiivinen tutkimus

Kvalitatiivinen eli laadullinen tutkimus pidetään usein kvantitatiiviseen tutkimukseen rinnastettavana sosiaalitutkimuksen metodina. Laadullisen ja määrällisen tutkimuksen metodit kuitenkin eroavat toisistaan. Vaikkakin nämä kaksi tutkimusmetodia eroavat toisistaan, ei niiden erottaminen toisistaan vastaa hyvin todellisuutta. Kaikessa tieteellisessä tutkimuksessa on paljon yhteisiä pyrkimyksiä, kuten pyrkimys loogiseen todisteluun ja objektiivisuuteen. Kvalitatiivisen ja kvantitatiivisen analyysin voi

erottaa toisistaan, mutta niitä voidaan myös soveltaa yhdessä saman tutkimusaineistoon. Laadullista ja määrällistä tutkimusta voidaankin pitää toistensa jatkumoina eikä poissulkevina vaihtoehtoina. (Alasuutari 2011, 26–28.)

Laadullisessa analyysissa ainestoa tarkastellaan usein kokonaisuutena. Laadullisessa analyysissa tilastolliset todennäköisyydet eivät kelpaa johdatteluiksi. Kvalitatiivisessa tutkimuksessa tutkimuksen suuri joukko tai tilastollinen argumentointi ei ole tarpeen taikka edes mahdollista. Laadullinen analyysi koostuu kahdesta osuudesta: havaintojen pelkistämisestä ja arvoituksen ratkaisemisesta. Havaintojen pelkistämisessä ainestoa tarkastellaan tietystä teoreettisestä näkökulmasta. Silloin kiinnitetään huomiota siihen, mikä on oleellista teoreettisen viitekehyksen kannalta. Arvoituksen ratkaisemisella tarkoitetaan puolestaan tulosten tulkintaa, laadullisen tutkimuksen tuloksia tulkitaan etsimällä esimerkiksi mahdollisia yhteyksiä tilastollisen tutkimuksen tuloksiin. (Mts. 31–33, 35.)

Opinnäytetyössä tutkitaankin ainestoa hyödyntäen myös laadullisen tutkimuksen menetelmiä tilastollisen tutkimuksen menetelmien lisäksi. Määrällisen tutkimuksen lisäksi aineistosta tehtiin havaintoja keskeisistä asioista teoreettisen viitekehyksen suhteen, sekä pyrittiin havaitsemaan yhteyksiä määrällisen tutkimuksen ja laadullisen tutkimuksen välillä.

Aineistonkeruumenetelmät

Laadullisen tutkimuksen aineistona toimivat erilaiset dokumentit, haastattelut ja havainnoinnit. Määrällisen tutkimuksen tiedot pohjautuvat tilastoihin ja kyselylomakkeisiin. (Kananen 2017, 67.) Kysely koostuu kysymyksistä, jotka koskevat tutkimusilmiötä. Kysely voidaan toteuttaa millä metodilla tahansa, on kuitenkin tärkeää saada edustava vastausjoukko kyselyllä. (Kananen 2015, 96–97.) Tutkimuksen aineisto kerättiin hyödyntäen laadullisen ja määrällisen tutkimuksen aineistonkeruumenetelmiä. Tutkimuksessa kerättiin tietoturvahaasteen suorittavilta kilpailijoilta palautekyselyllä mielipiteitä ja tuntemuksia tietoturvahaasteen vaikeuteen ja kiinnostavuuden suhteen. Kyselyllä tutkittiin myös kilpailijoiden kykyä tunnistaa tietoturvahaasteessa esiintyvät tietoturvapoikkeamat, sekä kilpailijoiden kykyä asettaa tietoturvahaasteen

tapahtumat aikajärjestykseen. Tietoturvahaasteeseen osallistuneiden suoritukset tilastoitiin ja analysoitiin käyttäen määrällisen tutkimuksen menetelmiä.

Aineistonanalyysimenetelmät

Tutkimustulosten analysoinnissa käytettiin laadullisen ja määrällisen tutkimuksen keinoja. Palautekyselyä tutkittiin laadullisen analyysin lähiluku metodilla. Lähiluvulla tarkoitetaan kirjallisten tekstien analyysia ja tulkintaa (Lähiluku 2015.). Erotteluanalyysia käytetään aineiston analyysissä silloin, kun on olemassa jokin ryhmittelevä muuttuja. Ryhmittelyanalyysin avulla pyritään määrittelemään millaisia samaan ryhmään kuuluvat ovat. (Kananen 2015, 109–110.) Tutkimuksen ryhmittelevä tekijä oli kilpailijan tietoturvaosaaminen, eli kuinka hyvin kilpailija pärjää tietoturvahaasteessa.

1.3 Capture the flag -harjoitukset

CTF eli Capture the flag -harjoitukset ovat eräänlaisia tietoturvakilpailuita. CTF-harjoituksiin voidaan osallistua joko ryhmissä tai yksilöinä riippuen kilpailusta. CTF-harjoitukset ovat usein ensimmäinen kosketuspinta kyberturvallisuusuraan juuri ryhmätyöskentelyn ja kilpailuasenteen vuoksi. Aihealueita CTF-harjoituksissa voivat olla esim. forensiikka, kryptografia, web-haavoittuvuuksien hyödyntäminen, takaisinmallinnus (reverse engineering) tai binääritason haavoittuvuuksien hyödyntäminen. (CTF 101 n.d.)

Google järjestää vuosittain CTF-harjoituksen, joka koostuu useista erilaisista tietoturvailmiöistä, kuten kryptografiasta ja web-tekniikoista. Tavoitteena osallistujilla on kerätä harjoituksesta tehtäväpisteitä eli lippuja. Googlen mukaan CTF-harjoitukset ovat hyväksi muun muassa ammattilaisille, jotka pyrkivät ylläpitämän ja kehittämään omaa ammattitaitoaan, mutta ne ovat mielenkiintoinen lähestymistapa myös vastaalkajille. (Google CTF 2019.)

Collegiate Cyber Defense Competitionin (CCDC) tarkoituksena on tarjota eri instituuteille kilpailuympäristö tietoturvaan liittyen. CCDC:n ympäristöt on suunniteltu arvioimaan opiskelijan ymmärrystä tietoturvailmiöiden parissa, sekä kyvykkyyttä hallita yri-

tyksen verkkoinfrastruktuuria. CCDC-tapahtumien tavoitteena on tarjota korkeakouluille työkalu, jolla korkeakoulut voivat mitata omia tietoturvakoulutusohjelmiaan. Näissä harjoituksissa pyritään yhdistämään kursseilla opitut teoriat ja käytännön taidot, sekä mitata niitä. Tapahtumien tavoitteena on myös herättää kiinnostusta ja tietoisuutta koulujen ja opiskelijoiden välillä. CCDC:n harjoitusympäristöt ovat kooltaan noin 50 työntekijän yrityksiä, joilla on verkkoinfrastruktuurissaan noin 7–10 palvelinta. Palvelimilla toimii useita eri palveluita, kuten yrityksien verkkosivut. CCDC-tapahtumissa eri tiimit saavat identtiset ympäristöt ja heidän tavoitteenansa ylläpitää yrityksen palveluita. Tiimien tavoitteena on myös havaita ja reagoida yritykseen kohdistuviin tietoturvauhkiin. (CCDC mission 2019.)

CTF-harjoituksia pidetään yleisesti hyvänä lähestymistapana tietoturvaan ja keinona havainnollistaa tietoturvauhkia kilpailijoiden keskuudessa, sekä mitata yksilöiden osaamista tietoturvailmiöiden parissa.

Tutkimustuloksia tietoturvahaasteista

Vuonna 2017 Teksasin yliopistossa tehdyn tutkimuksen mukaan kyberturvallisuuskilpailut saavat vuosittain enemmän huomioita merkittävänä tapana edistää kyberturvallisuuden opiskelua. Tutkimuksen mukaan on elintärkeää etsiä parempia keinoja saada vasta-alkajat mukaan tietoturvakoulutuksen laadun parantamiseen. Tutkimuksen mukaan CTF-harjoituksia järjestetään opetusmielessä, harjoitusmielessä sekä rekrytointien yhteydessä. Tutkimuksessa kerättiin noin 3600 eri CTF-haastetta 160 eri tietoturvakilpailusta. Tutkijat rakensivat oman CTF-haasteen opiskelijoille, ja haasteen sisältö sai positiivista palautetta. Haasteessa oli eritasoisia haasteita kuudesta eri kategoriasta: kryptografia, web-haavoittuvuudet, takaisinmallinnus, forensiikka, pwn eli erilaisia haittaohjelmia ja sekalaiset haasteet. Tutkimuksen kohderyhmä koostui 46 opiskelijasta, joille käsitteet ja tekniikat olivat jossain määrin tuttuja. Vain 8% oppilaista selviytyi haasteesta omatoimisesti. Tutkimuksessa keskityttiin hyökkääjän näkökulmaan, eikä puolustavan osapuolen näkökulmaan. (Burns, Gu, Jordan, Rios & Underwood 2017.)

Vuonna 2015 Tom Chothia ja Chris Novakovic tutkivat kuinka erään kurssin harjoitustyönä toiminut CTF-harjoitus korreloituu opiskelijan muihin suorituksiin kurssilla.

Kurssin harjoitustyönä toimineesta haasteesta paljastettiin viikoittain pienempiä osahaasteita opiskelijoille ratkaistavaksi. CTF-harjoitus koostui useista eri aihealueista kuten kryptologiasta ja web-haavoittuvuuksien löytämisestä. Tuloksista huomattiin oppilaiden kokeneen kurssin harjoitustyön haastavana, mutta kiinnostavana tapana tutkia harjoituksen tietoturvailmiöitä. Tuloksissa huomattiin myös, että opiskelijoiden löytämien lippujen määrä, eli osaaminen CTF-harjoituksessa korreloitui vahvasti opiskelijan osaamiseen teoriaosuudessa. (Chothia & Novakovic 2015.)

Tutkimusten perusteella tietoturvahaasteet toimivat myös hyvin kurssien harjoitustöinä. Tietoturvahaasteita voidaan myös käyttää rekrytointikeinona ja ne koetaan usein haastavina ja kiinnostavana keinona lähestyä tietoturvaa. Usein tietoturvahaasteet keskittyvät haavoittuvuuksien löytämiseen, eikä niinkään puolustavan osapuolen näkökulmaan eli tietoturvapoikkeamien havainnointiin.

Harjoitusten dokumentointi

Kyberharjoituksista saatu tieto tulisi aina dokumentoida. Harjoituksissa opittujen asioiden tulisi pyrkiä ottamaan huomaan kilpailijoiden erilaiset lähestymistavat harjoituksessa. Harjoituksen tulokset paljastavat usein hyvin toimivat osastot organisaatiossa, sekä organisaation mahdolliset puutteet tietoturvan suhteen. Harjoituksen aikana ja sen jälkeen kerätty palaute on arvokasta tietoa, jolla pystytään kehittämään kyberharjoituksia ja parantamaan harjoituksien hyödyllisyyttä. Tärkeää harjoituksissa on määrittää selkeästi harjoituksen tavoitteet. (Kick 2014, 20.)

1.4 Tietoturvapoikkeamat ja niiden hallinta

Tietoturvapoikkeama

Tietoturvapoikkeamaksi kutsutaan sellaista tapahtumaan, jossa on tapahtunut mahdollinen tietomurto tai tietoturvakontrollit ovat pettäneet. Tietoturvapoikkeama voi olla yksittäinen tai useiden tapahtumien sarja, jossa tapahtumat vastaavat aiempaa kuvausta ja kyseiset tapahtumat voivat mahdollisesti vahingoittaa yrityksen omaisuutta tai vaarantaa sen toimintaa. Tietoturvapoikkeaman ilmeneminen ei välttämättä tarkoita, että yritykseen kohdistunut hyökkäys on ollut onnistunut tai että sillä olisi ollut vaikutusta yrityksen luotettavuuteen (confidentiality), eheyteen (integrity)

tai saatavuuteen (accessibility), kaikkia tietoturvatapahtumia ei siis luokitella tietoturvaselkkaukseksi. (ISO/IEC 27035-1 2016, 2.)

Tietoturvaselkkaukset voivat olla tahallisia, kuten esimerkiksi tietoturvahyökkäyksen kohteena oleminen. Selkkaukset voivat myös olla tahattomia tapauksia, kuten inhimilliset erheet tai luonnonkatastrofit. Selkkauksien syntyperä voi olla joko tekninen, kuten haittaohjelmat tai sitten ei-tekninen, kuten varkaus tai laitteen katoaminen. Seuraamuksina tietoturvaselkkaukselle voi olla tietojen luvaton käyttö, muokkaus, tuhoaminen tai saatavuuden haittaaminen. Seuraamuksena voi myös olla yrityksen omaisuuden vaurioituminen. (Mts. 2.)

Tietoturvapoikkeamien hallinta

Tietoturvapoikkeamien hallintasuunnitelman tarkoituksena on pyrkiä dokumentoimaan kaikki aktiviteetit ja proseduurit mahdollisten tietoturvapoikkeamien ja haavoittuvuuksien suhteen, sekä tietoturvapoikkeaman aikana tapahtuneen kommunikoinnin. Yleisesti ottaen suunnitelman tulisi sisältää selkeät toimintatavat tietoturvapoikkeamien ja -selkkauksien hallintaan, tarvittavat työkalut tapahtumien havainnointiin. (ISO/IEC 27035-2 2016, 6–7.)

Tietoturvapoikkeamiin reagoimisessa tulisi pyrkiä pitämään mahdollinen selkkaus hallinnassa ja samalla pyrkiä määrittämään onko tapauksella vaikutusta yrityksen tuottamiin palveluihin. Poikkeaman sattuessa tulisi varmistaa, että kaikki todisteet on identifioitu, kerätty ja varastoitu oikein. Todisteita kerätään myöhempää analyysia varten. Jokaisesta tietoturvapoikkeamasta tulisi oppia jotain. Tutkimalla todisteita ja tapahtumien aikajanaa tulisi pyrkiä parantamaan yrityksen tietoturvakäytänteitä ja tarvittaessa myös tietoturvapoikkeamien hallintaa. (Mts. 11.)

Digital Forensics and Incident Response (DFIR) -harjoituksessa osallistujat tutkivat ympäristöön kohdistunutta tietoturvapoikkeamaa. DFIR-harjoitus on suunniteltu erityisesti teknisille asiantuntijoille, IT-päälliköille ja tietoturvapäälliköille, jotta organisaatioissa opittaisiin tunnistamaan paremmin tietoturvapoikkeamien eri indikaattorit ja reagoimaan niihin paremmin. (Digital Forensics and Incident Response exercise

2020.) Blue team CTF -harjoituksessa keskitytään uhkatoimijoiden toiminnan löytämiseen pelillistetyssä ympäristössä. Harjoituksessa on tarkoituksena etsiä hyökkääjän jättämät digitaalisesta todisteet ja koostaa hyökkääjän toimista aikajana. Harjoituksen jälkeen skenaario käydään läpi, jotta harjoitukseen osallistujat oppisivat löytämään paremmin hyökkääjien jättämät jäljet harjoitusympäristöstä. (Blueteam Capture the Flag, 2020.)

Tietoturvapoikkeamien havainnointi ja niiden dokumentointi on tärkeää, jotta olemassa olevia käytänteitä ja tietoturvapoikkeamien havainnointia voidaan yrityksissä parantaa. Hyvin dokumentoidun tietoturvapoikkeaman avulla yritykset pystyvät kehittämään omaa tietoturvaansa. Tietoturvahaasteen skenaario suunniteltiin Blue team CTF-harjoituksena, jossa kilpailijat pyrkivät havaitsemaan ympäristöstä tietoturvapoikkeamat ja hyökkääjän jättämät jäljet.

2 Virtuaaliympäristön suunnittelu

Tietoturvahaasteeseen suunniteltiin kuvitteellinen yritys. Kyseiselle kuvitteelliselle yritykselle suunniteltiin opetushallituksen määräyksen mukaisten osaamisvaatimusten perusteella verkkoinfrastruktuuri, jossa oli tarkoituksena havainnoida tietoturvahaasteen tietoturvapoikkeamia. Opetussuunnitelmassa olevien vähäisten tietoturvavaatimusten vuoksi virtuaaliympäristöä ja skenaariota suunniteltiin verkkoinfrastruktuuri edellä.

2.1 Tieto- ja tietoliikennetekniikan perustutkinnon osaamisvaatimukset

Tieto- ja tietoliikennetekniikan perustutkinnon palvelinjärjestelmät ja projektityöt osuudessa määritellään opiskelijan ammattitaitovaatimuksiksi mm. palvelimien verkkokäyttöjärjestelmien asennuksen ja pääkäyttäjän perustehtävät, sekä hakemistopalveluiden toimintaperiaatteet. Osaamistavoitteissa myös listataan palvelimien peruspalvelut, kuten nimipalvelut (DNS) ja dynaamisten verkkoasetusten jakelun ja hake-

mistopalveluiden hallitseminen. Samaisessa kokonaisuudessa mainitaan myös ryhmäkäytäntöjen (Group Policy) avulla käyttäjä-, tietokone- ja ohjelmistoasetuksien hallitseminen. Opiskelijan tulisi myös hallita WWW- ja FTP-palvelut, sekä palvelimien etäkäytön. (OPH M:84/011/2014, 40.)

Harjoituksen suunnittelussa pyrittiin vastaamaan mahdollisimman hyvin opetushallituksen määräyksessä esitettyihin osaamisvaatimuksiin. Ympäristössä toimiikin Windows Server 2012 R2 toimialueen pääpalvelimena ja sen keskeisinä palveluina toimii DNS, DHCP ja AD -palvelut. Tietoturvahaasteessa kilpailija asetetaan pääkäyttäjän rooliin ja hän vastaa mainittujen palveluiden turvallisuudesta ja toimivuudesta. Haasteympäristöön on myös lisätty sisäverkkoon tiedostopalvelin, jolla voidaan hyödyntää FTP-protokollan käyttöä. DMZ-alueelle (demilitarized zone) on lisätty myös web-palvelin, jota hallitaan SSH-yhteyden avulla, sekä web-käyttöliittymän kautta.

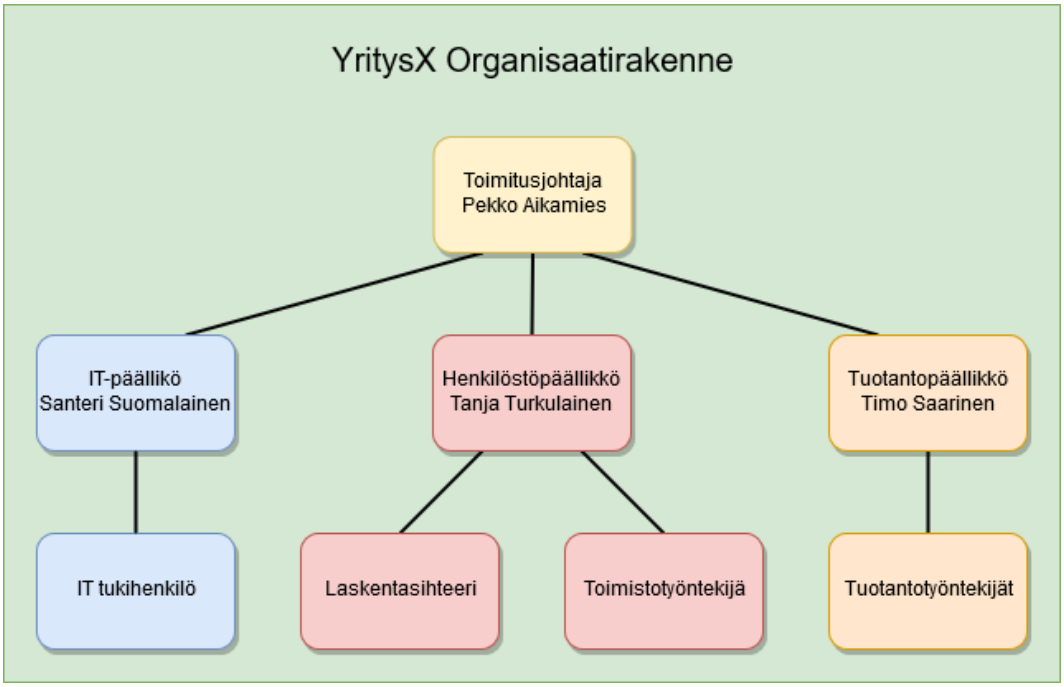
Varsinaisia tietoturvaosaamisvaatimuksia ei opetushallituksen määräyksessä sivuta kuin muutamilla selkeillä vaatimuksilla kuten, että opiskelija hallitsee palvelimien perus tietoturva-asiat (kuten salasanojen käyttö, tiedostojen suojaus ja palomuuri). Osaamisvaatimuksina on myös virustorjunta- ja haittaohjelmien poisto-ohjelmiston asentaminen palvelimiin, sekä suojatun etäyhteyden käyttäminen palvelimiin. (OPH M:84/011/2014, 40.)

Haasteympäristöön ei ole asennettu palvelimille erillisiä virustorjuntaohjelmistoja. Tarkoituksena oli tehdä haavoittuvainen ympäristö, jossa mahdollisia tietoturvapoikkeamia pystytään havainnoimaan ja analysoimaan. Tiedostojen suojaaminen on keskeinen asia haasteympäristössä. Arkaluonteiset tiedostot, kuten tuotesuunnittelua koskevat tiedostot halutaan pitää yrityksen sisällä ja estää mahdolliset tietovuodot. Salasanojen hallinnointi haasteympäristössä on varsinaisen loppukäyttäjän (esim. toimistotyöntekijä) vastuulla. Yrityksen sisäverkko eristettiin ulkoisesta verkosta palomuurilla. Harjoitusympäristön palvelimia hallittiin pääosin suojatun SSH-yhteyden avulla.

2.2 Kuvitteellisen YritysX:n kuvaus

2.2.1 Yrityksen toimiala ja organisaatiorakenne

YritysX on kuvitteellinen yhtiö, joka tuottaa tehtaallaan vinyylilevyjä. YritysX:n vuosittainen liikevaihto vuonna 2018 oli noin 1,5miljoonaa euroa. Yritys työllistää 12 henkilöä. Avainhenkilöitä yrityksessä on toimitusjohtaja Pekka Aikamies, henkilöstöpäällikkö Tanja Turkulainen, IT-päällikkö Santeri Suomalainen ja tuotantopäällikkö Timo Saarinen. Yritys on jaettu kolmeen osastoon HR-osasto, tuotanto ja IT-osasto (ks. kuvio 1).



Kuvio 1. YritysX:n organisaatiokaavio

HR-osasto

Toimitusjohtaja vastaa yrityksen suurista linjoista ja hoitaa pääosin markkinointi- ja myyntitehtäviä yrityksessä. Henkilöstöpäällikön alaisuudessa on laskentasihteeri ja yksi toimistotyöntekijä. Yrityksen laskentasihteeri hoitaa yrityksen palkanlaskennan

ja muun maksuliikenteen. Henkilöstöpäällikkö toimii ensisijaisena esimiehenä toimistotyöntekijälle ja laskentasihteerille ja on myös vastuussa yleisesti henkilöstön hyvinvoinnista. Toimistotyöntekijä hoitaa toimistonjuoksevia asioita, kuten tiedottamista ja myyntiä asiakkaiden suuntaan.

Tuotanto

Tuotantopäällikkö Timo Saarisen alaisuudessa on viisi tuotantotyöntekijää. Tuotantopäällikkö vastaa asiakkaalle tuotetuista levyistä. Tuotanto-osasto tuottaa päivittäin raportteja yrityksen johdolle tuotantovolyymeista ja tuotantolaadusta. Raporteilla pyritään analysoimaan tehtaalle tulevien tilausten toimitusaikoja ja mahdollisia ongelmakohtia tuotannossa.

IT-osasto

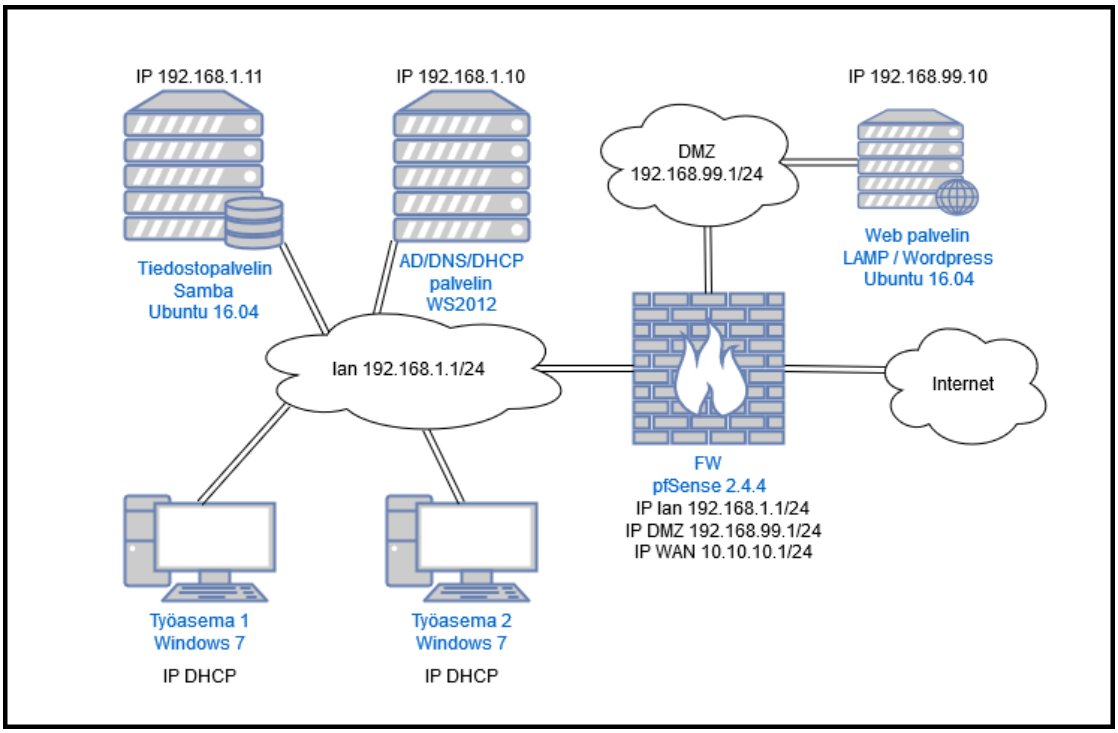
IT-osasto koostuu kokonaisuudessaan IT-päälliköstä ja yhdestä IT-tukihenkilöstä. IT-tukihenkilön työtehtävinä on ylläpitää toimialueen palveluita, toimia apuna loppukäyttäjille, vastata työasemien toimivuudesta, sekä ylläpitää ja kehittää toimialueen tietoturvaa IT-päällikön kanssa. IT-päällikkö vastaa yrityksen IT -strategiasta ja -hankkeista. IT-päällikkö on myös viimeisenä vastuussa yrityksen tietoturvasta. IT-päällikön työtehtäviin kuuluu myös yrityksen johdon ja hallitukselle raportoiminen mahdollisista puutteista ja hankkeista IT-infrastruktuurissa.

2.2.2 YritysX:n verkkoinfrastruktuuri

Virtuaaliympäristöstä jätettiin pois ylimääräiset työasemat. Virtuaaliympäristöön jäi kaksi työasemaa, joista toisella kuvattiin toimistoympäristön työasemia ja toisella tuotantoympäristön työasemia. Tuotantotyöntekijöiden käytössä olevalla työasemalla luodaan raportteja tuotannosta ja raportit siirretään tiedostopalvelimelle. Tiedostopalvelimelle on luotu oma tiedostojako, jonne tuotantoraportit ladataan päivän päätteeksi.

Haasteessa tuotantoympäristössä sijaitsevia työasemia mallinnettiin Työasemalla 1. Työasemalla 2 puolestaan mallinnettiin toimistotyöntekijän työasemaa. Työasemat saavat IP-osoitteet verkkotopologiassa olevalta Windows 2012 R2 DC-palvelimelta,

jossa toimii DHCP osoitteessa 192.168.0.10. Tiedostopalvelimena ympäristössä toimii Ubuntu Server 16.04. Tiedostojako palvelimella toteutettiin Samban avulla osoitteeseen 192.168.0.11. Palomuurina ympäristössä toimii pfSense 2.4.4, joka toimii samalla myös default gatewayna ympäristössä. Palomuurilla on kolme verkkorajapintaa, LAN sisäverkkoa kohden osoitteella 192.168.0.1/24, WAN rajapinta Internetiä kohden osoitteella 10.10.10.1/24 ja DMZ-verkkorajapinta 192.168.99.1/24 osoitteella. (ks. kuvio 2).



Kuvio 2. Harjoitukseen rajattu YritysX:n infrastruktuuri

3 Harjoituksessa käytetyt tekniikat

3.1 Active Directory hakemistopalvelu ja käyttäjätietokanta

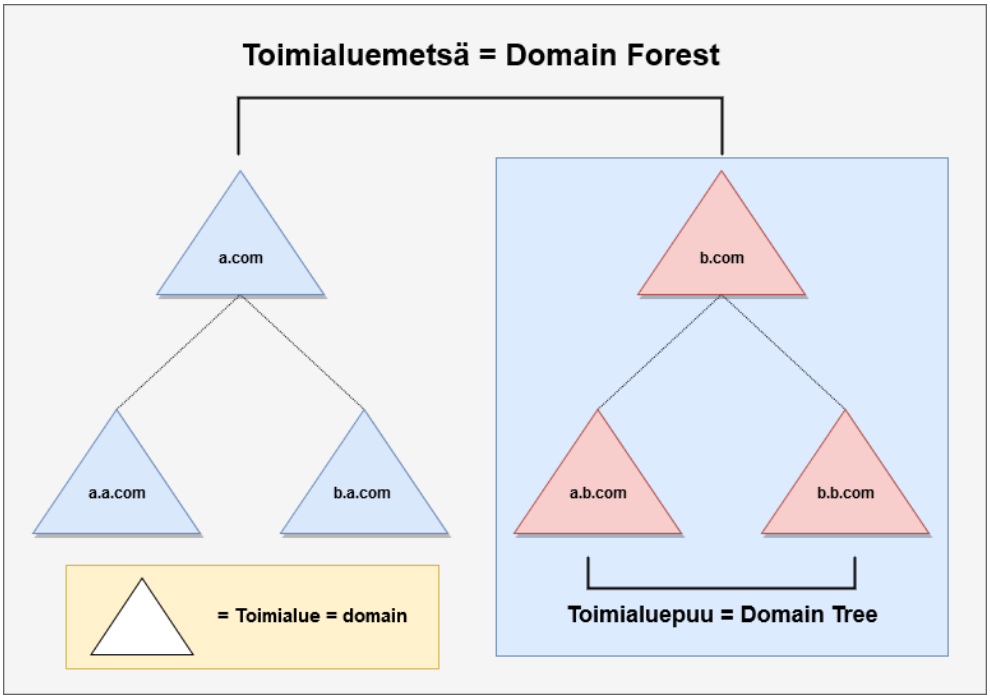
Active Directory on Microsoftin luoma hakemistopalvelu, joka koostuu useista palveluista, jotka toimivat Windows Server -alustalla. Active Directorya käytetään hallinnoimaan oikeuksia ja pääsyä verkkoresursseihin. AD tallentaa dataa objekteina. Objekti on yksittäinen elementti, kuten käyttäjä, työasema, palvelin tai esim. verkkotulostin. Objektit voidaan jakaa kahteen pääryhmään, joko resursseiksi (työasemat, tulostimet yms.) tai tietoturvakäytänteiksi, kuten käyttäjät ja käyttäjäryhmät. (Active Directory 2018.)

Toimialuepalvelu Active Directory Domain Services

Active Directoryn keskeisenä palveluna toimii Domain Services (AD DS). DS tallentaa hakemistotietoja ja käsittelee käyttäjän vuorovaikutusta domainin eli toimialueen kanssa. AD DS tarkistaa pääsyn, kun käyttäjä kirjautuu laitteeseen tai yrittää muodostaa etäyhteyden palvelimeen verkon kautta. AD DS hallitsee sitä, millä käyttäjillä on pääsy tiettyihin resursseihin. Järjestelmänvalvojille pystytään DS:n avulla antamaan laajemmat käyttöoikeudet kuin tavalliselle käyttäjälle. Palvelinta, jolla AD DS palvelu on toiminnassa, kutsutaan Domain Controlleriksi eli DC:ksi. (Mt.)

AD DS käyttää porrastettua rakennetta. Korkeimpana hierarkkisessa järjestelmässä on toimialuemetsä (domain forest), seuraavana tulee toimialuepuu (domain tree) ja viimeisenä toimialue eli domain. Tätä asetelmaa käytetään verkotettujen elementtien koordinoimiseksi. Puu koostuu yhdestä toimialueesta ja sen mahdollisista alitoimialueista (subdomain). Toimialuemetsä puolestaan koostuu useammasta toimialuepuusta ja sen mahdollisista alitoimialueista (ks. kuvio 3). (Active Directory 2017.)

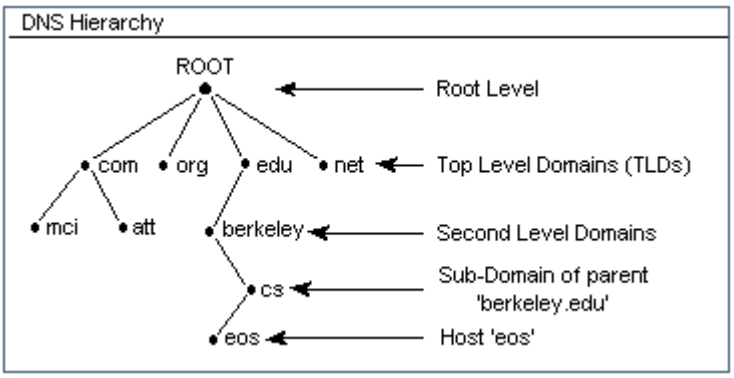
Yksi toimialue koostuu useista eri objekteista, jotka jakavat saman AD tietokannan. Toimialueilla on DNS (Domain Name System) rakenne. (Active Directory 2018.)



Kuvio 3. Toimialuemetsä

3.2 Domain Name System nimipalvelu

Nimipalvelu (DNS) koostuu hiearkisista toimialueista (domain). Jokaiselle toimialueen osalla viitataan, joko juuritason (Root), ylemmän tason (Top level domain), toisen tason (Second level domains) tai aliverkkotunnuksena (Sub-domain) (ks. kuvio 4). Jokainen FQDN:n (Fully Qualified Domain Name) taso erotetaan toisistaan pisteellä. DNS resolverit käyttävät pisteitä erottaakseen eri tasot toisistaan. DNS-nimien selvitys alkaa aina juuritasolta ja etenee sitten aina viimeiselle tasolle ja etsii sitten jäljelle jäävästä kohteesta tiedot. Tiedot (DNS-nimi, IP-osoite) voidaan tallentaa yhteen tai useampaan vyöhyketiedostoon (Zone files). Useista vyöhyketiedostoista koostuu vyöhyke (Zone), jota kutsutaan myös toimialueeksi. (DNS Hierarchy 2018.)



Kuvio 4. DNS Hierarchy (DNS Hierarchy 2018.)

3.3 Dynaaminen isäntäkonfiguraatioprotokolla

Dynaaminen isäntäkonfiguraatioprotokolla (DHCP) on asiakkaan ja palvelimen välinen protokolla, joka toimittaa asiakkaalle IP-osoitteen ja muut siihen liittyvät konfiguraatiotiedot, kuten aliverkon peitteen ja oletusyhdyskäytävän, automaattisesti palvelimelta. (Dynamic Host Configuration Protocol (DHCP) 2019.)

Jokaisella verkon laitteella on oltava oma uniikki IP-osoite, mahdollistaakseen verkon käytön. Laitteen vaihtaessa verkosta toiseen tulee myös sen osoitteen vaihtua. Ilman DHCP:tä uusi osoite pitäisi aina määrittää manuaalisesti ja verkosta poistuneiden laitteiden IP-osoitteet tulisi ottaa manuaalisesti uudelleen käyttöön. DHCP:n avulla tämä prosessi on automatisoitu ja keskitetty. DHCP-palvelin ylläpitää listaa IP-osoitteista ja vuokraa sitten osoitteita asiakkaille (client), kun asiakas sellaista pyytää. Osoitteiden ollessa dynaamisia ne palautuvat automaattisesti käytettävissä olevien IP-osoitteiden listaan, kun niitä ei enää käytetä. (Mt.)

3.4 Samba

Samba on ohjelma, jolla mahdollistetaan Linux ja Unix pohjaisten käyttöjärjestelmien yhteensopivuus Windows-käyttöjärjestelmien kanssa. Vuodesta 1992 lähtien Samban avulla on pystytty toteuttamaan stabiileja, sekä nopeita tiedosto- ja tulostinjakoja

kaikille asiakkaille, jotka käyttävät SMB/CIFS-protokollaa. Kyseisiin käyttöjärjestelmiin lukeutuu mm. kaikki DOS- ja Windows -käyttöjärjestelmät. (What is samba? n.d.)

Samba on tärkeä komponentti, kun halutaan helposti integroida Linux- tai Unix-palvelimia Windows AD-ympäristöön. Samban avulla Linux-palvelin voi toimia myös Domain Controllerina tai sitten vain tavallisena toimialueen jäsenenä. Samba on ohjelmistopaketti, joka antaa järjestelmänvalvojille joustavuutta ja vapautta asennuksen, konfiguroinnin ja järjestelmien suhteen. Näiden ominaisuuksiensa vuoksi Samba on kasvattanut suosiotaan julkaisustaan lähtien. (Mt.)

Winbind-komponentti

Unix-pohjaisten ja Microsoft Windows-käyttöjärjestelmien yhteensopivuus ja erityisesti tiedostojen jakaminen näiden kahden käyttöjärjestelmien välillä kärsisi suuresti, jos toimialueen käyttäjiä ja käyttäjäryhmiä ja niiden oikeuksia ei pystyttäisi integroimaan. Winbind on osa Samba-kokonaisuutta, joka ratkaisee yhtenäisen kirjautumisen ongelman. Winbind käyttää Microsoftin RPC-kutsuja, PAM-moduulia ja NSS-toiminnallisuutta mahdollistaakseen toimialueen käyttäjien ja käyttäjäryhmien toimivuuden Unix-käyttöjärjestelmissä samalla tavalla kuin Unix-käyttöjärjestelmien omat käyttäjät ja käyttäjäryhmät. (Winbind Use of Domain Accounts 2005.)

PAM-moduuli

PAM lyhenne tulee sanoista Pluggable Authentication Modules, sitä käytetään monentyyppisissä tehtävissä, johon tarvitaan autentikointia, auktorisointia ja muutoksien tekemistä, kuten salasanojen vaihtamista (What is PAM? 2016.). PAM tarjoaa järjestelmänvalvojille joustavuutta oikeudenhallinnan konfiguroinnin suhteen. Nykyään Unix-pohjaiset järjestelmät käyttävät PAMia hoitamaan autentikoinnin, auktorisoinnin ja resurssien hallinnan provisiontiin eri ohjelmille ja käyttäjille. (PAM-based distributed authentication 2003.)

NSS-toiminnallisuus

NSS eli Name Service Switch on toiminnallisuus, joka mahdollistaa järjestelmänvalvojan valitsemaan mitä nimi-informaatiopalvelua tai lähdettä käytetään etsimään tietoa. NSS:n avulla pystytään esimerkiksi määrittämään, että etsitäänkö toimialueen

nimet paikallisesti */etc/hosts* -tiedostosta vai esimerkiksi DNS-protokollan avulla verkosta. NSS-toiminnallisuuden avulla pystytäänkin lisäämään esim. paikallisen autentikoinnin lisäksi myös AD-autentikointi järjestelmään. (Name Service Switch (NSS) n.d.)

Kerberos-protokolla

Kerberos on MIT:n kehittämä autentikointiprotokolla. Kerberos-protokolla käyttää salaisen avaimen kryptografiaa tarjotakseen turvallisia yhteyksiä epäturvallisen verkon yli. Suurimpina etuina kerberos -protokollalla on vahva salaus ja kertakirjautuminen eli single-sign-on (SSO). Kertakirjautumisen avulla voidaan antaa käyttäjille pääsyjä järjestelmiin tai palveluihin. Kerberoksen kertakirjautumisella käyttäjätunnusta ja salasanaa kysytään vain kerran. (Introduction to Kerberos n.d.)

Kerberos toimii kolmannen osapuolen luotettavana palvelimena, jota kutsutaan Key Distribution Centerksi (KDC). Jokaista käyttäjää ja palvelua verkossa kutsutaan käytänteeksi. KDC koostuu kolmesta pääkomponentista. Ensimmäisenä komponenttina on autentikointipalvelin, joka hoitaa alustavan autentikoinnin ja antaa lippujen myöntämisliput eli ticket-granting ticketit (TGT) käyttäjille. Toisena pääkomponenttina on lippujen myöntämispalvelu, joka myöntää palvelulippuja, jotka toimivat aikaisemmin hankittujen TGT-lippujen perusteella. Kolmantena komponenttina on tietokanta käytänteistä, joka koostuu salaisista avaimista kaikille käyttäjille ja palveluille, jota se ylläpitää. (Mt.)

3.5 pfSense palomuuri ja reititin

pfSense on ilmainen avoimen lähdekoodin palomuuri- ja reititinprojekti, joka hyödyntää FreeBSD-käyttöjärjestelmää. pfSenseen on integroitu helppokäyttöinen web-käyttöliittymä, jolla palomuurin konfigurointi hoidetaan pääosin. pfSense tarjoaa monipuolisen ja tehokkaan palomuurin ja reititysalustan. pfSenseä voidaan käyttää aina yksittäisen laitteen palomuurina, kotiverkon suojaamiseen tai jopa isojen yritysten ja oppilaitosten verkkojen palomuurina. Projekti on saanut alkunsa vuonna 2004 Chris Buechlerin ja Scott Ullrichin toimesta. pfSensä käytetään usein vain palomuurina, mutta sitä voidaan myös käyttää LAN/WAN -reitittimenä tai jopa VPN/DHCP -palvelimena. (Buechler & Pingel 2019, 20–25.)

4 Skenaarion suunnittelu

4.1 Harjoituksen tietoturvailmiöt

Malwarebytesin raportin mukaan vuonna 2018 kyberhyökkäykset yrityksiin oli kasvanut 79 % edellisvuodesta. Tyypillisimpinä hyökkäyksinä oli mm. troijalaiset, vakoiluohjelmat ja kiristyshaittaohjelmat. (2019 State of Malware 2019, 17.)

Troijalaiset

Troijalaiset ovat yksi haittaohjelmien tyyppi. Troijalaiset naamioituvat tavallisiksi ohjelmiksi, mutta todellisuudessa sisältävät haitallista koodia. Troijalaiset yleensä suunnitellaan aiheuttamaan harmia loppukäyttäjälle tai varastamaan tältä tietoa. Troijalainen eroaa tavallisesta tietokoneviruksesta siten, etteivät ne voi suorittaa itseään vaan käyttäjän on tehtävä se. Troijalaiset eivät myöskään voi replikoida itseään. Troijalaisia voidaan toimittaa esimerkiksi sähköpostiviestien liitteenä. Käyttäjän avatessa sähköpostiliitteen ne suorittavat haitallisen koodinsa. Troijalaisia on monen tyyppisiä. Niiden tarkoitusperänä voi olla kiristää loppukäyttäjää lukitsemalla tiedostoja, varastaa sähköpostitietoja tai esimerkiksi sosiaalisen median tilitietoja. (What is a Trojan? n.d.)

Command and Control-haittaohjelmat

Command and control eli komentokanavahyökkäykset voivat laajimmillaan saastuttaa yrityksen ympäristön kokonaan. C2-hyökkäykset toteutetaan usein saastuttamalla ensin yksi työasema esimerkiksi sähköpostiliitteen avulla. C2-hyökkäykset käyttävät usein DNS-protokollaa saastuttaakseen muita työasemia verkossa. Työaseman saastumisen jälkeen C2-ohjelma alkaa keskustelemaan hyökkääjään määräämän C2-palvelimen kanssa. Hyökkääjä pystyy yhteyden muodostettuaan suorittamaan mitä tahansa haitallista koodia kohteessaan. C2-ohjelmia käytetään myös bottiverkkojen luomiseen. C2-hyökkäyksen seuraamuksena voi olla tietomurto, tuotantoa haittaavia häiriöitä ja mahdollisesti jopa DDoS-hyökkäyksiä. (Command-and-Control Explained n.d.)

Brute-force -hyökkäys

Brute-force -hyökkäyksiksi luokitellaan sellaiset tapahtumat, jotka pyrkivät esimerkiksi murtamaan salasanan tai käyttäjätunnuksen. Käytännössä brute-force -hyökkäyksessä kokeillaan järjestelmällisesti eri salasanoja käyttäjätunnuksille. Brute-force -hyökkäys on vanha tapa pyrkiä sisään käyttöjärjestelmiin, mutta on vieläkin tehokas riippuen salasanan kompleksisuusvaatimuksista. Kompleksisuusvaatimuksista riippuen salasanan murtaminen voi viedä muutamia sekunteja tai useita vuosia. Brute-force -hyökkäyksiä pystytään nopeuttamaan sanakirjojen ja numeroyhdistelmien avulla. (What's a Brute Force Attack? n.d.)

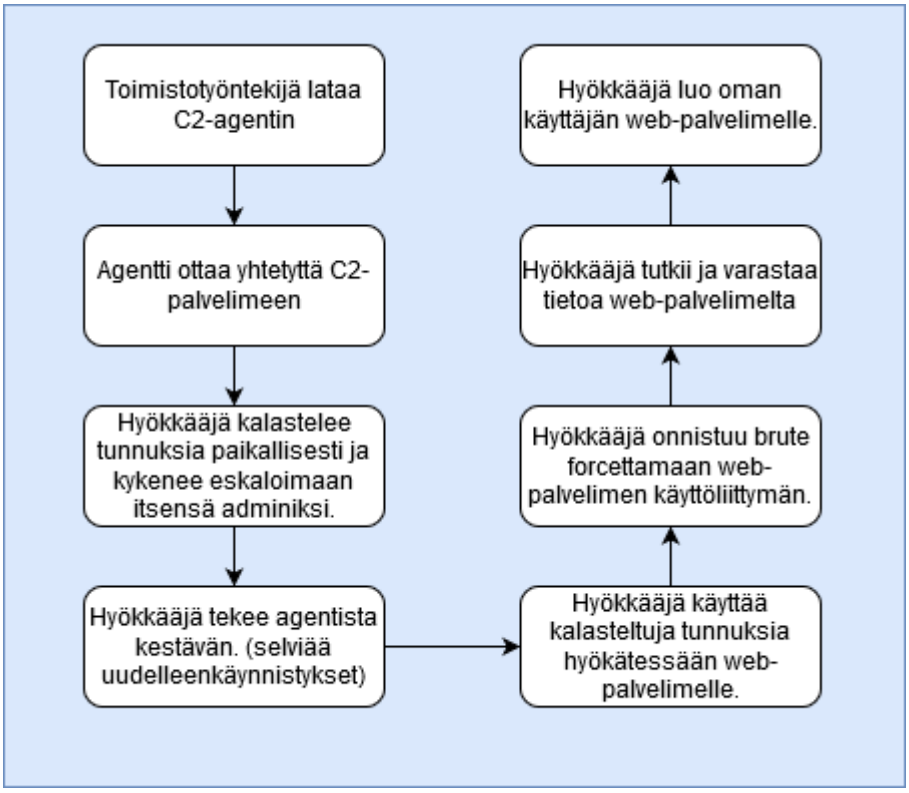
4.2 Tapahtumaketju

Skenaarion suunnittelussa pyrittiin mahdollisimman realistiseen ja ajankohtaisiin tietoturvailmiöihin. Tämän vuoksi skenaariota suunnitelmaa lähdettiin toteuttamaan pitkälti aiemmin mainitun Malwarebytesin raportin pohjalta. Skenaariossa yrityksen toimistotyöntekijä on ladannut internetistä tiedoston, joka onkin troijalainen. Yritykseen kohdistunut tietoturvapoikkeama laajenee troijalaisen jälkeen. Liitteessä 1 on kuvattu tietoturvahaasteen suorittajalle annettu tehtävänanto.

Taitaja2020 -kilpailussa kilpailijoille annettiin tehtävän suorittamiseen aikaa 3 tuntia. Jotta tietoturvahaasteessa oleva tietoturvapoikkeama olisi mahdollista suorittaa mainitussa aikaikkunassa, ei tietoturvapoikkeama saa olla liian laajalle levinnyt. Tietoturvapoikkeama ei myöskään saa olla teknisesti liian haastava, kun otetaan huomioon haasteeseen osallistuvien opintosuunnitelma ja osaamisvaatimukset tietoturvan suhteen. Ei voida myöskään olettaa kilpailijoiden kykenevän tutkimaan tietoturvapoikkeamaa kovin syvällisesti. Kilpailijan tärkein tehtävä onkin kyetä havaitsemaan ympäristössä vallitseva tietoturvapoikkeama.

Kuviossa 5 on kuvattu ympäristöön kohdistuvan tietoturvapoikkeaman tapahtumat. Tietoturvapoikkeama saa alkunsa, kun toimistotyöntekijä lataa vahingossa haittaohjelman ja suorittaa sen. Haittaohjelma ottaa sen jälkeen yhteyden palvelimeen, jota kautta agenttia eli haittaohjelmaa käskytetään. Hyökkääjä käskyttää agenttia ja kalastelee sen avulla paikallisesti tunnuksia ja pyrkii eskaloimaan oikeuksia. Varastettujen

tunnuksien avulla hyökkääjä onnistuukin brute-force -hyökkäyksen avulla kirjautumaan web-palvelimen WordPress-käyttöliittymään. Hyökkääjä sitten tutkii ja varastaa sieltä löytyvää tietoja, sekä luo itselleen takaoven, jotta kykenee jatkossakin varastamaan tietoja.



Kuvio 5. Hyökkäyksen tapahtumat

4.3 Tehtäväpisteiden suunnittelu

Tehtäväpisteiden suunnittelussa on otettu huomioon yleisimmät tietoturvapoikkeamat, joita yrityksiin kohdistuu. Tehtäväpisteiden suunnittelussa on myös otettu huomioon suunnitellun kohderyhmän oletettu osaamistaso. Tehtäväpisteet on toteutettu kohdennetulla hyökkäyksellä. Liitteessä 2 on esitetty tietoturvahaasteen tehtäväpisteet ja liitteessä 3 oikeat vastaukset.

Lippujen tarkoituksena on tarjota testaajalle selkeät tavoitteet. Toteuttamisen vaikeus on saada tehtyä sellaisia lippuja, että ne ovat myös testaajien tunnistettavissa, mutta että ne vastaisivat todellisia tilanteita mahdollisimman tarkasti. Tämän vuoksi lippuja ei voi nimetä kovin ilmeisesti. Lippujen sijoituspisteinä tulisi olla realistiset kohteet, kuten arkaluontoiset tiedostot. Nimeämiskäytännöllä tulisi hieman hälventää lippujen itsestäänselvyyttä. (Buchanan 2014.)

Tietoturvapoikkeamien hallinnassa on tärkeää pyrkiä keräämään todisteita mahdollisesta tietoturvaselkkauksesta ja pyrkiä todisteiden avulla parantamaan tietoturvaa ja tietoturvakäytänteitä. Tietoturvahaasteen kaikki tehtäväpisteet pohjautuvat todisteiden keräämiseen tietoturvapoikkeaman sattuessa. Kilpailijan tavoitteena oli löytää ympäristöstä tietoturvapoikkeaman aiheuttaja ja pyrkiä pinnallisesti havainnoimaan mitä haittaohjelma tekee, sekä pyrkiä hahmottamaan tietoturvapoikkeaman laajuus. Tehtäväpisteillä pyritään luomaan kilpailijalle käsitys yksinkertaisesta tietoturvapoikkeamasta ja poikkeamaan liittyvästä todisteiden keruusta.

Tehtäväpisteitä harjoituksessa on kymmenen ja niistä sai yhteensä viisitoista pistettä. Tehtäväpisteistä oli tarkoitus luoda helposti lähestyttäviä. Tavoitteena oli myös luoda haastavampia tehtäväpisteitä, joilla pyrittiin luomaan piste-eroa kilpailijoiden kesken. Tehtäväpiste 8 on ympäristön haastavin, sillä se on haittaohjelman luoma rekisterimerkintä, jonka avulla haittaohjelma suoritti itsensä aina sisäänkirjautumisen yhteydessä ja pyrki ottamaan yhteyttä C2-palvelimeen. Tehtäväpisteiden toteutuksesta tarkemmin kappaleessa 5.7.

5 Virtuaaliympäristön toteutus

5.1 Resurssien mitoitus

Taitaja2020-kisoihin ilmoitetuiksi resursseiksi kerrottiin 32GB RAM-muistia. Muista teknisistä lähtökohdista ei ollut tietoa, siksi tietoturvahaasteen suunnittelussa pyrit-

tiin toteuttamaan virtuaaliympäristö käyttäen mahdollisimman vähän muisti- ja tallennustilaresursseja. Virtuaaliympäristön käyttämät resurssit on esitetty taulukossa 1. Virtuaaliympäristön muistinkäyttöä pyrittiin rajoittamaan mahdollisimman paljon, jotta ympäristön käyttäminen onnistuisi pienemmilläkin resursseilla. Virtuaaliympäristö rakennettiin Virtualboxin versiolla 6.0.18. Virtuaaliympäristön käyttämiseen tarvitaan vähintään 16GB RAM-muistia.

Taulukko 1. Virtuaaliympäristön resurssit

Resurrsit	Muisti (MB)	Tallennustila virtuaalinen (GB)	Tallennustila käytännössä (GB)
Domain Controller	1536	50	8,6
Firewall	1024	16	1,51
Fileserver	768	15	3,79
Webserver	1536	10	2,41
Workstation-1	1536	32	7,83
Workstation-2	4096	32	13,95
kali	2048	25	11,95
Yhteensä	**12544**	**180**	**50,04**

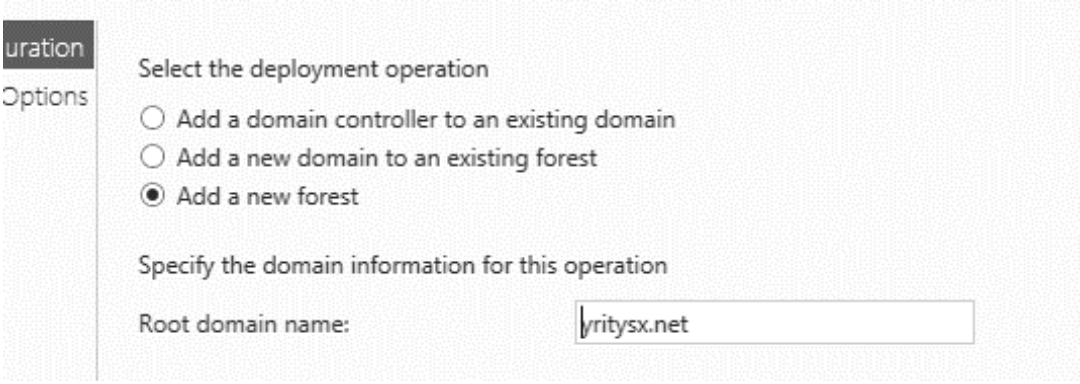
5.2 Windows serverin asentaminen

Virtuaaliympäristön keskeisenä virtuaalikoneena on Windows Server 2012 käyttöjärjestelmällä varustettu Domain Controller. Virtuaalikoneelle allokoitiin 1536MB muistia. Palvelimelle asennettiin kaikki keskeiset palvelut kuten AD, DNS ja DHCP. Muut harjoituksen suhteen turhat palvelut pyrittiin karsimaan pois minimoidakseen resurssien tarve.

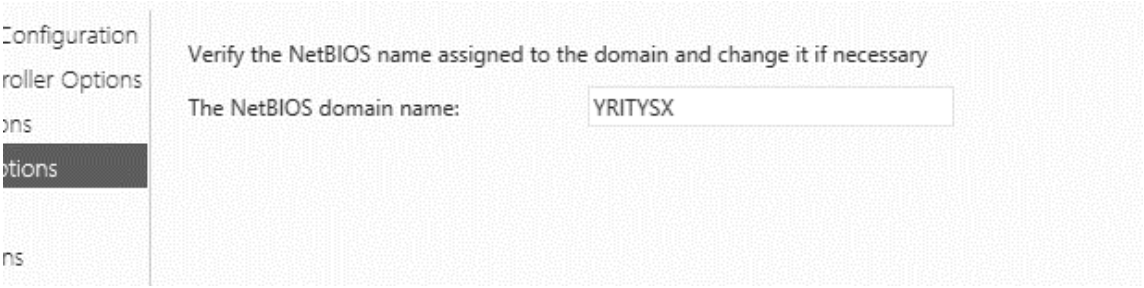
Toimialueen hakemistopalvelun määrittäminen

Active Directoryn luominen aloitettiin valitsemalla juuritason toimialuenimi. Tyypillisiä juuritason toimialuenimenä on yrityksen nimi ja toimialueen päätteenä net. Juuritason toimialuenimeksi valikoituikin siis yritysx.net (ks. kuvio 6). Juuritason toimialueen asennuksen yhteydessä tuli myös valita toimialueelle NetBIOS nimi, jonka avulla

käyttäjä pystyvät valitsemaan oikean toimialueen. NetBIOS nimeksi valikoitu pelkästään YRITYSX, koska kyseessä on yrityksen ainoa toimialue eikä muita toimialueita tule virtuaaliympäristöön (ks. kuvio 7).



Kuvio 6. Juuritason toimialuenimi

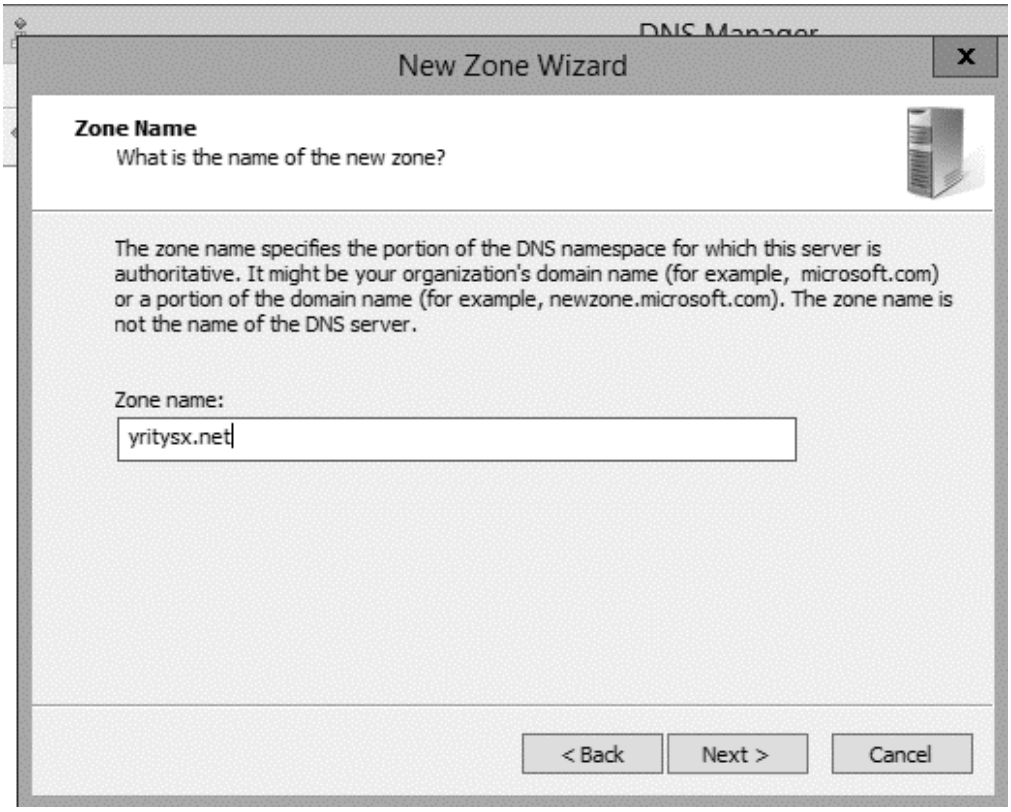


Kuvio 7. NetBIOS nimi

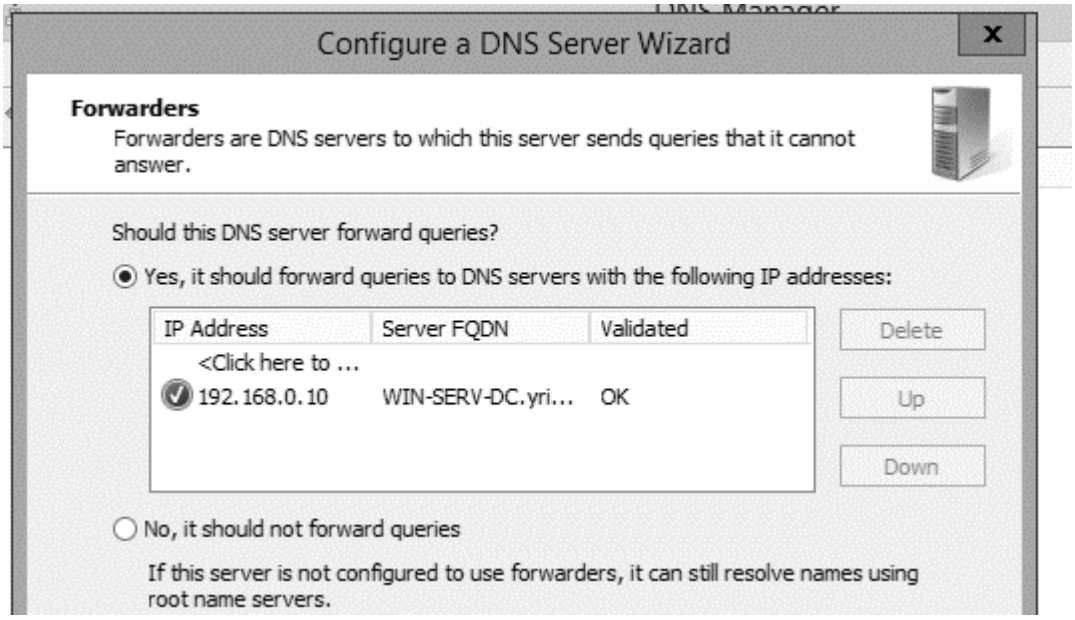
Nimipalvelun asennus ja määrittely

DNS-nimipalvelun määrittämisessä luotiin DNS-alueeksi yritysx.net seuraamalla samanlaista nimeämiskäytännettä kuin hakemistopalvelujen luomisessa (ks. kuvio 8). DNS-alueen nimeämisen jälkeen valittiin palvelin, joka hoitaa DNS-kyselyihin vastaamisen kyseisellä DNS-alueella. Koska kyseessä on verrattain pieni ympäristö, keskitettiin kaikki oleelliset palvelut Domain Controller-palvelimen varaan hallinnoinnin helpottamiseksi (ks. kuvio 9). Oleellista DNS-palvelun toimivuudessa on myös varmistaa

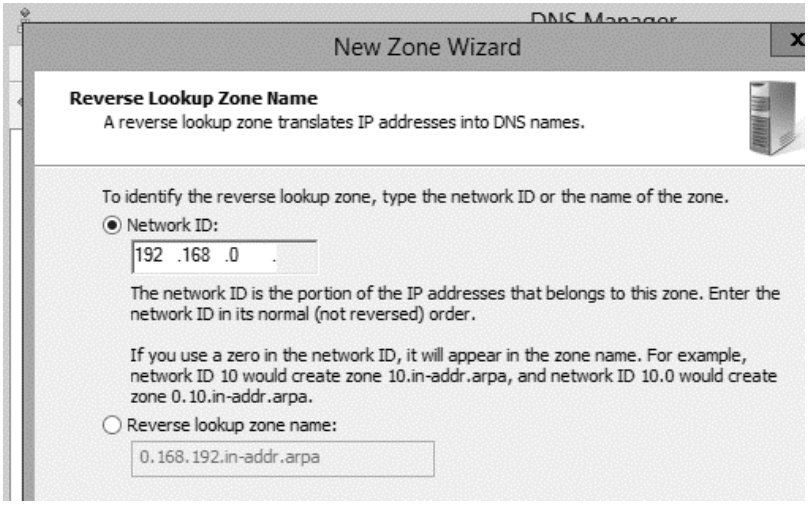
IP-osoitteiden kääntymisen myös nimiksi (ks. kuvio 10). Kyseistä toimintoa nimetään-kin reverse lookup zoneksi.



Kuvio 8. DNS alueen nimeäminen



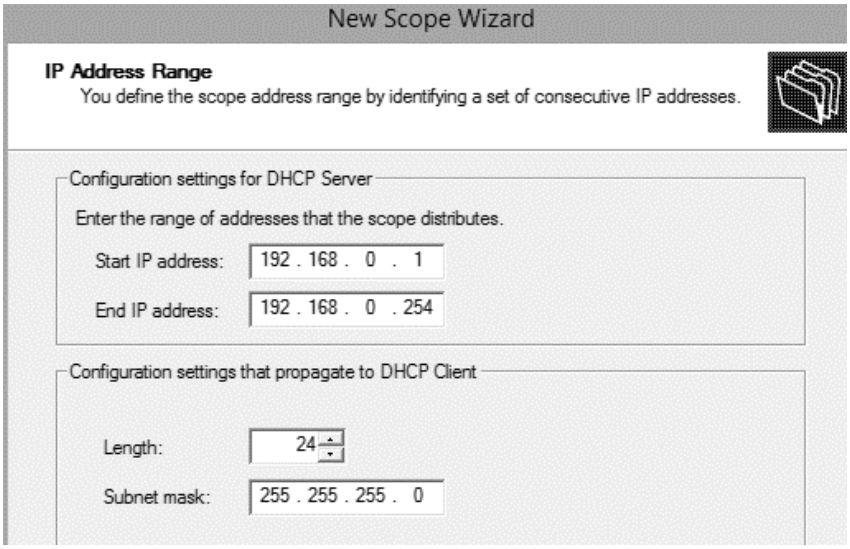
Kuvio 9. DNS kyselyiden välitys



Kuvio 10. Reverse lookup zonen määritys

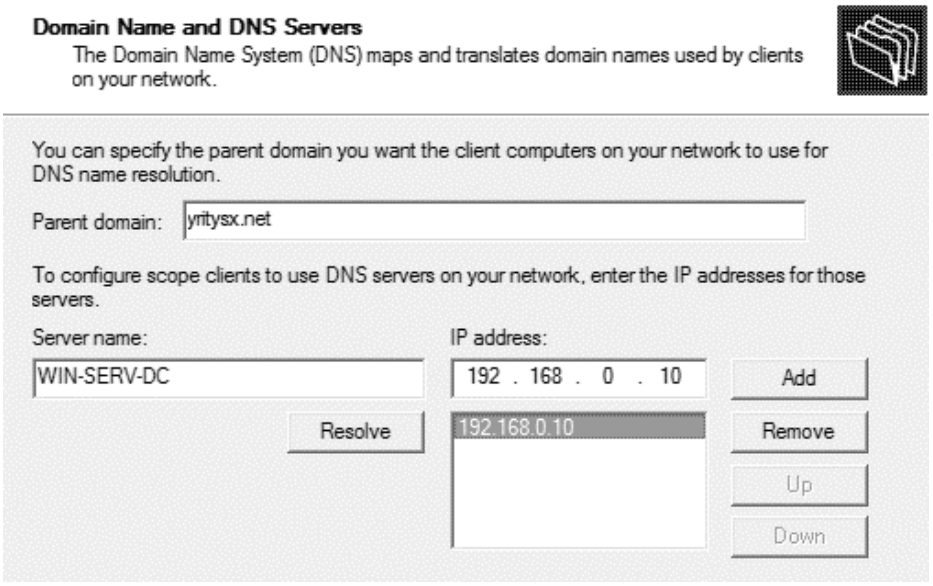
Dynaaminen isäntäkonfiguraatioprotokolla -palvelun asennus ja määrittely

DHCP-palvelu asennettiin helpottamaan IP-osoitteiden hallintaa. Yrityksen pienen sisäverkon myötä ei ollut tarvetta luoda paljon osoitteita sisältävää IP-osoiteavaruutta. IP-osoiteavaruudeksi määriteliin jo kuviossa 2 esitetty 192.168.0.1/24 osoiteavaruus (ks. kuvio 11).



Kuvio 11. DHCP:n IP-osoiteavaruus

Osoiteavaruudesta poistettiin ensimmäiset 20 osoitetta käytöstä. Nämä osoitteet on varattu muille tärkeille sisäverkon palvelimille ja niitä ei jaeta työasemien kesken. IP-osoitteiden vuokra-ajaksi valittiin yksi vuorokausi. DHCP:n määrittämisen yhteydessä määritettiin myös default gateway 192.168.0.1 ja DNS-palvelin osoitteeseen 192.168.0.10 (ks. kuvio 12). Määrittelyjen jälkeen palvelu tuli vielä valtuuttaa toimimaan kyseisellä toimialueella (ks. kuvio 13).



Kuvio 12. DNS-palvelin määrittäminen DHCP:n yhteyteen

Kuvio 13. DHCP-palvelimen valtuutus

5.3 Tiedostopalvelimen asennus

Yrityksen sisäverkkoon lisättiin tiedostopalvelin, jonka käyttöjärjestelmäksi valittiin Ubuntu 16.04. Käyttöjärjestelmäksi valikoitui Linux-pohjainen käyttöjärjestelmä resurssien käytön minimoimisen vuoksi. Tiedostopalvelimelle asetettiin muistinmääräksi 768MB.

Kerberoksen konfigurointi ja toimialueeseen liittyminen

Jotta tiedostopalvelin pystyttiin liittämään toimialueeseen, tuli siihen asentaa tarpeelliset ohjelmistot, kuten Samba, Kerberos ja Winbind. Tarvittavat asennuspaketit asennettiin seuraavalla komennolla:

sudo apt-get install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind

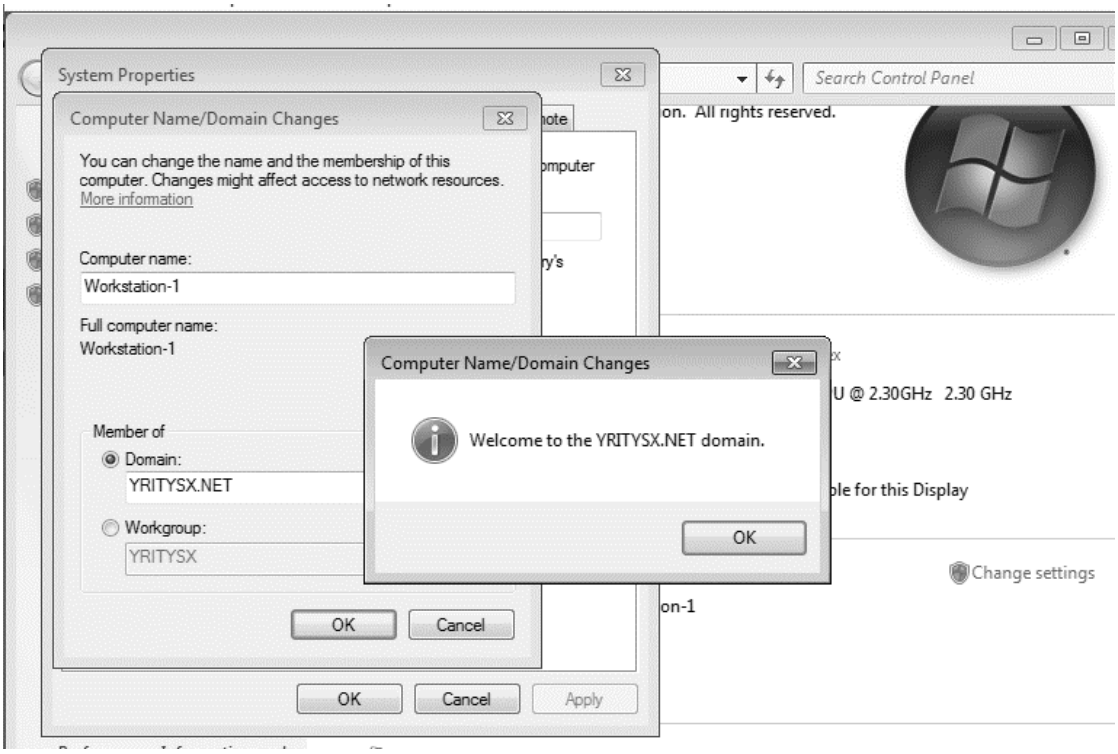
Asennuksen jälkeen palvelut konfiguroitiin liitteen 4 mukaisesti. Samba palvelun konfiguroinnista vastaa *smb.conf* tiedosto. Kyseisessä konfiguraatiotiedostossa on määritetty toimialue, jossa tiedostojako tapahtuu ja tiedostopolku tiedostojaolle. *Krb5.conf* tiedosto pitää sisällään Kerberoksen konfiguraatiot. Konfiguroinnin jälkeen tiedostopalvelin liitettiin toimialueeseen komennolla:

sudo net ads join -U administrator

Jotta toimialueen käyttäjät pystyvät käyttämään samoja tunnuksia myös tiedostopalvelimelle autentikoimisessa, tulee myös konfiguroida NSS-toiminnallisuus. NSS määrittää mitä nimi-informaatiopalvelua käytetään. Liitteessä 4 kohdassa 3 on NSS-konfiguraatio, jossa nimi-informaatiopalveluksi on määritetty myös Winbind. Winbind toimii varsinaisena autentikointipalveluna tiedostopalvelimen ja toimialueen välillä. Winbind tuli aktivoida käyttöön PAMin avulla. Tämän jälkeen toimialueen käyttäjät sallittiin käyttämään tiedostojakoa (ks. liite 4 kohta 4). Viimeisenä toimenpiteenä toimialueen pääkäyttäjät lisättiin *visudo* komennolla tiedostopalvelimen pääkäyttäjiksi ja todennettiin toimivuus (ks. liite 4 kohta 5).

5.4 Työasemat

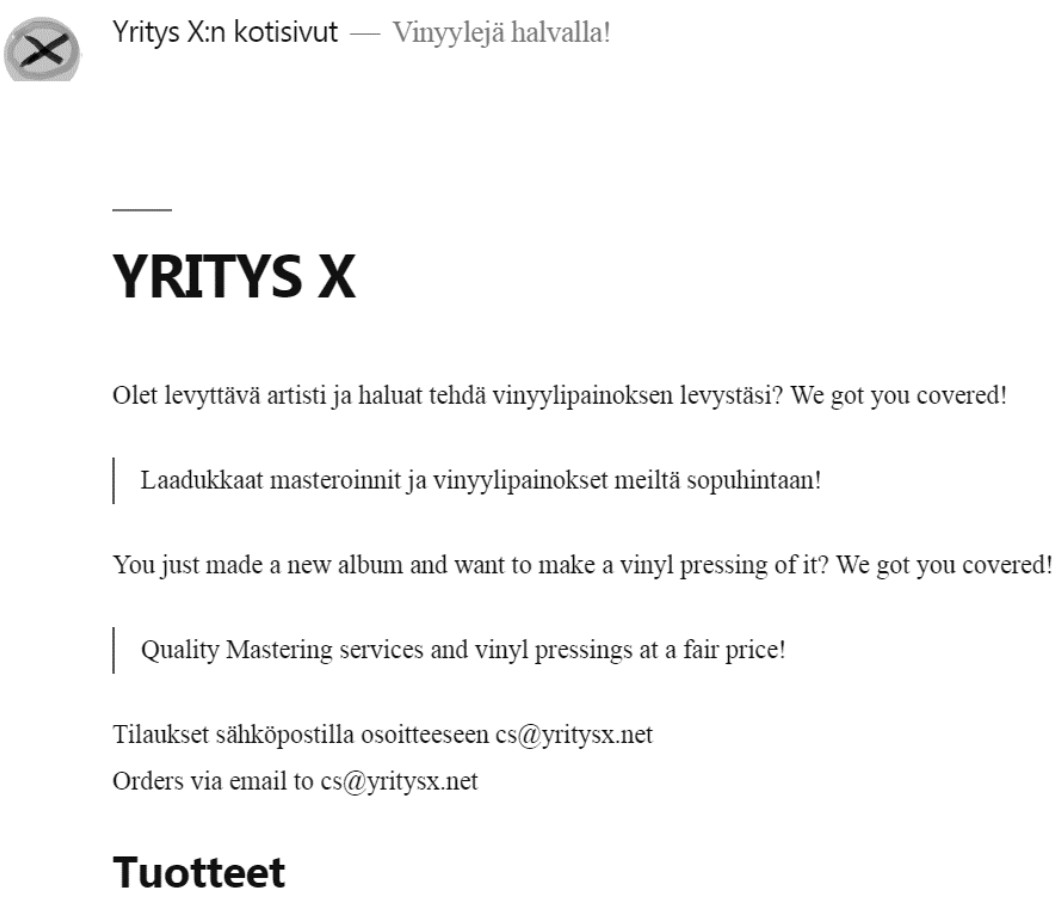
Harjoitusympäristöön lisättiin 2 työasemaa, joista Workstation-1 kuvaa tuotantoympäristön työasemia ja Workstation-2 kuvaa toimistotyöntekijöiden työasemia. Käyttöjärjestelmäksi työasemille valikoitui Windows 7. Työasemille ei juurikaan asennettu ylimääräisiä ohjelmistoja. Käyttöjärjestelmän asennuksen jälkeen työasemat liitettiin toimialueeseen (ks. kuvio 14). Työasemalle 2 asennettiin tehtävän ratkaisua varten mm. Autopsy- Netmon- ja Procmon-ohjelmistot. Kyseisille työkaluille luotiin myös pienimuotoiset ohjeet tehtävän suorittamisen helpottamiseksi (ks. liite 5). Työasemalle 1 asetettiin muistimääräksi 1536MB. Työasemalle 2 muistirajaksi asetettiin 4096MB ohjelmistojen tarpeiden vuoksi. Työasemalle 2 lisättiin myös myöhemmin järjestelmänvalvojan oikeudet käyttäjätunnukselle pliimatta.



Kuvio 14. Työaseman liittäminen toimialueeseen

5.5 Web-palvelin ja verkkosivut

Yrityksen DMZ-verkkoon luotiin web-palvelin, joka tarjoaa yrityksen verkkosivut. Käyttöjärjestelmäksi palvelimelle valittiin Ubuntu 16.04 ja muistirajaksi asetettiin 1536MB. Verkkosivujen käyttöliittymäksi valittiin WordPress, johon asennettiin audit-plugin lisäosa. Lisäosan tarkoituksen on helpottaa kilpailijoita havainnoimaan verkkosivuihin kohdistuvia tietoturvapoikkeamia ja tapahtumia. Verkkosivuja varten yritykselle sisältöä verkkosivuille ja yrityksen verkkosivuille suunniteltiin myös logo (ks. kuvio 15 ja kuvio 16).



Kuvio 15. Yritys X:n etusivun kuvankaappaus

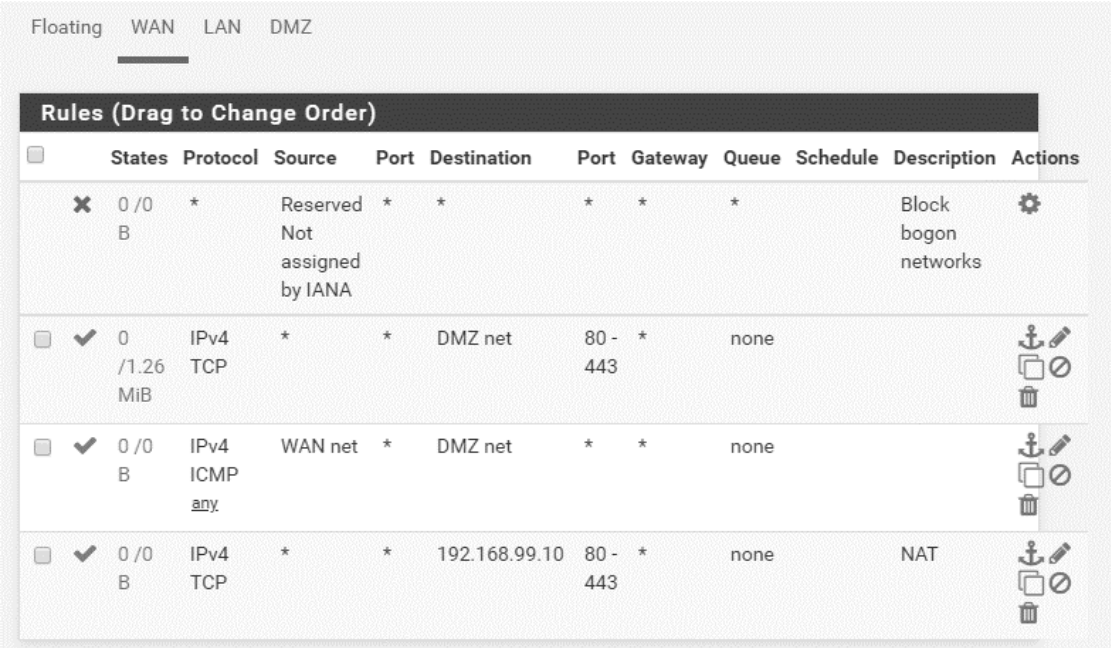
Kuvio 16. Yritys X:n logo

5.6 pfSense palomuuri

Yrityksen sisäverkko eristettiin WAN- ja DMZ-verkosta palomuurin avulla. Virtuaalikoneelle luotiin kolme erillistä verkkoliitintä. Yksi jokaista verkkoa kohden. Muistirajaksi koneelle asetettiin 1024MB.

Palomuurisäännöt

Palomuurisäännöt tehtiin mahdollisimman minimaalisiksi. WAN-verkon palomuurisäännöillä sallittiin liikenne vain WAN-verkosta DMZ-verkkoon. Lisäksi palomuurisääntöihin lisättiin sääntö, jolla tehtiin porttien 80 ja 443 (HTTP ja HTTPS) uudelleenohjaus DMZ-verkon Web-palvelimelle (ks. kuvio 17). Yrityksen sisäverkon palomuurisäännöt sallivat valmiiksi kaiken liikenteen LAN-verkosta muihin verkkoihin. Lisäksi yrityksen sisäverkossa sallittiin DMZ-verkosta tulevat DNS-kyselyt (ks. kuvio 18).

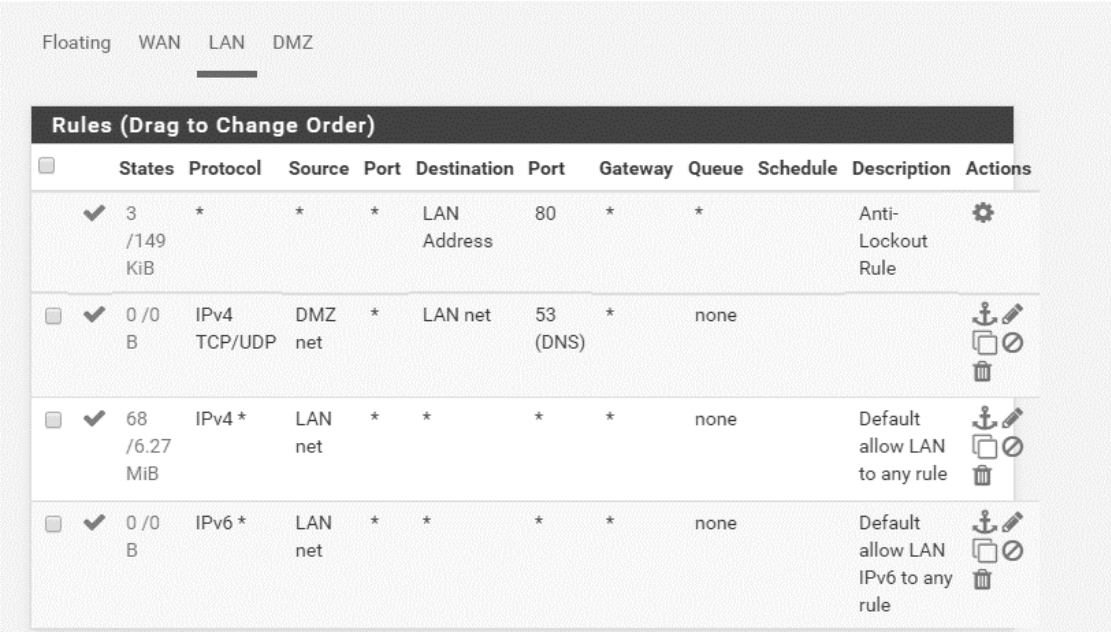


Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✖	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
✔	0 /1.26 MiB	IPv4 TCP	*	*	DMZ net	80 - 443	*	none			
✔	0 /0 B	IPv4 ICMP any	WAN net	*	DMZ net	*	*	none			
✔	0 /0 B	IPv4 TCP	*	*	192.168.99.10	80 - 443	*	none		NAT	

Kuvio 17. WAN-verkon palomuurisäännöt



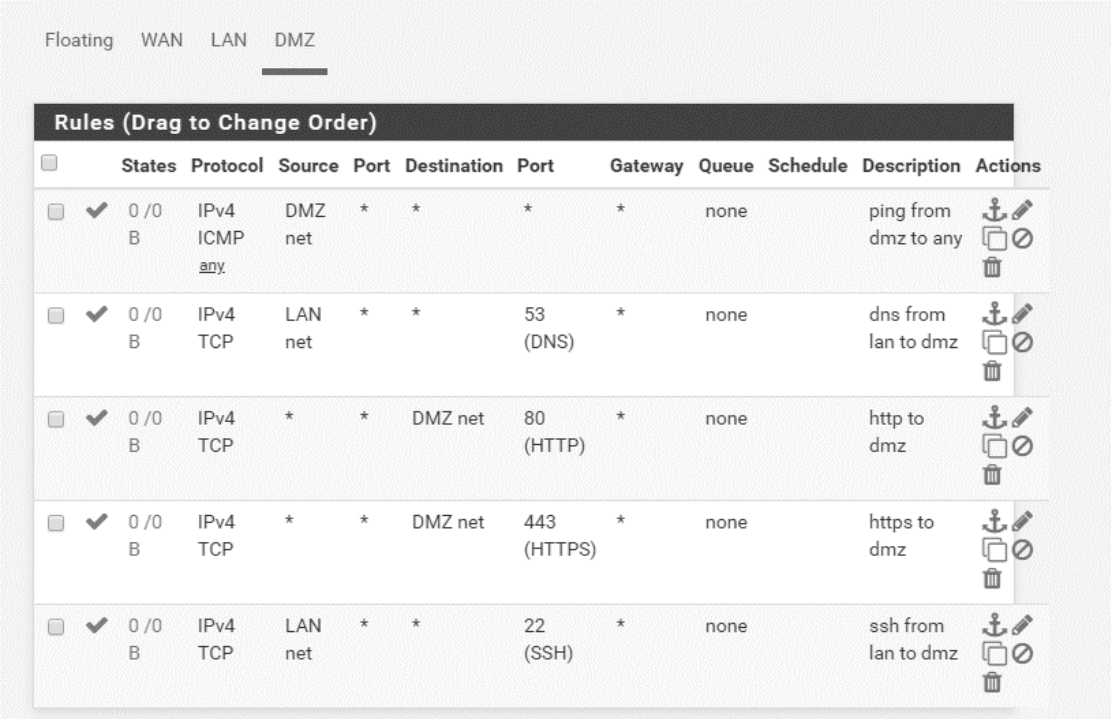
Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	3 /149 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✔	0 /0 B	IPv4 TCP/UDP	DMZ net	*	LAN net	53 (DNS)	*	none			
✔	68 /6.27 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✔	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Kuvio 18. LAN-verkon palomuurisäännöt

DMZ-verkon palomuurisäännöissä sallittiin SSH-yhteys LAN-verkosta DMZ-verkkoon. DMZ-verkkoon sallittiin myös kaikista verkoista tulevat HTTP- ja HTTPS-yhteydet, sekä DNS-kyselyt LAN-verkosta DMZ-verkkoon. Yhteyksien testauksia varten sallittiin myös ICMP-protokolla (ks. kuvio 19).

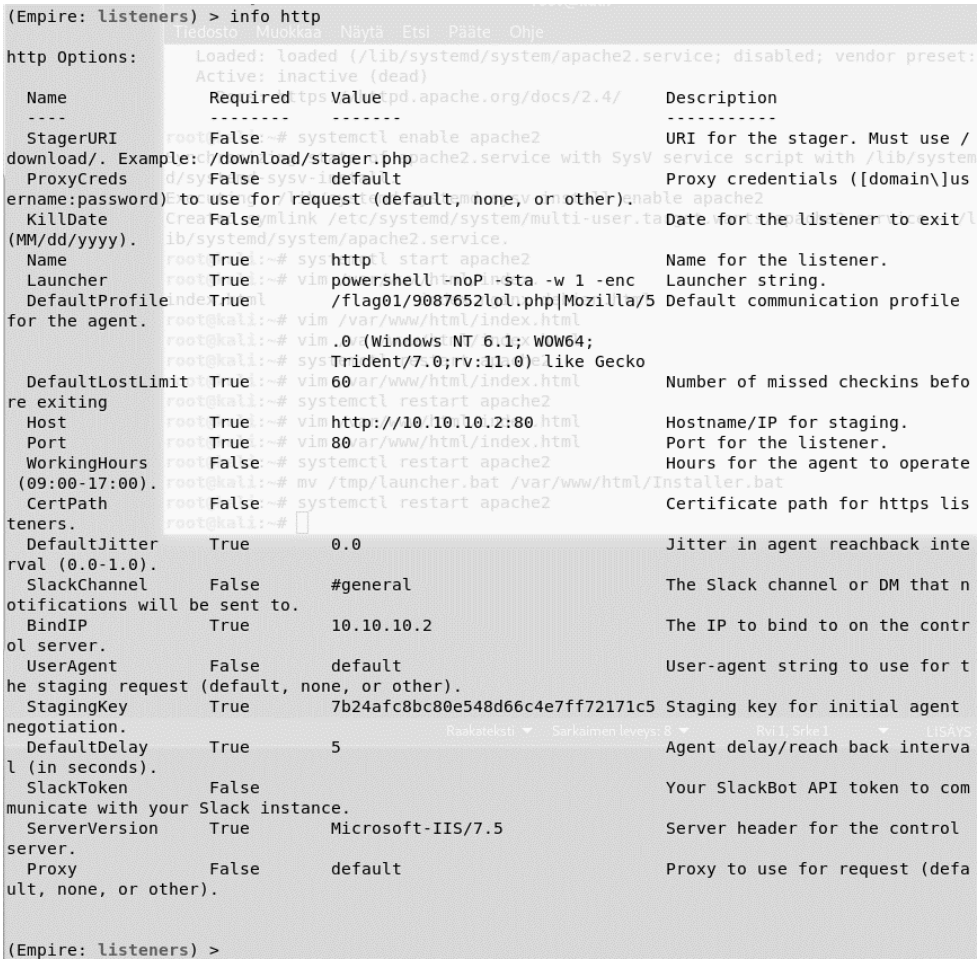


Kuvio 19. DMZ-verkon palomuurisäännöt

5.7 Tehtäväpisteiden toteutus

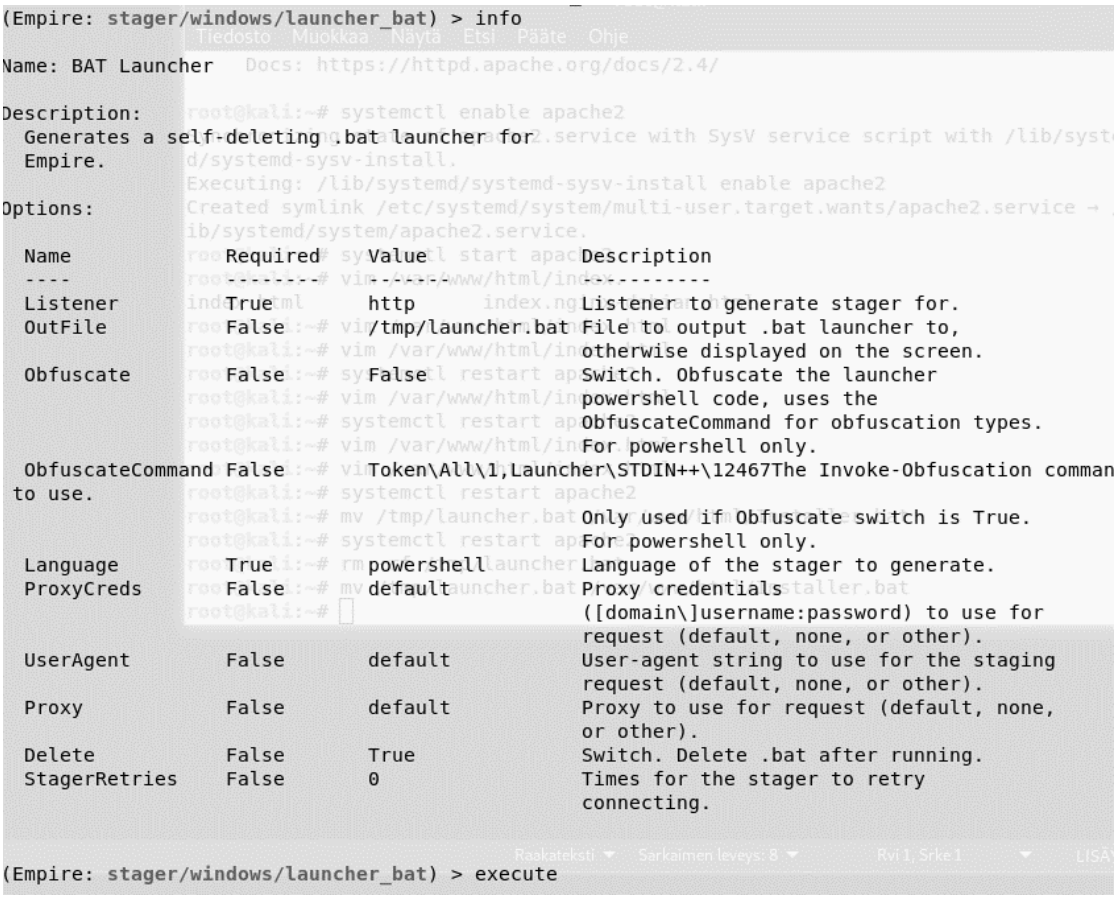
Tehtäväpisteiden toteutusta varteen WAN-verkkoon luotiin Kali Linux virtuaalikone. Kyseisellä virtuaalikoneella oli tarkoitus toteuttaa tehtäväpisteet kohdennetun hyökkäyksen avulla. Virtuaalikoneelle asetettiin 2048MB muistiraja. Kohdennetussa hyökkäyksessä käytettiin PowerShell Empire-ohjelmistoa luomaan C2-palvelin ja C2-agentit. Virtuaalikoneella toimi myös verkkosivut, jonka kautta uhri lataa skenaarion mukaisen troijalaisen.

Kohdennettu hyökkäys aloitettiin valmistelemalla C2-palvelin. Palvelimen kuuntelijan eli vastaanottimen protokollaksi asetettiin HTTP. Kuuntelija asetettiin toimimaan IP-osoitteessa 10.10.10.2 portissa 80. Samalla kuuntelijan ja agentin välisten pakettien kommunikointiprofiiliin (DefaultProfile) lisättiin ensimmäinen lippu (ks. kuvio 20). Kyseinen lippu on tarkoitus huomata analysoimalla verkkoliikennettä.



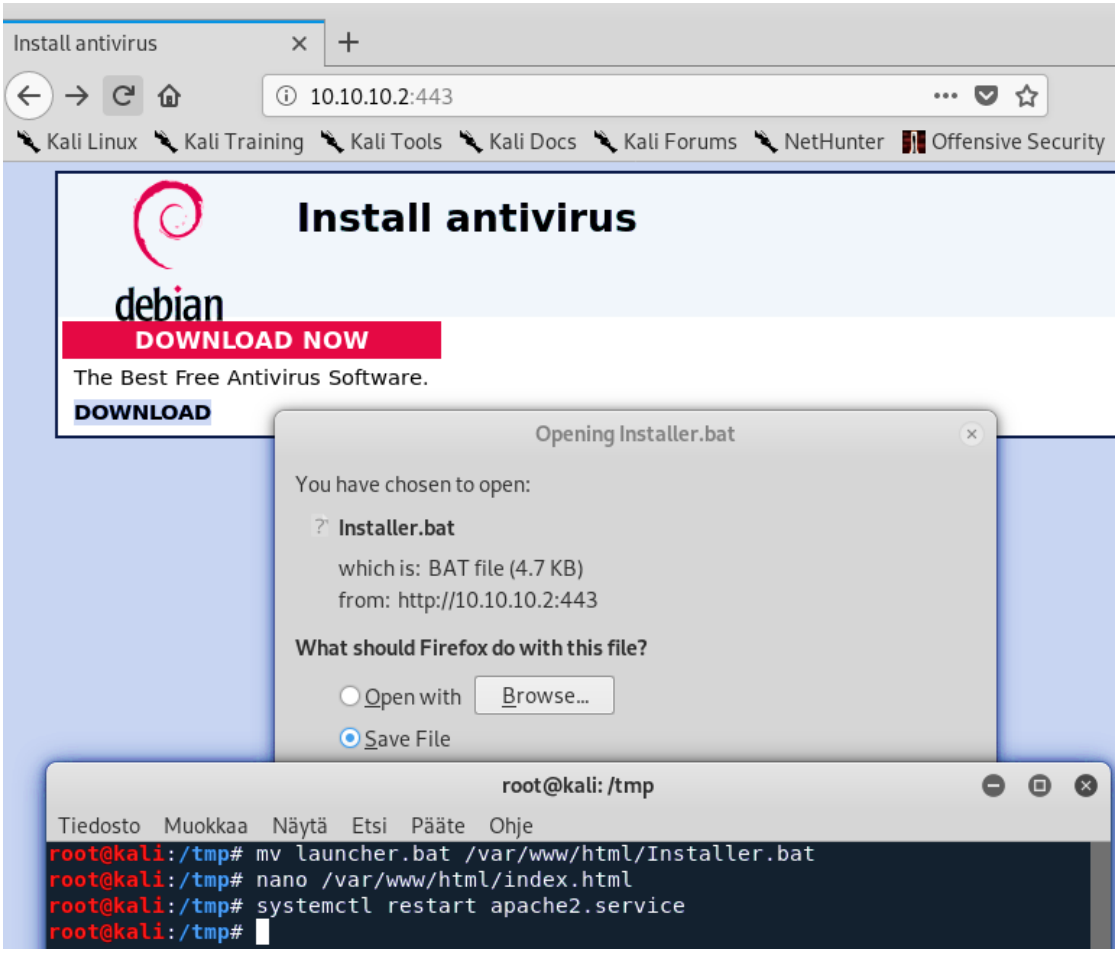
Kuvio 20. C2-kuuntelija

Valmisteluiden jälkeen luotiin varsinainen haittaohjelma eli agentti, jonka tarkoituksena on avata kommunikointiyhteys uhrin koneen ja C2-palvelimen välille. Haittaohjelman luomisen yhteydessä pystyi valitsemaan mahdolliset välityspalvelimet, mutta tässä yhteydessä ei käytetty erillisiä välityspalvelimia. Pakollisena valintana on kuuntelija. Kuuntelijaksi valittiin kuviossa 20 pohjustettu HTTP-kuuntelija (ks. kuvio 21).



Kuvio 21. Haittaohjelman luonti

Haittaohjelman luomisen jälkeen C2-palvelimelle pystytettiin verkkosivut, joiden kautta uhri tulisi lataamaan kyseisen haittaohjelman. Haittaohjelma nimettiin uudelleen ja siirrettiin verkkosivuille, sekä luotiin linkki osoittamaan kyseiseen tiedostoon ja varmistettiin verkkosivujen toimivuus (ks. kuvio 22).

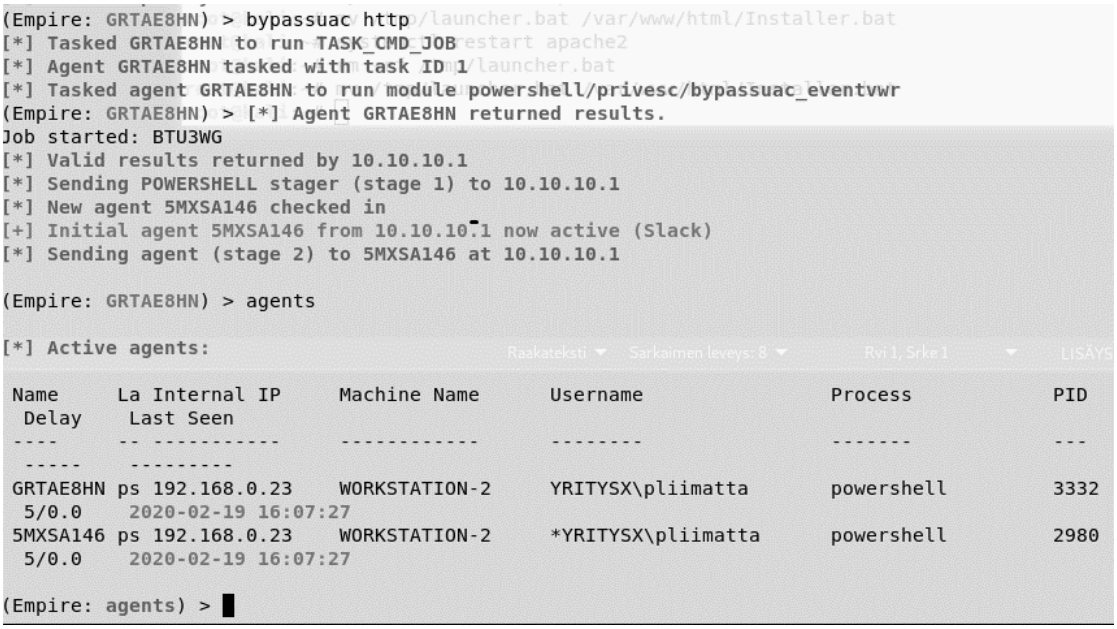


Kuvio 22. C2-palvelimen verkkosivut

Seuraavassa vaiheessa hyökkäystä kohdeyrityksen sisäverkosta uhri lataa haittaohjelman ja suorittaa sen. Uhrin suorittaessa haittaohjelman, haittaohjelma poistaa itsensä ja avaa komentoyhteyden hyökkääjän palvelimelle. Ensimmäinen avautuva yhteys paljastaa muun muassa kyseisen työaseman nimen ja IP-osoitteen ja käyttäjätunnuksen, jolla haittaohjelma on suoritettu. Haittaohjelma valitsee itselleen powershell-prosessin satunnaisesti valikoiduilla prosessinumerolla. High_integrity paljastaa onko hyökkääjä saanut järjestelmänvalvojan oikeudet kyseiseen työasemaan, mikäli tulos on 0 järjestelmänvalvojan oikeuksia ei ole saavutettu vielä (ks. kuvio 23).

Kuvio 23. Yhteys luotu uhrin työasemaan

Järjestelmänvalvojan oikeuksien puuttuessa voidaan yrittää saada ne käyttöön ohittamalla käyttäjätilien valvonta eli UAC (User Account Control). Käyttäjätilien valvonnan alkuperäisenä tavoitteena oli parantaa tietoturvaa rajoittamalla ohjelmistojen toimintaa. Kyseistä ominaisuutta voidaan myös väärinkäyttää ja sillä voidaan ohittaa käyttäjätileille asetettuja rajoituksia. Kuviossa 24 on esitetty käyttäjätilien valvonnan ohitus, jonka jälkeen alkuperäinen agentti luo uuden agentin, jolla on järjestelmänvalvojan oikeudet.



Kuvio 24. Järjestelmänvalvojan oikeuksien saaminen

Järjestelmänvalvojan oikeuksien saamisen jälkeen myös tunnustenkalastelusta tulee helpompaa laajempien oikeuksien vuoksi. Tunnustelunkalastelun avulla myös mahdollisesta brute-force hyökkäyksestä voi tulla helpompaa, jos käyttäjä sattuu käyttämään samaa salasanaa useassa eri paikassa. PoweShell Empire-ohjelmiston mukana tulee valmiina tunnustenkalasteluun sopiva lisäosa, Mimikatz (ks. kuvio 25). Mimikatz kerää järjestelmästä kaikenlaisia kirjautumistietoja ja palauttaa ne sitten hyökkääjälle (ks. kuvio 26).

```
(Empire: 5MXSA146) > mimikatz
[*] Tasked 5MXSA146 to run TASK_CMD_JOB
[*] Agent 5MXSA146 tasked with task ID 1
[*] Tasked agent 5MXSA146 to run module powershell/credentials/mimikatz/logonpasswords
(Empire: 5MXSA146) > [*] Agent 5MXSA146 returned results.
Job started: AH5S86
[*] Valid results returned by 10.10.10.1
[*] Agent 5MXSA146 returned results.
Hostname: Workstation-2.yritysx.net / S-1-5-21-4252475531-1125702568-4177972488

  .#####.   mimikatz 2.1.1 (x64) built on Nov 12 2017 15:32:00
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 145216 (00000000:00023740)
Session           : Interactive from 1
User Name         : pliimatta
Domain            : YRITYSX
Logon Server      : WIN-SERV-DC
Logon Time        : 16.2.2020 15:04:35
SID               : S-1-5-21-4252475531-1125702568-4177972488-1127
        msv :
         [00000003] Primary
         * Username : pliimatta
```

Kuvio 25. Mimikatz lisäosa

```
(Empire: 5MXSA146) > creds

Credentials:

  CredID  CredType   Domain                  UserName         Host             Password
  ------  --------   ------                  --------         ----             --------
  1       hash       yritysx.net             pliimatta        Workstation-2    a54721b2475ca0d
d71ae2b88496b36e8
  2       hash       yritysx.net             WORKSTATION-2$   Workstation-2    50d43695aa09031
24f949c7d7118bad1
  3       plaintext  yritysx.net             pliimatta        Workstation-2    kurkikuja123!

(Empire: 5MXSA146) >
```

Kuvio 26. Tunnustenkalastelulla saadut kirjautumistiedot

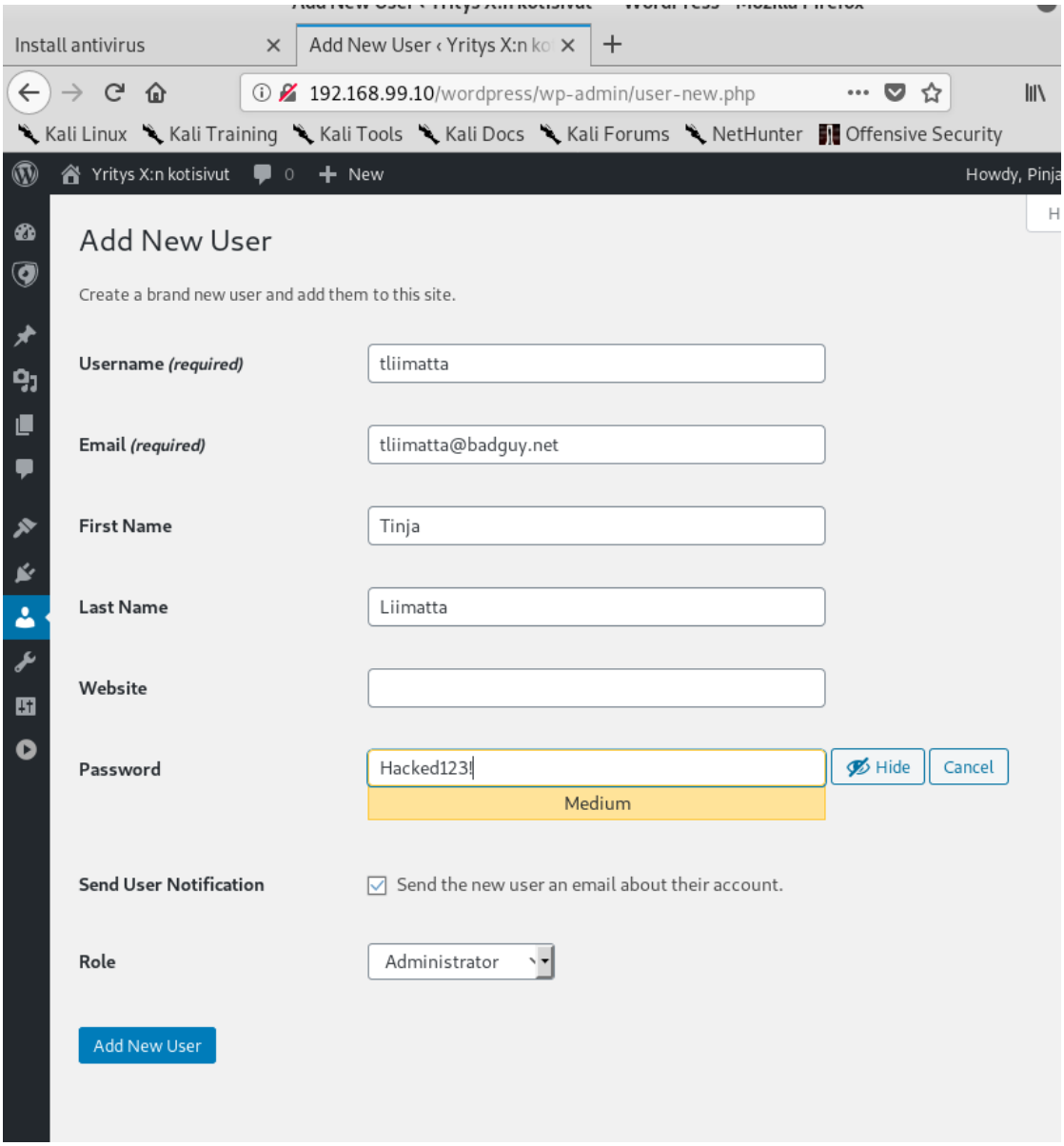
Onnistuneen tunnustenkalastelun jälkeen, oli tarkoitus asettaa uhrin järjestelmiin pysyvä jalansija ja varmistaa pääsy järjestelmiin myös jatkossa. PowerShell Empiressä tämäkin ominaisuus on valmiiksi implementoitu. PowerShell Empiren yhdellä moduulilla pystytään luomaan Windows käyttöjärjestelmiin rekisterimerkintä, jonka avulla haittaohjelma suorittaa itsensä aina uudestaan sisäänkirjautumisen yhteydessä. Rekisterimerkintä on kuitenkin helppo huomata, jos tietää mistä etsiä. Haittaohjelma

piilottaa rekisterimerkinnän Windowsin käynnistyksen yhteydessä suoritettavien ohjelmien rekisteriin. Kyseisen rekisterimerkinnän yhteyteen lisättiin lippu 2 (ks. kuvio 27). Liitteessä 3 kohdassa 9 on esitetty rekisterimerkinnän sijainti uhrin työasemalla.

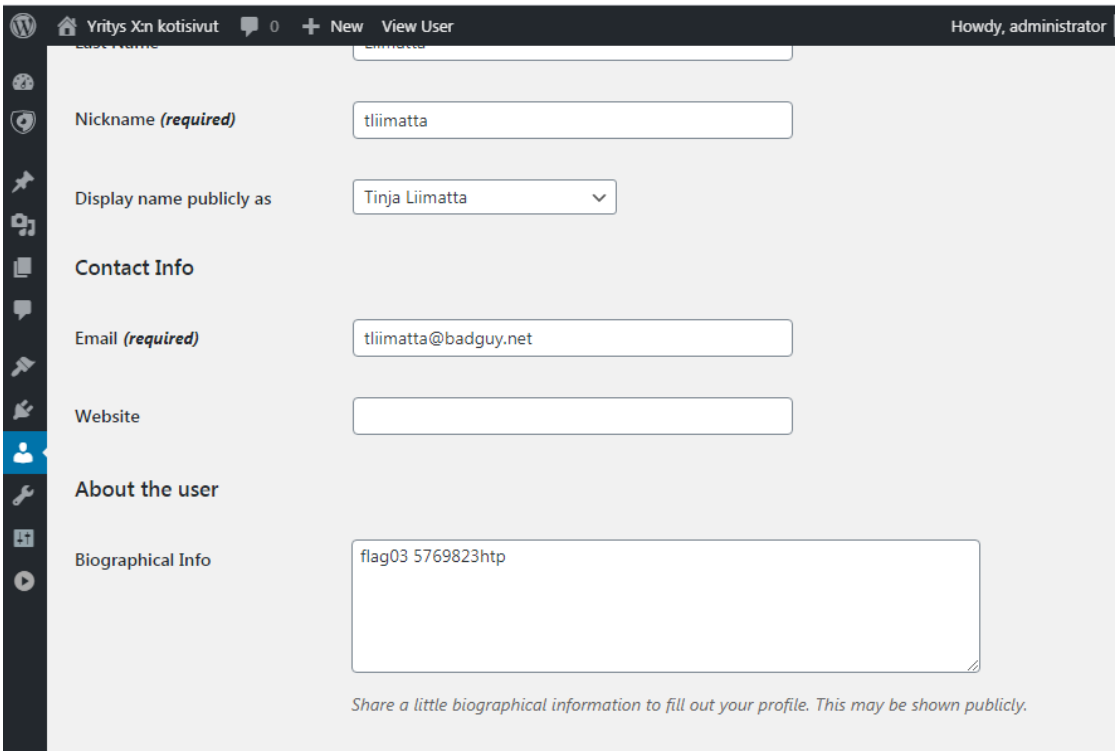
Kuvio 27. Rekisterimerkinnän teko ja lippu 2

Kohdennetun hyökkäyksen viimeisenä vaiheena oli pyrkiä murtautumaan yrityksen verkkosivuille. Tunnustenkalastelun avulla saatujen tietojen avulla pystyttiin murtamaan käyttäjän pliimatta tunnukset ja kirjautumaan niillä sisään yrityksen verkkosivuille. Liitteessä 3 kohdassa 6 pystytään havainnoimaan yrityksen puolelta, kuinka kyseinen ilmiö näkyy WordPressiin asennetussa audit-plugin lisäosassa. Käyttäjätunnuksen murtamisen jälkeen pyrittiin myös asettamaan pysyvä jalansija yrityksen verkkosivuille. Jalansija toteutettiin luomalla uusi käyttäjä WordPressiin ja pyrkimällä naamioimaan tämä muiden käyttäjien sekaan. Käyttäjän naamiointi toteutettiin luomalla lähes saman niminen käyttäjä WordPressiin (ks. kuvio 28). Käyttäjän luomisen

jälkeen sen kuvaukseen lisättiin lippu 3 (ks. kuvio 29). Kolmannen lipun tarkoituksena on saada kilpailija huomaamaan hyökkääjän saaneen jalansijan myös WordPress-käyttöliittymästä.



Kuvio 28. Uuden käyttäjän luominen wordpressiin



Kuvio 29. Lippu 3:n sijoitus

6 Tutkimustulokset

6.1 Tietoturvahaasteeseen osallistuneiden taustat

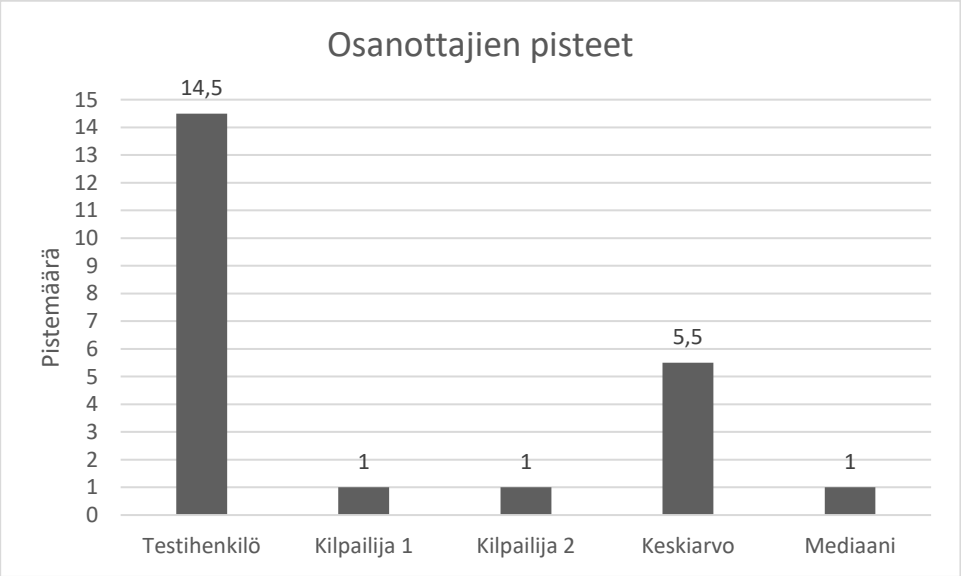
Tietoturvahaasteen oli tarkoitus olla osana Taitaja2020-tapahtumaa. Maailmanlaajuisen pandemian vuoksi tapahtuma kuitenkin peruttiin. Tapahtumassa oli tarkoitus kerätä aineistoa Taitaja2020-tapahtumaan osallistuvilta kilpailijoilta. Peruuntuneen tapahtuman vuoksi järjestettiin pieni suunniteltua kohderyhmää vastaava uusi kohderyhmä yhteistyössä Gradian kanssa. Tutkimusaineisto koostui kahdesta kohderyhmään kuuluvasta henkilöstä ja yhdestä testihenkilöistä. Testihenkilö oli neljännen vuoden AMK-opiskelija.

Testihenkilön perusteella ohjelmistojen käyttöohjeet huomattiin puutteellisiksi, joten ohjeita päivitettiin varsinaisia kilpailijoita varten. Ohjelmistojen käyttöohjeita selkiytettiin lisäämällä lisävaiheita (ks. Liite 5). Oikeat vastaukset tietoturvahaasteeseen

käytiin kilpailijoiden kanssa läpi tietoturvahaasteen jälkeen, jotta kilpailijat hyötyisivät harjoituksesta enemmän. Tietoturvahaasteeseen osallistuneet kilpailijat olivat kolmannen vuoden tieto- ja tietoliikennetekniikan perustutkinnon opiskelijoita.

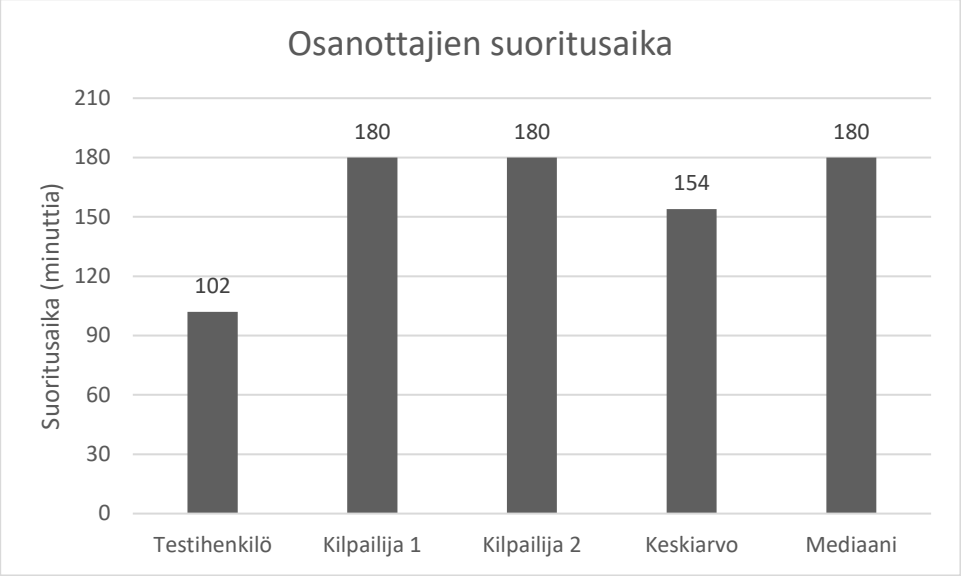
6.2 Kilpailijoiden pisteet

Maksimipistemäärä tietoturvahaasteesta oli viisitoista pistettä. Kilpailijoiden pistekeskiarvo harjoituksessa oli 5,5 ja mediaani kilpailijoiden keskuudessa oli 1. Parhaimman tuloksen harjoituksessa sai testihenkilönä toiminut osanottaja (ks. kuvio 30).



Kuvio 30. Kilpailijoiden pisteet

Kilpailijoiden keskimääräinen suoritusaika harjoituksessa oli 154 minuuttia. Nopein suoritusaika harjoituksessa oli testihenkilöllä ajassa 102 minuuttia. Suunniteltua kohderyhmää edustaneet kilpailijat 1 ja 2 molemmat käyttivät kaiken sallitun ajan eli 180 minuuttia. Näin ollen mediaaniksi muodostui 180 minuuttia (ks. kuvio 31).



Kuvio 31. Kilpailijoiden suoritusajat

6.3 Palautekyselyn tulokset

Kilpailijoilta kerättiin myös palautetta kyselyn muodossa tietoturvahaasteeseen liittyen. Palautekysely on liitteessä 6 ja palautekyselyn tulokset liitteessä 7. Liitteen 7 kohdassa 2 on esitetty palautekyselyyn vastanneiden arvioinnit tehtävän vaikeuteen liittyen. Tietoturvahaaste koettiin vaikeaksi. Kohderyhmään kuuluneet kilpailijat kokivat haasteen joko vaikeaksi tai liian vaikeaksi. Testihenkilön mielestä tehtävä oli haastavuudeltaan sopiva. Tehtävä koettiin kiinnostavana. Tietoturvahaasteen skenaario oli palautteen mukaan luotu hyvin ja realistinen (ks. liite 7 kohta 3).

Kohderyhmään kuuluneet kilpailijat kokivat tietoturvahaasteen parantaneen heidän käsitystään tietoturvahaasteessa esiintyneiden tietoturvapoikkeamien suhteen. Testihenkilölle kyseiset ilmiöt olivat jo entuudestaan tuttuja. Testihenkilö kuitenkin koki saaneensa paremman käsityksen haittaohjelmien pysyvyyden suhteen (ks. liite 7 kohta 4).

Kilpailijat kokivat harjoituksessa käytettyjen työkalujen eli ohjelmistojen käytön keskimäärin sopivan haastavaksi. Yksi kilpailijoista koki työkalujen käytön vaikeaksi, kun

taas toinen kohderyhmään kuuluvista koki sen helpohkoksi. Testihenkilö koki työkalujen käytön sopivaksi (ks. liite 7 kohta 5). Työkalut olivat entuudestaan tuntemattomia kaikille (ks. liite 7 kohta 6). Tietoturvahaasteen suorittaneista henkilöistä vain testihenkilönä toiminut AMK-opiskelija koki saaneen riittävästi koulutusta tietoturvan suhteen koulussa. Varsinaiseen kohderyhmään kuuluneet kilpailijat kokivat tietoturvakoulutuksen riittämättömäksi koulussa (ks. liite 7 kohta 7).

Kaikki tietoturvahaasteen suorittaneet henkilöt kokivat virtuaaliympäristön teknisen toteutuksen vastaavan koulussa opetettuja asioita (ks. liite 7 kohta 8). Kilpailija 1 koki ettei pystyisi luomaan tietoturvahaasteen tapahtumista karkeaa aikajanaa. Kilpailija 2 ja testihenkilö puolestaan kokivat kykenevänsä muodostamaan tapahtumista karkean aikajanan (ks. liite 7 kohta 9).

7 Johtopäätökset

Mikä on kilpailijoiden taso havainnoida tietoturvapoikkeamia suljetussa ympäristössä?

Tietoturvahaasteeseen osallistuneet kilpailijat eivät juurikaan onnistuneet havaitsemaan haasteessa olleita tietoturvapoikkeamia. Testihenkilönä toiminut AMK-opiskelija kykeni havaitsemaan selkeästi paremmin haasteessa ilmenneet tietoturvapoikkeamat. AMK-opiskelijan ja ammattiin opiskelevien välillä on selkeästi paljon eroa. Tutkimuksen otanta on kuitenkin liian pieni, jotta tutkimuksen tuloksesta voitaisiin varmistua. AMK-opiskelijoiden ja ammattiin opiskelevien välinen osaamisen ero on todennäköisesti kuitenkin huomattavasti pienempi suuremmalla otannalla. Kilpailijoiden kyky havaita tietoturvapoikkeamia riippuu kuitenkin kilpailijan osaamisesta.

Vuonna 2015 tehdyssä tutkimuksessa osoittautui, että aiemmin hankitulla tiedolla on merkitystä. Tutkimukseen osallistuneilla henkilöillä, jotka onnistuivat havaitsemaan ilmiöt paremmin ja tulkitsemaan ne oikein, omasivat jo entuudestaan osaamista tietoturvasta. Tutkimuksessa myös huomattiin, että kokeneemmat osasivat myös tunnistaa erilaiset hyökkäystyypit. (Ben-Asher & Gonzalez 2015.)

Toimiiko CTF-harjoitus kiinnostavana tapana tutustua ja tutkia tietoturvapoikkeamia ja parantavatko ne käsitystä tietoturvapoikkeamista?

Tietoturvahaaste kuitenkin koettiin kiinnostavaksi ja haastavaksi tavaksi lähestyä tietoturvailmiöitä. Tämä tulos vahvistaa aiemmista tutkimuksista saatua tulosta, jonka mukaan tietoturvahaasteet koettaisiin kiinnostaviksi ja haastaviksi (Chothia & Novakovic 2015.). Osa tietoturvahaasteen haasteellisuudesta johtuu haasteessa käytetyistä ohjelmistoista. Kaikille osallistuneille tietoturvahaasteessa olleet ohjelmistot olivat vieraita ja jokseenkin vaikeita käyttää. Mikäli ohjelmistot olisivat olleet entuudestaan tuttuja kohderyhmään kuuluville, olisivat heidän tuloksensa luultavasti olleet parempia. Kilpailijat kuitenkin kokivat tietoturvahaasteen parantaneen heidän käsitystään tietoturvasta. Myös AMK-opiskelija koki tietoturvahaasteen parantaneen käsitystä tietoturvapoikkeamista. Tietoturvahaasteiden koetaan siis parantavan käsitystä tietoturvailmiöistä.

Myös vuonna 2017 tehdyssä tutkimuksessa huomattiin, että tietoturvahaasteet lisäävät osallistujien osaamista. Tutkimuksessa myös huomattiin, että tietoturvahaasteet lisäsivät itseluottamista omaan osaamiseen. Tutkimuksessa korkeakouluopiskelijoille tehtiin kysely ennen tietoturvaharjoitusta ja sen jälkeen. (Leune & Petrilli 2017.) Toisessa vuonna 2017 tehdyssä tutkimuksessa, tietoturvahaasteiden koettiin myös kasvattavan tietoisuutta, osaamista, sekä itseluottamusta tietoturvan suhteen. Tutkimuksessa tutkittiin lukiolaisten osaamista teoriatasolla ja tutustuttamalla tutkittavat tietoturvan perusasioihin. (Brown, Ford, Haynes & Siraj 2017.)

Kykenevätkö kilpailijat asettamaan harjoituksen tapahtumat aikajärjestykseen?

Tutkimuksen kohderyhmään kuuluvista kilpailijoista toinen koki pystyvänsä muodostaa tietoturvahaasteen tapahtumista aikajanan. Asiasta ei kuitenkaan voida varmistua, sillä palautekyselyssä olevan kysymyksen (ks. liite 6 kohta 8) tarkoituksena oli saada karkea aikajana tapahtumista. Kysymys on kuitenkin vastaajien puolella väärinymmärretty ja vastaajat eivät ole kuvailleet tapahtumien aikajanaa. Myös testihenkilönä toiminut AMK-opiskelija vastasi ymmärtäneensä tapahtumien aikajanan, mutta ei myöskään kuvaillut vastauksessaan tietoturvahaasteen tapahtumia. Tuloksista ei voida siis varmistua ymmärsivätkö he oikeasti tapahtumien aikajanaa.

Aikajanan luominen tapahtumista on kriittinen osa tutkintaa, kun halutaan ymmärtää mitä järjestelmässä oikein tapahtui (Adderley 2019.). Kilpailijoiden luomien aikajanojen perusteella olisi pystytty tarkemmin arvioimaan kilpailijoiden ymmärrystä tietoturvailmiöistä. Aikajanat olisivat myös paljastaneet mahdolliset väärät tulkinnat tietoturvahaasteen tapahtumista.

Kokevatko kilpailijat tietoturvaopetuksen koulussa riittäväksi?

Ammattiin opiskelevat kokivat tietoturvaopetuksen olevan riittämätöntä, kun taas testihenkilönä toiminut AMK-opiskelija koki sen riittäväksi. Koulutuksen määrällä ja tasolla siis oli selkeästi vaikutusta osaamiseen. AMK-opiskelija pärjäsikin tietoturvahaasteessa selvästi paremmin kuin suunniteltuun kohderyhmään kuuluneet kilpailijat. Koulutuksella voikin olla vaikutusta osaamisen lisäksi myös itseluottamuksen suhteen. Tietoturvahaasteiden onkin koettu parantavan kilpailijoiden itseluottamusta ja osaamista tietoturvaosaamisensuhteen (Brown, Ford, Haynes & Siraj 2017.).

Eräässä artikkelissa olikin tutkittu tietoturvaosaamisen syvyyden ja laajuuden eroa. Artikkelissa huomattiin, kuinka eräässä tutkimuksessa oli havaittu, että syventävän koulutuksen saaneet opiskelijat pärjäsivät paremmin kuin opiskelijat, jotka olivat saaneet koulutusta monesta eri aihealueesta lukiossa. Artikkelissa myös todettiin, että opiskelijat, joilla oli jo entuudestaan tietoturvaosaamista, saivat parempia harjoittelupaikkoja. (Manson & Pike 2014, 51–52.)

8 Pohdinta

Aihe oli haastava asetetun näkökulman ja uutuutensa vuoksi. Tietoturvahaasteista löytyy jonkin verran tutkimuksia, mutta harvat tutkimukset on suunniteltu tietoturvapoikkeamien havainnoinnin kannalta. Suurin osa tietopohjasta käsitteleekin tietoturvahaasteiden hyödyllisyyttä yleisellä tasolla. Myöskään tietoturvahaasteiden suunnittelusta löytyvä artikkeleita ja tietolähteitä oli vaikea löytää olemalla lähdekriittinen. Tietoturvahaasteen suunnitteleminen ammattikoululaisille oli myös haastavaa opetussuunnitelman vähäisten tietoturvavaatimuksien vuoksi. Tutkimus onkin toteutettu

kehittämistutkimuksena soveltaen sekä laadullisen, että määrällisen tutkimuksen keinoja. Työn tutkimusmenetelmäksi valittiin kehittämistutkimus, koska kehittämistutkimuksen katsottiin soveltuvan parhaiten tutkimusongelman ratkaisemiseen. Kehittämistutkimuksella ratkaistiin tutkimuksen käytännön ongelma eli kuinka tietoturvahaasteeseen sopiva virtuaaliympäristö pystyttiin toteuttamaan. Kun käytännön ongelma tutkimuksessa oli ratkaistu, pystyttiin varsinainen tutkimus toteuttamaan.

Työn tavoitteena oli luoda haastava tietoturvahaaste ammattiin opiskeleville nuorille, joka vastaisi rakenteeltaan ammattiin opiskelevien opetussuunnitelmassa esitettyjä osaamisvaatimuksia. Työn tavoitteena oli myös selvittää ammattiin opiskelevien nuorten tasoa havaita tietoturvapoikkeamia suljetussa ympäristössä. Ammattiin opiskelevat ei juurikaan onnistuneet havaitsemaan tietoturvahaasteissa esiintyneitä tietoturvapoikkeamia. Kilpailijat kuitenkin kokivat tietoturvahaasteessa käytettyjen työkalujen käytön vaikeaksi, mikä saattaa osaltaan selittää ammattiin opiskelevien alhaiset pisteet. Toisaalta myös AMK-opiskelijalle työkalut olivat entuudestaan vieraita, mutta testihenkilönä toiminut AMK-opiskelija kuitenkin onnistui havaitsemaan kaikki ympäristössä vallinneet tietoturvapoikkeamat.

Työn suunnittelussa pyrittiin sovittamaan ammattikoululaisten opetussuunnitelmassa olevat vähäiset tietoturvavaatimukset mahdollisimman hyvin tietoturvahaasteeseen. Myös ajankohtaisia tietoturvailmiöitä sovitettiin tietoturvahaasteeseen. Tietoturvahaaste myös suunniteltiin mahdollisimman helposti lähestyttäväksi, jotta osallistujat eivät kokisi harjoitusta ylitsepääsemättömän vaikeaksi ja luovuttaisi sen takia. Työn suunnittelussa on onnistuttu hyvin, sillä virtuaaliympäristön infrastruktuurin koettiin vastaavan kilpailijoiden koulussa oppimia asioita. Harjoitus toteutettiin mahdollisimman realistisella tavalla eli tietoturvahaasteen toteutuksessa käytettiin hyökkäävää osapuolta, joka aiheuttaa tietoturvapoikkeaman hyökkäyksellään kohdeyritykseen.

Tutkimuksen aineistonkeruu oli aikaa vievää. Yhden testikerran järjestämiseen kului aikaa keskimäärin kahdeksan tuntia. Virtuaaliympäristön käyttämiseen vaadittavat resurssit rajoittivat myös testaamista. Haasteelliseksi osoittautui löytää aineistonkeruuhun sopivat tilat, jossa työasemissa olisi tarpeeksi resursseja. Aineistonkeruussa

käytettiin JAMKin tiloja. Koronaviruspandemian aikaan JAMKin tilojen käyttöä oli myös rajoitettu kuuteen henkilöön tilaa kohden, joten yksittäisen testikerran otannat jäivät rajoitusten vuoksi pieniksi. Gradian kanssa yhteistyössä toteutettuun testikertaan ei myöskään ilmestynyt sovittua viittä kilpailijaa. Sovituista kilpailijoista vain kaksi saapui tilaisuuteen. Tutkimuksessa kerätty aineisto on tämän vuoksi hyvin suppea. Ottaen huomioon tutkimusaikana olleet rajoitukset kokoontumisten suhteen, laajan aineiston kerääminen olisi vienyt useita kuukausia.

Tutkimustulosten luotettavuuden arviointi onkin haasteellista, sillä kehittämistutkimus ei ole yksittäinen tutkimusmetodi. Kehittämistutkimus kostuu tarvittaessa määrällisestä ja laadullisesta tutkimuksesta koostuva metodi, jolla ratkaistaan tutkimuskohteen ongelma. Kehittämistutkimuksen luotettavuutta arvioidaan siinä käytettyjen tutkimusmetodien arviointikriteerien perusteella. Tutkimustulosten pitää olla pysyviä eli tutkimustulokset eivät saa muuttua uusintamittauksen jälkeen. (Kananen 2015, 111—112.) Tutkimuksen tuloksia ei voida pitää kovin merkittävinä, mutta niitä voidaan pitää suuntaa antavina. Tutkimuksen otos on liian pieni, jotta sen avulla voitaisiin yleistää ammattiin opiskelevien kykyjä havaita tietoturvapoikkeamia suljetussa ympäristössä. Tuloksia voitaisiin kuitenkin hyödyntää ammattikoululaisten osaamisen kartoituksessa ja muokata kurssien sisältöjä enemmän tietoturvapainotteisiksi. Tutkimuksen tulokset kuitenkin vahvistavat aikaisemmissa tutkimuksissa saatuja tutkimustuloksia, joiden mukaan tietoturvahaasteet koetaan kiinnostaviksi, mutta haastaviksi tavoiksi lähestyä tietoturvaa.

Lopputuloksena tutkimustyöstä saatiin virtuaaliympäristö, jossa voidaan harjoitella tietoturvapoikkeamien havainnointia, tutkimusdataa tietoturvahaasteen suorittaneilta henkilöiltä, sekä tarkan dokumentoinnin tietoturvahaasteen suunnittelusta. Työstä syntynyttä virtuaaliympäristöä voidaan hyödyntää esimerkiksi opetuksessa JAMKilla tai Gradialla. Virtuaaliympäristöä voidaan myös käyttää pohjana tulevissa Taitaja-tapahtumissa.

Jatkokehitysideana virtuaaliympäristö voitaisiin siirtää pilviympäristöön. Siirtämällä virtuaaliympäristö pilveen, sen hallinnoinnista tulisi helpompaa ja tietoturvahaaste pystyttäisiin skaalaamaan tarvittaessa useammille kilpailijoille samanaikaisesti. Tämä

myös poistaisi resurssirajoitukset paikallisesti, joten tietoturvahaasteen suorittamiseen ei tarvittaisi, kuin pelkästään yhteys pilvipalveluun.

Lähteet

2019 State of Malware. 2019. Malwarebytes Labsin raportti haittaohjelmista. Viitattu 30.11.2019. https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf.

Active Directory. 2017. TechTerms verkksivusto. Muokattu 13.7.2017. Viitattu 11.11.2019. https://techterms.com/definition/active_directory.

Active Directory. 2018. TechTarget verkkosivusto. Muokattu 06.2018. Viitattu 11.11.2019. https://searchwindowsserver.techtarget.com/definition/Active-Directory.

Adderley, N. 2019. Graph-based Temporal Analysis in Digital Forensics. Viitattu 19.4.2020. https://scholar.afit.edu/cgi/viewcontent.cgi?article=3242&context=etd.

Alasuutari, P. 2011. Laadullinen tutkimus 2.0. Viitattu 24.11.2019. https://janet.finna.fi.

Ben-Asher, N., Gonzalez, C. 2015. Effects of cyber security knowledge on attack detection. Viitattu 18.4.2020. https://doi.org/10.1016/j.chb.2015.01.039.

Blueteam Capture The Flag. 2020. JYVSECTEC verkkosivut. Viitattu 15.4.2020. https://jyvsectec.fi/services/exercises/blueteam-ctf/.

Brown, E., Ford, V., Haynes, A., Siraj, A. 2017. Capture the Flag Unplugged: an Offline Cyber Competition. Viitattu 18.4.2020. https://dl.acm.org/doi/pdf/10.1145/3017680.3017783.

Buchanan C. 2014. Kali Linux CTF Blueprints. Packt Publishing 2014. Viitattu 20.11.2019. https://www.biblio.securityhacklabs.net/Hacking/General/Kali%20Linux%20CTF%20Blueprints.pdf.

Buechler C., Pingel J. 2019. The pfSense Book. Electric Sheep Fencing LLC. Viitattu 1.12.2019. https://docs.netgate.com/manuals/pfsense/en/latest/the-pfsense-book.epub.

Burns, T., Gu, Q., Jordan, T., Rios, C., Underwood, T. 2017. Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education, Department of Computer Science Texas State University ja Netspend corporation. Viitattu 18.11.2019. https://www.usenix.org/system/files/conference/ase17/ase17_paper_burns.pdf.

CCDC mission. 2019. National Collegiate cyber Defense Competition verkkosivut. Viitattu 18.11.2019. https://www.nationalccdc.org/index.php/competition/about-ccdc/mission.

Command-and-control explained. N.d. Paloalto networks verkkosivu. Viitattu 1.12.2019. https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained.

Chothia, T., Novakovic, C. 2015. An Offline Capture the Flag-Style Virtual Machine and an Assessment of its Value for Cybersecurity Education. Viitattu 15.3.2020. https://www.usenix.org/system/files/conference/3gse15/3gse15-chothia.pdf.

CTF 101. N.d. New Yorkin yliopiston OSIRIS Labin ja CTFd LLC:n kokoama tietosivu capture the flag harjoituksista. Viitattu 18.11.2019. https://ctf101.org/.

DNS Hierarchy. 2018. InetDaemon verkkosivusto. Muokattu 19.5.2018. Viitattu 12.11.2019. https://www.inetdaemon.com/tutorials/internet/dns/operation/hierarchy.shtml.

Dynamic Host Configuration Protocol (DHCP). 2019. Microsoft Docs verkkosivusto. Muokattu 28.9.2019. Viitattu 12.11.2019. https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top.

Digital Forensics and Incident Response exercise. 2020. JYVSECTEC verkkossivut. Viitattu 15.4.2020. https://jyvsectec.fi/services/exercises/dfir/.

Google CTF. 2019. Googlen capture the flag tietosivu. Viitattu 18.11.2019. https://buildyourfuture.withgoogle.com/events/ctf/.

Heikkilä, T. 2014. Tilastollinen Tutkimus. Viitattu 24.11.2019. https://janet.finna.fi.

Leune, K., Petrilli, S. 2017. Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. Viitattu 18.4.2020. https://dl.acm.org/doi/pdf/10.1145/3125659.3125686.

Introduction to Kerberos. N.d. IBM knowledge center verkkosivut. Viitattu 16.11.2019. https://www.ibm.com/support/knowledgecenter/en/SSCRJU_4.3.0/com.ibm.streams.cfg.doc/doc/setting-up-kerberos-overview.html.

ISO/IEC 27035-1. 2016. Information technology. Security techniques -- Information security incident management -- Part 1: Principles of incident management. Viitattu 24.11.2019. https://janet.finna.fi.

ISO 27035-2. 2016. Information technology -- Security techniques -- Information security incident management -- Part 2: Guidelines to plan and prepare for incident response. Viitattu 24.11.2019. https://janet.finna.fi.

Kananen, J 2015. Kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylän Ammattikorkeakoulun julkaisuja 212. Jyväskylä: Jyväskylän ammattikorkeakoulu. Viitattu 18.3.2020. https://janet.finna.fi.

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylän Ammattikorkeakoulun julkaisuja 234. Jyväskylä: Jyväskylän ammattikorkeakoulu. Viitattu 18.3.2020. https://janet.finna.fi.

Kick, J. 2014. Cyber Exercise Playbook. Viitattu 23.3.2020. https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf.

Lähiluku. 2015. Jyväskylän yliopiston avoimet oppimateriaalit. Aineiston analyysimenetelmät. Muokattu 10.4.2015. Viitattu 23.3.2020. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/lahiluku.

Manson, D., Pike R. 2014. The Case for depth in Cybersecurity education. Artikkeli ACM Inroads lehdessä. Viitattu 19.4.2020. https://dl.acm.org/doi/pdf/10.1145/2568195.2568212.

Name Service Switch (NSS). N.d. O'reilly verkkosivusto, LDAP System Administration by Gerald Carter. Viitattu 24.11.2019. https://www.oreilly.com/library/view/ldap-system-administration/1565924916/apas02.html.

OPH M:84/011/2014. Opetushallituksen määräys tieto- ja tietoliikennetekniikan perustutkinnosta. Tutkinnon osat. Viitattu 16.11.2019. https://eperusteet.opintopolku.fi/eperusteet-service/api/dokumentit/6345988.

PAM-based distributed authentication. 2003. Samba.org verkkosivut. Muokattu 31.5.2003. Viitattu.24.11.2019. https://www.samba.org/samba/docs/old/Samba3-HOWTO/pam.html.

Taitaja2020. 2020. Tulevaisuuden osaajat kohti Jyväskylän Taitaja2020-finaalia. Julkaistu 13.2.2020. Viitattu 24.2.2020.https://taitaja2020.fi/fi/uutiset/tulevaisuuden-osaajat-kohti-jyvaskylan-taitaja2020-finaalia/.

Taitaja-tapahtuma. N.d. Skills Finland verkkosivut. Viitattu 29.3.2020. https://skillsfinland.fi/taitaja-tapahtuma.

Teknologiayksikkö. N.d. JAMKin teknologiayksikkö. Viitattu 12.11.2019. https://www.jamk.fi/fi/Tietoa-JAMKista/Teknologiayksikko/.

Vaahtera, N. 2015. Arvioinnin kehittäminen ja tasaisen laadun turvaaminen –Arviointi tarjoilija -lajin ammattitaitokilpailussa. Opinnäytetyö, ylempi AMK. Turun ammattikorkeakoulu, palveluliiketoiminnan koulutusohjelma. Viitattu 28.4.2020. https://www.theseus.fi/bitstream/handle/10024/82599/Vahtera_Niina.pdf?sequence=1&isAllowed=y.

What's a Brute Force Attack? N.d. Kapersky yrityksen verkkosivut. Viitattu 24.2.2020. https://www.kaspersky.com/resource-center/definitions/brute-force-attack.

What is PAM? 2016. Blogikirjoitus medium.com verkkosivustolla. Muokattu 8.8.2016. Viitattu 24.11.2019. https://medium.com/information-and-technology/wtf-is-pam-99a16c80ac57.

What is Ransomware? N.d. Forcepoint verkkosivusto. Viitattu 1.12.2019. https://www.forcepoint.com/cyber-edu/ransomware.

What is samba? N.d. Samba.org verkkosivut. Viitattu 13.11.2019. https://www.samba.org/samba/what_is_samba.html.

What is Trojan? N.d. Norton verkkosivut. Viitattu 1.12.2019. https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html.

Winbind Use of Domain Accounts. 2005. Samba.org verkkosivu. Viitattu 19.11.2019. https://www.samba.org/samba/docs/old/Samba3-HOWTO/winbind.html.

Liitteet

Liite 1. Tehtävänanto Taitaja2020-kisailijoille

Tehtävänanto Taitaja2020 kisoihin.

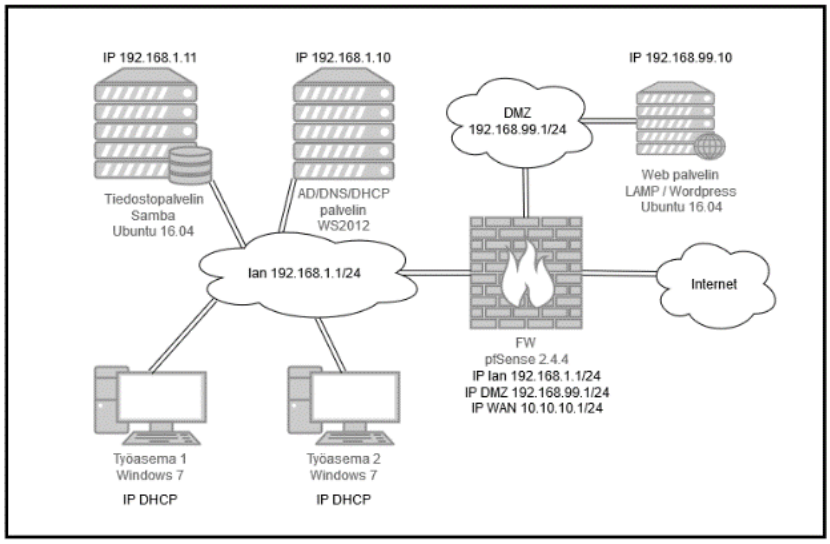
Skenaario:

Toimit YritysX:n IT-tukihenkilönä. Yritykseen on kohdistunut mahdollinen tietoturvapoikkeama. Toimistotyöntekijä on ilmoittanut oudosta virheviestistä, jonka koki koneellaan (Workstation 2). Toimistotyöntekijä muistaa suorittaneensa jonkin ohjelman aiemmin. Tutki mahdollista tietoturvapoikkeamaa ja etsi ympäristöstä kaikki mahdolliset merkit tietoturvapoikkeamasta. Huomioi kaikki laitteet ja palvelut, jotka ovat yrityksen omaisuutta.

Tietoa lipuista

Ympäristöön on piilotettu lippuja, joista saa pisteitä. Liput voivat sijaita missä tahansa mahdollisten tietoturvapoikkeamien yhteydessä. Liput koostuvat kahdesta osasta lipunnumerosta ja arvosta. Esimerkkilippu flag99:1234567aaa.

Alla olevassa kuvassa on YritysX:n verkkoinfrastruktuuri, josta selviää tärkeimmät IP-osoitteet ja palvelut ympäristöstä.



Tarvittavat tunnukset:

Domain tunnukset

mmallikas: Taitaja2020!
Administrator:admini123!

Paikalliset tunnukset työasemille.
admin:admin123!

Tunnukset web palvelimelle

root:Root123!

web:web123!

Paikalliset Tunnukset tiedostopalvelimelle

fileadmin:fileadmin123!

root:Root123!

Tunnukset wordpressiin

Administrator:adminiwp123!

Mmallikas: Mallikasmikko123!

Lisäksi workstation 2 virutaalikoneelle on asennettu työkaluja, kuten Autopsy, Procmon ja Netmon.

Liite 2. Taitaja2020, vastauslomake

Taitaja2020-finaali vastauslomake

1. Kuka latasi haittaohjelman työasemalle? (käyttäjätunnus) (1p)

2. Mistä osoitteesta haittaohjelma on ladattu? (IP ja portti 1,5p)

3. Minkä niminen haittaohjelma on ladattu? ---> (1p)

4. Minkä nimiseksi prosessiksi haittaohjelma on naamioitu? Prosessi ID? (1,5p)

5. Mihin osoitteeseen ottaa yhteyttä? (IP ja portti) (1,5p)

6. Mistä IP osoitteesta tullut kirjautumisyrityksiä web palvelimelle? ja mille käyttäjätunnuksille? (3p)

7. Mitä poikkeavaa wordpressissä on? (1p)

8. Flag1? (1,5p)

9. Flag2? (2p)

10. Flag3? (1p)

Liite 3. Taitaja2020, oikeat vastaukset

Taitaja2020-finaali OIKEAT VASTAUKSET

1. Kuka latasi haittaohjelman työasemalle? (käyttäjätunnus) (1p)

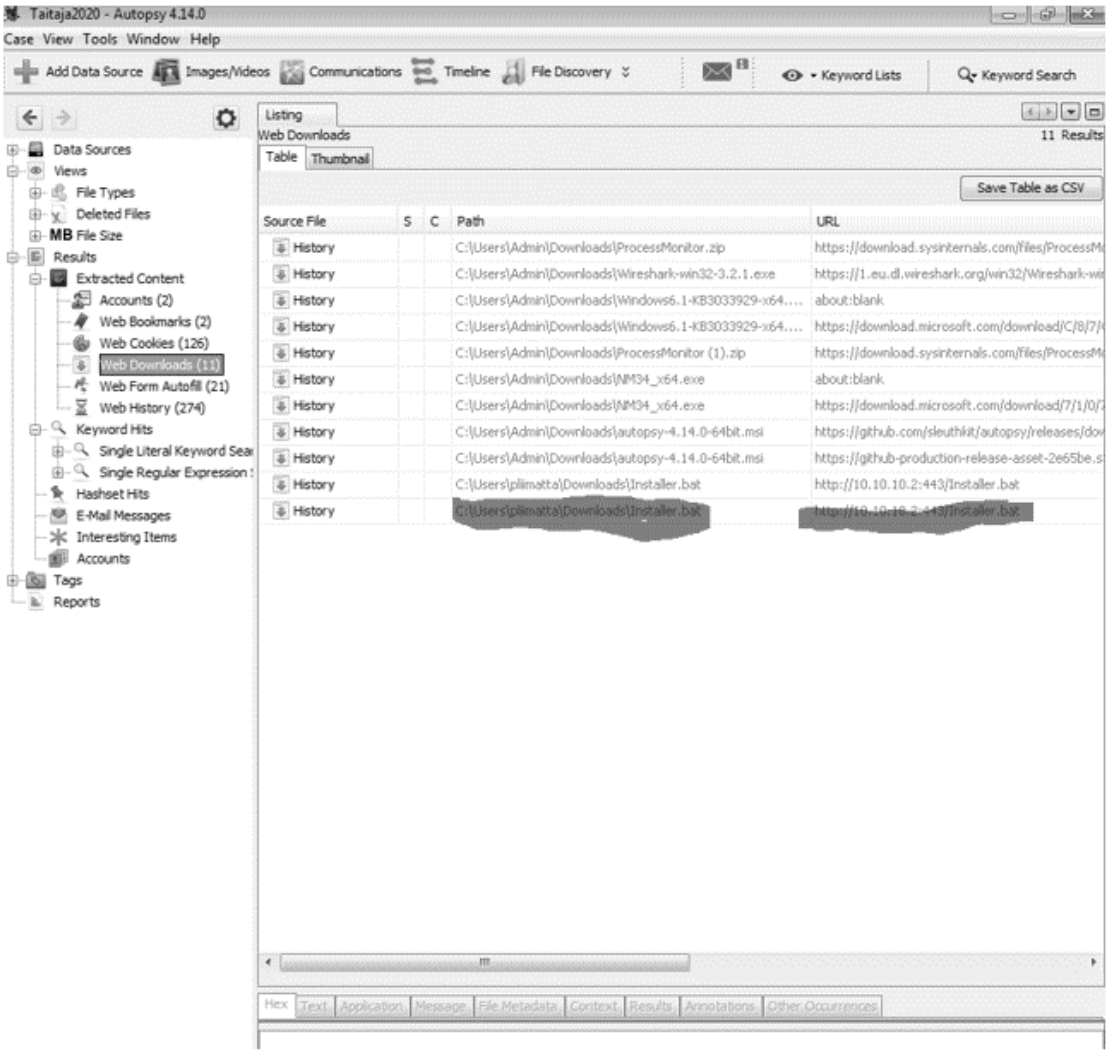
pliimatta

2. Mistä osoitteesta haittaohjelma on ladattu? (IP ja portti 1,5p)

10.10.10.2 443

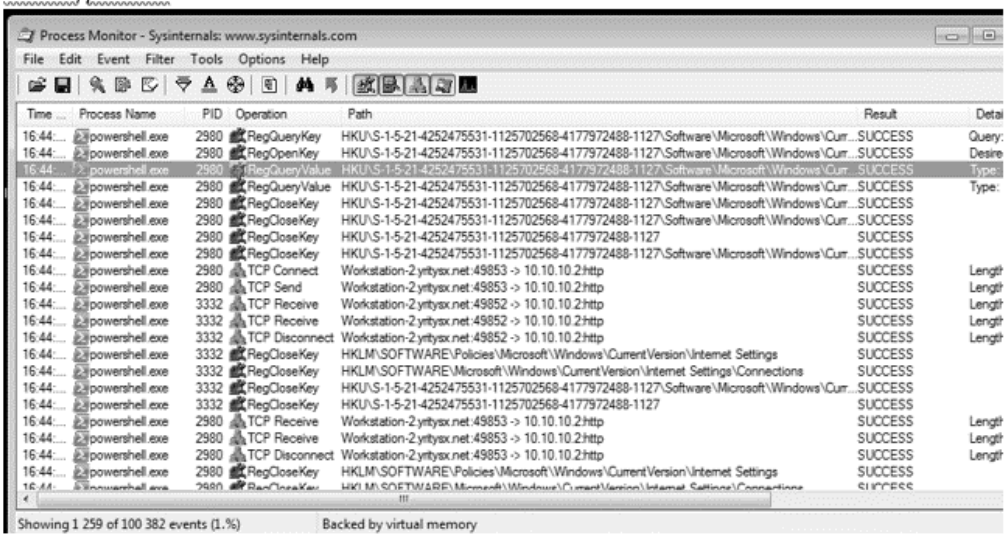
3. Minkä niminen haittaohjelma on ladattu? ---> (1p)

Installer.bat



4. Minkä nimiseksi prosessiksi haittaohjelma on naamioitu? Prosessi ID? (1,5p)

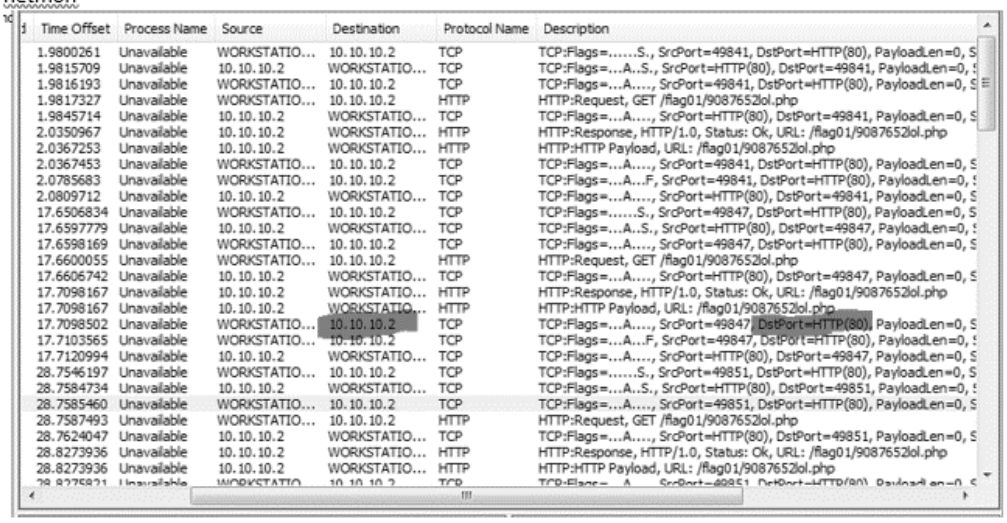
netmon/procmon



powershell.exe 2980 ja 3332

5. Mihin osoitteeseen ottaa yhteyttä? (IP ja portti) (1,5p)

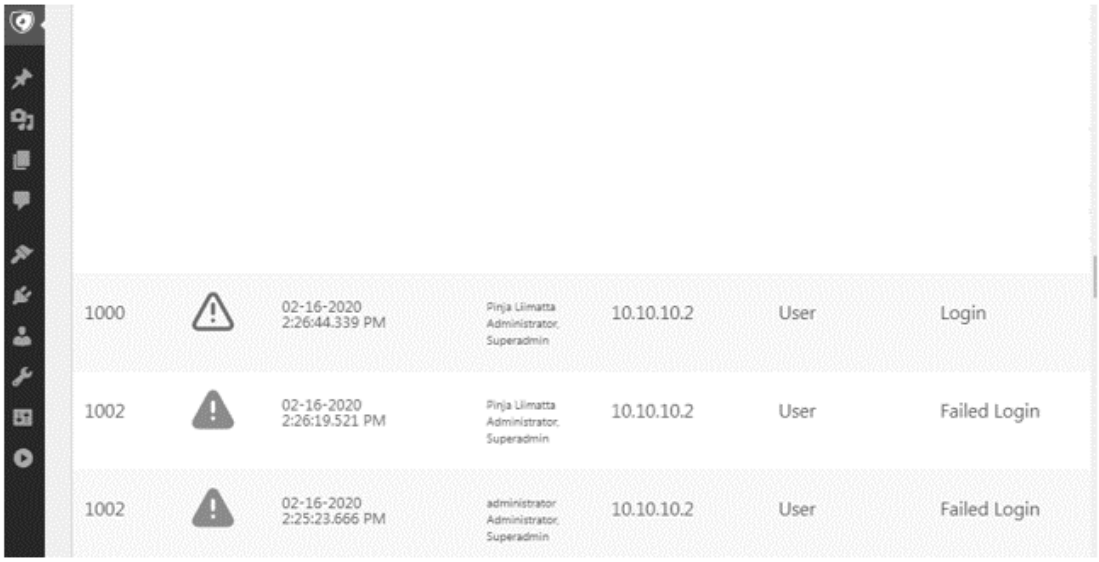
netmon



10.10.10.2 portti 80

6. Mistä IP osoitteesta tullut kirjautumisyrityksiä web palvelimelle? ja mille käyttäjätunnuksille? (3p)

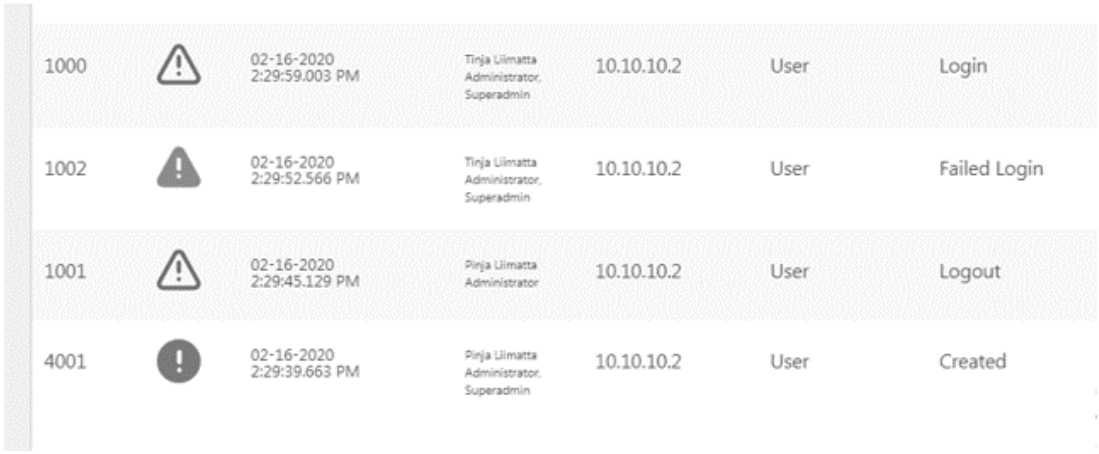
Wordpress audit plugin pliimatta ja administrator 10.10.10.2



1000		02-16-2020 2:26:44.339 PM	Pinja Liimatta Administrator, Superadmin	10.10.10.2	User	Login
1002		02-16-2020 2:26:19.521 PM	Pinja Liimatta Administrator, Superadmin	10.10.10.2	User	Failed Login
1002		02-16-2020 2:25:23.666 PM	administrator Administrator, Superadmin	10.10.10.2	User	Failed Login

7. Mitä poikkeavaa wordpressissä on? (1p)

Wordpress audit plugin pliimatta luonut käyttäjän tliimatta



1000		02-16-2020 2:29:59.003 PM	Tinja Liimatta Administrator, Superadmin	10.10.10.2	User	Login
1002		02-16-2020 2:29:52.566 PM	Tinja Liimatta Administrator, Superadmin	10.10.10.2	User	Failed Login
1001		02-16-2020 2:29:45.129 PM	Pinja Liimatta Administrator	10.10.10.2	User	Logout
4001		02-16-2020 2:29:39.663 PM	Pinja Liimatta Administrator, Superadmin	10.10.10.2	User	Created

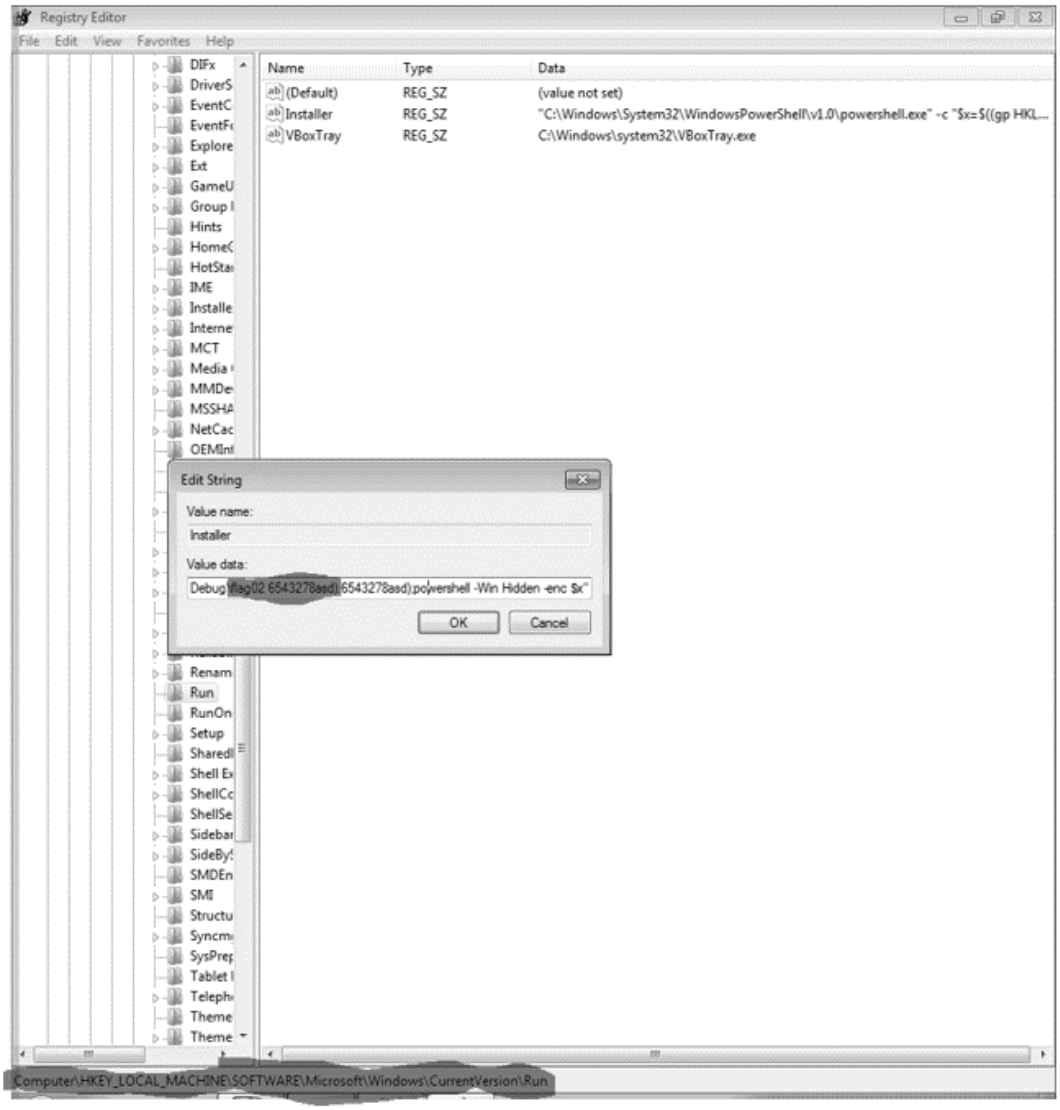
8. Flag1? (1,5p)

Netmon

Time Offset	Process Name	Source	Destination	Protocol Name	Description
1.9800261	Unavailable	WORKSTATIO...	10.10.10.2	TCP	TCP:Flags=.....S., SrcPort=49841, DstPort=HTTP(80), PayloadLen=0, S
1.9815709	Unavailable	10.10.10.2	WORKSTATIO...	TCP	TCP:Flags=...A..S., SrcPort=HTTP(80), DstPort=49841, PayloadLen=0, S
1.9816193	Unavailable	WORKSTATIO...	10.10.10.2	TCP	TCP:Flags=...A...., SrcPort=49841, DstPort=HTTP(80), PayloadLen=0, S
1.9817327	Unavailable	WORKSTATIO...	10.10.10.2	HTTP	HTTP:Request, GET /flag01/9087652lol.php
1.9845714	Unavailable	10.10.10.2	WORKSTATIO...	TCP	TCP:Flags=...A...., SrcPort=HTTP(80), DstPort=49841, PayloadLen=0, S
2.0350967	Unavailable	10.10.10.2	WORKSTATIO...	HTTP	HTTP:Response, HTTP/1.0, Status: Ok, URL: /flag01/9087652lol.php
2.0367253	Unavailable	10.10.10.2	WORKSTATIO...	HTTP	HTTP:HTTP Payload, URL: /flag01/9087652lol.php
2.0367453	Unavailable	WORKSTATIO...	10.10.10.2	TCP	TCP:Flags=...A...., SrcPort=49841, DstPort=HTTP(80), PayloadLen=0, S
2.0785683	Unavailable	WORKSTATIO...	10.10.10.2	TCP	TCP:Flags=...A...F, SrcPort=49841, DstPort=HTTP(80), PayloadLen=0, S
2.0809712	Unavailable	10.10.10.2	WORKSTATIO...	TCP	TCP:Flags=...A...., SrcPort=HTTP(80), DstPort=49841, PayloadLen=0, S
17.6506834	Unavailable	WORKSTATIO...	10.10.10.2	TCP	TCP:Flags=.....S., SrcPort=49847, DstPort=HTTP(80), PayloadLen=0, S
17.6597779	Unavailable	10.10.10.2	WORKSTATIO...	TCP	TCP:Flags=...A..S., SrcPort=HTTP(80), DstPort=49847, PayloadLen=0, S
17.6598169	Unavailable	WORKSTATIO...	10.10.10.2	TCP	TCP:Flags=...A...., SrcPort=49847, DstPort=HTTP(80), PayloadLen=0, S
17.6600055	Unavailable	WORKSTATIO...	10.10.10.2	HTTP	HTTP:Request, GET /flag01/9087652lol.php
17.6606742	Unavailable	10.10.10.2	WORKSTATIO...	TCP	TCP:Flags=...A...., SrcPort=HTTP(80), DstPort=49847, PayloadLen=0, S
17.7098167	Unavailable	10.10.10.2	WORKSTATIO...	HTTP	HTTP:Response, HTTP/1.0, Status: Ok, URL: /flag01/9087652lol.php
17.7098167	Unavailable	10.10.10.2	WORKSTATIO...	HTTP	HTTP:HTTP Payload, URL: /flag01/9087652lol.php
17.7098502	Unavailable	WORKSTATIO...	10.10.10.2	TCP	TCP:Flags=...A...., SrcPort=49847, DstPort=HTTP(80), PayloadLen=0, S
17.7103565	Unavailable	WORKSTATIO...	10.10.10.2	TCP	TCP:Flags=...A...F, SrcPort=49847, DstPort=HTTP(80), PayloadLen=0, S
17.7120994	Unavailable	10.10.10.2	WORKSTATIO...	TCP	TCP:Flags=...A...., SrcPort=HTTP(80), DstPort=49847, PayloadLen=0, S
28.7546197	Unavailable	WORKSTATIO...	10.10.10.2	TCP	TCP:Flags=.....S., SrcPort=49851, DstPort=HTTP(80), PayloadLen=0, S
28.7584734	Unavailable	10.10.10.2	WORKSTATIO...	TCP	TCP:Flags=...A..S., SrcPort=HTTP(80), DstPort=49851, PayloadLen=0, S
28.7585460	Unavailable	WORKSTATIO...	10.10.10.2	TCP	TCP:Flags=...A...., SrcPort=49851, DstPort=HTTP(80), PayloadLen=0, S
28.7587493	Unavailable	WORKSTATIO...	10.10.10.2	HTTP	HTTP:Request, GET /flag01/9087652lol.php
28.7624047	Unavailable	10.10.10.2	WORKSTATIO...	TCP	TCP:Flags=...A...., SrcPort=HTTP(80), DstPort=49851, PayloadLen=0, S
28.8273936	Unavailable	10.10.10.2	WORKSTATIO...	HTTP	HTTP:Response, HTTP/1.0, Status: Ok, URL: /flag01/9087652lol.php
28.8273936	Unavailable	10.10.10.2	WORKSTATIO...	HTTP	HTTP:HTTP Payload, URL: /flag01/9087652lol.php

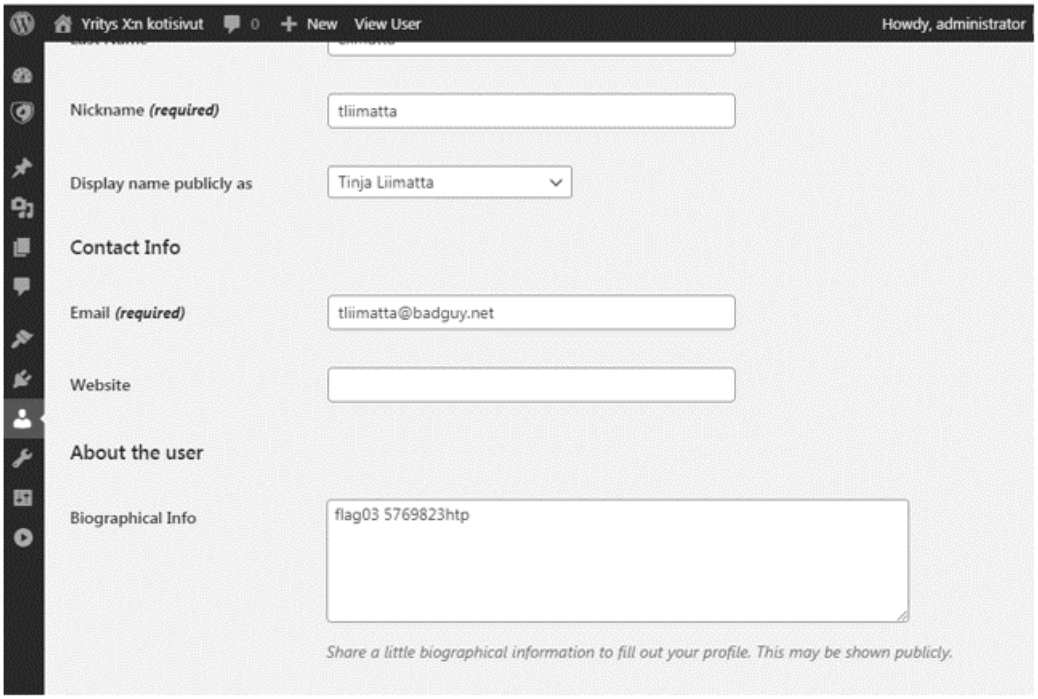
9. Flag2? (2p)

regedit --> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



10. Flag3? (1p)

    Wordpress ylimääräisen käyttäjän tliimat description



Liite 4. Tiedostopalvelin, konfiguraatiot

1. Samba konfiguraatio

```
root@filesrv:~# cat /etc/samba/smb.conf
[global]
        workgroup = yritysx
        realm = YRITYSX.NET
        netbios name = filesrv
        security = ADS
        dns forwarder = 192.168.0.10

idmap config * : backend = tdb
idmap config *:range = 50000-1000000

   template homedir = /home/%D/%U
   template shell = /bin/bash
   winbind use default domain = true
   winbind offline logon = false
   winbind nss info = template
   winbind enum users = yes
   winbind enum groups = yes

  vfs objects = acl_xattr
  map acl inherit = Yes
  store dos attributes = Yes
[JAKO]
        path = /srv/samba/JAKO/
        browseable = yes
        read only = no
        inherit acls = yes
        inherit permissions = yes
        create mask = 700
        directory mask = 700
        valid users = @"Domain Users"
        admin users = @"Domain Admins"
root@filesrv:~#
```

2. Kerberoskonfiguraatio

```
root@filesrv:~# cat /etc/krb5.conf
[libdefaults]
        default_realm = YRITYSX.NET
        default_tgs_enctypes = arcfour-hmac-md5 des-cbc-crc des-cbc-md5
        default_tkt_enctypes = arcfour-hmac-md5 des-cbc-crc des-cbc-md5
# The following krb5.conf variables are only for MIT Kerberos.
        krb4_config = /etc/krb.conf
        krb4_realms = /etc/krb.realms
        kdc_timesync = 1
        ccache_type = 4
```

```
        forwardable = true
        proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# Thie only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        v4_instance_resolve = false
        v4_name_convert = {
                host = {
                        rcmd = host
                        ftp = ftp
                }
                plain = {
                        something = something-else
                }
        }
        fcc-mit-ticketflags = true

[realms]
YRITYSX.NET = {
        kdc = win-serv-dc.YRITYSX.NET:88
        default_domain = YRITYSX.NET
    }
[domain_realm]
        yritysx.net = YRITYSX.NET
        .yritysx.net = YRITYSX.NET
        .mit.edu = ATHENA.MIT.EDU
        mit.edu = ATHENA.MIT.EDU
        .media.mit.edu = MEDIA-LAB.MIT.EDU
        media.mit.edu = MEDIA-LAB.MIT.EDU
        .csail.mit.edu = CSAIL.MIT.EDU
        csail.mit.edu = CSAIL.MIT.EDU
        .whoi.edu = ATHENA.MIT.EDU
        whoi.edu = ATHENA.MIT.EDU
        .stanford.edu = stanford.edu
        .slac.stanford.edu = SLAC.STANFORD.EDU
        .toronto.edu = UTORONTO.CA
```

```
        .utoronto.ca = UTORONTO.CA

[login]
        krb4_convert = true
        krb4_get_tickets = false
root@filesrv:~#
```

3. NSS konfiguraatio

```
root@filesrv:~# cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat winbind
group:          compat winbind
shadow:         compat winbind
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup: nis
root@filesrv:~#
```

4. Domain käyttäjien oikeuksien lisääminen tiedostojakoon

```
root@filesrv:~# setfacl -m group:"YRITYSX.NET\Domain Admins":rwx
/srv/samba/JAKO/
root@filesrv:~# setfacl -m group:"YRITYSX.NET\Domain Users":rwx
/srv/samba/JAKO/
root@filesrv:~# setfacl -R -m other::--- /srv/samba/JAKO
```

5. Domainkäyttäjien testaus

```
root@filesrv:~# getent passwd| grep -i yritysx
administrator:*:50000:50010::/home/YRITYSX/administrator:/bin/bash
guest:*:50001:50001:Guest:/home/YRITYSX/guest:/bin/bash
krbtgt:*:50002:50000:krbtgt:/home/YRITYSX/krbtgt:/bin/bash
ttestaaja:*:50003:50000:Teppo Testaaja:/home/YRITYSX/ttestaaja:/bin/bash
samba:*:50004:50000:SAMBA:/home/YRITYSX/samba:/bin/bash
mmallikas:*:50005:50000:Matti Mallikas:/home/YRITYSX/mmallikas:/bin/bash
tsaarinen:*:50006:50000:Timo Saarinen:/home/YRITYSX/tsaarinen:/bin/bash
santtila:*:50007:50000:Siiri Anttila:/home/YRITYSX/santtila:/bin/bash
tturmiola:*:50008:50000:Tiina Turmiola:/home/YRITYSX/tturmiola:/bin/bash
```

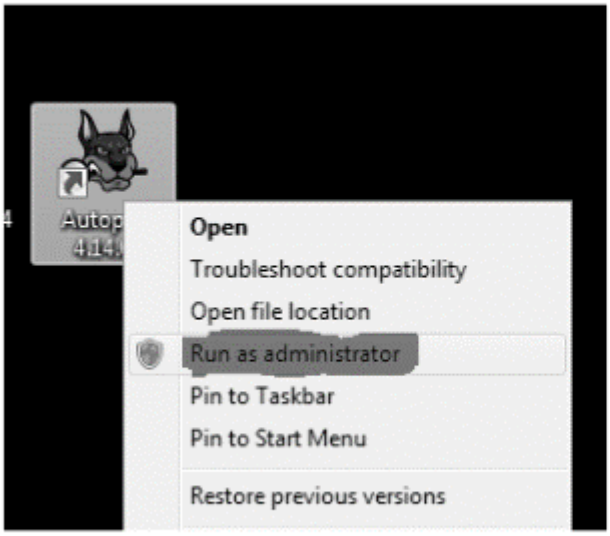
```
plaitela:*:50009:50000:Pekka Laitela:/home/YRITYSX/plaitela:/bin/bash
troland:*:50010:50000:Tommi Roland:/home/YRITYSX/troland:/bin/bash
sfender:*:50011:50000:Sami Fender:/home/YRITYSX/sfender:/bin/bash
ssmuolainen:*:50012:50000:Santeri Suomalai-
nen:/home/YRITYSX/ssmuolainen:/bin/bash
tturkulainen:*:50013:50000:Tanja Turkulai-
nen:/home/YRITYSX/tturkulainen:/bin/bash
elahtinen:*:50014:50000:Erkki Lahtinen:/home/YRITYSX/elahtinen:/bin/bash
pliimatta:*:50015:50000:Pinja Liimatta:/home/YRITYSX/pliimatta:/bin/bash
paikamies:*:50016:50000:Pekko Aikamies:/home/YRITYSX/paikamies:/bin/bash
root@filesrv:~#
```

Liite 5. Taitaja2020, Ohjelmien käyttöohjeet

Taitaja2020 Ohjelmistojen käyttöohjeet

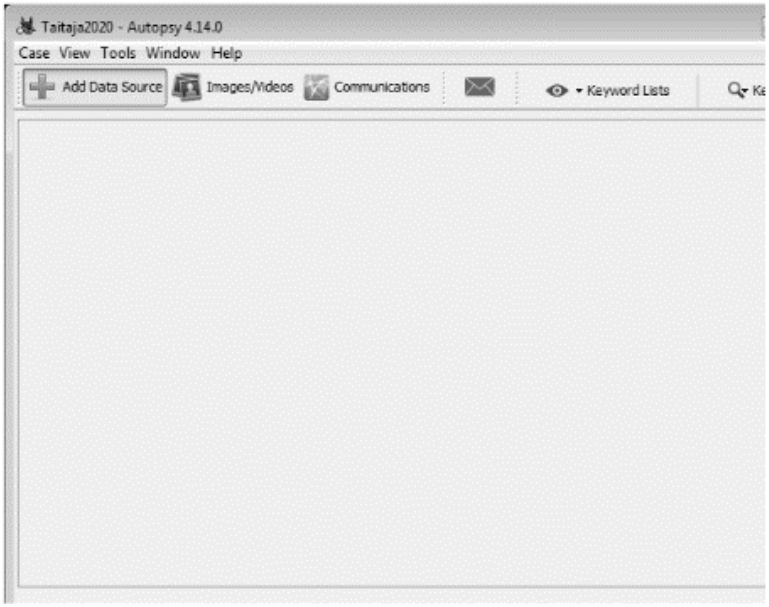
Autopsy

1. Käynnistä autopsy pääkäyttäjänä.

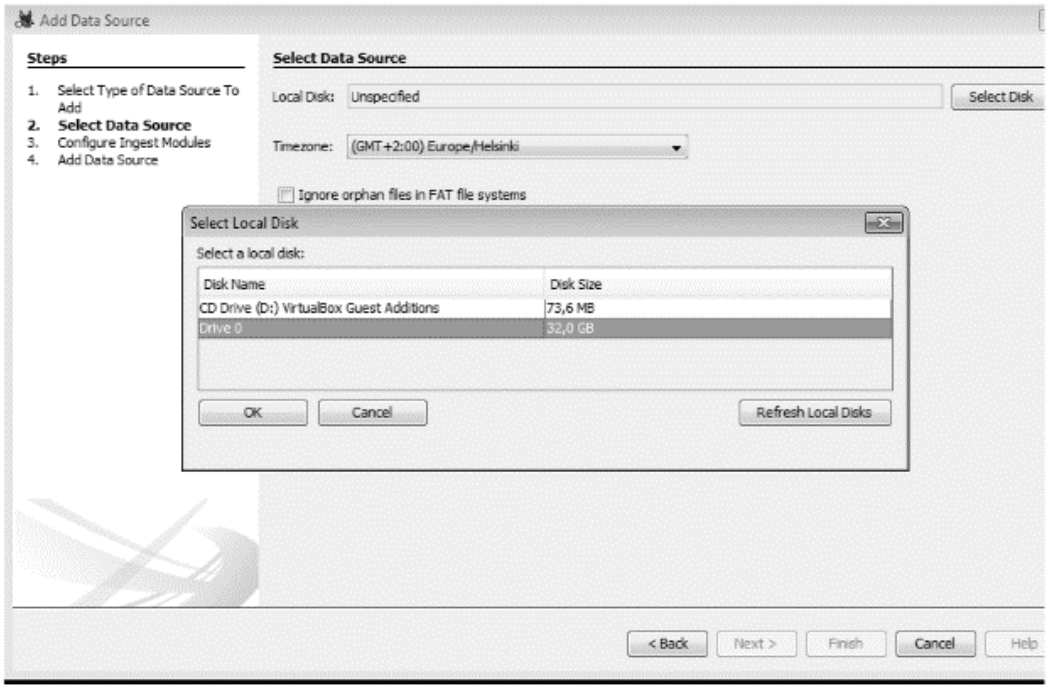


2. Avaa joko uusi tapaus tai avaa viimeisin.

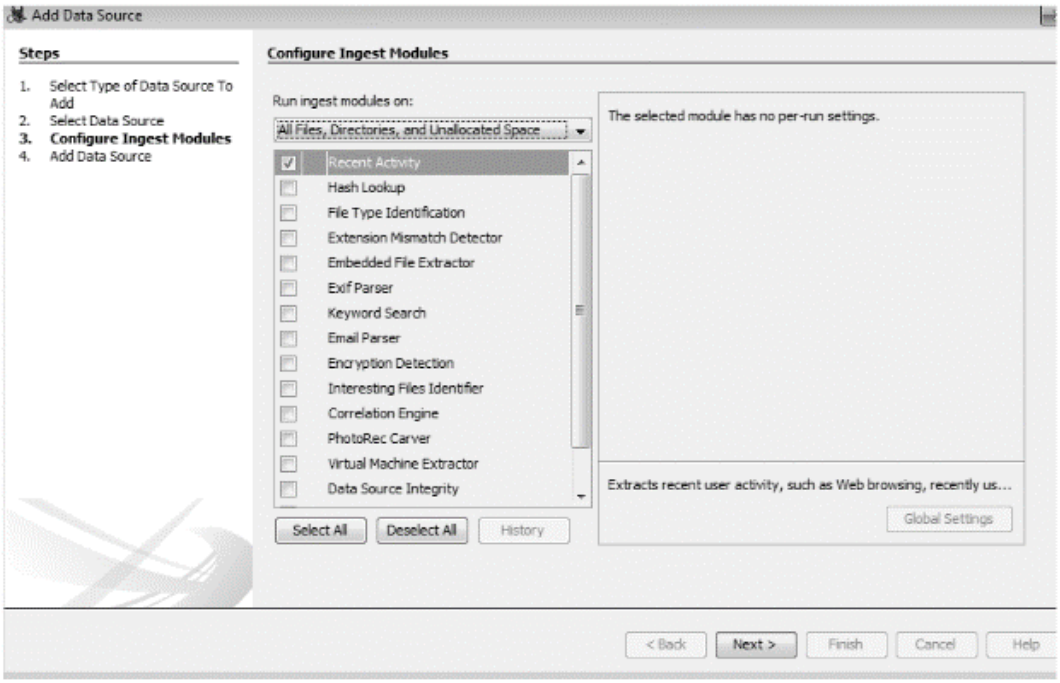
3. Lisää Datasource eli tietolähde, jota tutkitaan



4. Valitse Drive 0

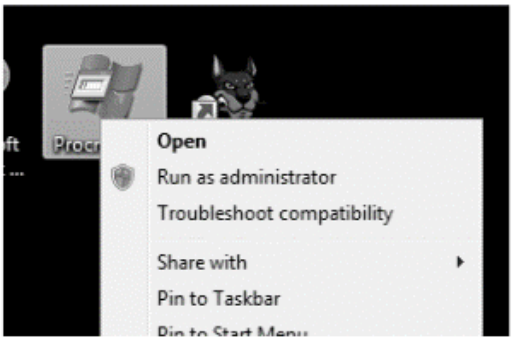


5. Suorita vain Recent Activity, se riittää tähän harjoitukseen.

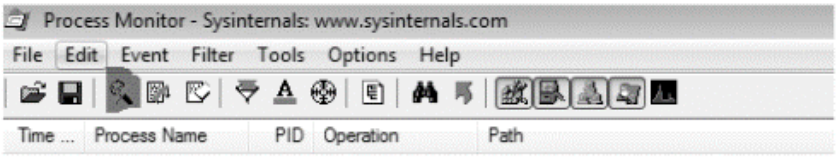


Procmon eli prosessimonitori

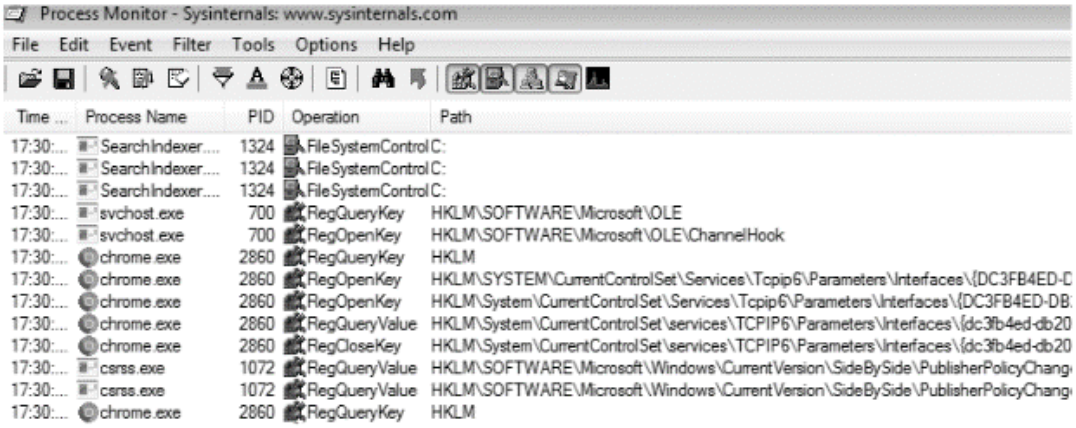
1. Aja pääkäyttäjänä



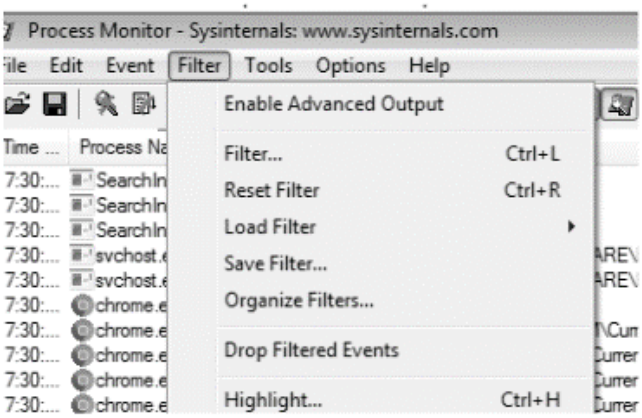
2. Ctrl + E tai kuvassa korostettu aloittaa capturen



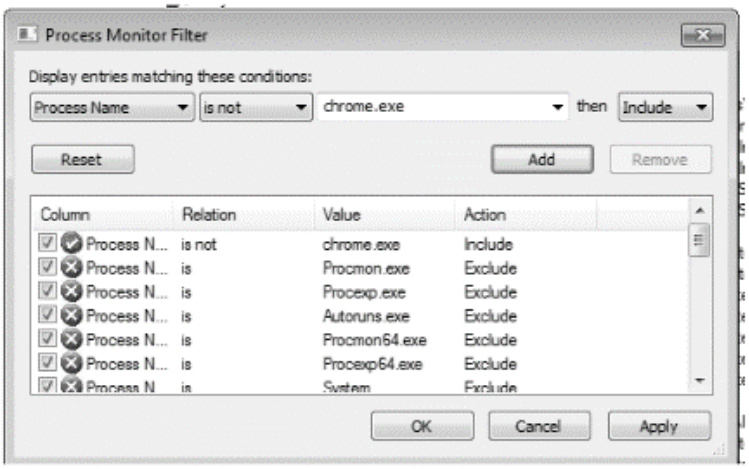
3. Process monitor listaa kaikkien prosessien toiminnot, Harjoituksessa riittää noin 5 minuutin tallennus, jonka jälkeen sen voi lopettaa ja alkaa tutkimaan prosesseja.



4. Prosesseja on paljon, joten kannattaa filteröidä varmat pois.

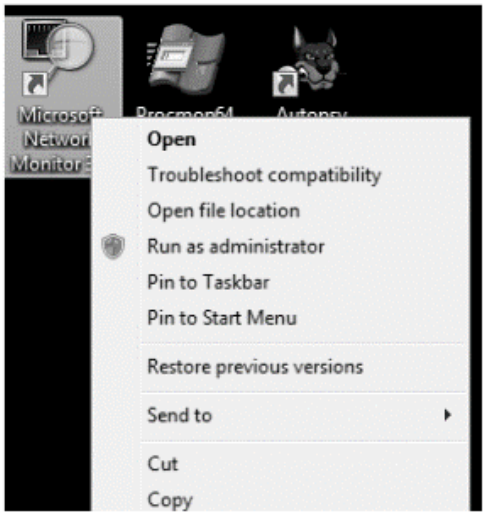


5. Filtereitä saa lisättyä painamalla add nappia,jonka jälkeen apply

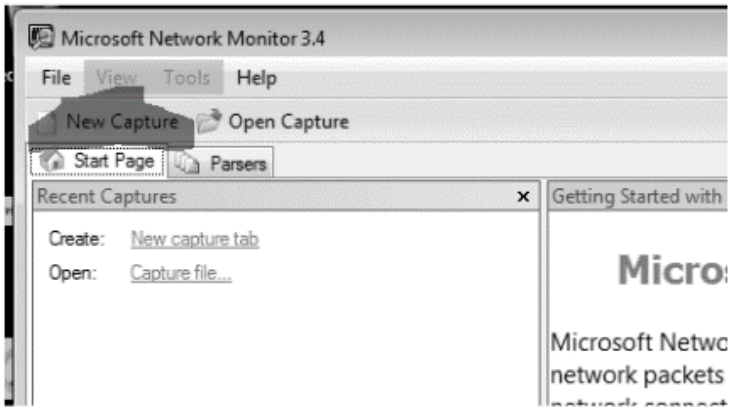


Netmon eli Network monitor

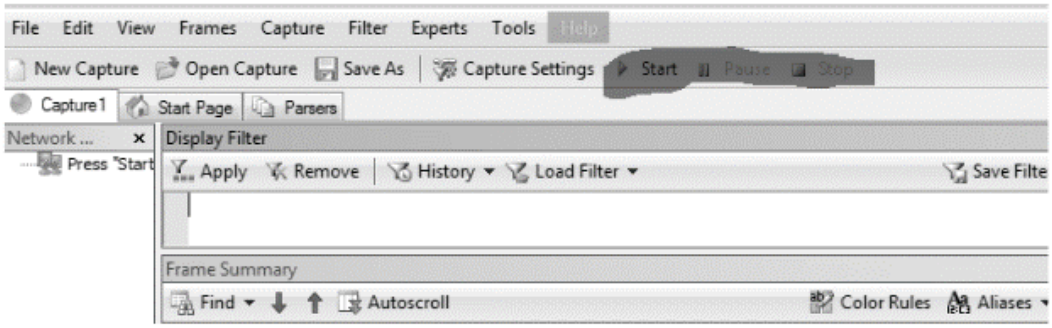
1. Suorita pääkäyttäjänä



2. Luo uusi tallennustieodsto eli capture



3. Aloita verkkoliikenteen tallennus, noin 5-10 minuuttia on riittävä tallennus pituus.



Liite 6. Taitaja2020, palautekysely

Palautekysely Taitaja2020 tietoturvahaasteesta

Palautekysely Taitaja2020-finaalin kilpailijoille tietoturvahaasteesta

*Pakollinen

1. Kilpailutunnus *

Oma vastauksesi

2. Kuinka vaikeaksi koit tehtävän yleisesti? (1=helppo, 2= helpohko, 3=sopiva, 4=vaikea, 5=liian vaikea) *

	1	2	3	4	5	
Helppo	○	○	○	○	○	Liian vaikea

3. Koitko tehtävän kiinnostavana tapana tutustua tietoturvapoikkeamiin? Mitä mieltä yleisesti tehtävästä? *

Oma vastauksesi

4. Koetko tehtävän parantaneen käsitystäsi kyseisistä tietoturvapoikkeamista? (C2 komentokanavat ja brute force hyökkäykset) Ymmärsitkö kyseisten tietoturvapoikkeamien periaatteet paremmin harjoituksen myötä? *

Oma vastauksesi

5. Kuinka vaikeaksi koit työkalujen käytöni? (1=helppo, 2= helpohko, 3=sopiva, 4=vaikea, 5=liian vaikea) *

	1	2	3	4	5	
Helppo	○	○	○	○	○	Liian vaikea

6. Olivatko harjoituksessa käytetyt työkalut sinulle tuttuja entuudestaan? *

- ○ Kyllä
- ○ Ei

7. Koetko saaneesi tarpeeksi koulutusta tietoturvan suhteen koulussa? *

- ○ Kyllä
- ○ En

8. Koitko harjoituksen teknisen toteutuksen vastaavan koulussa opetettuja teknisiä asioita? (Windows server ja Linux yms.) *

Oma vastauksesi

9. Pystytkö luomaan tapahtumista karkean aikajanan? (Mikä käynnisti tietoturvapoikkeaman? Mitä sitten tapahtui. jne.) *

Oma vastauksesi

10. Vapaa palaute

Oma vastauksesi

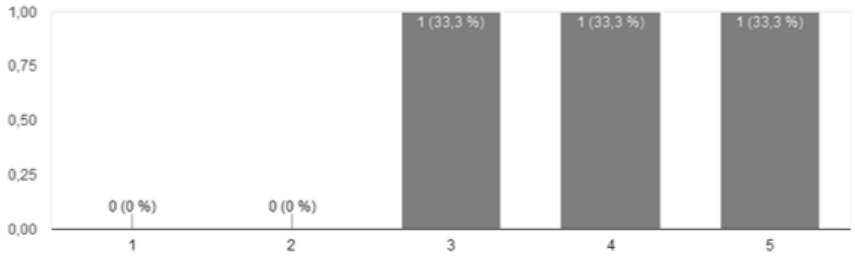
Lähetä

Liite 7. Taitaja2020, palautekyselyn tulokset

Palautekyselyn tuloksia

2. Kuinka vaikeaksi koit tehtävän yleisesti? (1=helppo, 2= helpohko, 3=sopiva, 4=vaikea, 5=liian vaikea)

3 vastausta



3. Koitko tehtävän kiinnostavana tapana tutustua tietoturvapoikkeamiin? Mitä mieltä yleisesti tehtävästä?

3 vastausta

- Kyllä, Tehtävässä oli ainakin haastetta mutta minulle ehkä vähän liiankin paljon.
- Tehtävässä käytiin hyviä (ilmaisita) IR -ohjelmistoja, joiden avulla tämän tyylisiä poikkeamia voidaan tutkia. Tehtävän tarjoama skenaario oli luotu hyvin sekä realistisen tuntuinen.
- todella kiinnostava

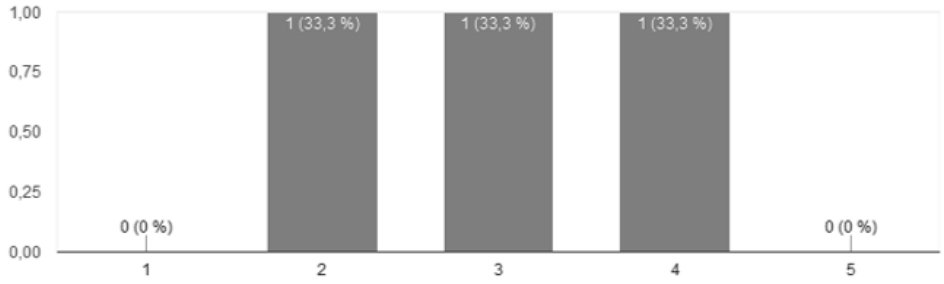
4. Koetko tehtävän parantaneen käsitystäsi kyseisistä tietoturvapoikkeamista? (C2-komentokanavat ja brute-force -hyökkäykset) Ymmärsitkö kyseisten tietoturvapoikkeamien periaatteet paremmin harjoituksen myötä?

3 vastausta

- jonkun verran
- Harjoituksen tietoturva poikkeamat eivät olleet minulle ennestään tuntemattomia, mutta sain paremman käsityksen mm. registryn käytöstä malwaren persistancessa.
- kyllä

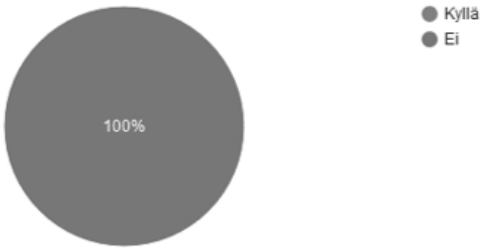
5. Kuinka vaikeaksi koit työkalujen käytöni? (1=helppo, 2= helpohko, 3=sopiva, 4=vaikea, 5=liian vaikea)

3 vastausta



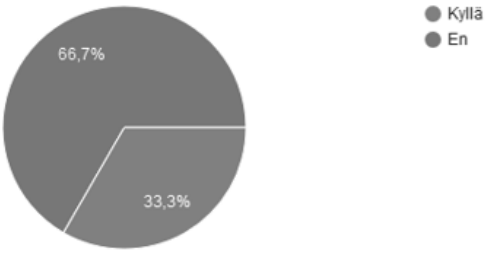
6. Olivatko harjoituksessa käytetyt työkalut sinulle tuttuja entuudestaan?

3 vastausta



7. Koetko saaneesi tarpeeksi koulutusta tietoturvan suhteen koulussa?

3 vastausta



8. Koitko harjoituksen teknisen toteutuksen vastaavan koulussa opetettuja teknisiä asioita? (Windows server ja Linux yms.)

3 vastausta

- Jonkun verran
- Kyllä, ad vaikutti toimivan ja FS oli integroitu toimimaan näpäkästi Linux -> Windows
- suurinpiirten

9. Pystytkö luomaan tapahtumista karkean aikajanan? (Mikä käynnisti tietoturvapoikkeaman? Mitä sitten tapahtui. jne.)

3 vastausta

- En valitettavasti pysty.
- Kyllä
- joo

10. Vapaa palaute

2 vastausta

- Tehtävässä oli haastetta ja oli toteutettu ammattimaisesti.
- Hyvää duunia Aku!