

Kyberharjoituksen suunnittelu

Kurssityö

Ville Pulkkinen
Joonas Mankinen
Mikael Romanov
Niko Tamminen
Niko Poutanen
Joni Korpihalkola

Harjoitustyö
Marraskuu 2017
Tekniikan ja liikenteen ala
Insinööri (AMK), tieto- ja viestintätekniikan tutkinto-ohjelma
Kyberturvallisuus

Sisältö

1	Johdanto	6
2	Organisaatio.....	6
2.1	Organisaatorakenne	7
2.2	Yhteistyökumppanit	7
2.3	Mahdollisia uhkatilanteita.....	7
2.4	Toimintamalli.....	8
3	Hissien tekniikka.....	9
4	Harjoituksen toiminta-ajatus ja käytettävä harjoitusmuoto	10
5	Harjoituksen tavoitteet.....	10
6	Rajaukset	11
7	Harjoituksen osallistujat ja toiminnallisuudet	11
7.1	Suunnitteluryhmän tehtävä	12
7.2	Suunnitteluryhmän kokoonpano	12
7.3	Harjoituksen ajankohta	13
8	Harjoituksen toteutus.....	13
8.1	Skenaario	13
8.2	Taustakertomus.....	13
8.3	Roolit	17
8.4	Pelitapahtumat	18
8.5	Aikataulutus.....	20
9	Yleiset vaatimukset harjoitusympäristölle.....	20
9.1	Harjoitusympäristön tulee olla eristetty ja hallittavissa	20
9.2	Ympäristön tulee olla etäkäytettävissä	20
9.3	Ulko-verkon palveluiden tulee olla saatavilla tarvittaessa.....	20

9.4	Virtualisointitekniikoiden käyttäminen	21
9.5	Teknisen ympäristön tulee olla modulaarinen.....	21
9.6	Julkisen palveluntarjoajan runkoverkko.....	21
9.7	Julkiset palvelut	21
9.8	Kattava tarjonta julkisia verkkosivustoja.....	21
10	Harjoituksen tekninen suunnittelu	22
10.1	Virtuaaliympäristö	22
10.2	Virtuaalikoneet	22
10.3	Virtuaaliverkko	23
10.4	IP-suunnittelu	23
10.5	Harjoitusympäristön topologia	24
10.6	DNS	25
10.7	NTP	26
10.8	HTTP.....	27
10.9	Hissien suunnittelu	27
10.10	Yrityksen päätoimipisteen suunnittelu	29
11	Harjoitusympäristön toteutus.....	30
11.1	Virtuaaliympäristö	30
11.2	Reititys.....	30
11.3	Verkon palvelut	31
11.3.1	DNS	31
11.3.2	NTP.....	32
11.3.3	HTTP.....	32
11.4	Yrityksen toimipiste.....	39
11.4.1	Tietoturva	39

12	Hyökkäysten tekninen toteutus	41
12.1	Verkkoskannaus.....	41
12.2	ARP-spoof	42
12.3	DoS.....	45
13	Harjoituksen säännöt.....	45
14	Harjoituksen arviointi	46
15	Pohdinta.....	46
16	Viitteet	47
17	Liitteet.....	47

Kuviot

Kuvio 1 Organisaatiorakenne	7
Kuvio 2 Toimintamalli.....	9
Kuvio 3 Tilanne-uutinen	14
Kuvio 4 Epäilyttävä venäläismies	15
Kuvio 5 IoT-uutinen	16
Kuvio 6 Hakkereita hissien lähellä.....	16
Kuvio 7	19
Kuvio 8 Etäyhteysportit	22
Kuvio 9 Virtuaalikoneet	23
Kuvio 10 Vynos reitittimet.....	23
Kuvio 11 IP-Suunnitelma	24
Kuvio 12 Ympäristön looginen topologia	25
Kuvio 13 DNS Verkkotunnukset	26
Kuvio 14 FINLAND-ISP looginen kuva.....	26
Kuvio 15 Hissien valvonta.....	28
Kuvio 16 Hissin scripti.....	28
Kuvio 17 Toimipisteen looginen topologia.....	29
Kuvio 18 Yrityksen LAN-verkot osoitteet	30
Kuvio 19 R1-Reitittimen OSPF	30
Kuvio 20 R1-reitittimen reittitaulu	31
Kuvio 21 Virtualhost konfigurointi	32
Kuvio 22 Virtualhost konfigurointi	33
Kuvio 23 Virtualhost konfigurointi	33
Kuvio 24 httpd lataa tiedostoja valitusta paikasta.....	33
Kuvio 25 Hostien määrittely.....	33
Kuvio 26 Twitter database.....	34
Kuvio 27 Iltajutku.fi database.....	34
Kuvio 28 osTicket database	34
Kuvio 29 GNU-socialin määrittely	35
Kuvio 30 GNU-socialin määrittely	36

Kuvio 31 GNU-social asennus.....	36
Kuvio 32 WordPressin määrittely.....	37
Kuvio 33 osTicketin määrittely	37
Kuvio 34 osTicketin määrittely	38
Kuvio 35 osTicketin määrittely	38
Kuvio 36 Palomuurisäännöt	40
Kuvio 37 Hyökkääjän reittitaulu	41
Kuvio 38 Netdiscover.....	41
Kuvio 39 Nmap kohteeseen	42
Kuvio 40 IP-Forwarding	42
Kuvio 41 Looginen kuva hyökkäyksen verkosta	43
Kuvio 42 ARP-spoof komento.....	43
Kuvio 43 TCP-paketit	44
Kuvio 44 TCP Selkokielineen data	45

Taulukot

No table of figures entries found.

1 Johdanto

Ryhmän tehtävän oli suunnitella ja toteuttaa kyberharjoitus, harjoituksen ympäristö sekä harjoituksen kulku kuvitteelliselle yritykselle, osana kyberharjoituksen suunnittelu- ja toteutus kurssia. Marraskuussa 2017 järjestettävään lyhyeen harjoitukseen valitaan luokaltamme yhden ryhmän suunnitelma, jonka pohjalta harjoitus toteutetaan. Harjoituksen kesto on kolme tuntia.

Jokainen ryhmä sai valita yritykselle jonkin liiketoiminnan alueen, jonka mukaan harjoitusta lähdettiin toteuttamaan. Ryhmämme valitsi kuvitteelliseksi yritykseksi hissejä valmistajan yrityksen, joka käyttää IoT-teknologiaa tuotteissaan.

”Kurssin tavoite ja sisältö: Opiskelija hallitsee keskeisimmät kyberharjoituksen suunnitteluun ja valmisteluun liittyvät osa-alueet: käsitteet, käytetyt toteutustavat ja yleisen harjoitukseen liittyvät rakenteelliset asiat. Lisäksi opiskelija hallitsee harjoituksen suunnittelun periaatteet ja osaa suunnitella yrityksen henkilöstölle sopivan harjoitusmallin vaatimusmäärittelyjen pohjalta huomioiden rajoitteet.

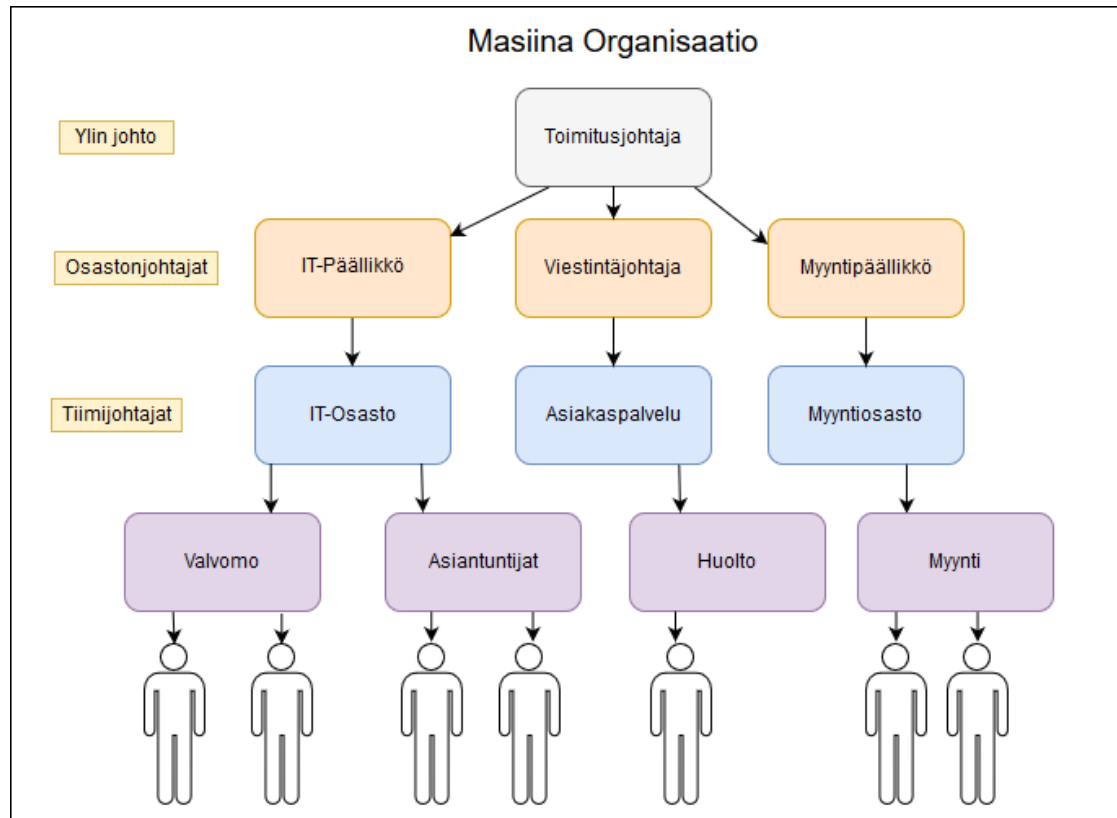
Opintojakso sisältää yleisesti kyberharjoituksen käsitteet ja vaatimukset. Opintojaksolla tutustutaan harjoituksen järjestämiseen ja harjoituksessa toimimiseen eri roolien kautta. Kurssilla suunnitellaan ”Kyberharjoituksen toteutus” –kurssin harjoituksen rakenne ja toimijoiden roolit.” (Opintojakson suunnitelma, kyberharjoituksen suunnittelu ja valmistelu. Saharinen K, Rintanen T)

2 Organisaatio

Organisaatio, jolle harjoitus suunniteltiin, oli hissejä valmistaja yritys ”Masiina”. Yritys toimii neljässä eri maassa, Suomessa, Venäjällä, Ruotsissa sekä Puolassa. Yrityksen päätoimipiste sijaitsee Jyväskylässä. Kaikissa muissa maissa on pienet sivutoimipisteet, jotka ovat vain satunnaisesti miehitettyjä. Jokaisessa maassa on yrityksen oma huoltohenkilöstö, jotka ovat tarvittaessa saatavilla.

2.1 Organisaatorakenne

Yrityksellä on myynti, IT sekä viestintäosasto. Jokaisella osastolla on osastonjohtaja sekä jokaisella osaston tiimillä on tiiminjohtaja, joka on tiimin lähin esimies. (Kuvio 1 Organisaatorakenne)



Kuvio 1 Organisaatorakenne

2.2 Yhteistyökumppanit

Yrityksellä on useita yhteistyökumppaneita ja alihankkijoita. Hissien verkkoyhteydet tarjoaa jokaisen maan paikallinen operaattori.

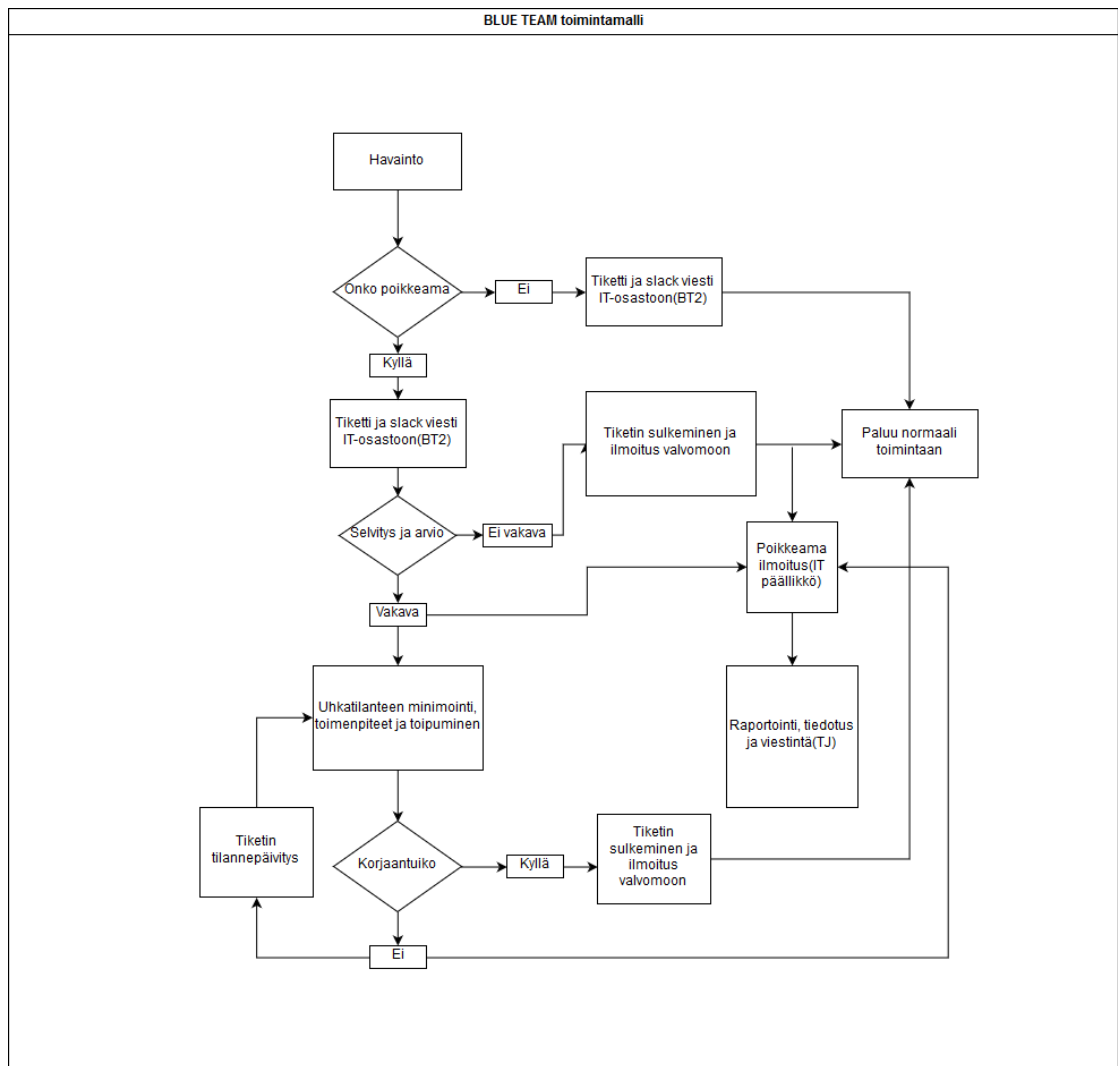
2.3 Mahdollisia uhkatilanteita

Mahdollisia uhkatilanteita yritykselle voivat olla fyysiset uhat ja kyberuhat. Yrityksen on varmistettava liiketoiminnan jatkuvuus jokaisella eri osa-alueella. Kyberuhat ja hyökkäykset voidaan kohdistaa suoraan yrityksen toimipisteisiin tai IoT-hisseihin, jotka ovat myös saatavilla verkossa. Mahdollisia uhkatilanteita yrityksen tietoverkossa voisivat olla:

- Palvelunestohyökkäykset
- Hissien anturitiedon väärentäminen
- Mahdollinen hissien manipulointi/mielivaltainen hallinta
- Haittaohjelmien levitys hissien verkossa
- Phishing huijaukset
- Ransomware ohjelmat

2.4 Toimintamalli

Yrityksen liiketoiminta perustuu hissien jatkuvaan toimintaan, sekä verkkosivujen saatavuuteen. Masiinan hissien antureiden dataa valvotaan valvomossa. Ongelmatilanteen sattuessa valvomosta tehdään tiketti, joka siirretään seuraavalle asiantuntijatasolle, joka on yrityksessä IT-osasto. IT-osasto siirtää ongelman tarvittaessa kenttähuoltoon, joka hoitaa laitteiden ja hissien fyysisen ylläpidon ja tarkistuksen. Jokaisesta poikkeamasta tehdään tiketti tikettienhallintajärjestelmään ja lisäksi laitetaan viesti vastaanottavalle tiimille poikkeamasta. Yrityksen toimintamalli on kuvattuna kaaviossa.



Kuvio 2 Toimintamalli

3 Hissien tekniikka

Hissien verkkoyhteys saadaan joltain paikalliselta operaattorilta xdsl, fttx ratkaisulla. Hisseissä olevat "IoT" laitteet ovat arm-piirin päälle rakennettuja laitteita. Hississä on useita eri antureita jotka mittaavat esimerkiksi lämpötilaa, hississä olevaa painoa ja kerrosta. Hissin voi myös pysäyttää etänä tiettyyn kerrokseen hätätapauksessa. Hissien kaikki data tallennetaan Masiinan konesaliin, jossa sijaitsee myös yrityksen pilvipalvelut.

IoT-hissien toimintaa simuloidaan harjoituksessa Python-kielellä kirjoitetulla skriptillä, joka lähettää selkoteksinä hissien tilannepäivityksiä valvomoon. Yhteyden muodostamiseen käytetään TCP-socketteja. Tilannepäivityksissä on hissien nykyinen ker-

ros, hissin lämpötila ja sen hetkisen lastin paino. Jos valvomon palvelimelle tulee ylimääräistä dataa, joka ei täsmää hissien lähettämän tekstin formaattiin tai lämpötila- tai painoraja ylittyy, tapahtuma tallennetaan lokitiedostoon.

4 Harjoituksen toiminta-ajatus ja käytettävä harjoitusmuoto

Harjoituksessa on punainen, sininen ja valkoinen tiimi. Punainen tiimi suorittaa erilaisia teknisiä hyökkäyksiä organisaation verkkoon ja laitteisiin. Sinisen tiimin tehtävänä on havaita, kirjata ja mahdollisesti torjua punaisen tiimin hyökkäykset. Valkoinen tiimi ohjaa harjoituksen kulkua, jotta harjoituksen tavoitteet saavutettaisiin. Tämä tapahtuu syötteillä, esimerkiksi lähettämällä sähköposteja tai keksimällä uutisartikkeleita, jotka vaikuttavat pelin tilaan. Valkoinen tiimi myös tekee havaintoja ja arvioi osallistuvien tiimien onnistumista tehtyjen havaintojen perusteella.

Harjoituksen toiminta-ajatuksena on ennestään päätettyjen kyberuhkin demoaminen ja henkilöstön valmiuden ja toiminnan testaaminen. Harjoitus suoritetaan suunnitteluryhmän määriteltujen pelitapahtumien pohjalta ja osallistuvia joukkueita arvioidaan heidän tekemien peliratkaisujen mukaan. Tarkoituksena on, että henkilöstö oppisi mahdollisista harjoituksen aikana suoritetuista virheistä tai nykyisen tietoturvajärjestelmän puutteista, ja osaisi siten korjata ne normaaliin työarkeen palatessa.

5 Harjoituksen tavoitteet

Tavoitteena vahvistaa yrityksen tietoturvaa ja parantaa toimintamallia kyberhyökkäyksen sattuessa. Oppia kuinka tunnistaa ja ehkäistä hyökkäyksiä, miten toivutaan hyökkäyksistä ja kuinka yrityksen toiminnan jatkuminen taataan hyökkäyksen alla esim. kuinka kauan serverit ovat alhaalla DDoSin takia. Tärkeitä tavoitteita on tilanteen laskelmointi ja isomman kuvan luominen tilanteesta, haittakohtien tarkastelu ja mahdollisten puutteiden paikkaaminen.

Tavoitteena on myös lisätä organisaation valmiutta ja kykyä kyberuhkan sattuessa. Selvennetään toimintamallit ongelmatilanteissa ja kehitetään toimintatapoja, jaetaan tärkeitä työtehtäviä ja -rooleja ja varmistutaan siitä, että oikeat henkilöt hoitavat yrityksen turvallisuutta ja että vain tarvittavat henkilöt ovat mahdollisesta ongelmati-

lanteesta tietoisia, jotta ei aiheuteta ongelmia yrityksen liiketoiminnalle. Harjoituksen jälkeen käydään läpi ongelmakohdat ja kehityksen kohteet, joita kehitetään koulutuksilla ja harjoituksilla. Annetaan palaute yrityksen tietoturvallisuudesta ja analysoidaan mitä on hyvää ja mitä puutteellista.

6 Rajaukset

Yksi organisaatio, ja keskitytään vain hisseistä löytyviin IoT-laitteisiin ja dataan, jota ko. laitteet lähettävät, varastoi tai välittää, sekä muihin yrityksen omiin palveluihin (esim. yrityksen kotisivut). Harjoituksen kesto on maksimissaan 3 tuntia.

Harjoituksen teknisen puolen rajaukset ympäristön käyttöön ja harjoituksessa toimimiseen löytyy jokaisen tiimin erillisestä ohjeesta, sekä kohdasta harjoituksen säännöt.

7 Harjoituksen osallistujat ja toiminnallisuudet

Harjoitukseen osallistuu yrityksen johtaja, valvomo, IT-tuki sekä huolto-osasto. IT-tuessa on kaksi henkilöä ja valvomossa kaksi henkilöä. Valvomo valvoo hissien lähettämää dataa, datan poikkeamien lokeja, sekä verkkosivun saatavuutta ja käyttää tietokenttärjestelmää ilmoittaakseen poikkeamat ja mahdolliset hyökkäysyritykset IT-tuelle. IT-osasto hoitaa ongelmatilanteet liittyen yrityksen verkon toimintaan, hissien toimintaan ja kyberhyökkäyksen sattuessa yrittää ratkaista hyökkäyksien aiheuttamat ongelmat. IT-osasto pitää huolen palveluiden saatavuudesta ja toiminnallisuudesta.

Punaisessa tiimissä on neljä henkilöä, jotka käyttävät kahta hyökkääjäkonetta eri sijainneissa. Punainen tiimi suorittaa ennalta määritettyjä hyökkäyksiä puolustavaa organisaatiota kohtaan. Tiimiä johtaa yksi henkilö, joka valvoo punaisen tiimin toimintaa, kirjoittaa ”twitteriin” hakkeriryhmän sosiaalisen median ilmoituksia, joita suunnitteluryhmä on tehnyt valmiiksi ja tarvittaessa kommunikoi valkoisen tiimin kanssa.

Valkoinen tiimi koostuu kuudesta henkilöstä, jotka ovat samoja kuin harjoituksen suunnittelijat. Valkoisen tiimin tehtävänä on tarjota harjoitukseen toimiva ympäristö,

tarjota siniselle ja punaiselle tiimille valmiita uutisia ja tviittejä, tarjota punaiselle tiimille pelisyötteet ja niihin vaadittavat komennot sekä varmistaa, että harjoitus etenee ja harjoituksen tavoitteet saataisiin suoritettua. Valkoinen tiimi valvoo ja havainnoi harjoituksen tapahtumia, sekä arvioi osallistuvien tiimien suorituksia.

7.1 Suunnitteluryhmän tehtävä

Suunnitteluryhmän tehtävänä on suunnitella yritykselle sopiva kyberharjoitus, joka sisältää yrityksen todellisia kyberuhkia ja määrittää harjoitukselle tavoitteet, jotka harjoituksen aikana on saavutettava. Suunnitteluryhmä suunnittelee ja toteuttaa harjoituksen teknisen ympäristön vastaamaan yrityksen todellista ympäristöä. Suunnitteluryhmä suunnittelee koko harjoituksen oletetun kulun ja valvoo, että harjoitus etenee toivotusti. Tehtävänä on myös keksiä harjoitukseen syötteitä ja komentoja, esimerkiksi antamalla punaiselle tiimille hyökkäyskohde, jolla testataan sinisen tiimin havaitsemiskykyä ja puolustusvalmiutta. Syötteiden tulisi olla realistisia ja niissä tulisi ottaa huomioon sinisen tiimin koulutustaso. Tällöin sininen tiimi saa uskottavan kuvan tilanteesta, ja myös oppii miten harjoituksen skenaariota voisi soveltaa työelämän tilanteisiin.

Suunnittelussa pitää ottaa huomioon, miten yrityksen henkilöstö jaetaan eri joukkueisiin, miten harjoitusympäristö rakennetaan ja mitä kalustoa harjoituksen toteuttamiseen pitäisi saada. Suunnittelijoiden pitää myös informoida yrityksen johtoa siitä, miten harjoitus saattaa vaikuttaa yrityksen toimintaan. Jos esimerkiksi käytetään yrityksen yksityisiä verkkoja, harjoituksen käyttämä verkko ja yrityksen käytössä oleva verkko tulisi erottaa toisistaan.

7.2 Suunnitteluryhmän kokoonpano

Suunnitteluryhmänä toimi kurssin ryhmä kaksi, jonka kokoonpano on muodostettu kuudesta kurssin opiskelijasta.

Suunnitteluryhmä:

- Ville Pulkkinen
- Joonas Mankinen
- Mikael Romanov
- Niko Tamminen

- Niko Poutanen
- Joni Korpihalkola

7.3 Harjoituksen ajankohta

Harjoitus järjestetään vuoden 2017 syksyllä.

8 Harjoituksen toteutus

Harjoitus toteutetaan teknistoiminnallisena harjoituksena sille toteutetussa ympäristössä. Harjoitusympäristö on toteutettu kurssin vaatimusten mukaisesti sisältäen oikean internetin palveluita ja toiminnallisuuksia.

8.1 Skenaario

Kilpailevan hissiyrityksen Moottorin liiketoiminta lähenee loppuaan. Viimeisenä oljenkortena Moottori päättää ryhtyä kehittämään älyhissejä, joita Masiina ja toinen hissiyritys Otus ovat tuoneet markkinoille. Moottori päättää palkata hakkeriryhmän kaappaamaan Masiinan hissien lähettämää dataa, jotta he pystyvät kehittämään omia hissejään markkinoilla olevien vertaiseksi. Hakkeriryhmä hyväksyy toimeksianton ja aloittaa hyökkäyskampanjan Masiinaa vastaan.

8.2 Taustakertomus

Kilpaileva hissiyritys Moottori on vuodesta 2010 yrittänyt päästä hissimarkkinoille omilla edullisimmilla hisseillään. Moottori ei ole onnistunut tavoitteessaan ja yrityksen elinkaari on lähenemässä loppuaan, jos he eivät pysty kehittämään hisseistään parempia. Moottori on yrittänyt tehdä omista hisseistään yhtä hyviä kuin Masiinan hissit mutta he eivät ole siinä onnistuneet, koska Masiinan suurin markkinaetu on hissianturit, jonka lähettämä data on salaista. Lisäksi Moottorin ja Masiinan toimitusjohtajilla on henkilökohtaista riitaa, jonka alkuperästä ei ole varmaa tietoa.(Kuvio 3 Tilanne-uutinen)

Porvoon murhaepäily on tuomarille ennestään tuttu mies - näin käsittely nyt etenee - Kotimaan uutiset - 10:40

Moottorin toimitusjohtaja Pepe Burgeri sanaharkassa Masiinan kanssa lehdistötilaisuudessa - "Saisivat painua v*ttuun" - Kotimaan uutiset - 10:33

Lewis Hamilton lyttää uudet F1-säännöt - "Se on syvältä" - Formulat - 10:30

HS: Sofi Oksanen vaatii ehdittelijoiden nimiä julkii - "Ei ole reilua, että yhden porsastelun vuoksi koko tiimi kärsii" - Viihdeuutiset - 10:28

Pohjois-Korea haukkui Trumpin: Ansaitsisi kuolemantuomion - Ulkomaan uutiset - 10:13

STT: Poliisi vaatii Porvoon puukottajan vangitsemista - oikeudenkäynti on huomenna - Kotimaan uutiset - 10:12

Kiinalainen maanviljelijä rakensi talon 30 000 maissintähkistä - tätä se näyttää - Asumisartikkelit -



Virkarikoksesta syytetty valtakunnansyyttäjä Matti Nissinen murtui Korkeimman oikeuden edessä, kirjoittaa Iltalehden toimittaja Marko-Oskari Lehtonen. [Lue lisää...](#)

Koulutusta veljensä yhtiöltä hankkinut valtakunnansyyttäjä Nissinen: "En tullut ollenkaan ajatelleeksi asiaa"

IoT laitteiden ongelmat jatkuvat - "Kiinan tuotteisiin ei voi luottaa"



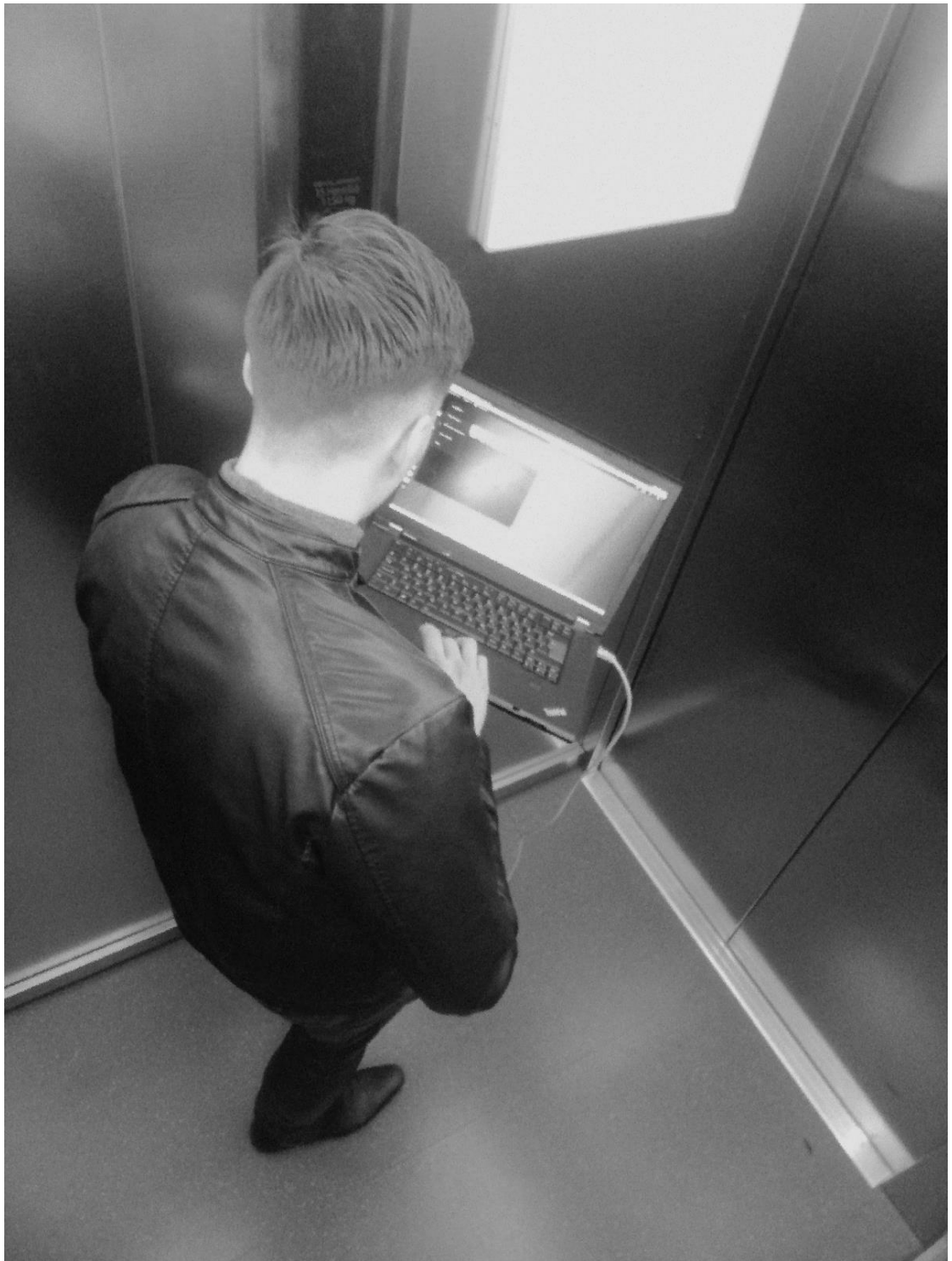
Masiinan toimitusjohtaja Sami Jaffa lyttää huhut! - "Ketään ei olla vakoiltu"



Moottorin toimitusjohtaja Pepe Burgeri sanaharkassa Masiinan kanssa lehdistötilaisuudessa - "Saisivat painua v*ttuun"

Kuvio 3 Tilanne-uutinen

Samaan aikaan Suomessa Otuksen, toisen hissiyrityksen, hissejä on mystisesti lakanut toimimasta. Valvontakamerat ovat huomanneet epäilyttävän venäläistaustaisen miehen liikkuvan hissien lähellä ennen tapahtumaa. (Kuvio 4)



Kuvio 4 Epäilyttävä venäläismies

Vartiomiehet ovat myös napanneet kiinni epäilyttävän miehen hissien lähellä, jonka he heittivät pois rakennuksesta. Epäillään, että nämä ovat hakkeriryhmän yrityksiä tehdä jotain hissien IoT – laitteisiin. (Kuvio 6)

TUOREIMMAT

KOTIMAA

Uusi tieto poliisilta: Porvoon murhaepäilty sieppasi lapsensa väkisin - "Ei minkäänlaista yhteisymmärrystä" 15:53

Tajuton mies löytyi suojatieltä Mannerheimintieltä Helsingissä - poliisi kaipaa silminnäkijähavaintoja 15:39

IL-TV-live: Orpo lyttysi opposition varjodutet: "Aikamoisia toiveiden tynnyreitä" 15:14

Poliisi: Oppilas uhkaili opettajaa teräseella Porissa 15:02

Rauman satamassa kuollut oli ulkomaalaisen laivan työntekijä - jäi kannella puristuksiin ja kuoli heti 14:40

IoT-Laitteista löynyt haavoittuvuuksia



JUURI NYT! Vakavia ongelmia Internet of things laitteissa! Lue lisää...

Kiinalainen insinööri Hao Dak Zin Zun Caiber kertoi että IoT-laitteiden tiedonsiirrossa on vakavia tietoturvaongelmia

LÄHETÄ UUTISVIHJE

LUETUIMMAT

TUOREIMMAT

Kaikki Uutiset Urheilu Viihde Muut

1. Cheek lopettaa uransa
2. Hyvästi 2000 euron ajokortti! Uusi laki toisi rajun hinnanpudotuksen
3. Suomalainen maalikuningas koki yllätyksen lihatiskillä Hongkongissa: "Tyttöystävä ei ole syönyt sen jälkeen lihaa"
4. Tällainen on Porvoon puukotuksesta epäilty isä: some täynnä kuvia autosta ja vähäpukaisista naisista
5. Tajuton mies löytyi suojatieltä Mannerheimintieltä Helsingissä - poliisi kaipaa silminnäkijähavaintoja

Kuvio 5 IoT-utinen

koskaan aiemmin 14.11. 14:37

TERVEYS

Annatto sinäkin tasoluista? Nuuskaaminen heikentää urheilusuoritusta 12:53

Univaje väsyttää myös aivosoluja 09:24

Roosa nauha -suurapuraha Ouluun - tutkijat jäljittävät perinnöllistä rintasyöpää 08:11

Epäiletkö nuoren sairastuneen syömishäiriöön? Toimi viisaasti 07:10

PERHE

Vahvista lapsen kehittyviä selviytymiskykyjä - sanoita tunteita ja keskity kuuntelemaan 07:14

Aidin vastaus pojan kysymykseen raskausarvista inspiroi ja voimaantuu 14.11. 19:45

Taaperokilareitit tulossa? Näin estät tilanteen kärjistymisen kiireessä 14.11. 10:04

"Isät eivät tke, isät eivät siivoa, isä ei uskalla jättää yksin vauvan kanssa..." Nyt puhuvat isät ja vastaavat välttelevin lausein 12.11. 09:02

RAKKAUS JA SEKSI

Ei tänään(kään) kulta - 10 asiaa, jotka saattavat tappaa seksihalut 11.11. 20:00

Onko sinut jätetty parisuhteesta? Kerro meille tarinasi 11.11. 09:24

Yli puolet naisista jää yhdynnässä ilman orgasmia - 6 mahdollista syytä, miksi nainen ei tule 10.11. 19:56

"Hän ei pettänyt fyysisesti, mutta tunnen oloni petettyksi" - näin päälette sopuun pornosta 09.11. 20:02

Technoroloksen tiloissa havaittu epäilyttävää toimintaa Otuksen hissien luona, Otuksen toimitusjohtaja kommentoi: "Taitavat olla tosissaan."



Hissivalmistaja Otus on havainnut myös aktiivisia tiedonkalastelu yrityksiä uuden sukupolven hissien verkossa. Lue lisää...

Nyt puhuu hissiahkerien kiinniottaja Niko "Vartiomies" Tamminen: "Tuli jonossa, lähti pinossa."



"Sää tulla koittamaan uudestaan" lisää Niko Tamminen. Lue lisää...

Ruoveden koripalloilijoiden päivän aloitusviisikko - Ville Pulkkinen asema joukkueessa on horjumaton



aamuruuhkassa - tynnyröintynyt vieruskaveri ei tunnistanut, reaktiosta tuli nettihitti 15.11.2017 09:52

2. Suomen hiihtolegendan hurja tulos Cooperin testissä vetää Iivo Niskosen ja Matti Heikkisen nöyräksi 14.11.2017 07:57

3. Patrik Laineen komea pistepurkki sai jatkoa - ikävä tilastovirhe saatiin kuntoon ottelun jälkeen 15.11.2017 06:41

ILTALEHTI.FI

1. Asiantuntijoiden karu arvio pelastaa: Näin Suomi on murskannut koulujärjestelmänsä

2. Kymmenet ihmiset kerääntyivät tragedian tapahtumapaikalle illan tullen - leikkikentän edessä valtava kynttilämeri

3. Musiikkitapahtumassa heitettiin yleisön sekaan ulostetta - järjestäjä yllättyi: "Lähti käistää"

4. Teollisuusliiton ponnalle yli 5 000 euron palkankorotus "Onhan se nyt tuntuva korotus, ei sitä kukaan voi kiistää"

5. MTV: Salatut elämät -sarjan rakastettu hahmo poistuu ohjelmasta yhdeksän vuoden jälkeen - varo juonipaljastuksia!

IL TV

Päivän katsotuimmat

1. Luonto näytti voimansa: salama iski matkustajalentokoneeseen 15.11.2017 06:29

2. Iso-Arskä jyrähti ilmastomuutoksesta:

Kuvio 6 Hakkereita hissien lähellä

Taustakertomukseen on otettu inspiraatiota oikean maailman tapahtumista, jossa Internet of Things laitteiden turvallisuudesta on herännyt suuria kysymyksiä.

Esimerkiksi ensimmäisessä viitteessä olevassa linkissä puhutaan siitä, kuinka vain harva valmistaja keskittyy IoT-laitteissa yksityisyyden suojaamiseen ja laitteiden turvallisuuteen. The Hacker News – uutissivusto on myös selvittänyt, että miljoonat IoT-laitteet käyttävät samoja kovakoodattuja SSH avaimia. (Viite 1)

IoT-laitteita on myös käytetty laajoihin DDoS hyökkäyksiin. Mirai-bottiverkko, joka käyttää haittaohjelmaa saadakseen Linux-pohjaisia käyttöjärjestelmiä haltuunsa, on suorittanut jopa 1 Tbps volyymin hyökkäyksiä verkkoihin. IoT-laitteet on helppo saada osaksi bottiverkkoa, koska niissä käytetään usein oletustunnuksia, kuten "admin/admin". (Viite 2)

Tänä vuonna on myös ilmestynyt BrickerBot-haittaohjelma, joka yrittää tuhota koko laitteen toiminnan. BrickerBot hyödyntää samaa heikkoutta IoT-laitteissa kuin Mirai, eli se kokeilee kirjautua sisään oletustunnuksilla. (Viite 3)

8.3 Roolit

Masiinan henkilöstö jaetaan kahteen siniseen tiimiin. Ensimmäisessä sinisessä tiimissä on yrityksen johtaja ja valvomon päivystäjät. Ensimmäisen tiimin tehtävänä on valvoa palvelimelle saapuvaa hissidataa, ja ilmoittaa vikatilanteista eteenpäin tiketti-järjestelmän avulla toiseen siniseen joukkueeseen. Toinen sininen joukkue koostuu yrityksen IT-osastosta, ja heidän tehtävänä on hallita sisäverkkoa, ylläpitää palvelimia ja luoda tilanteen mukaan uusia sääntöjä yrityksen PFSense – palomuriin.

Punaisen tiimin jäsenet värvätään yrityksen ulkopuolelta, ja heidät jaetaan myös kahteen joukkueeseen. Tiimi koostuu yhdestä tiimin johtajasta ja hänen alaisistaan. Johtajan tehtävänä on lukea punaiselle tiimille annetut toimintaohjeet ja valvoa, että hänen alaiset suorittavat komennot ohjeiden mukaisesti.

Valkoisesta tiimistä valitaan kaksi henkilöä avustamaan punaista ja sinistä tiimiä, jotta harjoitus kulkisi sujuvasti. Muut valkoisen tiimin jäsenet ovat pelinvalvoja, sekä he esittävät myös Masiinan huoltomiehiä, jotka sulkevat hissiskriptit, jos niistä ei

saavu dataa perille valvomoon. Valkoinen tiimi vastaa myös uutisten kirjoittamisesta. Valkoisesta tiimistä yksi vastaa koko harjoituksen kulusta. Valkoinen tiimi arvioi osallistuvien tiimien onnistumista pelitapahtumien ja niihin reagoimisen perusteella.

Harjoituksessa on myös ns. "violetti tiimi", joka seuraa harjoituksen kulkua sivusta ja koittaa poimia harjoituksesta oppimismateriaalia tulevia harjoituksia varten.

8.4 Pelitapahtumat

Hakkeriryhmällä on Kali Linux - hyökkäyskone Venäjän verkossa, jossa sijaitsee myös kaksi Masiinan hissiä. Punainen tiimi löytää hissiantureiden dataa lähettävän laitteen verkosta, sekä suorittaa ARP Spoofing - hyökkäyksen, jotta he näkisivät hissien lähettämän datan.

Seuraavaksi punainen tiimi estää hissien datalähetyksen kokonaan, nähdäkseen Masiinan reaktion. Masiina ottaa hissien pois käytöstä huollon ajaksi. Sinisen tiimin lähettämä huoltotiimi huomaa, että hissi toimii mutta ei lähetä dataa. Hissi otetaan turvallisuuksista pois käytöstä, eli valkoinen tiimi lopettaa hissiskriptin ajamisen.

Punainen tiimi huomaa Wiresharkista, että Masiina sulki datalähetyksen estämisen takia hissien, jonka jälkeen he aloittavat Masiinan verkon skannauksen, tavoitteena löytää haavoittuvuuksia. Sinisen tiimin tavoitteena on huomata skannaus ja lokittaa se heidän tikettijärjestelmään.

Punaisen tiimin tehtävänä on saada hissidata tietoonsa ja kun hissidataa on saatu, punainen tiimi tviittaa datasta kuvan Moottorille, joka palkkasi hakkeriryhmän.

Tämän jälkeen uutissivusto on julkaissut jutun, jossa kerrotaan, että Masiinan hissitietoja on vuotanut. Masiina vastaa julkisessa lausunnossa, että tämä ei ole totta.

Seuraavaksi punainen tiimi aloittaa kaksi hyökkäystä Masiinaa vastaan. Ensimmäinen hyökkäys on lähettää väärennettyä hissianturidataa valvomon monitorit täyteen, jotta he eivät voi seurata oikeita hissejään. Toinen hyökkäys on DoS hyökkäys masiinan verkkosivulle, jotta Masiinan asiakkaat eivät näe heidän ilmoituksiaan tai pysty ottamaan asiakaspalveluun yhteyttä. Sininen tiimi ottaa kaikki hissit pois käytöstä, sekä ilmoittaa, että sivut ovat alhaalla päivityksen takia. Samalla IT-tuen tavoitteena on estää liikenne hyökkäävästä IP:stä ja estää vääristä hisseistä tulevan liikenteen

myös. Punainen tiimi twiittaa, että Masiina valehtelee, ja että he ovat verkkosivun kaatumisen takana.

Pelitapahtuma	Syötetunnus	Syöte aika	Toimija	Kuvaus	Tavoite	Odotettu reaktio	Jakelukanava
PT1	RT_S1		RT	Venäjän verkon skannaus	Löytää verkon laitteet	Ei huomata	RT RUSSIA Kali Linux
PT2	RT_S2		RT	Hissin ARP-Spoofaus	Nähdä hissin lähettämä data	Ei huomata	RT RUSSIA Kali Linux
PT3	RT_S3		RT	Hissin datan lähetyksen estäminen	Selvittää miten Masiina reagoi	Masiina poistaa hissin käytöstä	RT RUSSIA Kali Linux
PT4	BT1_S1		BT	Huomaa, että RUS hissi ei lähetä dataa	Selvittää vika	Tiketti viasta ja lähetetään huoltomies tutkimaan	Tikettijärjestelmä
PT5			WT	Huoltomies sanoo, että hissi toimii normaalisti ja vika on ohjelmiston tai verkon puolella		BT poistaa hissin käytöstä	
PT6	BT2_S1		BT	Huoltomiehelle ilmoitus, että poistaa hissin käytöstä vian selvittämisen ajaksi	Selvittää vika		
PT7			WT	Hissiskriptin lopettaminen, eli hissin "poistaminen" käytöstä	RT huomaa Wiresharkista, että hissi ei lähetä dataa ja on otettu pois käytöstä	Suuremman hyökkäyksen valmistelu	Kone, jossa hissiskripti pyörii
PT8			RT	Masiinan toimipisteen skannaus	Löytää haavoittuvuuksia	Palomuuuri huomaa ja BT luo tiketin	RT RUSSIA Kali Linux
PT9			BT	Skannauksesta luodaan tiketti			BT tikettijärjestelmä
PT10			RT	Kaapatun hissidatan julkaiseminen twitteriin	Hämmennyksen luominen	Uutinen aiheesta ja Masiinalta julkinen lausunto	twitter.fi
PT11			WT	Uutinen: Hakkeritiimi julkaisi Masiinan hissin dataa			Iltajutku.fi
PT12			BT	Uutisen "oikaisu", hakkeritiimin väitös ei pidä paikkansa	Maineen säilyttäminen		twitter.fi, masiina.com
PT13			RT	Väärennetyn datan lähettäminen valvomokoneelle	Estää valvomoa näkemästä hissiin lähettämä data	BT poistaa hissit käytöstä	RT RUSSIA Kali Linux
PT14			RT	Masiina.com verkkosivun kaataminen	Kaataa Masiinan kotisivut DoS-hyökkäyksellä	BT huomaa hyökkäyksen ja estää liikenteen palomuurista	RT RUSSIA Kali Linux
PT15			BT	Huomaa ylimääräisen datan ja poistaa hissit käytöstä selvittääkseen ylimääräisen datan lähettäjä	Käskeyttää hissiin käytöstä poistamisesta ja ylimääräisen liikenteen estäminen	BT estää ylimääräisen datan lähettämisen palomuurista	pfSense
PT16			WT	Kaikkien hissiskriptien pysäyttäminen	Hissit pois käytöstä		Laitteet, joilla hissiskriptit pyörii
PT17			BT	DoS hyökkäyksen keskeyttäminen ja kotisivujen saaminen toimintaan	Hyökkäyksen esto palomuurista	Hyökkäävä IP-osoite estetään ja kotisivut saadaan takaisin	pfSense
PT18			BT	Julkinen lausunto, että hissit ovat pois käytöstä ohjelmistovian takia	Estetään tietojen leviäminen haavoittuvuuksista		twitter.fi, masiina.com
PT19			WT	Uutinen: Masiinan hissit pois käytöstä ohjelmistovian takia	Masiinan maineen säilyttäminen		Iltajutku.fi
PT20			BT	Ilmoitus: Kotisivut olivat alhaalla päivityksen takia	Maineen säilyttäminen		twitter.fi, masiina.com
PT21			WT	Uutinen: Masiinan kotisivut alhaalla päivityksen takia			Iltajutku.fi
PT22			RT	Twiitti: Masiina valehtelee, hissiin ongelma erilainen	Masiinan mustamaalaus		Twitter.fi
PT23			WT	Uutinen: Hakkeriryhmä ilmoitti Twitterissä olevan Masiinan ongelmien takana			Iltajutku.fi
PT24							
PT25							
PT26							
PT27							
PT28							
PT29							
PT30							

Kuvio 7

8.5 Aikataulutus

Kello 08.00 Harjoitteluun osallistuvat ryhmät perehdytään

Kello 08.45 Harjoitus alkaa

Kello 10.45 Harjoitus päättyy

Kello 11.00 Tilannekatsaus ja palaute

9 Yleiset vaatimukset harjoitusympäristölle

9.1 Harjoitusympäristön tulee olla eristetty ja hallittavissa

Ensimmäinen vaatimus kyberharjoitusympäristölle on, että ympäristön tulee olla eristettynä julkisesta internetistä. Eristys on tehty ympäristössämme siten, että virtuaalikoneiden verkkokortit ovat vain ”internal” verkossa ja eivät liikkennöi ulospäin NAT-tai bridged rajapintojen kautta.

9.2 Ympäristön tulee olla etäkäytettävissä

Yhtenä ympäristön vaatimuksina on, että ympäristön pitää olla etäkäytettävissä. Jos ympäristöä voidaan käyttää myös muualta kuin harjoitusympäristön sisältä niin pelaajan ei tarvitse välttämättä olla fyysisesti läsnä harjoitustilassa. Ympäristö on toteutettu yhdelle kannettavalle tietokoneelle joten ympäristö ei ole aina saatavilla. Etäkäyttö onnistuu kuitenkin samasta verkkosegmentistä ottamalla etätyöpöytäyhteys.

9.3 Ulkoverkon palveluiden tulee olla saatavilla tarvittaessa

Ympäristössä tulee olla mahdollisuus päästä kiinni ulkoisen verkon palveluihin hetkelisesti ja hallitusti niin, että ympäristön instanssi voi hakea vaikka tietyn päivityspaketin ulkoverkosta. Tapahtuman pitää olla suoritettuna niin, ettei ympäristön muut laitteet ole kyseisellä hetkellä kiinni laitteessa joka on kiinni ulkoverkossa. Tästä voidaan käyttää myös termiä ilmalukko. Ulkoverkon palvelu saadaan käyttöön kun yksittäisen virtuaalikoneen verkkokortti vaihdetaan siltaamaan ulkoverkkoon tai NAT:aamaan host koneelle.

9.4 Virtualisointitekniikoiden käyttäminen

Harjoitusympäristön toteuttamiseen tulisi käyttää virtualisointitekniikoita käytettävyyden ja kustannustehokkuuden takia. Ympäristöä on myös nopea muokata, jos koneet ovat virtuaalisia. Koko harjoitusympäristö pyörii Virtualbox Hypervisorin päällä.

9.5 Teknisen ympäristön tulee olla modulaarinen

Ympäristön modulaarisuutta voidaan helposti muokata ja ympäristöön voidaan lisätä uusia koneita. Verkkoja voidaan vaihtaa lennosta jos koneissa on vain verkkokortti li-sättynä.

9.6 Julkisen palveluntarjoajan runkoverkko

Jotta harjoitusympäristö olisi mahdollisimman realistinen, sinne on toteutettava julkinen operaattoriverkko. Ympäristössämme on useita reitittimiä, jotka tarjoavat ympäristön koneille reititysverkon, DNS-ja NTP palvelut.

9.7 Julkiset palvelut

Ympäristöön on toteutettava useita julkisia palveluita, jotta se olisi mahdollisimman realistinen. Ympäristöön on toteutettu DNS-nimipalvelu, NTP-aikapalvelu, WWW-hosting palvelut sekä DHCP-palvelu.

9.8 Kattava tarjonta julkisia verkkosivustoja

Ympäristön elävöittämiseksi verkossa on useita verkkosivustoja eri toteutuksilla. Ympäristöön on toteutettu sosiaalinen media twitter.fi, iltapäivälehti iltajutku.fi, operaattorin kotisivut operaattori.fi, yrityksen kotisivut masiina.com, tukipyyntöjä varten luotu tikettienhallintajärjestelmä support.masiina.com sekä viestintäkanava mattermost.masiina.com.

10 Harjoituksen tekninen suunnittelu

Harjoitusympäristöä suunniteltaessa on otettava huomioon harjoitukseen osallistujat, suunnitteluun varattu aika, sekä itse resurssit harjoitusympäristön toteutukseen.

10.1 Virtuaaliympäristö

Harjoitusympäristön toteutukseen käytetään virtualisointitekniikoita. Virtuaaliympäristöä ajetaan Lenovo Thinkpad W520:lla. Pelaajat ottavat etätyöpöytä yhteyden suunniteltuihin virtuaalikoneisiin Remote Desktop Connection ohjelmalla, joissa he käyttäytyvät pelimaailman sääntöjen mukaisesti. Virtuaaliympäristö on eristetty julkisesta verkosta, eikä ympäristöstä ole mahdollista päästä ulko verkkoon.

REMOTE HOST PORTS			
SWEDEN ELEVATOR	3391	POLAND VYOS	3403
SWEDEN ELEVATOR 2	3392	POLAND ELEVATOR	3404
SWEDEN VYOS	3392	POLAND ELEVATOR 2	3405
		POLAND ATTACKER	3406
RUSSIA VYOS	3394		
RUSSIA ELEVATOR	3395	FINLAND ELEVATOR	3407
RUSSIA ELEVATOR 2	3396	FINLAND ELEVATOR 2	3408
RUSSIA ATTACKER	3397	ISP HOSTING	3409
		ISP WORKSTATION	3410
MASIINA WS	3398	FINLAND VYOS 2	3411
FIREWALL	3399	DNS	3412
HTTP	3400	SLACK CHANNEL	3413
FINLAND VYOS 1	3401	NTP	3414
MASIINA SERVER	3402		

Kuvio 8 Etäyhteysportit

10.2 Virtuaalikoneet

Ympäristössä on useita eri virtuaalikoneita eri käyttöjärjestelmineen (Kuvio 9 Virtuaalikoneet). Työasemat ovat kevyitä Ubuntu koneita jotka ovat oiva valinta ympäristön toteutuksessa. Palomuurina toimii pfSense, joka on yksi parhaita ja monipuolimpia avoimen lähdekoodin palomuuriratkaisuja. Hyökkääjille on Kali Linux koneita, jotka sisältävät suuren määrän tietoturvatyökaluja hyökkäyksien tekemiseen. Julkiset palvelut ovat toteutettu CentOS 7 koneilla.

Virtuaalikoneet						
Palvelut	Käyttöjärjestelmä	RAM(MB)	HDD(GB)	Määrä	RAM Yht	HDD Yht
HTTP/DNS/NTP	Centos 7	512	2	4	2048	8
Palomuuuri	pfSense	512	2	1	512	2
Työasema	Lubuntu	512	2	2	1024	4
RED-Team	Kali Linux	1024	2	2	2048	4
Hissi	Lubuntu NOGUI	128	2	8	1024	16
Reititys	Vyos	512	2	5	2560	10
Yhteensä				22	9216	44

Kuvio 9 Virtuaalikoneet

10.3 Virtuaaliverkko

Ympäristön runkoverkon reititys on toteutettu Vyos virtuaalireitittimillä, jotka pohjautuvat Debian Linux käyttöjärjestelmään. Vyos reitittimien konfigurointi perustuu Juniperin JUNOS käyttöjärjestelmään ja sen ansiosta reititin on todella helppo konfiguroida (Kuvio 9 Vyos reitittimet).

Reitittimet			
Käyttöjärjestelmä	Isäntänimi	RAM	HDD
Vyos	FINLAND-R1	512 MB	2GB
Vyos	RUSSIA-R2	512 MB	2GB
Vyos	POLAND-R3	512 MB	2GB
Vyos	SWEDEN-R4	512 MB	2GB
Vyos	FINLAND-ISP	512 MB	2GB

Kuvio 10 Vyos reitittimet

10.4 IP-suunnittelu

Harjoitusympäristön IP-osoitteistus tehdään kuten oikeassa ympäristössä. Ympäristössämme IP-osoitteet ovat asetettu maakohtaisesti ja osoitteet ovat jaettu RIPE NCC IP-tietokannan perusteella eri maiden välille. Esimerkiksi verkko 62.106.5.0 on varattu suomeen tier-3 operaattorille. Ympäristössä on 5 reititintä, jotka ovat jaettu maakohtaisesti neljälle maalle.

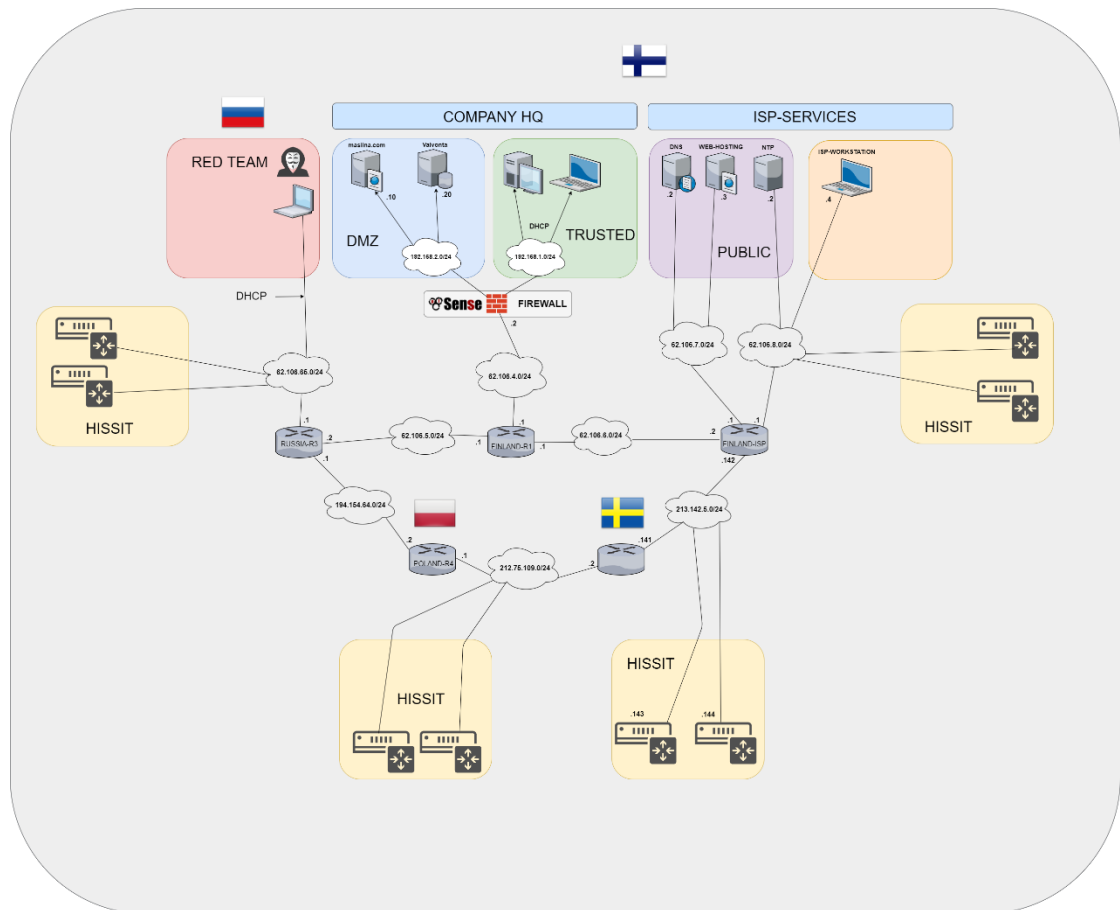
IP osoitteet otetaan 4 eri maasta jotka ovat kuvattuna topologiassamme. Alla IP-alueet eri maista mitkä valitsimme (Kuvio 10).

	FROM	IP-Address		TO	IP-Address
FIN_R1	Interface eth1	62.106.4.1/24	→	FW-1	62.106.4.2/24
	Interface eth2	62.106.5.1/24	→	RUS_R1 eth1	62.106.5.2/24
	Interface eth3	62.106.6.1/24	→	FIN_R5 eth1	62.106.6.2/24
	FROM	IP-Address		TO	IP-Address
RUS_R2	Interface eth1	62.106.5.2/24	→	FIN_R1 eth2	62.106.5.1/24
	Interface eth2	194.154.64.1/24	→	POL_R3 eth1	194.154.64.2/24
	Interface eth3	194.154.64.3/24	→	HISSI_GW_RUS	
	Interface eth4	194.154.65.1/24	→	RED_TEAM_GW_1	194.154.65.2/24
	FROM	IP-Address		TO	IP-Address
POL_R3	Interface eth1	194.154.64.2/24	→	RUS_R2 eth2	194.154.64.1/24
	Interface eth2	212.75.109.1/24	→	SWE_R4 eth1	212.75.109.2/24
	Interface eth3	212.75.109.3/24	→	HISSI_GW_POL	
	FROM	IP-Address		TO	IP-Address
SWE_R4	Interface eth1	212.75.109.2/24	→	POL_R3 eth2	212.75.109.1/24
	Interface eth2	213.142.5.141/24	→	FIN_R5 eth2	213.142.5.142/24
	Interface eth3	213.142.5.143/24	→	HISSI_GW_SWE	
	FROM	IP-Address		TO	IP-Address
FIN_R5	Interface eth1	62.106.6.2/24	→	FIN_R1 eth3	62.106.6.1/24
	Interface eth2	213.142.5.142/24	→	SWE_R4	213.142.5.141/24
	Interface eth3	62.106.6.3/24	→	HISSI_GW_FIN	
	Interface eth4	62.106.7.1/24	→	DNS	62.106.7.2
				HTTP	62.106.7.3
	Interface eth5	62.106.8.1/24	→	NTP	
	Interface eth6	62.106.9.1/24	→	PUBLIC DHCP	

Kuvio 11 IP-Suunnitelma

10.5 Harjoitusympäristön topologia

Harjoitusympäristön looginen topologia on rengasmainen (Kuvio 11), jossa kaikki reitittimet ovat kytketty renkaaksi. Rengastopologia ei ole redundantisesti hyvä ratkaisu, sillä jos yksi reititin putoaa pois verkosta niin osa palveluista ei toimi.



Kuvio 12 Ympäristön looginen topologia

10.6 DNS

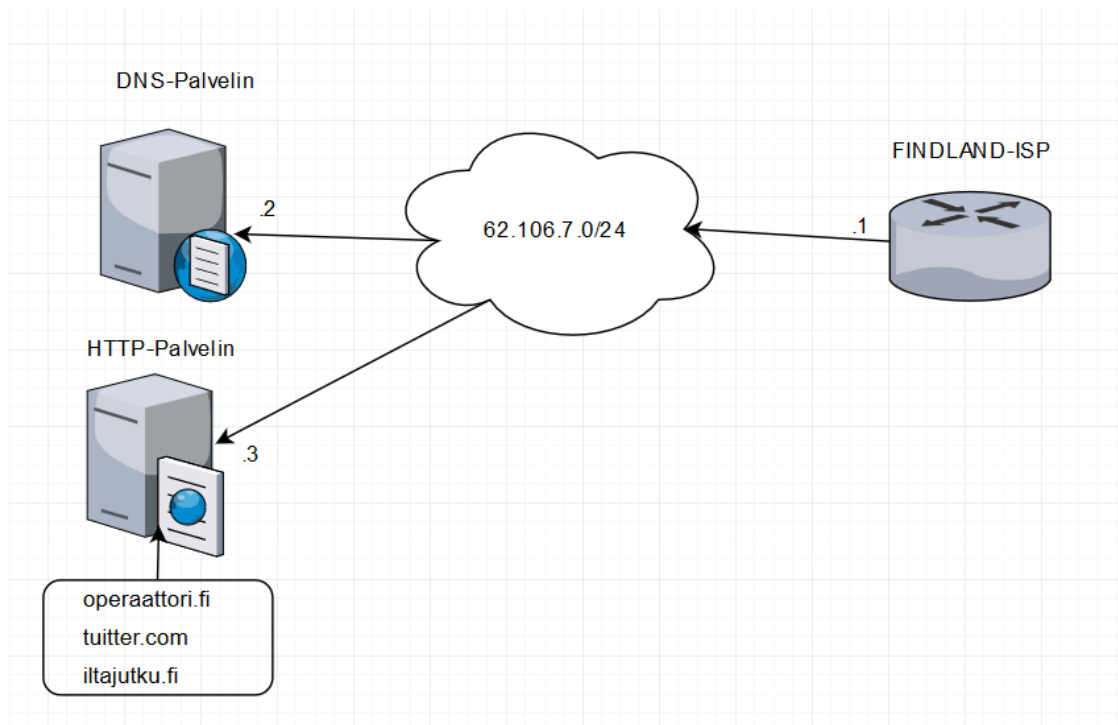
DNS(Domain Name System) on palvelu, joka kääntää verkkotunnuksia IP-osoitteiksi. Harjoitusympäristön DNS-palvelu toteutetaan bind9 DNS-Daemonilla, jonka saa asennettua monille Linux distribuutioille pakettienhallinnasta.

Ympäristössä DNS verkkotunnukset ovat kaikilla HTTP sivustoilla ja reitittimillä. Osa verkkosivuista ovat operaattorin saman IP-osoitteen takana virtualhosteina (Kuvio 12).

Verkkotunnus	IP-Osoite	Info
iltajutku.fi	62.106.7.3	vhost
masiina.com	62.106.4.2	-
operaattori.fi	62.106.7.3	vhost
twitteri.fi	62.106.7.3	vhost
router1.operaattori.fi	62.106.5.1	reititin
router2.operaattori.fi	194.154.64.1	reititin
router3.operaattori.fi	212.75.109.1	reititin
router4.operaattori.fi	213.142.5.141	reititin
router5.operaattori.fi	62.106.7.1	reititin

Kuvio 13 DNS Verkkotunnukset

DNS palvelin sijoitetaan operaattorin verkkoon FINLAND-ISP reitittimen rajapintaan 62.106.7.0/24 (Kuvio 13). DNS-palvelimen IP-osoite on 62.106.7.2 ja HTTP-palvelimen osoite on 62.106.7.3.



Kuvio 14 FINLAND-ISP looginen kuva

10.7 NTP

CentOS 7 koneelle asennettiin NTP-paketti, ja palvelinta muokattiin niin, että muut koneet harjoitusympäristön aliverkoista voivat suorittaa aikakyselyitä tälle palvelimelle. Koska palvelin ei ole yhdistetty ulkoiseen verkkoon, se antaa muille ajan omasta ajastaan.

10.8 HTTP

Harjoitusympäristöön toteutetaan useita eri verkkosivustoja simuloimaan oikean internetin sivustoja. Ympäristöön toteutetaan seuraavat verkkosivustot.

- Iltajutku.fi
- masiina.com
- operaattori.fi
- Ttwitter.fi
- Support.masiina.com
- Mattermost.masiina.com

Sivusto	Tyyppi	IP-osoite	CMS
Iltajutku.fi	Iltapäivälehti	62.106.7.3	Wordpress
Masiina.com	Yrityksen kotisivut	62.106.4.2	-
Operaattori.fi	Operaattorin kotisivut	62.106.7.3	-
Ttwitter.fi	Sosiaalinen media	62.106.7.3	GNU Social
Support.masiina.com	Tiketinhallintajärjestelmä	62.106.7.3	osTicket
Mattermost.masiina.com	Slackin tapainen viestintäsovellus yrityksen sisäiseen viestintään	62.106.7.3	Mattermost

Taulukko 1 Verkkosivustot

10.9 Hissien suunnittelu

Ympäristöön suunniteltiin kahdeksan hissiä, kaksi jokaiseen maahan. Hissien käyttäytymistä piti simuloida skripteillä, jotka lähettävät dataa verkon yli masiinan palvelimelle (Kuvio 14 hissien valvonta). Hissien toiminnallisuus toteutettiin Python ohjelmointikielellä. Hissit toteutettiin Lubuntu virtuaalikoneille, joista python löytyy jo esiasennettuna. Hissipalvelin kuuntelee TCP porttia 8888, johon hissit lähettävät dataa skriptiin määritetyn satunnaisen aikavälin mukaan. (Kuvio 15)

```

1  import socket
2  import sys
3
4  sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
5  sock.bind(("localhost",8888))
6  sock.listen(5)
7
8  while True:
9      client, addr = sock.accept()
10     print client.recv(1024)
11     client.close()

```

Kuvio 15 Hissien valvonta

Jokainen hissikone lähettää satunnaista dataa hissipalvelimelle TCP porttiin 8888.

```

1  import random
2  import time
3  import socket
4
5  class Elevator():
6
7      def __init__(self,ID,buildingname,floor,temperature,weight):
8          self.ID = ID
9          self.buildingname = buildingname
10         self.floor = floor
11         self.temperature = temperature
12         self.weight = weight
13
14     def changefloor(self, newfloor):
15         self.floor = newfloor
16
17     def changeweight(self, newweight):
18         self.weight = newweight
19
20     def changetemperature(self, newtemp):
21         self.temperature = newtemp
22
23     def randomize(self):
24         self.floor = random.randint(1,6)
25         self.weight = random.randint(0,500)
26         self.temperature = random.randint(15,25)
27
28     def senddata(self,address,port,data):
29         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
30         sock.connect((address,port))
31         sock.send(data)
32         sock.close()
33
34     def toString(self):
35         return "Elevator ID: " + str(self.ID) + " | " + "Building: " + self.buildingname + " | " + "Current Floor: " + str(self.flo
36
37 elevator = Elevator(1,"Dynamo",1,19,140)
38 while (True):
39     elevator.senddata("localhost",8888,elevator.toString())
40     time.sleep(60)
41     elevator.randomize()

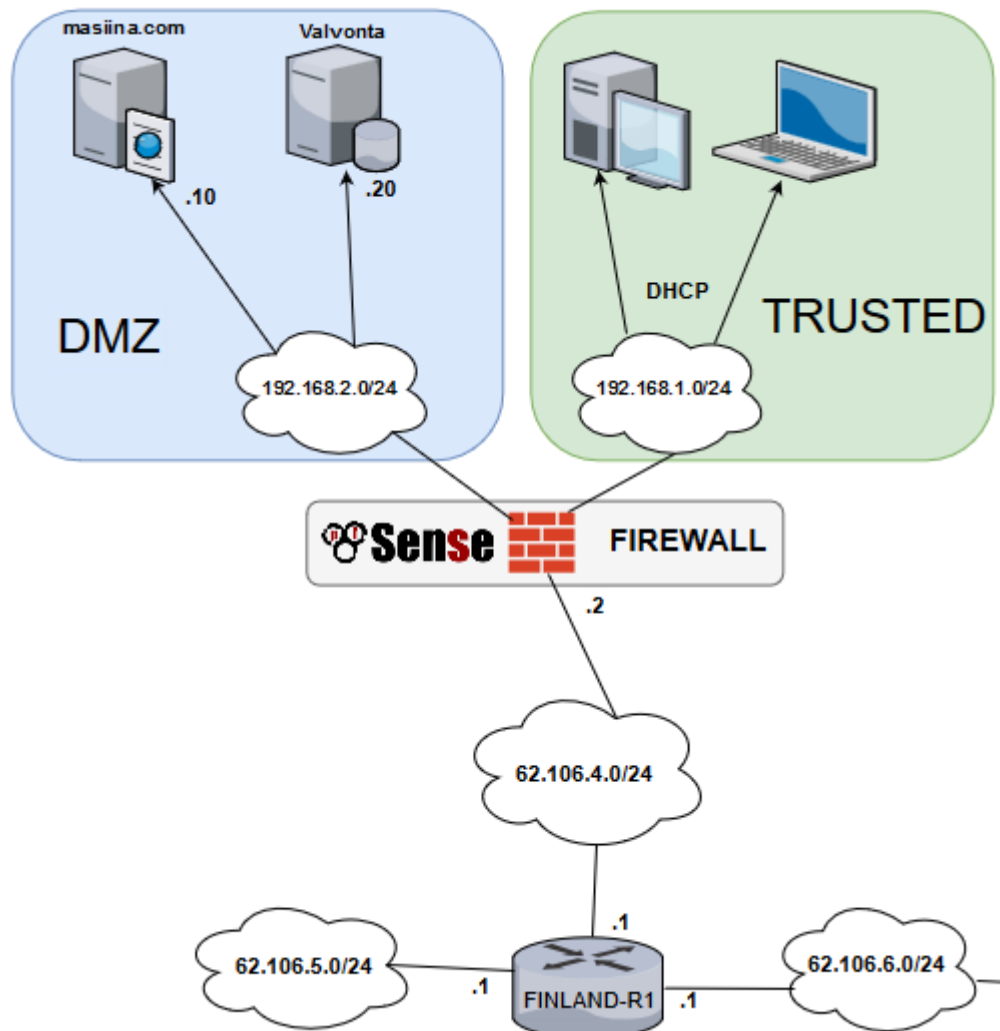
```

Kuvio 16 Hissin scripti

Hissipalvelin tarkistaa datan eheyden ja lokittaa virheet jos data on väärentyyppistä tai hissien anturi havaitsee poikkeaman (esim. Lämpötila ylittää tietyn arvon).

10.10 Yrityksen päätoimipisteen suunnittelu

Masiinan päätoimipiste sijaitsee ympäristössämme FINLAND-R1 reitittimen takana osoitteessa 62.106.4.2/24. Yrityksellä on oma palomuuuri, HTTP-palvelin sekä hissien valvontaan tarkoitettu palvelin, jota verkonvalvonta seuraa. (Kuvio 16)



Kuvio 17 Toimipisteen looginen topologia

Yrityksen palomuurit tekevät NAT-osoitteenmuunnoksen, jotta yhden IP-osoitteen takana voi olla monta laitetta. Masiinan LAN-verkko koostuu kahdesta privaatisesta aliverkosta. Ensimmäinen verkko 192.168.2.0/24 on tarkoitettu masiinan verkonvalvonnan laitteille ja HTTP-palvelimelle. HTTP-palvelin tarjoaa yrityksen omat verkkosivut julkisen verkon saataville. Toinen aliverkko 192.168.1.0/24 on tarkoitettu yrityksen työasemien käyttöön. Verkonvalvonnan osoitteet asetetaan staattisesti ja työasemat saavat IP-osoitteensa DHCP:llä.

Yrityksen privaattiverkot	TYYPPI	RAJAPINTA
Masiina_HTTP	192.168.2.10/24	STATIC
Masiina_SNMP	192.168.2.20/24	STATIC
Masiina_WS	192.168.1.0/24	DHCP
		Masiina_LAN

Kuvio 18 Yrityksen LAN-verkot osoitteet

11 Harjoitusympäristön toteutus

11.1 Virtuaaliympäristö

Harjoitusympäristömme on rakennettu Oraclen Virtualbox hypervisorin päälle. Virtualbox on ilmainen hypervisor, joka on yksinkertainen käyttää ja soveltuu usealle eri käyttöjärjestelmälle. Virtualboxista löytyy kaikki tarvittavat peruskomponentit virtualisointiin ja ympäristön pyörittämiseen.

11.2 Reititys

Ympäristön reititys on toteutettu viiden virtuaalisen Vynos reitittimen välillä. Reittien mainostus ja uudelleen jakaminen on toteutettu OSPF (Open Shortest Path First) reititysprotokollalla. Jokainen reititin osaa reitittää kaikkiin omiin rajapintoihin, jotka ovat määritelty. Muiden reitittimen reitit pitää saada reititysprotokollalta.

Reitittimen OSPF-konfiguraatioon on kerrottu, mitä verkkoja halutaan mainostaa. Kaikki staattiset reitit sekä yhdistetyt rajapinnat uudelleen mainostetaan seuraavalle reitittimelle(Kuvio 18 R1-Reitittimen OSPF)

```

}
protocols {
  ospf {
    area 0 {
      network 62.106.5.0/24
      network 62.106.6.0/24
    }
    redistribute {
      connected {
        metric-type 2
      }
      static {
        metric-type 2
      }
    }
  }
}

```

Kuvio 19 R1-Reitittimen OSPF

Reitittimen reititystaulusta voidaan katsoa mitä reittejä reititin on oppinut. (Kuvio 19)

```
vyos@FINLAND-R1:~$ sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 62.106.4.0/24 is directly connected, eth1
O  62.106.5.0/24 [110/10] is directly connected, eth0, 00:13:00
C>* 62.106.5.0/24 is directly connected, eth0
O  62.106.6.0/24 [110/10] is directly connected, eth5, 00:13:01
C>* 62.106.6.0/24 is directly connected, eth5
O>* 62.106.7.0/24 [110/20] via 62.106.6.2, eth5, 00:12:06
O>* 62.106.8.0/24 [110/20] via 62.106.6.2, eth5, 00:12:06
C>* 127.0.0.0/8 is directly connected, lo
O>* 194.154.64.0/24 [110/20] via 62.106.5.2, eth0, 00:12:49
O>* 194.154.65.0/24 [110/20] via 62.106.5.2, eth0, 00:12:49
O>* 194.154.66.0/24 [110/20] via 62.106.5.2, eth0, 00:12:48
O>* 212.75.109.0/24 [110/30] via 62.106.5.2, eth0, 00:12:35
O>* 213.142.5.0/24 [110/40] via 62.106.5.2, eth0, 00:12:35
vyos@FINLAND-R1:~$
```

Kuvio 20 R1-reitittimen reittitaulu

11.3 Verkon palvelut

Julkiseen verkkoon luotiin DNS, NTP ja WWW palvelut. Kaikki palvelut ovat operaattoriverkossa julkisilla IP-osoitteilla varustettuina.

Julkiset palvelut	
IP-Osoite	Palvelu
62.106.7.2	DNS
62.106.8.2	NTP
62.106.7.3	WWW

11.3.1 DNS

DNS-nimipalvelin toteutetaan bin9/named nimipalvelimen avulla. DNS-palvelin asennettiin Centos 7 käyttöjärjestelmän päälle. Bind9 nimipalvelin daemon löytyy suoraan centosin pakettien hallinnasta komennolla "yum install bind". Kun paketti on asennettu, niin dns-palvelin täytyy konfiguroida suunnitelman mukaisesti.

Jokaiselle verkko-osoitteelle luodaan zone ja kerrotaan mistä tämän zonen määrittelyt löytyvät. jokaiselle zonelle luodaan myös reverse zone jotta ip-osoite voidaan kääntää verkko-osoitteeksi.

11.3.2 NTP

NTP-aikapalvelin asennettiin myös centos 7 jakelun päälle. NTP-palvelimelle on luotu DNS-nimi 0.ntp.pool.fi jota käytetään kun asetetaan aikapalvelinta kellonajan synkronoisissa.

NTP-palvelimelle sallitaan kyselyt vain ympäristössä olevista aliverkoista.

```
GNU nano 2.3.1      File: /etc/ntp.conf

# Permit all access over the loopback interface.  This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict ::1
restrict 62.106.9.0 mask 255.255.255.0 nomodify notrap
restrict 213.142.5.0 mask 255.255.255.0 nomodify notrap
restrict 213.75.109.0 mask 255.255.255.0 nomodify notrap
restrict 194.154.64.0 mask 255.255.255.0 nomodify notrap
restrict 62.106.4.0 mask 255.255.255.0 nomodify notrap

# Hosts on local network are less restricted.
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
```

11.3.3 HTTP

Harjoitusympäristöön luotiin erillinen HTTP-palvelin, jolla pyörii kaikki tarvittavat nettisivut. Kaikki sivut löytää omilla domain nimillä, joka on toteutettu Virtualhosteilla.

```
GNU nano 2.3.1      File: /etc/httpd/sites-available/twitter.conf

NameVirtualHost *:80

<VirtualHost *:80>
    ServerName www.twitter.fi
    DocumentRoot /var/www/gnusoical
    ServerAlias twitter.fi
    DirectoryIndex index.php
    <Directory /var/www/gnusoical/>
        AllowOverride All
        Order Deny,Allow
        Allow from all
    </Directory>
</VirtualHost>

<VirtualHost *:80>
    ServerName www.iltajutku.fi
    DocumentRoot /var/www/wordpress
    ServerAlias iltajutku.fi
</VirtualHost>
```

Kuvio 21 Virtualhost konfigurointi

```
<VirtualHost *:80>
  ServerName www.operaattori.fi
  DocumentRoot /var/www/operaattori
  ServerAlias operaattori.fi
</VirtualHost>
```

Kuvio 22 Virtualhost konfigurointi

```
<Virtualhost *:80>
  ServerName www.support.masiina.com
  DocumentRoot /var/www/support/upload
  ServerAlias support.masiina.com
<Directory var/www/support/upload>
  DirectoryIndex index.html index.php
  Options FollowSymLinks
  AllowOverride ALL
  Require all granted
</Directory>
</VirtualHost>
```

Kuvio 23 Virtualhost konfigurointi

```
root@jamk-3a895c520a:/etc/httpd/conf
GNU nano 2.3.1 File: httpd.conf Modified
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
#EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
IncludeOptional sites-enabled/*.conf
```

Kuvio 24 httpd lataa tiedostoja valitusta paikasta

```
GNU nano 2.3.1 File: /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1 twitter.fi
127.0.0.1 iltajutku.fi
127.0.0.1 operaattori.fi
127.0.0.1 support.masiina.com
```

Kuvio 25 Hostien määrittely

Jokaiselle sivulle luodaan oma tietokanta MariaDB:llä.

```

MariaDB [(none)]> create database tvtter;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> grant all privileges on tvtter.* TO "root"@"localhost" identified by "jutku123"
-> ;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.00 sec)

```

Kuvio 26 Tvtter database

```

MariaDB [(none)]> create database iltajutku.fi
-> ;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> grant all privileges on iltajutku.fi.* to wpuser@localhost identified by 'jutku123';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.00 sec)

```

Kuvio 27 Iltajutku.fi database

```

MariaDB [(none)]> create database osticket;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> grant all privileges on osticket.* to osticketuser@localhost identified by 'jutku123';
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> _

```

Kuvio 28 osTicket database

Gnu-Social asennus selaimesta

Site settings

Site name

The name of your site

Fancy URLs ☐ enable
☒ disable

Fancy URL support detection failed, disabling this option. Make sure you renamed htaccess.sample to .htaccess.

Server SSL ☐ enable
☒ disable

Enabling SSL (https://) requires extra webserver configuration and certificate generation not offered by this installation.

Database settings

Hostname

Database hostname

Type ☒ MariaDB (or MySQL 5.5+)

Database type

Name

Database name

DB username

Database username

DB password

Database password (optional)

Kuvio 29 GNU-socialin määrittely

Administrator settings

Administrator nickname
Nickname for the initial user (administrator)

Administrator password
Password for the initial user (administrator)


Confirm password

Administrator e-mail
Optional email address for the initial user (administrator)

Site profile

Type of site
Initial access settings for your site

Kuvio 30 GNU-socialin määrittely

 **GNU social**
GNU social

Install GNU social

Page notice

- Initializing...
- Starting installation...
- Checking database...
- Creating database tables...
- Adding SMS carrier data to database...
- Adding notice source data to database...
- Adding foreign service data to database...
- Writing config file...
- An initial user with the administrator role has been created.
- Setting site profile...
- GNU social has been installed at <http://192.168.43.104/>
- **DONE!** You can visit your new GNU social site (log in as "masiina"). If this is your first GNU social install, make your experience the best possible by visiting our resource site to join the mailing list or IRC. FAQ is found here.

Kuvio 31 GNU-social asennus

Wordpressin asennus selaimella.

www.iltajutku.fi/wp-admin/install.php

Welcome to the famous five minute WordPress installation process! You may want to browse the [ReadMe documentation](#) at your leisure. Otherwise, just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title

Username
Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods and the @ symbol.

Password, twice
A password will be automatically generated for you if you leave this blank.

Medium
Hint: The password should be at least seven characters long. To make it stronger, use upper and lower case letters, numbers and symbols like ! " ? \$ % ^ & *.

Your E-mail
Double-check your email address before continuing.

Kuvio 32 WordPressin määrittely

oTicketin asennus selaimessa

oTicket Installer - Mozilla Firefox

support.masiina.com/setup/install.php

Thank You for Choosing oTicket!

We are delighted you have chosen oTicket for your customer support ticketing system!

The installer will guide you every step of the way in the installation process. You're minutes away from your awesome customer support system!

Prerequisites

Before we begin, we'll check your server configuration to make sure you meet the minimum requirements to install and run oTicket.

Required:
These items are necessary in order to install and use oTicket.

- ✓ PHP v5.3 or greater (5.3.6)
- ✓ MySQL extension for PHP (module loaded)

Recommended:
You can use oTicket without these, but you may not be able to use all features.

- ✓ GD2B extension
- ✗ PHP (SMTP) extension (Required for mail fetching)
- ✓ PHP XML extension (for XML API)
- ✓ PHP XML DOM extension (for HTML, email processing)
- ✓ PHP JSON extension (faster performance)
- ✓ Mbstring extension (recommended for all installations)
- ✓ Pchar extension (recommended for plugins and language packs)

[Continue >](#)

Copyright © 2013 oTicket.com

Kuvio 33 oTicketin määrittely

System Settings

The URL of your helpdesk, its name, and the default system email address

Helpdesk URL:

http://support.masiina.com/

Helpdesk Name:

Masiina Support

?

Default Email:

masiina@localhost.com

?

Primary Language:

English (United States) ▾

?

?

Helpdesk Name

The name of your support system e.g [Compar

Admin User

Your primary administrator account - you can add more users later.

First Name:

Masiina

?

Last Name:

Masiina

?

Email Address:

masiina@localhost.com

?

Username:

masiina

?

Password:

?

Retype Password:

?

Kuvio 34 osTicketin määrittely

Database Settings

Database connection information

MySQL Table Prefix:

ost_

?

MySQL Hostname:

localhost

?

MySQL Database:

osticket

?

MySQL Username:

osticketuser

?

MySQL Password:

?

Install Now

Need Help?

We provide [professional installation services](#) and commercial support. [Learn More!](#)

Kuvio 35 osTicketin määrittely

11.4 Yrityksen toimipiste

11.4.1 Tietoturva

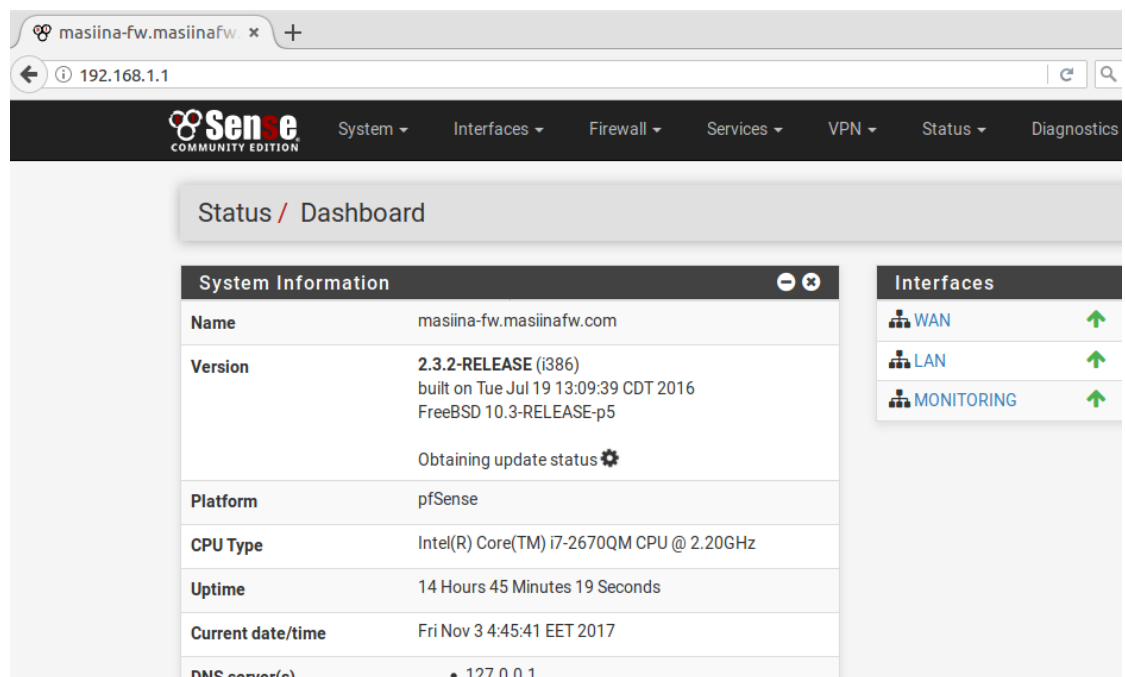
Yrityksen palomuuriksi valittiin pfSense palomuuuri, joka on FreeBSD pohjainen avoimen lähdekoodin palomuurijakelu. Palomuuuri on hyvin varusteltu, josta löytyy kaikki tarvitsemamme ominaisuudet toteutukseemme.

Palomuuriin asetettiin 3 eri rajapintaa ja IP-osoitteet.

```
WAN (wan)      -> vtnet0      -> v4: 62.106.4.2/24
LAN (lan)      -> vtnet1      -> v4: 192.168.1.1/24
MONITORING (opt1) -> vtnet2    -> v4: 192.168.2.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Palomuuria voidaan hallita web-konsolin kautta molemmista lähiverkoista.



Toimipisteen lähiverkkoon laitetaan DHCP-palvelu päälle, joka jakaa työasemille osoitteet 192.168.1.0/24 verkosta.

Services / DHCP Server / LAN

WAN

LAN

MONITORING

General Options

Enable

☒ Enable DHCP server on LAN interface

Deny unknown clients

☐ Only the clients defined below will get DHCP leases from this server.

Ignore denied clients

☐ Denied clients will be ignored rather than rejected.

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured

Subnet

192.168.1.0

Subnet mask

255.255.255.0

Available range

192.168.1.1 - 192.168.1.254

Range




192.168.1.10

192.168.1.245

From

To

Palomuriin asetetaan DNS-resolveri päälle ja lisäsäännöksi host-override joka määrittää, että www.masiina.com verkkosivut löytyvät paikalliselta domainilta. Ilman tätä sääntöä pfSense varoittaa DNS-rebind hyökkäyksestä, kun yritetään selata www.masiina.com palomuurin aliverkoista.

Host Overrides				
Host	Domain	IP	Description	Actions
www	masiina.com	192.168.2.10	Masiina	 
				 Add

Palomuurisäännöt					
Verkko	Lähde	Kohde	Protokolla	Portti	Palvelu
Monitoring	Hissi Addr	192.168.2.20	TCP	8888	Hissit
Monitoring	WAN Addr	192.168.2.10	TCP	80	HTTP
LAN	192.168.1.0/24	62.106.7.2	UDP	53	DNS
LAN	192.168.1.0/24	any	TCP	80	HTTP
LAN	192.168.1.0/24	any	TCP	443	HTTPS

Kuvio 36 Palomuurisäännöt

12 Hyökkäysten tekninen toteutus

Punainen tiimi toteuttaa hyökkäykset suunnitelman mukaan sinistä tiimiä vastaan käyttäen Kali Linuxin hyökkäystyökaluja.

12.1 Verkkoskannaus

Verkkoskannaus on ensimmäinen vaihe, kun yritetään etsiä mahdollisia hyökkäyksen kohteita. Route komennolla voidaan nähdä, että kaikki paketit hyökkääjältä menevät verkkoon 194.154.65.0. Voimme aloittaa skannaamisen tästä verkosta.

```
root@kali:~# ip route
default via 194.154.65.1 dev eth0
194.154.65.0/24 dev eth0 proto kernel scope link src 194.154.65.10
root@kali:~#
```

Kuvio 37 Hyökkääjän reittitaulu

Ensimmäinen yksinkertainen skannaus voidaan suorittaa netdiscover työkalulla, joka löytyy Kali Linuxista valmiiksi asennettuna.

```
root@kali:~# netdiscover -r 194.154.65.0/24
```

Samasta verkosta löytyi kaksi hostia, joista toinen on yhdyskäytävä hyökkääjälle.

Voimme nyt suorittaa tarkempia skannauksia koneelle, jonka IP-osoite on 194.154.65.11.

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 2 hosts. Total size: 240
-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
194.154.65.1 08:00:27:33:0b:8e    2     120 PCS Systemtechnik GmbH
194.154.65.11 08:00:27:c7:e5:18    2     120 PCS Systemtechnik GmbH
root@kali:~#
```

Kuvio 38 Netdiscover

Nmap työkalulla voimme skannata kohteesta avonaisia portteja, käyttöjärjestelmää, sekä palveluita, joita kohde mahdollisesti tarjoaa. Skannauksen tulosteesta voimme nähdä, että käyttöjärjestelmänä on Linux ja avoimia portteja on 22/tcp, jossa on koneen SSH-palvelu.

```

root@kali:~# nmap -A 194.154.65.11

Starting Nmap 7.40 ( https://nmap.org ) at 2017-11-01 13:33 EDT
Nmap scan report for 194.154.65.11
Host is up (0.00036s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      (protocol 2.0)
| fingerprint-strings:
|_  NULL:
|_  SSH-2.0-OpenSSH_7.4p1 Ubuntu-10
|_  ssh-hostkey:
|_    2048 d6:b4:13:6e:cc:6f:6d:de:0f:32:16:bb:1f:fe:a5:c2 (RSA)
|_    256 8a:06:db:4c:94:6f:80:df:88:75:93:16:0d:b4:d4:c4 (ECDSA)
|_ 1 service unrecognized despite returning data. If you know the service/version, please submit
|_ /cgi-bin/submit.cgi?new-service :
SF-Port22-TCP:V=7.40%I=7%D=11/1%Time=59FA0570%P=x86_64-pc-linux-gnu%r(NULL
SF:;20,"SSH-2\0-OpenSSH_7\4p1\x20Ubuntu-10\n");
MAC Address: 08:00:27:C7:E5:18 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.6 (97%), Linux 3.16 (95%), ASUS RT-N56U WAP (Linux 3.4
), Android 5.0 - 5.1 (93%), Linux 3.2 - 3.16 (93%), Linux 3.4 - 3.10 (93%), Linux 4.4 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.37 ms  194.154.65.11

OS and Service detection performed. Please report any incorrect results at https://nmap.org.
Nmap done: 1 IP address (1 host up) scanned in 22.46 seconds
root@kali:~#

```

Kuvio 39 Nmap kohteeseen

12.2 ARP-spoof

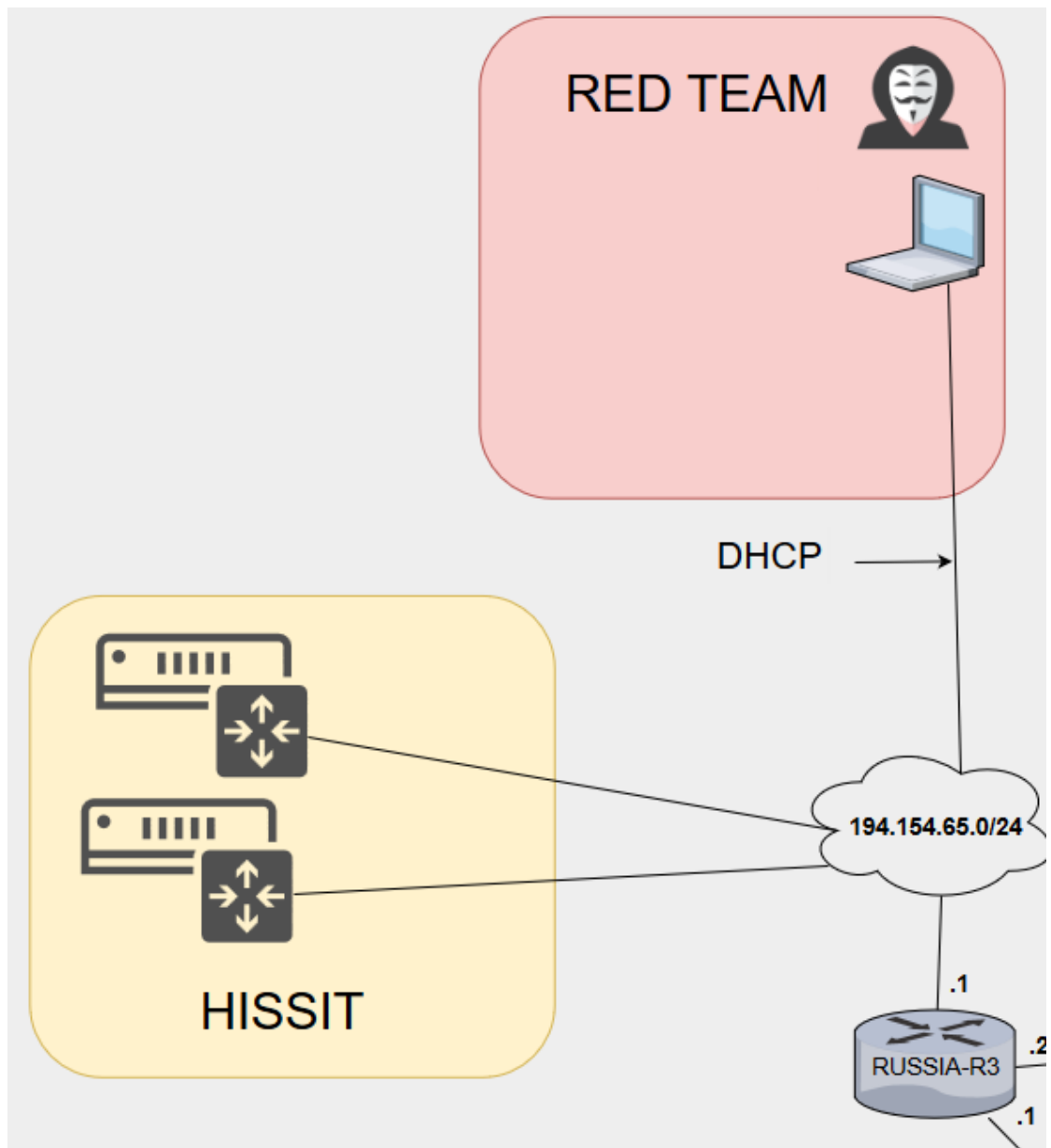
ARP-spoofin tarkoituksena on kertoa hyökkäyksen kohteelle väärä yhdyskäytävän osoite. Tämä mahdollistaa sen, että kaikki uhrin liikenne saadaan reititettyä hyökkääjän koneelle. Jotta hyökkäys olisi huomaamaton niin hyökkääjän on uudelleenreititettävä kohteen liikenne takaisin verkkoon. Tämä onnistuu laittamalla hyökkääjän koneella IP-forwarding päälle.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sysctl -p /etc/sysctl.conf
net.ipv4.ip_forward = 1
root@kali:~#

```

Kuvio 40 IP-Forwarding



Kuvio 41 Looginen kuva hyökkäyksen verkosta

ARP-spoof on varmasti yksi helpoimmista hyökkäyksistä Kali Linuxilla. Tarvitsee vain kertoa ohjelmalle kohteen IP-osoite sekä yhdyskäytävä.

```
root@kali:~# arpspoof -i eth0 -t 194.154.65.11 -r 194.154.65.1
```

Kuvio 42 ARP-spoof komento

Hyökkääjän kone lähettää kohteelle ARP-REPLY viestejä sanoen, että IP-osoite 194.154.65.1 löytyy MAC-osoitteesta 8:0:27:a4:6e:6b, joka onkin hyökkääjän oma MAC-osoite. Tällöin kohde luulee, että hänen yhdyskäytävä on kyseisessä MAC-osoitteessa, vaikka oikeasti ei ole.

```

root@kali:~# arpspoof -i eth0 -t 194.154.65.11 -r 194.154.65.1
8:0:27:a4:6e:6b 8:0:27:c7:e5:18 0806 42: arp reply 194.154.65.1 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:33:b:8e 0806 42: arp reply 194.154.65.11 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:c7:e5:18 0806 42: arp reply 194.154.65.1 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:33:b:8e 0806 42: arp reply 194.154.65.11 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:c7:e5:18 0806 42: arp reply 194.154.65.1 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:33:b:8e 0806 42: arp reply 194.154.65.11 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:c7:e5:18 0806 42: arp reply 194.154.65.1 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:33:b:8e 0806 42: arp reply 194.154.65.11 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:c7:e5:18 0806 42: arp reply 194.154.65.1 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:33:b:8e 0806 42: arp reply 194.154.65.11 is-at 8:0:27:a4:6e:6b

```

Nyt kaikki kohteen liikenne kiertää hyökkääjän koneen kautta. Hyökkääjä voi nyt tutkia verkkoliikennettä ja manipuloida paketteja mielivaltaisesti. Wireshark ohjelmalla hyökkääjä voi kuunnella verkkoliikennettä ja nähdä vaikkapa millä sivustoilla kohde vierailee. Kohde lähettää paljon tietoa TCP protokollan yli porttiin 8888 osoitteeseen 62.106.4.2. Koska liikenne on koko ajan samankaltaista niin halumme varmasti tietää mitä tietoa kone lähettää.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
Apply a display filter ... <Ctrl-/>							
No.	Time	Source	Destination	Protocol	Length	Info	
43	11.698065896	194.154.65.11	62.106.4.2	TCP	74	49176 → 8888	[SYN]
45	11.700134206	194.154.65.11	62.106.4.2	TCP	66	49176 → 8888	[ACK]
46	11.700137669	194.154.65.11	62.106.4.2	TCP	161	49176 → 8888	[PSH,
47	11.700266770	194.154.65.11	62.106.4.2	TCP	66	49176 → 8888	[FIN,
50	11.701466144	194.154.65.11	62.106.4.2	TCP	66	49176 → 8888	[ACK]
51	13.702838073	194.154.65.11	62.106.4.2	TCP	74	49178 → 8888	[SYN]
53	13.704452786	194.154.65.11	62.106.4.2	TCP	66	49178 → 8888	[ACK]
54	13.704694007	194.154.65.11	62.106.4.2	TCP	161	49178 → 8888	[PSH,
55	13.704697107	194.154.65.11	62.106.4.2	TCP	66	49178 → 8888	[FIN,
58	13.706648220	194.154.65.11	62.106.4.2	TCP	66	49178 → 8888	[ACK]
59	15.706989730	194.154.65.11	62.106.4.2	TCP	74	49180 → 8888	[SYN]
60	15.708556132	62.106.4.2	194.154.65.11	TCP	74	8888 → 49180	[SYN,
61	15.708726838	194.154.65.11	62.106.4.2	TCP	66	49180 → 8888	[ACK]
62	15.709020078	194.154.65.11	62.106.4.2	TCP	160	49180 → 8888	[PSH,
63	15.709023885	194.154.65.11	62.106.4.2	TCP	66	49180 → 8888	[FIN,
64	15.709908659	62.106.4.2	194.154.65.11	TCP	66	8888 → 49180	[ACK]
65	15.709912813	62.106.4.2	194.154.65.11	TCP	66	8888 → 49180	[FIN,
66	15.710152685	194.154.65.11	62.106.4.2	TCP	66	49180 → 8888	[ACK]
67	17.711873166	194.154.65.11	62.106.4.2	TCP	74	49182 → 8888	[SYN]
68	17.713214550	62.106.4.2	194.154.65.11	TCP	74	8888 → 49182	[SYN,
69	17.713292266	194.154.65.11	62.106.4.2	TCP	66	49182 → 8888	[ACK]
70	17.714687983	194.154.65.11	62.106.4.2	TCP	161	49182 → 8888	[PSH,
71	17.714694394	194.154.65.11	62.106.4.2	TCP	66	49182 → 8888	[FIN,
72	17.714695899	62.106.4.2	194.154.65.11	TCP	66	8888 → 49182	[ACK]
73	17.714696699	62.106.4.2	194.154.65.11	TCP	66	8888 → 49182	[FIN,
74	17.714836628	194.154.65.11	62.106.4.2	TCP	66	49182 → 8888	[ACK]
75	19.716123845	194.154.65.11	62.106.4.2	TCP	74	49184 → 8888	[SYN]

Kuvio 43 TCP-paketit

Kun tutkii paketteja tarkemmin, niin voimme huomata, että TCP PSH, ACK paketeissa on selkokieleistä dataa. Tämä data saattaa kiinnostaa hyökkääjää. sss

No.	Time	Source	Destination	Protocol	Length	Info
52	13.704308135	62.106.4.2	194.154.65.11	TCP	74	8888 → 49178 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
56	13.705767739	62.106.4.2	194.154.65.11	TCP	66	8888 → 49178 [ACK] Seq=1 Ack=96 Win=29056 Len=0
57	13.706423186	62.106.4.2	194.154.65.11	TCP	66	8888 → 49178 [FIN, ACK] Seq=1 Ack=97 Win=29056 Len=0
51	13.702838073	194.154.65.11	62.106.4.2	TCP	74	49178 → 8888 [SYN] Seq=0 Win=29200 Len=0 MSS=146
53	13.704452786	194.154.65.11	62.106.4.2	TCP	66	49178 → 8888 [ACK] Seq=1 Ack=1 Win=29312 Len=0
54	13.704694007	194.154.65.11	62.106.4.2	TCP	161	49178 → 8888 [FSH, ACK] Seq=1 Ack=1 Win=29312 Len=0
55	13.704697107	194.154.65.11	62.106.4.2	TCP	66	49178 → 8888 [FIN, ACK] Seq=96 Ack=1 Win=29312 Len=0
58	13.706648220	194.154.65.11	62.106.4.2	TCP	66	49178 → 8888 [ACK] Seq=97 Ack=2 Win=29312 Len=0

▶ Frame 54: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits) on interface 0
 ▶ Ethernet II, Src: PcsCompu_c7:e5:18 (08:00:27:c7:e5:18), Dst: PcsCompu_33:0b:8e (08:00:27:33:0b:8e)
 ▶ Internet Protocol Version 4, Src: 194.154.65.11, Dst: 62.106.4.2
 ▶ Transmission Control Protocol, Src Port: 49178, Dst Port: 8888, Seq: 1, Ack: 1, Len: 95
 ▶ Data (95 bytes)
 Data: 456c657661746f722049443a2031207c204275696c64696e...
 [Length: 95]

Wireshark · Follow TCP Stream (tcp.stream eq 6) · wireshark_eth0_20171101134728_InHqzd

Elevator ID: 1 | Building: Dynamo | Current Floor: 4 | Temperature: 17 Celsius | Weight: 297 kg

Kuvio 44 TCP Selkokielineen data

12.3 DoS

DoS (Denial of Service) eli palvelunestohyökkäys.

```
root@kali:~# apt-get install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
```

```
root@kali:~# pip3 install slowloris
Collecting slowloris
  Downloading Slowloris-0.1.4.tar.gz
Building wheels for collected packages: slowloris
  Running setup.py bdist_wheel for slowloris ... done
  Stored in directory: /root/.cache/pip/wheels/90/2e/a2/3d922f47834fd9ceb7bd499a31fld6c5e9c3e8824888c8a4f
Successfully built slowloris
Installing collected packages: slowloris
Successfully installed slowloris-0.1.4
root@kali:~#
```

13 Harjoituksen säännöt

- Punainen tiimi ei suorita hyökkäyksiä omin päin vaan etenee ohjeiden mukaisesti.
- Sininen tiimi ei estä liikennettä palomuurista ilman syytä.
- Jokainen tiimi pelaa oman roolinsa mukaisesti.
- Tiimin on oltava jatkuvasti toimintavalmiudessa.
- Tiimikohtaiset säännöt löytyvät tarkemmin tiimien omista ohjeistuksista.
- Valkoinen tiimi ohjeistaa.
- Matkapuhelimien käyttö harjoituksen aikana on kielletty!

14 Harjoituksen arviointi

Valkoinen tiimi arvioi harjoituksen onnistumista seuraavien kohtien perusteella:

- Onnistutaanko ratkaisemaan ongelmat, joita tulee vastaan
- Huomataanko ongelmia
- Millä tavalla ongelmiin reagoitiin, kun ne huomataan
- Kuinka kauan reagoimiseen meni aikaa
- Miten yrityksen toiminta jatkui ongelmien aikana
- Voidaanko yrityksen tietoturvaa parantaa
- Millä osa-alueilla henkilöstön osaamista pystytään parantamaan
- Onnistuttiinko parantamaan yrityksen valmiutta toimia ongelmatilanteissa
- Saatiinko harjoitus toteutettua halutulla tavalla

15 Pohdinta

Mielestämme harjoituksen suunnitteleminen onnistui hyvin ja vaadittuihin tavoitteisiin päästiin. Harjoituksen suunnitteluun ja tekniseen toteutukseen kului paljon aikaa ja vaivaa joka näkyy myös osittain dokumentissa. Kaikkien palveluiden dokumentaatioita ei saatu vielä dokumenttiin näkyville mutta ympäristö voi puhua puolestaan. Harjoituksen suunnitteleminen oli todella mielenkiintoista ja opettavaista.

16 Viitteet

Viite 1. How Will the Internet of Things Be Leveraged to Ruin Your Company's Day? Understanding IoT Security <https://securityintelligence.com/will-internet-things-leveraged-ruin-companys-day-understanding-iot-security/>

Viite 2. IoT-bottiverkot etsivät aktiivisesti internetiin kytkettyjä laitteita <https://www.viestintavirasto.fi/kyberturvallisuus/tietoturva-nyt/2016/10/ttn201610181402.html>

Viite 3. New 'BrickerBot' malware attack kills unsecured Internet of Things devices <https://www.digitaltrends.com/computing/brickerbot-malware-targets-iot-with-pdos-attacks/>

17 Liitteet

Liite 1. Perehdyttämismateriaali_Masiina.pptx

Liite 2. Sinisen tiimin toimintaohjeet

Liite 3. Punaisen tiimin toimintaohjeet