Harjoitussuunnitelma

Kyberharjoituksen suunnittelu ja valmistelu TTV15S6

Laaksonen Sebastian

Lajunen Anni

Martikainen Sergey

Ratas Aapo

Sundberg Jon

09/2017

Tieto- ja viestintätekniikka

Sisällysluettelo

[Versiohallinta 4](#_Toc500963773)

[Kuviot 5](#_Toc500963774)

[1 Johdanto 6](#_Toc500963775)

[1.1 Harjoituksen toiminta-ajatus ja käytettävä harjoitusmuoto 6](#_Toc500963776)

[1.2 Harjoituksen tavoitteet 6](#_Toc500963777)

[1.3 Rajaukset 7](#_Toc500963778)

[1.4 Osallistujat ja tehtävät 7](#_Toc500963779)

[1.4.1 Blue team 7](#_Toc500963780)

[1.4.2 Red team 8](#_Toc500963781)

[1.4.3 White team 9](#_Toc500963782)

[1.4.4 Green team 9](#_Toc500963783)

[2 Suunnittelu 10](#_Toc500963784)

[2.1 Suunnittelun aikataulu 10](#_Toc500963785)

[2.2 Suunnitteluryhmän kokoonpano ja tehtävät 10](#_Toc500963786)

[2.3 Harjoitustoiminnan suunnittelu 10](#_Toc500963787)

[2.3.1 Harjoituksen hallinnan suunnittelu 10](#_Toc500963788)

[2.3.2 Vaatimukset ja kuvaukset ympäristölle 11](#_Toc500963789)

[2.3.3 Tiedottaminen 11](#_Toc500963790)

[2.3.4 Rajapinnat 12](#_Toc500963791)

[2.3.5 Pelaavien tiimien perehdyttäminen 12](#_Toc500963792)

[2.3.6 Mahdolliset aikahypyt 12](#_Toc500963793)

[2.3.7 Riskien hallinta 12](#_Toc500963794)

[2.3.8 Tiedon välitys, säilytys ja ryhmätyötila 12](#_Toc500963795)

[2.3.9 VIP-vieraat 13](#_Toc500963796)

[2.3.10 Pääsy ympäristöön, lupien anominen 13](#_Toc500963797)

[3 Harjoituksen ajankohta 13](#_Toc500963798)

[4 Harjoituksen toteutus 14](#_Toc500963799)

[4.1 Blue teamin tehtävät 14](#_Toc500963800)

[4.1.1 IT-palvelut 14](#_Toc500963801)

[4.1.2 Pankin johto 14](#_Toc500963802)

[4.1.3 Pankin markkinointi ja tiedotuspalvelut 14](#_Toc500963803)

[4.1.4 Pankin asiakaspalvelu 14](#_Toc500963804)

[4.1.5 Asiakkaat 15](#_Toc500963805)

[4.2 Punaisen tiimin tehtävät 15](#_Toc500963806)

[4.3 Skenaario 15](#_Toc500963807)

[4.3.1 Taustakertomus 16](#_Toc500963808)

[4.3.2 Uhkatoimijat 16](#_Toc500963809)

[4.3.3 Uhkatoimijoiden toimenpiteet 16](#_Toc500963810)

[4.4 Pelitapahtumat 17](#_Toc500963811)

[4.5 Pelisyötteet 17](#_Toc500963812)

[5 Harjoitusympäristö 18](#_Toc500963813)

[5.1 Verkko-topologia 18](#_Toc500963814)

[5.2 Järjestelmien käyttötarkoitukset ja ohjeet 18](#_Toc500963815)

[5.3 Työkalut ja järjestelmät 19](#_Toc500963816)

[5.3.1 pfSense 19](#_Toc500963817)

[5.3.2 Bind9 19](#_Toc500963818)

[5.3.3 Web server (Pankin sivusto) 19](#_Toc500963819)

[5.3.4 Chat palvelu 19](#_Toc500963820)

[5.3.5 Käyttöjärjestelmät 19](#_Toc500963821)

[6 Harjoituksen arviointi 21](#_Toc500963822)

[7 Harjoituksen säännöt 21](#_Toc500963823)

[8 Perehdyttämissuunnitelma 21](#_Toc500963824)

[8.1 Yleisjärjestelyt 21](#_Toc500963825)

[8.2 Harjoitustavoitteet 22](#_Toc500963826)

[8.3 Taustakertomus 22](#_Toc500963827)

[8.4 Roolit 22](#_Toc500963828)

[8.4.1 White team & Green team 22](#_Toc500963829)

[8.4.2 Blue team 22](#_Toc500963830)

[8.4.3 Red team 22](#_Toc500963831)

[8.5 Harjoituksen säännöt 22](#_Toc500963832)

[8.6 Tekninen toimintaympäristö 23](#_Toc500963833)

[8.7 Turvallisuus 23](#_Toc500963834)

Versiohallinta

|  |  |  |
| --- | --- | --- |
| Mitä on tehty | PVM | Versio |
| Suunnitelman alustus | 14.9.2017 | 0.1 |
| Lisätty versionhallinta ja muokattu tekstejä | 21.9.2017 | 0.1.1 |
| Suunnittelun eteneminen | 21.9.2017 | 0.1.2 |
| Lisätty ”2 Suunnittelu” alle 2.4 harjoitustoiminnan suunnitteluosuudet | 27.9.2017 | 0.2 |
| Muokattu 4.2 Skenaariota | 27.9.2017 | 0.21 |
| Muita muutoksia dokumenttiin sekä toimintaan |  | 0.3 |
| Dokumentin valmistaminen palauteelle, sekä tarkistamiselle. | 07.11.2017 | 0.5 |
| Perehdyttämissuunnitelman lisäys | 10.11.2017 | 0.6 |
| Korjattu Karon antamien kommenttien mukaan dokumenttia | 11.12.2017 | 0.7 |
| Valmisteltu dokumentaatiota | 13.12.2017 | 0.8 |
| Dokumentin julkaisu | 13.12.2017 | 1.0 |

# Kuviot

Kuvio 1. Organisaatiokaavio

Kuvio 2. Verkkotopologia

# Johdanto

## Harjoituksen toiminta-ajatus ja käytettävä harjoitusmuoto

Harjoituksen ajatuksena on valmentaa harjoitukseen osallistujat työelämän mahdollisia ongelmatilanteita vastaan. Harjoituksessa tullaan kuvaamaan realistisia uhkia ja toimintatapoja niitä vastaan.

Harjoitus toteutetaan teknistoiminnallisena harjoituksena jolloin se vastaa realistisesti työelämän tarpeisiin.

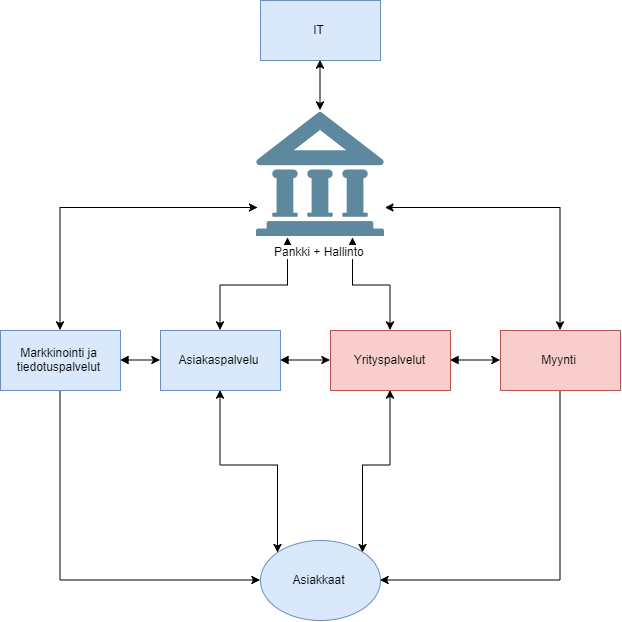
## Harjoituksen tavoitteet

Tavoitteita:

1. Epäilyttävien sähköpostien tunnistaminen ja toimiminen tilanteen vaativalla tavalla. Esim. pankin työntekijä ottaa yhteyttä it-asiantuntijapalveluun pankin sisäisessä chatissa (slack/whatsapp/telegram vast.)
2. Harjoituttaa henkilöstöä kriittisissä olosuhteissa.
3. Järjestäjien harjoituttaminen tuleviin kyberharjoituksiin (suunnittelu, johtaminen, palaute, jne.)
4. Osallistujien yhteistyön parantaminen, sekä organisaation sisäinen viestintä.

## Rajaukset

* Harjoituksen kesto maksimissaan kolme tuntia
* Teknistoiminnallinen harjoitus
* Sinisellä harjoitukseen osallistuvat ja punaisella ei osallistuvat (ks. Kuvio 1)



Kuvio 1. Organisaatiokaavio

## Osallistujat ja tehtävät

Osallistujat on kuvattu alapuolella tiimeittäin tehtävineen ja tiimin kokoineen.

### Blue team

Blue teamiin osallistuu organisaatiokaavion mukaiset osastot yrityksestä ja ne on kuvattu tarkemmin alla.

* IT (BT 1)
  + Pankin IT-tuki muille työntekijöille, palvelinylläpito ja tietoturvapalvelut
  + Tiimin koko on neljä henkilöä. Jokaisella oma työpiste.
* Markkinointi & tiedotuspalvelut (BT 2)
  + Vastaa pankin tiedotuksesta ja markkinoinnista. Ylläpitää imagoa.
  + Tiimin koko yksi – kaksi henkilöä harjoitukseen osallistuvien määrästä riippuen. Yksi työpiste.
* Asiakaspalvelu (BT 3)
  + Kosketuspinnassa pankin asiakkaisiin. Välittää IT-osastolle tikettejä.
  + Tiimin koko yksi – kaksi henkeä. Yksi työpiste.
* Asiakkaat (BT4)
  + Pankin asiakkaat kuvaavat päivittäistä toimintaa ja käyttävät pankin päivittäisiä palveluja.
  + Tiimin koko kolme henkeä. Kolme työpistettä.
* Hallinto (BT 5)
  + Pankin johto, tekevät päätöksiä ja organisoivat pankin toimintaa.
  + Tiimin koko yksi – kolme henkeä. Yksi työpiste.

### Red team

Hyökkäävä osasto. Koostuu harjoittelevista joukoista. Pankin korruptoitunut työntekijä ja joukko, joka vastaanottaa tiedot ja organisoi hyökkäyksen. Red teamiin kuuluu.

Tiimin koko kaksi – kolme henkeä. Yksi työpiste.

### White team

Järjestävä taho. Organisoi ja suunnittelee harjoituksen. Valvoo harjoitusta.

Tiimin koko viisi henkeä.

### Green team

Vikojen korjaukset harjoituksen aikana, kuten fyysisen laitteen hajoaminen.

Tiimin koko kaksi henkeä.

# Suunnittelu

## Suunnittelun aikataulu

Suunnittelu aloitettiin perehtymällä omaan aihealueeseen ja jakamalla karkeat vastuut harjoitussuunnitelmasta. Ensimmäisten versioiden jälkeen kirkastettiin ymmärrystämme verkon vaatimuksista, sekä alettiin hioa syötteitä ja aikatauluja, sekä tiimien kokoonpanoja ja alustavia kokoluokkia kohdilleen saadaksemme kuvan siitä, minkä kokoinen harjoitus tulee olemaan.

Teknistä suunnittelua alettiin toteuttaa verkon ja palveluiden määrittelyn muodossa. Samalla tarkentuivat syötteet, harjoituksen kulku ja laajuus. Hioimme white-tiimin tehtäviä ja keskustelimme ympäristön vaatimuksista.

## Suunnitteluryhmän kokoonpano ja tehtävät

Tämän harjoituksen on suunnitellut kyberharjoituksen suunnittelun ja toteutuksen vuoden 2017 toteutuksen ryhmä numero 7: Sebastian Laaksonen, Sergey Martikainen, Aapo Ratas, Jon Sundberg ja Anni Lajunen. Ryhmä toimii harjoituksen aikana white-tiiminä, joka valvoo harjoituksen kulkua.

White team toimii harjoituksen valvojana, joten se ei varsinaisesti osallistu harjoituksen toteutukseen kuin harjoituksen teknisenä tukena (nk. green team), ohjeistusten ja uutisten välitysten myötä.

## Harjoitustoiminnan suunnittelu

Harjoitustoiminnan suunnittelussa otetaan huomioon kaikki rajapinnat, mitkä harjoituksessa ovat oleellisessa asemassa.

### Harjoituksen hallinnan suunnittelu

Suunnittelijatiimi jaetaan tehtäviin, jolloin harjoituksen aikana jokainen suunnittelijoista pystyy keskittymään omaan alueensa ja johtamaan harjoitusta parhaalla mahdollisella tavalla.

Harjoituksen hallinnan suunnittelu kestää koko suunnittelun ajan, jolloin voidaan tarvittaessa tehdä muutoksia.

Esim. Punaisen tiimin hyökkääjälle annetaan kattavat ohjeet mitä tehdä alusta loppuun.

Mahdolliset käyttöohjeet tehdään tarvittaessa myös muille prosesseille, esim. miten verkon saa ylös.

### Vaatimukset ja kuvaukset ympäristölle

Harjoitus toteutetaan yhdessä tilassa jakaen tila pelattavien tiimien mukaan työpisteisiin. Red team ja white team sijoitetaan tilan perälle, ettei blue team vahingossakaan näe näiden tiimien tapahtumia.

Työntekijät käyttävät Mattermost – chattipalvelua, joka on konfiguroitu yrityksen verkkoon.

Asiakkaille on saatavilla tiketti-järjestelmä.

Operaattori toimii kyseisessä harjoituksessa joko kahtena työntekijänä, jotka ovat käymässä toimistolla tai puhelimen soiton päässä oleva tuki.

IT-palvelut hoitavat päivityksiä järjestelmiin, verkkovalvontaa ja muuta harjoituksen aikana.  Tarvittaessa tehdään dokumentointia sille, mitä pitää monitoroida.

IT-palveluiden työtilassa on tietokoneita, joissa on valvontatyökalut valmiina, sekä niillä pitää voida valvoa verkkoympäristöä.

### Tiedottaminen

* White team hoitaa tiedottamisen blue -ja red-teamille. Ilmoituksissa tiedotetaan tehtävässä ilmenevät muutokset ja uutiset. Whiteteam ei muuten puutu tehtävän etenemiseen, kuin ilmoitusten kautta.
* Aikataulu täsmentyy tehtävän lopullisen version mukaan. Aluksi whiteteam antaa molemmille (blue & red) tiimille ohjeet tehtävän aloittamiseksi. Kesken harjoituksen white team antaa tarvittaessa ilmoitusten avulla ohjeita ja muutoksia tehtävän edetessä. Lopuksi white-team antaa ilmoituksen, kun tehtävä on päättynyt.

### Rajapinnat

Blue- ja red-team eivät ole kontaktissa toisiinsa. Pankki on kontaktissa asiakkaisiin asiakaspalvelun, sekä sähköpostin kautta. Red-team on yhteydessä pankkiin internetin välityksellä, ja blue-team on pankin sisällä. Blue tiimillä on pääsy intranettiin.

### Pelaavien tiimien perehdyttäminen

Tiimit perehdytetään paikan päällä ennen harjoitusta. Blue teamille perehdytetään käyttöympäristö, sekä toimenkuva.

Red teamille perehdytetään blue teamin käytössä oleva tunnettu ympäristö, sekä suunnitellut hyökkäykset, tapahtumien kulku, sillä laajuudella, kuin hyökkäyksen toteuttaminen vaatii. Red teamille annetaan myös ohjeistus hyökkäystyökalujen käyttämiseen, sekä dokumentti, jonka pohjalta suoritetaan tarvittavat komennot.

### Mahdolliset aikahypyt

Tässä harjoituksessa ei ole aikahyppyjä.

### Riskien hallinta

Riskejä pyritään hallitsemaan testaamalla ympäristöjen toimivuus, sekä perehdyttämällä osallistujat kunnolla ja ajoittamalla harjoitus hyvin (tauotus, tarvittavat energianlähteet saatavilla) . Kaiken varalta paikalla on myös ylimääräistä kalustoa (koneita).

### Tiedon välitys, säilytys ja ryhmätyötila

Harjoitussuunnitelman versiot palautetaan viikoittain Optimaan ryhmän työtilaan. Lisäksi JAMK:n opiskelijoiden sähköpostin yhteydessä olevassa OneDrivessä on ryhmällä yhteinen jaettu kansio, jossa säilytetään kaikkia harjoituksen suunnitteluun liittyviä dokumentteja ja luonnosversiota. Projektipäällikkö on viikoittain vastuussa siitä, että uusi versio harjoitussuunnitelmasta ja viikkoraportti palautetaan viikoittain Optimaan.

Harjoituksen aikana tietoa välitetään pääasiassa uutisten ja perehdytyksen kautta. Tarvittaessa jaettavat dokumentit jaetaan tarvittaessa harjoituksessa käytettävän verkon yli.

Ryhmätyötilassa on jokaisella kaikkiin dokumentteihin muokkausoikeus, mutta varmistetaan, että word onlinen toimivuus, sillä että lisättävät tiedostot viedään tekstitiedostoina OneDriveen ja projektipäällikkö vuorottain täyttää ne pohjaan, että versionumerointi ei mene sekaisin, eikä tietoa huku.

Ryhmä työskentelee pääsääntöisesti itsenäisesti tai koululla vapaana olevissa luokissa. Lisäksi etänä yhteyttä pidetään WhatsApp-ryhmää ryhmäläisten kesken, sekä tarkoitukseen sopivaa puheyhteydellistä sovellusta, kuten Skype tai Discord.

### VIP-vieraat

Harjoituksen aikana mahdollisesti vierailevien VIP-vieraiden vierailu ei saa häiritä harjoitusta millään tavalla, koska harjoituksen aika on muutenkin lyhyt. Mahdollisille VIP-vierailla osoitetaan vierailusta vastaava henkilö, jolla on harjoituksen aikataulu tiedossa. Vieraat voivat seurata harjoitusta häiritsemättä sitä millään lailla paikan päällä, ja harjoituksen tauon aikana järjestetään tilaisuus esittää kysymyksiä. Vieraista vastaavan tehtävä on huolehtia vierailun aikataulu siten, että kyseiset toiminnot onnistuvat harjoitusta häiritsemättä.

### Pääsy ympäristöön, lupien anominen

Pankin palvelinhuoneeseen pääsyn luvat on merkattu ”huoltotyöksi”, jonka avulla verkko päästään saastuttamaan.

# Harjoituksen ajankohta

Harjoitus toteutetaan kahtena ajankohtana: harjoituksen perehdytys tapahtuu 16.11. klo 14.15 alkaen ja harjoitus toteutetaan 23.11. klo 14.15 alkaen.

Perehdytyspäivänä käydään nopeasti läpi harjoituksen keskeisimmät asiat ja varsinaisena toteutuspäivänä harjoitustilaan tullessa jaetaan osallistujille arvalla roolit, kuka toimii missäkin roolissa ja ohjeistus tarpeen ja roolin mukaan. Alussa osallistujat saavat tutustua ja lukea roolinsa läpi ennen kuin harjoitus alkaa.

Harjoituksen toteutukseen on aikaa maksimissaan kolme tuntia ja seuraavalla viikolla käydään läpi harjoituksen onnistuminen kokonaisuudessaan.

# Harjoituksen toteutus

## Blue teamin tehtävät

Alla on avattu blue –teamin tehtävät yksityiskohtaisesti.

### IT-palvelut

Valvovat yrityksen verkkoa, sekä web-sivustoa ja tekevät ylläpitotoimenpiteitä ja palvelinylläpitoa sekä korjaavat mahdollisia virhetilanteita. Vastaavat pankin sähköisten palveluiden toiminnasta.

### Pankin johto

Johtaa pankin työntekijöiden toimintaa ja tekee harjoituksen aikana päätöksiä esimerkiksi tiedottamisesta. Vastaa viimeisenä kaikesta toiminnasta ja kantaa vastuun toimenpiteistä.

### Pankin markkinointi ja tiedotuspalvelut

Ilmoittaa lehdistölle pankin uusista palveluista ja laatii vikatiedotteita vian pitkittyessä. Ylläpitävät pankin imagoa.

### Pankin asiakaspalvelu

Vastaa asiakkaiden yhteydenottoihin. Tekevät tikettejä asiakkaiden ilmoitusten mukaan. Käytössä on tikettijärjestelmä, sähköposti, sekä chatti-palvelu.

### Asiakkaat

Kuvaavat normaalia asiakaskäyttäytymistä pankille. Kun asiakkaat huomaavat, ettei pankin verkkosivu toimi, aloittavat pommittamaan erilaisia kanavia pitkin pankin asiakaspalvelua, sekä yrittävät päästä pankin sivustolle. Asiointi pankin verkkosivujen kautta pääsääntöisesti.

## Punaisen tiimin tehtävät

Hyökätä pankin sivustolle, ja pyrkiä saamaan se alas ja pitää alhaalla hämäyksen vuoksi tarpeeksi pitkään.

Varastaa sisäiseltä palvelimelta tietokannan asiakastiedoista korruptoituneen työntekijän avustuksella.

## Skenaario

Normaali jokapäiväinen toiminta. Uutisissa on ollut viime aikoina joitakin mainintoja erilaisista hakkeriryhmistä ja Pankki onkin ohjeistanut IT-tiimiä tarkistamaan verkkohyökkäyksien varalta ilmoituksia tarkemmin, kuin ennen.

Pankin johto lähettää viestin työntekijöille, että lähipäivinä tulee lisäinfoa mahdollisista koulutuksista/erillisohjeista. Samaan aikaan pankin järjestelmäasiantuntija, jolla on pääsy serverihuoneeseen, jossa sijaitsee mm. asiakasrekisteripalvelimet, lähettää ennalta valitsemalle työntekijälle sähköpostiviestin otsikolla ”Ohjeet sähköpostiviestien vastaanottamiseen”. Viesti sisältää liitteenä word-tiedoston, johon on kuitenkin koodattu haittaohjelma mukaan.

Pahaa-aavistamaton työntekijä avaa tiedoston, lataa sen koneelleen ja sallii muokkaamisen. Tällöin haittaohjelma lähtee leviämään asiakaspalvelun verkossa, aiheuttaen massiivisen bottiverkon kautta ohjatun DDoS-hyökkäyksen. Haittaohjelma avaa myös vaivihkaa VPN-tunnelin koneelta ulkoverkkoon.

Tämän seurauksena pankin asiakaspalvelu ruuhkautuu pahasti, koska mitkään pankin verkkopalvelut ei toimi ja koko IT-puolen väki joutuu paiskimaan töitä suurella tahdilla. Aiemmin mainittu järjestelmäasiantuntija menee serverihuoneeseen, ja korjatessaan ongelmia imuroi samalla vaivihkaa koko pankin asiakasrekisterin. Normaalisti serverihuoneessa työskentelee aina kaksi ihmistä yhtä aikaa, mutta poikkeustilanteessa järjestelmäasiantuntija päästetään yksin serverihuoneeseen, jolloin pystyy pyyhkimään tiedot imuroinnista.

Tämän jälkeen järjestelmänasiantuntija väittää menevänsä korjaamaan ongelmaa aiemmin viattomaksi uhriksi valitun työntekijän tietokoneelle, ja lataa asiakastiedot VPN-yhteyden kautta rikostovereilleen, jotka saman tien käynnistävät massiivisen soittelu- ja pankkitunnustiedustelukampanjan pankin asiakkaille ja myyvät käyttökelpoiset tiedot eteenpäin kalliilla.

### Taustakertomus

Viime viikkoina on havaittu useita verkkohyökkäyksiä pankkeihin. Pankkeja on kehotettu olemaan tarkkana. Monen pankin toimintaa on hankaloitettu laajoilla palvelunestohyökkäyksillä, jotka vaikuttavat erittäin negatiivisesti pankin maineeseen jättäen asiakkaat pulaan, kun pankkipalvelut eivät toimi.

Suomipankissa työskentelevä järjestelmäasiantuntija on pahasti veloissaan ja tutustuessaan uusiin tuttaviin, keksii huimapäisen suunnitelman käyttää hyökkäysuutisia hyväkseen kuullessaan, paljon arkaluontoisesta datasta maksetaan esimerkiksi tor-verkossa.

### Uhkatoimijat

Rikollistiimi, joka haluaa hyötyä pankin tiedoilla pimeillä markkinoilla.

Korruptoitunut työntekijä, joka on sisäpiiriläinen rikollistiimissä, työskentelee IT-tuessa.

### Uhkatoimijoiden toimenpiteet

Red – tiimin tehtävänä on ohjeiden mukaisesti hyökätä pankin verkkosivustolle ja kaataa se. Sivuston pitää olla alhaalla harjoituksen päätökseen asti.

Korruptoitunut työntekijä on pankin IT-palveluiden yksi työntekijöistä, jonka tehtävänä on mennä serveri-tietokoneelle ja ladata muistitikulleen salaisen tietokannan, jonka jälkeen lähettää sen uhrikoneeksi valikoidun työaseman kautta sen VPN-yhteydellä red-tiimille.

## Pelitapahtumat

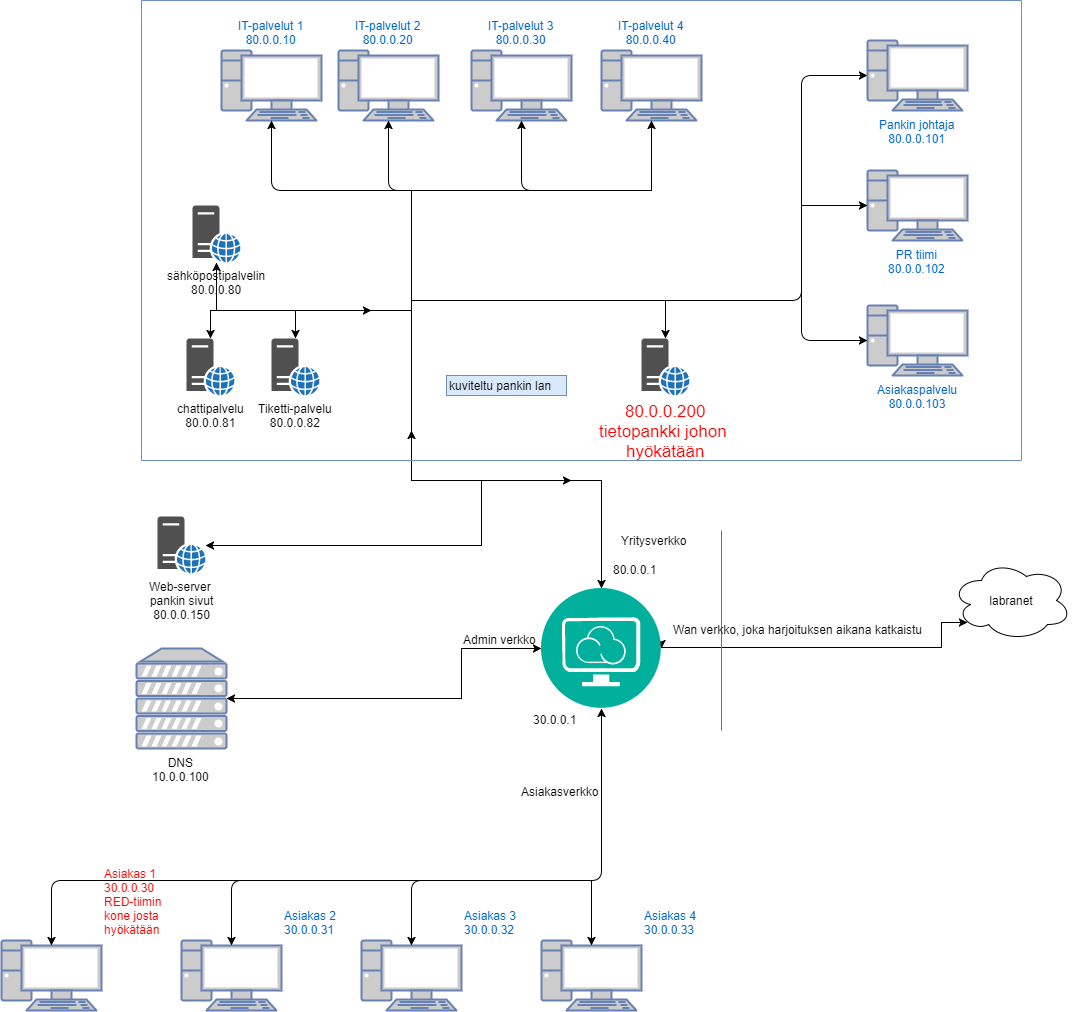
Pelitapahtumat käynnistyvät uutissyötteillä siitä, kuinka pankkeihin on hyökätty. Tämän jälkeen pankin johto ohjeistaa henkilökuntaa tulevan harjoituksen puitteissa, jota hyökkääjä käyttää hyväkseen. Hyökkääjä valitsee kohteen, lähettää sähköpostin joka sisältää saastuneen tiedoston. Tiedosto avaa vaivihkaa VPN-yhteyden RED-tiimille, joka tämän jälkeen käynnistää DDoS-hyökkäyksen, jolla kaadetaan pankin sivut. IT-tuen painiessa tämän ongelman kanssa ja asiakaspalvelun ruuhkautuessa hyökkääjä menee serverihuoneeseen korjaamaan tuhoja, jolloin samalla vaivihkaa imuroi pankin arkaluontoisia tietoja itselleen. Tämän jälkeen hyökkääjä menee ”korjaamaan” uhrin konetta ja lähettää tiedot RED-tiimille avatun VPN-yhteyden kautta. Lopuksi hyökkääjä siivoaa jälkensä minimoidakseen todisteet.

## Pelisyötteet

Syötteet on harjoitussuunnitelman liitteenä olevassa excel-taulukossa ajankulun mukaisessa kronologisessa järjestyksessä. Syötteissä on vielä toiminta, jos pelaajat eivät toimikkaan niin kuin oletetaan huolellisesta perehdytyksestä huolimatta.

# Harjoitusympäristö

## Verkko-topologia



Kuvio 2. Verkkotopologia.

## Järjestelmien käyttötarkoitukset ja ohjeet

Harjoituksessa kaikki osallistujat käyttävät Lubuntu –työasemia.

Selaimen kautta pankin työntekijät pääsevät käyttämään Chatti-palvelua (Mattermost) sisäiseen viestintään. Asiakaspalvelu käyttää tikettijärjestelmää ja sähköpostipalvelua viestinnässä asiakkaiden ja muiden pankin työntekijöiden kanssa.

Järjestelmien ohjeet löytyvät erillisinä liitteinä Optiman työtilasta.

## Työkalut ja järjestelmät

Kappaleessa kerrotaan miksi valittiin kukin järjestelmä tai työkalu kyseistä harjoitusta varten.

### pfSense

Harjoituksessa pfSense toimii eri verkkojen reitittimenä, sekä palomuurina niiden välille. Koska pfSensen asennus ja konfigurointi on suhteellisen helppoa, valittiin kyseinen työkalu sen takia.

### Bind9

Bind9 toimii harjoituksemme DNS:nä. Bind9 valittiin sen takia, koska tiimillä oli kokemusta sen aikaisemmasta käytöstä, sekä opettaja oli antanut omat ohjeet sen tekemiseen. Bind9

### Web server (Pankin sivusto)

Pankin verkkosivu luotiin linux-palvelimelle, jonka päälle asennettiin apache. Graafinen sivusto on luotu perinteiseksi html sivuksi. Linux-palvelin valittiin sen keveyden ja varmatoimisuuden takia.

### Chat palvelu

Harjoituksen chat -palveluna käytetään Mattermost sovellusta, joka on vapaasti ladattavissa verkosta. Mattermost asennettiin linux ympäristön päälle, jonka vuoksi käytimme harjoituksessa Debian käyttöjärjestelmää.

Debian valittiin sen kevyen käyttöliittymän puolesta. Debian on myös yleinen linux serveri myös yritysmaailmassa.

### Sähköposti

Sähköpostipalvelimena käytettiin Windows Server 2016:ta jonka päälle laitettiin hMailserver, joka mahdollistaa sähköpostin käytön sisäverkossa.

### Käyttöjärjestelmät

Kali Linux – helppo asentaa ja löytyy paljon valmiita työkaluja ja työkalukokonaisuuksia, jolloin dependencien asentaminen ei vie aikaa.

Lubuntu – koska harjoituksemme ympäristön laitteet ovat suhteellisen vanhoja ja tehottomia, lubuntu soveltuu hyvin käyttöympäristömme virtuaalikoneina siniselle tiimille.

Ubuntu server – käytetään web-serverin asennukseen, sekä DNS:än asentamiseen. Valittiin ubuntu, koska sen konfigurointi on hieman tutumpaa ja helpompaa verrattuna debian-pohjaisiin järjestelmiin.

Ubuntu Desktop – käytetään ainoastaan valkoisen tiimin kannettavassa tietokoneessa sitä varten, että päästään konfiguroimaan admin-verkkoa (esim. Pääsy pfsenseen).

### Tiketöintijärjestelmä (osTicket)

Tiketti järjestelmänä käytössä on siis Osticket, mikä on avoimen lähdekoodin tikettijärjestelmä. Palvelu on asennettu ubuntu serverille, jossa on myös asennettuna apache2, jonka rinnalla OsTicket toimii. Kyseessä on siis tikettijärjestelmä, johon saadaan yhteys verkkoselaimen kautta.

### Hyökkäystyökalu

Päätimme käyttää Slowloris- nimistä työkalua, koska sen asentaminen ja käyttäminen on todella helppoa. Ajatuksena harjoituksessamme ei ole tehdä siitä liian monimutkaista, joten Slowloris sopii hyvin käyttöömme.

### PKI - järjestelmä

Harjoitukseemme on myös suunniteltu Simple PKI - järjestelmän käyttö, jotta yhteys laitteen ja sivustojen välillä olisi salattu. Yksinkertaisen PKI järjestelmän asentaminen ei ole vaikeaa, mutta sen konfigurointi ja asentaminen sivustoille vie paljon aikaa, joten sitä ei varsinaisesti tuotu harjoitukseemme mukaan.

# Harjoituksen arviointi

Harjoituksen jälkeen kerätään osallistujilta palautetta siitä, mitä harjoituksessa kenenkin mielestä tapahtui, sekä siitä, kuinka hyvin kukakin omasta mielestään onnistui omassa roolissaan.

Arviointi tapahtuu osittain heti harjoituksen jälkeen, sekä osittain seuraavalla kerralla, jolloin puretaan harjoitus kokonaisuudessaan ja kerätään osallistujilta kehitysehdotuksia sekä onnistumisen paikkoja jatkokehitystä varten.

Arviointia varten tehdään verkkolomake, jossa käydään läpi jokainen osa-alue. Lomakkeessa on mahdollisuus vapaaseen sanaan, joka osassa on pakollinen.

# Harjoituksen säännöt

Harjoituksen säännöt luonnostellaan perehdytyksen suunnittelun yhteydessä (Ks. 8.5).

# Perehdyttämissuunnitelma

## Yleisjärjestelyt

Ennen harjoitusta on hyvä järjestää työtila niin, ettei harjoituksen alkaessa tarvitsisi eristää esim. pöytien välejä, jotta harjoittelijat pystyisivät paremmin uppoutumaan harjoitukseen.

Näkyvyys tilaan peitetään ulkoapäin. Harjoitukseen osallistuvat joukot järjestetään tilaan niin, ettei edelliseltä näytöltä voi luntata mitään kriittistä.

Joten perehdytyksen aikana järjestetään tarvittaessa pöydät paremmille paikoille (mikäli se on mahdollista), sekä asennetaan tarvittaessa sermit.

Harjoituksessa pidetään yhteinen organisoitu tauko, 15 minuuttia puolessa välissä harjoitusta.

## Harjoitustavoitteet

Harjoituksen tavoitteena on opettaa henkilöstöä eri aloilta käyttämään tietokoneita, sekä tutustua muiden työntekijöiden työhön.

Yhtenä tärkeimmistä tavoitteista on oppia tiedostamaan ja toimimaan, kun tilanne on päällä. Harjoituksessa kuitenkin tähän pääsee suurimmaksi osaksi vain sinisen tiimin IT-palvelut ja muun toiminnan osalta on tärkeää kommunikointi muiden kanssa.

Harjoituksen toinen tärkein tavoite on näyttää harjoittelevalle joukolle, ettei aina voi täysin estää tilanteita, eikä aina voi estää toimintaa, mutta tilanteen tapahduttua, voidaan palautua, kerätä palautetta ja parantaa sen osalta yrityksemme (pankin) toimintaa tulevaisuudessa.

## Taustakertomus

Taustakertomus on avattu jo aiemmin dokumentissa (Ks. 4.2.1).

## Roolit

### White team & Green team

Tiimien tehtävät on määritetty jo aiemmin dokumentissä (Ks 1.4.3).

### Blue team

Tiimien tehtävät on määritetty jo aiemmin dokumentissä (Ks 1.4.1).

### Red team

Tiimien tehtävät on määritetty jo aiemmin dokumentissä (Ks 1.4.2).

## Harjoituksen säännöt

Harjoituksen verkon ulkopuolelle hyökkääminen on täysin kiellettyä. Kaikki virtuaalikoneet irrotetaan DHCP-palvelimesta ja asetetaan tietokoneille staattiset IP-osoitteet, sekä default-gateway:t, että dns.

Harjoituksen kulku on myös suurimmaksi osaksi skriptattu, joten ohjeiden seuraaminen on erittäin tärkeää, varsinkin päätoimijoiden puolella (red-team ja IT-palvelut).

Jokainen osallistuja saa käyttää vain hänelle jaettuja käyttäjätunnuksia. Salasanaa ei saa vaihtaa.

Ei omia ulkoisia laitteita verkkoon.

Kommunikointi vain ja ainoastaan chat-palvelun kautta pois lukien johtaja, että saadaan kommunikointi talteen myöhempää analysointia varten.

## Tekninen toimintaympäristö

Tekninen toimintaympäristö on suunniteltu ja kuvattu kohdassa 5 (ks. 5.1)

## Turvallisuus

Kaikille jaetaan ohjeet siitä, mitä työkaluja, sivustoja, sekä sovelluksia saa käyttää. Muiden, kuin punaisen tiimin tehtävään kuuluvien on kiellettyä käyttämästä verkkoskannaus-työkaluja, sekä hyökätä IP-osoitteisiin.