Verkkokaupan kyberharjoitus

Ahola Aleksi

Hakkari Onni

Luukkanen Eetu

Puumalainen Pasi

Tikkanen Teemu

Kyberharjoitus

Syyskuu 2017

Tieto- ja viestintätekniikka

Tekniikan ja liikenteen ala

Sisällysluettelo

[1 JOHDANTO 2](#_Toc493755413)

[1.1 Toiminta-ajatus ja käytettävä harjoitusmuoto 2](#_Toc493755414)

[1.2 Harjoituksen tavoitteet 2](#_Toc493755415)

[1.3 Rajaukset 2](#_Toc493755416)

[1.4 Harjoituksen osallistujat 2](#_Toc493755417)

[2 HARJOITUKSEN SUUNNITTELU 2](#_Toc493755418)

[2.1 Suunnittelun aikataulu 2](#_Toc493755419)

[2.2 Suunnitteluryhmän tehtävä 2](#_Toc493755420)

[2.3 Suunnitteluryhmän kokoonpano 3](#_Toc493755421)

[3 HARJOITUKSEN AJANKOHTA 3](#_Toc493755422)

[4 HARJOITUKSEN TOTEUTUS 3](#_Toc493755423)

[4.1 Sinisten tiimien tehtävät 3](#_Toc493755424)

[4.2 Skenaario 3](#_Toc493755425)

[4.2.1 Taustakertomus 3](#_Toc493755426)

[4.2.2 Uhkatoimijat 3](#_Toc493755427)

[4.2.3 Uhkatoimijoiden toimenpiteet 3](#_Toc493755428)

[4.3 Pelitapahtumat 4](#_Toc493755429)

[4.4 Pelisyötteet 4](#_Toc493755430)

[5 HARJOITUSYMPÄRISTÖ 4](#_Toc493755431)

# JOHDANTO

## Toiminta-ajatus ja käytettävä harjoitusmuoto

Harjoituksen toiminta-ajatus on kehittää verkkokaupan kykyä estää ja puolustautua sitä vastaan kohdistetuilta kyberhyökkäyksiltä. Yleisten turvallisuusperiaatteiden ja sääntöjen kouluttaminen henkilöstölle.

## Harjoituksen tavoitteet

Päätavoite on lisätä verkkosivuston ja henkilöstön turvallisuustoimia ja testata sekä parantaa teknisen puolen ja henkilöstön toimintatehokkuutta mahdollisen sivustoon kohdistuvan hyökkäyksen aikana. Pyritään pitämään asiakastiedot turvassa ja verkkokaupan perustoiminnot ylhäällä.

## Rajaukset

Harjoitus on ajallisesti rajattu 3:en tuntiin, joka sisältää koulutuksen ja toimintaharjoituksen. Tämän aikana päästävä tavoitteisiin.

## Harjoituksen osallistujat

Verkkokaupan henkilöstö, jotka ovat päivittäin päätelaitteilla, jotka ovat yhteydessä suoraan sivuston hallintoon, servereihin, tietokantoihin ja hallintotyökaluihin.

# HARJOITUKSEN SUUNNITTELU

## Suunnittelun aikataulu

Suunnittelun aloitus 14.9.2017. Suunnitelma saatava esityskelpoiseksi 28.9.2017. Suunnitelman toteutuskelpoinen versio 4.10.2017 mennessä.

## Suunnitteluryhmän tehtävä

Suunnitteluryhmä suunnittelee ja toteuttaa kyberharjoituksen, jossa suunnitteluryhmä osallistuu valkoisessa, vihreässä ja punaisessa tiimissä. Valkoinen tiimi ylläpitää harjoitusta lisäämällä tapahtumia harjoitukseen ja ohjeistamalla sinistä tiimiä tarvittaessa. Vihreä tiimi ylläpitää tekniikkaa. Punainen tiimi on vihainen asiakas nimeltä Kimjongaml Pohjois-Koreasta, jonka tarkoituksena on aiheuttaa hankaluuksia siniselle tiimille.

## Suunnitteluryhmän kokoonpano

Ahola Aleksi, Hakkari Onni, Luukkanen Eetu, Puumalainen Pasi ja Tikkanen Teemu.

# HARJOITUKSEN AJANKOHTA

Harjoitus järjestetään 23.11.2017 klo. 8:00-11:00

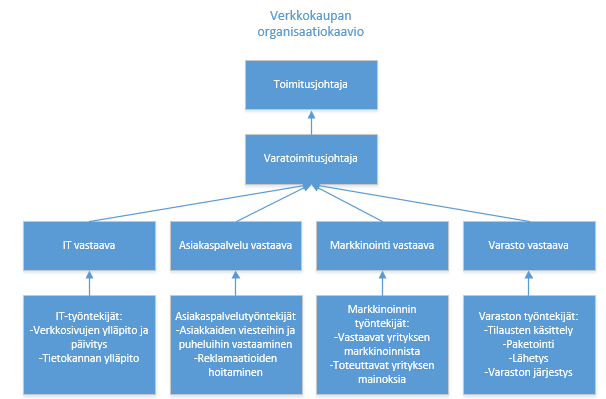
# HARJOITUKSEN TOTEUTUS

## Sinisen tiimin tehtävät

Sininen tiimi puolustautuu Kimjongamlin hyökkäyksiä vastaan. Tiimin pitää puolustautua palvelunestohyökkäyksiä sekä tietokantaan kohdistuvia hyökkäyksiä vastaan. Sinisen tiimin on pidettävä verkkokaupan sivut ja palvelut toiminnassa hyökkäyksistä huolimatta. Yrityksen toiminta ei saa keskeytyä.

## Skenaario

### Yritys



### Taustakertomus

Kimjongaml tilasi Keisari 1000-packin olutta, mutta saikin vain 100-packin Karjalaa. Suivaantunut asiakas päättää kostaa webbikaupalle huonosta palvelusta.

### Uhkatoimijat

Kimjongaml on uhkatoimija, sillä hän suuttui, kun verkkokauppa ei toimittanut oikeaa tuotetta.

### Uhkatoimijoiden toimenpiteet

- Verkkokaupan toiminnan hidastaminen

- Asiakastietojen kalastelu ja niiden vuotaminen nettiin

- Lunnaiden vaatiminen

## Pelitapahtumat

- Peli alkaa, punainen tiimi hyökkää sivustolle  
-Yritykseltä vaaditaan lunnaita 50 000€, jotta hyökkays lopetettaisiin  
-Punainen tiimi hankaloittaa yritystoiminnan harjoittamisen niin kauan kuin lunnaita ei makseta  
-Sininen tiimi tekee parhaansa selviytyäkseen tilanteesta ja estääkseen kyberhyökkäyksen  
-Peli loppuu

## Pelisyötteet

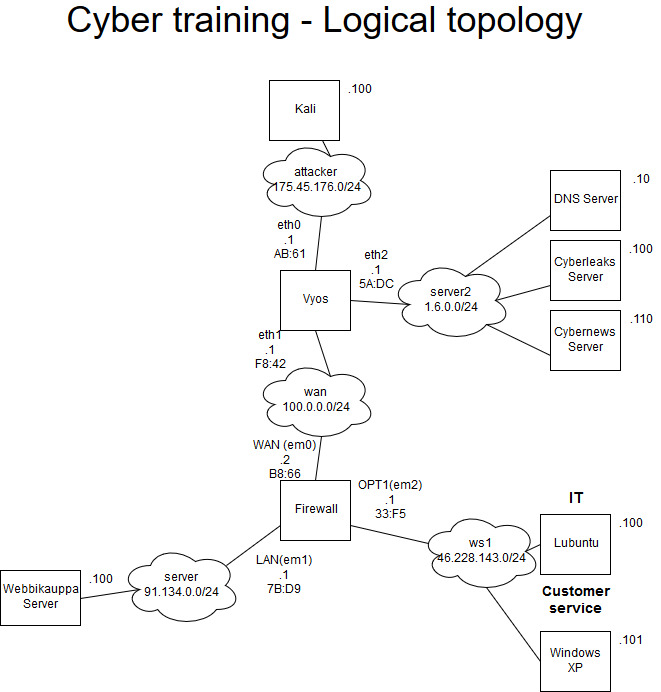
RT:n syötteet

* Hiiren käytöstä pois ottaminen (IT-henkilö)
* Asiakastietojen vuoto, lunnasvaatimus
* Tehdään huijaustilauksia, jotka sekoittavat verkkokaupan toimintaa

## Blue teamin tietoturvakontrollit

* Käytetään työkalua, jolla voidaan havaita RT:n exploitteja
* Pfsense, jolla pääsee hallitsemaan Webbikaupan tietoturvaa ja sinne tulevia yhteyksiä
* Mahdollinen pääsy hyökkääjän koneelle
* Mahdollisuus poistaa vuodetut tiedot Cyberleaks -sivustolta hyökkääjän koneelta löydettyjen tietojen avulla

# HARJOITUSYMPÄRISTÖ



# PEREHDYTYSSUUNNITELMA

## Johdanto / yleisjärjestelyt

Verkkokauppa yritys: webbikauppa.fi. Harjoitukseen osallistujat ottavat etäyhteyden harjoitusympäristössä oleville työasemille.

## Harjoitettavat organisaation osat / -roolit

Harjoitukseen osallistuu IT-osasto ja asiakaspalvelija-osasto (samassa verkossa). IT-osaston tehtävä on myös hallinnoida webbikauppa.fi palvelinta, joka sijaitsee julkisessa pilvessä.

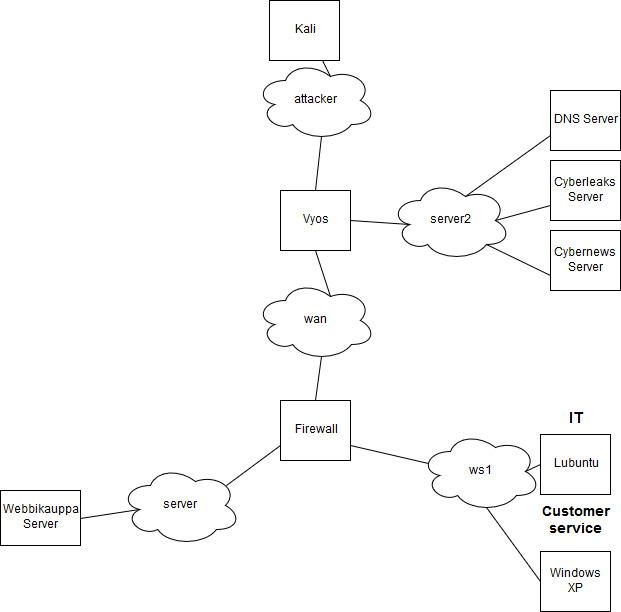
## Taustakertomus

Kimjongaml tilasi Keisari 1000-packin olutta, mutta saikin vain 100-packin Karjalaa. Suivaantunut asiakas päättää kostaa webbikaupalle huonosta palvelusta.

## Harjoitustavoitteet

Blueteamilla tavoite selviytyä tietomurrosta vihjeiden avulla. Harjoituksen tavoite on lisätä verkkosivuston ja henkilöstön turvallisuustoimia ja testata sekä parantaa teknisen puolen ja henkilöstön toimintatehokkuutta mahdollisen sivustoon kohdistuvan hyökkäyksen aikana. Pyritään pitämään asiakastiedot turvassa ja verkkokaupan perustoiminnot ylhäällä.

## Tekninen toimintaympäristö



Ajankohtaisia uutisia pääsee lukemaan cybernews.com osoitteesta ja muhkeita tietovuotoja pääsee tarkastelemaan osoitteessa cyberleaks.com. Keisari 1000-packin pääsee tilaamaan osoitteesta webbikauppa.fi.

## Harjoituksen toimintaperiaate ja säännöt

Organisaatio jaetaa siniseen ja punaiseen tiimiin. DdoS/DoS hyökkäysten käyttäminen on kielletty.

## Harjoituspäivän aikataulu

- 8.00 Harjoituksen valmistelu

- 8.30 Harjoitus alkaa

- 9.15 Tauko alkaa

- 9.30 Harjoitus jatkuu

- 11.00 Harjoitus päättyy

## Turvallisuus

Suljettu harjoitusympäristö.