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 vihaisen asiakkaan muodostama hakkeriryhmä nimeltään ”Cyber Attack Squad (CAS)”, 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

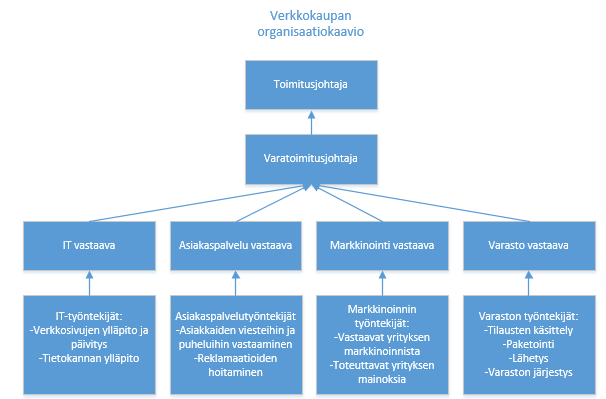
# HARJOITUKSEN TOTEUTUS

## Sinisen tiimin tehtävät

Sininen tiimi puolustautuu Cyber Attack Squadin 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

Työntekijä on avannut sähköpostiliitteen, joka on sisältänyt troijalaisen. Troijalainen on saastuttanut työpaikan koneen lisäten takaoven järjestelmään ja sitä kautta levinnyt koko yrityksen verkkoon. Yritykseltä on varastettu asiakastietoja asiakastietokannasta. Tieto tietomurrosta on tullut yritykselle median kautta.

### Uhkatoimijat

Asiakas suuttui, kun verkkokauppa ei toimittanut tuotteita eikä palauttanut rahoja. Verkkokaupan harmiksi asiakas pisti hakkeriryhmän(CAS) kasaan ja päätti kostaa huonosta palvelusta.

### Uhkatoimijoiden toimenpiteet

Cyber Attack Squad lähetti sähköpostin, joka sisälsi liitetiedoston. Liitetiedosto sisälsi troijalaisen, jonka luoman takaoven avulla päästään käsiksi koko yrityksen verkkoon. Kun verkkoon on päästy, aletaan kalastelemaan asiakastietoja. Samalla verkkokaupan toimintaa hidastetaan palvelunestohyökkäyksillä ja valetilauksilla. Verkkokaupalta vaaditaan lunnaita varastetuista tiedoista.

## Pelitapahtumat

-Työntekijä on avannut sähköpostin, jonka liitteenä on troijalainen  
-Troijalaisen avulla päästään käsiksi yrityksen Webbikaupan serverille ja saadaan sieltä asiakastietoja  
-Yritys saa tiedon median kautta, että heiltä on varastettu asiakastietoja ja niitä vuodetaan nettiin  
-Yritykseltä vaaditaan lunnaita 50 000€, jotta vuoto lopetettaisiin  
-Punainen tiimi hankaloittaa yritystoiminnan harjoittamisen niin kauan kuin lunnaita ei makseta ja vuotaa asiakastietoja internettiin  
-Sininen tiimi tekee parhaansa selviytyäkseen tilanteesta ja estääkseen kyberhyökkäyksen  
-Peli loppuu

## Pelisyötteet

RT:n syötteet

* Hiiren käytöstä pois ottaminen (IT-henkilö)
* Troijalaisen luoman backdoorin kautta varastetaan asiakastietoja
* Tehdään huijaustilauksia, jotka sekoittavat verkkokaupan toimintaa

## Blue teamin tietoturvakontrollit

* Käytetään työkalua, jolla voidaan havaita käytössä oleva ”takaovi” IT-henkilön koneella jonka jälkeen takaovi voidaan poistaa
* 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