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 toimia kyberhyökkäyksen aikana teknistoiminnallisella harjoituksella.

## Harjoituksen tavoitteet

Päätavoite on lisätä turvallisuutta ja toimintatehokkuutta hyökkäyksen aikana verkkokaupassa.

## Rajaukset

Harjoituksen maksimikesto 3 tuntia. Tämän aikana päästävä tavoitteeseen.

## Harjoituksen osallistujat

Verkkokaupan kaikki valkokauluksiset työntekijät osallistuvat harjoitukseen.

# HARJOITUKSEN SUUNNITTELU

## Suunnittelun aikataulu

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

## Suunnitteluryhmän tehtävä

Valkoinen tiimi ohjeistaa ja avustaa puolueettomasti muita tiimejä. Valkoinen tiimi osallistuu myös harjoitukseen puolueettomana entiteettinä.

## 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

## Sinisten tiimien tehtävät

Siniset tiimit puolustautuvat ja harjoittelevat toimintaa punaisia tiimejä vastaan.

## Skenaario

### Taustakertomus

Työntekijä on avannut sähköpostiliitteen, joka on saastuttanut koneen ja sitä kautta koko yrityksen verkon. Yritykseltä on varastettu arkaluontoista tietoa.

### Uhkatoimijat

Asiakas suuttui, kun verkkokauppa ei toimittanut tuotteita eikä palauttanut rahoja. Verkkokaupan harmiksi asiakas päätti kostaa.

### Uhkatoimijoiden toimenpiteet

Suuttunut asiakas päätti lähettää sähköpostin, joka sisälsi liitetiedoston. Liitetiedosto sisälsi troijalaisen, joka saastutti koko yrityksen verkon.

## Pelitapahtumat

-Aluksi kaikki on hyvin  
-Yritys saa tiedon median kautta, että heiltä on varastettu asiakastietoja ja niitä vuodetaan nettiin  
-Yritykseltä vaaditaan lunnaita, jotta vuoto lopetettaisiin  
-Lunnaiden määrä: 50000€  
-Punainen tiimi estää yritystoiminnan harjoittamisen niin kauan kuin lunnaita ei makseta  
-Sininen tiimi tekee parhaansa selviytyäkseen tilanteesta  
-Jos sininen tiimi päättää maksaa lunnaat verkkokauppa tykitetään alas  
-Kun 3 tuntia on kulunut verkkokauppa tykitetään alas ellei sininen tiimi ole poistanut haavoittuvuuksia  
-Peli loppuu

## Pelisyötteet

-Hidastetaan verkkokauppaa ddos:lla  
-Troijalaisen luoman back doorin kautta varastellaan lisätietoja  
-Tehdään huijaustilauksia, jotka hidastavat verkkokaupan toimintaa  
-Yksittäisten työntekijöiden ulos lukitseminen verkosta

# HARJOITUSYMPÄRISTÖ