Verkkokaupan kyberharjoitus

Ahola Aleksi

Hakkari Onni

Luukkanen Eetu

Puumalainen Pasi

Tikkanen Teemu

Kyberharjoitus

Syyskuu 2017

Tieto- ja viestintätekniikka

Tekniikan ja liikenteen ala

Sisällysluettelo

[Sisällysluettelo 1](#_Toc498615113)

[1 JOHDANTO 3](#_Toc498615114)

[1.1 Toiminta-ajatus ja käytettävä harjoitusmuoto 3](#_Toc498615115)

[1.2 Harjoituksen tavoitteet 3](#_Toc498615116)

[1.3 Rajaukset 3](#_Toc498615117)

[1.4 Harjoituksen osallistujat 3](#_Toc498615118)

[2 HARJOITUKSEN SUUNNITTELU 4](#_Toc498615119)

[2.1 Suunnittelun aikataulu 4](#_Toc498615120)

[2.2 Suunnitteluryhmän tehtävä 4](#_Toc498615121)

[2.3 Suunnitteluryhmän kokoonpano 4](#_Toc498615122)

[3 HARJOITUKSEN AJANKOHTA 4](#_Toc498615123)

[4 HARJOITUKSEN TOTEUTUS 4](#_Toc498615124)

[4.1 Sinisen tiimin tehtävät 4](#_Toc498615125)

[4.2 Skenaario 5](#_Toc498615126)

[4.2.1 Yritys 5](#_Toc498615127)

[4.2.2 Taustakertomus 5](#_Toc498615128)

[4.2.3 Uhkatoimijat 5](#_Toc498615129)

[4.2.4 Uhkatoimijoiden toimenpiteet 5](#_Toc498615130)

[4.3 Pelitapahtumat 6](#_Toc498615131)

[4.4 Pelisyötteet 6](#_Toc498615132)

[4.5 Blue teamin tietoturvakontrollit 6](#_Toc498615133)

[5 HARJOITUSYMPÄRISTÖ 7](#_Toc498615134)

[6 PEREHDYTYSSUUNNITELMA 7](#_Toc498615135)

[1.1 Johdanto / yleisjärjestelyt 7](#_Toc498615136)

[1.2 Harjoitettavat organisaation osat / -roolit 8](#_Toc498615137)

[1.3 Taustakertomus 8](#_Toc498615138)

[1.4 Harjoitustavoitteet 8](#_Toc498615139)

[1.5 Tekninen toimintaympäristö 9](#_Toc498615140)

[1.6 Harjoituksen toimintaperiaate ja säännöt 9](#_Toc498615141)

[1.7 Harjoituspäivän aikataulu 10](#_Toc498615142)

[1.8 Turvallisuus 10](#_Toc498615143)

[1.9 Ryhmän sisäiset tehtäväroolit 10](#_Toc498615144)

# 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. Tarkoittaen koko IT-osastoa ja asiakaspalvelu-osastoa. Myös toimitusjohtaja ja varatoimitusjohtaja osallistuvat harjoitukseen.

# HARJOITUKSEN SUUNNITTELU

## Suunnittelun aikataulu

Suunnittelun aloitus 14.9.2017. Suunnitelma saatava esityskelpoiseksi 28.9.2017. Suunnitelman toteutuskelpoinen versio 4.10.2017 mennessä. Suunnitelman lopullinen versio 29.11.2017 mennessä.

## Suunnitteluryhmän tehtävä

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

## 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

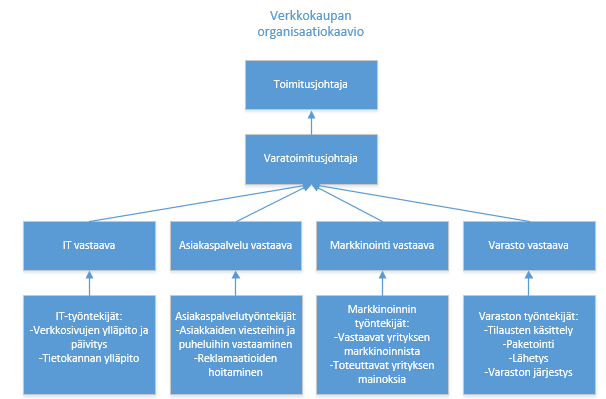
# HARJOITUKSEN TOTEUTUS

## 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



Kuvio 1. Verkkokaupan organisaatiokaavio

### Taustakertomus

Pohjois-Korealainen 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

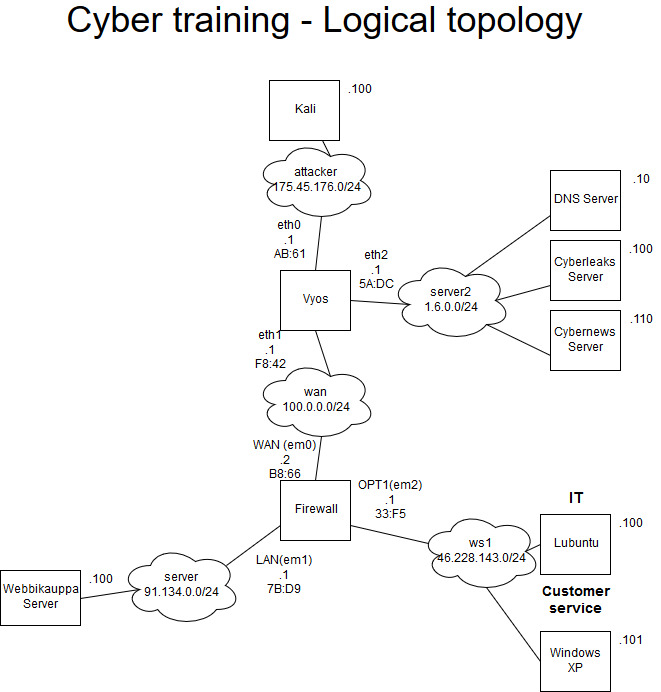
RT:n syötteet

* 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



Kuvio 2. Harjoitusympäristön looginen topologia

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Virtual Machine** | **IP-address** | **DNS** | **User** | **Pwd** | **User2** | **Pwd2** | **WP-User** | **WP-Pwd** |
| Vyos | - | - | vyos | vyos | - | - | - | - |
| Firewall | - | - | admin | 1337admin | - | - | - | - |
| DNS Server | 1.6.0.10 | - | root | root66 | user | user66 | root | root66 |
| Webbikauppa Server | 91.134.0.100 | webbikauppa.fi | root | root66 | user | user66 | root | root66 |
| Cyberleaks Server | 1.6.0.100 | cyberleaks.com | root | root66 | user | user66 | root | root66 |
| Cybernews Server | 1.6.0.110 | cybernews.com | root | root66 | user | user66 | root | root66 |
| Lubuntu | 46.228.143.100 | - | user | user66 | - | - | - | - |
| Windows XP | 46.227.143.101 | - | sulo | - | - | - | - | - |
| Kali | 175.45.1767.100 | - | root | root66 | - | - | - | - |

Taulukko 1. Harjoitusympäristön virtuaalikoneet

Harjoitusympäristössä simuloidaan internettiä suljetussa ympäristössä virtuaalikoneiden avulla käyttäen VirtualBox-ohjelmaa hyväksi. Harjoitusympäristössä on verkkokaupan verkko (server ja ws1), hyökkääjä (attacker) sekä ”yleiset”-palvelimet (server2). Kaikkia näitä yhdistää Vyos, joka mahdollistaa koneiden juttelemisen keskenään. Vyos jakaa DHCP:llä attacker- ja server2-verkkoon IP-osoitteet. Ympäristön kaikki palvelimet ovat Debian-pohjaisia. (ks. Kuvio 2)

Verkkokaupan verkko on pfSense-palomuurin takana. Palomuuri päästää DNS-kyselyt portista 53 lävitse sekä http-kyselyt portista 80 on sallittu. ICMP-kyselyt ovat myös sallittuja. Palomuuri jakaa DHCP:llä IP-osoitteet verkkokaupan koneille. Vyos:in ja palomuurin välissä linkkinä on 100.0.0.0/24 WAN. Verkkokaupan työasemat (ws1) ovat osoiteavaruudessa 46.228.143.0/24, joka oikeassa elämässä osoittaa Suomeen. Verkkokaupan web-palvelimen (server) osoiteavaruus 91.134.0.0/24 osoittaa taas Ranskaan. Näillä osoiteavaruuksilla simuloidaan verkkokaupan servereiden ja työasemien oikeaa sijaintia. Webbikauppa-palvelimella on kiinteä IP-osoite. Verkkokaupan domain-nimi on webbikauppa.fi. Työasemina toimivat IT-osastolla Lubuntu ja asiakaspalvelu-osastolla Windows XP. Lubuntu on vähän resursseja syövä käyttöjärjestelmä ja Windows XP:hen voidaan tehdä hyökkäyksiä vaivattomasti sen huonon tietoturvan vuoksi.

Hyökkääjän (attacker) osoiteavaruus 175.45.176.0/24 sijaitsee Pohjois-Koreassa, joka simuloi taustakertomuksen Pohjois-Korealaista hyökkääjää. Hyökkääjällä on käytössä käyttöjärjestelmänään Kali, koska se sisältää paljon erilaisia kyberhyökkäystyökaluja.

Yleiset palvelimet (server2) sijaitsevat osoiteavaruudessa 1.6.0.0/24, joka osoittaa Intiaan. Siellä sijaitsee DNS-palvelin, joka jakaa domain-nimet koko harjoitusympäristöön. Lisäksi server2:ssa on Cyberleaks- ja Cybernews-palvelimet, joilla on kiinteät IP-osoitteet. Näiden domain-nimet ovat cyberleaks.com ja cybernews.com.

## Cyberleaks-palvelin

## Cybernews-palvelin

## Webbikauppa-palvelin

# PEREHDYTYSSUUNNITELMA

## Johdanto / yleisjärjestelyt

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

## Harjoitettavat organisaation osat / -roolit

Organisaatiosta harjoitukseen osallistuu toimitusjohtaja, varatoimitusjohtaja, koko IT-osasto: IT-osaston vastuuhenkilö ja työntekijät, sekä ja asiakaspalvelija-osasto: asiakaspalveluosaston vastuuhenkilö ja työntekijät. IT-osaston tehtävä on myös hallinnoida webbikauppa.fi palvelinta, joka sijaitsee julkisessa pilvessä. Koko organisaatio kuuluu siniseen tiimiin. Punaiseen tiimiin kuuluvat harjoituksen järjestäjistä: Ahola Aleksi, Hakkari Onni, Luukkanen Eetu ja Puumalainen Pasi. Valkoisen tiimin ainut jäsen on harjoituksen järjestäjistä Tikkanen Teemu.

Harjoituksessa käytetään organisaatiokaavion mukaista mallia. Tarkoittaen sitä, että sinisen tiimin jäsenten tulee toimia normaalisti organisaation sisällä: pelitapahtumista ilmoitetaan aina ylemmällä esimiehelle, mikäli tapahtuma on ilmoitusluontoinen ja/tai vaatii esimiehen lupaa toimia. Lähtökohtaisesti toimitusjohtaja ja varatoimitusjohtaja ovat ainoat, jotka kommunikoivat järjestäjien kanssa, mikäli harjoituksen aikana ilmenee kysyttävää. Tällöin otetaan yhteys valkoiseen tiimiin.

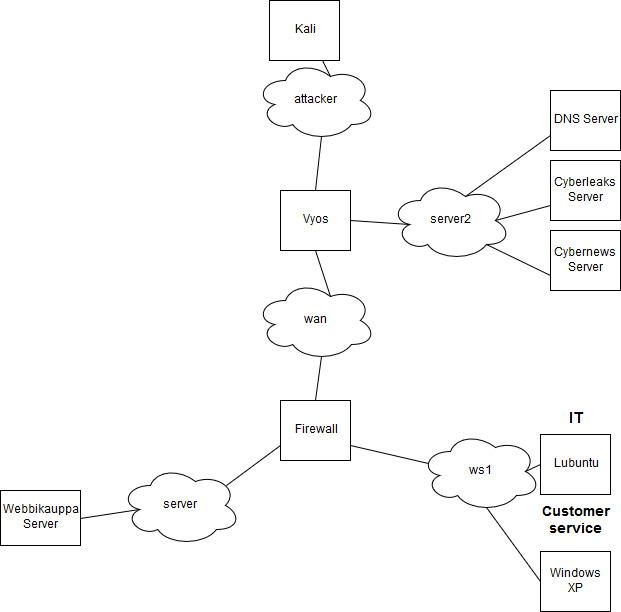
## Taustakertomus

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

## Harjoitustavoitteet

Sinisen tiimin tavoite on 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 jaetaan siniseen ja punaiseen tiimiin. Harjoituksessa pysytään Suomen lainsäädännön puitteissa. Tulipalon sattuessa seurataan hätäuloskäyntikylttejä ulos rakennuksesta. Kokoontumispaikka löytyy Schaumanin patsaan luota. DDoS/DoS hyökkäysten käyttäminen on kielletty, täten saadaan ympäristö pidettyä ylhäällä ja toimivana.

## Harjoituspäivän aikataulu

- 8.00 Harjoituksen valmistelu

- 8.30 Harjoitus alkaa

- 9.15 Tauko alkaa

- 9.30 Harjoitus jatkuu

- 11.00 Harjoitus päättyy, purku ja palaute

## Turvallisuus

Suljettu harjoitusympäristö.

## Ryhmän sisäiset tehtäväroolit

Vastuuhenkilö/harjoituksen vetäjä/valkoinen tiimi: Teemu Tikkanen

Punainen tiimi: Aleksi Ahola, Onni Hakkari, Eetu Luukkanen, Pasi Puumalainen