Verkkokaupan kyberharjoitus

Aleksi Ahola

Hakkari Onni

Luukkanen Eetu

Pasi Puumalainen

Tikkanen Teemu

Kyberharjoitus

Syksy 2017

Tieto- ja viestintätekniikka

Tekniikan ja liikenteen ala

Sisällysluettelo

[1 JOHDANTO 4](#_Toc499915129)

[1.1 Toiminta-ajatus ja käytettävä harjoitusmuoto 4](#_Toc499915130)

[1.2 Harjoituksen tavoitteet 4](#_Toc499915131)

[1.3 Rajaukset 4](#_Toc499915132)

[1.4 Harjoituksen osallistujat 4](#_Toc499915133)

[2 HARJOITUKSEN SUUNNITTELU 5](#_Toc499915134)

[2.1 Suunnittelun aikataulu 5](#_Toc499915135)

[2.2 Suunnitteluryhmän tehtävä 5](#_Toc499915136)

[2.3 Suunnitteluryhmän kokoonpano 5](#_Toc499915137)

[3 HARJOITUKSEN AJANKOHTA 5](#_Toc499915138)

[4 HARJOITUKSEN TOTEUTUS 5](#_Toc499915139)

[4.1 Sinisten tiimien tehtävät 5](#_Toc499915140)

[4.2 Skenaario 6](#_Toc499915141)

[4.2.1 Yritys 6](#_Toc499915142)

[4.2.2 Taustakertomus 6](#_Toc499915143)

[4.2.3 Uhkatoimijat 6](#_Toc499915144)

[4.2.4 Uhkatoimijoiden toimenpiteet 6](#_Toc499915145)

[4.3 Pelitapahtumat 7](#_Toc499915146)

[4.4 Pelisyötteet 9](#_Toc499915147)

[4.5 Blue teamin tietoturvakontrollit 9](#_Toc499915148)

[5 HARJOITUSYMPÄRISTÖ 10](#_Toc499915149)

[5.1 Cyberleaks-palvelin 14](#_Toc499915150)

[5.2 Cybernews-palvelin 14](#_Toc499915151)

[5.3 Webbikauppa-palvelin 14](#_Toc499915152)

[5.4 Ympäristön scriptit 15](#_Toc499915153)

[6 PEREHDYTYSSUUNNITELMA 15](#_Toc499915154)

[6.1 Johdanto / yleisjärjestelyt 15](#_Toc499915155)

[6.2 Harjoitettavat organisaation osat / -roolit 15](#_Toc499915156)

[6.3 Taustakertomus 16](#_Toc499915157)

[6.4 Harjoitusvaiheet 16](#_Toc499915158)

[6.5 Tekninen toimintaympäristö 17](#_Toc499915159)

[6.6 Harjoituksen toimintaperiaatteet ja säännöt 17](#_Toc499915160)

[6.7 Harjoituspäivän aikataulu 18](#_Toc499915161)

[6.8 Turvallisuus 18](#_Toc499915162)

[6.9 Ryhmän sisäiset tehtäväroolit 18](#_Toc499915163)

[7 ARVIOINTIVAIHE 18](#_Toc499915164)

**Kuviot**

[Kuvio 1. Verkkokaupan organisaatiokaavio 5](#_Toc499892142)

[Kuvio 2. Harjoitusympäristön looginen topologia 7](#_Toc499892143)

[Kuvio 3. Cyberleaks.com DNS-asetukset 10](#_Toc499892144)

[Kuvio 4. Webbikauppa.fi DNS-asetukset 10](#_Toc499892145)

[Kuvio 5. Cybernews.com DNS-asetukset 10](#_Toc499892146)

[Kuvio 6. DNS luotetut alueet 11](#_Toc499892147)

[Kuvio 7. Cyberleaks.com etusivu 11](#_Toc499892148)

[Kuvio 8. Cybernews.com etusivu 11](#_Toc499892149)

[Kuvio 9. Webbikauppa.fi etusivu 12](#_Toc499892150)

[Kuvio 10. Toimintaympäristö 14](#_Toc499892151)

**Taulukot**

[Taulukko 1. Pelitapahtumat 8](#_Toc499914995)

[Taulukko 2. Harjoitusympäristön virtuaalikoneet 11](#_Toc499914996)

**Liitteet**

[Liite 1. Punaisentiiminsyötteet.docx 19](#_Toc499915123)

[Liite 2. Kyselylomake.docx 19](#_Toc499915124)

# 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 13.12.2017 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.

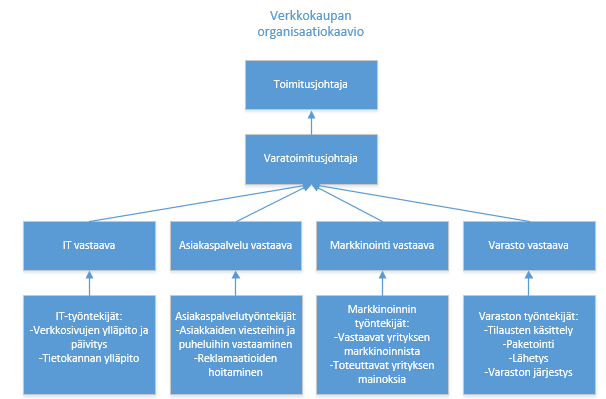
# HARJOITUKSEN TOTEUTUS

## Sinisten tiimien tehtävät

Sininen tiimi 2 puolustautuu Kimjongamlin hyökkäyksiä vastaan, joista sininen tiimi 1 raportoi kakkostiimille. Sinisen tiimin 2 pitää puolustautua palvelunestohyökkäyksiä vastaan. Sinisen tiimin 2 on pidettävä verkkokaupan sivut ja palvelut toiminnassa hyökkäyksistä huolimatta. Yrityksen toiminta ei saa keskeytyä. Sininen tiimi 2 hyökkää hyökkääjän koneelle löydettyään jalanjäljet palvelimelta. (ks. Taulukko 1)

## 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 BlackFriday:n aikaan, jolloin liikevaihto on suurimmillaan.

### Uhkatoimijat

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

### Uhkatoimijoiden toimenpiteet

-Verkkokaupan toiminnan hidastaminen

-Liikevaihdon pienentäminen

## Pelitapahtumat

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Pelitapahtuma** | **Syöteaika** | **Kuvaus** | **Tavoite** | **Jakelija** | **Jakelumenetelmä** |
| 001 |  | Blue team 1 seuraa tilausten tuloa. |  | WT | Suullinen |
| 002 |  | Blue team 2 on valmiudessa, kun BT1 ilmoittaa häiriöistä. BT2:n tavoite poistaa vuodetut tiedot internetistä. |  | WT | Suullinen |
| 003 | 8:45 | BT1 ja BT2 saavat tiedon, että asiakastietoja on vuodettu cyberleaks.com sivustolle. | Aiheuttaa sekasortoa | WT | cybernews.com |
| 004 | 8:50 | RT aloittaa jatkuvan palvelunestohyökkäyksen. | Hidastaa webbikaupan liikevaihtoa. | RT | Paperiohje |
| 005 | 9:00 | BT1 havaitsee liikevaihdon hidastuneen ja raportoi BT2:lle. | Nopea reagointi. | WT | Suullinen |
| 006 | 9:10 | BT2 estää jatkuvan palvelunestohyökkäyksen estämällä hyökkääjän IP-osoitteen. | Palauttaa webbikaupan toiminta normaaliksi. | WT | Suullinen |
| 007 | 9:30 | RT vaihtaa IP-osoitteensa ja jatkaa pavelunestohyökkäystä. | Hidastaa webbikaupan liikevaihtoa. | RT | Paperiohje |
| 008 | 9:35 | BT1 havaitsee liikevaihdon jälleen hidastuneen ja raportoi BT2:lle. | Nopea reagointi. | WT | Suullinen |
| 009 | 9:45 | BT2 estää jatkuvan palvelunesto hyökkäyksen estämällä hyökkääjän IP-osoitteen. | Palauttaa webbikaupan toiminta normaaliksi | WT | Suullinen |
| 010 | 9:50 | Cyberleaks.com julkaisee huhun, että hakkeri on jättänyt jalanjälkiä webbikauppa-palvelimelle | BT2 lähtee etsimään jalanjälkiä palvelimelta | WT | cybernews.com |
| 011 | 9:50 | RT vaihtaa IP-osoitteensa ja jatkaa pavelunestohyökkäystä. | Hidastaa webbikaupan liikevaihtoa. | RT | Paperiohje |
| 012 | 10:00 | BT1 havaitsee hyökkäyksen ja ilmoittaa BT2:lle. | Nopea reagointi. | WT | Suullinen |
| 013 | 10:05 | BT2 priorisoi jalanjälkien löytämisen hyökkäyksen edelle. BT2 löytää jalanjäljet pavelimelta. | Löytää base64 salatut tiedot | WT | Suullinen |
| 014 | 10:10 | BT2 murtaa salatut tiedot | Löytää hyökkääjän käyttäjätunnus ja salasana | WT | Suullinen |
| 015 | 10:15 | BT2 ottaa ssh-yhteyden samaan IP-osoitteeseen, josta tulee palvelunestohyökkäys. | Sulkea palvelunestohyökkäys lopullisesti | WT | Suullinen |
| 016 | 10:20 | BT2 sulkee hyökkäyksen | Lisätä webbikaupan liikevaihtoa | WT | Suullinen |
| 017 | 10:30 | BT2 löytää killswitch backdoorin vuotosivutolle ja käyttää sitä | Päättää peli ja poistaa vuodetut tiedot cyberleaks.com sivuilta. | WT | Suullinen |
| 018 | 11:00 | Peli päättyy. |  | WT, RT | Suullinen |

Taulukko 1. Pelitapahtumat

## Pelisyötteet

TÄHÄN RT:N OHJEET

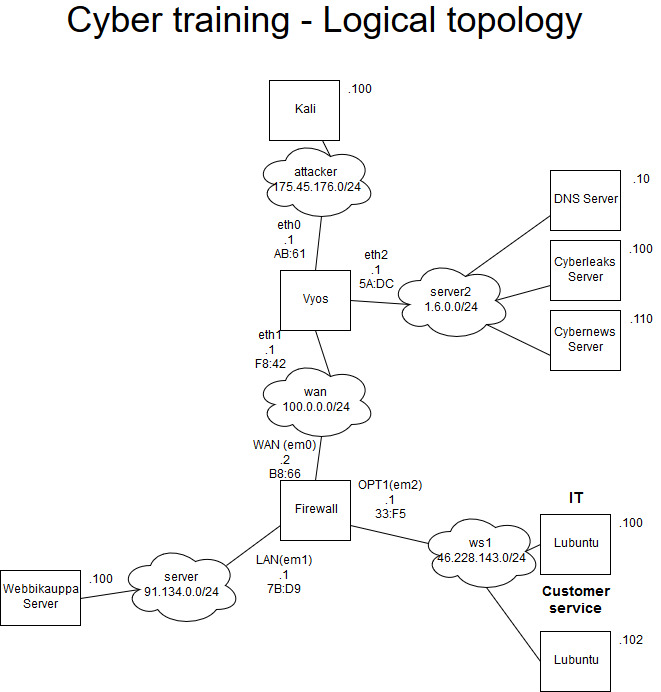
## Blue teamin tietoturvakontrollit

-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 | - | - | - | - |
| Lubuntu | 46.227.143.102 | - | user | user66 | - | - | - | - |
| Kali | 175.45.1767.100 | - | root | isecretlylovesouthkorea | - | - | - | - |

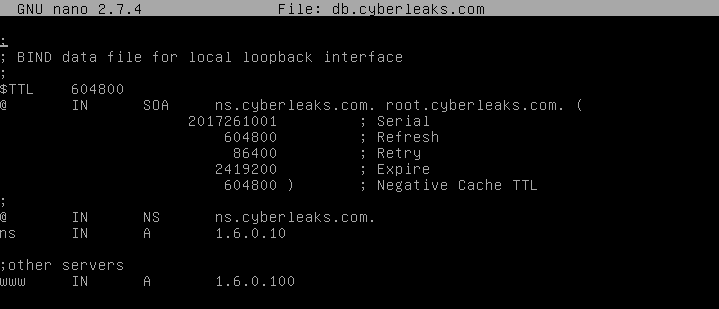
Taulukko 2. Harjoitusympäristön virtuaalikoneet

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)

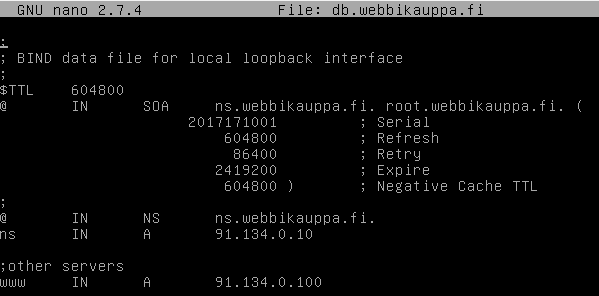
Verkkokaupan verkko on pfSense-palomuurin takana. Palomuuri päästää DNS-kyselyt portista 53 lävitse sekä http-kyselyt portista 80 on sallittu. ICMP-kyselyt ovat myös sallittuja. Palomuuri jakaa DHCP:llä IP-osoitteet verkkokaupan koneille. Vyos:in ja palomuurin välissä linkkinä on 100.0.0.0/24 WAN. Verkkokaupan 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 myös Lubuntu. Lubuntu on vähän resursseja syövä käyttöjärjestelmä, jonka takia Lubuntu valikoitui ympäristöön.

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.

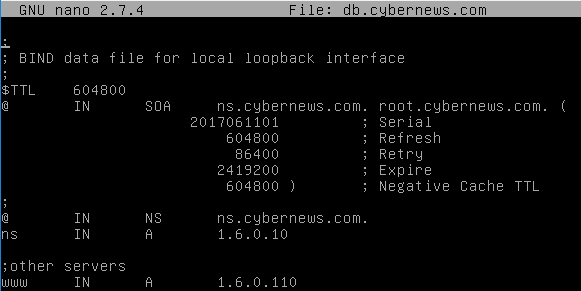
Yleiset palvelimet (server2) sijaitsevat osoiteavaruudessa 1.6.0.0/24, joka osoittaa Intiaan. Siellä sijaitsee DNS-palvelin, joka jakaa domain-nimet koko harjoitusympäristöön. Lisäksi server2:ssa on Cyberleaks- ja Cybernews-palvelimet, joilla on kiinteät IP-osoitteet. Näiden domain-nimet ovat cyberleaks.com ja cybernews.com. Alla DNS-asetukset (ks. Kuviot 3-6)



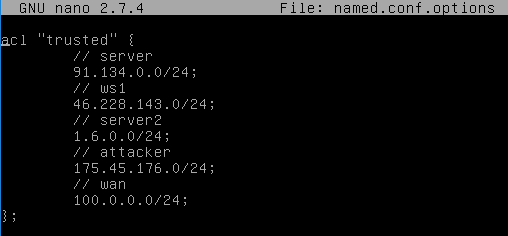
Kuvio 3. Cyberleaks.com DNS-asetukset



Kuvio 4. Webbikauppa.fi DNS-asetukset

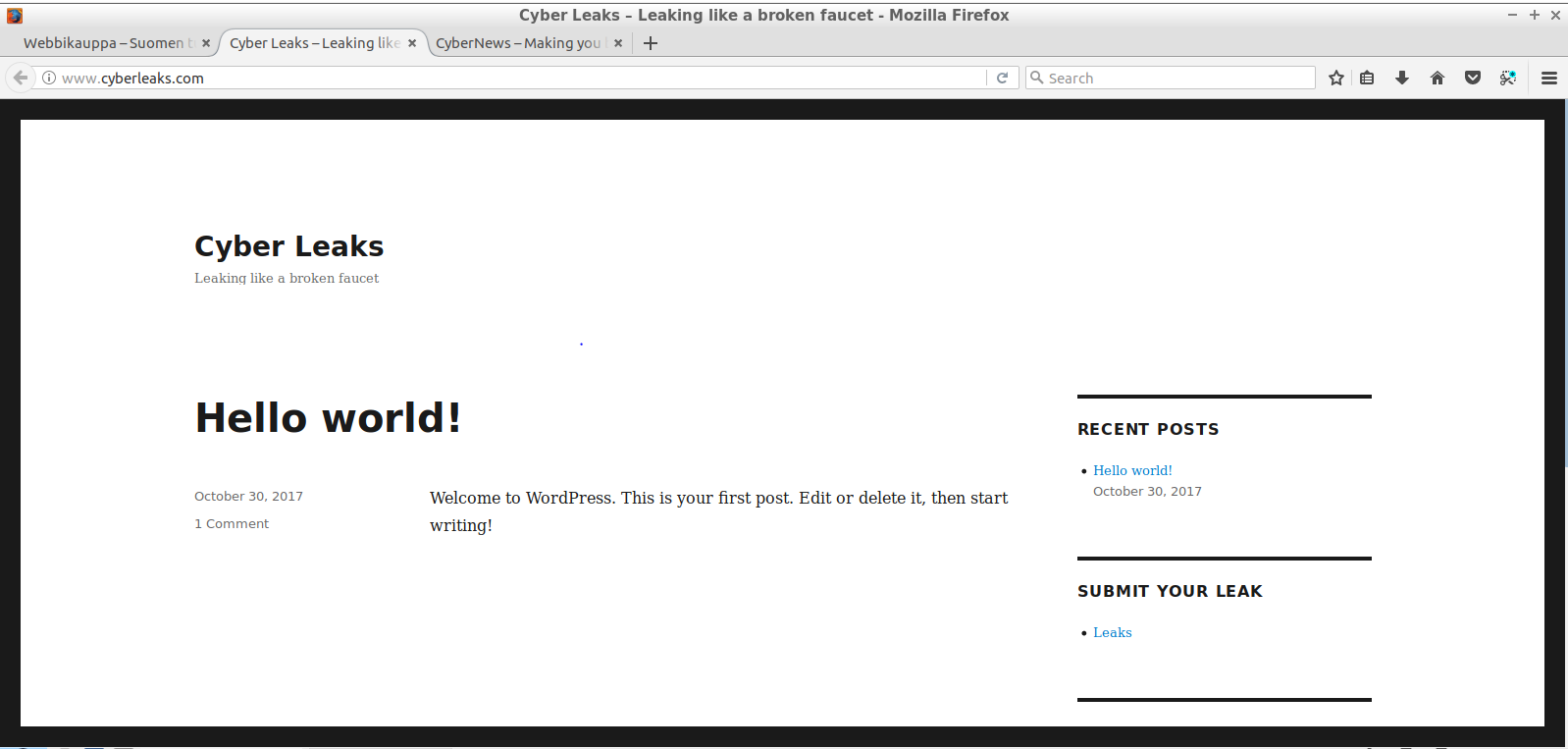


Kuvio 5. Cybernews.com DNS-asetukset



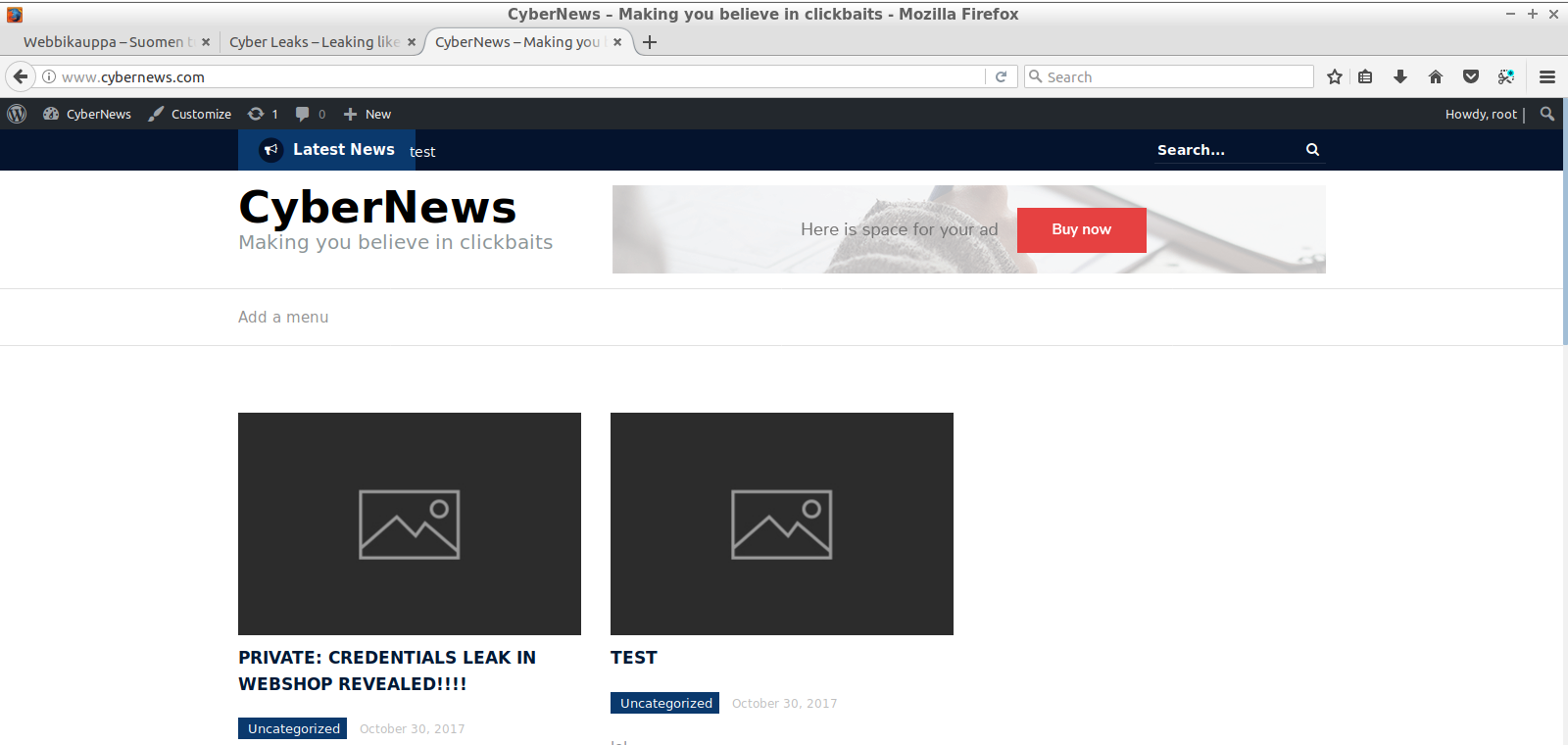
Kuvio 6. DNS luotetut alueet

## Cyberleaks-palvelin



Kuvio 7. Cyberleaks.com etusivu

## Cybernews-palvelin



Kuvio 8. Cybernews.com etusivu

## Webbikauppa-palvelin

Webbikauppa-palvelin tehtiin Debian-käyttöjärjestelmälle. Sivuston luonnissa käytettiin Wordpressiä. Sen domain-osoite on webbikauppa.fi. Sivustolla on myynnissä muutama esine verkkokaupan toiminnan mallintamista varten (mm. tietokone, näyttö). Wordpressiin lisättiin ostoskori- ja käyttäjätunnus-lisäosat, jotta sinne voi tehdä käyttäjätunnuksia ja lisätä tuotteita ostoskoriin niiden ostamista varten. Myös eräänlainen palomuuri-lisäosa asennettiin, jolla saadaan paranneltua sivuston tietoturvaa.



Kuvio 9. Webbikauppa.fi etusivu

## Ympäristön scriptit

### Customer Service

<https://github.com/LuckyHacker/cyber-security-training/tree/master/BlueTeam/CustomerService>

* orderservice.py
  + Ottaa vastaan tilauksia verkkokauppa palvelimelta.
* monitor\_orders.sh
  + Tilauslokitiedoston tarkastelija. Tämän avulla asiakaspalvelija pystyy seuraamaan tilauksia reaaliajassa.

### Webbikauppa-palvelin

<https://github.com/LuckyHacker/cyber-security-training/tree/master/BlueTeam/WebStore>

* ordersend.py
  + Lähettää satunnaisen tilauksen aina kun joku käy verkkokaupan ostoskorissa.

### Cyberleaks-palvelin

<https://github.com/LuckyHacker/cyber-security-training/tree/master/cyberleaks>

* client.py
  + Jotta kaikki tietojen vuotajat voivat lähettää tiedostot serverille (tälle ei enään käyttöä).
* server.py
  + Tietovuotojen vastaanottava scripti (tälle ei enään käyttöä).
* order-script.py
  + Tekee ”tilauksia” osoitteessa [www.webbikauppa.fi](http://www.webbikauppa.fi).
* cyberleaks-eraser.py
  + Hakkerin salainen backdoor cyberleaks palvelimella, jolla voi helposti poistaa kaikki vuodot tietokannasta.

# PEREHDYTYSSUUNNITELMA

## Johdanto / yleisjärjestelyt

Verkkokauppana toimiva 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 jaetaan kahteen siniseen tiimiin. Sininen tiimi 1 koostuu asiakaspalvelija-osastosta ja Sininen tiimi 2 koostuu IT-osastosta. Toimitusjohtaja ja varatoimitusjohtaja kuuluvat kumpaankin 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 sinisten tiimien 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.

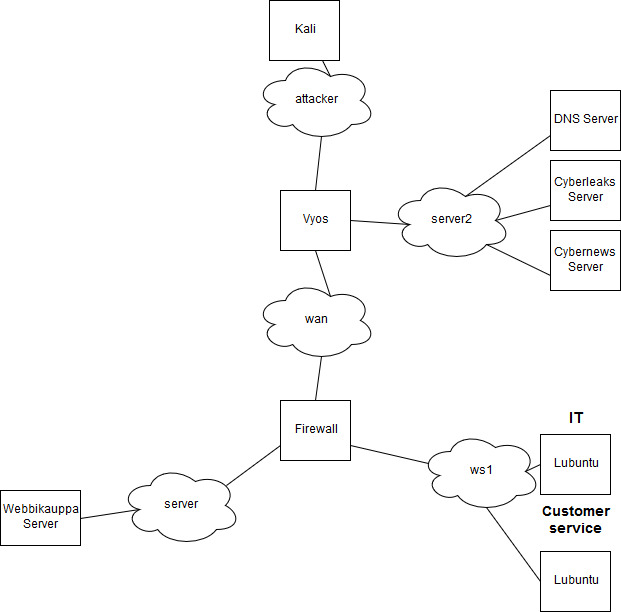
## Taustakertomus

Tässä esitetään kappaleen 4.4.2 taustakertomus.

## Harjoitusvaiheet

BT1:n tavoite on havaita palvelunestohyökkäyksen ja ilmoittaa niistä BT2:lle. BT2:n tavoite on estää palvelunestohyökkäykset, jotta liikevaihto ei häiriinny. 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, poistamaan asiakastiedot julkisilta sivuilta ja verkkokaupan perustoiminnot ylhäällä.

## Tekninen toimintaympäristö



Kuvio 10. 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 toimintaperiaatteet ja säännöt

Organisaatio jaetaan kahteen siniseen tiimiin. Punaista tiimiä edustavat harjoituksen järjestäjät. Harjoituksessa pysytään Suomen lainsäädännön puitteissa. Tulipalon sattuessa seurataan hätäuloskäyntikylttejä ulos rakennuksesta. Kokoontumispaikka löytyy Schaumanin patsaan luota. Jos et tiedä mitä olet tekemässä, älä tee vaan kysy vastuuhenkilöiltä. Palomuurista ei saa estää koko osoiteavaruutta.

## 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

Sininen tiimi 1: Asiakaspalvelu-osasto, toimitusjohtaja, varatoimitusjohtaja

Sininen tiimi 2: IT-osasto, toimitusjohtaja, varatoimitusjohtaja

# ARVIOINTIVAIHE

Harjoituksen jälkeen harjoitukseen osallistuneilta kerätään palaute erillisellä paperisella kyselylomakkeella. (ks. Liite 2) Vastaukset kootaan yhteen erilliseen dokumenttiin ja käydään lävitse.

**Liitteet**

Liite 1. Punaisentiiminsyötteet.docx

Liite 2. Kyselylomake.docx