HAAGA-HELIA
ammattikorkeakoulu

HAAGA-HELIAn tietoliikennelaboratorion tietoturva käyttäjän näkökulmasta

Sampo Tyllilä

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2013

HAAGA-HELIA
ammattikorkeakoulu

Tietojenkäsittelyn koulutusohjelma

Tiivistelmä

19.5.2013

Tekijä tai tekijät Sampo Tyllilä	**Ryhmätunnus tai aloitusvuosi** 2010
Raportin nimi HAAGA-HELIAn tietoliikennelaboratorion tietoturva käyttäjän näkökulmasta	**Sivu- ja liitesivumäärä** 38
Ohjaajat Titta Ahlberg	

Tämä opinnäytetyö on HAAGA-HELIAn IT-yksikölle toimeksiantona toteutettu selvitys HAAGA-HELIAn tietoliikennelaboratorion tietoturvasta käyttäjien näkökulmasta.

Selvityksen tarkoituksena on tutkia tietoliikennelaboratoriossa käyttäjän kirjautumistunnuksia vaarantavien tietoturvauhkien toteuttamisen mahdollisuutta, helppoutta ja huomaamattomuutta.

Selvitys toteutetaan tunnistamalla kirjautumistunnuksia vaarantavat tietoturvauhkat ja selvittämällä uhkien toteutumisen todennäköisyys testaamalla käytännössä uhkien toteuttamisen helppous ja huomaamattomuus.

Tuloksena todetaan käyttäjien kirjautumistunnuksien vaarantavien tietoturvauhkien olevan tietoliikennelaboratoriossa vakavia ja mahdollisia toteuttaa.

Asiasanat
Tietoturva, tietoturvauhka, tietoliikennelaboratorio

HAAGA-HELIA
University of Applied Sciences

Abstract

19 May 2013

Degree programme in information Technology

Authors Sampo Tyllilä	**Group or year of entry** 2010
The title of thesis The information security in the data communications laboratory at HAAGA-HELIA University of Applied Sciences from the users' point of view	**Number of report pages and attachment pages** 38
Advisor(s) Titta Ahlberg	

The purpose of this thesis was to investigate the possibility, easiness and undetectability of executing data security threats that would endanger the user login credentials in the data communications laboratory of HAAGA-HELIA University of Applied Sciences. The study was carried out from the users' perspective. This thesis was assigned by the HAAGA-HELIA ICT unit.

The thesis was carried out by identifying the data security threats that endanger users' login credentials. The probability of executing data security threats was studied by testing the easiness and undetectability of data security threats in practice.

The thesis indicated that the data security threats endangering the user login credentials are severe and possible to execute in the data communications laboratory of HAAGA-HELIA University of Applied Sciences.

Key words
Information security, data security threat, data communications laboratory

Sisällys

1 Johdanto

Tietoturva on nykypäivänä suuressa osassa tietotekniikan laajentuessa myös oppilaitoksissa. Opiskelijoiden tietoturvatarpeet ovat entistä isomassa roolissa, sillä lähes kaikki opetusmateriaali, oppilaiden sekä opettajien tiedot ja tiedostot löytyvät oppilaitoksen tarjoamista palveluista kirjautumistunnuksia vastaan.

Tietoliikennelaboratorio on tietojenkäsittelyopiskelijoille tarkoitettu rajoittamattomampi käyttöympäristö harjoitusten ja projektien toteuttamiseksi. Tietoliikennelaboratorion käyttäjillä on enemmän oikeuksia tehdä muutoksia tietoliikennelaboratorion tietokoneisiin verraten esimerkiksi HAAGA-HELIAn IT-yksikön ylläpitämien käyttöympäristöjen tietokoneisiin. Muun muassa tietokoneen käynnistyksessä käytettävää lähdettä on mahdollista muuttaa käyttäjän haluamaksi.

Selvityksen aihe on tärkeä, sillä tietoliikennelaboratoriossa pidettävien kurssien teoriaopetus ja harjoitukset tapahtuvat samassa käyttöympäristössä, jossa opiskelijat tekevät kursseilla suoritettavia tehtäviä. Kursseilla käytetään HAAGA-HELIAn tarjoamia palveluja, sekä hyödynnetään sosiaalisen median palveluita ja pilvipalveluita. Käyttäjät käyttävät tietoliikennelaboratoriossa useita henkilökohtaisia kirjautumistunnuksia HAAGA-HELIAn tarjoamien kirjautumistunnusten lisäksi.

Selvitys keskittyy HAAGA-HELIAn Pasilan toimipisteessä olevan tietoliikennelaboratorion tietoturvan tutkimiseen käyttäjien näkökulmasta. Selvitys on rajattu koskemaan käyttäjien kirjautumistunnuksia. Tavoitteena on tuoda HAAGA-HELIA ammattikorkeakoulun tietoon sen tietoliikennelaboratoriossa työskentelevien käyttäjien kirjautumistunnuksiin liittyviä tietoturvauhkia, sekä tutkia niiden toteuttamisen helppoutta ja huomaamattomuutta.

Päätutkimusongelmat ovat

- Onko tietoliikennelaboratoriossa mahdollista toteuttaa käyttäjien kirjautumistunnuksia vaarantavia tietoturvauhkia?
- Kuinka helposti ja huomaamattomasti tietoturvauhkat voidaan toteuttaa?

2 Tietoliikennelaboratorio

Tietoliikennelaboratorio koostuu HAAGA-HELIAn Pasilan toimipisteessä olevista tietokoneluokista, joiden päätarkoitus on tarjota tietojenkäsittelyn koulutusohjelman tietoliikennelaboratoriossa järjestettävien kurssien opiskelijoille käyttöympäristö erilaisilla kursseilla käytävien harjoitusten tekoon (Ahlgren, J. 2013).
Opiskelijat saavat tietoliikennelaboratoriossa olevan tietokoneen hallintaansa ohjelmallisesti, joka sallii heidän asentaa tietokoneille haluamiaan käyttöjärjestelmiä ja ohjelmia lisenssien puitteissa. Tietoliikennelaboratorion tietokoneissa on kaksi kovalevyosiota, joista toisessa käytetään Windows 7 -käyttöjärjestelmää yleistä opetusta varten ja toiseen kovalevyosioon opiskelija saa asentaa valitsemiaan käyttöjärjestelmiä ohjelmistoineen. Windows 7 -käyttöjärjestelmässä oppilaalla ei ole ylläpitotason oikeuksia ja omien ohjelmien asennus on estetty. Toiselle kovalevyosiolle käyttäjä saa täydet oikeudet asentamiinsa käyttöjärjestelmiin. (Ahlgren, J. 2013.)
Tietoliikennelaboratorion tietokoneissa käyttäjä voi valita tietokoneen käynnistyksessä käytettävän lähteen, esimerkiksi ulkoisen laitteen kuten vaihtokovalevyn tai DVD:n, joka voi sisältää käyttöjärjestelmän asennustiedostot tai DVD:ltä suoraan käytettävän käyttöjärjestelmän. (Ahlgren, J. 2013).

Tietoliikennelaboratoriossa järjestetään teoriaopetusta sekä käytännön harjoituksia. Oppilaat syöttävät tietoliikennelaboratoriossa kirjautumistunnuksiaan tarvitsemiinsa koulun tarjoamiin palveluihin, kuten Moodle sivustolle saadakseen opetusmateriaalia käyttöönsä tai palauttaakseen harjoitustuloksia. Opetuksessa käytettävä materiaali löytyy lähes poikkeuksetta HAAGA-HELIAssa opetukseen käytettävältä Moodle sivustolta, jonka kirjautumistunnukset käyvät lähes kaikkiin HAAGA-HELIAn tarjoamiin opiskelijoiden tarvitsemiin välttämättömiin palveluihin, kuten henkilökohtaisen verkkolevytilan käyttöön ja HAAGA-HELIAn opiskelijoille tarkoitettuun käyttöympäristöön, sekä sähköpostiin kirjautumiseen. (Ahlgren, J. 2013.)

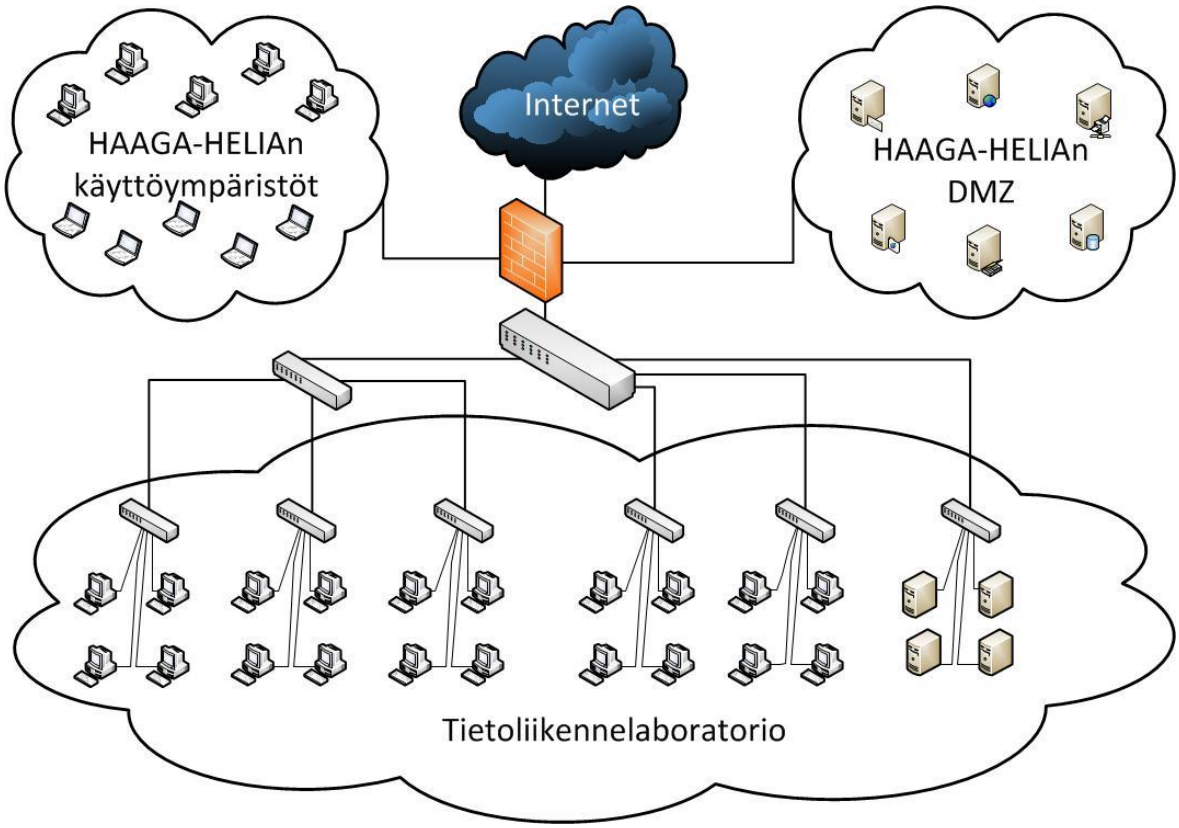
2.1 Rakenne

Tietoliikennelaboratorio koostuu opiskelijoiden käytössä olevista viidestä luokkatilasta, sekä toimintaan tarvittavista palvelimista ja kytkimistä. Jokainen tietoliikennelaboratori-

on tietokone on kytketty luokkatilassa olevaan kytkimeen. Kytkimet ovat edelleen yhdistetty HAAGA-HELIAn Pasilan toimipisteen kellarikerroksessa sijaitsevaan talojakamoon (kuvio1). (Ahlgren, J. 2013.)

Tietoliikennelaboratoriossa olevat palvelimet, sekä opettajatietokoneet ovat yhdistetty tietoliikennelaboratorion Windows-toimialueeseen ja niitä käytetään Windows-toimialueen kirjautumistunnuksilla. Opiskelijoiden käytössä olevia tietokoneita ei liitetä tietoliikennelaboratorion Windows-toimialueeseen. (Ahlgren, J. 2013.)

Tietoliikennelaboratorio on eristetty omaan fyysiseen verkkoonsa, joka on eristetty muista verkoista palomuurilla (kuvio 1) (Ahlgren, J. 2013).



Kuvio 1. Kuvaus tietoliikennelaboratorion rakenteesta HAAGA-HELIAssa.

2.2 Käyttäjät ja ylläpitäjät

Tietoliikennelaboratorion käyttäjät koostuvat tietojenkäsittelyn koulutusohjelman opiskelijoista ja opetuksesta vastaavista opettajista. Tietoliikennelaboratorion ylläpidosta vastaavat pääasiassa tietojenkäsittelyn koulutusohjelman opettajat HAAGA-HELIAn IT-yksikön avustuksella. (Ahlgren, J. 2013.)

HAAGA-HELIAssa jokainen kirjautumistunnuksen saanut henkilö joutuu hyväksymään kirjautumistunnuksia koskevat sopimusehdot, joissa määritetään opiskelijoille käyttöoikeuksien rajat. Sopimuksen mukaan opiskelija on vastuussa kirjautumistunnusten turvallisuudesta ja käyttäjätunnuksilla tapahtuvasta aineiston käytöstä. (HAAGA-HELIA 2012b.)
Vääriin käsiin joutuneet kirjautumistunnukset aiheuttavat mahdollisten vahingonteon sattuessa kirjautumistunnusten omistajalle vastuun korvauksista.

Tietoliikennelaboratoriokursseja käyville opiskelijoille kerrotaan kurssien yhteydessä sallitut ja kielletyt asiat myös lain näkökulmasta. Kielletyissä asioissa kerrotaan jo pelkän yrityksen olevan rangaistava teko. Ohjeistuksessa tulee myös ilmi tietoliikennelaboratorion kursseilla käytettävien käyttöjärjestelmien kirjautumistunnusten homogeenisuus, jonka takia verkkopalveluista kehotetaan kirjautumaan ulos ennen työasemalta poistumista. (HAAGA-HELIA 2012a.)

”Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.
Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta.
Yritys on rangaistava.” (Finlex 2013.)

3 Tietoturvauhkien tunnistaminen

”Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien ja palvelujen suojaamista sekä normaali- että poikkeusoloissa hallinnollisten ja teknisten toimenpiteiden avulla. Tietoturvallisuus rakentuu tiedon kolmen ominaisuuden - luottamuksellisuuden, eheyden ja käytettävyyden - turvaamisesta.” (Viestintävirasto 2012.)

Luottamuksellisuudella tarkoitetaan, että tietojen, järjestelmien ja palveluiden tulee olla vain saatavissa vain niihin oikeutetuilla henkilöillä ilman niiden paljastumista sivullisille (Viestintävirasto 2012).

Eheydellä tarkoitetaan, että tietojen, järjestelmien ja palvelujen tulee pysyä tallessa ja muuttumattomina laitteisto- ja ohjelmistovikojen, sekä luonnontapahtumien tai oikeudettomien ihmisten toiminnasta huolimatta (Viestintävirasto 2012).

Käytettävyydellä tarkoitetaan, että tietojen, järjestelmien ja palvelujen tulee olla tarvittaessa niihin oikeutettujen henkilöiden käytettävissä esteettä (Viestintävirasto 2012).

Selvityksen kannalta tietoturvallisuuden ulottuvuuksista oleellisin on luottamuksellisuus, sillä tavoitteena on turvata opiskelijan kirjautumistunnukset. Kirjautumistunnusten turvaaminen on oleellista, sillä niiden avulla pääsee käsiksi oppilaan henkilökohtaisiin tietoihin ja tiedostoihin, kuten sähköpostiin, verkkolevytilaan ja verkkopalveluissa sijaitseviin kurssitietoihin.

3.1 Tietoturvariskien hallinta

Tietoturvariski on vahingon vaara, joka kohdistuu tietoon tietoliikenteeseen tai tietojärjestelmään (Valtiovarainministeriö 2003, 78).

Tietoturvariskien hallinta on organisaation johdon vastuulla olevaa normaalia päätöksentekotoimintaa, jonka tavoitteena on taata toiminnan jatkuvuus (Valtiovarainministeriö 2003, 5).
Tietoturvariskien hallinta voidaan jakaa kolmeen vaiheeseen:

1. organisaation toiminnan kannalta tärkeiden tietojen ja niiden merkityksen tunnistaminen
2. tärkeisiin tietoihin liittyvien uhkien tunnistaminen ja arviointi
3. jatkotoimenpiteiden suunnittelu vahingon sattuessa

(Valtiovarainministeriö 2003, 9).

Selvityksessä keskitytään tietoturvariskien hallinnan toiseen vaiheeseen, eli tietoliikennelaboratorion käyttäjän kirjautumistunnuksiin liittyvien tietoturvauhkien tunnistamiseen ja arvioimiseen.

Tietoturvariskien hallinnassa uhkien tunnistaminen kannattaa toteuttaa organisaation toiminnan tuntevien henkilöiden kanssa ryhmätyönä (Valtiovarainministeriö 2003, 17).

Työryhmä sisältää vastuullisen vetäjän ja muun työryhmän. Työryhmässä suunnitellaan uhkien tunnistamisen toteutus, valitaan siihen käytettävä menetelmä, toteutetaan varsinainen uhkien tunnistaminen, sekä suunnitellaan jatkotoimenpiteiden organisointi. (Valtiovarainministeriö 2003, 17-18).

Uhkien tunnistamisen toteuttamiseen on erilaisia menetelmiä, joita voidaan käyttää myös rinnakkain. Menetelmiä ovat muun muassa kyselylomakkeet, haastattelut ja tarkistuslistat. Suunnitteluvaiheessa työryhmä miettii tunnistamiseen käytettävien menetelmien soveltuvuuden kohteeseen. (Valtiovarainministeriö 2003, 26.)

3.1.1 Uhkien tunnistamisen menetelmiä

Potentiaalisten ongelmien analyysi (POA) rakentuu useasta työryhmässä toteutettavasta vaiheesta. Potentiaalisten ongelmien analyysissa uhkien kartoitus toteutetaan työryhmän kesken aivoriihen muodossa. Aivoriihestä saadut ideat luokitellaan, jonka tuloksena saadaan jatkokäsittelyä vaativat uhkat, jotka otetaan yksityiskohtaisempaan tarkasteluun. Yksityiskohtaisemmassa tarkastelussa olevien uhkien riskin suuruus määritellään, jonka jälkeen suunnitellaan uhkiin varautuminen ja raportoidaan analyysityön tapahtumat huolellisesti. (Valtiovarainministeriö 2003, 69-73.)

Uhkapuut-menetelmässä uhkat jaotellaan järjestelmällisesti pienempiin osiin. Menetelmässä tietoturvaa koskevia uhkia jaetaan pienemmiksi niin kauan kuin mahdollista. Tämä tapa muodostaa uhkista puumallin. (Valtiovarainministeriö 2003, 28.)

Skenaariomenetelmä koostuu useiden tapausten läpikäymisestä, minkä avulla mahdolliset uhkat pyritään tunnistamaan. Menetelmä koostuu kahdesta vaiheesta, joista ensimmäisessä luodaan skenaariot ja toisessa muodostetaan tapausten pohjalta kuva suojausten nykytilasta ja tietoturvapuutteista. (Valtiovarainministeriö 2003, 28.)

Haavoittuvuusanalyysi perustuu aikaisempien riskitilanteiden ja tulevaisuudessa mahdollisten riskitilanteiden tunnistamiseen. Haavoittuvuusanalyysissa tunnistetaan suurimpiin riskeihin liittyvät osa-alueet, joiden perusteella pyritään vähentää riskien mahdollisuutta. (Valtiovarainministeriö 2003, 27-28.)

Tarkistuslista on karkea väline uhkien tunnistamiseen. Tarkistuslistoilla tunnistaa organisaatiota koskevat uhkat yksi kerrallaan. Tarkistuslistat eivät välttämättä kata täydellisesti organisaation toimintaan liittyviä uhkia, joten niitä käyttäessä kannattaa miettiä usean tarkistuslistan käyttöä. (Valtiovarainministeriö 2003, 30.)

3.1.2 Riskien suuruuden arviointi ja jatkokehityssuunnitelma

Uhkien tunnistamisen jälkeen arvioidaan riskien suuruus. Riskien suuruuden arviointi koostuu uhkan todennäköisyyteen ja siitä koituvien seurausten vakavuuden arvioimisesta. Nämä tiedot luokitellaan karkeasti taulukkoon, josta saa kuvan riskien keskinäisistä eroista. Taulukon perusteella voidaan muodostaa kuva riskien suuruudesta ja aloittaa jatkotoimenpiteiden suunnittelu. (Valtiovarainministeriö 2003, 41-43)

Jatkokehityssuunnitelma sisältää parannustoimenpiteitä tunnistettujen uhkien hoitamiseksi. Näistä suurimmat tunnetut riskit pyritään poistamaan ensi tilassa. (Valtiovarainministeriö 2003, 47)

3.2 Tutkimuksessa käytettävä uhkien tunnistamisen menetelmä

Tietoliikennelaboratorioiden käyttötarkoitus on erilainen kuin normaalitilanteissa oppilaitoksissa käytettävien tilojen, joten sen tietoturvauhkien tunnistamiseen tarvitaan joustavaa ja helposti selvitykseen sovellettavaa menetelmää. Yllä mainituista uhkien tunnistamisen menetelmistä potentiaalisten ongelmien analyysi soveltuu parhaiten selvityksen aikataulun ja resurssien puitteisiin.

Potentiaalisten ongelmien analyysissa uhkien tunnistaminen toteutetaan vaiheittain ryhmätyönä. Vaiheet jaetaan karkeasti neljään askeleeseen, uhkien tunnistamiseen, uhkien arviointiin, toimenpide-ehdotusten kehittämiseen ja analyysin raportointiin. (Valtiovarainministeriö 2003, 69-73.)

Uhkien tunnistaminen toteutetaan järjestämällä työryhmälle aivoriihiä. Aivoriihissä kerätään mahdolliset ongelmat ja uhkat, joista saadaan lajittelemalla jatkokäsittelyä vaativat uhkat. Jatkokäsittelyä vaativia uhkia tarkastellaan ja arvioidaan yksityiskohtaisemmin. (Valtiovarainministeriö 2003, 71.)

Toimenpide-ehdotusten kehittäminen toteutetaan kun jatkotoimenpiteitä vaativat uhkat on tarkasteltu ja arvioitu (Valtiovarainministeriö 2003, 73).

4 Tietoliikennelaboratorion tietoturvauhkien tunnistaminen

Työryhmä koostui kahdesta erillisestä ryhmästä, tietoliikennelaboratoriossa työskentelevistä opettajista, sekä HAAGA-HELIAn IT-yksikön IT-asiantuntijoista. Nämä ryhmät valittiin tietoturvauhkien tunnistamiseen, sillä molemmat ryhmät tuntevat kohteena olevan käyttöympäristön. Opettajien ryhmä tunnistaa tarkemmin tietoliikennelaboratorion toimintatavat ja mallit, kun taas IT-asiantuntijat tuntevat tietoturvariskit ja niiden menetelmät syvemmällä tasolla.

Aivoriihi koostui kahdesta vaiheesta. Ensimmäisessä vaiheessa opettajien ryhmälle pidettiin kokous, jossa käsiteltiin tietoliikennelaboratoriota koskevia tietoturvauhkia aivoriihen avulla ja kerättiin talteen tunnistetut uhkat. Toisessa vaiheessa pidettiin kokous IT-asiantuntijoille, jossa käytiin läpi opettajien ryhmän aivoriihestä saadut tulokset, tarkasteltiin tietoturvauhkatyyppejä syvällisemmin ja lajiteltiin ne kahteen ryhmään, erityisesti tietoliikennelaboratoriota koskeviin uhkiin ja myös HAAGA-HELIAn muissa käyttöympäristöissä toteutettaviin uhkiin.
Opettajille ja IT-asiantuntijoille järjestettyjen aivoriihien tuloksina tunnistetut tietoturvauhkat on kuvattu taulukossa 1. Taulukossa selvitetään koskeeko mahdollinen tietoturvauhka yleisesti HAAGA-HELIAn käyttöympäristöjä, vai erityisesti tietoliikennelaboratoriota. Erityisesti tietoliikennelaboratoriota koskeva tietoturvauhka on merkitty X-kirjaimella.

Taulukko 1. Aivoriihien tuloksena tunnistetut uhkat (liite2, liite3).

Tietoturvauhka	Selitys	Tietoliikennelaboratoriota erityisesti koskeva tietoturvauhka
Fyysinen näppäinpainallusten tallentaja	Tietokoneisiin kytketään fyysinen näppäinpainallusten tallentaja, joka tallentaa käyttäjän näppäinpainallukset.	
Kirjautumistunnusten	Samassa tilassa olevat	

vakoilu	henkilöt voivat nähdä kirjautumistunnukset kirjautumishetkellä.	
Käyttäjän omilta laitteilta leviävät haittaohjelmat	Opiskelijan omissa laitteissa olevat haittaohjelmat leviävät verkkoon.	
Lukittuun työasemaan tunkeutuminen	Tunkeudutaan tietokoneelta poistuneen opiskelijan lukittuun työasemaan.	**X**
Läpimeno salasanatiivisteellä – hyökkäys	Salasanatiivisteiden tulostamisen seurauksena mahdollinen suora hyökkäystapa käyttäjän tietokoneen haltuun saamiseksi.	**X**
Mies välissä – hyökkäys	Lähiverkossa toteutettu välimieshyökkäys kirjautumistunnusten saamiseksi.	**X**
Salasanatiivisteiden kopiointi	Käyttöjärjestelmiin tallennetut salasanat kopioidaan salasanatiivistemuodossa.	**X**
Ulkoverkosta pääsevät haittaohjelmat	Opiskelijan toiminnasta ulkoverkossa tarttuvat haittaohjelmat.	

4.1 Aivoriihien tulosten luokittelu

Aivoriihien tuloksina tunnistetut tietoturvauhkat voidaan jakaa kahteen kategoriaan, yleisiin tietoturvauhkiin ja erityisesti tietoliikennelaboratoriota koskeviin tietoturvauhkiin. Luokittelu on toteutettu IT-asiantuntijoiden aivoriihen yhteydessä.

4.1.1 Yleiset tietoturvauhkat

Yleisiin tietoturvauhkiin sisältyy fyysinen näppäinpainallusten tallentaja, kirjautumistunnusten vakoilu, käyttäjän laitteista, sekä ulkoverkosta verkkoon pääsevät haitat. Edellä mainitut tietoturvauhkat ovat mahdollisia käyttöympäristöstä riippumatta.

Fyysinen näppäinpainallusten tallentaja on yleisesti USB- tai PS/2-porttiin laitettava välikappale näppäimistön ja tietokoneen välissä, mikä tallentaa kaikki käyttäjän näppäinpainallukset tekstitiedostona fyysiseen näppäinpainallusten tallentajaan. Laite on mahdollista kytkeä niin tietoliikennelaboratorion tietokoneisiin kuin HAAGA-HELIAn käyttöympäristöjen tietokoneisiin.

Kirjautumistunnusten vakoilu on kirjautumistunnusten urkkimista samassa tilassa olevien henkilöiden toteuttamana. Tietoturvauhka olemassa tilasta riippumatta, jos muita henkilöitä on läsnä.

Käyttäjän omilta laitteilta leviävät haittaohjelmat ovat käyttäjän omille medioille tarttuneita haittaohjelmia, kuten viruksia, jotka leviävät käyttäjän liittäessä oman mediansa tietokoneeseen.

Ulkoverkosta pääsevät haitat ovat yleensä käyttäjän toiminnasta johtuvia tietokoneelle pääseviä haittaohjelmia, jotka käyttäjä ”kutsuu” ulkoverkosta tietokoneellensa.

4.1.2 Erityisesti tietoliikennelaboratoriota koskevat tietoturvauhkat

Erityisesti tietoliikennelaboratoriota koskevat tietoturvauhkiin lukeutuvat lukittuun työasemaan tunkeutuminen, salasanatiivisteiden kopiointi, mies välissä, sekä läpimeno salasanatiivisteellä –hyökkäys.

Lukittuun työasemaan tunkeutuminen on mahdollista tietoliikennelaboratoriossa, sillä kursseilla käytettävien käyttöjärjestelmien tai yleisesti käytetyissä käyttöjärjestelmissä kirjautumistunnukset ovat usein samat kaikille saman käyttöjärjestelmäkuvan käyttäjille. Käyttöjärjestelmän lukitseminen ei poista työasemaan tunkeutumisen mahdollisuutta, jos kyseessä on yleisesti kursseilla oleva käyttöjärjestelmä. HAAGA-HELIAssa jokaisella käyttäjällä on henkilökohtaiset tunnukset tunnuksia vastaavalle HAAGA-HELIAn käyttöympäristölle, mikä mahdollistaa työaseman lukituksen estäen muiden pääsyn tietokoneelle, ellei tunkeutuja tiedä tietokoneen lukittaneen käyttäjän kirjautumistunnuksia.

Salasanatiivisteiden kopiointi on mahdollista tietoliikennelaboratoriossa sillä tietokoneiden käynnistykseen käytetyn lähteen valitseminen on mahdollista, toisin kuin opiskelijoiden käytössä olevalla HAAGA-HELIAn käyttöympäristön tietokoneilla, joissa käynnistyksessä käytetyn lähteen valitseminen on estetty. Nykyisiin Windows käyttöjärjestelmiin tallentuu käyttäjän sisään kirjautuessa salasanatiiviste, joka on mahdollista kopioida erilaisilla työkaluilla. Tietoturvauhka koskee myös tietoliikennelaboratorion opettajien tietokoneita, joihin on tallentunut opettajien tietoliikennelaboratorion Windows-toimialueen ylläpitotason tunnukset. Tietoliikennelaboratorion Windows-toimialueen ylläpitotason käyttäjätunnusten avulla haitantekijä saattaa päästä vaikuttamaan tietoliikennelaboratorion palvelimiin vaarantaen koko tietoliikennelaboratorion.

Läpimeno salasanatiivisteellä –hyökkäys vaatii salasanatiivisteiden kopioimisen tietokoneilta ennen varsinaisen hyökkäyksen aloittamista. Onnistuneen hyökkäyksen jälkeen hyökkääjällä on mahdollisuus ottaa käyttäjän koko tietokone haltuunsa ja samalla saada käyttäjän kirjautumistunnukset sekä kaikki näppäinpainallukset selville. HAAGA-HELIAn käyttöympäristöjen käyttäjillä on yksilölliset kirjautumistunnukset, ja salasanatiivisteiden tulostaminen paikallisesti on estetty opetukseen käytetyssä HAAGA-HELIAN käyttöympäristössä estämällä käynnistyksessä käytetyn lähteen valitsemisen. Tämän vuoksi läpimeno salasanatiivisteellä –hyökkäys on tehoton opetukseen tarkoitetussa HAAGA-HELIAn käyttöympäristössä.

Mies välissä –hyökkäys on mahdollinen tietoliikennelaboratoriossa, jos hyökkääjä pääsee fyysisesti samaan verkkoon muiden käyttäjien kanssa. Hyökkäys vaarantaa käyttäjien verkkopalveluihin syöttämät kirjautumistunnukset. Hyökkäys on mahdollista toteuttaa ARP-väärennöksellä, ARP-taulun väärentämisellä, vale-DHCP-palvelimella, DNS-väärennöksellä ja DNS-välimuistin väärentämisellä.
HAAGA-HELIAn opetukseen tarkoitetussa käyttöympäristössä on estetty käynnistyksen lähteen valitseminen, joten hyökkääjä ei voi käyttää omaa käyttöjärjestelmäänsä hyökkäyksen toteuttamiseksi ja kytkiessään oman tietokoneensa HAAGA-HELIAn käyttöympäristön verkkoon, estetään tuntemattoman tietokoneen kommunikointi verkon yhdyskäytävän kanssa.

Kaikki tietoturvauhkat paitsi lukittuun työasemaan tunkeutuminen valittiin jatkotutkimusta varten, jossa tietoturvauhkat käytiin yksitellen läpi testien avulla. Testeissä arvioitiin tietoturvauhkan toteuttamisen mahdollisuus, helppous ja huomaamattomuus. Lukittuun työasemaan tunkeutuminen jätettiin jatkotutkimuksista pois, sillä tietoliikennelaboratoriossa järjestettävien kurssien käyttöjärjestelmien kirjautumistunnusten homogeenisuus on yleisesti tiedossa.

4.2 Tietoturvauhkien arviointi

Tietoturvauhkien arviointi toteutetaan testaamalla tietoturvauhkat käytännössä ja analysoimalla niistä saatuja tuloksia.
Testien tuloksien perusteella arvioidaan tietoturvauhkien onnistuneisuutta, toteuttamisen helppoutta ja huomaamattomuutta.
Selvityksessä tietoturvauhkan toteuttaminen on onnistunut, jos sille asetetut tavoitteet saavutetaan.
Tietoturvauhkan helppoutta mitataan sen valmisteluun ja toteuttamiseen kuluneella ajalla ja vaivannäöllä. Tietoturvauhkan toteuttamisen voidaan sanoa olevan helppoa, jos hyökkäyksen valmisteluun ja toteuttamiseen ei kulu kohtuutonta aikaa ja toteuttaminen onnistuu valmiita työkaluja käyttäen.
Huomaamattomuutta mitataan käyttäjälle näkyvänä epätavallisen toiminnan perusteella. Huomaamaton tietoturvauhka ei näy käyttäjän näkymässä millään tavalla, kun taas hel-

posti huomattu tietoturvauhka ilmenee käyttäjälle palomuuri- tai virustorjuntaohjelman ilmoituksena tai muuten selvästi epätavallisena toimintana näytön kuvaruudulla.

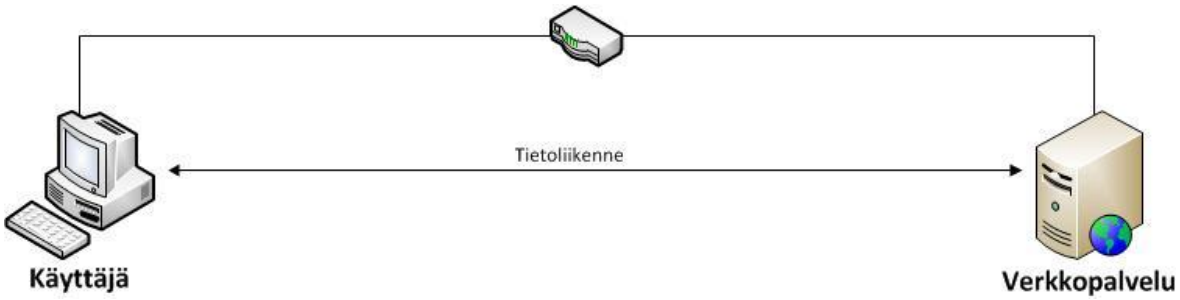
5 Tietoturvauhkien toteuttamistavat

Tietoliikennelaboratorion tietoturvauhkien tunnistamisesta saatujen jatkotoimenpiteitä vaativien tietoturvauhkien syvällisempi toteuttamistapojen tutkimus on esitetty tietoturvauhkatyyppien mukaisesti.

5.1 Mies välissä –hyökkäys

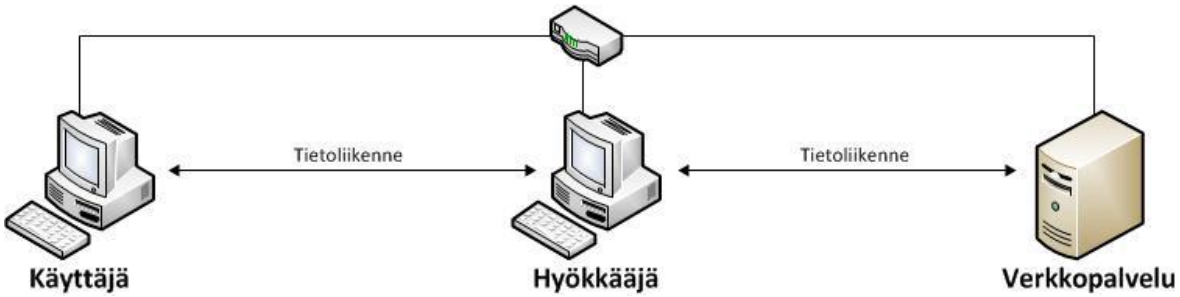
Mies välissä –hyökkäyksessä (Man in the middle) hyökkääjä pyrkii asettumaan uhrin ja verkkopalvelun tietoliikenneyhteyden väliin ja salakuuntelemaan tai muokkaamaan heidän välistä viestintää uhrien huomaamatta. (Erickson 2003, 186).

Normaalitilanteessa käyttäjä muodostaa tietoliikenneyhteyden suoraan verkkopalveluun (kuvio 4).



Kuvio 2. Yhteys ennen mies välissä -hyökkäystä.

Mies välissä –hyökkäyksen ollessa käynnissä uhrin tietoliikenne menee hyökkääjälle, joka välittää sen edelleen verkkopalveluun, jolloin hyökkääjä näkee kaiken uhrin ja verkkopalvelun välisen tietoliikenteen (kuvio 5).

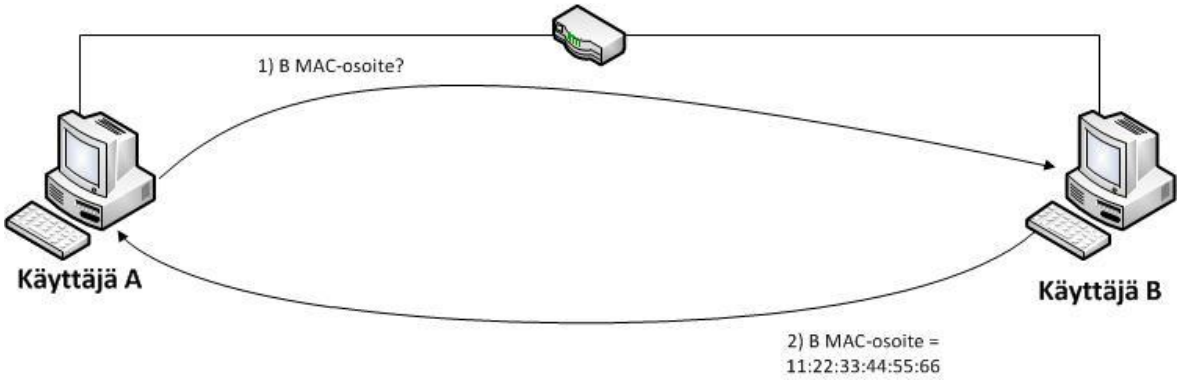


Kuvio 3. Yhteys mies välissä -hyökkäyksen jälkeen.

Mies välissä –hyökkäyksen voi toteuttaa monella eri menetelmällä ja niistä yleisimpiin lukeutuu ARP-taulun väärentäminen, sekä DNS-väärennös (Sanders 2010).

5.1.1 ARP-protokollan hyödyntäminen

ARP-protokollaa (Address Resolution Protocol) käytetään kun verkossa oleva laite haluaa tietää saman Ethernet-verkon toisen päälaitteen verkkotason osoitteen, eli MAC-osoitteen (Media Access Control) (Blank 2004, 35).
Käyttäjä A lähettää yleislähetyksenä kyselyn, jossa kysytään käyttäjän B MAC-osoitetta. Käyttäjä B tunnistaa itsensä kyselyn kohteeksi ja lähettää käyttäjä A:lle oman MAC-osoitteensa. (kuvio 6.)



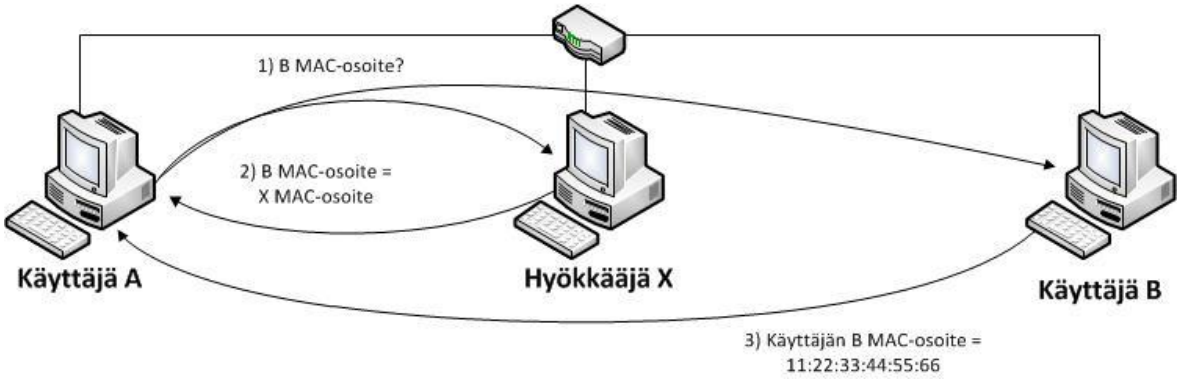
Kuvio 4. ARP-protokollan toiminnan kuvaus.

Kaikissa verkossa olevissa laitteissa on ARP-taulu, josta tarkistetaan osoiteparien olemassaolo ennen ARP-kyselyn lähettämistä. ARP-tauluun tallennetaan tilapäisesti ARP-kyselyiden vastauksista selviävät MAC- ja IP-osoiteparit. Vastauksista saadut käyttämättömät osoiteparit poistetaan ARP-taulusta kahden minuutin jälkeen tarpeettomina, ellei niitä tarvita uudestaan. Osoiteparien uudestaan tarvitseminen lisää niiden olemassaoloaikaa ARP-taulussa aina kahdella minuutilla 10 minuutin maksimiaikaan asti, minkä jälkeen osoiteparit poistetaan vanhentuneina. Osoiteparin poiston jälkeen kohdelaitteen IP-osoite joudutaan kysymään uudella ARP-kyselyllä. (Blank 2004, 35.)
ARP-taulu koostuu kolmesta eri tietueesta; IP-osoitteesta, MAC-osoitteesta ja tyypistä miten osoitepari on saatu. Tyyppi voi olla dynaaminen, jolloin osoitepari on saatu tauluun ARP-kyselyllä, tai staattinen, joka tarkoittaa osoiteparin olevan manuaalisesti asetettu. (Blank 2004, 35.)

ARP-protokollan ehdottomasti suurin heikkous on luottamus. Verkossa olevat laitteet luottavat ARP-kyselyn ja –vastauksen sisällön olevan paikkansa pitävää tietoa, joten

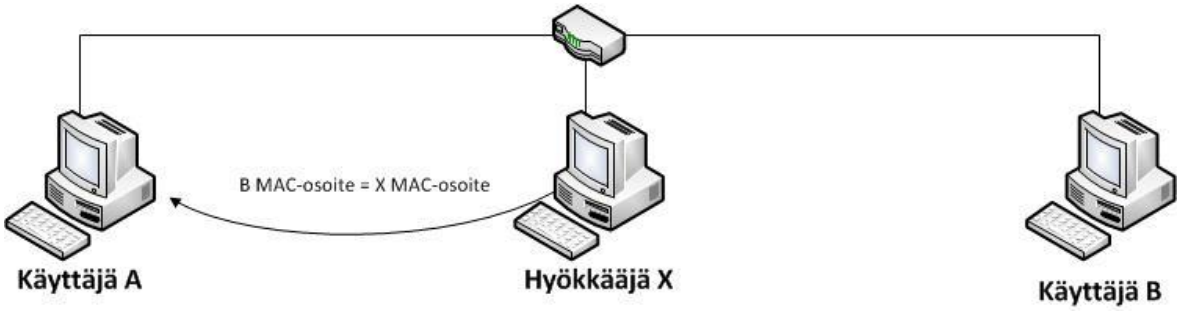
hyökkääjä voi lähettää väärennetyn ARP-vastauksen uhrille, joka tallentaa sen ARP-tauluunsa korvaten mahdollisesti aiemman olevassa olevan tietueen väärennetyllä. Tämä mahdollistaa mies välissä –hyökkäyksen toteutuksen ARP-kyselyjä ja –vastauksia muokkaamalla. (Krawetz 2006, 190-190.)

ARP-väärennös (ARP spoofing) perustuu ARP-protokollan ja sen heikkouksien hyödyntämiseen. ARP-väärennöstä pystytään hyödyntämään vain, jos hyökkääjä pääsee uhrin kanssa samaan verkkoon. ARP-väärennöksessä toimintaideana on vastata ARP-kyselyn lähettäneelle laitteelle nopeammin kuin kyselyn alkuperäinen kohdelaite, jolloin kyselyn lähettänyt laite tallentaa ARP-tauluunsa väärennetyn ARP-vastauksen. (Conway & Cordingley 2004, 42.)
Käyttäjä A lähettää yleislähetyksenä kyselyn, jossa kysytään käyttäjän B MAC-osoitetta. Hyökkääjä X lähettää vastauksen käyttäjälle A nopeammin kuin käyttäjä B, jolloin hyökkääjä X:n lähettämä vastaus tallentuu käyttäjän A ARP-tauluun. (kuvio 7).



Kuvio 5. ARP-väärennöksen toiminnan kuvaus.

ARP-taulun väärentämisessä (ARP-poisoning) laitteelle lähetetään ARP-vastaus, jota laite ei ole pyytänyt. ARP-vastaus sisältää IP-osoitteen ja sen omaavan laitteen MAC-osoitteen (Ciampa 2008, 106).
Hyökkääjä X lähettää väärennetyn ARP-vastauksen käyttäjälle A, vaikka käyttäjä A ei ole kysynyt käyttäjän B MAC-osoitetta. Käyttäjän A ARP-tauluun tallentuu hyökkääjä X:n lähettämä tietue. (kuvio 8.)



Kuvio 6. ARP-taulun väärentämisen toiminnan kuvaus.

Hyökkääjä voi käyttää ARP-taulun väärentämistä lähettämällä uhrilleen ARP-vastauksen, jossa on hyökkääjän MAC-osoite ja verkon yhdyskäytävän IP-osoite, ja lähettämällä yhdyskäytävänä toimivalle laitteelle ARP-vastauksen hyökkääjän MAC- ja uhrin IP-osoitteella. Hyökkääjän laitteen ollessa reitittävässä tilassa tietoliikenne kulkee uhrilta hyökkääjälle, joka välittää tiedon eteenpäin yhdyskäytävänä toimivalle laitteelle, ja yhdyskäytävältä tulevan liikenteen takaisin uhrille. (Ciampa 2008, 106.)

ARP-taulun väärentämistä hyödynnetään taulukossa 2 kuvattuihin tarkoituksiin.

Taulukko 2. ARP-taulun väärentämisen käyttötarkoitukset.

Tulos	Kuvaus
Tiedon varastaminen	Hyökkääjä korvaa oman MAC-osoitteensa ja varastaa toiselle taholle tarkoitettua tietoa.
Internetiin pääsyn estäminen	Hyökkääjä korvaa ARP-vastaukseen yhdyskäytävän MAC-osoitteen väärennetyllä osoitteella, jota ei lähiverkossa ole olemassa, ja lähettää sen uhrille. Tämä estää uhrilta Internetiin pääsyn.
Mies välissä -hyökkäys	Mies välissä –hyökkäyksessä hyökkääjä näkee kaiken tietoliikenteen uhrin tai uhrien ja reitittimen välillä syöttämällä niihin väärennetyt MAC-osoitteet.

5.1.2 DNS:n hyödyntäminen

DNS (Domain Name System) on Internetin nimipalvelujärjestelmä, joka mahdollistaa Internetin käytön nimillä IP-osoitteiden sijasta muuntamalla nimet IP-osoitteiksi. Internetiin kytketyt ohjelmat kommunikoivat keskenään numeraalisilla arvoilla (IP-osoite). IP-osoitteiden muistaminen olisi ihmisille vaikeaa, joten tätä varten käytetään nimiä, jotka on osoitettu niitä vastaaviin IP-osoitteisiin. (Blank 2004. 174.)
Tietokoneen nimen ja IP-osoitteen välinen suhde on määritelty DNS-tietueeseen, joka muistuttaa toimintamalliltaan puhelinluetteloa. DNS-tietueessa jokaiselle IP-osoitteelle on sitä vastaava verkkotunnus. DNS-tietueet löytyvät nimipalvelimilta, jotka ovat linkitetty toisiinsa. Käyttäjän yhdistäessä verkkotunnukseen tietokone kysyy ensin paikalliselta nimipalvelimelta verkkotunnuksen IP-osoitetta. Jos nimipalvelimen DNS-tietueessa ei löydy kyseisen verkkotunnuksen IP-osoitetta, ohjaa se kyselyn seuraavalle siihen linkitettyyn nimipalvelimeen ja niin edelleen, kunnes vastaus löytyy tai on löytymättä. (Blank 2004, 174.)

Käyttöjärjestelmissä on paikallinen hosts–tiedosto, johon on tallennettu ainakin laitteen paikallinen osoite ja sitä osoittava nimi. Laite tarkistaa ensisijaisesti hosts–tiedostonsa ja sen jälkeen DNS-välimuistinsa ottaessaan yhteyttä verkkotunnukseen tai IP-osoitteeseen. Jos verkkotunnus tai IP-osoite löytyy paikallisesta hosts–tiedostosta, käyttää laite siinä määriteltyjä tietueita. Muuten otetaan yhteys nimipalvelimeen. (Ciampa 2008. 103-104.)

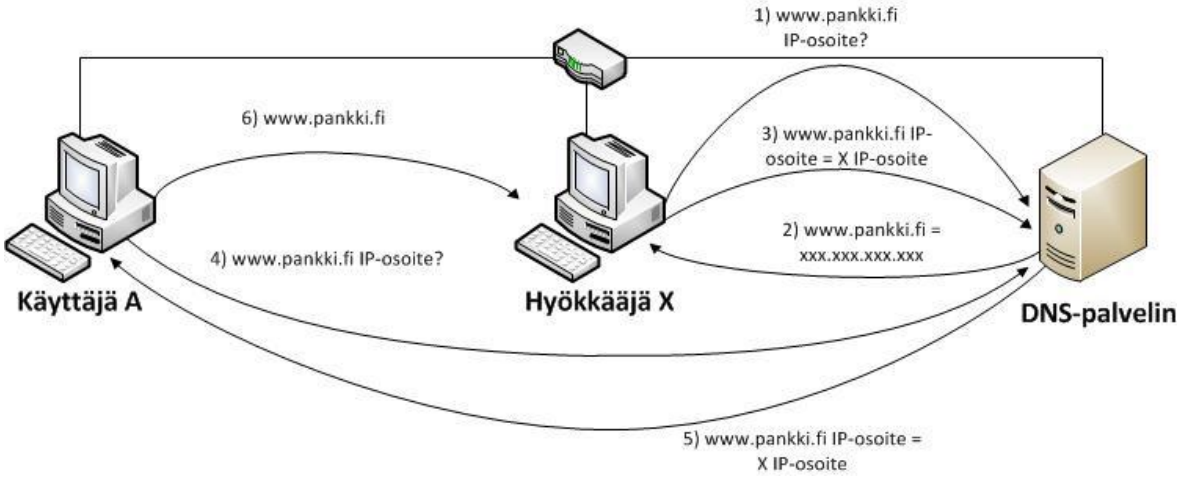
Käyttöjärjestelmissä hyödynnetään myös DNS-välimuistia, johon tallennetaan väliaikaisesti istunnolla käytettävät verkkotunnus- ja IP-osoiteparit. Tämä nopeuttaa DNS-välimuistissa löytyvien sivujen avaamista selaimella, koska verkkotunnuksia vastaavaa IP-osoitetta ei tarvitse uudestaan kysyä nimipalvelimelta. (Gibson 2011, 38.)

Paikallisen hosts-tiedoston, sekä DNS-välimuistin toimintaa voi hyödyntää DNS-välimuistin väärentämisessä (DNS poisoning).

DNS-väärennöksessä (DNS-spoofing) hyökkääjä huijaa uhria yhdistämään eri verkkotunnukseen, kuin uhri on alun perin menossa. Tämä voidaan toteuttaa, jos uhrin

verkossa toimiva DNS-palvelin saadaan vaarannettua ja syötettyä palvelimelle väärennettyä tietoa DNS-tietueeseen. (Graves 2010, 164.) Uhri voidaan huijata väärennetylle pankkisivustolle, jonne hän syöttää omat kirjautumistunnuksensa.

Hyökkääjä X kysyy DNS-palvelimelta www.pankki.fi IP-osoitetta. DNS-palvelin kertoo vastauksessaan www.pankki.fi:n IP-osoitteen. Hyökkääjä X lähettää väärennetyn DNS-vastauksen DNS-palvelimelle. Hyökkääjä X:n onnistuessa DNS-palvelin tallentaa DNS-väärennöksen sisältämät tietueet DNS-välimuistiinsa. Kun käyttäjä A kysyy DNS-palvelimelta www.pankki.fi:n IP-osoitetta ja saa vastauksena hyökkääjä X:n väärentämän DNS-tietueen. Käyttäjä A ohjautuu hyökkääjä X:n IP-osoitteeseen mennessään www.pankki.fi sivustolle. (kuvio 9.)

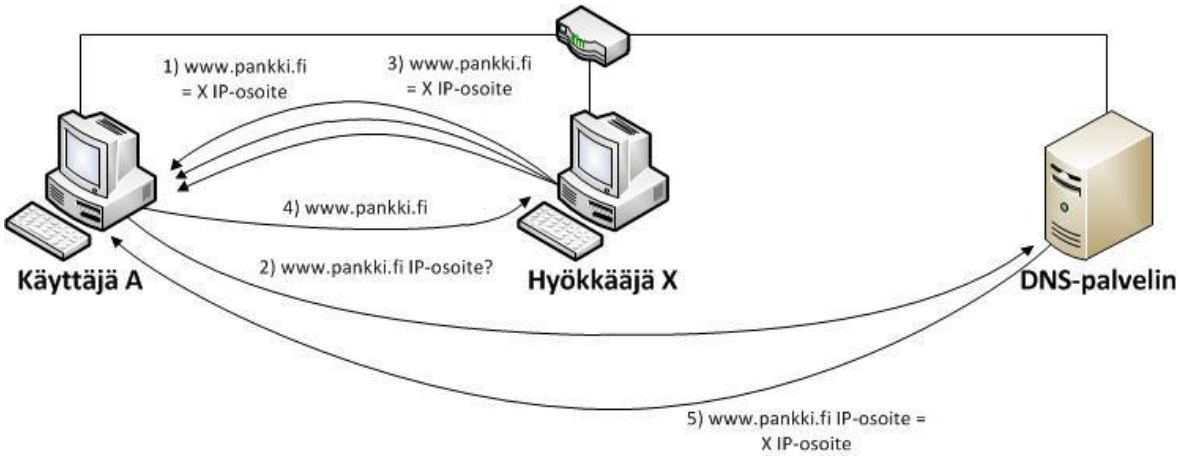


Kuvio 7. DNS-väärennöksen toiminnan kuvaus.

DNS-välimuistin väärentäminen (DNS-Poisoning) toimii samalla periaatteella kuin ARP-taulun väärentäminen. Hyökkääjä väärentää DNS-vastauksen ja lähettää sen suoraan kohteena olevalle laitteelle, tarkoituksenaan väärentää kohteen DNS-välimuisti väärentämillään IP-osoite- ja verkkotunnuspareilla (kuvio 10). Onnistuessaan myrkytyksessä uhri voidaan ohjata hyökkääjän haluamaan IP-osoitteeseen. (Krawetz 2006, 368-370.)

Hyökkääjä X lähettää toistuvasti väärennettyjä DNS-vastauksia käyttäjälle A. Käyttäjä A:n lähettäessä DNS-kyselyn DNS-palvelimelle saa se hyökkääjä X:ltä vastauksen kyse-

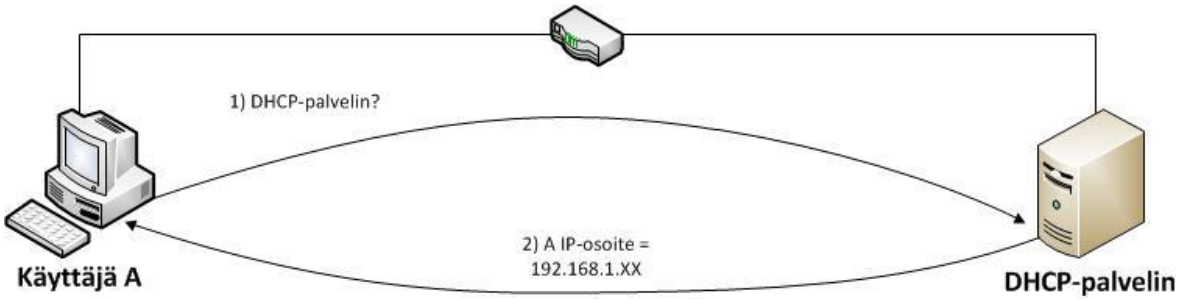
lyyn, jolloin käyttäjä A tallentaa DNS-tietueen omaan välimuistiinsa ja siirtyy sitä vastaavaan osoitteeseen, eikä välitä DNS-palvelimen vastauksesta. (kuvio 10.)



Kuvio 8. DNS-välimuistin väärentämisen toiminnan kuvaus.

5.1.3 Vale-DHCP palvelin

DHCP-palvelin on IP-osoitteiden automaattinen jakaja, jolla on määritetty IP-avaruus käytössään sisältäen jaettavat IP-osoitteet. Käyttäjäkone lähettää verkkoon liittyessään levitysviestillä paketin, jossa se kutsuu DHCP-palvelinta, joka kutsun vastaanottaessaan tarkistaa IP-avaruutensa vapaana olevien IP-osoitteiden varalta ja tarjoaa käyttäjän käyttöön vapaana olevan IP-osoitteen (kuvio 11). Käyttäjälle voi tulla useita IP-osoitteita verkossa olevilta DHCP-palvelimilta, joista se valitsee ensimmäisen tarjotun IP-osoitteen ja vastaa DHCP-palvelimelle hyväksyvänsä tarjotun IP-osoitteen. (Blank 2004, 99.)



Kuvio 9. DHCP-palvelimen toiminnan kuvaus.

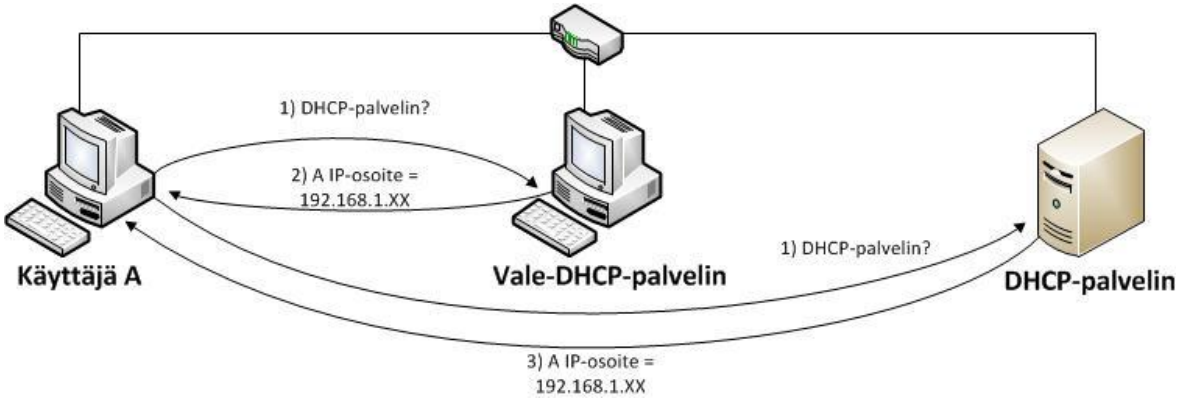
Vale-DHCP-palvelin (Rogue DHCP-server) on DHCP-palvelin, jota ei ole määritetty verkon varsinaiseen arkkitehtuuriin. Hyökkääjän istuttama vale-DHCP-palvelin

voi verkossa ollessaan määrittää DHCP:tä käyttäville työasemille vääriä IP-osoitteita tai monistaa alkuperäisiä IP-osoitteita. (Gupta 2002, 248-249.)

Tätä menetelmää voidaan käyttää palvelunestohyökkäyksessä estäen uhrien pääsy verkkoon, sekä mies välissä –hyökkäyksissä käyttäen hyökkääjän DHCP-palvelinta yhdyskäytävänä uhrien ja ulkoverkon välissä (Thompson 2005, 251).

Vale-DHCP-palvelinta voidaan myös käyttää hyväksi ARP-, sekä DNS-väärennöksien toteuttamisessa (Gupta & NIIT 2002, 243).

Käyttäjä A kutsuu DHCP-palvelinta. Vale-DHCP-palvelin vastaa nopeammin käyttäjä A:lle, jolloin käyttäjä A hyväksyy vale DHCP-palvelimelta saadun IP-osoitteen ja hylkää DHCP-palvelimelta saadun IP-osoitteen. (kuvio 12.)



Kuvio 10. Vale-DHCP-palvelimen toiminnan kuvaus.

5.2 Salasanatiivisteiden kopiointi

Salasanatiivisteiden kopiointi on suosittu tapa saada järjestelmien käyttäjätunnuksia. Salasanatiivisteiden kopioinnissa tavoite on saada salasanatiivisteet hyökkääjän haltuun, jotta ne voidaan purkaa tai hyödyntää sellaisenaan esimerkiksi läpimeno salasanatiivisteellä –hyökkäyksessä. Salasanatiivisteiden kopiointi käyttöjärjestelmästä onnistuu esimerkiksi Pwdump nimisellä avoimen lähdekoodin ohjelmakokoelmalla (Sikorski & Honig 2012, 236).

5.3 Läpimeno salasanatiivisteellä –hyökkäys

Läpimeno salasanatiivisteellä –hyökkäyksessä (Pass the hash attack) hyökkääjä tunkeutuu verkon yli uhrin tietokoneelle käyttäen hänen hallussaan olevia uhrin salasanatietoja sisältäviä LM (LAN Manager) ja NTLM (NT LAN Manager) salasanatiivisteitä. Toimenpide ei vaadi salasanatiivisteiden ratkomista selväkielisen salasanan selvittämiseksi,

mutta hyökkääjän on saatava salasanatiivisteet haltuunsa ennen hyökkäyksen toteuttamista. (Sikorski & Honig 2012, 236.)

6 Testit

Testit toteutettiin suunnittelemalla aluksi testien toteuttamisen kulku ja testeihin käytettävä ympäristö. Suunnittelun jälkeen toteutettiin varsinainen testaus, jonka tuloksia analysoitiin tietoturvauhkatyyppien mukaan.

6.1 Testien suunnittelu

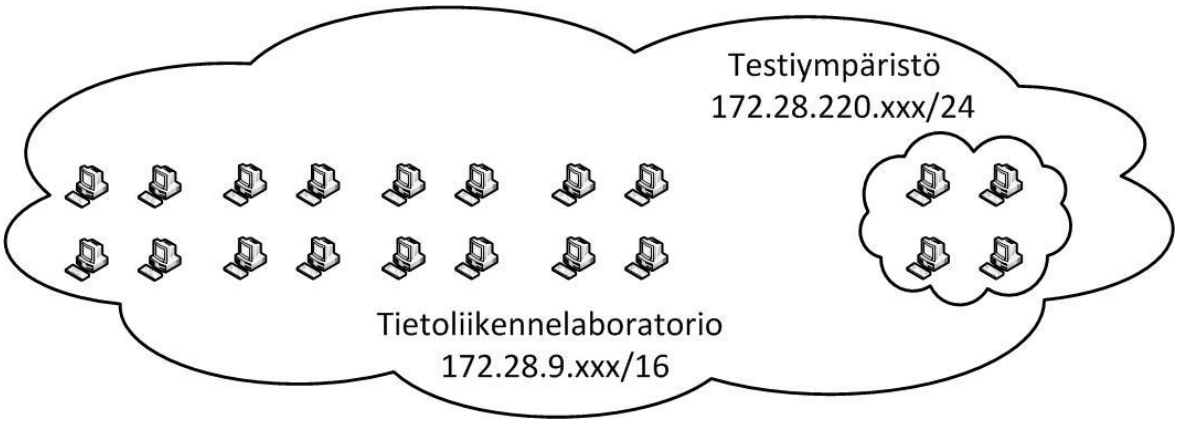
Testeihin valittiin jatkotoimenpiteitä vaativat tietoturvauhkat, joita ovat:

- mies välissä –hyökkäys
- salasanatiivisteiden kopiointi
- läpimeno salasanatiivisteellä –hyökkäys

Mies välissä –hyökkäyksen toteuttamiseksi on monta eri menetelmää, joten näistä valittiin yksinkertaisin ja helpoin toteuttamistapa, ARP-taulun väärentäminen. ARP-taulun väärentäminen valittiin testeihin, sillä sen toteutuksessa ei tarvitse tietää käyttäjän käyttämiä internet-sivustoja tai ohjata käyttäjää väärennetylle sivustolle, kuten DNS-välimuistin väärentämisessä. Vale-DHCP-palvelimen rakentaminen olisi ollut myös monimutkaisempi ja hitaammin toteutettavissa oleva vaihtoehto kuin ARP-taulun väärentäminen.

6.1.1 Testiympäristö

Testit toteutettiin tietoliikennelaboratoriossa muodostamalla neljälle koneelle oma aliverkko estäen yhteys muihin tietoliikennelaboratorion tietokoneisiin (kuvio 13).



Kuvio 11. Kuvaus testiympäristön rakenteesta tietoliikennelaboratoriossa.

6.1.2 Kohteena oleva käyttöjärjestelmä – Windows 7

Testien kohteena olevissa tietokoneissa oli käyttöjärjestelmänä yleiseen opetukseen tietoliikennelaboratoriossa käytetty Windows 7 64-bit Enterprise käyttöjärjestelmä, ilman uusimpia ohjelmistopäivityksiä. Käyttöjärjestelmän suojauksena oli oletuksena käytössä F-Secure Client Security 9.00, joka sisältää palomuurin, sekä viruksen- ja vakoiluohjelmien torjunnan. Windows:n oma palomuuri ei ollut oletuksena päällä.
Kohteeksi valittiin yleisesti opetukseen käytettävä Windows 7 käyttöjärjestelmä, sillä se on tietoliikennelaboratoriossa yleisimmin käytetty käyttöjärjestelmäkuva, jonka kanssa oppilaat kirjautuvat omilla kirjautumistunnuksillaan HAAGA-HELIAn tarjoamiin verkkopalveluihin opetuksen yhteydessä.

6.1.3 Hyökkäyksiin käytettävä käyttöjärjestelmä - BackTrack

Tutkimuksessa toteutettavaa testausta varten tarvittiin käyttöjärjestelmä, jonka avulla tietoturvauhkien toteuttaminen onnistui. BackTrack käyttöjärjestelmä sisältää tutkimuksen kannalta kaikki oleelliset työkalut tietoturvauhkien testaamiseen.

BackTrack on Linux-pohjainen vapaan lähdekoodin Ubuntu-jakelupakettiin pohjautuva Live DVD käyttöjärjestelmä, mikä on luotu varta vasten tietoturva-haavoittuvuuksien tutkimiseen. Live DVD formaatti mahdollistaa käyttöjärjestelmän käytön suoraan DVD:ltä ilman käytettävän tietokoneen kovalevylle asentamista; BackTrackin voi myös asentaa suoraan tietokoneen kovalevylle. (Ali & Heriyanto 2011, 9.)

BackTrack tarjoaa käyttäjälle kattavan tietoturvahaavoittuvuuksien testaamiseen tarkoitetun kokoelman ohjelmista. Ohjelmat voidaan jakaa seuraaviin kategorioihin (taulukko 3) (Ali & Heriyanto 2011, 9).

Taulukko 3. BackTrack:n sisältämät ohjelmat jaettuna kategorioihin.

Kategoria	Kategoria sisältää työkalut:
Tiedon kerääminen	tiedon keräämiseen kohteesta ja sen ympäristöstä.

Verkon kartoitus	verkon ja siinä olevien laitteiden kartoitukseen käyttäen esimerkiksi porttiskannausta.
Haavoittuvuuksien tunnistaminen	haavoittuvuuksien tunnistamiseen.
Web-ohjelmien analysointi	web-ohjelmien tarkkailuun ja analysointiin.
Radio verkon analysointi	langattomien verkon, bluetooth:n ja radiotaajuuksien analysointiin ja tarkkailuun.
Tunkeutuminen	toteuttamaan hyökkäyksiä kohdekoneelta löytyneisiin haavoittuvuuksiin.
Oikeuksien laajentaminen (eskalointi)	mahdollistamaan korkeimman tason oikeudet kohteessa.
Yhteyden ylläpito	ylläpitämään saatua yhteyttä kohteeseen.
IP-puheen analysointi (VOIP)	IP-puheen analysointiin.

6.1.4 Keskeisimmät työkalut

Tutkimuksen näkökulmasta keskisimmät BackTrack:n tarjoamat työkalut ovat arpspoof, bkhive, iptables, metasploit, netstat, nmap, samdump2 ja sslstrip.

Arpspoof uudelleenohjaa paketteja lähiverkossa kohteena olevalta laitteelta tai laitteilta toiselle laitteelle väärentämällä ARP-vastauksia (Irongeek 2013a).

Bkhive on Windows:n järjestelmä-avaimen saamiseksi suunniteltu työkalu. Järjestelmäavain on Windows:n ominaisuus, jolla lisätään ylimääräinen salauskerros tallennettuihin salasanatiivisteisiin. (Ubuntu packages, 2013a.)

Iptables on komentokehoteessa käytettävä ohjelma pakettien suodattamista varten (Ayuso).

Metasploit on vuonna 2003 julkaistu työkalu, jolla pystytään tunnistamaan tietoturvariskejä ja arvioimaan niiden haavoittuvuutta käytännön testeillä. Käyttäjä voi myös luo-

da metasploit:lla käytettäviä omia tietoturvatyökaluja, sekä hyökkäyksiä. (Gregg 2008, 203.)

Netstat ohjelmalla saadaan selville verkkoon liittyviä tietoja, kuten verkkoyhteydet. reititystaulut, verkkosovittimen tiedot, naamioidut yhteydet ja ryhmälähetys jäsenyydet (Ubuntu manuals 2010).

Nmap on verkon kartoitukseen tarkoitettu ohjelma, jolla voi muun muassa suorittaa porttiskannauksia (Lyon 1997).

Samdump2 on salasanatiivisteiden kopiointiin käytetty työkalu, joka vaatii Windows:n järjestelmä-avaimen (Ubuntu packages, 2013b).

Sslstrip työkalulla kaapataan verkossa liikkuva http-tietoliikenne ja seurataan https-linkkejä tai uudelleenohjauksia, mitkä muutetaan http-linkkejä muistuttaviksi tai homografisiksi https-linkeiksi (Marlinspike 2009).

6.2 Testaus

Testaus sisälsi erityisesti tietoliikennelaboratoriota koskevien jatkotoimenpiteitä vaativien tietoturvauhkien testaamisen. Testien tarkoituksena oli testata tietoliikennelaboratoriossa toteutettavien tietoturvauhkien toteuttamisen mahdollisuutta ja arvioida niiden toteuttamisen helppoutta ja huomaamattomuutta.

Testit salatussa liitteessä 1.

6.3 Tulokset

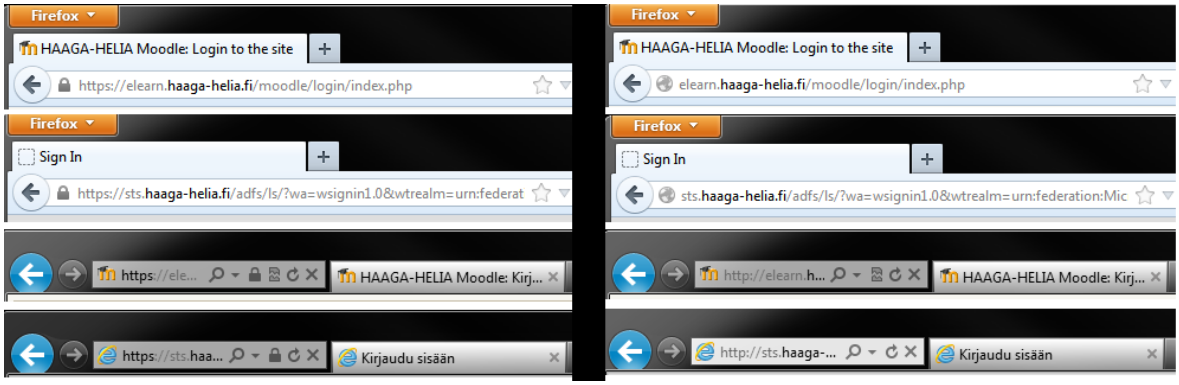
Testeistä saadut tulokset analysoitiin tietoturvauhkatyyppien mukaan. Analysoinnissa arvioitiin hyökkäyksen onnistuneisuutta, helppoutta ja huomaamattomuutta.

6.3.1 Salasanatiivisteiden kopioiminen

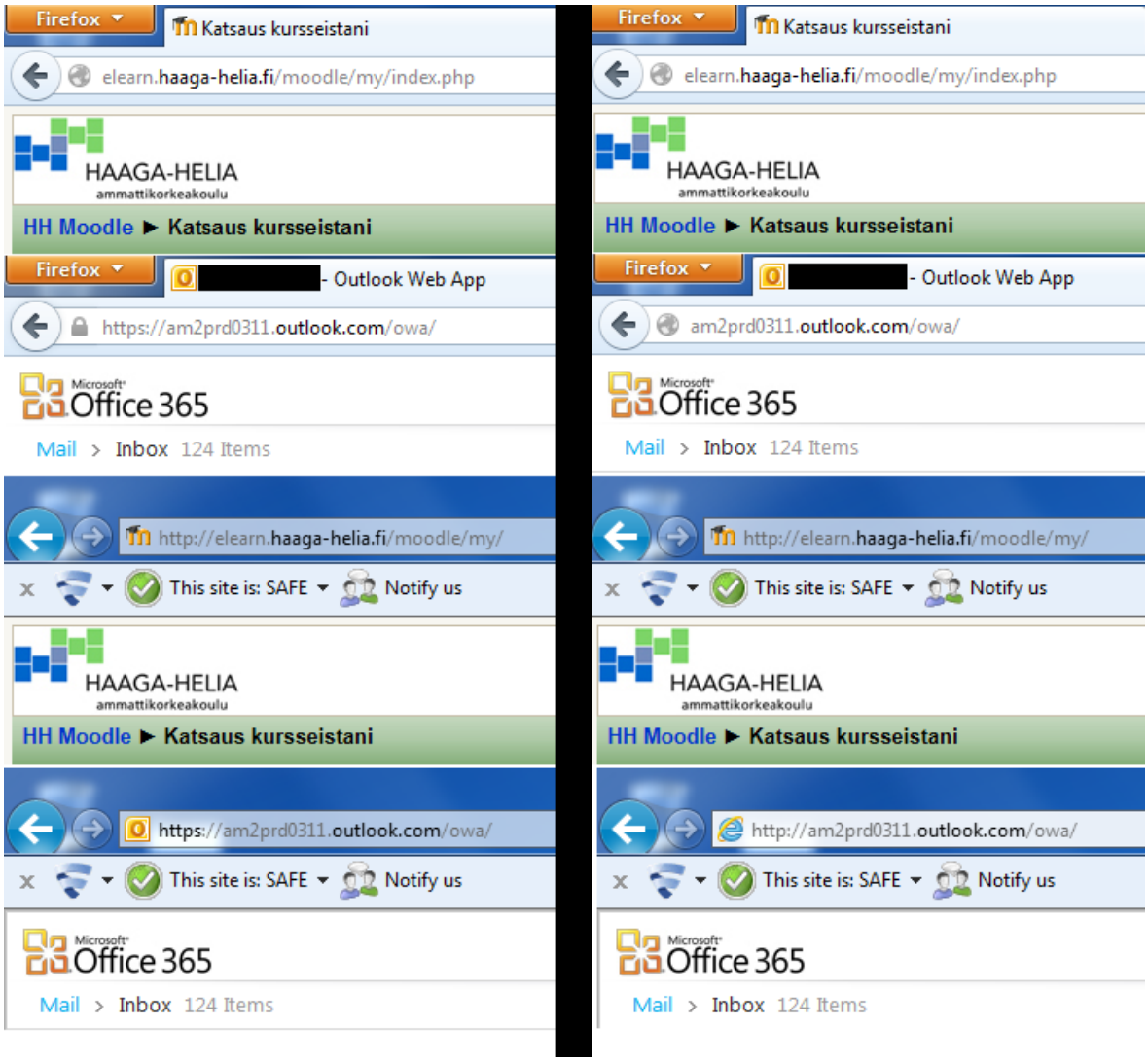
Salasanatiivisteiden kopioiminen onnistui helposti ja nopeasti kohteena olevalta tietokoneelta, jossa oli Windows 7 käyttöjärjestelmä asennettuna. Testeissä toteutettu salasanatiivisteiden kopioiminen voi herättää huomiota, sillä kohteena olevalle tietokoneelle oli mentävä fyysisesti toimenpiteen ajaksi.
Salasanatiivisteitä voidaan yrittää purkaa internetissä olevilla salasanatiivisteiden purkamiseen tarkoitetuilla sivustoilla tai paikallisesti tietokoneella. Purkamisen onnistuttua hyökkääjällä on hallussaan tietokoneen sisältämät kirjautumistunnukset selväkielisellä salasanalla.
Toinen vaihtoehto salasanatiivisteiden käyttöön on läpimeno salasanatiivisteellä – hyökkäys, jolloin salasanatiivistettä ei tarvitse purkaa vaan sitä voi käyttää salasanatiivistemuodossa.

6.3.2 Mies välissä –hyökkäys

Mies välissä –hyökkäyksen toteuttaminen oli nopeaa ja helppoa. Käyttäjän kirjautumistunnukset saatiin tallennettua uhrin syöttäessä niitä verkkopalveluihin.
Kuvioissa 14 ja 15 näkyy vasemmalla puolella ilman hyökkäystä uhrin näkymä Moodle ja Mymail, HAAGA-HELIAn opiskelijoiden sähköposti, verkkopalveluista ja oikealla puolella näkymä verkkopalveluista hyökkäyksen ollessa käynnissä. Kuviossa 14 näkyy käyttäjän näkymä kirjautumishetkellä kun taas kuviossa 15 on näkymä kirjautumisen jälkeen. Kuvioissa 14 ja 15 kaksi ylintä kuvariviä ovat Mozilla Firefox selaimesta ja kaksi alinta kuvariviä Internet Explorer selaimesta.



Kuvio 14. Kuvaus verkkopalveluista kirjautumishetkellä.



Kuvio15. Kuvaus verkkopalveluista kirjautumisen jälkeen.

Kuviot 14 ja 15 kuvastavat hyvin mies välissä –hyökkäyksen huomaamattomuutta. Mies välissä –hyökkäyksen huomaamiseksi käyttäjän on tarkkailtava osoiteriviä ja huomattava esimerkiksi suojattua yhteyttä käyttävän sivuston ”https”-merkinnän puuttuminen, sivuston kuvakkeen erilaisuus normaaliin tilanteeseen verrattuna ja suojattua yhteyttä ilmaisevan lukon kuvakkeen puuttuminen.

6.3.3 Läpimeno salasanatiivisteellä –hyökkäys

Läpimeno salasanatiivisteellä epäonnistui kun kohteena olevassa tietokoneessa oli palomuuri päällä, poikkeuksena Windows palomuuri ja käyttäjän jakama kansio. Käyttäjän jakaessa verkkoon kansion avautui käyttöjärjestelmän portti 445 ulkoverkkoon.

Hyökkäys onnistui kun kohteena olevassa tietokoneessa ei ollut palomuuria päällä. Hyökkäyksen onnistuessa hyökkääjä sai kohteena olevan tietokoneen haltuunsa ylläpitotason oikeuksilla ja pystyi esimerkiksi tallentamaan kaikki kohteena olevan tietokoneen näppäinpainallukset mukaan lukien verkkopalveluihin syötetyt kirjautumistiedot. Hyökkäystä on vaikea huomata, sillä kohteena olevalle tietokoneelle ei käyttäjän silmissä tapahdu mitään työpöytänäkymässä näkyvää. Hyökkäys käynnistää kohteena olevalla tietokoneella viruksen, joka on naamioitu muistuttamaan nimeltään muita Windows:n prosesseja, kuten ”explorer.exe”.

7 Pohdinta

Selvitys keskittyi HAAGA-HELIAn Pasilan toimipisteen tietoturvaan käyttäjien näkökulmasta painottaen kirjautumistunnusten tietoturvaa. Lähtökohta tutkimukselle oli halu arvioida tietoliikennelaboratoriossa tietoturvauhkien toteuttamisen mahdollisuutta. Tutkimuksen tavoitteena oli selvittää mitä tietoturvauhkia tietoliikennelaboratoriossa on mahdollista toteuttaa ja kuinka helposti ja huomaamattomasti ne ovat toteutettavissa.

Selvityksessä tietoturvauhkien tunnistamiseen käytettiin pontentiaalisten ongelmien analyysi menetelmää, jossa tietoliikennelaboratoriota koskevat tietoturvauhkat tunnistettiin keskustelumuotoisten aivoriihien avulla. Menetelmä soveltui hyvin suppeaan tietoturvauhkien tunnistamiseen selvityksen toteuttamiseen käytettyyn aikaan nähden. Kattavampi tietoturvauhkien tunnistaminen olisi voitu toteuttaa käymällä yksitellen kaikki tietoliikennelaboratoriossa mahdollisesti toteutettavat tietoturvauhkat läpi. Kyseessä olisi ollut tällöin laajempi ja kattavampi selvitys, joka olisi vaatinut enemmän aikaa kuin selvitykseen oli varattu.

7.1 Johtopäätökset

Selvityksessä toteutettujen testien tulokset kertovat tietoliikennelaboratoriossa toteutettavien uhkien olevan osittain mahdollisia. Tulokset ovat luotettavia ja ne pysyvät samoina uudelleen toistettuina.

Salasanatiivisteiden kopioiminen tietoliikennelaboratoriossa on mahdollista ja helppoa toteuttaa, mutta sen toteuttaminen voi kiinnittää huomiota, sillä kohteena olevalla tietokoneella pitää olla salasanan kopioimisen aikana. Tietoliikennelaboratoriossa salasanatiivisteiden kopioimisen vakavuus on tietoturvan kannalta suhteellista, sillä tietokoneissa olevat käyttöjärjestelmät ovat oppilaiden omia asennuksia tai yleiseen opetukseen käytössä oleva Windows 7 levykuva, mitkä sisältävät vain käyttöjärjestelmiin kohdistuvia kirjautumistunnuksia, ei oppilaiden HAAGA-HELIAn palveluihin käyttämiä kirjautumistunnuksia. Yleisesti opetuskäytössä olevan Windows 7 käyttöjärjestelmän salasanatiivisteissä on paikalliset ylläpitotason kirjautumistunnukset, jotka toimivat

kaikkiin saman levykuvan omaaviin tietokoneisiin. Opettajien tietokoneilla on opettajien tietoliikennelaboratorion Windows-toimialueen ylläpitotason kirjautumistunnuksia, joiden avulla on mahdollista aiheuttaa vahinkoa tietoliikennelaboratorion Windows-toimialueella.

Läpimeno salasanatiivisteellä –hyökkäys osoittautui vaikeasti toteutettavaksi tietoliikennelaboratoriossa sinne asennettujen palomuurien ja virustorjuntojen ansiosta. Vaikka tietoliikennelaboratorio on opiskelijoille tarkoitettu vapaampi ympäristö, on sinne asennettu palomuuri ja virustentorjunta yleisesti opetukseen käytettyyn Windows 7 käyttöjärjestelmään opiskelijaa suojaamaan. Ilman suojauksia, olisi opiskelijan kaikki kirjoittama tieto vaarassa, mukaan lukien sähköpostiviestien sisältö.

Mies välissä –hyökkäyksen toteuttaminen tietoliikennelaboratoriossa on mahdollista, nopeaa, helppoa ja lähes huomaamatonta kohteena olevalle käyttäjälle. Hyökkäys on vakava, sillä hyökkääjä saa uhrin kirjautumistunnukset selkokielisinä, mikä tarkoittaa niiden käyvän sellaisenaan niitä vastaaviin palveluihin. Vakavuutta lisää myös internetin käytön lisääntyminen tietoliikennelaboratoriossa, kuten Facebook:n ja omien henkilökohtaisten sähköpostien käyttäminen, joiden kirjautumistunnukset vaarantuvat yhtäläisesti mies välissä –hyökkäyksessä.

7.2 Suositukset

Salasanatiivisteiden kopioimisen estäminen on vaikeaa, sillä tietoliikennelaboratorio on suunniteltu opiskelijoille vapaampaan käyttöön kuin esimerkiksi HAAGA-HELIAn opiskeluun tarkoitettu käyttöympäristö. Tietoturvan lisääminen poistamalla salasanatiivisteiden kopioimiseen tarvitut ominaisuudet poistaisivat samalla tietoliikennelaboratorion tarkoituksen, eli vapaampana käyttöympäristönä toimimisen. Opettajien tietokoneilta käynnistyksessä käytettävän lähteen valinta olisi suotavaa estää tai suojata salasanalla, jonka vain opettajat tietäisivät. Tällä tavalla poistettaisiin mahdollisuus opettajien tietoliikennelaboratorion Windows-toimialueen kirjautumistunnusten kopioimisesta.

Läpimeno salasanatiivisteellä –hyökkäys on tällä hetkellä estetty tietoliikennelaboratoriossa yleisesti käytössä olevassa Windows 7 käyttöjärjestelmässä F-secure:n palomuurilla

ja viruksentorjunnalla. Levykuvaa muuttaessa on syytä painottaa näiden ominaisuuksien pysyvyyttä, jotta läpimeno salasanatiivisteellä -hyökkäys olisi jatkossakin estetty.

Mies välissä –hyökkäyksen estämiseksi olisi yleisesti suotavaa käyttää kiinteitä ARP-tauluja. Käyttämällä kiinteitä ARP-tauluja ei huomioida ARP-taulussa kiinteästi määritettyjen tietueiden päivitystä ARP-vastauksilla. Tätä vaihtoehtoa voisi soveltaa tietoliikennelaboratoriossa esimerkiksi asettamalla tietokoneilla yleiseen opetukseen käytettyyn Windows 7 käyttöjärjestelmäkuvan ARP-tauluun kiinteästi yhdyskäytävänä toimivan laitteen MAC-osoite. Tämä toimenpide estäisi ARP-taulun väärentämisen kohteena olevalla koneella, mikä tarkoittaisi mies välissä –hyökkäyksen toteuttamisen estämistä. Toinen vaihtoehto olisi käyttää verkkoa kuuntelevaa ohjelmaa kuten Arpwatchia. Arpwatch seuraa IP-osoitteita vastaavien MAC-osoitteiden vaihtumista. Epätavallisen käyttäytymisen esiintyessä ohjelma lähettää ylläpitäjälle sähköpostina ilmoituksen toiminnasta. (SecurityFocus, 2010.)
Jälkimmäinen vaihtoehto ei tosin ole toimiva tietoliikennelaboratoriossa, sillä tietokoneet saavat IP-osoitteensa DHCP-palvelimelta, jolloin tietokoneiden MAC-osoitteita vastaavat IP-osoitteet vaihtuvat usein tietokoneen uudelleenkäynnistyksen yhteydessä.

Tietoliikennelaboratorion käyttäjiä olisi hyvä muistuttaa tietoturvallisesta tavasta toimia tietoliikennelaboratoriossa. Muistuttamisen voisi toteuttaa seinille laitetuilla julisteilla, joissa painotettaisiin osoiterivin tarkkailua verkkopalveluita käytettäessä, sekä kerrottaisiin lyhyesti tietoliikennelaboratoriossa ehdottomasti kielletyt asiat, kuten toiminta jonka seurauksena toisten käyttäjien kirjautumistunnukset vaarantuvat. Muistuttamiseen voisi myös hyödyntää yleisesti opetukseen käytetyn Windows 7 käyttöjärjestelmäkuvan työpöydän taustakuvaa lisäämällä taustakuvaan ohjeet tietoturvallisesta tavasta toimia tietoliikennelaboratoriossa. Ohjeet olisivat käyttäjän nähtävillä aina tietokoneelle kirjauduttuessa.

7.3 Oppiminen tutkimuksen aikana

Ennen selvitysprosessin aloittamista tietoni tietoturvasta, tietoturvariskeistä ja –uhkista oli suppea. Pääosin tietoni koostui salasanoihin ja niiden muodostamiseen liittyvistä seikoista. Selvityksen etenemisen myötä tietouteni tietoturvasta ja siihen liittyvistä asi-

oista syveni huomattavasti. Selvityksen edetessä huomasin kiinnittäväni enemmän huomiota omaan käyttäytymiseeni tietoturvan kannalta. Vahvistin salasanojani ja tarkkailin varsinkin verkkopalveluihin kirjautuessa kaikkea normaalista poikkeavaa.

Selvityksen tekeminen on opettanut minulle lähdeaineistojen etsimistä ja hyödyntämistä, sekä projektinhallintaa ja organisointia. Näiden taitojen omaaminen on hyödyllistä varsinkin projektityyppisissä työtehtävissä.

Lähteet

Ali, S & Heriyanto, T. 2011. BackTrack 4 : Assuring Security by Penetration Testing. Packt Publishing Ltd. Olton Birmingham, GBR.

Alvaro, L. GNU MAC Changer. Luettavissa. http://www.alobbs.com/macchanger. Luettu. 21.2.2013

Ayuso, P. The netfilter.org "iptables" project. Luettavissa. http://www.netfilter.org/projects/iptables/index.html. Luettu. 21.2.2013.

Blank, G. Andrew. 2004. TCP/IP Foundations. Sybex. Alameda, CA. USA.

Conway, R. & Cordingley, J. 2004. Code Hacking : A Developer's Guide to Network Security. Charles River Media / Cengage Learning. Hernon, Va, USA.

Ciampa, M. 2008. CompTIA Security+ 2008 In Depth. Course Technology / Cengage Learning. Boston, MA, USA.

Finlex, 2013. 19.12.1889/39. Luettavissa. http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001. Luettu 25.4.2013.

Gibson, D. 2011. Microsoft Windows Security Essentials. Sybex. Hoboken, NJ, USA.

Lyon, G. 1997. Nmap Security Scanner. Luettavissa. http://nmap.org/. Luettu. 21.2.2013.

Graves, K. 2010. CEH : Certified Ethical Hacker Study Guide. Sybex. Hoboken, NJ, USA.

Gregg, M. 2008. Build Your Own Security Lab : A Field Guide for Network Testing. Wiley. Hoboken, NJ, USA.

Gupta, R. 2002. Windows 2000 Security. Course Technology / Cengage Learning. Boston, MA, USA.

Gupta, R & NIIT (Corporation) Staff. 2002. Windows 2000 Security. Course Technology / Cengage Learning. Boston, MA, USA.
Erickson, J. 2003. Hacking : The Art of Exploitation. No Starch Press, Incorporated. San Francisco, CA, USA.

HAAGA-HELIA 2012a. Tietoturva. Luettavissa. http://www.haaga-helia.fi/fi/courses/ta/ict1ta003.html. Luettu 25.4.2013.

HAAGA-HELIA 2012b. Verkko-opiskelusopimus. Luettavissa. http://www.haaga-helia.fi/fi/palvelut-ja-yhteistyo/it-palvelut/kuvat-ja-liitteet/Verkko-opiskelusopimus.pdf. Luettu 25.4.2013.

Irongeek. 2013. Manual Reference Pages – ARPSPOOF (8). Luettavissa. http://www.irongeek.com/i.php?page=backtrack-3-man/arpspoof. Luettu. 25.2.2013.

Irongeek. 2013. Manual Reference Pages – DNSSPOOF (8). Luettavissa. http://www.irongeek.com/i.php?page=backtrack-3-man/dnsspoof. Luettu. 25.2.2013.

Jyväskylän yliopisto. Tietoturvauhat. Luettavissa. https://koppa.jyu.fi/avoimet/mit/virtuaaliset-oppimisympaeristoet/oppimisympaeristoejen-tietoturva/tietoturvariskit. Luettu 16.4.2013.

Krawetz, N. 2006. Introduction to Network Security. Course Technology / Cengage Learning. Boston, MA, USA.

Marlinspike, M. 2009. Sslstrip. Luettavissa. http://www.thoughtcrime.org/software/sslstrip/. Luettu. 25.2.2013.

Preetham, V. 2002. Internet Security and Firewalls. Course Technology / Cengage Learning. Boston, MA, USA.

Sanders, C. 2010. Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1). Luettavissa. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html. Luettu. 25.2.2013.

SecurityFocus, 2010. Arpwatch. luettavissa. http://www.securityfocus.com/tools/142. Luettu 30.4.2013.

Sikorski, M & Honig, M. 2012. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press. San Francisco, CA, USA.

Thompson, S. 2005. Software Vulnerability Guide. Course Technology / Cengage Learning. Boston, MA, USA.

Ubuntu packages 2013a. Bkhive. Luettavissa. http://packages.ubuntu.com/hardy/bkhive. Luettu. 25.4.2013.

Ubuntu packages 2013b. Samdump2. Luettavissa. http://packages.ubuntu.com/hardy/samdump2. Luettu. 25.4.2013.

Ubuntu manuals 2010b. Netstat. Luettavissa. http://manpages.ubuntu.com/manpages/lucid/man8/netstat.8.html. Luettu. 21.2.2013.

Valtiovarainministeriö 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Luettavissa. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf. Luettu. 1.3.2013.

Viestintävirasto 2012. Tietoturva ja –suoja. Luettavissa. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html. Luettu. 19.2.2013.