Jan Hellberg

EETTINEN HAKKEROINTI OSANA JÄRJESTELMÄN TIETOTURVAA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Hellberg, Jan
Eettinen hakkerointi osana järjestelmän tietoturvaa
Jyväskylä: Jyväskylän yliopisto, 2019, 27 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Makkonen, Pekka

Yhteiskunnan siirtyessä koko ajan kohti tietoyhteiskuntaa yhä useammat toiminnot tapahtuvat verkon välityksellä. Tämä on nostanut erilaisten hyökkäysten määrää ja pakottaa yritykset ja organisaatiot panostamaan tietoturvallisuuteensa. Yksi parhaista tavoista vastata tähän haasteeseen on käyttää eettistä hakkerointia. Tässä tutkielmassa pyritään selvittämään mitä eettinen hakkerointi on, miten sitä tehdään ja millaisia tuloksia sillä saavutetaan. Tutkielma on toteutettu kirjallisuuskatsauksena. Tutkielmassa päädyttiin tuloksiin, että eettiselle hakkerille on tarkat kriteerit mitkä on täytettävä ja hänellä on käytössään monenlaisia työkaluja. Tutkielmassa todettiin myös, että eettisellä hakkeroinnilla saavutetaan tarkkoja tuloksia ja se on tärkeä osa nykyajan tietoturvaa.

Asiasanat: eettinen hakkerointi, tietoturva, penetraatiotestaus

ABSTRACT

Hellberg, Jan
Ethical hacking as a part of systems information security
Jyväskylä: University of Jyväskylä, 2019, 27 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Makkonen, Pekka

The continuing rise of digitalization forces even more services to be conducted via internet. This raises the amount of attacks against these systems and forces companies and organizations to put more emphasis on their information security. One of the best ways to achieve this is to use ethical hacking. This thesis aims to answer the following questions: what is ethical hacking, how is it done and what results does it get? This thesis was done as a literature review. This thesis provided following results: ethical hackers must fulfil multiple criteria and he/she has a lot of tools at his disposal. The thesis also concluded that ethical hacking provides accurate results and it is an essential part of todays information security.

Keywords: ethical hacking, information security, penetration testing

KUVIOT

KUVIO 1 Penetraatiotestauksen vaiheet 16
KUVIO 2 Tutkimuksessa löydetyt haavoittuvuudet 21

TAULUKOT

TAULUKKO 1 Ohjelmien löytöjen osuus ammattilaisten löytämistä haavoittuvuuksista 21

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

KUVIOT

TAULUKOT

1 JOHDANTO 6

2 EETTINEN HAKKERI 8
2.1 Black hat hacking 8
2.2 White hat hacking 9
2.3 Grey hat hacking 10
2.4 Eettisen hakkerin sertifikaatit 11
2.4.1 CEH-Sertifikaatti 11
2.4.2 CISSP-Sertifikaatti 12
2.4.3 GPEN-Sertifikaatti 13
2.4.4 Pohdintaa sertifikaateista 13

3 EETTISEN HAKKEROINNIN MENETELMÄT 14
3.1 Penetraatiotestaus 14
3.1.1 Voimankäytön säännöt penetraatiotestauksessa 14
3.1.2 Penetraatiotestauksen kulku 15
3.2 Sosiaalinen manipulointi 18

4 EETTISEN HAKKEROINNIN HYÖDYT TIETOTURVASSA 19
4.1 Case 1 A comparison of the efficiency and effectiveness of vulnerability discovery techniques 19
4.2 Case 2 Penetration Testing for Web Services 20
4.3 Tutkimusten perusteella tehdyt havainnot 22

5 YHTEENVETO 23

LÄHTEET 25

1 JOHDANTO

Nykyaikana, kun yhteiskunta on siirtymässä koko ajan kohti tietoyhteiskuntaa, joten yritykset ja organisaatiot hoitavat yhä enemmän toimintojaan internetin välityksellä. Myös miljoonat ihmiset käyttävät esimerkiksi verkkosovelluksia hankkiakseen informaatiota, suorittaakseen rahallisia transaktioita ja seurustellakseen. Tämä näkyy myös näitä palveluita kohdistuneiden hyökkäysten määrässä (Scholte, Balzarotti & Kirda, 2012). Liikenne- ja viestintäviraston (2008) mukaan erilaiset sähköiset palvelut ja asiointi ovat aina vain keskeisemmässä roolissa niin julkisen kuin yksityisen sektorin palvelujärjestelmässä. Kansalaisten on myöskin voitava luottaa, että heidän käyttämänsä palvelut ovat turvallisia ja heidän tietojensa käsittely on asianomaisella tasolla. Erilaiset hyökkäykset verkko-, sekä fyysisiä järjestelmiä kohtaan ovat muuttuneet koko ajan hienostuneemmiksi ja monimutkaisemmiksi. Palvelun tarjoajien täytyy pystyä varmistamaan palveluidensa tuvallisuus ja erilaisten tietojen oikeaoppinen käsittely. Tietoyhteiskunnan muuttuessa näillä tarjoajilla on velvollisuus huolehtia palveluidensa turvallisuuden jatkuvasta ylläpitämisestä (Liikenne- ja viestintäministeriö, 2008).

Näiden syiden takia on yritysten ja organisaatioiden syytä kiinnittää yhä enemmän huomiota tietoturvallisuuteensa ja keksiä uusia ja toimivampia tapoja sen varmistamiseksi.

Tässä tutkielmassa perehdytään tietoturvallisuuden kannalta tärkeään ilmiöön: Eettiseen hakkerointiin (engl. Ethical hacking). Eettinen hakkerointi tarkoittaa sitä, että tietoturva-ammattilaiset yrittävät löytää järjestelmästä haavoittuvuuksia käyttäen samoja menetelmiä, kuin oikeat hyökkääjät ja raportoivat löytönsä järjestelmän omistajalle. Eettiset hakkerit myös antavat omistajille ohjeet, miten haavoittuvuudet korjataan (C. C. Palmer, 2001).

Tämä tutkimus pyrkii vastaamaan seuraaviin kysymyksiin:

- Mitä eettinen hakkerointi on ja mitä se sisältää?
- Minkälaisia eettisen hakkeroinnin menetelmiä on olemassa?
- Tavoitetaanko eettisellä hakkeroinnilla parempia tuloksia kuin ”perinteisillä” tietoturvan kokeilukeinoilla?

Tutkielma toteutettiin kirjallisuuskatsauksena, jonka pohjana toimi Pirhosen ja Jauhiaisen raportointiohje (2018). Tiedonhaussa käytettiin pääasiallisesti Google Scholar palvelua, IEEE exploreria sekä Scopusta. Tärkeimpiä hakusanoja olivat *ethical hacking, penetration testing* ja näiden suomennoksia. Lähteiden arvioinnissa käytettiin Julkaisufoorumia ja viitteiden määrää.

Tutkielman rakenne on seuraavanlainen; toisessa luvussa käsitellään mitä eettinen hakkerointi on ja miten erilaisia hakkereita erotellaan. Tässä luvussa esitellään myös erilaisia sertifikaatteja, mitä eettinen hakkeri voi suorittaa. Kolmannessa luvussa käydään läpi, millaisia työkaluja eettisellä hakkerilla on käytössään. Ensiksi käsitellään penetraatiotestaus, eli hallittu hyökkäys järjestelmään, ja kerrotaan mitä vaiheita siihen kuuluu. Luvussa myös esitellään sosiaalinen manipulointi, eli käyttäjän manipulointia antamaan salattuja tietoja. Neljännessä luvussa esitellään saatuja tutkimustuloksia eettisen hakkeroinnin toimivuudesta. Viides ja viimeinen luku on yhteenveto, joka pitää sisällään kirjoittajan pohdintaa. Yhteenvedossa esitellään myös mahdollisia jatkotutkimusaiheita.

2 EETTINEN HAKKERI

Tässä luvussa käydään tarkemmin läpi tutkielman keskeiset käsitteet: eettinen hakkerointi, white hat hacking, black hat hacking, grey hat hacking. Luvussa käydään myös läpi eettiseen hakkerointiin liittyviä sertifikaatteja.

Jotta voidaan perehtyä paremmin eettiseen hakkerointiin, on tiedettävä keitä eettiset hakkerit ja ylipäänsä hakkerit ovat. Perinteisesti hakkerilla tarkoitettiin henkilöä, joka tykkää askarrella ohjelmistojen tai elektronisten järjestelmien kanssa. Hakkerit etsivät uusia tapoja toimia elektronisesti ja nauttivat siitä. Nykyään hakkerilla tarkoitetaan henkilöä, joka tunkeutuu järjestelmiin pahantahtoisesti tavoitellen omaa etua: rahaa, mainetta tai vaikka kostoa. Hakkerit voivat myös muuttaa tai poistaa saamaansa tietoa (Farsole, Kashikar & Zunzunwala, 2010). Koska nimitys hakkeri oli alun perin tarkoitettu kohteliaisuudeksi, pyrkivät tietoturva-ammattilaiset käyttämään käsitettä krakkeri (engl. cracker) tai tunkeutuja kun puhutaan rikollisesta hakkerista.

Hakkerit voidaan jaotella omiin kategorioihinsa, white hat, black hat ja grey hat, heidän tarkoitusperiensä perusteella. Tämä ”hattuihin” perustuva jaottelu juontaa juurensa lännenelokuviin, joissa ”hyvät” tyypit käyttävät valkoisia hattuja ja ”pahat” käyttävät mustia hattuja (Wilhelm & Andress, 2010). Eettisillä hakkereilla on tyypillisesti vahvat ohjelmointi-, sekä tietokoneverkkotaidot ja he ovat olleet useita vuosia tietokonealalla (C. C. Palmer, 2001).

2.1 Black hat hacking

Tämä luku käsittelee ”perinteistä” hakkerointia, eli järjestelmään tehtävää hyökkäystä ilman omistajan lupaa, yleensä oman edun kartoittamista varten.

Black hat hacking (suom. mustahattu hakkerointi) tarkoittaa edellä mainittua rikollista hakkeria eli krakkeria. MOT määrittelee krakkerin seuraavanlaisesti: ”**krakkeri**[6] hakkeri (1), joka aiheuttaa vahinkoa esim. tuhoamalla tietoja t. käyttämällä niitä omiin tarkoituksiinsa.” Näillä rikollisilla hakkereilla on monenlaisia motiiveja, joiden perusteella he suorittavat hyökkäyksiään. Black hat -

hakkeri saattaa esimerkiksi hakea itselleen rahallista hyötyä tai pyrkiä hakemaan kostoa jollekin taholle (Meyers, Powers & Faissol, 2009). Rahallista hyötyä krakkeri pyrkii saamaan esimerkiksi varastamalla pankkitietoja, lukitsemaan tiedostoja ja pyytämään korvausta niiden avaamisesta tai varastamalla ja myymällä esimerkiksi isojen yritysten yrityssalaisuuksia (Barber, 2001). He saattavat myös esimerkiksi hakea arvostusta tai pyrkivät kartuttamaan niin sanottuja ”sotasaaliita”.

Meyersin, Powersin ja Faissolin (2009) mukaan rikollisilla hakkereilla voi myöskin olla poliittisia tai ideologisia motiiveja. Tällaisia krakkereita kutsutaan *haktivisteiksi.* Haktivistit voivat esimerkiksi käyttää hyödykseen palvelunestohyökkäyksiä haitatakseen haluamansa sivun toimintaa ja edistääkseen oman sanomansa levittämistä. Haktivismista hyvänä esimerkkinä toimii vuonna 2005 tapahtunut hyökkäys, jossa turkkilaiset hakkerit pyrkivät vahingoittamaan tanskalaisia sivustoja, jotka jakoivat profeetta Muhammadista tehtyä poliittista sarjakuvaa (Seebruck, 2015). Tutkielmassa käsitellään käsite palvelunestohyökkäys paremmin tulevissa kappaleissa. Varsinkin aloittelevilla krakkereilla motivaattorina saattaa myös toimia älyllinen haaste, addiktio tai pelkkä uteliaisuus, sillä tekninen kynnys suorittaa hyökkäyksiä on matala. Viimeinen käsiteltävä motivaattori rikollisille krakkereille on nationalismiin pohjautuva ja heitä voidaan kutsua ”kyberterroristeiksi”. Tällaiset kyberterroristit pyrkivät ajamaan oman valtionsa etua tekemällä hyökkäyksiä esimerkiksi toisen valtion järjestelmiin. Tällaiset hyökkäykset saattavat olla valtion tukemia (Seebruck, 2015).

Siinä missä eettiset hakkerit ovat tekniseltä osaamiseltaan ammattilaisia, on Black hat -hakkereiden osaamisessa suuriakin eroja. Alemman tietotason omaavat krakkerit käyttävät esimerkiksi helposti saatavia valmiita ohjelmia suorittaessaan hyökkäyksiä, kun taas korkean tietotason omaavat krakkerit kirjoittavat itse ohjelmansa (Rogers, 2006). Rogersin (2006) mukaan myös rikollisten hakkereiden käytössä oleva laitteisto on hyvin eritasoista; jotkut saattavat tehdä hyökkäyksiä vanhoilla kannettavilla tietokoneilla, kun toisilla on käytössään viimeisintä teknologiaa olevat laitteistot. Varsinkin edellä mainittujen kyberterroristien suorittamat hyökkäykset ovat todella hyvin rahoitettuja ja he käyttävät parasta teknologiaa. Tällaisesta kyberterrorismista hyvä esimerkki on vuonna 2007 Viroa kohtaan suoritettu kyberhyökkäys venäläisen sotamuistomerkin poistamisen jälkeen. Tässä hyökkäyksessä saatiin lamautettua verkkosivut Viron parlamentilta, usealta valtiolliselta sanomalehdeltä ja Viron keskuspankilta (Meyers ym., 2009).

2.2 White hat hacking

Tässä luvussa selitetään mitä white hat hacking tarkoittaa, eli omistajan luvalla suoritettavaa järjestelmän haavoittuvuuksien etsimistä.

White hat hacking (suom. valkohattu hakkerointi) on synonyymi tutkielmassa käytettävälle *eettiselle hakkeroinnille.* Kun aiemmin määritettyyn termiin

hakkeri lisätään termi *eettinen* (etiikkaan perustuva, moraalinen, MOT) saadaan käsite eettinen hakkeri eli valkohattuhakkeri. Yritysten miettiessä tapoja, joilla lähestyä hakkeroinnin esittämää uhkaa, päädyttiin tulokseen, että yksi parhaista tavoista arvioida oman järjestelmän turvallisuutta on palkata itsenäinen tietoturva-ammattilainen yrittämään murtautua järjestelmään. Nämä tietoturva-ammattilaiset, eli eettiset hakkerit, käyttävät samoja työkaluja ja tekniikoita kuin pahantahtoiset krakkerit, mutta he eivät vahingoita järjestelmiä eivätkä varasta tietoja. Eettiset hakkerit tekevät löytämistään aukoista raportin, jossa kerrotaan myös, miten ne korjataan ja antavat tämän raportin järjestelmän omistajalle (Farsole ym., 2010).

Eettisen hakkerin on oltava luotettava, sillä järjestelmään murtautuessaan he pääsevät käsiksi yritykselle tärkeisiin tietoihin, joiden ei todennäköisesti toivota päätyvän ulkopuolisten käsiin. Eettinen hakkeri pitää järjestelmää testatessaan niin sanotusti ”yrityksen avaimia” hallussaan. (C. C. Palmer, 2001). Valkohattuhakkeri eroaa rikollisesta mustahatusta etenkin valtuutuksen osalta. Siinä missä rikollinen krakkeri hyökkää järjestelmään omin lupinensa, on eettisen hakkerin ja järjestelmän omistajan sovittava valtuutuksesta. Järjestelmän omistajan luvan saamisen jälkeen on molempien osapuolten vielä sovittava suoritettavan testin laajuudesta; millaisia resursseja käytetään ja mihin järjestelmän aspekteihin keskitytään. Eettisen hakkerin on tarkasti pysyttävä saamiensa valtuuksien sisällä, eikä hän saa lähteä suorittamaan omia testejään (Engebretson, 2013). Eettisen hakkerin käyttämiä resursseja eli työkaluja käsitellään myöhemmässä luvussa. Eettisen hakkerin ammattitaitoa ja luotettavuutta voidaan arvioida esimerkiksi hänen hankkimiensa sertifikaattien avulla, joita käsitellään myöhemmässä luvussa.

2.3 Grey hat hacking

Aikaisemmissa luvuissa mainittujen valkohattujen ja mustahattujen lisäksi on olemassa niin sanottuja grey hat-hakkereita (suom. harmaahattu hakkeri), jotka putoavat edellä mainittujen hakkereiden välimaastoon. Harmaahattu eroaa mustahatusta siten, että mustahattu, eli rikollinen hakkeri, pyrkii järjestelmään ilman lupaa oman edun kartoittamiseksi, kun taas harmaahattu pyrkii järjestelmään myös ilman lupaa, mutta ei hae tällä omaa etuaan (Falk, 2014). Harmaahattu etsii oma-aloitteisesti järjestelmiä, joihin voi tunkeutua ja tuo nämä haavoittuvuudet järjestelmän omistajan tietoon. Harmaahatun ja mustahatun välinen ero on tapauskohtaisesti hyvin pieni, kuten esimerkiksi Anonymous-haktivistijärjestön toiminta (Chandrika, 2014).

2.4 Eettisen hakkerin sertifikaatit

Eettisille hakkereille on olemassa erilaisia sertifikaatteja, jotka takaavat hänen ammattitaitonsa ja luotettavuutensa. Suurin osa ammattimaisista eettisistä hakkereista hankkivat ainakin kaksi sertifikaattia olemassa olevista vaihtoehdoista (Caldwell, 2011). Seuraavissa alaluvuissa esitellään muutamia sertifikaatteja, jotka eettisen hakkerin on mahdollista hakea

2.4.1 CEH-Sertifikaatti

Tässä luvussa käsitellään EC-Councilin myöntämää Certified Ethical Hacker (CEH) sertifikaattia. Luvun tiedot on noudettu seuraavasta lähteestä (EC-Council, 2019). CEH-sertifikaatin tarkoituksena on määrittää ja valvoa minimistandardeja, joita eettiset hakkerit noudattavat ja tuoda esiin, että sertifikaatin saaneet henkilöt täyttävät tai ylittävät määritetyt standardit. Sertifikaatin saamiseksi on osoitettava tarpeelliset tietotaidot erilaisista eettisen hakkeroinnin menetelmistä. CEH-sertifikaatti on yksi yleisimmin hyväksytyistä sertifikaateista. Sertifikaatin saamiseksi on täytettävä tietyt kriteerit ja suoritettava tietotaitoa testaava koe. Täytettäviä kriteereitä on kaksi vaihtoehtoa: joko eettisen hakkerin on osallistuttava EC-Councilin järjestämään koulutukseen tai hänen tulee osoittaa työkokemus kahden vuoden ajalta informaatioturvallisuusalalta.

EC-Council järjestää itse koulutusta, jonka käytyään eettinen hakkeri voi hakea lupaa osallistua CEH-sertifikaattikokeeseen. EC-Councilin tarjoaman koulutuksen hinta on 850 dollaria ja sen voi suorittaa esimerkiksi virtuaalitilassa itsenäisesti tai ohjaajan kanssa. Koulutus pitää sisällään valtavan määrän informaatiota. Koulutukseen kuuluu esimerkiksi yli 140 työpajaa, jotka simuloivat oikean elämän tilanteita. Koulutuksessa tutustutaan myös yli 2200 yleisesti käytettyyn työkaluun, joita rikolliset hakkerit käyttävät. Teoreettisella puolella kurssilla on esimerkiksi yli 1685 diaa, joiden luvataan auttavan eettistä hakkeria ymmärtämään erityisen monimutkaisia turvallisuuskonsepteja. Koulutuksessa käydään läpi esimerkiksi verkkojen skannausta, sosiaalista manipulointia, palvelunestohyökkäyksiä ja langattomien verkkojen murtamista.

Toinen tapa, jolla eettinen hakkeri voi täyttää kriteerit kokeeseen osallistumiseen on aikaisempi työkokemus. Hakijalla pitää olla vähintään kahden vuoden työkokemus informaatioturvallisuuteen liittyvältä alalta. Hakijan on pystyttävä toimittamaan sellaisen suosittelijan yhteystiedot, joka pystyy varmistamaan, että hakijalla on hänen ilmoittamansa kokemus. Tällainen suosittelija voi olla esimerkiksi esimies tai valvoja.

Eettisen hakkerin täytettyä edellä mainitut kriteerit voi hän hakea lupaa osallistua sertifikaattikokeeseen. Luvan hakeminen maksaa 100 dollaria ja se on sisällytetty EC-Councilin järjestämän koulutuksen maksuun, joten erikseen sen joutuu maksamaan ne hakijat, jotka hakevat lupaa työkokemuksen perusteella. Luvan saatuaan hakijoille annetaan varmistusnumero, jolla he saavat ostaa koepaketin 950 dollarin hintaan. Koe koostuu 125 monivalintakysymyksestä,

jotka käsittelevät eettisen hakkeroinnin eri aspekteja, kuten erilaisia tietojärjestelmiä ja eettisen hakkerin etiikkaa. Koekysymykset otetaan kysymyspankista, jotta kokeen luotettavuus säilyy hyvänä. Kokeen kesto on noin neljä tuntia. Hyväksytyn kokeen jälkeen eettinen hakkeri saa itselleen CEH-sertifikaatin, joka on voimassa kolme vuotta.

2.4.2 CISSP-Sertifikaatti

Tässä luvussa käsitellään International Information System Security Certification Consortium, (ISC)², myöntämää Certified Information Systems Security Professional (CISSP) sertifikaattia. Luvun tiedot on noudettu seuraavasta lähteestä ((ISC)², 2019). CISSP-sertifikaatin tarkoitus on osoittaa, että sen omistavat henkilöt omaavat perinpohjaiset tietotaidot kyberturvallisuudesta ja pystyvät hyödyntämään niitä käytännön tilanteissa. CISSP-sertifikaatti toimii myös hyvänä osoituksena sen omistajana luotettavuudesta ja ammattietiikasta. CISSP on (ISC)²:n mukaan yksi halutuimmista sertifikaateista.

CISSP-sertifikaatin saamiseksi hakijalla pitää olla työkokemusta, läpäistä koe ja saada jo valmiiksi sertifikaatin omistavan henkilön suositus. Työkokemuksen osalta hakijalla on oltava viiden vuoden edestä työkokemusta vähintään kahdelta alalta (ISC)²:n määrittelemistä kahdeksasta. Näitä kahdeksaa alaa (ISC)² kutsuu nimellä ”Common Body of Knowledge” (CBK) ja ne toimivat myös vaaditun kokeen pohjana. Hakija voi korvata yhden vuoden työkokemuksesta, jos häneltä löytyy tietoturvallisuuteen liittyvän alan koulutus. Seuraavassa listassa on vapaasti suomennettuna kyseiset alat.

- Tietoturva ja Riskien hallinta (Security and Risk Management)
- Fyysinen tietoturva (Asset Security)
- Tekninen tietoturva (Security Engineering)
- Verkot ja tietoliikenne (Communications and Network Security)
- Pääsynhallinta (Identity and Access Management)
- Tietoturvan arviointi ja testaaminen (Security Assessment and Testing)
- Operatiivinen tietoturva (Security Operations)
- Ohjelmistokehityksen tietoturva (Software Development Security)

Työkokemuksen täytyttyä on hakijan valmistauduttava kokeeseen. Kokeessa on 100-150 kysymystä edellä mainituilta osa-alueilta. Hakija voi joko opiskella itsenäisesti tai osallistua (ISC)²:n järjestämään koulutukseen. Koulutusta voi suorittaa paikan päällä luokkahuoneessa, internetissä omaan tahtiin tai opettajan johdolla. Kokeen kesto on enintään kolme tuntia ja kielenä toimii englanti. Kokeen hinta on tutkielmaa kirjoitettaessa 650 euroa.

Hyväksytyn koesuorituksen jälkeen hakijan on toimitettava suositus henkilöltä, joka on hyväksytysti suorittanut CISSP-sertifikaatin. Suosituksen antaja todentaa hakijan ilmoittaman työkokemuksen ja sen, että hakija on hyvässä arvostuksessa ja omaa oikeanlaiset eettiset arvot. Sertifikaatti on voimassa kolme

vuotta, jonka aikana sertifikaatin haltijan on hankittava 120 CPE-pistettä (Continued Professional Education), joiden tarkoituksena on varmistaa, että tietotaitoa kehitetään sekä maksettava 85 dollarin vuosimaksut. CPE-pisteitä sertifikaatin haltija voi hankkia esimerkiksi osallistumalla erilaisiin opetustapahtumiin, lukemalla ja kirjoittamalla tutkimuspapereita tai tekemällä vapaaehtoistyötä alalla.

2.4.3 GPEN-Sertifikaatti

Tässä luvussa käsitellään Global Information Assurance Certificationin (GIAC) myöntämää GIAC Penetration Tester (GPEN) sertifikaattia. GPEN-sertifikaatin tarkoituksena on osoittaa, että sertifikaatin haltija omaa laajat tietotaidot erilaisista rikollisten hakkereiden käyttämistä hyökkäyksistä ja työkaluista. Sertifikaatin haltija on myös todistanut olevansa luotettava. Luvun tiedot on noudettu seuraavasta lähteestä (GIAC, 2019).

Aikaisemmin mainituista sertifikaateista GPEN eroaa sillä, että sen saamiseksi ei ole vastaavia kriteereitä, kuten työkokemusta tai tiettyä kurssia. GPEN-sertifikaatin saamiseksi on hakijan suoritettava 1899 dollaria maksava koe, joka pitää sisällään 82-115 kysymystä, jotka käsittelevät erilaisia penetraatiotestaamisen osa-alueita. Seuraavassa listassa on muutama näistä osa-alueista.

- Edistyneet salasanahyökkäykset
- Penetraatiotestauksen suunnittelu
- Tietoliikenteen skannaus ja analysointi

GPEN-sertifikaatin hakija voi opiskella itsenäisesti näitä osa-alueita tai hän voi osallistua erilaisille kursseille, jotka valmistavat tähän kokeeseen. Tällaista kurssia järjestää esimerkiksi GIAC:n perustanut SANS-instituutti. Kurssin hinta on 6610 dollaria ja sen kesto on viisi päivää. Tällaisella kurssilla käydään läpi ja suoritetaan erilaisia eettisen hakkeroinnin menetelmiä.

GPEN-sertifikaatin oikeuttavan kokeen suoritettuaan eettinen hakkeri saa itselleen neljä vuotta voimassa olevan todistuksen. Sertifikaatin uusiminen maksaa 429 dollaria ja sen voi uusia kahdella tavalla. Ensimmäinen tapa on käydä edellä mainittu koe uudelleen ja päästä se läpi. Toinen tapa on kerryttää edellisessä luvussa mainittuja CPE-pisteitä. CPE-pisteitä täytyy kerryttää 36 tämän neljän vuoden aikana.

2.4.4 Pohdintaa sertifikaateista

Aikaisempien lukujen perusteella voidaan todeta, että eettiselle hakkerille on olemassa monenlaisia sertifikaatteja mitä voi suorittaa. Tutkielman kirjoittajan mielestä sertifikaatteja ei voi suoraan verrata keskenään, sillä ne käsittelevät jokainen eri asioita eri tarkkuudella. On mielenkiintoista miten erilaisia vaatimuksia ja hintoja eri sertifikaateille on. Yksi jatkotutkimuksen aihe voisi olla, että miten sertifikaatit vaikuttavat eettisen hakkerin työllistymiseen ja palkkaan.

3 EETTISEN HAKKEROINNIN MENETELMÄT

Tässä luvussa käydään läpi erilaisia tunnettuja eettisen hakkeroinnin menetelmiä, kuten penetraatiotestausta, käyttäen erilaisia työkaluja ja sosiaalista manipulointia.

3.1 Penetraatiotestaus

Tässä luvussa käydään läpi eettisen hakkerin järjestelmän testauksen fyysistä, eli laitteistoon kohdistuvaa, testausta eli penetraatiotestausta. Luvussa käydään läpi mitä penetraatiotestaus on ja erilaisia työkaluja, mitä eettinen hakkeri käyttää suorittaakseen järjestelmän penetraatiotestausta, kuten Wireshark ja Kali Linux.

Penetraatiotestauksessa luodaan analyysi jostain systeemin aspektista, kuten siitä, että pystyykö hyökkääjä saamaan pääsyn salattuun tiedostoon. Penetraatiotestauksessa geneerinen tavoite, kuten ”murtaudu järjestelmään” on liian laaja, joten penetraatiotestauksessa pitää käydä ilmi, että halutaanko tietää, kuinka helppoa järjestelmään on murtautua, vai esimerkiksi, että onko olemassa useampi tapa murtautua kyseiseen järjestelmään (Bishop, 2007). Alaluvuissa käydään ensiksi läpi ennen varsinaisen penetraatiotestauksen suorittamista vaadittavaa sopimusta eettisen hakkerin ja yrityksen välillä. Tätä sopimusta kutsutaan voimankäytön säännöiksi. Seuraavassa alaluvussa esitellään varsinaisen järjestelmän fyysinen testaus eli penetraatiotestaus.

3.1.1 Voimankäytön säännöt penetraatiotestauksessa

Ennen kuin penetraatiotestausta aletaan suorittamaan, on yrityksen ja eettisen hakkerin sovittava niin sanotuista ”voimankäytön säännöistä”, joissa käydään läpi millä tavalla testi tullaan suorittamaan (Najera-Gutierrez & Ansari, 2018). Seuraavassa listassa esitellään mistä osapuolten tulisi ainakin sopia. Esitellyt asiat avataan paremmin omissa kappaleissaan.

- Penetraatiotestin tyyppi ja laajuus
- Asiakkaan IT-henkilökunnan yhteystiedot ja huomioiminen
- Herkkäluontoisen datan käsittely
- Tilannetapaamiset ja -raportit

Caldwellin (2011) mukaan, penetraatiotestin tyyppejä on kolmea erilaista: black box, white box ja grey box. Black box testauksessa eettiselle hakkerille ei anneta mitään muuta tietoa kuin yrityksen nimi. Loput testin kannalta tarpeelliset tiedot eettisen hakkerin on hankittava itse. Tällainen lähestymistapa on lähimpänä yleisimpiä hyökkäyksiä. Toisessa testaustyypissä, eli white boxissa, eettiselle hakkerille annetaan kaikki hänen haluamansa tieto. Tämä voi pitää sisällään esimerkiksi tiedon siitä, millaista verkkotopologiaa yritys käyttää ja millainen laitteisto heillä on käytössään. Tässä testaustyypissä saatetaan myös antaa esimerkiksi ohjelmiston koko lähdekoodi eettiselle hakkerille. Tämän kaltaisella testillä voidaan hyvin testata pystyvätkö esimerkiksi yrityksen sisäiset henkilöt tekemään asioita, joita heidän ei pitäisi pystyä tekemään. Viimeisessä testaustyypissä, eli grey boxissa, eettiselle hakkerille annetaan rajoitettu määrä tietoa. Täten voidaan simuloida esimerkiksi sosiaalisen manipuloinnin kautta saatujen tietojen käyttöä (Caldwell, 2011). Penetraatiotestin laajuudella tarkoitetaan sitä, että mitä järjestelmän osa-alueita testillä tutkitaan.

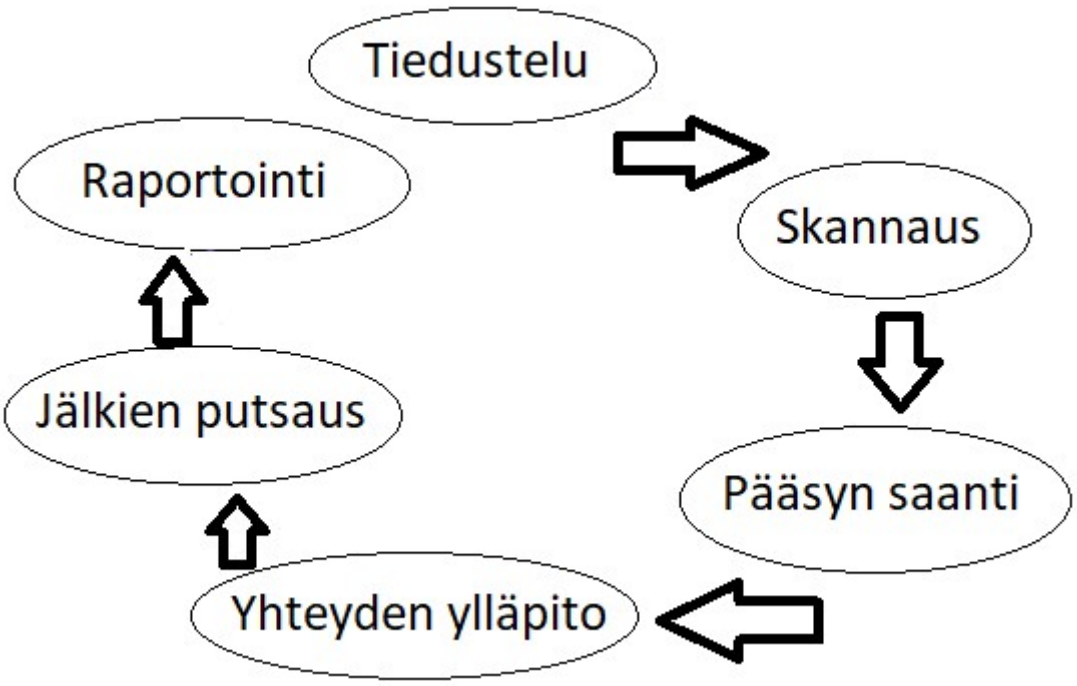
Asiakkaan IT-henkilökunnan yhteystietojen osalta pitää sopia siitä, että keneen eettinen hakkeri voi ottaa yhteyttä, jos testiä suoritettaessa tulee ongelmia. Tällainen ongelma voi olla esimerkiksi kohdetietokoneen kaatuminen, jonka ratkaisemiseksi se pitää käynnistää uudelleen. Penetraatiotestiä suoritettaessa voidaan myös testata IT-henkilökunnan reagoiminen oikeisiin hyökkäyksiin. Edellä mainitun syyn takia on siis sovittava, että tuleeko IT-henkilökunta olemaan tietoinen testistä vai ei. Jos kyseessä on testi, josta henkilökunta on tietoinen, pitää heille ilmoittaa tarkat päivämäärät, milloin testi tehdään ja IP-osoite, josta hyökkäys tulee (Najera-Gutierrez & Ansari, 2018).

Kuten luvussa 2.2 kerrottiin, saattaa eettinen hakkeri törmätä penetraatiotestausta suorittaessaan yrityksen arkaluontoiseen dataan. Eettisen hakkerin ja yrityksen on siis sovittava, miten tätä dataa käsitellään testin aikana. On syytä sopia esimerkiksi siitä, että käydäänkö testaajan ja yrityksen välinen kommunikointi salattuna ja miten eettinen hakkeri säilyttää saamaansa dataa. Sopimuksessa on myös syytä käydä läpi, milloin ja kuinka usein eettinen hakkeri raportoi edistyksestään yritykselle. Hyvän käytännön mukaista on, että eettinen hakkeri raportoi tarkat ajat, milloin hän on mitäkin hyökkäystä tehnyt, jotta yrityksen IT-henkilökunta voi tarkastaa omista raporteistaan, että miten yrityksen järjestelmät ovat reagoineet (Najera-Gutierrez & Ansari, 2018).

3.1.2 Penetraatiotestauksen kulku

Eettisen hakkerin ja yrityksen päästyä yhteisymmärrykseen voimankäytön säännöistä siirrytään varsinaiseen penetraatiotestaukseen. Voimankäytön sään-

nöissä määritellyn tyypin ja laajuuden perusteella eettinen hakkeri päättää miten ja millä työkaluilla hän suorittaa penetraatiotestauksen. Penetraatiotestauksen vaiheet on havainnollistettu kuviossa 1. Tutkielman selkeyttämisen vuoksi havainnollistetaan vain penetraatiotestaus verkon kautta, eikä keskitytä esimerkiksi paikan päällä tehtävään testaukseen.



KUVIO 1 Penetraatiotestauksen vaiheet (Patil, Jangra, Bhale, Raina & Kulkarni, 2017)

Penetraatiotestauksen ensimmäinen vaihe on tiedustelu. Tässä vaiheessa eettinen hakkeri pyrkii hankkimaan tarvitsemansa tiedot kohdejärjestelmästä. Voimankäytön säännöissä on saatettu määritellä testin tyypiksi ”white box”, jolloin eettisen hakkerin ei tarvitse itse hankkia tietoja. Tiedusteluvaiheessa eettisen hakkerin on saatava selville millaista laitteistoa kohdejärjestelmä käyttää, mitkä näistä laitteista ovat käytössä, onko verkossa avoimia portteja, millaista verkkoliikennettä porteista kulkee ja kohteen verkon kartoitus (Patil ym., 2017). Kohdejärjestelmän tietoja eettinen hakkeri voi hakea esimerkiksi ”whois” työkalun avulla. Työkalu on valmiiksi asennettuna esimerkiksi Kali Linux käyttöjärjestelmässä, jota eettiset hakkerit usein käyttävät. Whois työkalun avulla eettinen hakkeri saa tietoonsa paljon hyödyllistä tietoa kohteesta (Baloch, 2014).

Seuraavassa vaiheessa eli skannauksessa eettinen hakkeri etsii niin sanottuja ”avoimia ovia” järjestelmään. Skannauksen aikana eettisen hakkerin on etsittävä haavoittuvuuksia kohteesta. Tässä vaiheessa eettinen hakkeri pyrkii selvittämään kohteessa käytettävät käyttöjärjestelmät, palomuurit, mahdolliset tunkeilijan havaitsemisjärjestelmät ja millainen on kohdejärjestelmän verkkotopologia. Tämän jälkeen eettinen hakkeri aloittaa ensimmäisen hyökkäyksen,

jossa yritetään saada yhteys kohteeseen ja tämän avulla hankitaan lisää tietoa järjestelmästä (Patil ym., 2017). Tässä vaiheessa eettinen hakkeri voi käyttää avukseen Kali Linuxista löytyvää ”WhatWeb” työkalua. Whatweb pitää sisällään yli 1700 liitännäistä, joiden avulla eettinen hakkeri voi hakea järjestelmässä käytettäviä moduuleita, kuten JavaScript kirjastoja, Web-palvelimia ja SQL virheitä. WhatWeb-työkalun lisäksi Kali Linuxista löytyy Nmap-työkalu, joka pystyy kertomaan kohdejärjestelmän käyttöjärjestelmän, mahdolliset palomuurit ja avoimet portit (Baloch, 2014).

Kolmannessa vaiheessa eettinen hakkeri pyrkii saamaan itselleen pääsyn järjestelmään ja pitämään sen neljännessä vaiheessa. Aikaisempien vaiheiden perusteella löydettyjä haavoittuvuuksia hyödyntäen eettinen hakkeri yrittää päästä järjestelmään käsiksi. Usein tämä tarkoittaa salasanojen murtamista tai ohittamista. Tähän soveltuva ohjelma on esimerkiksi Kali Linuxista löytyvä ”John The Ripper”, jolla voi tehdä esimerkiksi väsytyshyökkäyksen, eli hyökkäyksen missä kokeillaan eri salasanavaihtoehtoja oikean löytämiseksi. Eettisen hakkerin päästyä sisään järjestelmään hän pyrkii pitämään itsensä sisällä järjestelmässä, jonka kautta hän voi pyrkiä murtautumaan muihin järjestelmiin ja etsimään tietoja (Patil ym., 2017). Eettinen hakkeri pyrkii hankkimaan itselleen mahdollisimman suuret oikeudet järjestelmän sisällä käyttämällä esimerkiksi Kali Linuxista löytyvää Metasploit-ohjelmistokehystä, tarkemmin Metasploitin sisältä löytyvää Meterpreteriä. Meterpreter sijaitsee kokonaan kohteen muistissa, eikä täten kirjoita mitään levylle. Meterpreteriä käyttämällä eettinen hakkeri voi tutkia kohdejärjestelmää tarkemmin ja suorittaa haluaamaansa koodia. Tavoitteena on saada järjestelmätason käyttöoikeudet, poistaa mahdolliset turvajärjestelmät, kuten palomuurit pois käytöstä ja mahdollisesti asentaa järjestelmään takaovi, jota eettinen hakkeri voi käyttää hyödykseen. Näiden jälkeen eettinen hakkeri on valmis tutkimaan järjestelmää tarkemmin ja suorittamaan penetraatiotestauksensa loppuun (Baloch, 2014).

Viidennessä vaiheessa eettinen hakkeri pyrkii tuhoamaan penetraatiotestauksen jättämät mahdolliset jäljet järjestelmän lokitiedostoista. Tällaisia jälkiä on voinut syntyä esimerkiksi kirjautumisyrityksistä. Eettinen hakkeri voi tässäkin vaiheessa käyttää hyväkseen Metasploit-ohjelmistokehystä taikka työkalua nimeltä OSForencics, joka on suunniteltu lokitiedostojen poistamiseen ja rekisterin putsaamiseen (Patil ym., 2017).

Viimeisessä vaiheessa eettisen hakkerin tulee kirjoittaa tekemistään löydöistä tarkka raportti järjestelmän omistajalle. Raporttia tehdessä tulee ottaa huomioon ketkä kaikki sen tulevat lukemaan ja mikä heitä siinä kiinnostaa. Toimitusjohtajaa tai hallitusta varten raportista tulee löytyä heitä varten tehty tiivistelmä, joka ei pidä sisällään teknisesti liian vaikeita termejä. Tästä tiivistelmästä tulee tulla ilmi selkeästi mitä penetraatiotestissä tehtiin, mikä sen tulos oli, mikä on eettisen hakkerin arvio mahdollisesta riskistä tällä hetkellä ja miten riski pienenee, jos aukot korjataan eettisen hakkerin kuvailemalla tavalla. Tiivistelmän lisäksi raportista pitää käydä teknisemmin ilmi, mitä haavoittuvuuksia eettinen hakkeri löysi ja miten niitä pystyi käyttämään hyväksi. Eettisen hakkerin on myös raportissaan kerrottava, miten nämä haavoittuvuudet voidaan kor-

jata. Raportista on hyvä löytyä jonkinlainen riskianalyysi järjestelmän heikkouksista (Baloch, 2014).

3.2 Sosiaalinen manipulointi

Eettinen hakkerointi ei rajoitu pelkästään järjestelmän fyysiseen testaamiseen vaan eettinen hakkeri pyrkii myös testaamaan käyttäjät. Tätä kutsutaan sosiaaliseksi manipuloinniksi, jossa eettinen hakkeri voi esimerkiksi kokeilla tietojenkalastelua järjestelmän käyttäjiltä. Yrityksen tietoturva ei ole taattu, vaikka yrityksellä olisi käytössään viimeisintä teknologiaa olevat järjestelmät ja tarkkaan mietityt tietoturvakäytänteet sillä sen käyttäjät pysyvät usein järjestelmän heikoimpana lenkkinä (Švehla, Sedinić & Pauk, 2016).

Sosiaaliseksi manipulaatioksi kutsutaan tietoturvahyökkäyksiä, joissa manipuloidaan käyttäjiä paljastamaan informaatiota, jota voidaan käyttää datan varastamiseen tai esimerkiksi, jolla saadaan pääsy järjestelmään (Peltier, 2006). Sosiaalisessa manipuloinnissa on tyypillistä, että hyökkääjä esittää olevansa esimerkiksi yrityksen työntekijä tai palveluntarjoaja ja rakentaa kohteen luottamusta käyttämällä esimerkiksi tunnettujen työntekijöiden nimiä, jolloin kohde uskoo hyökkääjän olevan kuka hän väittää olevansa. Tämän jälkeen hyökkääjä usein kehittää tarinan, jolla pyritään vetoamaan kohteen tunteisiin, jonka seurauksena hyökkääjälle annetaan hänen haluamansa tieto (Thornburgh, Oct 8, 2004).

Yksi sosiaalisen manipuloinnin yleisimmistä keinoista on tietojenkalastelu (engl. phishing). Yleisin tietojenkalastelukeino on väärennetyn sähköpostin lähettäminen, jonka avulla pyritään ohjaamaan käyttäjä väärennetylle sivulle, joka näyttää aidolta. Tällaisella tietojenkalastelusivustolla pyritään hankkimaan käyttäjän kirjautumistunnuksia, pankkitietoja tai esimerkiksi sosiaaliturvatunnusta (Chaudhry, Chaudhry & Rittenhouse, 2016). Moderneissa selaimissa on suojat, esimerkiksi osoiterivin luona näkyvä punainen lukko, jotka pyrkivät näyttämään käyttäjälle, että kyseinen sivu ei ole luotettava. Nämä suojat eivät kuitenkaan täysin takaa käyttäjän suojaa, sillä niihin ei esimerkiksi välttämättä osata kiinnittää huomiota (Alsharnouby, Alaca & Chiasson, 2015). Alsharnoubyn ym. (2015) suorittaman tutkimuksen mukaan käyttäjät eivät pystyneet tunnistamaan kaikkia tietojenkalasteluyrityksiä, vaikka he tiesivät etsiä niitä testin aikana.

4 EETTISEN HAKKEROINNIN HYÖDYT TIETOTURVASSA

Tässä kappaleessa käydään läpi, miten eettisten hakkerien suorittamat penetraatiotestaukset hyödyttävät erilaisten järjestelmien tietoturvaa verrattuna olemassa oleviin tietoturvan kokeilukeinoihin. Eettisen hakkeroinnin tärkeys yrityksille nousee esiin esimerkiksi EU:n yleisen tietosuoja-asetuksen artiklassa 32. Artikla 32 määrittelee, että järjestelmien tarjoajilla pitää olla prosessi, jonka avulla voidaan säännöllisesti testata, määrittää ja arvioida järjestelmän turvallisuutta (EU, 2016).

4.1 Case 1 A comparison of the efficiency and effectiveness of vulnerability discovery techniques

Tässä kappaleessa käydään läpi tämän tutkimuksen tekemät havainnot (Austin, Holmgreen & Williams, 2013). Austinin ym. (2013) suorittamassa tutkimuksessa pyritään vertaamaan neljän eri testaustavan avulla löydettyjä haavoittuvuuksia. Tutkimuksessa testattiin kolme eri järjestelmää: Tolven eCHR, OpenEMR ja PatientOS. Nämä kolme järjestelmää ovat terveydenhuollon elektronisia potilasjärjestelmiä.

Tutkimuksessa käytettiin neljää erilaista testaustapaa haavoittuvuuksien löytämiseksi: eksploratiivinen manuaalinen penetraatiotestaus, systemaattinen penetraatiotestaus, automatisoitu penetraatiotestaus ja staattinen koodin analysointi. Ensimmäinen testaustapa, eli eksploratiivinen penetraatiotestaus tarkoittaa sitä, että penetraatiotestausta lähdetään suorittamaan ilman tarkkaa suunnitelmaa testin kulusta. Testin kulku siis määräytyy tekijän ammattitaidon ja aikaisemman kokemuksen mukaan ja siinä kokeillaan erilaisia hyökkäyksiä satunnaisesti järjestelmän eri osiin. Toisessa testaustavassa, eli systemaattisessa penetraatiotestauksessa luotiin tarkka suunnitelma penetraatiotestauksessa suoritettavista hyökkäyksistä.

Kolmas testaustapa, eli automatisoitu penetraatiotestaus tarkoitti tutkimuksessa sitä, että järjestelmän haavoittuvuuksia kartoitettiin käyttämällä täysin automatisoitua IBM Rational AppScan-ohjelmaa. AppScan-ohjelmalle annettiin tunnukset järjestelmään, minkä jälkeen se yritti etsiä haavoittuvuuksia automaattisesti.

Neljäs testaustapa, eli staattinen koodin analysointi tarkoitti sitä, että Austin ym. käyttivät Fortify 360-ohjelmaa. Fortify 360 kävi automaattisesti läpi kohteiden lähdekoodia pyrkien löytämään haavoittuvuuksia.

Exploratiivisessa penetraatiotestauksessa käytettiin Tolven eCHR-järjestelmän testaukseen 15 tuntia, jonka aikana ei löydetty haavoittuvuuksia. OpenEMR-järjestelmän tutkimiseen käytettiin 30 tuntia aikaa, jonka aikana löydettiin 12 haavoittuvuutta. Näistä 12 haavoittuvuudesta, jokainen oli ”oikea” haavoittuvuus, eli sitä olisi pystynyt hyödyntämään oikeassa hyökkäyksessä. PatientOS-järjestelmään käytettiin aikaa 14 tuntia, jonka aikana löydettiin yksi haavoittuvuus.

Systemaattisessa penetraatiotestauksessa käytettiin 60 tuntia aikaa testin suunnitteluun ja 6-8 tuntia järjestelmien testaukseen. Suunnitelluista 137 testistä OpenEMR ei läpäissyt 63 testiä, Tolven eCHR 67 testiä ja Patient OS 37 testiä. Melkein kaikki haavoittuvuudet olivat sellaisia, että niitä olisi pystynyt hyödyntämään hyökkäyksessä.

Automaattisessa penetraatiotestauksessa Tolven eCHR-järjestelmän osalta AppScan-ohjelman annettiin skannata itsenäisesti kahdeksan tunnin ajan. Tänä aikana löydettiin 37 haavoittuvuutta, joista 22 olivat ”oikeita”. OpenEMR-järjestelmään käytettiin aikaa kuusi ja puoli tuntia, jonka aikana löydettiin 735 haavoittuvuutta, joista 710 olivat ”oikeita”. AppScan-ohjelmaa ei pystytty ajamaan PatientOS-järjestelmässä.

Staattisessa koodin läpikäynnissä löydettiin Fortify 360-ohjelman avulla Tolven eCHR-järjestelmästä 3765 haavoittuvuutta, joista 50 olivat ”oikeita. OpenEMR-järjestelmästä löydettiin 5036 haavoittuvuutta, joista 1321 olivat ”oikeita” haavoittuvuuksia. PatientOS-järjestelmästä löydettiin 12 333 haavoittuvuutta, joista 145 olivat ”oikeita” haavoittuvuuksia.

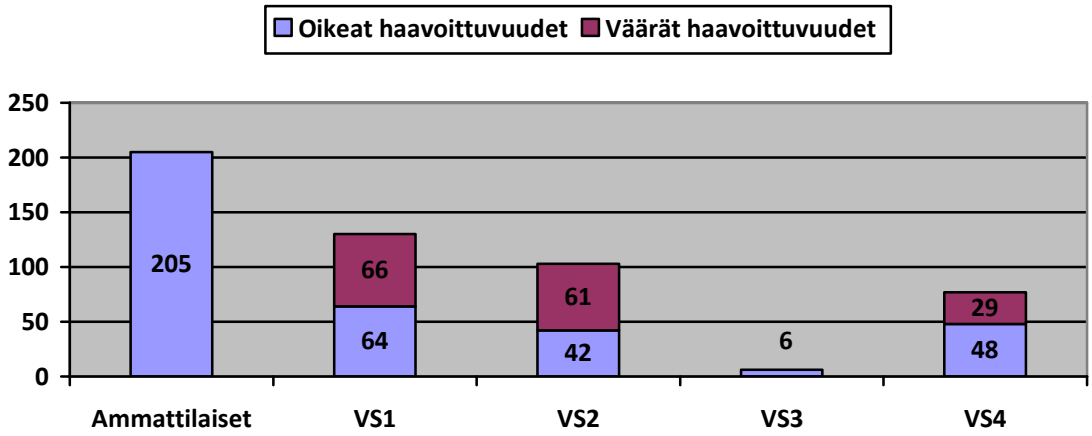
Yksikään tutkimuksessa käytetty testaustapa ei löytänyt kaikkia haavoittuvuuksia, vaan jokaisella tavalla löydettiin uniikkeja haavoittuvuuksia. Tutkimuksessa todettiin, että systemaattisella penetraatiotestauksella pystyttiin löytämään vakavimmat haavoittuvuudet, mitä muilla testeillä ei löydetty. Staattisella koodin analysoinnilla löydettiin eniten haavoittuvuuksia, mutta näiden läpikäynti oli aikaa vievä prosessi. Tutkimuksen tuloksena oli, että haavoittuvuuksia etsiessä kannattaa käyttää monenlaisia työkaluja parhaimman lopputuloksen saamiseksi. (Austin ym., 2013)

4.2 Case 2 Penetration Testing for Web Services

Tässä kappaleessa käydään läpi tämän tutkimuksen tekemät havainnot (Antunes & Vieira, 2013). Antunesin ja Vieiran (2013) suorittamassa tutkimuksessa

pyrittiin vertaamaan neljän eri automatisoidun ohjelman tehokkuutta haavoittuvuuksien löytämisessä. Näiden ohjelmien löytämiä tuloksia verrattiin tuloksiin, jotka löysi ryhmä, joka koostui neljästä ammattilaisesta.

Tutkimuksessa käytettiin seuraavia ohjelmia: HP WebInspect, IBM Rational AppScan, Acutenix Web Vulnerability Scanner ja nimeämätön akateeminen prototyyppi. Tutkimuksessa työkaluista käytettiin koodinimiä: VS1, VS2, VS3 ja VS4. Testi suoritettiin 25 verkkosovellukselle, jotka kaikki oli kirjoitettu Java-ohjelmointikielellä. Kuviossa 2 esitetään työkalujen ja ammattilaisten löytämät haavoittuvuudet.



KUVIO 2 Tutkimuksessa löydetyt haavoittuvuudet (Antunes & Vieira, 2013)

Edellä olevasta kuviosta huomataan, että jokainen työkalu löysi eri määrän haavoittuvuuksia, joista osa oli niin sanottuja ”vääriä” haavoittuvuuksia, eli niitä ei olisi voinut hyödyntää hyökkäyksessä. Kuviosta ei käy ilmi se asia, että eri työkalut löysivät erilaisia haavoittuvuuksia keskenään, eikä yksikään löytänyt kaikkia haavoittuvuuksia. Tutkimuksessa laskettiin ohjelmien löytämien ”oikeiden” haavoittuvuuksien osuus ammattilaisten löytämistä haavoittuvuuksista. Esittelen prosentit taulukossa 1.

Ohjelma	Osuus ammattilaisten haavoittuvuuksista (%)
VS1	31.22%
VS2	20.49%
VS3	2.93%
VS4	23.41%

TAULUKKO 1 Ohjelmien löytöjen osuus ammattilaisten löytämistä haavoittuvuuksista

Taulukosta huomataan, että käytetyistä työkaluista VS1 löysi eniten haavoittuvuuksia, mutta ylsi silti vain 31.22%:n tarkkuuteen. Tämän perusteella tutkijat päätyivät tulokseen, että näillä ohjelmilla on kaksi ongelmaa: ne löytävät paljon ”vääriä” haavoittuvuuksia ja niiden tarkkuus ei ole lähelläkään samaa tasoa kuin ammattilaisten. (Antunes & Vieira, 2013)

4.3 Tutkimusten perusteella tehdyt havainnot

Edellä olevissa luvuissa mainitut tutkimukset antoivat samankaltaisia tuloksia. Tutkimuksissa verrattiin eettisten hakkereiden tekemiä löydöksiä muihin olemassa oleviin tietoturvan kokeilukeinoihin. Austinin ym. (2013) tekemässä tutkimuksessa käytettiin erilaisia penetraatiotestauksen tyylejä, kuten systemaattista ja automatisoitua penetraatiotestausta ja näiden löytämiä tuloksia verrattiin ohjelman, joka käytti staattista koodin läpikäyntiä, tekemiin löydöksiin. Antunes ja Vieira (2013) taas tutkivat miten erilaiset automatisoidut penetraatioohjelmat pärjäävät ammattilaisille haavoittuvuuksien löytämisessä.

Ensimmäisessä tutkimuksessa eniten haavoittuvuuksia löysi staattiseen koodin läpikäyntiin suunniteltu ohjelma, joka eroaa toisen tutkimuksen tuloksista, joiden mukaan ammattilaiset olivat selkeästi parempia kuin käytetyt ohjelmat. Molempien tutkimusten perusteella voidaan todeta, että olemassa olevien ohjelmien suurin puute on löydettyjen haavoittuvuuksien tarkkuus. Tämä tarkkuuden alhaisuus johtaa siihen, että tuloksien läpikäynti on pitkä ja aikaa vievä prosessi, jotta löydetään ne oikeat haavoittuvuudet, jotka voivat vahingoittaa järjestelmää. Molempien tutkimusten tulosten perusteella voidaan sanoa, että eettinen hakkeri löytää paremmin vakavimmat haavoittuvuudet järjestelmästä, kuin automatisoidut ohjelmat. Näiden tulosten perusteella on selkeää, että eettisen hakkerin suorittamilla penetraatiotestauksilla on tärkeä osa erilaisten järjestelmien tietoturvassa, mitä ei ohjelmilla pystytä korvaamaan.

Erilaisia empiirisiä tutkimuksia eettisen hakkeroinnin hyödyistä ei löytynyt paljoa. Edellä mainituista tutkimuksista kumpikaan ei käsitellyt eettisen hakkerin suorittamaa penetraatiotestausta kokonaisuudessaan. Kuvittelen, että moni voisi olla kiinnostunut tällaisista tutkimuksista, joissa esitetään mitä konkreettista hyötyä eettisestä hakkeroinnista on, esimerkiksi kuinka paljon järjestelmää vastaan tehdyt hyökkäykset laskevat penetraatiotestauksen jälkeen. Tämä onkin hyvä aihe jatkotutkimuksen kannalta.

5 YHTEENVETO

Tutkielmalla pyrittiin saamaan vastaus seuraaviin kysymyksiin: mitä eettinen hakkerointi on ja mitä se sisältää, minkälaisia eettisen hakkeroinnin menetelmiä on olemassa ja tavoitetaanko eettisellä hakkeroinnilla parempia tuloksia kuin ”perinteisillä” tietoturvan kokeilukeinoilla? Lukija voi myös tutkimuksen pohjalta miettiä, miten oman organisaation tietoturvaa pystyisi parantamaan eettisellä hakkeroinnilla.

Tutkielmassa käytiin läpi mitä eettinen hakkerointi on ja miten se eroaa rikollisesta hakkeroinnista käyttämällä lännenelokuvista tuttuja ”hattuja”. Tutkielmassa todettiin, että eettisen hakkerin erottaa rikollisesta hakkerista järjestelmän omistajalta saatu oikeutus suoritettavaan hyökkäykseen. Tutkielmassa käytiin myös pintapuolisesti läpi näiden kahden edellä mainitun hakkerin väliin jäävä ”harmaahattu”, jolla ei ole lupaa, mutta hän ei hae omaa etua hyökkäyksellä. Tutkielmassa kävi ilmi, että eettiselle hakkerille on monenlaisia vaatimuksia, kuten tekninen tietotaito ja luotettavuus. Näiden vaatimuksien täyttämisen osoittavia sertifikaatteja käytiin läpi ja todettiin, että eettisellä hakkerilla on monta erilaista sertifikaattia, jotka hän voi suorittaa.

Seuraavaksi tutkielmassa käytiin läpi, millaisia eettisen hakkeroinnin menetelmiä on olemassa. Eettinen hakkeri voi suorittaa järjestelmään hallitun penetraatiotestauksen, jonka tarkoituksena on kartoittaa järjestelmästä löytyvät haavoittuvuudet. Tutkielmassa kävi ilmi, että penetraatiotestaus on pitkä prosessi, joka alkaa järjestelmän omistajan luvan hankkimisella ja päättyy raportin tekemiseen, missä esitetään löydetyt heikkoudet ja niiden korjaukset. Penetraatiotestauksen suorittamiseen eettinen hakkeri voi käyttää monenlaisia työkaluja, joista tärkeimpänä kirjoittaja pitää Kali Linuxia, joka itsessään pitää sisällään kaiken mitä eettinen hakkeri tarvitsee. Näitä työkaluja käytiin läpi todella pintapuolisesti. Tutkielmassa myös todettiin, että eettinen hakkeri ei testaa pelkästään järjestelmän fyysistä osapuolta, vaan voi myös pyrkiä kokeilemaan sen käyttäjät sosiaalisen manipuloinnin avulla, sillä he ovat usein järjestelmän heikoin lenkki. Tärkeimpänä sosiaalisen manipuloinnin keinona kirjoittaja nosti esille tietojenkalasteluyritykset väärennettyjen sähköpostien ja sivujen avulla.

Tutkielmassa pyrittiin selvittämään, millaisia tuloksia eettisellä hakkeroinnilla saadaan verrattuna muihin tietoturvan kokeilukeinoihin. Tutkielmassa esitettiin kaksi case-tutkimusta, missä verrattiin kuinka hyvin eettiset hakkerit löytävät järjestelmästä haavoittuvuuksia verrattuna automatisoituihin ohjelmiin.

Tämän tutkielman tulosten perusteella voidaan todeta, että eettiseksi hakkeriksi ryhtyminen on pitkä prosessi, joka vaatii todella kovaa tietotaitoa. Tulokset antavat myös ymmärtää, että eettisen hakkerin pitää hankkia erilaisia sertifikaatteja pysyäkseen kilpailukykyisenä. Tutkielmassa todettiin, että eettisen hakkeroinnin konkreettisia hyötyjä käsitteleviä tutkimuksia ei löydy paljoa, mutta käsiteltyjen tutkimusten perusteella voidaan todeta, että eettisellä hakkeroinnilla saavutetaan tarkempia tuloksia kuin automatisoiduilla ohjelmilla. Tulosten perusteella kävi myös ilmi, että järjestelmän tietoturvan kannalta kannattaa hyödyntää myös ohjelmia, sillä ne saattavat lyhentää eettisen hakkerin työtaakkaa. Konkreettisten tutkimuksien puuttuessa ei voida tarkasti kertoa millainen hyöty suoritetusta penetraatiotestauksesta on.

Tutkielma suoritettiin kirjallisuuskatsauksena ja kyseessä oli kandidaatin tutkielma. Näiden rajoitteiden takia tutkielmassa päädyttiin käsittelemään esimerkiksi työkaluja hyvin pintapuolisesti, jotta tutkielma ei venyisi liikaa. Näiden rajoitteiden takia myös tutkimuksen tulokset jäivät osittain vajaaksi, sillä aiheesta ei löytynyt paljoa valmista tietoa.

Tutkielmassa saatujen tulosten pohjalta kirjoittajalle nousi esiin muutamia jatkotutkimuksen aiheita. Kuten edellä mainittiin; eettisen hakkeroinnin konkreettisista hyödyistä ei ole tehty paljoa empiiristä tutkimusta. Kirjoittajan mielestä tätä tulisi tutkia enemmän ja siitä olisi varmasti hyötyä esimerkiksi yrityksille. Toiseksi jatkotutkimuksen aiheeksi nousi erilaisten sertifikaattien vaikutus eettisen hakkerin työllistymiseen. Erilaisia sertifikaatteja voisi enemmän verrata keskenään ja suorittaa haastattelututkimusta niiden omistajien kanssa.

LÄHTEET

(ISC)². (2019). CISSP – certified information systems security professional. Haettu osoitteesta https://www.isc2.org/Certifications/CISSP

Alsharnouby, M., Alaca, F. & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69-82.

Antunes, N. & Vieira, M. (2013). Penetration testing for web services. *Computer, 47*(2), 30-36.

Austin, A., Holmgreen, C. & Williams, L. (2013). A comparison of the efficiency and effectiveness of vulnerability discovery techniques. *Information and Software Technology, 55*(7), 1279-1288.

Baloch, R. (2014). *Ethical hacking and penetration testing guide* Auerbach Publications.

Barber, R. (2001). Hackers profiled—who are they and what are their motivations? *Computer Fraud & Security, 2001*(2), 14-17.

Bishop, M. (2007). About penetration testing. *IEEE Security & Privacy, 5*(6)

C. C. Palmer. (2001). Ethical hacking. *IBM Systems Journal, 40*(3), 769-780. doi:10.1147/sj.403.0769

Caldwell, T. (2011). Ethical hackers: Putting on the white hat. *Network Security, 2011*(7), 10-13. doi:10.1016/S1353-4858(11)70075-7

Chandrika, V. (2014). Ethical hacking: Types of ethical hackers. *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11*(1)

Chaudhry, J. A., Chaudhry, S. A. & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and its Applications, 10*(1), 247-256.

EC-Council. (2019). Certified ethical hacker certification. Haettu osoitteesta https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Engebretson, P. (2013). *The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy* Elsevier.

EU. (2016). *Gdpr*

Falk, C. (2014). Gray hat hacking: Morally black and white. *Gray Hat Hacking: Morally Black and White,*

Farsole, A. A., Kashikar, A. G. & Zunzunwala, A. (2010). Ethical hacking. *International Journal of Computer Applications (IJCA), 1*(10), 14-20.

GIAC. (2019). GIAC penetration tester (GPEN). Haettu osoitteesta https://www.giac.org/certification/penetration-tester-gpen

Liikenne- ja viestintäministeriö. (2008). *Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi*

Meyers, C. A., Powers, S. S. & Faissol, D. M. (2009). Taxonomies of cyber adversaries and attacks: A survey of incidents and approaches. *Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches,*

Najera-Gutierrez, G. & Ansari, J. A. (2018). *Web penetration testing with kali linux: Explore the methods and tools of ethical hacking with kali linux* Packt Publishing Ltd.

Patil, S., Jangra, A., Bhale, M., Raina, A. & Kulkarni, P. (2017). *Ethical hacking: The need for cyber security* IEEE.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Edpacs, 33*(8), 1-13. doi:10.1201/1079.07366981/45802.33.8.20060201/91956.1

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation, 3*(2), 97-102.

Scholte, T., Balzarotti, D. & Kirda, E. (2012). *Have things changed now? an empirical study on input validation vulnerabilities in web applications* doi://doi.org/10.1016/j.cose.2011.12.013

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation, 14*, 36-45.

Švehla, Z. L., Sedinić, I. & Pauk, L. (2016). *Going white hat: Security check by hacking employees using social engineering techniques* IEEE.

Thornburgh, T. (Oct 8, 2004). *Social engineering* ACM. doi:10.1145/1059524.1059554

Wilhelm, T. & Andress, J. (2010). *Ninja hacking: Unconventional penetration testing tactics and techniques* Elsevier.