TIETOTURVATESTAUS PALVELUNTARJOAJAN NÄKÖKULMASTA

Heikki Juurakko

Opinnäytetyö
Marraskuu 2014
Tietojenkäsittely

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely

JUURAKKO, HEIKKI:
Tietoturvatestaus palveluntarjoajan näkökulmasta

Opinnäytetyö 54 sivua, joista liitteitä 13 sivua
Marraskuu 2014

Opinnäytetyön tarkoituksena oli tutustua siihen, miten ja miksi tietoturvatestausta tehdään. Tässä työssä oli myös tavoitteena luoda testausohje, jonka avulla palveluntarjoaja pystyisi helposti etsimään tietoturva-aukkoja asiakaspäätelaitteista käyttäen kahta tietoturvaskanneria, Nmapia ja Openvasia.

Käytännön tietoturvatestaus osoitti, että asiakaspäätelaitteista voidaan löytää avoimia portteja ja haavoittuvuuksia tietoturvaskannereilla. Tuloksena syntyi testausohje, jonka avulla kuka tahansa pystyy käyttämään Nmapia ja Openvasia tietoturvatesteissään.

Tietoturvatestit osoittivat, että asiakaspäätelaitteista voidaan myös löytää tietoturva-aukkoja. Kuka tahansa pystyy luodun testausohjeen avulla etsimään haavoittuvuuksia mistä tahansa laitteesta, jossa vain on IP-osoite. Jatkokehitysideana tälle opinnäytetyölle voisi olla, että tutustuttaisiin laitespesifeihin tietoturva-aukkoihin. Asiakaspäätelaitteista löydetyistä tietoturva-aukoista voitaisiin ylläpitää päivitettävää listaa.

Asiasanat: tietoturvatestaus, hakkeri, tietoturvaskanneri.

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Information Systems

JUURAKKO, HEIKKI:
Vulnerability Testing Service: The Point of View of Internet Service Provider

Bachelor's thesis 54 pages, appendices 13 pages
November 2014

The purpose of this thesis was to explore how and why security testing is done. In this work, the aim was also to create a testing guide for the service provider to be able to trace and identify security holes in customer's routers and modems using two security scanners, Nmap and Openvas.

Practical security testing showed that open ports and vulnerabilities can be found using these two security scanners. A Testing guide was made to facilitate the use of Nmap and Openvas in security tests.

The result of the security testing showed that there were security holes in customer's routers and modems. The testing guide was made to facilitate tracing vulnerabilities from devices that have an IP-address. Vulnerabilities found in the customer's routers and modems were corrected. For further development of this thesis examination of device-specific security holes will be a top priority.

Key words: penetration testing, hacker, security scanner.

SISÄLLYS

1 JOHDANTO

Opinnäytetyön nimi on Tietoturvatestaus palveluntarjoajan näkökulmasta. Opinnäytetyön tarkoituksena on tutustua siihen, mitä tietoturvatestaus on, ja miten tietoturvatestausta tehdään. Tässä työssä luodaan myös testausohje työn toimeksiantajalle, Anvia Oyj:lle. Ohjeen avulla voidaan etsiä erilaisista asiakaspäätelaitteista avoimia portteja sekä mahdollisia tietoturvauhkia. Asiakaspäätelaite tässä työssä tarkoittaa adsl-modeemia tai reititintä, joiden avulla kuluttajat voivat yhdistää itsensä Internetiin.

Tietoturvatestaus on hyvin laaja kokonaisuus, joten aihetta on jo tässä vaiheessa rajattu. Tietoturvatestauksen kohteena ovat asiakaspäätelaitteet eli adsl-modeemit ja -reitittimet, joita operaattorit yleensä myyvät asiakkaille. Tietoturvatestaus tehdään ohjelmallisesti käyttäen Kali Linuxiin asennettuja sovelluksia, Nmapia sekä Openvasia. Nmap ja Openvas ovat tietoturvaskannereita, joiden avulla asiakaspäätelaitteista voidaan etsiä avoimia portteja sekä mahdollisia haavoittuvuuksia. Hyökkäyskoodia en tule kirjoittamaan, enkä myöskään kovin kattavasti käsittele laitespesifejä tietoturva-aukkoja.

Työssä käydään ensin läpi, mitä tietoturvatestaus todellisuudessa tarkoittaa. Tässä kappaleessa kerrotaan vielä eri hakkerityypeistä, sillä todella moni sekoittaa termit krakkeri ja hakkeri keskenään. Tämän jälkeen kerrotaan tietoturvatestauksen eri vaiheista, joita on kuusi. Sitten kerrotaan itse työosiosta, jossa tutkin, miten asiakaspäätelaitteista voidaan etsiä avoimia portteja ja haavoittuvuuksia käyttäen kahta tietoturvaskanneria, Nmapia sekä Openvasia. Seuraavaksi kerrotaan hieman luodusta testausohjeesta, jossa käytetään samoja sovelluksia kuin työosiossakin: Nmappia sekä Openvasia. Lopuksi pohditaan, kuinka hyvin projekti on onnistunut, sekä luetellaan muutamia jatkokehitysideoita työlle.

Valitsin aiheen siksi, että toimeksiantajallani on selkeä tarve tällaiselle testausohjeelle. Asiakaspäätelaitteet ovat tänä päivänä todella monipuolisia laitteita, joten mahdollisia haavoittuvuuksiakin voi löytyä enemmän. Luotavan testausohjeen avulla Anvia pystyy omissa testeissään nopeasti ja helposti kartoittamaan mahdolliset tietoturva-aukot, joita heidän myymistään laitteista voi löytyä. Tämän jälkeen he voivat raportoida

asiakaspäätelaitteesta löydetyt tietoturva-aukot laitteen valmistajalle, mikä toivottavasti johtaisi ohjelmistopäivityksen luontiin. Työstä tulee olemaan hyötyä myös kaikille niille, joita kiinnostaa oman laitteistonsa tietoturva. Nmapilla sekä Openvasilla voidaan skannailla niin yksittäisiä kohteita, kuin suuria verkostoja kerralla. Jos laitteella on vain IP-osoite, voidaan siitä etsiä avoimia portteja sekä mahdollisia haavoittuvuuksia käyttäen näitä kahta skannaustyökalua.

Tietoturvatestauksesta löytyy paljon materiaalia, sillä aihe on todella laaja. Päälähteenä työssä käytettiin Lee Allenin kirjoittamaa kirjaa, Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guidea. Tässä kirjassa on tiivistetysti selitetty, mitä tietoturvatestaus kokonaisuudessaan on. Toinen hyvä päälähde oli Penetration Testing Execution Standardin WWW-sivut, jossa käydään erittäin tarkasti läpi tietoturvatestauksen eri vaiheet. Nmapista ja sen toiminnasta löytyi runsaasti tietoa jo Nmapin omilta sivuilta. Openvasista taas oli niukasti saatavilla tietoa, joten Openvasin teoriaosuus jäi vähäiseksi. Työssä käytettävät lähteet olivat pääasiassa muutaman vuoden vanhoja, sillä esimerkiksi Nmapin- sekä Penetration Testing Execition Standardin WWW-sivut päivittyvät jatkuvasti. Kirjallinen materiaali oli pääosin myös muutaman vuoden ikäistä.

2 TIETOTURVATESTAUS

2.1 Mitä se on?

Tietoturvatestaus voidaan luokitella oikeudelliseksi ja valtuutetuksi toiminnaksi, jossa pyritään löytämään ja hyväksikäyttämään tietojärjestelmissä olevia tietoturvaongelmia. Tämän tarkoituksena on parantaa kyseisen tietojärjestelmän tietoturvan tasoa. Tässä prosessissa luodaan haavoittuvuuksia kohtaan hyökkäyksiä, joilla pyritään osoittamaan, että järjestelmän heikkoudet ovat todellisia. Asianmukaisesti tehty tietoturvatesti päättyy testaajan ilmoittamiin tietoturvaongelmiin sekä korjausehdotuksiin. Kokonaisuutena tietoturvatestauksen ideana on paikata tietojärjestelmän aukot käyttäen samoja työkaluja, joita hakkerit käyttävät. (Engebretson & Kennedy, 2013.)

Tietoturvatestauksen tarkoituksena on jäljitellä oikean hyökkääjän toimia ja pyrkiä murtautumaan järjestelmän tärkeimpiin osiin. Onnistuneessa tietoturvatestissä testaaja pystyy kiistattomasti todistamaan järjestelmän tietoturva-aukkojen olevan todellinen uhka, joka pahimmassa tapauksessa toteutuessaan voi tarkoittaa yritykselle tulojen menetystä. (Allen 2012, 8.)

Yleisen arvion mukaan kaupallisissa sovelluksissa tuhannessa rivissä koodia on 1–7 virhettä. Windows 2000 -versiossa on noin 35 miljoonaa koodiriviä, joten virheitä olisi noin 35 000–245 000. Jotkin virheet ovat täysin näkymättömiä, osa taas voi tehdä järjestelmästä epävakaan. (Järvinen 2006, 23–24.)

2.2 Hakkerityypit

Termi hakkeri tarkoitti alun perin teknisesti taitavaa ihmistä, joka halusi oppia lisää laitteista muokkaamalla niitä paremmin soveltuvaksi omiin tarpeisiin. Sana juontaakin juurensa aikaan ennen henkilökohtaisia tietokoneita. 1950-luvulla MIT:n opiskelijat käyttivät hakkerointi-sanaa kuvailemaan kepposia, joita he tekivät. (Munson 2012.)

White Hat Hackers – Valkohattuhakkerit

Kuten Hollywoodin lännenelokuvissa, hyvikset pitävät päässään valkoista hattua. Valkohattu terminä tarkoittaa eettistä hakkeria, joka noudattaa täysin lakia. He eivät koskaan murtaudu järjestelmään tai verkkoon ilman lupaa, vaan etsivät jatkuvasti järjestelmistä tietoturva-aukkoja parantaakseen järjestelmän turvallisuutta. Tietoturva-aukon löytäessään valkohattuhakkerit pyrkivät saman tien ilmoittamaan löydetystä aukosta laitteen tai ohjelman valmistajalle, jotta he voisivat tehdä päivityksen, joka korjaisi ongelman. (Munson 2012.)

Valkohattuhakkerit voivat olla yritysten palkkaamia tietoturva-alan ammattilaisia, joiden tehtävänä on tehdä tietoturvatestausta yrityksien järjestelmiä vastaan. He käyttävät samoja hakkerointityökaluja kuin krakkerit, voidakseen etsiä järjestelmistä tietoturva-aukkoja. Valkohattuhakkerin täytyykin osata käyttää samoja hyökkäystyökaluja ja menetelmiä kuin krakkeri. Vaikka monet ex-krakkerit työskentelevätkin tietoturvakonsultteina, arvostetaan valkohattuhakkereita kuitenkin enemmän, sillä heidän toimensa vaikuttavat kokonaisvaltaisesti eettisemmältä. (Munson 2012.)

Crackers: The Black Hats

Mustahattuhakkerit ovat tietokonemaailman lainsuojattomia. Mustahattuhakkereita kutsutaan myös nimellä krakkeri. Krakkerit murtautuvat yleensä järjestelmiin saadakseen henkilökohtaista hyötyä, tehdäkseen ilkivaltaa tai oikeuden rehennellä asiasta jälkeenpäin foorumeilla ja IRC-kanavilla. Krakkerin ei tarvitse olla erityisen taitava tai osaava. Valtaosa krakkereista on henkilöitä, jotka eivät osaa luoda omia hyökkäystyökaluja, vaan turvautuvat valmiisiin ohjelmiin, joiden avulla hyökkäyksiä voidaan tehdä. (Munson 2012.)

Krakkerit pyrkivät peittämään jälkeenpäin jälkensä, mutta koska heillä ei yleensä ole todellista osaamista, saavat tietoturva-alan ammattilaiset heidät napattua suhkot helposti kiinni. (Munson 2012.)

Vaikka useimmat krakkerit ovat taitamattomia, eivät kaikki kuitenkaan ole vaarattomia. Osa krakkereista toimii IT-konsultteina ja ohjelmoijina, jotka ovat oppineet käytännön kautta, miten tietoverkot ja -järjestelmät toimivat. Heillä on syvällistä tietoa verkko-

ohjelmoinnista ja he pystyvät luomaan omia työkaluja, jotka osaavat hyödyntää löydettyjä tietoturva-aukkoja. Turvallisen ympäristön luonnissa täytyykin ottaa huomioon ne krakkerit, jotka pystyvät luomaan omia hyökkäystyökaluja. (Munson 2012.)

Vähemmän taitavat krakkerit käyttävät yleensä asiantuntevien krakkerien hyökkäystyökaluja murtautuakseen järjestelmiin. Vaikka asiantuntevia krakkereita on suhteessa vähän verrattuna vähemmän taitaviin krakkereihin, voidaan heidän luomiaan hyökkäystyökaluja ja haittaohjelmia käyttää tehokkaasti hyökkäyksiin tietoturva-aukkoja vastaan. (Munson 2012.)

Skriptipennut - Script kiddies

Useimpia krakkereita voidaan kutsua skriptipennuiksi (script kiddies). Tämän kaltaisilla krakkereilla ei ole todellista teknillistä ymmärrystä, ja yleensä he eivät osaa myöskään ohjelmoida. Voidakseen murtautua järjestelmiin, he turvautuvat muiden luomiin hyökkäystyökaluihin He eivät välttämättä myös täysin ymmärrä, miten nämä hyökkäystyökalut todellisuudessa toimivat. (Munson 2012.)

Skriptipentujen yleinen harrastus on murtautua verkkosivuille, joiden tietoturvassa on vakavia puutteita. He voivat korvata kohteen kotisivun joksikin muuksi. Jos skriptipentu pystyy murtautumaan järjestelmään, kertoo se yleensä siitä, että järjestelmänvalvoja ei ole asentanut tarvittavia korjauspäivityksiä laitteille. (Munson 2012.)

Harmaahattuhakkerit - Gray Hats

Harmaahattuhakkeri on eettinen hakkeri, joka tasapainottelee laillisen ja laittoman hakkeroinnin välillä. Kuten valkohattuhakkerit, harmaahatut etsivät tietoturva-aukkoja ja raportoivat niistä. Toisin kuin valkohatut, he useimmiten julkaisevat tietoturva-aukon ennen kuin antavat sovelluskehittäjille mahdollisuuden korjata ongelman. Harmaahattujen mukaan tällainen toimintamalli pakottaa yritykset korjaamaan ohjelmistonsa. (Munson 2012.)

Harmaahatut voivat myös murtautua järjestelmään ilman lupaa, vaikka heidän tarkoituksenaan olisikin löytää tietoturva-aukot sekä raportoida löydöksistä oikeille tahoille.

Vaikka on parempi, että harmaahattu on etsimässä verkon reikiä, eikä mustahattu, ei näiden toimia kuitenkaan pysty erottamaan toisistaan. Harmaahatut voivat tahtomattaan aiheuttaa myös todellista vahinkoa kohteen verkkoon, vaikka heidän tarkoituksenaan onkin tehdä hyvää. (Munson 2012.)

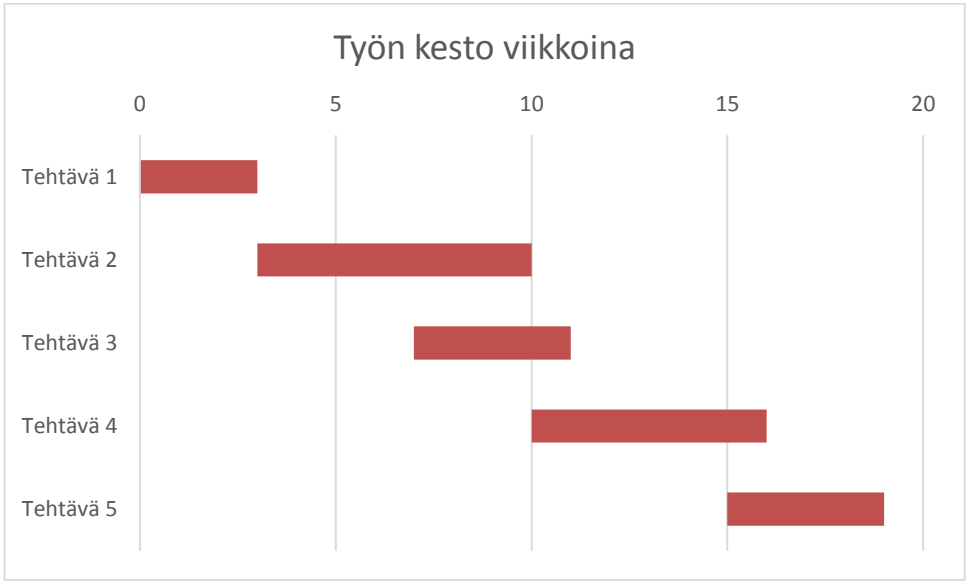
Taitavat harmaahattuhakkerit voivat luoda sovelluksia, jotka hyödyntävät tunnettuja laitteiden ja järjestelmien tietoturva-aukkoja. Tästä on hyötyä järjestelmänvalvojille ja tietoturvan ammattilaisille, jotka voivat käyttää näitä sovelluksia omissa tietoturvatesteissään. Valitettavasti myös krakkerit voivat käyttää samoja sovelluksia vähemmän jaloihin tarkoituksiin (Munson 2012).

3 TESTAUSVAIHEET

3.1 Ennen testiä

Ennen tietoturvatestauksen aloittamista täytyy ottaa tietyt vaatimukset huomioon. Testi täytyy rajata kunnolla, määrittää aikataulut, määrittää testin tyyppi (Blackbox, White-box), miten kolmannen osapuolen laitteet hoidetaan, sekä mikä mahdollinen IP-osoitealue on. (Allen 2012, 10).

Onnistuneessa tietoturvatestissä testin rajat on tarkoin määritelty. Asiakkaiden tulee myös tietää testin mahdollisista seuraamuksista sekä lisäkuluista, joita ei ole sopimuksessa mainittu. Testille annetaan alkamis- ja päättymispäivä. Dokumentti voimankäyttövaltuuksista on asiakirja (rules of engagement), jossa määritetään muun muassa IP-alueet, rakennukset, käytettävät työtunnit sekä asiat, jotka on rajattu testin ulkopuolelle. Asiakkaan tulisi tarkoin tietää, minkä tyyppisiä tuloksia voi testaajalta odottaa. Asiakkaan kanssa kannattaa myös sopia kokouksista etukäteen. (Allen 2012, 12). Tietoturvatestauksen kestoon kannattaakin käyttää esimerkiksi kuvan 1 kaltaista Gantt-kaaviota, joka auttaa työn suunnittelussa ja resursoinnissa.



Kuva 1. Gantt-kaavio

Kaavion avulla on myös helpompi hahmottaa mahdolliset ongelmakohdat, jotka voivat tuottaa ylimääräistä työtä tietoturvatestaajalle (Penetration Testing Execution Standard, 2012a).

3.2 Tiedusteluvaihe

Tietoturvatestaajan tulee informoida yritystä siitä, minkälaista tietoa yrityksestä on saatavilla julkisesti. Tämä informaatio vaihtelee kohteittain, mutta muun muassa asiakkaan IP-alueet, domain nimet, sähköpostiosoitteet, julkiset taloudelliset tiedot, organisaation tiedot, käytettävät teknologiat, tehtävänimikkeet, puhelinnumerot voivat olla julkisesti saatavia tietoja kohdeyrityksestä. Internetistä voi myös löytää salaiseksikin luokiteltuja dokumentteja käyttäen pelkästään Googlen hakutoimintoa. (Allen 2012, 44).

Tietoturvatestauksessa julkisen tiedon keräämistä kutsutaan nimellä OSINT (open source intelligence). OSINT:n tarkoituksena on kerätä organisaatiosta mahdollisimman paljon tietoa julkisista lähteistä. OSINT:n avulla pyritäänkin luomaan isompi kokonaisuus yhdistelemällä eri tietolähteistä saatavia tietoja (Nettibisnes.info, 2010). OSINT:sta on kolme erilaista muotoa: passiivinen tiedonhaku, semi-passiivinen tiedonhaku sekä aktiivinen tiedonhaku. (Penetration Testing Execution Standard, 2012b).

Passiivisessa tiedonhaussa itse kohteeseen ei olla suoraan yhteydessä, joten tässä vaiheessa ei suoriteta minkäänlaisia skannauksia asiakkaan verkkolaitteille. Tietoa etsitäänkin kolmannen osapuolen lähteistä, kuten vaikkapa Googlesta. (Penetration Testing Execution Standard, 2012b) Julkista tietoa ovat muun muassa verotiedot, blogit, akateemiset lähteet ja tutkimusraportit (Allen 2012, 45). Passiivisen tiedonhaun tulokset saattavat kuitenkin olla jo vanhentunutta, tai kokonaan väärää tietoa, sillä kolmannen osapuolen lähteet eivät välttämättä ole kovin luotettavia. (Penetration Testing Execution Standard, 2012b).

Semi-passiivisessa tiedonhaussa tietoturvatestaaja pyrkii siihen, että tiedonhaku näkyy tavallisena netin käyttönä tiedustelun kohteena olevalle yritykselle. IP-kyselyitä tehdään vain tunnettuihin nimipalvelimiin sekä kohteen piilotettuja palvelimia tai tiedostoja ei pyritä etsimään. Web Crawlereita tai porttiskannauksia ei myöskään suoriteta, sillä tarkoituksena on vain etsiä metadataa julkaistuista dokumenteista ja tiedostoista. Tarkoi-

tuksena on olla herättämättä huomiota tiedonkeräyksellä. Tiedustelun kohde voi jälkeenpäin huomata logeistaan olleensa jonkinlaisen tiedustelun kohteena, mutta sitä on vaikea kohdistaa takaisin kenellekään. (Penetration Testing Execution Standard, 2012b).

Aktiivisessa tiedonhaussa pyritään aktiivisesti kartoittamaan kohteen verkko, joten tässä vaiheessa kohteen tulisi huomata joutuneensa tiedustelun kohteeksi. Tässä vaiheessa skannataan kohteen verkkolaitteita etsien haavoittuvuuksia avoimista palveluista, etsien käyttäjiltä piilotettuja hakemistoja, tiedostoja ja palvelimia. Suurin osa tästä toiminnasta kuuluu tyypillisen ”tiedustelun” ja ”skannauksen” vaiheisiin, joita tietoturvatestaaja tekee tietoturvatesteissään. (Penetration Testing Execution Standard, 2012b).

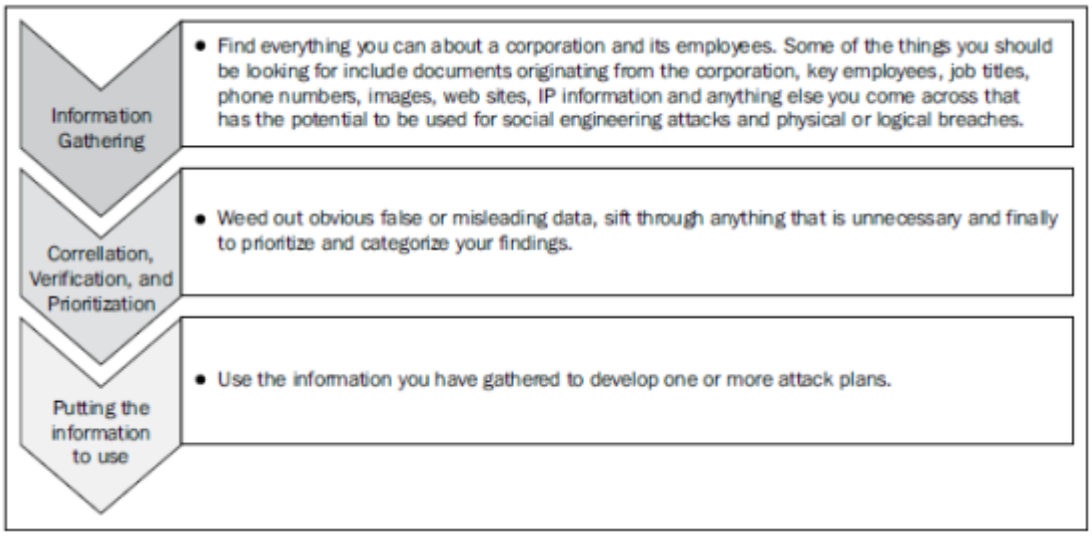
Aktiivisessa tiedonhaussa ollaan suoraa kohteen kanssa tekemisissä. Aktiivista testausta voi olla vaikkapa Nmap-skannaus, jolla pyritään selvittämään, mitkä kohteen porteista ovat auki:

```
Open - the port is able to receive data
Closed - the port is not able to receive data
```

Kun skanneri on huomannut, että portti on auki, voi portin takana olla jokin haavoittuva palvelu. Esimerkiksi portin 23 ollessa auki, voidaan olettaa, että Telnet-palvelu on kohteessa päällä. Skanneri saattaakin ilmoittaa, että kyseessä on palvelu, joka ei salaa kirjautumistietoja. (Penetration Testing Execution Standard, 2012c).

Tiedustelun vaiheet

Tiedustelu on kaikkein tehokkainta silloin, kun se on toteutettu vaiheittain. Vaiheita on kolme, joita kannattaa noudattaa omassa työssään. Kuvassa 2 on kuvattu tiedustelun kulku:



Kuva 2. Tiedustelun kulku (Allen 2012, 46, kuvankaappaus)

Yksinkertaisena esimerkkinä tiedustelun vaiheista voisi olla seuraava tapaus. Asiakkaan ulkoisista reitittimistä on saatavilla julkisesti tietoa. Tiedustelun vaiheet olisivat tässä tapauksessa seuraavanlaiset:

1. Pystytään vahvistamaan, että asiakkaan ilmoittamat IP-alueet kuuluivat todellakin asiakkaalle.
2. Havaitaan, että usean reitittimen oletusasetuksia ei ole muutettu. Tämä tieto tarkistetaan oikeaksi.
3. Kerätyn aineiston perusteella paras tapa päästä järjestelmän sisälle on hyväksikäyttää ulkoisista reitittimistä löydettyä tietoturva-aukkoa, ja päästä niiden kautta järjestelmään sisälle.

Tämä on yksinkertainen esimerkki tiedustelun työkulusta. Oikeassa elämässä on monia tekijöitä, jotka vaikuttavat tietoturvatestaajan päätöksiin. Tiedustelun aikana kerätty tieto on ratkaiseva tekijä tietoturvatestauksen onnistumisessa.

3.3 Riskianalyysi

Riskianalyysi luodaan sen jälkeen, kun verkon määrittely sekä skannausvaihe on saatu suoritettua loppuun. Riskianalyysin tarkoituksena on selvittää mahdolliset uhat sekä niiden vaikutukset yrityksen kyvylle jatkaa liiketoimintaa mahdollisen hyökkäyksen jälkeen. Tarkoituksena on kartoittaa kaikki asiakasyrityksen tärkeinä pitämät varat, jot-

ka eivät saisi vaarantua hyökkäyksen aikana. Ensisijainen hyökkäyskohde voisi olla vaikkapa yrityksen asiakastiedot. Hyökkääjä joutuu kuitenkin kaivamaan nämä tiedot tietokantapalvelimesta, joka taas voidaan laskea toissijaiseksi kohteeksi. Näin hyökkääjä on ensin käyttänyt toissijaista kohdetta hyväkseen, jotta hän pääsi käsiksi asiakastietoihin, joka taas oli ensisijainen kohde. (Penetration Testing Execution Standard, 2012d).

3.4 Hyökkäysvaihe

Tarvitaan vain yksi taitava hyökkääjä, joka tietoturva-aukon löydettyään kirjoittaa sitä hyödyntävän hyökkäyskoodin. Tämän jälkeen hyökkääjä voi julkaista internetissä ohjeet siitä, miten tietoturva-aukkoa voidaan hyväksikäyttää. Tämän seurauksena kuka tahansa vähänkään osaava, tietotekniikasta kiinnostunut henkilö, voi toteuttaa hyökkäyksen, joka hyväksikäyttää tätä tietoturva-aukkoa (Järvinen 2006, 25–26).

Kun järjestelmään on murtauduttu sisään, on suositeltavaa tutkia laite läpikotaisin. Tässä vaiheessa tulisi keskittyä tunnuksien keräämiseen, järjestelmän tarjoamien palveluiden listaamiseen sekä verkkotopologian tutkimiseen. Onko verkko jaettu osiin, onko verkkolaitteille olemassa useita IP-osoitteita, vai onko järjestelmä virtualisoitu. Tietojen läpikäymiseen tarvittavista komennoista sekä menetelmistä kannattaa tehdä etukäteen lista. Tällainen toimintasuunnitelma nopeuttaa murretun järjestelmän/koneen tietojen läpikäyntiä, helpottaa raportin kirjoittamista sekä vähentää riskiä unohtaa asioita. (Allen 2012, 242).

3.5 Jälkihyökkäys

3.5.1 Tarpeellisuus

Hyvässä tietoturvatestissä on tietyt tavoitteet, jotka pyritään saavuttamaan. Tavoitteina voivat olla muun muassa pääsy tärkeään tietokantaan tai järjestelmänvalvojan tunnuksen saaminen, minkä avulla voidaan lukea yksityisiä sähköpostiviestejä. Asiakas ei välttämättä pidä satunnaisen järjestelmän murtamista kriittisenä uhkana. Tietoturvatestaajan

tuleekin antaa asiakkaalle konkreettiset todisteet siitä, miten löydetty tietoturva voi aiheuttaa asiakkaalle rahallisia menetyksiä (Allen L 2012, 239).

3.5.2 Käytetyt menetelmät

Takaovi on sovellus, joka sijaitsee kohdekoneessa ja mahdollistaa hyökkääjän pääsyn takaisin tähän koneeseen. Yleensä takaovi on piilotettu prosessi, joka toimii kohdekoneessa. Monet hyväksikäytöt ovat lyhytaikaisia. Ne toimivat ja tarjoavat pääsyn niin kauan, kunnes hyväksikäytetty ohjelma tai prosessi on käynnissä. Kohdekoneen uudelleenkäynnistys lakkauttaa etäyhteyden kohdekoneeseen. Tarkoituksena onkin luoda takaovi, jonka kautta kohdekoneeseen saadaan jälleen yhteys. (Engebretson & Kennedy, 2013).

Rootkit on erikoisohjelma, joka istuttaa itsensä syvälle käyttöjärjestelmän uumeniin suorittaen monenlaisia tehtäviä, antaen hakkerille mahdollisuuden piilottaa taustaprosesseja ja ohjelmia. Rootkitteja voidaan käyttää monissa erilaisissa tilanteissa, kuten laajentamaan käyttöoikeuksia, tallentamaan näppäinlyöntejä, asentamaan takaovia ja tekemään muita pahoja toimenpiteitä. Rootkitteja on myös vaikea havaita, sillä ne toimivat käyttöjärjestelmää alemmalla tasolla, kernelin sisällä. Normaalit ohjelmat toimivat yleensä korkeammalla tasolla käyttöjärjestelmässä. Kun virustorjuntasovelluksen pitää suorittaa tietty toiminta, täytyy sen välittää tieto järjestelmän alemmalle tasolle. Rootkit taas voi muokata tätä käskyä alemmalla tasolla ja välittää tämän tiedon virustorjuntasovellukselle. (Engebretson & Kennedy, 2013).

Rootkit ei ole itsessään hyväksikäyttö-sovellus. Rootkit tallennetaan kohdekoneeseen sen jälkeen, kun konetta on hyväksikäytetty. Rootkitteja käytetäänkin yleensä piilottamaan tiedostoja tai ohjelmia sekä ylläpitämään salaista takaovipääsyä järjestelmän sisään. (Engebretson & Kennedy, 2013).

3.6 Loppuraportti

3.6.1 Tiivistelmä

Tiivistelmäosuuden tulee olla lyhyt katsaus tietoturvatestistä saaduista löydöksistä. Tämän dokumentin, tai aliraportin, pituus ei saisi ylittää kahta sivua ja sen tulisi sisältää vain testauksen kohokohdat. Tiivistelmässä ei tarvitse olla teknillisiä yksityiskohtia tai terminologiaa. Tämä raportti kirjoitetaan hallituksen jäsenille ja ei-tekniselle johdolle, joten kielen täytyy olla neutraalia. Tarkoituksena on, että kuka tahansa kadunmies saa käsityksen siitä, mitä ollaan tehty sekä mitä ollaan löydetty.

Tiivistelmässä on tärkeää läpikäydä löydetyt tietoturvariskit ja kertoa siitä, miten nämä vaikuttavat yrityksen tai organisaation toimintaan. Dokumentin tulisi myös tarjota linkkejä ja viittauksia yksityiskohtaiseen raporttiin, jotta asiasta kiinnostuneet voivat tutkia teknillisiä yksityiskohtia tarkemmin. Tiivistelmässä kannattaa myös kertoa tietoturvatestin laajuudesta ja tarkoituksesta, sekä kertoa yrityksen tai organisaation yleisestä riskiluokituksesta. (Engebretson & Kennedy, 2013).

3.6.2 Yksityiskohtainen raportti

Tässä osiossa on kattava listaus sekä yksityiskohdat siitä, mitä on löydetty tietoturvatestin aikana. Tämän raportin kohdeyleisönä ovat atk-päälliköt, tietoturva-asiantuntijat, verkon ylläpitäjät sekä ne, joilla on vaadittavaa tietotaitoa ymmärtääkseen tekstin teknisen luonteen. Tämä raportin osa auttaa teknistä henkilöstöä ymmärtämään, mikä tietoturvassa on vikana, sekä miten järjestelmän tietoturvaa voitaisiin parantaa. (Engebretson & Kennedy, 2013).

Tietoturvauhista kerrottaessa testin tekijän tulee olla rehellinen ja suora asiakasta kohtaan sekä kertoa löydöksistään objektiivisesti. Kriittiset uhat kannattaa esitellä ensin. Tämä tekee raportin lukemisesta helpompaa ja asiakas saa paremman kuvan siitä, mitä asioita yhtiön tai organisaation tietoturvassa kannattaa ensiksi parantaa. Kriittisimmistä uhista sekä onnistuneista järjestelmän vaarantamisista kannattaa ottaa kuvankaappaukset. Lukijalle nämä ovat kiistattomia todisteita järjestelmän tietoturvaongelmista. (Engebretson & Kennedy, 2013).

Aina kun mahdollista, kannattaa raportissa kertoa, miten järjestelmän tietoturvaa voisi parantaa. Muun muassa Nessus-tietoturvaskanneri kertoo, miten tietyn tietoturvaongelman voisi korjata. Internetissä on myös monia tietokantoja, joista löytyy tietoa haavoittuvuuksista ja tietoturvariskeistä. Näitä tietokantoja ovat muun muassa Exploit-db.com, nvd.nist.gov, cvedetails.com, cve.mitre.org tai vaikkapa osvdb.org. Googlesta löytyy myös oikeilla hakusanoilla tietoa eri haavoittuvuuksista ja siitä, miten haavoittuvuudet saataisiin korjattua. Mahdollisia ratkaisuja voivat olla muun muassa päivitysten lataaminen, sovellusversion päivittäminen uudempaan, konfiguraatiotiedostojen päivitys tai itse laitteiston päivitys uudempaan versioon. (Engebretson & Kennedy, 2013).

Raportista pitää käydä ilmi, miten tietty tietoturvauhka on löydetty. Onkin siis hyvä kertoa käytetyistä sovelluksista ja tekniikoista, joita on käytetty uhan löytämiseksi. Kannattaakin tehdä linkityksiä raakadataosion puolelle, jossa käydään läpi se, minkälaisia tuloksia tietyt sovellukset ja tekniikat ovat saaneet aikaiseksi. (Engebretson & Kennedy, 2013).

3.6.3 Raakadata

Tämä osio raportista sisältää teknisiä yksityiskohtia ja erilaisten sovelluksien tuottamaa raakadataa. Käytettäessä tilaustyönä tehtyjä sovelluksia, skriptejä tai muuta omaa koodia, kannattaa miettiä, mitä kaikkea haluaa paljastaa asiakkaalle. Useimmiten on kuitenkin turvallista antaa kaikki tiedot käytetyistä työkaluista, joita on käytetty tietoturvatestaamisessa. Tämä ei kuitenkaan tarkoita sitä, että kaikista sovelluksissa käytettävistä komennoista ja kytkimistä tarvitsisi kertoa yksityiskohtaisesti; tärkeintä on kirjoittaa siitä, mitä nämä sovellukset ovat tulostaneet. Jälkikäteen voidaan siivota raakadataosiosta sellaisia komentoja ja tekniikoita, joita ei haluta paljastaa asiakkaalle jostain syystä. (Engebretson & Kennedy, 2013).

4 CASE ASIAKASPÄÄTELAITTEIDEN SKANNAUS

4.1 Testauksen tarpeellisuus

Brasiliassa 2011 tapahtui laaja tietoturvaisku, jossa yksi firmware-haavoittuvuus, kaksi haitallista skriptiä ja 40 krakkerien ylläpitämää DNS-palvelinta vaaransivat kuuden eri valmistajan asiakaspäätelaitteiden tietoturvan. Tämän johdosta 4.5 miljoonaa brasilialaista internetin käyttäjää joutui hiljaisen, mutta valtavan hyökkäyksen kohteeksi. Hyökkäyksen tarkoituksena oli päästä käsiksi asiakaspäätelaitteen hallintapaneeliin, jonka seurauksena asiakaspäätelaitteen asetuksia, muun muassa DNS-palvelimen osoiteasetuksia, voitiin muuttaa. Tämä mahdollisti sen, että rikolliset pystyivät ohjaamaan asiakkaan liikenteen heidän ylläpitämiin domaineihin. Tämän avulla he pystyivät ohjaamaan liikennettä hienotunteisesti sekä jatkamaan laajempaa hyökkäystä herättämättä epäilyksiä. Vahingolliset DNS-palvelimet ohjasivat uhreja rikollisten pystyttämiin domaineihin, joissa sijaitsivat samankaltaiset sivut, kuin vaikkapa Brasilian pankeilla oli. Jotkut rikolliset taas ohjasivat uhrejaan sivuille, joissa uhrit tietämättään asensivat haittaohjelmia koneilleen. (Assolini, 2012)

Tällaiset tapaukset ovat kiusallisia varsinkin palveluntarjoajille, jotka tarjoavat asiakkailleen haavoittuvia asiakaspäätelaitteita. Tämän kaltaiset tapaukset voivat myös pilata omalta osaltaan palveluntarjoajan maineen, sekä tuottaa näin taloudellista haittaa palveluntarjoajalle. Tämän takia olisikin hyvä, että myös asiakaspäätelaitteiden tietoturvaan perehdyttäisiin paremmin testaamalla laitteet kunnolla, ennen kuin laitteita ruvetaan myymään asiakkaille.

4.2 Testauksen lähtökohdat

Tarkoituksena oli tutustua siihen, miten tietoturva-aukkoja voitaisiin löytää asiakaspäätelaitteista. Asiakaspäätelaite tässä työssä tarkoittaa mitä tahansa kuluttajatason langatonta reititintä, adsl-modeemia, vdsl-modeemia tai muuta vastaavaa laitetta. Aikaa ei ollut täysimittaiselle tietoturvatestille, joten tehokkain ja nopein tapa löytää tietoturva-aukkoja asiakaspäätelaitteista on erilaisten skannereiden käyttö. Skannereiden avulla

voidaan kätevästi kartoittaa avoimet portit sekä mahdolliset tietoturva-aukot. Testauksessa laitteita skannailtiin lähinnä sisäverkosta käsin, sillä tällöin oli mahdollista löytää paremmin mahdollisia tietoturva-aukkoja.

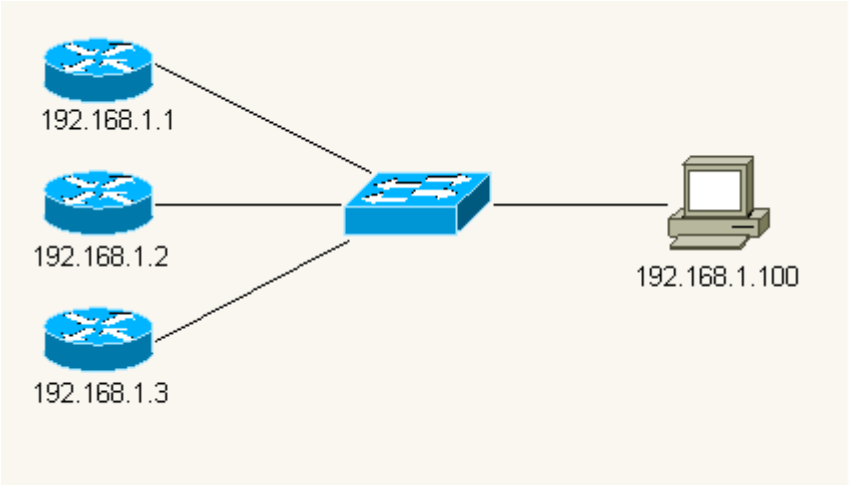
Projektissa skannattiin monia eri verkon aktiivilaitteita, mutta tässä luvussa tulen käsitellään vain TP-Linkin mallia TD-W8961ND.

4.3 Kuva testiympäristöstä

Testiverkko oli todella yksinkertainen, sillä tarvittiin vain tietokone, johon oli asennettu Kali-Linux, sekä testattava asiakaspäätelaite. Kuvassa 3 on yksinkertainen testiverkko.

Kuva 3. Kuva testiverkosta

Jos testattavana on useita laitteita, lisätään testiverkkoon kytkin, johon voidaan liittää useita asiakaspäätelaitteita. Kuvassa 4 on testiverkko, jossa on useampi asiakaspäätelaite.



Kuva 4. Testiverkosta, jossa useita testattavia kohteita

4.4 Työkalujen esittely

Tässä testausohjeessa käytetään Nmapia sekä Openvasia. Molemmat työkalut löytyvät valmiiksi asennettuina Kali Linuxista. Kali Linux on Debianista johdettu Linux-distribuutio, joka on tehty varta vasten tietoturvatestaamiseen. Kali Linuxin voi ladata osoitteesta http://www.kali.org/downloads/. Kätevimmin Kali Linuxia ajaa suoraan virtuaalikoneelta, esimerkiksi Virtualboxilla tai Vmwarella.

Debianille ja Ubuntulle saa asennettua Nmapin komennolla `sudo apt-get install nmap / sudo aptitude install nmap`. Windowsille Nmapin saa ladattua osoitteesta http://nmap.org/download.html kohdasta Microsoft Windows binaries. Ohjeet Openvasin asentamiseksi eri alustoille löytyy sivulta http://www.openvas.org/download.html. Openvasin työpöytäversio löytyy myös Kali Linuxista valmiiksi asennettuna, mutta tässä työssä käytetään selainversiota.

4.5 Käytetyt ohjelmat

4.5.1 Nmap

Nmapin esittely

Nmap julkaistiin 1.9.1997 Phcrack-lehden numerossa 51, artikkelissa 11. Nmapilla ei ollut aluksi versionumeroa, sillä Nmapin kehittäjä, Gordon "Fyodor" Lyon, ei aikonut kehittää Nmapia enempää. Ensimmäisessä Nmapin versiossa olikin vain noin 2000 riviä koodia. Nmap oli alunperin vain Linuxille tarkoitettu yksinkertainen porttiskanneri. (The History and Future of Nmap 2014). Nmapin viimeisin versio on julkaistu 22.8.2014 ja se on versionumero 6.47.

Nmap (Network Mapper) on avoimeen lähdekoodiin perustuva työkalu verkkojen tutkimiseen ja suojauksen valvontaan. Nmap suunniteltiin alunperin skannaamaan nopeasti laajaa verkkoa, mutta se toimii myös hyvin yhtä kohdetta vastaan. Nmap käyttää raakoja IP-paketteja, joiden avulla voidaan selvittää, mitkä laitteet ovat verkossa. Verkon laitteista voidaan myös selvittää, mitä palveluita verkon laitteet tarjoavat, minkälaiset käyttöjärjestelmät niissä pyörivät, minkälaiset palomuurit niissä ovat käytössä sekä kymmeniä muita ominaisuuksia. (Nmap Description 2014).

Nmapin tuloste koostuu skannatuista kohteista, sekä mahdollisista lisätiedoista, jotka on saatu selville käyttämällä lisäkytkimiä. Tärkein tieto on kohta taulukko mielenkiintoisista porteista. Tässä taulukossa on mainittuna portin numero, käytetty protokolla, palvelun nimi sekä portin tila. Portin tila voi joko olla avoin (open), suodatettu (filtered), suljettu (closed) tai suodattamaton (unfiltered). Avoin portti tarkoittaa, että kohdekoneen sovellus kuuntelee yhteyksiä sekä saapuvia paketteja tulevan tähän porttiin. Suodatettu- tila tarkoittaa sitä, että palomuuri, suodatin tai jokin muu verkon osa suodattaa liikenteen, joten Nmap ei voi kertoa, onko kohteen portti avoin vai suljettu. Portti on suljettu silloin, kun mikään sovellus ei ole portin takana kuuntelemassa liikennettä. Portti on määritetty suodattamattomaksi, jos ne vastaavat Nmapin kutsuihin, mutta Nmap ei pysty määrittämään, onko portti suljettu vaiko avoin. Tällöin Nmap raportoi portin olevan

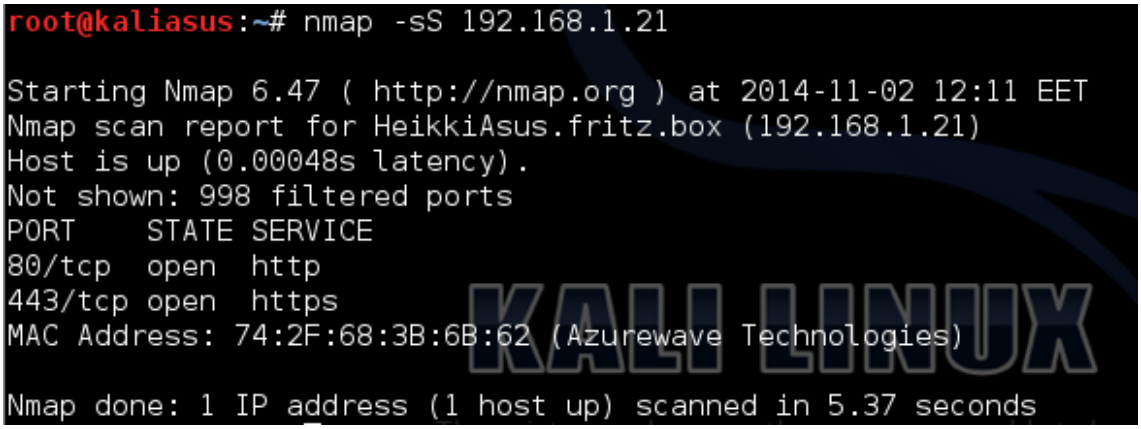
joko avoin|suodatettu (open|filtered) tai suljettu|suodatettu (closed|filtered). Nmapin tulosteessa voi myös olla mukana versiotiedot, kun tarvittava kytkin on valittu mukaan skannaukseen. Kun IP-protokollan tarkistuskytkin on valittu, (-sO), tarjoaa Nmap tietoa myös tuetuista IP-protokollista. (Nmap Description 2014).

Esimerkkejä Nmapin käytöstä

Näissä esimerkeissä kohdekoneena on käytetty kannettavaa, johon on asennettu Windows 8.1 käyttöjärjestelmä.

TCP SYN Scan (-sS) on Nmapin oletus skannaustapa. Tätä tekniikkaa kutsutaan myös usein nimellä half-open-skannaukseksi, koska Nmap ei luo täydellistä TCP-yhteyttä kohteeseen. Nmap lähettää SYN-paketin kohteeseen jääden kuuntelemaan vastausta. SYN/ACK-vastaus tarkoittaa sitä, että portti kuuntelee (open). RST-paketti tarkoittaa sitä, että portin takana ei ole kukaan kuuntelemassa. Jos portilta ei tule vastausta, merkataan portti filtteröidyksi. (Port Scanning Techniques 2014.)

Windows-koneessa olivat auki portit 80 ja 443, joiden takaa löytyivät palvelut http sekä https. Kuvassa 5 on annettu komento, sekä tuloste.

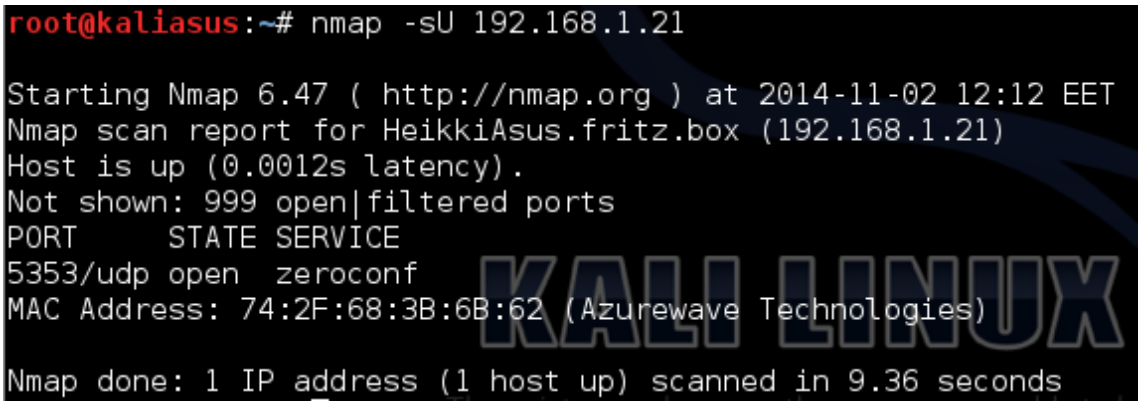


Kuva 5. Windows koneen avoimet TCP-portit (Nmap 2014, kuvankaappaus)

Vaikka useimmat suosituimmista palveluista Internetissä toimii TCP-protokollalla, ovat UDP-palvelut laajalti käytössä. DNS, SNMP sekä DHCP ovat kolme yleisintä palvelua. Koska UDP-skannaus on yleisesti ottaen hitaampaa sekä vaikeampaa verrattuna TCP-skannaukseen, sivuuttavat monet tietoturva-asiantuntijat nämä portit. Tämä on virhe,

sillä haavoittuvat UDP-palvelut ovat yleisiä, sekä mahdollinen hyökkääjä myös pyrkii löytämään haavoittuvat UDP-palvelut. (Port Scanning Techniques 2014.)

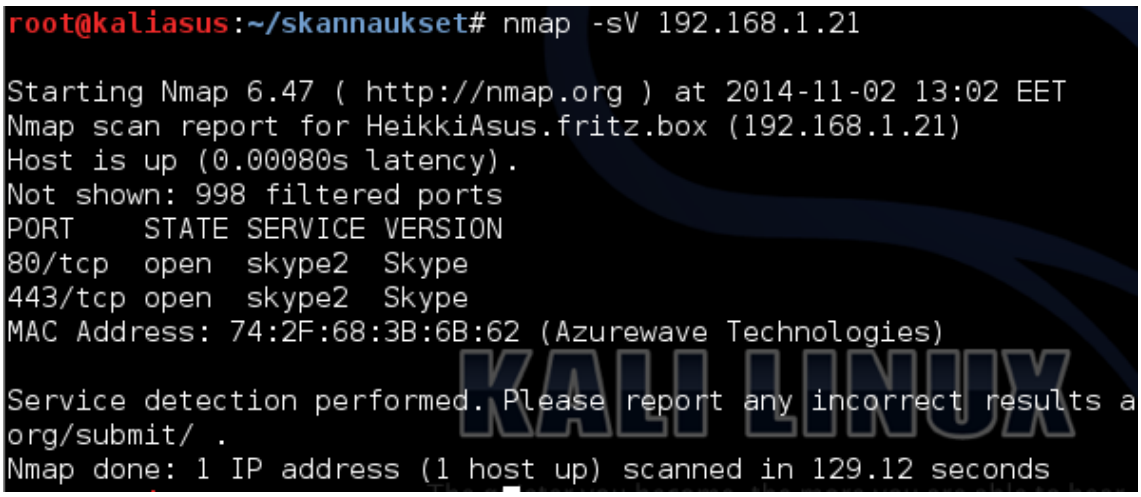
Kuten kuvasta 6 näkyy, oli Windows koneessa UDP-portti 5353 auki. Portin takaa löytyi palvelu zeroconf.



Kuva 6. Windows koneen avoimet UDP-portit (Nmap 2014, kuvankaappaus)

Version tunnistus on tekniikka, jonka avulla voidaan tutkia, mikä ohjelmistoversio pyörii kohdekoneen avoimien porttien takana. Version tunnistus käyttää ensin TCP SYN-skannausta, koska Nmapin tulee ensin tietää, mitkä portit ovat auki. (Nmap from Beginner to Advanced 2014.)

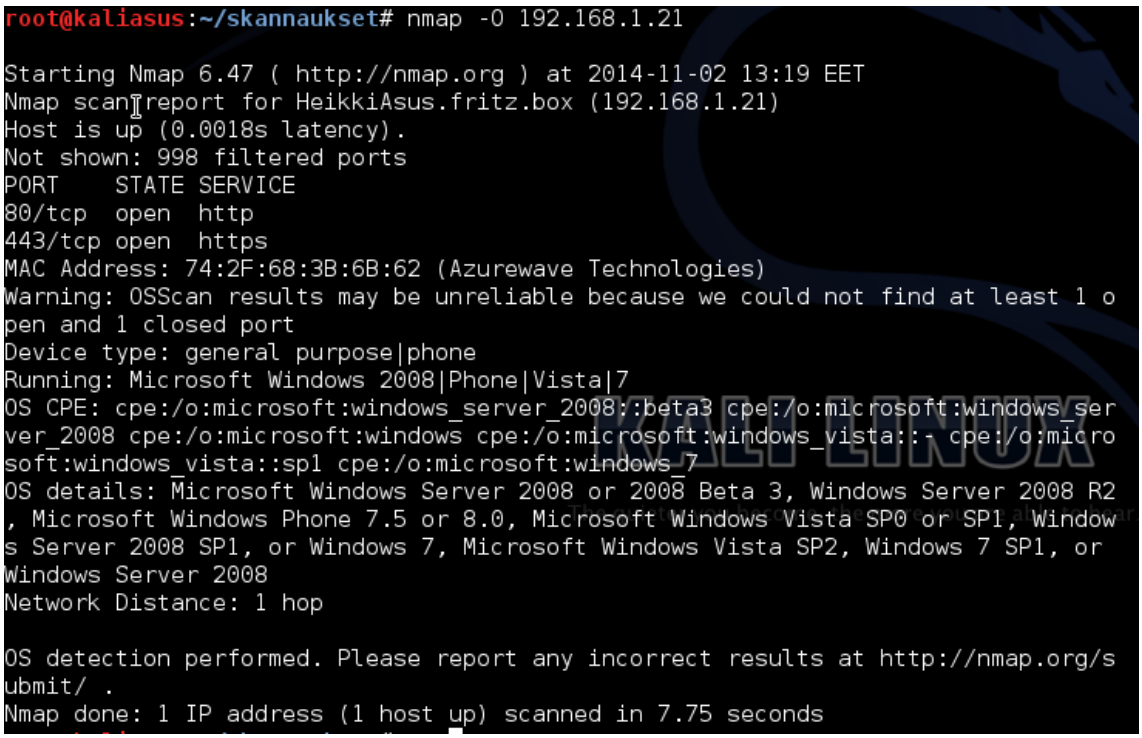
Kuten kuvasta 7 näkyy, löytyi Windows koneesta Skype2-palvelu, joka toimii porttien 80 ja 443 takana.



Kuva 7. Windows koneen porttien takaa löytyneet palvelut (Nmap 2014, kuvankaappaus)

Nmapin yksi tärkeimmistä ominaisuuksista on käyttöjärjestelmän tunnistus. Tämä on todella kätevää tietoturvatestauksen aikana, sillä käyttöjärjestelmän perusteella tietoturvatestaaja voi jo helposti olettaa, mitä mahdollisia haavoittuvuuksia kohdekoneesta voidaan löytää. Nmapissa on tietokanta nimeltä nmap-os-db, joka sisältää tiedot yli 2600:sta eri käyttöjärjestelmästä. Nmap lähettää sekä TCP- että UDP-paketteja kohdekoneeseen, ja tämän jälkeen tutkii vastauksia verraten niitä tietokantaan. (Port Scanning Techniques 2014.)

Kuvassa 8 Nmap havaitsi, että kohdekoneessa pyörii Windows käyttöjärjestelmä. Nmap ei kuitenkaan osannut tarkasti sanoa, mikä versio Windowsista pyörii kohdekoneessa.



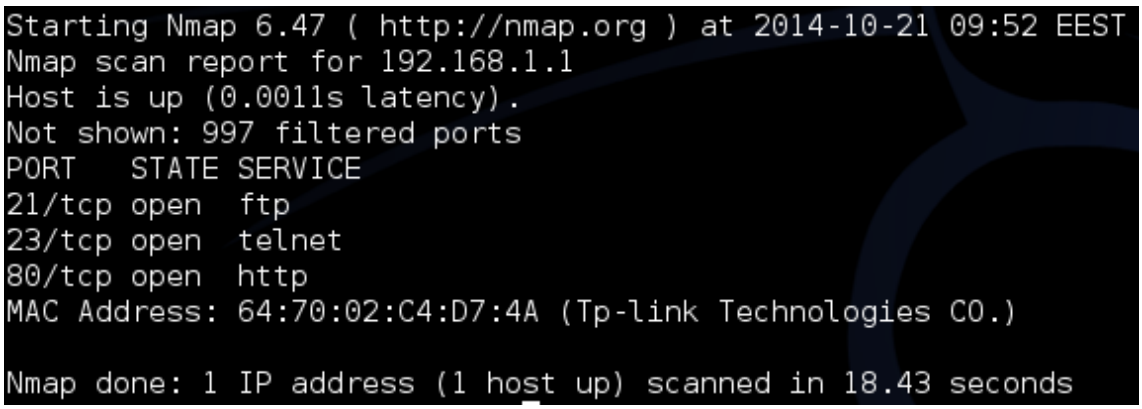
Kuva 8. Nmapin arvio mahdollisesta käyttöjärjestelmästä (Nmap 2014, kuvankaappaus)

4.5.2 Nmapin käyttö projektissa

Aluksi katsotaan Nmapilla, mitkä portit ovat auki. Komento on

nmap -T3 -Pn 192.168.1.1

-T on aikakytkin -T5 on nopein skannaus, mutta se ei välttämättä löydä kaikkea. -T0 on taas todella hidas skannaus, joka löytää parhaiten. -T3 on hyvä kompromissi. Kytkin -Pn pitää kohdetta aktiivisena, joten Nmap ei lähetä ICMP ping -pakettia kohteeseen. Lopuksi annettu IP-osoite on kohde, jota Nmap ryhtyy skannaamaan. Skannauksen päätyttyä Nmap tulostaa kuvan 9 tulosteen.



Kuva 9. Nmapin tuloste (Nmap 2014, kuvankaappaus)

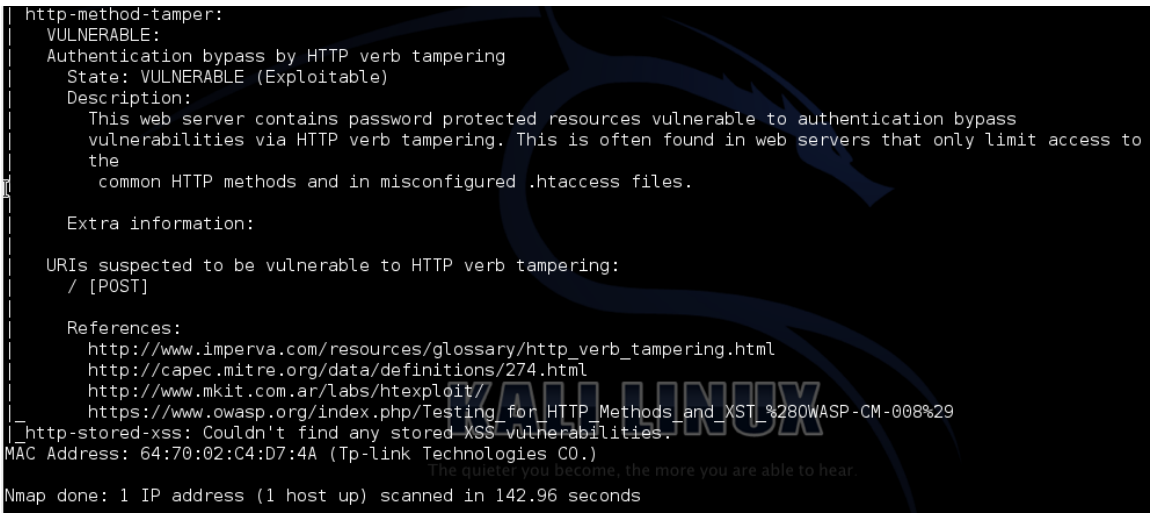
Kuten tulosteesta voidaan päätellä, ovat portit 21, 23 sekä 80 auki. Vastaavasti palvelut ftp, telnet sekä http ovat päällä TP-Linkissä.

Nmapin haavoittuvuuskannaus

Vaikka Nmap on pohjimmiltaan porttiskanneri, pystyy sillä kuitenkin kartoittamaan jonkin verran myäs mahdollisia haavoittuvuuksia. Tämä tapahtuu Nmap scripting engineä (NSE) käyttäen. Komento on

nmap -Pn -T3 --script vuln 192.168.1.1

Komennon osat -Pn sekä -T3 on selitetty aikaisemmassa esimerkissä. Komennon osa --script vuln on NSE:n yksi ominaisuuksista. Tämän komennon avulla Nmap pyrkii löytämään haavoittuvuuksia skannattavasta laitteesta. Skannauksen päätyttyä Nmap antaa kuvan 10 tulosteen.



Kuva 10. Haavoittuvuustestauksen tulokset tiivistettynä (Nmap 2014, kuvankaappaus)

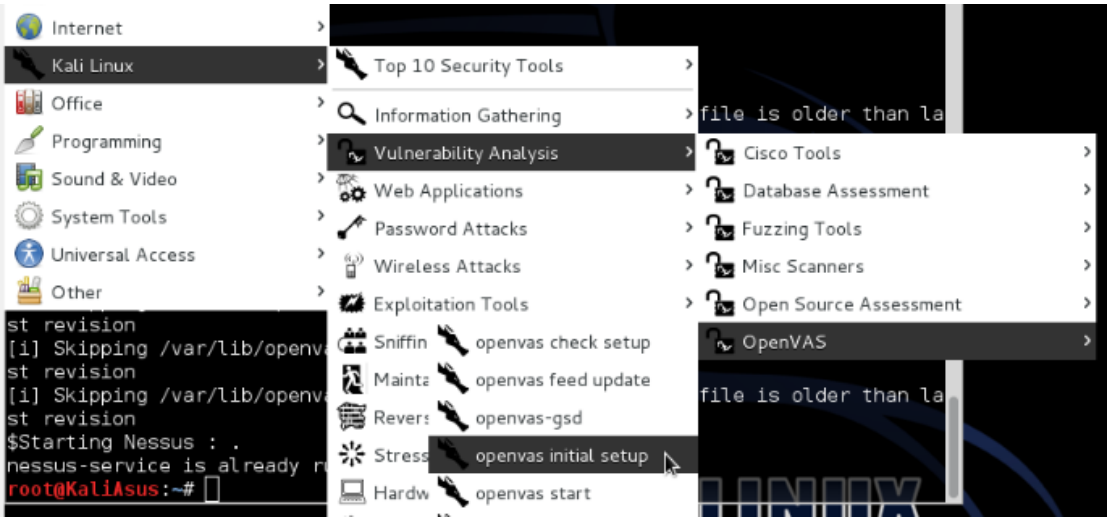
Nmap kertoo, että kohteessa on salasanalla suojattuja kohteita, joita pystyy tarkastelemaan ilman laitteelle kirjautumista. Nmap ilmoittaa, että mahdollisen haavoittuvuuden saattaa aiheuttaa POST-metodi. Seuraavaksi kohdetta skannataan Openvasia käyttäen, jotta tästä haavoittuvuudesta löydettäisiin lisää tietoa.

4.5.3 Openvas

Open Vulnerability Assessment Systems (OpenVAS) on ohjelmistokehys, johon kuuluu useita eri palveluita sekä ohjelmia, joiden avulla pystytään skannaamaan laitteista etsien haavoittuvuuksia. (About OpenVAS 2014.) OpenVAS syntyi vuonna 2005, kun Tenable Network Security muutti Nessuksen lähdekoodin suljetuksi. Nessuksen vielä avoimesta lähdekoodista julkaistiin GNessUs, joka myöhemmin nimettiin OpenVASiksi.

4.5.4 Openvasin käyttö projektissa

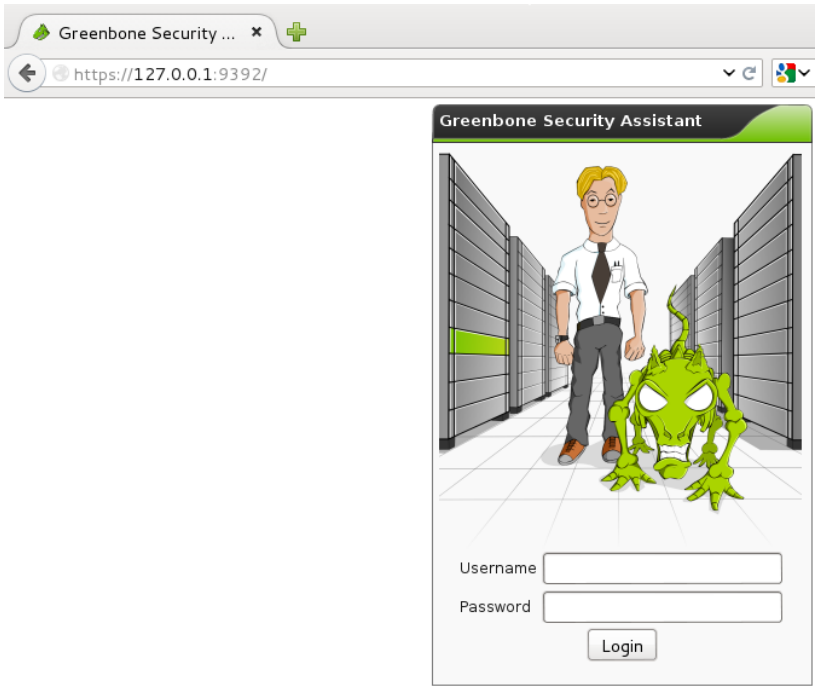
Kuvassa 11 valmistellaan Openvas käyttökuntoon. Tämä tapahtuu seuraavasti: Applications -> Kali Linux -> Vulnerability Analysis -> OpenVas -> openvas initial setup.



Kuva 11. Openvasin asennus (Openvas 2014, kuvankaappaus)

Tämä prosessi kestää hetken. Lopuksi ohjelma kysyy admin-käyttäjätunnukselle salasanaa.

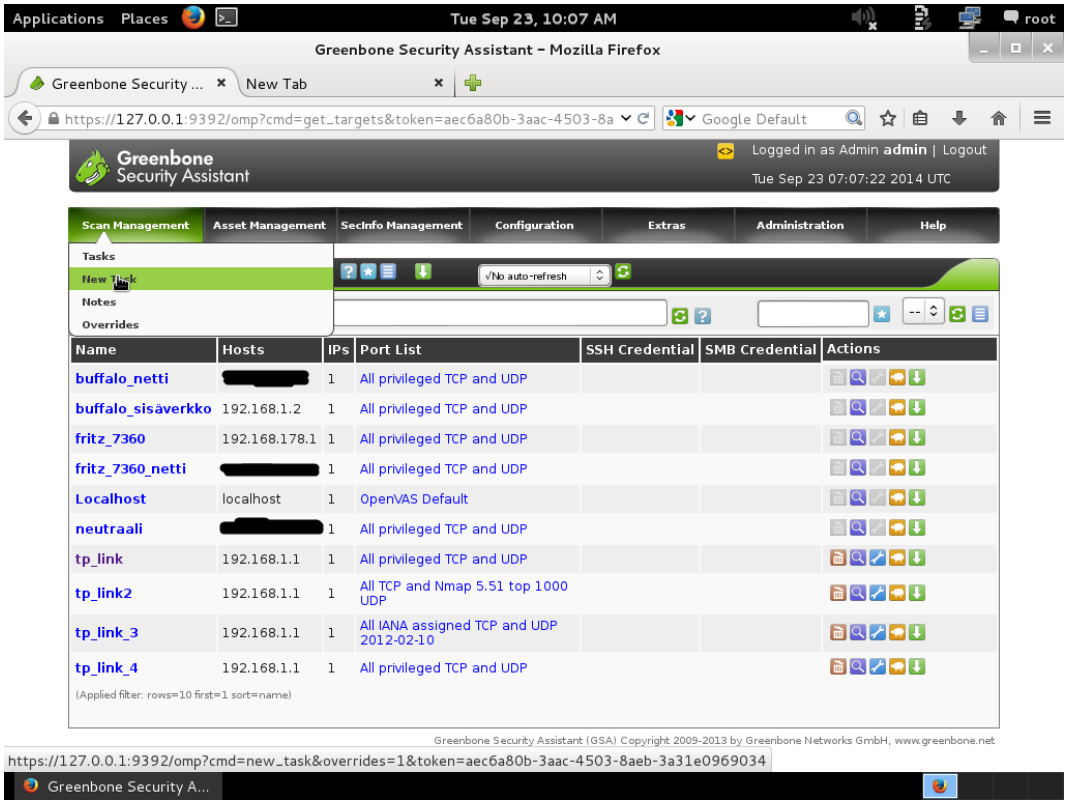
Openvas käynnistetään seuraavasti: Applications -> Kali Linux -> Vulnerability Analysis -> Openvas -> openvas start. Tässä menee hetki. Kun sovellus on käynnistynyt, aukaistaan internetselain sekä kirjoitetaan osoite https://127.0.0.1:9392. Kirjautumisruutu näyttää kuvan 12 mukaiselta.



Kuva 12. Openvasin etusivu (Openvas 2014, kuvankaappaus)

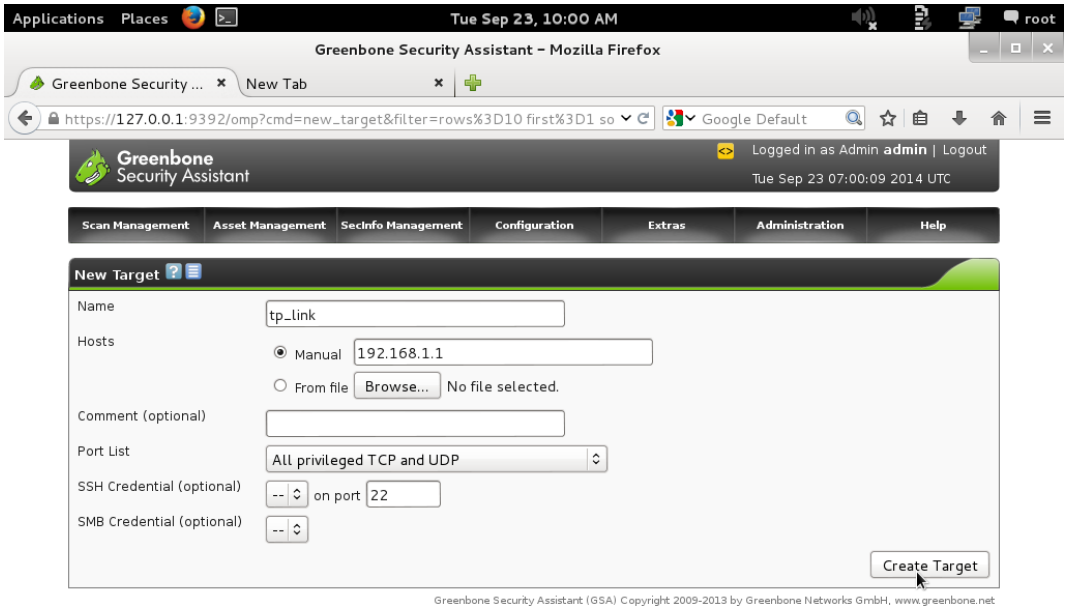
Skannauskohteen sekä uuden tehtävän luonti

Kuvassa 13 luodaan uusi kohde seuraavasti: Configuration -> Targets.



Kuva 13. Skannauskohteet (Openvas 2014, kuvankaappaus)

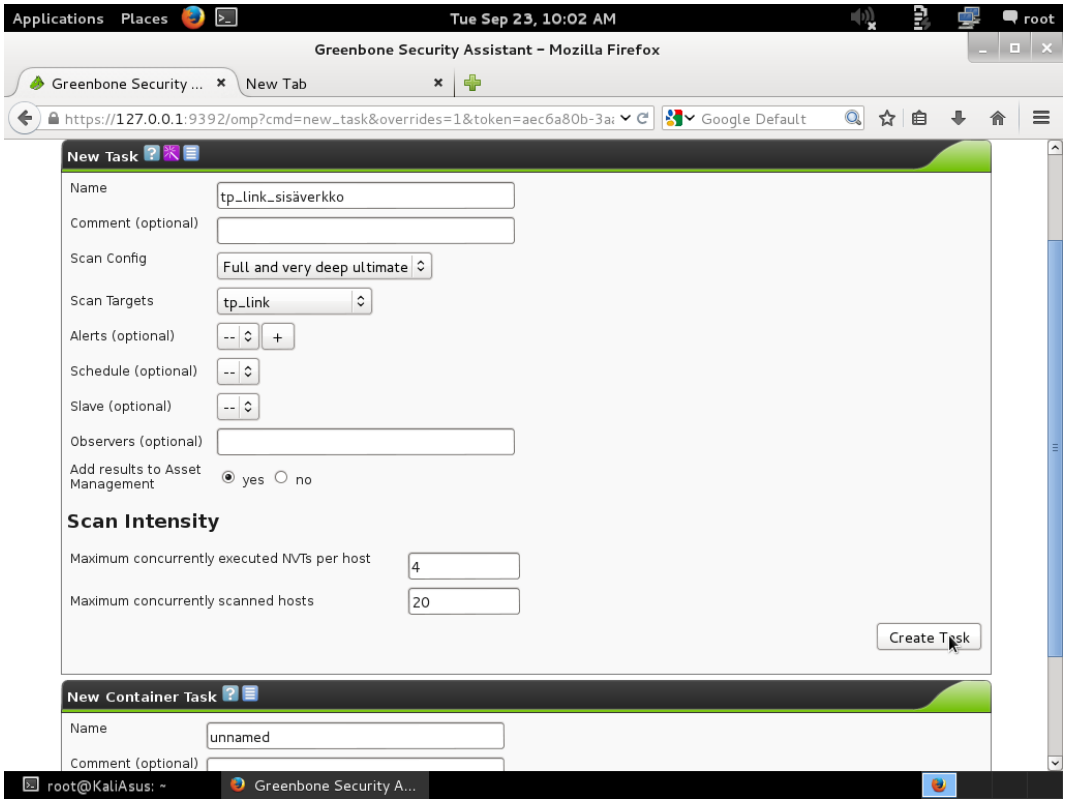
Kuvassa 14 tähteä painamalla päästään luomaan uutta kohdetta.



Kuva 14. Luodaan uusi kohde (Openvas 2014, kuvankaappaus)

Hostiksi määritetään yksittäinen ip-osoite tai tietty alue muodolla 192.168.1.1–100. Port list-kohdassa voidaan valita, mikä porttialue otetaan skannaukseen mukaan. Esimerkissä valittiin All privileged TCP and UDP, eli TCP / UDP portit väliltä 1–1024 otettiin mukaan skannaukseen.

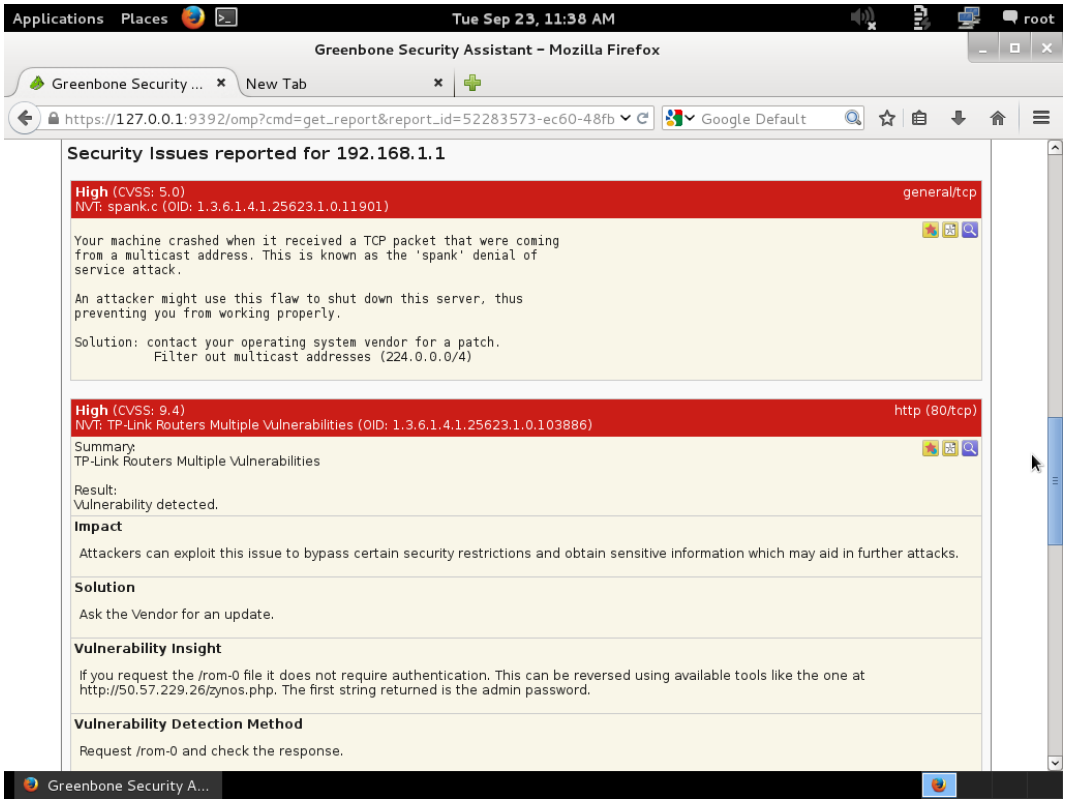
Kuvassa 15 luodaan uusi tehtävä Scan Management -> New Task. Tehtävälle annetaan nimi, sekä määritetään Scan Targets -kohtaan luotu kohde. Scan Configiksi kannattaa laittaa Full and very deep ultimate, sillä tämä on perusteellisin skannaustyyppi, joka löytää parhaiten tietoturva-aukkoja.



Kuva 15. Uuden skannauksen luonti (Openvas 2014, kuvankaappaus)

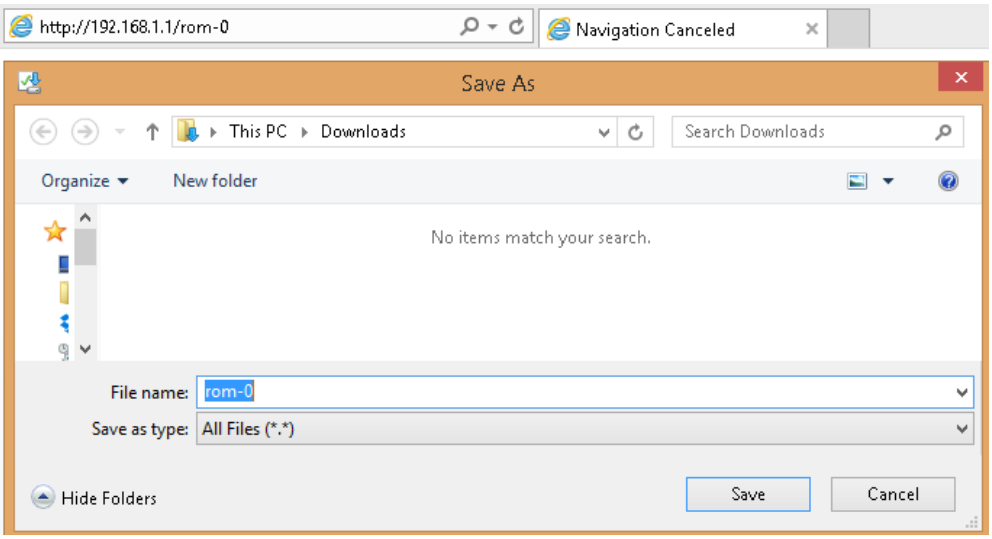
Löydetty haavoittuvuus

Openvasia käyttäen TP-Linkissä olleesta haavoittuvuudesta saatiin lisää tietoa. Full and very deep ultimate -skannauksen jälkeen löydettiin kuvan 16 mukainen tietoturva-aukko.



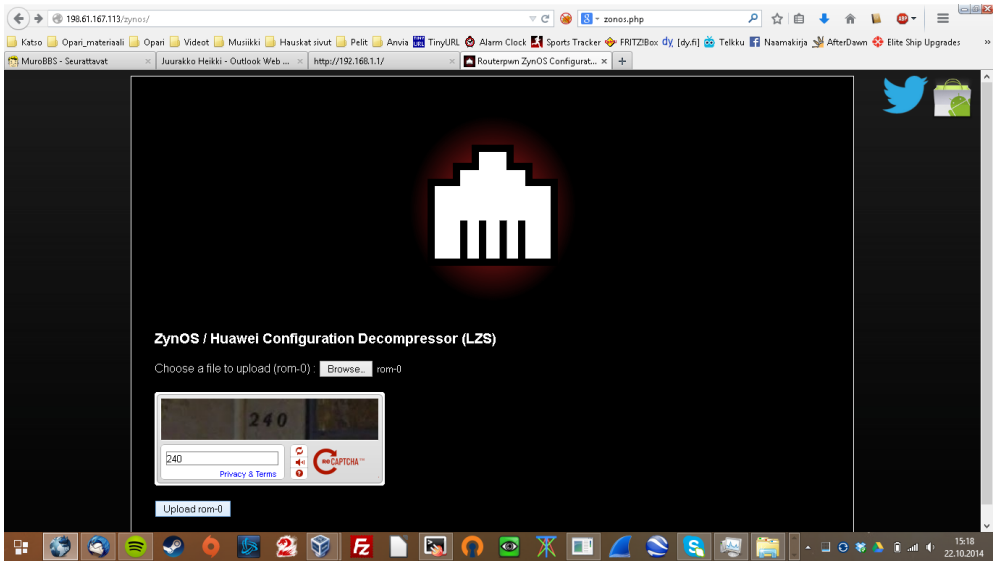
Kuva 16. Löydetty tietoturva-aukko (Openvas 2014, kuvankaappaus)

Tässä dokumentissa kerrotaan, että rom-0-tiedoston pystyy lataamaan TP-Linkistä ilman kirjautumista. Tässä tiedostossa mainitaan muun muassa admin-käyttäjän salasana. Tätä voidaan testata käytännössä. Avataan selain ja annetaan osoite 192.168.1.1/rom-0. Kuvassa 17 selain haluaa ladata rom-0-tiedoston.



Kuva 17. Ladataan rom-0-tiedosto (Adsl-modeemin hallintasivu 2014, kuvankaappaus)

Tämä tiedosto sisältää muun muassa koodinpätkän, joka sisältää admin-tunnuksen salasanan. Tämän jälkeen Googlesta haetaan hakusanalla zynos.php oikea sivu, johon voidaan lähettää rom-0-tiedosto tutkittavaksi. Kuvassa 18 zynos.php-internetsivu.



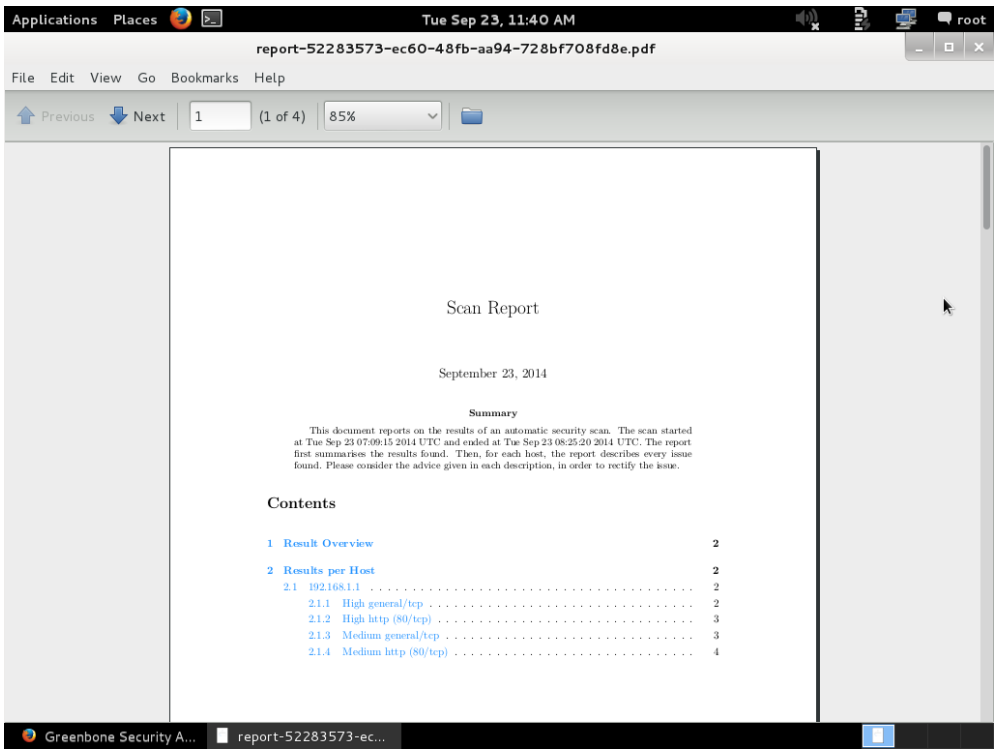
Kuva 18. Zynos.php-sivu (Zynos.php 2014, kuvankaappaus)

Browse-kohdasta etsitään rom-0-tiedosto sekä annetaan oikea captcha-merkkijono. Tämän jälkeen zynos.php muuttaa koodinpätkän salasanaksi, kuten kuvassa 18 näkyy.

Kuva 19. Admin-tunnuksen salasana selkokielisenä (Zynos.php 2014, kuvankaappaus)

Kuten kuvasta voidaan päätellä, on TP-Linkin admin-tunnuksen salasana s4l4s4n4. Nmap ilmoitti, että tämäntapainen haavoittuvuus on löydetty, mutta Nmap ei kuitenkaan osannut tarkemmin kertoa tästä haavoittuvuudesta. Openvas skannauksen avulla tästä haavoittuvuudesta saatiinkin enemmän tietoa.

Lopuksi löydetyistä haavoittuvuuksista voidaan luoda kuvan 20 mukainen tulostettava raportti, vaikkapa pdf-muodossa.



Kuva 20. Pdf-raportti TP-Linkin haavoittuvuuksista (Openvas 2014, kuvankaappaus)

4.5.5 Ohjelmien valinnasta

Miksi juuri Nmap sekä Openvas?

Nmapin valitsin projektiini siksi, koska sitä on aktiivisesti kehitetty jo vuodesta 1997. Tämä tarkoittaakin sitä, että Nmapiin löytyy todella kattavat ohjeet nmapin internet-sivuilla, osoitteesta nmap.org. Ohjelmasta on myös omat versiot muun muassa Windowsille, Linuxille kuin Mac OS:lle. Löytyypä Android-versiokin, joka perustuu lähes täysin Nmapin lähdekoodiin. Nmapin avulla verkkolaitteita voikin skannailla melkein millä tahansa laitteella. Nmapin lisenssinä on GNU-hankkeen yleinen lisenssi (GNU General Public License), joten kuka tahansa voi käyttää Nmapia ilmaiseksi etsiessään muun muassa avoimia portteja, palveluita sekä mahdollisia haavoittuvuuksia. Nmap löytyy myös esiasennettuna Kali Linuxista.

Alun perin aioin valita Nessuksen osaksi projektiani, mutta Nessuksen vuoden kestävä lisenssi olisi maksanut yritykselle 1500 dollaria. Seuraava hyvä vaihtoehto olikin sitten Openvas, jonka lisenssinä on GNU-hankkeen yleinen lisenssi. Openvasinkin kohdalla myös yritykset voivat käyttää tätä ohjelmaa etsiessään mahdollisia haavoittuvuuksia kohdeverkosta. Openvasia myös kehitetään koko ajan paremmaksi niin käytettävyydeltään kuin toiminnoiltaan. Siitä ei myöskään ole haittaa, että Openvas on esiasennettuna Kali Linuxiin.

Muita samanlaisia ohjelmia

Projektissani käytin ainoastaan Nmapia ja OpenVASia. Markkinoilla on kuitenkin tarjolla monta muuta samanlaista sovellusta, joilla voidaan skannailla verkkolaitteita etsien muun muassa avoimia portteja, palveluita ja haavoittuvuuksia.

Nessus on yksi suosituimmista ja parhaimmista tietoturvaskannereista. Se oli alun perin vapaa ohjelmisto, mutta vuonna 2005 se muuttui suljetuksi. Kaupallinen lisenssi maksaakin 1 500 dollaria per vuosi, mikä kuitenkin on edullinen verrattuna muihin kaupallisiin kilpailijoihin. Ilmainen lisenssi löytyy, mutta se on rajoitettu vain yksityiskäyttöön, sekä ominaisuuksia on karsittu. Nessusta päivitetään jatkuvasti ja tällä hetkellä siinä on 46 000 pluginia. Tärkeimpiä ominaisuuksia ovat etänä sekä paikallisesti tehtävät tietoturvatestit, WWW-pohjainen käyttöliittymä sekä mahdollisuus kirjoittaa omia plugineita. (Network Security Tools 2014.)

Secunia PSI (Personal Software Inspector) on ilmainen työkalu, jonka avulla voidaan havaita tietoturva-aukkoja sekä päivittämättömiä ohjelmia sekä plugineita, jotka altistavat pc:n hyökkäyksille. Anti-virus ohjelmat harvoin estävät hyökkäyksiä, jotka kohdistuvat haavoittuviin ohjelmiin sekä plugineihin. Secunia PSI tarkistaa vain sen koneen tietoturvan, johon se on asennettu. Kaupallisella versiolla, Secunia CSI (Corporate Software Inspector) pystytään skannaamaan myös muitakin saman verkon koneita. (Network Security Tools 2014.)

QualysGuard on suosittu SaaS (software as a service) haavoittuvuuksien hallintatyökalu. Sen webbipohjainen käyttöliittymä tarjoaa mahdollisuudet verkon kartoitukseen sekä

haavoittuvuuksien arvioimiseen. Sisäiset skannaukset hoidetaan Qualyksen laitteilla, jotka kommunikoivat pilvipalvelun kanssa. (Network Security Tools 2014.)

Microsoft Baseline Security Analyzer (MBSA) on helppokäyttöinen työkalu, joka on suunniteltu pk-yrityksissä työskenteleville IT-ammattilaisille. MBSA:n avulla voidaan helposti määrittää, kuinka turvallinen heidän Microsoft ympäristönsä on. MBSA:n avulla skannataan viikoittain yli miljoona tietokonetta. (Network Security Tools 2014.)

4.6 Testausohje

Opinnäytetyön yhtenä tehtävänä oli luoda testausohje, jonka avulla haavoittuvuuksia voitaisiin etsiä nopeasti ja helposti asiakaspäätelaitteista. Tässä testausohjeessa neuvotaan, miten kohteesta voidaan löytää avoimet portit, palvelut sekä mahdolliset haavoittuvuudet. Ohjelmiksi valitsin Nmapin sekä Openvasin, koska ne perustuvat GNU-hankkeen yleiseen lisenssiin (GNU General Public License). Tämä tarkoittaakin sitä, että myös yritykset voivat käyttää näitä sovelluksia vapaasti ilman lisenssimaksua. Näitä ohjelmia on myös helppo käyttää, sillä Nmapin kotisivuilla on todella kattavat ohjeet, miten Nmapin eri kytkimet toimivat. Openvasiin löytyy myös tämän omilta kotisivuilta hyvät ohjeet, kuinka päästä alkuun haavoittuvuusskannauksessa. Kali Linuxista löytyy myös kyseiset sovellukset valmiina asennettuna, joten tämäkin asia tukee näiden sovellusten valintaa.

Monet internetpalveluntarjoajat pyrkivät testaamaan myyntiin tulevat laitteet. Tarkoituksena on tutkia, löytyykö asiakaspäätelaitteista kaikki tarvittavat ominaisuudet. Testattavia asioita ovat muun muassa vaikkapa wpa2-salaus langattomassa verkossa, toimivatko kaikki adsl2+:n ominaisuudet kunnolla, tai vaikkapa, pyrkiikö asiakaspäätelaite hakemaan uudestaan IP-osoitetta, kun verkkokaapeli on syystä tai toisesta irrotettu hetkeksi. Internetpalveluntarjoaja voi ottaa luomani testausohjeen osaksi omia testejään, minkä avulla voidaan pikaisesti tutkia, onko asiakaspäätelaitteessa mahdollisia haavoittuvuuksia. Jos asiakaspäätelaitteesta löytyy mahdollinen tietoturvaongelma, palveluntarjoaja voi ilmoittaa tästä suoraan valmistajalle. Tämän jälkeen valmistaja toivottavasti pyrkii korjaamaan havaitun ongelman julkaisten uuden firmwaren asiakaspäätelaitteelle.

Testausohjeen rakenne

Testausohjetta rakentaessa täytyy ottaa huomioon muutamia asioita. Ensin täytyy kertoa, kenelle ohje on tarkoitettu. Ohjeessa kannattaa myös esitellä ympäristö sekä näyttää konkreettisesti, miten ohjelma toimii. Ohjeessa kannattaa myös perustella, miksi tietty asia tehdään niin kuin se tehdään. (Korpela 2000.)

Testausohjeessa ensin esitellään testausympäristö, jossa asiakaspäätelaitteita voidaan testata. Testausympäristö on samankaltainen, kuin kuvissa 2 ja 3. Tämän jälkeen kerrotaan työkaluista, joita testauksessa tarvitaan. Nämä työkalut ovat Nmap sekä OpenVAS. Käyttöjärjestelmäksi suositellaan Kali Linuxia, mutta testausohjeessa on myös ohjeet Nmapin sekä OpenVASin asentamiseksi myös muille Linux-distribuutioille sekä Windowsille.

Testausohjeessa käydäänkin samat asiat läpi, kuin tämän opinnäytetyön työosiossa. Ensiksi Nmapilla etsitään avoimet portit, asiakaspäätelaitteessa pyörivä käyttöjärjestelmä sekä mahdolliset haavoittuvuudet. Tämän jälkeen esitellään, kuinka OpenVAS saadaan käyttökuntoon. Seuraavaksi luodaankin uusi skannauskohde, sekä aloitetaan itse skannaus. Lopuksi OpenVASista voidaan tulostaa pdf-muodossa raportti löydetyistä haavoittuvuuksista. Testausohje on työn liitteenä 1.

POHDINTA

Tässä opinnäytetyössä pohdittiin, mitä tietoturvatestaus on. Lopuksi luotiin testausohje, jonka avulla asiakaspäätelaitteesta voidaan etsiä avoimia portteja sekä haavoittuvuuksia. Alun perin oli tarkoitus käsitellä tarkemmin muun muassa sitä, minkälaisia haavoittuvuuksia asiakaspäätelaitteista jo löytyy. Tietoturva-aukot kun ovat oikea ongelma, joiden avulla rikolliset voivat luoda todella massiivisia bottiverkkoja, joita käyttävät omiin rikollisiin hankkeisiinsa. Itse testauksessa piti alun perin skannailla asiakaspäätelaitteita myös ulkoapäin, mutta tämä jäi ajanpuutteen vuoksi toteuttamatta.

Testausohjeessa käyttämäni metodit soveltuvat kaikkien sellaisten verkkolaitteiden skannaukseen, joilla on IP-osoite. Nmapilla sekä Openvasilla voidaan skannata niin yritystason reitittimiä sekä palvelimia kuin kännyköitä tai vaikkapa tulostimia, etsien avoimia portteja sekä mahdollisia haavoittuvuuksia. Jos laite vain on verkossa, voi siitä löytyä mahdollisia tietoturva-aukkoja, joita voidaan käyttää hyödyksi rikollisiin toimiin.

Opinnäytetyön tavoite on jotakuinkin saavutettu, sillä lopputuloksena syntyi testausohje, jonka avulla Anvia pystyy etsimään asiakaspäätelaitteista nopeasti ja helposti avoimia portteja sekä mahdollisia haavoittuvuuksia. Tämä testausohje on myös sovellettavissa muihinkin Anvian ylläpitämiin palveluihin, kuten reitittimiin sekä erilaisiin palvelimiin. Testausohjetta tulisikin ylläpitää sekä laajentaa aina tarvittaessa, jotta mahdolliset tietoturva-aukot voitaisiin löytää mahdollisimman vaivattomasti järjestelmästä.

Jatkokehitysideana tälle opinnäytetyölle voisi olla, että tutustuttaisiin enemmän laitespesifeihin tietoturvaongelmiin. Yhtenä vaihtoehtona olisi luoda lista, johon merkitään Anvian myymät asiakaspäätelaitteet ja niistä löydetyt tietoturva-aukot. Tämä lista päivittyisi aina, kun uusi asiakaspäätelaite otetaan operaattorin tuotevalikoimaan tai asiakaspäätelaitteelle on julkaistu uusi firmware, joka on mahdollisesti korjannut tunnettuja tietoturva-aukkoja. Tämä kuitenkin vaatisi aktiivista alan seurantaa ja tutkimustyötä, jotta pysyttäisiin ajan tasalla nykyisten tietoturvaongelmien määrästä ja laadusta.

LÄHTEET

About OpenVAS. 2014. Luettu 1.11.2014.
http://www.openvas.org/about.html

Adsl-modeemin hallintasivu. 2014. Kuvankaappaus TP-Link TD-W8961ND:n hallinta-sivusta.
http://192.168.1.1

Allen, L. 2012. Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide. Birmingham: Packt Publishing Ltd.

Assolini, F. 2012. The Tale of One Thousand and One DSL Modems. Luettu 15.11.2014.
http://securelist.com/blog/research/57776/the-tale-of-one-thousand-and-one-dsl-modems/

Engebretson, P. & Kennedy, D. 2013. The Basics of Hacking and Penetration Testing. Second Edition. Waltham: Elsevier Inc.

Järvinen, P. 2006. Paranna tietoturvaasi. Jyväskylä: Docendo Finland Oy.

Korpela, J. 2000. Yksinkertaisen neuvon antaminen. Viitattu 24.11.2014.
https://www.cs.tut.fi/~jkorpela/metaopas/yks.html

Munson, L.2014. What are the main differences between hackers and crackers? Luettu 28.11.2013.
http://www.security-faqs.com/what-are-the-main-differences-between-hackers-and-crackers.html

Nettibisnes.info. 2010. OSINT verkossa eli laillisen nettitiedustelun perusteet. Viitattu 10.2.2014.
http://www.nettibisnes.info/osint-verkossa-eli-laillisen-nettitiedustelun-perusteet/

Network Security Tools. 2014. Luettu 2.11.2014.
http://sectools.org/tag/vuln-scanners/

Nmap. 2014. Luettu 11.11.2014.
http://nmap.org/

Nmap Description. 2014. Viitattu 7.10.2014.
http://nmap.org/book/man.html#man-description

Nmap from Beginner to Advanced. 2014. Luettu 2.11.2014.
http://resources.infosecinstitute.com/nmap/

Openvas. 2014. Luettu 11.11.2014.
http://www.openvas.org/

Penetration Testing Execution Standard 2012a. Pre-engagement. Viitattu 6.2.2014. http://www.pentest-standard.org/index.php/Pre-engagement

Penetration Testing Execution Standard 2012b. Intelligence Gathering. Viitattu 10.2.2014.
http://www.pentest-standard.org/index.php/Intelligence_Gathering

Penetration Testing Execution Standard 2012c. Vulnerability Analysis.Viitattu 14.10.2014.
http://www.pentest-standard.org/index.php/Vulnerability_Analysis

Penetration Testing Execution Standard 2012d. Threat Modeling. Viitattu 5.3.2014.
http://www.pentest-standard.org/index.php/Threat_Modeling

Port Scanning Techniques. 2014. Luettu 2.11.2014.
http://nmap.org/book/man-port-scanning-techniques.html

The History and Future of Nmap.2014. Luettu 6.10.2014.
http://nmap.org/book/history-future.html

Zynos.php. 2014. Luettu 11.11.2014.
http://198.61.167.113/zynos/

LIITTEET

Liite 1. Testausohje

TESTIOHJE Sivu 1 / 13

VER. 0.01

Osasto/Toimisto:
Dokumentin laatija: Heikki Juurakko 15.9.2014

Tietoturvatestausta skannereiden avulla

Sisältö

Revisiotieto

Revisio	Nimi	Syy
0.01		Ensimmäinen versio

Yleistä

Projekti

Projekti: Tietoturvatestaus

Testattu laite/palvelu

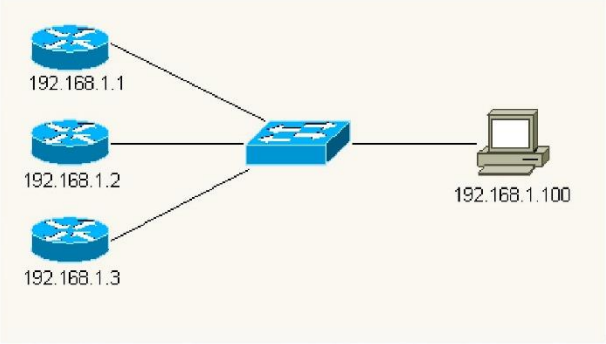
Tämän raportin tarkoituksena on opastaa testaajaa käyttämään Nmap:ia sekä Openvasia, joiden avulla asiakaspäätelaitteesta voidaan etsiä avoimet portit sekä mahdolliset haavoittuvuudet.

Testi setup

Kuva testiverkosta:

Perus porttiskannaus suoritetaan tällöin komennolla nmap 192.168.1.1.

Jos testattavana useita laitteita, testiverkko voi näyttää tältä:



Tällaisessa tilanteessa käytetään komentoa nmap 192.168.1.1,2,3 porttiskannaukseen. Tämän komennon avulla porttiskannaus tehdään kaikkiin kolmeen asiakaspäätelaitteeseen.

Työkalut

Tässä testausohjeessa käytetään Nmap:ia sekä Openvasia. Molemmat työkalut löytyvät valmiiksi asennettuina Kali Linuxista. Kali Linux on Debianista johdettu Linux- distribuutio, joka on tehty vartavasten tietoturvatestaamiseen. Kali Linuxin voi ladata osoitteesta http://www.kali.org/downloads/. Kätevimmin Kali Linuxia ajaa suoraan virtuaalikoneelta, esimerkiksi Virtualboxilla tai Vmwarella.

Jos et aio käyttää Kali Linuxia, niin tässä on vaihtoehtoiset ohjeet:

Debianille ja Ubuntulle Nmapin saa asennettua komennolla sudo apt-get install nmap / sudo aptitude install nmap. Windowsille Nmapin saa ladattua osoitteesta http://nmap.org/download.html kohdasta ”Microsoft Windows binaries”.

Ohjeet Openvasin asentamiseksi eri alustoille löytyy sivulta http://www.openvas.org/download.html. Openvasin työpöytäversio löytyy myös Kali Linuxista valmiiksi asennettuna, mutta tässä ohjeessa käytetään selainversiota.

Tämä testausohje on tehty käyttäen Kali Linuxia. Nmap sekä Openvas on jo asennettu, mutta Openvas pitää laittaa ensin käyttökuntoon. Tässä teustasohjeessa tähän on kuitenkin ohjeet.

Referenssit

http://en.wikipedia.org/wiki/Kali_Linux
http://nmap.org/book/man-briefoptions.html
http://nmap.org/book/nse-usage.html
http://nmap.org/download.html
http://www.kali.org/downloads/

Nmap skannaukset

Selitykset käytettäville kytkimille

Nmap kytkimet:

-A	(aggressive scan) Etsii käyttöjärjestelmän, kohteen version, tekee tracerouten sekä tekee skriptiskannauksen.
-h	Help. Tämän avulla voidaan etsiä pikaisesti tietoa Nmapin eri kytkimistä.
-O	Etsii käyttöjärjestelmän.
-Pn	Pitää kaikkia skannattavia kohteita aktiivisina.
-p-	Ottaa kaikki portit mukaan testiin.
-sU	UDP- porttiskannaus
-sV	Etsii avoimen portin takana olevan palvelinohjelmiston tiedot.
-T	Aikakytkin -T5 on nopein skannaus, mutta ei välttämättä löydä kaikkea. -T0 on taas todella hidas skannaus, mutta löytää parhaiten. -T3 on hyvä kompromissi.
-v	Tekee tulosteesta runsassanaisemman.

NSE kytkimet:

--script banner	Etsii mahdollisen bannerin, joka kohteessa on.
--script vuln	Etsii mahdollisia haavoittuvuuksia, joita kohteessa on.

Linuxin komentorivikomennot:

grep	Voidaan tulostaa halutut rivit, jotka sisältävät määritetyn merkkijonon.

Mitkä portit ovat auki?

Komentovaihtoehtoja:
nmap 192.168.1.1
nmap -Pn -p- 192.168.1.1 | grep 'open'
-T kytkimellä voidaan lisätä skannauksen tarkkuutta.

Mikä käyttöjärjestelmä?

Komentovaihtoehtoja:
nmap –O -p- 192.168.1.1
nmap –v –O -p- 192.168.1.1
nmap –A -p- 192.168.1.1

Jos ei näillä komennoilla näytä käyttöjärjestelmää, niin –osscan-guess kytkimellä pyrkii antamaan parhaimman arvauksen

-T kytkimellä voidaan lisätä skannauksen tarkkuutta

Minkälainen banneri löytyi?

Komentovaihtoehtoja:
nmap –script banner 192.168.1.1
-T kytkimellä voidaan lisätä skannauksen tarkkuutta

Mitä haavoittuvuuksia löytyi?

Komentovaihtoehtoja:
nmap –script vuln 192.168.1.1
-T kytkimellä voidaan lisätä skannauksen tarkkuutta

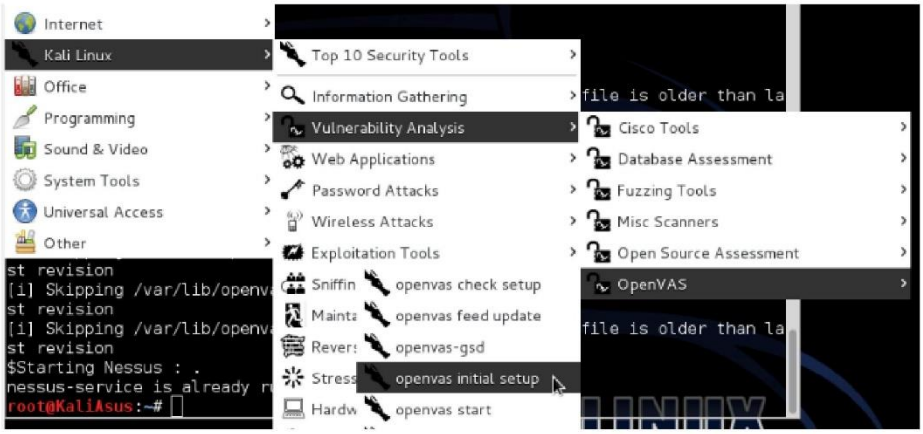
Mitä eri tietokannat kertoivat löydetyistä haavoittuvuuksista?

Tietokantoja:
http://www.cvedetails.com/vulnerability-search.php
http://www.exploit-db.com/search/
http://web.nvd.nist.gov/view/vuln/search
http://www.rapid7.com/db/modules/

Openvas skannaukset

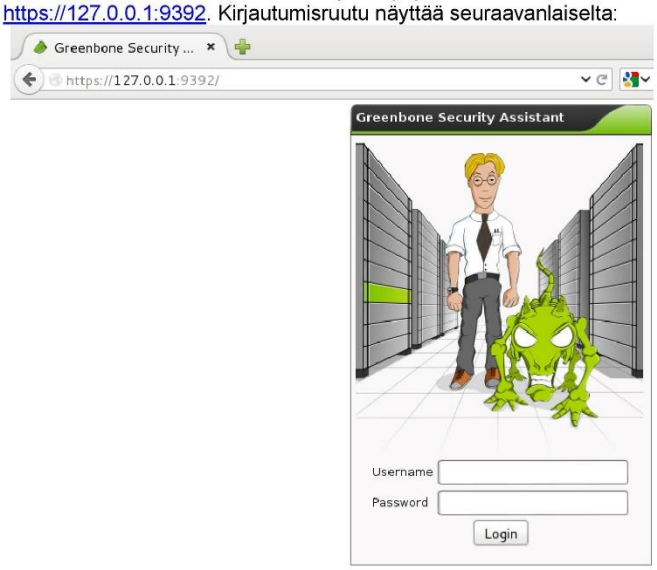
Openvasin asentaminen käyttökuntoon

Ensiksi valmistellaan Openvas käyttökuntoon. Tämä tapahtuu seuraavasti. Applications -> Kali Linux -> Vulnerability Analysis -> OpenVas -> openvas initial setup:



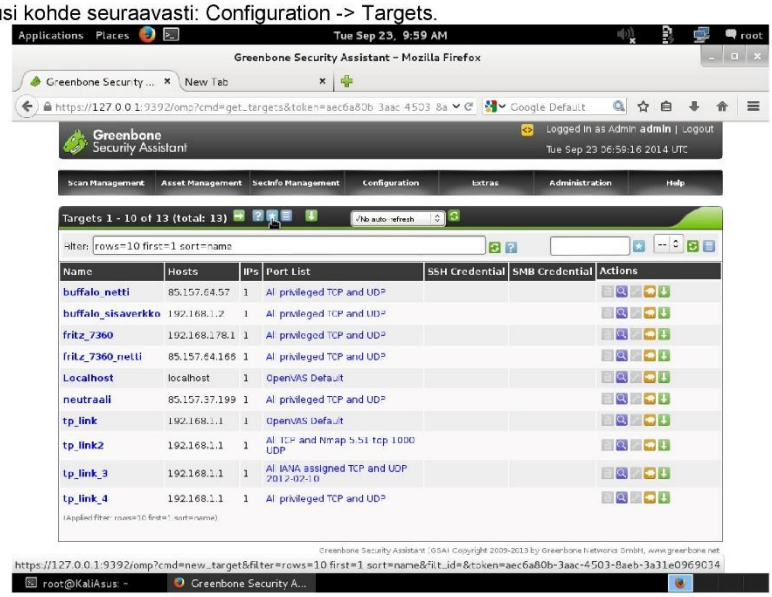
Tämä prosessi kestää hetken. Lopuksi ohjelma kysyy admin- käyttäjätunnukselle salasanaa.

Openvas käynnistetään seuraavasti: Applications -> Kali Linux -> Vunlerability Analysis -> OpenvVas -> openvas start. Tässä menee hetki. Kun sovellus on käynnistynyt, aukaistaan internet selain sekä kirjoitetaan osoite https://127.0.0.1:9392. Kirjautumisruutu näyttää seuraavanlaiselta:

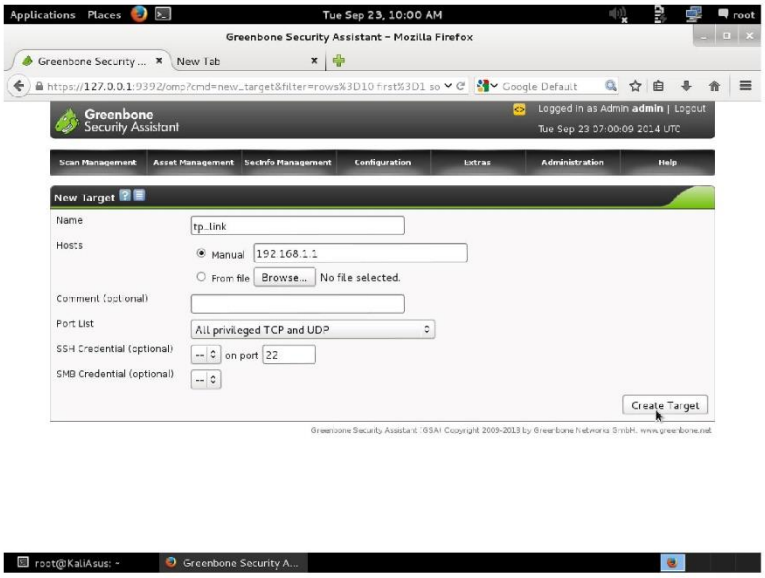


Skannauskohteen sekä uuden tehtävän luonti

Luodaan uusi kohde seuraavasti: Configuration -> Targets.

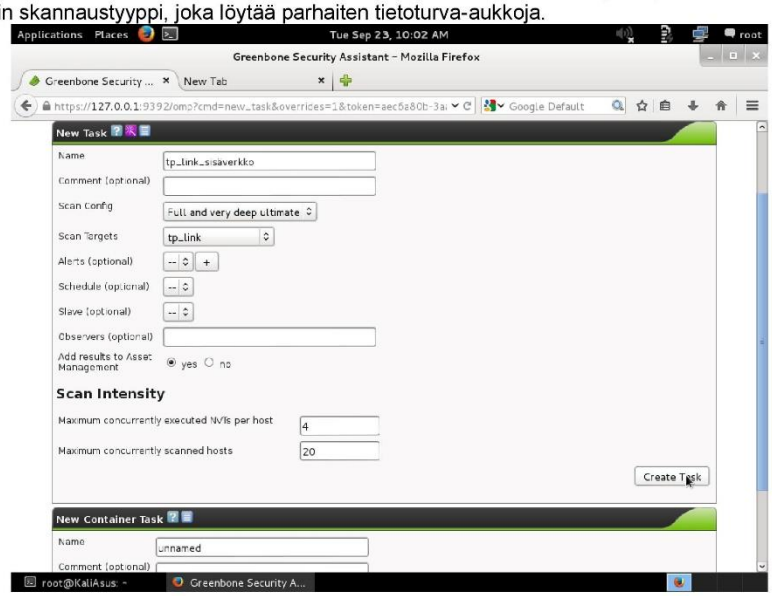


Tähteä painamalla päästään luomaa uutta kohdetta:



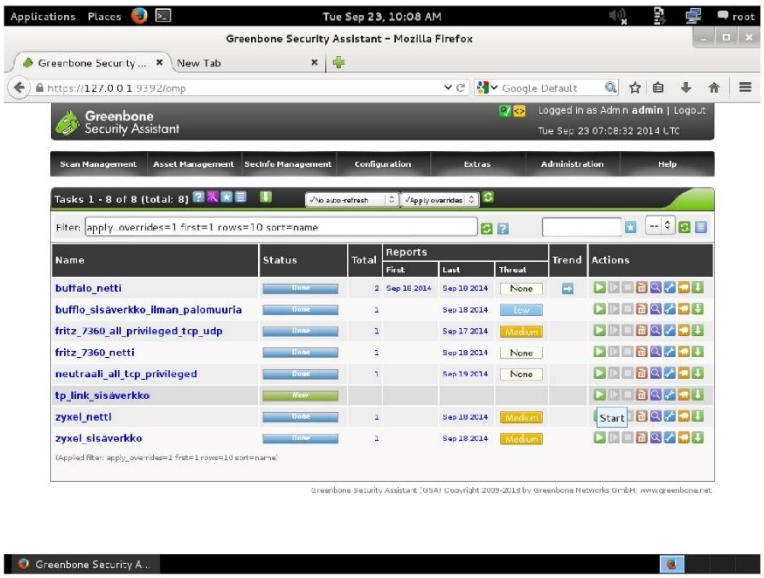
Hostiksi määritetään yksittäinen ip- osoite tai tietty alue muodolla 192.168.1.1-100. Port list- kohdassa voidaan valita, mikä porttialue otetaan skannaukseen mukaan. Esimerkissä valittiin ”All privileged TCP and UDP”, eli TCP / UDP portit väliltä 1-1024 otettiin mukaan skannaukseen.

Uusi tehtävä luodaan Scan Management -> New Task. Annetaan tehtävälle nimi, sekä määritetään Scan Targets- kohtaan luotu kohde. Scan Configiksi kannattaa laittaa ”Full and very deep ultimate”, sillä tämä on perusteellisin skannaustyyppi, joka löytää parhaiten tietoturva-aukkoja.

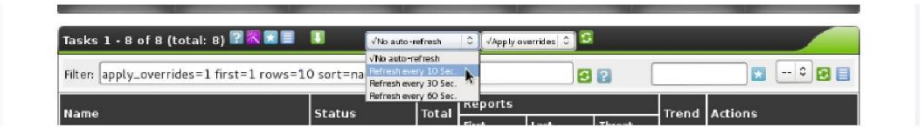


Skannauksen aloittaminen

Skannaus aloitetaan seuraavasti: Scan Management -> Tasks. Listalta etsitään äsken luotu tehtävä, sekä painetaan vihreää play- nappia aloittaen kohteen skannauksen.

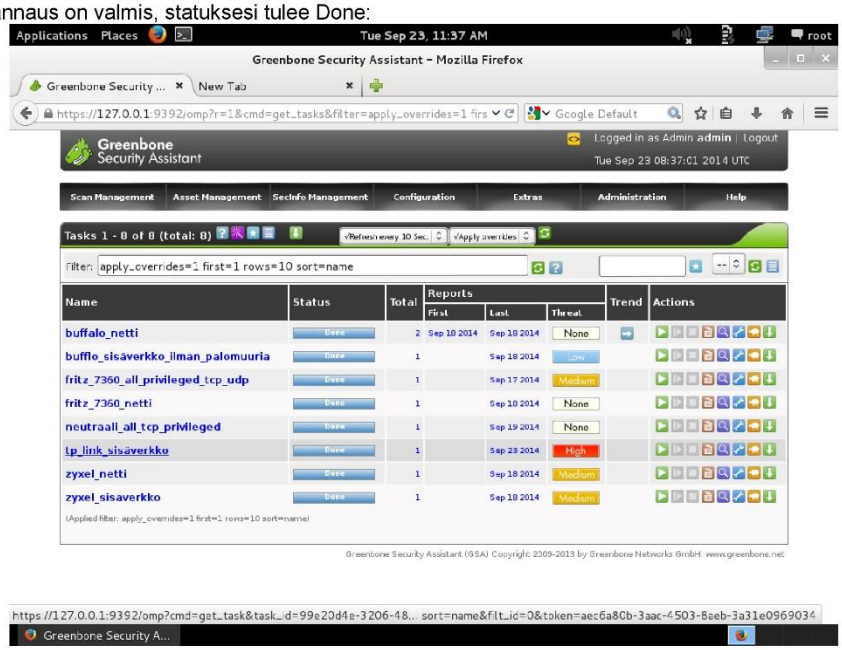


Skannauksen edistymistä voi seurata laittamalla päivityksen päälle:

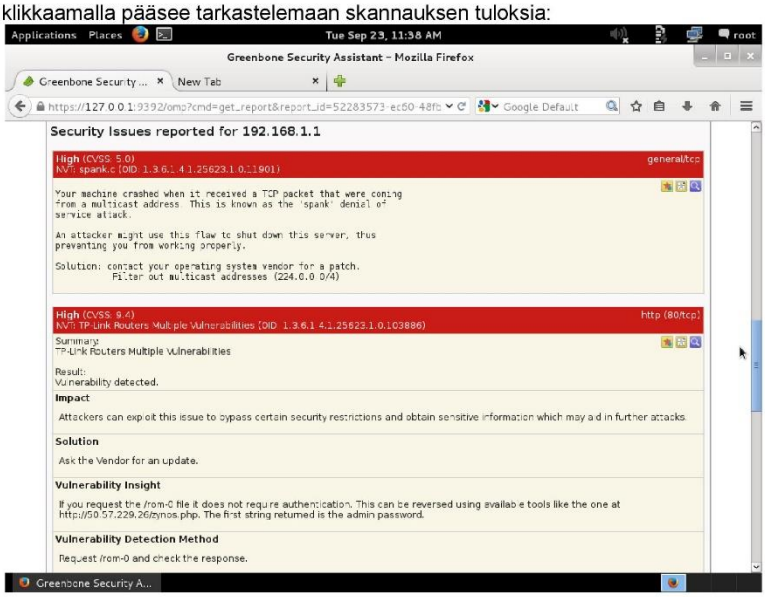


Skannaus valmis

Kun skannaus on valmis, statuksesi tulee Done:

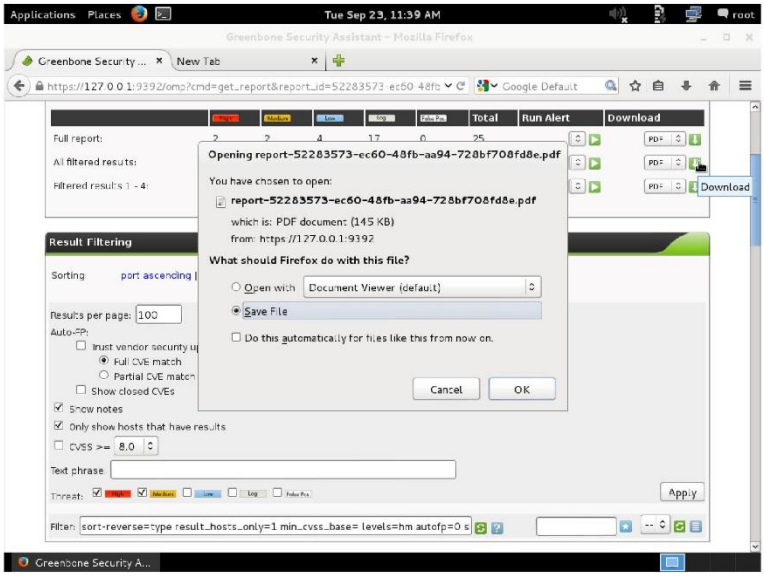


Skannausta klikkaamalla pääsee tarkastelemaan skannauksen tuloksia:



Raportin lataus ja katselu pdf- muodossa

Ladataan raportti pdf- muodossa:



Pdf raportti näyttää tältä: