LAUREA

Virtuaaliympäristön luominen opetuskäyttöön

Kärkkäinen Mikko

Pulkkinen Lauri

2011 Laurea leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Virtuaaliympäristön luominen opetuskäyttöön

Mikko Kärkkäinen
Lauri Pulkkinen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Maaliskuu, 2011

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Mikko Kärkkäinen
Lauri Pulkkinen

Virtuaaliympäristön luominen opetuskäyttöön

Vuosi 2010 Sivumäärä 64

Tämän opinnäytetyön tilaajana toimii Laurean Neon-laboratorio. Työn tarkoituksena on luoda virtuaaliympäristö, jossa voisi käyttää tietoturvaohjelmia ja joita voisi hyödyntää opetuskäytössä, erityisesti tietojenkäsittelyn tietoturvaopetuksessa. Ohjelmien runsaan tarjonnan vuoksi työhön on valittu kaksi suosittua tietoturvaan liittyvää ohjelmistoa. Työ on rajattu vain vapaan lähdekoodin ohjelmistoihin. Työ suoritetaan lisäksi Linux-pohjaisena ja virtualisointi VirtualBox -ohjelmistolla, koska niistä ei synny kustannuksia.

Työ jakautui kahteen vaiheeseen. Ensimmäisessä vaiheessa tutkimme ja testailimme eri ohjelmia ja valitsimme niistä sopivimmat. Valitsimme kaksi vapaaseen lähdekoodiin perustuvaa ohjelmaa. NMAP-porttiskannerin verkkotiedustelua varten ja OpenVAS-haavoittuvuuksien etsintä ja arviointi työkalun. Toisessa vaiheessa suoritimme ohjelmien asennukset sekä konfiguroinnin.

Tämä konstruktiivinen tutkimustyö ei liity Laurean aikaisempiin projekteihin. Laureassa ei ole aikaisemmin ollut vastaavaa virtuaaliympäristöä. Työssä kerrotaan yleisesti käytetyistä ohjelmista, minkä lisäksi yksityiskohtaisesti koko virtuaaliympäristön asennuksen ja jokaisen käytetyn ohjelmiston asennus ja –käyttöohjeet.

Projektin tavoitteena oli luoda virtuaaliympäristö sekä saada valitut ohjelmat toimimaan. Lopputulos saavutettiin, mutta huomasimme, että toteutetun virtualisoinnin kautta tämä ei välttämättä ole paras vaihtoehto, mutta toimiva, jos olisi oma palvelin. Jos palvelimella ajaisi palvelinohjelmat, niin virtualisoinnin kautta voisi ajaa asiakasohjelmat. Näin järjestelmää pystyisivät käyttämään useat henkilöt samaan aikaan, mikä olisi tarkoituksen mukaista opetuskäytössä.

Asiasanat Virtualisointi. Linux, NMAP, OpenVAS

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Business Information System

Mikko Kärkkäinen
Lauri Pulkkinen

Creating a virtual environment for educational use

Year 2010 Pages 64

This thesis was commissioned by Laurea Neon laboratory. The purpose is to create a virtual environment in which to run security software, and which could also be used in teaching, particularly in data processing and information security education. Because of abundant supply of software, it was decided to choose two most appropriate programs. It was decided to limit the use only to open source software. Work is also carried out on a Linux-based virtualization, with the free VirtualBox as the virtualization solution, so there will be no additional costs.

The work is divided into two phases. The first phase of the study is to research and test various programs and choose the most suitable ones. It was decided to choose two open source software, the NMAP port scanner and the OpenVAS vulnerability and evaluation tool. At the second stage, it was time to carry out the installation of software.

This thesis is not related to previous Laurea projects and Laurea has not previously had a similar virtual environment. There will be a general review of all programs used and detailed instructions for installing and using all the software required.

The final goal of the project was to create a virtual environment and have selected programs working correctly. The final result was achieved, but it was found out that the chosen virtualization solution was not necessarily the best solution, but would be more effective if there was a dedicated server. The server software should be run on the server and the client software by virtualization, so the system would be faster and serve more people at the same time, which would be more useful as part of teaching use in future.

Key words Virtualization, Linux, NMAP, OpenVAS

Sisällys

1 Johdanto

Laureassa olisi käyttöä virtuaaliselle ympäristölle, jossa opiskelijat voisivat testata erilaisten porttien ja haavoittuvuuksien tiedusteluun tarkoitettuja ohjelmia, kuten NMAP ja OpenVAS. Tällaista järjestelmää ei ole aikaisemmin ollut Laureassa. Siitä olisi paljon hyötyä erityisesti tietojenkäsittelyn tietoturvaopetuksessa.

Tämä työ ei liity aikaisempiin Laurean hankkeisiin. Toteutamme tämän opinnäytetyön avoimen lähdekoodin ohjelmilla, joten Laurealle ei synny kustannuksia. Virtualisointi toteutetaan VirtualBox-ohjelmistolla. Käyttöjärjestelmänä toimii Linux Xubuntu 10.04, koska se on helppokäyttöinen ja kevyt käyttöjärjestelmä. Virtuaaliympäristöä voisi jatkossa hyödyntää opetuskäytössä. Tarkoituksena olisi saada valitsemamme ohjelmat toimimaan Linuxissa. Valitut ohjelmat ovat NMAP ja OpenVAS. Tulemme dokumentoimaan myös kaikkien käytettävien ohjelmien asentamisohjeet.

Työn alkupuoli sisältää teoriaosuuden. Kerromme teoriaa virtuaalisoinnista, verkkotiedustelusta, haavoittuvuuksien etsimisestä ja käyttämistämme ohjelmista. Työn lopussa on kattavat asennusohjeet koko virtuaaliympäristölle ja käytettäville ohjelmille.

Tarkoitus olisi saada virtuaaliympäristöstä ohjelmineen mahdollisimman toimintavarma ja helppokäyttöinen, jotta opiskelijat voisivat hyötyä siitä. Kyseinen virtuaaliympäristö olisi tarkoitus rakentaa Laurea leppävaaran Neon-laboratorion tiloihin. Lisäksi ohjelmien asentamisohjeista ja käyttöohjeista tarkoitus tehdä niin yksityiskohtaiset, että asentaminen ja käyttäminen sujuisi helposti kaikilta.

Omat oppimistavoitteemme ovat oppia, miten rakentaa toimiva virtuaaliympäristö, jota voisi hyödyntää opetustarkoituksissa. Lisäksi saada lisää kokemusta virtuaalisoinnista ja Linuxista, sekä tietoturvallisuuden testaukseen tarkoitetuista ohjelmistoista ja niiden toiminnasta

Saimme asennettua valitsemamme ohjelmat ja dokumentoitua jokaisen käyttämämme ohjelman asentamisohjeet. Ensin asensimme Linuxin ja sen jälkeen muut ohjelmat: Virtualbox, NMAP ja OpenVAS. Asennuksen yhteydessä dokumentoimme asennusohjeet. Saimme toimivan järjestelmän rakennettua, mutta tällaisena sitä ei vielä pystyisi hyödyntämään kunnolla opetuskäytössä. Huomasimme myös, että virtualisointi ei olisi välttämättä oikea vaihtoehto, mutta sen avulla on mahdollista saada toimiva järjestelmä. Jotta useat käyttäjät voisivat samaan aikaan käyttää järjestelmää, tarvittaisiin sille oma palvelin. Palvelimella voisi ajaa palvelinohjelmat ja virtualisoinnin kautta asiakasohjelmat eri koneissa, niin järjestelmää voisi käyttää useat käyttäjät samaan aikaan, mikä olisi tarkoituksenmukaista opetuskäytössä.

2 Tutkimuksellinen kehittämistyö

2.1 Määritelmä

Tutkimuksellisessa kehittämisessä pyritään yleensä ratkaisemaan jotain käytännön ongelmia. Se voi saada alkunsa monista eri syistä, kuten organisaation kehittämistarpeista tai halusta saada aikaan muutoksia.
(Ojasalo, Moilanen & Ritalahti 2009, 11-55.)

Kehittämistyö kuvataan usein prosessiksi, koska se vie aikaa ja koostuu useista vaiheista. Prosessin kautta on helpompi tarkastella toimintaansa ja pysyä aikataulussa. Kaikenlainen kehittämistyö voidaan ajatella yksinkertaiseksi muutostyön prosessiksi, jossa on kolme vaihetta, jotka ovat suunnittelu, toteutus ja arviointi.
(Ojasalo, Moilanen & Ritalahti 2009, 11-55.)

2.2 Tutkimuksellisen kehittämistyön prosessimalli

Tyypillinen malli tutkimuksellisen kehittämistyön prosessista käsittää kuusi vaihetta, vaikka usein vaiheiden eroa voi olla vaikea nähdä ja usein joudutaan palaamaan taaksepäin ennen kuin prosessi voi edetä. Ensimmäinen vaihe on kehittämiskohteen tunnistaminen ja alustavien tavoitteiden määritteleminen. Alkuvaiheessa päätimme lähteä hahmottamaan uudistamisperustaista kehittämistyötä ja kohteen valittuamme aloimme miettimään tavoitteita. Päämäärämme oli tehdä virtuaaliympäristö Laurean Neon-laboratorioon, jossa voisi käyttää tietoturvaohjelmia.
(Ojasalo, Moilanen & Ritalahti 2009, 11-55.)

Toinen vaihe on kehittämiskohteeseen perehtyminen teoriassa ja käytännössä. Tässä vaiheessa on tärkeä tehdä kunnollinen taustatyö ja tutustua kehittämiskohteeseen perusteellisesti. Pintapuolisella tarkastuksella havaitaan usein vain oireet, mutta ei todellisia syitä. Tässä vaiheessa aloimme kerätä tietoa aiheesta tutustumalla alan niin kirjallisiin kuin sähköisiin julkaisuihin. Julkaisujen suuren määrän vuoksi jouduimme jo tässä vaiheessa hieman rajaamaan työtämme ja keskityimme enemmän tarkastelemaan virtualisointiin liittyviä julkaisuja.
(Ojasalo, Moilanen & Ritalahti 2009, 11-55.)

Kolmas vaihe on kehitystehtävän määritteleminen ja kehittämiskohteen rajaaminen eli määritellään tarkasti mihin pyritään. Päätimme rajata työmme siten, että siitä ei aiheutuisi kustannuksia Laurealle ja sen takia päätimme käyttää vain vapaan lähdekoodin ohjelmia. Virtuaaliympäristöön päätimme valita kaksi tietoturvaohjelmaa. Virtualisoinnin päätimme hoitaa VirtualBox-ohjelmalla, joka on vapaan lähdekoodin ohjelma. Tämän jälkeen päätimme, että

virtuaaliympäristömme on Linux -pohjainen ja käyttämämme ohjelmat ovat NMAP-porttiskanneri ja OpenVAS, joka on haavoittuvuuksien etsintä- ja arviointi työkalu. (Ojasalo, Moilanen & Ritalahti 2009, 11-55.)

Neljännessä vaiheessa laaditaan tietoperusta ja valitaan lähestymistapa. Tässä vaiheessa kokosimme keskeiset teoriat. Valitsimme lähestymistavaksi konstruktiivisen tutkimuksen, koska tavoitteenamme oli saada aikaan konkreettinen tuotos, joka tässä tapauksessa oli virtuaaliympäristö, jossa opiskelijat voisivat testailla tietoturvaohjelmia.
(Ojasalo, Moilanen & Ritalahti 2009, 11-55.)

Viidennessä vaiheessa toteutetaan ja julkaistaan kehittämishanke. Kirjoitimme muistiinpanoja koko prosessin ajan ja työ eteni versiosta toiseen. Koska kirjoittajia oli kaksi, jouduimme aika usein kokoomaan tuotoksemme yhteen ja tarkastelemaan, miten prosessi etenee. Keskeinen osa työtämme oli myös ohjelmien asennukset ja asennusohjeiden kirjaukset.
(Ojasalo, Moilanen & Ritalahti 2009, 11-55.)

Kuudennessa ja samalla viimeisessä vaiheessa arvioidaan kehittämisprosessi ja sen tulokset. Pääsimme tavoitteeseemme, joka oli saada virtuaaliympäristö ja valitsemamme ohjelmat toimimaan Laurean Neon-laboratoriossa. Huomasimme kuitenkin, että virtualisoinnin kautta tämä ei välttämättä olisi paras vaihtoehto.
(Ojasalo, Moilanen & Ritalahti 2009, 11-55.)

3 Virtualisointi

3.1 Historia

Virtualisointi on 2000-luvun trendi, mutta se keksittiin jo 1960-luvulla. Idean keksijänä pidetään englantilaista Christopher Stracheyta. Atlas-projekti 1960-luvun alussa oli ensimmäinen, jossa käytettiin hyödyksi Straycheyn ideaa. IBM:n M44/44x-projekti 1960-luvun puolivälissä oli toinen, jota pidetään merkittävänä virtuaalisoinnin kehittymisen kannalta. Siihen aikaan virtuaalisoinnista käytettiin termiä Time sharing.

1990-luvulle tultaessa eri yhtiöillä on ollut erilaisia virtuaalisointiratkaisuja vaihtelevalla menestyksellä, mutta varsinainen virtuaalisoinnin uusi aalto alkoi 1990-luvun lopussa. Silloin VMware toi virtuaalisoinnin x86-palvelimiin. Tämän jälkeen monet yhtiöt ovat tuoneet omat virtualisointiratkaisunsa markkinoille. VMwaren lisäksi isoimpia markkinoilla kamppailijoita ovat Microsoft ja Citrix. (Amit Singh)

3.2 Virtualisoinnin määritelmä ja hyödyt

Virtualisointia on monenlaista, joista yleisimpiä on palvelinvirtualisointi ja työpöytävirtualisointi. "Palvelimissa virtualisointi tarkoittaa yksinkertaisesti kuvattuna sitä, että yhdessä fyysisessä laitteessa ajetaan yhden käyttöjärjestelmän sijasta useita virtuaalipalvelimia. Niistä kukin pyörittää itsenäisesti omaa käyttöjärjestelmäänsä." (Mäntylä, 2008). Työpöytävirtualisoinnissa käyttäjän työasema on yhteydessä palvelimella sijaitsevaan virtuaalikoneeseen ja sovellukset ajetaan sitä kautta käyttäjälle. (Mäntylä 2008.)

Virtualisoinnin avulla tehostetaan toimintaa ja saavutetaan paljon hyötyä niin taloudellisesti kuin ekologisesti. Sen avulla saadaan parannettua laitteiden käyttöastetta ja sitä kautta saadaan kustannussäästöjä. Työasemille saadaan asennettua sovellukset keskitetysti, eikä tarvitse erikseen käydä läpi jokaista työasemaa. Siinä yritykset säästävät paljon aikaa ja rahaa.

Palvelinvirtualisoinnin avulla säästetään tilaa, kun palvelimia tarvitaan vähemmän ja näin myös sähkönkulutusta saadaan pienennettyä, mikä tuo taas omalta osaltaan kustannussäästöjä. (Atea 2010.)

3.3 Virtualisointitekniikat

Emulointi

Emulointi tarkoittaa sitä, että tietokoneella ajetaan ohjelmistoja, jotka jäljittelevät jonkin toisen tietokoneen toimintaa siten, että koneella voidaan ajaa tälle toiselle, usein vanhentuneelle tietokoneelle kirjoitettuja ohjelmistoja. Emulaatio voidaan toteuttaa myös laitteistopohjaisesti, jolloin uudempi komponentti pystyy ymmärtämään vanhemmalle komponentille kirjoitettua koodia. (What is emulation?)

Paravirtualisointi

Emuloivaa laitteistovirtuaalisointia parempi virtuaalisointitekniikka, jossa virtualisoivan käyttöjärjestelmän emuloinnin sijaan muokataan virtualisoitavan käyttöjärjestelmän rakennetta toimimaan virtuaalikonemoottorin käskykannalla. Täysvirtuaalisoinnista tämä eroaa siten, että järjestelmään tarvitsee asentaa erillinen isäntäkäyttöjärjestelmä, jonka avulla tarjotaan rajapinta luotaville virtuaalikoneille. Isäntäkäyttöjärjestelmän virtuaalisointirajapinta tarjoaa virtuaalipalvelimille niiden tarvitsemat ajurit käytettäviä laitteita varten. Täysivirtuaalisoinnissa virtuaalipalvelimet ovat suorassa yhteydessä palvelimen fyysiseen laitteistoon, paravirtualisoinnissa nämä käskyt kulkevat isäntäkäyttöjärjestelmän virtuaalisointirajapinnan kautta. (VMware, Understanding Full Virtualization, Paravirtualization, and Hardware Assist)

Täysvirtualisointi

Toisin kuin paravirtualisointia käyttävissä virtuaaliohjelmistoissa, täysvirtualisointiohjelmisto ei tarvitse esiasennettua käyttöjärjestelmää toimiakseen. Kun käytetään täysvirtualisointi ratkaisua, tarjoaa sitä tukeva ohjelmisto suoran fyysisen koneen laitteistoon toisin kuin paravirtualisoidussa ympäristössä.

Yksi täysvirtuaalisoinnin eduista on sen nopeus verrattuna paravirtualisointiin. Suurin syy sen nopeuteen on se, että virtuaalipalvelimet voivat keskustella suoraan fyysisen palvelimen laitteiston kanssa, tekemättä erillistä mutkaa virtuaalisointiohjelmiston kautta. Jokaista käyttöjärjestelmää, jota voidaan ajaa fyysisessä laitteistossa, voidaan ajaa myös täysvirtuaalisointia käyttävissä virtuaalikoneissa.

Täysvirtuaalisoinnin hyviä puolia ovat mm. toisistaan eristetyt palvelimet sekä se, että asennettavat käyttöjärjestelmät voidaan asentaa muokkaamattomina. Täysvirtuaalisointi mahdollistaa myös lähes yhtä nopean toimivuuden kuin se, että käytössä olisi fyysinen palvelin. Täysvirtuaalisoinnin huonona puolena taas on se, että kyseisellä arkkitehtuurilla on tietyt laitteisto ja ohjelmisto vaatimukset, mutta uusien versioiden myötä myös laitetuki paranee jatkuvasti. Huonona puolena on myös se, että käskyjen välittäminen sekä emulointi laskevat järjestelmän suorituskykyä. (VMware, Understanding Full Virtualization, Paravirtualization, and Hardware Assist)

3.4 VirtualBox

VirtualBox on Sun Microsystemsin kehittämä ohjelma mm. käyttöjärjestelmien virtualisointiin. Se tukee yleisimpiä käyttöjärjestelmiä kuten Windows, Linux, Mac OS X ja Solaris. Siitä on kaksi eri versiota.

Täysversio on ilmainen kotikäyttäjille ja opetuskäyttöön mutta maksullinen yrityskäyttöön. Se on lisensoitu Personal Use and Evaluation License (PUEL) -lisenssillä. Avoimen lähdekoodin versio on toiminnallisesti samanlainen kuin täysversio, mutta se ei tue kaikkia ominaisuuksia esimerkiksi USB-portteja. VirtualBox on julkaistu GNU General Public License (GPL) -lisenssillä. (VirtualBox User Manual, 9)

4 Verkkotiedustelu

Port scanning, eli verkkotiedustelu. Verkkotiedustelun avulla voidaan selvittää kohteen aukinaiset portit, minkä avulla pyritään selvittämään mahdollisia haavoittuvuuksia sekä aukkoja esimerkiksi palvelimessa, johon verkkotiedustelu tehtiin.

Verkkotiedustelua yleensä käytetään, kun testataan esimerkiksi yritysverkon tai palvelimen turvallisuutta. Verkkotiedustelu ei kuitenkaan ole pelkästään ylläpitäjien työkalu, vaan verkosta löytyy myös ilmaisia ohjelmia eri käyttöjärjestelmille, joten kotikäyttäjät voivat testata myös oman verkkonsa turvallisuutta.

Verkkotiedustelua voidaan käyttää myös tietomurtoihin käyttäen hyväksi tuloksia, joita portti-tiedustelu raportoi käyttäen hyväksi erilaisia haavoittuvuuksien etsimiseen sekä hyväksikäyttämiseen tarkoitettuja ohjelmistoja.

Yksi suosituimmista verkkotiedustelun työkaluista on Nmap, jonka saa ilmaiseksi useille eri käyttöjärjestelmille. Verkosta löytyy myös kotikäyttäjille www –selaimen kautta ajettavia verkkotiedustelutestejä, joilla voidaan selvittää kotikoneen aukinaisia portteja ja turvallisuutta. (Bradley Tony)

4.1 Nmap-verkkotiedustelutyökalu

Nmap on ilmaiseen lähdekoodiin perustuva verkkotiedusteluun (port scanning/mapping) tarkoitettu työkalu. Nmap toimii yleisimmillä käyttöjärjestelmillä esimerkiksi Windows, Linux, Mac OS X ja Unix. Nmapia ajetaan normaalisti komentokehotteen kautta, joka mahdollistaa myös sen etäkäytön.

Nmap osaa selvittää esimerkiksi valitun tietoverkon turvallisuusasetuksista riippuen erilaiset isäntäosoitteet (hostname), käyttöjärjestelmän, koneessa pyörivät palvelut ja niiden ohjelmistoversion, jonka jälkeen Nmap luo ns. ”kartan” palveluista ja koneista. (Nmap, Nmap Reference Guide)

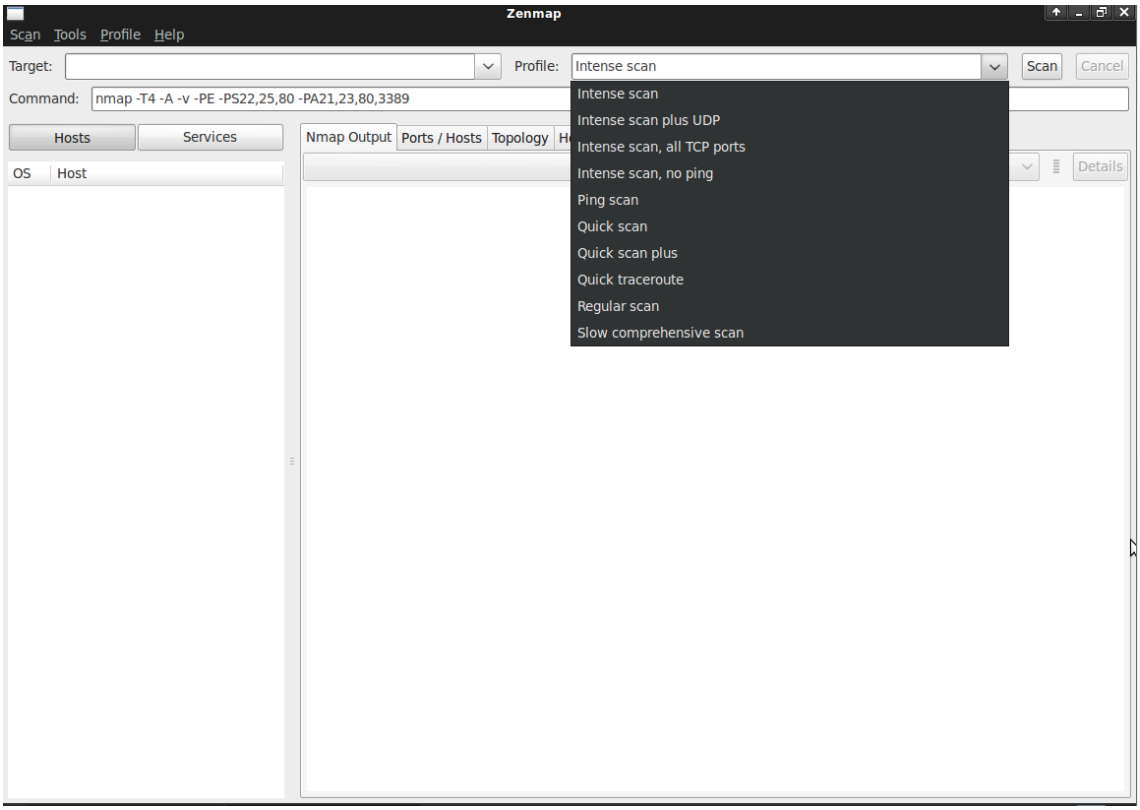
Nmap sisältää varsin kattavan joukon erilaisia tiedustelumetodeja ja vaihtoehtoja, listan tästä saa kirjoittamalla komentokehotteessa ”nmap –help”. Kokonainen Help –tiedosto löytyy liitteistä, liite 1 Nmap-aputiedosto.

4.1.1 Zenmap

Zenmap on virallinen graafinen käyttöliittymä Nmap-sovellukseen. Se on erityisesti tarkoitettu aloittelijoille helpomman käytettävyyden takia, mutta se sisältää kaikki samat ominaisuudet kuin komentokehotteesta ajettava Nmap, minkä lisäksi Zenmap sisältää myös kehittyneitä valmiita hakuvaihtoehtoja kokeneille käyttäjille. (Nmap, Zenmap GUI Users' Guide)

Zenmap käynnistetään komentokehotteesta komennolla ”sudo zenmap”.

Kuvassa 1 on Zenmapin perusnäkymä, missä on listattuna valmiit laajemmat tiedustelumetodit.



Kuva 1: Zenmap

4.1.2 Esimerkki 1: Nmap tiedustelu komentokehotteesta

Alla esimerkki aivan perustiedustelusta, joka ajettiin virtuaalipalvelimelta komentokehotteesta alla olevalla komennolla.

nmap -A -T4 www.laurea.fi

Parametri –A mahdollistaa käyttöjärjestelmän urkkimisen, sen version, skripti –tiedustelun sekä jäljittämisen kohteeseen (trace route).

Parametri –T4 tekee tiedustelusta aggressiivisemman, näin nopeuttaen tiedustelun lopputuloksien saantia.

Kohteena toimii Laurean oma www –palvelin. Kun Nmap on käynnistynyt, tulostaa ohjelma tulokset ruutuun tekstimuodossa, ulostuonti kokonaisuudessaan löytyy myös liitteistä, liite 2 Nmap-tiedustelu 1.

Starting Nmap 5.00 (http://nmap.org) at 2010-09-21 10:13 EEST
Interesting ports on 193.166.246.147:
Not shown: 990 filtered ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	http?	
135/tcp	open	msrpc?	
445/tcp	open	microsoft-ds?	
1025/tcp	open	NFS-or-IIS?	
1044/tcp	open	unknown	
1067/tcp	open	instl_boots?	
1311/tcp	open	rxmon?	
3389/tcp	open	ms-term-serv?	
5002/tcp	open	rfe?	
20031/tcp	open	unknown	

Ensimmäisenä Nmap listaa aukinaiset portit ja sen käyttääkö se tcp- vai udp-protokollaa. Service valikon alla Nmap yrittää päätellä, minkälainen palvelu kyseisessä portissa pyörii. Alla osuus tiedustelun ulostuonnista, mikä löytyy myös liitteistä, liite 2 Nmap-tiedustelu 1.

Host script results:
| smb-os-discovery: Windows Server 2003 R2 3790 Service Pack 2
| LAN Manager: Windows Server 2003 R2 5.2
| Name: WORKGROUP\PIHTA
|_ System time: 2010-09-21 10:14:43 UTC+3
|_ nbstat: ERROR: Name query failed: TIMEOUT

Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 152.99 seconds

Nmap osaa myös näyttää, että Laurean www-palvelimen käyttöjärjestelmänä on Windows Server 2003.

Lisää tietoja saa ajamalla monimutkaisempia tiedusteluita käyttäen apuna manuaalia tai kokeilemalla valmiita tiedusteluvaihtoehtoja Zenmapin kautta.

4.1.3 Esimerkki 2: Zenmap-tiedustelu

Ajoimme Zenmapin kautta virtuaalipalvelimen isäntäkoneelle ”Intense scan” -tiedustelun, jonka voisi ajaa myös komentokehotteesta alla olevalla komennolla.

nmap –T4 –A –v –PE –PS22,25,80 –PA21,23,80,3389 x.x.x.x

Parametri –A mahdollistaa käyttöjärjestelmän urkkimisen, sen version, skripti –tiedustelun sekä jäljittämisen kohteeseen (trace route).

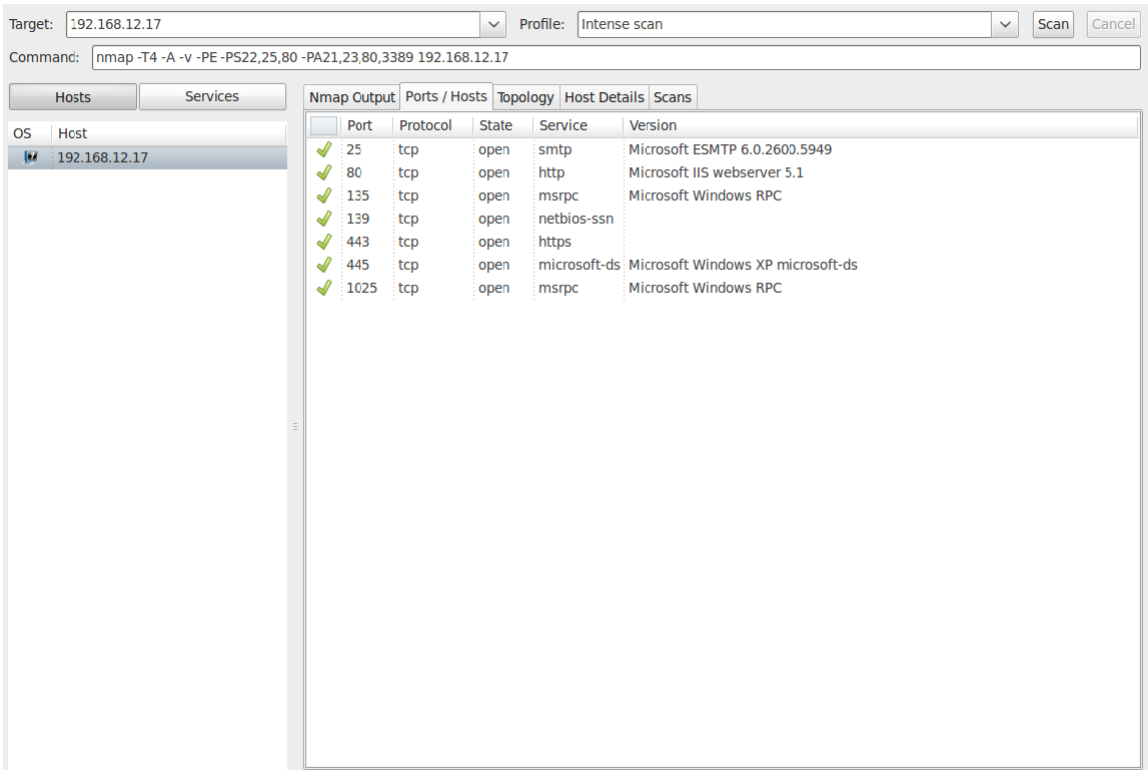
Parametri –PA lähettää TCP ACK pingin valitsemiin portteihin, 21 (FTP), 23 (Telnet) 80 (WWW) ja 3389 (RDP, Remote Desktop Protocol). TCP ACK pingin tarkoituksena on tunnustella valittuja portteja TCP ACK pingin kautta, mitä ei välttämättä ole aina estetty palomuureissa.

Parametri –PE on ”ICMP Echo”, mikä on tehokas tapa tiedustella sisäisessä verkossa, kunhan palomuuri ei estä paketteja.

Parametri -PS lähettää TCP/SYN-paketit valitsemiin portteihin: 22 (SSH), 25 (SMTP) ja 80 (WWW). Käytännössä tämä tarkoittaa sitä, että tyhjä TCP-paketti lähetetään valitsemiin portteihin, mikä sisältää SYN viitteen. Viitteen sisältävä paketti kokeilee luoda toimivan yhteyden kyseiseen porttiin, näin hakien lisätietoja.

Parametri –T4 tekee tiedustelusta aggressiivisemman, näin nopeuttaen tiedustelun lopputuloksien saantia.

Parametri –v (verbosity) lisää tiedustelun ulostuonnin astetta, mikä mahdollistaa laajempien lisätietojen kertomisen tiedustelun lokitiedostossa.



Kuva 2: Intense scan -tiedustelu

Tiedustelu löysi isäntäkoneeltamme mm. aukinaisen SMTP -palvelimen. Alla olevia tiedustelun ulostuonnin tietoja voisimme käyttää hyväksi haavoittuvuuksien etsimiseen esim. OpenVAS -skannerilla. Kokonainen tiedustelun ulostuonti löytyy liitteistä, liite 3 Nmap-tiedustelu 2.

25/tcp open smtp Microsoft ESMTP 6.0.2600.5949
| smtp-commands: EHLO Neon-labra2 Hello [192.168.12.17], SIZE 2097152, PIPELINING, DSN, ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY
|_ HELP This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT VRFY

Isäntäkoneelta löytyi myös Microsoft IIS versio 5.1 -web palvelin.

80/tcp open http Microsoft IIS webserver 5.1
| html-title: You are not authorized to view this page
|_ Requested resource was http://192.168.12.17/localstart.asp

Ajetun tiedustelun kokonainen lokitiedosto löytyy liitteistä, liite 2 Nmap-tiedustelu 2.

4.2 Haavoittuvuuksien etsiminen

Vulnerability scanning, eli suomeksi haavoittuvuuksien etsiminen käytännössä tarkoittaa sitä, että esimerkiksi. verkkotiedustelun kautta saatuja tietoja vertaillaan haavoittuvuuksien etsimiseen tarkoitetun ohjelmiston tietokannasta löytyviin tietoihin. Tietokannat yleensä päivittyvät lähes joka päivä, jos kyseessä on maksullinen ohjelmisto.

Yksityiskäyttäjille tarkoitettuja ilmaisia haavoittuvuuksien etsintäohjelmia ovat mm. Nessus sekä Openvas, yrityskäyttöön löytyy mm. eEye Retina sekä Nessuksen maksullinen versio.

Haavoittuvuuksien etsimisohjelmia käyttävät yleensä verkon ylläpitäjät tai heidän palkkaamat tietoturva-asiantuntijat, mutta koska ohjelmia saa ilmaiseksi, voi kotikäyttäjät käyttää niitä myös ilkivallan tekoon.

Osa ohjelmistoista sisältää vain tietokannan, mikä sisältää tiedot haavoittuvuuksista ja miten kyseinen reikä on paikattavissa, mutta jotkin lisäosat mahdollistavat koodin ajamisen, mikä kokeilee tunkeutua palvelimeen tai sovellukseen, josta haavoittuvuus löytyi, koittaen saada pääkäyttäjän oikeudet.

Verkkotiedusteluun sekä haavoittuvuuksien etsimiseen tarkoitetut ohjelmistot ovat olennainen asia yritysten sekä muiden isojen verkkojen tietoturvallisuutta. (Tony Bradley, Introduction to Vulnerability Scanning)

4.2.1 OpenVAS

OpenVAS (The Open Vulnerability Assessment System) on avoimeen lähdekoodiin perustuva haavoittuvuuksien etsimiseen (vulnerability scanning) tarkoitettu ohjelmisto. OpenVAS on johdannainen Nessus –ohjelmistosta. OpenVASin uusimmat versiot pyörivät vain Linuxilla, toisinkuin Nessus, josta löytyy myös Windows versiot. (OpenVAS Compedium, 9)

OpenVAS käyttää hyväkseen päivittäin päivittyvää listaa mahdollisista haavoittuvuuksista (NVT, Network Vulnerability Tests plugins). Tällä hetkellä (August 2010) OpenVAS osaa tunnistaa yli 18000 haavoittuvuutta. (OpenVAS, About OpenVAS NVT Feed)

OpenVAS koostuu useasta eri komponentista ja työkalusta, jotka myös perustuvat vapaaseen lähdekoodiin.

Pääkomponentit OpenVAS –ohjelmistossa ovat:

openvas-libraries, eli kirjastotiedot
openvas-scanner, eli palvelinohjelmisto
openvas-client, eli asiakasohjelmisto

Tämän lisäksi OpenVAS käyttää useita muita eri työkaluja, esim. Nmap. Muita OpenVASin pluginien käyttämiä ohjelmia, joita asensimme on w3af (Web Application Attack and Audit Framework) -ohjelmiston, mikä on tarkoitettu erilaisten verkkosovellusten haavoittuvuuksien etsimiseen sekä hyväksikäyttämiseen. (w3af, FAQ)

Toinen asentamamme plugin -ohjelma on Nikto, mikä on tarkoitettu www –palvelimien haavoittuvuuksien etsimiseen. Nikto sisältää yli 6400 haavoittuvuutta CGI –tiedostoista sekä se osaa etsiä tietoja väärin asennetuista www –palvelimista. (nikto2, Description)

4.2.2 OpenVAS-käyttöohjeet

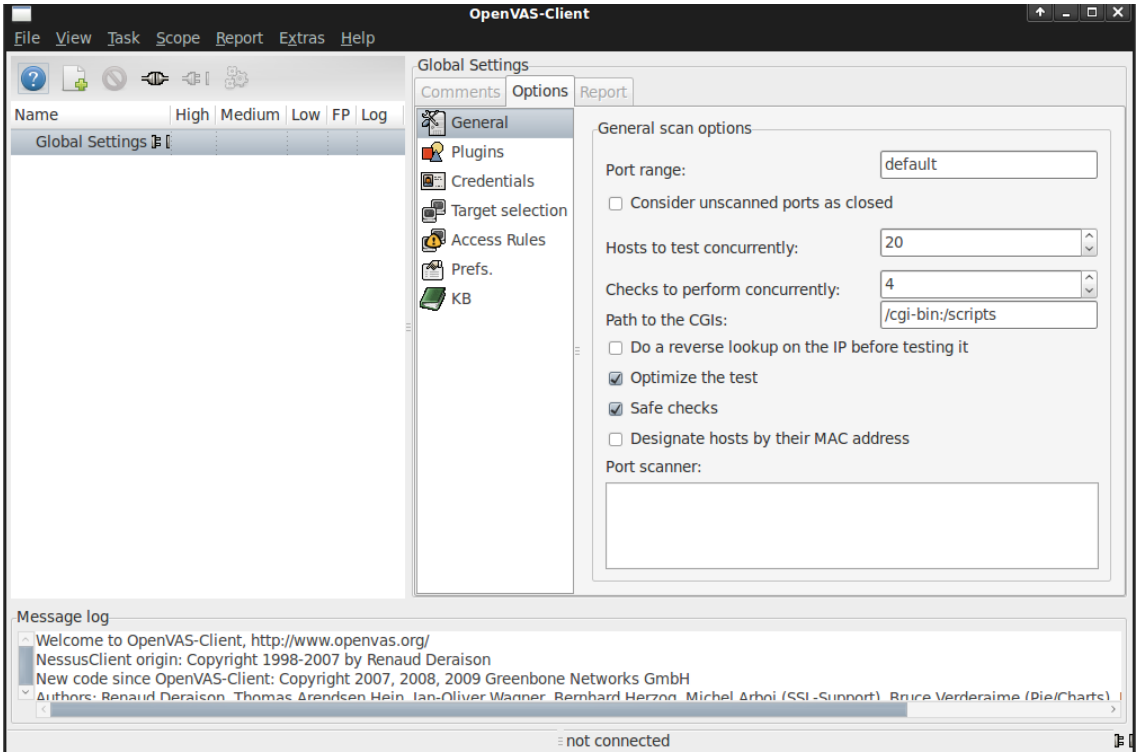
OpenVAS käynnistetään komentokehotteesta, ensimmäiseksi on käynnistettävä OpenVAS –palvelin, tämä tapahtuu komenolla

sudo openvassd

Tämän jälkeen OpenVAS lataa tarvittavat pluginit (liitännäistiedostot), mikä vie hetken aikaa.

Kun pluginit ovat lataantunut, käynnistetään OpenVAS –asiakasohjelmisto komentokehotteesta komennolla

sudo OpenVAS-Client



Kuva 3: OpenVAS perusnäkymä

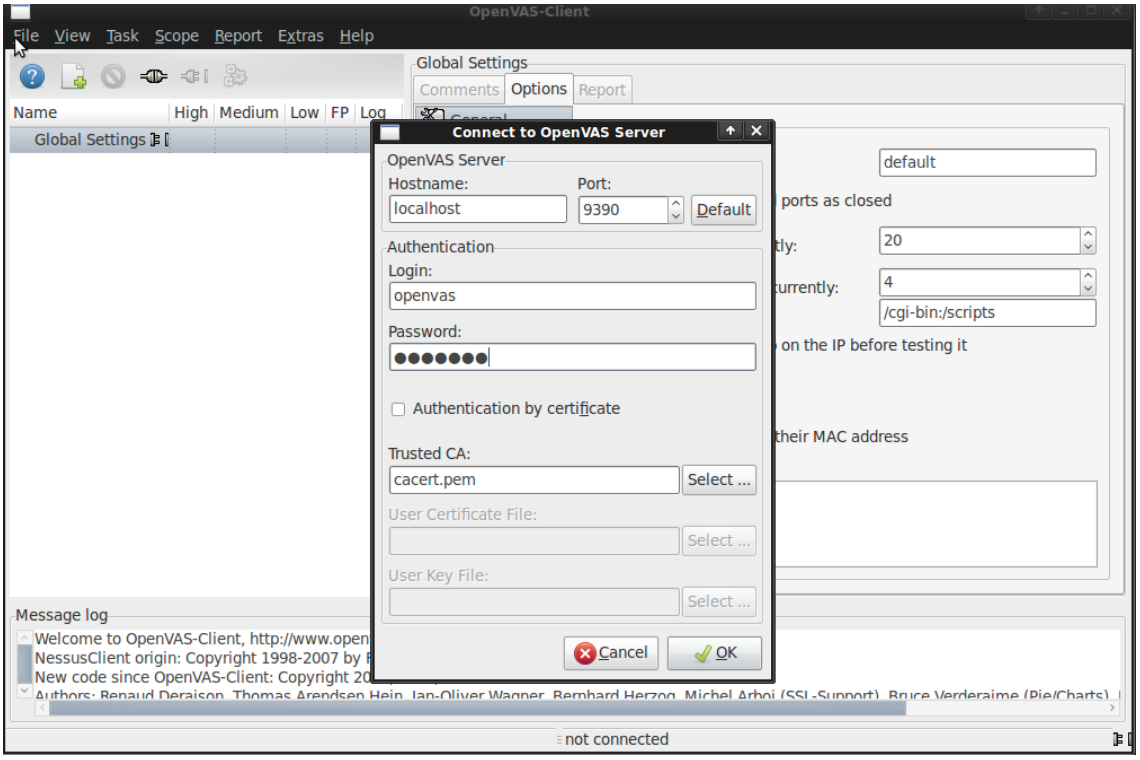
Seuraavaksi valitaan Options valikon alta ”Optimize the test” ja klikataan se päälle, tämä optio nopeuttaa tiedustelua.

Myös ”Safe checks” laitetaan päälle, sillä muuten OpenVAS saattaa ajaa sellaisia tiedusteluita, mitkä voivat kaataa tietokoneen mitä skannataan. Haittapuolena tässä on se, että tiedustelu ei välttämättä löydä kaikkea tarvittavaa informaatiota, joten Safe checks –option käyttäminen on tapauskohtaista.

4.2.3 Tiedustelu

Ensiksi on otettava yhteys ”Global Settings” palvelimeen, tämä tapahtuu valitsemalla ”File” --valikosta Connect, minkä jälkeen OpenVAS kysyy käyttäjätunnusta ja salasanaa, mitkä määrittelimme aikaisemmin molempiin pelkkä ”openvas”.

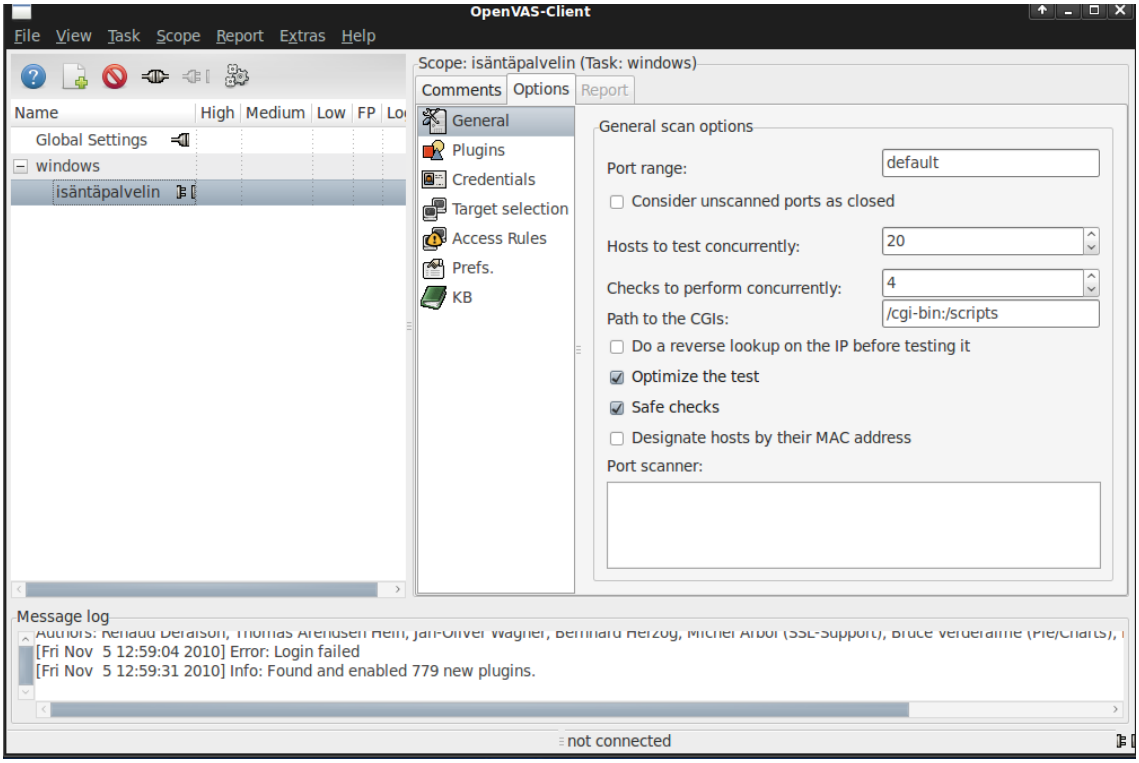
Yhdistäminen vie hetken aikaa, riippuen koneen nopeudesta ja pluginien määrästä.



Kuva 4: Luodaan yhteys OpenVAS palvelimeen

1. Valitaan ”Task” -valikosta New ja nimetään tulevan tiedustelun toimi esim. ”Windows”.

2. Valitaan ”Scope” -valikosta New ja nimetään tulevan tiedustelun nimeksi esim. ”Isäntäpalvelin”.



Kuva 5: OpenVAS määritelty tiedustelu

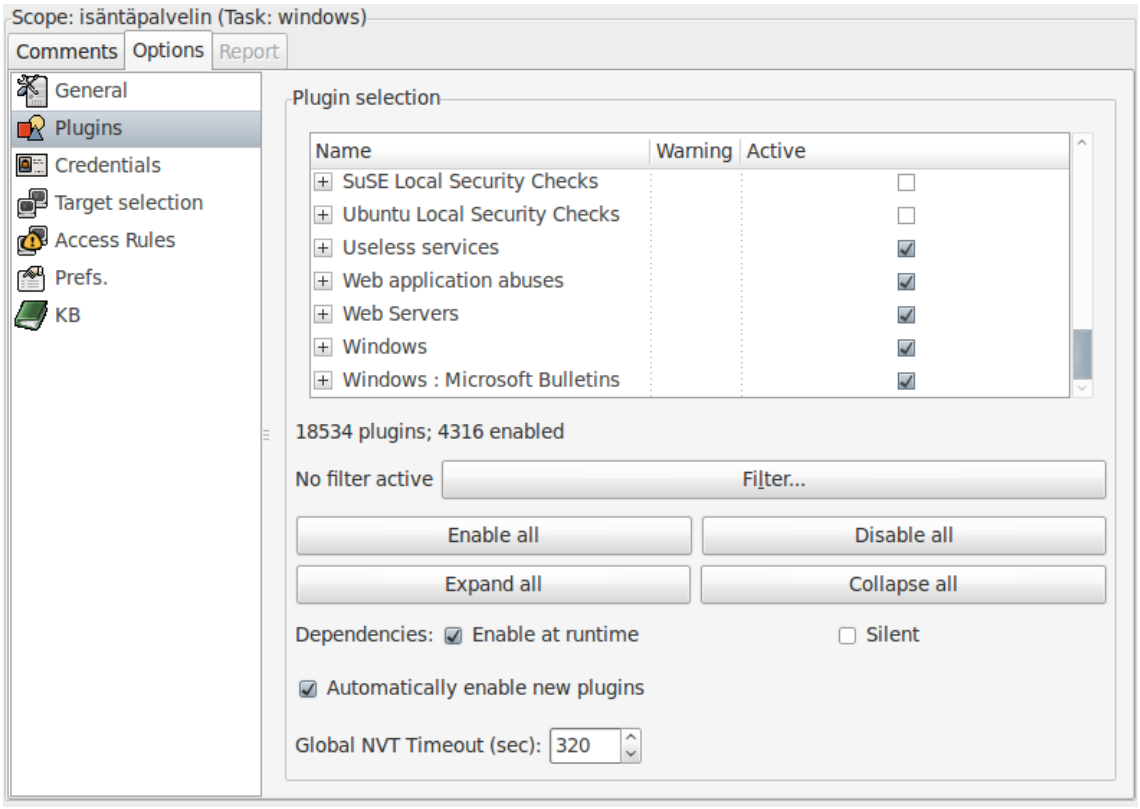
3. Valitaan valikosta isäntäpalvelin, minkä jälkeen valitaan ”File” -valikosta tuttuun tapaan Connect. Kirjaudutaan sisään ja odotetaan että pluginit lataantuvat.

4. Koska tuleva tiedustelu tulee kohdistumaan Windows -palvelimeen, on syytä määritellä käytettäviä plugineja. Siirrytään option -valikosta Plugins kohtaan, mistä poistamme turhia plugineja, täten nopeuttaen tulevaa tiedustelua.

Pluginit, joita poistimme olivat:

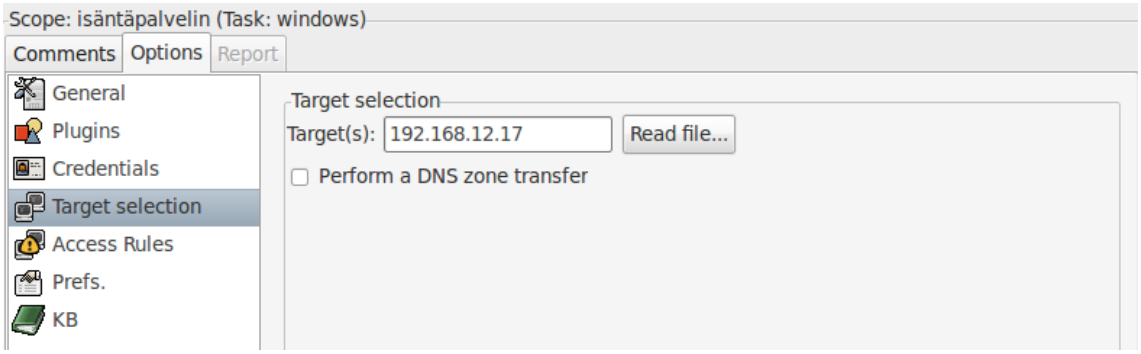
Kaikki Linux/Unix Local Security Check -pluginit (Tiedustelun kohteena Windows -palvelin)
Brute Force Attacks (Saattaa kaataa kohdepalvelimen)
CISCO (Ainoastaan hyödyllinen CISCO -laitteita kohtaan)
Databases (Palvelimella ei ole tietokantapalveluita)
IT-Grundschutz -pluginit (Kehitysvaiheessa ja kieli vain saksaksi)

Luomalla ”Scope” valikosta uusia tiedusteluita, voidaan määritellä tarkemmin mitä plugineja tullaan käyttämään. Esimerkiksi web -palvelimiin valitaan vain web -palvelin/linux/windows pluginit tai mailipalveluihin vain mail server -pluginit.



Kuva 6: Plugin valikko

5. Määritellään kohteen ip -osoite ”Options” valikon alta ”Target selection” kohdasta, tällä kertaa kohteenamme on kone, mihin olemme asentaneet käytettävän virtuaalipalvelimen.

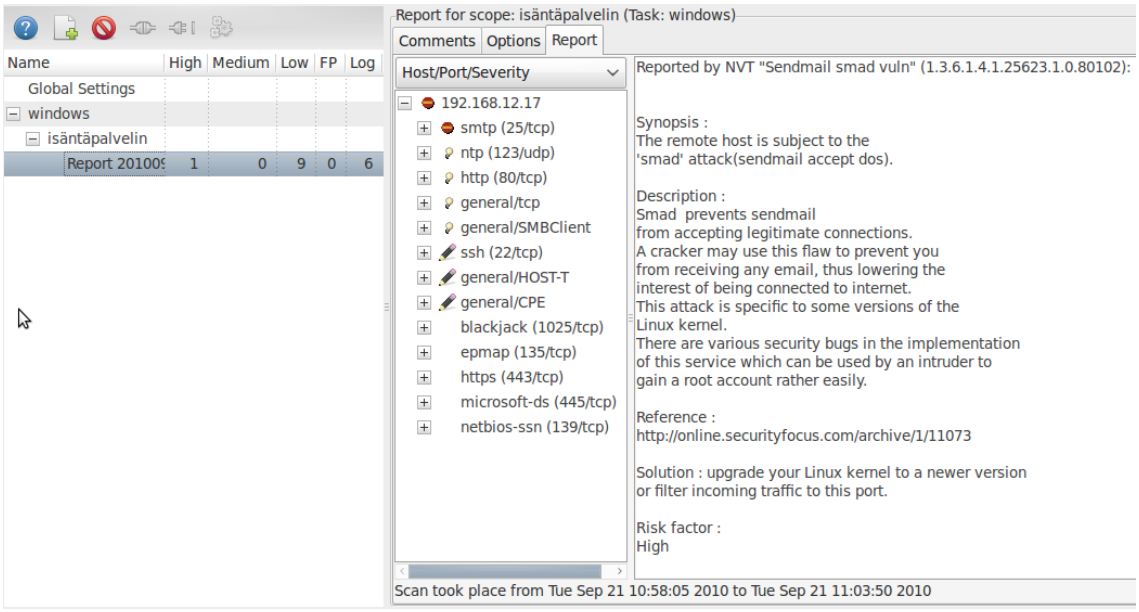


Kuva 7: Target selection

6. Käynnistetään tiedustelu menemällä ”Scope” valikkoon, mistä valitsemme ”Execute”. Tiedustelu kestää riippuen pluginien määrästä ja koneen tehoista.

4.2.4 Tiedustelun tulokset

Kun tiedustelu on käyty läpi, ilmestyy valikkoon tutkitut portit ja mahdolliset tietoturva-aukot, mitä OpenVAS löysi.



Kuva 8: Tiedustelun tulokset

Kuvassa vasemmalla näemme, että OpenVAS löysi 1 korkean luokan haavoittuvuuden, sekä 6 matalan luokan haavoittuvuutta.

Security Note

Reported by NVT "Services" (1.3.6.1.4.1.25623.1.0.10330):

An SMTP server is running on this port
Here is its banner :
220 Neon-labra2 Microsoft ESMTP MAIL Service, Version: 6.0.2600.5949 ready at Tue, 21 Sep 2010 10:58:13 +0300

Security Hole
Reported by NVT "Sendmail smad vuln" (1.3.6.1.4.1.25623.1.0.80102):

Synopsis :
The remote host is subject to the 'smad' attack(sendmail accept dos).

Description :

Smad prevents sendmail from accepting legitimate connections. A cracker may use this flaw to prevent you from receiving any email, thus lowering the interest of being connected to internet.

This attack is specific to some versions of the Linux kernel.

There are various security bugs in the implementation of this service which can be used by an intruder to gain a root account rather easily.

Reference :
http://online.securityfocus.com/archive/1/11073

Solution : upgrade your Linux kernel to a newer version or filter incoming traffic to this port.

Risk factor :
High

OpenVASin mukaan mail –palvelimessa (SMTP, portti 25) on haavoittuvuus, mutta koska isäntäpalvelin on Windows ja haavoittuvuus koskee Linuxia, niin tämä ei koske meitä.

Kuvassa oikealla näemme portit, jotka OpenVAS tiedusteli sekä selityksen mahdollisista haavoittuvuuksista.

Täysi lokitiedosto tiedustelusta löytyy liitteistä, liite 4 Openvas-testitulokset.

5 Asennusohjeet

Toimiva virtuaalipalvelin koostuu neljästä eri ohjelmistosta. Virtualisointia varten käytämme ohjelmaa nimeltä VirtualBox.

Käyttöjärjestelmänä toimii Xubuntu Linux, johon asennetaan Nmap verkkotiedustelua (port scanning) varten ja OpenVas ohjelmisto haavoittuvuuksien etsimiseen (vulnerability scanning). Tarvitset seuraavat ohjelmat:

VirtualBox
VirtualBox 3.x versio, ladattavissa osoitteesta http://www.virtualbox.org/wiki/Downloads, otetaan Windows hosts x86/amd64 versio.

Jos asennetaan omalle palvelimelle, ei VirtualBoxia tarvitse asentaa, vaan siirrytään suoraan kohtaan Xubuntun asentaminen.

Xubuntu
Xubuntu - xubuntu-10.04-desktop-i386.iso, ladattavissa osoitteesta http://se.archive.ubuntu.com/mirror/cdimage.ubuntu.com/xubuntu/releases/10.04/release/xubuntu-10.04-desktop-i386.iso tai http://www.xubuntu.org/get

Nmap
Nmap ja Nmapin graafinen käyttöliittymä ladataan Xubuntun omalla pakettimanagerilla, ohjeet löytyvät Nmapin asennuksen alta.

OpenVas
Asennuksessa käytämme tällä hetkellä uusimpia 3.1 ja 3.0 versioita, ne ovat ladattavissa http://www.openvas.org sivustolta.

Tarvitsemamme komponentit ovat:
openvas-libraries 3.x
openvas-scanner 3.x
openvas-client 3.x

Näitä tiedostoja ei tarvitse ladata etukäteen, vaan ne haetaan vasta Xubuntun asentamisen jälkeen.

5.1 Asennuksessa käytettävät komennot

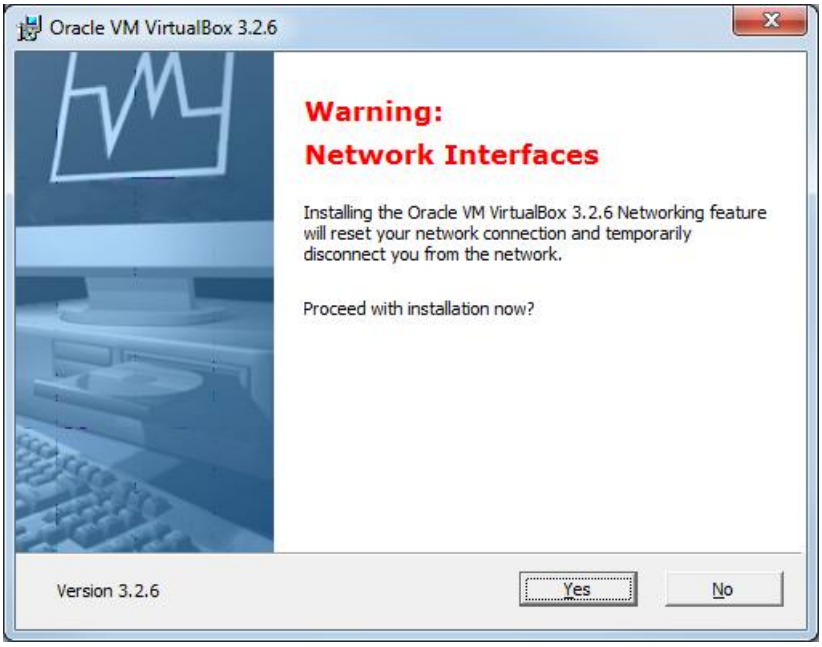
sudo	Ohjelma komentojen suorittamiseen, tässä tapauksessa pääkäyttäjän oikeuksilla
sudo apt-get update	Päivitetään pakettienhallinnan pakettilistan tiedot
sudo apt-get upgrade	Päivitetään järjestelmään asennetut paketit
sudo apt-get install	Asennetaan uusi paketti
sudo reboot	Käynnistetään kone uudelleen
sudo updatedb	Päivitetään palvelimen paikallinen tietokanta
sudo ldconfig	Päivitetään linkit ja välimuisti palvelimen uusimpiin versioihin
mkdir	Luodaan uusi hakemisto
cd	Vaihdetaan hakemistoa
wget	Ohjelma tiedostojen lataamiseen komentokehotetta käyttäen
tar	Ohjelma pakettien tekemiseen ja purkamiseen
sudo ./configure	Tarkistaa ennen paketin kääntämistä löytyykö koneesta tarvittavat tiedot kirjastot ja ohjelmistot
sudo make	Kääntää paketin toimivaksi
sudo make install	Asentaa paketin käyttöjärjestelmään

5.2 Virtualisointi

5.2.1 VirtualBox

Tämän vaiheen voi jättää välistä, jos sovellukset asennetaan omalle palvelimelle virtuaalisoinnin sijasta.

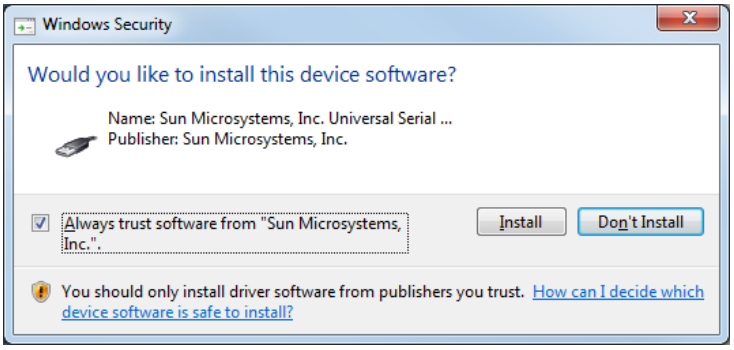
1. Käynnistetään VirtualBox-3.x-Win.exe. Edetään painamalla Next, kunnes tullaan kuvan 9 kohtaan:



Kuva 9: Virtualboxin asennus varoittaa katkeavasta internet yhteydestä

2. Hyväksytään tämä, valitaan Yes ja seuraavaksi Install.

Windows saattaa kysyä lisälupia erilaisten ajureitten asentamiseen, hyväksytään kaikki valitsemalle ”Always trust software from ”Sun Microsystems, Inc.”.” ja valitaan Install.

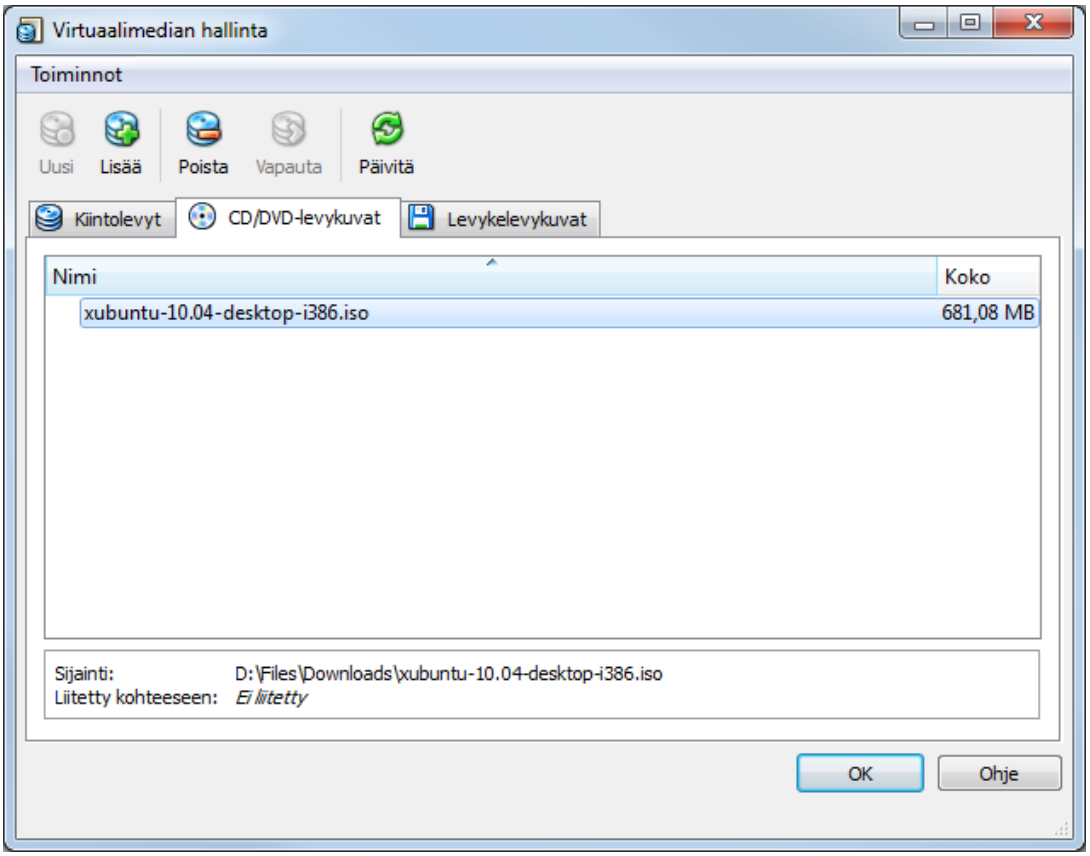


Kuva 10: Tarvittavien ajureiden asennus

3. Asennuksen jälkeen valitaan Finish ja käynnistetään VirtualBox virtuaaliympäristön luomista varten.

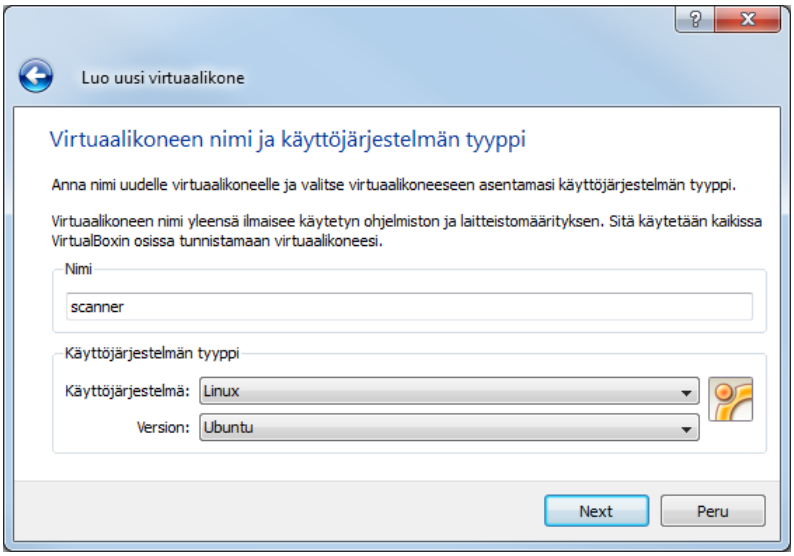
5.2.2 Virtuaaliympäristön luominen

1. Lisätään Xubuntun .iso -tiedosto virtuaalimedioiden hallintaan painamalla Ctrl+D , siirrytään CD/DVD-levykuvat välivalikkoon ja painetaan Lisää kuvaketta, etsitään tiedosto ja valitaan OK.



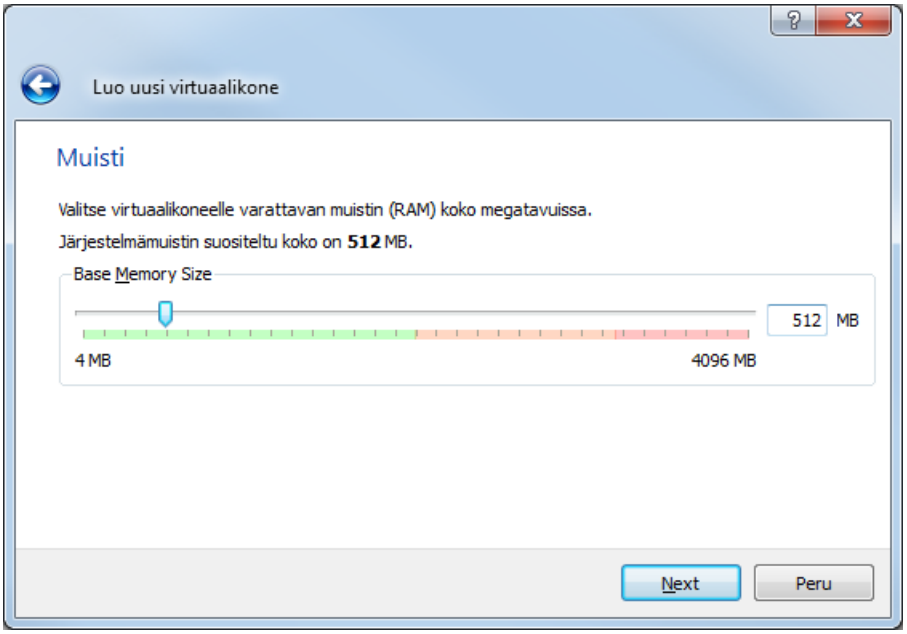
Kuva 11: Virtuaalimedian hallinta

2. Luodaan uusi virtuaalikone Ctrl+N näppäinyhdistelmällä. Edetään ja määritellään palvelimen nimi, käyttöjärjestelmäksi Linux ja versioksi Ubuntu.



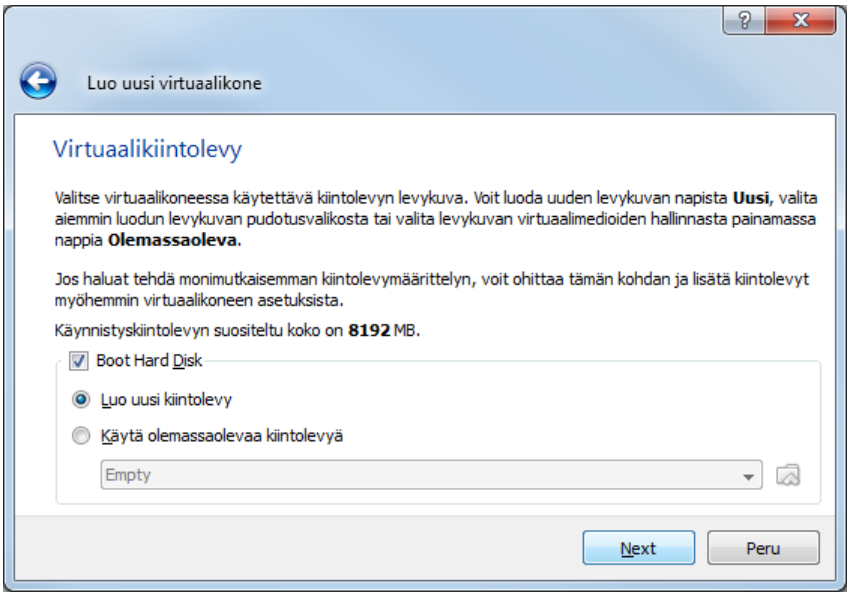
Kuva 12: Virtuaalikoneen luominen

3. Määritellään muisti, minkä olisi hyvä olla vähintään puolet tietokoneen muistista.



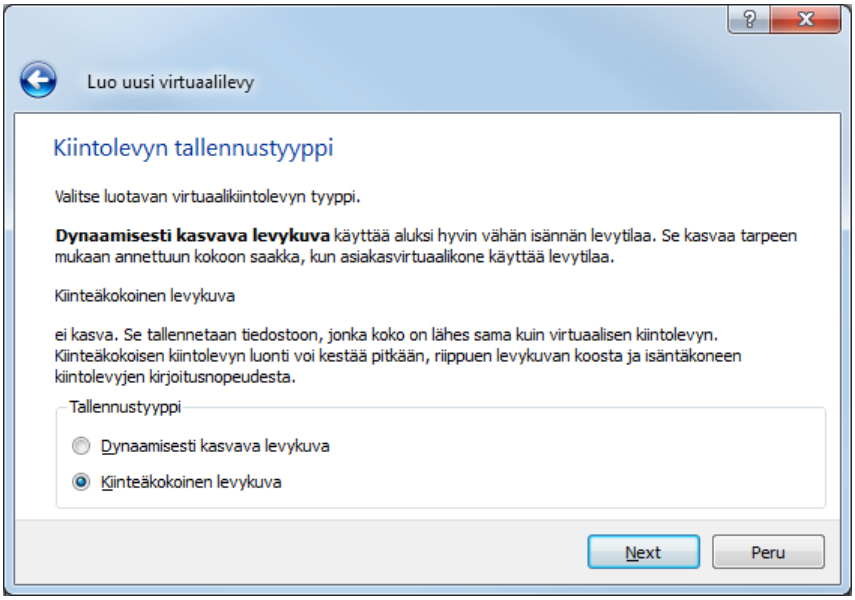
Kuva 13: Virtuaalikoneen muistin asettaminen

4. Kiintolevyasetuksissa valitaan Next.



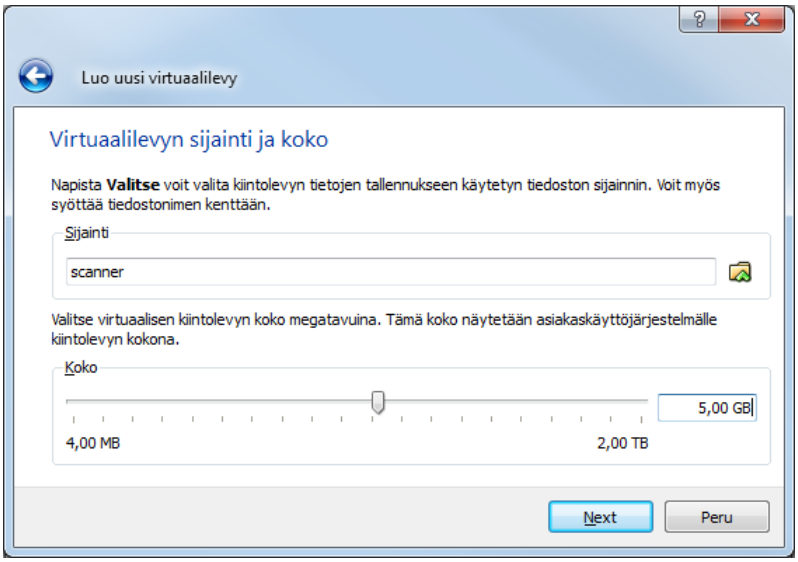
Kuva 14: Uuden virtuaalisen kiintolevyn luominen

5. Valitaan Kiinteäkokoinen levykuva



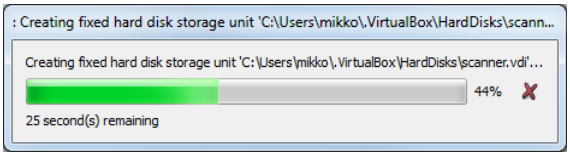
Kuva 15: Kiintolevykuvan määritteleminen

6. Määritellään virtuaalilevyn sijainti ja kiintolevytila, esim. 5 GB on riittävä tätä projektia varten.



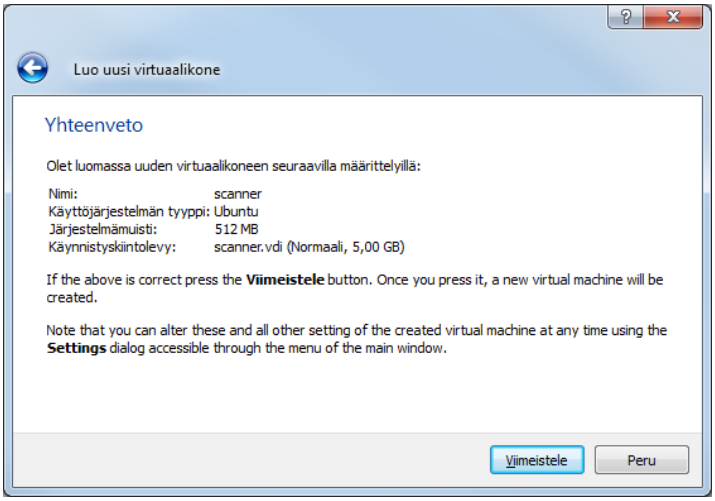
Kuva 16: Virtuaalilevyn sijainnin ja koon määritteleminen

7. Edetään ja painetaan Viimeistele näppäintä, tämä vie hetken kun luodaan uutta virtuaali-kiintolevyä.



Kuva 17: Virtuaalilevyn luominen

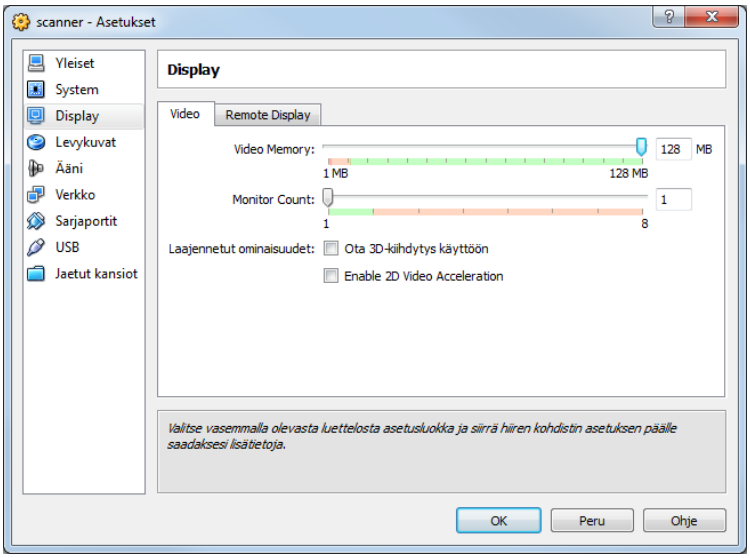
8. Valitaan viimeistele.



Kuva 18: Asennuksen viimeistely

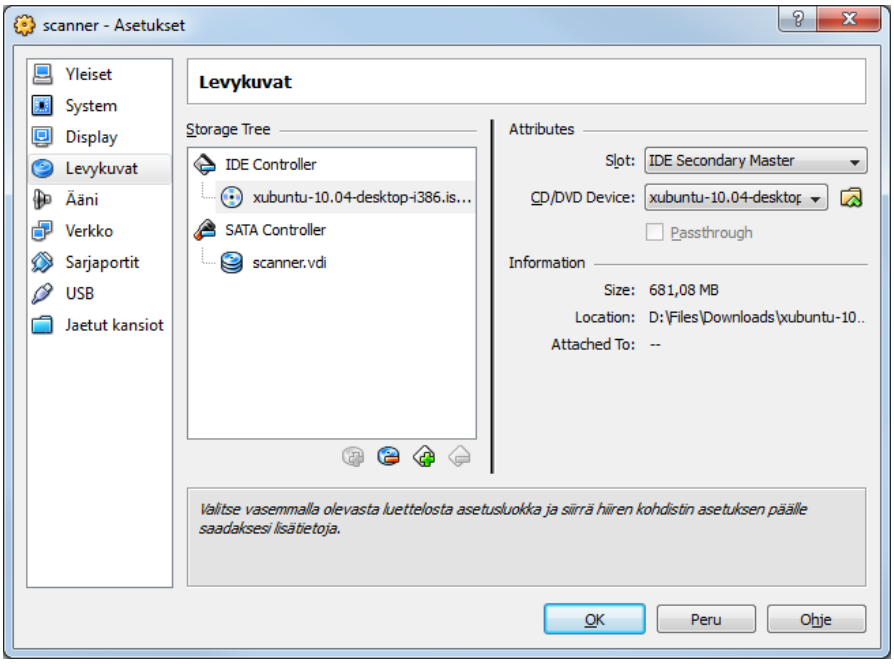
5.2.3 Asetusten määritteleminen virtuaalikoneeseen

1. Valitaan valikosta virtuaalikone, meidän tapauksessa nimesimme sen scanner:ksi ja painetaan Ctrl+S, valitaan valikosta Display ja laitetaan Video Memory määräksi suurin mahdollinen sallittu muistimäärä.



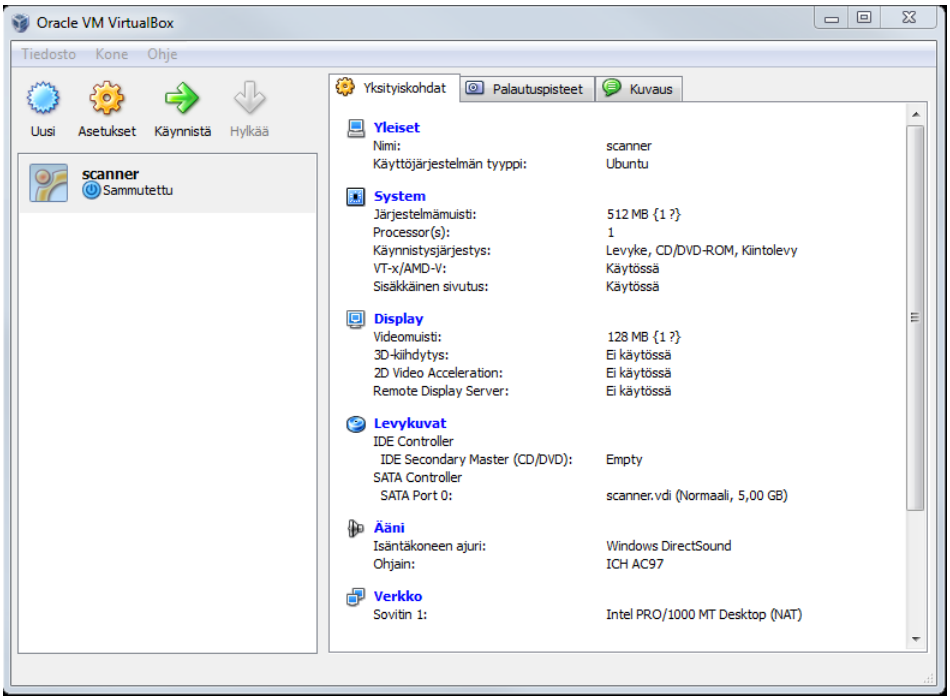
Kuva 19: Virtuaalikoneen näytönohjaimen muistimäärä

2. Siirrytään levykuvat valikkoon, valitaan CD/DVD Device ja sieltä Xubuntun .iso -tiedosto asennusta varten. Valitaan Ok painike.



Kuva 20: Xubuntun levykuvan määritteleminen

3. Aloitetaan Xubuntun asentaminen valitsemalla valikosta scanner ja valitaan Käynnistä näppäin.

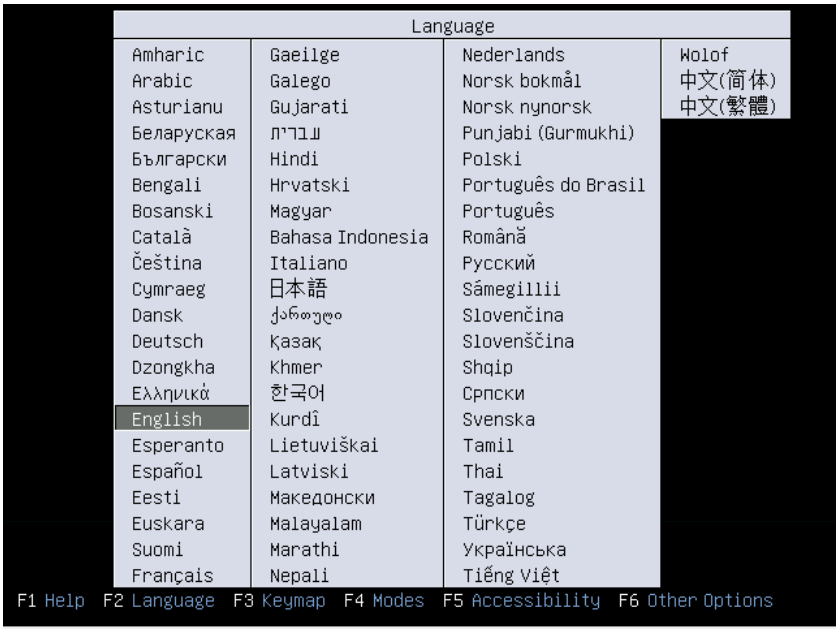


Kuva 21: VirtualBox perusvalikko ja yhteenveto virtuaalikoneen asetuksista

5.3 Käyttöjärjestelmä

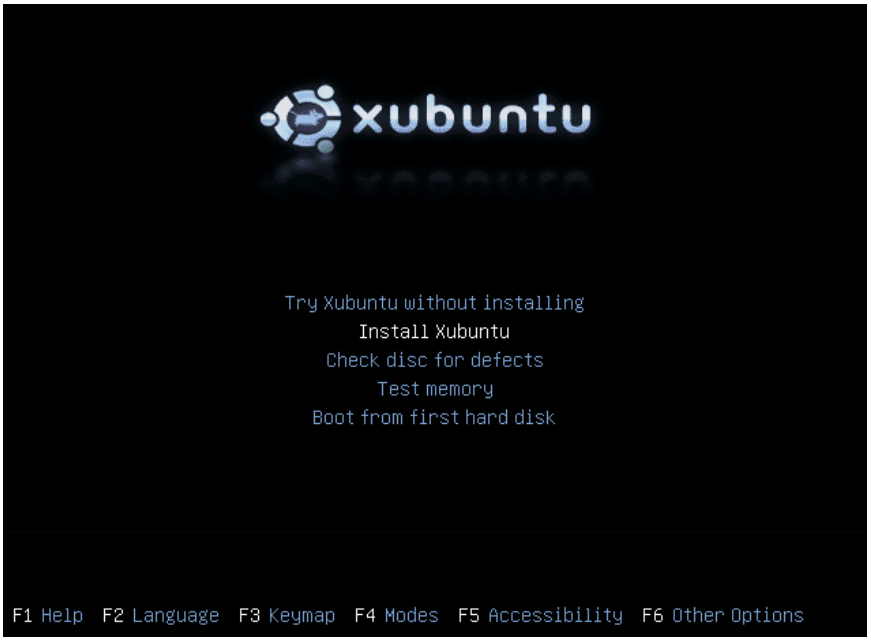
5.3.1 Xubuntu

1. Xubuntun asentaminen on hyvin yksinkertaista. Ensiksi valitsemme kielen, suositeltavaa on valita Englanti.



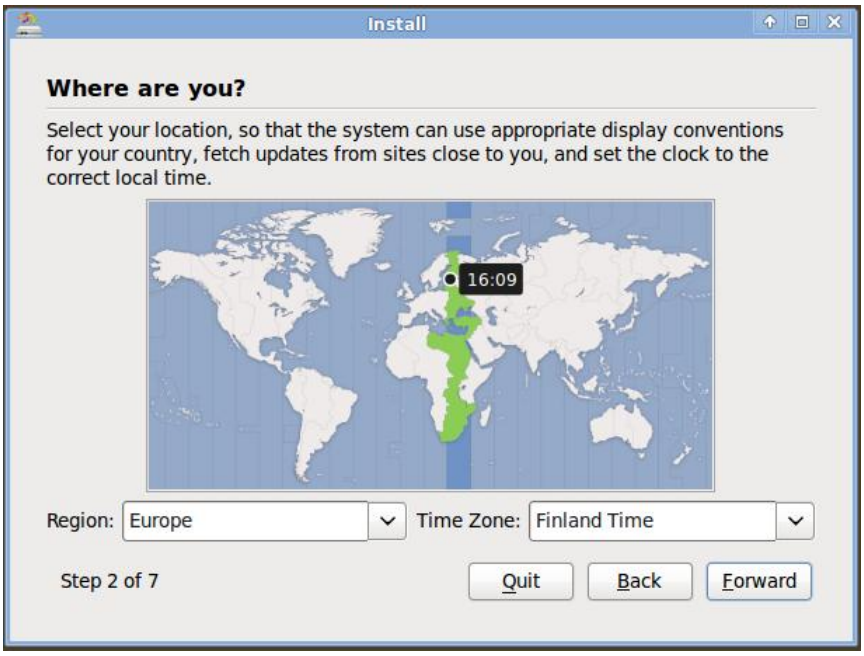
Kuva 22: Xubuntun asennusprosessin kielen määritteleminen

2. Valitaan Install Xubuntu.



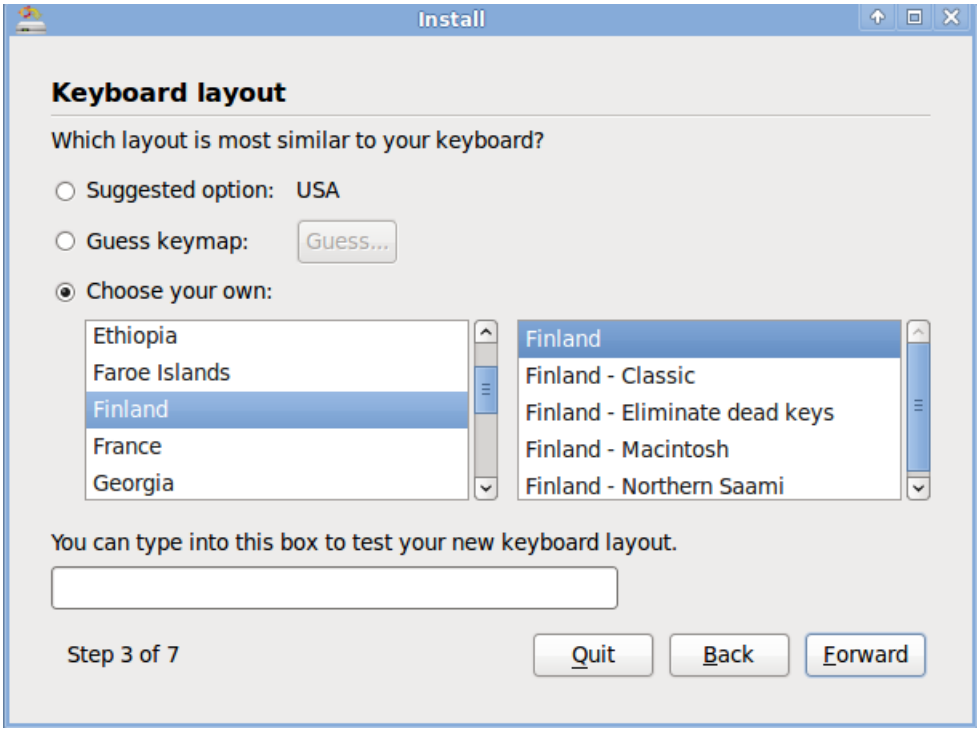
Kuva 23: Xubuntun asennusprosessin aloittaminen

3. Valitaan aikavyöhyke ja klikataan Forward.



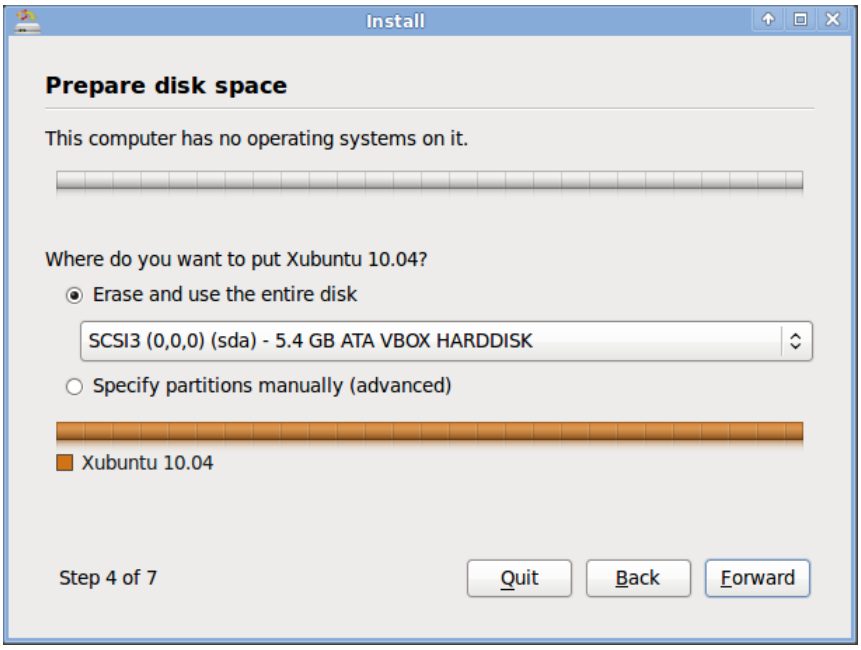
Kuva 24: Virtuaalipalvelimen aikavyöhykkeen määritteleminen

4. Määritellään näppäimistön asetukset, valitaan Finland ja klikataan Forward.



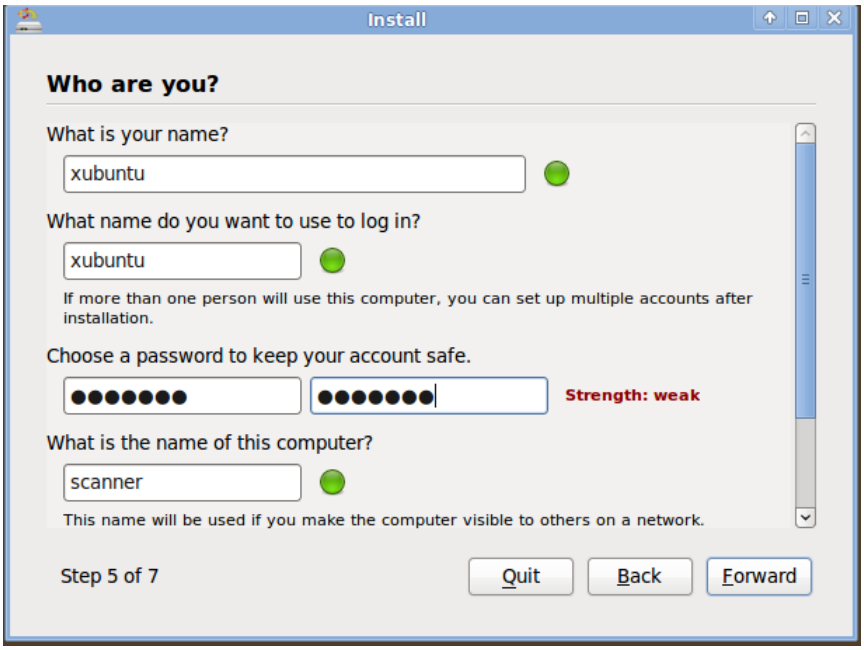
Kuva 25: Näppäinasetuksien määritteleminen

5. Alustetaan kiintolevy ja valitaan Forward.



Kuva 26: Virtuaalipalvelimen kiintolevyn alustus

6 Määrittelemme käyttäjätunnuksen, salasanan ja koneen nimen. Esim. käyttäjätunnus xubuntu ja salasana xubuntu.



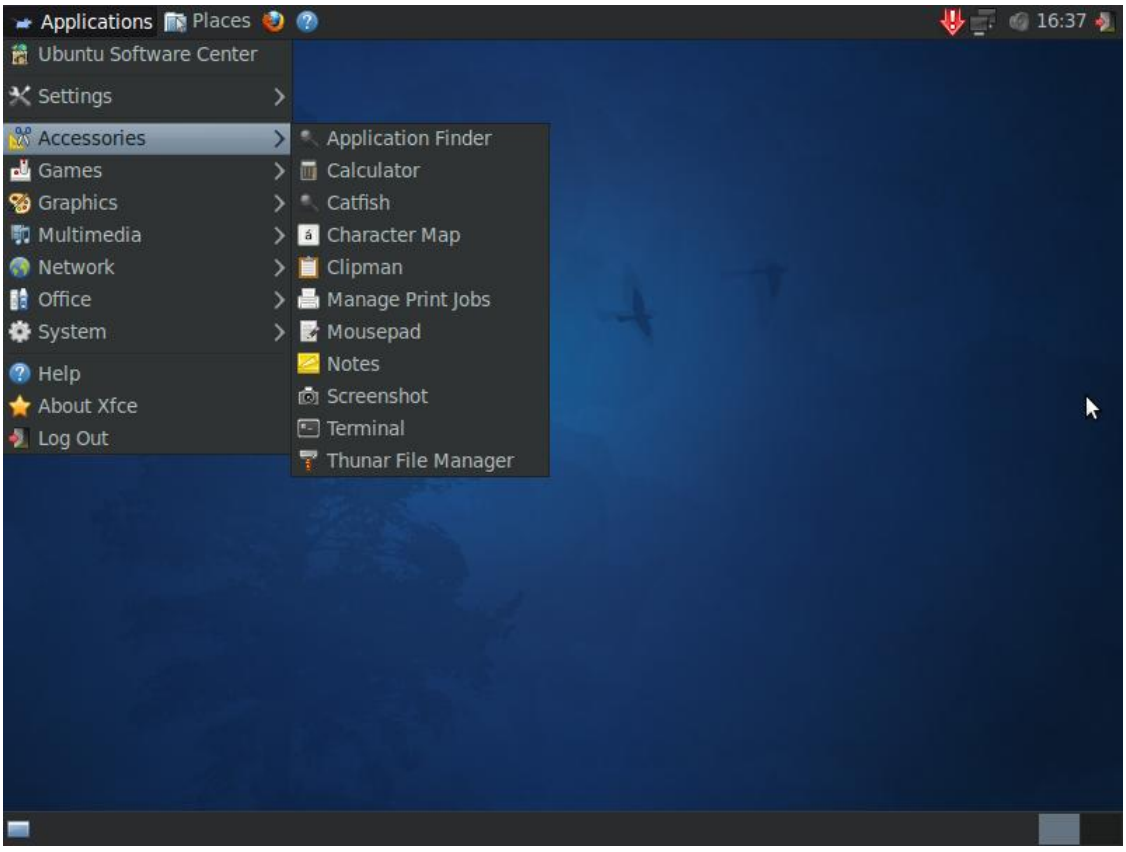
Kuva 27: Virtuaalipalvelimen, käyttäjätunnuksen ja salasanan määrittely

7. Xubuntu asentuu kovalevylle. Tämä vie hetken. Kun asennus on valmis, valitaan Reboot ja käynnistetään Xubuntu uusiksi.

Jos asennus tehtiin VirtualBoxin kautta, sammutamme koneen ensin valitsemalla VirtualBoxin valikoista Kone -> Sulje -> Sammuta kone -> Ok, jonka jälkeen painetaan Ctrl+D -> valitaan CD/DVD-levykuvat valikko -> Xubuntu ja vapautetaan .iso tiedosto Ctrl+L näppäinyhdistelmällä, tämän jälkeen painamme näppäintä Del Xubuntu .iso -tiedoston kohdalla ja poistamme sen valikosta ja seuraavaksi käynnistämme virtuaalikoneen uudelleen.

5.3.2 Xubuntun päivittäminen

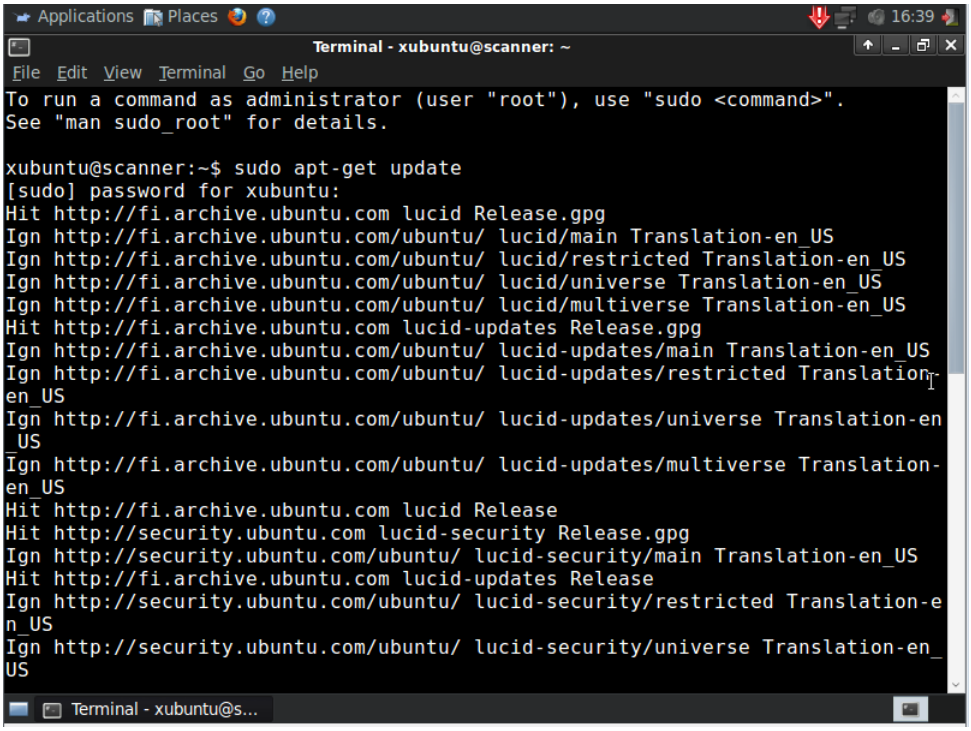
Xubuntun käynnistyttyä kirjaudumme sisään luomillamme tunnuksilla. Päivittäminen tapahtuu helpointen menemällä Applications valikon kautta Accessories valikkoon ja käynnistämällä ohjelma nimeltä Terminal, mikä on komentokehote Linuxille.



Kuva 28: Xubuntun perusnäkymä ja valikot

1. Seuraavalla komentosarjalla päivitämme ohjelmistojen ja kirjastojen listan. Xubuntu kysyy salasanaa.

sudo apt-get update



Kuva 29: Xubuntun päivitysprosessi

2. Aloitetaan varsinainen päivittäminen komennolla

sudo apt-get upgrade

Tämä päivittää käyttöjärjestelmän, jonka jälkeen se on käynnistettävä uudelleen.

3. Kone käynnistetään uudelleen komennolla

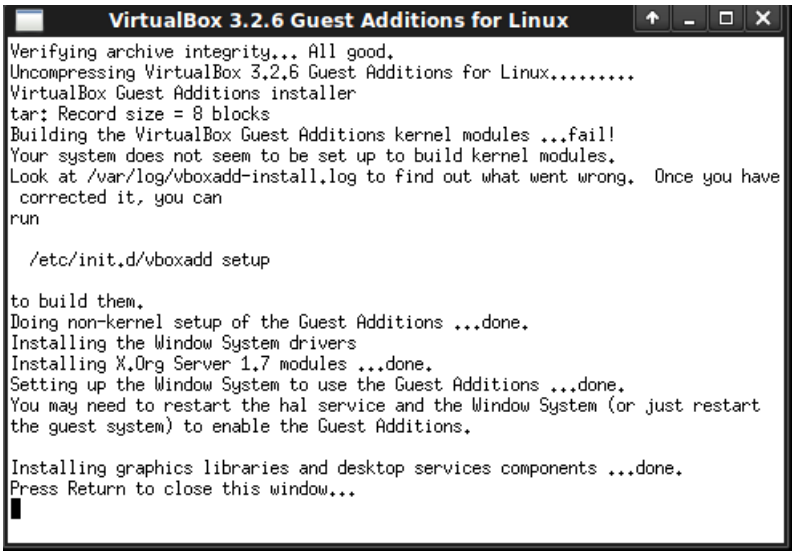
sudo reboot

Jos kone ei käynnisty automaattisesti, käynnistetään se VirtualBoxin valikosta normaaliin tapaan.

5.3.3 VirtualBox Guest Additions -lisäosa

Paremman toimivuuden takaamiseksi pitää asentaa VirtualBox Guest Additions ohjelmisto. Tämä lisää suorituskykyä, parempaa käytettävyyttä ja mahdollistaa kokonaisen näyttötilan käytön.

Asennus tapahtuu käynnistämällä virtuaalipalvelin, kirjautumalla sisään ja menemällä VirtualBoxin valikkoon laitteet ja valitsemalla sieltä Asenna lisäosat.



Kuva 30: Virtualbox Guest Additions asennus

Asennuksen jälkeen on virtuaalipalvelin käynnistettävä uusiksi.

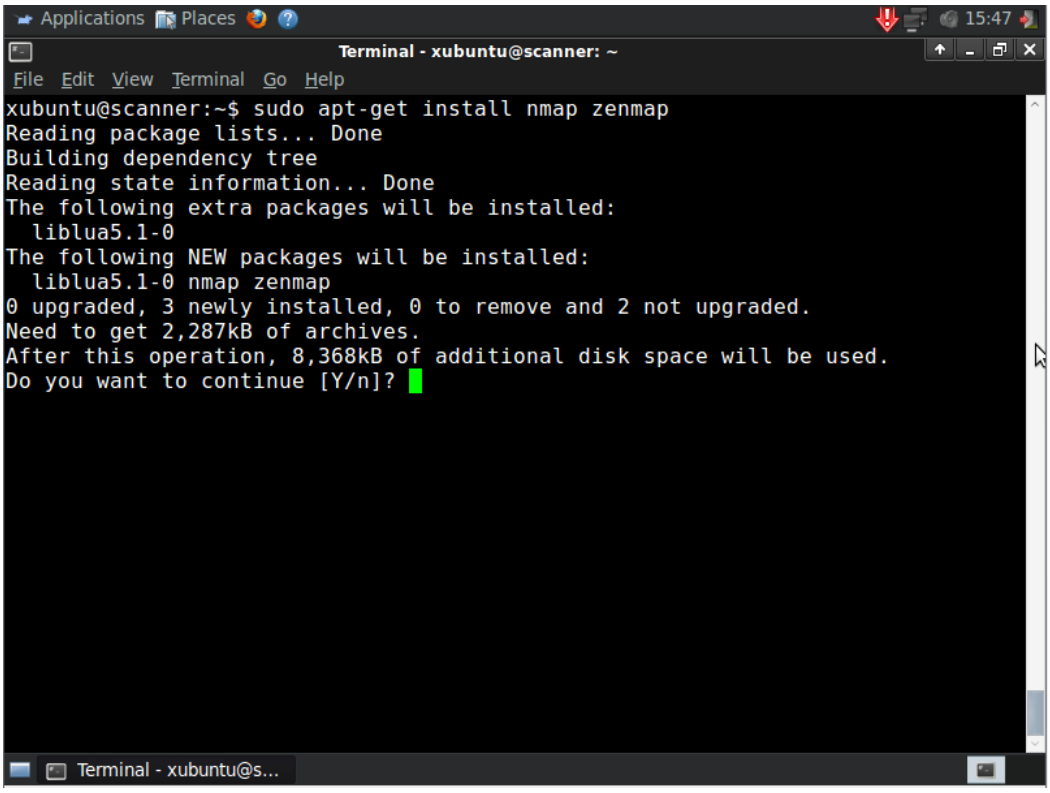
5.4 Apuohjelmistot

5.4.1 Nmap ja Zenmap

1. Nmapin ja Zenmapin asentamisen tapahtuu käynnistämällä komentokehote ja kirjoittamalla komento

sudo apt-get install nmap zenmap

2. Valitaan Y kun Xubuntun pakettimanageri kysyy halutaanko asentaa kyseiset ohjelmat.



Kuva 31: NMAP ja Zenmap asennus

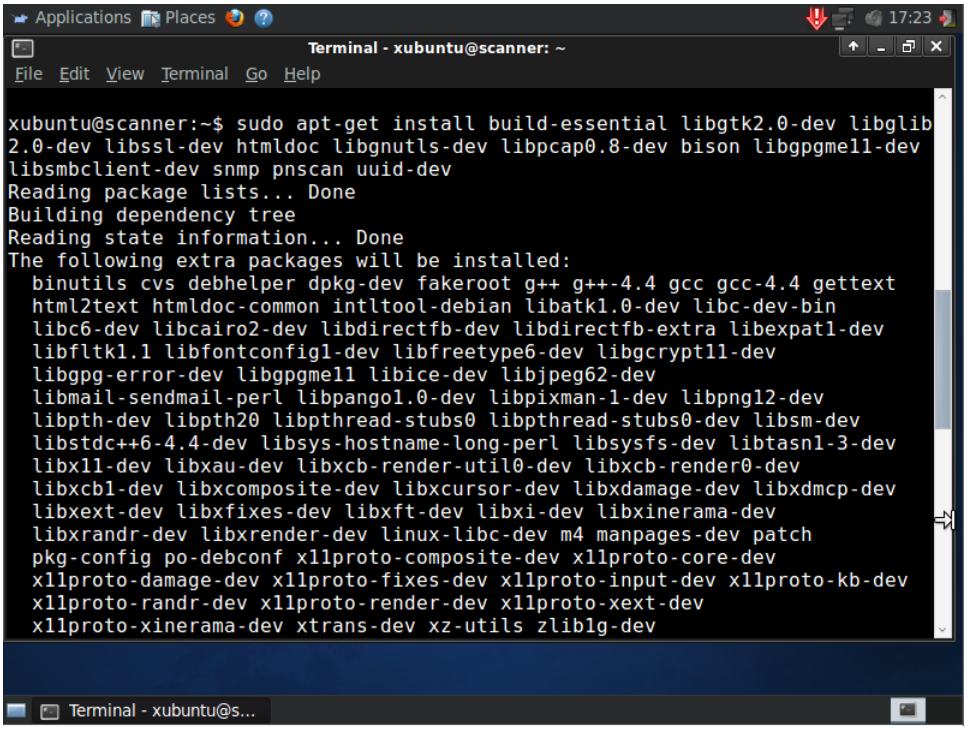
5.4.2 OpenVas

Ennen OpenVasin asennusta, joudumme hakemaan muita ohjelmia ja kirjastoja käyttämällä Xubuntun pakettimanageria. Käynnistetään komentokehote menemällä Applications valikkoon, josta valitsemme Accesories ja sieltä Terminal.

1. Ladataan koneelle tarvitsemamme paketit

sudo apt-get install build-essential libgtk2.0-dev libglib2.0-dev libssl-dev htmldoc libgnutls-dev libpcap0.8-dev bison libgpgme11-dev libsmbclient-dev snmp pnscan uuid-dev cmake

2. Asennus ilmoittaa lataavansa muita lisäpaketteja, kirjoitetaan Y ja painetaan Enter.



Kuva 32: Tarvittavien ohjelmakirjastojen asentaminen

3. Seuraavaksi kirjoitamme komennot

sudo updatedb
sudo ldconfig

4. Luodaan hakemistot tarvittavia tiedostoja varten, jonka jälkeen siirrymme kyseiseen hakemistoon

mkdir openvas
cd openvas

5. Haetaan wget komennolla tarvittavat OpenVas tiedostot

wget http://wald.intevation.org/frs/download.php/767/openvas-libraries-3.1.3.tar.gz
wget http://wald.intevation.org/frs/download.php/754/openvas-scanner-3.1.0.tar.gz
wget http://wald.intevation.org/frs/download.php/757/ openvas-client-3.0.1.tar.gz

Huom! Jos paketteja ei löydy, tarkista toimivat linkit http://www.openvas.org sivuilta.

6. Puretaan ladatut paketit

```
tar zxvf openvas-libraries-3.1.3.tar.gz
tar zxvf openvas-scanner-3.1.0.tar.gz
tar zxvf openvas-client-3.0.1.tar.gz
```

7. Käännetään ja asennetaan openvas-libraries paketti lähdekoodista

```
cd openvas-libraries-3.1.3
sudo ./configure
sudo make
sudo make install
sudo ldconfig
```

8. Käännetään ja asennetaan openvas-scanner paketti

```
cd ../openvas-scanner-3.1.0
sudo ./configure
sudo make
sudo make install
```

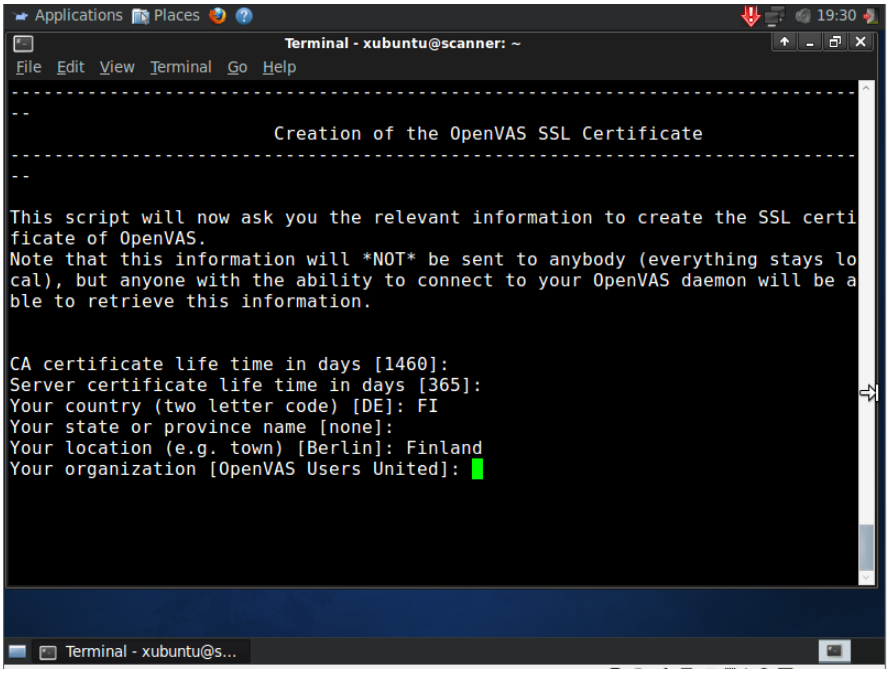
9 Käännetään ja asennetaan openvas-client paketti

```
cd ../openvas-client-3.0.1
sudo ./configure
sudo make
sudo make install
sudo updatedb
sudo ldconfig
```

10. Luodaan sertifikaatti OpenVasia varten

```
sudo openvas-mkcert
```

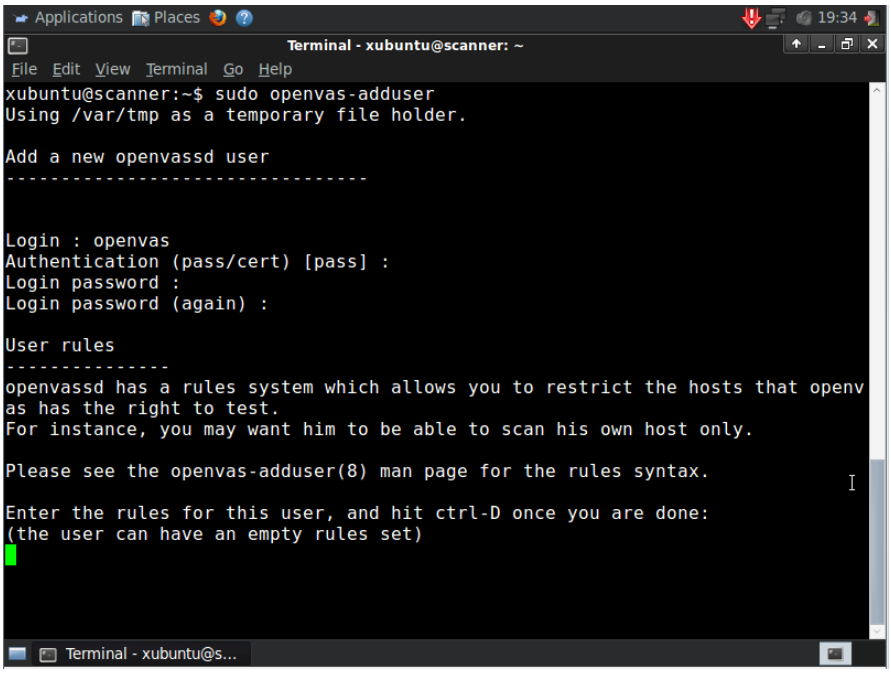
Edetään alla olevan kuvan tietojen mukaan



Kuva 33: Sertifikaatin luominen OpenVAS:iin

11. Luodaan käyttäjätunnus OpenVas palvelinta varten

sudo openvass-adduser



Kuva 34: Käyttäjätunnuksen luominen

Edetään ohjeitten mukaan, esim. käyttäjätunnukseksi ja salasanaksi openvas, painetaan Ctrl+D yhdistelmää, minkä jälkeen ohjelmisto kysyy vahvistetaanko tiedot ja valitaan Y.

12. Päivitetään OpenVasin pluginit, jotta palvelimella olisi uusimmat tiedot haavoittuvuuksista.

sudo openvas-nvt-sync

13. Seuraavaksi asennetaan lisäohjelmia, joita OpenVasin pluginit käyttävät hyväkseen erilaisissa skannausmetodeissa. Tämä tapahtuu komennolla

sudo apt-get install w3af nikto

14. Asennuksen jälkeen on Xubuntu käynnistettävä uudelleen, tämä tapahtuu kirjoittamalla

sudo reboot

5.5 Virtuaalipalvelimen kloonaus

Virtuaalipalvelimen kloonaus tarkoittaa sitä, että voidaan kopioida asennettu virtuaalipalvelin toiselle koneelle, ilman sitä, että pitäisi käydä läpi kaikki asennuksen kohdat läpi uudestaan. Kloonattu virtuaalipalvelin on identtinen.

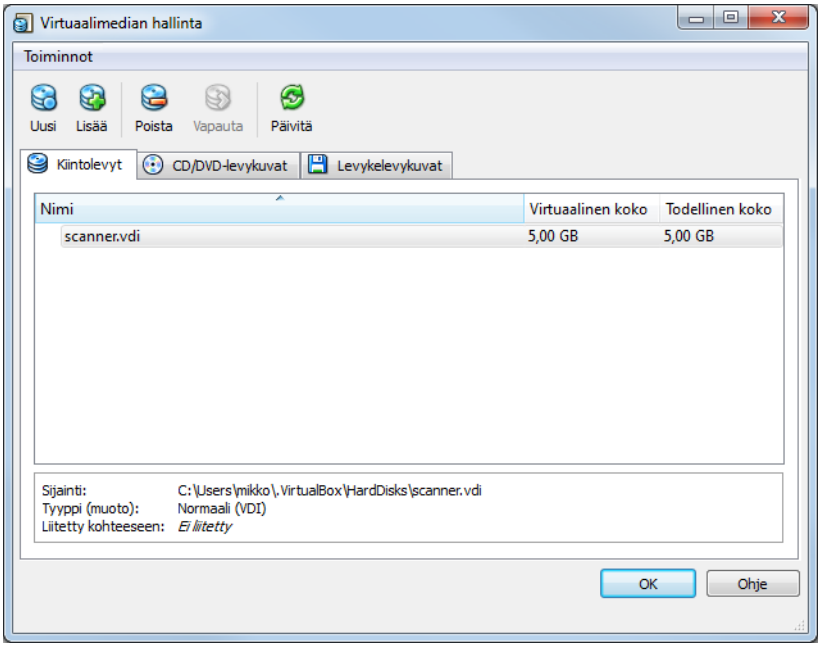
1. On asennettava VirtualBox uudelle koneelle, tämä tapahtuu normaalisti ohjeiden mukaan.

2. Kopioidaan aikaisemmalta palvelimelta virtuaalikiintolevy joko tarpeeksi isolle muistitikulle tai ulkoiselle kiintolevylle.

Virtuaalikiintolevy sijaitsee VirtualBoxin ”.virtualbox\harddisks” hakemistossa, ellei muuten olen määritelty. Esim. käytimme isäntäkoneena Windows XP:tä, joten virtuaalikiintolevy sijaitsee hakemistossa ”c:\documents and settings\administrator\.virtualbox\harddisks\”. Tiedosto on aina .vdi –päätteinen, meidän tapauksessa virtuaalikiintolevy oli nimetty scanner.vdi:ksi.

Tämän jälkeen siirretään virtuaalikiintolevy uudelle palvelimelle kyseiseen hakemistoon.

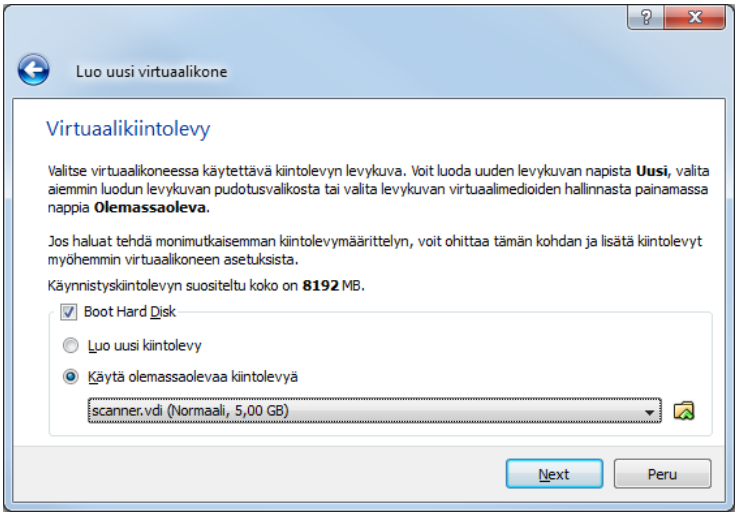
3. Käynnistetään VirtualBox, siirrytään virtuaalimedioiden hallintaan Ctrl+D näppäinyhdistelmällä. Valitaan ”Lisää” pikakuvake ja etsitään juuri kopioimamme virtuaalikiintolevy. Valitaan ok.



Kuva 35: Virtuaalikiintolevyjen hallinta

4. Edetään VirtualBox:n asennusohjeiden vaiheiden 2 ja 3 mukaan.

5. Seuraavaksi valitaan ”Käytä olemassa olevaa kiintolevyä, kiintolevyä ei valmiiksi näy listalla, on määriteltävä hakemisto missä se sijaitsee.



Kuva 36: Kloonatun virtuaalikiintolevyn valitseminen

6. Valitaan viimeistele, määritellään virtuaalipalvelimen ”Video Memory” aikaisempien ohjeiden mukaan, minkä jälkeen virtuaalipalvelin voidaan käynnistää normaaliin tapaan.

6 Yhteenveto

Työn tarkoituksena oli saada Laurean Neon-laboratorioon toimiva virtuaaliympäristö, jossa voisi käyttää NMAP-porttiskanneria ja OpenVAS-haavoittuvuuksien etsintä- ja arviointityökalua. Kyseistä virtuaaliympäristöä olisi tarkoitus käyttää opetuskäytössä. Lisäksi heti alussa rajasimme aiheen siten, että teemme tämän ympäristön niin, ettei siitä synny kustannuksia Laurealle eli käytämme vain vapaan lähdekoodin ohjelmia. Alustana päätimme käyttää Linux Xubuntua, sen keveyden ja helppokäyttöisyyden vuoksi.

Työn alussa tutustuimme virtualisointiin yleisesti ja aloimme etsiä tietoa aiheesta. Virtualisointia olimme käsitelleet pintapuolisesti aikaisemmilla opintojaksoilla. Aloimme myös selvittää millä, ohjelmalla virtualisointi kannattaisi toteuttaa ja päädyimme Virtualbox-nimiseen ohjelmaan, joka on myös vapaan lähdekoodin ohjelma.

Tämän jälkeen aloitimme tutkimaan ja vertailemaan erilaisia tietoturvaan liittyviä ohjelmia kuten porttiskannereita ja haavoittuvuuksien etsintäohjelmia. Lopulta päädyimme valitsemaan NMAP-porttiskannerin ja OpenVAS haavoittuvuuksien etsintä- ja arviointityökalun.

Kun ohjelmat, joilla työ tultaisiin toteuttamaan oli valittu, aloitimme ohjelmien asentamisen Neon-laboratorion tiloissa. Ensimmäisenä asensimme Linux Xubuntun. Sen jälkeen muut käyttämämme ohjelmat. Asentaminen vei paljon aikaa, mutta saimme lopulta ohjelmat toimimaan. Asentamisvaiheessa teimme myös yksityiskohtaiset ohjeet jokaisen asentamamme ohjelman kohdalla.

Huomasimme kuitenkin, että toteutetun virtuaalisoinnin kautta kyseinen virtuaaliympäristö ei olisi välttämättä paras mahdollinen vaihtoehto opetuskäytössä, jossa sitä käyttäisi monta käyttäjää samaan aikaan, sillä Neon-laboratorion tietokoneissa ei riitä tarpeeksi tehoja virtualisoidun palvelimen sekä asiakasohjelmiston pyörittämiseen kunnolla ja aikaa säästävästi samaan aikaan.

Järjestelmä tulisi toimimaan paremmin, jos resurssit jaettaisiin palvelimen ja virtualisoidun asiakasohjelmiston kesken. OpenVAS-palvelinohjelmisto asennettaisiin täysin omalle tai ennestään pyörivälle Linux-palvelinkoneelle, jos sellainen löytyy Laurean ympäristöstä.

OpenVAS-asiakasohjelmistoa voitaisiin ajaa Neon-laboratorion koneista asennusohjeiden mukaan virtualisoidun ympäristön kautta ja miksei myös vaikkapa kannettavista, kunhan yhteys palvelinkoneelle on taattu.

Näin järjestelmää voisi käyttää useat henkilöt samaan aikaan. Tämä olisi tarkoituksen mukaista opetuskäytössä.

Tätä projektia oli mielenkiintoista tehdä ja virtualisoinnin kanssa olemme varmasti myös tulevaisuudessa tekemisissä. Välillä kohtasimme vastoinkäymisiä mutta onnistuimme jatkamaan ja saamaan työn päätökseen. Tiimityöskentelymme toimi hyvin koko projektin ajan.

Lähteet

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. 2009. 1. painos Porvoo: WSOYpro.

Sähköiset lähteet

Amit Singh, An Introduction to Virtualization. 10.11.2010
http://www.kernelthread.com/publications/virtualization

Atea 2010, Virtualisointi tuo joustoa ja kustannussäästöjä niin konesaliin kuin toimistonkin puolelle. 10.11.2010
http://www.atea.fi/www.atea.fi/virtualisointi

Bradley Tony, Introduction to Port Scanning. 15.12.2010
http://netsecurity.about.com/cs/hackertools/a/aa121303.htm

Bradley Tony, Introduction to Vulnerability Scanning. 15.12.2010
http://netsecurity.about.com/cs/hackertools/a/aa030404.htm

Mäntylä J-M, 2008. Virtualisointi mullistaa tietotekniikan. 30.08.2010
http://www.tietoviikko.fi/cio/article192316.ece

nikto2, Description. 13.12.2010
http://cirt.net/nikto2

Nmap, Nmap Reference Guide. 13.12.2010
http://nmap.org/book/man.html#man-description

Nmap, Zenmap GUI Users' Guide. 13.12.2010
http://nmap.org/book/zenmap.html#zenmap-intro

OpenVAS, About OpenVAS NVT Feed. 13.12.2010
http://openvas.org/openvas-nvt-feed.html

OpenVAS, OpenVAS Compedium, Version 1.0.1. 13.12.2010
http://wald.intevation.org/frs/download.php/558/openvas-compendium-1.0.1.pdf

Virtualbox, User Manual, Version 4.0.2. 30.08.2010
http://download.virtualbox.org/virtualbox/UserManual.pdf

VMware, Understanding Full Virtualization, Paravirtualization, and Hardware Assist. 30.08.2010
http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf

w3af, FAQ. 13.10.2010
http://w3af.sourceforge.net/faq.php

What is emulation? Koninklijke bibliotheek, Nationale bibliotheek van Nederland. 30.08.2010
http://www.kb.nl/hrd/dd/dd_projecten/projecten_emulatiewatis-en.html

Kuvat

Liitteet

Liite 1 Nmap-aputiedosto

```
Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file

HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host

SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  -F: Fast mode - Scan fewer ports than the default scan
```

```
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>

SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)

SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
          directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.

OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively

TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second

FIREWALL/IDS EVASION AND SPOOFING:
```

-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
--adler32: Use deprecated Adler32 instead of CRC32C for SCTP checksums

OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--log-errors: Log errors/warnings to the normal-format output file
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.

EXAMPLES:

```
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
```

Liite 2 Nmap-tiedustelu 1

Starting Nmap 5.00 (http://nmap.org) at 2010-09-21 10:13 EEST

Interesting ports on 193.166.246.147:
Not shown: 990 filtered ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	http?	
135/tcp	open	msrpc?	
445/tcp	open	microsoft-ds?	
1025/tcp	open	NFS-or-IIS?	
1044/tcp	open	unknown	
1067/tcp	open	instl_boots?	
1311/tcp	open	rxmon?	
3389/tcp	open	ms-term-serv?	
5002/tcp	open	rfe?	
20031/tcp	open	unknown	

Host script results:
| smb-os-discovery: Windows Server 2003 R2 3790 Service Pack 2
| LAN Manager: Windows Server 2003 R2 5.2
| Name: WORKGROUP\PIHTA
|_ System time: 2010-09-21 10:14:43 UTC+3
|_ nbstat: ERROR: Name query failed: TIMEOUT

Service detection performed. Please report any incorrect results at http://nmap.org/submit/

Nmap done: 1 IP address (1 host up) scanned in 152.99 seconds

Liite 3 Nmap-tiedustelu 2

Starting Nmap 5.00 (http://nmap.org) at 2010-09-21 10:17 EEST

NSE: Loaded 30 scripts for scanning.

Initiating Ping Scan at 10:17
Scanning 192.168.12.17 [8 ports]
Completed Ping Scan at 10:17, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 10:17
Completed Parallel DNS resolution of 1 host. at 10:17, 0.03s elapsed

Initiating SYN Stealth Scan at 10:17
Scanning 192.168.12.17 [1000 ports]

Discovered open port 445/tcp on 192.168.12.17
Discovered open port 135/tcp on 192.168.12.17
Discovered open port 139/tcp on 192.168.12.17
Discovered open port 25/tcp on 192.168.12.17
Discovered open port 80/tcp on 192.168.12.17
Discovered open port 443/tcp on 192.168.12.17
Discovered open port 1025/tcp on 192.168.12.17
Completed SYN Stealth Scan at 10:17, 4.76s elapsed (1000 total ports)

Initiating Service scan at 10:17
Scanning 7 services on 192.168.12.17
Completed Service scan at 10:18, 86.25s elapsed (7 services on 1 host)

Initiating OS detection (try #1) against 192.168.12.17
Retrying OS detection (try #2) against 192.168.12.17

Initiating Traceroute at 10:18
192.168.12.17: guessing hop distance at 1
Completed Traceroute at 10:18, 10.02s elapsed

Initiating Parallel DNS resolution of 2 hosts. at 10:18
Completed Parallel DNS resolution of 2 hosts. at 10:18, 0.00s elapsed

NSE: Script scanning 192.168.12.17.
NSE: Starting runlevel 1 scan
Initiating NSE at 10:18
Completed NSE at 10:18, 1.58s elapsed

NSE: Starting runlevel 2 scan
Initiating NSE at 10:18
Completed NSE at 10:19, 40.02s elapsed
NSE: Script Scanning completed.

Host 192.168.12.17 is up (0.00055s latency).

Interesting ports on 192.168.12.17:
Not shown: 993 filtered ports

PORT	STATE	SERVICE	VERSION
25/tcp	open	smtp	Microsoft ESMTP 6.0.2600.5949

| smtp-commands: EHLO Neon-labra2 Hello [192.168.12.17], SIZE 2097152, PIPELINING, DSN, ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY
|_ HELP This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT VRFY

80/tcp	open	http	Microsoft IIS webserver 5.1

| html-title: You are not authorized to view this page
|_ Requested resource was http://192.168.12.17/localstart.asp

135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	
443/tcp	open	https?	
445/tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
1025/tcp	open	msrpc	Microsoft Windows RPC

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

```
Service Info: Host: Neon-labra2; OS: Windows

Host script results:
|  nbstat: NetBIOS name: NEON-LABRA2, NetBIOS user: <unknown>, NetBIOS MAC:
00:22:64:33:43:45
|  Name: NEON-LABRA2<00>       Flags: <unique><active>
|  Name: NEON-LABRA2<20>       Flags: <unique><active>
|  Name: WORKGROUP<00>         Flags: <group><active>
|  Name: WORKGROUP<1e>         Flags: <group><active>
|  Name: WORKGROUP<1d>         Flags: <unique><active>
|_ Name: \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|  smb-os-discovery: Windows XP
|  LAN Manager: Windows 2000 LAN Manager
|  Name: WORKGROUP\NEON-LABRA2
|_ System time: 2010-09-21 10:18:58 UTC+3

TRACEROUTE (using port 21/tcp)
HOP RTT  ADDRESS
1   ...
2   0.28 192.168.12.17

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 147.11 seconds
Raw packets sent: 2060 (93.920KB) | Rcvd: 98 (4616B)
```

Liite 4 OpenVAS-testitulokset

192.168.12.17

smtp (25/tcp)

Security Hole
Reported by NVT "Sendmail smad vuln" (1.3.6.1.4.1.25623.1.0.80102):

Synopsis :
The remote host is subject to the 'smad' attack(sendmail accept dos).

Description :
Smad prevents sendmail from accepting legitimate connections. A cracker may use this flaw to prevent you from receiving any email, thus lowering the interest of being connected to internet.

This attack is specific to some versions of the Linux kernel.

There are various security bugs in the implementation of this service which can be used by an intruder to gain a root account rather easily.

Reference :
http://online.securityfocus.com/archive/1/11073

Solution : upgrade your Linux kernel to a newer version or filter incoming traffic to this port.

Risk factor :
High

Security Note
Reported by NVT "Services" (1.3.6.1.4.1.25623.1.0.10330):

An SMTP server is running on this port
Here is its banner :
220 Neon-labra2 Microsoft ESMTP MAIL Service, Version: 6.0.2600.5949 ready at Tue, 21 Sep 2010 10:58:13 +0300
ntp (123/udp)

Security Note
Reported by NVT "NTP read variables" (1.3.6.1.4.1.25623.1.0.10884):

A NTP (Network Time Protocol) server is listening on this port.

Risk factor : Low

http (80/tcp)

Security Note
Reported by NVT "Nikto (NASL wrapper)" (1.3.6.1.4.1.25623.1.0.14260):

Here is the Nikto report:
- Nikto v2.03/2.04

+ Target IP: 192.168.12.17
+ Target Hostname: 192.168.12.17
+ Target Port: 80
+ Start Time: 2010-09-22 11:00:35

+ Server: Microsoft-IIS/5.1
- Root page / redirects to: localstart.asp
+ No CGI Directories found (use '-C all' to force check all possible dirs)

- Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH

+ OSVDB-877: HTTP method ('Allow' Header): 'TRACE' is typically only used for debugging and should be disabled. This message does not mean it is vulnerable to XST.

+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.

+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.

+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.

+ OSVDB-0: HTTP method ('Allow' Header): 'PROPFIND' may indicate DAV/WebDAV is installed. This may be used to get directory listings if indexing is allowed but a default page exists.
+ OSVDB-0: HTTP method ('Allow' Header): 'PROPPATCH' indicates DAV/WebDAV is installed.
+ OSVDB-: HTTP method ('Allow' Header): 'SEARCH' indicates DAV/WebDAV is installed, and may be used to get directory listings if Index Server is running.

- Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH

+ OSVDB-877: HTTP method ('Public' Header): 'TRACE' is typically only used for debugging and should be disabled. This message does not mean it is vulnerable to XST.

+ OSVDB-5646: HTTP method ('Public' Header): 'DELETE' may allow clients to remove files on the web server.

+ OSVDB-397: HTTP method ('Public' Header): 'PUT' method could allow clients to save files on the web server.

+ OSVDB-5647: HTTP method ('Public' Header): 'MOVE' may allow clients to change file locations on the web server.

+ OSVDB-0: HTTP method ('Public' Header): 'PROPFIND' may indicate DAV/WebDAV is installed. This may be used to get directory listings if indexing is allowed but a default page exists.

+ OSVDB-0: HTTP method ('Public' Header): 'PROPPATCH' indicates DAV/WebDAV is installed.

+ OSVDB-: HTTP method ('Public' Header): 'SEARCH' indicates DAV/WebDAV is installed, and may be used to get directory listings if Index Server is running.

+ Microsoft-IIS/5.1 appears to be outdated (4.0 for NT 4, 5.0 for Win2k)

+ OSVDB-877: TRACK / : TRACK option ('TRACE' alias) appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details

+ OSVDB-877: TRACE / : TRACE option appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details

+ Default account found for '192.168.12.17' at /localstart.asp (ID 'Administrator', PW '). Generic account discovered

- Successfully authenticated to realm "192.168.12.17".

+ OSVDB-3092: GET /iishelp/iis/misc/default.asp : Default IIS page found.

+ 3577 items checked: 21 item(s) reported on remote host
+ End Time: 2010-09-22 11:02:56 (141 seconds)

+ 1 host(s) tested

Test Options: -h 192.168.12.17 -p 80

==========
Reported by NVT "w3af (NASL wrapper)" (1.3.6.1.4.1.25623.1.0.80109):

Here is the w3af report:
[Tue Sep 21 11:01:26 2010 - information] Auto-enabling plugin: grep.error500
[Tue Sep 21 11:01:26 2010 - Enabled plugins] plugins
[Tue Sep 21 11:01:26 2010 - Enabled plugins] audit sqli, xss
[Tue Sep 21 11:01:26 2010 - Enabled plugins] audit config sqli
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back
[Tue Sep 21 11:01:26 2010 - Enabled plugins] audit config xss
[Tue Sep 21 11:01:26 2010 - Enabled plugins] set checkStored True
[Tue Sep 21 11:01:26 2010 - Enabled plugins] set numberOfChecks 3
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back
[Tue Sep 21 11:01:26 2010 - Enabled plugins] plugins
[Tue Sep 21 11:01:26 2010 - Enabled plugins] grep error500
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back
[Tue Sep 21 11:01:26 2010 - Enabled plugins] plugins
[Tue Sep 21 11:01:26 2010 - Enabled plugins] output textFile, console, gtkOutput
[Tue Sep 21 11:01:26 2010 - Enabled plugins] output config textFile
[Tue Sep 21 11:01:26 2010 - Enabled plugins] set verbose False
[Tue Sep 21 11:01:26 2010 - Enabled plugins] set fileName /tmp/openvas-w3af-192.168.12.17-80.rep
[Tue Sep 21 11:01:26 2010 - Enabled plugins] set httpFileName /tmp/openvas-w3af-192.168.12.17-80.http
[Tue Sep 21 11:01:26 2010 - Enabled plugins] set showCaller False
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back

[Tue Sep 21 11:01:26 2010 - Enabled plugins] output config console
[Tue Sep 21 11:01:26 2010 - Enabled plugins] set verbose False
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back
[Tue Sep 21 11:01:26 2010 - Enabled plugins] output config gtkOutput
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back
[Tue Sep 21 11:01:26 2010 - Enabled plugins] plugins
[Tue Sep 21 11:01:26 2010 - Enabled plugins] discovery yahooSiteExplorer
[Tue Sep 21 11:01:26 2010 - Enabled plugins] discovery config yahooSiteExplorer
[Tue Sep 21 11:01:26 2010 - Enabled plugins] set resultLimit 300
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back
[Tue Sep 21 11:01:26 2010 - Enabled plugins] target
[Tue Sep 21 11:01:26 2010 - Enabled plugins] set target http://192.168.12.17:80
[Tue Sep 21 11:01:26 2010 - Enabled plugins] back
[Tue Sep 21 11:01:26 2010 - error] There is no point in searching yahoo site explorer for site: "192.168.12.17" . Yahoo doesnt index private pages.
[Tue Sep 21 11:01:26 2010 - information] Found 1 URLs and 1 different points of injection.
[Tue Sep 21 11:01:26 2010 - information] The list of URLs is:
[Tue Sep 21 11:01:26 2010 - information] - http://192.168.12.17:80
[Tue Sep 21 11:01:26 2010 - information] The list of fuzzable requests is:
[Tue Sep 21 11:01:26 2010 - information] - http://192.168.12.17:80 | Method: GET
[Tue Sep 21 11:01:26 2010 - information] Starting sqli plugin execution.
[Tue Sep 21 11:01:26 2010 - information] Starting xss plugin execution.
[Tue Sep 21 11:01:26 2010 - information] Finished scanning process.
[Tue Sep 21 11:01:27 2010 - console] termios error: (25, 'Inappropriate ioctl for device')
[Tue Sep 21 11:01:27 2010 - console]
[Tue Sep 21 11:01:27 2010 - console] termios error: (25, 'Inappropriate ioctl for device')
[Tue Sep 21 11:01:27 2010 - console] got shell?

general/tcp

Security Note
Reported by NVT "Check open ports" (1.3.6.1.4.1.25623.1.0.10919):

** All ports were skipped by this check because some
** scripts could not connect to them before the defined timeout

This might be an availability problem related which might be

due to the following reasons :

- The remote host is now down, either because a user turned it
off during the scan

- A network outage has been experienced during the scan, and the remote
network cannot be reached from the OpenVAS server any more

- This OpenVAS server has been blacklisted by the system administrator
or by automatic intrusion detection/prevention systems which have detected the
vulnerability assessment.

In any case, the audit of the remote host might be incomplete and may need to
be done again

==========
Reported by NVT "Traceroute" (1.3.6.1.4.1.25623.1.0.51662):

Here is the route from 10.0.2.15 to 192.168.12.17
10.0.2.15
192.168.12.17
==========
Reported by NVT "Checks for open tcp ports" (1.3.6.1.4.1.25623.1.0.900239):
Open TCP ports are 443, 1025, 445, 135, 25, 139, 80
==========
Reported by NVT "OS fingerprinting" (1.3.6.1.4.1.25623.1.0.102002):

ICMP based OS fingerprint results:

Unable to detect remote OS. No match found.

Log Message

Reported by NVT "Information about the scan" (1.3.6.1.4.1.25623.1.0.19506):
Information about this scan :

OpenVAS version : 3.1.3.
Plugin feed version : 201008271056

Type of plugin feed : OpenVAS NVT Feed
Scanner IP : 10.0.2.15
Port scanner(s) : openvas_tcp_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Max hosts : 20
Max checks : 4
Scan Start Date : 2010/9/21 10:58
Scan duration : 335 sec
==========

Reported by NVT "SSH Authorization" (1.3.6.1.4.1.25623.1.0.90022):
No port for an ssh connect was found open.
Hence local security checks might not work.

general/SMBClient

Reported by NVT "SMB Test" (1.3.6.1.4.1.25623.1.0.90011):
OS Version = WINDOWS 5.1
Domain = WORKGROUP
SMB Serverversion = WINDOWS 2000 LAN MANAGER

ssh (22/tcp)

Reported by NVT "Determine OS and list of installed packages via SSH login" (1.3.6.1.4.1.25623.1.0.50282):

This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.

Risk factor : None

general/HOST-T

Reported by NVT "Host Summary" (1.3.6.1.4.1.25623.1.0.810003):

traceroute:10.0.2.15,192.168.12.17
ports:443,1025,445,135,25,139,80

general/CPE

Reported by NVT "CPE Inventory" (1.3.6.1.4.1.25623.1.0.810002):
No CPE identities could be determine