VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Markku Pakka

VIRTUALISOINTI VIRTUALBOX-OHJELMAN AVULLA

Liiketalous ja matkailu

2011

VAASAN AMMATTIKORKEAKOULU
Liiketalouden ja matkailun koulutusohjelma

TIIVISTELMÄ

Tekijä	Markku Pakka
Opinnäytetyön nimi	Virtualisointi VirtualBox-ohjelman avulla
Vuosi	2011
Kieli	suomi
Sivumäärä	48
Ohjaaja	Jarmo Laasanen

Tutkielmassani käsittelen aluksi palvelimia ja niiden tietoturvaa yleisesti, koska palvelinten tietoturva on tärkeää virtualisoitujen käyttöjärjestelmien turvallisuuden ja toimivuuden kannalta. Sen jälkeen siirryn käsittelemään virtualisointia ja sen tulevaisuutta.

Seuraavaksi tutkin VirtualBox-ohjelmaa. Aluksi asennan VirtualBox-ohjelman Windows Vista-koneelle. Sen jälkeen käsittelen VirtualBoxin käyttöliittymää ja asennan Ubuntun virtuaalikäyttöjärjestelmäksi VirtualBoxin avulla.

Sen jälkeen siirryn tarkastelemaan VirtualBoxin käyttöliittymän eri toimintoja (tilannekuvat ja Virtual Media Manager). Lopuksi testaan VirtualBoxin toimivuutta USB muistikorttien kanssa ja analysoin ongelmia, joihin törmäsin VirtualBoxia käyttäessäni. Lisäksi tarkastelen hieman vieraslisäosia, joita testasin VirtualBoxissa.

Avainsanat Virtualisointi, palvelimet, VirtualBox, Ubuntu.

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

ABSTRACT

Author	Markku Pakka
Title	Virtualization with VirtualBox-program
University	University of Applied Sciences
Year	2011
Language	Finnish
Pages	48
Name of Supervisor	Jarmo Laasanen

The aim of this thesis was to study VirtualBox-program. At first this servers and server security were examined on a general level. The security of servers is important for the security and the functioning of the virtualized operating systems. After that virtualization and its future were examined.

Next a program called VirtualBox was studied. First a copy of the VirtualBox program was installed on a Windows Vista computer. After that the user interface of VirtualBox program was discussed and Ubuntu guest operating system was installed using VirtualBox program.

Following that different functions of VirtualBox user interface, snapshots and Virtual Media Manager, were examined. Finally, the functionality of VirtualBox with USB memory sticks and the problems that were encountered using VirtualBox were examined. Some of the observations about guest additions that were tested on VirtualBox were included in the study.

Keywords Virtualization, Servers, VirtualBox, Ubuntu

SISÄLLYS

1. JOHDANTO

1.1 Tutkimusaihe

Tutkielmani käsittelee virtualisointia, palvelimia ja VirtualBox-ohjelmaa. Halusin tutkia virtualisointia ilmaisohjelmien avulla. Valitsin VirtualBox-ohjelman sen hyvän maineen ja mielenkiintoisuuden vuoksi. Koska virtualisointi on tulevaisuudessa oman työni kannalta tärkeää, halusin tutustua erilaiseen ohjelmaan yleisesti käytettyyn VMware-ohjelmaan verrattuna. Erilaiseksi VirtualBoxin tekee lähinnä sen ilmaisuus, toki ko. ohjelmasta kaupallinenkin versio löytyy.

Haluan tutkielmani avulla selvittää, voisiko pieni yritys hoitaa virtualisointinsa ilmaisohjelman avulla vai tuleeko siitä liikaa ongelmia pienyrittäjälle. Tähän ajatukseen ensimmäisen kerran törmäsin opintoihini liittyvässä harjoittelussa, jossa pohdin uusia tapoja työnantajalleni hoitaa yrityksen tietotekniikkaa. Silloin mietin myös mahdollisuuksia hyödyntää virtualisointia, mutta kaupallisten ohjelmien suuret lisenssimaksut olivat este.

Tutkielmassani käsittelen aluksi teoriapainotteisesti palvelimia ja niiden tietoturvaa yleisesti. Palvelinten tietoturva on tärkeää virtualisoitujen käyttöjärjestelmien turvallisuuden ja toimivuuden kannalta. Sen vuoksi tutkin palvelinten tietoturvaa ja se on tutkimukseni kannalta tärkeä aihealue.

Sen jälkeen siirryn käsittelemään virtualisointia ja sen tulevaisuutta. Koska virtualisointi tulee vuosi vuodelta yleistymään, on tärkeää pohtia sen mahdollisia ongelmia ja hyötyjä nyt ja myöhemmin.

Lopuksi siirryn itse VirtualBox-ohjelman asennukseen. Tutkimuksessani asennan VirtualBox-ohjelman Windows Vista-koneelle. Sen jälkeen kerron vähän VirtualBoxin käyttöliittymästä ja asennan Ubuntun virtuaalikäyttöjärjestelmäksi VirtualBoxin avulla. Kuvien ja kuvatekstien avulla tutkimuksen lukijalle selviää helposti eri vaiheet ja ohjeiden avulla on helppo asentaa VirtualBox. Kerron tarkem-

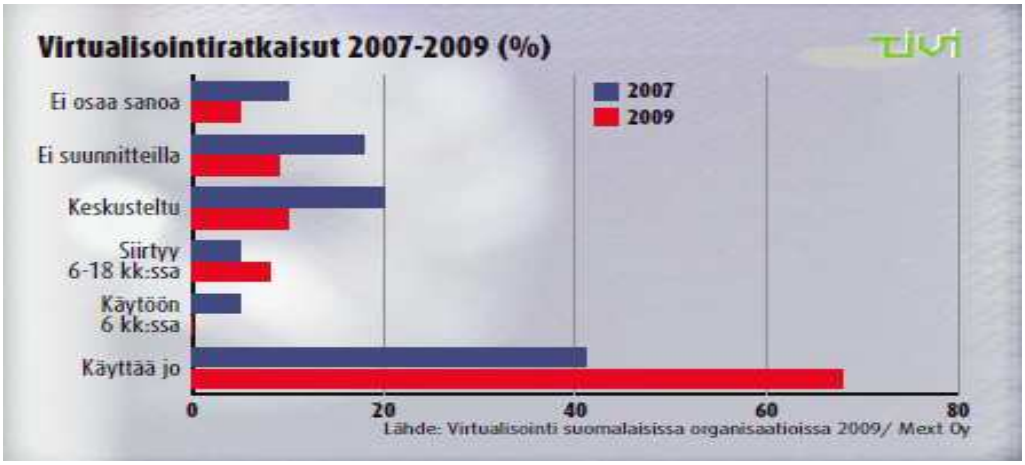
min VirtualBoxin käyttöliittymän eri toiminnoista mm. tilannekuvat (snapshot) ja Virtual Media Manager.

Lopuksi testaan VirtualBoxin toimivuutta USB muistikorttien kanssa ja analysoin ongelmia, joita ilmenee VirtualBoxia käyttäessäni.

1.2 Yleistä virtualisoinnista

Virtualisoinnilla tarkoitetaan yleisesti yhdessä fyysisessä laitteistossa suoritettavaa ohjelmistopohjaista ratkaisua, jonka avulla suoritetaan yhtä aikaa virtuaalisesti yhtä tai useampaa käyttöjärjestelmää. (Pitkänen 2008)

Virtualisointi on kasvava trendi IT- maailmassa. ”Vuonna 2007 vain 41 prosenttia suomalaisista isoista organisaatioista ja yrityksistä ilmoitti käyttävänsä virtualisointia. Tällä hetkellä käyttäjiä on 68 prosenttia organisaatioista ja jopa 75 prosenttia yrityksistä.” (Mäkinen 2009)



Kuva 1. Virtualisointi suomalaisissa organisaatioissa 2009 /Mext Oy. Lähde: Mäkinen 2009

Virtualisointia on ollut käytössä jo pitkän aikaa. Esimerkiksi Windows 95-käyttöjärjestelmässä ajettiin vanhoja MS-DOS-ohjelmia virtuaalisesti. Usein virtualisointia käytetään palvelimissa, mutta levytilan virtualisointi on myös yleistä. (Wikipedia 2010: Virtualization)

Virtualisoinnista on myös hyötyä eri käyttöjärjestelmien ja/tai ohjelmien testauksessa ja myös Internetin selailemisessa. Virtuaalikoneet ovat täysin erillään isäntäjärjestelmästä, joten viruksen tai järjestelmävirheen tapahtuessa on helppoa vain sulkea kyseinen virtuaalikone ja käynnistää uusi virtuaalikone toimivasta tilannekuvasta (Snapshot). (Wikipedia 2010: Virtualization,)

Nykyään palvelinten virtualisoinnin antaessa merkittäviä etuja ajatellaan usein, että asentamalla työasemakäyttöjärjestelmä palvelinten virtualisointiin tarkoitetulle alustalle saavutetaan samat hyödyt myös työasemakäytössä. Työasemavirtualisoinnissa käyttäjällä on toimipisteessään ”kevyt” työasema, joka käyttää konesalissa olevaa työasemakäyttöjärjestelmää. (Rantanen: Virtualisointia kaikkialla)

Kun puhutaan sovellusten virtualisoinnista, tarkoitetaan tapaa, jonka avulla asennettavan sovellutuksen eri komponentit (tiedostot ja rekisteri) ”irroitetaan” käyttöjärjestelmästä (usein Windows). Virtualisoitu sovellus “kopioidaan” työasemaan, jossa se voidaan suorittaa paikallisesti. Sovellusvirtualisointituotteesta riippuen voidaan tarvita tai ei tarvita erillisiä palvelimia.” (Rantanen)

2. PALVELIMET

2.1 Palvelinten tietoturva

Tietoturvan tarkoitus on suojata yksilön tai yhteisön tärkeää tietoa siten, että tietoihin ei pääse käsiksi asiattomat henkilöt tai tahot. Tietoturvan tärkeyttä on lisännyt tiedon sähköistyminen ja Internetin käytön lisääntyminen. Tietoturvan tehtävä on suojata sekä sisäisiä että ulkoisia uhkia vastaan. (Goman 2010: 11–12, Ruohonen 2002)

Uhat voidaan vapaasti luokitella kolmeen ryhmään: tunkeutuminen, palveluestot ja tietovarkaudet. Ulkoisia uhkia ovat luvattomat yhteydet palvelimeen ja verkkoon erilaisia tietoturva-aukkoja hyväksi käyttäen. Tietoturva-aukko voi olla melkein mikä tahansa. Se voi olla esimerkiksi auki oleva portti, heikko salaus tai salasana. Palvelimeen otettua luvatonta yhteyttä voidaan käyttää tiedon keräämiseen palvelimista ja verkosta. Tietoa voidaan käyttää hyväksi ja yrittää päästä käsiksi palvelimella oleviin tietoihin. Tietoliikennettä seuraamalla voidaan teoriassa selvittää käyttäjätunnuksia ja salasanoja keräämällä tietoja palvelimien ja verkon suojauksesta. (Goman 2010: 11–12, Ruohonen 2002)

Luvattomilla yhteyksillä voidaan tiedon keräämisen lisäksi häiritä verkon ja palvelimen toimintaa kuormittamalla verkkoa roskaliikenteellä, jota kutsutaan myös DoS-hyökkäykseksi (Denial Of Service). DoS-hyökkäys on esimerkki palvelunestohyökkäyksestä ja hyökkäyksien takana voi olla yksittäinen henkilö tai ohjelma. (Goman 2010: 11–12, Ruohonen 2002)

Sisäiset uhat ovat samankaltaisia ulkoisten uhkien kanssa, mutta niissä hyökkäys tapahtuu verkon sisältä päin. Sisäinen hyökkäys tarkoittaa siis sitä, että hyökkääjä on fyysisesti kirjautunut tietoverkkoon ja samalla onnistunut kiertämään sisä- ja ulkoverkon väliset palomuurit ja suojaukset. (Goman 2010: 11–12)

Tietoturvan tarkoitus tietojen suojaamiseksi on olla luottamuksellista eli tieto on käytettävissä vain niillä henkilöillä tai tahoilla, joiden kuuluukin tietää asiasta. Tieto ei saa olla muuttunut millään tavalla esim. etäyhteyden aikana. Tietoon ei

voi luottaa, jos sen eheys on vaarantunut. Tieto on oltava helposti ja vaivattomasti oikeiden henkilöiden tai tahojen käytettävissä. Luotettavuus, eheys ja käytettävyys määrittelevät tietoturvan tavoitteet. Lisäksi näitä kolmea tavoitetta voidaan täydentää tarkistamalla kiistämättömyys, tunnistus ja todennus. (Wikipedia: Virtualization)

”Luottamuksellisuutta voidaan parantaa salauksella ja pääsynhallinnalla. Eheyttä edistetään tarkistussummilla, tarkistuskoodeilla ja digitaalisilla allekirjoituksilla. Myös käyttäjän todentaminen ja kiistämättömyys voidaan ainakin jollain tasolla varmistaa digitaalisella allekirjoituksella tai muilla todennustavoilla. Saatavuus edellyttää riittävän tiedonsiirtokapasiteetin varaamista, mikä on toisaalta mahdotonta häirintähyökkäyksenkin edessä.” (Wikipedia: Tietoturva)

Tietoturvasuunnitelman ja riskianalyysien kartoittaminen on hyödyllistä yrityksille. Niiden avulla saadaan selville yrityksen tarpeet ja voidaan määritellä resurssitarpeet paremmin. Tietoturvasuunnitelma koostuu mm. palomuurien, virustorjunnan, käyttäjien koulutuksen ja tietoliikennelaitteiden tarpeellisuus kartoituksesta. Riskianalyysissä tarkastellaan tietoturvauhkien todennäköisyyksiä ja haittoja. Riskianalyysi kartoituksen avulla voidaan paremmin hallita tietoturvan aiheuttamia kuluja ja tietoturvan tason järkevyyttä. (Goman 2010: 11–12, Wikipedia: Virtualization)

2.1.1 Palomuurit

Palomuuri (Firewall) on eristävä moniosainen järjestelmä, jonka tarkoitus on rajata kahden tai useamman verkon välistä liikennettä erilaisin sääntöihin perustuvien tietoturvakäytäntöjen avulla. Palomuuria käytetään suojaamaan avoimesta Internet-yhteydestä tulevia hyökkäyksiä vastaan. Erilaisten sääntöjen avulla voidaan esim. suodattaa sisään tulevista yhteyksistä pois kaikki muu paitsi tarvittava minimi. Useissa yrityksissä suositellaan työntekijöiden koneilta ulospäin lähtevän liikenteen kontrollointia palomuurin avulla tietosuojan turvaamiseksi. Palomuurijärjestelmä koostuu useimmiten kahdenlaisista komponenteista: Pakettisuodatin ja

yhdyskäytävä. Palomuuri saattaa myös vastaanottaa ohjeita tunkeilijan havaitsemisjärjestelmältä estettävästä liikenteestä. (Wikipedia: Palomuuri)

Palomuurien avulla yrityksen sisäverkko pidetään erillään Internetistä. Tietoturva ei ole kunnossa, jos palomuureja ei ole asennettu. Kaikki yrityksen verkossa liikkuva tieto olisi kaikkien saatavilla, jos palomuuria ei olisi rajoittamassa ulko- ja sisäverkon liikennettä. Palomuuri voi olla mm. erillinen laite, palvelin, reititin tai ohjelmisto. Yrityksissä voidaan käyttää näitä kaikkia tai vain joitakin. Pienissä verkoissa, esim. pienyritykset tai kotitaloudet, palomuurina toimivat yleensä ohjelmistopohjaiset palomuurit tai reitittimet. Pienverkkojen turvana voidaan käyttää myös palomuuriksi rakennettuja työasemia. (Wikipedia: Palomuuri, Goman 2010: 11–12)

Pakettisuodatuspalomuurit (packet filtering) ovat tavallisimpia käytössä olevia palomuureja. Pakettisuodatuspalomuureissa pakettivirrasta seulotaan paketit lähde- ja kohdeosoitteen sekä porttien perusteella. Näitä on kahdentyyppisiä, tilattomia (stateless) ja tilallisia (stateful). Tilaton palomuuri vertaa jokaista pakettia säännöstöön; jos paketti ei ole sallittu, sitä ei välitetä eteenpäin. Tilallinen palomuuri mahdollistaa liikenteen tarkemman valvonnan. Tilallinen palomuuri pitää kirjaa muodostetuista TCP-yhteyksistä ja virallisista UDP-yhteyksistä ja sallii vain yhteyteen kuuluvat paketit. TCP-yhteyksillä tutkitaan myös se, että tilasiirtymät ovat laillisia eli käytännössä tilallinen palomuuri pitää yllä samoja tietoja kuin TCP/IP-paketti. (Wikipedia: Palomuuri, Goman 2010: 11–12)

Tilattoman palomuurin ongelma on se, että paluupakettien portteja ei voida kaikissa protokollissa tietää tarkasti, minkä takia esimerkiksi joidenkin verkkopelien toimivuuden vuoksi kaikki portit yli portin 1024 on avattava paluuyhteydelle, jolloin tällä porttialueella olevaan palveluun voidaan ottaa yhteys ilman palomuurin väliintuloa. (Wikipedia: Palomuuri, Goman 2010: 11–12)

Tilallinen palomuuri tarkistaa jokaisen paketin kohdalla kuuluuko se johonkin olemassa olevaan yhteyteen. Olemassa oleviin yhteyksiin liittyvät paketit päästetään läpi. Kun TCP-yhteys avataan, tutkitaan ensin, onko yhteys sallittu palomuu-

rin sääntöjen perusteella. Hyväksytyn yhteyden tiedot lisätään palomuurin yhteyslistaan, ja jatkossa kaikki kyseiseen yhteyteen liittyvät paketit päästetään läpi, samoin myös usein sallitaan yhteyteen liittyvät ICMP-sanomat. Yhteyden sulkeutuessa, tai kun yhteys on ollut käyttämättömänä tietyn ajan, yhteyden tiedot poistetaan yhteyslistalta, eikä kyseiseen yhteyteen kuuluvia paketteja enää päästetä läpi. Tilallisessa palomuurissa on sama ongelma tuntemattomien protokollien kanssa kuin tilattomassakin, mutta siihen voidaan tarvittaessa lisätä sääntöjä tunnettuja protokollia varten. Pakettisuodatin toimii kuljetuskerroksella. (Wikipedia: Palomuuri, Goman 2010: 11–12)

Sovelluspalomuurissa paketin sisältämää dataa tarkkaillaan. Paketin portin ollessa esimerkiksi 25 (SMTP) niin paketista tarkistetaan, sisältääkö se laittomia komentoja. Myös muille palomuurityypeille ongelmallinen aktiivinen FTP toimii tämäntyyppisessä palomuurissa, koska palomuuri lukee avattavan datakanavan portin numeron FTP-komentokanavan sanomasta ja sallii yhteyden siihen. Palomuuri voi myös suodattaa liikennettä sisällön perusteella esimerkiksi estämällä HTTP-paketeista tunnettuja turvallisuusaukkoja hyödyntävät murtoyritykset. Sovelluspalomuuri toimii sovelluskerroksella. (Wikipedia: Palomuuri, Goman 2010: 11–12)

Nykyaikaiset työasemakohtaiset palomuurit ovat useimmiten sovellus- ja tilallisen palomuurin yhdistelmiä, joissa myös sovellus vaikuttaa siihen, sallitaanko jokin yhteys. Perinteisiin palomuureihin erona on, tiedetäänkö tarkkaan mitkä palvelut ovat sallittuja ja mikä liikenne kohdistuu työasemaan. Perinteiset palomuurit joutuvat toimimaan vähempien tietojen perusteella. (Wikipedia: Palomuuri)

”Pakettisuodatusta käyttävillä palomuureilla on kuitenkin heikkoutensa, joten yksinään ne eivät takaa yrityksen tietoturvallisuutta. Internet-liikenne portista 80 on palomuurin näkökulmasta harmitonta, mutta voi pitää sisällään haitallista tietoa. Palomuuriin tulevasta liikenteestä pidetään yllä lokia. Lokitiedostojen avulla voidaan seurata palomuuriin saapuvaa liikennettä hyvinkin tarkasti. Näin palomuurin ylläpito helpottuu. Lokien avulla voidaan paikallistaa esim. tietoliikennelaitteissa olevia viallisia konfiguraatioita.” (Goman 2010: 11–12)

2.1.2 IDS

IDS-järjestelmä (Intrusion Detection System) voi olla palomuurien ohella tietoverkon suojana. IDS-järjestelmällä voidaan tunnistaa alkavia hyökkäyksiä ja toimia ennen kuin hyökkäyksistä koituu vaaraa suojatulle verkolle. (Rantasaari 2003)

IDS-järjestelmä toimii tutkimalla järjestelmän kirjausketjuja. Melkein kaikki järjestelmässä tehtävät toiminnot tallentuvat lokitiedostoihin, mistä voidaan saada selville mahdolliset järjestelmään tehdyt tunkeutumisyritykset. Koska lokitiedostojen koot saattavat olla valtavan kokoisia, niin niiden manuaalisesti tutkiminen ei ole järkevää. IDS-järjestelmä käyttää hyväkseen hyökkäysmalleja, joiden avulla se etsii hyökkäyksen merkkejä lokitiedostoista. IDS-järjestelmän avulla palomuurista läpi pääsevä hyökkäys voidaan huomata. IDS-järjestelmä voidaan konfiguroida esimerkiksi lähettämään sähköpostia verkon ylläpitäjille, jos hyökkäyksen tunnuspiirteet omaava tapahtuma sattuu. (Rantasaari 2003)

2.1.3 Palvelimien virustorjunta

Pelkästään palomuurit ja IDS-järjestelmät eivät riitä palvelimien suojaamiseksi. Palomuurit eivät esimerkiksi suodata pois Internet-liikenteen mukana tulevaa haitallista tietoa tai huomaa saastuneita liitetiedostoja sähköpostissa. Tämän takia palvelimet tarvitsevat virustorjuntaohjelmiston korjaamaan turvallisuusongelman. Esimerkiksi postinsuodatuksen avulla voidaan estää sähköpostin kautta leviäviä haittaohjelmia. Virustorjuntaohjelmat myös tarkistavat käyttäjien tallentamat tiedostot ja Internet-sivut, joissa käyttäjä liikkuu. (Goman 2010: 14–15)

Virustorjuntaa hallitaan yleensä keskitetysti palvelimella toimivan hallintaosan avulla. Hallintaosa määrittää virustorjuntapolitiikat, joita työasemat ja muut palvelimet noudattavat. Keskitetty hallinta parantaa verkon turvallisuutta. Tällöin vaka-

vat virustorjunnat voidaan havaita helpommin ja saastunut kone saadaan pois verkosta normaalia nopeammin. Lisäksi keskitetty hallinta helpottaa virustorjunnan ylläpitoa. (Goman 2010: 14–15)

Haitallista ohjelmaa, joka kopioi itseään, kutsutaan tietokonevirukseksi. Tietokonevirukset leviävät isäntäohjelmien avulla. Tietokonevirus voi saastuttaa ohjelmia, tiedostoja tai minkä tahansa osan tietokoneesta, myös BIOS:in. Virus ei leviä itsekseen, vaan se tarvitsee ulkopuolisen tiedoston. Vaikka virustorjunta kehittyy, uusia ja erilaisia viruksia ilmestyy kiihtyvällä tahdilla lisää. Virukset voivat aiheuttaa suuriakin vahinkoja tietojärjestelmissä. (Goman 2010: 15–16)

Tietokoneviruksia on useita erilaisia mm. tiedostovirukset, tiedostomadot, makrovirukset, käynnistyslohkovirukset ja Troijan hevoset. On olemassa myös viruksia, jotka muuntavat toimintatapaansa isäntäkoneen vaihtuessa. Tällöin niiden tunnistaminen vaikeutuu (ns. polymorphiset virukset). ”Virusten ohjelmointi ei ole kovin vaikeaa, ja jotkut oppilaitokset jopa opettavat virusten laatimista, tarkoituksena opettaa tuntemaan virusten toimintatapoja ja siten vastustamaan niitä.” (Paananen 2003: 329)

Haittaohjelmia on monenlaisia esim. vakoiluohjelmia (Spyware) ja peloitteluohjelmia (Scareware). Vakoiluohjelmilla tarkoitetaan ohjelmia tai tekniikkoja, joiden avulla esin kerätään tietoa kohteesta salaa ja sitten lähetetään tiedot eteenpäin kohteen tietämättä. Peloitteluohjelmilla tarkoitetaan ilmaista hyötyohjelmaa (virustorjuntaohjelmaa tai vastaavaa tietoturvasovellusta), joka on löytävinään käyttäjän koneelta viruksia tai muita haittasovellutuksia. (Järvinen 2010)

Vakoiluohjelmat tasapainottelevat laillisuuden ja hyvän markkinointitavan harmaalla alueella. Vakoiluohjelmia voidaan lisätä toisten ohjelmien mukaan ja ne ovat laajasti käytössä. Vakoiluohjelmien käyttäminen markkinoinnissa ei ole nykyisin laitonta, vaikka se onkin usein epäilyttävää tai moraalisesti arveluttavaa. Vakoiluohjelma yrittää asentaa itsensä käyttäjän koneelle salaa käyttäjältä ja pyrkii myös pysymään salassa. Siitä voi olla maininta jonkin muun asennettavan ohjelman asennuksessa, mutta maininta on hukutettu esim. lisenssitekstin sekaan,

jota käyttäjä ei yleensä lue. Vakoiluohjelma ei yleensä ole haitallinen koneen toiminnan kannalta, koska se ei monista itseään tai aiheuta muuten harmia isäntäkoneelleen. Sen vuoksi, varsinkaan ilmaiset virustorjuntaohjelmat, eivät aina huomaa vakoiluohjelmia. (Kirves 2003, Goman 2010: 16–17)

Palvelimen tietoturvan kannalta vakoiluohjelmat muodostavat selvän uhkatekijän. Vakoiluohjelma saattaa laittaa levitykseen arkaluontoista materiaalia, kuten käyttäjätunnuksia, salasanoja tai muuta vastaavaa. Lisäksi vakoiluohjelman saastuttama käyttäjä yleensä saa sähköpostin välityksellä tulevia mainoksia (eli spammia). (Kirves 2003, Goman 2010: 16–17)

Pelotteluohjelmistojen määrä on lisääntynyt merkittävästi viime vuosien aikana. Pelotteluohjelmalla tarkoitetaan ilmaista hyötyohjelmaa (virustorjuntaohjelma tai vastaava tietoturvasovellus). Pelotteluohjelma on löytävinään käyttäjän koneelta viruksia tai muita haittasovellutuksia. Pelotteluohjelmaa mainostetaan yleensä hyvin aggressiivisesti mm. tuomalla ruudulle ponnahdusvalikko (pop-up) ikkunoita, valeskannauksia ja yritetään pakottaa lataamaan ohjelmaa. Tällöin käyttäjä voi tietoturvauhkien pelossa asentaa pelotteluohjelman. Pelotteluohjelma ei kuitenkaan kerro totuutta löydöistään tai pahimmillaan se saattaa asentaa käyttäjän koneelle löytämänsä virukset ja muut haittatekijät. Ohjelmisto voi myös ilmoittaa käyttäjälle pystyvänsä poistamaan löydetyt haittaohjelmat, jos käyttäjä lataa ohjelmasta maksullisen täyden version. Siten pelotteluohjelmat huijaavat tietoturvauhkien avulla käyttäjää ostamaan maksullisen version ohjelmastaan. Pelotteluohjelman tekijät saavat näin rahaa ja samalla levittävät haitallisia ohjelmiaan. (Kotilainen 2010, Goman 2010: 16–17)

Pelotteluohjelma vaikuttaa tietoturvayhtiö McAfeen mukaan joka päivä ainakin miljoonaan ihmiseen. Kahden viime vuoden aikana pelotteluohjelmien määrä on paisunut kuusinkertaiseksi ja pelkästään viimeisen vuoden aikana ongelma on nelinkertaistunut. McAfeen mukaan rikolliset ovat rakentaneet yli 2900 petollista tietoturvaongelmaa. (Kotilainen 2010)

2.2 Fyysinen tietoturva

Fyysinen tietoturva on yksi tietoturvan peruskivistä. Fyysisen tietoturvan tarkoituksena on varmistaa, ettei kukaan pääse varastamaan esimerkiksi koneita, kovalevyjä tai muita varmuuskopioita. Fyysisen tietoturvan tarkoitus on myös varmistaa, että kukaan ei pääse fyysiseen verkkoon kiinni huomaamatta tai kopioimaan tietoja. Fyysiseen tietoturvaan kuuluu myös olemassa olevan tiedon suojaaminen ulkopuolisilta haitoilta ja myös riskeiltä kuten tulipaloilta ja sähkökatkoksilta. Kun tehdään arviota fyysisestä tietoturvasta, tulee tehdä riskianalyysit eri uhkatekijöiden todennäköisyyksistä ja aiheutuvista haitoista. Riskianalyysin tehtävä on auttaa yritystä kohdentamaan resurssejaan tietoturvan kannalta oikeisiin seikkoihin. (Tietoturvan peruskivet, Goman 2010: 17–19)

Fyysisen tietoturvan toteutumisen kannalta olisi tärkeää, että oikeuksia päästä esimerkiksi palvelintiloihin olisi vain yrityksen tietotekniikkatuella ja yleisenä sääntönä kannattaisi pitää sitä, että jokainen yrityksen työntekijä saa vain ne oikeudet, mitä tarvitsee työnsä tekemiseen. Yrityksen ollessa suljettuna yrityksen tiloja olisi hyvä suojata mm. hälytysjärjestelmällä ja vartioinnilla. Myös ovien avaamisesta olisi hyvä tulla merkintä lokiin kulunvalvonnan seuraamiseksi. (Tietoturvan peruskivet, Goman 2010: 17–19)

Palvelin- ja tiedonvarastointitiloissa on syytä olla hyvät sammutusjärjestelmät. Palvelimet tulisi olla suojattu sähkökatkoksen varalta varavirralla varageneraattorien (UPS) avulla. Tiedostojen varmuuskopiot tulisi säilyttää eri paikassa kuin palvelimet ja alkuperäiset tiedot säilytetään. Varmuuskopiot ja muut tärkeät resurssit kannattaisi laittaa turvaan paloturvallisiin kaappeihin mahdollisten tulipalojen varalta. Toisaalta liiallinen ylilyönti turvallisuudessa ei myöskään ole järkevää. Sen takia riskianalyysin tekeminen on tärkeää ja myös kustannustehokasta. (Tietoturvan peruskivet, Goman 2010: 17–19)

3. VIRTUALISOINTI

Virtualisoinnin määritelmiä löytyy monia. Yhden määritelmän mukaan virtualisointi on tekniikka kätkeä koneen fyysiset ominaisuudet muilta järjestelmiltä, ohjelmistoilta ja loppukäyttäjiltä. Tämä sisältää yhden fyysisen resurssin ilmenemisen useana loogisena resurssina tai se voi sisältää usean fyysisen resurssin ilmenemisen yhtenä loogisena resurssina. Virtualisointi vaatii normaalin ajatustavan muuttamista yrityksissä. Normaali tapa on ollut jo pitkään hankkia uusi fyysinen palvelinlaitteisto aina, kun se on ollut tarpeen. Tietojärjestelmissä on käytetty periaatetta ajaa yhtä palvelinta vain yhtä määrättyä tehtävää varten, esimerkkinä voidaan mainita sähköpostipalvelin, kotisivupalvelin tai tallennuspalvelin. Näin on vältetty ongelmat, joita ohjelmistot voivat aiheuttaa toisilleen. Tämä ajatustapa on luonut melkoiset määrät ylikapasiteettia yrityksiin. Sen vuoksi resursseja on tuhlattu tuottavan työn kustannuksella. (Virtualization overview, Wikipedia: Virtualization)

Virtualisoinnissa joukko fyysisiä resursseja jaetaan loogisiin resurssiosioihin. Palvelinten virtualisoinnin ansiosta voidaan yhdessä fyysisessä palvelimessa ajaa useita eri virtuaalipalvelimia useilla eri käyttöjärjestelmillä. (Virtualization overview, Wikipedia: Virtualization)

Virtualisoinnin avulla palvelimien käyttöastetta pystytään nostamaan korkeammaksi nykyisestä. Virtualisoinnin yleistymisen avaintekijöitä ovat kustannusten laskeminen, erittäin alhaiset palvelinten käyttöasteet ja tarve parantaa hallintaa. Palvelinten vähentäminen virtualisoinnin avulla aiheuttaa suoria säästöjä mm. laitteistoissa, sähkössä, jäähdytyksessä, lattiatilassa ja helpottuneessa asennuksessa sekä ylläpidossa. (Virtualization overview, Wikipedia: Virtualization)

Laitteistotoimittajat ovat kehittäneet valtavasti ominaisuuksia virtualisoinnin helpottamiseen. Yhtenä näistä voidaan mainita prosessorivalmistajien kehittämät laajennukset prosessoriin vain virtualisointia varten. Uusia palvelimia myös myydään sulautetulla virtualisointialustalla, jolloin palvelimen kapasiteetti on helppo lisätä olemassa oleviin resursseihin tai vaihtoehtoisesti koneen kapasiteetti voi-

daan jakaa useaan toisistaan erotettuun lohkoon ja voidaan ajaa useaa eri järjestelmää yhtäaikaisesti yhdessä laitteistossa. (Kris Buytaert, Rogier Dittner, David Rule. 2007:12)

Table 1.2 Benefits of Virtualization

Category	Benefit
Consolidation	Increase server utilization
	Simplify legacy software migration
	Host mixed operating systems per physical platform
	Streamline test and development environments
Reliability	Isolate software faults
	Reallocate existing partitions
	Create dedicated or as-needed failover partitions
Security	Contain digital attacks through fault isolation
	Apply different security settings to each partition

Kuva 2. Benefits of Virtualization. Lähde: Buytaert ym. 2007: 12.

3.1 Virtualisoinnin tulevaisuus

Siinä vaiheessa, kun vanhentuneet ja ikääntyneet laitteet tarvitsevat päivitystä nykyaikaisiin järjestelmiin, on hyvä hetki harkita virtuaaliseen infrastruktuurin siirtymistä. (Buytaert ym. 2007: 33)

Yritykset voivat laskea varmuuskopio järjestelmien hintoja käyttämällä hyväkseen virtualisoinnin hyötyjä. Virtualisointi antaa myös suurempaa joustavuutta ja helpottaa IT-organisaatioiden toimintoja. Virtualisoinnin hyödyt voidaan ulottaa palvelinkeskuksen ulkopuolelle eli käyttäjän työpöydälle. Työpöydän virtualisointi voi auttaa organisaatiota alentamaan kustannuksia ja samalla säilyttämään kontrollin heidän käyttäjien ympäristöstä ja lisätä tietoturvaa ilman ylimääräisiä kustannuksia. (Buytaert ym. 2007: 33)

Virtualisointi on ja tulee olemaan kotonaan ohjelman kehitys syklissä. Sen kaltaiset teknologiat auttavat kehitystyössä, testauksessa, julkaisussa ja prosessissa samalla nostaen tuloksellisuutta ja lyhentäen aikaväliä suunnittelusta myyntiin. (Buytaert ym. 2007: 33)

3.2 Virtualisointi palvelimissa

Virtualisointia käytetään useaan eri tarkoitukseen. Yleisimmät käytetyt tekniikat ovat alusta-, resurssi-, sovellus- ja työpöytävirtualisointi. Alustavirtualisointi jaetaan kolmeen osaan, käyttöjärjestelmävirtualisointiin, paravirtualisointiin ja laitteistovirtualisointiin. (Virtualization overview, Wikipedia: Virtualization)

Käyttöjärjestelmävirtualisoinnilla tarkoitetaan sitä, että virtualisointirajapinta sijoitetaan käyttöjärjestelmän ja virtualisoitujen palvelujen väliin. Resursseja voidaan partitioida useille palveluille samanaikaisesti virtualisointirajapinnan avulla. Virtualisointirajapinta huolehtii eri virtuaaliympäristöjen ylläpidosta, eristyksestä ja luo virtuaalipalvelimelle näkymän yhdestä palvelimesta, kuitenkin jakaen taustalla sijaitsevan isäntäkoneen ytimen yhteiset resurssit. (Virtualization overview)

Laitteistovirtualisoinnissa virtualisointirajapinta asettuu fyysisen palvelimen ja virtualisoitujen vieraskäyttöjärjestelmien väliin. Virtualisointirajapinta näkyy vieraskäyttöjärjestelmälle fyysisenä laitteistona. Laitteistovirtualisoinnissa ei käytetä isäntäkäyttöjärjestelmää fyysisen laitteiston avulla, vaan käyttöjärjestelmä asennetaan virtuaaliohjelmiston mukana. Laitteistovirtualisointi tarjoaa suoran pääsyn isäntäkoneen resursseihin vähentäen yhteensopivuusongelmia isäntäkoneen laitteiston kanssa, tuoden prosessien suorittamiseen nopeutta ja parantaen yleistä käyttövarmuutta. (Virtualization overview)

Paravirtualisointi (avustettu virtualisointi) on tilanne, jossa palvelun suunnittelussa otetaan huomioon, että sitä tullaan ajamaan virtuaaliympäristössä. Paravirtu-

alisoinnin avulla isäntäkäyttöjärjestelmä ja vieraskäyttöjärjestelmä keskustelevat keskenään nopeammin. Paravirtualisointi tarjoaa potentiaalisia suorituskyvyn parannuksia, mutta tämä virtualisointimalli vaatii, että pääkäyttöjärjestelmä on erityisesti modifioitu toimimaan vieraskäyttöjärjestelmien kanssa. (Virtualization overview, Wikipedia: Virtualization)

4. VIRTUALISOINTI VIRTUALBOX -OHJELMAN AVULLA

VirtualBox-ohjelman voi hakea osoitteesta: www.virtualbox.org/download.

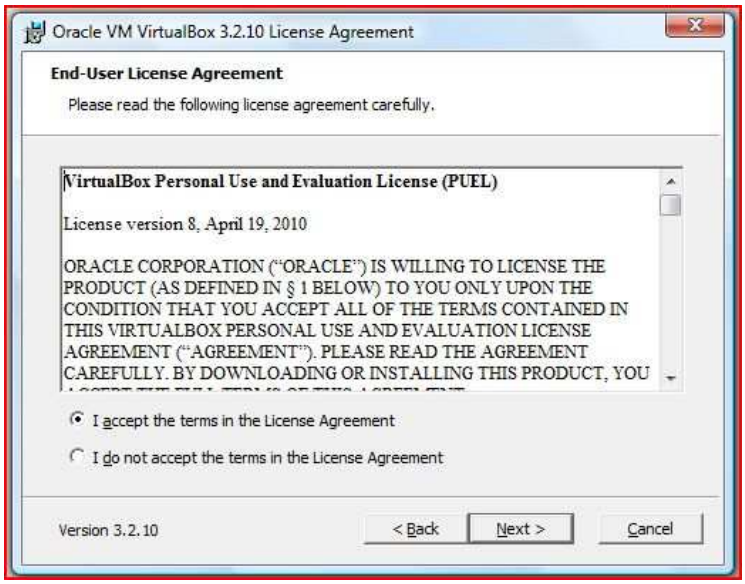
VirtualBox on ilmainen (siitä on olemassa myös kaupallinen versio) ja tämän käyttämäni ohjelman versio on 3.2.12 (tällä hetkellä uusin versio). VirtualBox on ulkoasultaan samankaltainen VMware Workstationin kanssa ja käytettävissä olevat toiminnotkin ovat samankaltaisia, joten VMwaren käyttäjät oppivat nopeasti käyttämäään VirtualBoxia. VirtualBox on käännettynä usealle eri kielelle(myös suomeksi), mutta käytännön syistä en ryhtynyt suomenkielisen version tarkastelua tekemään vaikka se olisikin helpottanut paljon.

4.1 Asennus

Ohjelman asennuksen aikana ruudulle tulee monta erilaista ikkunaa, jotka vaativat käyttäjän huomiota.

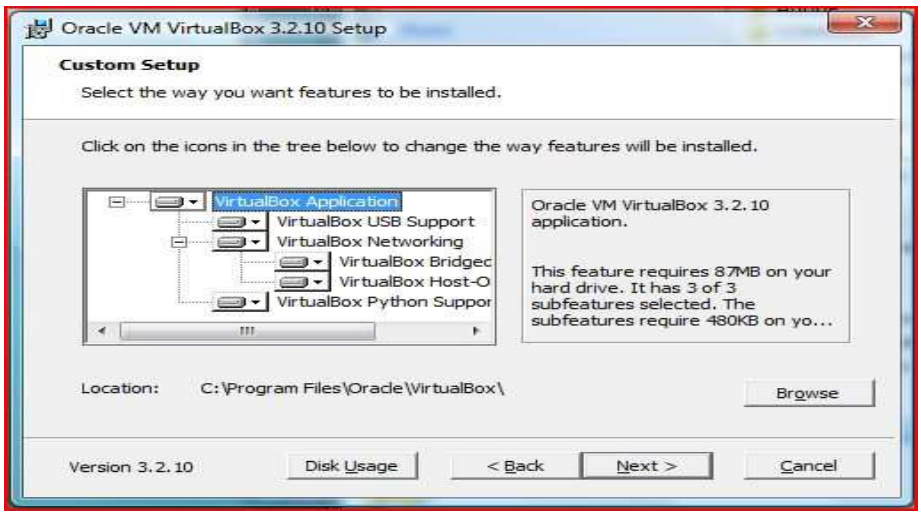
Kuva 3. Asennuksen alku.

Käyttäjältä kysytään hyväksyntää käyttöehdoista. Koska en ymmärtänyt puoliakaan käyttöehtojen asioista tein niin kuin suurin osa muista käyttäjistä eli hyväksyin käyttöehdot niitä suuremmin miettimättä. Asennus ei edisty, jos käyttäjäehtoja ei hyväksytä.



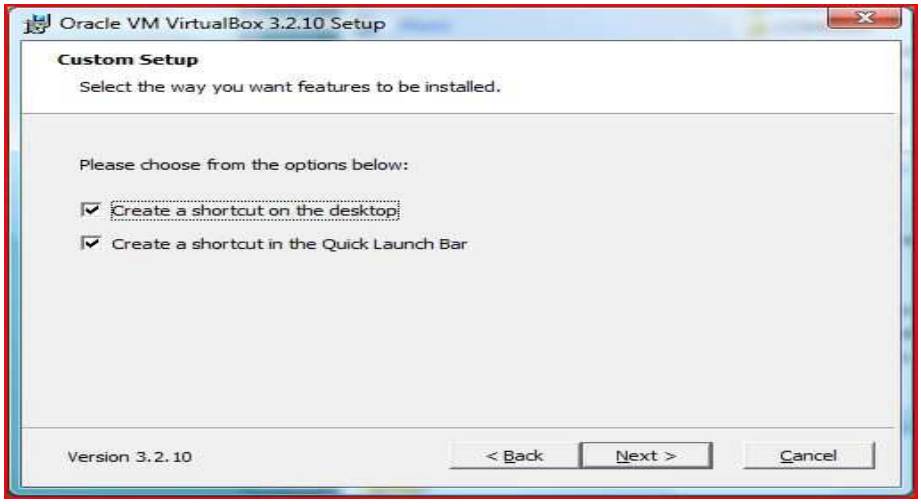
Kuva 4. Käyttäjäehdot.

Käyttäjäehtojen hyväksymisen jälkeen asennusohjelma kysyy, mitä ominaisuuksia asennetaan. Asensin VirtualBoxin antaman ehdotuksen mukaisesti kaikki, mitä oli valittavana eli oletusarvoisen asennuksen. Edistyneemmät käyttäjät varmasti olisivat tehneet toisin, mutta käytännön syistä päädyin asentamaan oletusasetuksien mukaisesti ohjelman.



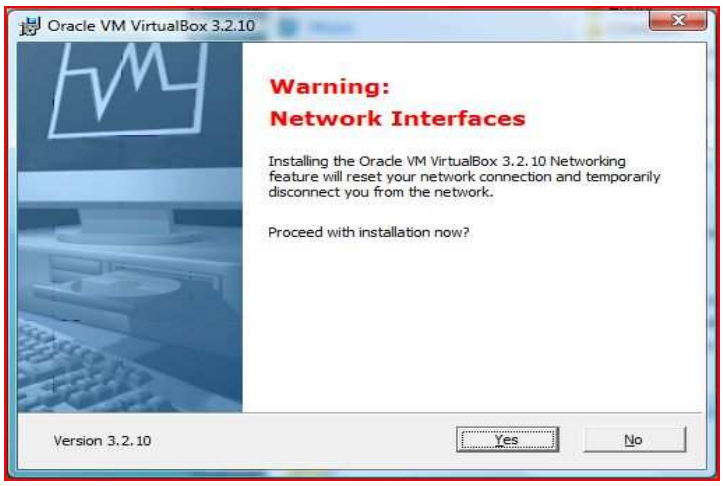
Kuva 5. Asennusvaihtoehdot.

Asennusohjelma myös kysyi pikakuvakkeiden asennuksesta.



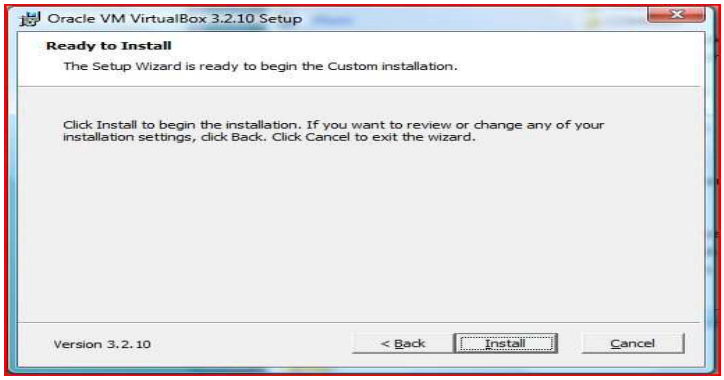
Kuva 6. Pikakuvakkeet.

Tämän jälkeen ohjelma alkoi asentaa verkkoajureita.



Kuva 7. Verkkoajureiden asennus.

Itse asennus alkoi kaikkien asetuksien valitsemisen jälkeen.



Kuva 8. Asennuksen alkaminen.

Asennuksen aikana asennusohjelma kysyi Windows Vistassa neljä eri kertaa ajureiden asentamisen hyväksymisestä. Koska asensin ohjelman oletusarvojen mukaan, niin hyväksyin ajureiden asennuksen.

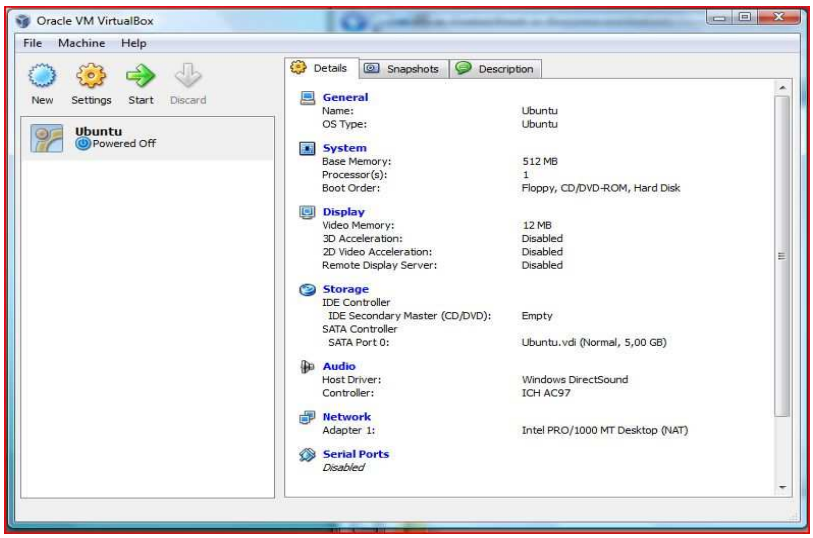
Kuva 9. Ajureiden asennus.

Asennuksen valmistuttua olikin aika käynnistää itse ohjelma.

Kuva 10. Asennuksen valmistuminen.

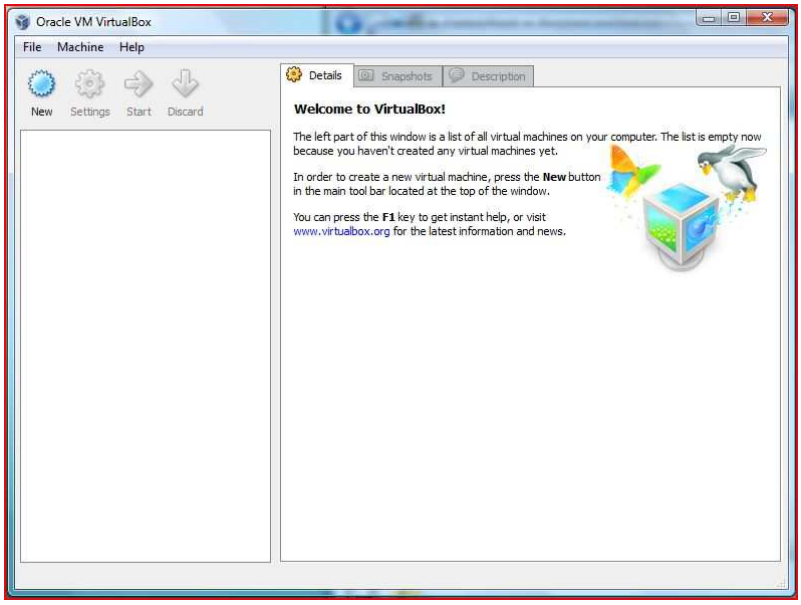
4.2 VirtualBoxin käyttöliittymä ja käyttöjärjestelmän asennus

VirtualBoxin käyttöliittymän saa näkymään monella eri kielellä, mutta itse valitsin käytössä olevaksi kieleksi englannin. VirtualBoxin käyttöliittymä on hyvin samankaltainen esimerkiksi VMware Playerin käyttöliittymän kanssa.



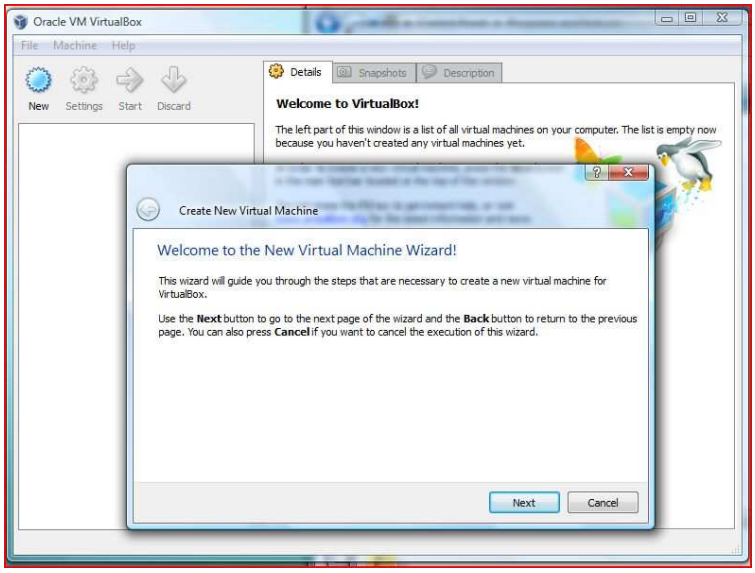
Kuva 11. VirtualBoxin käyttöliittymä.

Päätin aloittaa käyttöliittymän asennuksen ja valitsin käyttöjärjestelmäksi Ubuntun. Uuden käyttöjärjestelmän asennus aloitetaan painamalla ”New” nappulaa. Myös Virtual Media Manageria olisi voinut käyttää uuden käyttöjärjestelmän asennuksessa.



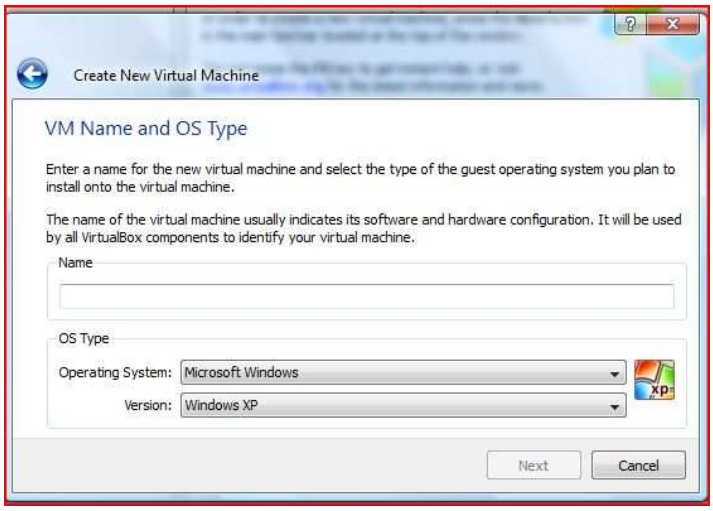
Kuva 12. Käyttöjärjestelmän asennus.

Uuden käyttöjärjestelmän asennusta helpottamaan VirtualBoxissa on ohjattu asennustoiminto, joka avustaa käyttöliittymän asennuksessa.



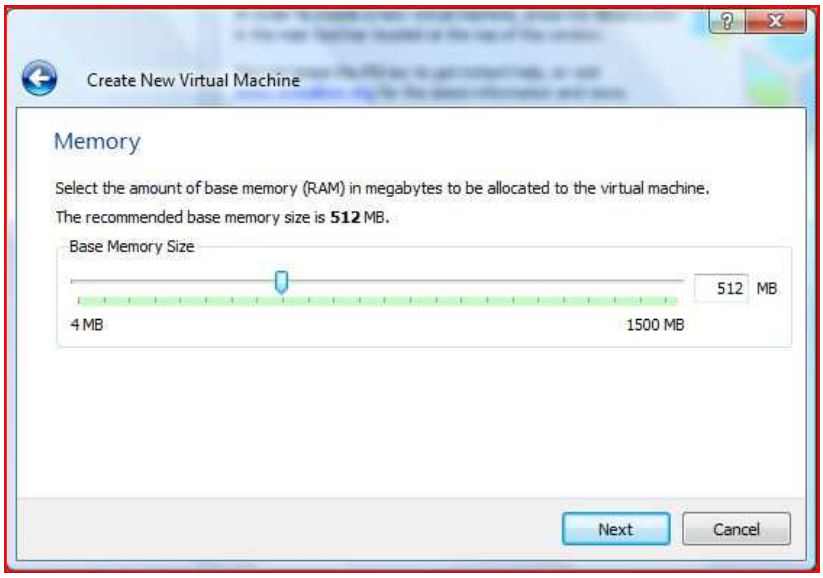
Kuva 13. Käyttöjärjestelmän asennusvelho kuva 1.

Käyttöjärjestelmän asennusohjelma kysyy aluksi, minkä nimen käyttöjärjestelmälle annetaan ja mikä on käyttöjärjestelmän ja version nimi.



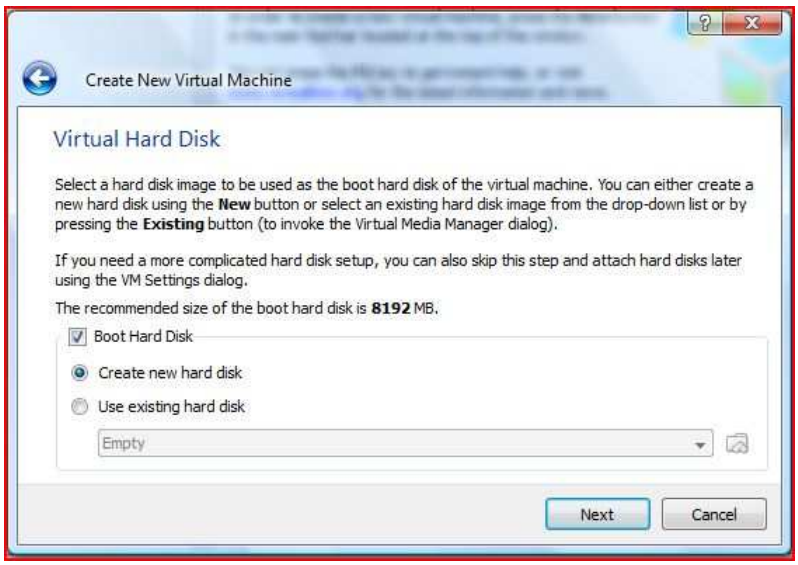
Kuva 14. Käyttöjärjestelmän asennusvelho kuva 2.

Seuraavaksi käyttöjärjestelmän asennusohjelma kysyy, kuinka paljon virtuaalisen käyttöjärjestelmän käyttöön annetaan muistia. Valitsin oletusarvon 512MB muistia virtuaalisen käyttöjärjestelmän käyttöön, koska halusin testata käyttöjärjestelmän toimivuutta pienillä muistimäärillä.



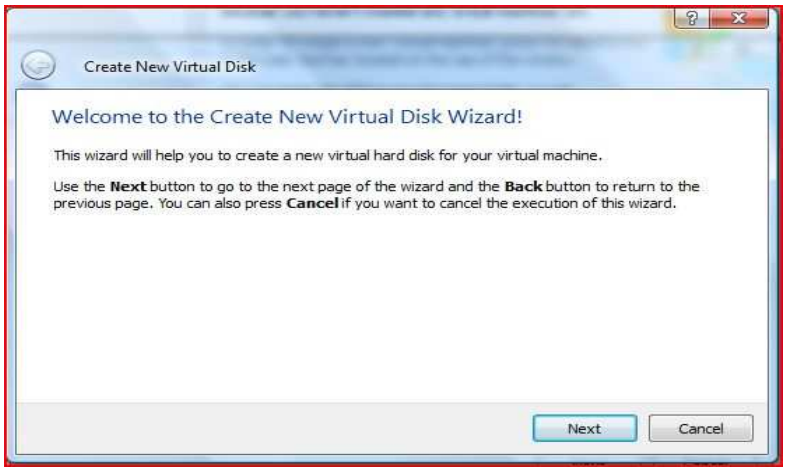
Kuva 15. Käyttöjärjestelmän käytössä olevan muistin määrä.

Seuraavaksi käyttöjärjestelmän asennusohjelma halusi tietää käyttöjärjestelmälle tarkoitetun virtuaalisen kiintolevyn tietoja eli onko kyseessä käynnistyslevy vai ei ja onko kyseinen virtuaalinen kiintolevy jo olemassa.



Kuva 16. Käyttöjärjestelmän kiintolevyn valinta.

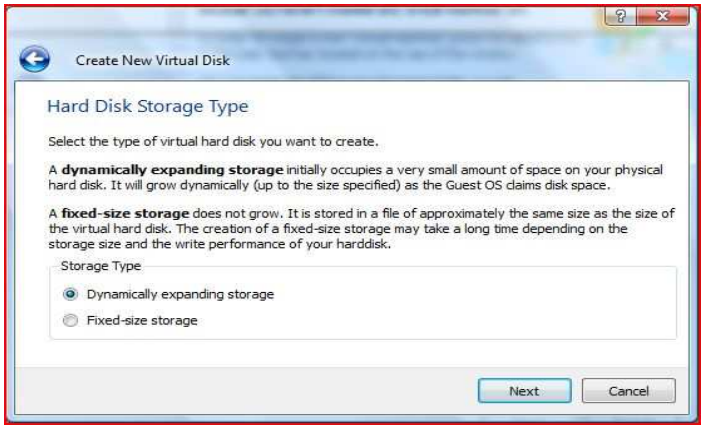
Valitsin uuden kiintolevyn asennuksen, jonka jälkeen ohjelma alkoi kysellä uuden kiintolevyaseman tietoja.



Kuva 17. Kiintolevyn luontivelho.

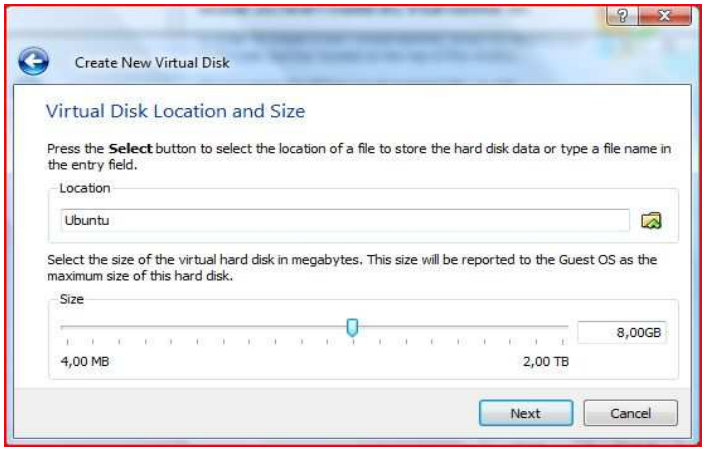
Vaihtoehtona kiintolevyn tyypistä oli ”dynaamisesti kasvava tallennustila” tai ”valmiiksi määritelty tallennustila”. Valitsin dynaamisesti kasvavan tallennustilan,

koska mieluummin annan kiintolevytilaa virtuaalisen käyttöjärjestelmän käyttöön mahdollisimman vähän.



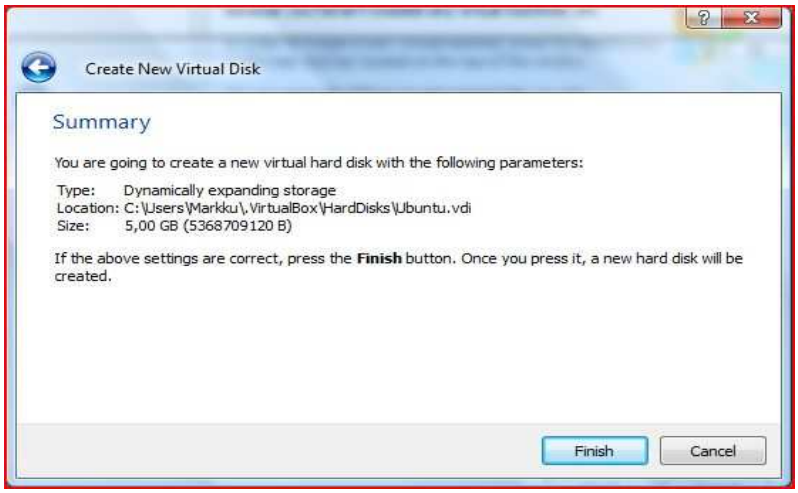
Kuva 18. Kiintolevyn tyyppi.

Tämän jälkeen alkoi käyttöjärjestelmälle varatun kiintolevytilan koon määrittäminen.



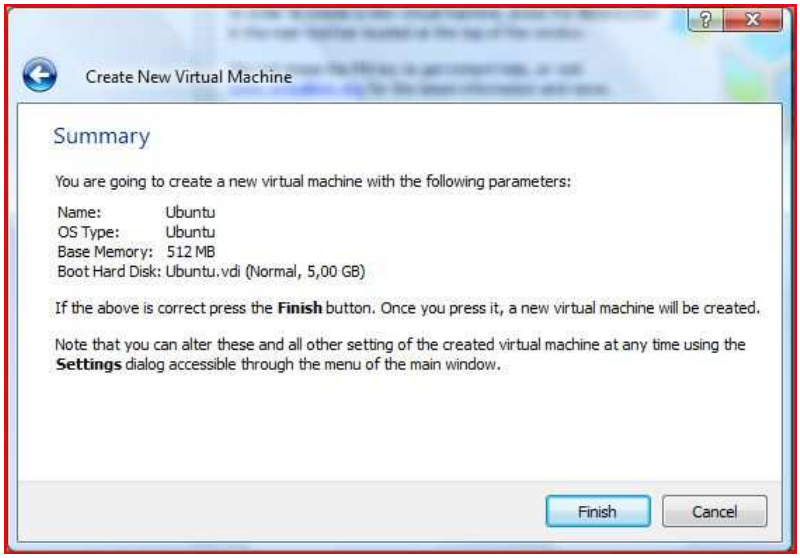
Kuva 19. Kiintolevyn koon määrittäminen.

Asennusohjelma pyysi vielä varmistamaan, että kiintolevystä annetut tiedot olivat oikeita.



Kuva 20. Käyttöjärjestelmän asennus ja kiintolevyn koko.

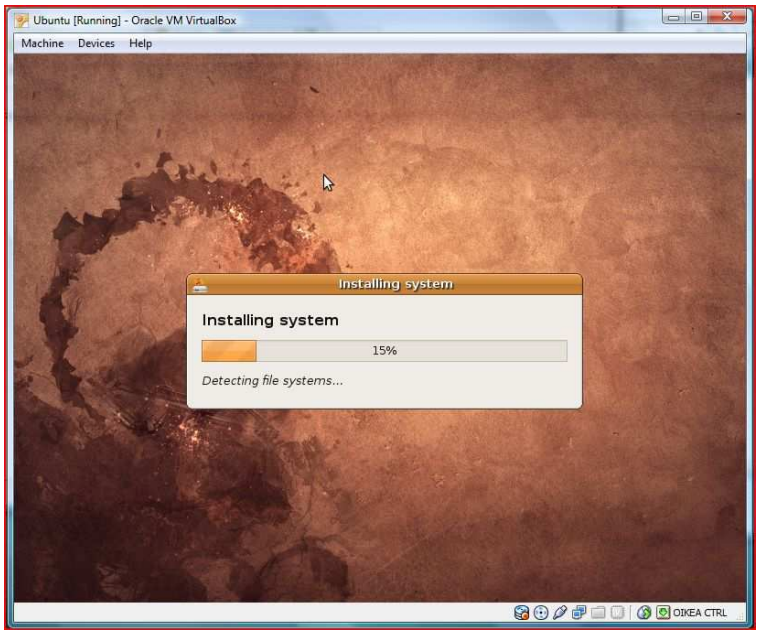
Lopuksi käyttöjärjestelmän asennusohjelma näytti yhteenvedon kaikista annetuista tiedoista, ennen kuin uuden virtuaalisen koneen luominen alkoi.



Kuva 21. Virtuaalisen koneen asennus.

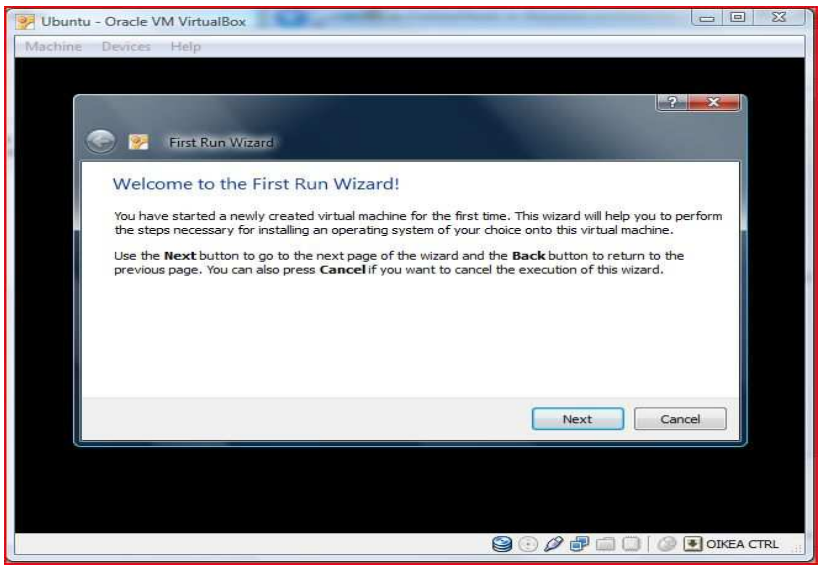
4.3 Ubuntun asennus

Itse Ubuntun asennus alkoi ihan normaalisti. Asensin Ubuntun oletusasetuksilla, mutta itse asennusvaiheessa Vistan virransäästöominaisuudet aiheuttivat muutaman kerran asennuksen epäonnistumisen ja VirtualBox-ohjelman kaatumisen sen myötä. Koska asensin kannettavalle tietokoneelle kyseistä käyttöjärjestelmää, en tarkemmin puuttunut virransäästöominaisuuksien aiheuttamaan ohjelman kaatumiseen. Pöytäkoneessa tapahtuneessa VirtualBoxin avulla uuden virtuaalisen käyttöjärjestelmän asennuksessa ei vastaavia ongelmia tullut eteen.



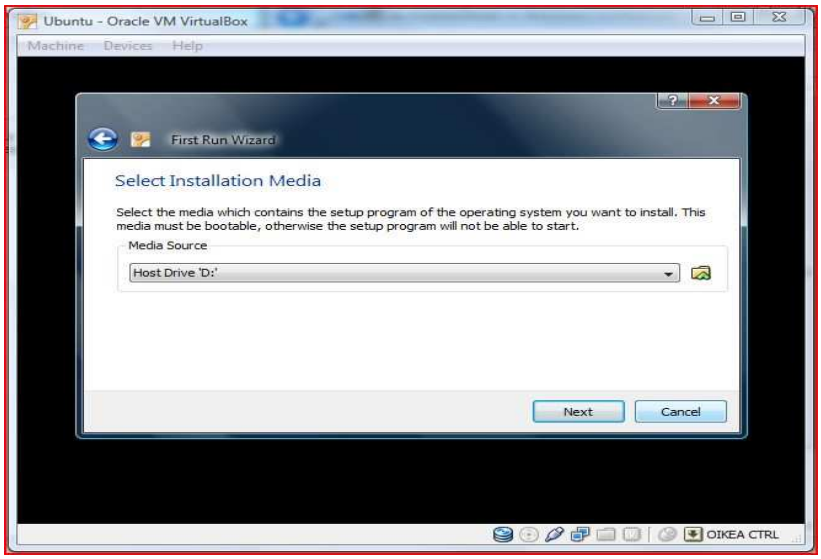
Kuva 22. Ubuntun asennus kuva.

Asennusohjelma kysyi uuden käyttöjärjestelmän asentamisen aikana, mistä asennettava käyttöjärjestelmä löytyy.



Kuva 23. Käyttöjärjestelmän asennus kuva.

Asennusohjelman sijainnin valinta oli helppoa, koska käytössäni oli Ubuntu-käyttöjärjestelmän sisältävä CD-levy (tosin kyseinen CD sisälsi vanhan 8.1 versi-on).

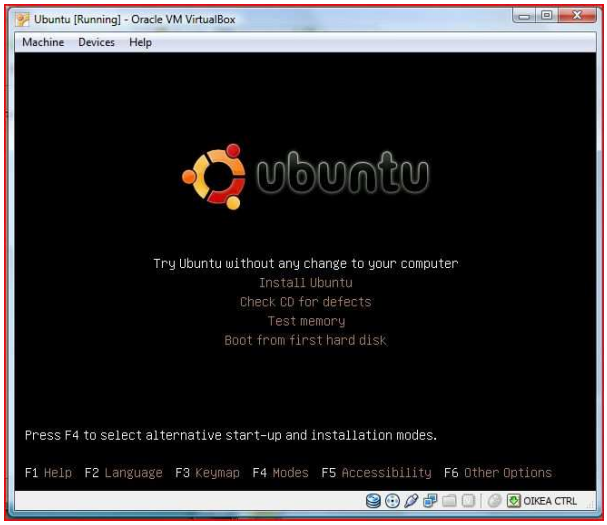


Kuva 24. Asennettavan käyttöjärjestelmän sijainnin määrittely.

Ubuntun asennusohjelma kysyi asennusohjelman kieliasetuksia aluksi. Koska käytössäni oli englanninkielinen Windows Vista, päätin asentaa Ubuntun englannin kielellä.

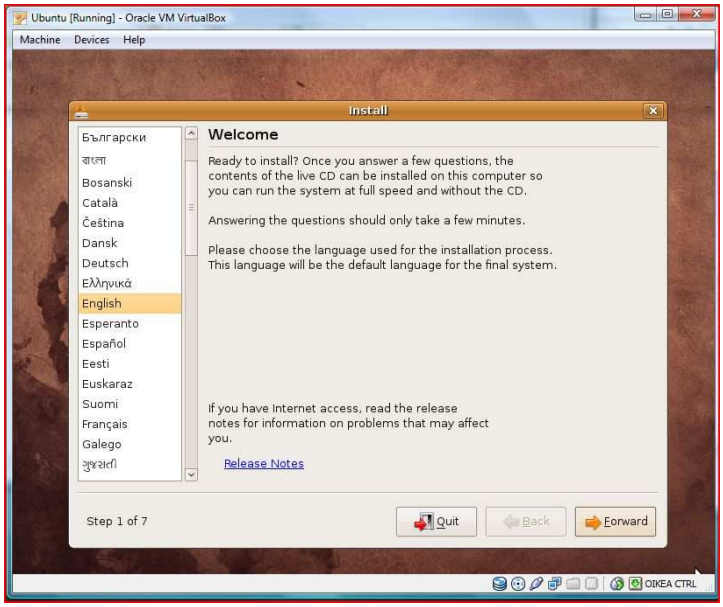
Kuva 25. Ubuntun asennus, kielimäärittely.

Kieliasetuksien määrittelyn jälkeen ohjelma kysyi tarkemmin, millaisen version Ubuntusta halusin asentaa. Valitsin täyden version asennuksen ”Install Ubuntu”.



Kuva 26. Ubuntun asennus valikko.

Tämän jälkeen asennusohjelma kysyi vielä Ubuntu-käyttöjärjestelmän käyttämän kielen.

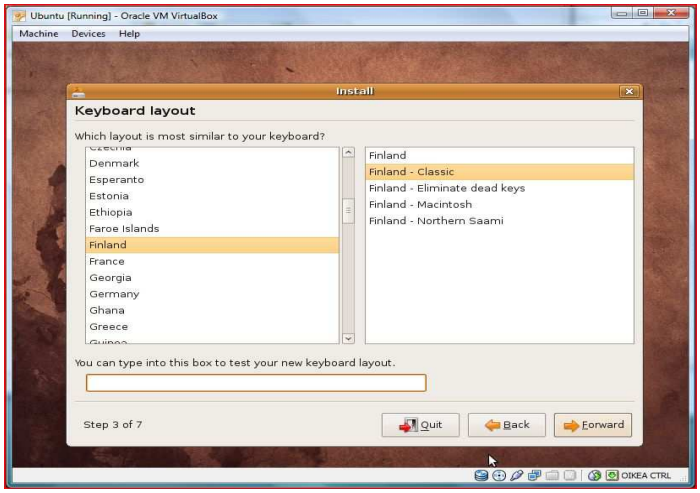


Kuva 27. Ubuntu-käyttöjärjestelmän kieliasetukset.

Seuraavaksi olikin vuorossa aikavyöhykkeen ja sijainnin määrittely. Valitsin sijainniksi Helsinki, Finland ja ohjelma osasi itse määrittää aikavyöhykkeen.

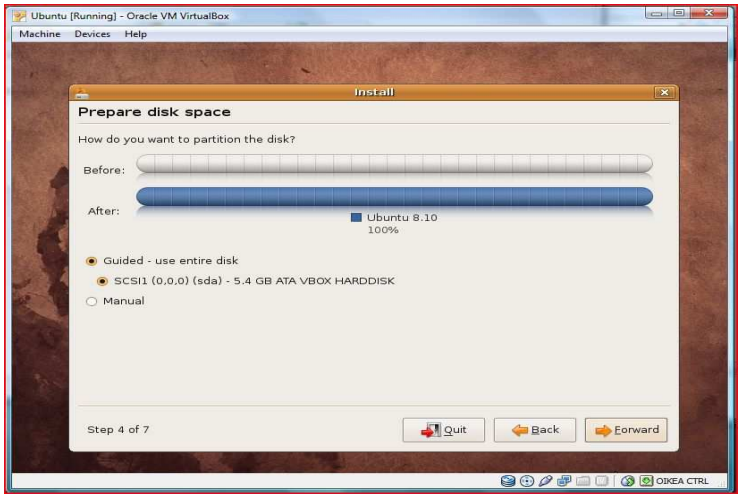
Kuva 28. Ubuntu käyttöjärjestelmän aikavyöhykkeen määrittely.

Aikavyöhykkeen määrittämisen jälkeen asennusohjelma kyseli käytettävissä olevan näppäimistön tietoja.



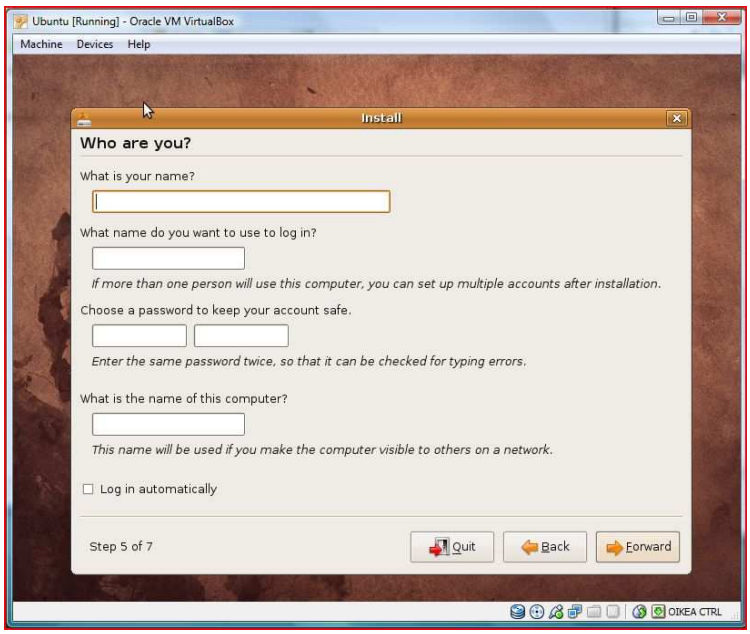
Kuva 29. Ubuntun näppäimistön asetuksien määrittely.

Näppäimistön asetuksien määrittelyn jälkeen alkoikin käyttöjärjestelmän käyttämän kiintolevytilan asetuksien määrittely.



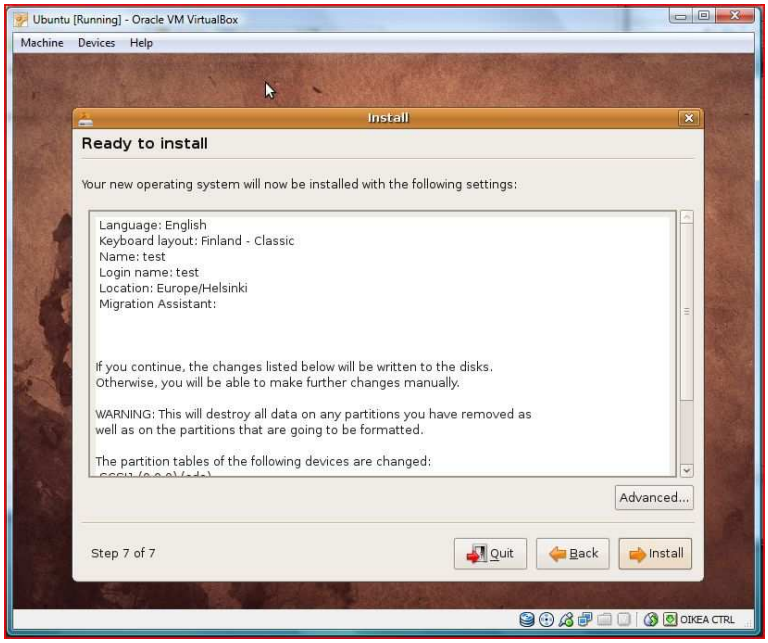
Kuva 30. Ubuntu – käyttöjärjestelmän kiintolevyn käytön määrittely.

Käyttäjätietojen ja salasanan määrittely olikin seuraavaksi vuorossa, tässä vaiheessa kyseessä on pääkäyttäjän tietojen ja salasanan määrittely, eli piti olla tarkkana, että kirjoitti itselle ylös tiedot (käyttäjätunnus ja salasana).



Kuva 31. Ubuntun käyttäjätietojen ja salasanan määritys.

Seuraavaksi tulikin yhteenveto määritellyistä asetuksista, jonka jälkeen itse asennus pääsi alkamaan.

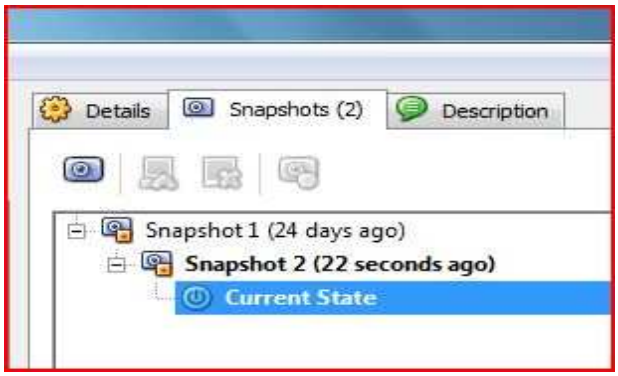


Kuva 32. Ubuntun asennustietojen yhteenveto.

Käyttöliittymän asennuksen jälkeen olikin aika siirtyä tilannekuvan (snapshot) tekoon.

4.4 Tilannekuva (Snapshot)

Käyttöjärjestelmän asentamisen jälkeen kannattaa ottaa toimivasta kokoonpanosta tilannekuva (snapshot).



Kuva 33. Snapshot kuva 1.

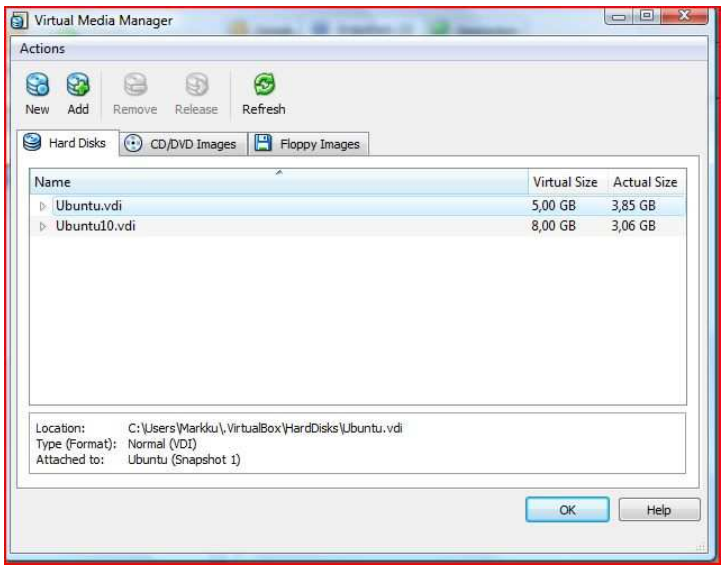
Toimivan edellisen tai vanhemman kokoonpanon pystyy vikatilanteessa palauttamaan tilannekuvan avulla. Tosin, jos ei ole otettuna tilannekuvia vanhemmasta kokoonpanosta, se ei aina ole mahdollista.

Kuva 34. Snapshot kuva 2.

Snapshot-välilehdessä olevilla 4 painikkeilla voidaan tehdä uusi tilannekuva, palauttaa tilannekuva, poistaa tilannekuva ja näyttää tilannekuvan tiedot.

4.5 Virtual Media Manager

VirtualBoxissa on myös ohjelma nimeltä Virtual Media Manager uusien virtuaalisien kiintolevyjen ja vanhojen virtuaalisten käyttöjärjestelmien tuomiseen käytettäväksi. Virtual Media Managerista käy myös ilmi dynaamisesti kasvavien virtuaalikiintolevyjen käyttämä tila, oikeasti virtuaalikiintolevyjen käytössä oleva tila ja muita asioita.



Kuva 35. Virtual Media Manager.

Virtual Media Managerin ehkä tärkein toiminto mielestäni on kuitenkin virtuaalisen käyttöjärjestelmän tarvitseman oikean kiintolevytilan näyttäminen ja vertaus tilannekuvien (snapshot) käyttämään kokoon. On hyvä tietää, kuinka paljon virtuaalisen käyttöjärjestelmän kiintolevytilavaatimukset ovat eri tilannekuvien (snapshot) aikana muuttuneet.

5. VIRTUALBOXIN TOIMIVUUDEN TESTAUS

5.1 VirtualBox ja USB-muistit

VirtualBoxin ilmaisversion tuki USB-muisteille ja muistitikuille on aika olematon, välillä virtualisoitu käyttöjärjestelmä (Ubuntu) tunnistaa USB-muistitikun ja välillä ei. Vaikka muistitikku näyttäisikin toimivan oikein, sitä ei aina pysty silti käyttämään.

Uuden muistitikun toimivuus VirtualBoxissa on epävarmempaa kuin vanhemman muistitikun. Ilmaisversion tuki onkin enimmäkseen suunnattu vanhojen muistitikkujen toimivuutta ajatellen.

Kaupallisessa versiossa USB -muistien tuki on ilmoitettu tuetuksi ominaisuudeksi.

USB -muistin voi saada toimivaksi avaamalla VirtualBox -ohjelman valikon suraavasti:

> Machine → Settings → USB → Add new empty filter → OK → käynnistämällä käyttöjärjestelmän → Laittamalla USB -muistin koneeseen kiinni ja vastaamalla velho (Wizard) ohjelman kysymyksiin. → antaa ohjelman hakea ajurit ja asentaa ne → ottamalla USB -muistin irti koneesta → käynnistämällä uudelleen käyttöjärjestelmän → laittamalla USB -muistin kiinni koneeseen ja USB -muisti pitäisi olla tunnistettuna.

5.2 VirtualBoxin ongelmat

Kannettavalla tietokoneella VirtualBoxin käyttö on epävarmaa. Milloin tahansa VirtualBox:in käynnistämä käyttöliittymä saattaa kannettavan tietokoneen mennessä virransäästötilaan lakata toimimasta.

VirtualBox:ia käyttäessä kannettavassa tietokoneessa kannattaakin siis laittaa VirtualBox:in käytön ajaksi virransäästöominaisuudet mahdollisimman myöhään käynnistyviksi tai pois päältä. Virtalähteen ollessa kiinni kannettavassa tietokoneessa virransäästöominaisuuksien pois päältä laittaminen ei aiheuta suuria ongelmia, mutta kannettavan ollessa poissa verkkovirrasta virransäästöominaisuuksien pois päältä laittaminen saattaa aiheuttaa ongelmia virran keston kanssa.

5.3 VirtualBoxin vieraslisäosat

VirtualBoxin asennuksen jälkeen on hyvä myös asentaa virtualisoituun käyttöjärjestelmään vieras lisäosia (Guest additions). Vieraslisäosat tuovat parannuksia virtualisoidun käyttöjärjestelmän käyttöön.

Vieraslisäosia ovat: hiiren kohdistimen integrointi, jaetut kansiot, parempi näyttö tuki, saumattomat ikkunat, geneeriset isäntä/vieraskommunikointikanavat, ajan synkronisointi, jaettu leikepöytä, automaattiset kirjautumiset. (VirtualBox Manual: Chapter 4. Guest Additions)

5.3.1 Jaetut kansiot

Jaetut kansiot toiminnon avulla voidaan käyttää isäntäkäyttöjärjestelmän tiedostoja vieraskäyttöjärjestelmästä. Tämä on samankaltainen verkkojaon kanssa Windows-verkossa paitsi, että jaetut kansiot eivät vaadi verkkoa, ainoastaan vieraslisäosan. Jaetut kansiot on tuettuna Windows- (2000 tai uudempi), Linux- ja Solaris-vieraskäyttöjärjestelmissä. Jaetun kansion täytyy fyysisesti sijaita isäntä ko-

neella ja olla jaettuna vieras käyttöjärjestelmälle joka käyttää erityistä tiedostojärjestelmä ajuria vieraslisäjärjestelmissä isäntäjärjestelmän kanssa keskusteluun. Windows vierasjärjestelmille jaetut kansiot on tehty pseudo-verkko uudelleenohjauksella, Linux ja Solaris vieraskäyttöjärjestelmissä vieraslisäosat hankkivat virtuaalisen tiedostojärjestelmän. (VirtualBox Manual)

5.3.2 Laitekiihdytetyt grafiikat (OpenGL ja Direct3D 8/9)

VirtualBox vieras lisäosissa on kokeellinen laitteisto 3D tuki Windows, Linux ja Solaris vieraskäyttöjärjestelmille.

Tämän ominaisuuden avulla, jos sovellus virtuaalisen käyttöjärjestelmän sisällä käyttää 3D-ominaisuuksia OpenGL tai Direct3D 8/9 ohjelmointi rajapintojen kautta, eikä emuloi niitä ohjelmiston kautta (mikä voi olla hidasta), VirtualBox yrittää käyttää isäntäkäyttöjärjestelmän 3D-laitteistoa. Tämä toimii kaikissa tuetuissa isäntäalustoissa (Windows, Mac, Linux, Solaris), mikäli isäntäkäyttöjärjestelmä voi käyttää kiihdytettyä 3D-laitteistoa alun perin. (VirtualBox Manual)

3D-kiihdystys on ainoastaan saatavilla tietyissä Windows-, Linux- ja Solaris-vierasjärjestelmissä.

1. Windows vierasjärjestelmän 3D-kiihdytys vaatii Windows 2000, Windows XP, Vista tai Windows 7. OpenGL ja Direct3D 8/9 (ei Windows 2000 kanssa) on tuettu (kokeellinen).

   OpenGL Linuxissa vaatii kernel 2.6.27 tai uudemman sekä X.org serverin versio 1.5 tai uudemman. Ubuntu 10.10 ja Fedora 14 on testattu ja toettu toimiviksi.

   OpenGL Solaris vieraskäyttöjärjestelmillä vaatii X.org serveriversion 1.5 tai uudemman.

2. Vieraslisäosat täytyy olla asennettuna.

3. Koska 3D tuki on vielä kokeellinen, se on poissa päältä oletusasetuksena ja se täytyy käsin laittaa päälle VM-asetuksista (VirtualBox Media Manager → Machine → Settings → Display → rasti ruutuun Enable 3D Acceleration)

Teknisesti VirtualBox toteuttaa tämän asentamalla lisälaitteistoa 3D-ajureihin vieraskäyttöjärjestelmään, johon vieraslisäosat on asennettu. Tämä ajuri toimii laitteisto 3D-ajurina ja raportoi vieraskäyttöjärjestelmälle, että virtuaalinen laitteisto pystyy 3D laitteistokiihdytykseen. Kun sovellus vieraskäyttöjärjestelmässä pyytää laitteiston kiihdytystä OpenGL- tai Direct3D-ohjelmointiliitännältä, nämä pyynnöt lähetetään isäntäkäyttöjärjestelmälle erityisen kommunikaatiotunnelin kautta. Tämän tunnelin on VirtualBox toteuttanut ja isäntätietokone suorittaa pyydetyn 3D-operaation isäntäkoneen ohjelmointiliitäntöjen kautta. (VirtualBox Manual)

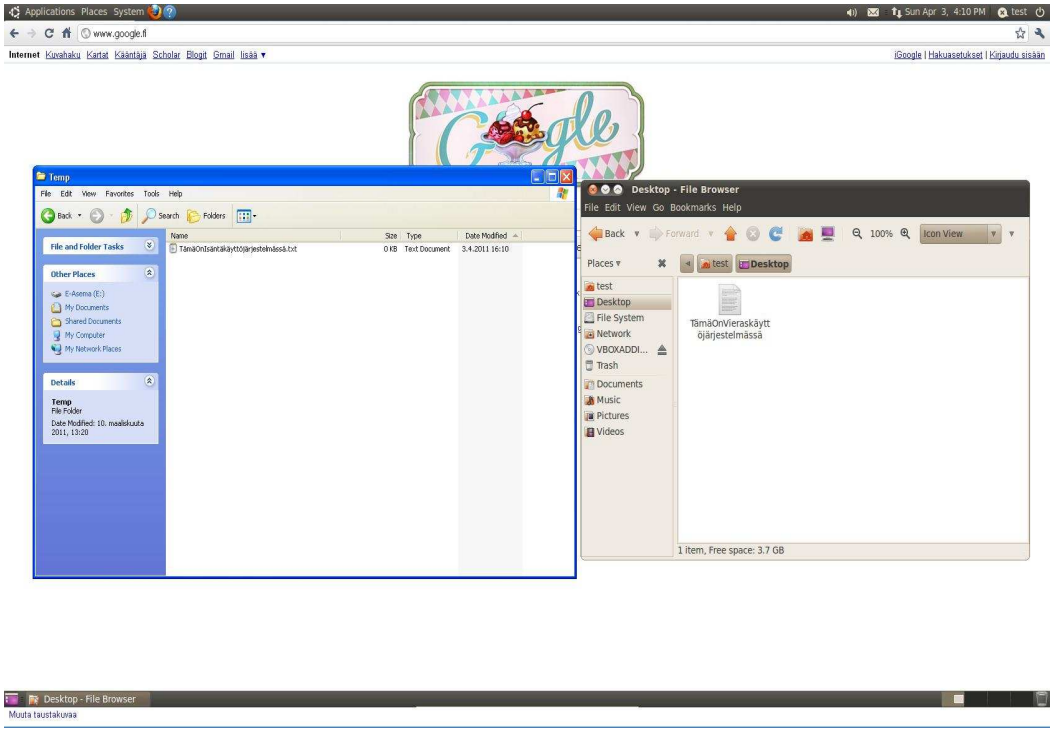
5.3.3 Saumattomat ikkunat (Seamless windows)

VirtualBoxin ”saumaton ikkuna” ominaisuuden avulla voit saada ne ikkunat, jotka ovat virtuaalisen tietokoneen näytöllä näkymään vierekkäin isäntätietokoneen ikkunoiden kanssa. Tämä ominaisuus on tuettu seuraavissa vieraskäyttöjärjestelmissä (olettaen, että vieraslisäosat on asennettu):

- Windows-vieraskäyttöjärjestelmät (tuki lisätty VirtualBox 1.5 versiosta alkaen)

- Tuetut Linux- ja Solaris-vieraskäyttöjärjestelmät, joissa ajetaan X Window-järjestelmää (lisätty VirtualBox 1.6 versiosta alkaen)

Sen jälkeen kun saumattomat ikkunat on otettu käyttöön, VirtualBox häivyttää vieraskäyttöjärjestelmän työpöydän taustan näkyvistä, sallien ajon vieraskäyttöjärjestelmän ikkunoita saumattomasti isäntäkäyttöjärjestelmän ikkunoiden rinnalla. (VirtualBox Manual)



Kuva 36. Saumattomat ikkunat (Seamless windows).

6. YHTEENVETO

Virtualisointi on tullut jäädäkseen. Vanhojen palvelinten prosessoritehojen ja kiintolevyjen hyötykäyttö virtualisoimalla on tuonut säästöjä konesalien päivitys ruljanssiin. Suuri osa yrityksistä käyttää nykyään virtualisointia tavalla tai toisella hyödykseen.

Virtuaalisten käyttöjärjestelmien käyttäminen esimerkiksi erilaisten ohjelmien luomisessa ja testauksessa on arkipäivää. Ennen käytettiin montaa eri tietokonetta, joissa oli eri käyttöjärjestelmät ja/tai asennettiin monta käyttöjärjestelmää tietokoneeseen, ohjelmien toimivuuden ja yhteensopivuuden tarkastelemiseen. Nykyään nämä testit voidaan tehdä virtualisoinnin avulla ja testin aiheuttaessa vakavia ongelmia käytettävässä olevalle virtuaaliselle käyttöjärjestelmälle, asia voidaan korjata ottamalla käyttöön edellisen toimivan kokoonpanon tilannekuvan (snapshot).

Virtuaaliset käyttöjärjestelmät ovat myös ihanteellisia erilaisten Internet-sivujen toimivuuden tarkastelussa eri käyttöjärjestelmien Internet-selaimilla. Ohjelmia luodessa on myös helpompi huomata virtualisoinnin avulla erilaisia käyttöjärjestelmiä käyttämällä mahdolliset yhteensopivuusongelmat.

VirtualBox-ohjelma oli helppo asentaa. Toimivuudeltaan siinä on vielä parantamisen varaa, vaikka ilmaisohjelmaksi se on todella hyvä. Ongelmat johtuivat lähinnä ilmaisversion USB-tuen heikosta toimivuudesta vieraslisäosien asentamattomuuden takia. Vieraslisäosien asentamisen jälkeen USB-tuki alkoi toimia hieman paremmin. Kaupallisessa versiossa USB-tuki on ilmoitettu toimivan ilman vieraslisäosien asentamista.

VirtualBoxin ilmaisversion vakaudessa oli myös ongelmia kannettavalla tietokoneella ohjelmaa käyttäessä. Ongelmat johtuivat kannettavan virransäästöominaisuuksista, jotka saattoivat aiheuttaa VirtualBox-ohjelman kaatumisen.

LÄHTEET

Buytaert Kris, Rogier Dittner, David Rule. (2007). The best damn server virtualization book period. Saatavilla www-muodossa: <URL: http://books.google.fi/books?id=L4iSishz58EC&lpg=PR5&ots=ZqtS_Fnglo&dq=buytaert%20kris%20the%20best%20damn&pg=PR5#v=onepage&q&f=false>

Goman, Mikko. (2010). Windows-palvelimien tietoturvan raportointi. Savonia-ammattikorkeakoulu. Saatavilla www-muodossa: <URL: https://publications.theseus.fi/bitstream/handle/10024/14031/Goman_mikko.pdf?sequence=1>

Järvinen, Petteri. 2010. Varo Scarewarea. *Tietokone*, 1/2010.

Kirves, Antti. *Mitä on spyware?* Digitoday 26.3.2003. [online]. [viitattu 6.1.2011]. Saatavilla www-muodossa: <URL:http://www.digitoday.fi/tietoturva/2003/03/26/mita-on-spyware/200310595/66>

Kotilainen, Samuli. Scareware vaikuttaa miljoonaan käyttäjään päivässä. Tietokone 14.3.2010. [online]. [viitattu 6.1.2011]. Saatavilla www-muodossa: <URL:http://www.tietokone.fi/uutiset/scareware_vaikuttaa_miljoonaan_kayttajaan_paivassa>

Paananen, Juha. (2000). Tietotekniikan peruskirja. WSOY.

Rantanen Petri. Virtualisointia kaikkialla, [online]. [viitattu 6.1.2011]. Saatavilla www-muodossa: URL:http://virtualisointi.blogspot.com

Rantasaari, Antti. (2003). Tunkeutumisen havaitseminen. Helsingin yliopisto.

Pitkänen, Jarmo. (2008). Tietokone: Päivän Softa: Microsoftilta maksutonta virtualisointia, [online]. [viitattu 6.1.2011]. Saatavilla www-muodossa: <URL:http://www.tietokone.fi/uutiset/2008/paivan_softa_microsoftilta_maksutonta_virtualisointia>

Ruohonen, Mika. (2002). *Tietoturva*. Docendo Finland

Tietoturvan peruskivet. [online]. [viitattu 6.1.2011]. Saatavilla www-muodossa: <URL:http://users.tkk.fi/mkangasl/tsp/4.perus.html>

Mäkinen, Ville. (2009). Tietoviikko: Virtualisointi teki murron, [online]. [viitattu 6.1.2011].
Saatavilla www-muodossa: <URL:http://www.tietoviikko.fi/kaikki_uutiset/article285493.ece>

Virtualization overview. [online]. [viitattu 6.1.2011]. Saatavilla www-muodossa: <URL:http://www.vmware.com/pdf/virtualization.pdf>

VirtualBox Manual: Chapter 4. Guest Additions. [online]. [Viitattu 3.4.2011] Saatavilla www-muodossa: <URL: http://www.virtualbox.org/manual/ch04.html>

Wikipedia: Palomuuri. [online]. [viitattu 6.1.2011]. Saatavilla www-muodossa: URL:http://fi.wikipedia.org/wiki/Palomuuri

Wikipedia: Tietoturva. [online]. [viitattu 6.1.2011]. Saatavilla www-muodossa: <URL:http://fi.wikipedia.org/wiki/Tietoturva>

Wikipedia: Virtualization. [online]. [viitattu 6.1.2011]. Saatavilla www-muodossa: <URL: http://en.wikipedia.org/wiki/Virtualization>