KYMENLAAKSON AMMATTIKORKEAKOULU

Liiketalous / tietojenkäsittelyn koulutusohjelma

Jaakko Mäkinen

LINUXIN TIETOTURVA

Opinnäytetyö 2009

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

Tietojenkäsittely

MÄKINEN JAAKKO	Linuxin tietoturva
Opinnäytetyö	30 sivua
Työn ohjaaja	Lehtori Päivi Hurri
Syyskuu 2009	
Avainsanat	Linux, käyttöjärjestelmät, tietoturva, työasema

Linux-käyttöjärjestelmän käyttöä perustellaan usein sen kilpailevia järjestelmiä paremmalla tietoturvalla. Tietoturva on käsitteenä kuitenkin käyttöjärjestelmää laajemmalle ulottuva, eikä ole käytettyjen teknologioiden ja ohjelmistojen monimutkaisuuden vuoksi helposti hallittavissa. Työn tarkoituksena oli selvittää, miten Linux-työaseman tietoturvaa hallitaan ja mitä tietoturvanäkökohtia tulee ottaa huomioon Linuxin työasemakäytössä kotona ja yrityksissä.

Työssä käydään läpi tietoturvan peruskäsitteet ja selvitetään käytännön toimet Linux-käyttäjän tietoturvan varmistamiseksi. Tietoturvaa pohditaan sekä käyttäjän että ylläpitäjän näkökulmasta ja tutkitaan, miten käyttäjiä ja heille annettuja oikeuksia hallinnoidaan.

Linux on niin koti- kuin yrityskäytössäkin vieläkin harvinainen valinta työaseman käyttöjärjestelmäksi. Kun Linuxin käyttö on kuitenkin lisääntymässä myös työasemissa, on järjestelmän tietoturvaratkaisut osattava. Työssä pohditaan lähinnä yleisellä tasolla mitä käyttäjän tulee osata tehdäkseen Linux-työasemastaan turvallisen.

Linuxin loogiset tietoturvaan vaikuttavat ratkaisut vaativat käyttäjältä perehtymistä ja nostavat siten järjestelmän turvallisen hallinnan oppimiskynnystä. Työssä selvitetään mitä yksittäisen Linux-koneen käyttäjän on vähintään tehtävä voidakseen turvallisesti käyttää ja ylläpitää Linuxia.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Business Management

MÄKINEN, JAAKKO	Linux Security
Bachelor's Thesis	30 pages
Supervisor	Päivi Hurri, Senior lecturer
September 2009	
Keywords	Linux, operating systems, security, workstation

It is often said that Linux as an opearating system is more secure than others. In this thesis the security of Linux as an operating system is evaluated. The thesis explains how the most common security practises of a Linux-workstation function and what measures should be taken to secure a computer that uses Linux as an operating system.

The work describes the basics of information security and proceeds into details of Linux-system. The aim of the work was to find out how easy or difficult maintaining security in Linux is and what needs to be done in order to further enhance a Linux-workstation's safety.

The thesis was carried out from the point of view of an ordinary computer user, not an expert. The research was conducted as personal exploration into the world of Linux with the help of literature and online sources.

It transpired that using Linux safely requires quite a lot of basic information regarding information security in general and the operating system in particular. For anyone wanting to learn to use Linux safely, a lenghty learning curve is to be expected. In conclusion, it appears that a Linux-system can be very safe.

SISÄLLYS

TERMIT JA LYHENTEET

apt Advanced Package Tool. Debian-projektin kehittämä työkalu pakettienhallinnan helpottamiseen.

aptitude Aptitude on Debian-pohjaisissa jakeluissa käytettävä paketinhallintajärjestelmän työkalu.

Demoni eli daemon on Linuxissa taustaprosessina toimiva palvelu. Taustaprosessit toteuttavat Linux-järjestelmässä esimerkiksi tulostuksen.

GNU-projekti Amerikkalaisen Richard M. Stallmanin alulle panema vapaiden ohjelmistojen kehitysprojekti.

Linux-jakeluversio Linux-ytimen ympärille koottu kokonaisuus, joka sisältää mm. GNU-projektin ohjelmia sekä joukon sovellusohjelmia.

RPM *RPM Package Manager* (alunperin *RedHat Package Manager*) on Redhat-pohjaisissa järjestelmissä käytettävä paketinhallintajärjestelmä.

Root Järjestelmän pääkäyttäjä.

yum Yellow Dog Updater, Modified. Yum on alunperin Redhat Linuxia varten laajennettu ja muokattu versio Yellow Dog Linuxin Yellowdog Updaterista (YUP).

1 JOHDANTO

Linux on vapaa ja useimmiten ilmainen UNIX-tyyppinen käyttöjärjestelmä, joka soveltuu erilaisiin tietokoneisiin. Linuxin luoja on Linus Torvalds, joka aloitti Linuxin kehittämisen 1990-luvun alussa. Linux on yleiskieleen vakiintunut nimi, jolla tarkoitetaan koko käyttöjärjestelmää. Itse asiassa Linux on käyttöjärjestelmän ydin (kernel). Alkujaan Linux levisi käyttöön varsinkin palvelimena, mutta nykyään se on myös varsin yleisesti käytetty järjestelmä työasemissa.

Tutkimustyön tarkoituksena on selvittää, miten Linux-työaseman tietoturvaa hallitaan ja millaisia hallinnollisia, fyysisiä ja loogisia keinoja on käytettävissä työaseman turvaamiseksi. Työssä kuvatuilla keinoilla on tarkoitus helpottaa Linux-työasemaa käyttävien tietoturvaosaamista.

Työ on tarkoituksella rajattu koskemaan työasemakäyttöä, sillä Linux-palvelimen tietoturva on jo laajempi asia, minkä lisäksi siitä on jo kirjoitettu paljon. Työssä ei myöskään käsitellä Linux-työaseman tietoturvaa minkään yksittäisen jakeluversion näkökulmasta, vaan esitellään yleisiä, useimmille jakeluversioille yhteisiä toimintoja.

2 TIETOTURVAN PERUSTEKIJÄT

Tietoturvan kolme perustekijää ovat tiedon luottamuksellisuus, tiedon eheys ja tiedon käytettävyys (Pirtilä, T. 2007). Luottamuksellisuudella tarkoitetaan pyrkimystä siihen, ettei kukaan pysty käyttämään oikeudettomasti tietoa, jota ei ole hänelle tarkoitettu. Tiedon eheydellä pyritään siihen, ettei ulkopuolinen taho voi ilman lupaa muuttaa tiedon sisältöä. Tiedon käytettävyydellä tarkoitetaan tietoa tallentavan tai liikennöivän järjestelmän turvaamista siten, että järjestelmään kuuluvat palvelut, koneet ja tietoverkot toimivat. (Järvinen 2002, 24.)

2.1 Tietoturvan muut periaatteet

Tiedon todentamisella pidetään huoli siitä, että käyttäjä, kone tai palvelu on se, kuka sen oletetaan olevan. Pääsynvalvonta huolehtii siitä, etteivät todentamattomat tahot pääse tietoon käsiksi. Kiistämättömyydellä tarkoitetaan tehtyjen toimien sitovaa todistamista. (Järvinen 2002, 27.)

2.2 Hallinnollinen turvallisuus

Tietojärjestelmien ja tietoliikenneratkaisuiden toteutuksessa hallinnolliset menetelmät ovat ensiarvoisen tärkeitä, sillä niillä pyritään määrittelemään organisaation tietoturvapolitiikka. Tärkeää on kirjata tarvittavat turvallisuuskäytännöt, jotta niiden toteutumista voidaan valvoa. (Rantala 2003, 318.)

2.3 Fyysinen turvallisuus

Koneiden, laitteiden ja kaapelien suojaus luvattomalta käytöltä, esimerkiksi sijoittamalla ne lukolliseen tilaan, kulunvalvonnan ulottuville, on tiedon fyysistä turvallisuutta. Lisäksi täytyisi ottaa huomioon tulipalot ja vesivahingot sekä turvata sähkön saanti. Nämä fyysisen turvallisuuden keinot pätevät yhtä hyvin yksittäisiin työasemiin kuin palvelimiinkin. (Rantala 2003, 318.)

2.4 Looginen suojautuminen

Tietojärjestelmän suojaaminen ohjelmistojen asetuksilla ja erilaisilla ohjelmilla tai laitteilla on järjestelmän loogista suojaamista. Siinä käytetään hyväksi käyttäjäoikeuksien rajaamista, salasanoja, lokitiedostojen analysointia, palomuuriasetuksia ja varmuuskopiointia. (Rantala 2003, 319, 323, 324, 330, 331, 332.)

3 LINUX-TYÖASEMAN TIETOTURVASUUNNITELMA

Linuxin käyttäjän olisi, kuten muidenkin käyttöjärjestelmien käyttäjien, hyvä tehdä selkeä suunnitelma tietoturvan noudattamiseksi. Tietoturvasuunnitelma kannattaa tehdä ohjeen muotoon, jotta käyttäjä voisi sitä tehokkaasti hyödyntää. Liikoja teknisiä yksityiskohtia ohjeessa kannattaa välttää, sillä ne yleensä vain hämmentävät käyttäjää. Mieluummin tulisi käyttää esimerkkejä, joilla luodaan käytännönläheisiä ohjeita (Hakala ym. 2006, 10).

Tietoturvasuunnitelman toteuttaminen käytännössä tapahtuu pitämällä järjestelmä ajan tasalla. Ohjelmointivirheiltä on vaikeaa välttyä, joten käytettävät ohjelmat olisi syytä päivittää säännöllisesti. Ohjelmointivirheiden paikkaukset asentuvat näin säännöllisesti. Hyvällä salasanalla ja käyttäjätunnuksella estetään ulkopuolisten pääsy järjestelmään. Siksi salasanan tulee olla riittävän hyvä, niin ettei sitä ole helppo arvata ja että salasana on tarpeeksi pitkä. Lisää salasanakäytännöistä kerrotaan seuraavassa luvussa.

Pääkäyttäjän tunnusta tulisi käyttää vain tarvittaessa. Koska pääkäyttäjän tunnuksella voi tehdä mitä tahansa, tulisi sitä käyttää vain, mikäli se on ehdottoman tarpeellista. Siksi pääkäyttäjien määrä tulisi säännöllisesti varmistaa */etc/passwd*-tiedostosta, ja huolehtia, ettei järjestelmässä ole kuin yksi pääkäyttäjä.

Jokainen toimiva palvelu on toimiva ohjelma ja muodostaa mahdollisen haavoittuvuuden ohjelmointivirheen kautta. Siksi on perusteltua pitää toiminnassa vain ne ohjelmat, joita tarvitsee. Pitämällä tarpeettomat verkkopalvelut pois käytöstä varmistetaan, etteivät ne vaaranna tietoturvaa.

Lokien tarkkailu tulisi olla mukana tietoturvasuunnitelmaa laadittaessa. Lokitiedostoihin tallennetaan tietoja järjestelmän toiminnasta ja toiminnan virheistä, ohjelmien käytöstä sekä käyttäjistä ja sisäänkirjautumisyrityksistä. Ongelmien selvittämisessä ne ovatkin suuri apu käyttäjälle. Tietoturvan kannalta tärkeitä lokeja ovat */var/log/secure* ja */var/log/auth.log*, jotka antavat tietoa kirjautumisista ja -yrityksistä.

Linux-ohjelmia voidaan ajaa eri käyttäjien oikeuksin, joten käyttäjäoikeuksista huolehtiminen on olennaista. Varsinkin root- eli pääkäyttäjän oikeuksista tulisi pitää tarkasti huolta.

Varmuuskopiointisuunnitelman tekeminen ja sen ajantasaisena pitäminen on tärkeää. Tiedostojen varmuuskopiointi säännöllisesti, ja sen automatisointi, helpottaa vikatiloista palautumista ja säästää aikaa ja kustannuksia.

Koska käynnistysasetuksista voi määritellä järjestelmän käynnistymään tilaan, jossa järjestelmää voi käyttää pääkäyttäjän oikeuksin, tulisi käynnistyslataimelle asettaa salasana. Muussa tapauksessa mahdollisella murtautujalla on avoin pääsy järjestelmään.

4 KÄYTTÄJÄTUNNUKSET JA SALASANAT

Linux-työasema on usean käyttäjän ns. moniajojärjestelmä, jolloin käyttäjät pääsevät käyttämään sitä käyttäjätunnusten ja salasanojen avulla (Durham 2002, 4). Linuxissa tiedostoilla ja hakemistoilla on erilaisia oikeuksia: pääsy-, luku-, kirjoitus- ja/tai suoritusoikeus (Kapanen 2004, 603). Tiedoston luomisen yhteydessä tiedoston luonut henkilö ja hänen käyttäjäryhmänsä saavat sekä luku- että kirjoitusoikeudet. Muut käyttäjät ja käyttäjäryhmät saavat vain lukuoikeudet. Koska käyttöoikeudet ja käyttäjien salasanat muodostavat Linux-tietoturvan perustan, on niille annettava tarpeeksi painoarvoa (Rantala 2003, 323).

Käyttäjätunnuksen alla ovat yhdelle käyttäjälle kuuluvat tiedostot, resurssit ja tiedot (Koski 2000, 99). Erilaisia käyttäjiä ja -ryhmiä voi Linuxissa olla useita. Tärkein rooli on järjestelmän pääkäyttäjän eli rootin rooli. Root eli ns. superuser on järjestelmän käyttörajoitusten ulkopuolella (Rantala 2003, 323). Siksi on erityisen tärkeää huolehtia siitä, että vain luvalliset käyttäjät voivat käyttää root-tunnusta. Pääkäyttäjän tunnuksen käyttö tulisi minimoida, jotta esimerkiksi vahingossa tapahtuva datan häviäminen voitaisiin estää. Oman lisämausteensa asiaan tuo se, että Linuxissa voi olla useita

pääkäyttäjiä samanaikaisesti. Tämä on tosin harvinaista työasemakäytössä, varsinkin kotikäyttäjillä.

Linux-järjestelmän käyttäjätiedot sisältävä tekstitiedosto on nimeltään /etc/passwd. Siinä on seitsemällä kaksoispistein erotetulla kentällä määritelty jokainen järjestelmän käyttäjä. Ensimmäinen kenttä on käyttäjänimi, toinen salasana, kolmas numeerinen käyttäjätunnus, neljäs numeerinen ryhmätunnus, viides täydellinen nimi, kuudes kotihakemisto ja seitsemäs aloittava komentotulkki (Koski 2000, 100). Seuraavassa esimerkiksi listaus /etc/passwd-tiedoston käyttäjätiedoista:

$ more /etc/passwd
root:x:0:0:root:/root:/bin/bash
...
jamak:x:1000:1000:Jaakko Mäkinen,,,:/home/jamak:/bin/bash
Nykyään Linux-jakeluversiot käyttävät ns. shadow- eli varjosalasanaa. Shadow-järjestelmässä salakirjoitetut salasanat sijaitsevat /etc/shadow-tiedostossa (Rantala 2003, 325). Esimerkki /etc/shadow-tiedostosta:

$ sudo more /etc/shadow
root:!:13895:0:99999:7:::
...
jamak:1O/s4EkX5$NzkPvrFPZwdNlF7.CKPCt.:13895:0:99999:7:::

Koska vain root-käyttäjällä on lukuoikeus tiedostoon, salasanojen arvaaminen käyttämällä erityistä salasanojen murtamiseen tehtyä ohjelmistoa vaikeutuu (Rantala 2003, 325).

Hyvän salasanan tulisi olla vähintään kahdeksan merkkiä pitkä, eikä se saisi muistuttaa minkään kielen sanoja (Rantala 2003, 325). Salasanan ei pitäisi olla henkilökohtaiseen elämään liittyvä, eikä sitä pitäisi voida johtaa henkilön nimestä tai käyttäjätunnuksesta (Järvinen 2002, 340). Sekä pien- että suuraakkosia tulisi käyttää erikoismerkkien kanssa. Näin hidastetaan ns. raa'alla voimalla – eli laskentateholla – tehtäviä mur-

tautumisyrityksiä (Järvinen 2002, 341). Ääkkösten eli skandien käyttöä Linuxin salasanoissa ei suositella. Kaikki ohjelmat eivät ymmärrä niitä aakkosiksi tai edes muiksi merkeiksi. Lisäksi salasana pitäisi vaihtaa riittävän usein, myös kotikoneella. Yrityksissä Linux-työasemien ylläpitäjät voivat asettaa salasanat vanhenemaan tietyn ajan jälkeen, jolloin käyttäjien on pakko vaihtaa salasanansa. Järvinen (2002, 342) kehottaa käyttämään salasanan muodostamisen apuna lentäviä lauseita tai aforismeja: *PEO-KIVTOHT – Paha ei ole kenkään ihminen, vaan toinen on heikompi toista (Leino).* Tällaiseen salasanaan voidaan vielä liittää erikoismerkkejä.

5 KÄYTTÄJÄTUNNUSTEN JA -RYHMIEN HALLINTA

Tietoturvan kannalta käyttäjätunnusten ja -ryhmien hallinta on tärkeää siksi, että ylläpitäjä voi ryhmittelemällä käyttäjät lisätä tai rajoittaa heidän oikeuksiaan (Durham 2002, 245). Kun Linux-järjestelmä on asennettu, luodaan ns. tavallinen käyttäjä, jos sitä ei ole luotu jo asennuksen yhteydessä. Samalla tälle käyttäjälle annetaan salasana ja mahdollisesti määritellään käyttäjän ryhmä sekä kotihakemisto (Rantala 2003, 154). Käyttäjien ryhmätiedot löytyvät /etc/group- tiedostosta. Seuraavassa lyhennetty listaus /etc/group- tiedostosta:

```
$ more /etc/group
root:x:0:
...
cdrom:x:24:haldaemon,jamak
...
scanner:x:104:hplip,jamak
```

Ryhmätiedosto muodostuu neljästä kaksoispistein erotellusta kentästä: ensimmäinen on ryhmän nimi, toinen on tavallisesti tyhjä, mutta voi sisältää ryhmän salasanan, kolmas on ryhmän numeerinen GID-tunnus (group-ID) eli ryhmän käyttäjätunnus ja neljäs kenttä sisältää ryhmään kuuluvat käyttäjät (Durham 2002, 246). Järjestelmän pää-

käyttäjä voi vaihtaa paitsi tiedoston myös käyttäjäryhmän käyttöoikeuksia. Tämän voi tehdä komennolla **chown** (change file owner and group). Jos on tarpeen vaihtaa käyttäjän ryhmää, käytetään komentoa **chgrp**. **Chown**-komennolla on -R-optio, jolla saadaan vaihdettua koko hakemistopuun omistus yhdellä komennolla:

$ chown -R jamak.kaalisaha hakemistolistaus

(Rantala 2003, 157, 158). Ylläpidon voi toisinaan olla tarpeellista poistaa käyttäjätunnus. Se tapahtuu **userdel**- komennolla:

$ userdel umppa
Tällöin poistuvat /etc/passwd, /etc/shadow ja /etc/group- tiedostoista kaikki käyttäjän umppa tiedot. Käytettäessä **userdel**-komennon -r-optiota, voidaan poistaa myös käyttäjän kotihakemisto (Rantala 2003, 154). Joissakin tapauksissa voi tulla tarpeelliseksi lukita käyttäjän tunnus. Se tehdään kirjoittamalla /etc/shadow- tiedostoon kyseisen käyttäjätunnuksen kohdalle joko asteriski (*), tai huutomerkki (!). Tämän tekniikan teho perustuu siihen, että Linuxin käyttämät salausalgoritmit eivät tunnista näitä merkkejä (Rantala 2003, 155). Jos on tarpeen määritellä käyttäjän ryhmä järjestelmässä, se voidaan tehdä komennolla **usermod**. Jos komennolla ei muuttujilla määritetä mihin ryhmiin käyttäjä kuuluu, **usermod** poistaa käyttäjän niistä ryhmistä joita ei mainita.

$ usermod -g paaryhma -G tiimi01,tiimi02

Usermod-komennon -g-optiolla asetetaan sen uuden ryhmän nimi tai numero, johon käyttäjä kuuluu. -G-optio taas listaa – ilman välilyöntejä – kaikki ne ryhmät, joihin käyttäjä kuuluu primääriryhmän (esimerkissä paaryhma) lisäksi (Siever, Figgins & Weber 2003, 468).

6 HAKEMISTOJEN JA TIEDOSTOJEN KÄYTTÖOIKEUDET

Usean käyttäjän moniajojärjestelmänä Linux antaa määritellä käyttöoikeudet erikseen tiedoston ja hakemiston omistajalle, omistajaryhmälle ja muille käyttäjille (Rantala 2003, 73). Jokainen näistä tahoista, omistaja (u, user), omistajaryhmä (g, group) ja muut käyttäjät (o, others) voivat saada eritasoisia oikeuksia. Taulukossa 1 esitetään tiedostojen käyttöoikeudet.

Taulukko 1. Tiedostojen käyttöoikeudet (Durham 2002, 252.)

r	lukuoikeus
w	kirjoitusoikeus
x	suoritusoikeus
X	suoritusoikeus, jos tiedosto on hakemisto, tai sillä on jo suoritusoikeus
s	asettaa käyttäjä- tai ryhmä-ID:n (UID tai GID) suorituksen yhteydessä
t	asettaa tiedoston save-text-attribuutin
u	tiedoston nykyisen omistajan oikeudet
g	tiedoston omistajaryhmän oikeudet
o	muille käyttäjille asetetut oikeudet

Lukuoikeus antaa oikeuden avata tiedoston, lukea sitä ja kopioida sen. Kirjoitusoikeus mahdollistaa tiedostoon kirjoittamisen ja sen sisällön muuttamisen. Suoritusoikeudella tiedoston voi käynnistää suoritukseen. (Rantala 2003, 73, 74.) Komennolla **ls** ja sen -l-optiolla voidaan tulostaa tiedoston käyttöoikeudet:

$ ls -l oikeudet.txt
-rwx------ 1 jamak jamak 0 2008-03-26 11:29 oikeudet.txt

Listauksessa tulostuu kymmenestä kentästä muodostuva rivi. Taulukossa 2 on kerrottu kenttien merkitys. Tietoturvan kannalta jokainen kenttä on merkitsevä ja ylläpitäjän pitää osata lukea hakemistolistausta.

Taulukko 2. Tiedostojen käyttöoikeudet hakemistolistauksessa

Kenttä	Selitys
1	Tiedoston tyyppi
2	Omistajan oikeudet
3	Omistajaryhmän oikeudet
4	Muiden käyttäjien oikeudet
5	Tiedostoon osoittavien linkkien lukumäärä
6	Tiedoston omistaja
7	Tiedoston omistajaryhmä
8	Tiedoston koko tavuina
9	Aikaleima
10	Tiedoston nimi

Hakemistojen ja tiedostojen käyttöoikeuksia muutetaan **chmod**-komennolla (change file access permission, change mode) (Rantala 2003, 76). Jotta tiedostojen oikeuksia pääsee muuttamaan, on oltava joko pääkäyttäjä tai tiedoston omistaja. **Chmod**-komentoa voidaan käyttää kahdella tavalla: symbolisesti ja numeerisesti. Symbolisella tavalla käytetään kirjaimia u (tiedoston omistava käyttäjä), g (käyttäjäryhmä), o (muut käyttäjät) sekä a (kaikki käyttäjät) (Durham 2002, 251). Numeerisella tavalla oikeudet määritellään numerosarjana oktaalimuodossa (oktaalijärjestelmässä käytetään lukuja 0-7). Taulukossa 3 on esitetty, mistä **chmod**-komennon numeeriset oktaalimuodot ovat peräisin.

Taulukko 3. Oktaaliluvut, niitä vastaavat bitit sekä käyttäjäoikeudet

Oktaalijärjestelmän luku	Bitit	Oikeudet
0	000	---
1	001	--x
2	010	-w-
3	011	-wx
4	100	r--
5	101	r-x
6	110	rw-
7	111	rwx

Taulukosta 3 nähdään, että pyrittäessä suojaamaan tiedostot tehokkaasti, olisi käytettävä **chmod**-komentoa oktaaliluvulla 700. Näin annetaan tiedoston täydet oikeudet vain

tiedoston omistajalle, samalla kun muut käyttäjät ja ryhmät eivät saa ko. tiedostoon mitään oikeuksia (Rantala 2003, 78).

6.1 Lokitiedostot

Oli kyse sitten turvallisuudesta tai vianetsinnästä, lokitiedostoihin tutustuminen on tärkeää. Kotonakaan työasema-Linuxia käyttävän ei kannata ylenkatsoa lokeja, sillä ne antavat tietoa mm. tunkeutumisyrityksistä ja järjestelmän käyttäjistä (Durham 2002, 330).

Tiedostossa /var/log/messages on tietoa lähes kaikista koneen tapahtumista, kun taas /var/log/secure tiedostosta nähdään, onko kirjautumisen yhteydessä yritetty antaa vääriä salasanoja (Rantala 2003, 330). Linux-järjestelmän pääkäyttäjän on mahdollista käyttää syslog-demonia (**syslogd**) eli ohjelmaa, joka kirjoittaa lokitiedostot. Tämän ohjelman avulla voidaan ohjata lokitiedostot myös muualle kuin järjestelmän oletuksena käyttämiin tiedostoihin. **Syslogd**:llä pystytään ajastamaan lokien kirjoittaminen ja määrittelemään, miten lokeja käytetään. Lokien kirjoittaminen tapahtuu tiedostoon /etc/syslog.conf kirjattujen sääntöjen avulla (Durham 2002, 330).

6.2 Tiedostojen tarkkailu

Arkaluontoista dataa sisältäviä tiedostoja tulisi tarkkailla säännöllisesti. Tietomurron yhteydessä luvaton käyttäjä on voinut saada käyttöoikeuksia, joiden avulla hän on pystynyt muuttamaan tiedostoja. Muutettuja tiedostoja käytetään esimerkiksi lähettämään järjestelmän salasanatiedosto murtautujalle. Tiedostojen muuttumista voidaan tarkkailla tarkistussummien avulla. (Durham 2002, 330.)

6.3 Järjestelmän dokumentointi

Järjestelmän dokumentointi auttaa hallitsemaan omaa tietokonetta tietoturvan kannalta mahdollisimman tehokkaasti. Uuden järjestelmän asennuksessa asioiden kirjaaminen ylös helpottaa konfiguraatiota ja saattaa säästää hermoja ja aikaa. Myös jo asennetun

järjestelmän muutosten dokumentointi lisää käytön varmuutta. Yleisesti kannattaa kirjata ylös, mitä on tehty ja milloin, sekä mitä muutoksia tai tuloksia toimenpiteillä on saavutettu. Loki- ja asetustiedostojen pitäminen ajan tasalla auttaa, paitsi tietoturvaongelmien, myös muiden ongelmatilanteiden ratkaisemisessa. Yrityksissä työaseman käyttäjiä voidaan dokumentoida monella tavalla. (Durham 2002, 331.)

7 VARMUUSKOPIOINTI JA TUHOAMINEN

Koski (2000, 107) toteaa datan menettämiseen olevan *neljä perussyytä: laiteviat, ohjelmavirheet, ihmisen toiminta tai luonnononnettomuudet.* Huolimatta siitä, että varmuuskopioinnista muistutetaan nykyään kaikkialla, on datan menettäminen edelleen valitettavan yleistä. Jotta Linux-työaseman tiedostojen varmistaminen ei jäisi tekemättä, tulisi hyödyntää eri jakeluversioiden mukana tulevia tai ilmaisena verkosta saatavia varmistustyökaluja. Monet näistä ohjelmista, kuten **tar** (Tape ARchive), ovat jo vanhaa UNIX-perua.

Varmistustyökalun ja käytettävän varmistusvälineen valinta pitäisi tehdä yhdessä (Koski 2000, 109). Yksittäisen työaseman varmistaminen on vielä suhteellisen yksinkertaista, mutta yrityksissä kymmenistä tai jopa sadoista työasemista muodostuva järjestelmä asettaa varmistukselle todellisia haasteita. Kotikäyttäjänkin olisi hyvä tehdä varmistusstrategia, jolla päätetään, mitä varmuuskopioidaan ja mille medialle tai laitteelle, millä ohjelmilla varmistus tehdään, ja miten varmistus automatisoidaan (Rantala 2003, 197).

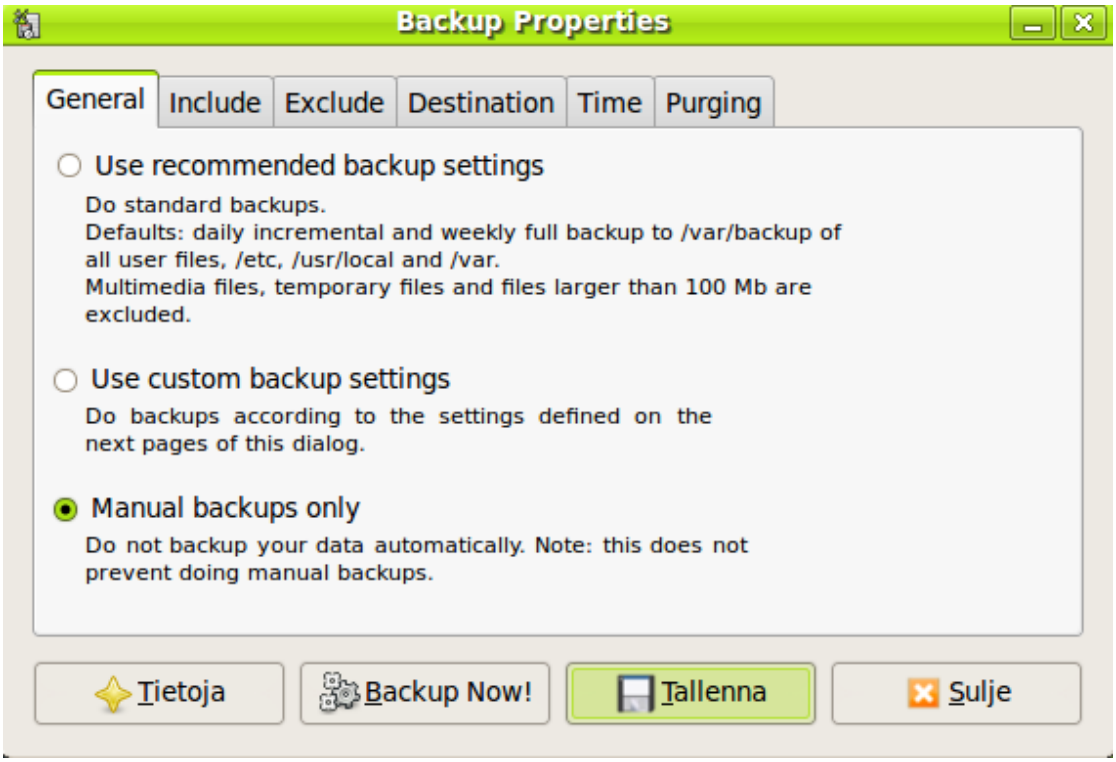
Linux-työasemassa ilmeinen varmuuskopioinnin kohde on käyttäjän kotihakemisto. Sen lisäksi käyttäjien tietoja, kuten salasanoja, sisältävät tiedostot kannattaa kopioida. Varmuuskopioinnissa on yksinkertaisinta varmistaa ensin kaikki data kerran (täysvarmistus) ja sen jälkeen tallentaa vain edellisestä kerrasta muuttunut data (muutosvarmistus eli inkrementaalinen varmistus). (Rantala 2003, 198.)

Esimerkki **tar**-ohjelmalla otetusta varmistuksesta:

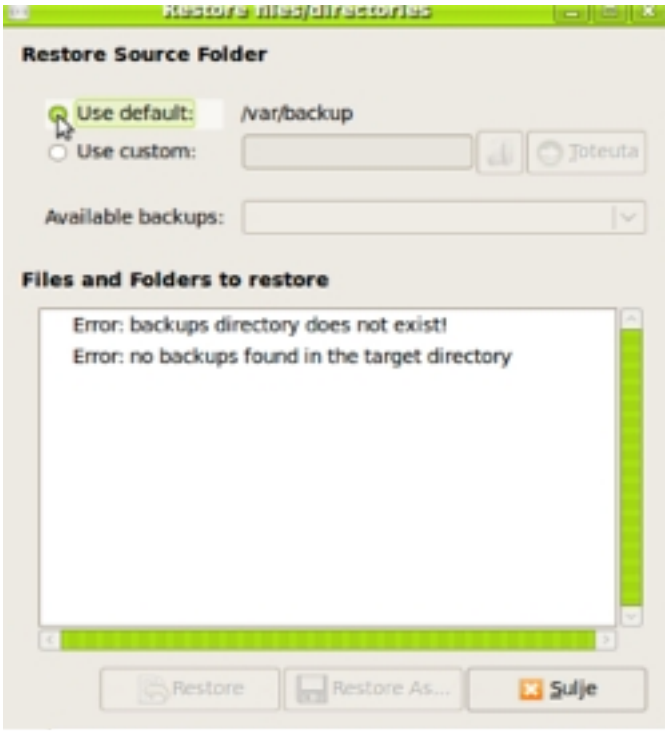
$ tar -cpzf /var/backups/kotitiedosto.tar.gz /home

Tässä **tar**-ohjelma käyttää optioita -c (--create eli luo), -p (--same-permissions eli käytetään samoja tiedosto-oikeuksia kuin alkuperäisessä tiedostossa), -z (--gzip eli käytetään gzip-ohjelmaa pakkaamiseen tai purkamiseen) ja -f (määrittelee pakattavan tai purettavan tiedoston) (Siever ym. 2003, 429-434). Käyttäjän kotihakemistosta tehdään varmuuskopio tiedostoon /var/backups/kotitiedosto.tar.gz.

Varmuuskopiointiin on olemassa myös graafisia työkaluja, tässä niistä yksi, Simple Backup. Ohjelmalla voidaan ottaa varmuuskopio mistä tahansa tiedostojärjestelmän yksittäisestä tiedostosta tai hakemistosta. Erilaisia sääntöjä luomalla voidaan myös jättää osia järjestelmästä kopioimatta. Sääntöjä voidaan luoda säännöllisten lausekkeiden avulla tai tiedostotyyppien avulla. Kuvassa 1 on valittu manuaalinen varmuuskopionti. Lisäksi kopioitavien tiedostojen koolle voidaan asettaa rajoituksia. Ohjelman avulla voidaan tehdä varmuuskopio paikalliselle levylle, tai sitten voidaan kopioida verkon yli toiselle koneelle vaikkapa sftp- tai ftp-yhteyden kautta.



Kuva 1. Simple Backup-ohjelman asetusikkuna, jossa valittuna manuaalisten varmuuskopiointien valinta.

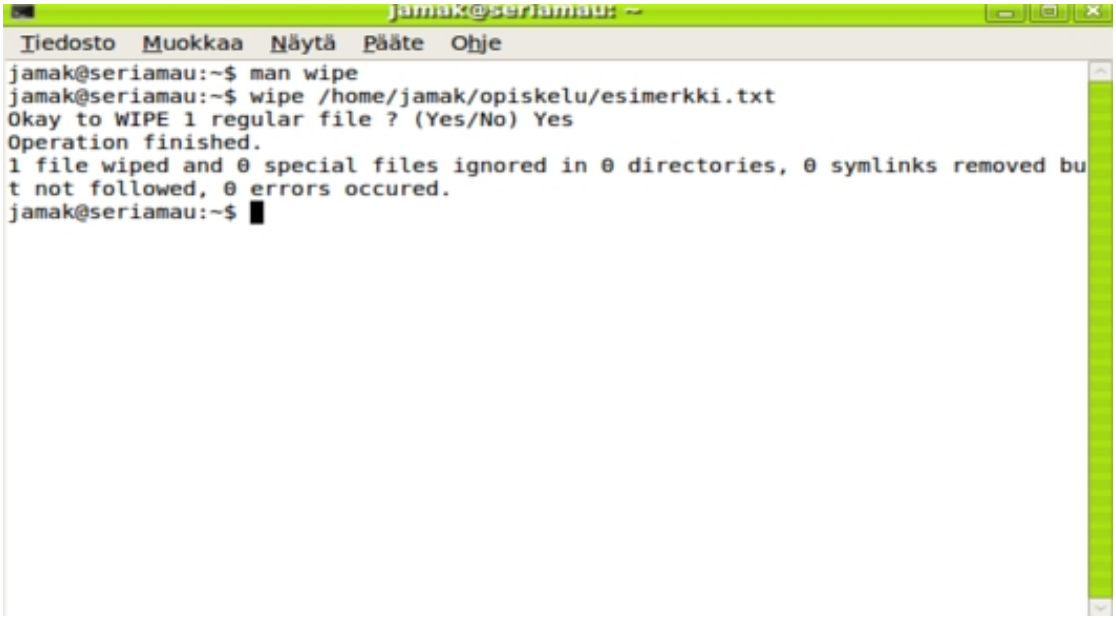


Kuva 2. Simple Backup-ohjelman tiedostojen palautusikkuna ennen kirjoittajan tekemiä toimenpiteitä.

Varmuuskopioinnin automatisointi voidaan Linuxissa tehdä **cron**-komennolla. **Cron**illa varmuuskopiointi voidaan ajastaa tapahtumaan haluttuun aikaan käyttämällä käyttäjäkohtaisia tiedostoja /var/spool/cron -tiedostossa. Ajamalla komento **crontab** haetaan crontab-tiedostoista suoritettavat komentorivit sekä ajojen ajankohdat. Ajankohdat merkitään viiteen kenttään: minuutit, tunnit, kuukauden päivä, kuukausi ja viikonpäivä. (Siever ym. 2003, 96.)

Tiedostojen tuhoamiseen Linuxissa on useita ohjelmia, joista suurin osa on komentorivipohjaisia, tosin myös graafiselle käyttöliittymällä varustettuja ohjelmia löytyy. Ns. journaloivien tiedostojärjestelmien kohdalla täytyy tiedostoja tuhotessa olla tarkkana, sillä samalla kun dataa toisaalla tuhotaan, saattaa journaloiva järjestelmä kirjoittaa samaa dataa toisaalle.

Wipe-ohjelma tulee Linuxin mukana, ja se on helppokäyttöinen. Komentoriville kirjoitetaan ohjelman nimi *wipe*, ja sen jälkeen tuhottavan tiedoston sijainti ja nimi. Kuvassa 3. on esimerkki tiedoston tuhoamisesta wipe-ohjelmalla.



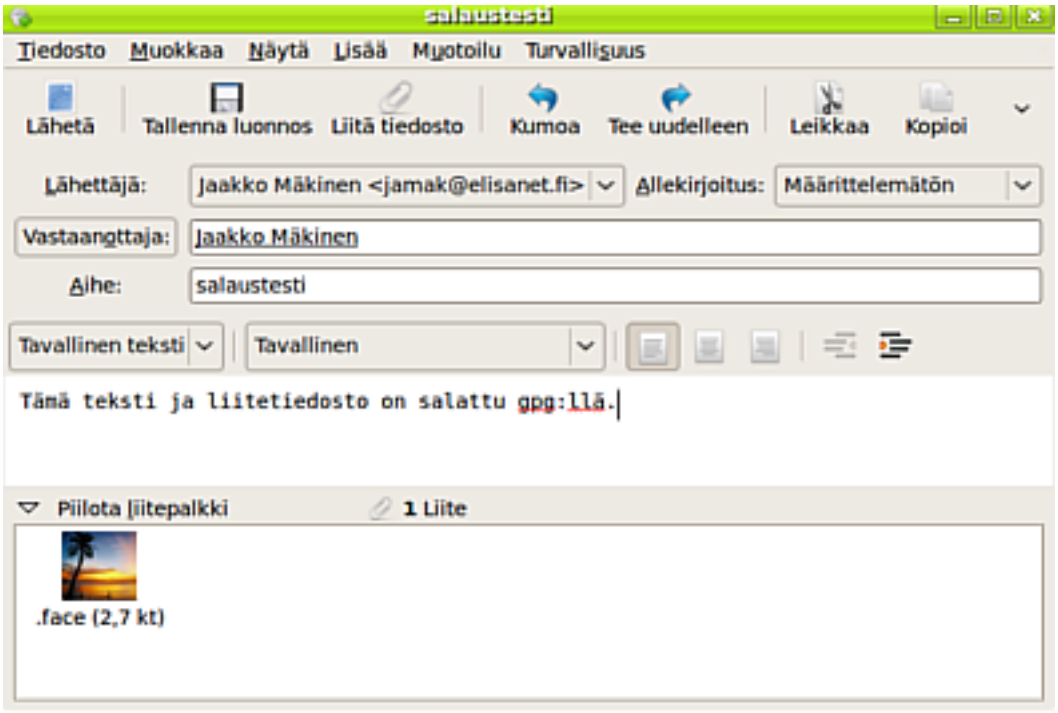
Kuva 3. Wipe-ohjelman käyttöä komentoriviltä esimerkkitiedoston tuhoamiseksi

8 TIEDON SALAAMINEN

Tiedon salaaminen on tietoturvan kannalta tärkeää, koska tietoliikenteen ja tietokoneiden turvallisuus on riippuvaista salakirjoitusmenetelmistä ja niiden sovelluksista. Salakirjoituksen tavoitteena on muuntaa data sellaiseen muotoon, että vain lähettäjä ja vastaanottaja saavat tiedon selville. Datan sisältö muunnetaan jollakin salakirjoitusmenetelmällä ja sen jälkeen se, jolla on tieto käytetystä salausmenetelmästä ja purkamiseen tarkoitettu avain, voi purkaa salatun datan alkuperäiseen muotoon ja lukea sen (Hakala ym. 2006, 372).

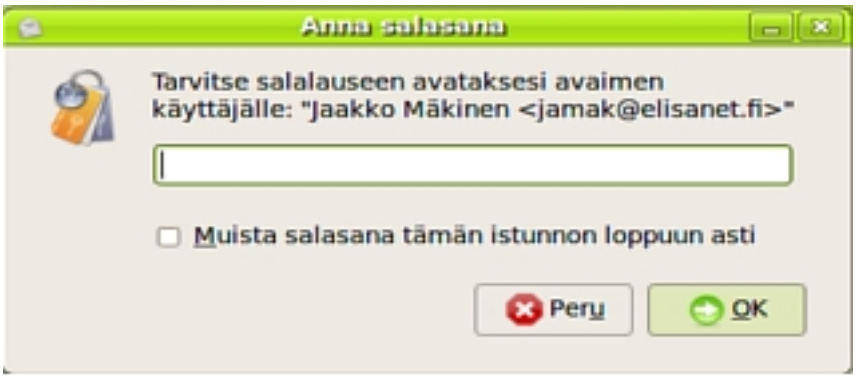
Linuxissa Evolution-sähköpostiohjelmassa voidaan käyttää PGP-salausta. Salausta varten tarvitaan avainpari, jonka luomiseen käytetään **gnupg**-ohjelmaa. Ohjelmaa käytetään komentoriviltä, mutta siihen on saatavissa graafisen käyttöliittymä nimel-

tään GNU Privacy Assistant. Seuraavassa esimerkkinä itselleni lähetetty salattu viesti ja liitetiedosto.



Kuva 4. Sähköpostiviesti ja liitetiedosto, jotka on salattu pgp-ohjelmalla.

Kun salattua viestiä avataan, täytyy antaa aiemmin määritelty salainen lause, jolla viesti saadaan avattua.



Kuva 5. Tekstikenttään annetaan salainen avain eli aiemmin määritelty salainen lause, jotta sähköpostiviestin pääsee lukemaan.

Tiedonsiirrossa suositellaan nykyään tiedon salaamista. Kaikissa käyttöjärjestelmissä toimiva SSH, Secure Shell-järjestelmä, on käytössä myös Linuxissa. Yleisimmin SSH-yhteyksiä käytetään Linuxissa komentorivin eli päätteen avulla. Yhteydenpito vaatii

SSH-asiakasohjelman sekä -palvelimen. SSH-asiakaspääteohjelmia ja -palvelimia on useita eri tyyppisiä, mutta yleensä mitään yhteensopivuusongelmia ei eri versioiden välillä ole (Hakala ym. 2006, 388).

9 PALOMUURI

Aiemmin Linuxin palomuurina toimivat pakettisuodatusohjelmistot **ipfwdm** ja **ipchains**. Nykyisin asiaa hoitaa **iptables**-suodatus (Hakala ym. 2006, 204). **Iptables** toimii liikenteen suodattajana ja pakettien muokkaajana. Pakettisuodatinpalomuurin toimintaperiaate on tutkia saapuvien datapakettien lähde- ja kohdeosoitteet ja joko estää tai sallia paketti kohdeverkkoon (Krutz, Vines 2003, 90). Liikennettä suodattaessa **iptables** päättää, reitittääkö se paketin edelleen vai jakaako sen paikalliselle koneelle. Paikallisen koneen paketti siirretään tulevan liikenteen suodattimeen, jossa tarkistetaan, kuuluuko se sallittujen pakettien listalle (input-suodatin). Mikäli paketti kuuluu sallittuihin, se siirretään paikalliselle prosessille (local process). Jos pakettia ei ole tarkoitettu paikalliselle laitteelle, se reititetään edelleen. Ensin tarkistetaan reitityksen päällekytkentä (ip_forward). Jos reititystä ei ole kytketty, paketti poistetaan DROP-toiminnolla. Jos reititys on kytketty, tarkistetaan siihen liityvät forward-säännöt ja tutkitaan, pitääkö paketti reitittää uudelleen. Ulospäin suuntautuvan liikenteen laillisuus tarkistetaan output-suodattimessa. **Iptables**-suodatuksessa liikenne estetään DROP- tai REJECT-toiminnoilla. Liikenne voidaan myös kirjata lokiin LOG-toiminnolla tai hyväksyä ACCEPT-toiminnolla.

Pakettien muokkauksessa voidaan käyttää osoitteenkäännöstä, jolla voidaan muuttaa paketin kohdeosoite toiminnolla DNAT. Lähdeosoite muutetaan toiminnolla SNAT tai voidaan myös käyttää reitittimen liitynnän osoitetta (MASQUERADE). Liikenteen ohjaus toiseen porttiin hoidetaan toiminnolla REDIRECT (Hakala ym. 2006, 206).

Yleisin **iptablesin** käyttötapa työasemassa on estää ulkopuolelta tuleva ei-haluttu liikenne. Tällaisessa suojauksessa estetään ensin kaikki tuleva liikenne ja sen jälkeen sallitaan vain halutut liikennöintitavat (Hakala ym. 2006, 207).

Yllä pähkinänkuoressa kuvattu **iptablesin** toimintaperiaate antaa jonkinlaisen käsityksen siitä, miten vaikeaa sen käyttöön ottaminen ja konfigurointi on. Tämän vuoksi nykyään yhä useammat jakeluversiot sisällyttävät käyttöjärjestelmän asennukseen graafisen työkalun palomuurin asettamiseksi. Tällaisia ohjelmia ovat esimerkiksi Guarddog ja Firestarter. Ne on suunnattu myös aloittelijoille ja keskitason käyttäjille, joten niiden käyttöönotto ei vaadi perehtymistä **iptables**iin.

Vielä joitakin vuosia sitten vain harvan Linux-jakeluversion mukana tuli esiasetettu palomuuriohjelma, nykyisin lähes kaikki merkittävät Linux-versiot ottavat järjestelmän asennuksen yhteydessä graafisella käyttöliittymällä varustetun palomuuriohjelman käyttöön. Seuraavassa kuvassa (Kuva 6.) esitetään Firestarter-palomuurin käyttöliittymä. Kuvassa näkyvät aktiiviset verkkoyhteydet (alimpana), sekä saapuvat ja lähtevät paketit ja palomuurin tila (aktiivinen). Keskellä kuvaa näkyy tietoa verkkolaitteista, yhteystyypeistä, sekä vastaanotetun ja lähetetyn liikenteen määrä megatavuina. Keskellä oikealla Activity-sarakkeessa näkyy käytetty kaistanleveys kilotavuina sekunnissa.

Kuva 6. Firestarter-palomuurin käyttöliittymä (Junnonen, Firestarter screenshots)

Linux-käyttöjärjestelmän tietoturvan kokonaiskuva muodostuu palomuurin lisäksi monesta muustakin asiasta. Palomuuri on hyvä lisä, mutta se ei yksin ole riittävä tae työaseman turvallisuuden takaamiseksi. (Rantala 2003, 332.)

10 HAITTAOHJELMAT

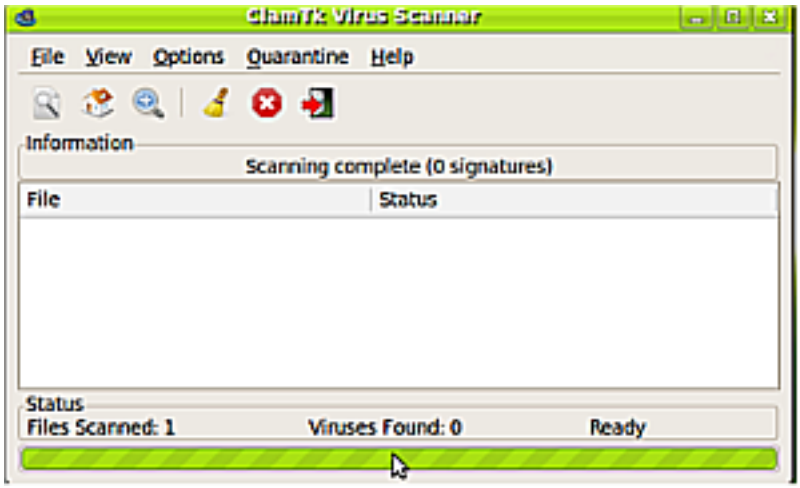
Linux on kulkenut pitkän tien Unixiin pohjautuvana käyttöjärjestelmänä. Koska Unix – ja siis myös siihen pohjautuva Linux – oli alunperinkin suunniteltu moniajojärjestelmäksi, otettiin siinä alusta lähtien tietoturva vakavasti. Tämä ei kuitenkaan tarkoita, että Linux-käyttäjät olisivat turvassa haittaohjelmilta. (Järvinen 2002, 272.)

Linuxin Windowsia parempi tilanne haittaohjelmien suhteen on seurausta Linux-käyttäjien lukumäärän vähäisyydestä verrattuna markkinajohtajan, Windowsin käyttäjämääriin. Toisaalta Linuxia työasemissaan, miksei palvelimissakin, käyttävät ovat vielä nykyäänkin keskivertokäyttäjiä taitavampia tietokoneen käyttäjiä. He osaavat ottaa tietoturvan huomioon tekemisissään.

Jos käy, kuten Järvinen (2002, 272) uskoo, eri käyttöjärjestelmille yhteiset sovellukset tulevat yleistymään ja samalla myös Linuxin nykyisenkaltainen ”lintukotoelämä” päättyy.

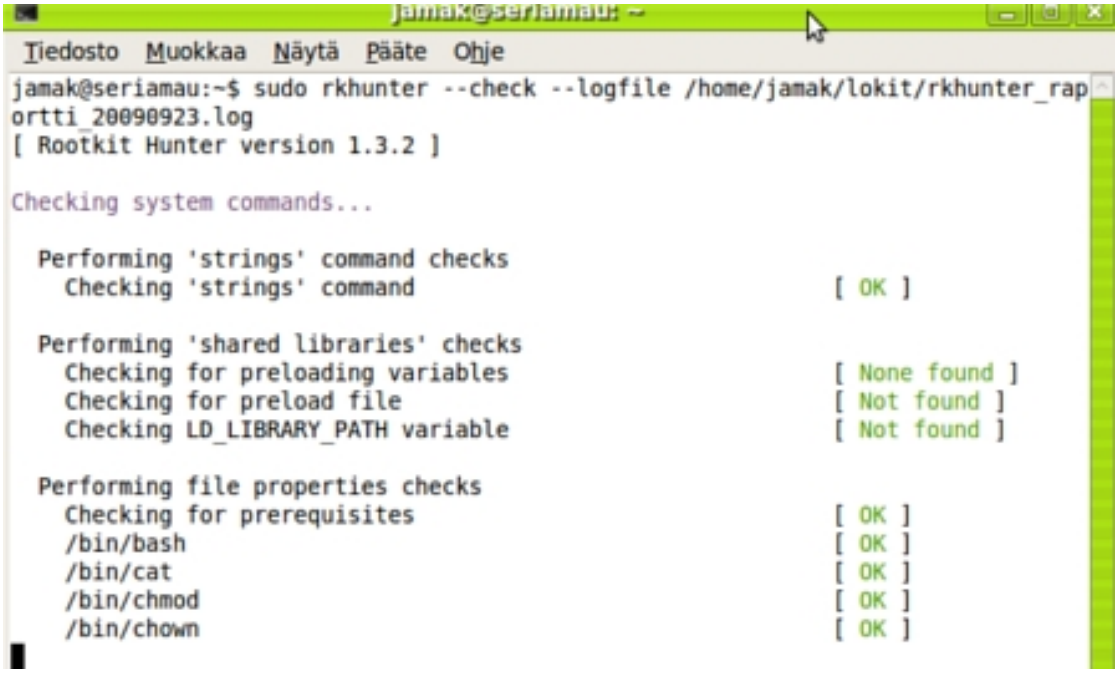
Useat tietoturvaohjelmistoja valmistavat yhtiöt tekevät ilmaisia anti-virusohjelmia Linuxille. Tunnettuja ja yleisesti käytettyjä ilmaisohjelmia ovat islantilainen F-Prot ja kehitystyönsä eri puolille maailmaa jakanut ClamAV. Myös isot kaupalliset toimijat, kuten suomalainen F-Security tarjoavat haittaohjelmatorjuntaa Linux-palvelimille ja -työasemille.

Kuvassa 7 näkyy ilmainen antivirus-ohjelma ClamAv ja sen graafinen käyttöliittymä ClamTk toiminnassa:



Kuva 7. ClamTk virus-skanneri toiminnassa. Viruksia ei löytynyt.

Virusten lisäksi on muitakin haittaohjelmia, kuten ns. rootkit-ohjelmat. Rootkitit ovat ohjelmia, joiden avulla pyritään varastamaan tietoja, käynnistämään palvelunestohyökkäyksiä tai salaamaan tunkeutujan aikaansaannoksia. Linuxissa rootkit-ohjelmia voi yrittää havaita **chkrootkit**- ja **rkhunter**-ohjelmilla. Kuvassa 8 esitellään **rkhunter**-ohjelman käyttöä.



Kuva 8. Rootkit Hunter (rkhunter)-ohjelma etsii rootkit- ja takaoviohjelmia.

Kun **rkhunter**-ohjelma käynnistetään, sille annetaan parametrit ja kerrotaan, tallennetaanko ohjelman tulostama lokitiedosto. Lokitiedostosta voi ohjelman ajamisen jälkeen

tarkistaa yksityiskohtaisesti mahdolliset rootkit-ohjelmat ja sen, minne rootkitit ovat sijoittuneet tiedostojärjestelmässä. **Chkrootkit**-ohjelma toimii pitkälti samalla tavalla kuin **rkhunter**. Ohjelma käy läpi järjestelmän binääritedostot ja lokitiedostot ja tutkii, onko niitä muutettu. Muutetuista tiedostoista annetaan varoitus. **Chkrootkit** tekee käyttäjän niin halutessa lokitiedoston, josta voi tarkastella ohjelman löytämiä poikkeamia.

11 OHJELMIEN PÄIVITTÄMINEN

Eri jakeluversioilla on omat ns. paketinhallintatyökalunsa. Debian käyttää **apt** ja **aptitude**-ohjelmia ja Fedora Red Hatin kehittämää **RPM**-järjestelmää, sekä sen kehittyneempää versiota **yum**ia. Näiden työkalujen tarkoitus on helpottaa järjestelmän ylläpitoa ja ohjelmien ja päivitysten asentamista.

Linuxin alkutaipaleella ohjelmien asentaminen ja päivittäminen vaati jonkin verran seikkailuhenkeä. Ohjelmat piti kääntää lähdekoodista konekielelle. Ensin haettiin ohjelma netistä, minkä jälkeen lähdekoodipaketti purettiin. Seuraavaksi ajettiin skripti **./configure** ja toivottiin parasta. Usein ohjelman ajaminen tyssäsi johonkin kehityskirjaston riippuvuusongelmaan. Kun **configure**-skripti oli ajettu, ohjelma käännettiin komennolla **make**. Sen jälkeen komennettiin pääkäyttäjän oikeuksin **make install**.

Koska ohjelmien asentaminen oli aluksi noin työlästä, kehitettiin mainitut työkalut käyttäjien riemuksi. Nykyiset paketinhallintatyökalut osaavat ottaa huomioon tarvittavat kirjastoriippuvuudet ja tarvittaessa noutaa verkosta puuttuvat kirjastot.

Järjestelmän pitäminen ajantasaisena vaatii uusimpien ohjelmaversioiden asentamista. Ne eivät ainoastaan tuo uusia ominaisuuksia ohjelmiin, vaan paikkaavat myös tietoturva-aukkoja. Niinpä päivitysten asentaminen kannattaa ottaa tavaksi tai jopa automatisoida.

12 SELINUX

Järjestelmän turvallisuuden parantamiseen on olemassa vielä joitakin edistyksellisiä työkaluja, joiden käyttö vaatii jo huomattavaa perehtymistä. Eräs tällainen työkalu on SELinux, Security Enhanced Linux. Se on Yhdysvaltain kansallisen turvallisuusviranomaisen, NSA:n, kehittämä laajennus Linuxiin. Sen avulla Linuxin käytönvalvonnan turvallisuustasoa voidaan nostaa.

SELinux perustuu pakollisen pääsynvalvonnan (mandatory access control, MAC) käyttöön. Pakollisessa pääsynvalvonnassa tiedot ja käyttäjät luokitellaan eri ryhmiin ja luokituksen mukaan voidaan kieltää tai sallia käyttäjiltä pääsy johonkin tietoon (TUT, 2005).

SELinuxissa on ytimeen liitettäviä osia ja siihen kuuluvia apuohjelmia. Nykyisissä, ainakin yleisimmin käytetyissä Linux-jakeluversioissa, SELinux on jakelun mukana, joten sitä ei tarvitse erikseen asentaa.
SELinuxin voi asettaa käyttöönoton yhteydessä toimimaan kahdessa eri tilassa. Ensimmäisessä tilassa SELinux ainoastaan varoittaa käyttäjää tilanteissa, joissa asetettuja säännöstöjä rikotaan. Tilasta käytetään nimitystä salliva tila eli *permissive*. Toisessa tilassa, eli toimeenpanevassa tilassa, *enforced*, SELinux estää asetettujen sääntöjen rikkomisen (Kuutti & Rantala 2007, 329).

SELinuxin käyttöönotto on varsinaisen käyttöjärjestelmän asentamista vaativampi suoritus ja vaatii siksi huolellisuutta ja perehtymistä. Tavallisen kotikäyttäjän ei edes ole tarpeellista asentaa laajennusta.

SELinux toimii itsenäisesti, eivätkä muut Linuxin oikeuksienhallintaan ja turvallisuuteen liittyvät asetukset ja ohjelmat vaikuta sen käyttöön. SELinuxin voidaankin sanoa täydentävän tavallista Linux-asennusta (Kuutti & Rantala 2007, 329).

13 TUNKEUTUMISEN HAVAITSEMINEN JA ESTÄMINEN

Palomuurin ja järjestelmän toiminnasta kertovien lokien lisäksi tietojärjestelmässä olisi hyvä olla jokin menetelmä, jolla pystyisi havaitsemaan, onko järjestelmään tunkeuduttu. Tällaisia menetelmiä kutsutaan tunkeilijan havaitsemisjärjestelmiksi, englanniksi Intrusion Detection System, IDS. IDS-järjestelmässä on erilaisia sisäänrakennettuja sääntöjä, joita verrataan lokien dataan ja palomuurin tavanomaiseen liikenteeseen (Savonia AMK 2008).

IDS-järjestelmiä on kahdenlaisia: laitekohtaisia (Host IDS) ja verkkopohjaisia (Network IDS). Konekohtaiset järjestelmät tarkkailevat lokeja tai tiedostojärjestelmän muutoksia ja verkkopohjaiset taas tutkivat verkon liikennettä (Tietokone 2005).

Mahdollisen tunkeutumisen jälkeen otetaan käyttöön tunkeutumisen estämiseen tarkoitetut menetelmät, joista käytetään nimeä intrusion prevention system, IPS. Kuten IDS, on myös IPS verkko- tai järjestelmätasolla toteutettu tunkeutumisia estävä järjestelmä.

IDS-järjestelmä on tehokas silloin, kun se mahdollisimman nopeasti havaitsee tunkeutumisyrityksen ja antaa mahdollisuuden tunkeutumisen torjuntaan käyttämällä IPS-järjestelmää. Nyrkkisääntönä on, että mitä aikaisemmassa vaiheessa tunkeutumisyritys havaitaan, sitä vähemmän vahinkoa aiheutuu (Viestintävirasto 2007).

Linuxiin on saatavana useita tunkeutumisen havaitsemiseen ja estämiseen tarkoitettuja ohjelmistoja. Eräs tällainen on **Snort**, vapaaseen lähdekoodiin perustuva IDS-ohjelma. Snortissa on IDS-säännöstö, jonka avulla voidaan tarkkailla tietoliikennettä.

14 YHTEENVETO

Tiesin aihetta valitessani tietoturvan olevan hyvin laaja kokonaisuus. Mitä en tiennyt oli se, että myös Linux-työaseman tietoturva on iso kokonaisuus. Kun otin tavoitteeksi selvittää, miten Linuxin tietoturvaa hallitaan, ajattelin, etten noin kymmenen vuoden Linux-kokemuksella enää löydä juuri mitään uutta asiasta. Olinpa väärässä. Käyttäjä-

tunnusten ja -ryhmien hallinnassa riitti opiskeltavaa, samoin tiedostojen käyttöoikeuksien kanssa.

Työn kestäessä päädyin siihen tulemaan, että Linuxin turvallinen käyttö edellyttää yllättävän paljon osaamista. Muihin käyttöjärjestelmiin tottuneille oppimiskynnys on varsin korkea ja tarvitaan harrastuneisuutta, jotta jaksaa kivuta ylöspäin Linux-tikapuilla. Oma kokemukseni Linux-työaseman kanssa on ollut voittopuolisesti palkitseva, äärimmäisen turhautumisen lomassa, tietysti.

En usko, että Linux yleistyy ihan pian työasemien käyttöjärjestelmänä. Sen vuoksi se saa olla vielä hetken verraten rauhassa suurelta haittaohjelmainvaasiolta. Kun Linux-käyttäjien määrä hiljalleen lisääntyy, kasvaa myös ymmärrys hyvistä tietoturvakäytännöistä, joiden varassa Linuxia on kehitetty jo pitkälti toistakymmentä vuotta.

LÄHTEET

Durham, J. 2002. Linux+ -sertifikaatti. 1. painos. Helsinki: IT-press.

Junnonen, T. Firestarter. Screenshots. Saatavissa: http://www.fs-security.com/screenshots.php [viitattu 9.9.2009].

Järvinen, P. 2002. Tietoturva & yksityisyys. 2. painos. Porvoo: Docendo.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. 1.painos. Jyväskylä: Docendo.

Kapanen, T. 2004. Linux koulutuspaketti. 1. painos. Helsinki: IT-press.

Koski, R. 2000. Linux – käyttäjän käsikirja. Jyväskylä: IT-press.

Kuutti, W. & Rantala, A. 2007. Linux. 3. laitos, 1. painos. Porvoo: Docendo.

Pakollinen pääsynvalvonta. Tampereen Teknillinen Yliopisto. Saatavissa: http://sec.cs.tut.fi/maso//teksti.php?id=25 [viitattu 24.9.2009].

Pirtilä, T. 2007. Tietosuoja ja tietoturvallisuus. Luento. 6.9.2007. Kouvola: Kymenlaakson ammattikorkeakoulu.

Rantala, A. 2003. Linux. 1. painos. Porvoo: Docendo.

Siever, E., Figgins, S. & Weber, A. 2003. Linux in a Nutshell. 4. painos. Sebastopol: O'Reilly Media, Inc.

Tunkeilijan havannointi ja IDS. Savonia ammattikorkeakoulu. 2008. Saatavissa: http://openlab.savonia-amk.fi/wiki/index.php/Tunkeilijan_havannointi_ja_IDS_(Goman) [viitattu 25.9.2009].

Tunkeutumisen havaitsemis- ja estojärjestelmät. Viestintävirasto. 2007. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/tunkeutuminen.html [viitattu 25.9.2009].

Varkaita Verkossa. Tietokone. 2005. Saatavissa: http://www.tietokone.fi/lukusali/artikkelit/2005tk10/tunkeilu.htm [viitattu 25.9.2009].