



Koventaminen – Labra 4

Ryhmä 3

Juha-Matti Hietala

Markus Pollari

Topi Liljeqvist

Maija Virta

Oppimistehtävä

Huhtikuu 2023

Tekniikan ala

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

Sisältö

1 Johdanto	4
2 Teoria.....	5
2.1 Linux	5
2.2 Docker	5
2.2.1 Miksi käyttää kontteja?	6
2.3 Wordpress.....	6
2.4 Rkhunter.....	7
3 Dokumentaatio - Linux, Docker & Wordpress koventaminen.....	7
3.1 Linux koventaminen.....	7
3.1.1 Linux – SSH.....	7
3.1.2 Linux – Lynis asentaminen.....	15
3.1.3 Linux – Lynis koventaminen.....	18
3.2 Certbot & Wordpress koventaminen.....	20
3.3 Docker koventaminen	31
3.3.1 SElinux päälle dockeriin	31
3.3.2 Docker toimimaan Rootlessina	33
4 Pohdinta.....	36
Lähteet	37

Kuvat

Kuva 1 VLE harjoitus ympäristö	4
Kuva 2 Snapshot aloitustilanteesta.....	7
Kuva 3 käyttäjien luontia	8
Kuva 4 Käyttäjätöiden testausta	8
Kuva 5 SSH avaimen luontia.....	9
Kuva 6 SSH avainparien luontia	9
Kuva 7 Kopioitu private key	10
Kuva 8 Private key tallennus	10
Kuva 9 Putty Key Generator.....	11
Kuva 10 Putty Key Generator warning.....	11
Kuva 11 Private key.....	12
Kuva 12 Puttyn SSH authentication	12
Kuva 13 Putty Configuration done.....	13

Kuva 14 Kaikkien käyttäjien saved sessions.....	13
Kuva 15 Root käyttäjän SSH kirjatumisen esto	14
Kuva 16 SSH kirjautuminen Puttyn kautta - Markus	14
Kuva 17 Git asennus.....	15
Kuva 18 Lynis asennus.....	15
Kuva 19 Lynis audit system	16
Kuva 20 Lynis audit system alkutilanteen tallentaminen	16
Kuva 21 Lynis audit eka_audit.txt	17
Kuva 22 Lynis suggestions	17
Kuva 23 Lynis kovennus 1	18
Kuva 24 Lynis kovennus 2	18
Kuva 25 Root kirjautuminen	19
Kuva 26 Lynis kovennus 3 – rkhunter työkalun lataaminen	19
Kuva 27 Lynis kovennus 3 – rkhunter	20
Kuva 28 Pluginien lataaminen.....	20
Kuva 29 Instructions for requesting a certificate.....	21
Kuva 30 Ohjeiden seuraamista	21
Kuva 31 Lisäoikeuksia.....	22
Kuva 32 Sertifikaattipyyntö.....	22
Kuva 33 Successfully received certificate	22
Kuva 34 Muutoksia.....	23
Kuva 35 Docker muutokset	23
Kuva 36 Docker ps	23
Kuva 37 Palomuurin muutoksia	24
Kuva 38 Palomuurin muutos	24
Kuva 39 Sertifikaatti	24
Kuva 40 Site address muutos	25
Kuva 41 Lisäoikeuksia.....	25
Kuva 42 chmod -R 777	26
Kuva 43 WordPress 6.1.1	26
Kuva 44 Update themes.....	27
Kuva 45 Onnistuneet päivitykset	27
Kuva 46 Automaattiset päivitykset	28
Kuva 47 Päivitys asetuksien laittamista	28

Kuva 48 Easy Update Manger	28
Kuva 49 Limit login attempts.....	29
Kuva 50 Backup plugin	29
Kuva 51 Backup	29
Kuva 52 Testausta	30
Kuva 53 Kali WPScan.....	30
Kuva 54 Kali WPScan tuloksia	31
Kuva 55 SELinux.....	31
Kuva 56 SELinuxin toiminnan testaus	32
Kuva 57 sudo useradd testuser.....	32
Kuva 58 private key rootless userille	33
Kuva 59 iptables	33
Kuva 60 sudo dnf install -y	34
Kuva 61 Succesfully created context rootless.....	34
Kuva 62 Onnistunut harjoitus	35

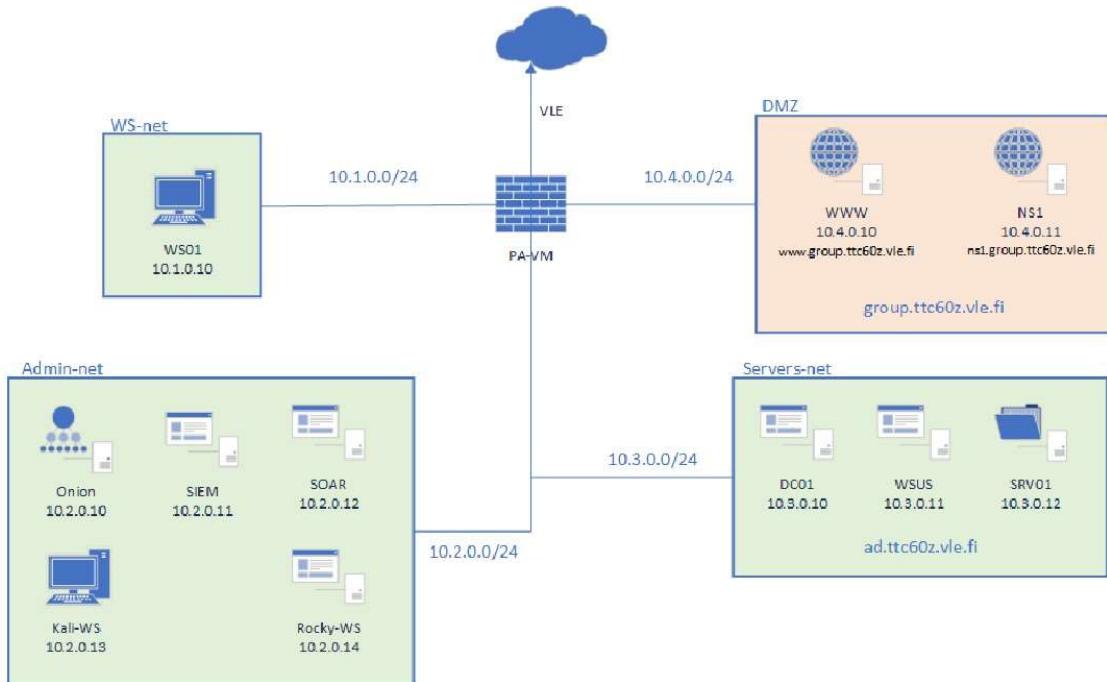
1 Johdanto

Dokumentaatio on osana koventamisen kurssin (TTC6050-3002) laboratorioharjoituksia. Lab4 tarjottuksena on harjoitella Linux, Docker ja Wordpressin koventamista.

Harjoituksen kohteena käytetään WWW-palvelinta. Teorialla ja harjoituksella ryhmän jäsenet saavat taidot ja ymmärryksen Linuxin koventamisesta Lynis ohjelmistolla. Lisäksi tehdään SSH kovennuksia ja Wordpress Kovennuksia asetuksien kautta, sekä Docker kovennuksia. Kokonaisuus on laaja ja jaettuna useammalle viikolle.

Harjoituksen kokonaisuus dokumentoidaan kuvankaappaauksilla, joiden avulla havainnollistetaan harjoitustekniikat. Osa-alueet on jaettu omiksi kokonaisuuksiksi luettavuuden takia. Lisäksi harjoitustyössä esitetään teoria Linuxista, Dockerista ja Wordpressistä yleisesti. Harjoitustyön lopussa lisäksi esitetään pohdinta harjoitustyön tekemisestä.

1. Ympäristö



Kuva 1 VLE harjoitus ympäristö

2 Teoria

2.1 Linux

Linux on käyttöjärjestelmän ydin (eng. kernel), joka on lisensioitu GPLv2-lisenssillä. Sen on kehittänyt Linus Torvalds ja se on julkaistu vuonna 1991.

Linux-ydin on osa käyttöjärjestelmää, sen alimmalla osalla lähimpänä tietokonelaitteista. Ydin on kuin siemen kovan kuoren sisällä, ja se on käyttöjärjestelmässä ja ohjaa kaikkia laitteiston tärkeimpiä toimintoja, olipa kyseessä puhelin, kannettava tietokone, palvelin tai mikä tahansa muu tietokone. (What is the Linux kernel? 2019.)

Käyttöjärjestelmän kokonaisuuteen kuuluu myös ohjelmakirjastoja, järjestelmäohjelmia, käyttöliittymiä ja sovellusohjelmia. Keskeisimmät ovat Linuxin tapauksessa yleensä GNU-projektiin keräämiä tai kehittämiä. Yleisimpiä ovat Debian GNU/Linux tai Mandriva GNU/Linux. (What is Linux? 2023.)

Linux on vapaa ohjelmisto, minkä takia kuka tahansa voi tehdä siihen muutoksia. Esimerkiksi ero näkyy Linux:issa ja Windows:silla, jotka ovat arkkitehtuuriltaan vastakohtia systeemissä mielessä. Toinen on monoliittinen (Windows, kiinteä paketti) ja toinen atomistinen, mahdollisimman pelkistetty ydin (Linux). (What is Linux? 2023.)

2.2 Docker

Docker on avoimen lähdekoodin alusta sovellusten kehittämiseen, julkaisemiseen ja suorittamiseen. Sen avulla pystyy erottamaan sovellukset muusta infrastruktuurista Dockerin tarjoamalla kyllä pakata sovellukset kontteihin, jotka ovat kevyitä ja sisältävät kaikki sovelluksen suorittamiseen vaaditut riippuvuudet. Näin ei tarvitse välittää siitä, mitä isäntäkoneelle on asennettu. Kontit ovat erillisiä toisistaan omilla työkaluillaan, mutta pystyvät kommunikoimaan toistensa kanssa. (Docker overview, n.s; del Alba, 2022)

Kontteja verrataan monesti virtuaalikoneisiin, mutta näiden välillä on joitain tärkeitä eroavaisuuksia. Virtuaalikoneet toimivat täydellä kopiolla käyttöjärjestelmästä, kun taas kontit jakavat isän-

täytimen, joka tekee niistä huomattavasti kevyempiä ja tehokkaampia virtuaalikoneisiin verrat-tuna. Docker kontteja pystyy käyttämään kaikissa koneissa, joissa on Docker engine asennettuna. (del Alba, 2022)

Docker on kirjoitettu Go-ohjelmointikielellä ja se hyödyntää useita Linux-ytimen ominaisuuksia toi-mintaansa. Docker käyttää "namespaces" teknologiaa konttien eristämiseen. Kun kontti ajetaan, Docker luo joukon namespaceja kyseiselle kontille. Jokainen kontin osa toimii erillisessä namespa-cessa ja sen käyttöoikeus on rajoitettu kyseiseen namespaceen. (Docker overview, n.s)

2.2.1 Miksi käyttää kontteja?

Konttien käyttöön on monia syitä, ohessa esitetty muutama oleellinen:

Joustavuus: Kontteja pystyy käyttämään millä tahansa alustalla, joka tukee Dockeria. Alusta voi olla esimerkiksi serveri, virtuaalikone, pilvipalvelussa oleva kone tai läppäri. Tämä tekee ohjelmistojen siirtelystä alustalta toiselle helppoa ja helpottaa myös DevOps tiimien työskentelyä kehityk-sessä, testauksessa ja tuotannossa. (del Alba, 2022)

Nopeus: Kontit pystytään käynnistämään ja sulkemaan nopeasti, mikä tekee niistä ideaaleja ohjel-mille, jotka täytyy käynnistää nopeasti tarvittaessa. (del Alba, 2022)

Toistettavuus: Kontit voidaan helposti monistamaan tehdäkseen identtisiä kopioita tietystä ympä-ristöstä. Tämä on käytännöllistä luodessa testaus- ja kehitysympäristöjä, jotka vastaavat tuotanto-ympäristöä. (del Alba, 2022)

Turvallisuus: Kyky eristää kontit helpottavat ohjelmistojen suojaamista hyökkäyksiä ja vahingossa tapahtuvia tietovuotoja vastaan. (del Alba, 2022)

2.3 Wordpress

Teknisellä tasolla WordPress tarkoittaa avoimen lähdekoodin sisällönhallintajärjestelmää, joka on nopea sekä luotettava ja joka perustuu PHP (PHP, Hypertext Preprocessor) -ohjelmointikieleen sekä MySQL-tietokantaan (Kinnunen 2019, 4).

Wordpress on lisensioitu GPLv2 mukaisesti, mikä tarkoittaa, että kuka tahansa voi muokata tai käyttää WordPress -ohjelmistoa ilmaiseksi. Wordpress on suosituin WWW- sisällönhallintajärjestelmä. (Kinnunen 2019, 4.)

2.4 Rkhunter

Rkhunter (Rootkit Hunter) on tietoturva valvontatyökalu POSIX yhteensopiville järjestelmiille. Sen avulla pystytään skannaamaan ympäristöä mahdollisilta haavoittuvuuksilta kuten rootkiteiltä. Rkhunter etsii mm. rootkittien oletushakemistoja, väärin määritettyjä käyttöoikeuksia piilotettuja tiedostoja ja vertaa tärkeiden tiedostojen hasheja tunnettuihin hyviin tiedostoihin. (rkhunter, 2022)

3 Dokumentaatio - Linux, Docker & Wordpress koventaminen

3.1 Linux koventaminen

3.1.1 Linux – SSH

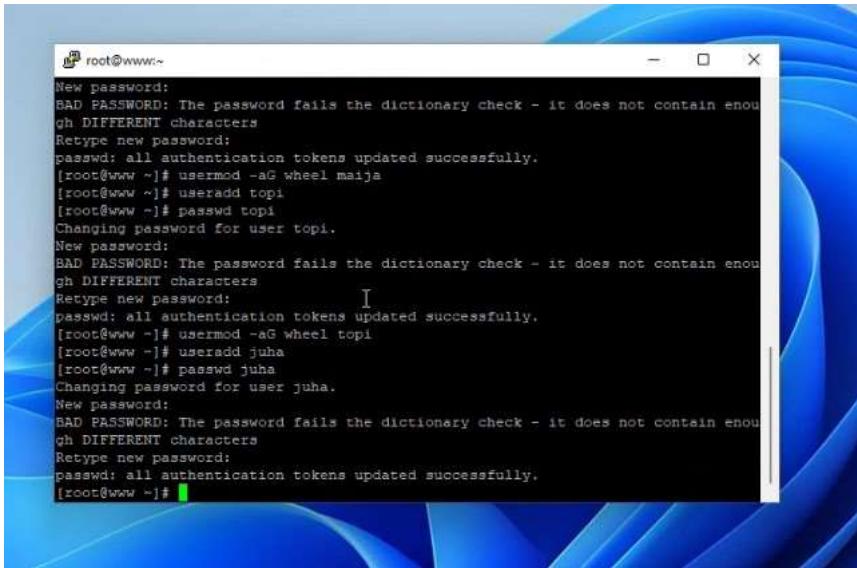
Aloitettiin labra ottamalla snapshot labra aloitustilanteesta. Sekä sallimalla Palo Altosta WStoDMZ kun otetaan ssh yhteys WS01 koneelta Puttyn kautta WWW:lle.



Kuva 2 Snapshot aloitustilanteesta

Kirjauduttiin WS01 koneelta SSH yhteydellä Pyttulle WWW:lle. Luotiin kaikille ryhmäläisille oma tunnus koneelle, sudo oikeuksin. Esitetty kuvassa 3.

```
useradd topi
passed topi
usermod -aG wheel topi
```



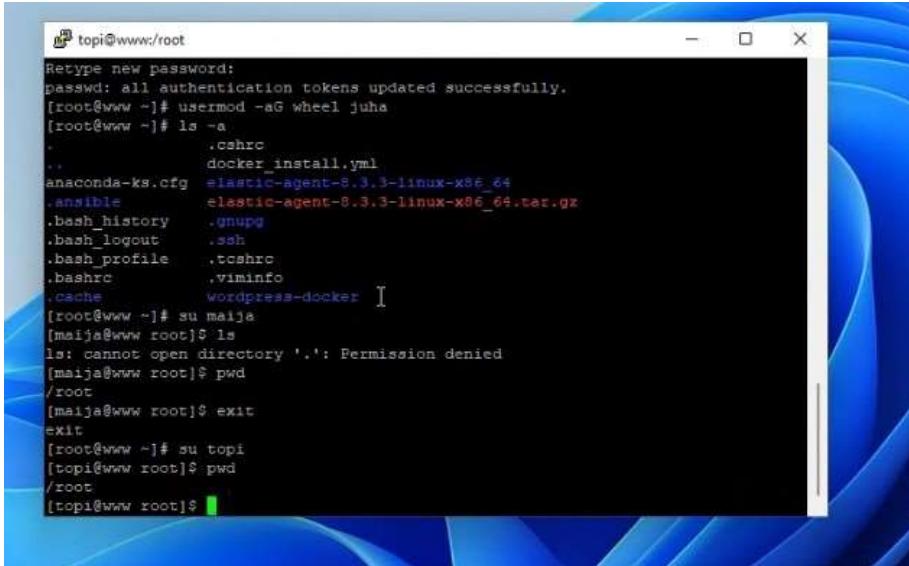
```

root@www:~#
New password:
BAD PASSWORD: The password fails the dictionary check - it does not contain enough DIFFERENT characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@www ~]# usermod -aG wheel maija
[root@www ~]# useradd topi
[root@www ~]# passwd topi
Changing password for user topi.
New password:
BAD PASSWORD: The password fails the dictionary check - it does not contain enough DIFFERENT characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@www ~]# usermod -aG wheel topi
[root@www ~]# useradd juha
[root@www ~]# passwd juha
Changing password for user juha.
New password:
BAD PASSWORD: The password fails the dictionary check - it does not contain enough DIFFERENT characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@www ~]#

```

Kuva 3 käyttäjien luontia

Testattiin, että käyttäjät on luotu onnistuneesti, vaihdettiin jokaiseen käyttäjään su-komennolla (esim. su maija). Esitetty kuvassa 4.



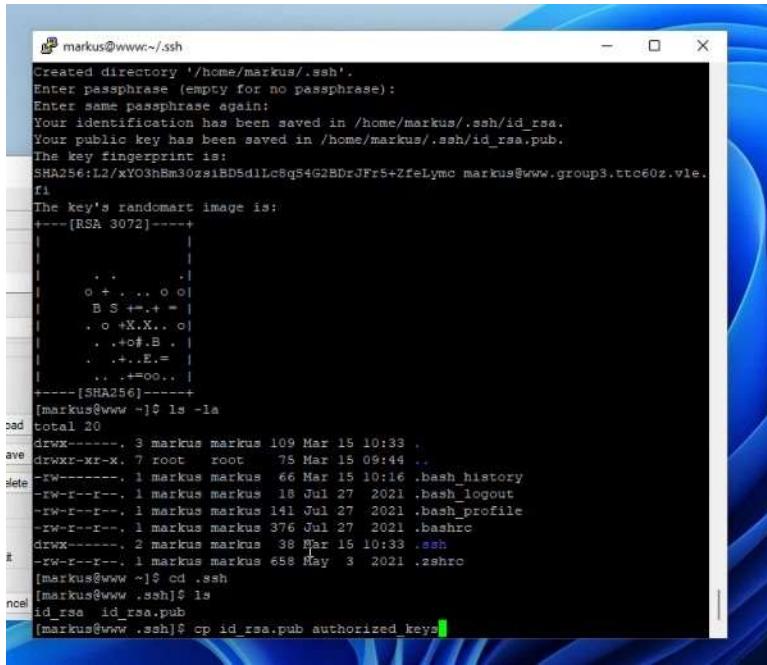
```

topi@www:~#
Retype new password:
passwd: all authentication tokens updated successfully.
[root@www ~]# usermod -aG wheel juha
[root@www ~]# ls -a
.
.. .cshrc
.. docker_install.yml
anaconda-ks.cfg elastic-agent-8.3.3-linux-x86_64
.ansible elastic-agent-8.3.3-linux-x86_64.tar.gz
.bash_history .gnupg
.bash_logout .ssh
.bash_profile .tcshrc
.bashrc .viminfo
.cache Wordpress-docker
[root@www ~]# su maija
[maijs@www root]$ ls
ls: cannot open directory '.': Permission denied
[maijs@www root]$ pwd
/root
[maijs@www root]$ exit
exit
[root@www ~]# su topi
[topi@www root]$ pwd
/zoot
[topi@www root]$

```

Kuva 4 Käyttäjätilien testausta

Seuraavaksi sallittiin SSH jokaisen tunnuksilla. Esimerkiksi Markuksen käyttäjätunnuksen salliminen (Sama toimenpide toistettiin jokaisen tunnuksilla). Luotiin komennolla **ssh-keygen** uusi todennusavainpari SSH:lle. Sitten kopioitiin cp id_rsa.pub → authorised_keys jonka jälkeen kopioitiin private key ja tallennettiin se note++ avulla omaan tiedostoon. Esitetty kuvissa XX

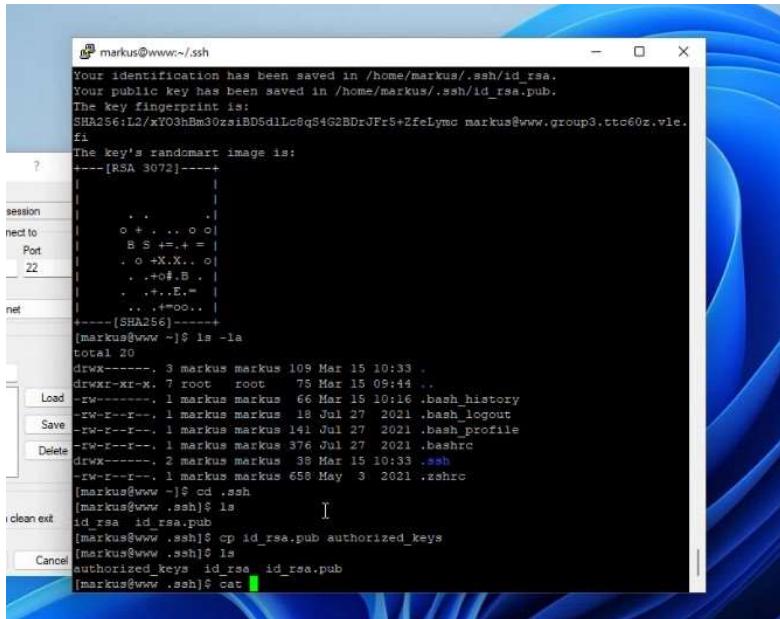


```

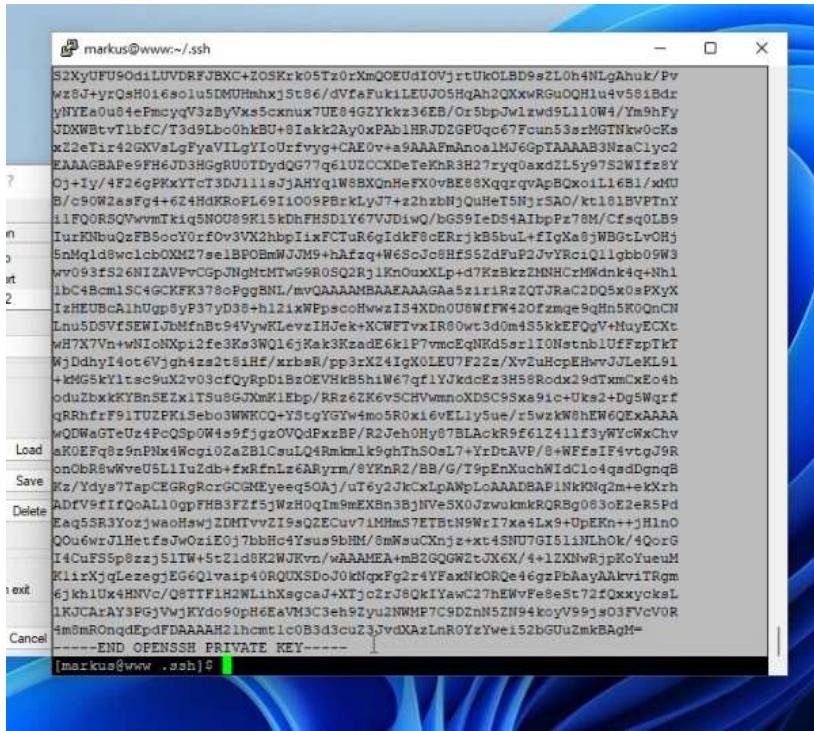
markus@www:~/.ssh
Created directory '/home/markus/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/markus/.ssh/id_rsa.
Your public key has been saved in /home/markus/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:L2/xYO3hBm30zsiBD5d1Lc8qS4G2BDrJFr5+ZfeLymo markus@www.group3.ttc60z.vle.
fi
The key's randomart image is:
+---[RSA 3072]---+
| . . .
| . . .
| . . .
| . . .
| . . .
| . . .
| . . .
| . . .
| . . .
+---[SHA256]---+
[markus@www ~]$ ls -la
total 20
drwx-----, 3 markus markus 109 Mar 15 10:33 .
drwxr-xr-x, 7 root root 75 Mar 15 09:44 ..
-rw-r--r--, 1 markus markus 66 Mar 15 10:16 .bash_history
-rw-r--r--, 1 markus markus 18 Jul 27 2021 .bash_logout
-rw-r--r--, 1 markus markus 141 Jul 27 2021 .bash_profile
-rw-r--r--, 1 markus markus 376 Jul 27 2021 .bashrc
drwx-----, 2 markus markus 38 Mar 15 10:33 .ssh
-rw-r--r--, 1 markus markus 658 May 3 2021 .zshrc
[markus@www ~]$ cd .ssh
[markus@www .ssh]$ ls
id_rsa id_rsa.pub
[markus@www .ssh]$ cp id_rsa.pub authorized_keys

```

Kuva 5 SSH avaimen luontia



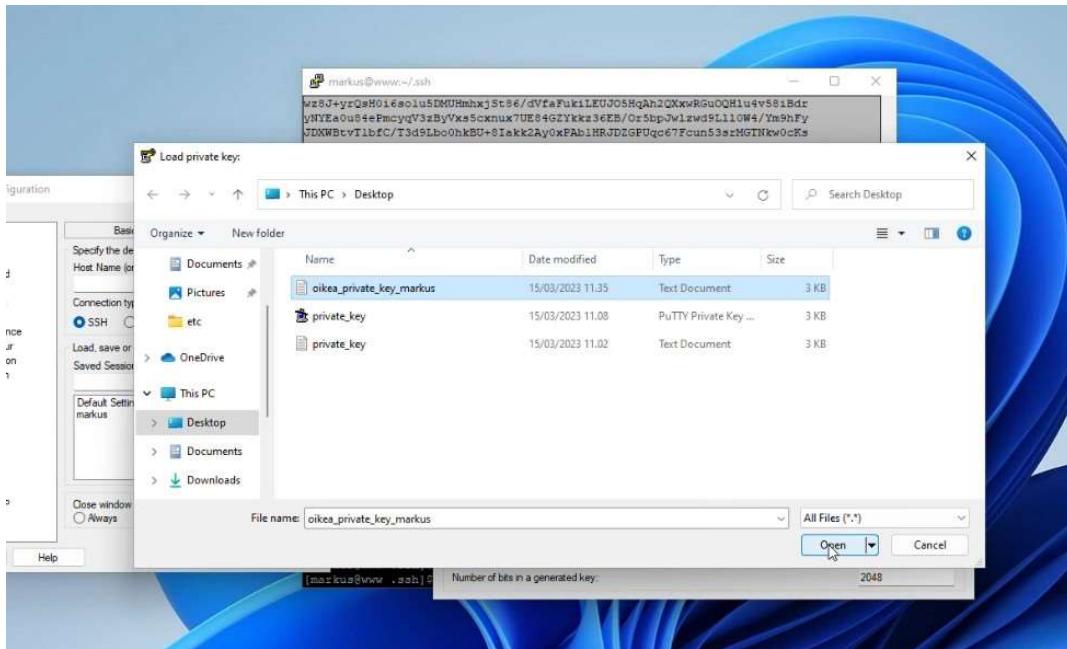
Kuva 6 SSH avainparien luontia



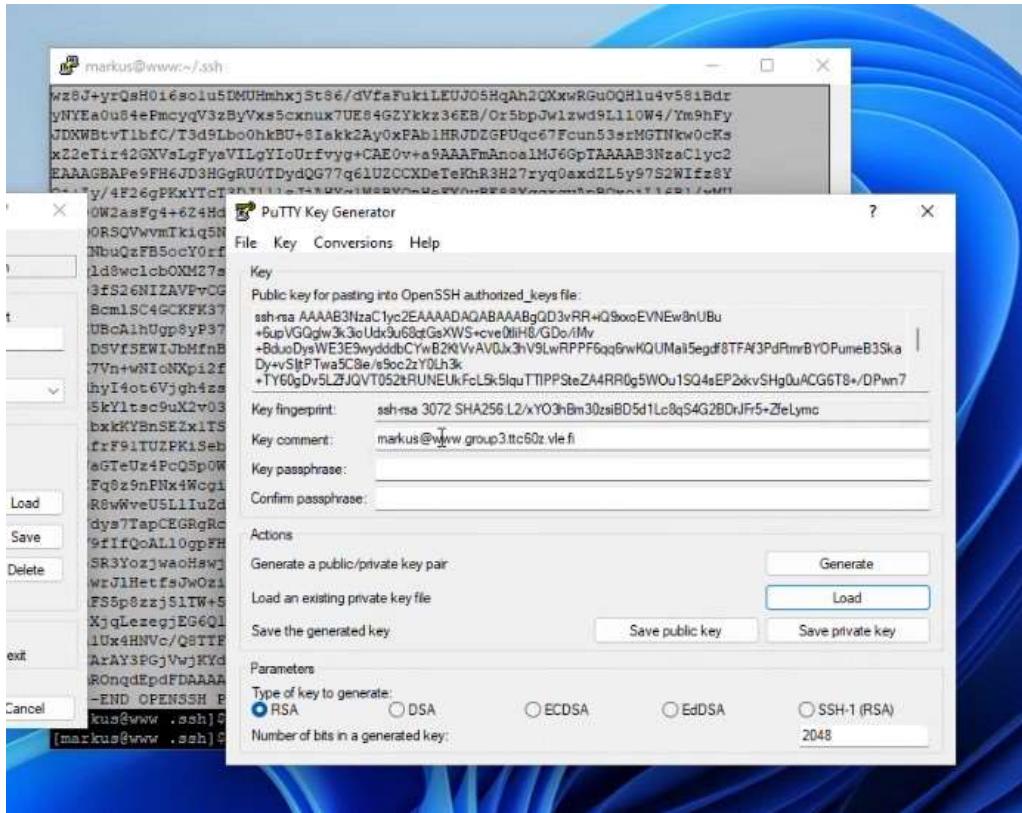
```

markus@www:~/ssh
S2XyUFU90diLUUVDRFJBXC+ZOSKrk05Tz0rXmQCEUD1GVjrTUkCLBD9zL0h4NlgAhuk/Pv
wzSj+yrsQsH016solu5DMUhmhxjSt86/dVfaFuk1LEUJ05HqAh2QXxwRGuOQHlu4v58iBdr
yNVEa0u4eFmcyyqV3zbYVxs5cxnx7UE84GZYkkz36EB/Or5bpJwlwd9L110W4/Ym9hFy
JDXWBtvTlbfC/T3d9Lbo0hkBU+8Iakk2Ay0xPAb1HRJDZGPFUqc67Fcun53srMGTNkw0cRs
xZzeTir42GXVsLgFyaVILyIoUrfvvgy+CAEoV+a9AAAFmAnoelM/6GpTAANAB3nzaCly2
EAAAGBAp89FH6JD3HGGRuOTDydgQ77q6LUZCCMdeTeKhR3H27ryq0axdZL5y97S2Wlfz8Y
Oj+Iy/4F7eqPKXYTC3Dj111sJJAHTq1WSBXQnHeFx0vBES8XqqrqvApBQxoiL16B1/xHU
B/c90W2asFq4+624hdKRoFL69I1005PBrkLyJ7+z2hbzNjQuHET5Hj5sAC/t181BVPtNY
i1FQ0RSQVwmTkisqNGU83k15kDfH5DLY67VJDiwQ/BG591eDS4A1bpPz78M/CfsqOLB9
IurKnbuQzFBsocY0rf0v3VX2hbpIixFCtR6gIdkF8cRRrjkBSbuL+fIqXa8jWBGtLvOHj
5nLqlid8wc1cbOMX27se1B0PbmWJM9M+harfz+wEScjcsHES52dFuP2JvYRciQ1lgb90W93
wv093fS26NzZAVPvGpJNqMtMTw9R0SQ2Rj1KnOuxXlp+47KzBkzZMNHCzRMWdnkq4+nH1
lbC4Bcm1SC4GCKFK378cPggnNL/mvQAJJAMAAEAAAAGRA5z1riRzZQTJRzC2DQ5w0sPxy
IzHEUBcA1huqpbyF37y08+h121xWFpscoHwzL54Xdm0u5WffW42OfzmgeqBQhns5R0QnCN
LnubR58WveIJBmfBc94VwRLevzIHJek-XCWTvrxIR80wt3d0m455kkF0QvMuyECxt
wHTX7Vn+wNi0Nxp1fe3Ks3W016jKak3KzadE6k1p7vncEqNkd5zr110Nstbn10ffFzpTkt
WjDhyI4ot6Vjgh4zs2t81hf/xrbtsR/pb3rX241qK0LEU7F22z/Xv2uHcpEHrvJLeK91
+KMGSkYltsc9uX2v03cfQyRpDiBzOEVHk5hiW6?qf1YJkdcfz3H58Rdx29dTxmCxEo4h
oduBzxkKYBnSEZx1TSu8GJXmR1Epb/RRz6ZK6vsCHVwmnxDSC95xa9ic-Uks2+Dg5Wqrf
qRRhfrF91TUZPK1Seb03WNKCO+YStgYgtw4mo5R0u16EL1y5ue/r5wzKw8tNEW60ExAAAAA
wQDWaGTeUz4FcQSp0W4s9fjgzOVQdPxzBP/R2Jeh0Hy07BLAckR9f612411f3yWycWxChv
aK0EFq8z9nfNxwWcg102aZB1CsulQ4Rmkmlk9ghThNSoL7+YrdtAVP/8+wFfsIF4vtgJ9R
onObR58WveISSL1u2db+fxRfnLz6AByrm/8YKmRZ/BB/G/T9pEnKuchW1dC1o4qdDgngB
Kz/Ydys/TapCEGRgRcrGCGNEyeeg50Aj/uTeyJjkCxLpANyLoAAJDBAP1NkKNq2m+e+kXrh
ADFV9fIfQoAll0gpFHB3F5jWzHoQlm9mEXBn3BjNVeSX0jzwuLkmkRQRBg083oE2eR5Pd
Eq9fSLR58WveISSL1u2db+fxRfnLz6AByrm/8YKmRZ/BB/G/T9pEnKuchW1dC1o4qdDgngB
QoU6wrlJ1HNetfsJwOziE0j7bbfc4Ysuo5bHM/0mNsuCXnjz+xt4SNH7G15LiNLh0k/QorG
I4CuFS5p0zzj5LTW+5t2lsK2WJKvn/wAAAMEA+mBZGQGWitJX6X/4+1ZNwRjpKoYueuM
M1krXjgLezegjEG6Q1vaip40RQUXSDoJ0kNqxFg2+4YFaxHkORQe46gPbAayAAlkv1TRqm
6jkh1Ux4HNv/c/8TTFLH2WLihXagcaJ+xtjzrJ8QkIXyawC7hEWvFe8e5t72fQxycckzL
1KJCArAY3PGjVwjKVdo90pR6EaVM3C3eh9Zyu2NMF7C9DzN5Z194koy989js03FVcVOR
4m5mRONqdEp/FDAAAAAH21hcmtlcoB3d3cu23jvdxAzLnR0YzYwe152bg0u2mkBAqM=
-----END OPENSSH PRIVATE KEY-----
[markus@www .ssh] $
```

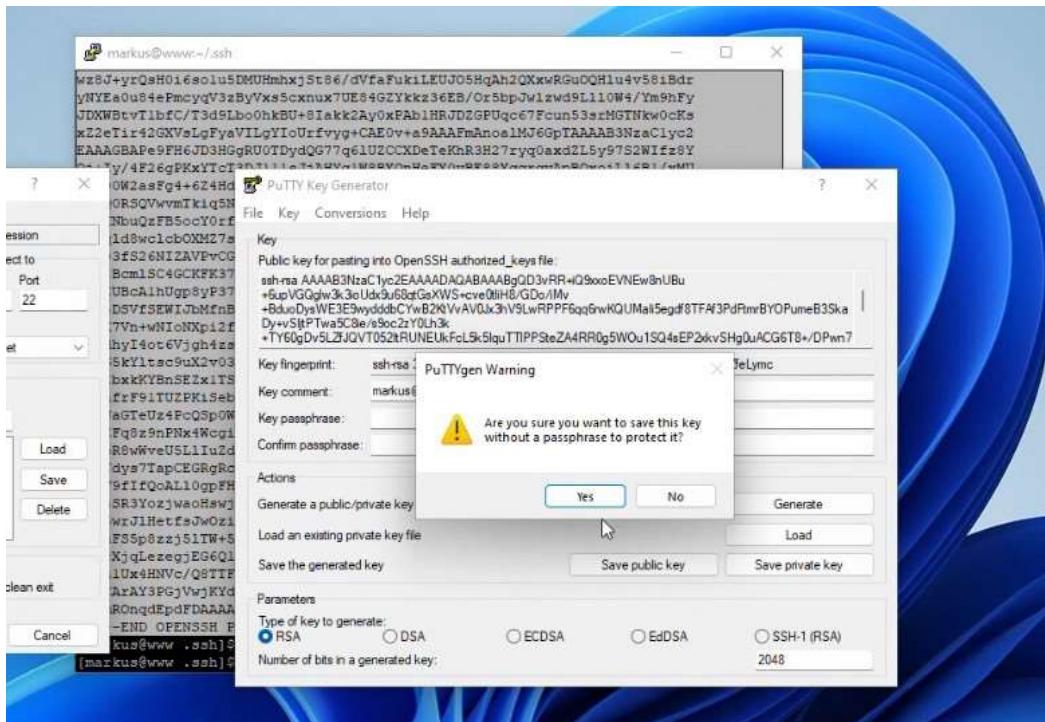
Kuva 7 Kopioitu private key



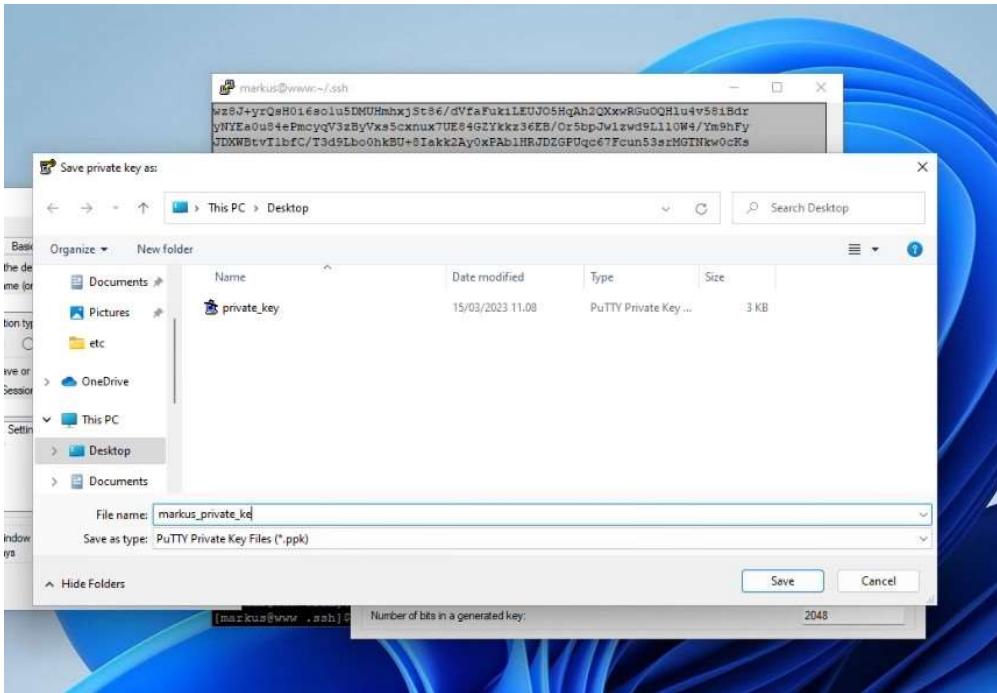
Kuva 8 Private key tallennus



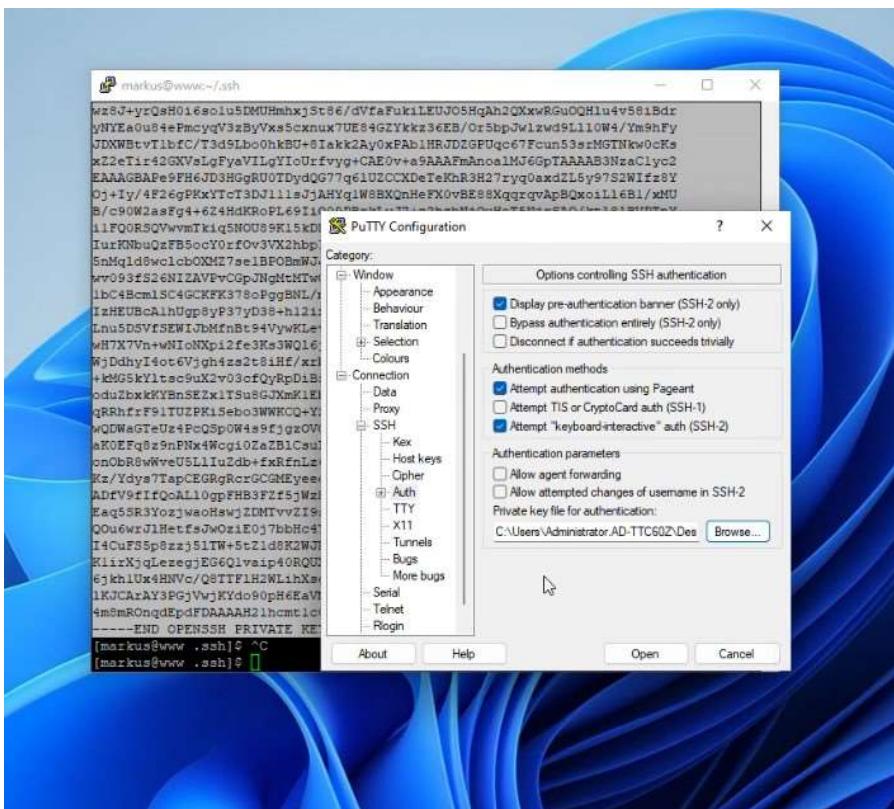
Kuva 9 Putty Key Generator



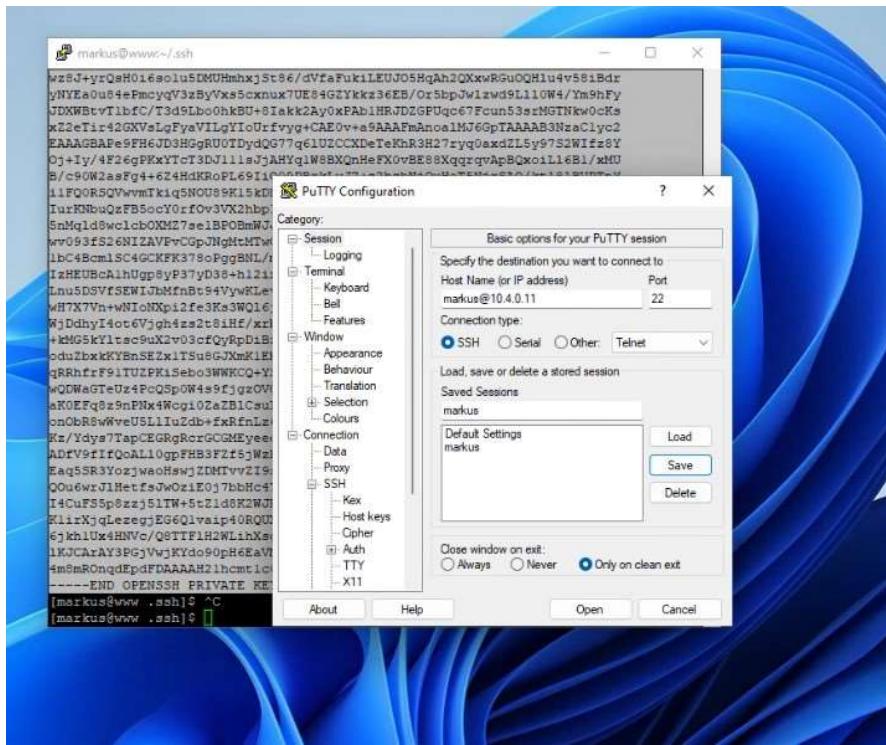
Kuva 10 Putty Key Generator warning



Kuva 11 Private key

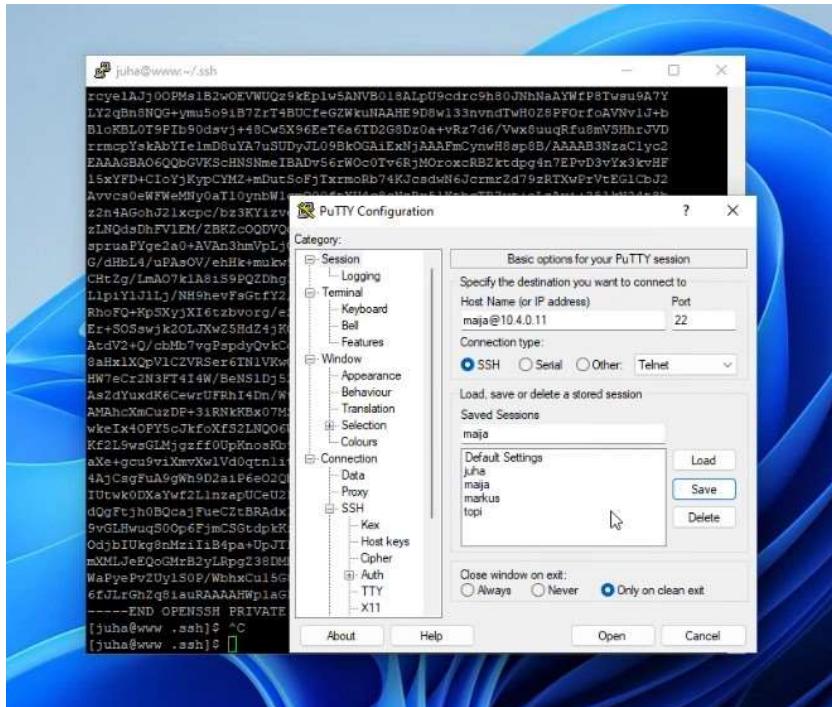


Kuva 12 Puttyn SSH authentication



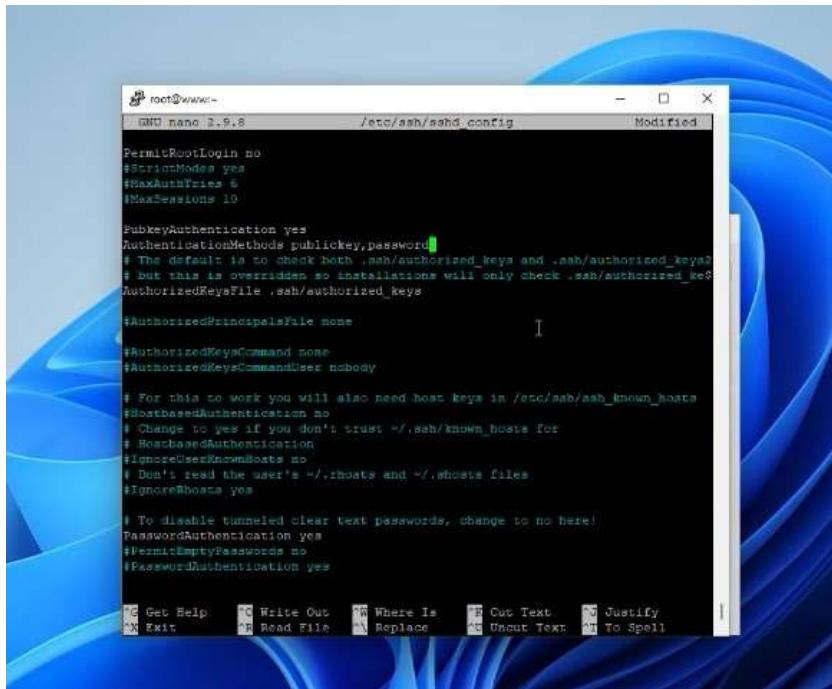
Kuva 13 Putty Configuration done

Kaikille luodut tallennetut kirjautumistiedot jatkossa kirjautumista helpottamaan. Esitetty kuvassa alla.



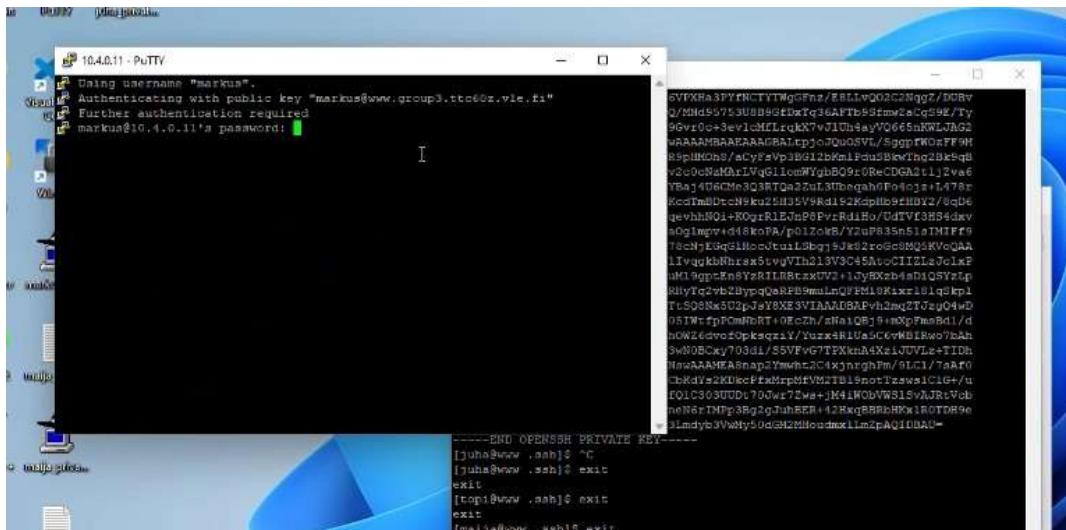
Kuva 14 Kaikkien käyttäjien saved sessions

Komennoilla sudo nano etc/ssh/sshd_config muokattiin: estettiin SSH kirjautuminen root-käytäjältä ja lisättiin että kirjautuminen vaatii todennuksen (publickey) ja salasanan (Kuva 15).



Kuva 15 Root käyttäjän SSH kirjatumisen esto

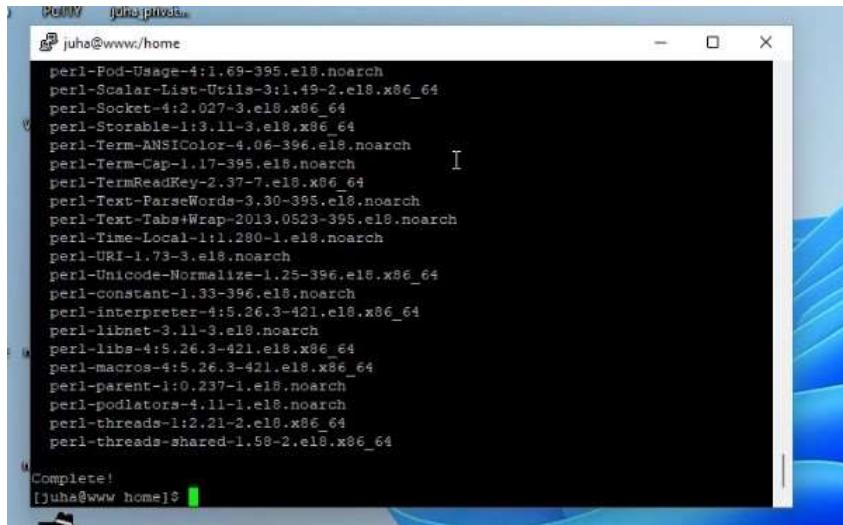
Testataan toimivuutta, eli Putlyn kautta pitäisi päästää kirjautumaan tallennetuilla tiedoilla niin että salasanaa kysytään. Toimii ongelmitta joka tunnuksella, esitetty alla Markuksen tunnuksilla kirjautuminen kuvassa 16.



Kuva 16 SSH kirjautuminen Puttyn kautta - Markus

3.1.2 Linux – Lynis asentaminen

Ensin gitin asentaminen(Kuva 17), kun oli ensin PaloAltosta otettu lataamisen estävä sääntö pois (DMZ to VLE). Asennus komennolla **sudo dnf install git**.

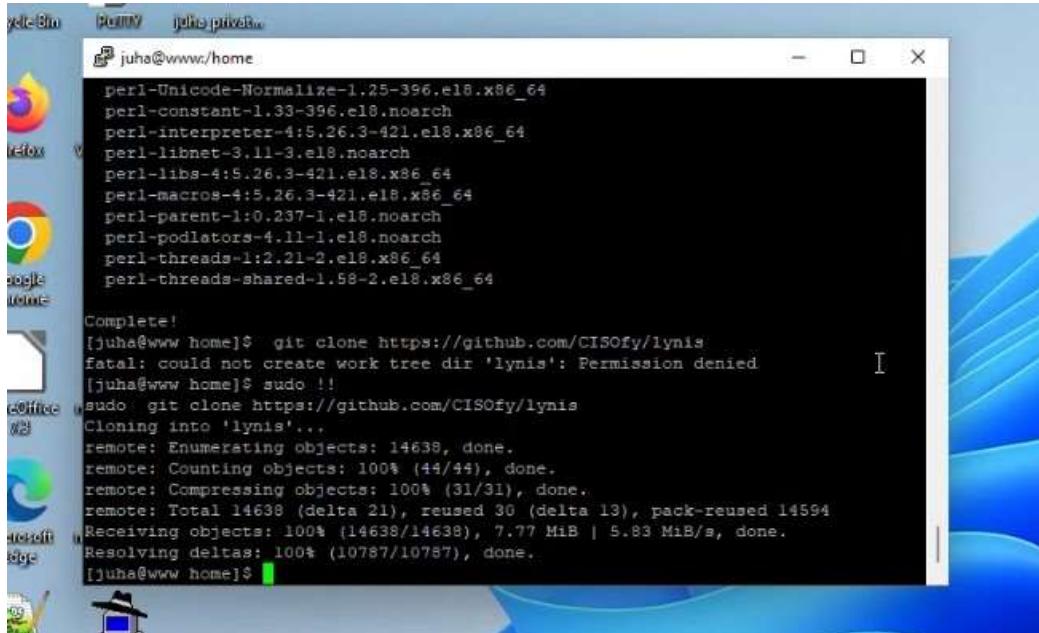


```
Perl-W  juha private
juha@www:/home
perl-Pod-Usage-4:1.69-395.el8.noarch
perl-Scalar-List-Utils-3:1.49-2.el8.x86_64
perl-Socket-4:2.027-3.el8.x86_64
perl-Storable-1:3.11-3.el8.x86_64
perl-Term-ANSIColor-4.06-396.el8.noarch
perl-Term-Cap-1.17-395.el8.noarch
perl-TermReadKey-2.37-7.el8.x86_64
perl-Text-ParseWords-3.30-395.el8.noarch
perl-Text-Tabs+Wrap-2013.0523-395.el8.noarch
perl-Time-Local-1:1.280-1.el8.noarch
perl-URI-1.73-3.el8.noarch
perl-Unicode-Normalize-1.25-396.el8.x86_64
perl-constant-1.33-396.el8.noarch
perl-interpreter-4:5.26.3-421.el8.x86_64
perl-libnet-3.11-3.el8.noarch
perl-libs-4:5.26.3-421.el8.x86_64
perl-macros-4:5.26.3-421.el8.x86_64
perl-parent-1:0.237-1.el8.noarch
perl-podlators-4.11-1.el8.noarch
perl-threads-1:2.21-2.el8.x86_64
perl-threads-shared-1.58-2.el8.x86_64

Complete!
[juha@www home]$
```

Kuva 17 Git asennus

Sitten Lynis asennus komennolla: **git clone https://github.com/CISOfy/lynis** (Kuva 18).



```
yele-Bin  Perl-W  juha private
juha@www:/home
perl-Unicode-Normalize-1.25-396.el8.x86_64
perl-constant-1.33-396.el8.noarch
perl-interpreter-4:5.26.3-421.el8.x86_64
perl-libnet-3.11-3.el8.noarch
perl-libs-4:5.26.3-421.el8.x86_64
perl-macros-4:5.26.3-421.el8.x86_64
perl-parent-1:0.237-1.el8.noarch
perl-podlators-4.11-1.el8.noarch
perl-threads-1:2.21-2.el8.x86_64
perl-threads-shared-1.58-2.el8.x86_64

Complete!
[juha@www home]$ git clone https://github.com/CISOfy/lynis
fatal: could not create work tree dir 'lynis': Permission denied
[juha@www home]$ sudo !!
[sudo] password for juha:
sudo: git clone https://github.com/CISOfy/lynis
Cloning into 'lynis'...
remote: Enumerating objects: 14638, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (31/31), done.
remote: Total 14638 (delta 21), reused 30 (delta 13), pack-reused 14594
Receiving objects: 100% (14638/14638), 7.77 MiB | 5.83 MiB/s, done.
Resolving deltas: 100% (10787/10787), done.
[juha@www home]$
```

Kuva 18 Lynis asennus

Seuraavaksi ajettiin **-/lynis audit system** komento, jonka perusteella voidaan katsoa ehdotettuja kovennuksia. Esitetty kuvassa 19 alla.

```
[+] Name services
- Checking search domains [ FOUND ]
- Searching DNS domain name [ FOUND ]
  Domain name: group3.ttc60z.vle.fi
- Checking /etc/hosts [ NONE ]
  - Duplicate entries in hosts file [ NOT FOUND ]
  - Presence of configured hostname in /etc/hosts [ NOT FOUND ]
  - Hostname mapped to localhost [ OK ]
  - Localhost mapping to IP address [ OK ]

[+] Ports and packages
-----[+]
- Searching package managers [ FOUND ]
  - Searching DNF package manager
    - Querying DNF package manager [ FOUND ]
  - Using DNF to find vulnerable packages [ NONE ]
  - Checking package audit tool
    Found: dnf [ INSTALLED ]

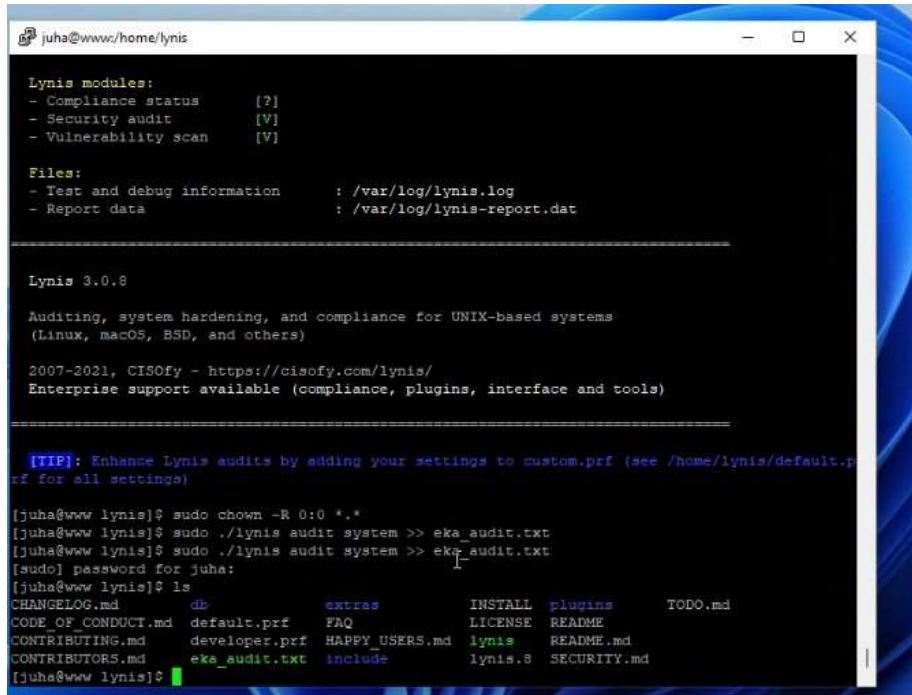
[+] Networking
```

Kuva 19 Lynis audit system

Otettiin talteen lyniksen auditoinnin jälkeen 'alkutilanne' ennen kuin tehdään kovennukset. Komentolla **sudo ./lynis audit system >> eka_audit.txt** esitetty kuvissa alla.

```
[juha@www lynis]$ ls
CHANGELOG.md  db      FAQ      LICENSE  README
CODE_OF_CONDUCT.md  default.prf  HAPPY_USERS.md  lynis  README.md
CONTRIBUTING.md  developer.prf  include   lynis.8  SECURITY.md
CONTRIBUTORS.md  extras     INSTALL  plugins  TODO.md
[juha@www lynis]$ sudo cd /var/log/
[juha@www lynis]$ ls
CHANGELOG.md  db      FAQ      LICENSE  README
CODE_OF_CONDUCT.md  default.prf  HAPPY_USERS.md  lynis  README.md
CONTRIBUTING.md  developer.prf  include   lynis.8  SECURITY.md
CONTRIBUTORS.md  extras     INSTALL  plugins  TODO.md
[juha@www lynis]$ sudo ./lynis audit system >> eka_audit.txt
-bash: eka_audit.txt: Permission denied
[juha@www lynis]$ sudo ./lynis audit system >> eka_audit.txt
-bash: eka_audit.txt: Permission denied
[juha@www lynis]$ touch eka_audit.txt
touch: cannot touch 'eka_audit.txt': Permission denied
[juha@www lynis]$ sudo !!
sudo touch eka_audit.txt
[juha@www lynis]$ sudo ./lynis audit system >> eka_audit.txt
-bash: eka_audit.txt: Permission denied
[juha@www lynis]$ sudo !!
sudo sudo ./lynis audit system >> eka_audit.txt
-bash: eka_audit.txt: Permission denied
[juha@www lynis]$ ls
CHANGELOG.md  db      extras     INSTALL  plugins    TODO.md
CODE_OF_CONDUCT.md  default.prf  FAQ      LICENSE  README
CONTRIBUTING.md  developer.prf  HAPPY_USERS.md  lynis  README.md
CONTRIBUTORS.md  eka_audit.txt  include   lynis.8  SECURITY.md
[juha@www lynis]$ chmod 777 eka_audit.txt
chmod: changing permissions of 'eka_audit.txt': Operation not permitted
[juha@www lynis]$ sudo !!
sudo chmod 777 eka_audit.txt
[juha@www lynis]$ sudo ./lynis audit system >> eka_audit.txt
```

Kuva 20 Lynis audit system alkutilanteen tallentaminen



```

juha@www:~/home/lynis

Lynis modules:
- Compliance status      [?]
- Security audit         [V]
- Vulnerability scan     [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data              : /var/log/lynis-report.dat

=====
Lynis 3.0.8
Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2021, CISOFy - https://ciscofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

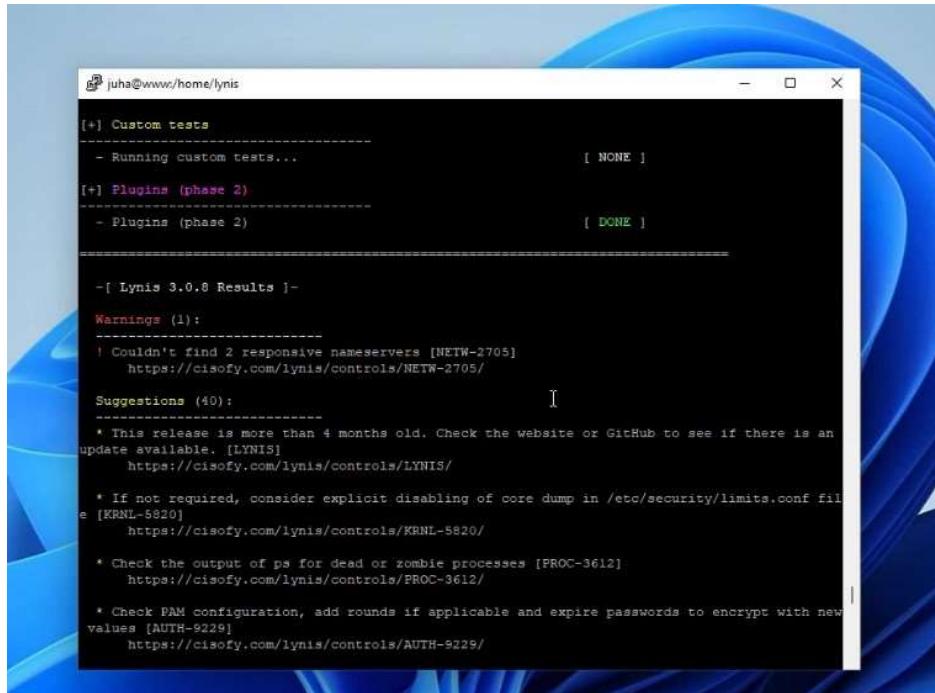
=====
[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /home/lynis/default.prf for all settings)

[juha@www lynis]$ sudo chown -R 0:0 *
[juha@www lynis]$ sudo ./lynis audit system >> eka_audit.txt
[juha@www lynis]$ sudo ./lynis audit system >> eka_audit.txt
[sudo] password for juha:
[juha@www lynis]$ ls
CHANGELOG.md    db        extras      INSTALL  plugins    TODO.md
CODE_OF_CONDUCT.md default.prf  FAQ        LICENSE  README
CONTRIBUTING.md developer.prf HAPPY_USERS.md lynis    README.md
CONTRIBUTORS.md eka_audit.txt include    lynis.8   SECURITY.md
[juha@www lynis]$ 

```

Kuva 21 Lynis audit eka_audit.txt

Seuraavaksi tarkastettiin paljonko Lyniksen huomauttamia asioita on, joita voisi koventaa (Kuva 22). Näitä oli 40 kpl (suggestions) ja näistä valittiin meidän mielestämme oleellisimmat kovennukset



```

juha@www:~/home/lynis

[+] Custom tests
-----[+]
- Running custom tests...                                [ NONE ]

[+] Plugins (phase 2)
-----[-]
- Plugins (phase 2)                                     [ DONE ]

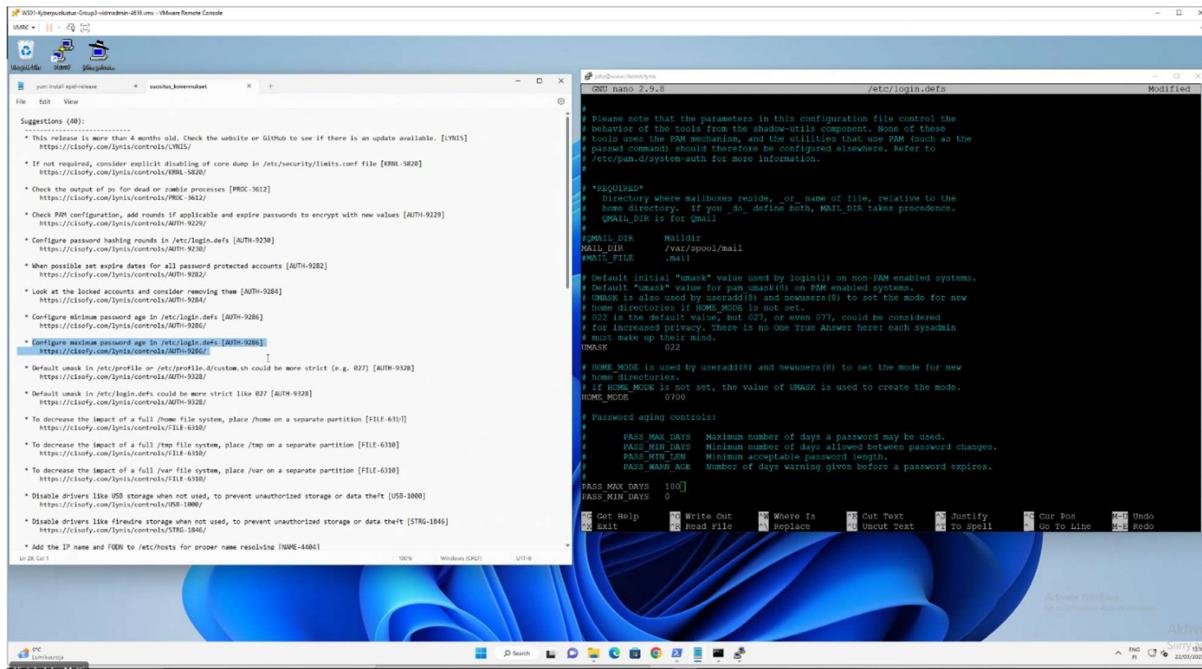
-----[+]
- Lynis 3.0.8 Results
-----[+]
- Warnings (1):
-----[+]
! Couldn't find 2 responsive nameservers [NETW-2705]
  https://ciscofy.com/lynis/controls/NETW-2705/
-----[+]
- Suggestions (40):
-----[+]
* This release is more than 4 months old. Check the website or GitHub to see if there is an
  update available. [LYNIS]
  https://ciscofy.com/lynis/controls/LYNIS/
* If not required, consider explicit disabling of core dump in /etc/security/limits.conf fil
  e [KRNL-5820]
  https://ciscofy.com/lynis/controls/KRNL-5820/
* Check the output of ps for dead or zombie processes [PROC-3612]
  https://ciscofy.com/lynis/controls/PROC-3612/
* Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new
  values [AUTH-9229]
  https://ciscofy.com/lynis/controls/AUTH-9229/
-----[+]

```

Kuva 22 Lynis suggestions

3.1.3 Linux – Lynis koventaminen

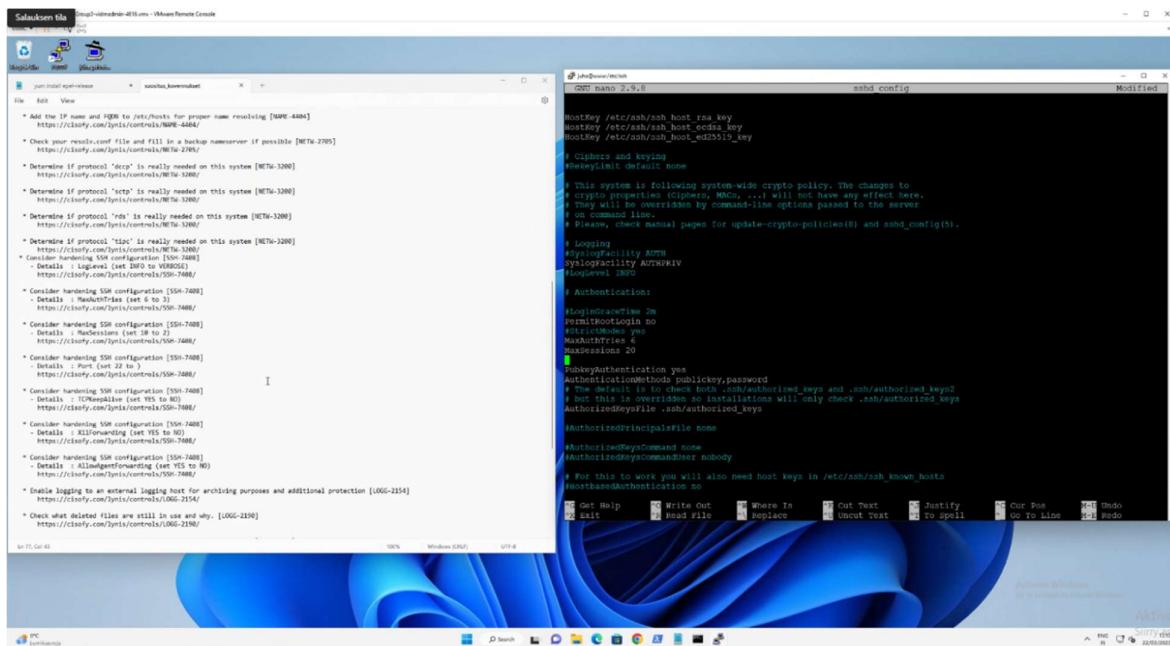
Kovennus 1: Määriteltiin salasanalle enimmäiskä ja asetettiin se 180 päivään.



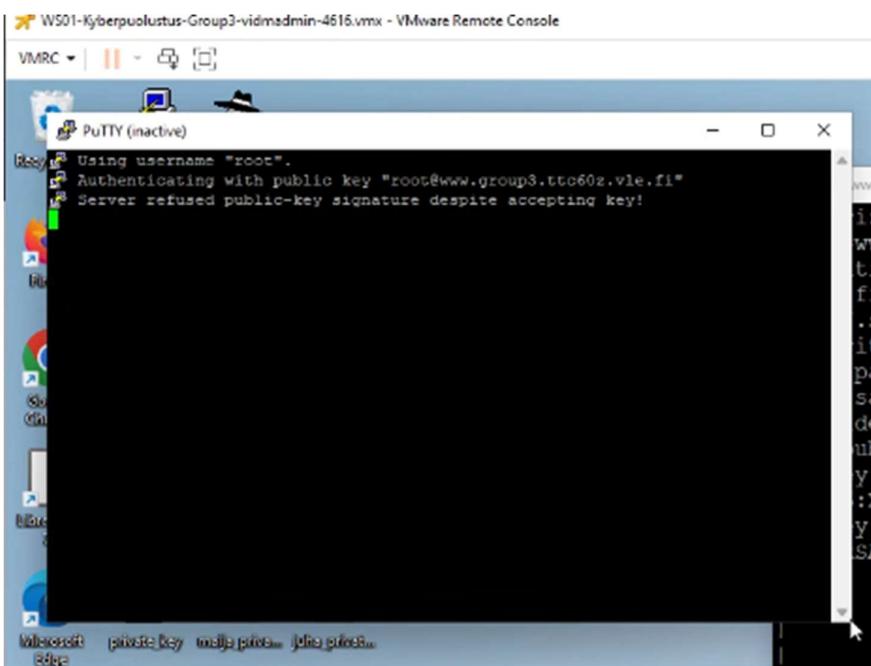
Kuva 23 Lynis kovennus 1

Kovennus 2: Kovennettiin SSH:ta, asetettiin maksimi istunnot 20 ja maksimi tunnistus yritykset 6.

Laitettiin myös root kirjautuminen pois päältä. Esitetty kuvissa 24 ja 25.



Kuva 24 Lynis kovennus 2



Kuva 25 Root kirjautuminen

Kovennus 3: Ladattiin rkhunter työkalu, jonka avulla pystytään skannaamaan ympäristö ja löytämään mahdollisia haittaohjelmia.

```
[juna@www ~]$ sudo dnf --enablerepo=epel -y install rkhunter
Error: This command has to be run with superuser privileges (under the root user on most systems).
[juna@www ~]$ sudo dnf --enablerepo=epel -y install rkhunter
[sudo] password for juha:
Last metadata expiration check: 2:47:07 ago on Wed 22 Mar 2023 09:37:25 AM EET.
Dependencies resolved.
Package          Architecture Version       Repository      Size
Installing:
rkhunter         noarch    1.4.6-7.el8   epel           212 k
Installing dependencies:
mailx            x86_64    12.5-29.el8   basesos        256 k
Transaction Summary
Install 2 Packages

Total download size: 468 k
Installed size: 1.3 M
Downloading Packages:
(1/2): mailx-12.5-29.el8.x86_64.rpm                               1.5 MB/s | 256 kB     00:00
(2/2): rkhunter-1.4.6-7.el8.noarch.rpm                            240 kB/s | 212 kB     00:00
Total                                         284 kB/s | 468 kB     00:01

Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing:
Installing : mailx-12.5-29.el8.x86_64
Installing  : rkhunter-1.4.6-7.el8.noarch
Running scriptlet: rkhunter-1.4.6-7.el8.noarch
Verifying   : mailx-12.5-29.el8.x86_64
Verifying   : rkhunter-1.4.6-7.el8.noarch

Installed:
mailx-12.5-29.el8.x86_64                                     rkhunter-1.4.6-7.el8.noarch
Complete!
```

Kuva 26 Lyyris kovennus 3 – rkhunter työkalun lataaminen

```

rkhunter: Performing system configuration file checks
  Checking for passwordless accounts [ None found ]
  Checking for passwd file changes [ Warning ]
  Checking for group file changes [ Warning ]
  Checking root account shell history files [ OK ]

rkhunter: Performing system configuration file checks
  Checking for an SSH configuration file [ Found ]
  Checking if SSH root access is allowed [ Warning ]
  Checking if SSH protocol v1 is allowed [ Not set ]
  Checking for other suspicious configuration settings [ None found ]
  Checking for a running system logging daemon [ Found ]
  Checking for a system logging configuration file [ Found ]
  Checking if syslog remote logging is allowed [ Not allowed ]

rkhunter: Performing filesystem checks
  Checking /dev for suspicious file types [ None found ]
  Checking for hidden files and directories [ None found ]

[Press <ENTER> to continue]

System checks summary
-----
File properties checks...
  Required commands check failed
  Files checked: 136
  Suspect files: 4

Rootkit checks...
  Rootkits checked : 495
  Possible rootkits: 0

Applications checks...
  All checks skipped

The system checks took: 2 minutes and 20 seconds

All results have been written to the log file: /var/log/rkhunter/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter/rkhunter.log)

ljuha@www /$ 

```

Kuva 27 Lynis kovennus 3 – rkhunter

3.2 Certbot & Wordpress koventaminen

Certbot - Eikäsi menimme CNS.VLE.FI sivulle. Sieltä saimme ohjeet, että ensimmäiseksi pitää ladata tarvittavat pluginit (Kuva 28).

```

msja@www:~/wordpress-docker
Verifying : python3-zope-component-4.3.0-8.el8.noarch          14/16
Verifying : python3-zope-event-4.2.0-12.el8.noarch           15/16
Verifying : python3-zope-interface-4.6.0-1.el8.x86_64        16/16

Installed:
certbot-1.22.0-1.el8.noarch
python-josepy-doc-1.9.0-1.el8.noarch
python3-acme-1.22.0-4.el8.noarch
python3-certbot-1.22.0-1.el8.noarch
python3-certbot-dns-rfc2136-1.22.0-1.el8.noarch
python3-configargparse-0.14.0-6.el8.noarch
python3-distro-1.4.0-2.module+el8.3.0+120+426d8ba9.noarch
python3-dns-1.16.0-11.el8.noarch
python3-josepy-1.9.0-1.el8.noarch
python3-parsedatetime-2.5-1.el8.noarch
python3-pyOpenSSL-19.0.0-1.el8.noarch
python3-pyrfc3339-1.1-1.el8.noarch
python3-requests-toolbelt-0.9.1-4.el8.noarch
python3-zope-component-4.3.0-8.el8.noarch
python3-zope-event-4.2.0-12.el8.noarch
python3-zope-interface-4.6.0-1.el8.x86_64

Complete!
[root@www wordpress-docker]# 

```

Kuva 28 Pluginien lataaminen

Lisäsimme meidän domainin nimen CNS.VLE.FI sivulle ja saatiin alla olevassa kuvassa näkyvät ohjeet sieltä seuraavaksi.

Instructions for requesting a certificate

Make sure the following information is correct:

- FQDN: www.group3.ttc60z.vle.fi

Create configuration for certbot (/etc/pki/tls/rfc2136.ini):

```
dns_rfc2136_server = 198.18.100.7
dns_rfc2136_port = 53
dns_rfc2136_name = www.group3.ttc60z.vle.fi.
dns_rfc2136_secret = 5y/wUgll13c2A140Fxc99xVEb7a9ztxaiWAvvCJAP0I=
dns_rfc2136_algorithm = HMAC-SHA256
```

Make sure the file has sane permissions:

```
chmod 600 /etc/pki/tls/rfc2136.ini
```

Finally, request a certificate:

```
certbot certonly --dns-rfc2136 --dns-rfc2136-credentials /etc/pki/tls/rfc2136.ini --dns-rfc2136-propagation-seconds 30 -d www.group3.ttc60z.vle.fi
```

If the request succeeds, certificates will be placed in /etc/letsencrypt/. You can add additional parameters such as --apache or --nginx to further automate certificate advanced use.

Requirements:

Make sure certbot and dns-rfc2136 plugin is installed. Commands for Centos 8:

```
yum install epel-release
yum install certbot python3-certbot-dns-rfc2136
```

Renewals

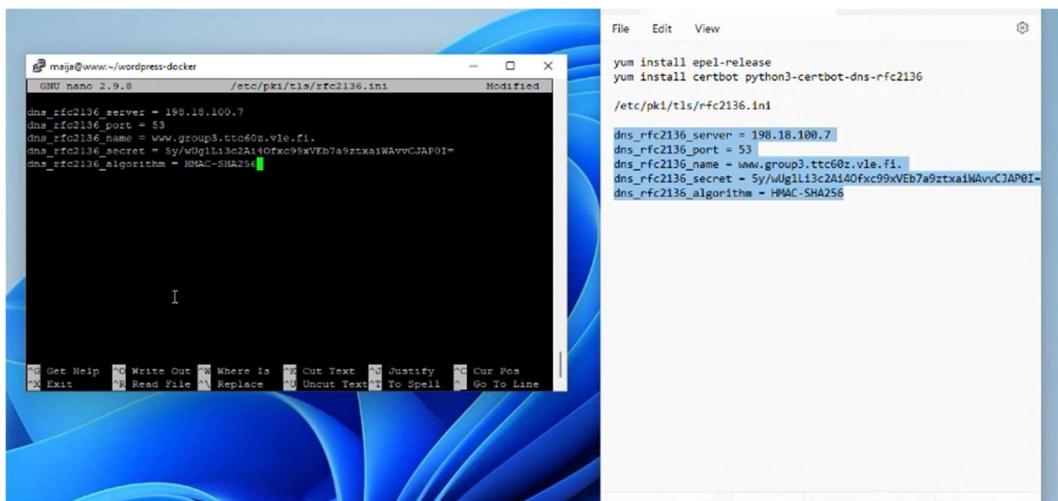
Most of the time, renewals are handled nowadays with systemd timers and certbot-renew.service. If you need to reload a webserver during renewal, use --deploy-hook

You can include this afterwards using certbot renew --force-renew --deploy-hook ... which will force a renewal and update the configuration files for that domain

Disclaimer

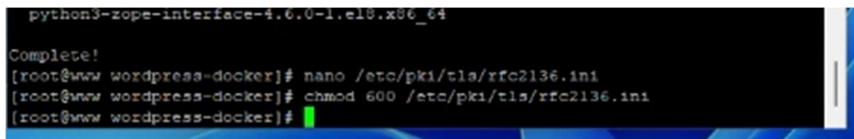
Kuva 29 Instructions for requesting a certificate

Seurasimme ohjeita ja menimme komennolla sudo nano /etc/pki/tls/rfc2136.ini tiedostoon ja lisäsimme alla olevassa kuvassa olevat 5 riviä sinne (Kuva 30).



Kuva 30 Ohjeiden seuraamista

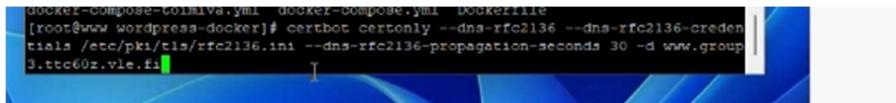
Tämän jälkeen annoimme lisäoikeuksia tiedostolle chmod 600 komennolla, esitetty kuvassa 31.



```
python3-zope-interface-4.0.0-1.el8.x86_64
Complete!
[root@www wordpress-docker]# nano /etc/pki/tls/rfc2136.ini
[root@www wordpress-docker]# chmod 600 /etc/pki/tls/rfc2136.ini
[root@www wordpress-docker]#
```

Kuva 31 Lisäoikeuksia

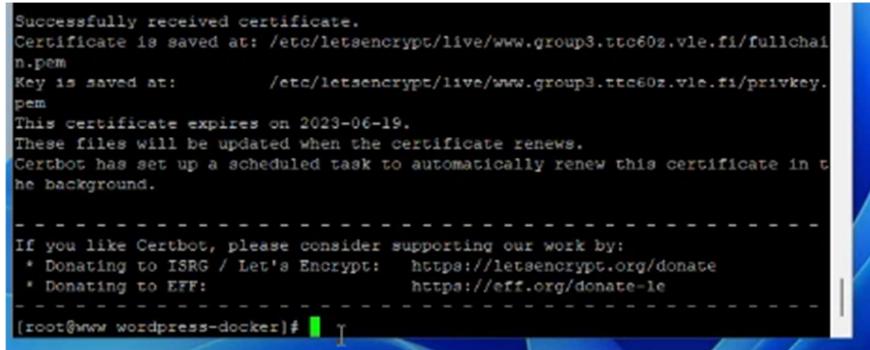
Seuraavaksi teimme sertifikaatti pyynnön ja laitoimme sähköpostin, jonka jälkeen odotimme 30 sekuntia että DNS säädöö tulee voimaan.



```
docker-compose-lolimiva.yml docker-compose.yml Dockerfile
[root@www wordpress-docker]# certbot certonly --dns-rfc2136 --dns-rfc2136-credentials /etc/pki/tls/rfc2136.ini --dns-rfc2136-propagation-seconds 30 -d www.group3.ttc60z.vle.fi
```

Kuva 32 Sertifikaattipyyntö

Odotuksen jälkeen saimme ilmoituksen onnistuneesta sertifikaatista, sekä otimme talteen avaimen.

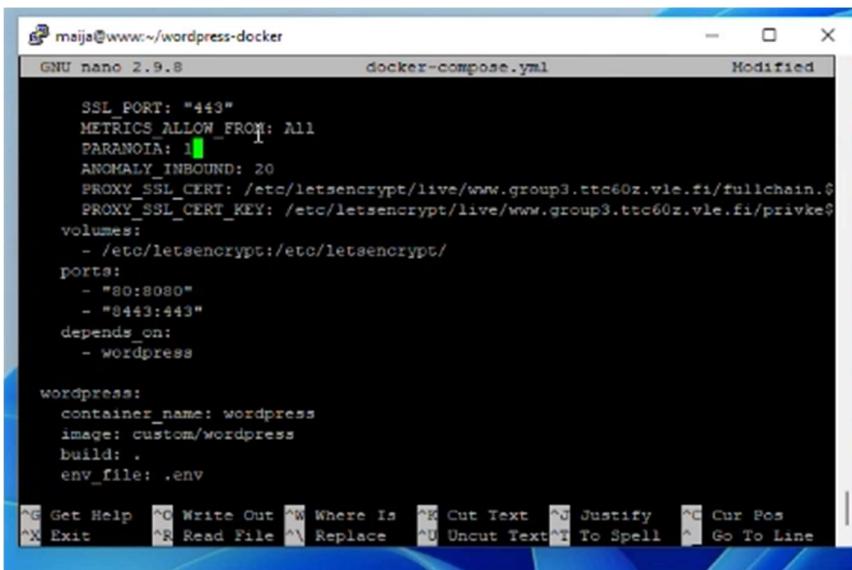


```
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/www.group3.ttc60z.vle.fi/fullchain.pem
Key is saved at:          /etc/letsencrypt/live/www.group3.ttc60z.vle.fi/privkey.pem
This certificate expires on 2023-06-19.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

-----
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                   https://eff.org/donate-le
-----
[root@www wordpress-docker]#
```

Kuva 33 Successfully received certificate

Menimme komennolla: nano docker-compose.yml ja lisäsimme avaimet sinne ja teimme tarvittavat muutokset (Kuva 34) .



```

maija@www:~/wordpress-docker
GNU nano 2.9.8           docker-compose.yml          Modified

SSL_PORT: "443"
METRICS_ALLOW_FROM: All
PARANOIA: 1
ANOMALY_INBOUND: 20
PROXY_SSL_CERT: /etc/letsencrypt/live/www.group3.ttc60z.vle.fi/fullchain.pem
PROXY_SSL_CERT_KEY: /etc/letsencrypt/live/www.group3.ttc60z.vle.fi/privkey.pem
volumes:
- /etc/letsencrypt:/etc/letsencrypt/
ports:
- "80:8080"
- "8443:443"
depends_on:
- Wordpress

Wordpress:
container_name: wordpress
image: custom/wordpress
build: .
env_file: .env

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^A Replace   ^U Uncut Text ^I To Spell ^L Go To Line

```

Kuva 34 Muutoksia

Seuraavaksi tehdään komento docker-compose up -d. Tämä katsoo, onko tullut muutoksia dockeriin ja päivittää sen, jos on (Kuva 35).



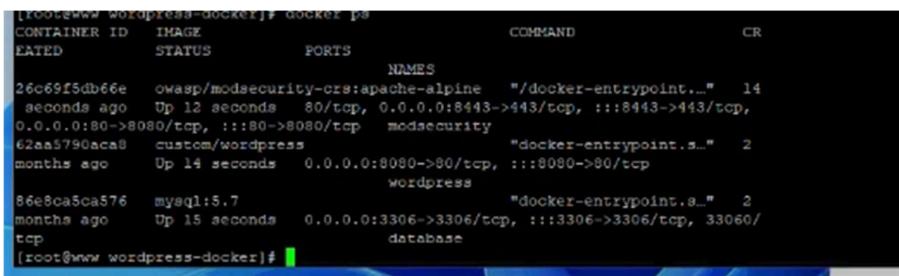
```

[root@www wordpress-docker]# nano docker-compose.yml
[root@www wordpress-docker]# docker-compose up -d
Starting database ... done
Starting wordpress ... done
Recreating modsecurity ... done
[root@www wordpress-docker]#

```

Kuva 35 Docker muutokset

Varmistetaan, onko dockeri päällä (Kuva 36).



CONTAINER ID	IMAGE	COMMAND	CR			
CREATED	STATUS	PORTS	NAMES			
26c69f5db66e	owasp/modsecurity-crss:apache-alpine	"/docker-entrypoint..."	14 seconds ago	Up 12 seconds	80/tcp, 0.0.0.0:8443->443/tcp, :::8443->443/tcp, 0.0.0.0:80->8080/tcp, :::80->8080/tcp	modsecurity
62aa5790aca8	custom/wordpress	"docker-entrypoint.s..."	months ago	Up 14 seconds	0.0.0.0:8080->80/tcp, :::8080->80/tcp	wordpress
86e8ca5ca576	mysql:5.7	"docker-entrypoint.s..."	months ago	Up 15 seconds	0.0.0.0:3306->3306/tcp, :::3306->3306/tcp, 33060/tcp	database

Kuva 36 Docker ps

Seuraavaksi mennään palomuuriin tekemään muutoksia (Kuva 37 & 38).

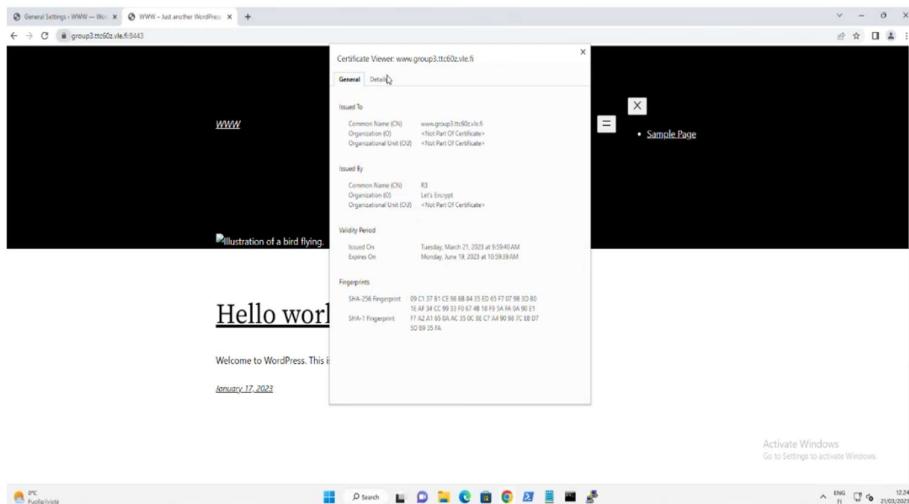
6	www.8443	none			any	any		any	none	destination-translation	
										address: 10.4.0.11	
										port: 8443	

Kuva 37 Palomuurin muutoksia

Security													16 items ↗	
NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS						
1 Internet_8443	none	universal		any	any	any		any	any	any	HTTPS-ON...	Allow	none	1
2 WS-T0-VLE	none	universal		any	any	any		any	any	any	web-browsing	Agent	Allow	17269

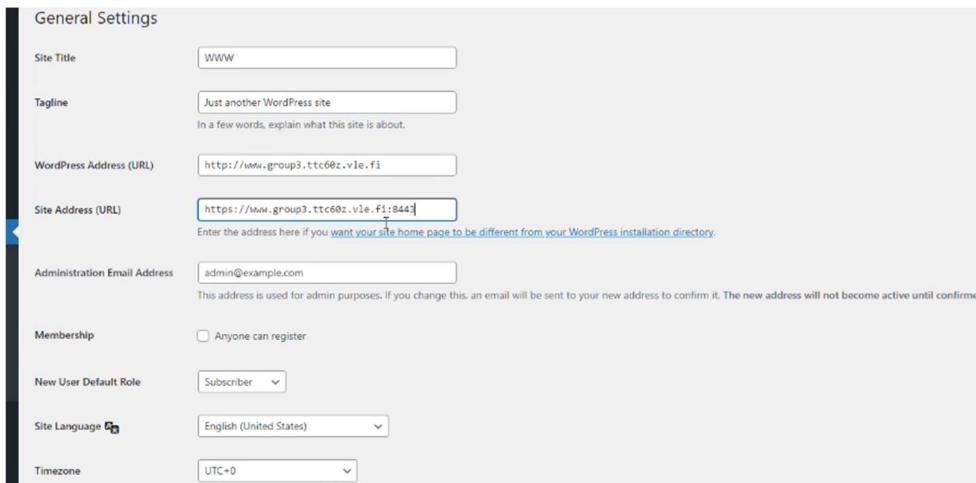
Kuva 38 Palomuurin muutos

Tämän jälkeen, jos kaikki meni hyvin, niin pitäisi sertifikaatti olla sivuillamme ja siellähän se. Esitettty kuvassa 39.



Kuva 39 Sertifikaatti

Seuraavaksi menimme wordpress sivulle tekemään muutoksia lisääsimme Site address kohtaan alkuun https ja loppuun portin 8443. Esitetty kuvassa 40.



Kuva 40 Site address muutos

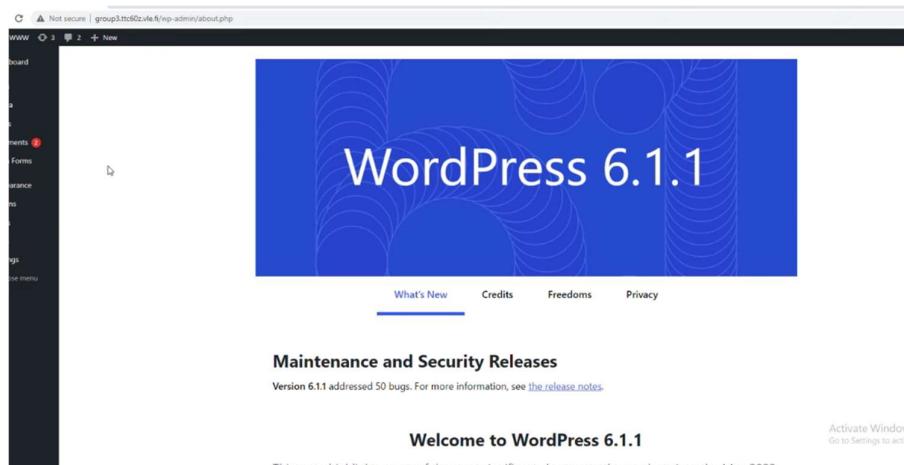
Tämän jälkeen aloimme koventamaan wordpress sivustoa ja ajattelimme, että päivitetään se ensimmäiseksi, koska siellä oli 3 päivitystä odottamassa. Eihän se onnistunut, valitti että ei pysty luoda kansiota ja ei ole oikeuksia. Olimme oikeilla jäljillä, että pitää käydä antamassa lisäoikeuksia ja kävimme antamassa kaikille 3 kansiolle niin kuin piti, mutta ei siltikään toiminut ja kokeilimme kaiken näköisiä muita ohjeita, mutta niistäkään ei ollut apua. Lopulta päätimme kysyä opettajalta apua ja saimme aika nopeaa vastauksen ongelmaamme, että kansioille piti antaa rekursiivisena oikeudet, että se menee myös sen sisällä oleville tiedostoille. Tämän jälkeen alkoi toimia ja saattiin päivitettyä Wordpress, sekä pluginit. Esitetty kuvissa alla.

```
[root@www wordpress-docker_wordpress]# ls
data
[root@www wordpress-docker_wordpress]# cd _data
[root@www _data]# ls
index.php      wp-blog-header.php    wp-content      wp-login.php      xmlrpc.php
license.txt    wp-comments-post.php  wp-cron.php    wp-mail.php
readme.html    wp-config-docker.php wp-includes    wp-settings.php
wp-activate.php wp-config.php       wp-links-opml.php wp-signup.php
wp-admin       wp-config-sample.php wp-load.php    wp-trackback.php
[root@www _data]# chmod 777 wp-admin wp-content wp-includes
[root@www _data]#
```

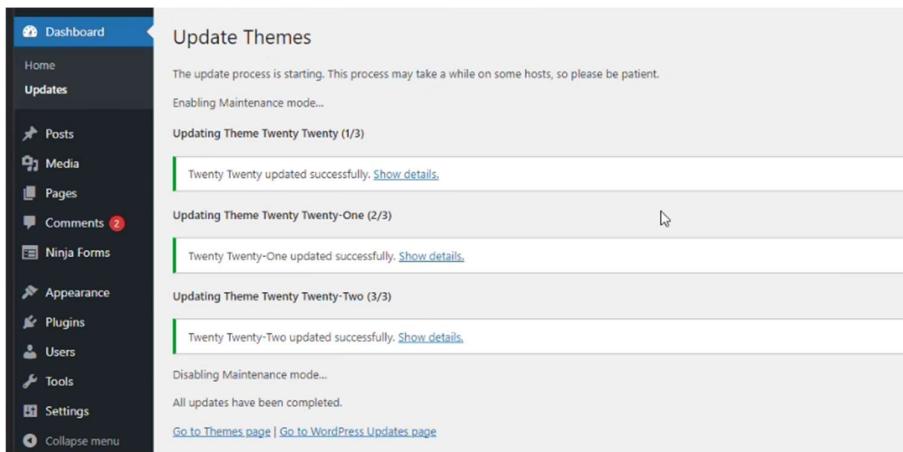
Kuva 41 Lisäoikeuksia

```
[root@www wp-content]# cd ..
[root@www _data]# chmod -R 777 wp-admin wp-content wp[includes
chmod: cannot access 'wp_admin': No such file or directory
chmod: cannot access 'wp_content': No such file or directory
chmod: cannot access 'wp_includes': No such file or directory
[root@www _data]# chmod -R 777 wp-admin wp-content wp-includes
[root@www _data]# ls -la
total 236
drwxr-xr-x. 5 33 tape 4096 Mar 21 12:22 .
drwx-----x. 3 root root 19 Jan 17 15:01 ..
-rw-r--r--. 1 33 tape 261 Jun 24 2022 .htaccess
-rw-r--r--. 1 33 tape 405 Feb 6 2020 index.php
-rw-r--r--. 1 33 tape 19915 Jan 1 2022 license.txt
-rw-r--r--. 1 33 tape 7401 Mar 22 2022 readme.html
-rw-r--r--. 1 33 tape 7165 Jan 21 2021 wp-activate.php
drwxrwxrwx. 9 33 tape 4096 May 24 2022 wp-admin[redacted]
-rw-r--r--. 1 33 tape 351 Feb 6 2020 wp-blog-header.php
-rw-r--r--. 1 33 tape 2338 Nov 10 2021 wp-comments-post.php
-rw-r--r--. 1 33 tape 5480 Jun 24 2022 wp-config-docker.php
-rw-r--r--. 1 33 tape 5656 Jan 17 15:02 wp-config.php
-rw-r--r--. 1 33 tape 3001 Dec 14 2021 wp-config-sample.php
drwxrwxrwx. 7 33 tape 95 Mar 21 12:22 wp-content[redacted]
-rw-r--r--. 1 33 tape 3943 Apr 28 2022 wp-cron.php
drwxrwxrwx. 26 33 tape 12288 May 24 2022 wp-includes[redacted]
-rw-r--r--. 1 33 tape 2494 Mar 19 2022 wp-links-opml.php
-rw-r--r--. 1 33 tape 3973 Apr 12 2022 wp-load.php
-rw-r--r--. 1 33 tape 48498 Apr 29 2022 wp-login.php
-rw-r--r--. 1 33 tape 8577 Mar 22 2022 wp-mail.php
-rw-r--r--. 1 33 tape 23706 Apr 12 2022 wp-settings.php
-rw-r--r--. 1 33 tape 32051 Apr 11 2022 wp-signup.php
-rw-r--r--. 1 33 tape 4748 Apr 11 2022 wp-trackback.php
-rw-r--r--. 1 33 tape 3236 Jun 8 2020 xmlrpc.php
[root@www _data]#
```

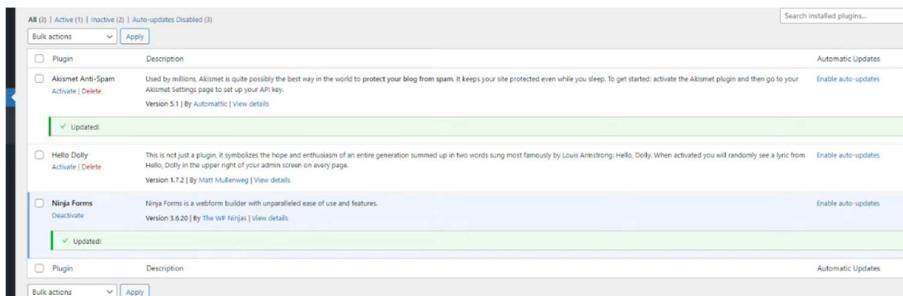
Kuva 42 chmod -R 777



Kuva 43 WordPress 6.1.1



Kuva 44 Update themes



Kuva 45 Onnistuneet päivitykset

Päivityksien jälkeen latasimme muutaman lisä pluginin parantamaan wordpressin turvallisuutta. (Easy update manager, jolla voidaan hallinnoida päivityksiä. Muutimme asetukset, että se päivittää kaikki automaattisesti (Kuvat 46,47,48). Seuraavaksi latasimme Limit login attempts, koska kirjautumis sivulla ei ollut ollenkaan mitään kirjautumisen estoa, jolloin hyökkääjä voi yrittää kirjautua käyttäjälle niin monta kertaa kuin haluaa ja jos on huono salasana niin hyökkääjä saa sen saa nopeasti ja helposti tietoansa. Latoimme kirjautumis ehtoihin, että 5 yrityksen jälkeen menee 20 minuutiksi lukkoon ja 4 lukituksen jälkeen 24 tunniksi (Kuva 49). Vielä viimeiseksi latasimme backup pluginin (Kuva 50).

The screenshot shows the 'Easy Updates Manager' settings page. At the top, there's a banner with links to other plugins: 'UpdraftPlus', 'UpdraftCentral', and 'WP-Optimize'. Below the banner, there are tabs for 'General', 'Plugins', 'Themes', 'Logs', 'Advanced', and 'Premium'. The 'General' tab is selected.

Updates settings

- Disable all updates**: This section contains two buttons: 'Enable all updates' (green) and 'Disable all updates' (grey). A note below says: 'This is a master switch and will enable or disable updates for the WordPress installation. Switching updates off is not recommended.' Below these buttons is a note: 'Updates are allowed; however, you still need to configure the updates below.'
- Quick configuration actions**: This section contains four buttons: 'WordPress default settings' (green), 'Auto update everything' (grey), 'Disable auto updates' (grey), and 'Custom' (grey).
- WordPress core updates**: This section contains four buttons: 'Manually update' (green), 'Disable core updates' (grey), 'Auto update all minor versions' (grey), and 'Auto update all releases' (grey). To the right, there's a note: 'Activate Windows' and 'Go to Settings to activate Windows.'

Kuva 46 Automaattiset päivitykset

This screenshot shows the 'Updates settings' section of the 'Easy Update Manger' plugin. It includes several sections:

- Disable all updates**: A note says: 'This is a master switch and will enable or disable updates for the WordPress installation. Switching updates off is not recommended.' Below are buttons for 'Enable all updates' (green) and 'Disable all updates' (grey).
- Quick configuration actions**: Buttons include 'WordPress default settings' (green), 'Auto update everything' (grey), 'Disable auto updates' (grey), and 'Custom' (grey).
- WordPress core updates**: Buttons include 'Manually update' (green), 'Disable core updates' (grey), 'Auto update all minor versions' (grey), and 'Auto update all releases' (grey). There's also a checkbox for 'Allow development versions to be replaced with a new minor/major version'.
- Plugin updates**: Buttons include 'Manually update' (green), 'Disable plugin updates' (grey), 'Enable auto updates' (green), 'Disable auto updates' (grey), and 'Choose per plugin' (grey).
- Theme updates**: Buttons include 'Manually update' (green), 'Disable theme updates' (grey), 'Enable auto updates' (green), 'Disable auto updates' (grey), and 'Choose per theme' (grey).

Kuva 47 Päivitys asetuksien laittamista

All Plugins		Description	Automatic Updates
<input type="checkbox"/>	Plugin	Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam. It keeps your site protected even while you sleep. To get started: activate the Akismet plugin and then go to your Akismet Settings page to set up your API key.	Managed by Easy Updates Manager.
<input type="checkbox"/>	Akismet Anti-Spam Activate Delete	Version 5.1 By Automatic View details	
<input type="checkbox"/>	Easy Updates Manager Deactivate	Manage and disable WordPress updates, including core, plugin, theme, and automatic updates - Works with Multisite and has built-in logging features.	Managed by Easy Updates Manager.
<input type="checkbox"/>	Hello Dolly Activate Delete	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page.	Managed by Easy Updates Manager.
<input type="checkbox"/>	Limit Login Attempts Reloaded Upgrade to Premium Customize Settings Deactivate	Block excessive login attempts and protect your site against brute force attacks. Simple, yet powerful tools to improve site performance.	Managed by Easy Updates Manager.
<input type="checkbox"/>	Ninja Forms Deactivate	Ninja Forms is a webform builder with unparalleled ease of use and features.	Managed by Easy Updates Manager.
<input type="checkbox"/>	Plugin	Version 3.6.20 By Saturday Drive View details	Automatic Updates

Activate Windows
Go to Settings to activate Windows.

Kuva 48 Easy Update Manger

Local App

Lockout	5 allowed retries 20 minutes lockout 4 lockouts increase lockout time to 24 hours 1 hours until retries are reset
Trusted IP Origins	REMOTE_ADDR

Specify the origins you trust in order of priority, separated by commas. We strongly recommend that you **do not** use anything other than REMOTE_ADDR since other headers can be easily spoofed.

Examples: HTTP_X_FORWARDED_FOR, HTTP_CF_CONNECTING_IP, HTTP_X_SUURI_CLIENTIP

Kuva 49 Limit login attempts

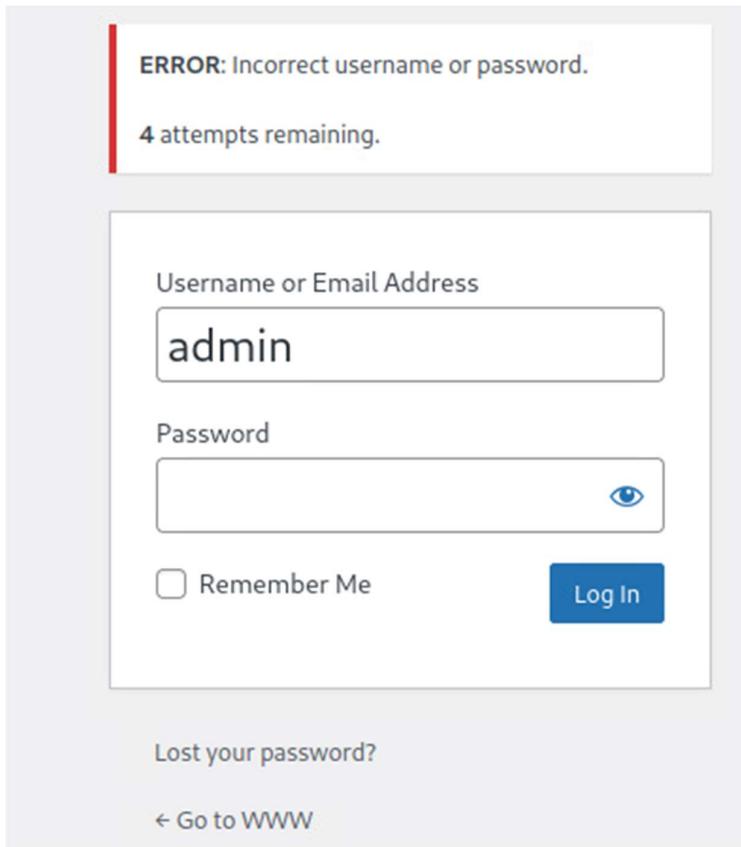
The screenshot shows the Local App settings interface. Under the 'Lockout' section, there are input fields for 'allowed retries' (5), 'minutes lockout' (20), 'lockouts increase lockout time to' (24 hours), and 'hours until retries are reset' (1). Below this is a 'Trusted IP Origins' section with a field for 'REMOTE_ADDR'. A note says: 'Specify the origins you trust in order of priority, separated by commas. We strongly recommend that you **do not** use anything other than REMOTE_ADDR since other headers can be easily spoofed.' Examples listed include HTTP_X_FORWARDED_FOR, HTTP_CF_CONNECTING_IP, and HTTP_X_SUURI_CLIENTIP.

Kuva 50 Backup plugin

The screenshot shows the Duplicator Pro backup plugin setup screen. At the top, it says 'Scan Time: 0.24 sec.' Below that is a 'Setup' section with 'System', 'WordPress', and 'Migration Status' items, all marked as 'Good'. The main area is titled 'Archive zip' and contains sections for 'Files' (92.19MB, uncompressed) and 'Database' (2.28MB, uncompressed). Under 'Files', there are 'Size Checks', 'Addon Sites', 'Name Checks', and 'Read Checks' sections, all marked as 'Good'. Under 'Database', there is an 'Overview' section marked as 'Good'. At the bottom, a note says 'Migrate large, multi-gig sites with Duplicator Pro!' and there are 'Back', 'Rescan', and 'Build' buttons. The 'Build' button is highlighted with a cursor icon.

Kuva 51 Backup

Lopuksi kokeilimme, että kirjautumis sivusto toimii niin kuin pitää ja ettei näissä uusissa plugineissä ei ole tietoisia haavoittuvuuksia, joten teimme kalilla wpscannin sivuillemme (Kuvat 53 & 54).



Kuva 52 Testausta

Kuva 53 Kali WPScan

```

| Query Parameter In Install Page (Aggressive Detection)
| - http://www.group3.ttc60z.vle.fi/wp-includes/css/dashicons.min.css?ver=6.1.1
| - http://www.group3.ttc60z.vle.fi/wp-includes/css/buttons.min.css?ver=6.1.1
| - http://www.group3.ttc60z.vle.fi/wp-admin/css/forms.min.css?ver=6.1.1
| - http://www.group3.ttc60z.vle.fi/wp-admin/css/l10n.min.css?ver=6.1.1

^[[34m[!]]^[[0m The main theme could not be detected. cookie,socket

^[[32m[+]]^[[0m Enumerating All Plugins (via Passive Methods)
^[[32m[+]]^[[0m Checking Plugin Versions (via Passive and Aggressive Methods)

^[[34m[i]]^[[0m Plugin(s) Identified:

^[[32m[+]]^[[0m limit-login-attempts-reloaded
| Location: http://www.group3.ttc60z.vle.fi/wp-login.php/wp-content/plugins/limit-login-attempts-reloaded/
| Latest Version: 2.25.13
| Last Updated: 2023-03-02T11:59:00.000Z

| Found By: URLs In Homepage (Passive Detection)
| Confirmed By: URLs In 404 Page (Passive Detection)

| The version could not be determined.

^[[32m[+]]^[[0m Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups -: |=====

^[[34m[i]]^[[0m No Config Backups Found.

^[[33m[!]]^[[0m No WPScan API Token given, as a result vulnerability data has not been output.
^[[33m[!]]^[[0m You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

^[[32m[+]]^[[0m Finished: Tue Mar 21 12:51:23 2023
^[[32m[+]]^[[0m Requests Done: 141
^[[32m[+]]^[[0m Cached Requests: 183
^[[32m[+]]^[[0m Data Sent: 48.61 KB
^[[32m[+]]^[[0m Data Received: 65.473 KB
^[[32m[+]]^[[0m Memory used: 234.219 MB
^[[32m[+]]^[[0m Elapsed time: 00:00:08

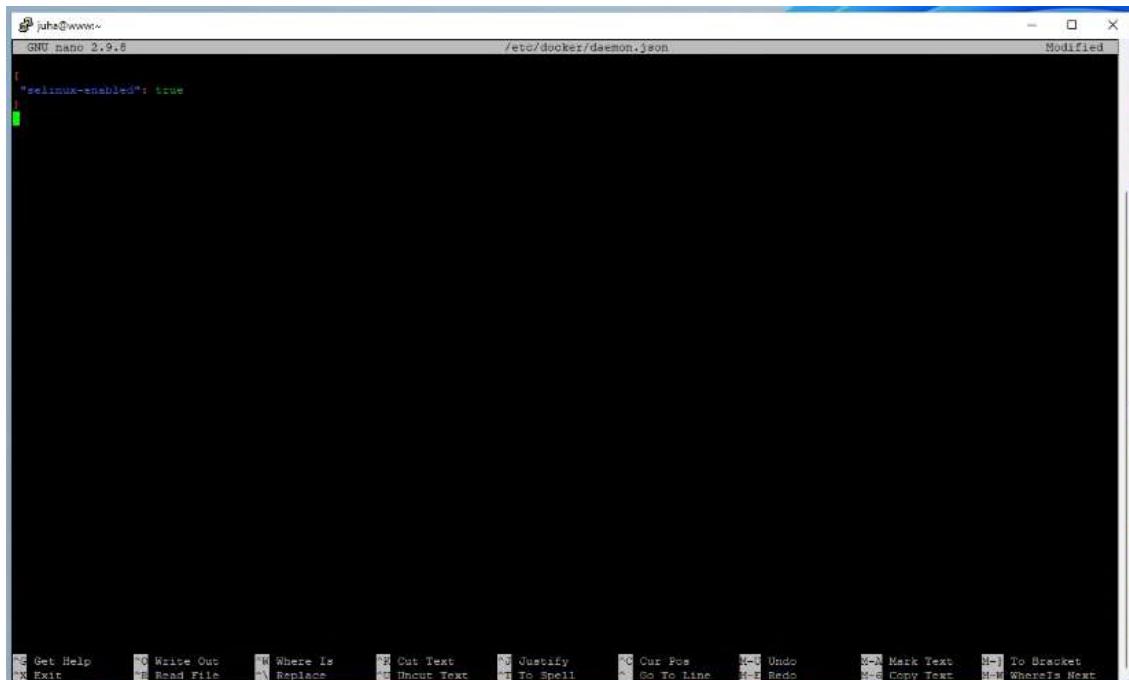
```

Kuva 54 Kali WPScan tuloksia

3.3 Docker koventaminen

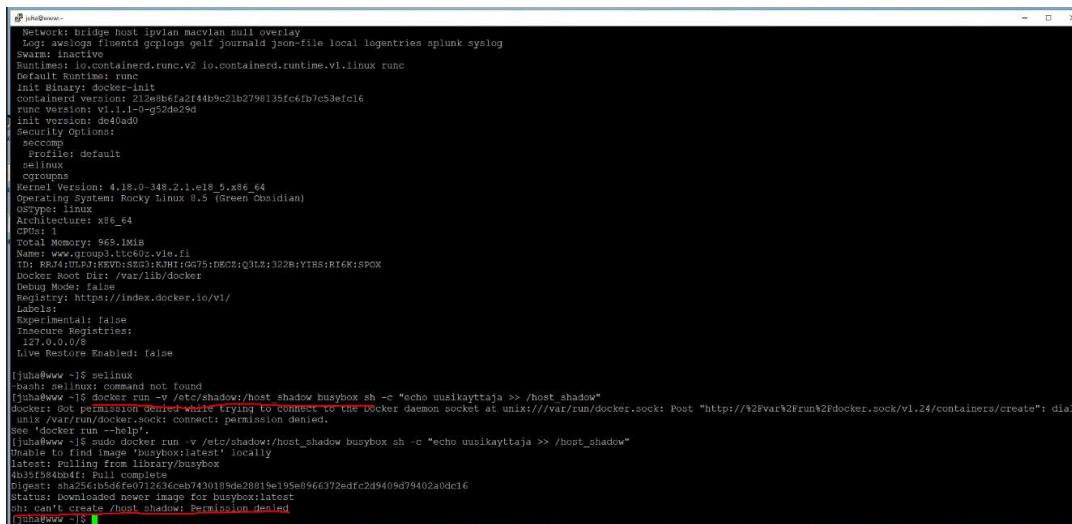
3.3.1 SELinux päälle dockeriin

Aloitettiin pistämällä SELinux päälle dockeriin (Kuva 55).



Kuva 55 SELinux

SELinuxin toiminta pystytään testaamaan koittamalla ajaa host-tiedoston manipulaatio käsky, ku vasta huomataan, että käsky ei mene läpi.

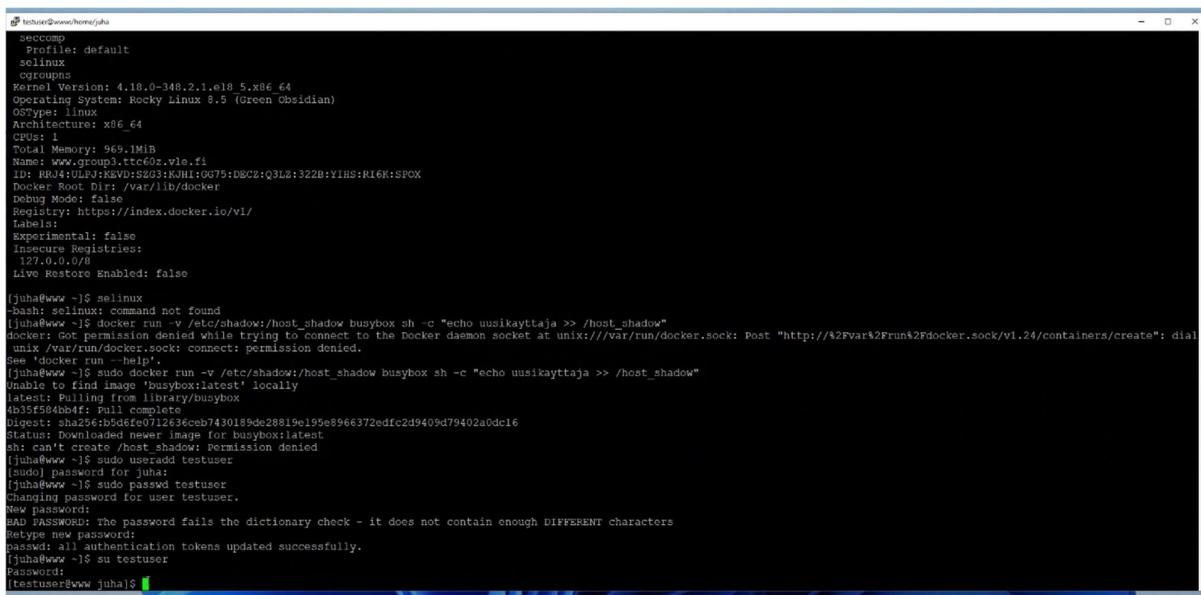


```

[juha@www ~]
Network: bridge host ipvlan macvlan null overlay
Log: /dev/log fluentd/goplogs gelf journald json-file local logentries splunk syslog
Storage: file
Runtimes: io.containerd.runc.v2 io.containerd.runtime.v1.linux runc
Default Runtime: runc
Init Binary: docker-init
Container ID: 212e9b6f2af4fb9c21b2798135fc6fb7c53efc16
Image Version: v1.13.1-gf2de29d
Init Version: do40ad0
Security Options:
  seccomp
    Profile: default
    selinux
    cgroups
Kernel Version: 4.18.0-348.2.1.e18.5.x86_64
Operating System: Rocky Linux 8.5 (Green Obsidian)
OS Type: linux
Architecture: x86_64
CPUs: 1
Total Memory: 969.1MiB
Name: rhel8-192-168-1-100-vm
ID: RRJ4:1LPJ:KEV0:SG03:KJH1:G075:DEC2:Q3L2:322B:YIHS:RI6K:SPOX
Docker Root Dir: /var/lib/docker
Debug Mode: false
Registry: https://index.docker.io/v1/
Labels:
Experimental: false
Insecure Registries:
  127.0.0.0/8
Live Restore Enabled: false
[juha@www ~]$ selinux
bash: selinux: command not found
[juha@www ~]$ docker run -v /etc/shadow:/host_shadow busybox sh -c "echo uusikayttaja >> /host_shadow"
docker: get permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Post "http://$2Fvar%2Frun%2Fdocker.sock/v1.24/containers/create": dial unix /var/run/docker.sock: connect: permission denied.
See 'docker run --help'.
[juha@www ~]$ sudo docker run -v /etc/shadow:/host_shadow busybox sh -c "echo uusikayttaja >> /host_shadow"
Unable to find image 'busybox:latest' locally
latest: Pulling from library/busybox
4b35f584abb4: Pull complete
Digest: sha256:bb5dfe0712636ccb7430189de28819e195e096f372edfc2d9409d79402a0dc16
Status: Downloaded newer image for busybox:latest
sh: can't create /host_shadow: Permission denied
[juha@www ~]$
```

Kuva 56 SELinuxin toiminnan testaus

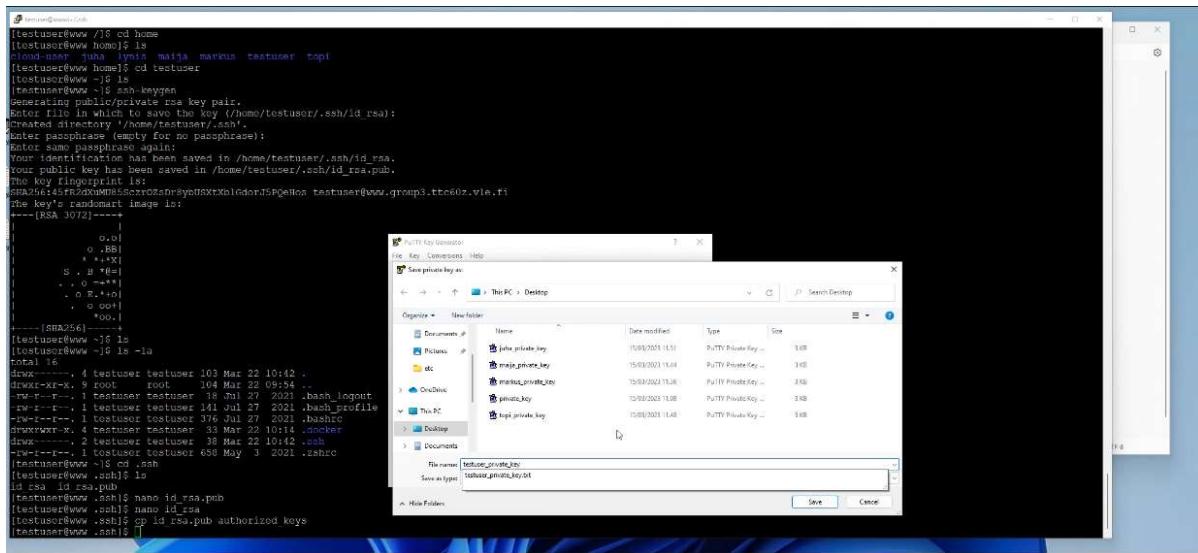
Luotiin uusi käyttäjä ilman root oikeuksia, rootless dockerin asennusta varten (Kuva 57).



```

[juha@www ~]
seccomp
  level: default
  selinux
  cgroups
Kernel Version: 4.18.0-348.2.1.e18.5.x86_64
Operating System: Rocky Linux 8.5 (Green Obsidian)
OS Type: linux
Architecture: x86_64
CPUs: 1
Total Memory: 969.1MiB
Name: rhel8-192-168-1-100-vm
ID: RRJ4:1LPJ:KEV0:SG03:KJH1:G075:DEC2:Q3L2:322B:YIHS:RI6K:SPOX
Docker Root Dir: /var/lib/docker
Debug Mode: false
Registry: https://index.docker.io/v1/
Labels:
Experimental: false
Insecure Registries:
  127.0.0.0/8
Live Restore Enabled: false
[juha@www ~]$ selinux
bash: selinux: command not found
[juha@www ~]$ docker run -v /etc/shadow:/host_shadow busybox sh -c "echo uusikayttaja >> /host_shadow"
docker: get permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Post "http://$2Fvar%2Frun%2Fdocker.sock/v1.24/containers/create": dial unix /var/run/docker.sock: connect: permission denied.
See 'docker run --help'.
[juha@www ~]$ sudo docker run -v /etc/shadow:/host_shadow busybox sh -c "echo uusikayttaja >> /host_shadow"
Unable to find image 'busybox:latest' locally
latest: Pulling from library/busybox
4b35f584abb4: Pull complete
Digest: sha256:bb5dfe0712636ccb7430189de28819e195e096f372edfc2d9409d79402a0dc16
Status: Downloaded newer image for busybox:latest
sh: can't create /host_shadow: Permission denied
[juha@www ~]$ sudo useradd testuser
[juha@www ~]$ sudo passwd testuser
[sudo] password for juha:
[juha@www ~]$ sudo passwd testuser
Changing password for user testuser.
New password:
BAD PASSWORD: the password fails the dictionary check - it does not contain enough DIFFERENT characters
Retype new password:
passwd: all authentication tokens updated successfully.
[juha@www ~]$ su testuser
Password:
[testuser@www juha]$
```

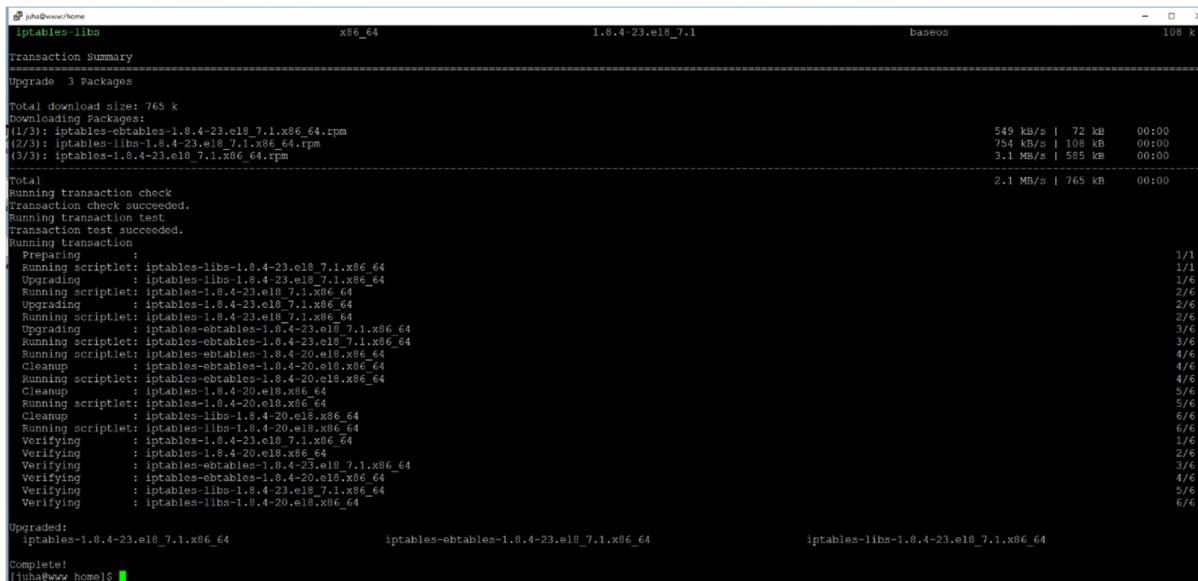
Kuva 57 sudo useradd testuser



Kuva 58 private key rootless userille

3.3.2 Docker toimimaan Rootlessina

Seurattiin dockerin sivulta löytyviä ohjeita rootless dockerin asentamiseen ja seurattiin niitä. Ensimmäiset 2 kuvalta (Kuvat 59, 60) ovat ennakoedellytyksiä, jotka suositeltiin tehtäväksi ennen rootless dockerin asennusta, jonka vuoksi ne on tehty root käyttäjällä.



Kuva 59 iptables

```

[juha@www home]$ sudo sh -eux <<EOF
#####
END #####
(testuser@www home)$ su juha
Password:
[juha@www home]$ sudo dnf install -y fuse-overlayfs
Is this password for juha?
Last update on 2023-03-22 at 09:37:25 UTC
Dependencies resolved.
=====
Package           Architecture      Version            Repository      Size
Upgrading:
fuse-overlayfs          x86_64        1.9-1.module+el8.7.0+1154+147ffa21       appstream    72 k
Transaction Summary
Upgrade 1 Package
Total download size: 72 k
Downloading Packages:
fuse-overlayfs-1.9-1.module+el8.7.0+1154+147ffa21.x86_64.rpm
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : fuse-overlayfs-1.9-1.module+el8.7.0+1154+147ffa21.x86_64
Upgrading : fuse-overlayfs-1.9-1.module+el8.7.0+1154+147ffa21.x86_64
  Using scriptlet: fuse-overlayfs-1.9-1.module+el8.7.0+1154+147ffa21.x86_64
  Cleanup   : fuse-overlayfs-1.7.1-1.module+el8.5.0+710+4c471e88.x86_64
  Running scriptlet: fuse-overlayfs-1.7.1-1.module+el8.5.0+710+4c471e88.x86_64
Verifying  : fuse-overlayfs-1.9-1.module+el8.7.0+1154+147ffa21.x86_64
Verifying  : fuse-overlayfs-1.7.1-1.module+el8.5.0+710+4c471e88.x86_64
Upgraded:
fuse-overlayfs-1.9-1.module+el8.7.0+1154+147ffa21.x86_64
Complete!
[juha@www home]$ 

```

Kuva 60 sudo dnf install -y

Dockerin asennettiin dockerd-rootless-setuptool.sh install käskyllä ja aloitettiin systemctl --user start docker käskyllä.

```

[testuser@www /]
/usr/bin/dockerd-rootless.sh
|- 192691 /proc/self/exe --net=slirp4netns --mtu=65520 --slirp4netns sandbox-auto --slirp4netns
seccomp=auto --disable-host-loopback --port-driver=builtin --copy-up=/etc --copy-up=/run --propagation=rsl
+ve /usr/bin/dockerd-rootless.sh
|- 192706 slirp4netns --mtu=65520 -r 3 --disable-host-loopback --enable-sandbox --enable-seccomp
192691 tap0
|- 192714 dockerd
|- 192729 containerd --config /run/user/1005/docker/containerd/containerd.toml --log-level info
+ DOCKER_HOST=unix:///run/user/1005/docker.sock
+ /usr/bin/docker version
Client: Docker Engine - Community
Version:           20.10.16
API version:       1.41
Go version:        go1.17.10
Git commit:        aa7e414
Built:             Thu May 12 09:17:20 2022
OS/Arch:           linux/amd64
Context:           default
Experimental:     true

Server: Docker Engine - Community
Engine:
Version:           20.10.16
API version:       1.41 (minimum version 1.12)
Go version:        go1.17.10
Git commit:        f756502
Built:             Thu May 12 09:15:41 2022
OS/Arch:           linux/amd64
Experimental:     false
containerd:
Version:           1.6.4
GitCommit:         212e8b6fa2f44b9c21b2798135fc6fb7e53efc16
runc:
Version:           1.1.1
GitCommit:         v1.1.1-0-g52de29d
docker-init:
Version:           0.19.0
GitCommit:         de40ad0
+ systemctl --user enable docker.service
Created /home/testuser/.config/systemd/user/default.target.wants/docker.service → /home/testuser/.config/systemd/user/docker.service.
[INFO] Installed docker.service successfully.
[INFO] To control docker.service, run: 'systemctl --user (start|stop|restart) docker.service'
[INFO] To run docker.service on system startup, run: 'sudo systemctl enable --linger testuser'

[INFO] Creating CLI context "rootless"
Successfully created context "rootless"

[INFO] Make sure the following environment variables are set (or add them to ~/.bashrc):
export PATH=/usr/bin:$PATH
export DOCKER_HOST=unix:///run/user/1005/docker.sock

[testuser@www /]$ systemctl --user start docker
[testuser@www /]$ I

```

Kuva 61 Succesfully created context rootless

```

$ docker service ls
* service_name    mode  task_count  image
  rootless         replicated 1  testuser/testrootless

$ curl -s https://github.com/docker/docker/releases/download/v20.10.16/docker.tgz | tar -xvz
$ curl -s https://github.com/docker/docker/releases/download/v20.10.16/docker | chmod +x
$ ./docker --version
Docker: 20.10.16
API version: 1.41 (minimum version 1.12)
Go version: go1.17.10
OS/Arch: linux/amd64
Built: Thu May 12 09:17:20 2022
OS/Arch: linux/amd64
Experimental: false
Container ID: 21ce856fa2ff4b9c21b2798135fc6fb7c53efc16
Version: 1.4.4
GitCommit: v1.4.4-0-g52de2bd
Name: docker
GitCommit: v1.1.1-0-g52de2bd
dockerd-init: 0.19.0
GitCommit: dev19ad0
+ systemctl --user enable docker.service
[INFO] Installed docker.service successfully.
[INFO] To control docker.service, run: systemctl --user {start|stop|restart} docker.service
[INFO] To run docker.service on system startup, run: sudo logindctl enable-lmager testuser
[INFO] CLI context "rootless" already exists
[INFO] Make sure the following environment variables are set (or add them to ~/.bashrc):
export PATH=/usr/bin:$PATH
export DOCKER_HOST=unix:///run/user/1005/docker.sock

$ docker ps
CONTAINER ID  IMAGE COMMAND CREATED STATUS PORTS NAMES
(testuser@www)  15

```

The terminal window shows the configuration and startup of the Docker daemon in a rootless environment. It includes the download and extraction of the Docker binary, setting environment variables, and listing running containers.

Kuva 62 Onnistunut harjoitus

4 Pohdinta

Lab4 tarkoituksesta oli harjoitella Linux, Docker ja Wordpressin koventamista. Harjoituksen kohdeena käytettiin WWW-palvelinta.

Teorialla ja harjoituksella ryhmän jäsenet saivat taidot ja ymmärryksen Linuxin koventamisesta Lynis ohjelmistolla. Lisäksi toteutettiin SSH kovennuksia ja Wordpress kovennuksia asetuksien kautta, sekä Docker koventamista niin, että oli ideana saada Docker pyörimään käyttäjällä, jolla ei ole root oikeuksia('rootlessina'), jolloin jos joku "korkkaa" dockerin, niin sillä ei voida tehdä paljoa harmia. Kokonaisuus oli todella laaja ja siksi jaettuna useammalle viikolle. Lisäksi harjoitustyössä esitettiin teoria Linuxista, Dockerista ja Wordpressistä yleisesti.

Harjoitustyön tekemiseen meni aikataulullisesti pari viikkoa, mutta sitä työstettiin monta tuntia kerrallaan, siksi se saatiin tehtyä nopeammin kuin annettu 4 viikon aikaraja. Haastavin osuuus ryhmän jäsenille oli Dockerin ajaminen rootlessina.

Saimme apua opettajalta ja tilanne selvisi, mutta aika kauan kerkesimme yhdessä yrittää ratkaista ongelmaa. Omalla tavallaan jokaisessa labrassa tähän asti paras osuus oppimiseen on juuri virhetilanteet, joiden takia on otettava askelia taaksepäin ja tuplatarkastettava, että kaikki on tehty oikein ohjeiden mukaan. Näin saman asian toistaminen uudestaan parantaa aihealueen syvempää oppimista ja sekä tehtävien tarkoitusta ja niiden tavoitteiden ymmärtämistä.

Lähteet

Del Alba, Lucero. 9.12.2022. What Is Docker?. Viitattu 3.4.2023. <https://www.sitepoint.com/what-is-docker/>

Docker overview. n.s. Dockerin kotisivut. Viitattu 3.4.2023. <https://docs.docker.com/get-started/overview/>

Kinnunen, I. 2019. WordPress teemakehitys. Opinnäytettyö, AMK Haaga-Helia Ammattikorkeakoulu, Tietojenkäsittelyn koulutusohjelma. Viitattu 4.4.2023.

<https://www.theseus.fi/bitstream/handle/10024/180314/WordPress%20Teemakehitys.pdf?sequence=2&isAllowed=y>

Rkhunter. 2022. archlinux verkkosivut. Viitattu 3.4.2023. <https://wiki.archlinux.org/title/Rkhunter>

What is Linux?. 2023. Red Hat ohjelmistoyhtiön verkkosivut. Viitattu 23.3.2023. <https://www.red-hat.com/en/topics/linux/what-is-linux>

What is the Linux kernel?. 2019. Red Hat ohjelmisto yhtiön verkkosivut. Viitattu 23.3.2023. <https://www.redhat.com/en/topics/linux/what-is-the-linux-kernel>

