



Labra 5 - Koventaminen

Ryhmä 3

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Markku Sutinen

Harjoitustyö

Huhtikuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

Sisältö

1	Johdanto	2
2	Teoria.....	2
2.1	2FA.....	2
2.2	MFA eli monivaiheinen tunnistautuminen	3
3	Toteutus	4
3.1	2FA Docker	4
3.1.1	Todennus	9
3.2	2FA SSH.....	11
3.2.1	Todennus	14
4	Pohdinta.....	17
	Lähteet	18

Kuviot

Kuvio 1.	admin panel.....	5
Kuvio 2.	Asennus wizard	5
Kuvio 3.	Asennuksen hyväksyntä	6
Kuvio 4.	QR-koodi.....	7
Kuvio 5.	Todennus.....	7
Kuvio 6.	Palautuskoodit	8
Kuvio 7.	Asetukset näkyvät välilehdellä WP 2FA	8
Kuvio 8.	Todentautuminen	9
Kuvio 9.	Todentautuminen	10
Kuvio 10.	Todennus toimi	10

1 Johdanto

Kyseisen laboratorioharjoituksen tarkoitus on tutustua MFA-käytäntöihin sekä ottaa kyseinen käytäntö käyttöön VLE-ympäristössä sekä Wordpressin kirjautumiseen, että WWW –palvelimen SSH-kirjautumisen kohdalla.

2 Teoria

2.1 2FA

Kaksivaiheinen tunnistautuminen, lyhyesti 2FA, on lisäkerros suojaamaan verkkotilejä. Se auttaa estämään luvattoman pääsyn tileihin ja suojaa identiteettivarkaudelta. Tämä menetelmä vaatii todistamaan henkilöllisyyden kahdella eri tavalla, esimerkiksi salasanalla ja puhelimeesi lähetetyllä koodilla, turvakysymyksellä, sormenjäljellä tai erityisellä sovelluksella. (F-Secure - Mikä on kaksivaiheinen tunnistautuminen (2FA)? 2024.)

Englanniksi kaksivaiheinen tunnistautuminen tunnetaan nimellä "two-factor authentication" tai 2FA, ja jos tunnistautumisessa käytetään kahta tai useampaa menetelmää, puhutaan monivaiheisesta tunnistautumisesta eli MFA:sta (multi-factor authentication). Nämä menetelmät tekevät tileihin murtautumisen vaikeammaksi, mikä on tärkeää, sillä rikolliset voivat varastaa henkilötietoja tai rahoja, jos he pääsevät tileihin käsiksi. (F-Secure - Mikä on kaksivaiheinen tunnistautuminen (2FA)? 2024.)

Kaksivaiheinen vahvistus toimii niin, että ensin syötetään käyttäjätunnus ja salasana, mutta näiden lisäksi käyttäjän on annettava toinen todiste henkilöllisyydestä. Salasanat voivat olla haavoittuvaisia, sillä ne voidaan varastaa tai murtaa, ja käyttäjätunnukset ovat usein helposti saatavilla. Monet ihmiset käyttävät samaa salasanaa useilla tileillä, mikä lisää riskiä. Salasanojenhallintaohjelmat voivat auttaa luomaan ja hallitsemaan vahvoja salasanoja ilman, että henkilön tarvitsee muistaa niitä kaikkia. (F-Secure - Mikä on kaksivaiheinen tunnistautuminen (2FA)? 2024.)

Kaksivaiheisen tunnistautumisen menetelmät voidaan jakaa kolmeen luokkaan: jotain mitä tiedät (kuten salasana), jotain mitä omistat (kuten puhelin tai erityinen laite) ja jotain mitä olet (kuten sormenjälki tai kasvontunnistus). Monet verkkopalvelut tarjoavat kaksivaiheista tunnistautumista,

mutta se ei välttämättä ole oletusarvoisesti käytössä, joten käyttäjien on itse aktivoitava se asetuksista. Kaksivaiheisen tunnistautumisen käyttöönotto ja käyttö vaihtelevat palvelun mukaan, ja joissakin tapauksissa se voidaan vaatia vain uudella laitteella kirjautuessa tai joka kerta kirjauduttaessa. (F-Secure - Mikä on kaksivaiheinen tunnistautuminen (2FA)? 2024.)

2.2 MFA eli monivaiheinen tunnistautuminen

Monivaiheisella tunnistautumisella tarkoitetaan sitä, että henkilöllisyyden varmistamiseen käytetään kahta tai useampaa tunnistautumistapaa. Käyttäjätilien kaappausyritykset muuttuvat erittäin vaikeiksi, kun käytössä on monivaiheinen tunnistautuminen. Esimerkiksi salasanan vaarantuminen ei mahdollista käyttäjätilille kirjautumista, kun käytössä on monivaiheinen tunnistautuminen. Monivaiheinen tunnistautuminen ei vaadi ylimääräisten koodien tai tunnusten käyttöä. Ylimääräinen tunnistautumistekijä on kertakäyttöinen. Käyttäjä saa esim. numerosarjan kirjautumistapahtuman yhteydessä valitsemallaan tavalla. (Monivaiheinen tunnistaminen suojaa käyttäjätilejasi 2023).

Monivaiheinen tunnistautuminen perustuu tiettyihin perusperiaatteisiin:

- jotain mitä tiedän?
 - o esimerkiksi salasana
- jotain mitä omistan
 - o esimerkiksi matkapuhelimeen lähetettävä mobiilivarmenne
- jotain mitä olen.
 - o yksilöivä ominaisuus, kuten sormenjälki

(Monivaiheinen tunnistaminen suojaa käyttäjätilejasi. 2023)

joidenkin lähteiden mukaan lisätunnistautumiskeinoina voidaan käyttää myös,

- jotain missä olen
 - o kuten ip osoitteen tunnistaminen tai geopaikannus
- jotain mitä teen
 - o kuten käytöksen profilointi, hiirenliikkeiden analysointi tai vaikka kävelyn analyysi

(Multifactor Authentication Cheat Sheet 2024)

Useissa palveluissa käyttäjän on mahdollista valita usean eri tunnistautumistavan väliltä. Näitä ovat mm. salasana, sormenjälkitunniste, vahvistusviesti sähköpostiin tai puhelimeen, todennuslaite, muuttuva PIN-koodi, palautuskoodi, todennussovellus.

MFAta käyttöönotettaessa moni palvelu tarjoaa listan kertakäyttöisistä numerosarjoista, joilla MFA on mahdollista kiertää, mikäli pääsy ensisijaiseen tunnistautumismenetelmään on estynyt. (Monivaiheinen tunnistaminen suojaa käyttäjätilejäsi. 2023). Muita tapoja MFA:n palauttamiseen on vaatia palvelua käyttöönotettaessa usean eri tavan MFA (kuten digitaalinen sertifikaatti tai One-Time Passoword Core ja yhteystieto johon palautussalasana lähetetään), tällä voidaan pienentää riskiä MFA:n palauttamisesta, jos yksittäinen todennuskeino ei ole käytettävissä tai katoaa. (Multifactor Authentication Cheat Sheet 2024).

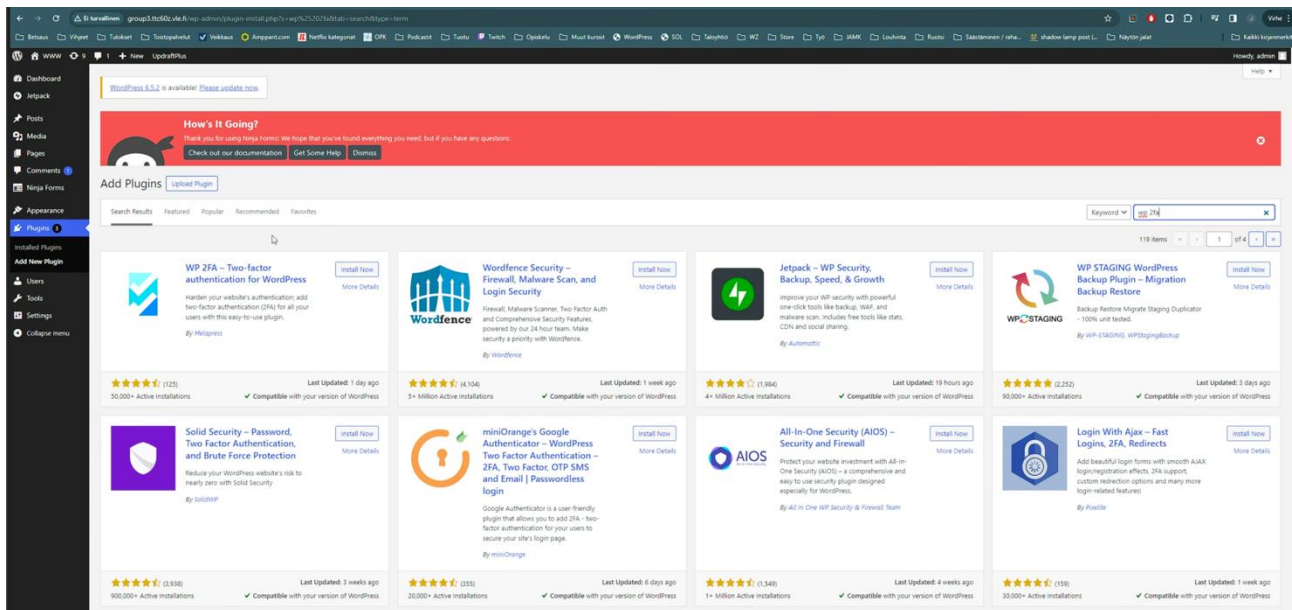
Monivaiheisen tunnistautumisen heikkouksina on pidetty hankaluutta, koska se vaatii perinteisen salasanan lisäksi toisenkin menetelmän käyttöä. Riippuvuutta toisesta tekijästä, jos käytössä on esimerkiksi vain yksi toinen tekijä, kuten älypuhelin. Sen käytön estyminen voi estää tunnistautumisen kokonaan. Myös kustannukset voivat lisääntyä, jos tunnistautumiseen tarvitaan erillistä laitetta. (Multifactor Authentication Cheat Sheet 2024).

3 Toteutus

3.1 2FA Docker

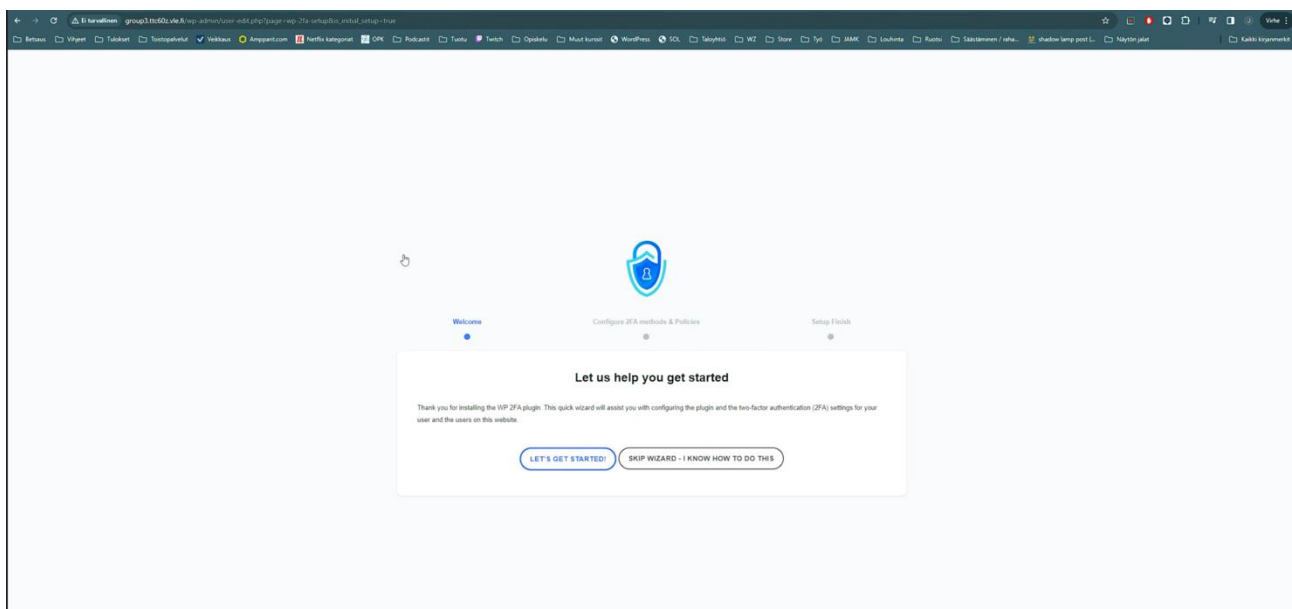
Aloitetaan kaksivaiheisen tunnistautumisen asentaminen dockerille kirjautumalla WWW-palvelimen wordpress admin hallintapaneelille, joka löytyy osoitteesta:

<http://www.group3.ttc60z.vle.fi/wp-admin/>. Siirrytään plugins välilehdelle ja asennetaan WP 2FA – Two-factor authentication for WordPress ohjelmistokomponentti, plugins (ks. Kuvio 1). Koska teimme koventamisen labra 4:ssä välivaiheen, joka on kuvattu asentamisen labraohjeessa, asennus menee suoraan läpi. Asennusohjeessa oli välivaihe, jossa hakemistoon /var/www omistajaksi ja ryhmäksi asetetaan www-data. Tällä varmistetaan, että verkkopalvelin voi lukea ja kirjoittaa tiedostoja kyseisessä hakemistossa.



Kuvio 1. admin panel

Kun ohjelmistokomponentti plugin on asennettu, avautuu asennus wizard, joka ohjaa käyttäjää asentamaan palvelun (ks. Kuvio 2).

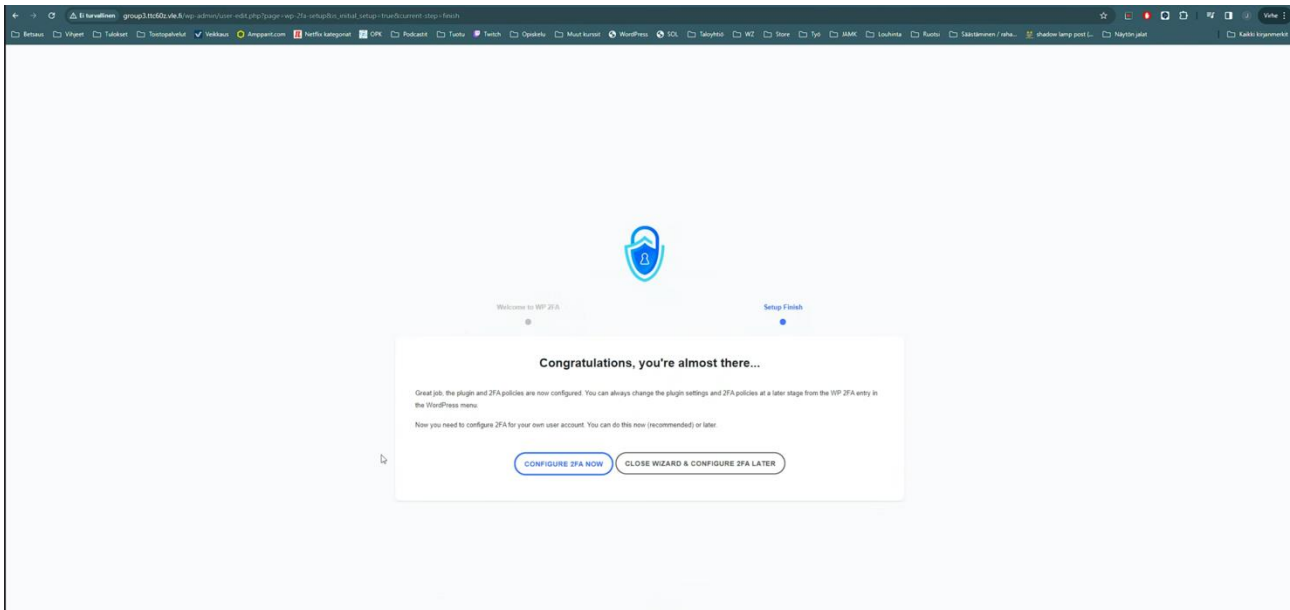


Kuvio 2. Asennus wizard

Valitaan asennuksen aikana seuraavat asetukset:

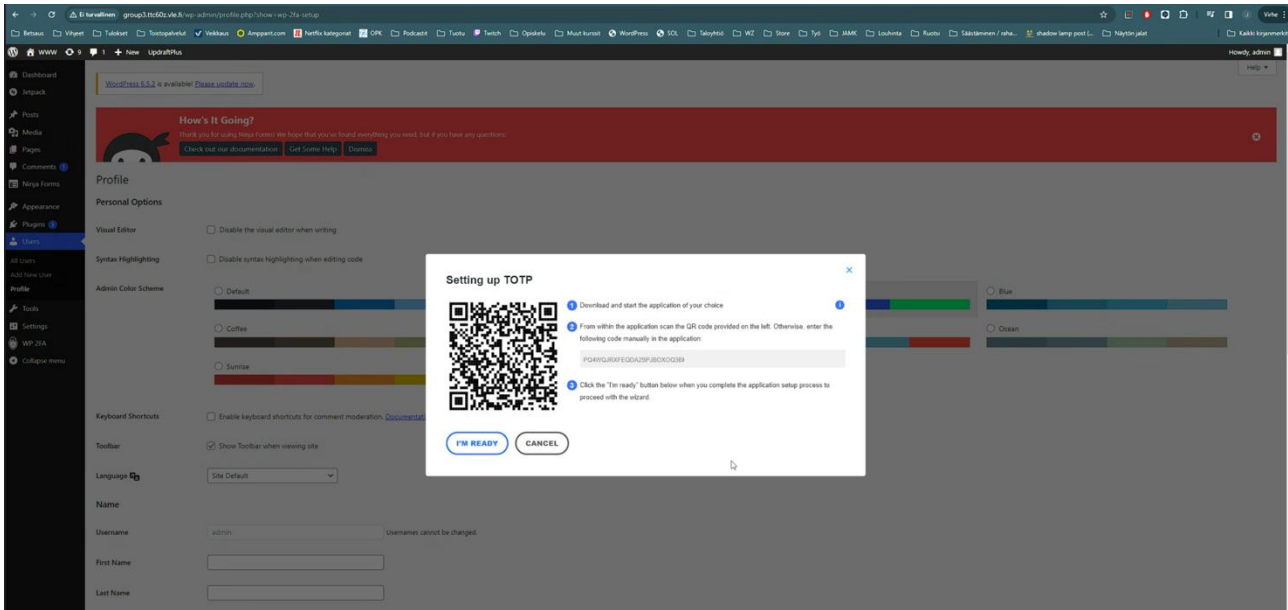
- One-time code via 2FA
- Backupcodes
- Do you want to enforce 2FA for some, or all the users -> valitaan all users
- How long should the grace period for your users be -> valitaan users have to configure 2FA straight away

Kun asetukset on valittu, hyväksytään ne ja aloitetaan asennus valitsemalla configure 2FA now (ks. Kuvio 3)



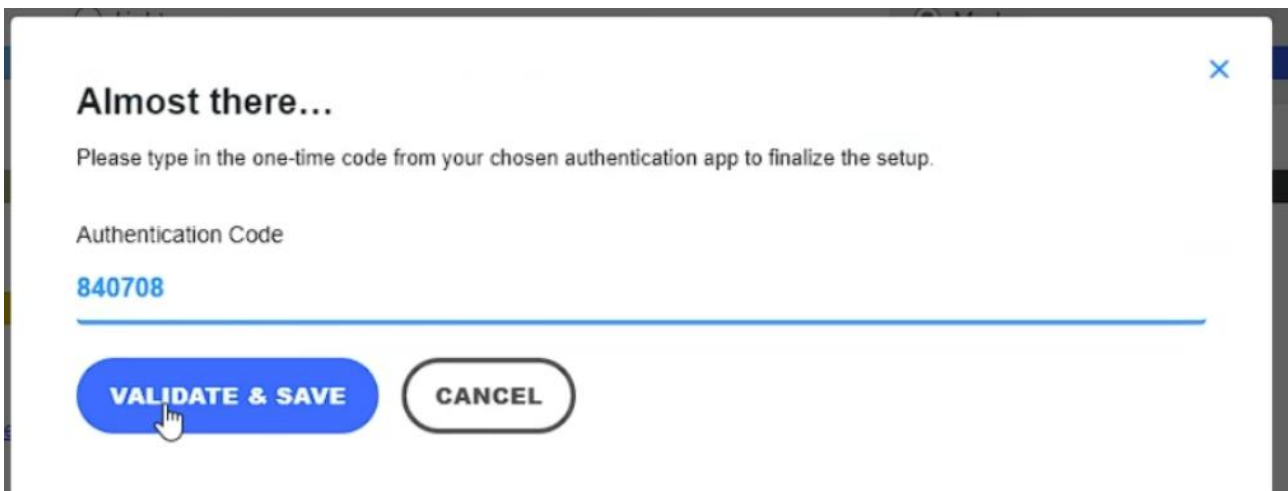
Kuvio 3. Asennuksen hyväksyntä

Seuraavaksi asennus ohjaa asentamaan Google authenticatorin ja wizard luo QR-koodin (ks. Kuvio 4), joka pitää tuoda laitteelle esimerkiksi omalle puhelimelle, jossa Google authenticator on asennettu ja otettu käyttöön.



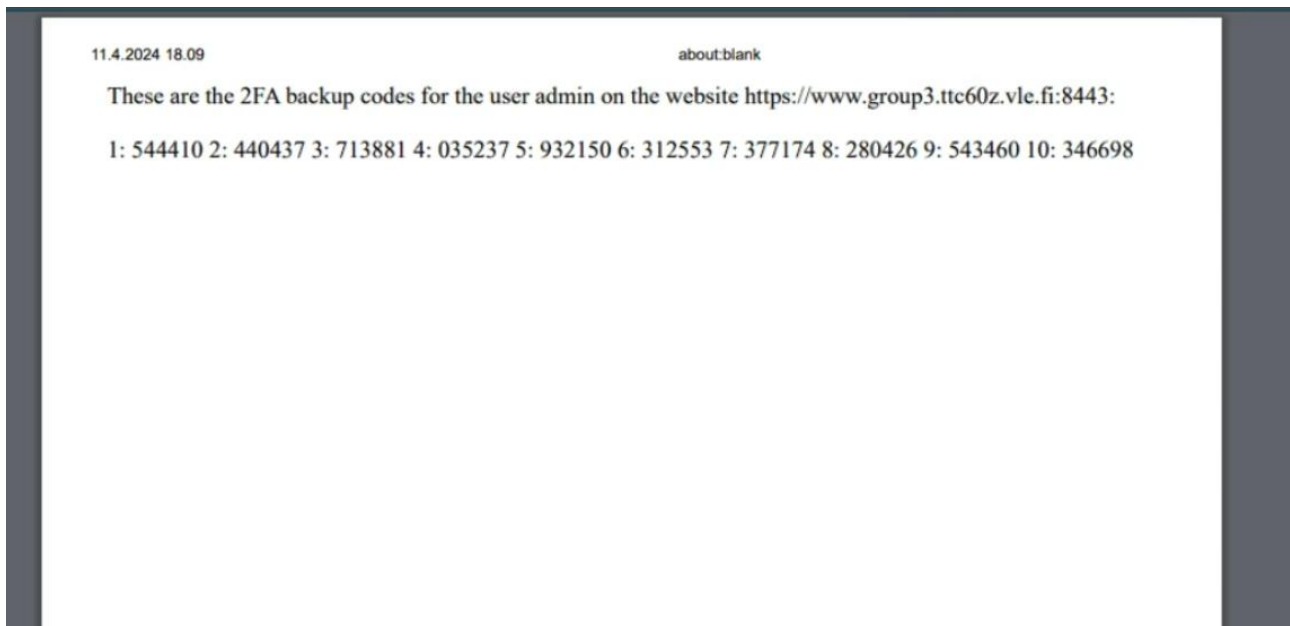
Kuvio 4. QR-koodi

Kun QR-koodi on tuotu Google authenticatoriin se luo kuusinumeroisen todennusnumeron, jota wizard pyytää (ks. Kuvio 5).



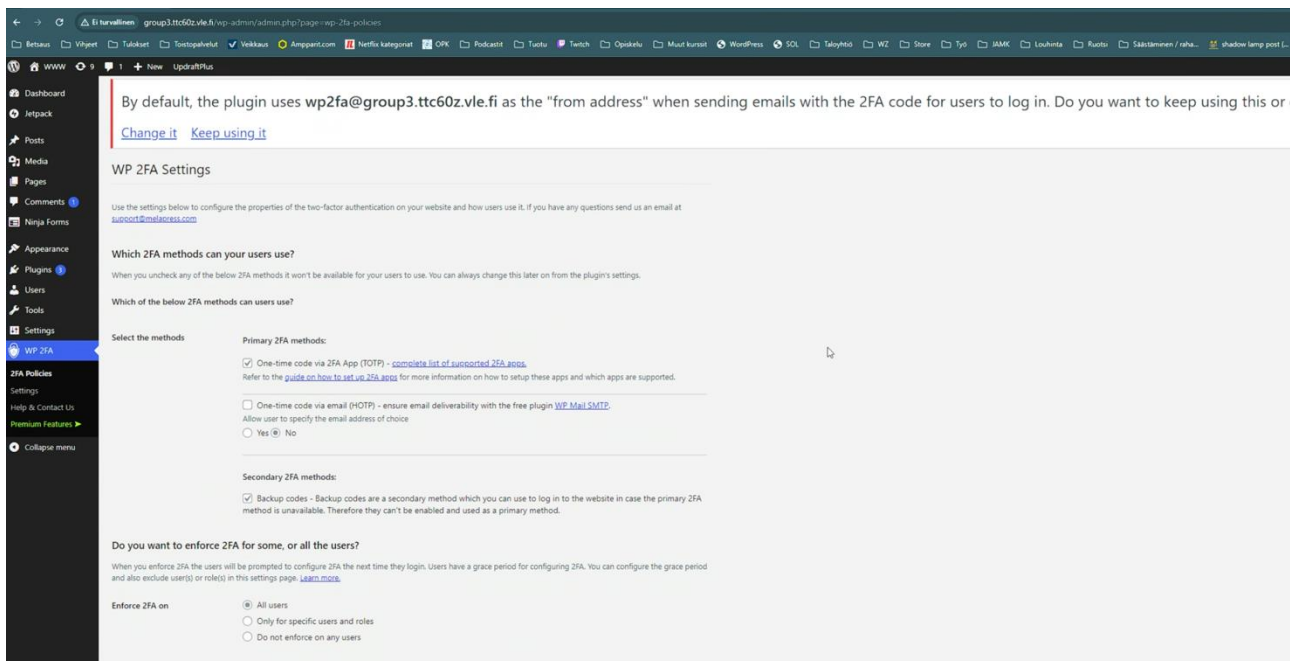
Kuvio 5. Todennus

Asennus luo myös palautuskoodit (ks. Kuvio 6).



Kuvio 6. Palautuskoodit

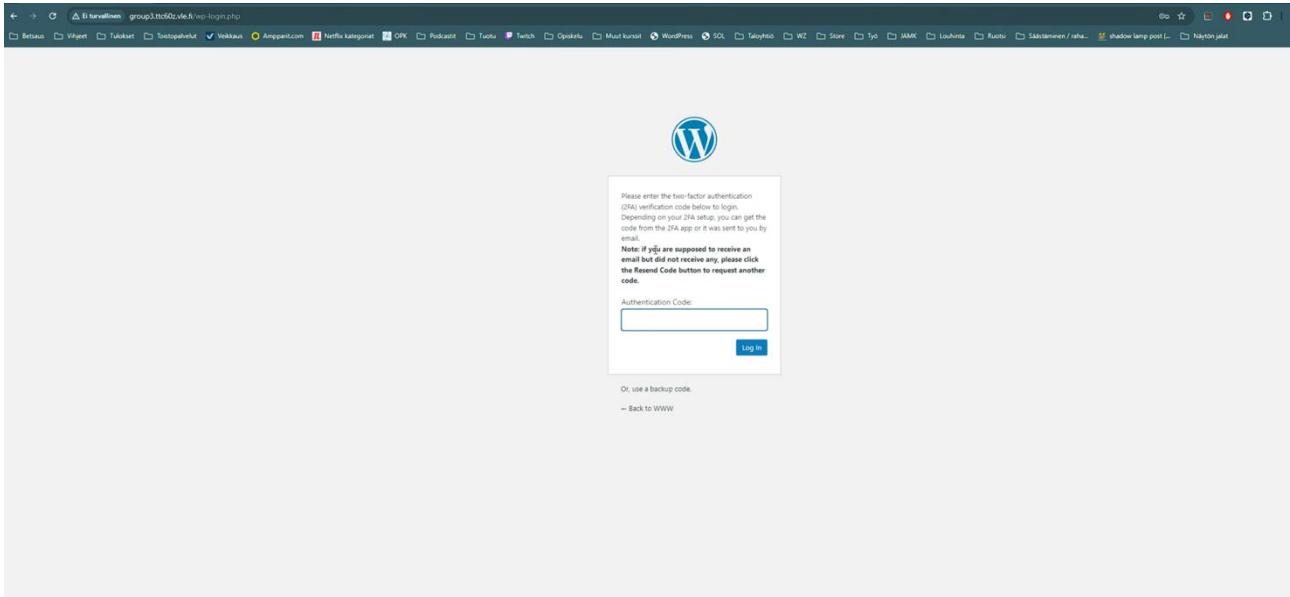
Tämän jälkeen asennus on valmis ja asetukset näkyvät valikossa (ks. Kuvio 7).



Kuvio 7. Asetukset näkyvät välilehdellä WP 2FA

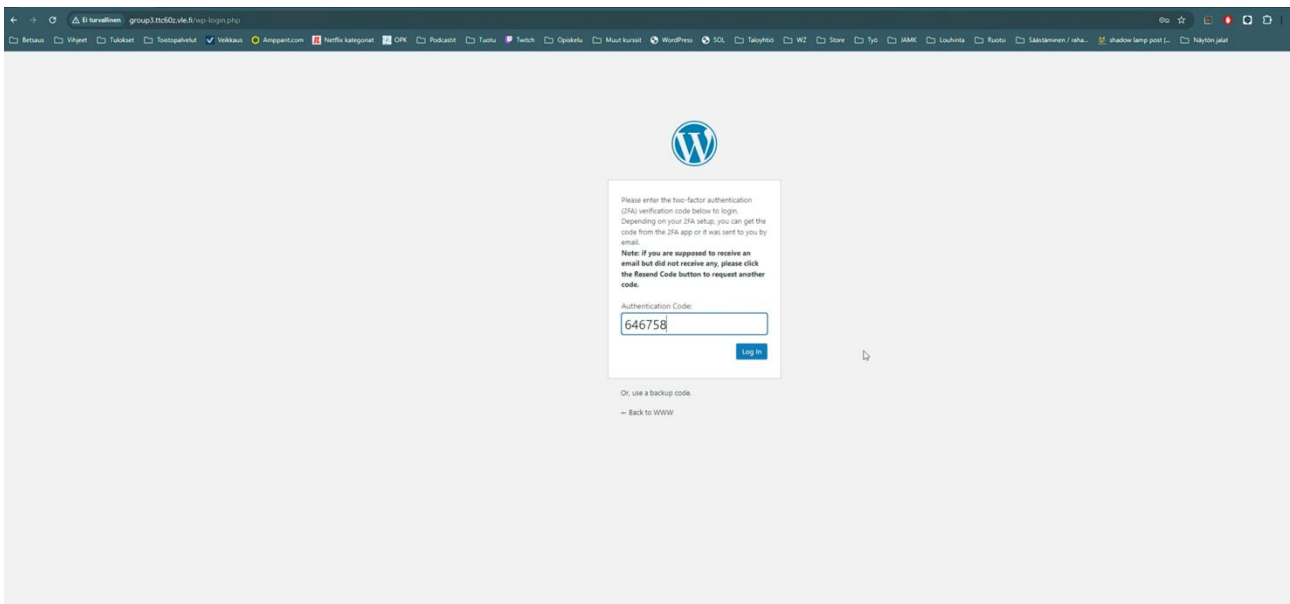
3.1.1 Todennus

Asennuksen jälkeen kirjaudutaan sivuilta ulos ja testataan, toimiiko kaksivaiheinen tunnistautuminen. Kirjaudutaan uudelleen sivuille ja huomataan, että uusi todennuskuvake, jossa pyydetään syöttämään kuusinumeroinen luku. (ks. Kuvio 8).



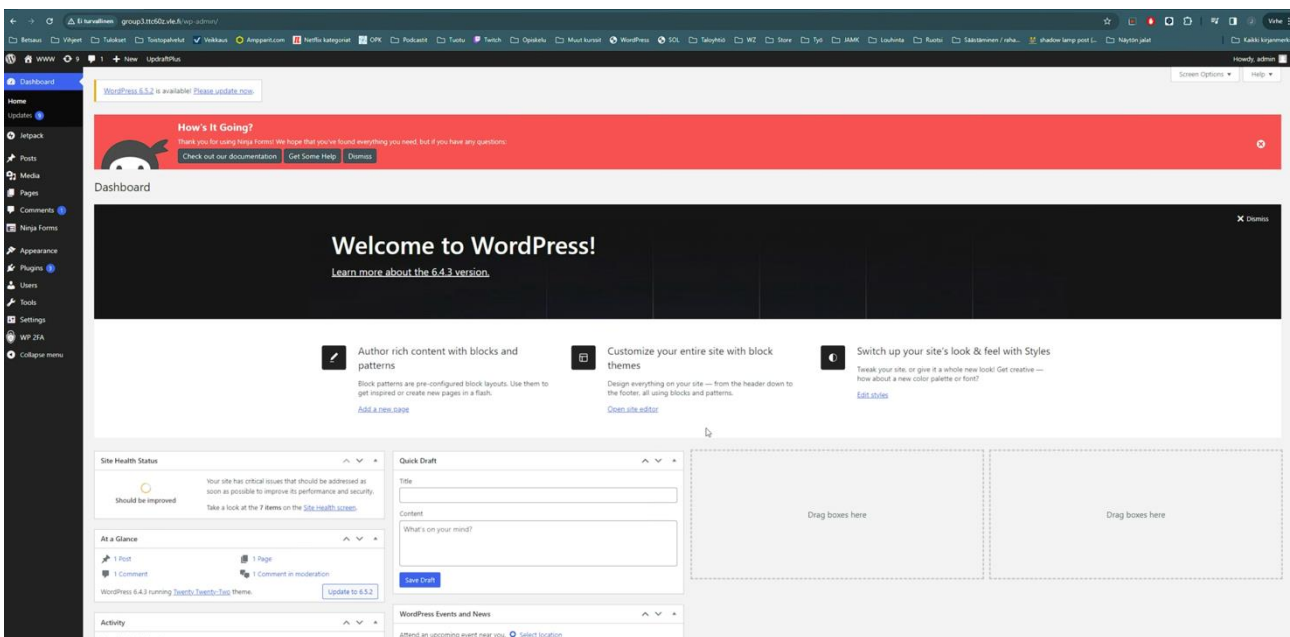
Kuvio 8. Todentautuminen

Katsotaan luku Googlen authenticator sovelluksesta ja syötetään numerot (ks. Kuvio 9). Sinulla on lyhyt aika syöttää numerot, koska luvut vaihtuvat nopeasti.



Kuvio 9. Todentautuminen

Todennus toimi hienosti ja pääsimme sivuille (ks. Kuvio 10).



Kuvio 10. Todennus toimi

3.2 2FA SSH

Teimme kaksivaiheisen tunnistautumisen myös WWW-palvelimen SSH-kirjautumiseen. Aloitimme antamalla komennot: `sudo dnf install -y epel-release` ja `sudo dnf install -y google-authenticator` qrencode qrencode-libs eli asensimme Extra Packages for Enterprise Linux liittyvän paketin nimeä epel-release. EPEL luo, ylläpitää ja hallinnoin lisäpaketteja Enterprise Linuxille. Toinen komento asentaa Google Authenticator ohjelmiston, QR-koodien luomiseen tarkoitetun ohjelmiston (qrencode) ja qrencoden kirjastot. Asentamisen jälkeen ajoimme komennon `google-authenticator -s ~/.ssh/google_authenticator` joka tee uuden salaisen avaimen `~/.ssh/` kansioon. Vastattuamme kyllä kohtaan ”haluatko todennustunnusten olevan aikaperusteisia?” ilmestyi QR-koodi (ks. Kuvio 11). joka pitää skannata oman puhelimen Google Authenticator sovelluksella.



Kuvio 11. QR-koodi

Tämän jälkeen siirryimme kohtaan, jossa konfiguroidaan SSH Daemon käyttämään Google Authenticatoria. Avasimme `sshd_config` tiedoston ja laitoimme `UsePAM`, `ChallengeResponseAuthentication` ja `PermitRootLogin` kohtaan `yes` (ks. Kuvio 12).



```

root@www: /etc/ssh/sshd_config
GNU nano 2.9.8 Modified

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
#PasswordAuthentication no

# Change to no to disable s/key passwords
ChallengeResponseAuthentication yes
#ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
#GSSAPIEnableK5users no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without

```

Kuvio 12. sshd_config tiedosto

Suljimme tiedoston ja avasimme PAM rule tiedoston, minne lisäsimme kaksi riviä (ks. Kuvio 13). Alempi rivi ottaa käyttöön kaksivaiheisen tunnistautumisen. Tallensimme ja suljimme tiedoston minkä jälkeen käynnistimme SSH daemonin uudestaan, jotta muutokset tulevat voimaan.

```

GNU nano 2.9.8 /etc/pam.d/sshd Modified
##PAM-1.0
auth        substack    password-auth
auth        include     postlogin
#two-factor authentication via Google Authenticator
auth        required    pam_google_authenticator.so secret=${HOME}/.ssh/google_authenticator
account     required    pam_sepermit.so
account     required    pam_nologin.so
account     include     password-auth
password    include     password-auth
# pam_selinux.so close should be the first session rule
session     required    pam_selinux.so close
session     required    pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session     required    pam_selinux.so open env_params
session     required    pam_namespace.so
session     optional    pam_keyinit.so force revoke
session     optional    pam_motd.so
session     include     password-auth
session     include     postlogin
  
```

Kuvio 13. PAM rule tiedosto

Siirryimme kohtaan, jossa todennus tehdään julkisella avaimella ja kaksivaiheisella tunnistautumisella. Avasimme uudestaan sshd_config tiedoston missä UsePAM, ChallengeResponseAuthentication ja PermitRootLogin olivat jo yes. Lisäsimme AuthenticationMethods publickey,keyboard-interactive rivin tiedoston loppuun (ks. Kuvio 14). Kyseinen rivi kertoo SSH daemonille että käyttäjän pitää läpäistä julkisen avaimen todennus ja challenge-response todennus. Tallensimme ja suljimme tiedoston ja menimme takaisin PAM rule tiedostoon, josta kommentoimme kohdan auth substack password-auth (ks. Kuvio 15). Tämä poistaa salasana todennuksen käytöstä. Tallensimme tiedoston ja käynnistimme SSH daemonin uudestaan.

```

GNU nano 2.9.8 /etc/ssh/sshd_config
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS

# override default of no subsystems
Subsystem sftp /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
AuthenticationMethods publickey,keyboard-interactive

```

Kuvio 14. sshd_config tiedoston loppuun uusi rivi

```

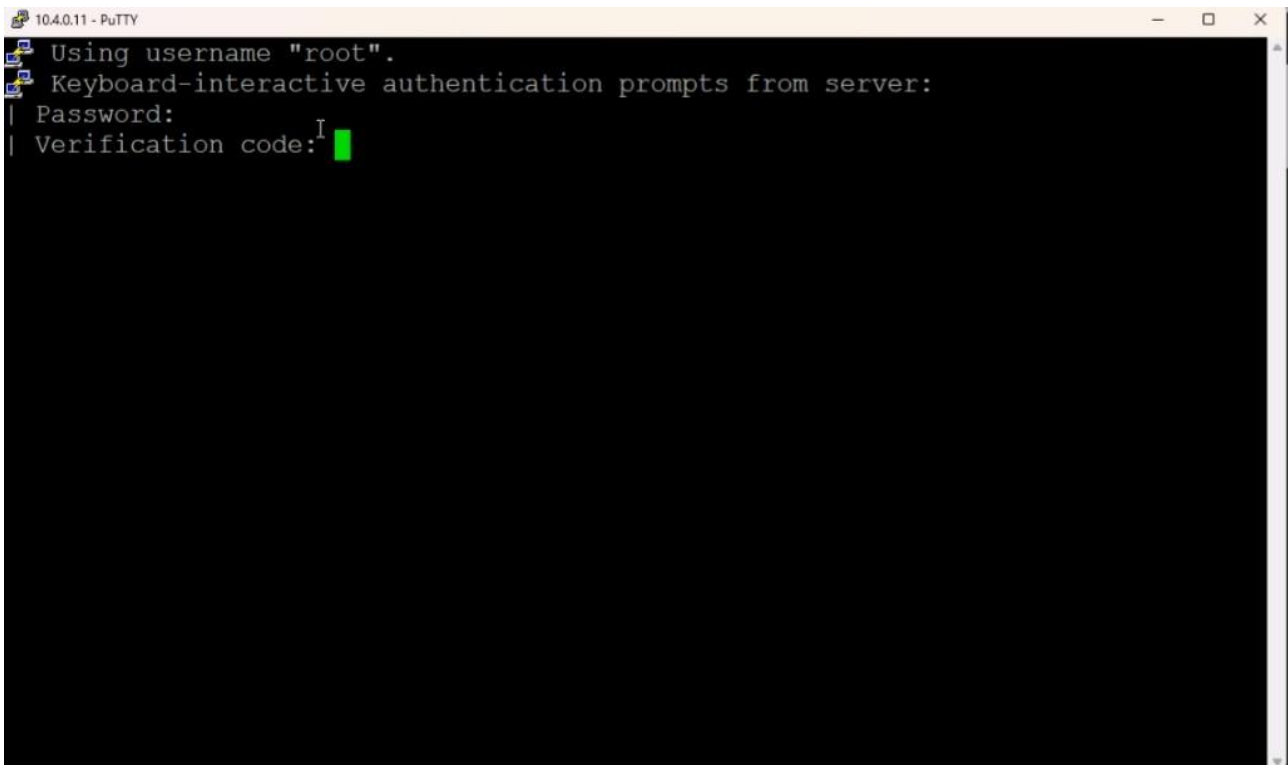
GNU nano 2.9.8 /etc/pam.d/ssh
#PAM-1.0
auth substack password-auth
auth include postlogin
#Two-factor authentication via Google Authenticator
auth required pam_google_authenticator.so secret=${HOME}/.ssh/google_authenticator
account required pam_sesmit.so
account required pam_nologin.so
password include password-auth
# pam_selinux.so close should be the first session rule
session required pam_selinux.so close
session required pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session required pam_selinux.so open env_params
session required pam_namespace.so
session optional pam_keyinit.so force revoke
session optional pam_motd.so
session include password-auth
session include postlogin

```

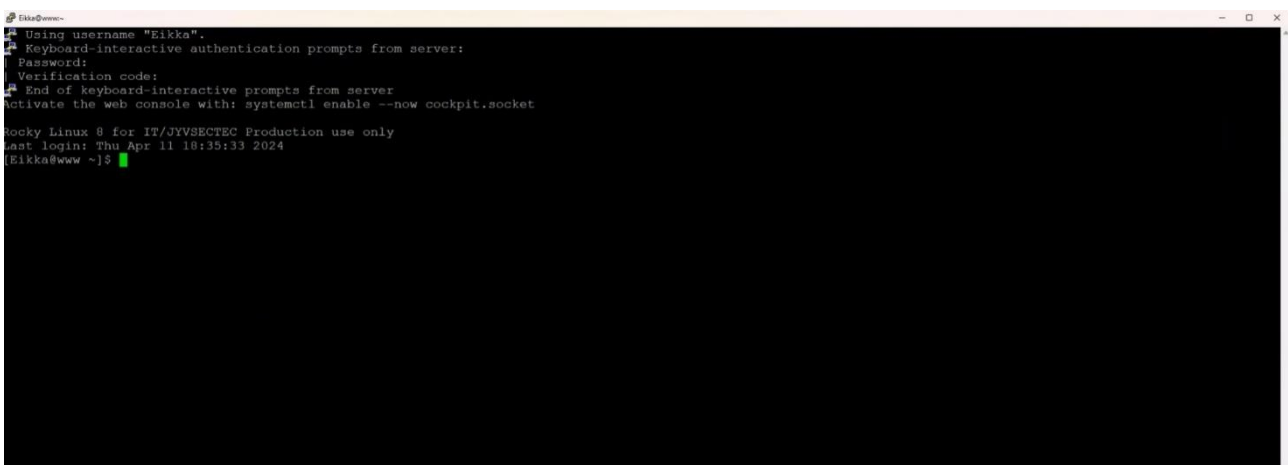
Kuvio 15. PAM rule tiedostosta salasanatodennuksen estäminen

3.2.1 Todennus

Aluksi teimme kaksivaiheisen todennuksen toimimaan salasanatodennuksen kanssa ja rootilta sekä Eikalta kysyttiin salasanaa sekä todennuskoodia (ks. Kuvio 16 ja Kuvio 17) mikä löytyi Google Authenticator sovelluksesta puhelimesta. Puhelin ei muuten anna ottaa kuvankaappausta kyseisen sovelluksen todennuskoodista. Kokeilin vielä näytön tallennusta ja avasin sovelluksen mutta siinä kohtaa ruutu menee mustaksi, joten kuvia puhelimen sovelluksesta ei ole, joista näkyisi root ja Eikka sekä heidän vaihtuvat todennuskoodinsa.

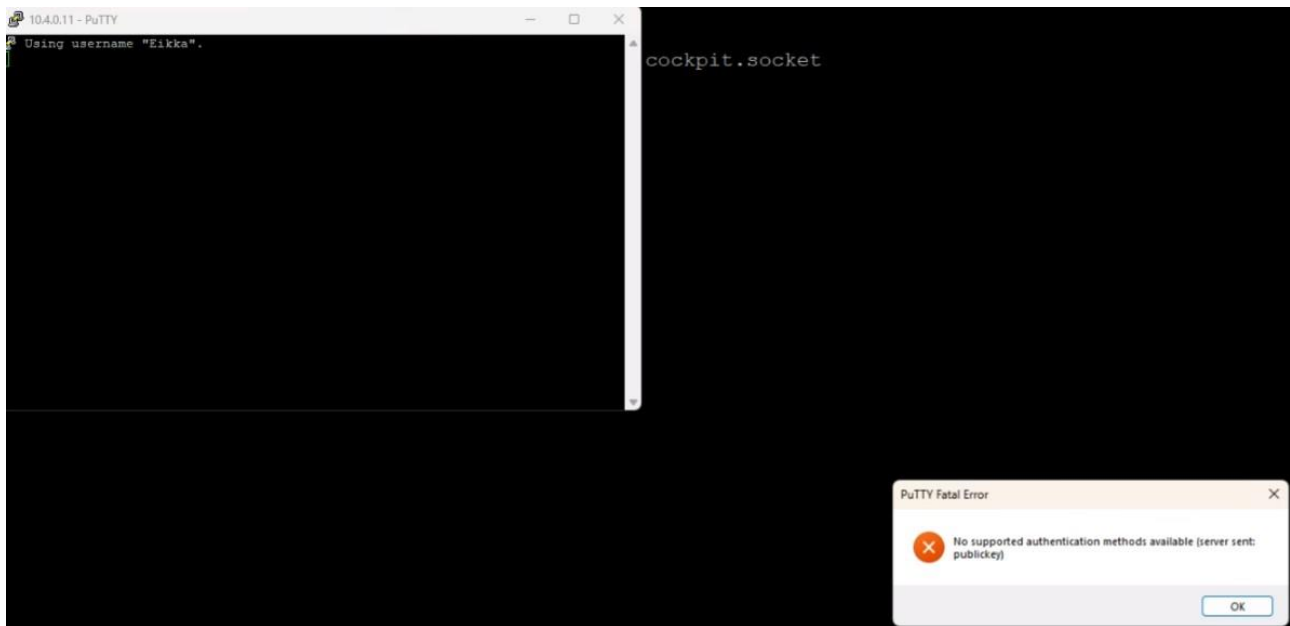


Kuvio 16. rootin todennus



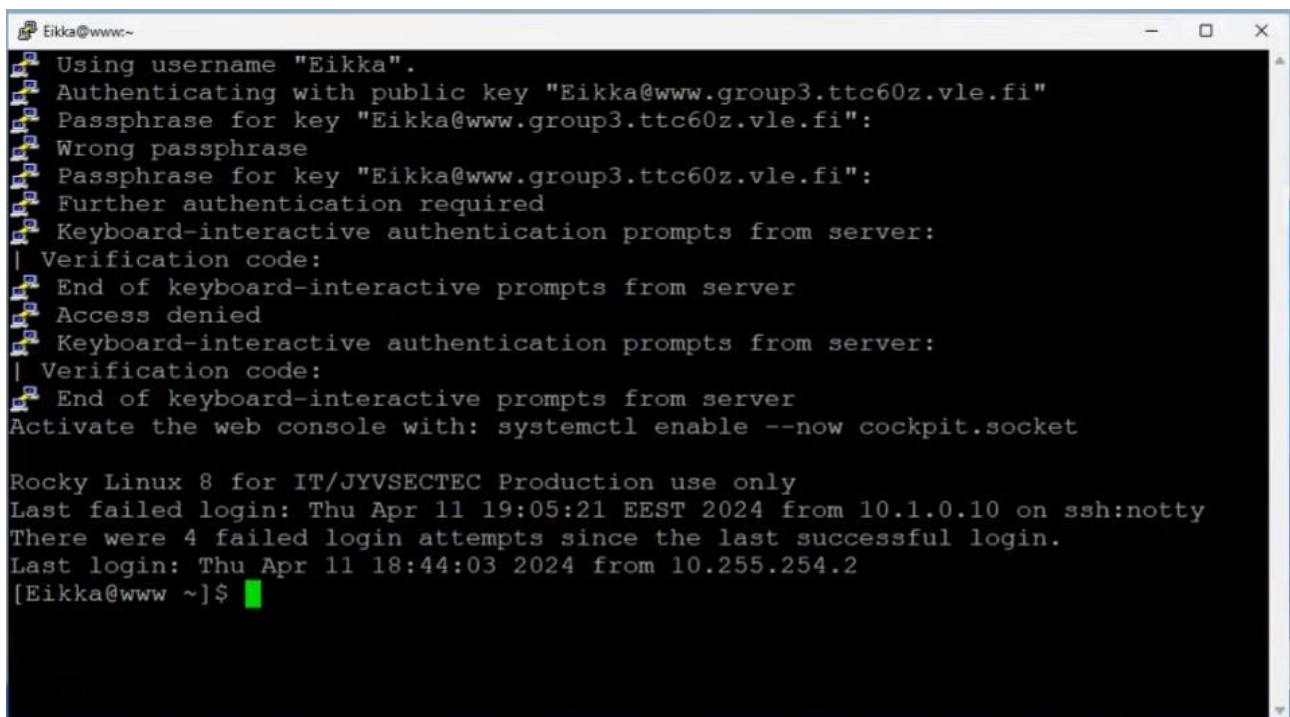
Kuvio 17. Eikan todennus

Viimeisessä kohtaa teimme kaksivaiheisen todennuksen toimimaan julkisen avaimen kanssa. Lisäsimme ja muutimme kahta tiedostoa ja kaikki toimi niin kuin piti. Kokeilimme ensin kirjautua Eikalle käyttäjältä, jolla ei ollut yksityistä avainta ja saimme error viestin (ks. Kuvio 18).



Kuvio 18. Error viesti

Tämän jälkeen kirjauduimme Eikalle käyttäjältä, jolla oli yksityinen avain ja kirjautuminen meni läpi käyttäen julkista avainta, kysyen passphrasea ja todennuskoodia (ks. Kuvio 19).



Kuvio 19. Kaksivaiheinen tunnistautuminen toimii julkisen avaimen kanssa

4 Pohdinta

Tämä labra oli selkeä ja suoraviivainen toteuttaa. Osa kohdista oli tehty jo edellisissä labroissa. Ainoa ongelma koko labran aikana oli, että yhtä qr-koodia ei pystytty suoraan lukemaan puttyä kautta, vaan käsin piti kirjoitella annettu salasana Google-authenticatoriin. Labra oli mielenkiintoinen ja saimme hyvän kuvan siitä miten 2fa/mfa saadaan erilaisiin palveluihin lisättyä.

Lähteet

F-Secure - Mikä on kaksivaiheinen tunnistautuminen (2FA)? 2024. Viitattu 16.4.2024.

<https://www.f-secure.com/fi/articles/what-is-two-factor-authentication>

Monivaiheinen tunnistautuminen suojaa käyttäjätilesi. 2023. Traficom. Viitattu 14.4.2024.

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi>

Multifactor Authentication Cheat Sheet. 2024. OWAS Cheat Sheet Series. Viitattu 14.4.2024.

https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html

