Linux videot: <https://www.youtube.com/playlist?list=PLZw_fXxI6L50ovlxunMvWw-bEDc3TiBQp>

Contents

[TLDR 1](#_Toc180736539)

[fail2ban FTP palvelimelle 5](#_Toc180736540)

# TLDR

1. Asenna paketti fail2ban
2. Valitse palvelu, jolle haluat suojauksen jail.conf
3. Määritä palvelulle haluamasi asetukset jail.conf
4. Määritä systemd backendiksi
5. Käynnistä palvelu uudestaan
6. Testaa toiminta esim. käyttämällä vääriä salasanoja
7. Katso fail2ban-client status komennolla, että bännit tuli

Fail2ban on paketti, jolla saadaan suojattua erilaisia yhteyksiä palvelimelle kuten SSH yhteys. Se havaitsee epäonnistuneet kirjautumisyritykset ja antaa bännit niille. Tämä torjuu ns. Brute Force hyökkäyksiä, joissa yritetään arvata salasana oikein todella nopeaan tahtiin.

**Fail2Ban ohje**

Ohjeen luonut: Aleksi Sievälä TITI17BR

Fail2Banin asennus:

**sudo apt install -y fail2ban**

Fail2Banin tärkeimmät tiedostot:

**/etc/fail2ban/jail.conf** # pääkonffi

**/var/log/fail2ban.log** # logi yleisille tiedoille palvelimesta

Otetaan pääkonffista backup:

**sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.conf.backup**

Fail2Banin perus syntaxi:

….

**[estettävä daemon]**

**enabled = true / false**

….

Ilman erillistä muokkausta, kaikki palvelut ovat poissa käytöstä. Jos palvelu halutaan ottaa käyttöön, tulee lisätä estolle rivi:

**enabled = true** # palvelu käytössä

Pääkonffi tiedostosta tulee aina löytyä kohta:

**[DEFAULT]**

Default estoon voidaan määritellä sääntöjä, jotka pätevät kaikkiin käytössä oleviin palveluihin, kuten:

**bantime = 120** # estoaika sekuntteina

**maxretry = 3** # sallittu yritysmäärä ennen estoa

**ignoreip = 127.0.0.1/8** # ip-osoite johon estot eivät vaikuta

**findtime = 600** # aika jonka jälkeen yritysmäärä raukeaa jos ei täynnä

**protocol = tcp** # protokolla, jota fail2ban käyttää

**port = 0-65535** # estetyt portit (kannattaa määritellä erikseen estoissa)

**logpath = /var/log/auth.log** # logi jota fail2ban käyttää estoihin

jail.conf konfiguraatiossa määritä backend käyttämään systemd toimintoa, muuten fail2ban ei todennäköisesti toimi!

Tämä saattaa löytyä suoraan myös [sshd] jailin alta, joten vaihda se sieltä.

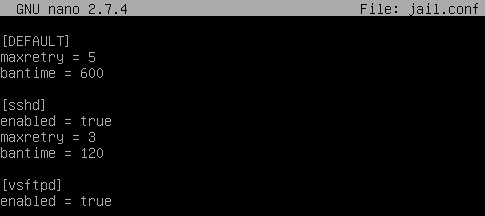
A screenshot of a computer error

Description automatically generated

**Aina kun fail2banin konffia muokataan, muista käynnistää palvelin uudestaan:**

**sudo systemctl restart fail2ban**

Jos estossa määritellään erikseen sääntö, joka on jo määritelty default kohdassa, eston erikseen määritelty sääntö yliajaa defaultin säännön, esim:

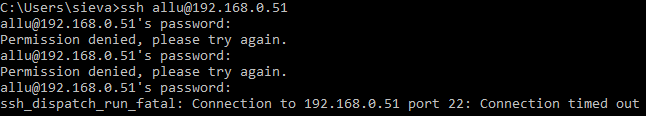


Ota huomioon, jos käytät jotakin muuta kuin ssh oletusporttia, joudut määrittämään [sshd] alle portin. Esim:

**port = 1234**

Tässä konffissa ssh daemon käyttää sille erikseen määriteltyjä sääntöjä, mutta vsftp daemon käyttää defaultissa määriteltyjä sääntöjä.

Kun yritetään ottaa ssh yhteys palvelimeen, jossa on ylläoleva fail2ban konfigurointi ja epäonnistutaan salasanassa kolme kertaa, saadaan ilmoitus:



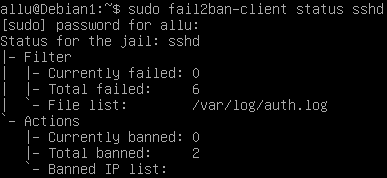
Tämän jälkeen yhteyttä ei saa otettua 120 sekunttiin vaikka salasana olisikin oikea.

Fail2Banin tietyn palvelun tietoja ja toimintaa voidaan tarkastella komennolla:

**sudo fail2ban-client status ‘palvelu’**

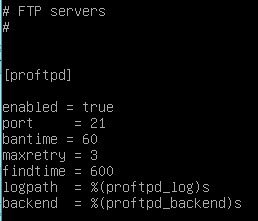
esim.

**sudo fail2ban-client status proftpd**

****

# fail2ban FTP palvelimelle

Seuraavilla asetuksilla saataisiin Fail2ban toimimaan myös proftpd FTP-palvelimen kanssa. **Muista erityisesti kohta enabled = true. Ilman sitä ei homma toimi!**



Bänni näyttäisi tältä:

