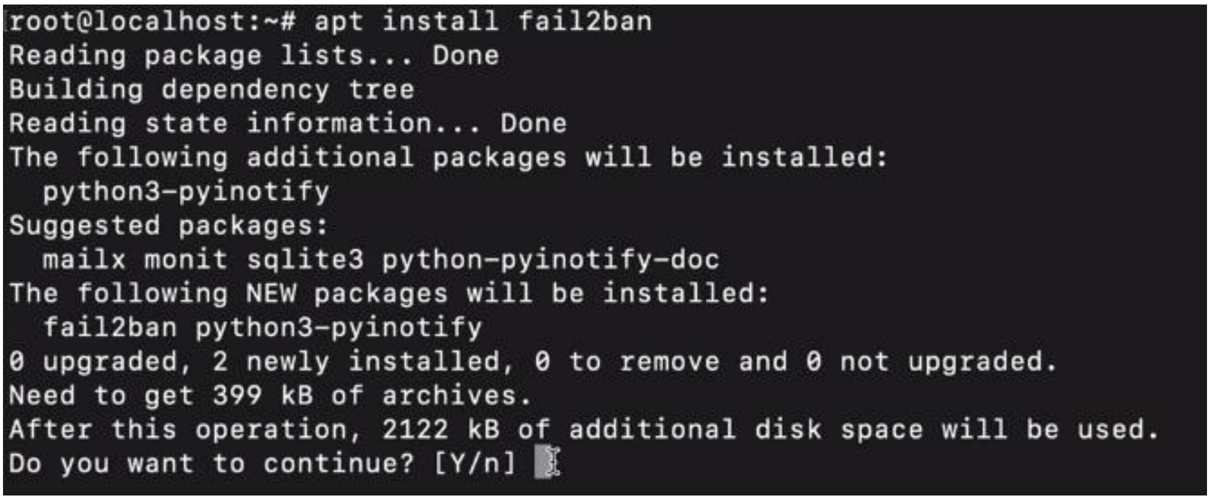
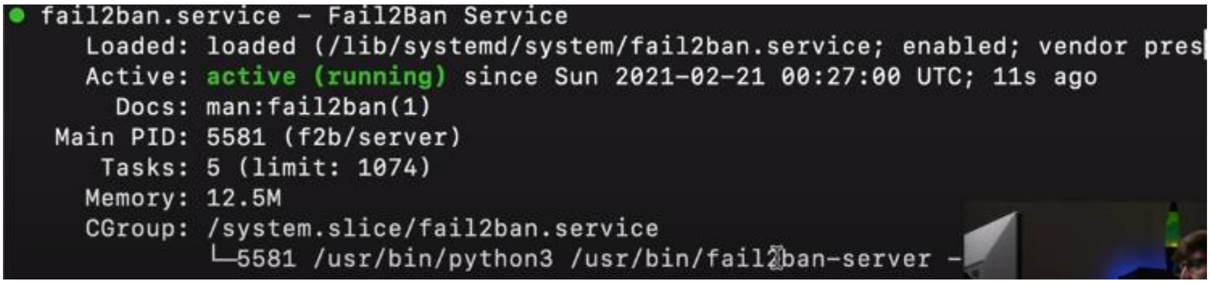
Ex8: Use Fail2ban to scans log files and bans IPs that show the malicious signs

Fail2ban is an open-source software tool used for monitoring log files and banning IP addresses that show malicious signs, such as too many failed login attempts. It is commonly used as a security measure to protect servers against brute-force attacks and other types of malicious activity.



```
root@localhost:~# apt install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 399 kB of archives.
After this operation, 2122 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Systemctl status fail2ban: running



```
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor pres
     Active: active (running) since Sun 2021-02-21 00:27:00 UTC; 11s ago
       Docs: man:fail2ban(1)
   Main PID: 5581 (f2b/server)
      Tasks: 5 (limit: 1074)
     Memory: 12.5M
     CGroup: /system.slice/fail2ban.service
             └─5581 /usr/bin/python3 /usr/bin/fail2ban-server -
```

Step2: cd /etc/fail2ban

Ls

Fail2ban.conf jail.conf

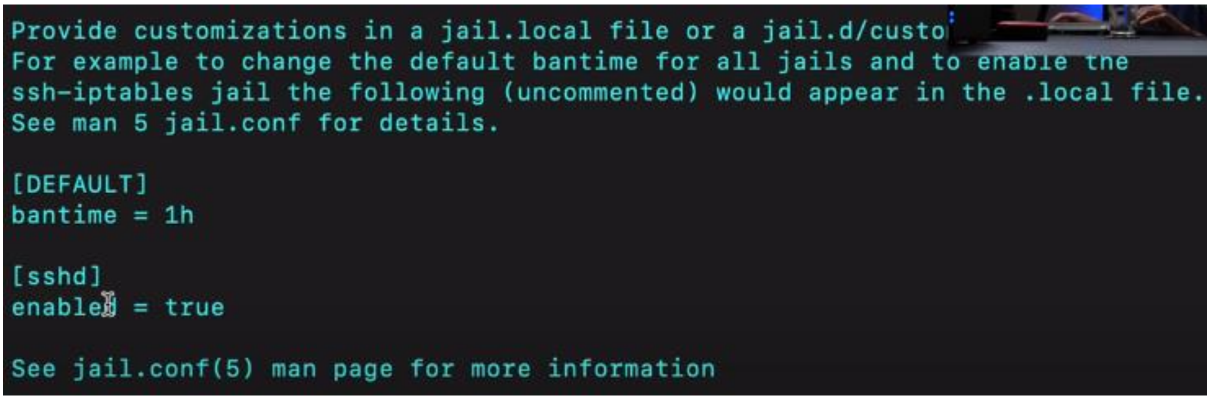
Step3:

Cp fail2ban.conf fail2ban.local

Cp jail.conf jail.local

Step: open jail.local

Sshd is open

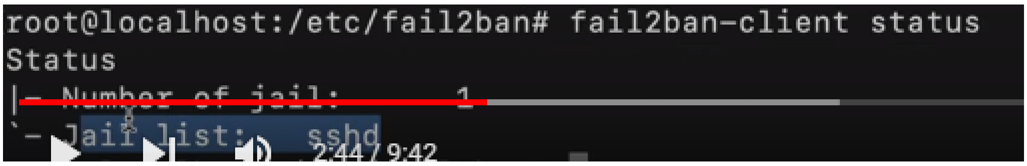


```
Provide customizations in a jail.local file or a jail.d/custo
For example to change the default bantime for all jails and to enable the
ssh-iptables jail the following (uncommented) would appear in the .local file.
See man 5 jail.conf for details.

[DEFAULT]
bantime = 1h

[sshd]
enabled = true

See jail.conf(5) man page for more information
```



```
root@localhost:/etc/fail2ban# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
```

Jail is 1