

Day 44

Exploitation Analyst

Firewalls and TCP wrappers:

Fail2ban client command:

What is Fail2ban?

fail2ban-client is the command-line tool used to interact with the Fail2ban service. It lets you check status, manage jails, and control bans without directly editing configs or restarting services. For example:

- fail2ban-client status → shows all active jails.
- fail2ban-client status sshd → shows details of the SSH jail (like banned IPs).
- fail2ban-client set sshd banip <IP> → manually ban an IP.
- fail2ban-client set sshd unbanip <IP> → unban an IP.
- fail2ban-client reload → reload rules without restarting Fail2ban.

Exploring Fail2ban client command:

Steps:

```
root@debian:/etc/fail2ban# fail2ban-client status
Status
|- Number of jail:      1
|_ Jail list:          ssh
root@debian:/etc/fail2ban# /etc/init.d/fail2ban status
● fail2ban.service - LSB: Start/stop fail2ban
   Loaded: loaded (/etc/init.d/fail2ban)
   Active: active (running) since Sat 2017-06-10 12:57:40 EDT; 9min ago
     Process: 18083 ExecStop=/etc/init.d/fail2ban stop (code=exited, status=0/SUCCESS)
     Process: 18102 ExecStart=/etc/init.d/fail2ban start (code=exited, status=0/SUCCESS)
    CGroup: /system.slice/fail2ban.service
            └─18112 /usr/bin/python /usr/bin/fail2ban-server -b -s /var/run/fail2ban/fail2ban.sock -p /var/run...

Jun 10 12:57:39 debian systemd[1]: Starting LSB: Start/stop fail2ban...
Jun 10 12:57:40 debian fail2ban[18102]: Starting authentication failure monitor: fail2ban.
Jun 10 12:57:40 debian systemd[1]: Started LSB: Start/stop fail2ban.
root@debian:/etc/fail2ban#
```

```
root@debian:/etc/fail2ban# fail2ban-client status ssh
Status for the jail: ssh
|- filter
| |_- File list:      /var/log/auth.log
| |_- Currently failed: 0
| |_- Total failed:   6
|_- action
| |_- Currently banned: 0
| |_- IP list:
| |_- Total banned:   1
root@debian:/etc/fail2ban# fail2ban-client reload
root@debian:/etc/fail2ban# fail2ban-client reload ssh
root@debian:/etc/fail2ban# fail2ban-client stop
Shutdown successful
root@debian:/etc/fail2ban# fail2ban-client start
2017-06-10 13:08:05,420 fail2ban.server [18378]: INFO Starting Fail2ban v0.8.13
2017-06-10 13:08:05,420 fail2ban.server [18378]: INFO Starting in daemon mode
```

--The End--