**Day 43**

**Exploitation Analyst**

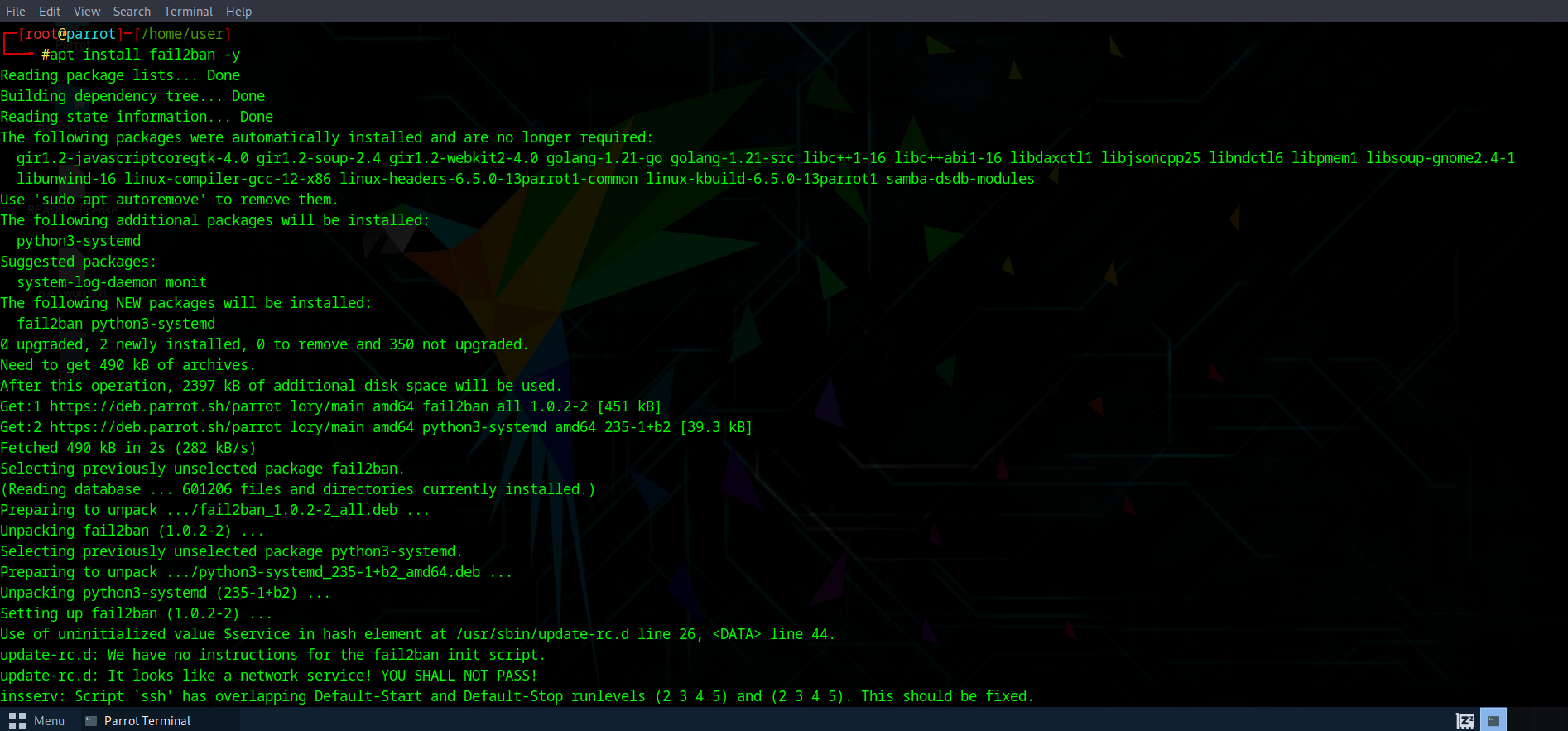
**Firewalls and TCP wrappers:**

**Fail2ban:**

**What is Fail2ban?**

Fail2ban is a security tool that helps protect Linux servers from brute-force attacks. It works by monitoring log files (like SSH, Apache, Nginx, etc.) for repeated failed login attempts or suspicious activity. When it detects too many failures from the same IP, it automatically bans that IP by adding a temporary firewall rule (using iptables or firewalld). This reduces the risk of attackers guessing passwords or overwhelming services.

Installing it: apt install fail2ban -y



**Exploring Fail2ban:**

Steps:

Search for the fail2ban using: aptitude search fail2ban



To use it, change the directory: use cd /etc/fail2ban

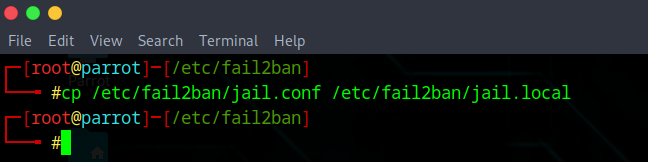


Here’s what those files/folders mean in /etc/fail2ban:

* **fail2ban.conf** → Main configuration (logging, backend).
* **jail.conf** → Default “jails” (services to protect). Never edit directly; copy to jail.local or use jail.d/.
* **jail.d/** → Place your custom jail configs here.
* **filter.d/** → Contains regex filters Fail2ban uses to detect malicious log entries.
* **action.d/** → Defines what to do when an IP is banned (usually add an iptables rule).
* **paths-\*.conf** → OS-specific log file paths (so Fail2ban knows where to look).

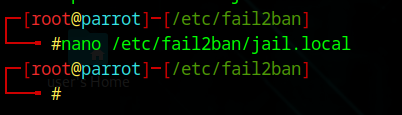
Never edit jail.conf directly. Instead:

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

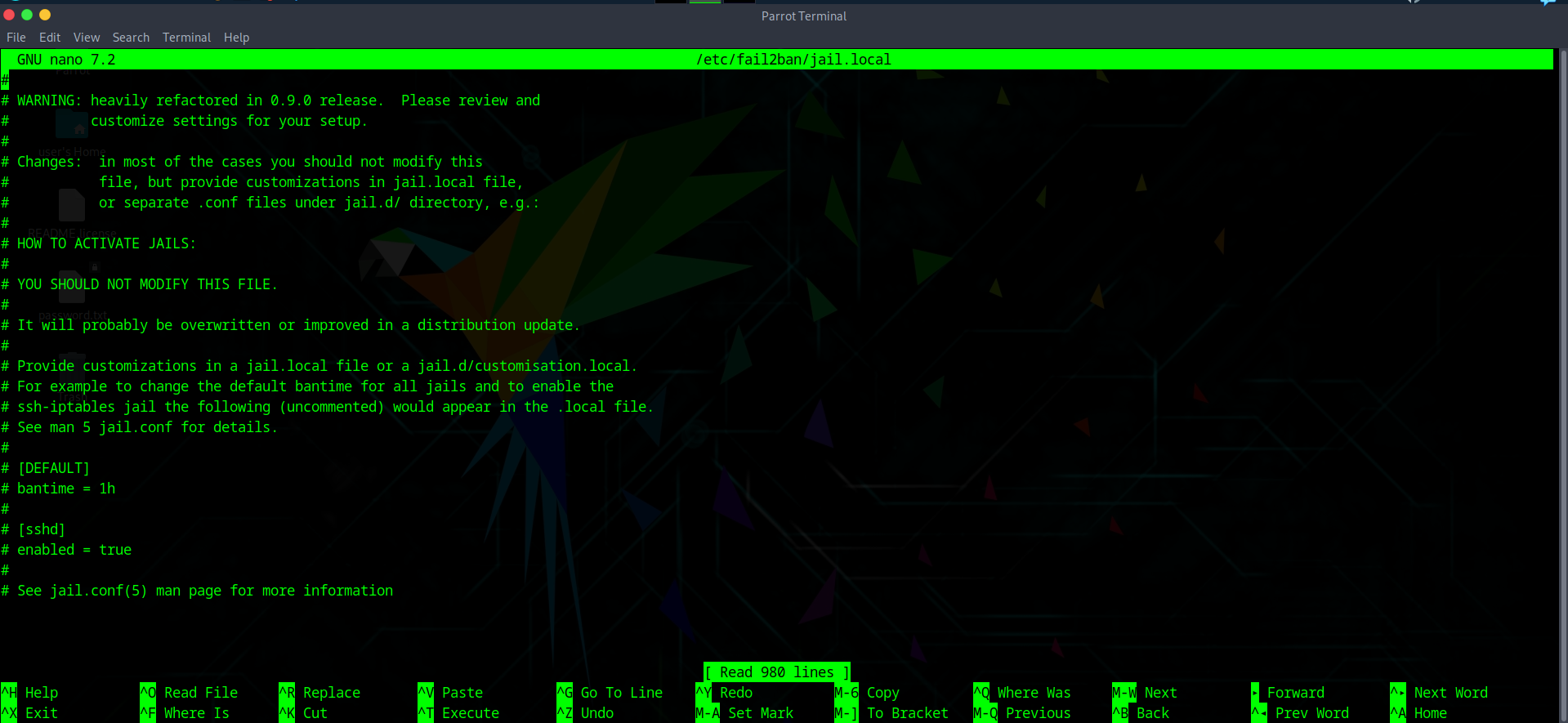


Use command to edit the jail.local file:

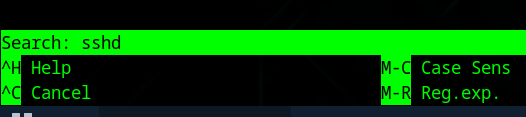
*nano /etc/fail2ban/jail.local*

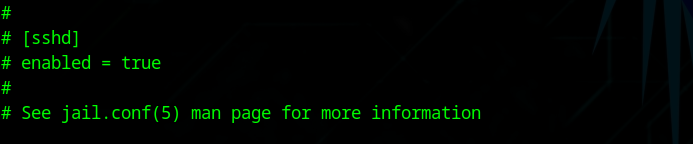


Following window will appear:

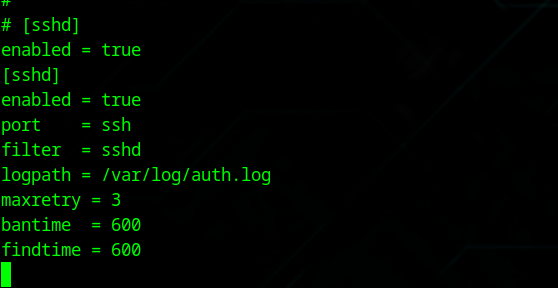


Look for the ‘sshd’ section:



Following section will appear: 

Edit that section like this:

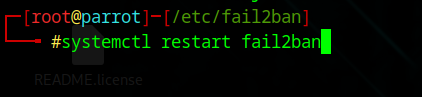


Meaning:

* **enabled** → turn on SSH jail
* **maxretry = 3** → after 3 failed attempts, ban
* **bantime = 600** → ban IP for 10 minutes
* **findtime = 600** → failed attempts counted within 10 min

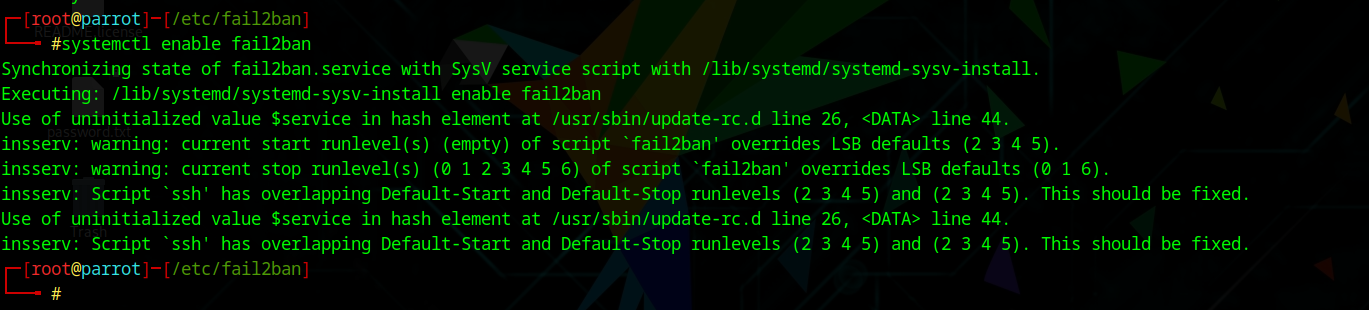
Save the changes, and then restart the fail2ban using the following command:

*sudo systemctl restart fail2ban*



Enable this on boot using the following command:

*sudo systemctl enable fail2ban*



Verify it’s working by checking status of SSH jail:

*fail2ban-client status sshd*



**What happens in background?**

Fail2ban works in the background by constantly monitoring log files, such as /var/log/auth.log for SSH, and looking for repeated failed login attempts using regex filters. When the number of failures exceeds the configured threshold within a set time window, Fail2ban automatically adds a temporary firewall rule (via iptables) to block the attacker’s IP, either dropping their traffic silently or rejecting it. The ban lasts for the specified duration, after which Fail2ban removes the rule, restoring normal access. This way, it dynamically protects services by combining log monitoring with automatic firewall updates, without affecting legitimate users.

--The End--