**Day 38**

**Exploitation Analyst**

**Control Remote Connections:**

**How can we control remote connections in Linux?**

You can control remote connections in Linux by:

1. **SSH configuration** (/etc/ssh/sshd\_config) – restrict users, change port, disable root login.
2. **Firewall rules** (ufw, iptables) – allow/block specific IPs or ports.
3. **TCP wrappers** (/etc/hosts.allow, /etc/hosts.deny).
4. **Fail2Ban** – block repeated failed login attempts.
5. **Disabling unnecessary services** (systemctl disable service).

**Why we need to control remote connections?**

We need to control remote connections to:

1. **Prevent unauthorized access** – stop attackers from logging in.
2. **Limit attack surface** – only allow trusted users/IPs.
3. **Protect sensitive data** – prevent data theft or modification.
4. **Mitigate brute-force attacks** – reduce risk of password guessing.
5. **Ensure system stability** – avoid unauthorized processes consuming resources.

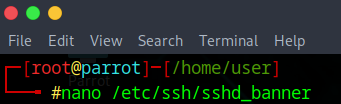
**Steps to Control Remote Connections by SSH banner:**

**Regarding SSH banners:**

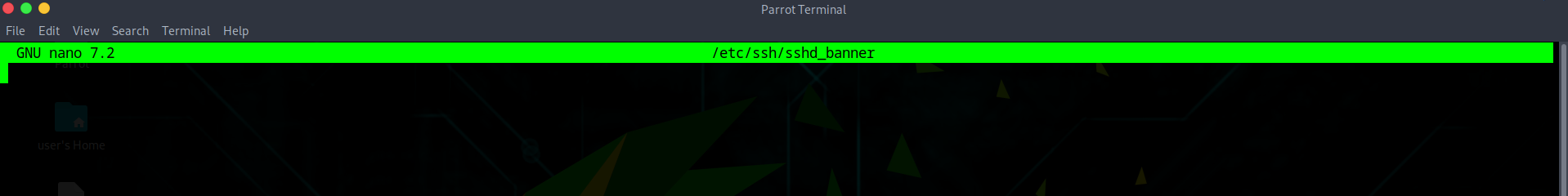
* Before login: Displayed before authentication. Used for legal warnings or notices. Configured in Banner /etc/ssh/sshd\_banner in /etc/ssh/sshd\_config.
* After login: Displayed after authentication, usually via /etc/motd or shell profile (~/.bash\_profile). Can show system info or messages.

Steps:

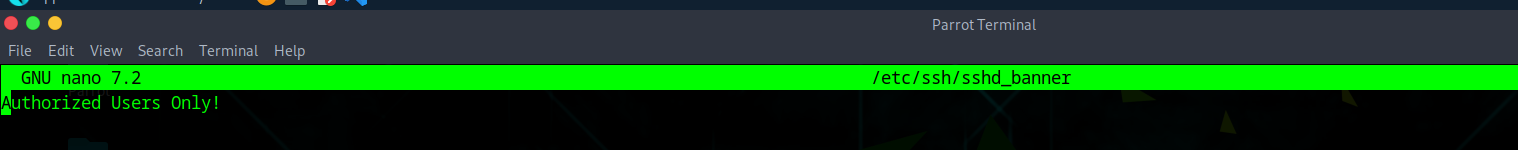
Open the /etc/ssh/sshd\_banner file using nano text editor:



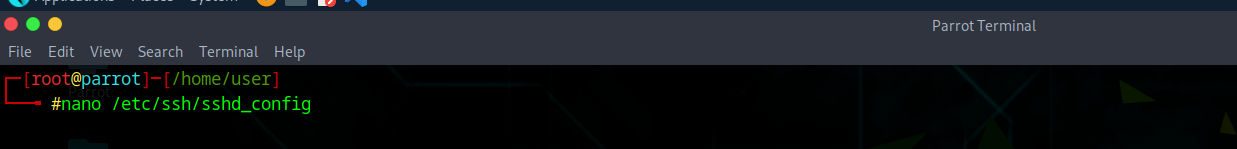
Following screen will appear:



Write your message:



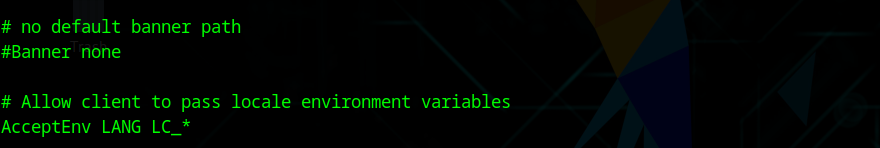
Now, open the SSH config from the file /etc/ssh/sshd\_config:



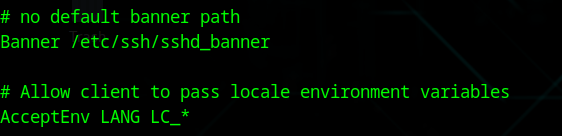
Following screen will appear:



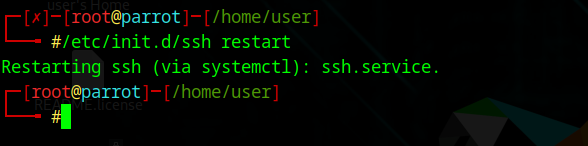
Press Ctrl + F and search for “banner”: following section should be found commented.



Edit it, remove that # symbol, and also add the path of /etc/ssh/sshd\_banner over there:



Save it, and then restart the SSH: using the command /etc/init.d/ssh restart



**You should see the banner before login.**

--The End--