**Day 40**

**Exploitation Analyst**

**Control Remote Connections:**

**Remove Root login from SSH:**

**Why disabling root SSH login is a good idea?**

* Root has full power – if compromised, attacker owns the system.
* Attackers always target root – brute-force bots try "root" username first.
* Audit trail – using normal users + sudo gives logs of *who* did what.

**What was earlier (if root login allowed)?**

* Anyone knowing the root password could directly SSH as root.
* No accountability (all actions just appear as root).
* Higher risk of brute-force attacks succeeding.

**What changes when we disable it?**

* Remote root login blocked.
* Users must log in as normal accounts and use sudo for admin tasks.
* Increases accountability + reduces direct attack surface.

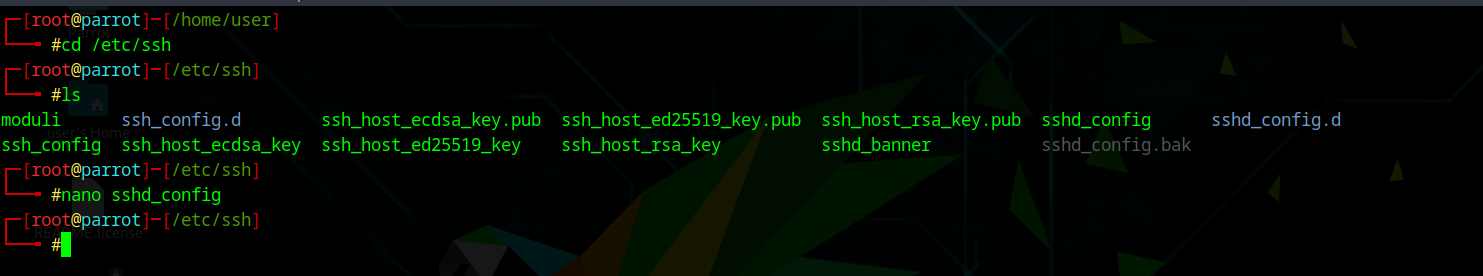
**What happens in the background?**

* sshd checks sshd\_config.
* When PermitRootLogin no, it rejects login attempts with username root before password/key check.
* Authentication only proceeds for non-root accounts.

**Steps to Remove Root login from SSH:**

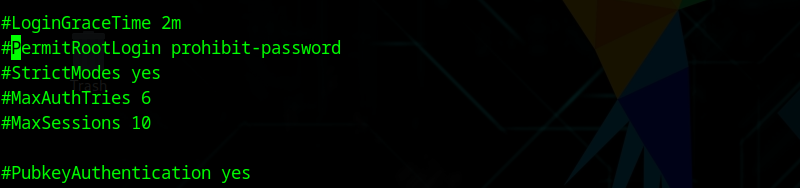
Steps:

First navigate to the /etc/ssh and open the sshd\_config by nano:



Following window will appear:



Press Ctrl + F and type “PermitRootLogin” to visit that section of the file:

Change it to like shown below:



* PermitRootLogin yes → allow root login.
* PermitRootLogin no → disable root login (recommended).
* PermitRootLogin prohibit-password → allow only key-based login for root.

Save it, and restart: systemctl restart ssh

