

# 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:

```
[root@parrot]~/home/user
#cd /etc/ssh
[root@parrot]~/etc/ssh
#ls
moduli      ssh_config.d      ssh_host_ecdsa_key.pub  ssh_host_ed25519_key.pub  ssh_host_rsa_key.pub  sshd_config  sshd_config.d
ssh_config  ssh_host_ecdsa_key  ssh_host_ed25519_key    ssh_host_rsa_key          sshd_banner           sshd_config.bak
[root@parrot]~/etc/ssh
#nano sshd_config
[root@parrot]~/etc/ssh
#
```

Following window will appear:



```
File Edit View Search Terminal Help
GNU nano 7.2 sshd_config

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

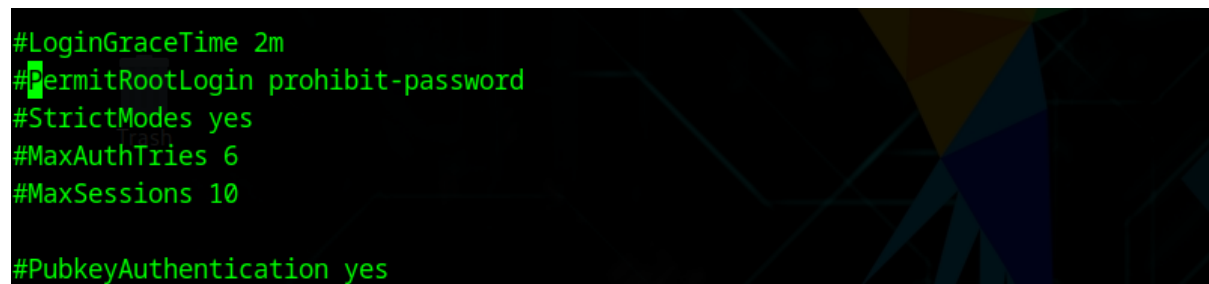
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

Help Read File Replace Paste Go To Line Redo Copy Where Was Next Forward Next Word
Exit Where Is Cut Execute Undo Set Mark To Bracket Previous Back Prev Word Home
Menu Parrot Terminal
```

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



```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

Change it to like shown below:



```
# Authentication:
password.txt
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

- 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`



```
File Edit View Search Terminal Help
[root@parrot]~# systemctl restart ssh
[root@parrot]~#
```