Module 6- Linux server - Manage basic networking & Security

1. Use ifconfig or ip to view and configure network interfaces.

ANS : **View interfaces**

ifconfig # show active interfaces

ifconfig -a # show all interfaces

ip addr show # show IP addresses

ip link show # show link-layer info

Assign IP address

with ifconfig

sudo ifconfig eth0 192.168.1.100 netmask 255.255.255.0

with ip

sudo ip addr add 192.168.1.100/24 dev eth0

Bring interface up/down

with ifconfig

sudo ifconfig eth0 up

sudo ifconfig eth0 down

with ip

sudo ip link set eth0 up

sudo ip link set eth0 down

Remove IP address

sudo ip addr del 192.168.1.100/24 dev eth0

2. Use ping to test network connectivity.

ANS :

ping 192.168.1.1 # ping router/local device

ping google.com # ping website

ping -c 4 google.com # send 4 packets only

ping 8.8.8.8 # ping Google DNS

3. Understand basic firewall configuration using FIREWALL-CMD.

ANS :

Check firewall status

sudo firewall-cmd --state

List active zones

sudo firewall-cmd --get-active-zones

List all rules in current zone

sudo firewall-cmd --list-all

Add a service (e.g., http) temporarily

sudo firewall-cmd --add-service=http

Add a service permanently

sudo firewall-cmd --add-service=http --permanent

sudo firewall-cmd --reload

Open a port temporarily (e.g., 8080/tcp)

sudo firewall-cmd --add-port=8080/tcp

Open a port permanently

sudo firewall-cmd --add-port=8080/tcp --permanent

sudo firewall-cmd --reload

Remove a service permanently

sudo firewall-cmd --remove-service=http --permanent

sudo firewall-cmd –reload

4. Add ssh services in firewall

ANS :

sudo firewall-cmd --add-service=ssh --permanent

sudo firewall-cmd –reload

5. Graphically manage the firewall

ANS :

Install firewall-config

sudo apt install firewall-config # Debian/Ubuntu

sudo dnf install firewall-config # CentOS/RHEL/Fedora

Open the graphical firewall manager

sudo firewall-config

6. What is selinux Security

ANS :

SELinux (Security-Enhanced Linux): A Linux security feature that **controls access to files, processes, and ports** to protect the system.

Modes:

- Enforcing → Blocks unauthorized access

- Permissive → Logs violations but does not block
- Disabled → Turns off SELinux

Example Commands:

Check status

sestatus

Set mode temporarily

sudo setenforce 1 # Enforcing

sudo setenforce 0 # Permissive

Set mode permanently

sudo nano /etc/selinux/config

Change: SELINUX=enforcing

7. How to Set Static IP in Linux?

AND :

Set static IP, gateway, and DNS for interface eth0

sudo nmcli con mod eth0 ipv4.addresses 192.168.1.100/24

sudo nmcli con mod eth0 ipv4.gateway 192.168.1.1

sudo nmcli con mod eth0 ipv4.dns "8.8.8.8 8.8.4.4"

sudo nmcli con mod eth0 ipv4.method manual

Bring the connection down and up to apply

sudo nmcli con down eth0

sudo nmcli con up eth0