Linux Server - Linux Basics And Networking

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

Ans:

View Interfaces:

- ip a (modern)
- ifconfig (legacy)

Bring Interface Up/Down:

- sudo ip link set <interface> up/down
- sudo ifconfig <interface> up/down

Configure IP Address:

- sudo ip addr add <IP>/<CIDR> dev <interface>
- sudo ifconfig <interface> <IP> netmask <netmask>

Set Default Gateway:

- sudo ip route add default via <gateway IP> dev <interface>
- sudo route add default gw <gateway IP> <interface>

50. Use ping to test network connectivity.

Ans:

1. **Open the command prompt (Windows) or terminal (Mac/Linux).**
    - **Windows:** Press the Windows key, type cmd, and press Enter.
    - **Mac:** Open Finder, go to Applications -> Utilities -> Terminal.

    - **Linux:** Open the terminal application (usually Ctrl+Alt+T).
2. **Type ping followed by a space and then the address you want to test.** This can be:
    - **A website address (like google.com):** This checks if you can reach the website's server.
    - **An IP address (like 192.168.1.1 - often your router):** This checks if you can reach a specific device on your network.
3. **Press Enter.**
4. **Look at the results:**
    - **"Reply from..." followed by an IP address and time:** This means the connection is working. The "time" indicates how fast the response was (lower is better).
    - **"Request timed out" or "Destination host unreachable":** This usually means there's a problem with the connection to the address you tried to ping. It could be that the device is off, the address is wrong, or there's a network issue in between.

Example:

To test if you can reach Google, you would type in the command prompt or terminal:

```
#Bash

#ping google.com
```

51. Understand basic firewall configuration using FIREWALL-CMD.

Ans:

- **Zones:** Think of them as security levels (e.g., public, private). Network interfaces are assigned to zones.

- **Status:** sudo firewall-cmd --state checks if the firewall is running.
- **Active Zones:** sudo firewall-cmd --get-active-zones shows which interfaces belong to which zones.
- **List Rules:** sudo firewall-cmd --list-all --zone=<zone> shows rules for a specific zone.
- **Allow Service:** sudo firewall-cmd --zone=<zone> --add-service=<service> --permanent && sudo firewall-cmd --reload allows predefined traffic (e.g., http, ssh).
- **Allow Port:** sudo firewall-cmd --zone=<zone> --add-port=<port>/<protocol> --permanent && sudo firewall-cmd --reload allows specific port/protocol (e.g., 8080/tcp).
- **Remove Rule:** Use --remove-service or --remove-port instead of --add-service or --add-port, followed by --permanent and --reload.
- **--permanent:** Makes rules last after reboot.
- **--reload:** Applies permanent rules to the running firewall.

52. Add ssh services in firewall Graphically manage the firewall.

Ans:

For firewall-config:

1. Open **firewall-config**.
2. Select your **active zone**.
3. Check the box next to **"ssh"** in the "Services" tab.
4. Go to **Options** -> **Runtime to Permanent** (or configure in the "Permanent" tab and reload).
5. Close **firewall-config**.

For GUFW:

1. Open **GUFW (Graphical Uncomplicated Firewall)**.
2. Enable **UFW (Uncomplicated Firewall)** if needed.

3. Click the **"+"** button.
4. Either:
   - Set **Direction** to "Allow", **Protocol** to "TCP", and **Port** to "22".
   - Go to the "Preconfigured" tab, select **"SSH"**, and click "Add".
5. Click **"Add"**.
6. Close **GUFW**.

53.What is selinux Security.

Ans:

SELinux (Security-Enhanced Linux) enhances Linux security beyond standard permissions (Discretionary Access Control - DAC) by implementing **Mandatory Access Control (MAC)**.

How it Works:

- **Security Contexts (Labels):** Every process and system resource gets a security label detailing its type, user, and role.
- **Policies:** Central rules define allowed interactions between these labels (e.g., a web server process can read web files but not system binaries).
- **Enforcement:** The kernel's SELinux module checks these labels against the policies for every access attempt. Access is **allowed only if a policy rule permits it**, regardless of file ownership or user permissions.

Key Benefits:

- **Increased Security:** Adds a strong layer of defense against exploits and privilege escalation.

- **Process Isolation:** Limits the damage if an application is compromised by confining its access.
- **Granular Control:** Allows very precise rules about what processes can do with specific resources.
- **Mitigates Misconfigurations:** Can prevent security holes caused by accidental errors.

54. How to Set Static IP in Linux?

Ans:

1. **Identify Interface:** Use ip a to find your network interface name (e.g., eth0, wlan0).
2. **Gather Info:** Obtain your desired static IP, subnet mask, gateway IP, and DNS server IPs.

Configuration Methods (Choose One):

- **NetworkManager (GUI/nmcli):** Use the graphical network settings or the nmcli command-line tool to modify the connection's IPv4 settings to "Manual" and enter your static IP details. Apply changes by reconnecting or using nmcli con down/up.
- **Configuration Files (Distribution-Specific):**
  - **Debian/Ubuntu (netplan):** Edit YAML files in /etc/netplan/ with static IP details and apply with sudo netplan apply.
  - **Debian/Ubuntu (/etc/network/interfaces):** Modify the interface to static and define address, netmask, gateway, and dns-nameservers. Restart networking service.
  - **CentOS/RHEL/Fedora:** Edit connection files in /etc/NetworkManager/system-connections/ setting

method=manual under [ipv4] and providing IP details. Restart NetworkManager.

3. **Verify:** Use ip a to confirm the new IP and test connectivity with ping.

Explanation of Terms:

- **Static IP:** A permanent, manually assigned IP address for your device.
- **DHCP:** Dynamic Host Configuration Protocol, automatically assigns IP addresses.
- **Network Interface:** The software interface representing your physical network connection.
- **IP Address:** A unique numerical identifier for your device on the network.
- **Subnet Mask:** Defines the network portion of the IP address.
- **Gateway:** The router's IP address, allowing communication outside your local network.
- **DNS Servers:** Translate domain names (like https://www.google.com/search?q=google.com) into IP addresses.