**Module 6- Linux server - Manage basic networking & Security**

**49. Use ifconfig or ip to View and Configure Network Interfaces**

Using ifconfig:

The ifconfig command is used to configure and display network interface parameters for a network using TCP/IP. Although it is deprecated in favor of the ip command, it is still widely used.

View Network Interfaces:

ifconfig

This command displays all active network interfaces and their details, such as IP address, netmask, and broadcast address.

Configure Network Interface:

sudo ifconfig eth0 192.168.1.100 netmask 255.255.255.0

This command assigns the IP address 192.168.1.100 and netmask 255.255.255.0 to the eth0 interface.

Using ip:

The ip command is a more powerful and versatile tool for network configuration.

View Network Interfaces:

ip addr show

This command displays all network interfaces and their details.

Configure Network Interface:

sudo ip addr add 192.168.1.100/24 dev eth0

This command assigns the IP address 192.168.1.100 with a subnet mask of 255.255.255.0 to the eth0 interface.

Bring Interface Up/Down:

sudo ip link set eth0 up

sudo ip link set eth0 down

These commands bring the eth0 interface up or down, respectively12.

**50. Use ping to Test Network Connectivity**

The ping command is used to test the reachability of a host on an IP network and measure the round-trip time for messages sent from the originating host to a destination computer.

Basic Ping Command:

ping google.com

This command sends ICMP ECHO\_REQUEST packets to google.com and waits for ECHO\_REPLY packets. It helps determine if the host is reachable and measures the time taken for the round trip.

Ping a Specific IP Address:

ping 192.168.1.1

This command pings the device with the IP address 192.168.1.1.

Specify Number of Packets:

ping -c 4 google.com

This command sends exactly 4 packets to google.com and then stops34.

**51. Understand Basic Firewall Configuration Using firewall-cmd**

firewall-cmd is a command-line tool for managing firewalld, a dynamic firewall daemon.

Check Firewall Status:

sudo firewall-cmd --state

This command checks if firewalld is running.

View Active Zones:

sudo firewall-cmd --get-active-zones

This command lists all active zones and their associated interfaces.

Add a Service to a Zone:

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

This command allows HTTP traffic in the public zone permanently.

Reload Firewall:

sudo firewall-cmd --reload

This command reloads the firewall rules to apply any changes made56.

**52. Add SSH Services in Firewall**

To allow SSH traffic through the firewall, you need to add the SSH service to the appropriate zone.

Add SSH Service:

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

This command allows SSH traffic in the public zone permanently.

Reload Firewall:

sudo firewall-cmd –reload

**53. Graphically Manage the Firewall (sorry but I copied from chatGPT 😢😢)**

To manage the firewall graphically on Linux, you can use tools like GUFW (Graphical Uncomplicated Firewall). GUFW is a graphical front-end for UFW (Uncomplicated Firewall), which is a user-friendly interface for managing firewall rules.

Install GUFW:

sudo apt install gufw

Launch GUFW:

You can find it in your applications menu or start it from the terminal by typing gufw.

Enable/Disable Firewall:

Use the status toggle to enable or disable the firewall.

Add Rules:

You can add rules to allow or deny specific traffic by clicking on the “Rules” tab and configuring the desired settings1.

**54.**

**55. What is SELinux Security?**

Security-Enhanced Linux (SELinux) is a security architecture integrated into the Linux kernel that provides a mechanism for supporting access control security policies, including mandatory access controls (MAC). It was originally developed by the NSA and is now maintained by the open-source community.

How SELinux Works:

SELinux uses security policies to define what actions are allowed or denied for different processes and users.

It labels all files, processes, and ports with a security context.

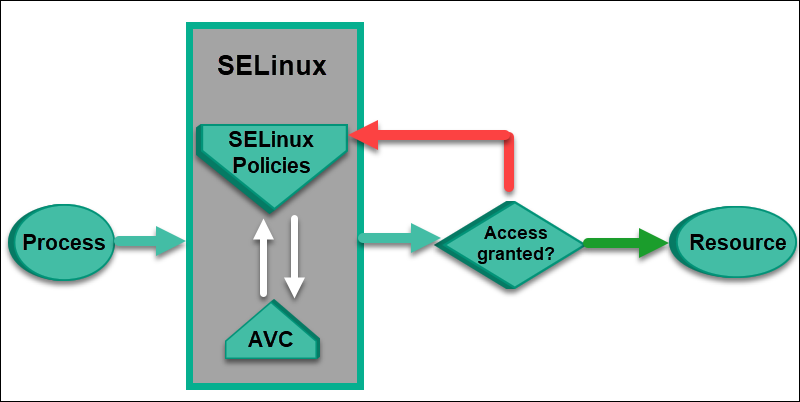
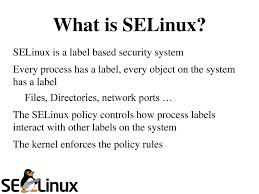
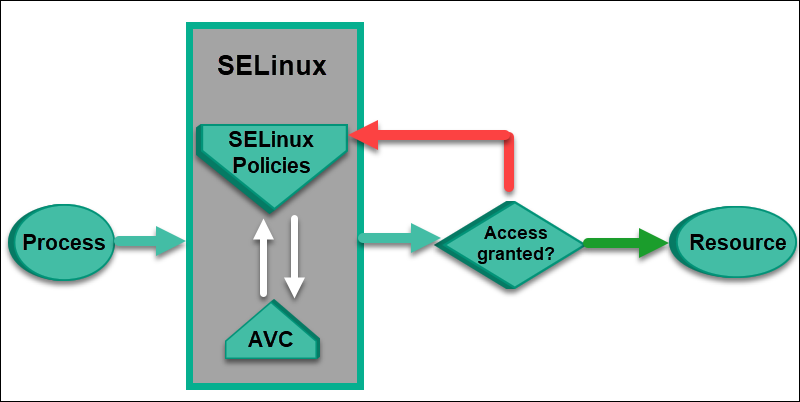
When a process attempts to access a resource, SELinux checks the policy to determine if the action is permitted23.

Modes of Operation:

Enforcing: SELinux policy is enforced, and access is denied based on the policy.

Permissive: SELinux policy is not enforced, but violations are logged.

Disabled: SELinux is turned off.



**56. How to Set Static IP in Linux?**

Setting a static IP address in Linux can be done using different methods depending on the distribution. Here’s a general approach using Netplan, which is common in Ubuntu and other Debian-based distributions:

Locate Netplan Configuration File:

cd /etc/netplan/

Edit Configuration File:

Open the configuration file (e.g., 01-netcfg.yaml) with a text editor:

sudo nano 01-netcfg.yaml

Modify the File:

Add or modify the following lines to set a static IP:

network:

version: 2

ethernets:

eth0:

dhcp4: no

addresses:

- 192.168.1.100/24

gateway4: 192.168.1.1

nameservers:

addresses:

- 8.8.8.8

- 8.8.4.4

Apply the Configuration:

sudo netplan apply

Verify the Configuration:

ip a