50. Use ifconfig or ip to view and configure network interfaces
ifconfig (older command):

To view network interfaces:
bash
Copy code
ifconfig
To configure an IP address:
bash
Copy code
sudo ifconfig eth0 192.168.1.100 netmask 255.255.255.0 up
To disable an interface:
bash
Copy code
sudo ifconfig eth0 down
ip (modern and recommended command):

To view network interfaces:
bash
Copy code
ip a
To configure an IP address:
bash
Copy code
sudo ip addr add 192.168.1.100/24 dev eth0
To bring an interface up:
bash
Copy code
sudo ip link set eth0 up
To bring an interface down:
bash
Copy code
sudo ip link set eth0 down
51. Use ping to test network connectivity
The ping command is used to check the connectivity between your computer and another device.
Basic usage:
bash
Copy code
ping 192.168.1.1
To stop the ping after a certain number of packets:
bash
Copy code
ping -c 4 192.168.1.1
To continuously ping:
bash
Copy code
ping 192.168.1.1

52. Understand basic firewall configuration using firewall-cmd
The firewall-cmd command is part of firewalld (the default firewall management tool in many Linux distributions such as RHEL and CentOS).
To check the status of the firewall:
bash
Copy code
sudo firewall-cmd --state
To list active zones:
bash
Copy code
sudo firewall-cmd --get-active-zones
To allow a specific port (e.g., port 80):
bash
Copy code
sudo firewall-cmd --zone=public --add-port=80/tcp --permanent
To reload the firewall after changes:
bash
Copy code
sudo firewall-cmd --reload
53. Add SSH services in firewall
To allow SSH service (port 22) in the firewall:
bash
Copy code
sudo firewall-cmd --zone=public --add-service=ssh --permanent
To reload the firewall:
bash
Copy code
sudo firewall-cmd --reload
54. Graphically manage the firewall
You can use Firewall-config, a graphical interface for firewalld.
To install:
bash
Copy code
sudo yum install firewall-config   # RHEL/CentOS
sudo apt-get install firewall-config # Ubuntu/Debian
Once installed, you can launch it from the terminal:
bash
Copy code
firewall-config
55. What is SELinux Security?
SELinux (Security-Enhanced Linux) is a set of kernel-level security enhancements that provides a mechanism for enforcing security policies. It works by controlling access to resources based on predefined security rules.
SELinux operates in three modes:
Enforcing: SELinux policies are enforced.
Permissive: SELinux allows actions but logs them.
Disabled: SELinux is turned off.
To check SELinux status:
bash
Copy code

getenforce
To set SELinux to permissive mode:
bash
Copy code
sudo setenforce 0
To permanently disable SELinux (in /etc/selinux/config):
bash
Copy code
SELINUX=disabled
56. How to Set Static IP in Linux?
To set a static IP on Linux, you'll modify the network configuration file or use a command-line tool, depending on your system.

Using NetworkManager (nmcli):

bash
Copy code
sudo nmcli con mod "System eth0" ipv4.addresses 192.168.1.100/24 ipv4.gateway 192.168.1.1 ipv4.dns "8.8.8.8"
sudo nmcli con mod "System eth0" ipv4.method manual
sudo nmcli con up "System eth0"
Manually editing the network configuration file (/etc/sysconfig/network-scripts/ifcfg-eth0 for RHEL/CentOS, /etc/network/interfaces for Debian/Ubuntu):

RHEL/CentOS: Edit the file /etc/sysconfig/network-scripts/ifcfg-eth0:

bash
Copy code
TYPE=Ethernet
BOOTPROTO=static
IPADDR=192.168.1.100
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
DNS1=8.8.8.8
ONBOOT=yes
Then restart the network service:

bash
Copy code
sudo systemctl restart network
Debian/Ubuntu: Edit the file /etc/network/interfaces:

bash
Copy code
auto eth0
iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
gateway 192.168.1.1

dns-nameservers 8.8.8.8
Then restart networking:

bash
Copy code
sudo systemctl restart networking