*Module :20 Linux server - Manage basic networking & Security*

*Assignment Level Basic*

1. *Full form of “ping “*

*Ans. Packet InterNet Groper*

1. *What is the use of “ping “command?*

*Ans. Ping is a simple computer network software utility used to test and verify the reachability of a host on an Internet Protocol (IP) network. It works by sending packets from the source to the target host which if it is accessible through the network, then sends packets back.*

1. *What is the meaning of “prefix” is?*

*Ans. A prefix is the path on your host computer a software package is installed under. Packages that have a prefix will place all parts under the prefix path. Packages for your host computer typically use a default prefix of /usr/local on FreeBSD and Linux. You have to select a prefix for your installation.*

1. *Which protocol is used in PING?*

*Ans. The "ping" utility primarily uses the Internet Control Message Protocol (ICMP) to perform its network diagnostic functions. ICMP is a network protocol that is part of the Internet Protocol Suite (TCP/IP). It is used to send error messages, operational information, and diagnostic messages between network devices.*

1. *Port number of ICMP?*

*Ans. ICMP has no concept of ports, as TCP and UDP do, but instead uses types and codes. Commonly used ICMP types are echo request and echo reply (used for ping) and time to live exceeded in transit (used for traceroute).*

1. *What is network ID and broadcast ID in IP range?*

*Ans. In IP addressing, an IP range typically consists of a range of IP addresses that fall within a specified network segment. Within this IP range, you can define two important addresses: the Network ID and the Broadcast ID.*

* ***Network ID****: The Network ID (also known as the Network Address) is the first IP address in an IP range that represents the network itself. It identifies the network segment to which the IP addresses belong. All hosts within the same network share the same network ID. This address is used for routing purposes to determine whether a packet should be sent within the local network or forwarded to another network. It has all host bits set to 0 in the subnet mask.*
* ***Broadcast ID****: The Broadcast ID (also known as the Broadcast Address) is the last IP address in an IP range that is used for broadcasting messages to all hosts within the network segment. When a packet is addressed to the broadcast address, it is received by all hosts on the network. The broadcast address has all host bits set to 1 in the subnet mask.*

*For example, if you have an IP range of 192.168.1.0 to 192.168.1.255 with a subnet mask of 255.255.255.0, the Network ID would be 192.168.1.0 (where all host bits are 0) and the Broadcast ID would be 192.168.1.255 (where all host bits are 1).*

*It's important to note that the concept of broadcast addresses is less commonly used in modern networking due to the prevalence of subnetting and more efficient methods of communication. Additionally, with the adoption of IPv6, broadcast communication has been largely replaced by multicast and anycast communication mechanisms.*

1. *What is gateway?*

*Ans. A gateway is a network node used in telecommunications that connects two networks with different transmission protocols together. Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.*

1. *What is SeLinux?*

*Ans. SELinux stands for Security Enhanced Linux, which is an access control system that is built into the Linux kernel. It is used to enforce the resource policies that define what level of access users, programs, and services have on a system.*

1. *Wright down the list of SELINUX modes and their uses*

*Ans. SELinux (Security-Enhanced Linux) offers several modes of operation that determine how it enforces access controls and policies on a system. Each mode serves different purposes and provides varying levels of security. The common SELinux modes are:*

* ***Enforcing Mode****: In this mode, SELinux actively enforces the access control policies defined in its security policies. It denies any actions that violate these policies and generates audit logs for analysis. Enforcing mode provides strong security by preventing unauthorized actions and access.*
* ***Permissive Mode****: Permissive mode also enforces access control policies, but it doesn't deny any actions. Instead, it generates audit logs for actions that would have been denied in enforcing mode. This mode is useful for testing and troubleshooting because it allows you to see how SELinux policies would affect system behavior without blocking any actions.*
* ***Disabled Mode****: In disabled mode, SELinux is effectively turned off, and no access control policies are enforced. This mode might be used if you encounter compatibility issues or need to troubleshoot SELinux-related problems. However, it significantly reduces the security benefits SELinux provides.*

*These modes are set at the kernel level and can be configured during system boot or runtime. System administrators can choose the appropriate mode based on their security requirements and the specific needs of their environment.*

*It's important to note that while SELinux can enhance system security, it also requires proper configuration and management. Enabling SELinux in enforcing mode without understanding its policies and behaviors can lead to unexpected issues. Therefore, administrators should be familiar with SELinux concepts and consider their organization's security needs when configuring SELinux modes.*

1. *In which mode is reboot required after modification?*

*Ans. In the context of SELinux modes, changing between "Enforcing Mode" and "Permissive Mode" usually requires a reboot for the changes to take full effect. This is because SELinux mode changes involve modifications to the kernel's security policy, and a reboot ensures that the new policy is applied consistently throughout the system.*

*When transitioning from "Enforcing Mode" to "Permissive Mode," or vice versa, it's recommended to reboot the system to ensure that SELinux operates as intended with the chosen mode.*

*However, it's important to consult your specific Linux distribution's documentation, as some distributions may provide tools or procedures that allow you to change SELinux modes without a reboot or with minimal disruption. Always consider the impact on your system and any services running before making changes to SELinux modes.*

1. *What is SeLinux Booleans*

*Ans. SELinux Booleans are a feature within SELinux (Security-Enhanced Linux) that allows system administrators to fine-tune and customize the security policies applied to the system. Booleans are binary values (either "on" or "off") that represent specific security settings or permissions for various system behaviors. By toggling these Booleans, administrators can modify the behavior of SELinux policies without needing to write or modify complex policy rules.*

1. *Which command is used to check the selinux contents*

*Ans. To check the SELinux context and security-related information for files, you can use the ls command with the -Z option. This option displays the SELinux context associated with each file or directory. Here's the command: ls -Z <filename>*

1. *What is a firewall? why we use*

*Ans. A firewall is a security system designed to prevent unauthorized access into or out of a computer network. Firewalls are often used to make sure internet users without access are not able to interface with private networks, or intranets, connected to the internet.*

1. *What is a firewall?*

*Ans. A firewall is a network security device that monitors traffic to or from your network*

1. *Which command is used for graphically managing firewall?*

*Ans. The command used for graphically managing the firewall on many Linux distributions is often specific to the desktop environment being used. Here are some examples of commands that can be used to launch graphical firewall management tools on popular desktop environments:*

* ***GNOME (Gnome Control Center):*** *gnome-control-center firewall*
* ***KDE (System Settings******):*** *systemsettings5*
* ***XFCE (GUI Firewall Management******):*** *sudo gufw*
* ***Cinnamon (Firewall Configuration******):*** *firewall-config*
* ***Unity (Firewall Configuration******):*** *firewall-config*
* ***Mate (Firewall Configuration******):*** *firewall-config*

1. *Which command is used for command line manage firewall?*

*Ans. The command-line tool commonly used to manage the firewall in Linux systems is iptables. However, keep in mind that iptables is a powerful but relatively complex utility that provides a way to configure and manage packet filtering and network address translation rules in the Linux kernel's netfilter framework.*

1. *What is the use of “–get-default-zone “?*

*Ans. The --get-default-zone option is used with the firewall-cmd command, which is a command-line utility for managing firewalld, a dynamic firewall management tool in Linux. Firewalld provides a way to manage and configure network firewall rules and settings on Linux systems.*

*When you use the --get-default-zone option with the firewall-cmd command, it displays the currently set default zone for firewalld. In firewalld, zones are predefined sets of rules and configurations that define the level of trust and security for different network interfaces or connections.*

*Assignment Level Intermediate to Advance*

1. *Which command is used to manage IP addressing in Linux 7.0?*

*Ans. In Linux 7.0 and later versions, the ip command is commonly used to manage IP addressing and network configurations. The ip command is a powerful and versatile tool for configuring network interfaces, routes, and various networking parameters. It replaces the older ifconfig and route commands and offers more advanced features and flexibility.*

1. *By default, which name will be assigned to network card in RHEL?*

*And. Linux network interfaces used the naming convention eth [0123…]. However, in RHEL7/CentOS7, the default network interface name is based on firmware, topology, and location information.*

1. *Which command is used to add/create a new network connection?*

*Ans. In Red Hat Enterprise Linux (RHEL) and many other Linux distributions, you can use the nmcli command to manage network connections, including adding and creating new network connections. nmcli stands for Network Manager Command-Line Interface and provides a powerful way to interact with Network Manager, which is the default network management service on many Linux systems.*

1. *From which command is used to show the network connection?*

*Ans. nmcli connection show command is to show the network connection.*

Task: 1

1. *Open graphically IP management*

*Ans. Done in lab.*

1. *Check current lan connection*

*Ans. Done in lab.*

1. *Add new connection name “KAMAL”*

*Ans. Done in lab.*

1. *Connect “eth0” to this new connection “KAMAL”*

*Ans. Done in lab.*

1. *Up the new connection “KAMAL”*

*Ans. Done in lab.*

1. *Show the info about the new connection*

*Ans. Done in lab.*

1. *Assign and append new IP on new connection “KAMAL”*

*Ans. Done in lab.*

1. *Reload the connections*

*Ans. Done in lab.*

1. *Again, create new connection with same name “KAMAL”*

*Ans. Done in lab.*

1. *Delete both new connections one by one.*

*Ans. Done in lab.*

1. *Assign new hostname*

*Ans. Done in lab.*

1. *Restart the Network Manager*

*Ans. Done in lab.*

Task :2

1. *Check current selinux mode*

Ans. Done in lab.

1. *Change selinux mode into “permissive”*

Ans. Done in lab.

1. *Change selinux mode into “Enforcing”*

Ans. Done in lab.

1. *Start server machine.*

Ans. Done in lab.

1. *Change the default selinux mode to permissive via VIM*

Ans. Done in lab.

1. *Check selinux contents on process*

Ans. Done in lab.

1. *Install httpd.services*

Ans.

1. *Check selinux contents on /var/www/html*

Ans.

1. *Create new .html file in /var/www/html*

Ans.

1. *Open this file in Firefox and check is accessible or not*

Ans.

1. *Delete this .html file*

Ans.

1. *Create new .html file on desktop*

Ans.

1. *Move this file in /var/www/html*

Ans.

1. *Now, open this file and check is accessible or not*

Ans.

1. *Update selinux contents on this file*

Ans.

1. *See the status of all booleans*

Ans.

1. *“ON” the booleans of httpd\_use\_nfs*

Ans.

1. *Get a list of only modified Boolean*

Ans.

1. *Get details of all selinux logs*

*Ans.*

Task:3

1. *Show current default zone?*

*Ans.*

1. *Show all firewall zone*

Ans.

1. *Get list of services which is running in current zone*

Ans.

1. *Show all profile of all zones*

Ans.

1. *Remove ssh services*

Ans.

1. *Reload the firewall*

Ans.

1. *Add ssh services in firewall*

Ans.

1. *Graphicallymanagethefirewall*

*Ans.*