Quiz 4

kiranraj jonnalagadda

1. List the possible ways to check if your system is listening on port 56

answer: to check certain port is listening in our system we can use

netstat -an | grep “56”

2. Which command is used to run a service automatically after boot.

Answer:

upstart

3. Explain 3 way handshake?

Answer: The 3 way handshake takes place between client and server using tcp-ip protocol-type

first client sends a syn packet to server then client will send a syn and a fin bit to the client and then connection is established and then the client sends the syn packet this way of connection with tcp-ip in client and server is known as 3 way handshake.

4. Write a command to configure your script to run only when system boots into GUI and not to any other runlevel.

Answer:

5. Explain briefly about LD\_LIBRARY\_PATH

answer:LD\_LIBRARY\_PATH is an enviornment variable listing extra paths that the linux load-time linker should use when locating these libraries.its simply a colon-separated list of the form.

6. What are the differences between TCP and UDP packets and how do these differences

relate to differences in the two protocols?

Answer:

Tcp: tcp is a connection oriented protocol.

The packets in tcp ip protocol arrives in sequential order.

In a stream if any packet missing then it will resend the request and combine together.

They read packets one after the other .here one packet ends and begins another.

Udp: tcp is a connectionless protocol.

The packets in udp protocol are not orderd or sequential.

As it is connectionless no tracking is available about the connection. And stream is not in flow.

They read one packet per one read call.

7. Explain how the ping command works, in terms of what protocol and message types

are used and how.

Answer:

ping command is used to check whether a given ip or server is sending request back or responding. This helps to check the ip statistics.

Eg ping google.com.

Uses icmp protocol.and uses echo to print the messages.

8. Give a command which enables www and ssh access your firewall.

9. Give a command to remove all rules from an iptable.

Iptables -F

10. Briefly describe iptables. Write rules for the following:

a. Allow incoming SSH only from a specific network.

b. Allow incoming http and https

c. block a specific ip addresses.

Answer:

a:iptables [-a] chain ssh

b:iptables [-a] chain [http,https]

c: iptables [drop]chain