Quiz 4

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

answer: possible way to check is by using “netstat” command. So for example to check port 80 on TCP, you can do this: netstat -np TCP | find "56" which will give the datails about system listening to port 56 or not.

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

Answer: upstart

3. Explain 3 way handshake?

Answer: A three-way-handshake is a method used in a TCP/IP network to create a connection between a local host/client and server. It is a three-step method that requires both the client and server to exchange SYN and ACK packets before actual data communication begins.

A client node sends a SYN data packet over an IP network to a server on the same or an external network. The target will open ports that can accept and initiate new connections. When the server receives the SYN packet from the client node, it responds and returns a confirmation receipt - the ACK packet or SYN/ACK packet. The client node receives the SYN/ACK from the server and responds with an ACK packet.

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

5. Explain briefly about LD\_LIBRARY\_PATH

answer: LD\_LIBRARY\_PATH is the predefined environmental variable in Linux/Unix which sets the path which the linker should look in to while linking dynamic libraries/shared libraries.

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

relate to differences in the two protocols?

Answer: tcp

1.Reliability: TCP is connection-oriented protocol. When a file or message send it will get delivered unless connections fails. If connection lost, the server will request the lost part. There is no corruption while transferring a message.

2.Ordered: If you send two messages along a connection, one after the other, you know the first message will get there first. You don't have to worry about data arriving in the wrong order.

3.Heavyweight: - when the low level parts of the TCP "stream" arrive in the wrong order, resend requests have to be sent, and all the out of sequence parts have to be put back together, so requires a bit of work to piece together.

Udp:

1.Reliability: UDP is connectionless protocol. When you a send a data or message, you don't know if it'll get there, it could get lost on the way. There may be corruption while transferring a message.

2.Ordered: If you send two messages out, you don't know what order they'll arrive.

3.Lightweight: No ordering of messages, no tracking connections, etc. It's just fire and forget! This means it's a lot quicker, and the network card / OS have to do very little work to translate the data back from the packets.

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

are used and how.

Answer: Ping is used diagnostically to ensure that a host computer the user is trying to reach is actually operating. Ping works by sending an Internet Control Message Protocol Echo Request to a specified interface on the network and waiting for a reply.

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

Answer: ssh - sudo uwf enable

www - netsh firewall set opmode enable

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

Answer: iptables -F

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

a. Allow incoming SSH only from a specific network.

Answer: Using this iptables rule we will block all incoming connections to specific port with specific IP address.

iptables -A INPUT -p tcp -s 77.66.55.44 --dport ssh -j ACCEPT

iptables \_A INPUT -p tcp –dport ssh -j REJECT

b. Allow incoming http and https

answer: The following rules allows all incoming SSH, HTTP and HTTPS traffic.

iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state ESTABLISHED -j ACCEPT

c. block a specific ip addresses.

Answer:to block a specific ip we can use rule as - iptables -A INPUT -s IP-ADDRESS -j DROP