Quiz 4\_Ashish Raymonds

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

Ans : -> lsof -i :56

->lsof -i :56 | grep LISTEN

->$ sudo netstat -plnt | grep ':56'

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

Ans : **Upstart**

3. Explain 3 way handshake?

Ans:

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 (acknowledgment) packets before actual data communication begins.

A three-way-handshake is also known as a TCP handshake.

A three-way-handshake is primarily used to create a TCP socket connection. It works when:

A client node sends a SYN data packet over an IP network to a server on the same or an external network.

The objective of this packet is to ask/infer if the server is open for new connection.

The target server must have 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.

Ans : By Using chkconfig script on.

5. Explain briefly about LD\_LIBRARY\_PATH

Ans:

LD\_LIBRARY\_PATH is an environment variable. It is used for debugging a new library or a non standard library. It is also used for which directories to search. Path to search for directories needs to given. The variable can be set by using setenv—LD\_LIBRARY\_PATH--$PATH

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

relate to differences in the two protocols?

Ans: TCP is a connection oriented stream over an IP network. It guarantees that all sent packets will reach the destination in the correct order.

This imply the use of acknowledgement packets sent back to the sender, and automatic retransmission,

causing additional delays and a general less efficient transmission than UDP.

UDP a is connection-less protocol. Communication is datagram oriented.

The integrity is guaranteed only on the single datagram. Datagrams reach destination and can arrive out of order or don't arrive at all.

It is more efficient than TCP because it uses non ACK.

It's generally used for real time communication, where a little percentage of packet loss rate is preferable to the overhead of a TCP connection.

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

are used and how.

Ans:

Ping (Program on the application layer)

Opens a 'raw' socket to IP Layer

IP layer (Layer 2 on OSI) packages ICMP packet and sends it

Since there is no TCP layer in between, the Ping (program) has to monitor all the incoming ICMP packets and filter only the one's from the destination.

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

Ans:

netstat -a |grep ssh

start ssh

/etc/init.d/sshd start | stop | restart

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

Ans :

iptables --flush

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.

Ans:

**iptables** is a user-space application program that allows a system administrator to configure the tables provided by the **Linux** kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores.

a) iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

b) iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT

c) BLOCK\_THIS\_IP="x.x.x.x"

iptables -A INPUT -s "$BLOCK\_THIS\_IP" -j DROP