Quiz 5

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

A. nmaplocalhost | grep 56

netstat -ntlp | grep 56

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

A. chkconfig

3. Explain 3 way handshake?

A. SYN - system 1 sends SYN signal to rmote system

SYN-ACK - remote sysstem receives the syn signal and sends ack signal

ACK - system again receives ack signal from remote system and connection is established

For Example: When you ping to a machine you are sending a SYN signal which is ACK by the remote machine then it sends a SYN ACK signal back to the host machine. Then the host machine receives SYN ACK and sends the ACK signal back to confirm the same.

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

A. chkconfig ‚Äìlevel 5 servicename on

chkconfig ‚Äìlevel 1234 servicename off

5. Explain briefly about LD\_LIBRARY\_PATH

A. LD\_LIBRARY\_PATH is used to specify directories of libraries.

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

relate to differences in the two protocols?

A. Primary differences are that TCP packets include flags and sequence numbers, due to the fact that TCP connections have state (can be in various states), and are reliable in terms of making sure all transmitted data is received and is kept in the original order

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

are used and how.

A. ping uses the ICMP protocol. It sends an ICMP ECHO\_REQUEST packet to a machine to elicit an ICMP ECHO\_RESPONSE response packet

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

A. iptables -A INPUT -p tcp -i eth0 --dport 22 --sport 1024:65535 \

-m state --state NEW -j ACCEPT

iptables -A INPUT -p tcp -i eth0 --dport 80 --sport 1024:65535 \

-m state --state NEW -j ACCEPT

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

A. 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.