Quiz 4

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

Ans: netstat -a –n will show all of the network connections open and the listening ports on your machine. 0.0.0.0:56

nmaplocalhost | grep 56

netstat -ntlp | grep 56

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

Ans: to start a servive : [<ServerName>] start <ServiceName> [<ServiceArguments>]

To run automatically: upstart

This question is for redhat linux – chkconfig

Please go through this link for reference.

<http://www.thegeekstuff.com/2011/06/chkconfig-examples/>

and also refer the material.

3. Explain 3 way handshake?

Ans: Mainly Three way handshake involves there steps:

1. First the client sends a SYN message to server.
2. Then server receive SYN and send SYN and ACK reply message to client .
3. Then client receive this SYN+ACK and send ACK to server to establish connection.

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

Ans: GRUB\_CMDLINE\_LINUX\_DEFAULT="text"

chkconfig ‚Äìlevel 5 servicename on

chkconfig ‚Äìlevel 1234 servicename off

<http://www.thegeekstuff.com/2011/06/chkconfig-examples/>

5.Explain briefly about LD\_LIBRARY\_PATH

Ans: 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?

Ans:UDP:\* No end to end Connection between to machines

\*The data received at the receiver end is not in stream as in TCP but as a complete block of data.

\* UDP is an unconnected datagram protocol

Tcp: \* End to end Connection is maintained between to machines.

\* The data received at the receiver end is a stream in TCP

\* TCP is a reliable, connected stream protocol.

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

are used and how.

Ans: The PING command is used to test the connection and latency between two network connections. These connections can be either in a local area network or a wide area network or the internet as a whole. The PING command sends packets of information to a specified IP Address and then measures the time it takes to get a response from the specified computer or device.

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

Please refer link and also material:

<http://searchnetworking.techtarget.com/definition/ping>

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

Tcp dpt:www

Tcp dpt:ssh

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

<http://bencane.com/2012/09/17/iptables-linux-firewall-rules-for-a-basic-web-server/>

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

Ans:iptable -F

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

Iptabels: IP Tables is a Lower Level Firewall Implementation Solution available in Linux Systems.

1. Allow incoming SSH only from a specific network.

Ans: iptables -A INPUT -i eth0 -p tcp -s 192.168.1.0/25 --dport 22 -m state --state

1. Allow incoming http and https

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 a specific ip addresses.

Ans: **iptables -A INPUT -s 192.168.1.0/24 -j DROP**

**Iptables** is used to set up, maintain, and inspect the tables of IPv4 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a `target', which may be a jump to a user-defined chain in the same table.