Quiz 4

Pavan kumar P

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

Ans) ->$ sudonetstat -plnt | grep ':56'

**nmaplocalhost | grep 56**

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

Ans) upstart

This question is for redhat linux – chkconfig

Please go through this link for reference.

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

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.

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

Ans) we should write the level of GUI

chkconfig ‚Äìlevel 5 servicename on

chkconfig ‚Äìlevel 1234 servicename off

please refer the link:

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

5. Explain briefly about LD\_LIBRARY\_PATH

Ans) LD\_LIBRARY\_PATH is used by your program to search for directories containing the libraries after it has been successfully compiled and linked.

Explain more about this.

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 connection oriented and reliable where as UDP is connection less and unreliable.

2) TCP needs more processing at network interface level where as in UDP it’s not.

3) TCP uses, 3 way handshake, congestion control, flow control and other mechanism to make sure the reliable transmission.

4) UDP is mostly used in cases where the packet delay is more serious than packet loss

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

are used and how.

The **ping** command is a very common method for troubleshooting the accessibility of devices. It uses a series of Internet Control Message Protocol (ICMP) Echo messages to determine:

* Whether a remote host is active or inactive.
* The round-trip delay in communicating with the host.
* Packet loss.

The **ping** command first sends an echo request packet to an address, then waits for a reply. The ping is successful only if:

* the echo request gets to the destination, and
* the destination is able to get an echo reply back to the source within a predetermined time called a timeout. The default value of this timeout is two seconds on Cisco routers

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

Ans) netstat -a |grepssh

startssh

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

. 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:

a. Allow incoming SSH only from a specific network.

b. Allow incoming http and https

c. block a specific ip addresses.

Ans) )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