Name : Abhinav Ponnala Quiz 4 (Solutions)

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

Ans: netstat -anp | grep 56

nmaplocalhost | grep 56

2. 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/>

and also refer the material.

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**: chkconfig script on.**

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: **Linux has the concept of shared libraries, i.e. libraries of code that aren't baked into executables, but instead are dynamically linked when the program is executed. The executable simply contains references to names of libraries that are required.**

**LD\_LIBRARY\_PATH is an environment variable listing extra paths that the Linux load-time linker should use when locating these libraries. It's simply a colon-separated list of the form**.

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

relate to differences in the two protocols?

Ans: **There are two types of Internet Protocol (IP) traffic. They are TCP orTransmission Control Protocol and UDP or User Datagram Protocol. TCP is connection oriented – once a connection is established, data can be sent bidirectional. UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.**

**TCP** [ensures](http://www.diffen.com/difference/Ensure_vs_Insure) a reliable and ordered delivery of a stream of bytes from user to [server](http://www.diffen.com/difference/Server_vs_Workstation) or vice versa. **UDP** is not dedicated to end to end connections and communication does not check readiness of receiver.

|  |
| --- |
|  |

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

are used and how.

Ans: **If you are having connectivity problems, you can use the ping command to check the destination IP address you want to reach and record the results. The ping command displays whether the destination responded and how long it took to receive a reply. If there is an error in the delivery to the destination, the ping command displays an error message.**

* **Ping your computer (by address, not host name) to determine that TCP/IP is functioning. (Pinging your computer does not verify that your network adapter is functioning.)**
* **Ping the local router to determine whether the router is running.**
* **Ping beyond your local router**

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.

Ans**: netstat -a |grep ssh**

**start ssh**

**/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 ip table.

Ans: Use ‘iptables –flush’ option to delete all the rules.

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.

Ans**: Iptables is used to set up, maintain, and inspect the tables of IP 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.**

**a**. **iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT**

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

c. **iptables -I INPUT -s 1.2.3.4 -j DROP**