1. What is the architecture of LINUX? (Hardware, kernel, shell, utilities/applications)
2. What are the features of UNIX? (multiuser, multitasking, portability, security and communication)
3. Features of LINUX OS. (portable, open-source, multi-user, multiprogramming, hierarchical file system, shell, security)
4. What is the difference between Kernel and Shell?
5. What are the different types of shells? (Bourne, ($) C( %) and Korn ($))
6. What are the types of shell in UNIX? Default shell of LINUX?
7. What is the meaning of the terms multiprogramming, multiuser and multithreading?
8. What are different essential pieces of LINUX? ( BootLoader, Kernel, Daemons, The Shell, Graphical server, Desktop environment and applications)
9. Why should LINUX may be preferred over other OS?
10. What are LINUX most popular distributions?
11. LINUX File System.
12. Basic Commands pwd, who, cd, cd .. , ls, mkdir, rmdir, touch, cat, cp, mv, rm, chmod, passwd, grep, vi, man, more, tall, wc, du, df,

**$find /home/swati/Desktop -name "\*.docx" –print**

**$ ls -l test.docx**

-rwxrwxr-x 1 swati swati 9870 Jul 15 2014 test.docx

**$ ln test.docx test1.docx**

**$ ls -l test\*.docx**

-rwxrwxr-x 2 swati swati 9870 Jul 15 2014 test1.docx

-rwxrwxr-x 2 swati swati 9870 Jul 15 2014 test.docx

**$ rm test1.docx**

**$ ls -l test\*.docx**

-rwxrwxr-x 1 swati swati 9870 Jul 15 2014 test.docx

**$ file test.docx**

test.docx: Microsoft Word 2007+

**$ nano file1.txt**

**$ nano file2.txt**

**$ cat file1.txt**

hi,

how are you?

bye

**$ cat file2.txt**

HI. how are you?

where are you going?

Bye

**$ cmp file1.txt file2.txt**

file1.txt file2.txt differ: byte 1, line 1

**$ chmod u+x file1.txt**

**$ chmod g+x file1.txt**

**$ chmod u+r, g-x, o+rw file1.txt**

**$ chmod ugo=r file1.txt**

**$ chmod 740 file1.txt**

**$chown test1 file1.txt**

**$chgrp tecompgrp file1.txt**

**$ tac file1.txt**

bye

how are you?

hi,

**$ cat file1.txt**

hi,

how are you?

Bye

**$tail -2 file1.txt**

how are you?

Bye

**$head -2 file1.txt**

hi,

how are you?

**$ ps**

PID TTY TIME CMD

3253 pts/1 00:00:00 bash

3493 pts/1 00:00:00 ps

**$ sort file1.txt**

bye

hi,

how are you?

**$kill 120**

**$mail <username>**

**$wall ,msg>**

**$ date**

Thu Feb 19 15:02:38 IST 2015

**$who**

swati :0 2015-02-19 12:15 (:0)

swati pts/1 2015-02-19 14:12 (:0.0)

**$who am i**

swati pts/1 2015-02-19 14:12 (:0.0)

**$ cal**

February 2015

Su Mo Tu We Th Fr Sa

1 2 3 4 5 6 7

8 9 10 11 12 13 14

15 16 17 18 19 20 21

22 23 24 25 26 27 28

$

**The Linux kernel was invented by**

A. Linus pauling B. Linus Torvalds C.Linus Thorwalds D. Linus Van Pelt.

**Which of the following is not a Linux GUI**

A. Xfree86 B. KDE C. Motif D. Gnome

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ makes it possible to run Windows and Linux Kernel simultaneously in parallel on the same machine.

**Which Linux distribution is the basis for Ubuntu?**

A. Debian B. Fedora C. CentOS

**How many primary partitions can exist on one drive?**

A. 16 B. 4 C.2 D. 1

**The Ping command operated by using**

A. NSLoop B.SMS C.ICMP D.SNMP

**The command used to query internet name servers interactively for information is**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**The netstat command is used to list TCP connections\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ARP stands for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, which is used to find \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**WEB SERVER**

Q The command is a used to determine the path that an IP packet has taken to reach a destination is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Q Virtual hosting is a method ­­­­­­­­­­­­ to\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Q Command to install Apache web server on Ubuntu \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Q Name of main configuration file of Apache server\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Q Port on which Apache server works? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What is virtual hosting?**

Virtual hosting is a method for hosting multiple domain names on a server using a single IP address. Virtual hosting allows one server to share its resources, such as memory and processor cycles, in order to use its resources more efficiently.

**Create a new user file and add a user with username "test" and password "test".**

**htpasswd -c /usr/local/etc/httpd/users test**

User will be prompted to provide the password. The -c argument tells htpasswd to create new file for users. To add more users, -c argument can be omitted.

**You need to install Apache web server on Ubuntu server. How can you download and install the Apache2 package?**

**sudo apt-get install Apache2**

**What are Iptables?**

Iptables are user space application programs that allow a system administrator to configure the tables provided by the Linux kernel firewall.

**Which privilege is required to operate iptables?**

Iptables require root user privilege for execution, otherwise they fail to function.

**What type of ports are 80 and 443?**

The port 80 is a regular port while port 443 is a secure port.

**What is the query to install update package of Apache server?**

**sudo apt-get update**

**How to check the version of Apache server ?**

apache2 –v

**What is meaning of “Listen” in httpd.conf file ?**

Port number on which to listen for nonsecure (http) transfers.

**What is DocumentRoot ?**

it is a location of files which are accessible by clients from the web server. By default, the Apache HTTP server in RedHat Enterprise Linux is configured to serve files from the /var/www/html/ directory.

**On which port Apache server works ?**

http – port 80

https – port 443

**Name of main configuration file of Apache server ?**

httpd.conf

**On which version of apache you have worked ?**

httpd-2.2.3

**What is the difference between a restart and a graceful restart of a web server?**

During a normal restart, the server is stopped and then started, causing some requests to be lost. A graceful restart allows Apache children to continue to serve their current requests until they can be replaced with children running the new configuration.

**If you have only one IP address, but you want to host two web sites on your server. What will you do?**

In this case we can use **Name Based Virtual hosting.**

ServerName 10.111.203.25

NameVirtualHost \*:80

<VirtualHost \*:80>

ServerName web1.test.com

DocumentRoot /var/www/html/web1

</VirtualHost>

<VirtualHost \*:80>

ServerName web2.test2.com

DocumentRoot /var/www/html/web2

</VirtualHost>

**Can I serve content out of a directory other than the DocumentRoot directory?**

Yes, by using “Alias” we can do this.

**Can you record all the cookies sent to your server by clients in Web Server logs?**

Yes, update **CustomLog** in httpd.conf file.

**Which of the following best explains why Apache Web servers are able to handles multiple requests?**

A. In addition to port 80, Apache opens ports 8080, 8000, and others to handle the additional requests.

**B. Apache is able to spawn child processes that handle requests before they die.**

C. Apache uses therenice service to load balance between different system daemons.

D. Upon reaching a set number of requests, Apache uses a raw socket to adjust a system’s bandwidth to handle the additional requests.

**Ans: B**

**What is location of log files for Apache server ?**

/var/log/httpd/error\_log or /var/log/apache2/error.log

**What are the types of virtual hosts ?**

a. name-based

b. IP-based.

Name-based virtual host means that multiple names are running on each IP address.

IP-based virtual host means that a different IP address exists for each website served. Most configurations are named-based because it only requires one IP address.

**Command to restart/start Apache web server ?**

service httpd restart/start

**Is it possible to record the MAC (hardware) address of clients that access your server ?**

No

**What is Apache?**

Apache is Web server application.

**Question: What is use of Apache in Web Server?**

Apache's role is all about communication over networks, and it uses the TCP/IP protocol (Transmission Control Protocol/Internet Protocol which allows devices with IP addresses within the same network to communicate with one another).

**From where the Apache name comes?**

The name "Apache" derives from the word "patchy" that the Apache developers used to describe early versions of their software development.

**Is Apache open source?**

Yes, It is

**Who is Initial Author of Apache?**

Robert McCool

**In which language Apache is written?**

'C' Language

**What is offical website of Apache?**

httpd.apache.org

**On a fresh install, which three config files Apache will have**

**srm.conf, access.conf and httpd.conf**

The first two are remnants from the NCSA times, and generally you should be ok if you delete the first two, and stick with httpd.conf.

**What’s the command to stop Apache? –**

$sudo /etc/init.d/apache2 stop

**What is mod\_vhost\_alias?**

It allows hosting multiple sites on the same server via simpler configurations.

**What does htpasswd do?**

It creates a new user in a specified group, and asks to specify a password for that user.

**FTP**

**What is FTP?**

FTP stands for File Transfer Protocol. An FTP server allows clients to connect to it either anonymously or with a username and password combination. After successful authentication, files can be transferred back and forth between the server and client. The files are neither encrypted nor compressed.

FTP client connects to the FTP server by establishing an FTP control connection to port 21 of the server. Your commands such as ‘ls’ and ‘get’ are sent over this connection. Whenever the client requests data over the control connection, the server initiates data transfer connections back to the client. The source port of these data transfer connections is always port 20 on the server, and the destination port is a high port (greater than 1024) on the client.

Q The directive that allow Anonymous FTP is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Q What does VSFTPD Stands for? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Q The directive to set ftp banner in ubuntu is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Q The port no for TFTP? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Please note vsftpd.conf file is used to control various aspects of configuration.**

**However, the format of file is very simple and it contains comment or directive.**

**Comment lines begins with a ‘#‘ are ignored and a directive line has the following format.**

**option=value**

**How to allow/deny specific users access to the FTP server ?**

To deny specific users access to the FTP server, add their usernames to the /etc/vsftpd/ ftpusers file. By default, system users such as root and nobody are included in this list.

**What is meaning of max\_clients parameter ?**

Maximum number of clients that can connect at one time. If set to 0, the number of clients is unlimited.

**I want to copy multiple files without prompting for any info, how can I do that one?**

ftp -i ftpserver

**Local users cannot log in. How to resolve this issue?**

Check “local\_enable=YES” in your /etc/vsftpd/vsftpd. conf to allow local users to log in.

**Important Configuration file for vsftp server ?**

The FTP server uses the /etc/vsftpd/vsftpd.conf configuration file. Using this file, you can set options for displaying a custom banner message after users log in, setting the default file permissions for uploaded files, and setting the port on which to listen for incoming connections.

**On which port VSFTP server works?**

FTP uses two ports, 20 and 21. By default, the FTP server listens for requests on port 21. After a connection is established, the client sends commands to the server on port 21. However, port 20 is used when the server sends data back to the client.

**How to restart VSFTP server ?**

service vsftpd restart, /etc/init.d/vsftpd restart

**How to allow Anonymous FTP ?**

Anonymous FTP is enabled by default by setting the anonymous\_enable directive in /etc/vsftpd/vsftpd.conf to YES.

**What is Passive mode?**

Passive mode, like active mode, is initiated by the FTP client application. When requesting data from the server, the FTP client indicates it wants to access the data in passive mode and the server provides the IP address and a random, unprivileged port (greater than 1024) on the server. The client then connects to that port on the server to download the requested information.

**Explain directive “session\_support”?**

When enabled, vsftpd attempts to maintain login sessions for each user through Pluggable Authentication Modules (PAM).

**How to change vsftpd default port?**

Set "listen\_port" option in "vsftpd.conf"

**Does vsftpd support IPv6?**

Yes. In Linux Like operating system vsftpd(Very Secure FTP Daemon) is ftp server , which provides the features of downloading and uploading files to the ftp space.

**What does VSFTPD Stands for ?**

VSFTPD stands for Very Secure FTP Daemon.

**What are the defaults ports used in linux ftp server ?**

Ans: Port 20 – This is the data transfer port. All the all subsequent data transfers between the client and server are done using this port.

Port 21 – On this port control connection is established. All commands we send and the ftp server’s responses to those commands will go over the control connection, but any data sent back (such as “ls” directory lists or actual file data in either direction) will go over the data connection.

**What is the configuration file of vsftpd ?**

‘/etc/vsftp/vsftpd.conf’

**How to disable Anonymous user in vsftpd ?**

Ans: Edit the conf file ‘/etc/vsftpd/vsftpd.conf’ and change below directive and restart the ftp service.

anonymous\_enable=NO

**How to set ftp banner in linux ?**

Ans: Open the file ‘/etc/vsftpd/vsftpd.conf’ and set the below directive :

ftpd\_banner= “Enter New Banner Here”

**What is the Difference between TFTP and FTP Server?**

TFTP is File Transfer Protocol which usages User Datagram Protocol (UDP) whereas FTP usages Transmission Control Protocol (TCP). TCP usages port number 20 for Data and 21 for control by default whereas TFTP usages port 69 by default.

**Is it Possible to maintain log of FTP requests and responses?**

Yes! We can log FTP requests and responses. What we need to do is to modify the binary value of parameter ‘**log\_ftp\_protocol**’. If set to Yes, it will log all the requests, responses. The log may be very useful in Debugging. The default value of above parameter is NO which means no logs are maintained by default.

**How to display certain text message before a client connects to FTP server. How would you get this done?**

Answer : We can achieve this by setting ‘banner\_file’. We need to set ftpd\_banner=/path/to/banner-file in vsftpd.conf file.

**How would you block an IP which is acting malicious on your internal private VSFTP network?**

We can Block IP either by adding the suspicious IP to ‘/etc/hosts.deny’ file or alternatively adding a DROP rule for the suspicious IP to iptables INPUT chain.

**How to disable directory listing in a FTP server?**

Answer : The parameter ‘dirlist\_enable’ comes to rescue at this point. The value of ‘dirlist\_enable’ should be set to NO. The default value is YES.

# Add this line to disable directory listing.

dirlist\_enable=NO

**What is default directory for ftp / Anonymous user ?**

Ans : ‘/var/ftp’ is the default directory for ftp or Anonymous user

**How to enable only limited/allowed users are able to login via ftp ?**

Ans: This can be done by editing the file ‘/etc/vsftpd/vsftpd.conf’ and add the below directives :

userlist\_enable=YES

userlist\_file=/etc/vsftpd.user\_list

userlist\_deny=NO

The file specified by userlist\_file will now contain users that are able to login.

**How to disable certain FTP commands?**

There are some individual settings (e.g. dirlist\_enable) or you can specify a complete set of allowed commands with “cmds\_allowed”.

**How to restrict some IP’s not use my FTP server?**

vsftpd can integrate with tcp\_wrappers (if built with this support). It is enabled with the setting “tcp\_wrappers=YES”.

**Does vsftpd support IPv6?**

Yes, as of “version 1.2.0″.

**SSH Secure Shell to login remotely**

SSH stands for Secure Shell is a network protocol, used to access remote machine in order to execute command-line network services and other commands over a Network. SSH is Known for its high security, cryptographic behavior and it is most widely used by Network Admins to control remote web servers primarily.

Q. To access remote machine in a secure manner the protocol used is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

stands for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What is the default port & configuration file of SSH Server ?**

22 is default port for ssh and ‘/etc/ssh/sshd\_config’ is the configuration file.

Q: Name Configuration file of SSH Server \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What is the configuration file of ssh client ?**

‘ /etc/ssh/ssh\_config ‘ is configuration file for ssh client.

**What is SSH port forwarding ?**

SSH Port Forwarding, sometimes called SSH Tunneling, which allows you to establish a secure SSH session and then tunnel arbitrary TCP connections through it. Tunnels can be created at any time, with almost no effort and no programming.

**ssh -L localport:host:hostport user@ssh\_server -N**

where:

-L – port forwarding parameters

localport – local port (chose a port that is not in use by other service)

host – server that has the port (hostport) that you want to forward

hostport – remote port

-N – do not execute a remote command, (you will not have the shell)

user – user that have ssh access to the ssh server (computer)

ssh\_server – the ssh server that will be used for forwarding/tunneling

Without the -N option you will have not only the forwarding port but also the remote shell.

**How to allow only specific users to ssh your linux server ?**

Open the file ‘/etc/ssh/sshd\_config’ and add the parameter ‘AllowUsers user1 user2′ & then restart the ssh server.

**What is the use of scp command ?**

SCP stands for Secure Copy ,it copies files between hosts over a network. It uses ssh for data transfer & uses the same authentication and provides the same security as ssh. Unlike rcp, scp will ask for passwords or passphrases if they are needed for authentication.

**How to check SSH server’s Version ?**

Using the command ‘ ssh -V ‘ we can find the ssh server’s version.

**How to Copy the file “server.txt” from the local machine to a remote host using port 2751 in /opt folder.**

**scp -P 2751 /home/server.txt** [**root@mail.linuxtechi.com:/opt**](mailto:root@mail.linuxtechi.com:/opt)

**SSH is configured on what Port Number, by default? How to change the port of SSH?**

SSH is configured on port 22, by default. We can change or set custom port number for SSH in configuration file.

We can check port number of SSH by running the below one liner script, directly on terminal.

# grep Port /etc/ssh/sshd\_config [On Red Hat based systems]

# grep Port /etc/ssh/ssh\_config [On Debian based systems]

To change the port of SSH, we need to modify the configuration file of SSH which is located at ‘/etc/ssh/sshd\_config‘ or ‘/etc/ssh/ssh\_config‘.

# nano /etc/ssh/sshd\_config [On Red Hat based systems]

# nano /etc/ssh/ssh\_config [On Debian based systems]

Searh for the Line.

Port 22

And replace ‘22‘ with any UN-engaged port Number say ‘1080‘. Save the file and restart the SSH service to take the changes into effect.

# service sshd restart [On Red Hat based systems]

# service ssh restart [On Debian based systems]

**SSH or Telnet? Why? What is the difference?**

Both SSH and Telnet are network Protocol. Both the services are used in order to connect and communicate to another machine over Network. SSH uses Port 22 and Telnet uses port 23 by default. Telnet send data in plain text and non-encrypted format everyone can understand whereas SSH sends data in encrypted format. Not to mention SSH is more secure than Telnet and hence SSH is preferred over Telnet. SSH uses a public key for authentication while Telnet does not use any authentication.SSH adds a bit more overhead to the bandwidth compared to Telnet

**How to add welcome/warning message as soon as a user login to SSH Server?**

In order to add a welcome/warning message as soon as a user logged into SSH server, we need to edit file called ‘/etc/issue’ and add message there.

**# nano /etc/issue**

And add your custom message in this file. See, below a screen grab that shows a custom message as soon as user logged into server.

SSH Login Banner

SSH Login Message

**SSH has two protocols? Justify this statement.**

Answer : SSH uses two protocols – Protocol 1 and Protocol 2. Protocol 1 is older than protocol 2. Protocol 1 is less secure than protocol 2 and should be disabled in the config file.

Again, we need to open the SSH configuration file and add/edit the lines as shown below.

# protocol 2,1

to

Protocol 2

Save the configuration file and restart the service.

**Is it possible to pass input to SSH from a local file? If Yes! How?**

Answer : Yes! We can pass input to SSH from a local file. We can do this simply as we do in scripting Language. Here is a simple one liner command, which will pass input from local files to SSH.

# ssh username@servername < local\_file.txt

**What is the difference between service and process?**

A process is any piece of software that is running on a computer. For example, your anti-virus software runs in the background as a process, which was automatically started when the computer booted. Some processes start when your computer boots, others are started manually when needed.

Some processes are services that publish methods to access them, so other programs can call them as needed. Printing services would be an example of a service type of process, where your email program can just call the print services process to say it wants to print, and the service does the actual work.

**What are the Linux-based security tools?**

Selinux

Firewall

iptables

Tcp-wrappers

**What are the basic elements of firewall?**

A firewall should be able to filter packets (drop/pass them) based on certain rules specified by the user. The rules may be used to identify an incoming packet to the computer or outgoing packet from the computer, it can be based on target port number/ip add, traffic from a particular Network card etc…

The firewall rules can be in a tabular form (saved on the disk) from where the firewall software can read them and implement it. **iptables** firewall on Linux is a great example

**What is the UID and GID of root user? Can a normal user can change the ownership of a file? What is the command to change ownership of a file?**

The root UID/GID is 0 (zero). Which is why he can able to intervene in all normal users files even though he don’t had permission. A normal user will don’t have the permission to change ownership of file. The command to change ownership is < chown user.user file >

**What is the diff b/w ext2 and ext3?**

Ext3 is a tiny bit slower than ext2 is, but it holds tremendous advantages.

There is really only one difference between ext2 and ext3, and that is that ext3 uses a journal to prevent filesystem corruption in the case of an unclean shutdown (ie. before the filesystem is synced to disk). That makes ext3 a bit slower than ext2 since all metadata changes are written to the journal, and then flushed to disk, but on the other hand you don’t risk having the entire filesystem destroyed at power failure or if an unwitted person turns the computer off uncleanly. You don’t have to check the filesystem after an unclean shutdown either.

**What does nslookup do?**

Nslookup is a program used to find information about internet Domain Name server.

The two modes of nslookup are: Interactive and non-interactive.

Using ‘interactive mode’ user can query the name servers for the information pertaining to hosts and domains.

Using ‘non-interactive mode’ the user can just print the name and requested information of a host.

**What is the difference between UDP and TCP?**

TCP is a Transmission Control Protocol.UDP is a User Datagram Protocol.

There are four major differences between UDP and TCP:

1. TCP can establish a Connection and UDP cannot.

2. TCP provides a stream of unlimited length, UDP sends Small packets.

3.TCP guarantees that as long as you have a connection data sent will arrive at the destination, UDP provides not guarantee delivery.

4. UDP is faster for sending small amounts of data since no connection setup is required, the data can be sent in less time than it takes for TCP to establish a connection.

**What command do you run to check file system consistency?**

Need to run fsck [file system consistency check] command to check file system consistency and repair a

**How to see unallocated hard disk space on linux**

**df -h**

**How do u find remote machine operating system and version?**

**nmap -A –v 192.168.1.100**

**How do you port scanning with netstat command?**

**netstat –an**

**Linux Network monitoring Tools?**

netstat and ss – Network Statistics

iptraf – Real-time Network Statistics

tcpdump – Detailed Network Traffic Analysis

strace – System Calls

/Proc file system – Various Kernel Statistics

# cat /proc/cpuinfo

# cat /proc/meminfo

# cat /proc/zoneinfo

# cat /proc/mounts

Nagios – Server And Network Monitoring

Cacti – Web-based Monitoring Tool

Gnome System Monitor – Real-time Systems Reporting and Graphing

**What is mean by system calls?**

A system call is the mechanism used by an application program to request service from the operating system. On Unix-based and POSIX-based systems, popular system calls are open, read, write, close, wait, exec, fork, exit, and kill. Many of today’s operating systems have hundreds of system calls. For example, Linux has 319 different system calls. FreeBSD has about the same (almost 330). Tools such as strace and truss report the system calls made by a running process.

**Important port no:**

**NFS – 2049**

**FTP – 20, 21**

**SAMBA – 445**

**SSH – 22**

**DNS – 53**

**POP3 – 110**

**IMAP – 143**

**HTTPS – 443**

**HTTP – 80**

**How do u extract files from iso cd images in linux?**

mount –o loop disk1.iso /mnt/iso