**1.When do you need a virtual hosting ?**

The term Virtual Host refers to the practice of maintaining more than one server on one machine, as differentiated by their apparent hostname. For example, it is often desirable for companies sharing a web server to have their own domains, with web servers accessible as www.company1.com and www.company2.com, without requiring the user to know any extra path information.

**2.In which port telnet is listening?**

23

**3.How to get the listening ports which is greater than 6000 using netstat ?**

**4.How to block and openrelay ?**

Open relays are e-mail servers that are configured to accept and transfer e-mail on behalf of any user anywhere, including unrelated third parties.

The qmail-smtpd daemon will consult the rcpthosts control file to determine valid destination addresses, and reject anything else.

**5.What is sandwitch configuration in qmail ?**

Qmail + Clam + Spamassassin- This is normally called Sandwitch configuration in qmail.

**6.Advantages of Qmail ?**

More secure, better designed, modular, faster, more reliable, easier to configure, don't have to upgrade it every few months or worry about being vulnerable to something due to some obscure feature being enabled

qmail supports host and user masquerading, full host hiding, virtual domains, null clients, list-owner rewriting, relay control, double-bounce recording, arbitrary RFC 822 address lists, cross-host mailing list loop detection, per-recipient checkpointing, downed host backoffs, independent message retry schedules, etc. qmail also includes a drop-in ``sendmail'' wrapper so that it will be used transparently by your current UAs.

**7.What is the difference between POP3 and IMAP ?**

**The Difference**

POP3 works by reviewing the inbox on the mail server, and downloading the new messages to your computer. IMAP downloads the headers of the new messages on the server, then retrieves the message you want to read when you click on it.

When using POP3, your mail is stored on your PC. When using IMAP, the mail is stored on the mail server. Unless you copy a message to a "Local Folder" the messages are never copied to your PC.

Scenarios of Use

POP3

 You only check e-mail from one computer.

 You want to remove your e-mail from the mail server.

IMAP

 You check e-mail from multiple locations.

 You use Webmail.

**8.How to drop packets using iptables ?**

Iptables -A INPUT -s xx.xx.xx.xx -d xx.xx.xx.xx -j DROP

**9.Daily routines of Linux Administrators ?**

\*.Check the health of servers

\*.Check for updates

\*.Check the Backup

\*.Check with the trouble ticketing system for any unread ticket.

\*.Troubleshoot if there any problem

\*.Installation of new servers, if needed.

\*.Report to the Boss

**10.How to take the Dump of a MySQL Database ?**

Mysqldump databasename > dumpname

**11.How to know the CPU usage of each process ?**

Top, uptime

**12.How to bind another IP in a NIC ?**

Copy the contents eth0 to eth1, and change the ipaddress. Restart the network. .

**13.Transparently proxy all web-surfing through Squid box**

iptables -t nat -A PREROUTING -i eth1 -tcp --dport 80 -j DNAT --to

iptables -t nat -A PREROUTING -i eth1 -tcp --dport 80 -j DNAT --to

**14.Transparently redirect web connections from outside to the DMZ web server.**

iptables -t nat -A PREROUTING -i eth0 -d 192.168.1.1 -dport 80 -j DNAT –to

**15 Howto Activate the forwarding**

echo 1 >/proc/sys/net/ipv4/ip\_forward

**16.Kill spoofed packets**

for f in /proc/sys/net/ipv4/conf/\*/rp\_filter; do

echo 1 > $f

done.

$iptables -A LDROP --proto tcp -j LOG --log-level info \ --log-prefix “TCP Drop”

1) What is Linux?  
  
Linux is an operating system based on UNIX, and was first introduced by Linus Torvalds. It is based on the Linux Kernel, and can run on different hardware platforms manufactured by Intel, MIPS, HP, IBM, SPARC and Motorola. Another popular element in Linux is its mascot, a penguin figure named Tux.  
  
  
2) What is the difference between UNIX and LINUX?  
  
Unix originally began as a propriety operating system from Bell Laboratories, which later on spawned into different commercial versions. On the other hand, Linux is free, open source and intended as a non-propriety operating system for the masses.  
  
3) What is BASH?  
  
BASH is short for Bourne Again SHell. It was written by Steve Bourne as a replacement to the original Bourne Shell (represented by /bin/sh). It combines all the features from the original version of Bourne Shell, plus additional functions to make it easier and more convenient to use. It has since been adapted as the default shell for most systems running Linux.  
  
4) What is Linux Kernel?  
  
  
  
The Linux Kernel is a low-level systems software whose main role is to manage hardware resources for the user. It is also used to provide an interface for user-level interaction.  
  
5) What is LILO?  
  
LILO is a boot loader for Linux. It is used mainly to load the Linux operating system into main memory so that it can begin its operations.  
  
6) What is a swap space?  
  
A swap space is a certain amount of space used by Linux to temporarily hold some programs that are running concurrently. This happens when RAM does not have enough memory to hold all programs that are executing.  
  
7) What is the advantage of open source?  
  
Open source allows you to distribute your software, including source codes freely to anyone who is interested. People would then be able to add features and even debug and correct errors that are in the source code. They can even make it run better, and then redistribute these enhanced source code freely again. This eventually benefits everyone in the community.  
  
8 ) What are the basic components of Linux?  
  
Just like any other typical operating system, Linux has all of these components: kernel, shells and GUIs, system utilities, and application program. What makes Linux advantageous over other operating system is that every aspect comes with additional features and all codes for these are downloadable for free.  
  
9) Does it help for a Linux system to have multiple desktop environments installed?  
  
In general, one desktop environment, like KDE or Gnome, is good enough to operate without issues. It’s all a matter of preference for the user, although the system allows switching from one environment to another. Some programs will work on one environment and not work on the other, so it could also be considered a factor in selecting which environment to use.  
  
10) What is the basic difference between BASH and DOS?  
  
The key differences between the BASH and DOS console lies in 3 areas:  
– BASH commands are case sensitive while DOS commands are not;  
– under BASH, / character is a directory separator and acts as an escape character. Under DOS, / serves as a command argument delimiter and is the directory separator  
– DOS follows a convention in naming files, which is 8 character file name followed by a dot and 3 character for the extension. BASH follows no such convention.  
  
11) What is the importance of the GNU project?  
  
This so-called Free software movement allows several advantages, such as the freedom to run programs for any purpose and freedom to study and modify a program to your needs. It also allows you to redistribute copies of a software to other people, as well as freedom to improve software and have it released to the public.  
  
12) Describe the root account.  
  
The root account is like a systems administrator account, and allows you full control of the system. Here you can create and maintain user accounts, assigning different permissions for each account. It is the default account every time you install Linux.  
  
13) What is CLI?  
  
CLI is short for Command Line Interface. This interface allows user to type declarative commands to instruct the computer to perform operations. CLI offers an advantage in that there is greater flexibility. However, other users who are already accustom with using GUI find it difficult to remember commands including attributes that come with it.  
  
14) What is GUI?  
  
GUI, or Graphical User Interface, makes use of images and icons that users click and manipulate as a way of communicating with the computer. Instead of having to remember and type commands, the use of graphical elements makes it easier to interact with the system, as well as adding more attraction through images, icons and colors.  
  
15) How do you open a command prompt when issuing a command?  
  
To open the default shell (which is where the command prompt can be found), press Ctrl-Alt-F1. This will provide a command line interface (CLI) from which you can run commands as needed.  
  
16) How can you find out how much memory Linux is using?  
  
From a command shell, use the “concatenate” command: cat /proc/meminfo for memory usage information. You should see a line starting something like: Mem: 64655360, etc. This is the total memory Linux thinks it has available to use.  
  
17) What is typical size for a swap partition under a Linux system?  
  
The preferred size for a swap partition is twice the amount of physical memory available on the system. If this is not possible, then the minimum size should be the same as the amount of memory installed.  
  
18) What are symbolic links?  
  
Symbolic links act similarly to shortcuts in Windows. Such links point to programs, files or directories. It also allows you instant access to it without having to go directly to the entire pathname.  
  
19) Does the Ctrl+Alt+Del key combination work on Linux?  
  
Yes, it does. Just like Windows, you can use this key combination to perform a system restart. One difference is that you won’t be getting any confirmation message and therefore, reboot is immediate.  
  
20) How do you refer to the parallel port where devices such as printers are connected?  
  
Whereas under Windows you refer to the parallel port as the LPT port, under Linux you refer to it as /dev/lp . LPT1, LPT2 and LPT3 would therefore be referred to as /dev/lp0, /dev/lp1, or /dev/lp2 under Linux.  
  
21) Are drives such as harddrive and floppy drives represented with drive letters?  
  
No. In Linux, each drive and device has different designations. For example, floppy drives are referred to as /dev/fd0 and /dev/fd1. IDE/EIDE hard drives are referred to as /dev/hda, /dev/hdb, /dev/hdc, and so forth.  
  
22) How do you change permissions under Linux?  
  
Assuming you are the system administrator or the owner of a file or directory, you can grant permission using the chmod command. Use + symbol to add permission or – symbol to deny permission, along with any of the following letters: u (user), g (group), o (others), a (all), r (read), w (write) and x (execute). For example the command chmod go+rw FILE1.TXT grants read and write access to the file FILE1.TXT, which is assigned to groups and others.  
  
23) In Linux, what names are assigned to the different serial ports?  
  
Serial ports are identified as /dev/ttyS0 to /dev/ttyS7. These are the equivalent names of COM1 to COM8 in Windows.  
  
24) How do you access partitions under Linux?  
  
Linux assigns numbers at the end of the drive identifier. For example, if the first IDE hard drive had three primary partitions, they would be named/numbered, /dev/hda1, /dev/hda2 and /dev/hda3.  
  
  
25) What are hard links?  
  
Hard links point directly to the physical file on disk, and not on the path name. This means that if you rename or move the original file, the link will not break, since the link is for the file itself, not the path where the file is located.  
  
26) What is the maximum length for a filename under Linux?  
  
Any filename can have a maximum of 255 characters. This limit does not include the path name, so therefore the entire pathname and filename could well exceed 255 characters.  
  
27)What are filenames that are preceded by a dot?  
  
In general, filenames that are preceded by a dot are hidden files. These files can be configuration files that hold important data or setup info. Setting these files as hidden makes it less likely to be accidentally deleted.  
  
28) Explain virtual desktop.  
  
This serves as an alternative to minimizing and maximizing different windows on the current desktop. Using virtual desktops, each desktop is a clean slate where you can open one or more programs. Rather than minimizing/restoring all those programs as needed, you can simply shuffle between virtual desktops with programs intact in each one.  
  
29) How do you share a program across different virtual desktops under Linux?  
  
To share a program across different virtual desktops, in the upper left-hand corner of a program window look for an icon that looks like a pushpin. Pressing this button will “pin” that application in place, making it appear in all virtual desktops, in the same position onscreen.  
  
30) What does a nameless (empty) directory represent?  
  
This empty directory name serves as the nameless base of the Linux file system. This serves as an attachment for all other directories, files, drives and devices.  
  
31) What is the pwd command?  
  
The pwd command is short for print working directory command. It’s counterpart in DOS is the cd command, and is used to display the current location in the directory tree.  
  
32) What are daemons?  
  
Daemons are services that provide several functions that may not be available under the base operating system. Its main task is to listen for service request and at the same time to act on these requests. After the service is done, it is then disconnected and waits for further requests.  
  
33) How do you switch from one desktop environment to another, such as switching from KDE to Gnome?  
  
Assuming you have these two environments installed, just log out from the graphical interface. Then at the Log in screen, type your login ID and password and choose which session type you wish to load. This choice will remain your default until you change it to something else.  
  
34) What are the kinds of permissions under Linux?  
  
There are 3 kinds of permissions under Linux:  
– Read: users may read the files or list the directory  
– Write: users may write to the file of new files to the directory  
– Execute: users may run the file or lookup a specific file within a directory  
  
35) How does case sensitivity affect the way you use commands?  
  
When we talk about case sensitivity, commands are considered identical only if every character is encoded as is, including lowercase and uppercase letters. This means that CD, cd and Cd are three different commands. Entering a command using uppercase letters, where it should be in lowercase, will produce different outputs.  
  
36) What are environmental variables?  
  
Environmental variables are global settings that control the shell’s function as well as that of other Linux programs. Another common term for environmental variables is global shell variables.  
  
37) What are the different modes when using vi editor?  
  
There are 3 modes under vi:  
– Command mode – this is the mode where you start in  
– Edit mode – this is the mode that allows you to do text editing  
– Ex mode – this is the mode wherein you interact with vi with instructions to process a file  
  
38) Is it possible to use shortcut for a long pathname?  
  
Yes, there is. A feature known as filename expansion allows you do this using the TAB key. For example, if you have a path named /home/iceman/assignments directory, you would type as follows: /ho[tab]/ice[tab]/assi[tab] . This, however, assumes that the path is unique, and that the shell you’re using supports this feature.  
  
39) What is redirection?  
  
Redirection is the process of directing data from one output to another. It can also be used to direct an output as an input to another process.  
  
40) What is grep command?  
  
grep a search command that makes use of pattern-based searching. It makes use of options and parameters that is specified along the command line and applies this pattern into searching the required file output.  
  
41) What could possibly be the problem when a command that was issued gave a different result from the last time it was used?  
  
One highly possible reason for getting different results from what seems to be the same command has something to do with case sensitivity issues. Since Linux is case sensitive, a command that was previously used might have been entered in a different format from the present one. For example, to lists all files in the directory, you should type the command ls, and not LS. Typing LS would either result in an error message if there is no program by that exact name exist, or may produce a different output if there is a program named LS that performs another function.  
  
42) What are the contents in /usr/local?  
  
It contains locally installed files. This directory actually matters in environments where files are stored on the network. Specifically, locally-installed files go to /usr/local/bin, /usr/local/lib, etc.). Another application of this directory is that it is used for software packages installed from source, or software not officially shipped with the distribution.  
  
43) How do you terminate an ongoing process?  
  
Every process in the system is identified by a unique process id or pid. Use the kill command followed by the pid in order to terminate that process. To terminate all process at once, use kill 0.  
  
44) How do you insert comments in the command line prompt?  
  
Comments are created by typing the # symbol before the actual comment text. This tells the shell to completely ignore what follows. For example: “# This is just a comment that the shell will ignore.”  
  
45) What is command grouping and how does it work?  
  
You can use parentheses to group commands. For example, if you want to send the current date and time along with the contents of a file named OUTPUT to a second file named MYDATES, you can apply command grouping as follows: (date cat OUTPUT) > MYDATES  
  
46) How do you execute more than one command or program from a single command line entry?  
  
You can combine several commands by separating each command or program using a semicolon symbol. For example, you can issue such a series of commands in a single entry:  
  
  
ls –l cd .. ls –a MYWORK which is equivalent to 3 commands: ls -l cd.. ls -a MYWORK  
1  
ls –l cd .. ls –a MYWORK which is equivalent to 3 commands: ls -l cd.. ls -a MYWORK  
  
\*\*Note that this will be executed one after the other, in the order specified.  
  
47) Write a command that will look for files with an extension “c”, and has the occurrence of the string “apple” in it.  
  
Answer:  
  
  
 Find ./ -name “\*.c” | xargs grep –i “apple”  
1  
 Find ./ -name “\*.c” | xargs grep –i “apple”  
  
  
48) Write a command that will display all .txt files, including its individual permission.  
  
Answer:  
  
  
ls -a -l \*.txt  
1  
ls -a -l \*.txt  
  
  
49) Write a command that will do the following:  
-look for all files in the current and subsequent directories with an extension c,v  
-strip the,v from the result (you can use sed command)  
-use the result and use a grep command to search for all occurrences of the word ORANGE in the files.  
  
  
Find ./ -name “\*.c,v” | sed ‘s/,v//g’ | xargs grep “ORANGE”  
1  
Find ./ -name “\*.c,v” | sed ‘s/,v//g’ | xargs grep “ORANGE”  
  
  
50) What, if anything, is wrong with each of the following commands?  
a) ls -l-s  
b) cat file1, file2  
c) ls – s Factdir  
  
Answers:  
a) there should be space between the 2 options: ls -l -s  
b) do not use commas to separate arguments: cat file1 file2  
c) there should be no space between hyphen and option label: ls –s Factdir  
  
  
What is Kerberos used for?  
Kerberos is used for secure network logon.  
  
Which partition store system configuration files in Linux system?  
/etc partition stores system configuration files in Linux.  
  
What is the purpose of the MD5 option on passwords?  
MD5 is an encryption method that encrypts the password before saving.  
  
Name any four general password rules for user account.  
Include at least eight total characters  
Use the string in an unrepeated way  
Avoid use words that can be found in the dictionary  
Avoid use dates of significance, such as a birthday or anniversary  
A better method of password security is to create difficult-to-break passwords that are easy for the users to remember.  
  
What is the alternative method to a GUI installation in Linux ?  
Linux provides text base installation as the alternative method of GUI installation.  
  
What is the purpose of the swapon command ?  
swapon command is used to activate a already created swap partition. It cannot be used to create a new swap partition.  
  
What is gzip?  
gzip is a compression utility created by the GNU project.  
  
What is tar?  
tar is an archive utility that is used to create tape backups.  
  
Which is the standard command used to uncompress gzip files?  
The standard command used to uncompress gzip files is gunzip.  
  
What is the RPM switch for only installing packages?  
The command line switch for installing an RPM is -i.  
  
What is the command used to install an RPM package named demofilename2.2-2.i386.rpm?  
The most common command used to install an RPM package is rpm -ivh. Following command will install the given package  
#rpm -ivh demofilename2.2-2.i386.rpm  
  
What is the command used to remove an RPM package named demofilename2.2-2.i386.rpm?  
The most common command used to remove an RPM package is rpm -evh. Following command will remove the given package  
#rpm -evh demofilename2.2-2.i386.rpm  
  
What is the command used to update an RPM package named demofilename2.2-2.i386.rpm?  
The most common command used to update an RPM package is rpm -Uvh. Following command will update the given package and remove the old.  
#rpm -Uvh demofilename2.2-2.i386.rpm  
  
Which command is used to see which RPM version of gzip was installed on the system?  
#rpm -q gzip  
  
Where are the automatically mounted file systems listed?  
The automatically mounted file systems are listed in the file /etc/fstab.  
  
While installing the new RPM what common steps should take ?  
You should follow these common steps  
Use RPM tools should be used to query or verify the installed packages to  
confirm the installation of any previous packages.  
Check the signature of new package  
RPM should be installed or upgraded by first using the test mode to verify that it works, and then it should be installed  
At the end query the RPM and verify the installation of RPM  
Which organization controls the official releases and updates of the X Window System?  
The X Consortium at www.x.org controls the official release and updating of the X Window System  
  
PPP is most often used to create?  
PPP is most often used to create serial point-to-point connections.  
  
When attempting to connect to www.example.com you got unknown host message. Which service is most likely not functioning properly?  
DNS  
  
Samba is used to provide support for which protocol?  
Samba is used to support the Microsoft SMB/CIFS systems.  
  
What command is used to load a module into the kernel?  
The insmod command is used to load a module into the kernel  
  
Name one of the most secure method of remote access.  
SSH is the most secure method of remote access  
  
With respect to a Linux system’s RAM, how large should the swap file be?  
Generally the size of the swap file should be twice the size of installed RAM.  
  
How would you create a backup of the fstab file to the /backup folder?  
Use cp command to create the backup.  
#cp /etc/fstab /backup  
  
What command is used to exit the edit mode of VI editor?  
The [esc] key is used to exit from the edit mode of VI editor.  
  
What key combination will exit from VI editor and not save the changes made?  
Esc + q +! Key combination will exit VI without saving the changes.  
  
What command would you use to create a file system on a new hard drive?  
The mkfs command is used to create file systems.  
  
What fstab file do?  
The fstab file is used to automatically mount file systems.  
  
What inittab file do?  
The /etc/inittab file is used to perform the default state and terminal connections for a Linux system.  
  
What command can you use to verify the current active shell?  
The env command will display the current active shell.  
  
Where is the file . bashrc located?  
The . bashrc file is usually located in the /home/username directory.  
  
What function does the .bash\_profile file perform?  
The function of the .bash\_profile file is to provide login initialization commands.  
  
What function does the .bash\_logout file perform?  
The function of the .bash\_logout is to provide logout functions  
  
What function does the .bashrc file perform?  
The function of the .bashrc file is to provide shell configuration commands.  
  
  
Which version of RHEL officially supports LUKS encryption?  
From version 6 or higher LUKS encryption is officially supported by RHEL.  
  
What is the default virtualization technology for RHEL6 ?  
Default virtualization technology is KVM.  
  
Can you configure KVM Virtual machine on 32 bit system ?  
No, KVM virtualization requires at least 64 bit system.  
  
What is default mode of SELinux during the installation of RHEL ?  
In RHEL5 you have to choose the mode which you want.  
From RHEL6 default mode is Enforcing during the installation.  
However you can change the mode of SELinux after installation, only difference between RHEL5 and RHEL6 is that in RHEL5 asks you to choose the mode while RHEL6 does not let you to choose the mode during the installation.  
  
Which remote management service is allowed through the default firewall and by default installed in RHEL?  
By default SSH is always installed in RHEL. SSH uses port 22 which is allowed through the default firewall rules.  
  
Which standard directory is used by vsFTP server for file sharing ?  
Default Standard directory for ftp is /var/ftp/pub.  
  
Which standard directory is used by Apache web server for HTML files ?  
standard directory for HTML files is /var/www/html  
  
What is the default partition layout during the installation ?  
Default partition Layout is the LVM.  
  
Which necessary partition cannot be a part of logical volume group ?What is the Minix?  
Minix is the UNIX clone written by Andrew Tanenbaum at VU University, in Amsterdam when universities were no longer allowed access to the UNIX source code. MINIX also inspired the creation of the Linux kernel.  
  
What does POSIX stand for?  
POSIX stands for Portable Operating System Interface for Computer Environments. It is the standard for ensuring compatibility between UNIX versions.  
Who posted the source code of Linux kernel on the Internet and invited other programmers to modify and enhance it.?  
In 1991 Linus Torvalds, a 21-year-old student at the University of Helsinki Finland posted the source code of Linux kernel on the Internet and invited other programmers to modify and enhance it.  
  
Are Linux and UNIX are same ?  
Linux kernel was built to work like UNIX but doesn’t use any of the UNIX code—this is why Linux is not UNIX. A kernel is the core of any operating system.  
  
Who initiated the GNU Project?  
GNU project was initiated by Richard Stallman on 27 September 1983 at MIT. Main motive of this project was to give freedom and control in use of software's. GNU software guarantees these freedom-rights legally via its license. Users are free to run the software, share it, copy it, distribute it, study it and modify it.  
  
Under which licenses Linux kernel released?  
The Linux kernel is released under the GNU General Public License version 2 (GPLv2), and is developed by contributors worldwide.  
  
What does GPL mean?  
GPL stands for General Public License and it was created to protect the intent of the GNU project.  
  
Linux was originally created to run on what platform?  
Linux was originally created to run on the Intel x86 platform.  
  
Name the Linux services which provides network printing.  
CUPS provide network printing between Linux systems. It can be used with Samba service to extend network printing to windows systems.  
  
Which Linux service is used to provide network file storage ?  
NFS service is used to provide file sharing.  
  
Which Linux service is used as a database server ?  
MySQL and PostgreSQL are Linux database server.  
  
Which Linux service is used to turn a Linux system in proxy server ?  
Squid service can be used to turn any Linux system into an in proxy server.  
  
Which components of Linux provides pre-written code that a developer can use ?  
Linux libraries contain pre-written code that a developer can reuse in their applications.  
Your company purchased 5 new laptops. Laptop have Intel core i3 processor and Window 8 installed. Your network admin wants to install RHEL on them, but is concerned that it cannot be done because they already have Window 8 installed. Can this be done ?  
Yes you can install any operating system as long as the hardware is compatible. Hardware and operating systems are modular. Computer hardware is not tied in any way to a particular OS. Every OS have some minimum hardware requirements, if your hardware meets with that requirements, you can install that OS.  
You are a network administrator, your company wants you to download the source code of latest Linux kernel for the developer team. Can you do this?  
Source code of Linux kernel is available under the GPL license. Under the GPL, you are free to download the Linux source code and modify it.  
Your company have less funds but need a reliable file server set up? Which OS and file server service can you use ?  
Use Linux operating with NFS file service.  
You have purchased new laptop and want to resell old one, but you don't want to violate any licensing for OS. What can you do to avoid violating a software license?  
You can install Linux OS. All major software's for Linux are available under the GPL, those you can use without violating any software license.  
boot partition cannot be a part of logical volume group. You must have create it as a regular partition.  
  
Which partitions are recommended for custom layout of partition ?  
/  
/boot  
/home  
swap  
  
What step during the installation could you take to prevent a program from creating temporary files that fill up the entire space ?  
You can create a separate /tmp partition prevents a program from creating temporary files that fill up the entire filesystem.  
  
What is the kickstart ?  
kickstart is a installation method used in RHEL. A kickstart installation is started from a kickstart file, which contains the answers to all the questions in the installation program.  
  
Name any of two third party distribution based on RHEL6 source code.  
CentOS and Scientific Linux  
  
Which Log file contains all installation message?  
install.log.syslog file contains all messages that were generated during the installation.  
  
  
What Squid service do?  
Squid provides the Proxy service, which caches and filters web traffic.  
  
Which popular office suite freely available for both Microsoft and Linux ?  
Open office suite is freely available. You can install it on both OS Microsoft and Linux.  
  
You company recently switched from Microsoft to Linux. All their documents are created on Microsoft office 2007. How will you manage documents created on Microsoft office 2007 ?  
Install open office suite in Linux. It allows you work with Microsoft documents.  
  
Name any of three spreadsheet programs, those are equivalent to Microsoft Excel and available for Linux?  
Openoffice calc [Free]  
KOffice Kspread [Free]  
StarOffice Base [commercial ]  
Corel Quattro [commercial]  
  
What is the SMTP ?  
SMTP is the most common protocol for an e-mail server.  
  
What is NNTP ?  
NNTP is the common protocol which is used for news services. LeafNode and INN are examples of news servers.  
  
What Samba service do ?  
The Samba service provides Microsoft SMB support in Linux so that Linux machines can connect to Microsoft network resources.  
Which service provides searching capabilities on an intranet or domain?  
Dig is the common name of the service that provides searches on an intranet or domain.  
Which service can be used with NFS to provide remote file access for UNIX systems?  
NIS is used with NFS to provide remote file access for UNIX systems.  
  
What is MTA?  
MTA is a service of Sendmail server, which transfer mail from one network or host to another network or host.  
  
Name a connection-less protocol for file transfer.  
TFTP is a connection-less protocol for file transfer.  
  
You company wants to run Web Server on their intranet. Which Linux package should you use for this ?  
To run a Web server, you should install the Apache Web server.  
  
You company have slow internet connection. Which Linux service you can use to manage internet connection ?  
You should use Squid proxy server, which allows to manage the web contents and also cache the web pages to decrease the amount of traffic going to Internet.  
  
You have tasked with implementing new Linux systems in your lab, those will be used in training of Linux. What type of Linux distribution should you choose?  
For LAB environment you can use free Linux version of Linux distribution. In test system at company or in a Lab environment where usually no real risk in making mistakes you should use free version of Linux. While distribution itself maybe free or nearly free, you will be required to pay for technical support. In Lab environment where time permits you, instead of seeking helping hands, try to solve the issue at your own, that could a great learning experience.  
  
You have tasked with implementing a new Linux server in your network that will store confidential information of company. Your lab technician have fedora. Should you use it for your new server?  
You could use it, but you should not use it for server. It is not recommended to use an obscure, unsupported distribution for critical server. A well-know, well-supported distribution like RHEL would be a better choice. If a technical problem occurs at some point after the server has been installed, you need to be able to call someone and get an answer immediately rather than searching on internet to find a solution. You should be able to solve the issue and get the server back into production as fast as possible.  
  
You are installing a Linux system that will run a software that creates very large log files. Which directory should you create separate partition for ?  
Create a separate partition at /var directory.  
  
You are installing a Linux system that will provide file storage for a number of network users. Which directory should you create separate partition for?  
Create a separate /home directory.  
  
Which port should you open in your host firewall to run web server?  
By default web server use port 80 and 443 which you need to open in firewall.  
  
Which IP addressing should you use for Server?  
For server you should always use static IP address.  
  
Which IP address should you use for client desktop?  
For client you can use both static and dynamic method. For easy management using DHCP to assign IP address would be the best option.  
  
You are installing RHEL in new system that will be used by software developer to develop advance program. Which option should you choose during the installation, while installation program ask you to choose the set of software?  
Choose Software Development Workstation and use customize now option to select additional packages.  
  
You are installing RHEL in new system that will used by an administrative assistant to type documents, create presentations, and manage e-mail. Which option should you choose during the installation, while installation program ask you to choose the set of software?  
Choose Desktop and use customize now option to select additional packages.  
  
Which partition is used for virtual memory by a Linux system?  
swap  
  
Which ports should you open in host firewall for an email server?  
Open port 110 which is used by the POP3 e-mail protocol.  
Open port 25 which is used by the SMTP e-mail protocol.  
Open port 143 which is used by the IMAP e-mail protocol.  
  
Your Linux system have two SCSI hard disk drives. The first drive is assigned as SCSI ID 0, and the second drive is assigned SCSI ID 1. How these will be refers in system?  
/dev/sda point to the first SCSI drive.  
/dev/sdb points to the second SCSI drive  
  
Your Linux system have a single IDE hard disk drive. How partitions will be refers on the IDE drive?  
hd refers for IDE hard disk  
a refers for first hard disk. If system have multiple hard disk use b for second, c for third and so on till last hard disk.  
1 refers for first partition, 2 for second partition and so on till last partition.  
For example  
/dev/hda1 points to the first partition on the first IDE  
/dev/hdd4 points to the fourth partition on the fourth IDE  
/dev/hdc2 points to the second partition on the third IDE  
  
  
Which file have runlevel configuration?  
/ect/inittab  
  
What command would you use to shut down the system in 100 seconds?  
#shutdown -h 100  
  
What daemon controls the print spooling process?  
The Line Printing Daemon (lpd) controls the print spooling process.  
  
What configuration file defines the default runlevel for the init process?  
/etc/inittab file defines the default runlevel for the init process.  
  
Which command can you use to shut down and halt a Linux System?  
The halt command will shut down a Linux system without rebooting  
  
What init level should you set to bring the system to single-user mode?  
init 1 will bring the system to single-user mode  
A user wants to restart the NFS server because they want to enable changes made in the configuration file. What command accomplishes this task?  
#service nfs reload  
The reload command will tell the system to stop the service, reload the configuration file, and restart the service  
  
What command can you use to reboot a Linux system?  
The command to reboot a Linux system is reboot  
  
What mode must you be in when using vi editor to input text into a file?  
To insert text in the vi editor, you must be in insert mode  
  
What runlevel does init 1 represent?  
init 1 represents runlevel1.Runlevel 1 is used for single user mode.  
One user from your company left the job without telling root account password of his system. To reset root password, in which mode you need to boot the system?  
To reset the root password, we need to boot the system in single user mode.  
  
What runlevel does init 2 represent?  
init2 represents rulevel 2. runlevel 2 is used for multiuser without networking.  
Some users are complaining that the DHCP server is not running. After examine the running processes on the system, you notice that the process is not present. What command should   
  
you use to start the DHCP service?  
Because the service is currently not running, use the start command  
#service dhcpd start  
  
What runlevel does init 5 represent?  
Runlevel 5 is used to boot up a full multiuser system and to automatically start X-windows.  
What tar argument is used to extract files from an archive?  
To extract files from an archive, use the -x argument in the tar command.  
  
What init runlevel should be set to shut down and reboot the system?  
init runlevel 6 is used to shut down and reboot the system  
  
What command would you use to add the user name vickey?  
#useradd vickey  
This command will add the user viceky with default options. But this will not be able to login in system until you set a password for it. To set password use following command  
#passwd vickey  
  
Which runlevel currently not is used ?  
Runlevel 4 is not used.  
Your company hired a new developer for temporary periods to speed up the ongoing project. You are tasked to create a new user account which should be disabled automatically on 5 may 2014. How would you do that?  
Use -e option with useradd command. -e option allows you to set the date on which the user account will be disabled. The date is specified in the format YYYY-MM-DD. Following command will do the assigned task  
#useradd -e 2014-05-05  
  
Which command should you use to change the user information listed form finger command?  
chfn command is used to change the information listed from finger command.  
What runlevel does init 6 represent?  
Runlevel 6 is used to reboot the system.  
  
You are tasked to delete a user account with all his associated files including his home directory and mail folder. How will you do that ?  
#userdel -r [username]  
Above command will delete user account as well all his associated files including his home directory and mail folder.  
A user comes to you and complain that his system was starting fine in GUI mode, but from last reboot system is starting in command line interface. What is the most likely cause of the problem?  
In the /etc/inittab file, the default runlevel is probably set to 3, which tells it to start the system in command line.  
  
What files are updated when adding a group?  
/etc/group and /etc/gshadow files contains group information in Linux system. So these files would be updated every time whenever new group is added.  
  
What command is used to delete a group?  
The groupdel command will delete a group.  
  
What runlevel does init 3 represent?  
init3 represents rulevel 3. runlevel 3 is used for multiuser with networking.  
  
What command will display the directory path that is currently in use?  
pwd command will display the directory path that is currently in use.  
  
A user type 'cd ~ ' on command prompt, what this command will do?  
This command will move user to his or her home directory. ~ represents home directory in Linux.  
  
A user comes to you and complain that his system start fine, but as soon as it is almost loaded it reboot again. What is the most likely cause of the problem?  
In the /etc/inittab file, the default runlevel is probably set to 6, which tells it to reboot right after the system has started.  
  
Which command will list all the files and sub-directories in a directory and include the access rights?  
ls -l command will list all the files and sub-directories in a directory and include the access rights.  
  
Which command will list all the files in a directory including hidden files?  
ls -a command will list all the files in a directory including hidden files.  
  
What is the correct syntax for the move command?  
The correct syntax for the move command is  
mv [options] [source] [destination]  
  
Which character option with chmod command allows the execute-only permission if the file is a directory?  
The x option is used to allow execute only if the file is a directory.  
  
How will you display confirmation of the change of ownership of a file from rhuser1 to rhuser2?  
Use --verbose option with chown command. For example  
#chown --verbose rhuser2 /tmp/testfile  
  
Which command is used to un-mount a DVD?  
Use umount command to un-mount the DVD or CD or any other mounted media.  
  
What runlevel does init 0 represent?  
Runlevel 0 is used to halt /shutdown the system.  
  
Which command will display the total size of all files, without listing the files, in a user's home directory?  
The command du -c -s /home/user will display the total size of all files, without listing the files  
  
Which command will display the available space of each partition in megabytes (MB)?  
The command df -m will display the available space of each partition in MB.  
  
Hard drive in your system is full and you want new hard drive. However sales department would not approve the expenditure without proof. Which tool would you use get a proof?  
Use df command to justify the available free space in hard disk.  
  
A user comes to you and complain that his system start fine, but as soon as it is almost loaded it shuts down again. What is the most likely cause of the problem?  
In the /etc/inittab file, the default runlevel is probably set to 0, which tells it to shutdown right after the system has started.  
  
  
What command do you use to format a partition with a file system?  
You could use mkfs command to format partition with file system.  
  
Which command will assign IP address 192.168.1.1 and subnet mask 255.255.255.0 to eth0 network interface?  
ifconfig command can be used to assign IP address. Following command will do the given task  
ifconfig eth0 192.168.1.1 netmask 255.255.255.0  
  
Which option in fdisk will display the partition table?  
In fidisk utility, the "p" command will print the partition table.  
  
To create a recurring scheduled task, which Linux scheduling tool should you use?  
The cron command allows you to create recurring tasks  
  
What command can you use to enable an Ethernet network interface that has already been configured?  
To enable already configured interface use  
ifconfig [interface] up  
command. For example to up eth0 interface use following command  
#ifconfig eth0 up  
  
How will you decompress the demo.tar.gz file?  
To decompress use following command  
#tar -zxvf demo.tar.gz  
  
A core dump file contains this message, “Program terminated with signal 11, segmentation fault.” What does this message indicate?  
The core file will tell you what exactly caused the program to crash. So this message indicate that the program crashed because of a segmentation fault in memory.  
  
What command runs fdisk on the first ATA/IDE hard drive?  
The first ATA/IDE hard drive is hda, so the command would be  
# fdisk /dev/hda  
  
An application is creating several, very large core dump files. What should the administrator do if he has no intention of debugging these files?  
If administrator have no intention of keeping these files for debugging purposes, they should be deleted because they are wasting valuable disk space, and may cause system to run out of space.  
  
When checking the partition information on your hard drive with fdisk, you notice that one of the partitions is formatted as "Linux Swap" and is approximately 512MB in size. What is the purpose of this partition?  
The Linux swap file is used for virtual memory to store additional information that cannot fit into current memory. This swap file allows information to be cached on disk, and can be retrieved very quickly. Heavy use of the swap file indicates a low memory condition.  
  
What sort of kernel error can cause a Linux system to crash and write a memory core dump?  
Kernel panic error can cause a Linux system to crash. A kernel panic indicates that a kernel process has crashed. This is a very serious error that causes the entire Linux system to crash. These core dumps should be analyzed carefully to find the root cause of the problem.  
An administrator wants to assign an IP address of 192.168.1.10, a subnet mask of 255.255.255.0, and a broadcast address of 192.168.1.254 to eth1. What command will accomplish this task?  
Following command will do this task  
ifconfig eth1 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.254  
What command should you use to set up a job to run at 11:15 a.m. today?  
When you are only running the job once at the specified time, you should always use the at command. In this case following command will do the task  
#at 11:15  
  
You are tasked to set up a schedule to perform automatic checks of available disk space at the end of the day. How can you accomplish this task?  
To accomplish this task set up cron to run a script that will check the disk space daily at 7:00 p.m. The output will be e-mailed to the root account. You can compare the results from day to day to analyze disk space usage.  
Your cron file should look similar to the following:  
\* 19 \* \* \* df -kl  
  
As a administrator you need to terminate the sendmail process. How will you do that?  
First you need to determine the PID of sendmail so it can be killed.  
#ps -ef |grep sendmail  
Now you can use kill command to terminate the process associated with sendmail.  
You noticed a kernel error message during the boot process, but it scrolled before you could read this? What log file could you check to find out that message?  
The log file that contains kernel boot messages is /var/log/dmesg.  
  
You execute a command that is going to take a long time. How can you get back to your shell prompt to perform other task?  
You can use bg command to send a running process to the background.  
  
You need to kill all instances of Web Server? What command will you execute to do this?  
You can use killall httpd command to kill all httpd process. httpd process run web server.  
  
How can you list all running process?  
Use ps -ef command to list all running process.  
#ps -ef  
  
As a Linux admin you want to know what processes are being run by user sumit. What command can you use ?  
You can use #ps -au command to list all the process owned by user. Following command will do the assigned task  
#ps -au sumit  
  
Which log file keeps track of all user logins and logouts?  
/var/log/wtmp log file keeps track of all user logins and logouts.  
  
What is the first process that is run when a Linux system starts, and is responsible for starting all other system processes and services?  
The init process is the first process to be run. It is the parent process of all other Linux system processes, services, and daemons that are needed to run the system.  
  
Which command will you use to bring a process in foreground, which is running in the background?  
The fg command immediately moves the program to the foreground.  
  
An administrator has accidentally killed a core process. What is the result of this action?  
Killing a core process can potentially crash your system because many critical services rely on these core processes  
  
As a administrator you need to monitor the /var/log/messages file in real time to resolve the issue? How would you do that?  
You can use tail command with -f option. Following command will do the assigned task  
#tail -f /var/log/messages  
  
From the output of ps command how will you determine the ID number of the parent process of a particular program?  
PPID refers to the parent process identification number.  
  
While scanning the /var/log/messages file, you notices an error stating an authentication failure for root. What could this mean?  
Any failed login attempts for root are logged into the /var/log/messages file. It indicate that some has tried to login as root.  
As an administrator you noticed from top command that an unidentified process is using up all CPU and memory. You suspects that is a user's process that has run away. How should you fix this ?  
The process should be immediately killed before it consumes so many resources that the server cannot run properly, and therefore crash.  
  
What command can an administrator use to track real-time information on processes and the resources that they are using?  
The top command is used to monitor processes and resources in real-time.  
A developer with username sanjay has told you that one or his processes seem to be locked up and he cannot it. He reported that it a bug in his code and may quickly use up all CPU and RAM resources on the server. How will you tack the process and terminate it?  
Your first step is to identify the process, use ps command  
#ps -au sanjay  
Now run top command to compare the process running, and verify which one is using the most resources. After you have identified the problem process, you can use the kill command to terminate it. Because the user was unable to stop the process, you should probably force a kill signal to make sure that the process stops:  
#kill -9 [PID of process]  
Now, to verify that it has stopped, run the ps command again on the user:  
ps -au sanjay  
  
  
Why should you periodically update the kernel and package versions?  
To enhance the security of system you should ensure that you are using the latest versions kernel and software packages that contain the most recent security updates.  
During a recent strikes at office, several archive tapes of the system were damaged and ruined. What can you do to prevent the physical damage in future?  
You should store them at offsite.  
  
Why should you avoid the Telnet to administer a Linux system remotely?  
Telnet use most insecure method for communication. It send data across the network in plain text format. Someone easily find out the password using the network tool.  
  
A file is unable to be restored from tape due to several device and media errors. What is most likely the cause?  
Media errors usually indicate that the tape media is damaged, or that the tape drive heads need cleaning.  
  
Your FTP Server recently hacked. Due to the amount of damage, the entire server needs to be restored. How should you restore the original kernel system files?  
You cannot restore the entire operating system from tap back up device. So you should reinstall the core operating system, and then restore system configuration files and user data from tape backup device.  
  
Your company hire a contract employee for two months. What should the Linux administrator do to enhance security on the employee's account?  
While creating new user account for this user, administrator should set the expiration date for his account, so that if the employee leaves or does not have their contract renewed, the account will be automatically disabled.  
  
Which backup strategy only backs up files that have changed since the last full backup?  
Differential backup will backup files that have changed since the last full backup.  
Name a service which should you disable on a Linux Server which is acting as both a Web and FTP Server.  
The finger service should be disabled because a remote user can get important information about the system by using that command.  
  
Why it is recommended to store backup tapes to an offsite storage facility?  
Because this will prevent the backup taps from being destroyed during a natural disaster at the server site. It also prevents the tapes from being stolen.  
  
A newbie enabled the root session for FTP server. is it ok?  
No, he has put the security of entire server on risk. You should disable to root session as soon as possible.  
  
A user complains you that he is unable to set '123' as his password. Why would not the system allow this password?  
There would be a minimum length rule for password, which is blocking user to use this password. Default minimum length rule for password is six characters. It means a user cannot have password less than six characters.  
  
Your company is running Web Server. One dedicate account holder customer complains that his visitors are able to scan the directory tree. Which directive would you configure to stop web server from listing the directory?  
You should remove / comment the "Options Indexes" directive from the main configuration file ' httpd.conf' of the web server. This is a security measure so that remote users can’t scan the directory tree of the server looking for security holes. Server won’t show directory listings if requested by a user.  
  
What type of backup strategy can you use to fully back up a system every night?  
You can use full backup strategy that will always perform a full backup of all files. This takes much more time and space than other methods, but is it the most complete method and allows for easy file restoration.  
  
How can you enhance the security of password file?  
Linux keep user account information in a text file called /etc/passwd. This file also store one way encrypted password. This file is accessed by several tools to get user information, so file need to world readable. This is a security risk. To minimize the security risk you can use shadow password format. This method save account information in regular file /etc/passwd. However, the password is stored as a single "x" character (not actually stored in this file). A second file, called "/etc/shadow", contains encrypted password as well as other information such as account or password expiration values, etc. The /etc/shadow file is readable only by the root account and is therefore less of a security risk  
  
What command should be used to make a tar archive to a disk file system located in /mnt/backup?  
The correct command is tar -cvf /mnt/backup. The /mnt/backup directory should be on another machine to be fully effective as a backup strategy.  
You have just finished the installation of sever. This server is going to be use as file server. Default installation have send mail service running, while this server will never send any e-mails. How should you deal with send mail service?  
You should disable the send mail service if server is not being used for mail purpose. Leaving them running can increase the chance of a security vulnerability being exploited, and unauthorized use of sendmail relay.  
  
What command can you use to back up an entire file system most efficiently?  
The easiest command to use to back up an entire file system is the dump command. Files can be restored from a dump operation by using the restore command.  
Which necessary steps should you take to enhance the security of server just after the initial installation?  
Kernel and packages should be upgraded to the latest versions.  
Unnecessary services and daemons should be disable.  
Enable and configure firewall  
Set a complex password policy.  
  
While auditing user accounts, an administrator notices that one of the users has a blank password. What should he do to the account?  
To prevent further use of the account, which is an immediate security risk, disable it and set a temporary password for the user for the next time they login.  
Which backup strategy backs up all files that have changed since the last backup?  
An incremental backup will only back up files that have changed since the last backup.  
  
Your company has terminated a server administrator. What is first thing as an administrator should you do to enhance the security?  
Because the server administrator knows the root password for the server, it should be changed immediately to prevent them from tampering with the system.  
You are setting up an FTP server. Only company employees are allowed to use the FTP services. What should you configure on the FTP server to enhance security?  
You should disable the anonymous FTP account, so that only users with a username and password can access the system.  
What is the location of system configuration files that should be backed up on a regular basis?  
The /etc directory contains most of the Linux system configuration files.  
  
Which permission allows a user to run an executable with the permissions of the owner of that file?  
The Set-User-ID is a special permission that allows a user to run an executable with the permissions of the owner of that file.  
What command can you use to make a tape archive file of a /home directory, and send it to the /dev/tape device?  
The correct command is tar -cvf /dev/tape /home.  
The -xvf option is used to extract files from an archive.  
  
Employees at your company are lazy in changing the password. As a system administrator what can you do to minimize the security risk?  
You can setup a password policy which enforce user to change his password after a specific time periods.  
Which program should you use to connect a system remotely?  
You should always use SSH to connect a system remotely. SSH is a secure method that encrypts the entire session.  
  
To save disk space, an administrator wants to backup files, and then remove them from the server permanently. What kind of backup operation is this?  
An archive operation will take the files, back them up to a device, and then remove the files from the original server.  
What does firewall do?  
Firewall is a device or service which can be used to protect the network or system from other outside networks.  
  
  
Due to power fluctuation, your system starts up from a powered off state. You receive a warning error stating that the machine was not shut down properly, and fsck will be run. What is the cause of this message?  
If your hard drive file systems are not unmounted properly, the fsck utility will automatically run the next time the system is started to fix any inconsistencies before they are mounted again. If they are not fixed, the file system can quickly become corrupt.  
  
A junior system administrator is trying to read through a large log file using the cat command. Because it is so large, the cat command scrolls the file right to the end without allowing the start of the file to be read. What command can he be used to more easily read the file?  
He can use less command instead of using cat command, which allows him to scroll through the file.  
  
When you try to boot a Linux system, you receive a message stating that it canot mount the /home partition because of errors. While debugging , you found that it occur due to data error. What can you do to fix the problem?  
You can use fsck utility that enable you to recover from the errors.  
  
During the bootup of a Linux system, there is no output on the monitor, the machine beeps, and then halts the boot-up process. What is the most likely cause of the problem?  
If the system would not even get to the POST stage, the problem is most likely with the motherboard itself. You should count and compare the number of beeps to the BIOS manual in order to determine which specific component failed.  
  
Which utility could you use to repair the corrupted file system?  
You can use fsck to repair the corrupted file system.  
  
What must you do before performing fsck on a file system?  
The fsck utility can only run on a file system that is unmounted. If it were active, fsck would not be able to properly repair the drive, and may cause further corruption.  
  
A Linux administrator wants to review the messages that scrolled up the screen during a system boot. How can this be accomplished?  
The boot kernel messages are saved to the log file /var/log/dmesg. He can check this file.  
A user complains you that his system was running fine, before he rebooted. When it starts up, no display appears on the screen and the system is beeping. What may this indicate?  
Because the system was running fine before reboot and during the it got problem even before the operating system is loaded, the problem is hardware-based, and is most likely caused by a problem with the system board.  
  
A user has sent an e-mail, but within minutes the e-mail is returned stating that the address could not be found. What is the most likely cause of the error?  
If the e-mail was returned, all mail services are working properly, but the destination e-mail address was wrong.  
Your system crashed and being restarted, but a message appears, indicating that the operating system cannot be found. What is the most likely cause of the problem ?  
This kind of problem most likely to be associated with hard disk. There might be some issue with either MBR or hard disk.  
  
A user can not access a remote server. Which command he can use to verify that remote server is up?  
He can use ping command to check whatever remote server is up or not.  
  
A newbie administrator is having tough time to locate the httpd.conf file. What command line tool he can use to find file?  
He should first try with locate command. find command would be his next tool.  
  
A user has decided to come into work overnight to get some work done. Unfortunately, he is not able to login, even though he is using his proper name and password. What is the most likely cause of the problem?  
In high security environments some organizations choose to implement time restrictions on accounts, so user would not be able to login after office time.  
  
A Linux administrator is noticing odd system behavior. Which log file should he check to find general system log messages?  
The general log stored in /var/log/messages file.  
  
Instead of properly shutting down a Linux system, an user mistakenly just turned the machine off with the on/off switch. What will happen when the system restarts?  
When the system shuts down abnormally and the file systems are not properly mounted, the fsck utility will automatically check the disks for errors and inconsistencies in order to repair them.  
  
A newbie system admin is having trouble with the options for a particular command. What is the best resource to use for information on the command?  
He can use man command to get detail of the options. A quick way to get help about options is to use --help option. Most Linux command support this option and return with brief information on how to use that command.  
  
You are tasked to examine a log file in order to find out why a particular application keep crashing. Log file is very lengthy, which command can you use to simplify the log search using a search string ?  
You can use grep command to output the log file. You can specify the keyword of desired application to look for, grep command than displays all instances of that word in log file.  
  
A user is trying to check his mail by using the pop3 protocol and port 143. But mail program could not connect to the mail server to retrieve mail. What is the most likely cause of the problem?  
User is using wrong port number. Port number 143 is used for imap, he should use port 110 instead of 143.  
  
A developer is constantly making changes in his applications source file, then running application to see if is throwing any error. Which command can he use to see the log file in real time, instead of reopening the log file each time?  
He can use tail command with -f options to see a file being updated in real time. He do not need to reopen the file to see any changes.  
An administrator has made changes to a daemon's configuration file. When he checks the process, it is still running with old behavior. What is the reason behind it?  
He need to restart the service to process can read and implement the new configuration.  
  
An application process has just failed on a Linux system. What should you examine first to find out the root of the problem?  
When an application fails, the first thing that you should do to help troubleshoot the problem is to examine the application logs for the particular error that caused the application to fail.  
  
During a software package installation, an error occurs warning that a certain library is missing, and the installation aborts. What is the most likely cause of the problem?  
Many software packages are dependent on other programs to function properly. If these dependencies do not exist, you must install them before installing your software package.  
  
What command should be used to show the first 10 lines of a file?  
The command to show the first 10 lines of a file is head -100 filename.  
  
What command can an administrator use to see the status of a print queue?  
The lpq command can be used to see the status of a print queue.  
  
  
1. What is ldd?  
  
List dynamic dependencies – print shared library dependencies  
  
Eg: – # vim new.c  
  
# gcc new.c –o new  
  
# ldd new  
  
  
2. What is the command to uninstall processes in Linux?  
  
rpm –e sendmail  
-e – remove  
  
3. What is the command for finding the highest memory occupied file in Linux?  
  
du –ah / | sort –n –r | head –n 1  
  
du – estimate file space usage  
-a – write counts for all files, not just directories  
-h – print sizes in human readable format (eg. 1K 234M 2G)  
  
sort – sort lines of text files  
-n – compare according to string numerical value  
-r – reverse the result of comparisons  
  
head – output the first part of files  
-n – number of lines  
  
4. What are the Linux boot files?  
  
1./boot/grub/grub.conf: contains boot disk parameters  
2./etc/fstab: contains File systems which need to mount at boot time  
3./etc/initab: Contains default run level  
4./etc/init.d/rc.d/rcN.d: This is a dir it contains  
  
5. Difference between swap partition and swap file?  
  
Swap partition is maintained as a separate partition. Same swap partition can be used for two OS within single machine.  
  
Suppose if the system crashes, there is a chance to recover or it may not  corrupt the partition.  
  
Less fragmented.  
  
Where as swap file takes very less space. We can increase the space very easily, compared to swap partition. Swap file system fragmented.  
  
If  the system crashes then there is a huge chance to lost the swap file system.  
  
6. A file which is not deleted by normal user and also root (using rm), for that type of file how we delete it?  
  
Using chattr command, we need to change the attributes and then we remove using rm command.  
  
Eg: – chattr -iIu example  
rm -rf example  
  
7. Difference between nfs soft and hard mounting points?  
  
Hard mount option: – If the client fails to access the server, then the connection hangs and once the system is up then it will again access the server.  
  
Soft: – If the client failed to connect the server, it immediately gives the error report and closes the connection.  
  
8. If we transfer 100 files by ftp to remote server, how to know the files are successfully transfer or some file are not transferred?  
  
ftp>mput 1 2 3 …. 100  
ftp> ls –l  
  
9. I know ssh, telnet, dns,apache all are worked on TCP/UDP but i want to know any one service which are working on UDP only?  
  
snmptrap 162/udp  
snmptrap – simple network management protocol trap  
snmptrapd is an SNMP application that receives and logs  
  
10. I want to built a fire wall using iptables. My condition is ” inbound to 192.168.0.2 with a port of 80 from 172.168.0.1 should accept”  
  
iptables –A INPUT –p tcp –dport 80 –s 172.168.0.1 –d 192.168.0.2 –j ACCEPT  
  
11. I want to see how many interfaces (Ethernet cards) are working using single command?  
  
ifconfig  
  
12. What is the status code 403,404 represented in apache server?  
  
403 represent forbidden error, means if a file misses some selinux security context.  
  
404 represent that there is a cgi script missing or web pages missing.  
  
13. How to monitor ports in a linux machine, with single command?  
  
nmap localhost  
  
14. In my linux machine, i lost /etc/passwd file and /etc/shadow file, then how can i recover it?  
  
Normally in linux we must have backup by default for /etc/passwd and /etc/shadow files  
  
/etc/passwd —> /etc/passwd-  
/etc/shadow —> /etc/shadow-  
  
from there we can copy or restore. If both are not available. Then follow below steps:  
  
1. reboot  
2. Single user mode [ single init=/bin/bash ]  
3. pwconv  
4. check /etc/passwd and /etc/shadow files are there  
5. sync  
6. init 3 or reboot with init 3  
  
15. what r the different command to check ram,process and hdd of linux machine  
  
To check ram in your system:  
#free  
  
To check process  
#ps  
#top  
  
To check hdd  
#fdisk  
#sfdisk -l  
  
16.If i run ls command it will show me the junk output what is problem and how to resolve it  
  
Set your terminal setting by stty and before that, export ls command to PATH variable  
  
17. WHAT IS THE MEANING OF AIX  
  
AIX (Advanced Interactive eXecutive) is an open operating system from IBM which is based on a version of UNIX. AIX/ESA was designed for IBM’s System/390 or large server hardware platform. AIX/6000 is an operating system that runs on IBM’s workstation platform, the RISC System/6000.  
  
18. Why ls -F dev/log file output indicate as = sign at end of the file name?  
  
Standard output  
  
19. What is nis server?  
  
NIS is a service that provides any user on a network with the same working environment irrespective of the system on that network, which has been used for login purpose.  
  
For example if NIS server is set up in a single system and configured to hold user accounts and their passwords and access information. Then any user on that network can login to his/her account from any system (with nis client running) on that configured network. This gives a look and feel that the user is logged into his/her own system. But actually it’s the account on the NIS server that is mounted on the local sytem user login.  
  
20. What command can you use to review boot messages?  
  
Dmesg  
  
21. Who invented unix?  
  
Unix was created in 1969 by Ken Thompson and Dennis Ritchie at Bell Laboratories.  
  
22. Write a cron entry for the following scenario:- At 10:30 AM for every Sunday of every 1st month of a quarter.  
  
30 10 \* 1-12/3 7  
  
23. What is the difference between RHEL4 & RHEL5?  
  
RHEL4: No yum server, Selinux, secure, no cd key  
RHEL5: yum server, advanced selinux, more secure, virtualization  
  
24. What is the command to make a process to run in the foreground from background?  
  
When the process is running, press “control+Z”. Now at the command prompt, type “bg”  
  
25. What are the init levels in Linux?  
  
7 level  
  
  
  
1. 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.  
  
  
2. How to view crond status? If it’s show service is not found.  
  
Service crond restart  
  
3. My clients are getting services from servers but how to know which client is using which service. is there any files to keep information about these? Clients used ftp, nis, samba, apache, squid, nfs and mail services how to know how many users got service from server side with date, time and client system ip?  
  
Mail server – /var/log/mail/maillog [RedHat,centos]  
ssh – /var/log/secure  
Apache – /var/log/http/access.log  
nfs – /var/lib/nfs/rmtab  
  
4. How to FTP user access other directory except his own home directory?  
  
vim /etc/vsftpd/vsftpd.conf  
Chroot\_list\_enable=yes  
  
5. What are the Linux-based security tools?  
  
Selinux  
Firewall  
iptables  
Tcp-wrappers  
  
6. 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  
  
7. What is a command to display top 10 users who are using huge space?  
  
du -sh /home/\* | sort -r | head -10  
  
8. How do find all failed login attempts via ssh?  
  
tail -f /var/log/secure | grep Failed  
  
9. How do you configure Linux system as a router?  
  
vim /etc/sysctl.conf  
net.ipv4.ip\_forward=1  
system-config-network  
eth0 192.168.1.120 eth0:1 172.24.0.1  
255.255.255.0 255.255.0.0  
172.24.0.1 192.168.1.120  
  
10. 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 >  
  
11. 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. Ext3 has three levels of journalling. Metadata (ie. internal filesystem structures) are always journalled, so that the filesystem itself is never corrupted. How ordinary data is written to the file system is controllable, though. The default option is the “ordered” mode, which causes file contents to be written to the filesystem before metadata is even committed to the journal. The highest reliable mode is called the “journal” mode, which causes file data to be committed to the journal before it is flushed to its final place, like the metadata. The least reliable mode, but rumoured to be the fastest, is called the “writeback” mode, which makes no promises at all regarding the consistency of file data. Only metadata is output reliably in writeback mode. So as for anything else, it’s mainly a matter of priority. If you don’t want ultimate speed, go with ext3. If you need the highest speed that is theoratically aquirable though, then go with ext2. For that to be effective you’ll probably need a really advanced hard drive controller, though.  
  
12. As the system administrator you need to review Bob’s cronjobs. What command would you use?  
  
crontab –lu Bob  
  
13. What command is used to remove the password assigned to a group?  
  
gpasswd –r groupname  
  
14. What are the different RAID levels?  
  
♣ RAID level 0  
♣ RAID level RAID level 1  
♣ RAID level 2  
♣ RAID level 3  
♣ RAID level 4  
♣ RAID level 5  
♣ RAID level 6  
♣ RAID level 10  
♣ RAID level 50  
  
15. How do you create a swapfile?  
  
dd if=/dev/zero of=/swapfile bs=1024 count=200M  
mkswap /swapfile  
swapon /swapfile  
  
16. 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.  
  
17. 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 gurantees 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 then it takes for TCP to establish a connection.  
  
18. 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 Linux / UNIX file system.  
  
fsck  
  
19. What is the command to remove Lvm ,Pv and vg  
  
1st remove the entry on /etc/fstab file & save – quit.  
2nd remove LVM – lvremove lvname  
3rd remove VG – vgremove vgname  
4th remove PV – pvremove pvname  
  
20. How to create SAMBA server in fedora 9 Linux?  
  
yum install samba -y  
  
yum install samba-swat –y  
  
vi /etc/samba/smb.conf  
  
comment = windows sharing  
path = path/your/share/directory  
valid users = surendra  
writable = yes  
browseable = yes  
  
then type testparm for code testing.  
  
smbpasswd -a username  
smbpasswd -e username  
  
service smb restart  
chkconfig smb on  
  
21. How to schedule cron backup to run on 4th Saturday of month?  
  
\* \* \* \* 6 weekdaynum 4 && sh /backup/test.sh  
  
22. What is an inode?  
  
ext2 and ext3 file systems keep a list of the files they contain in a table called an inode table. The inode is referenced by its number. This is unique within a file system.  
  
The inode contains the metadata about files. Among the data stored in the inode is  
  
File type  
  
File permissions  
  
Link count  
  
User ID number of the file owner and the group ID number of the associated group  
  
Last modification time  
  
Location of the data on the hard disk  
  
Other metadata about the file  
  
ls -li – view inode number only  
  
stat /etc/passwd – view inode details  
  
23. How to see unallocated hard disk space on linux  
  
df -h  
  
24. How do u find remote machine operating system and version?  
  
nmap -A –v 192.168.1.100  
  
25. How do you port scanning with netstat command?  
  
netstat –an  
  
26. Linux system monitoring Tools?  
  
top – Process Activity Command  
vmstat – System Activity, Hardware and System Information  
w – Find out Who Is Logged on And What They Are Doing  
Uptime – Tell How Long the System Has Been Running  
ps – Displays the Processes  
free – Memory Usage  
iostat – Average CPU Load, Disk Activity  
sar – Collect and Report System Activity  
mpstat – Multiprocessor Usage  
pmap – Process Memory Usage  
  
27. 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  
28. 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.  
  
29. Important port no:  
  
NFS – 2049  
FTP – 21  
SAMBA – 445  
SSH – 22  
DNS – 53  
POP3 – 110  
IMAP – 143  
HTTPS – 443  
HTTP – 80  
  
30. How do u extract files from iso cd images in linux?  
  
mount –o loop disk1.iso /mnt/iso  
  
  
1)Give me 15 commands which you use frequently  
  
Depends on the environment you work. Some examples are  
  
mkdir — For creating folders( use -p option to create multiple folders at a time)  
ls –List folders/files( check what ls -1 do)  
  
top — To monitor system activities  
  
lsof –To check whats happening on the server and which process open which file.  
  
netstat -tcp –Gives you complete picture about network connection details.  
  
vnstat –Gives you Network band width statics  
  
sh –For running shell scripts  
  
history –For monitoring the commands executed by users  
  
cd –For changing directories  
  
vi –-For editing configuration files.  
  
chmod –To change permissions of folders and files.  
  
mount –For mounting formated partitions.  
  
service –For start/restart/stop a service.  
  
chkconfig –For permanent on/off a service.  
  
fdisk -l –To list all the partitions  
  
This is my own list, you can have your list.  
  
2)Give me some commands for user management.  
  
last, chage, chsh, lsof, chown, chmod, useradd, userdel, newusers.  
  
3)Give me syntax checking commands for following services  
  
DNS, SAMBA, Apache etc  
  
4)What is the command to do password less logins to other machines.  
  
expect and ssh-keygen  
  
5)Give me some security monitoring related commands.  
  
lsof, netstat, top, ps -ef, tail, last, tcpdump, sestatus, history, w.  
  
6)What is the difference between man, info, whatis commands and a –help option for a command?  
  
whatis gives you one line answer.  
  
–help option for a command gives you one line answers for each option supported by a command  
  
man command gives you medium size info.  
  
info command gives full details about a commands, lots and lots of information about a command.  
  
  
  
1. Have you heard of iptables and firewall in Linux? Any idea of what they are and for what it is used?  
  
Answer : I’ve been using iptables for quite long time and I am aware of both iptables and firewall. Iptables is an application program mostly written in C Programming Language and  
is released under GNU General Public License. Written for System administration point of view, the latest stable release if iptables 1.4.21.iptables may be considered as firewall   
for UNIX like operating system which can be called as iptables/netfilter, more accurately. The Administrator interact with iptables via console/GUI front end tools to add and define   
firewall rules into predefined tables. Netfilter is a module built inside of kernel that do the job of filtering.  
Firewalld is the latest implementation of filtering rules in RHEL/CentOS 7 (may be implemented in other distributions which I may not be aware of). It has replaced iptables interface   
and connects to netfilter.  
  
2. Have you used some kind of GUI based front end tool for iptables or the Linux Command Line?  
  
Answer : Though I have used both the GUI based front end tools for iptables like Shorewall in conjugation of Webmin in GUI and Direct access to iptables via console.And I must admit   
that direct access to iptables via Linux console gives a user immense power in the form of higher degree of flexibility and better understanding of what is going on in the background, if not anything other. GUI is for novice administrator while console is for experienced.  
  
3. What are the basic differences between between iptables and firewalld?  
  
Answer : iptables and firewalld serves the same purpose (Packet Filtering) but with different approach. iptables flush the entire rules set each time a change is made unlike firewalld.  
Typically the location of iptables configuration lies at ‘/etc/sysconfig/iptables‘ whereas firewalld configuration lies at ‘/etc/firewalld/‘, which is a set of XML files.Configuring a  
XML based firewalld is easier as compared to configuration of iptables, however same task can be achieved using both the packet filtering application ie., iptables and firewalld.  
Firewalld runs iptables under its hood along with it’s own command line interface and configuration file that is XML based and said above.  
  
4. Would you replace iptables with firewalld on all your servers, if given a chance?  
  
Answer : I am familiar with iptables and it’s working and if there is nothing that requires dynamic aspect of firewalld, there seems no reason to migrate all my configuration from  
iptables to firewalld.In most of the cases, so far I have never seen iptables creating an issue. Also the general rule of Information technology says “why fix if it is not broken”.   
However this is my personal thought and I would never mind implementing firewalld if the Organization is going to replace iptables with firewalld.  
  
5. You seems confident with iptables and the plus point is even we are using iptables on our server.  
  
What are the tables used in iptables? Give a brief description of the tables used in iptables and the chains they support.  
  
Answer : Thanks for the recognition. Moving to question part, There are four tables used in iptables, namely they are:  
Nat Table  
Mangle Table  
Filter Table  
Raw Table  
Nat Table : Nat table is primarily used for Network Address Translation. Masqueraded packets get their IP address altered as per the rules in the table. Packets in the stream traverse Nat Table only once. ie., If a packet from a jet of Packets is masqueraded they rest of the packages in the stream will not traverse through this table again. It is recommended not to filter in this table. Chains Supported by NAT Table are PREROUTING Chain, POSTROUTING Chain and OUTPUT Chain.  
  
Mangle Table : As the name suggests, this table serves for mangling the packets. It is used for Special package alteration. It can be used to alter the content of different packets and their headers. Mangle table can’t be used for Masquerading. Supported chains are PREROUTING Chain, OUTPUT Chain, Forward Chain, INPUT Chain, POSTROUTING Chain.  
  
Filter Table : Filter Table is the default table used in iptables. It is used for filtering Packets. If no rules are defined, Filter Table is taken as default table and filtering is done on the basis of this table. Supported Chains are INPUT Chain, OUTPUT Chain, FORWARD Chain.  
  
Raw Table : Raw table comes into action when we want to configure packages that were exempted earlier. It supports PREROUTING Chain and OUTPUT Chain.  
  
6. What are the target values (that can be specified in target) in iptables and what they do, be brief!  
  
Answer : Following are the target values that we can specify in target in iptables:  
ACCEPT : Accept Packets  
QUEUE : Paas Package to user space (place where application and drivers reside)  
DROP : Drop Packets  
RETURN : Return Control to calling chain and stop executing next set of rules for the current Packets in the chain.  
  
  
7. Lets move to the technical aspects of iptables, by technical I means practical.  
  
How will you Check iptables rpm that is required to install iptables in CentOS?.  
  
Answer : iptables rpm are included in standard CentOS installation and we do not need to install it separately. We can check the rpm as:  
# rpm -qa iptables  
  
iptables-1.4.21-13.el7.x86\_64  
If you need to install it, you may do yum to get it.  
  
# yum install iptables-services  
8. How to Check and ensure if iptables service is running?  
  
Answer : To check the status of iptables, you may run the following command on the terminal.  
# service status iptables [On CentOS 6/5]  
# systemctl status iptables [On CentOS 7]  
If it is not running, the below command may be executed.  
  
---------------- On CentOS 6/5 ----------------   
# chkconfig --level 35 iptables on  
# service iptables start  
  
---------------- On CentOS 7 ----------------   
# systemctl enable iptables   
# systemctl start iptables   
We may also check if the iptables module is loaded or not, as:  
  
# lsmod | grep ip\_tables  
9. How will you review the current Rules defined in iptables?  
  
Answer : The current rules in iptables can be review as simple as:  
# iptables -L  
Sample Output  
  
Chain INPUT (policy ACCEPT)  
target     prot opt source               destination           
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED  
ACCEPT     icmp --  anywhere             anywhere              
ACCEPT     all  --  anywhere             anywhere              
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh  
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited  
  
Chain FORWARD (policy ACCEPT)  
target     prot opt source               destination           
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited  
  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source               destination  
10. How will you flush all iptables rules or a particular chain?  
  
Answer : To flush a particular iptables chain, you may use following commands.  
  
# iptables --flush OUTPUT  
To Flush all the iptables rules.  
  
# iptables --flush  
11. Add a rule in iptables to accept packets from a trusted IP Address (say 192.168.0.7)  
  
Answer : The above scenario can be achieved simply by running the below command.  
# iptables -A INPUT -s 192.168.0.7 -j ACCEPT   
We may include standard slash or subnet mask in the source as:  
  
# iptables -A INPUT -s 192.168.0.7/24 -j ACCEPT   
# iptables -A INPUT -s 192.168.0.7/255.255.255.0 -j ACCEPT  
12. How to add rules to ACCEPT, REJECT, DENY and DROP ssh service in iptables.  
  
Answer : Hoping ssh is running on port 22, which is also the default port for ssh, we can add rule to iptables as:  
To ACCEPT tcp packets for ssh service (port 22).  
  
# iptables -A INPUT -s -p tcp --dport 22 -j ACCEPT   
To REJECT tcp packets for ssh service (port 22).  
  
# iptables -A INPUT -s -p tcp --dport 22 -j REJECT  
To DENY tcp packets for ssh service (port 22).  
  
  
# iptables -A INPUT -s -p tcp --dport 22 -j DENY  
To DROP tcp packets for ssh service (port 22).  
  
  
# iptables -A INPUT -s -p tcp --dport 22 -j DROP  
13. Let me give you a scenario. Say there is a machine the local ip address of which is 192.168.0.6. You need to block connections on port 21, 22, 23, and 80 to your machine. What will you do?  
  
Answer : Well all I need to use is the ‘multiport‘ option with iptables followed by port numbers to be blocked and the above scenario can be achieved in a single go as.  
# iptables -A INPUT -s 192.168.0.6 -p tcp -m multiport --dport 21,22,23,80 -j DROP  
The written rules can be checked using the below command.  
  
# iptables -L  
  
Chain INPUT (policy ACCEPT)  
target     prot opt source               destination           
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED  
ACCEPT     icmp --  anywhere             anywhere              
ACCEPT     all  --  anywhere             anywhere              
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh  
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited  
DROP       tcp  --  192.168.0.6          anywhere             multiport dports ssh,telnet,http,webcache  
  
Chain FORWARD (policy ACCEPT)  
target     prot opt source               destination           
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited  
  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source               destination  
  
  
  
  
1. What is a Computer Network?  
  
Ans: A computer network is a connection network between two or more nodes using Physical Media Links viz., cable or wireless in order to exchange data over pre-configured services and Protocols. A computer network is a collective result of – Electrical Engineering, Computer Science, Telecommunication, Computer Engineering and Information Technology involving their theoretical as well as practical aspects into action. The most widely used Computer Network of Today is Internet which supports World Wide Web (WWW).  
  
2. What is DNS?  
  
Ans: DNS stands for Domain Name System. It is a Naming System for all the resources over Internet which includes Physical nodes and Applications. DNS is a way to locate to a resource easily over a network and serves to be an essential component necessary for the working of Internet.  
  
It is always easy to remember xyz.com that to remember its IP(v4) address 82.175.219.112. The condition gets more worse when you have to deal with IP(v6) address 2005:3200:230:7e:35dl:2874:2190. Now think of the scenario when you have a list of 10 most visited resource over Internet? Didn’t the things get more worse to remember? It is said and proved scientifically that humans are good in remembering names as compared to numbers.  
  
The Domain Name System functions to assign Domain Names by mapping corresponding IP addresses and works in a Hierarchical and Distributed Fashion.  
  
3. What are IPv4 and IPv6? Who manages these?  
  
Ans: IPv4 and IPv6 are the versions of Internet Protocol which stands for Version4 and Version6 respectively. IP address is an unique value which represents a device over network. All the device over Internet must have a valid and Unique address to function normally.  
  
IPv4 is a 32 bit numeric representation of devices over Internet, most widely used till date. It supports upto 4.3 billion (4,300,000,000) unique IP addresses. Seeing the continuing growth of Internet with more and more devices and users linking to Internet there was a need of better version of IP address which could support more users. Hence came IPv6 in 1995. An example of IPv4 is:  
  
82.175.219.112  
IPv6 is a 128 bit numeric representation of devices over Internet. It supports as much as 340 trillion, trillion, trillion (340,000,000,000,000,000,000,000,000,000,000,000,000) unique IP address. This is sufficient to provide more than a billion of IP addresses to every human being on earth. Sufficient for centuries. With the invent of IPv6, we need not to bother about depleting Unique IP addresses. An example of IPv6 is:  
  
 2005:3200:230:7e:35dl:2874:2190  
4. Give a brief description of PAN, LAN, HAN, SAN, CAN, MAN, WAN, GAN.  
  
Ans: PAN stands for Personal Area Network. It is a connection of Computer and Devices that are close to a person VIZ., Computer, Telephones, Fax, Printers, etc. Range Limit – 10 meters.  
  
LAN stands for Local Area Network. LAN is the connection of Computers and Devices over a small Geographical Location – Office, School, Hospital, etc. A LAN can be connected to WAN using a gateway (Router).  
  
HAN stands for House Area Network. HAN is LAN of Home which connects to homely devices ranging from a few personal computers, phone, fax and printers.  
  
SAN stands for Storage Area Network. SAN is the connection of various storage devices which seems local to a computer.  
  
CAN stands for Campus Area Network, CAN is the connection of devices, printers, phones and accessories within a campus which Links to other departments of the organization within the same campus.  
  
MAN stands for Metropolitan Area Network. MAN is the connection of loads of devices which spans to Large cities over a wide Geographical Area.  
  
WAN stands for Wide Area Network. WAN connects devices, phones, printers, scanners, etc over a very wide geographical location which may range to connect cities, countries and ever continents.  
  
GAN stands for Global Area Network. GAN connects mobiles across the globe using satellites.  
  
5. What is POP3?  
  
Ans: POP3 stands for Post Office Protocol Version3 (Current Version). POP is a protocol which listens on port 110 and is responsible for accessing the mail service on a client machine. POP3 works in two modes – Delete Mode and Keep Mode.  
  
Delete Mode: A mail is deleted from the mailbox after successful retrieval.  
Keep Mode: The Mail remains Intact in the mailbox after successful retrieval.  
6. What is the criteria to check the network reliability?  
  
Ans: A network Reliability is measured on following factors.  
  
Downtime: The time it takes to recover.  
Failure Frequency: The frequency when it fails to work the way it is intended.  
7. What is a router?  
  
Ans: A router is a physical device which acts as a gateway and connects to two network. It forwards the packets of data/information from one network to another. It acts as an interconnection Link between two network.  
  
8. What are the use of cross and standard cables? Where do you find their usages?  
  
Ans: A Network cable may be crossover as well as straight. Both of these cables have different wires arrangement in them, which serves to fulfill different purpose.  
  
Area of application of Straight cable  
  
Computer to Switch  
Computer to Hub  
Computer to Modem  
Router to Switch  
Ares of application of Crossover cable  
  
Computer to Computer  
Switch to Switch  
Hub to Hub  
9. What do you mean by Bandwidth?  
  
Ans: Every Signal has a limit of its upper range and lower range of frequency of signal it can carry. This range of limit of network between its upper frequency and lower frequency is termed as Bandwidth.  
  
10. What do you mean by MAC address? Does it has some link or something in common to Mac OS of Apple?  
  
Ans: MAC stands for Media Access Control. It is the address of the device identified at Media Access Control Layer of Network Architecture. Similar to IP address MAC address is unique address, i.e., no two device can have same MAC address. MAC address is stored at the Read Only Memory (ROM) of the device.  
  
MAC Address and Mac OS are two different things and it should not be confused with each other. Mac OS is a POSIX standard Operating System Developed upon FreeBSD used by Apple devices.  
  
That’s all for now. We will be coming up with another articles on Networking series every now and then. Till then, don’t forget to provide us with your valuable feedback in the comment section below.  
  
  
  
1. What do you mean by Proxy Server? What is the use of Proxy Server in Computer Networks?  
  
Answer : A Proxy Server refers to physical machine or Application which acts intermediate between client and resource provider or server. A client seeks for file, page or data from the the proxy server and proxy server manages to get the requested demand of client fulfilled by handling all the complexities in between.  
Proxy servers are the backbone of WWW (World Wide Web). Most of the proxies of today are web proxies. A proxy server handles the complexity in between the Communication of client and Server. Moreover it provides anonymity on the web which simply means your identity and digital footprints are safe. Proxies can be configured to allow which sites client can see and which sites are blocked.  
  
2. What is Squid?  
  
Answer : Squid is an Application software released under GNU/GPL which acts as a proxy server as well as web cache Daemon. Squid primarily supports Protocol like HTTP and FTP however other protocols like HTTPS, SSL,TLS, etc are well supported. The feature web cache Daemon makes web surfing faster by caching web and DNS for frequently visited websites. Squid is known to support all major platforms including Linux, UNIX, Microsoft Windows and Mac.  
3. What is the default port of squid and how to change its operating port?  
  
Answer : The default port on which squid runs is 3128. We can change the operating port of squid from default to any custom unused port by editing its configuration file which is located at /etc/squid/squid.conf as suggested below.  
Open ‘/etc/squid/squid.conf’ file and with your choice of editor.  
  
# nano /etc/squid/squid.conf  
Now change this port to any other unused port. Save the editor and exit.  
  
http\_port 3128  
Restart the squid service as shown below.  
  
# service squid restart  
4. You works for a company the management of which ask you to block certain domains through squid proxy server. What are you going to do?  
  
Answer : Blocking domain is a module which is implemented well in the configuration file. We just need to perform a little manual configuration as suggested below.  
a. Create a file say ‘blacklist’ under directory ‘/etc/squid’.  
  
# touch /etc/squid/blacklist  
b. Open the file ‘/etc/squid/blacklist’ with nano editor.  
  
# nano /etc/squid/blacklist  
c. Add all the domains to the file blacklist with one domain per line.  
  
.facebook.com  
.twitter.com  
.gmail.com  
.yahoo.com  
...  
d. Save the file and exit. Now open the Squid configuration file from location ‘/etc/squid/squid.conf’.  
  
# nano /etc/squid/squid.conf  
e. Add the lines below to the Squid configuration file.  
  
acl BLACKLIST dstdom\_regex -i “/etc/squid/blacklist”  
http\_access deny blacklist  
f. Save the configuration file and exit. Restart Squid service to make the changes effective.  
  
# service squid restart  
5. What is Media Range Limitation and partial download in Squid?  
  
Answer : Media Range Limitation is a special feature of squid in which just the required data is requested from the server and not the whole file. This feature is very well implemented in various videos streaming websites like Youtube and Metacafe where a user can click on the middle of progress bar hence whole video need not be fetched except for the requested part.  
The squid’s feature of partial download is implemented well within windows update where downloads are requested in the form of small packets which can be paused. Because of this feature a update downloading windows machine can be restarted without any fear of data loss. Squid makes the Media Range Limitation and Partial Download possible only after storing a copy of whole data in it. Moreover the partial download gets deleted and not cached when user points to another page until Squid is specially configured somehow.  
  
6. What is reverse proxy in squid?  
  
Answer : Reverse proxy is a feature of Squid which is used to accelerate the web surfing for end user. Say the Real server ‘RS’ contains the resource and ‘PS’ is the proxy Server. The client seek some data which is available at RS. It will rely on RS for the specified data for the first time and the copy of that specified data gets stored on PS for configurable amount of time. For every request for that data from now PS becomes the real source. This results in Less traffic, Lesser CPU usages, Lesser web resource utilization and hence lesser load to actual server RS. But RS has no statistics for the total traffic since PS acted as actual server and no Client reached RS. ‘X-Forwarded-For HTTP’ can be used to log the client IP although on RS.  
Technically it is feasible to use single squid server to act both as normal proxy server and reverse proxy server at the same point of time.  
  
7. Since Squid can be used as web-cache Daemon, is it possible to Clear its Cache? How?  
  
Answer : No Doubt! Squid acts as web-cache Daemon which is used to accelerate web surfing still it is possible to clear its cache and that too very easily.  
a. First stop Squid proxy server and delete cache from the location ‘/var/lib/squid/cache’ directory.  
  
# service squid stop  
# rm -rf /var/lib/squid/cache/\*<  
b. Create Swap directories.  
  
# squid -z  
8. A client approaches you, who is working. They want the web access time be restricted for their children. How will you achieve this scenario?  
  
Say the web access allow time be 4’o clock to 7’o clock in the evening for three hours, sharply form Monday to Friday.  
  
a. To restrict web access between 4 to 7 from Monday to Friday, open the Squid configuration file.  
  
# nano /etc/squid/squid.conf  
b. Add the following lines and save the file and exit.  
  
acl ALLOW\_TIME time M T W H F 16:00-19:00  
shttp\_access allow ALLOW\_TIME  
c. Restart the Squid Service.  
  
# service squid restart  
9. Squid stores data in which file format?  
  
Answer : Data stored by Squid is in ufs format. Ufs is the old well-known Squid storage format.  
10. Where do cache gets stored by squid?  
  
Answer : A squid stores cache in special folder at the location ‘/var/spool/squid’.  
  
  
  
1. How will you suspend a running process and put it in the background?  
  
Answer : In order to suspend a running process/job and put it in the background we need to use the key combination Ctrl+z.  
2. What are the minimum number of partitions required to install Linux and How will you check boot messages?  
  
Answer : The /root partition alone is sufficient to perform the whole task however minimum three partitions are recommended to install Linux. These are root, boot and swap. An IDE Hard Disk Drive supports upto 63 partitions and SCSI Hard Disk Drive supports up-to 15 partitions.  
In order to check boot messages we need to use cat or dmesg commands as shown below.  
  
# cat /var/log/messages  
  
OR   
  
# dmesg  
3. Name the Daemon responsible for tracking System Event on your Linux box?  
  
Answer : The Daemon ‘syslogd’ is responsible for tracking system information and stores the tracked logs in specific log files.  
4. What are the minimum requirements to run command ‘fsck’ on root partition?  
  
Answer : The /root partition must be mounted as read only mode and not read-write to execute fsck command on root partition.  
5. How to copy /home directory hierarchically to another directory. How will you do it?  
  
Answer : A Linux command ‘cpio’ comes to rescue here. The ‘cpio’ utility copies files and directories hierarchically over another location.  
6. How will you automate the rotation of logs in Linux?  
  
Answer : A Linux command ‘logrotate’ comes to rescue when it comes to automate the logs in Linux.  
7. How to know who has scheduled the job?  
  
Answer : The Linux command ‘at’ along with switch ‘-l’ is all we need to use in order to check who has scheduled the job.  
8. How to view the contents of the tar ball without extracting it. How will you do this?  
  
Answer : We need to use command ‘tar’ with options ‘-tvf’. The options ‘t’ (Display the contents), ‘v’ (Verbose), ‘f’ (files).  
9. What is page Fault and how it happens?  
  
Answer : A program request for some data and if it is not available in the Memory it is called as page fault. Page Fault occurs as a result of program shutdown.  
10. What are return codes in program?  
  
Answer : A return code is the feature of Shell. The result of return code shows the status of a program. A successful program after execution returns ‘0’, && can be used to prioritize which application will be executing first.  
  
  
  
Q1. You have a file (say virgin.txt). You want this file to be alter-proof so that no one can edit or delete this file, not even root. What will you do?  
  
Answer : In order to make this file immune to editing and deleting we need to use command “chattr”. Chattr changes the attributes of a file on Linux System.  
The Syntax of command chattr, for the above purpose is:  
  
# chattr +i virgin.txt  
Now try to remove the file using normal user.  
  
$ rm -r virgin.txt   
  
rm: remove write-protected regular empty file `virgin.txt'? Y   
rm: cannot remove `virgin.txt': Operation not permitted  
Now try to remove the file using root user.  
  
# rm -r virgin.txt   
  
cannot remove `virgin.txt': Operation not permitted  
Q2. If several users are using your Linux Server, how will you find the usage time of all the users, individually on your server?  
  
Answer : To fulfill the above task, we need to execute command ‘ac’. The Linux command ‘ac’ may not be installed, in your Linux box, by default. On a Debian based System you need a package ‘acct’ installed to run ac.  
# apt-get install acct  
# ac -p   
  
(unknown)                     14.18   
server                             235.23   
total      249.42  
Q3. Which is preferred tool to create Network Statistics for your server?  
  
Answer : A mrtg stands for Multi Router Traffic Grapher is one of the most commonly used tool to monitor network Statistics. mrtg is most widely recommended FOSS tool, which is very powerful. mrtg may not be installed on your Linux Box, by default and you need to install it manually from repo.  
# apt-get install mrtg  
Q4. It is possible to send query to BIOS from Linux Command Line?  
  
Answer : Yes! it is possible to send query and signals to BIOS, directly from the command line. For this you need a tool called “biosdecode”. On my Debian wheezy (7.4), it is already installed.  
# biosdecode   
  
# biosdecode 2.11   
  
ACPI 2.0 present.   
 OEM Identifier: LENOVO   
 RSD Table 32-bit Address: 0xDDFCA028   
 XSD Table 64-bit Address: 0x00000000DDFCA078   
SMBIOS 2.7 present.   
 Structure Table Length: 3446 bytes   
 Structure Table Address: 0x000ED9D0   
 Number Of Structures: 89   
 Maximum Structure Size: 184 bytes   
PNP BIOS 1.0 present.   
 Event Notification: Not Supported   
 Real Mode 16-bit Code Address: F000:BD76   
 Real Mode 16-bit Data Address: F000:0000   
 16-bit Protected Mode Code Address: 0x000FBD9E   
 16-bit Protected Mode Data Address: 0x000F0000   
PCI Interrupt Routing 1.0 present.   
 Router ID: 00:1f.0   
 Exclusive IRQs: None   
 Compatible Router: 8086:27b8   
 Slot Entry 1: ID 00:1f, on-board   
 ...  
 Slot Entry 15: ID 02:0c, slot number 2  
Q5. Most of the Linux Server are headless, i.e., they run in command mode only. No GUI is installed. How will you find hardware description and configuration of your box?  
  
Answer : It is easy to find Hardware description and configuration of a headless Linux Server using command “dmidecode”, which is the DMI table decoder.  
# dmidecode  
The output of dmidecode is extensive. It will be a nice idea to redirect its output to a file.  
  
# dmidecode > /path/to/text/file/text\_file.txt  
Q6. You need to know all the libraries being used and needed by a binary, say ‘/bin/echo’. How will you achieve desirable output?  
  
Answer : The command ‘ldd’, which print shared library dependencies of a binary in Linux.  
$ ldd /bin/echo   
  
linux-gate.so.1 =>  (0xb76f1000)   
libc.so.6 => /lib/i386-linux-gnu/i686/cmov/libc.so.6 (0xb7575000)   
/lib/ld-linux.so.2 (0xb76f2000)  
Q7. You are working for the country’s army. You have a file (say “topsecret.txt”) which contains confidential and country’s security Information, Nuclear missiles, etc. What will be your preferred method to delete this file?  
  
Answer : The file, being so confidential needs special deletion technique which can not be recovered by any means. For this, to implement practically we need to utilize an application “shred”. Shred tool overwrites a file repeatedly several times, thus making file recovery for any illegal activity almost nil and practically impossible.  
# shred -n 15 -z topsecret.txt  
shread – overwrite a file to hide its contents, and optionally delete it.  
  
-n – Overwrites the files n times  
-z – Add a final overwrite with zeros to hide shredding.  
Note: The above command overwrites the file 15 times before overwriting with zero, to hide shredding.  
  
Q8. Is it possible to mount an NTFS partition on Linux?  
  
Answer : Yes! We can mount an NTFS partition/disk on Linux system using application ‘mount.ntfs’ which optionally is called as ‘ntfs-3g’ in order to mount ntfs partition on Linux System.  
For more information, read article on how to monitor an NTFS Partition on Linux.  
  
Q9. What and where you need to edit so that the default desktop at login will be KDE, which at present is GNOME.  
  
Answer : We need to edit a file ‘/etc/sysconfig/desktop’ and add/edit the below lines to load KDE by default and not GNOME.  
DESKTOP=”KDE”  
DISPLAYMANAGER=”KDE”  
Save the file with above content. Next time when machine boots, it automatically will load KDE as default display manager.  
  
Q10. What does an intrid image file refers to?  
  
Answer : An intrid is Initial Ram Disk Image that loads into Memory after Power On Self Test (POST) in order to improve machine I/O performance. intrid contains temporary root file system.  
That’s all for now. I’ll be here again with another interesting topic, worth knowing. Till then stay tuned and connected to Tecmint. Don’t forget to provide us with your valuable feedback in comment section.  
  
  
  
1. SSH is configured on what Port Number, by default? How to change the port of SSH?  
  
Answer : 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]  
2. As a security implementation, you need to disable root Login on SSH Server, in Linux. What would you suggest?  
  
Answer : The above action can be implemented in the configuration file. We need to change the parameter ‘PermitRootLogin’ to ‘no’ in the configuration file to disable direct root login.  
To disable SSH root login, open the configuration file located at ‘/etc/ssh/sshd\_config‘ or ‘/etc/ssh/ssh\_config‘.  
  
# nano /etc/ssh/sshd\_config [On Red Hat based systems]  
  
# nano Port /etc/ssh/ssh\_config [On Debian based systems]  
Change the parameter ‘PermitRootLogin‘ to ‘no‘ and restart the SSH service as show above.  
  
3. SSH or Telnet? Why?  
  
Answer : 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.  
4. Is it possible to login to SSH server without password? How  
  
Answer : Yes! It is possible to login to a remote SSH server without entering password. We need to use ssh-keygen technology to create public and private keys.  
Create ssh-keygen using the command below.  
  
$ ssh-keygen  
Copy public keys to remote host using the command below.  
  
$ ssh-copy-id -i /home/USER/.ssh/id\_rsa.pub REMOTE-SERVER  
Note: Replace USER with user name and REMOTE-SERVER by remote server address.  
  
The next time we try to login to SSH server, it will allow login without asking password, using the keygen. For more detailed instructions, read how to login remote SSH server without password.  
  
5. How will you allows users and groups to have access to SSH Sever?  
  
Answer : Yes! It is possible to allow users and groups to have access to SSH server.  
Here again we need to edit the configuration file of SSH service. Open the configuration file and add users and groups at the bottom as show below and then, restart the service.  
  
AllowUsers Tecmint Tecmint1 Tecmint2  
AllowGroups group\_1 group\_2 group\_3  
6. How to add welcome/warning message as soon as a user login to SSH Server?  
  
Answer : 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  
7. 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.  
  
8. Is it possible to trace unauthorized login attempts to SSH Server with date of Intrusion along with their corresponding IP.  
  
Answer : Yes! we can find the failed login attempts in the log file created at location ‘/var/log/secure’. We can make a filter using the grep command as shown below.  
# cat /var/log/secure | grep “Failed password for”  
Note: The grep command can be tweaked in any other way to produce the same result.  
  
9. Is it possible to copy files over SSH? How?  
  
Answer : Yes! We can copy files over SSH using command SCP, stands for ‘Secure CopY’. SCP copies file using SSH and is very secure in functioning.  
A dummy SCP command in action is depicted below:  
  
$ scp text\_file\_to\_be\_copied Your\_username@Remote\_Host\_server:/Path/To/Remote/Directory  
For more practical examples on how to copy files/folders using scp command, read the 10 SCP Commands to Copy Files/Folders in Linux.  
  
10. 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  
  
  
  
1. What is Exim Service? What is the purpose of this Service?  
  
Answer : Exim is an Open Source Mail Transfer Agent (MTA) which deals with routing, receiving and delivering of Electronic Mail. Exim service serves to be a great replacement of sendmail service which comes bundled with most of the distro.  
2. What is NIS server? What is the purpose of NIS Server?  
  
Answer : The NIS server, serves the purpose of dealing with Network Information Service which in-turn facilitates to login to other Systems with same log-in credentials. NIS is a directory service protocol which functions in Client-Server Model.  
3. What will you prefer for a reverse proxy in Linux?  
  
Answer : Reverse Proxy refers to the type of proxy that retrieves resources on account of client from server(s). The solution of ‘Reverse Proxy’ in Linux is squid as well as Apache reverse Proxy. However ‘squid’ is more preferred than ‘Apache reverse Proxy’ because of its simplicity and straight forward nature.  
4. You are getting following codes (2xx, 3xx, 4xx, 5xx) in Apache, at some point of time. What does this means?  
  
Answer : In Apache each error code points towards a specific area of problem.  
  
2xx : Request of connection Successful  
3xx: Redirection  
4xx: Client Error  
5xx: Server Error  
5. You are asked to stop Apache Service through its control Script. What will you do?  
  
Answer : The Apache service is controlled using a script called apachectl. In order to stop apache using its control script we need to run.  
# apachectl stop [On Debian based Systems]  
# /etc/inid.t/httpd stop [On Red Hat based Systems]  
6. How is ‘apachectl restart’ different from ‘apachect1 graceful’  
  
Answer : The ‘apachect1 restart’ when executed will force Apache to restart immediately, before the task complete whereas ‘apachectl graceful’ will wait for the current task to be finished before restarting the service. Not to mention ‘apachectl graceful’ is more safe to execute but the execution time for ‘apachect1 restart’ is less as compared to ‘apachectl graceful’.  
7. How will you configure the nfs mounts to export it, from your local machine?  
  
Answer : The /etc/export allows the creation of nfs exports on local machine and make it available to the whole world.  
8. You are supposed to create a new Apache VirtualHost configuration for the host www.Tecmint.com that is available at /home/Tecmint/public\_html/ and maintains log at /var/log/httpd/ by default.  
  
Answer : You need to create a Apache virtual host container in main apache configuration file located at ‘/etc/httpd/conf/httpd.conf’. The following is the virtual container for host www.tecmint.com.  
  
DocumentRoot /home/Tecmint/public\_html  
ServerName www.Tecmint.com  
Server Alias Tecmint.com  
CustomLog /var/log/httpd/Tecmint.com.log combined  
ErrorLog /var/log/httpd/Tecmint.com.error.log

9. You are supposed to dump all the packets of http traffic in file http.out. What will you suggest?  
  
Answer : In order to dump all the network traffic, we need to use command ‘tcpdump’ with the following switches.  
# tcpdump tcp port 80 -s0 -w http.out  
10. How will you add a service (say httpd) to start at INIT Level 3?  
  
Answer : We need to use ‘chkconfig’ tool to hook up a service at INIT Level 3 by changing its runlevel parameter.  
chkconfig –level 3 httpd on  
  
  
  
1. Let’s say you maintains a backup on regular basis for the company you are working. The backups are maintained in Compressed file format. You need to examine a log, two months old. What would you suggest without decompressing the compressed file?  
  
Answer : To check the contents of a compressed file without the need of decompressing it, we need to use ‘zcat’. The zcat utility makes it possible to view the contents of a compressed file.  
# zcat ­f phpshell­2.4.tar.gz  
2. You need to track events on your system. What will you do?  
  
Answer : For tracking the events on the system, we need a daemon called syslogd. The syslogd daemon is useful in tracking the information of system and then saving it to specified log files.  
Running ‘syslogd‘ application in terminal generates log file at the location ‘/var/log/syslog‘. The syslogd application is very useful in troubleshooting Linux sytems. A sample log file looks similar to below.  
  
syslongd command  
syslongd  
3. How will you restrict IP so that the restricted IP’s may not use the FTP Server?  
  
Answer : We can block suspicious IP by integrating tcp\_wrapper. We need to enable the parameter “tcp\_wrapper=YES” in the configuration file at ‘/etc/vsftpd.conf’. And then add the suspicious IP in the ‘host.deny’ file at location ‘/etc/host.deny’.  
Block IP Address  
  
Open ‘/etc/hosts.deny’ file.  
  
# vi /etc/hosts.deny  
Add the IP address that you want to block at the bottom of the file.  
  
#  
# hosts.deny    This file contains access rules which are used to  
#               deny connections to network services that either use  
#               the tcp\_wrappers library or that have been  
#               started through a tcp\_wrappers-enabled xinetd.  
#  
#               The rules in this file can also be set up in  
#               /etc/hosts.allow with a 'deny' option instead.  
#  
#               See 'man 5 hosts\_options' and 'man 5 hosts\_access'  
#               for information on rule syntax.  
#               See 'man tcpd' for information on tcp\_wrappers  
#  
vsftpd:172.16.16.1  
4. Tell us the difference between Telnet and SSH?  
  
Answer : Telnet and SSH both are communication protocol which are used to manage remote system. SSH is Secured, which requires exchanging of key opposite of telnet which transmit data in plain text, which means telnet is less secure than SSH.  
6. You need to stop your X server. When you tries to kill your X server, You got an error message that you cannot quit X server. What will you do?  
  
Answer : When killing a X server, it won’t work normal way like doing ‘/etc/init.d/gdm stop’. We need to execute a special key combination ‘Ctrl+ Alt+ Back Space’ which will force X server to restart.  
6. What is the difference between command ‘ping’ and ‘ping6’?  
  
Answer : Both the commands are same and used for the same purpose except that the fact that ping6 is used with ipv6 IP address.  
7. You want to search for all the \*.tar files in your Home directory and wants to delete all at once. How will you do it?  
  
Answer : We need to use find command with rm command to delete all “.tar” files.  
# find /home/ ­name '\*.tar' | xargs rm ­rf  
8. What is the difference between locate and slocate command?  
  
Answer : The slocate looks for the files that user have access whereas locate will search for the file with updated result.  
9. You need to search for the string “Tecmint” in all the “.txt” files in the current directory. How will you do it?  
  
Answer : We need to run the fine command to search for the text “Tecmint” in the current directory, recursively.  
# find -­name “\*.txt” | xargs grep “Tecmint”  
10. You want to send a message to all connected users as “Server is going down for maintenance”, what will you do?  
  
Answer : This can be achieved using the wall command. The wall command sends a message to all connected users on the sever.  
# echo please save your work, immediately. The server is going down for Maintenance at 12:30 Pm, sharply. | wall  
wall command  
  
  
  
  
  
FTP stands for ‘File Transfer Protocol‘ is one of the most widely used and standard protocol available over Internet. FTP works in a Server/­Client architecture and is used to transfer file. Initially FTP client were command-­line based. Now most of the platform comes bundled with FTP client and server program and a lot of FTP Client/Server Program is available. Here we are presenting 10 Interview Questions based on Vsftp (Very Secure File Transfer Protocol) on a Linux Server.  
  
VsFTP Interview Questions  
10 VsFTP Interview Questions  
1. What is the Difference between TFTP and FTP Server?  
  
Answer : 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.  
Note: Briefly you can say FTP usages port 21 by default when clarification between Data and Control is not required.  
  
2. How to Restrict Users and Disallow browsing beyond their Home Directories? How?  
  
Answer : Yes! It is possible to restrict users to their home directories and browsing beyond home directories. This can be done by enabling chroot option in ftp configuration file (i.e. vsftpd.conf).  
chroot\_local\_user=YES  
3. How would you manage number of FTP clients that connect to your FTP server?  
  
Answer : We need to set ‘max\_client parameter’. This parameter controls the number of clients connecting, if max\_client is set to 0, it will allow unlimited clients to connect FTP server.The maximum client parameter needs to be changed in vsftpd.conf and the default value is 0.  
  
4. How to limit the FTP login attempts to fight against botnet/illegal login attempts?  
  
Answer : We need to edit ‘max\_login\_fails parameter’. This parameter manages the maximum number of login attempts before the session is killed. The default value is ‘3’ which means a maximum of ‘3’ login attempts are possible failing which the session will be killed.  
5. How to enable file upload from anonymous users to FTP Server?  
  
Answer : Anonymous users can be allowed to upload files to FTP server by modifying parameter ‘anon\_upload\_enable’. If Value of anon\_upload\_enable is set to Yes, Anonymous users are permitted to upload files. In order to have a working anonymous upload, we must have parameter ‘write\_enable’ activated. The Default Value is NO, which means anonymous upload is disabled.  
6. How would you disabled downloads from FTP server?  
  
Answer : Disabling Downloads from FTP Server can be implemented by modifying the parameter ‘download\_enable’. If set to NO, all download request will be denied. The Default value is YES which Means, Downloading is Enabled.  
7. How to enable and permit FTP login to local users?  
  
Answer : The parameter ‘Local\_enable’ is responsible for managing local users login. In order to activate local users login, we must set ‘local\_enable=yes’ in file vsftpd.conf. The default value is NO, which means Local User Login is not permitted.  
8. Is it Possible to maintain log of FTP requests and responses?  
  
Answer : 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.  
Note: In order to create and maintains logs successfully, the parameter ‘xferlog\_std\_format’ must be enabled.  
  
9. How to disable the login for few seconds, in case of failed login. How will you achieve this?  
  
Answer : The number of seconds we need to pause in case of failed login attempt can be achieved by modifying the value of parameter ‘delay\_failed\_login’. The default value is 1.  
10. 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.  
FTP is a very Useful tool and is vast yet very interesting. Moreover it is useful from Interview Point of View. We have taken the pain to bring these questions to you and will cover more of these questions in our future article. Till then stay tuned and connected to Tecmint.  
  
  
Please note vsftpd.conf file is used to control various aspects of configuration as specified in this article. By default, the vsftpd searches for the configuration file under /etc/vsftpd/vsftpd.conf. 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  
Before we start the Question and their well explained Answer we would like to answer a question “Who is going to attend FTP Interview?”. Well no one. Perhaps no one would be attending FTP interview. But we are presenting subject wise questions to maintain a systematic approach so that in any Interview, you wont get a new question which you wont be knowing on any of the topics/subjects we covered here.  
  
11. How would you block an IP which is acting malicious on your internal private VSFTP network?  
  
Answer : 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.  
Block IP using host.deny file  
  
Open ‘/etc/hosts.deny’ file.  
  
# vi /etc/hosts.deny  
Append the following line at the bottom of the file with the IP address that you want to block access to FTP.  
  
#  
# hosts.deny    This file contains access rules which are used to  
#               deny connections to network services that either use  
#               the tcp\_wrappers library or that have been  
#               started through a tcp\_wrappers-enabled xinetd.  
#  
#               The rules in this file can also be set up in  
#               /etc/hosts.allow with a 'deny' option instead.  
#  
#               See 'man 5 hosts\_options' and 'man 5 hosts\_access'  
#               for information on rule syntax.  
#               See 'man tcpd' for information on tcp\_wrappers  
#  
vsftpd:172.16.16.1  
Block IP using iptables rule  
  
To block FTP access to particular IP address, add the following drop rule to iptables INPUT chain.  
  
iptables -A RH-Firewall-1-INPUT -p tcp -s 172.16.16.1 -m state --state NEW -m tcp --dport 21 -j DROP  
12. How to allow secured SSL connections to Anonymous users? How would you do?  
  
Answer : Yes! It is possible to allow anonymous users to use secured SSL connections. The value of parameter ‘allow\_anon\_ssl’ should be ‘YES’ in the vsftpd.conf file. If it, set to NO it wont allow anonymous users to use SSL connections. The default value is NO.  
# Add this line to enable secured SSL connection to anonymous users.  
allow\_anon\_ssl=YES  
13. How to allow Anonymous users to create new directory and write to that directory?  
  
Answer : We need to edit the parameter ‘anon\_mkdir\_write\_enable’ and set it’s value to ‘YES’. But in order to make the parameter working, ‘write\_enable’ must be activated. The default is NO.  
# Uncomment this to enable any form of FTP write command.  
write\_enable=YES  
# Uncomment this if you want the anonymous FTP user to be able to create  
# new directories.  
anon\_mkdir\_write\_enable=YES  
14. How to enable Anonymous downloads, but disable permission to write?  
  
Answer : In the above said scenario, we need to edit the parameter ‘anon\_world\_readable\_only’. The parameter should be enabled and set to ‘YES’. The default value is YES.  
# Add this line to enable read only permission to anonymous users.  
allow\_anon\_ssl=YES  
15. How to CHMOD all Anonymous uploads automatically. How would you do?  
  
Answer : To chmod all anonymous uploads automatically, we need to edit the parameter ‘chmod\_enable’ and set it to ‘YES’. Anonymous users never get to use SITE CHMOD. The default value is YES.  
# Add this line to chmod all anonymous uploads automatically.  
chmod\_enable=YES  
16. 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  
17. How to maintain sessions for logins of VSFTP. How will you do?  
  
Answer : The parameter ‘session\_support’ needs to be modified. This parameter controls and manages vsftp attempts to maintain session for logins. The default value is NO.  
# Add this line to maintain session logins.  
session\_support=YES  
18. How to display time in local time zone, when listing the contents of directory?  
  
Answer : The parameter ‘usr\_localtime’ needs to be modified. If enabled, vsftpd will list directory files in local time zone format. The default is to display GMT. The default value is NO.  
# Add this line to display directory listing in local time zone.  
usr\_localtime=YES  
19. How will you limit the maximum transfer rate from VSFTP server?  
  
Answer : To limit the maximum transfer rate of VSFTP server we need the parameter ‘anon\_max\_rate’ in bytes per second, for anonymous client. The default value is 0 which means unlimited.  
# Add this line to limit the ftp transfer rate.  
anon\_max\_rate=0 # 0 means unlimited  
20. How will you timeout the idle session of VSFTP?  
  
Answer : The parameter ‘idle\_session\_timeout’ needs to be modified here. The timeout in second, which is the maximum time an anonymous user can spend in a session between his client machine and VSFTP server. As soon as the the timeout triggers, the client is logged out. The default time is 300.  
# Add this line to set the ftp timeout session.  
idle\_session\_timeout=300  
  
  
  
  
1. How will you add a new user (say, tux) to your system.?  
  
useradd command  
adduser command  
linuxconf command  
All of the above  
None of the above  
Answer : All of the above commands i.e., useradd, adduser and linuxconf will add an user to the Linux system.  
2. How many primary partition is possible on one drive?  
  
1  
2  
4  
16  
Answer : There are a maximum of ‘4‘ primary partition possible on a drive.  
3. The default port for Apache/Http is?  
  
8080  
80  
8443  
91  
None of the above.  
Answer : By default Apache/Http is configured on port 80.  
4. What does GNU stand for?  
  
GNU’s not Unix  
General Unix  
General Noble Unix  
Greek Needed Unix  
None of the above  
Answer : GNU stands for ‘GNU‘s not Unix‘.  
5. You typed at shell prompt “mysql” and what you got in return was “can’t connect to local MySQL server through socket ‘/var/mysql/mysql.sock’”, what would you check first.  
  
Answer : Seeing the error message, I will first check if mysql is running or not using commands service mysql status or service mysqld status. If mysql service is not running, starting of the service is required.  
Note:The above error message can be the result of ill configured my.cnf or mysql user permission. If mysql service starting doesn’t help, you need to see into the above said issues.  
  
6. How to Mount a windows ntfs partition on Linux?  
  
Answer : First install ntfs­3g pack on the system using apt or yum tool and then use “mount sudo mount ­t ntfs­3g /dev//” command to mount Windows partition on Linux.  
7. From the following which is not an RPM based OS.?  
  
RedHat Linux  
Centos  
Scientific Linux  
Debian  
Fedora  
Answer : The ‘Debian‘ operating system is not an RPM based and all listed above are ‘RPM‘ based except Debian.  
8. Which command can be used to rename a file in Linux.?  
  
mv  
ren  
rename  
change  
None of the Above  
Answer : The mv command is used to rename a file in Linux. For example, mv /path\_to\_File/original\_file\_name.extension /Path\_to\_File/New\_name.extension.  
9. Which command is used to create and display file in Linux?  
  
ed  
vi  
cat  
nano  
None of the above  
Answer : The ‘cat‘ command can be used to create and display file in Linux.  
10. What layer protocol is responsible for user and the application program support such as passwords, resource sharing, file transfer and network management?  
  
Layer 4 protocols  
Layer 5 protocols  
Layer 6 protocols  
Layer 7 protocols  
None of the above  
Answer : The ‘Layer 7 Protocol‘ is responsible for user and the application program support such as passwords, resource sharing, file transfer and network management.  
  
  
  
1. How will you add a new user (say, tux) to your system.?  
  
useradd command  
adduser command  
linuxconf command  
All of the above  
None of the above  
Answer : All of the above commands i.e., useradd, adduser and linuxconf will add an user to the Linux system.  
2. How many primary partition is possible on one drive?  
  
1  
2  
4  
16  
Answer : There are a maximum of ‘4‘ primary partition possible on a drive.  
3. The default port for Apache/Http is?  
  
8080  
80  
8443  
91  
None of the above.  
Answer : By default Apache/Http is configured on port 80.  
4. What does GNU stand for?  
  
GNU’s not Unix  
General Unix  
General Noble Unix  
Greek Needed Unix  
None of the above  
Answer : GNU stands for ‘GNU‘s not Unix‘.  
5. You typed at shell prompt “mysql” and what you got in return was “can’t connect to local MySQL server through socket ‘/var/mysql/mysql.sock’”, what would you check first.  
  
Answer : Seeing the error message, I will first check if mysql is running or not using commands service mysql status or service mysqld status. If mysql service is not running, starting of the service is required.  
Note:The above error message can be the result of ill configured my.cnf or mysql user permission. If mysql service starting doesn’t help, you need to see into the above said issues.  
  
6. How to Mount a windows ntfs partition on Linux?  
  
Answer : First install ntfs­3g pack on the system using apt or yum tool and then use “mount sudo mount ­t ntfs­3g /dev//” command to mount Windows partition on Linux.  
7. From the following which is not an RPM based OS.?  
  
RedHat Linux  
Centos  
Scientific Linux  
Debian  
Fedora  
Answer : The ‘Debian‘ operating system is not an RPM based and all listed above are ‘RPM‘ based except Debian.  
8. Which command can be used to rename a file in Linux.?  
  
mv  
ren  
rename  
change  
None of the Above  
Answer : The mv command is used to rename a file in Linux. For example, mv /path\_to\_File/original\_file\_name.extension /Path\_to\_File/New\_name.extension.  
9. Which command is used to create and display file in Linux?  
  
ed  
vi  
cat  
nano  
None of the above  
Answer : The ‘cat‘ command can be used to create and display file in Linux.  
10. What layer protocol is responsible for user and the application program support such as passwords, resource sharing, file transfer and network management?  
  
Layer 4 protocols  
Layer 5 protocols  
Layer 6 protocols  
Layer 7 protocols  
None of the above  
Answer : The ‘Layer 7 Protocol‘ is responsible for user and the application program support such as passwords, resource sharing, file transfer and network management.  
  
  
Q.1: What is the core of Linux Operating System?  
  
Shell  
Kernel  
Command  
Script  
Terminal  
Answer : Kernel is the core of Linux Operating System. Shell is a command Line Interpreter, Command is user Instruction to Computer, Script is collection of commands stored in a file and Terminal is a command Line Interface  
Q.2: What Linus Torvalds Created?  
  
Fedora  
Slackware  
Debian  
Gentoo  
Linux  
Answer : Linux Torvalds created Linux, which is the kernel (heart) of all of the above Operating System and all other Linux Operating System.  
Q.3: Torvalds, Wrote most of the Linux Kernel in C++ programming Language, do you agree?  
  
Answer : No! Linux Kernel contains 12,020,528 Lines of codes out of which 2,151,595 Lines are comments. So remaining 9,868,933 lines are codes and out of 9,868,933 Lines of codes 7,896,318 are written in C Programming Language.  
The remaining Lines of code 1,972,615 is written in C++, Assembly, Perl, Shell Script, Python, Bash Script, HTML, awk, yacc, lex, sed, etc.  
  
Note : The Number of Lines of codes varies on daily basis and an average of more than 3,509 lines are being added to Kernel.  
  
Q.4: Linux initially was developed for intel X86 architecture but has been ported to other hardware platform than any other Operating System. Do you agree?.  
  
Answer : Yes, I do agree. Linux was written for x86 machine, and has been ported to all kind of platform. Today’s more than 90% of supercomputers are using Linux. Linux made a very promising future in mobile phone, Tablets. In-fact we are surrounded by Linux in remote controls, space science, Research, Web, Desktop Computing. The list is endless.  
Q.5: Is it legal to edit Linux Kernel?  
  
Answer : Yes, Kernel is released under General Public Licence (GPL), and anyone can edit Linux Kernel to the extent permitted under GPL. Linux Kernel comes under the category of Free and Open Source Software (FOSS).  
Q.6: What is the basic difference between UNIX and Linux Operating System.  
  
Answer : Linux Operating System is Free and Open Source Software, the kernel of which is created by Linus Torvalds and community. Well you can not say UNIX Operating System doesn’t comes under the category of Free and Open Source Software, BSD, is a variant of UNIX which comes under the category of FOSS. Moreover Big companies like Apple, IBM, Oracle, HP, etc. are contributing to UNIX Kernel.  
Q. 7: Choose the odd one out.  
  
HP-UX  
AIX  
OSX  
Slackware  
Solaris  
Answer : Slackware is the odd in the above list. HP-UX, AIX, OSX, Solaris are developed by HP, IBM, APPLE, Oracle respectively and all are UNIX variant. Slackware is a Linux Operating System.  
Q.8: Is Linux Operating system Virus free?  
  
Answer : No! There doesn’t exist any Operating System on this earth that is virus free. However Linux is known to have least number of Viruses, till date, yes even less than UNIX OS. Linux has had about 60-100 viruses listed till date. None of them actively spreading nowadays. A rough estimate of UNIX viruses is between 85 -120 viruses reported till date.  
Q.9: Linux is which kind of Operating System?  
  
Multi User  
Multi Tasking  
Multi Process  
All of the above  
None of the above  
Answer : All of the Above. Linux is an Operating System which supports Multi User, Running a Number of Processes performing different tasks simultaneously.  
Q.10: Syntax of any Linux command is:  
  
command [options] [arguments]  
command options [arguments]  
command [options] [arguments]  
command options arguments  
Answer : The correct Syntax of Linux Command is Command [options] [arguments].  
Q.11: Choose the odd one out.  
  
Vi  
vim  
cd  
nano  
Answer : The odd one in the above list is cd. Vi, vim and nano are editors which is useful in editing files, while cd command is used for changing directory.  
  
  
  
1. What is Apache web server?  
  
Answer : Apache web server HTTP is a most popular, powerful and Open Source to host websites on the web server by serving web files on the networks. It works on HTTP as in Hypertext Transfer protocol, which provides a standard for servers and client side web browsers to communicate. It supports SSL, CGI files, Virtual hosting and many other features.  
2. How to check Apache and it’s version?  
  
Answer : First, use the rpm command to check whether Apache installed or not. If it’s installed, then use httpd -v command to check its version.  
[root@tecmint ~]# rpm -qa | grep httpd  
  
httpd-devel-2.2.15-29.el6.centos.i686  
httpd-2.2.15-29.el6.centos.i686  
httpd-tools-2.2.15-29.el6.centos.i686  
[root@tecmint ~]# httpd -v  
  
Server version: Apache/2.2.15 (Unix)  
Server built:   Aug 13 2013 17:27:11  
3. Apache runs as which user? and location of main config file?.  
  
Answer : Apache runs with the user “nobody” and httpd daemon. Apache main configuration file: /etc/httpd/conf/httpd.conf (CentOS/RHEL/Fedora) and /etc/apache2.conf (Ubuntu/Debian).  
4. On which port Apache listens http and https both?  
  
Answer : By default Apache runs on http port 80 and https port 443 (for SSL certificate). You can also use netstat command to check ports.  
[root@tecmint ~]# netstat -antp | grep http  
  
tcp        0      0 :::80                       :::\*                        LISTEN      1076/httpd            
tcp        0      0 :::443                      :::\*                        LISTEN      1076/httpd  
5. How do you install Apache Server on your Linux machine?  
  
Answer : Simply, you can use any package installer such as yum on (RHEL/CentOS/Fedora) and apt-get on (Debian/Ubuntu) to install Apache server on your Linux machine.  
[root@tecmint ~]# yum install httpd  
[root@tecmint ~]# apt-get install apache2  
6. Where you can find all configuration directories of Apache Web Server?  
  
Answer : By default Apache configuration directories installed under /etc/httpd/ on (RHEL/CentOS/Fedora) and /etc/apache2 on (Debian/Ubuntu).  
[root@tecmint ~]# cd /etc/httpd/  
[root@tecmint httpd]# ls -l  
total 8  
drwxr-xr-x. 2 root root 4096 Dec 24 21:44 conf  
drwxr-xr-x. 2 root root 4096 Dec 25 02:09 conf.d  
lrwxrwxrwx  1 root root   19 Oct 13 19:06 logs -> ../../var/log/httpd  
lrwxrwxrwx  1 root root   27 Oct 13 19:06 modules -> ../../usr/lib/httpd/modules  
lrwxrwxrwx  1 root root   19 Oct 13 19:06 run -> ../../var/run/httpd  
[root@tecmint ~]# cd /etc/apache2  
[root@tecmint apache2]# ls -l  
total 84  
-rw-r--r-- 1 root root  7113 Jul 24 16:15 apache2.conf  
drwxr-xr-x 2 root root  4096 Dec 16 11:48 conf-available  
drwxr-xr-x 2 root root  4096 Dec 16 11:45 conf.d  
drwxr-xr-x 2 root root  4096 Dec 16 11:48 conf-enabled  
-rw-r--r-- 1 root root  1782 Jul 21 02:14 envvars  
-rw-r--r-- 1 root root 31063 Jul 21 02:14 magic  
drwxr-xr-x 2 root root 12288 Dec 16 11:48 mods-available  
drwxr-xr-x 2 root root  4096 Dec 16 11:48 mods-enabled  
-rw-r--r-- 1 root root   315 Jul 21 02:14 ports.conf  
drwxr-xr-x 2 root root  4096 Dec 16 11:48 sites-available  
drwxr-xr-x 2 root root  4096 Dec  6 00:04 sites-enabled  
7. Can Apache be secured with TCP wrappers?  
  
Answer : No, It can’t be secured with the TCP wrappers since it doesn’t support libwrap.a library of Linux.  
8. How to change default Apache Port and How Listen Directive works in Apache?  
  
Answer : There is a directive “Listen” in httpd.conf file which allows us to change the default Apache port. With the help of Listen directive we can make Apache listen on different port as well as different interfaces.  
Suppose you have multiple IPs assigned to your Linux machine and want Apache to receive HTTP requests on a special Ethernet port or Interface, even that can be done with Listen directive.  
  
To change the Apache default port, please open your Apache main configuration file httpd.conf or apache2.conf file with VI editor.  
  
[root@tecmint ~]# vi /etc/httpd/conf/httpd.conf  
  
[root@tecmint ~]# vi /etc/apache2/apache2.conf  
Search for the word ”Listen”, comment the original line and write your own directive below that line.  
  
# Listen 80  
Listen 8080  
  
OR  
  
Listen 172.16.16.1:8080  
Save the file and restart the web server.  
  
[root@tecmint ~]# service httpd restart  
  
[root@tecmint ~]# service apache2 restart  
9. Can we have two Apache Web servers on a single machine?  
  
Answer : Yes, we can run two different Apache servers at one time on a Linux machine, but the condition for that is they should listen on different ports and we can change the ports with Listen directive of Apache.  
10. What do you mean by DocumentRoot of Apache?  
  
Answer : DocumentRoot in Apache means, it’s the location of web files are stored in the server, the default DocumentRoot of Apache is /var/www/html or /var/www. This can be changed to anything, by setting up “DocumentRoot” in a virtual host of configuration file of domain.  
11. How to host files in different folder and what is Alias directive?  
  
Answer : Yes, this can be achieved by Alias directive in the main Apache configuration file. Alias directive maps resources in File system, it takes a URL path and substitute it with a file or directory path on the system with is set up to redirect.  
To use Alias directive, Its the part of mod\_alias module of Apache. The default syntax of Alias directive is:  
  
Alias /images /var/data/images/  
Here in above example, /images url prefix to the /var/data/images prefix that mean clients will query for “http://www.example.com/images/sample-image.png” and Apache will pick up the “sample-image.png” file from /var/data/images/sample-image.png on the server. It’s also known as URL Mapping.  
  
12. What do you understand by “DirectoryIndex”?  
  
Answer : DirectoryIndex is the name of first file which Apache looks for when a request comes from a domain. For example: www.example.com is requested by the client, so Apache will go the document root of that website and looks for the index file (first file to display).  
The default setting of DirectoryIndex is .html index.html index.php, if you have different names of your first file, you need to make the changes in httpd.conf or apache2.conf for DirectoryIndex value to display that to your client browser.  
  
#  
# DirectoryIndex: sets the file that Apache will serve if a directory  
# is requested.  
#  
# The index.html.var file (a type-map) is used to deliver content-  
# negotiated documents.  The MultiViews Option can be used for the  
# same purpose, but it is much slower.  
#  
DirectoryIndex index.html index.html.var index.cgi .exe  
13. How to disable Directory listing when an index file is missing?  
  
Answer : If, the main index file is missing in the website root directory, then the Apache will lists all the contents like files and folder of the website on the browser instead of Main website pages.  
To stop Apache directory listing, you can set the following rule in the main configuration file globally or in .htaccess file for a particular website.  
  
  
   Options -Indexes  
  
14. What are different log files of Apache Web Server?  
  
Answer : The default log files of Apache Web Server are access log “/var/log/httpd/access\_log” and error log :/var/log/httpd/error\_log”.  
15. What do you understand by “connection reset by peer” in error logs?  
  
Answer : When the server is serving any ongoing Apache request and end user terminates the connection in between, we see “connection reset by peer” in the Apache error logs.  
16. What is Virtual Host in Apache?  
  
Answer : The Virtual Host section contains the information like Website name, Document root, Directory Index, Server Admin Email, ErrorLog File location etc.  
You are free to add as many directives you require for your domain, but the two minimal entries for a working website is the ServerName and DocumentRoot. We usually define our Virtual Host section at the bottom of httpd.conf file in Linux machines.  
  
Sample VirtualHost  
  
  
   ServerAdmin webmaster@dummy-host.example.com  
   DocumentRoot /www/docs/dummy-host.example.com  
   ServerName dummy-host.example.com  
   ErrorLog logs/dummy-host.example.com-error\_log  
   CustomLog logs/dummy-host.example.com-access\_log common  
  
ServerAdmin : Its usually the email address of the website owner, where the error or notification can be sent.  
DocumentRoot : location where the web files are located in the server(Necessary).  
ServerName : Its the domain name which you want to access from your web browser(Necessary).  
ErrorLog : Its the location of the log file where all the domain related logs are being recorded.  
17. What’s the difference between and ?  
  
Answer :  
is used to set element related to the URL / address bar of the web server.  
refers that the location of file system object on the server  
18. What is Apache Virtual Hosting?  
  
Answer : Apache Virtual hosting is the concept of hosting multiple website on a single web server. There are two types of Virtual hosts can be setup with Apache are Name Based Virtual hosting and IP based virtual hosting.  
For more information, read on How to Create Name/IP based Virtual Hosts in Apache.  
  
19. What do you understand by MPM in Apache?  
  
Answer : MPM stands for Multi Processing Modules, actually Apache follows some mechanism to accept and complete web server requests.  
20. What is the difference between Worker and Prefork MPM?  
  
Answer : Both MPMs, Worker and prefork has their own mechanism to work with Apache. It totally depends on you that in which mode you want to start your Apache.  
Basic difference between Worker and MPM is in their process of spawning the child process. In the Prefork MPM, a master httpd process is started and this master process starts manages all other child processes to serve client requests. Whereas, In the worker MPM one httpd process is active, and it uses different threads to serve client requests.  
Prefork MPM uses multiple child processes with one thread each, where worker MPM uses multiple child processes with many threads each.  
Connection handling in the Prefork MPM, each process handles one connection at a time, whereas in the Worker mpm each thread handles one connection at a time.  
Memory footprints Prefork MPM Large memory footprints, where Worker has smaller memory footprints.  
21. What’s the use of “LimitRequestBody” and how to put limit on your uploads?  
  
Answer : LimitRequestBody directive is used to put a limit on the upload size.  
For example: I want to put limits of 100000 Bytes in the folder /var/www/html/tecmin/uploads. So, you need to add following directive in Apache configuration file.  
  
  
LimitRequestBody 100000  
  
22. What is mod\_perl and mod \_php?  
  
Answer :  
mod\_perl is an Apache module which is compiled with Apache for easy integration and to increase the performance of Perl scripts.  
mod\_php is used for easy integration of PHP scripts by the web server, it embeds the PHP interpreter inside the Apache process. Its forces Apache child process to use more memory and works with Apache only but still very popular.  
23. What is Mod\_evasive?  
  
Answer : Its a third-party module which helps us to prevent your web server from the web attacks like DDOS because it performs only one task at a time and performs it very well.  
For more information, read the article that guides you how to install and configure mod\_evasive in Apache.  
  
24. What is Loglevel debug in httpd.conf file?  
  
Answer : With the help of Loglevel Debug option, we can get/log more information in the error logs which helps us to debug a problem.  
25. What’s the use of mod\_ssl and how SSL works with Apache?  
  
Answer : Mod\_ssl package is an Apache module, which allows Apache to establish its connection and transfer all the data in a secure encrypted environment. With the help of SSL certificates, all the Login details and other important secret details get transferred in an encrypted manner over the Internet, which prevents our data from Eavesdropping and IP spoofing.  
How SSL works with Apache  
  
Whenever an https requests comes, these three steps Apache follows:  
  
Apache generates its private key and converts that private key to .CSR file (Certificate signing request).  
Then Apache sends the .csr file to the CA (Certificate Authority).  
CA will take the .csr file and convert it to .crt (certificate) and will send that .crt file back to Apache to secure and complete the https connection request.  
These are just most popular 25 questions being asked these days by Interviewers, please provide some more interview questions which you have faced in your recent interview and help others via our Comment section below.  
  
  
Some of the Changes in RHEL 7 are listed below as compare with RHEL 6 .  
Default root file system is XFS  
Linux 3.10 kernel.  
A new systemctl command replaces chkconfig and service, although scripts allow you to still use the legacy commands.  
Docker: The biggest new addition to RHEL 7 is tight integration of Docker, the explosively popular application-virtualization technology.  
Boot-loader GRUB2  
Samba 4.1 and BTRFS makes an appearance  
  
RHEL-7 installation source:-  
http  
https  
ftp  
ntfs  
  
  
RHEL-7 Software Selection  
Minimal install  
Infrastructure server  
File and print server  
Basic web server  
Virtualization Host  
Server with GUI  
  
RHEL-7 Installation Destination  
standard partition - A standard partition can contain a file system or swap space, or it can provide a container for software RAID or an LVM physical volume.  
BTRFS - Btrfs is a file system with several device-like features. It is capable of addressing and managing more files, larger files, and larger volumes than the ext2, ext3, and ext4 file systems.  
LVM - Creating an LVM partition automatically generates an LVM logical volume. LVM can improve performance when using physical disks.  
LVM Thin Provisioning - Using thin provisioning, you can manage a storage pool of free space, known as a thin pool, which can be allocated to an arbitrary number of devices when  
needed by applications. The thin pool can be expanded dynamically when needed for costeffective allocation of storage space.  
  
  
xfs - XFS is a highly scalable, high-performance file system that supports file systems up to 16 exabytes (approximately 16 million terabytes), files up to 8 exabytes (approximately 8 million  
terabytes), and directory structures containing tens of millions of entries. XFS supports metadata journaling, which facilitates quicker crash recovery. The XFS file system can also be  
defragmented and resized while mounted and active. This file system is selected by default and is highly recommended  
The maximum supported size of an XFS partition is 500 TB.  
  
ext4 - The ext4 file system is based on the ext3 file system and features a number of improvements. These include support for larger file systems and larger files, faster and more  
efficient allocation of disk space, no limit on the number of subdirectories within a directory, faster file system checking, and more robust journaling.  
The maximum supported size of an ext4 file system in Red Hat Enterprise Linux 7 is currently 50TB.  
  
ext3 - The ext3 file system is based on the ext2 file system and has one main advantage - journaling. Using a journaling file system reduces time spent recovering a file system after  
a crash as there is no need to check the file system for metadata consistency by running the fsck utility every time a crash occurs.  
  
ext2 - An ext2 file system supports standard Unix file types, including regular files, directories, or symbolic links. It provides the ability to assign long file names, up to 255 characters.  
  
vfat - The VFAT file system is a Linux file system that is compatible with Microsoft Windows long file names on the FAT file system.  
  
swap - Swap partitions are used to support virtual memory. In other words, data is written to a swap partition when there is not enough RAM to store the data your system is processing.  
  
BIOS Boot - A very small partition required for booting a device with a GUID partition table (GPT) on a BIOS system.  
  
EFI System Partition - A small partition required for booting a device with a GUID partition table (GPT) on a UEFI system.  
  
  
/boot - non LVM  
/root - LVM  
/home - LVM  
/var  - LVM  
  
  
NFS:-  
yum install nfs-utils  
/etc/exports  
systemctl start nfs.service  
systemctl reload nfs.service  
  
HTTP:-  
yum install httpd  
systemctl start httpd.service  
  
FTP:-  
yum install vsftpd  
vi /etc/vsftpd/vsftpd.conf  
systemctl start vsftpd.service  
systemctl restart vsftpd.service  
  
Ports Used By Network Protocols  
NFS - 2049,111,20048  
HTTP - 80  
HTTPS - 443  
FTP - 21  
  
BLKID - command line utility to locate/print block device attributes.  
  
Boot Method                             Installation Source   
Full installation media (D VD or USB) - The boot media itself.  
Minimal boot media (CD or USB) - Full installation DVD ISO image or the installation tree extracted from this image,placed in a network location or on a hard drive.  
Network boot (PXE) - Full installation DVD ISO image or the installation tree extracted from this image,placed in a network location.  
  
All Red Hat Enterprise Linux installations include the following network services:  
centralized logging through the syslog utility  
email through SMTP (Simple Mail Transfer Protocol)  
network file sharing through NFS (Network File System)  
remote access through SSH (Secure SHell)  
resource advertising through mDNS (multicast DNS)  
  
GRUB2 - Grand Unified Bootloader version 2  
  
The installation program installs GRUB2 either in the master boot record (MBR) or the GUID partition table (GPT) of the device for the root file system. In order to  
determine which of these methods to use,the installation program considers the following variations:  
BIOS systems, and UEFI systems in BIOS compatibility mode  
  
MBR if the size of the disk is less than 2 TB.  
GPT if the size of the disk is more than 2 TB.  
  
Redundant arrays of independent disks (RAIDs)  
  
RAID0 - Optimized performance (stripe)  
Distributes data across multiple disks. Level 0 RAID s offer increased performance over standard partitions, and can be used to pool the storage of multiple disks into  
one large virtual device. Note that Level 0 RAID s offer no redundancy, and that the failure of one device in the array destroys data in the entire array. RAID 0 requires at  
least two RAID partitions.  
  
RAID1 - Redundancy (mirror)  
Mirrors all data on one disk onto one or more other disks. Additional devices in the array provide increasing levels of redundancy. RAID 1 requires at least two RAID  
partitions.  
  
RAID4 - Error detection (parity)  
Distributes data across multiple disks, and uses one disk in the array to store parity information that safeguards the array in case any disk within the array fails.  
Because all parity information is stored on one disk, access to this disk creates a bottleneck in the performance of the array. RAID 4 requires at least three RAID  
partitions.  
  
RAID5 - Distributed error detection  
Distributes data and parity information across multiple disks. Level 5 RAIDs therefore offer the performance advantages of distributing data across multiple  
disks, but do not share the performance bottleneck of level 4 RAIDs because the parity information is also distributed through the array. RAID5 requires at least  
three RAID partitions.  
  
RAID6 - Redundant  
Level 6 RAIDs are similar to level 5 RAIDs, but instead of storing only one set of parity data, they store two sets. RAID 6 requires at least four RAID partitions.  
  
RAID10 - Redundancy (mirror) and Optimized performance (stripe)  
Level 10 RAID s are nested RAIDs or hybrid RAIDs. They are constructed by distributing data over mirrored sets of disks. For example, a level 10 RAID array  
constructed from four RAID partitions consists of two mirrored pairs of striped partitions. RAID 10 requires at least four RAID partitions.  
  
  
/tmp/anaconda.log general Anaconda messages  
/tmp/program.log all external programs run during the installation  
/tmp/storage.log extensive storage module information  
/tmp/packaging.log yum and rpm package installation messages  
/tmp/sysloghardware-related system messages  
  
Refresh the boot loader configuration by executing the following command:  
# grub2-mkconfig --output=/boot/grub2/grub.cfg  
  
Graphical Login  
systemctl set-default graphical.target  
systemctl set-default multi-user.target  
  
PXE Server:-  A preboot execution environment (PXE) server allows the installation program to boot over the network. After you boot the system, you complete the  
installation from a different installation source, such as a local hard drive or a location on a network.  
  
Hostname:- fully qualified domain name(FQDN).  
  
yum install tftp-server  
In the /etc/xinetd.d/tftp configuration file, change the disabled parameter from yes to no .  
Allow incoming connections to the tftp service in the firewall:  
# firewall-cmd --add-service= tftp  
mkdir /var/lib/tftpboot/pxelinux  
cp publicly\_available\_directory/usr/share/syslinux/pxelinux.0  /var/lib/tftpboot/pxelinux  
A sample configuration file at /var/lib/tftpboot/pxelinux/default  
cp /path/to/x86 \_64/os/images/pxeboot/{vmlinuz,initrd.img}  /var/lib/tftpboot/pxelinux/  
systemctl start tftp.service xinetd.service dhcpd.service  
systemctl enable tftp.service xinetd.service dhcpd.service  
  
Kickstart  
yum install pykickstart  
After installing the package, you can validate a Kickstart file using the following command:  
$ ksvalidator /path/to/kickstart.ks  
  
  
Network Time Protocol – NTP- is a protocol which runs over port 123 UDP at Transport Layer and allows computers to synchronize time over networks for an accurate time.  
  
yum install ntp  
vim /etc/ntp.conf  
server 0.centos.pool.ntp.org iburst  
server 1.centos.pool.ntp.org iburst  
server 2.centos.pool.ntp.org iburst  
server 3.centos.pool.ntp.org iburst  
  
Now configure your ntp server to allow LAN systems to keep synchronize their time from this server. To do it add following entry in configuration file  
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap  
  
# firewall-cmd --add-service=ntp --permanent  
# firewall-cmd --reload  
  
# systemctl start ntpd  
# systemctl enable ntpd  
# systemctl status ntpd  
  
After NTP daemon has been started, wait a few minutes for the server to synchronize time with its pool list servers, then run the following commands to verify NTP peers synchronization status and your system time.  
# ntpq -p  
# date -R  
  
  
NFS:-  
Server  
yum install nfs-utils rpcbind  
mkdir -p /opt/nfs  
/etc/exports  
/opt/nfs 10.1.1.18(no\_root\_squash,rw,sync)  
firewall-cmd --zone=public --add-port=2049/tcp --permanent  
firewall-cmd --reload  
service rpcbind start; service nfs start  
service nfs status  
  
Client  
yum install nfs-utils rpcbind  
mkdir -p /mnt/nfs  
  
Configuring permanent NFS mount  
systemctl enable nfs-server  
vi /etc/fstab  
10.1.1.110:/opt/nfs /mnt/nfs nfs defaults  0 0  
  
Mount User Home Directory  
mkdir -p /exports/rhel7  
mount --bind /home/rhel7/ /exports/rhel7/  
vi /etc/fstab  
/home/rhel7    /exports/rhel7   none    bind  0  0  
  
vi /etc/exports  
/exports/rhel7 10.1.1.18(no\_root\_squash,rw,sync)  
  
Re-export all NFS directories  
exportfs -ra  
  
Firewall:-  
systemctl stop firewalld  
systemctl disable firewalld  
  
Selinux:-  
[root@dlp ~]#  
vi /etc/selinux/config  
# This file controls the state of SELinux on the system.  
# SELINUX= can take one of these three values:  
# enforcing - SELinux security policy is enforced.  
# permissive - SELinux prints warnings instead of enforcing.  
# disabled - No SELinux policy is loaded.  
SELINUX=disabled  
# change  
# SELINUXTYPE= can take one of these two values:  
# targeted - Targeted processes are protected,  
# minimum - Modification of targeted policy. Only selected processes are protected.  
# mls - Multi Level Security protection.  
SELINUXTYPE=targeted  
[root@dlp ~]# reboot  
  
  
Services  
systemctl -t service  
systemctl list-unit-files -t service  
systemctl --all  /start/stop/reload/restart/status/enable/disable  
chkconfig --list  
  
yum - Yellowdog Updater Modified  
yum -y update  
Add Repositories  
Commands  
yum install/update/remove/groupinstall/groupupdate/groupremove/list/check-update/info/search/deplist  
Options  
yum -y/--enablerepo=repo/--disablerepo=repo/--exclude=package/--noplugins  
  
  
NFS:-  
yum install nfs-utils nfs-utils-lib  
systemctl enable rpcbind  
systemctl enable nfs-server  
systemctl enable nfs-lock  
systemctl enable nfs-idmap  
  
systemctl start rpcbind  
systemctl start nfs-server  
systemctl start nfs-lock  
systemctl start nfs-idmap  
  
mkdir /var/unixmen\_share  
chmod 777 /var/unixmen\_share  
  
vi /etc/exports  
  
/var/unixmen\_share  192.168.1.0/24(rw,sync,no\_root\_squash,no\_all\_sqash)  
  
whereas  
  
/var/unixmen\_share - shared directory  
192.168.1.0/24 - Ip address range of clients  
rw - writable permissions to shared folder  
sync - syncronize shared directory  
no\_root\_squash - enable root privilege  
no\_all\_squash - enable user's authority  
  
systemctl restart nfs-server  
  
yum install nfs-utils nfs-utils-lib  
  
systemctl enable rpcbind  
systemctl enable nfs-server  
systemctl enable nfs-lock  
systemctl enable nfs-idmap  
  
systemctl start rpcbind  
systemctl start nfs-server  
systemctl start nfs-lock  
systemctl start nfs-idmap  
  
mount -t nfs 192.168.1.101:/var/unixmen\_share/  /var/nfs\_share/  
  
connection timeout  
  
then we have to run this cmd -> rpcinfo -p  
  
firewall-cmd --permanent --add-port=111/tcp  
firewall-cmd --permanent --add-port=54302/tcp  
firewall-cmd --permanent --add-port=20048/tcp  
firewall-cmd --permanent --add-port=2049/tcp  
firewall-cmd --permanent --add-port=46666/tcp  
firewall-cmd --permanent --add-port=42955/tcp  
firewall-cmd --permanent --add-port=875/tcp  
  
firewall-cmd --reload  
  
  
TOPICS  - Installing, Administering, Troubleshooting, Configuring, Monitoring, Upgrading.(RHEL,FEDORA,CENTOS,UBUNTU,WINDOWS)  
  
DHCP  
DNS  
NTP  
NFS  
FTP  
SAMBA  
APACHE  
PAM  
YUM  
TCPWRAPPERS  
IPTABLES  
SELINUX  
VIRTUALIZATION  
ADMINISTRATION OF USERS & GROUPS   
MANAGING SYSTEM SECURITY & FILE PERMISSIONS  
SQUID  
SENDMAIL,QMAIL,IMAP & POP3 - MAIL SERVERS  
BACKUP FILESYSTEM & DATA  
RAID  
LVM  
QUOTAS  
CRON  
PXE  
RSYNC  
NAGIOS  
KERNEL COMPILATIONS  
MYSQL & PostgreSQL