35

April-24
Page no - 13

Scoring Indicators (SET 1)

COURSE NAME: SERVER ADMINISTRATION

COURSE CODE: TED (21) 6131B **QID :** *2102240136*

Q No	Scoring Indicators	Split score	Sub Total	Total score
	PART A			9
I. 1	Red Hat Enterprise Linux (RHEL), Fedora, Debian, Mandrake, Ubuntu, Kubuntu, openSUSE, CentOS, Gentoo	0.5 x Any 2	1	
I. 2	User, Group, Others	0.5 x Any 2	1	
I. 3	Regular files (-),Directory files (d),Special files	0.5 x Any 2	1	
I. 4	userID ,GroupID	0.5 x 2	1	
I. 5	ps	1	1	
I. 6	ifconfig ip address add	1 x Any 1	1	
I. 7	Apache, NGINX, Lighttpd, H2O Web Server	1 x Any 1	1	
I. 8	Network File System (NFS)	1	1	
I. 9	Dump, restore	0.5 x 2	1	
	PART B			24
II. 1	Read (r) : The read permission allows you to open and read the content of a file. But you can't do any editing or modification in the file. Write (w) : The write permission allows you to edit, remove or rename a file. Execute (x): In Linux system, you can't run or execute a program unless execute permission is set.	3x1	3	
II. 2	Editors used for editing text files, writing codes, updating user instruction files etc. A Linux system supports multiple text editors.	Explanation: 1.5 Eg.	3	

	Example text editors are vi, emacs, joe, pico, Gedit	0.5x3		
II. 3	move files - mv, copy file cp ,list files ls	1x3	3	
II. 4	Patch files can be downloaded from the same site from which the kernel is downloaded. Once you have the patch file downloaded, You will next decompress the patch file and the then the patch program is run , which will then do the actual work of patching/updating your kernel.	3	3	
II. 5	1. useradd [options] LOGIN useradd -n user1 (created user1) passwd user1 (setting password) 2. usermod [options] LOGIN usermod -u 1600 user1 (changed UID to 1600) 3. userdel [options] LOGIN userdel user1 (user1 deleted)	1x3	3	
II. 6	ifconfig eth0 192.168.1.42 ip address add eth0 192.168.1.42	1.5x2	3	
II. 7	Samba is a powerful suite of applications that help UNIX-based systems (such as Linux) interoperate with Windows-based and other operating systems. Samba transparently provides file and print sharing services to Windows clients as well as other networked clients running other operating systems	3	3	
II. 8	Dynamic Host Configuration Protocol Daemon (DHCPD), the DHCP server, is responsible for serving IP addresses and other relevant information upon client request. Since DHCP is broadcast-based, a server will have to be present on each subnet for which DHCP service is to be provided. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. IP	3	3	

	addresses are dynamic and leased to a DHCP Client on request.			
II.9	Linux comes with several command-line (CLI) tools that can be used for backing up or restoring data dump and restore: The dump tool works by making a copy of an entire file system. The restore tool can then pull any and all files from this copy To support incremental backups, dump uses the concept of dump levels. A dump level of 0 means a full backup. Any dump level above 0 is an incremental relative to the last time a dump. The dump utility stores all the information about its dumps in the /etc/dumpdates file. The restore program reads the dump files created by dump and extracts individual files and directories from them.	3	3	
II.10	• The amount of data that needs to be backed up: • Backup hardware and backup medium • The amount of network throughput that needs to be supported • The speed and ease of data recovery • Data deduplication issues • Tape management	0.5x6	3	

	PART C			42
III	A complete Linux system package called a distribution. It contains the Linux kernel and supporting libraries and software. Distributions, also called distros, can be described as different operating system versions built on top of the underlying Linux Kernel to support a variety of use-cases and preferences. A distribution comprises everything necessary to get Linux to exist as a functional operating system. Most distros are customized for specific user group. We can get Linux based OS by downloading one of the Linux distros.	Explanation: 4 Eg. 1.5 +1.5	7	7

	Linux distributions can be broadly categorized into two groups. Commercial distros, and the non-commercial distros. The commercial distros generally offer support for their distribution at a cost. The commercial distros a have a longer release life cycle. The non-commercial distros are free. They are mostly community supported and maintained. Non-commercial distros e.g.: (Any 2) 1.5 Marks Fedora, openSUSE, Ubuntu, Linux Mint, Gentoo, and Debian Commercial distros e.g.: (Any 2) 1.5 Marks Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise (SLE), Ubuntu Pro.			
IV.	The kernel of any operating system is the core of all the system's software. The kernel is a core component of an operating system and serves as the main interface between the computer's physical hardware and the processes running on it. Functions of a Kernel. 1.Device Management: A kernel maintains a list of all the available devices, and this list may be already known, configured by the user, or detected by OS at runtime. 2.Memory Management: The kernel has full control for accessing the computer's memory. Each process requires some memory to work, and the kernel enables the processes to safely access the memory. 3.Resource Management: One of the important functionalities of Kernel is to share the resources between various processes. It must share the resources in a way that each process uniformly accesses the resource. The kernel also provides a way for synchronization and inter-process communication (IPC). 4.Accessing Computer Resources: A kernel is responsible for accessing computer resources such as RAM and I/O devices. RAM or Random-Access Memory is used to contain both data and instructions.	7	7	7

V.	1. Normal users can access only what they own or have been given permission to run. Normal users on Linux run with reduced permissions – for example, they can't install software or write to system directories The root user has maximum permissions and can do anything to the system. The root user is allowed to access all files and programs in the system, whether or not root owns them. The root user is often called a superuser. 2. useradd allows you to add a single user to the system - useradd [options] LOGIN 3. usermod command allows you to modify an existing user in the system - usermod [options] LOGIN 4. userdel command does the exact opposite of useradd—it removes existing users - userdel [options] LOGIN 5. groupadd [options] GROUP 6. groupdel group 7. groupmod [options] GROUP	1x7	7	7
VI.	• For any operating system to boot on standard PC hardware, you need what is called a boot loader • The boot loader is the first software program that runs when a computer starts. It is responsible for handing over control of the system to the operating system • Boot loader will reside in the Master Boot Record (MBR) of the disk • GRUB, is the most common boot loader that comes with the newer distributions of Linux **Any 2 X 1 = 2 marks** The GRUB boot process happens in stages. Each stage is taken care of by special GRUB image files.	2+5	7	7

	Two of the stages are essential, and the other stages are optional and dependent on the particular system setup. Stage 1 The image file used in this stage is essential and is used for booting up GRUB. It is usually embedded in the MBR of a disk or in the boot sector of a partition. The file used in this stage is named stage1. A Stage 1 image can next either load Stage 1.5 or load Stage 2 directly. Stage 2 The Stage 2 images actually consist of two types of images: the intermediate (optional image) and the actual stage2 image file. The optional images are called Stage 1.5. The Stage 1.5 images serve as a bridge between Stage 1 and Stage 2. Stage 1.5 image helps to locate the Stage 2 image Stage2 image is the core of GRUB. It contains the actual code to load the kernel that boots the OS, it displays the boot menu, and it also contains the GRUB shell from which GRUB commands can be entered. The GRUB shell is interactive and helps to make GRUB flexible Other types of Stage 2 images are the stage2_eltorito image, the nbgrub image, and the pxegrub image The stage2_eltorito image is a boot image for CD-ROMs The nbgruband pxegrub images are both network-type boot images that can be used to bootstrap asystem over the network **GRUB Explanation – 5 marks**			
VII.	1. user information is stored in etc/password file. Fields of passwd files /etc/passwd file stores the user's login, encrypted	1x7	7	7

	password entry, UID, default GID, name (sometimes called GECOS), home directory, and login shell. Each line in the file represents information about a user. The lines are made up of various standard fields, with each field delimited by a colon. 2. Username Field - login field or the account field. It stores the name of the user on the system 3. Password Field - This field contains the user's encrypted password 4. User ID Field (UID) - This field stores a unique number that the operating system and other applications use to identify the user and determine access privileges. 5. Group ID Field (GID) - The group ID entry. It is the numerical equivalent of the primary group to which the user belongs. 6. GECOS - This field can store various pieces of information for a user, user description, full name (first and last name), telephone number, and so on. This field is optional and as a result can be left blank. 7. Directory- This is usually the user's home directory, it can also be any location on the system. used to place configuration files that are unique to that user			
VIII.	• Syslog is a utility for capturing and logging system information. This system information can be stored locally, remotely, or both. • Linux logs gives a detailed account of all events, requests, and activity on the system. • Log files can be used to monitor critical events in the kernel, the server. • Linux systems have a very flexible and powerful logging system. which enables to record any system	1x7	7	7

	events and then manipulate the logs to retrieve the information you require • Logging Daemon is used for system logging .Linux distributions use the syslogd (sysklogd) daemon to provide this service. • Each log entry consists of a single line containing the date, time, host name, process name, PID, and the message from that process. • Each log message has a facility and a priority. The facility tells you from which subsystem the message originated, and the priority tells you the message's importance • Programs send their log entries to syslogd, which consults the configuration file /etc/syslogd.conf or /etc/syslog and, when a match is found, writes the log message to the desired log file.			
IX.	route Using route is one of the easiest ways to display your route table—simply run route without any parameters. 2 Marks netstat -r the netstat program is used to display the status of all of the network connections on a host. with the -r option, it can display routing table. 2 Marks # ip route show table main The ip command can also be used to manipulate the routing table on a Linux host. This is done by using the route object with the ip command. The route command will display the default routing tables on the system—the main table. 3 Marks	2+2+3	7	7

X.	FTP used for transferring a file from one computer to another. It facilitates the exchange of files between an FTP client and an FTP server FTP uses two ports: a control port (port 21) and a data port (port 20). The control port serves as a communication channel between the client and the server for the exchange of commands and replies. The data port is used purely for the exchange of data, which can be a file, part of a file, or a directory listing FTP can operate in two modes: active FTP mode and passive FTP mode 2 Marks Active FTP mode: the client connects from a port to the FTPserver's command port (port 21). When the client is ready to transfer data, the server opens a connection from its data port (port 20) to the IP address and port combination provided by the client.The key here is that the client does not make the actual data connection to the server but instead informs the server of its own port by issuing the PORT command; the server then connects back to the specified port. The server can be regarded as the active party in this FTP mode. 2.5 Marks Passive FTP mode The FTP client issues the PASV command to indicate that it wants to access data in the passive mode, the server responds with an IP address and port number which is not its normal data port (port 20)to which the client can connect to transfer the data.Here the client tells the server to "listen" on a data port that is not its normal data port.The key difference here is that it is the client that initiates the connection to the port and IP address	2+ 2.5+2.5	7	7

	provided by the server. Here the server can be considered the passive party in the data communication. 2.5 Marks			
XI.	1. ServerRoot This is used for specifying the base directory for the web server by default, is the /etc/httpd/ directory Syntax: ServerRoot directory-path 2. Listen This is the port(s) on which the server listens for connection requests,the default value for this is 80 Syntax: Listen [IP-address:] portnumber 3. ServerName This defines the hostname and port that the server uses to identify itself. Syntax: ServerName fully-qualified-domain-name[: port] 4. ServerAdmin This is the e-mail address that the server includes in error messages sent to the client. Syntax: ServerAdmin e-mail_address 5. DocumentRoot This defines the primary directory on the web server from which HTML files will be served to requesting clients the default value for this is /var/www/html/ 6. MaxClients This sets a limit on the number of simultaneous requests that the web server will service 7. LoadModule This is used for loading or adding other modules into Apache's running configuration. It adds the specified module to the list of active modules. Syntax: LoadModule module filename	1x7	7	7
XII.	1. route:-is the command used for managing routes	1x7	7	7

	2. cmd:-Either add or del, depending on whether you are adding or deleting a route. If you are deleting a route, the only other parameter you need is addy. 3. type:-Either -net or -host, depending on whether addy represents a network address or a router address. 4. addy:-The destination network to which you want to offer a route. 5. netmask mask:-Sets the netmask of the addy address to mask. 6. gw gway:-Sets the router address for addy to gway. Typically used for the default route. 7. dev dn:-Sends all packets destined to addy through the networkdevice dn			
XIII.	• The amount of data that needs to be backed up: Determining exact count of the data to be backed up is an important when estimating backup needs, expected data growth must be included in data estimation. Data changes and change frequency must be considered. • Backup hardware and backup medium The type of hardware you choose should reflect the amount and type of data you need to back up, the frequency of when you're backing it up, and whether it is necessary that backups get rotated to an offsite location. The common choices available are tape, disk, recordable CDs, recordable DVDs,Storage Area Network (SAN), Network Attached Storage (NAS), and other networked storage arrays. • The amount of network throughput that needs to be supported Understand network infrastructure,Look at where the data is coming from and where it's going. consider a backup sequence that won't back up two	1x7	7	7

	machines on the same collision domain at the same time. Gathering all this information will help you estimate the bandwidth necessary to perform backups • The speed and ease of data recovery Recover response time must be considered while backup evaluation. Depending on the speed and ease of data recovery appropriate backup solution must be decided. there is no point of havg an expesive backup solution when the backed up data is not readily available to the people when they need it most. • Data deduplication issues Data deduplication deals with reducing unnecessary redundant data in a storage system. see how we could avoid accumulate multiple copies of the same data or files in the storage. redundancy is not only inefficient, but it adds to the total costs of performing backups • Tape management As the size of your backups grows, will need to manage the data you back up. while choosing backup tools consider their indexing and tape management features of the backup tool			
XIV.	Three of the main Samba daemons are: smbd, nmbd, and winbindd The **smbd** daemon handles the actual sharing of file systems and printer services for clients. It is also responsible for user authentication and resource-locking issues. Every time a client authenticates itself, smbd makes a copy of itself; the original goes back to listening to its primary port for new requests, and the copy handles the connection for the client. The copy stays in memory as long as there is a connection from	7	7	7

	the client. **The nmbd** daemon is responsible for handling NetBIOS name service requests. nmbd can also be used as a replacement Windows Internet Name Server (WINS).Unlike smbd, nmbd does not create a new instance of itself to handle every query. In addition to name service requests, nmbd handles requests from master browsers, domain browsers, and WINS servers.The services provided by the smbd and nmbd daemons complement each other **winbindd** is used to query native Windows servers for user and group information, which can then be used on purely Linux/UNIX platforms.It does this by using Microsoft Remote Procedure Call (RPC) calls, PAM, and the name service switch (NSS) capabilities.			

	provided by the server. Here the server can be considered the passive party in the data communication. 2.5 Marks			
XI.	1. ServerRoot This is used for specifying the base directory for the web server by default, is the /etc/httpd/ directory Syntax: ServerRoot directory-path 2. Listen This is the port(s) on which the server listens for connection requests,the default value for this is 80 Syntax: Listen [IP-address:] portnumber 3. ServerName This defines the hostname and port that the server uses to identify itself. Syntax: ServerName fully-qualified-domain-name[: port] 4. ServerAdmin This is the e-mail address that the server includes in error messages sent to the client. Syntax: ServerAdmin e-mail_address 5. DocumentRoot This defines the primary directory on the web server from which HTML files will be served to requesting clients the default value for this is /var/www/html/ 6. MaxClients This sets a limit on the number of simultaneous requests that the web server will service 7. LoadModule This is used for loading or adding other modules into Apache's running configuration. It adds the specified module to the list of active modules. Syntax: LoadModule module filename	1x7	7	7
XII.	1. route:-is the command used for managing routes	1x7	7	7