**Darey.io - PROJECT BASED LEARNING**

**1. Software Development Life Cycle (SDLC): is a process used by the software industry to design, develop and test high quality softwares.**

**2. Lamp Stack: The LAMP stack id an acronym denoting one of the most common software stacks for many of the web’s most popular applications. However, LAMP now refers to a generic software stack model and it’s components are largely interchangeable. The full meaning of the acronym LAMP is for the Operating system, LINUX; the web server, APACHE; The database server, MYSQL; and the programming language, PHP or PERL.**

**3. Understanding The concept of ‘chmod’ and ‘chown’ commands in linux:**

**In Linux, users can belong to one or more groups. Also, both users and groups can be the owners of files and directories. As well as details of ownership, each file has metadata about its access permissions. chown and chmod are the tools we use to manipulate ownership and access permissions of files and directories**

**Linux is a multi user OS which means that it supports multiple users at a time.**

**As many people can access the system simultaneously and some resources are shared, Linux controls access through ownership and permissions.**

## **Linux file ownership**

**In Linux, there are three types of owners: user, group, and others .**

### **Linux User**

**A user is the default owner and creator of the file. So this user is called owner as well.**

### **Linux Group**

**A user-group is a collection of users. Users that belonging to a group will have the same Linux group permissions to access a file/ folder.**

**You can use groups to assign permissions in a bulk instead of assigning them individually. A user can belong to more than one group as well.**

### **Other**

**Any users that are not part of the user or group classes belong to this class.**

## **Linux File Permissions**

**File permissions fall in three categories: read, write, and execute.**

### **Read permission**

**For regular files, read permissions allow users to open and read the file only. Users can't modify the file.**

**Similarly for directories, read permissions allow the listing of directory content without any modification in the directory.**

### **Write permission**

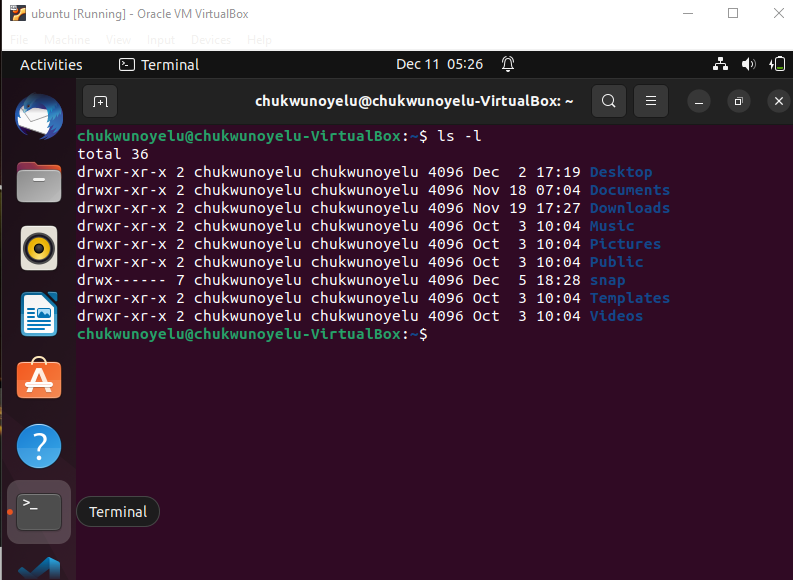
**When files have write permissions, the user can modify (edit, delete) the file and save it.**

**For folders, write permissions enable a user to modify its contents (create, delete, and rename the files inside it), and modify the contents of files that the user has write permissions to.**

### **Execute permission**

**For files, execute permissions allows the user to run an executable script. For directories, the user can access them, and access details about files in the directory.**

**Note that we can find permissions of files and folders using long listing (**l**s command)**

****

**4. Learn what TCP and UPD terms mean and how they are different. List down ports most commonly used in Web (http, https, ssh, telnet, ftp, sftp, telnet):**

**TCP stands for Transmission Control Protocol. UDP stands for User Datagram Protocol. Both protocols allow network applications to exchange data between nodes. The main difference between both is that TCP is a connection-oriented DNS**

### **IP protocol**

**IP stands for Internet Protocol. This protocol works with TCP and UDP protocols. It provides a unique identity to each node on the computer network. This identity is known as an IP address. An IP address is a software address of the node on a computer network. There are two versions of IP protocol: IPv4 and IPv6. IPv4 uses 32 bits to create an IP address while IPv6 uses 128 bits to create an IP address.**

**DNS**

**DNS stands for Domain Name Service. This service allows us to access a node by its name. By default, nodes use IP addresses to identify each other on the network. DNS service allows us to map a name to an IP address. When we access a node by its name, the DNS service translates the name into the IP address. Let's take an example.**

**Suppose you want to access the home page of Yahoo's site. For this, you enter the following address in your web browser.**

**https://www.yahoo.com**

**Your web browser connects the configured DNS server and sends a request to convert the entered address into the IP address. DNS server translates the address into the IP address and sends the IP address of Yahoo's site. Your browser accesses Yahoo's site and displays it on the viewport. Without DNS service, your browser will not be able to access Yahoo's site.**

### **NAT**

**NAT stands for Network Address Translation. This protocol translates one IP address to another. This can be a source address or a destination address. Two basic implementations of NAT can be used: static and dynamic. In the static NAT, a manual translation is performed. In the dynamic NAT, an automatic address translation is performed by an address translation device. Static NAT is used to translate destination IP addresses in packets as they come into your network, but you can translate source addresses also. Dynamic NAT is used to translate source IP addresses in packets as they go out of your network. In dynamic NAT, the global address assigned to the internal user isn’t that important, since outside devices don’t directly connect**

**to your internal users—they just return traffic to them that the inside user requested.**

**protocol while UDP is a connectionless protocol.**

### 

### **SNMP (Simple Network Management Protocol)**

**Simple Network Management Protocol is a TCP/IP protocol for monitoring networks and network components. SNMP uses small utility programs called agents to monitor behavior and traffic on the network. These agents can be loaded onto managed devices such as hubs, NIC's, servers, routers, and bridges. The gathered data is stored in a MIB (management information base). To collect the information in a usable form, a management program console polls these agents and downloads the information from their MIBs, which then can be displayed as graphs, charts and sent to a database program to be analyzed.**

### **SMB (Server Message Block)**

**SMB is a file-sharing protocol. It allows networked computers to transparently access files that reside on remote systems over a variety of networks. The SMB protocol defines a series of commands that pass information between computers. It is mainly used by Microsoft Windows-equipped computers. SMB works through a client-server approach, where a client makes specific requests and the server responds accordingly.**

### **FTP (File Transfer Protocol)**

**One of the earliest uses of the Internet, long before Web browsing came along, was transferring files between computers. The File Transfer Protocol (FTP) is used to connect to remote computers, list shared files, and either upload or download files between local and remote computers.**

**FTP runs over TCP, which provides a connection-oriented, guaranteed data-delivery service. FTP is a character-based command interface, although many FTP applications have graphical interfaces. FTP is still used for file transfer purposes, most commonly as a central FTP server with files available for download. Web browsers can make FTP requests to download programs from links selected on a Web page.**

### **TFTP (Trivial File Transfer Protocol)**

**TFTP is used when a file transfer does not require an acknowledgment packet during file transfer. TFTP is used often in the router configuration. TFTP is similar in operation to FTP. TFTP is also a command-line-based utility.**

**One of the two primary differences between TFTP and FTP is speed and authentication. Because TFTP is used without acknowledgment packets, it is usually faster than FTP. TFTP does not provide user authentication like FTP and therefore the user must be logged on to the client and the files on the remote computer must be writable. TFTP supports only unidirectional data transfer (unlike FTP, which supports bi-directional transfer). TFTP is operated over port 69.**

### **HTTP (Hypertext Transfer Protocol)**

**HTTP is often called the protocol of the Internet. HTTP received this designation because most Internet traffic is based on HTTP. When a user requests a Web resource, it is requested using HTTP. The following is a Web request:**

**http://www.example.com**

**When a client enters this address into a Web browser, DNS is called to resolve the Fully Qualified Domain Name (FQDN) to an IP address. When the address is resolved, an HTTP get request is sent to the Web server. The Web server responds with an HTTP send response. Such communication is done several times throughout a single session to a Web site. HTTP uses TCP for communication between clients and servers. HTTP operates on port 80.**

### **HTTPS (Hypertext Transfer Protocol Secure)**

**HTTPS is for Web sites using additional security features such as certificates. HTTPS is used when Web transactions are required to be secure. HTTPS uses a certificate-based technology such as VeriSign.**

**Certificate-based transactions offer mutual authentication between the client and the server. Mutual authentication ensures the server of the client identity and ensures the client of the server identity. HTTPS, in addition to using certificate-based authentication, encrypts all data packets sent during a session.**

### **SMTP (Simple Mail Transfer Protocol)**

**SMTP is a standard electronic-mail protocol that handles the sending of mail from one SMTP to another SMTP server. To accomplish the transport, the SMTP server has its MX (mail exchanger) record in the DNS database that corresponds to the domain for which it is configured to receive mail.**

**When equipped for two-way communication, mail clients are configured with the address of a POP3 server to receive mail and the address of an SMTP server to send mail. The clients can configure server parameters in the properties sheets of the mail client, basing the choices on an FQDN or an IP address.**

### **POP3 / IMAP4 (Post Office Protocol version 3 / Internet Message Access Protocol version 4)**

**Post Office Protocol 3 (POP3) and Internet Message Access Protocol 4 (IMAP4) are two application-layer protocols used for electronic messaging across the Internet. POP3 is a protocol that involves both a server and a client. A POP3 server receives an e-mail message and holds it for the user. A POP3 client application periodically checks the mailbox on the server to download mail. POP3 does not allow a client to send mail, only to receive it. POP3 transfers e-mail messages over TCP port 110.**

**IMAP4 is an alternate e-mail protocol. IMAP4 works in the same way as POP3. In this, an e-mail message is held on a server and then downloaded to an e-mail client application. Users can read their e-mail messages locally in their e-mail client application, but they can't send an e-mail message using IMAP4. When users access e-mail messages via IMAP4, they have the option to view just the message header, including its title and the sender's name, before downloading the body of the message. Users can create, change, or delete folders on the server, as well as search for messages and delete them from the server.**

### **Telnet**

**Telnet stands for Telecommunication Network. It is a virtual terminal protocol. It allows a user to access a system remotely. In remote control, a session appears in which the user can manage the files on the remote computer, although the session appears to be functioning locally. Telnet is an early version of a remote control application.**

**Telnet is very basic; it offers solely character-based access to another computer. You can often use Telnet to manage equipment that lacks a monitor. For example, most routers have Telnet enabled so that the administrator can log in and manage the router. Telnet also provides a quick check to make certain that network connectivity is functioning. Because Telnet sits at the application layer, if it can connect to a remote host, you can be certain that network connectivity between the two hosts is operational, as well as all lower-layer protocols.**

### **SSH (Secure Shell)**

**SSH is a program for logging in to and executing commands on a remote machine. It provides secure encrypted communications between two untrusted hosts over an insecure network. When SSH connects and logs in to a specified computer, the user must prove his/her identity to the remote machine which is transmitted across the connection using data encryption. This process makes SSH impervious to Internet eavesdroppers who might otherwise steal account information.**

### **ICMP (Internet Control Message Protocol)**

**ICMP provides network diagnostic functions and error reporting. ICMP also provides a little network help for routers. When a router is being overloaded with route requests, the router sends a source quench message to all clients on the network, instructing them to slow their data requests to the router.**

### **ARP (Address Resolution Protocol)**

**The Address Resolution Protocol (ARP) is an Internet layer protocol that helps TCP/IP network components find other devices in the same broadcast domain. ARP uses a local broadcast (255.255.255.255) at layer 3 and FF:FF:FF:FF:FF:FF at layer 2 to discover neighboring devices.**

### **RARP (Reverse Address Resolution Protocol)**

**RARP is sort of the reverse of an ARP. In an ARP, the device knows the layer 3 address, but not the data link-layer address. With a RARP, the device doesn’t have an IP address and wants to acquire one. The only address that this device has is a MAC address. Common protocols that use RARP are BOOTP and DHCP**

### **NTP (Network Time Protocol)**

**The Network Time Protocol is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem. It provides accuracy's typically within a millisecond on LANs and up to a few tens of milliseconds on WANs.**

### **SCP (Secure Copy Protocol)**

**Secure Copy or SCP is a means of securely transferring computer files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol. The protocol itself does not provide authentication and security; it expects the underlying protocol, SSH, to secure this. The SCP protocol implements file transfers only. It does so by connecting to the host using SSH and there executes an SCP server (SCP). SCP server connects with SCP client and transfers files securely.**

### **LDAP (Lightweight Directory Access Protocol)**

**Lightweight Directory Access Protocol, or LDAP, is a networking protocol for querying and modifying directory services running over TCP/IP. A directory is a set of information with similar attributes organized logically and hierarchically. The most common example is the telephone directory, which consists of a series of names organized alphabetically, with an address and phone number attached.**

### **IGMP (Internet Group Multicast Protocol)**

**The Internet Group Management Protocol is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming and allows more efficient use of resources when supporting these uses.**

### **LPD (Line Printer Daemon) /LPR (Line Printer Remote)**

**The Line Printer Daemon protocol/Line Printer Remote protocol (or LPD, LPR) also known as the Berkeley printing system, is a set of programs that provide printer spooling and network print server functionality for Unix-like systems.**

**The most common implementations of LPD are the official BSD UNIX operating system and the LPRng project. The Common Unix Printing System (or CUPS), which is more common on modern Linux distributions, borrows heavily from LPD.**