|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Agnel Charities*  **Fr. C. Rodrigues Institute of Technology, Vashi**  **Department of Electronics and Telecommunication Engg.**  **SUB:-Linux & Networking & Server Configuration ( LNSC) ECL-604** | | |  |  |
| **Telnet Server Setup on Ubuntu** | | |  |
| **EXPT NO** | **13** |  |  |
| **AIM** | **Telnet Server Setup** | |  |
| **THEORY**  **PROCEDURE** | Telnet is a remote login program. Telnet is a protocol used to provide remote access to a command-line interface over a network. The protocol was initially designed for interacting with remote computer systems through a terminal emulation program. Telnet is still widely used today, although it has been largely replaced by more secure protocols like SSH.   |  |  | | --- | --- | |  | How to Configure Telnet Service on Linux Machine | Learn Linux CCNA CEH  IPv6 Cyber-Security Online |   Telnet is a network protocol used to virtually access a computer and to provide a two-way, collaborative and text-based communication channel between two machines. It follows a user command Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocol for creating remote sessions. The Telnet protocol uses a client-server architecture, where the Telnet server runs on a remote computer system, and the Telnet client runs on a local computer system. The Telnet client initiates a connection to the Telnet server by specifying the hostname or IP address of the server and the port number on which the Telnet server is listening.  Once a connection is established, the Telnet client sends all user input to the Telnet server, which processes the input and sends back the output. The Telnet server can execute any command that is available on the system, and the output is displayed on the Telnet client's screen.  Telnet is an unencrypted protocol, which means that all data transmitted over the network can be intercepted and read by anyone with access to the network. This makes Telnet insecure for transmitting sensitive information, such as login credentials or financial data. To address this security concern, a more secure alternative called SSH was developed, which uses encryption to protect the data transmitted over the network.  The steps for setting up and using a Telnet server:  **Step 1: Install the Telnet server software** On a Linux machine, you can install the Telnet server software package using the package manager (e.g., **"yum install telnet-server" or "apt-get install telnetd")**.  You can install a Telnet server software package on your server depending on the operating system you are using. For example, on a Windows machine, you can enable the Telnet server from the "Turn Windows features on or off" menu.    **Step 2: Configure the Telnet server** After installing the Telnet server, you need to configure it by editing the configuration file. The location and name of the configuration file depend on the Telnet server software you are using. In the configuration file, you can specify the port number on which the Telnet server will listen, the maximum number of concurrent connections, the authentication mechanism to use (e.g., username/password or public key authentication), and other settings.  **Make sure firewall settings and port for telnet**  **# ufw status** ………if inactive type next cmd  **#ufw enable** ………observe active status of telnet  #ufw allow 23 …….telnet port number , rule added  #ufw status ……verify status ,allowed  #apt install net-tools -y …….to run net cmds  #ifconfig …..to know ip address of telnet server  **Step 3: Start the Telnet server** Once you have configured the Telnet server, you can start it by running the appropriate command. Again, the command depends on the Telnet server software you are using. For example, on a Linux machine, you can start the Telnet server by running the "**systemctl start telnetd**" command. | |  |
|  | **Step 4: Connect to the Telnet server** from windows and or linux machine in network: To connect to the Telnet server, you need a Telnet client application installed on your local machine. Most operating systems come with a Telnet client pre-installed. To connect to the Telnet server, you need to specify the **hostname or IP address of the server and the port number on which the Telnet server is listening**. Once you establish a connection, you **can interact with the remote command-line interface as if you were physically present on the server.**  From windows 10 or11 open **‘ control panel’,** click on **‘programs and features’,** click on **‘Turn Windows features on or off’ ,** search **’ Telnet Client’ and tick the check box.** After completion of requested changes click on close.  Windows 10: Install Telnet Client  Now type **‘run’ on windows start , open cmd prompt,**  On cmd prompt type **telnet ip address of telnet server machine**  **c:\users\admin> telnet** [**192.168.110.11**](file:///\\192.168.110.11)  **Enter login credential of server : type user login name and password.**  **Observe Ubuntu telnet server terminal is accessible on windows ,run linux commands, run some python files…**    **Step 5: Disconnect from the Telnet server** To disconnect from the Telnet server, you can either type **"exit" or "quit"** at the command prompt or use the Telnet client's disconnect command. On Ubuntu machine you can stop service:  **#systemctl stop telnetd** | |  |
| **CONCLUSION** | Setting up a Telnet server on Ubuntu can be a useful lab experiment to learn about remote access and networking protocols and how it works. However it is important to note that Telnet is an unencrypted protocol and is not secure for transmitting sensitive information. Therefore, it is not recommended to use Telnet in a production environment. It is strongly recommended to use a more secure alternative like SSH instead. Additionally, it is important to take proper security measures, such as configuring firewalls and implementing user authentication, to protect the Telnet server from unauthorized access and potential security threats. | |  |