Podili sunil gopi
B.tech iv year, IT
208X1A1229
KALLAM HARANADHAREDDY
INSTITUTE OF TECH.

Task -2

1. Port 20(FTP): 1. Traditionally used for FTP data transfer (server-side). 2. Not always used in modern setups due to security concerns and alternatives. 3. Caution advised, as other applications can use it and FTP itself has vulnerabilities.

2. Port 21(FTP): FTP's chatty commander, barking orders (upload, download) but leaving data deliveries to others. Unencrypted, so anyone can listen in! Use secure options like SFTP (port 22) for sensitive files.

3. Port 22(SECURE SHELL): SSH's secure gateway, whisking data encrypted between computers, unlike chatty FTP's megaphone.

4. Port23(Telnet): Once the go-to for remote access (Telnet), but now a security nightmare due to no encryption. Opt for secure alternatives like SSH (port 22) to keep your data safe and hush-hush.

5. Port25(SMTP): Port 25 can be associated with sending email (SMTP), but its use is declining due to security concerns and the adoption of more secure alternatives. For standard email usage, consult your email provider or client for the recommended port settings, as port 25 might be blocked.

6. Port 53(DNS): Port 53 is one of the most critical ports on the internet, ensuring smooth website navigation. While tampering with this port is uncommon, it's essential to use reputable DNS servers for security and privacy.
7. Port 67/68(DHCP) : Port 67: Listens on the server side, waiting for requests from devices. Port 68: Used by devices to broadcast requests for configuration information.

8. Port 80(HTTP): Port 80 is the default port for HTTP, the protocol that allows you to access websites. When you type a URL into your web browser, it sends a request to the website's server on port 80. The server then sends back the website's files, which your browser displays. Port 80 is not encrypted, which means that anyone who can see your traffic can see the data that is being sent between your browser and the website. This includes things like your login credentials, credit card numbers, and other sensitive information.

9. Port 123(NTP): the designated channel for NTP, a protocol that synchronizes computer clocks across the internet. Think of it as a global timekeeper, ensuring smooth operation for various applications, like financial transactions or online gaming.

10. Port 161/162(SNMP): Primarily used by SNMP managers to send commands and requests to SNMP agents on network devices. Think of it as the manager instructing the workers. Port 162: Used by SNMP agents to send notifications (traps) back to the manager about events or issues on the network. Imagine the workers alerting the manager of any problems.

11. Port 389(LDAP): Enables applications to access and manage information in directory services, like user authentication, authorization, and directory lookup. A phonebook for the digital world, storing user information like usernames, passwords, and group memberships.

12. Port 443(HTTPS): The default port for Hypertext Transfer Protocol Secure (HTTPS). Purpose: Establishes secure communication over the internet by encrypting data. Think of it as: A secure tunnel protecting information like credit card numbers or login credentials when browsing websites.