**ASIM SHIKHAR 21BCE2595**

***PORTS AND THEIR VULNERABILITES***

**Port 20 (FTP - File Transfer Protocol, Data Port):**

Description: Port 20 is used as the data port for FTP, a protocol for transferring files over a network.

Vulnerabilities: FTP, especially in its unencrypted form (FTP without TLS/SSL), can be vulnerable to eavesdropping and data interception. Additionally, FTP servers can be targeted for unauthorized access, potentially leading to data breaches.

**Port 21 (FTP - File Transfer Protocol, Control Port):**

Description: Port 21 is used as the control port for FTP, handling commands and control functions.

Vulnerabilities: Similar to port 20, FTP on port 21 can also be vulnerable to eavesdropping and unauthorized access if not properly secured. FTP is an old protocol and lacks some of the security features of modern file transfer methods.

**Port 22 (SSH - Secure Shell):**

Description: Port 22 is used for SSH, a secure protocol for remote access and secure file transfers.

Vulnerabilities: While SSH is considered secure when properly configured, it can be vulnerable to brute force attacks if weak passwords are used or if security configurations are not set up correctly. Additionally, outdated SSH server software may have known vulnerabilities.

**Port 23 (Telnet - Telecommunication Network):**

Description: Port 23 is used for Telnet, a protocol for remote terminal access.

Vulnerabilities: Telnet is highly insecure as it transmits data, including login credentials, in plain text. Attackers can easily intercept sensitive information when Telnet is used, making it a significant security risk.

**Port 24 (Private Use):**

Description: Port 24 is designated for private use and doesn't have a standard, well-defined application associated with it.

Vulnerabilities: Vulnerabilities on port 24 would depend on the specific application or service using it, which can vary widely.

**Port 25 (SMTP - Simple Mail Transfer Protocol):**

Description: Port 25 is used for SMTP, a protocol for sending email messages between servers.

Vulnerabilities: Port 25 can be vulnerable to email-related threats, such as spam, phishing, and email spoofing. Misconfigured SMTP servers can also be exploited by attackers to send malicious emails.

**Port 53 (DNS - Domain Name System):**

Description: Port 53 is used for DNS, which translates human-readable domain names into IP addresses.

Vulnerabilities: DNS is vulnerable to various attacks, including DNS spoofing, cache poisoning, and Distributed Denial of Service (DDoS) attacks. If an attacker can manipulate DNS responses, they can redirect users to malicious websites.

**Port 69 (TFTP - Trivial File Transfer Protocol):**

Description: Port 69 is used for TFTP, a simple file transfer protocol.

Vulnerabilities: TFTP lacks authentication and encryption, making it susceptible to unauthorized access and data interception. It should only be used in trusted, controlled environments.

**Port 80 (HTTP - Hypertext Transfer Protocol):**

Description: Port 80 is used for HTTP, the protocol for web browsing.

Vulnerabilities: HTTP traffic is often unencrypted, which can lead to data interception. Vulnerabilities in web server software or applications running on port 80 can be exploited by attackers to compromise web servers or steal data.

**Port 123 (NTP - Network Time Protocol):**

Description: Port 123 is used for NTP, a protocol for synchronizing system clocks on a network.

Vulnerabilities: NTP can be susceptible to DDoS attacks when it's used in amplification attacks. Attackers can also manipulate time synchronization, which can affect various network services.

**Port 110 (POP3 - Post Office Protocol version 3):**

Description: Port 110 is used for POP3, a protocol for retrieving email from a mail server.

Vulnerabilities: POP3 can be vulnerable to unauthorized access if weak passwords are used. Additionally, it typically transmits email messages in plain text, which can expose email contents to interception.

**Port 143 (IMAP - Internet Message Access Protocol):**

Description: Port 143 is used for IMAP, a protocol for retrieving and managing email from a mail server.

Vulnerabilities: Like POP3, IMAP can also be vulnerable to unauthorized access if weak passwords are used. IMAP, however, offers more advanced features and can be configured to use encryption (IMAPS) to enhance security.