**TASK-2**

**Port and Vulnerabilities**

**Port no 20 (FTP-DATA)& Port no 21(FTP)-File Transfer Protocol (FTP) ports that let users send and receive files from servers.**

* FTP doesn’t have encryption for data transfer or authentication
* Can easily exploit this port through cross-site scripting, brute-forcing passwords, and directory traversal attacks.

**Port no 22(SSH)- Used for remote management, TCP port for ensuring** [**secure remote access**](https://www.netwrix.com/remote_access_security_best_practices.html?cID=70170000000kgEZ) **to servers.**

* Hackers can exploit port 22 by using leaked SSH keys or brute-forcing credentials.
* Threat actors can exploit this port by using a private key to gain access to the system

**Port no 23(TELNET)- TCP protocol that lets users connect to remote devices**

* vulnerable to spoofing, malware, credential brute-forcing, and credential sniffing.

**Port no 25(SMTP)- Simple Mail Transfer Protocol, TCP port for receiving and sending emails**

* vulnerable to spoofing and mail spamming if not secure.

**Port no 53(DNS)- Used for zone transfers and maintaining coherence between the server and the DNS database**

* A common exploit on the DNS ports is the Distributed Denial of Service (DDoS) attack.

**Port no 69(TFTP)-Trivial File Transfer Protocol, used to send and receive files between users and servers.**

* it’s a UDP port, it doesn’t require authentication, which means it’s faster but less secure.
* does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to trick TFTP into giving access to files.
* can be exploited using password spraying

**Port no 80(HTTP)- HyperText Transfer Protocol**

* Vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.

**Port no 110(POP3)-Known as the Post Office Protocol, it is used by email clients to synchronize and download mail from remote mail servers**

* Brute Force Attacks: Attackers can attempt to guess email account passwords through brute force attacks, exploiting weak or commonly used passwords.
* Email Account Compromise: Once attackers gain access to email accounts, they can read, modify, or delete sensitive information. They may also use compromised accounts for spam or phishing campaigns.
* Data Interception: Email data transmitted through this port can be intercepted by attackers if not properly encrypted.

**Port no 123(NTP)-allows the synchronization of system clocks (from desktops to servers)**

* Reflection/Amplification DDoS: The Network Time Protocol (NTP) can be abused by attackers to initiate Distributed Denial of Service (DDoS) attacks using reflection and amplification techniques.
* Time Skewing: If NTP servers are misconfigured or improperly secured, attackers can manipulate time settings, causing synchronization issues across a network.

**Port no 143(IMAP)-Internet Message Access Protocol is an application layer Internet protocol that allows an e-mail client to access email on a remote mail server.**

* Brute Force Attacks: Just like with POP3, attackers can target IMAP servers with brute force attacks to gain unauthorized access to email accounts.
* Email Exposure: IMAP allows attackers to access email folders and content, potentially exposing sensitive information or intellectual property.
* Malicious Attachment Upload: Attackers can use compromised accounts to upload malicious attachments, which could lead to malware distribution or other cyber threats.
* Email Manipulation: Attackers could modify or delete emails, leading to data loss or tampering.

**Port no 443(HTTPS)- HyperText Transfer Protocol Secure (**[**which is the more secure version of HTTP**](https://www.makeuseof.com/tag/ssl-certificate-need-one/)**)**

* vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.