Task-2

FIND THE VULNERABILTIES PERFOMED ON THE DIFFERENT PORTS :

1.Port no. (20,21)

port number 20 ,21 is commonly associated with ftp(file transfer protocol).

FTP stands for File Transfer Protocol. Port 20 and 21 are solely TCP ports used to allow users to send and to receive files from a server to their personal computers.

The FTP port is insecure and outdated and can be exploited using:

- Anonymous authentication. You can log into the FTP port with both username and password set to "anonymous".
- Cross-Site Scripting.
- Brute-forcing passwords.
- Directory traversal attacks.

2.(port no.22) SSH (22)

SSH stands for Secure Shell. It is a TCP port used to ensure secure remote access to servers. You can exploit the SSH port by brute-forcing SSH credentials or using a private key to gain access to the target system.

3.port no.23[Telnet (23)]

The Telnet protocol is a TCP protocol that enables a user to connect to remote computers over the internet. The Telnet port has long been replaced by SSH, but it is still used by some websites today. It is outdated, insecure, and vulnerable to malware. Telnet is vulnerable to spoofing, credential sniffing, and credential brute-forcing.

4. SMTP (25)

SMTP stands for Simple Mail Transfer Protocol. It is a TCP port used for sending and receiving mails. It can be vulnerable to mail spamming and spoofing if not well-secured

5. DNS (53)

DNS stands for Domain Name System. It is both a TCP and UDP port used for transfers and queries respectively. One common exploit on the DNS ports is the Distributed Denial of Service (DDoS) attack.

6. TFTP (69)

TFTP stands for Trivial File Transfer Protocol. It's a UDP port used to send and receive files between a user and a server over a network. TFTP is a simplified version of the file transfer protocol. Because it is a UDP port, it does not require authentication, which makes it faster yet less secure.

7.port no.80 HTTP / HTTPS (443, 80, 8080, 8443)

HTTP stands for HyperText Transfer Protocol, while HTTPS stands for HyperText Transfer Protocol Secure (secure than HTTP). These are the most popular and widely used protocols on the internet, and as such are prone to many vulnerabilities. They are vulnerable to SQL injections, cross-site scripting, cross-site request forgery, etc

8.Port no.110 [post office protocol]:-

Port 110 is associated with the Post Office Protocol version 3 (POP3), which is used for receiving email messages from a mail server to a client device. This protocol is quite old and lacks encryption by default, making it vulnerable to several security issues. Here are a couple of vulnerabilities associated with port 110:

1. **Plain Text Transmission:** POP3 was designed without encryption in mind, meaning that usernames and passwords are sent in plain text. This makes it susceptible to eavesdropping attacks, where malicious actors can intercept the data being transmitted and gain access to login credentials.
2. **Brute Force Attacks:** Since the authentication process in POP3 involves sending the username and password in clear text, attackers can attempt to brute force login credentials with relative ease. Without proper security measures, this can lead to unauthorized access.
3. **Credential Harvesting:** Attackers can exploit vulnerabilities in the mail client or server software to harvest usernames and passwords, potentially leading to unauthorized access not only to email accounts but also to other services if the same credentials are reused.
4. **Lack of Encryption:** The lack of encryption means that messages and attachments transferred between the server and the client can be intercepted and read by anyone with access to the network traffic.

To mitigate these vulnerabilities, it's recommended to:

- Use secure variants of email protocols such as POP3 over TLS (POP3S) or Internet Message Access Protocol (IMAPS) over TLS, which encrypt the communication between the client and the server.
- Implement strong, unique passwords for email accounts.
- Regularly update email client software to ensure security patches are applied.
- Employ network security measures like firewalls and intrusion detection systems to detect and prevent unauthorized access.

- Educate users about the risks of plain text authentication and encourage them to use secure alternatives.

9.Port 123 [Network time protocol] :

Port 123 is used for the Network Time Protocol (NTP), which is used for synchronizing clocks on computer systems. Some vulnerabilities associated with NTP include:

1. Amplification Attacks: NTP servers can be exploited in amplification attacks where attackers send small requests with a forged source IP address to NTP servers. The servers then respond with larger amounts of data to the spoofed IP address, potentially causing DDoS attacks.

2. Reflection Attacks: Similar to amplification attacks, reflection attacks involve sending requests to NTP servers, which then reply to the target IP address with a larger response. This can be used to overload target systems.

3. Denial of Service (DoS): NTP vulnerabilities can be exploited to launch DoS attacks against servers by sending specially crafted packets that consume resources and disrupt normal functionality.

To mitigate these vulnerabilities, network administrators should:

- Implement access control and filtering mechanisms to prevent unauthorized access to NTP servers.

- Regularly update NTP software to patch known vulnerabilities.

- Use rate limiting and other techniques to prevent amplification and reflection attacks.

- Monitor NTP server traffic for unusual patterns.

9.Port 143[internet message protocol]:

Port 143 is associated with the Internet Message Access Protocol (IMAP), used for receiving email messages from a mail server to a client device. Some vulnerabilities associated with IMAP include:

1. **Brute Force Attacks:** Attackers can attempt to brute force login credentials due to the lack of encryption during the authentication process in standard IMAP.

2. **Data Exposure:** Similar to POP3, without encryption, messages and attachments transferred between the server and client can be intercepted and read by malicious actors.

3. Email Spoofing and Phishing: Vulnerabilities in email clients or servers can lead to email spoofing, where attackers send emails that appear to be from a legitimate source to deceive recipients into taking harmful actions.

To enhance security:

- Use IMAPS (IMAP over TLS) to encrypt communication between clients and servers.

- Ensure email clients and servers are updated with the latest security patches.

- Educate users about email security, phishing, and the importance of strong passwords.

11.Port 443:

Port 443 is used for secure communications over the HTTPS protocol, often associated with web browsing and encrypted data transfer. While this port is generally considered secure due to the use of SSL/TLS encryption, vulnerabilities can still arise:

1. TLS Vulnerabilities: Weaknesses in the SSL/TLS protocols can lead to vulnerabilities such as Heartbleed, POODLE, and others that compromise the encryption and expose sensitive data.

2. Certificate Vulnerabilities: Expired, misconfigured, or compromised SSL certificates can lead to security risks.

3. Man-in-the-Middle Attacks: While SSL/TLS is designed to prevent this, misconfigurations or compromised certificates can enable attackers to intercept and modify data.

To ensure security:

- Use strong encryption protocols and keep them updated.
- Regularly renew and verify SSL certificates.
- Stay informed about emerging SSL/TLS vulnerabilities and apply patches promptly.