Saumyaa Prajapat
21BCI0265

Task2:

1. **Port 20 (FTP Data Transfer):**

- Description:

Port 20 is used for FTP (File Transfer Protocol) data transfer, where actual files are transferred between the client and the server.

- Vulnerabilities:
  - Data Interception: Data transferred over FTP is not encrypted by default, making it susceptible to interception by attackers monitoring the network.
  - Brute Force Attacks: Attackers can attempt to guess login credentials through brute force, as FTP doesn't usually have strong mechanisms to prevent such attacks.

2. **Port 21 (FTP Control):**

- Description:

Port 21 is used for FTP control commands, including authentication and managing files on the server.

- Vulnerabilities:
  - Command Injection: Malicious input can be used to inject commands into the FTP server, potentially leading to unauthorized access or data manipulation.
  - Weak Authentication: FTP's reliance on plain text authentication makes it vulnerable to credential sniffing and brute force attacks.

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

- Description:

Port 22 is the default port for SSH, a secure protocol used for remote access and secure command execution on remote machines.

- Vulnerabilities:
  - Brute Force Attacks: If weak passwords are used, attackers can launch brute force attacks to gain unauthorized access.
  - Vulnerabilities in SSH Implementations: Flaws in SSH server software can lead to vulnerabilities that attackers could exploit to gain access to a system.

4. **Port 23 (Telnet):**

- Description:

Port 23 is used for Telnet, a protocol that allows remote command-line access to a system.

- Vulnerabilities:
  - Plain Text Communication: Telnet sends data, including passwords, in plain text, making it susceptible to eavesdropping and sniffing attacks.
  - Unauthorized Access: Weak or default passwords can lead to unauthorized access, and attackers can also perform brute force attacks.

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

- Description:

Port 25 is used for SMTP, the protocol responsible for sending and relaying email messages between servers.

- Vulnerabilities:

- Email Spoofing: Lack of strong authentication can lead to email spoofing, where attackers send emails that appear to come from a legitimate source.
- Mail Relaying: Misconfigured SMTP servers can be exploited by attackers to relay spam or phishing emails through them.

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

- Description:

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

- Vulnerabilities:
  - DNS Spoofing: Attackers can manipulate DNS responses to redirect users to malicious websites, leading to phishing or malware distribution.
  - DNS Amplification Attacks: Misconfigured DNS servers can be abused to amplify DDoS attacks, overwhelming target systems with traffic.

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

- Description:

Port 69 is used for TFTP, a simplified version of FTP often used for transferring firmware and configuration files.

- Vulnerabilities:
  - Lack of Authentication: TFTP lacks strong authentication mechanisms, making it susceptible to unauthorized access and file manipulation.
  - Lack of Encryption: Data transferred via TFTP is not encrypted, exposing sensitive information to interception.

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

- Description:

Port 80 is the default port for HTTP, used for serving web pages and resources over the internet.

- Vulnerabilities:
  - Cross-Site Scripting (XSS): Poorly sanitized user inputs can lead to malicious scripts being executed in users' browsers, compromising their security.
  - SQL Injection: Improperly sanitized database queries can allow attackers to manipulate databases and gain unauthorized access to data.

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

- Description:

Port 110 is used for POP3, a protocol for retrieving email from a mail server to a client.

- Vulnerabilities:
  - Plain Text Authentication: POP3 originally used plain text passwords, making it vulnerable to eavesdropping and password interception.
  - Email Download Without Encryption: Emails downloaded using POP3 are typically not encrypted during transmission, potentially exposing sensitive content.

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

- Description:

Port 123 is used for NTP, a protocol for synchronizing the time of computer systems over a network.

- Vulnerabilities:

- NTP Amplification Attacks: Misconfigured NTP servers can be exploited to amplify DDoS attacks, similar to DNS amplification attacks.
- Time-Based Attacks: Manipulating time synchronization can impact the security of cryptographic protocols relying on accurate time.

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

- Description:

Port 143 is used for IMAP, a protocol for accessing and managing email on a remote mail server.

- Vulnerabilities:
  - Cleartext Credentials: IMAP originally transmitted passwords in cleartext, allowing attackers to intercept them and gain unauthorized access.
  - Email Content Exposure: IMAP's synchronization nature can expose email content, potentially including sensitive information, to attackers.

12. **Port 443 (HTTPS - Hypertext Transfer Protocol Secure):**

- Description:

Port 443 is the default port for HTTPS, the secure version of HTTP, used for encrypted communication and secure data transmission.

- Vulnerabilities:
  - TLS/SSL Vulnerabilities: Weak SSL/TLS configurations or vulnerabilities in the SSL/TLS protocol itself can lead to data breaches and man-in-the-middle attacks.
  - Certificate Issues: Improperly configured or expired SSL certificates can result in browser warnings and potential security risks.