Name :- Ch.V.S.Dhiraj Reg No :- 21BCE5717

Task - 2

Different types of port Vulnerabilities :-

1.) Port 20(FTP) :-

- Protocol used :- TCP
- Vulnerabilities :-

FTP is known for being outdated and insecure. As such, attackers frequently exploit it through :-

- Brute-forcing passwords.
- Anonymous authentication.
- Cross-site scripting.
- Directory traversal attacks.

2.) Port 21(FTP) :-

- Protocol used :- TCP
- Vulnerabilities :-

FTP is known for being outdated and insecure. As such, attackers frequently exploit it through:-

1. Brute-forcing passwords.
2. Anonymous authentication.
3. Cross-site scripting.

4. Directory traversal attacks.

3.) Port 22(SSH) :-

- Protocol used :- TCP
- Vulnerabilities :-

Port 22 is for Secure Shell (SSH). It's a TCP port for ensuring secure access to servers. Hackers can exploit port 22 by using leaked SSH keys or brute-forcing credentials.

4.) Port 23(TELNET) :-

- Protocol used :- TCP
- Vulnerabilities :-

Port 23 is a TCP protocol that connects users to remote computers. For the most part, Telnet has been superseded by SSH, but it's still used by some websites. Since it's outdated and insecure, it's vulnerable to many attacks, including credential brute forcing, spoofing and credential sniffing.

5.) Port 25(SMTP) :-

- Protocol used :- TCP

- Vulnerabilities :-

Port 25 is a Simple Mail Transfer Protocol (SMTP) port for receiving and sending emails. Without proper configuration and protection, this TCP port is vulnerable to spoofing and spamming.

6.) Port 53(DNS) :-

- Protocol used :- TCP and UDP.
- Vulnerabilities :-

Port 53 is for Domain Name System (DNS). It's a UDP and TCP port for queries and transfers, respectively. This port is particularly vulnerable to DDoS attacks.

7.) Port 69(TFTP) :-

- Protocol used :- UDP.
- Vulnerabilities :-

SolarWinds TFTP (Trivial File Transfer Protocol) Server is vulnerable to a denial of service, caused by an error when handling Read Request requests.

By sending a specially-crafted Read Request to UDP port 69, a remote attacker could exploit this vulnerability to cause the server process to crash.

8.) Port 80(HTTP) :-

- Protocol used :- TCP and UDP.
- Vulnerabilities :-

HTTP is the hottest protocol on the internet, so it is often targeted by attackers. It is especially vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.

9.) Port 110(POP3) :-

- Protocol used :- TCP.
- Vulnerabilities :-

1.) Unencrypted Communication.

2.) Brute Force Attacks.

3.) Email Spoofing and Phishing.

4.) Data Interception.

5.) Credential Harvesting.

6.) Mailbox Manipulation.

- Both this and IMAP port has the same vulnerabilities.

10.) Port 123(NTP) :-

- Protocol used :- TCP.
- Vulnerabilities :-

If open the attackers can attack this port using DDOS attacks, inject malicious codes, disrupt the server, intercept with network time synchronization. It can also provide attackers with sensitive information to exploit.

11.) Port 143(IMAP) :-

- Protocol used :- TCP.
- Vulnerabilities :-

1.) Unencrypted Communication.

2.) Brute Force Attacks.

3.) Email Spoofing and Phishing.

4.) Data Interception.

5.) Credential Harvesting.
6.) Mailbox Manipulation.

12.) Port 143(HTTPS) :-

- Protocol used :- TCP.
- Vulnerabilities :-

HTTPS is the hottest protocol on the internet, so it is often targeted by attackers. It is especially vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.