Stuti Maitra Sarkar
21BCI0126

Ports:

1. Port 20/21 (FTP):

- Vulnerabilities: FTP, or File Transfer Protocol, can be vulnerable to unauthorized access if weak or default credentials are used. It's susceptible to brute force attacks and can expose sensitive data during file transfers. Additionally, FTP bounce attacks can be used to conduct port scans and bounce traffic through an FTP server to reach other services.

2. Port 22 (SSH):

- Vulnerabilities: SSH, or Secure Shell, is generally considered secure but can be vulnerable to attacks if server configuration is not properly maintained. Vulnerabilities may include weak user passwords, outdated SSH server software, and brute force attacks, which can lead to unauthorized access to systems.

3. Port 23 (Telnet):

- Vulnerabilities: Telnet, a legacy protocol, is highly insecure as it transmits data, including login credentials, in plain text. Attackers can intercept this information and potentially gain unauthorized access to systems. The use of Telnet is strongly discouraged in favor of more secure alternatives like SSH.

4. Port 25 (SMTP):

- Vulnerabilities: SMTP servers may have vulnerabilities that could lead to email spoofing, spam attacks, and email relaying. Misconfigured SMTP servers can be used in phishing campaigns, potentially compromising email communications.

5. Port 53 (DNS):

- Vulnerabilities: DNS servers can be targeted in various ways, including DNS cache poisoning, amplification attacks, and distributed denial-of-service (DDoS) attacks. Exploiting vulnerabilities in DNS servers can lead to disruptions in network services and DNS hijacking.

6. Port 69 (TFTP):

- Vulnerabilities: Trivial File Transfer Protocol (TFTP) is known for its lack of security features. Vulnerabilities in TFTP can result in unauthorized file access, data tampering, and even the execution of malicious files if not properly secured.

Stuti Maitra Sarkar
21BCI0126
Task 1

7. Port 80 (HTTP):

- Vulnerabilities: Web servers running on port 80 may be vulnerable to a range of web-based attacks, including SQL injection, cross-site scripting (XSS), and server misconfigurations. These vulnerabilities can result in website defacement, data breaches, and unauthorized access.

8. Port 110 (POP3):

- Vulnerabilities: POP3 servers can be vulnerable to unauthorized email access if weak or stolen credentials are used. They are also susceptible to attacks like man-in-the-middle (MITM), where an attacker can intercept emails being transferred between the server and the client.

9. Port 123 (NTP):

- Vulnerabilities: Network Time Protocol (NTP) servers can be abused for distributed denial-of-service (DDoS) amplification attacks. Vulnerabilities in NTP servers can result in the exploitation of servers and disrupt network time synchronization, affecting various network services.

10. Port 143 (IMAP):

- Vulnerabilities: IMAP servers, similar to POP3, can be susceptible to unauthorized email access and interception if strong authentication and encryption mechanisms are not in place. Vulnerabilities can result in data exposure and compromise of email communication.

11. Port 443 (HTTPS):

- Vulnerabilities: While HTTPS (HTTP over TLS/SSL) is secure in terms of data encryption during transmission, the web applications and services running on HTTPS can have vulnerabilities. Common issues include misconfigurations, server vulnerabilities, and web application flaws like SQL injection, which can lead to data leaks or unauthorized access.

Proper security practices such as regular updates and patches, strong authentication, encryption, firewall rules, intrusion detection systems, and vigilant monitoring are essential for mitigating these vulnerabilities. Additionally, conducting penetration testing and vulnerability assessments can help identify and address potential weaknesses on open ports.