**Name: Lakshmi Likitha Malemarpuram**

**Reg no: 21BCE8963**

**Email:** [**likitha.21bce8963@vitapstudent.ac.in**](mailto:likitha.21bce8963@vitapstudent.ac.in)

**DATE: 24-08-2023**

**DAY: THURSDAY**

**TASK 2 – Ports and Vulnerabilities**

1. Port 20/21 (FTP):

- Use: FTP Data Transfer (20) and FTP Control (21).

- Vulnerabilities: Brute force attacks, unauthorized file transfers.

- Hacking Actions: Brute forcing credentials, uploading/downloading malicious files.

2. Port 22 (SSH):

- Use: SSH (Secure Shell) for remote access.

- Vulnerabilities: Brute force attacks, insecure key management.

- Hacking Actions: Brute forcing, exploiting weak SSH keys.

3. Port 23 (Telnet):

- Use: Telnet for remote command-line access.

- Vulnerabilities: Plain text communication, command injection.

- Hacking Actions: Sniffing credentials, injecting malicious commands.

4. Port 25 (SMTP):

- Use: SMTP for sending emails.

- Vulnerabilities: Email spoofing, email bombing.

- Hacking Actions: Spoofing emails, overwhelming email servers.

5. Port 53 (DNS):

- Use: DNS for domain name resolution.

- Vulnerabilities: DNS hijacking, amplification attacks.

- Hacking Actions: Redirecting users, DDoS attacks.

6. Port 69 (TFTP):

- Use: TFTP for simple file transfers.

- Vulnerabilities: File injection, data interception.

- Hacking Actions: Injecting malicious files, capturing data.

7. Port 80/443 (HTTP/HTTPS):

- Use: HTTP (80) and HTTPS (443) for web browsing.

- Vulnerabilities: XSS, SQL injection, DDoS.

- Hacking Actions: Injecting malicious scripts, database manipulation, DDoS attacks.

8. Port 110 (POP3):

- Use: POP3 for retrieving emails.

- Vulnerabilities: Credential theft, email content exposure.

- Hacking Actions: Intercepting credentials, unauthorized email access.

9. Port 123 (NTP):

- Use: NTP for time synchronization.

- Vulnerabilities: NTP amplification attacks.

- Hacking Actions: Abusing NTP servers for DDoS attacks.

10. Port 143 (IMAP):

- Use: IMAP for retrieving emails with more features.

- Vulnerabilities: Email manipulation.

- Hacking Actions: Unauthorized email access, email tampering.