task 2

task 2 different ports and their vulnerabilities

1. **Port 20 (FTP-DATA)**:

-FTP Data Interception

-FTP Data Injection

-FTP Data Tampering

-FTP Data Eavesdropping

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

- Brute Force Attacks

- Anonymous Access Exploitation

- Command Injection

- Directory Traversal

- DoS Attacks

- Data Interception

- Malware Distribution

3. **Port 22 (SSH)**:

- Brute Force Attacks

- Password Guessing

- SSH Key Exploitation

- Man-in-the-Middle Attacks

- Worm Propagation

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

- Password Sniffing

- Brute Force Attacks

- Man-in-the-Middle Attacks
- Data Interception
- Command Injection

5. **Port 25 (SMTP)**:
- Email Spoofing
- SPAM Distribution
- Email Relay Exploitation
- DoS Attacks
- Mailbombing

6. **Port 53 (DNS)**:
- DNS Spoofing
- DNS Cache Poisoning
- DNS Amplification (DoS)
- Zone Transfer Exploitation
- Subdomain Enumeration

7. **Port 69 (TFTP)**:
-TFTP Brute Force Attack
-TFTP Read/Write Attack
-TFTP Directory Traversal
-TFTP Denial of Service (DoS)
-TFTP Malware Distribution

8. **Port 80(HTTP)**:
- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- DoS Attacks (HTTP Flood)
- Server Misconfiguration Exploitation

- Directory Enumeration

9. **Port 110 (POP3)**:

- Brute Force Attacks

- Credential Sniffing

- DoS Attacks

- Email Eavesdropping

10. **Port 123 (NTP)**:

-NTP Amplification Attack

-NTP Reflection Attack

-NTP Exploitation

-NTP Abuse

11. **Port 143 (IMAP)**:

- Brute Force Attacks

- Credential Sniffing

- Command Injection

- DoS Attacks

- Email Eavesdropping

10. **Port 443 (HTTPS)**:

- SQL Injection

- Cross-Site Scripting (XSS)

- Cross-Site Request Forgery (CSRF)

- DoS Attacks (HTTP Flood)

- Server Misconfiguration Exploitation

- Directory Enumeration