**Task 2: Ports and vulnerabilities:**

1. Port 20:

- Description: FTP Data Transfer

- Protocol: TCP

- Vulnerabilities: FTP is inherently insecure as it transmits data, including passwords, in plain text. It's also susceptible to brute force attacks and FTP bounce attacks.

2. Port 21:

- Description: FTP Control

- Protocol: TCP

- Vulnerabilities: Similar to port 20, FTP control is also susceptible to plain text transmission of data, brute force attacks, and bounce attacks.

3. Port 22:

- Description: SSH (Secure Shell)

- Protocol: TCP

- Vulnerabilities: While SSH is considered secure, vulnerabilities can arise from weak passwords, outdated software versions, and misconfigurations. Brute force attacks and vulnerabilities in the SSH implementation can also pose risks.

4. Port 23:

- Description: Telnet

- Protocol: TCP

- Vulnerabilities: Telnet sends data, including passwords, in plain text, making it highly insecure. It's vulnerable to eavesdropping, man-in-the-middle attacks, and brute force attacks.

5. Port 25:

- Description: SMTP (Simple Mail Transfer Protocol)

- Protocol: TCP

- Vulnerabilities: SMTP servers can be exploited for spam relaying and email spoofing. Misconfigured servers can also be abused for unauthorized email sending.

6. Port 53:

- Description: DNS (Domain Name System)

- Protocol: UDP/TCP

- Vulnerabilities: DNS can be susceptible to cache poisoning, DDoS attacks (especially amplification attacks using DNS), and DNS hijacking, where users are redirected to malicious websites.

7. Port 69:

- Description: TFTP (Trivial File Transfer Protocol)

- Protocol: UDP

- Vulnerabilities: TFTP lacks authentication and encryption, making it a potential vector for unauthorized file access and transfers. It's often used for transferring firmware and configuration files in networking devices.

8. Port 80:

- Description: HTTP (Hypertext Transfer Protocol)

- Protocol: TCP

- Vulnerabilities: HTTP is the foundation of the web and is susceptible to various attacks, including Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and SQL injection. Insecure configurations and outdated software can also lead to vulnerabilities.

9. Port 110:

- Description: POP3 (Post Office Protocol version 3)

- Protocol: TCP

- Vulnerabilities: POP3, like other plain text protocols, exposes usernames and passwords during authentication. Without encryption, credentials can be intercepted. Brute force attacks can also target weak passwords.

10. Port 123:

- Description: NTP (Network Time Protocol)

- Protocol: UDP

- Vulnerabilities: NTP can be exploited in DDoS attacks by amplifying traffic. Attackers can use vulnerable NTP servers to overwhelm targets with traffic, causing service disruption.

11. Port 143:

- Description: IMAP (Internet Message Access Protocol)

- Protocol: TCP

- Vulnerabilities: IMAP vulnerabilities include credential interception, email exposure, and potential for unauthorized access to emails if the server is misconfigured or compromised.

12. Port 443:

- Description: HTTPS (Hypertext Transfer Protocol Secure)

- Protocol: TCP

- Vulnerabilities: While HTTPS is designed to provide secure communication over the web, vulnerabilities can arise from weak SSL/TLS configurations, expired certificates, and implementation flaws that could lead to exploits like Heartbleed.