TASK-2

VULNEBRATIES ACTION ON PORTS

PORT 20

Port 20 is associated with FTP data transfer. Vulnerabilities include:

- Brute Force Attacks: Unauthorized access by guessing credentials.
- Anonymous Access: Misconfigured servers allow anonymous access.
- Weak Encryption: Lack of encryption exposes data to interception.
- Port Scanning: Attackers scan for open FTP ports.
- DoS Attacks: Flood server with requests, causing unresponsiveness.
- Malicious File Uploads: Upload harmful files if not properly validated.
- Directory Traversal: Some servers may allow unauthorized access to files.
- Outdated Software: Running outdated FTP software exposes known vulnerabilities.
- Insecure Configuration: Poorly configured servers may expose sensitive data.
- To secure FTP, use SFTP or FTPS, enforce strong access controls, update software, and monitor logs for suspicious activity. Consider modern file-sharing alternatives.

PORT NO 21

- An open port 21 indicates an FTP server, which can have vulnerabilities:

- Brute Force Attacks: Unauthorized login attempts.
- Anonymous Access: Misconfigured servers allow unrestricted access.
- Weak Encryption: Data interception risk; use FTPS or SFTP.
- Command Injection: Malicious commands if input isn't validated.

- DoS Attacks: Overload server, causing unresponsiveness.
- Port Scanning: Identifying targets for further attacks.
- Malicious File Uploads: Uploading harmful files.
- Directory Traversal: Unauthorized access to files.
- Outdated Software: Known vulnerabilities if not updated.
- Insecure Configuration: Exposure of sensitive data.
- Secure FTP with SFTP/FTPS, strong access controls, updates, monitoring, and consider modern alternatives.

PORT NO 22

Port 22 is the default port for the SSH (Secure Shell) protocol, which is used for secure remote access and administration of systems. If port 22 is open on a server, it indicates that SSH is running, and there are several potential vulnerabilities and security concerns to be aware of:

An open port 22 indicates SSH service, which can have vulnerabilities:

- Brute Force Attacks: Unauthorized login attempts.
- Weak Passwords: Vulnerable to password cracking.
- Weak Encryption: Risk of eavesdropping if weak ciphers are used.
- SSH Key Management: Poorly managed keys can lead to unauthorized access.
- Outdated Software: Running old SSH software exposes known vulnerabilities.
- DoS Attacks: Overloading the SSH server with connection requests.
- Port Scanning: Identifying targets for further attacks.
- SSH Key Theft: Unprotected keys can be stolen for unauthorized access.

Secure SSH by using strong authentication (preferably key-based), regular updates, monitoring logs, and implementing security measures like IP restrictions and intrusion detection systems.

PORT NO 80

Port 80 is the default port for HTTP (Hypertext Transfer Protocol), which is used for serving web pages and web applications over the internet. An open port 80 indicates that a web server is running, and there are several common vulnerabilities and potential risks associated with it:

- XSS: Injection of malicious scripts in web pages.
- SQL Injection: Unauthorized database access via manipulated input.
- Directory Traversal: Unrestricted access to files and directories.
- Server Misconfiguration: Exposing sensitive information.
- DoS Attacks: Overloading the server.
- CSRF: Forcing users to perform actions unknowingly.
- Insecure File Uploads: Allowing malicious uploads.
- Outdated Software: Running old, vulnerable software.
- Security Misconfigurations: Improper permissions.
- Sensitive Data Exposure: Mishandling sensitive data.

Secure port 80 with regular updates, input validation, proper access controls, encryption (HTTPS), and security education.

PORT NO 110

Port 110 is the default port for the POP3 (Post Office Protocol version 3) service, which is used for retrieving emails from a mail server. If port 110 is open, it indicates that a POP3 server is running, and there are several vulnerabilities and security concerns associated with it

An open port 110 indicates a POP3 email server, which can have vulnerabilities:

- Brute Force Attacks: Unauthorized login attempts.
- Plain Text Transmission: Data sent in plain text, vulnerable to eavesdropping.
- Man-in-the-Middle Attacks: Intercepting and altering email communications.
- Credential Harvesting: Phishing to steal email credentials.
- Denial of Service (DoS) Attacks: Overloading the server.
- Email Content Security: No protection against malicious email content.
- Weak Passwords: Vulnerable to unauthorized access.

Secure POP3 by using encryption (like POP3S), strong passwords, regular updates, monitoring, and educating users on email security best practices. Consider using more secure email protocols and solutions when possible.

PORT NO 143

Port 143 is the default port for the IMAP (Internet Message Access Protocol) service, which is used for retrieving and managing emails from a mail server. If port 143 is open, it indicates that an IMAP server is running, and there are several vulnerabilities and security concerns associated with it

An open port 143 indicates an IMAP email server, which can have vulnerabilities:

- Brute Force Attacks: Unauthorized login attempts.
- Plain Text Transmission: Data sent in plain text, vulnerable to eavesdropping.
- Man-in-the-Middle Attacks: Intercepting and altering email communications.
- Credential Harvesting: Phishing to steal email credentials.
- Denial of Service (DoS) Attacks: Overloading the server.
- Email Content Security: No protection against malicious email content.
- Weak Passwords: Vulnerable to unauthorized access.

Secure IMAP by using encryption (like IMAPS), strong passwords, regular updates, monitoring, and educating users on email security best practices. Consider more secure email protocols and solutions when possible.

PORT N0 443

Port 443 is the default port for HTTPS (Hypertext Transfer Protocol Secure), which is used for secure web browsing. When this port is open, it indicates that a web server is running with SSL/TLS encryption enabled. While SSL/TLS is designed to provide strong security for data in transit, there can still be vulnerabilities and security concerns related to web applications and server configurations. Here are some potential vulnerabilities and risks associated with an open port 443

An open port 443 indicates a secure web server (HTTPS). Vulnerabilities may include:

- TLS Issues: Weak encryption protocols and ciphers.
- Certificate Problems: Expired or misconfigured SSL/TLS certificates.

- Web Application Vulnerabilities: XSS, SQL injection, CSRF, and insecure session management.
- Server Misconfigurations: Exposing sensitive files and directories.
- Outdated Software: Running old web server or applications.
- DoS Attacks: Attempting to overload the server.

To secure port 443, maintain up-to-date security configurations, certificates, software, and employ web security best practices. Regular monitoring and security assessments are essential.