Task 2

AI for Cyber Security

Vulnerabilities if the Respective ports are open:

1. **Port Number – 20 – FTP DATA**
    - Data Exposure – Unencrypted Transmission, Lack of Integrity
    - Brute Force Attacks – Weak Authentication, Dictionary Attacks
2. **Port Number – 21 – FTP Control**
    - Authentication Bypass – Weak Credentials, Anonymous Access
    - Command Injection – Malicious Commands, Remote Code Execution
3. **Port Number – 22 – SSH**
    - Password Sniffing – Packet Sniffing, Man in the Middle Attacks
    - Brute Force Attacks – Weak Credentials, SSH keys
4. **Port Number – 23 – TELNET**
    - Session Hijacking – Session Interception
    - Command Execution, Malware Delivery
5. **Port Number – 25 – SMTP**
    - Email Spoofing and Identity Fraud – Sender Address Forgery, Domain Impersonation
    - Email Content Manipulation – Email Tampering, Data Interception
6. **Port Number – 53 – DNS**
    - DNS Spoofing – DNS Spoofing, Cache Poisoning
    - DDoS Attacks – Amplification Attacks, Reflection Attacks
7. **Port Number – 69 – TFTP**
    - Information Disclosure – File Enumeration, Configuration Exposure
    - DDoS Attacks – Resource Exhaustion, Amplification Attacks
8. **Port Number – 80 – HTTP**
    - Web Application Attacks – Cross-Site Scripting, SQL Injection
    - Sensitive Data Exposure – Insecure Transmission, Directory Listing

9. **Port Number – 110 – POP3**
    - Account Lockout, DoS Attacks
    - Unencrypted Communication – Plaintext Transmission
10. **Port Number – 123 – NTP**
    - Server Exploitation and Vulnerabilities – Vulnerability Exploitation, Server Misconfiguration
    - Information Leakage and Reconnaissance – Response Packet analysis, Network Topology Discovery
11. **Port Number – 143 – IMAP**
    - Account Lockout, DoS Attacks
    - Credential Theft and Unauthorized Access
12. **Port Number – 443 – HTTPS**
    - Server-side Vulnerabilities – Software Exploits, Injection Attacks
    - Session Hijacking and Data Interception – Session sniffing, Traffic Analysis