AI FOR CYBER SECURITY WITH IBM QRADAR

Name: J. Manasa

TASK-2: Vulnerabilities of different ports

Port 20 and 21: FTP (File Transfer Protocol) ports, which can be susceptible to unauthorized access and data breaches.

Port 22: SSH (Secure Shell) port, vulnerable to brute force attacks and weak authentication.

Port 23: Telnet port, known for transmitting data in an unencrypted form, making it prone to eavesdropping and unauthorized access.

Port 25: SMTP (Simple Mail Transfer Protocol) port, often exploited for spamming and email-related attacks.

Port 53: DNS (Domain Name System) port, can be used for DDoS attacks and DNS spoofing.

Port 69: TFTP (Trivial File Transfer Protocol) port, lacks authentication and encryption, making it susceptible to unauthorized access and data manipulation.

Port 80: HTTP (Hypertext Transfer Protocol) port, commonly targeted for web application vulnerabilities and attacks like SQL injection.

Port 110: POP3 (Post Office Protocol version 3) port, susceptible to unauthorized email access.

Port 123: NTP (Network Time Protocol) port, can be exploited in DDoS amplification attacks.

Port 143: IMAP (Internet Message Access Protocol) port, potential for unauthorized email access and data breaches.

Port 443: HTTPS (Hypertext Transfer Protocol Secure) port, while encrypted, can still be susceptible to attacks like man-in-the-middle attack.