NAME: NANDIGAM KAMALI HARIPRIYA
REG NO: 21BCE2746

AI for Cyber Security with IBM Qradar (AI for Web Security)
24th August, 2023
Task 2: Determine the Vulnerabilities in the open ports.
Port no's: 20, 21, 22, 23, 25,53, 69, 80, 110, 123, 143, 443

Port No:20 (File Transfer Protocol FTP Data) &21 (FTP Control)
(Port 20&21 have the same vulnerabilities)
1) The server allows for anonymous logins, giving attackers unrestricted access.
2) Older FTP servers are frequently susceptible to known attacks.
3) Data transmitted by FTP servers is sent in clear text, which makes it susceptible to eavesdropping.

Port No:22 (Secure Shell SSH)
1) Attackers may use unreliable SSH keys to access the system.
2) Brute-force attacks may be possible against SSH servers and they could be exposed to well-known attacks.

Port No:23 (Telnet)
1) Data is sent in clear text using the insecure protocol telnet.
2) Security concerns might also come from password-based access and weak authentication.
3) Telnet servers are frequently out-of-date and open to known vulnerabilities.

Port No:25 (Simple Mail Transfer Protocol SMTP)
1) Spam and phishing attacks can target SMTP servers.
2) Denial-of-service attacks may target SMTP servers.

Port No:53 (Domain Name System DNS)
1) Cache poisoning attacks against DNS servers have the potential to reroute visitors to malicious websites.
2) Denial-of-service attacks may target DNS servers.

Port No:69 (Trivial File Transfer Protocol TFTP)
1) The TFTP protocol transfers data in plain text and is unsafe.
2) TFTP has limited security protections and is vulnerable to exploitation if properly secured.
3) Data tampering and unauthorized file access are possible dangers.

Port No:80 (Hypertext Transfer Protocol HTTP)
Numerous vulnerabilities, such as injection attacks (SQL injection, XSS), incorrect setups, and out-of-date software, can affect web servers on port 80.

Port No:110 (Post Office Protocol POP3)

1) Email retrieval protocol POP3 has weak security. If it is not secured (use POP3S/SSL), users and passwords may be made available.
2) Attackers may be able to intercept email communications by using POP3 servers as a man-in-the-middle.
3) Denial-of-service attacks may be able to target POP3 servers.

Port No:123 (Network Time Protocol NTP)
DDoS may be produced by exploiting NTP servers improperly in amplification attacks. Ensure access control and adequate settings.

Port No:143 (Internet Message Access Protocol IMAP)
1) Another email protocol with security risks is IMAP, which has weak authentication and incorrect settings.
2) Attackers may be able to intercept email communications by using IMAP servers as a man-in-the-middle.
3) It is vulnerable DDos

Port No:443 (HTTPS - HTTP Secure)
Although HTTPS is typically safe, it is nonetheless susceptible to attacks including SSL/TLS flaws, certificate problems, and web application flaws.