Task – 2

Name : C DEVAKI NANDAN REDDY

Port and Vulnerabilities

Determine the vulnerabilities in the open ports

Port nos(20,21,22,23,25,53,69,80,110,123,143,443)

A Refresher on Ports

Ports are logical constructs that identify a specific type of network service. Each port is linked to a specific protocol, program or service, and has a port number for identification purposes. For instance, secured Hypertext Transfer Protocol (HTTPS) messages always go to port 443 on the server side, while port 1194 is exclusively for OpenVPN.

Any port can be targeted by threat actors, but some are more likely to fall prey to cyberattacks because they commonly have serious shortcomings, such as application vulnerabilities, lack of two-factor authentication and weak credentials.

Here are the most vulnerable ports regularly used in attacks:

Ports 20 and 21 (FTP)

Port 20 and (mainly) port 21 are File Transfer Protocol (FTP) ports that let users send and receive files from servers.

FTP is known for being outdated and insecure. As such, attackers frequently exploit it through:

- Brute-forcing passwords
- Anonymous authentication (it's possible to log into the FTP port with "anonymous" as the username and password)
- Cross-site scripting

- Directory traversal attacks

Port 22 (SSH)

Port 22 is for Secure Shell (SSH). It's a TCP port for ensuring secure access to servers. Hackers can exploit port 22 by using leaked SSH keys or brute-forcing credentials.

Port 23 (Telnet)

Port 23 is a TCP protocol that connects users to remote computers. For the most part, Telnet has been superseded by SSH, but it's still used by some websites. Since it's outdated and insecure, it's vulnerable to many attacks, including credential brute-forcing, spoofing and credential sniffing.

Port 25 (SMTP)

Port 25 is a Simple Mail Transfer Protocol (SMTP) port for receiving and sending emails. Without proper configuration and protection, this TCP port is vulnerable to spoofing and spamming.

Port 53 (DNS)

Port 53 is for Domain Name System (DNS). It's a UDP and TCP port for queries and transfers, respectively. This port is particularly vulnerable to DDoS attacks.

Ports 137 and 139 (NetBIOS over TCP) and 445 (SMB)

Server Message Block (SMB) uses port 445 directly and ports 137 and 139 indirectly. Cybercriminals can exploit these ports through:

- Using the EternalBlue exploit, which takes advantage of SMBv1 vulnerabilities in older versions of Microsoft computers (hackers used EternalBlue on the SMB port to spread WannaCry ransomware in 2017)
- Capturing NTLM hashes
- Brute-forcing SMB login credentials

Ports 80, 443, 8080 and 8443 (HTTP and HTTPS)

HTTP and HTTPS are the hottest protocols on the internet, so they're often targeted by attackers. They're especially vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.

Ports 1433,1434 and 3306 (Used by Databases)

These are the default ports for SQL Server and MySQL. They are used to distribute malware or are directly attacked in DDoS scenarios. Quite often, attackers probe these ports to find unprotected database with exploitable default configurations.

Port 3389 (Remote Desktop)

This port is used in conjunction with various vulnerabilities in remote desktop protocols and to probe for leaked or weak user authentication. Remote desktop vulnerabilities are currently the most-used attack type; one example is the BlueKeep vulnerability.