Task -2 24-08-23 Thursday

Identify the vulnerability of ports if they are open-

What is an open port?

An open port is a network port that accepts traffic either using TCP or UDP and allows communication with underlying server technologies. Open ports are required when hosting remote services to which end-users can connect.

Port 20- is traditionally associated with the File Transfer Protocol (FTP) data channel. FTP is a protocol used for transferring files between a client and a server over a network. Port 20 specifically handles the data transfer from the server to the client during an FTP session.

Vulnerability include- **Data Exposure**: If an FTP server is not properly configured or secured, an attacker could potentially gain unauthorized access to sensitive files stored on the server.

 **Unauthorized Access**: If access controls and authentication mechanisms are not properly implemented, attackers might be able to connect to the FTP server and browse or download files without proper authorization.

Port 21 is traditionally associated with the File Transfer Protocol (FTP) control channel. FTP is used for transferring files between a client and a server over a network. Port 21 handles the control commands and initial connection establishment for an FTP session.

1. **Brute Force Attacks**: Attackers may attempt to guess usernames and passwords for FTP accounts through brute force attacks. Weak or default credentials can be exploited.
2. **Credentials Exposure**: If credentials are transmitted in plain text (not using secure protocols), attackers with network monitoring capabilities can intercept and obtain the credentials.

Port 22-SSH stands for Secure Shell. It is a TCP port used to ensure secure remote access to servers. You can exploit the SSH port by brute-forcing SSH credentials or using a private key to gain access to the target system.

Port 23-The Telnet protocol is a TCP protocol that enables a user to connect to remote computers over the internet. The Telnet port has long been replaced by SSH, but it is still used by some websites today. It is outdated, insecure, and vulnerable to malware. Telnet is vulnerable to spoofing, credential sniffing, and credential brute-forcing.

Port 25-SMTP stands for Simple Mail Transfer Protocol. It is a TCP port used for sending and receiving mails. It can be vulnerable to mail spamming and spoofing if not well-secured.

Port 53-DNS stands for Domain Name System. It is both a TCP and UDP port used for transfers and queries respectively. One common exploit on the DNS ports is the Distributed Denial of Service (DDoS) attack.,dns cache poisoning ,dns amplification

Port 80,443-HTTP stands for HyperText Transfer Protocol, while HTTPS stands for HyperText Transfer Protocol secure.These are the most popular and widely used protocols on the internet, and as such are prone to many vulnerabilities. They are vulnerable to SQL injections, cross-site scripting, cross-site request forgery, etc

Port 69-TFTP stands for Trivial File Transfer Protocol. It's a UDP port used to send and receive files between a user and a server over a network. TFTP is a simplified version of the file transfer protocol. Because it is a UDP port, it does not require authentication, which makes it faster yet less secure.

It can be exploited using password spraying and unauthorized access, dos attacks.

Port 110-Port 110 is traditionally associated with the Post Office Protocol version 3 (POP3), which is used for retrieving email messages from a mail server to a client device. An open port 110 can introduce vulnerabilities if not properly configured or secured.

Vulnerability include credtional interception, man in the middle attacks

Port 123- is commonly associated with the Network Time Protocol (NTP), which is used to synchronize the clocks of computers and network devices over a network.

Vulnerability include server hijacking,denial of service

Port 143- is associated with the Internet Message Access Protocol (IMAP), which is used for accessing and managing email messages stored on a mail server. IMAP allows users to view, organize, and manipulate their email messages from various devices while keeping the messages stored on the server.

Vulnerability include man in the middle,brute force attacks,