Task-2

Date- 24/8/2023

Port and Vulnerabilities-

1. Port number 20- (FTP-Data)

Port 20 is traditionally associated with the FTP (File Transfer Protocol) data channel.
FTP is a network protocol used for transferring files between a client and a server.
When a file transfer occurs using FTP, the actual file data is sent over port 20. In an FTP session, after the initial connection is established on port 21 (the FTP control port), port 20 is used to transmit the actual files being uploaded from the client to the server or downloaded from the server to the client.

Vulnerabilities on Port 20-

1.Unauthorized Access: If an FTP server is misconfigured or lacks proper authentication and authorization mechanisms, it may allow unauthorized access to files and directories on the server. This can lead to data breaches and unauthorized file transfers.

2.Brute Force Attacks: Attackers may attempt to gain access to an FTP server by conducting brute force attacks on port 20. They try different username and password combinations until they find valid credentials, potentially compromising the server's security.

2. Port number 21- (FTP)

Port 21 (FTP Control Port): Port 21 is used for the FTP control channel. The control channel is responsible for establishing the initial connection and managing the FTP session. When an FTP client connects to an FTP server, it does so on port 21. This port is used for sending FTP commands from the client to the server and receiving responses from the server.
The FTP control channel handles tasks such as authentication (logging in with a username and password), navigating directories, listing files, and initiating data transfers. It is essentially the "communication channel" that controls the overall FTP session.

Vulnerabilities on Port 21-

1. FTP Bounce Attack: In a FTP bounce attack, an attacker leverages an FTP server as a proxy to attack other servers or networks. This can potentially be used to bypass firewalls and security measures. While this is more of an issue with the FTP protocol itself rather than Port 21 specifically, it can affect the server's security.

2. Weak Authentication: FTP servers often rely on username and password combinations for authentication. If weak or easily guessable credentials are used, attackers may gain

unauthorized access to the FTP server, potentially leading to data breaches or unauthorized file transfers.

3. Port number 22- (SSH)

Port 22 is commonly associated with the SSH (Secure Shell) protocol, and it serves as the default port for SSH communications. SSH is a network protocol used for secure remote access to systems and secure file transfers. Port 22 is crucial for managing and securing remote connections to servers and network devices.
SSH is designed to provide secure authentication, encrypted data communication, and secure remote administration.

Vulnerabilities on Port 22-

1.Weak or Compromised SSH Keys: SSH allows users to authenticate using public-private key pairs, which are more secure than password authentication. However, if the private key is weak or compromised, attackers can gain unauthorized access. It's crucial to protect private keys and promptly revoke them if they are lost or compromised.

2.Port Scanning and Enumeration: Port 22 is frequently targeted during port scanning and enumeration activities to identify systems with SSH services. Implement security measures, such as rate limiting or IP whitelisting, to protect against brute force and scanning attempts.Attackers may attempt to enumerate valid usernames on an SSH server to launch targeted attacks. It's essential to obscure the response for invalid usernames to make it harder for attackers to gather information about valid accounts.

4. Port number 23- (TELNET)

Port 23 is the default port for the Telnet protocol, which is used for remote terminal access and control of computers and network devices.
It provides a text-based terminal interface, allowing a user to log in and interact with a remote system's command-line interface as if they were physically present at that system.

Vulnerabilities on Port 23-

1.Lack of Encryption: One of the most critical vulnerabilities of Telnet is its complete lack of encryption. Telnet sessions transmit all data, including login credentials and command exchanges, in plain text. This makes it susceptible to eavesdropping and interception by attackers monitoring network traffic.

2.Man-in-the-Middle Attacks: Telnet sessions are vulnerable to man-in-the-middle (MITM) attacks, where an attacker intercepts the communication between the client and the server. This allows them to capture data, modify commands, and potentially steal sensitive information like login credentials.

5. Port number 25- (SMTP) Simple mail transfer protocol

Port 25 is the default communication channel for the Simple Mail Transfer Protocol (SMTP), the protocol responsible for sending email messages. SMTP servers listen on Port 25 to accept incoming email connections, while SMTP clients connect to this port to send emails. Port 25 plays a vital role in the exchange of email messages, but it has been associated with security concerns, including spam and email spoofing.

Vulnerabilities on Port 25-

1.Spam Relay: One of the most significant vulnerabilities related to Port 25 is the potential for open SMTP relays. An open relay is an SMTP server that allows anyone to send email through it without authentication. Malicious actors can abuse open relays to send massive volumes of spam, using the server's resources and potentially causing it to become blacklisted.

2. Email spoofing and harvesting:
Email Spoofing: Port 25 can be exploited for email spoofing, where attackers forge the sender's email address to deceive recipients. This can lead to phishing attacks and the dissemination of malicious content.
Email Harvesting: Malicious actors often perform email harvesting by scanning Port 25 to identify active SMTP servers and collect email addresses. These addresses can be used for spam campaigns or targeted attacks.

6. Port number 53- (DNS) Domain name system

Port 53 is associated with the Domain Name System (DNS), a critical service on the internet. DNS is responsible for translating human-readable domain names (like www.example.com) into IP addresses (like 192.0.2.1), allowing computers to locate and communicate with each other over the internet. DNS is a protocol used for resolving domain names to IP addresses and vice versa. It helps users and devices locate resources, such as websites and email servers, using human-readable addresses instead of numerical IP addresses.

Vulnerabilities on Port 53-

1. DNS Cache Poisoning: DNS cache poisoning occurs when an attacker manipulates the DNS cache of a DNS resolver (server) with fraudulent DNS data. This can lead to the redirection of legitimate domain name resolutions to malicious IP addresses. Cache

poisoning attacks can compromise the integrity of DNS data and lead to various security risks.

2.DNS Amplification Attacks: In DNS amplification attacks, an attacker sends small DNS queries with a spoofed source IP address to open DNS resolvers, which then respond with much larger DNS responses. This can lead to overwhelming traffic directed at the target's IP address, causing a Distributed Denial of Service (DDoS) attack.

7. Port number 69- (TFTP) Trivial file transfer protocol

Port 69 is associated with the Trivial File Transfer Protocol (TFTP), a simple and lightweight file transfer protocol used for transferring files between networked devices.
TFTP is a minimalistic file transfer protocol that allows for the transfer of files between a client and a server. It is typically used in network environments where a small, fast, and straightforward file transfer method is required.

Vulnerabilities on Port 69-

1.Directory Traversal: Some TFTP servers may not implement adequate access controls, allowing clients to perform directory traversal attacks. This means that a malicious client could potentially access files outside the intended directory, gaining unauthorized access to sensitive information.

2.Lack of Authentication: TFTP does not provide any built-in authentication mechanisms. This means that anyone who can reach a TFTP server on Port 69 can potentially read from or write to the server without any form of user or device authentication. This lack of authentication makes TFTP particularly vulnerable to unauthorized access and data manipulation.

8. Port number 80- (HTTP) Hypertext transfer protocol

Port 80 is a well-known and commonly used port in computer networking, and it is associated with the Hypertext Transfer Protocol (HTTP).
Port 80 is the default port used by web servers for serving web pages and other web resources using the HTTP protocol. HTTP is the foundation of the World Wide Web and is used for communication between web clients (typically web browsers) and web servers.

Vulnerabilities on Port 80-

1.Cross-Site Scripting (XSS): XSS attacks occur when malicious scripts are injected into web pages and executed in the browsers of unsuspecting users. Attackers can use Port 80

to deliver these malicious scripts through vulnerable web applications, potentially leading to data theft, session hijacking, or defacement of web pages.

2.SQL Injection: SQL injection attacks involve manipulating user input to execute unauthorized SQL queries on the web server's database. If a web application on Port 80 is not properly protected against SQL injection, attackers can gain unauthorized access to databases, steal sensitive information, or manipulate data.

9. Port number 110- (POP3) Post office protocol 3-

Port 110 is associated with the Post Office Protocol version 3 (POP3), which is a widely used email retrieval protocol.
POP3 is an email retrieval protocol used by email clients (such as Outlook, Thunderbird, or Apple Mail) to retrieve emails from a remote email server. It allows users to download emails from the server to their local devices.
Port 110 is the default port used by POP3 servers for incoming email communication. When an email client wants to check for new messages or retrieve emails, it connects to the POP3 server on Port 110.

Vulnerabilities on Port 110-

1.Credential Theft: If attackers gain access to a network or computer, they can capture login credentials used for POP3 authentication on Port 110. This can result in unauthorized access to the email account and potentially lead to identity theft or email account compromise.

2.Man-in-the-Middle (MitM) Attacks: Attackers can perform MitM attacks by intercepting and altering the communication between the email client and the POP3 server on Port 110. They can manipulate email content, steal login credentials, or insert malicious code into emails.

10. Port number 123- (NTP) Network time protocol -

Port 123 is associated with the Network Time Protocol (NTP), a protocol used to synchronize the time of computer systems and network devices across the internet. The Network Time Protocol (NTP) is a networking protocol designed to synchronize the clocks of computers and network devices. It is used to maintain accurate time across a network or the internet, ensuring that all devices have a consistent and precise time reference.

Vulnerabilities on Port 123-

1.Amplification Attacks: NTP servers can be abused in amplification attacks, where an attacker sends a small request to an NTP server, and the server responds with a much

larger response to a spoofed target. This can lead to significant traffic amplification, potentially causing Distributed Denial of Service (DDoS) attacks.

2.Traffic Interference: Attackers may manipulate NTP traffic to interfere with time synchronization, potentially leading to inaccurate time on affected systems. This can disrupt network operations and cause issues with services relying on accurate time.

11. Port number 143- (IMAP) Internet message access protocol -

Port 143 is associated with the Internet Message Access Protocol (IMAP), which is used for email retrieval and management. IMAP allows email clients to access and manage email messages stored on a remote email server.
IMAP (Internet Message Access Protocol) is one of the two primary email retrieval protocols, with the other being POP3 (Post Office Protocol version 3). IMAP is designed for more advanced email management, allowing users to view, organize, and manipulate email messages stored on a remote server.

Vulnerabilities on Port 143-

1.Eavesdropping: Unencrypted IMAP sessions on Port 143 can be susceptible to eavesdropping, where attackers passively monitor network traffic to gather sensitive information, including email content and user credentials.

2.Session Hijacking: If an attacker gains access to an active IMAP session on Port 143, they can potentially hijack the session and impersonate the legitimate user, gaining control of the email account.

12. Port number 443- (HTTPS) Secure implementation of HTTP-

Port 443 is a well-known and widely used port in computer networking, and it is associated with the Hypertext Transfer Protocol Secure (HTTPS).
Port 443 is primarily used for secure web communication using the HTTPS protocol. HTTPS is an extension of HTTP (Hypertext Transfer Protocol) and adds a layer of security by encrypting data exchanged between a web browser (or client) and a web server.

Vulnerabilities on Port 443-

1.Weak SSL/TLS Configurations: Vulnerabilities can arise if SSL/TLS configurations are not properly configured or are using outdated encryption algorithms. Weak cipher suites or outdated protocols (e.g., SSLv3) can expose servers to vulnerabilities like the POODLE attack.

2.Expired or Invalid SSL/TLS Certificates: An expired or improperly configured SSL/TLS certificate can lead to security warnings in web browsers or vulnerabilities that allow attackers to intercept or manipulate encrypted traffic.