Saloni Ghule 21bce1967

TASK 2

PORT AND VULNERABILITIES:

Ports 20 :

FTP –DATA is known for being outdated and insecure.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)

Port 21:

Businesses need to think about using port 21 FTP to transfer files in their organization due to the unencrypted nature of FTP transmissions. Using FTP can expose sensitive information and network credentials to an attacker when transmitting data across the network or the Internet.

Port 22:

As such, Port 22 is subject to countless, unauthorized login attempts by hackers who are attempting to access unsecured servers. A highly effective deterrent is to simply turn off Port 22 and run the service on a seemingly random port above 1024

Port 23:

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 For the most part, Telnet has been superseded by SSH, but it's still used by some websites. Since it's outdated and insecure, it's vulnerable to many attacks, including credential brute-forcing, spoofing and credential sniffing.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:

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:

While using source port equal to 53 UDP packets may be sent by passing the remote firewall, and attacker could inject UDP packets, in spite of the presence of a firewall.

Port 69:

SolarWinds TFTP (Trivial File Transfer Protocol) Server is vulnerable to a denial of service, caused by an error when handling Read Request requests. By sending a specially-crafted Read Request to UDP port 69, a remote attacker could exploit this vulnerability to cause the server process to crash.

Port 80:

Port 80 isn't inherently a security risk. However, if you leave it open and don't have the proper configurations in place, attackers can easily

use it to access your systems and data. Unlike port 443 (HTTPS), port 80 is unencrypted, making it easy for cybercriminals to access, leak and tamper with sensitive data.

Port 110:

The issues include: "Buffer Overflows," "Cross-Site Scripting" attacks, "SQL Injection," and many others.

Port 123:

NTP is vulnerable to MitM attacks. These attacks allow unauthorized users to intercept, read, and modify traffic sent between clients and servers. NTP is particularly susceptible to MitM attacks due to the reliance on a small set of servers and the algorithm used to choose a server with which to sync.

Port 143:

One of the biggest security issues with IMAP is that it transmits logins from the client to the server in plain text by default, meaning usernames and passwords are not encrypted. (An encrypted login is obscured using complex mathematical equations so an attacker would not be able to understand it just by reading it.)

Port 443:

What Are the Port 443 Vulnerabilities? Port 443 has the same exposure as the HTTPS and TLS protocols. Vulnerabilities can include the following: Man-in-the-middle (MITM) attacks, where a hacker intercepts the communication between the client and server to steal sensitive information.