Assignment 2-AI CYBER SECURITY

What Kind of vulnerability attacks can be performed if particular Port is open?

1.Port 20 and 21- These are FTP , Data is shared and authentication is done without encryption.So,Cybercriminals can use Brute Force passwording, cross –site scripting,etc.

2.Port 22-It is TCP, often used for secure remote access to server.Possible attacks- Brute Force passwording, cross –site scripting,etc.

3.Port 23- It is vulnerable to attacks like credential Brute Force, spoofing, credential sniffing.

4.Port 25-It is SMPT ,used for sending and receiving email. It is vulnerable to spoofing and spamming.

5. Port 53- It's a UDP and TCP port for queries and transfers, respectively. This port is particularly vulnerable to DDoS attacks.

6.Port 69- 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.

7. Port 80- 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.

8. Port 110- POP3 bounce attack this attack exploits a flaw in the way POP3 handles bounced emails.

9. PORT 123-Run Replay attack using capture OTP.

10. Port 143-It is TCP ,it is vulnerable to Buffer overflow,Authentication flaws,Cipher downgrade attacks etc.

11.Port 443- 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.