26-3-21

Telnet

↳ Telnet-application layer protocol.

↳ Predecessor of SSH

↳ No encryption so, plain text communication

Usage : Telnet <ip><port>

eg) Telnet 10.0.1.1 23

Using this we can connect to Telnet.

Telnet Default port - 23

Note : In telnet session ctrl +] ^] is used to close the session

FTP

↳ File Transfer protocol.

↳ Transfer files over network.

↳ Similar to Telnet, both control and data channel in FTP uses unencrypted communication.

↳ Man in the middle can get sensitive data including passwords.

FTP working :

↳ operates at 2 channel.

↳ port 20 → Send Commands / establish / maintain connection

Port 21 → Transfer data

↳ 2 channel → Control / Command channel
→ Data channel.

↳ It uses client - Server model

client initiate a connection by providing the Credentials, wheras Server verifies it and open a session. after Session opens, FTP client execute FTP Commands.

Active & Passive

- In an Active FTP connection, the client opens a port and listens. The server is required to actively connect to it.
- In a Passive FTP connection, the server opens a port and listens (passively) and the client connects to it.

Enumeration:

- All network services can be enumerated by the use of NMAP for knowing OS, version which is used to find CVE in exploitation phase.

> Note: In one older FTP version, we can change the home directory of any user without authentications, FTP Server will asks for password if user exists, due to this bug, usernames are easily guessed

- NMAP - A switch tries to find anonymous login is possible or not & it gets the content present in it, if anonymous login is possible. It is done by ftp-anon script

Exploitation:

Methods:

i) Using username as Anonymous and empty password sometimes let you in the FTP Server.

ii) Bruteforce the FTP using username & password wordlist with the help of hydra

Note: Hydra supports FTP, RDP, Telnet, SSH etc.,

eg:) hydra -t 4 -l dale -P /usr/share/wordlists/rockyou.txt -vV 10.10.10.6 ftp"

Protocal

Here, consider the username is date

thread → 4

P → Password wordlist pass

Bruteforce