

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

Telnet Default Port - 23

Using this we can connect to Telnet.

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

FTP

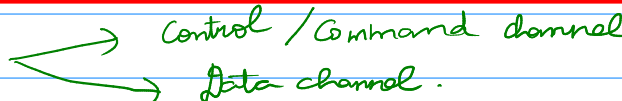
- ↳ File Transfer protocol.
- ↳ Transfer files over network.

- ↳ 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, whereas 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 CUE in exploitation phase.

Note: In one older FTP version, we can change the home directory of any user without authentication, FTP server will ask 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) Brute force the FTP using username & password wordlist with the help of Hydra.

eg.) `hydra -t 4 -l dale -P /usr/share/wordlists/rockyou.txt -vV 10.10.10.6 ftp`
Here, consider the (username is dale)
thread → 4
P → password wordlist pass

Note:

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

Protocol

Brute force