

Fawn

Take away

skills

FTP

Network

Protocols

Reconnaissance

Anonymous/Guest Access

major target of this assignment is enumerate also identify the potential issues with ftp

- FTP is server - client architecture model based file transferring protocol
- often issues are not using encrypted tunnel through tls/ssl and misconfiguration often the victim of man in the middle attack
- Filezilla is an GUI based file transferring protocol used
- having just ip address and hosts will only able run one task at target time yet hence the ports were introduced in order to run different services at a time
- Port 21 is ftp

Enumeration

ICMP scan

Getting the reply back from vpn tunnel

```
kali@Kali: ~  
--(kali@Kali)-[~]  
--$ ping 10.10.10.10  
PING 10.10.10.10: 64 bytes of data.  
64 bytes from 10.10.10.10: icmp_seq=1 ttl=63 time=15.6 ms  
64 bytes from 10.10.10.10: icmp_seq=2 ttl=63 time=23.9 ms  
64 bytes from 10.10.10.10: icmp_seq=3 ttl=63 time=53.3 ms  
64 bytes from 10.10.10.10: icmp_seq=4 ttl=63 time=60.9 ms  
^Z  
zsh: suspended ping 10.10.10.10  
--(kali@Kali)-[~]  
--$
```

Scanning the target

```
--(kali@Kali)-[~]  
--$ nmap -sV 10.10.10.10  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-02 22:40 CET  
Nmap scan report for 10.10.10.10  
Host is up (0.025s latency).  
Not shown: 999 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 3.0.3  
Service Info: OS: Unix
```

the open port is identified as the ftp also using the version detection

since the rule is to gain much information as you can during an enumeration

FTP

- since the port is open there is possibility of trying to hack in the file server using the login protocol if there is a mis configuration

we can manipulate it by using anonymous option in the login credentials

```
(kali@kali)-[~]  
$ ftp  
Connect to 192.168.1.1.  
220 (vsftpd) ready.  
Name (192.168.1.1:~): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

so using “get” command we can download any file which ftp contains since there is a misconfiguration it can be done

```
ftp> ls  
229 Entering Extended Passive Mode (|||36254|)  
150 Here comes the directory listing.  
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt  
226 Directory send OK.  
ftp> cat flag.txt  
?Invalid command.  
ftp> get flag.txt  
local: flag.txt remote: flag.txt  
229 Entering Extended Passive Mode (|||8498|)  
150 Opening BINARY mode data connection for flag.txt (32 bytes).  
100% |*****| 32 2.42 KiB/s 00:00 ETA  
226 Transfer complete.  
32 bytes received in 00:00 (0.56 KiB/s)  
ftp>
```

so now the the downloaded file will view the flag.txt

```
(kali㉿kali)-[~]  
$ cat flag.txt  
035db21c881520061c53e036e44f815
```

Q and A

TASK 1

What does the 3-letter acronym FTP stand for?

- file transfer protocol

TASK 2

Which port does the FTP service listen on usually?

- 21

TASK 3

What acronym is used for the secure version of FTP?

- SFTP

TASK 4

What is the command we can use to send an ICMP echo request to test our connection to the target?

- ping

TASK 5

From your scans, what version is FTP running on the target?

- vsftpd 3.0.3

TASK 6

From your scans, what OS type is running on the target?

- unix

TASK 7

What is the command we need to run in order to display the 'ftp' client help menu?

- ftp -h

TASK 8

What is username that is used over FTP when you want to log in without having an account?

- anonymous

TASK 9

What is the response code we get for the FTP message 'Login successful'?

- 230

TASK 10

There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system.

- ls

TASK 11

What is the command used to download the file we found on the FTP server?

- get

SUBMIT FLAG

Submit root flag

035db21c881520061c53e0536e44f815