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 wictim 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

Scanning the target

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

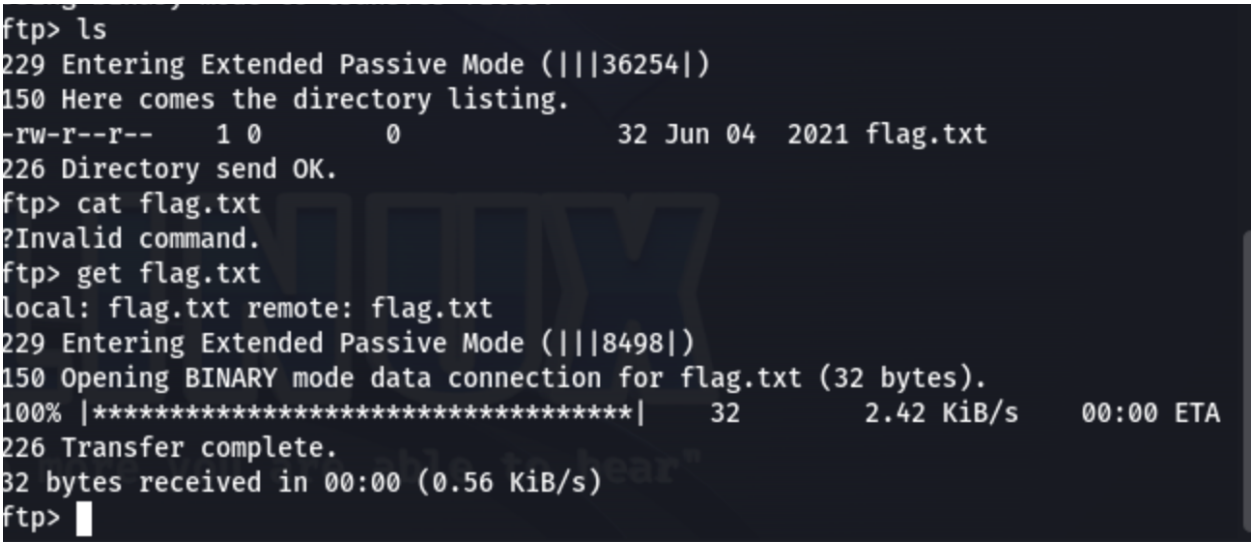
since the rule is to gain much information as you can during an enumeration

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

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



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

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