ATTACK DEFENSE

by PentesterAcademy

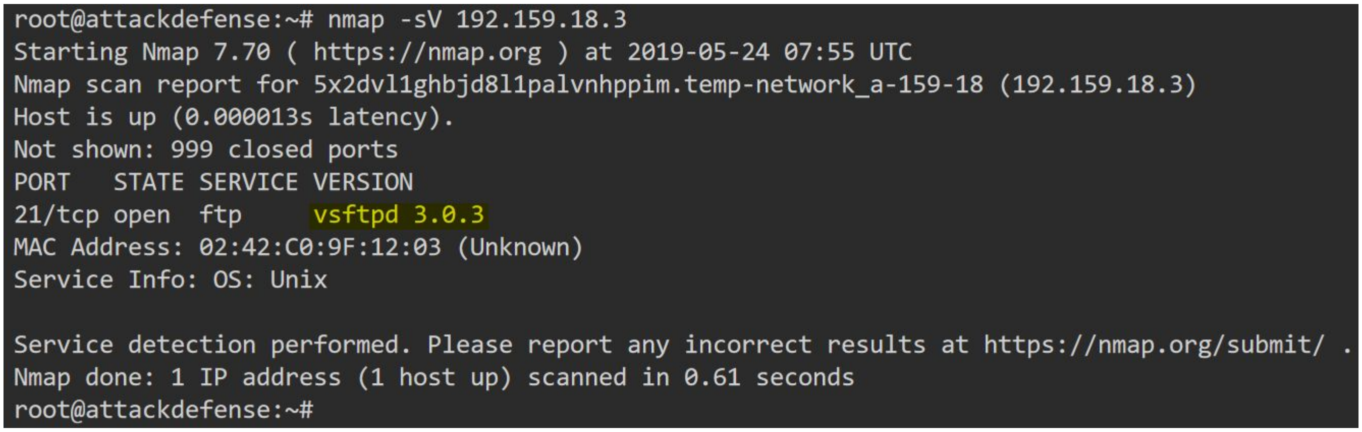
Name	VSFTPD Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=519
Type	Network Recon : FTP Servers

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. Find the version of vsftpd server.

Answer: vsftpd 3.0.3

Command: nmap -sV 192.159.18.3



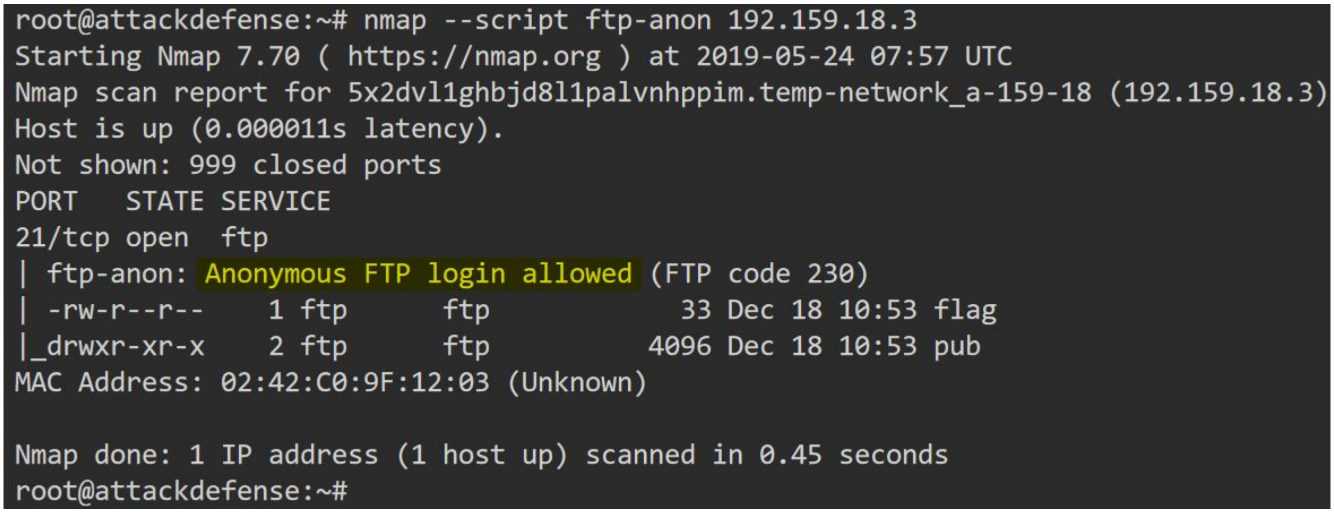
```
root@attackdefense:~# nmap -sV 192.159.18.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 07:55 UTC
Nmap scan report for 5x2dvl1ghbjd8l1palvnhppim.temp-network_a-159-18 (192.159.18.3)
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
MAC Address: 02:42:C0:9F:12:03 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
root@attackdefense:~#
```

Q2. Check whether anonymous login is allowed on the ftp server using nmap script.

Answer: Allowed

Command: nmap --script ftp-anon 192.159.18.3



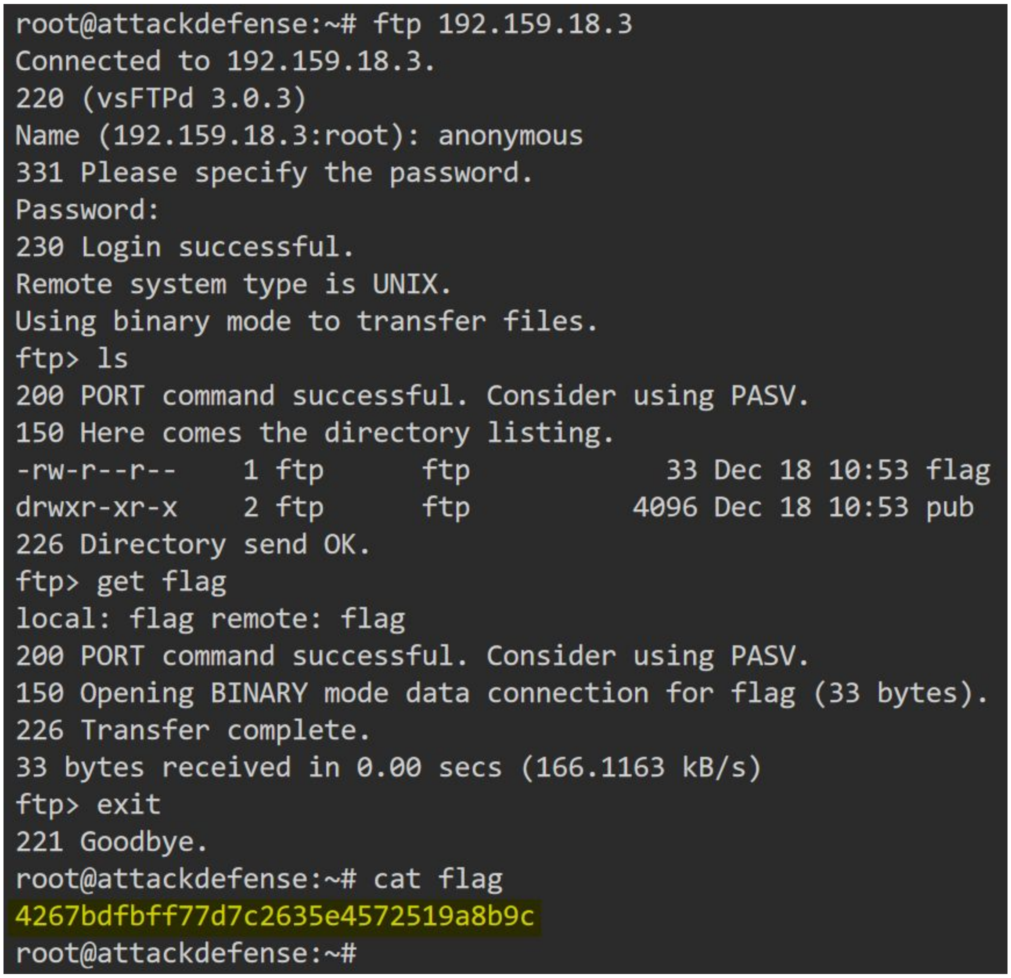
```
root@attackdefense:~# nmap --script ftp-anon 192.159.18.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 07:57 UTC
Nmap scan report for 5x2dvl1ghbjd8l1palvnhppim.temp-network_a-159-18 (192.159.18.3)
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 ftp      ftp            33 Dec 18 10:53 flag
|_drwxr-xr-x    2 ftp      ftp          4096 Dec 18 10:53 pub
MAC Address: 02:42:C0:9F:12:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
root@attackdefense:~#
```

Q3. Fetch the flag from FTP server.

Answer: 4267bdfbff77d7c2635e4572519a8b9c

Commands:
ftp 192.159.18.3
Enter username “anonymous” and empty password
ls
get flag
exit
cat flag



```
root@attackdefense:~# ftp 192.159.18.3
Connected to 192.159.18.3.
220 (vsFTPd 3.0.3)
Name (192.159.18.3:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            33 Dec 18 10:53 flag
drwxr-xr-x    2 ftp      ftp          4096 Dec 18 10:53 pub
226 Directory send OK.
ftp> get flag
local: flag remote: flag
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for flag (33 bytes).
226 Transfer complete.
33 bytes received in 0.00 secs (166.1163 kB/s)
ftp> exit
221 Goodbye.
root@attackdefense:~# cat flag
4267bdfbff77d7c2635e4572519a8b9c
root@attackdefense:~#
```

References:

1. vsftpd (https://security.appspot.com/vsftpd.html)
2. ftp (https://linux.die.net/man/1/ftp)
3. ftp-anon (https://nmap.org/nsedoc/scripts/ftp-anon.html)