Blue Team Junior Analyst (BTJA)

Reference: https://elearning.securityblue.team/home/courses/free-courses/blue-team-junior-analyst-pathway-bundle#description

Tomás Villaseca C.

Tomas.villaseca.c@gmail.com

linkedin.com/in/tomasvc93/

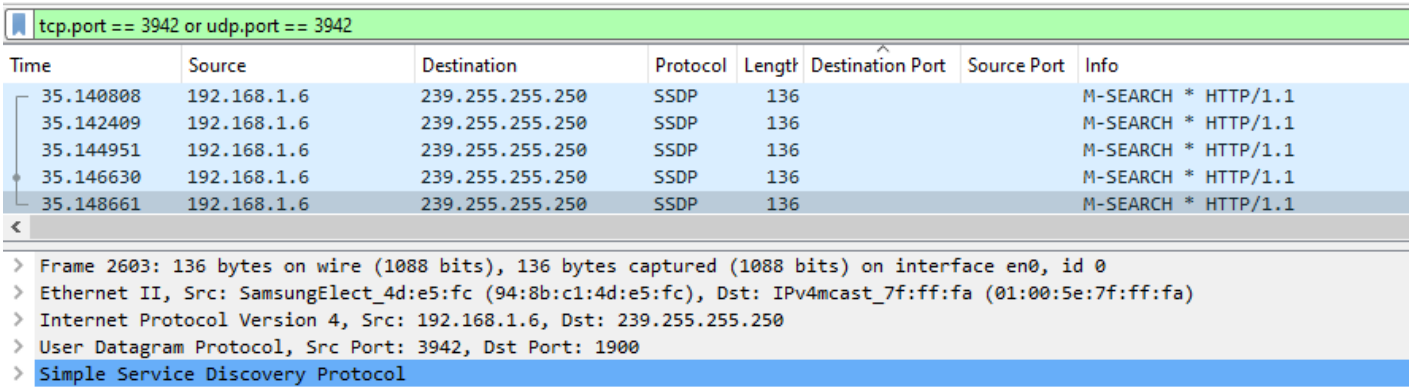
Table of Contents

1 - Introduction to Network Analysis

Analysis with Wireshark

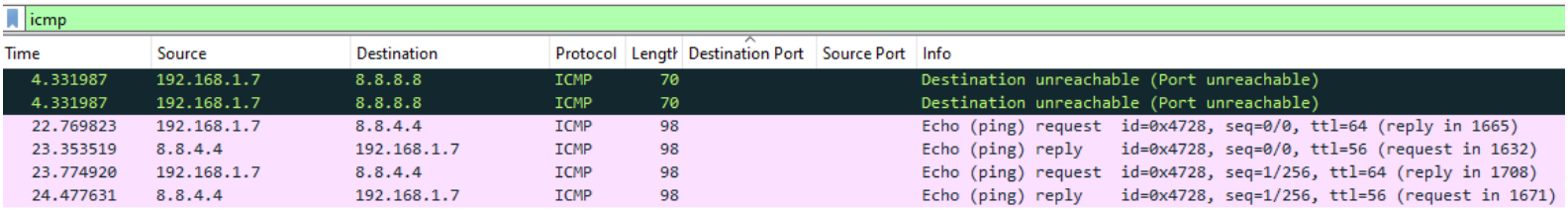
1.11 - Wireshark Activity Question PCAP 1

1. Which protocol was used over port 3942?



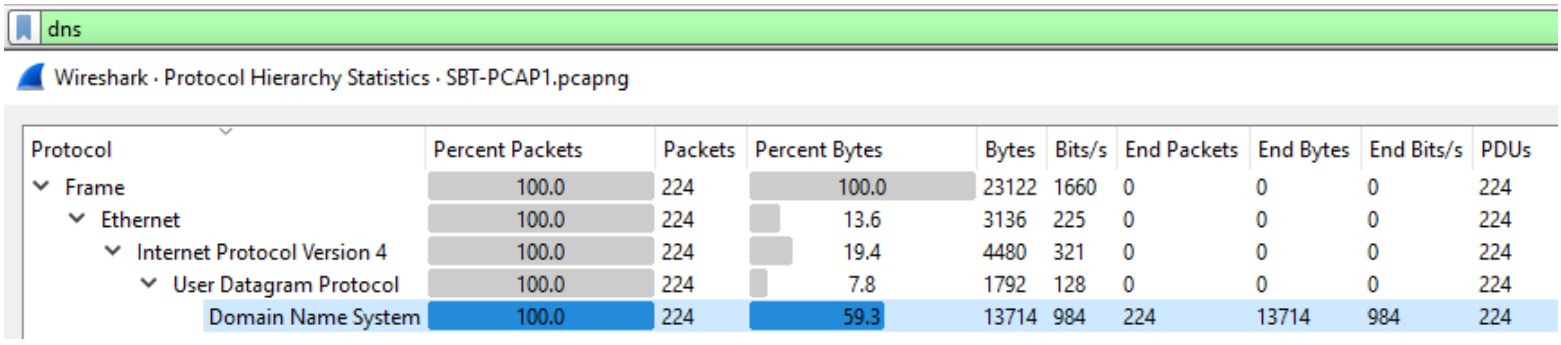
Simple service discovery protocol (SSDP)

2. What is the IP address of the host that was pinged twice?



IP address of the host that was pinged twice is 8.8.4.4

3. How many DNS query responses packets where captured?



dns.flags.response == 1

Wireshark · Protocol Hierarchy Statistics · SBT-PCAP1.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	90	100.0	12506	898	0	0	0	90
Ethernet	100.0	90	10.1	1260	90	0	0	0	90
Internet Protocol Version 4	100.0	90	14.4	1800	129	0	0	0	90
User Datagram Protocol	100.0	90	5.8	720	51	0	0	0	90
Domain Name System	100.0	90	69.8	8726	626	90	8726	626	90

Total number of DNS query response packets was 90.

- dns.flags.response == 0 → Packet is a DNS query.
- dns.flags.response == 1 → Packet is a DNS response.

4. What is the IP address of the host which sent the most number of bytes?

Wireshark · Endpoints · SBT-PCAP1.pcapng

Endpoint Settings

Name resolution

Limit to display filter

Ethernet · 10 | IPv4 · 73 | IPv6 · 5 | TCP · 236 | UDP · 108

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
115.178.9.18	2,993	2 MB	1,409	2 MB	1,584	207 kB
192.168.1.7	9,455	5 MB	5,043	732 kB	4,412	4 MB
216.58.199.68	727	447 kB	356	385 kB	371	61 kB

IP Address 115.178.9.18 sent the most number of bytes (2MB).

1.12 - Wireshark Activity Question PCAP 2

1. What is the WebAdmin password?

http

Time	Source	Destination	Protocol	Length	Destination Port	Source Port	Info
14.300943	192.168.56.1	192.168.56.111	HTTP	154	80	50488	GET /index.html HTTP/1.1
14.301688	192.168.56.111	192.168.56.1	HTTP	974	50488	80	HTTP/1.1 200 OK (text/html)
33.097733	192.168.56.1	192.168.56.111	HTTP	156	80	50492	GET /password.txt HTTP/1.1
33.098392	192.168.56.111	192.168.56.1	HTTP	320	50492	80	HTTP/1.1 200 OK (text/plain)

tcp.stream eq 2074

Wireshark · Follow HTTP Stream (tcp.stream eq 2074) · SBT-PCAP2.pcapng

```
GET /password.txt HTTP/1.1
Host: 192.168.56.111
User-Agent: curl/7.54.0
Accept: */*

HTTP/1.1 200 OK
Date: Sun, 09 Feb 2020 00:11:21 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Sat, 08 Feb 2020 23:53:54 GMT
ETag: "1a-59e19380137c2"
Accept-Ranges: bytes
Content-Length: 26
Content-Type: text/plain

WebAdmin Password: sbt123
```

2. What is the version number of the attacker's FTP server?

ftp

Time	Source	Destination	Protocol	Length	Destination Port	Source Port	Info
186.732952	192.168.56.1	192.168.56.103	FTP	82	49183	21	Response: 220 pyftpdlib 1.5.5 ready.
186.735295	192.168.56.103	192.168.56.1	FTP	70	21	49183	Request: USER anonymous
186.735673	192.168.56.1	192.168.56.103	FTP	87	49183	21	Response: 331 Username ok, send password.
186.735861	192.168.56.103	192.168.56.1	FTP	74	21	49183	Request: PASS IEUser@IEWIN7
186.736130	192.168.56.1	192.168.56.103	FTP	77	49183	21	Response: 230 Login successful.
192.215254	192.168.56.103	192.168.56.1	FTP	62	21	49183	Request: TYPE I
192.215535	192.168.56.1	192.168.56.103	FTP	80	49183	21	Response: 200 Type set to: Binary.
195.272905	192.168.56.103	192.168.56.1	FTP	82	21	49183	Request: PORT 192,168,56,103,192,32
195.280247	192.168.56.1	192.168.56.103	FTP	95	49183	21	Response: 200 Active data connection established.
195.281111	192.168.56.103	192.168.56.1	FTP	72	21	49183	Request: RETR malware.exe
195.282868	192.168.56.1	192.168.56.103	FTP	108	49183	21	Response: 125 Data connection already open. Transfer starting.
195.285467	192.168.56.1	192.168.56.103	FTP	78	49183	21	Response: 226 Transfer complete.
198.310586	192.168.56.103	192.168.56.1	FTP	60	21	49183	Request: QUIT
198.310808	192.168.56.1	192.168.56.103	FTP	68	49183	21	Response: 221 Goodbye.

```
> Frame 4243: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface vboxnet0, id 0
> Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PCSSystemtec_10:b8:d0 (08:00:27:10:b8:d0)
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.103
> Transmission Control Protocol, Src Port: 21, Dst Port: 49183, Seq: 1, Ack: 1, Len: 28
v File Transfer Protocol (FTP)
  > 220 pyftpdlib 1.5.5 ready.\r\n
  [Current working directory: ]
```

FTP Server initial response (with response code "220" = "OK"):

- Version of FTP Server → pyftpdlib 1.5.5

3. Which port was used to login to gain access to the victim Windows host?

Attacker IP Address → 192.168.56.1 → Filter

After WebAdmin password request → Series of ACK indicates an established connection → Port 8081

ip.src_host == 192.168.56.1

Time	Source	Destination	Protocol	Length	Destination Port	Source Port	Info
33.097733	192.168.56.1	192.168.56.111	HTTP	156	80	50492	GET /password.txt HTTP/1.1
33.098415	192.168.56.1	192.168.56.111	TCP	66	80	50492	50492 → 80 [ACK] Seq=91 Ack=255 Wi
33.105547	192.168.56.1	192.168.56.111	TCP	66	80	50492	50492 → 80 [FIN, ACK] Seq=91 Ack=2
33.105806	192.168.56.1	192.168.56.111	TCP	66	80	50492	50492 → 80 [ACK] Seq=92 Ack=256 Wi
53.513518	192.168.56.1	192.168.56.103	TCP	78	8081	50493	50493 → 8081 [SYN, ECE, CWR] Seq=0
53.513843	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=1 Ack=1 Wir
53.518865	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=1 Ack=122 W
57.724155	192.168.56.1	192.168.56.103	TCP	77	8081	50493	50493 → 8081 [PSH, ACK] Seq=1 Ack=
57.774155	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=12 Ack=160
58.788171	192.168.56.1	192.168.56.103	TCP	70	8081	50493	50493 → 8081 [PSH, ACK] Seq=12 Ack
58.824873	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=361
58.825431	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=562
58.825942	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=762
58.826204	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=962
58.826350	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=1162
58.826527	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=1362
58.826651	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=1562
58.826837	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=1762
58.826966	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=1962
58.827162	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=2162
58.827426	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=2362
58.827643	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=2962
58.827914	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=3162
58.828089	192.168.56.1	192.168.56.103	TCP	66	8081	50493	50493 → 8081 [ACK] Seq=16 Ack=3386

4. What is the name of a confidential file on the Windows host?

Searching into the TCP Stream of the series of ACKs:

Wireshark · Follow TCP Stream (tcp.stream eq 2075) · SBT-PCAP2.pcapng

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser>cd Desktop
cd Desktop

C:\Users\IEUser\Desktop>dir
dir
 Volume in drive C is Windows 7
 Volume Serial Number is 3C9E-098B

 Directory of C:\Users\IEUser\Desktop

02/08/2020  04:07 PM    <DIR>          .
02/08/2020  04:07 PM    <DIR>          ..

09/16/2019  05:22 PM                 0 .lock
08/22/2019  04:59 AM            30,000 BOF.m3u
04/20/1997  03:43 PM             9,728 CODBCLog.dll
12/04/1995  02:08 PM            27,136 Ctl3d32.dll.nt
01/31/1996  01:28 PM            26,624 Ctl3d32.dll.Win95
08/20/2019  01:40 AM             1,041 Easy RM to MP3 Converter.lnk
08/22/2019  04:59 AM               107 EasyRM.py
02/08/2020  03:44 PM               379 Employee_Information_CONFIDENTIAL.txt
01/02/2018  05:21 PM               830 eula.lnk
```

Confidential File → Employee_Information_CONFIDENTIAL.txt

5. What is the name of the log file that was created at 4:51 AM on the Windows host?

In the same TCP stream, search for the log file created at 4:51 AM:

```
08/16/2019  06:38 PM             6,197 howto.html
08/16/2019  06:42 PM               327 log.txt
06/18/1996  05:19 PM             3,072 log.wav
07/16/2019  04:51 AM               585 LogFile.log
06/18/1996  05:18 PM             6,248 login.wav
09/13/1996  10:47 AM         1,013,520 Mfc42.dll
08/16/2019  06:38 PM             4,453 mimetypes.ini
08/16/2019  06:38 PM             2,030 minishare.css
```

Log File → LogFile.log

Analysis with TCPDump

1.21 - TCPDump Activity Question PCAP 4

1. **How many UDP packets have been captured?**

```
┌──(tvc93㉿kali)-[~/Desktop]
└─$ tcpdump -r SBT-PCAP4.pcap --count udp
reading from file SBT-PCAP4.pcap, link-type EN10MB (Ethernet), snapshot length 262144
3290 packets
```

Number of UDP packets captured → 3290 packets

2. **How many TCP packets have both the SYN and ACK flags set?**

In order to match packets with multiple TCP flags, we must calculate the decimal value of the flag section of the TCP header.

0	0	0	1	0	0	1	0
C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N

for packets with the SYN and ACK flags set, the decimal value becomes 00010010

- 00010010 = 18
- tcpdump expression → *tcp[tcpflags]==18*

```
┌──(tvc93㉿kali)-[~/Desktop]
└─$ tcpdump -r SBT-PCAP4.pcap --count "tcp[tcpflags]==18"
reading from file SBT-PCAP4.pcap, link-type EN10MB (Ethernet), snapshot length 262144
20 packets
```

Number of TCP packets with both SYN and ACK flag set → 20 packets

3. **Which version of Chrome was used to connect to securityblue.team?**

```
┌──(tvc93㉿kali)-[~/Desktop]
└─$ tcpdump -r SBT-PCAP4.pcap -vvv | grep "User-Agent"
reading from file SBT-PCAP4.pcap, link-type EN10MB (Ethernet), snapshot length 262144
        User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
        User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
```

Version of Chrome used to connect to securityblue.team → 80.0.3987.87

4. **How many packets have a TTL value of 38?**

The expression ip[x] refers to a byte offset within the IP header. Here are all the possible offsets within the IP header that you might use with ip[x]:

1. **ip[0]**: Version and IHL (Internet Header Length)
2. **ip[1]**: Type of Service (ToS) / Differentiated Services Code Point (DSCP) / Explicit Congestion Notification (ECN)
3. **ip[2:2]**: Total Length
4. **ip[4:2]**: Identification
5. **ip[6:2]**: Flags and Fragment Offset
6. **ip[8]**: Time to Live (TTL)
7. **ip[9]**: Protocol
8. **ip[10:2]**: Header Checksum
9. **ip[12:4]**: Source IP Address
10. **ip[16:4]**: Destination IP Address

```
┌──(tvc93㉿kali)-[~/Desktop]
└─$ tcpdump -r SBT-PCAP4.pcap --count "ip[8]==38"
reading from file SBT-PCAP4.pcap, link-type EN10MB (Ethernet), snapshot length 262144
710 packets
```

Number of packets with TTL value of 38 → 710 Packets

1.22 - TCPDump Activity Question PCAP 5

1. **What is the name of the PNG file on the webserver at 192.168.56.111?**

```
┌──(tvc93㉿kali)-[~/Desktop]
└─$ tcpdump -A -r SBT-PCAP5.pcap | grep png
reading from file SBT-PCAP5.pcap, link-type EN10MB (Ethernet), snapshot length 262144
<li><a href="proprietary.png">proprietary.png</a>
```

- **-A** → Displays the packet contents in ASCII

Name of PNG file → proprietary.png

2. **Which version of OpenSSH is running on the server?**

```
┌──(tvc93㉿kali)-[~/Desktop]
└─$ tcpdump -r SBT-PCAP5.pcap | grep OpenSSH
reading from file SBT-PCAP5.pcap, link-type EN10MB (Ethernet), snapshot length 262144
06:04:28.890396 IP 192.168.56.1.50157 > 192.168.56.111.ssh: Flags [P.], seq 1:22, ack
 21: SSH: SSH-2.0-OpenSSH_7.6
06:04:28.895665 IP 192.168.56.111.ssh > 192.168.56.1.50157: Flags [P.], seq 1:34, ack
 33: SSH: SSH-2.0-OpenSSH_7.9p1 Debian-10
```

Web Server is 192.168.56.111 → OpenSSH Version 7.9p1

3. **On which port is the .zip file being served?**

```
┌──(tvc93㉿kali)-[~/Desktop]
└─$ tcpdump -A -r SBT-PCAP5.pcap | grep .zip -B 3
reading from file SBT-PCAP5.pcap, link-type EN10MB (Ethernet), snapshot length 262144
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.4 Safari/605.1.15
Accept-Language: en-us
Accept-Encoding: gzip, deflate
--
06:04:58.454287 IP 192.168.56.111.3016 > 192.168.56.1.50159: Flags [P.], seq 1:207, ack 1, win 227, options [nop,nop,TS val 71010977 ecr 649163791], lengt
h 206
E...    @@.@.? ...8o..8.......>8I........".....
.;..&.t.PK..
.       ......O 0:6...........ziptest.txtUT     ..< .. ]< .. ]ux..............|........WO.eq.PK.. 0:6........PK....
.       ......O 0:6.....................ziptest.txtUT ... < .. ]ux.............PK.........Q ... g.....
```

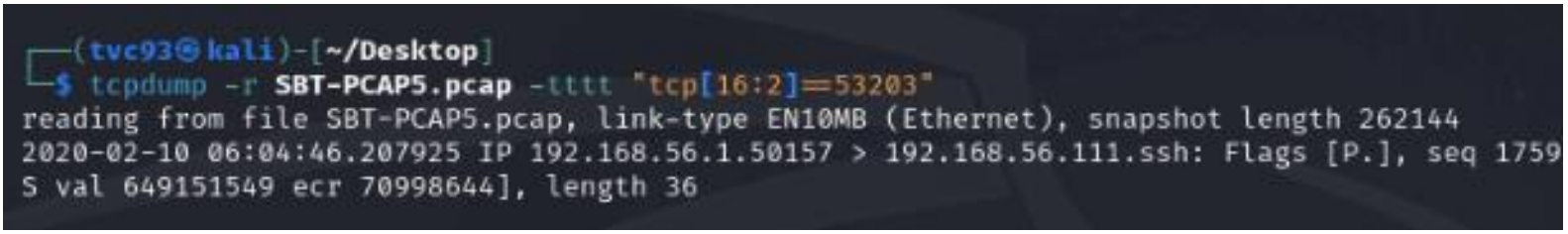
- **-B 3** → Option used with grep to include 3 lines of leading context before each match (displays the three lines immediately before each line that matches the pattern).

Source Port for the .zip file → 3016

4. When was a packet with a TCP checksum value of 53203 captured?

The expression tcp[x] refers to a byte offset within the TCP header. The [x:2] part indicates that you're looking at a two-byte (16-bit) value starting at offset x. Here are all the possible offsets within the TCP header that you might use with tcp[x]:

1. **tcp[0:2]**: Source port
2. **tcp[2:2]**: Destination port
3. **tcp[4:4]**: Sequence number (4 bytes)
4. **tcp[8:4]**: Acknowledgment number (if ACK flag is set) (4 bytes)
5. **tcp[12:1]**: Data offset, Reserved, NS (bits within a single byte)
6. **tcp[13:1]**: Flags (CWR, ECE, URG, ACK, PSH, RST, SYN, FIN)
7. **tcp[14:2]**: Window size
8. **tcp[16:2]**: Checksum
9. **tcp[18:2]**: Urgent pointer (if URG flag is set)



- **-tttt** → Option used to print the timestamp for each packet that includes date and time down to the microsecond.

Time of capture of the packet with checksum of value 53203 → 06:04:46.207925

Network Analysis Challenge

1.31 - Challenge Questions PCAP 3

1. What is the MAC address of the attacker?

ftp

Time	Source	Destination	Protocol	Length	Destination Port	Source Port	Info
34.948941490	192.168.56.1	192.168.56.103	FTP	82	49170	21	Response: 220 pyftpdlib 1.5.5 ready.
38.353106144	192.168.56.103	192.168.56.1	FTP	70	21	49170	Request: USER anonymous
38.353724005	192.168.56.1	192.168.56.103	FTP	87	49170	21	Response: 331 Username ok, send password.
44.597337411	192.168.56.103	192.168.56.1	FTP	70	21	49170	Request: PASS anonymous
44.597690647	192.168.56.1	192.168.56.103	FTP	77	49170	21	Response: 230 Login successful.
58.801134022	192.168.56.103	192.168.56.1	FTP	82	21	49170	Request: PORT 192,168,56,103,192,19
58.802225057	192.168.56.1	192.168.56.103	FTP	95	49170	21	Response: 200 Active data connection established.
58.805761368	192.168.56.103	192.168.56.1	FTP	98	21	49170	Request: RETR Alevis_Employee_Information_Chart.csv
58.806605711	192.168.56.1	192.168.56.103	FTP	108	49170	21	Response: 125 Data connection already open. Transfer starting.
58.807803920	192.168.56.1	192.168.56.103	FTP	78	49170	21	Response: 226 Transfer complete.
61.062868989	192.168.56.103	192.168.56.1	FTP	60	21	49170	Request: QUIT
61.063373903	192.168.56.1	192.168.56.103	FTP	68	49170	21	Response: 221 Goodbye.

```
> Frame 559: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0
v Ethernet II, Src: PCSSystemtec_10:b8:d0 (08:00:27:10:b8:d0), Dst: PCSSystemtec_3d:27:5d (08:00:27:3d:27:5d)
  > Destination: PCSSystemtec_3d:27:5d (08:00:27:3d:27:5d)
  > Source: PCSSystemtec_10:b8:d0 (08:00:27:10:b8:d0)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.1
> Transmission Control Protocol, Src Port: 49170, Dst Port: 21, Seq: 1, Ack: 29, Len: 16
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

MAC Address of attacker → 08:00:27:3d:27:5d

2. What is the type of attack which is taking place that allows the attacker to listen in on conversations between the central server and another host?

Type of attack → Man in the middle

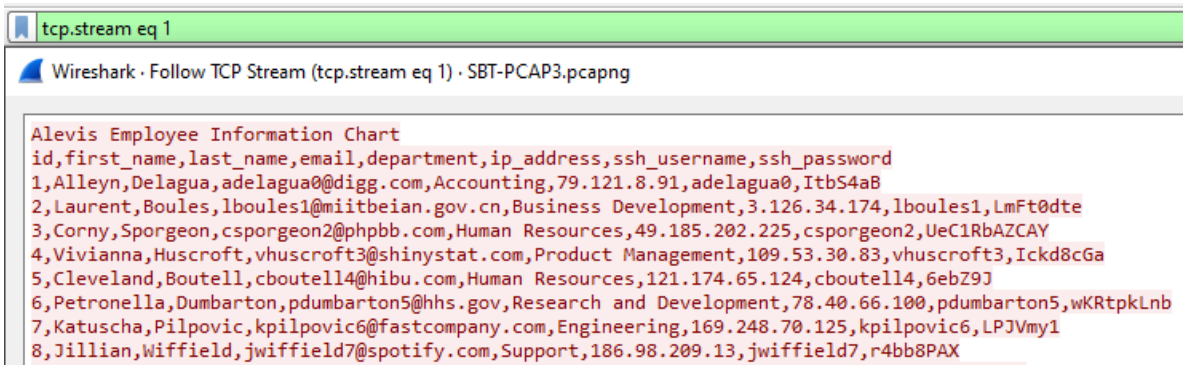
3. What is the file which was downloaded from the central server?

TCP Stream of the initial attack and advancing on the stream to search for answers:

tcp.stream eq 0

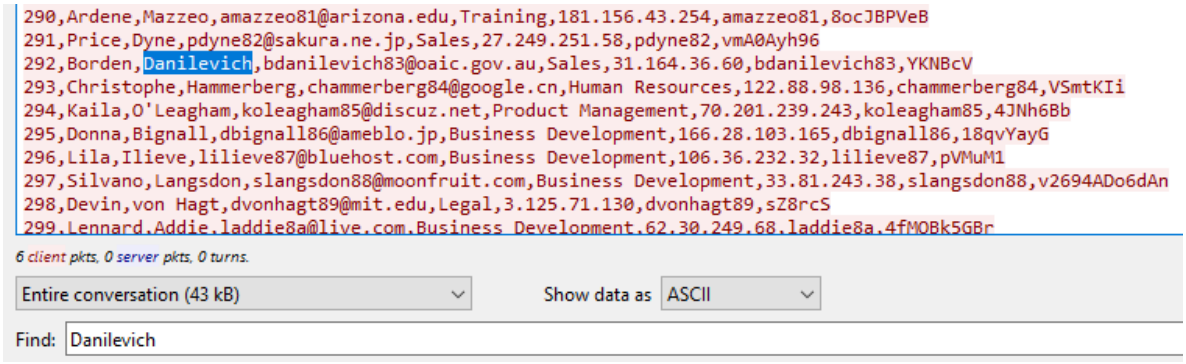
Wireshark · Follow TCP Stream (tcp.stream eq 0) · SBT-PCAP3.pcapng

```
220 pyftpdlib 1.5.5 ready.
USER anonymous
331 Username ok, send password.
PASS anonymous
230 Login successful.
PORT 192,168,56,103,192,19
200 Active data connection established.
RETR Alevis_Employee_Information_Chart.csv
125 Data connection already open. Transfer starting.
226 Transfer complete.
QUIT
221 Goodbye.
```



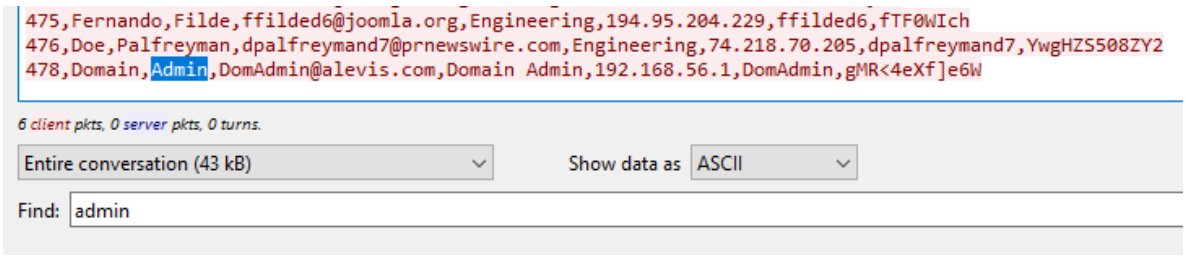
Downloaded file from the central server → Alevis_Employee_Information_Chart.csv

4. What department does Borden Danilevich work in?



Department of Borden Danilevich → Sales

5. What is the SSH password of the Domain Administrator?



Domain Administrator SSH Password → gMR<4eXf]e6W

2 - Introduction to OSINT

Intelligence Cycle

2.11 - Intelligence Cycle

Intelligence Cycle = Iterative model that describes a series of stages and procedures that a researcher has to perform to convert the collected data and information into intelligence products capable of bringing solutions to an organization.

1. **Planning & Direction** = Stage where you determine the purpose of your research (problem) and what kind of information you are looking for.

2. **Collection** = Gathering of data and information.
   - Identification of which processes will be used for the collection of information.
   - Using all available techniques to obtain the data that will help carry out your intelligence operation.

3. **Processing** = Processing of collected data and information.

   - Application of decoding, decryption, validation, and evaluation techniques.
   - Objective → Filter the huge amount of data obtained to identify useful data for your research.

4. **Analysis** = Analysis to produce meaningful intelligence.

   - Analysis of all filtered information to obtain the answers and solutions to our initial problem.
   - Creation of a coherent intelligence product.

5. **Dissemination** = Dissemination of intelligence clients.

   - Deliver the intelligence product to stakeholders that requested it.
   - Help stakeholders with informed and appropriate decision to confront the original problem.

OSINT Tools & Services

2.21 - OSINT Tools

1. **The Harvester** = The Harvester is a command-line information-gathering tool that utilizes OSINT sources to gather information about the target domain and retrieves information such as hostnames, IP addresses, employees (and their positions), email addresses, and much more.

2. **Maltego** = Maltego is a high-level data mining and information gathering tool, capable of obtaining real-time data on different types of entities (companies, people, websites, etc.), and representing them graphically through nodes, showing all the connections that the program was able to obtain over the Internet, about the subject under investigation.

3. **Tweetdeck** = Social media dashboard application for managing Twitter accounts.

    - There are approximately 500 million tweets a day. That's a lot of information to get through, but
    - TweetDeck makes it a lot easier to monitor trends, follow hashtags, and perform live searches.
    - OSINT → Monitor for vulnerabilities affecting common software (such as browsers), major operation systems, and threat actors on twitter using the Tweetdeck "search" capability (Example: #0day OR #zeroday).

4. **Google Dorks** = Google Dorks are search hacks where we can use special arguments in a normal Google query to find specific information.

    a) **Dork Format** → operator:keyword

    - **Finding Files** → Search "example.com filetype:pdf"
    - **Subdomain Enumeration** → Search "site:example.com -site:www.example.com"

    b) **Dork** → inurl: (value) → Look for specific keywords

    - **Finding admin login portals** → Search "inurl: admin"

5. **TinEye** = TinEye is an image search and recognition company, which offers customers the ability to receive alerts when their images are identified on the internet.

    - **Reverse Image Searches** → Upload an image and see where else it is present on the internet.

6. **Google Image Search** = Google functionality that allows you to search for an image URL or upload an image (very similar to TinEye).

OSINT Challenge

2.31 - OSINT Challenge Scenario

You work for a law enforcement organization, and you have been assigned to track a person-of-interest, that is believed to be associated with a hacking group that recently compromised a Managed Service Provider (MSP) and are trying to sell the stolen credentials on both the clear net and dark web. Another team is focusing on the dark web lead, so you have been tasked with using OSINT sources to build up a profile on the individual and attempt to locate any evidence that links them to the MSP breach and sale of account details. You have been provided with some information to start your investigation.

Your manager has provided you with the following starting information:

- **Twitter handle used by actor:** @sp1ritfyre

You can download a list of the information you have been asked to retrieve about the subject (.txt file). You should use this to help you find the right information, ready to hand in during the Challenge Submission in the next lesson. This will help to keep you on track, and not gather information that is not relevant to the current investigation.

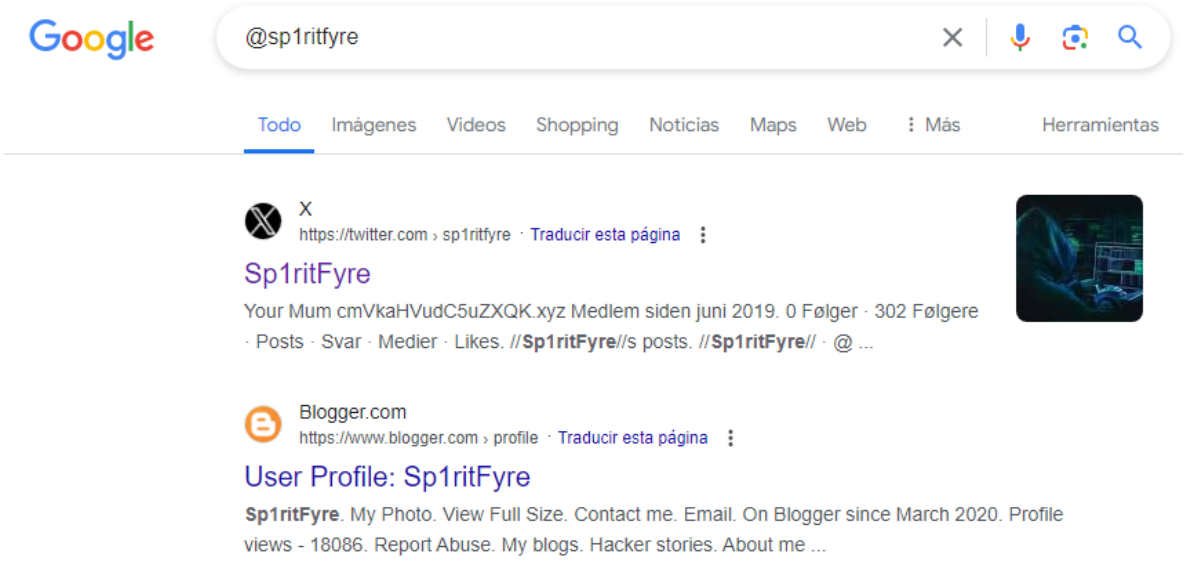
Tips and Advice:

- **Read** the template “SBT-OSINT-Challenge-Report.txt” properly. This will help you gather the information you actually need, instead of falling down a rabbit-hole.
- DNS TXT records can be used to show text strings. Don’t forget to check if the owner has left a comment!
- **Some information may be encoded in Base64 or Hexadecimal so that it is not immediately human-readable. You can use online sites to decode them! Make sure you understand what B64 and Hexadecimal strings look like, so you can identify and convert them!**

SBT-OSINT-Challenge-Report.txt: (Clear text)

```
 _____________   _____ _    ____   ________ ___   _       _
|   _   | ___ \ /  ___| | / /\ \ / /  ___/ _ \ | |     | |
| | | | |_/ / \ `--.| |/ /  \ V /| |_ / /_\ \| |     | |
| | | |  __/   `--. \    \   \ / |  _||  _  || |     | |
\ \_/ / |     /\__/ / |\  \  | | | |  | | | || |____| |____
 \___/\_|     \____/\_| \_/  \_/ \_|  \_| |_/\_____/\_____/


Investigation into MSP data breach. Clear web investigation team.

================================++================================


Known Info:
=================
Twitter Handle: @sp1ritfyre

Required Info:
=================
[1] First Name:
[2] Last Name:
[3] Age:
[4] Country:
[5] Interests (5 minimum):
[6] Hacker's employer (company name):
[7] Hacker's position within company:

Online Presence:
================================
[8] Self-Owned Website (Hacker owns the domain):
[9] Other Websites (Person does not own the domain, such as blogs):

Evidence Collection:
================================
[10] Any URLs of webpages that directly tie individual to MSP
breach:

Email Addresses Utilized:
================================
[11] What email addresses have been used by the hacker? (2)

================================++================================
```

1. Search @sp1ritfyre on google.



- First Google Search result → Twitter account

cmVkaHVudC5uZXQK.xyz

- Base64 decoder → redhunt.net (domain owned by the hacker)

- Second Google Search result → Blogger account

Sp1ritFyre

Ver tamaño completo

Contacto
Correo electrónico

En Blogger desde marzo de 2020

Vistas del perfil - 18090

Denunciar abuso

Mis blogs

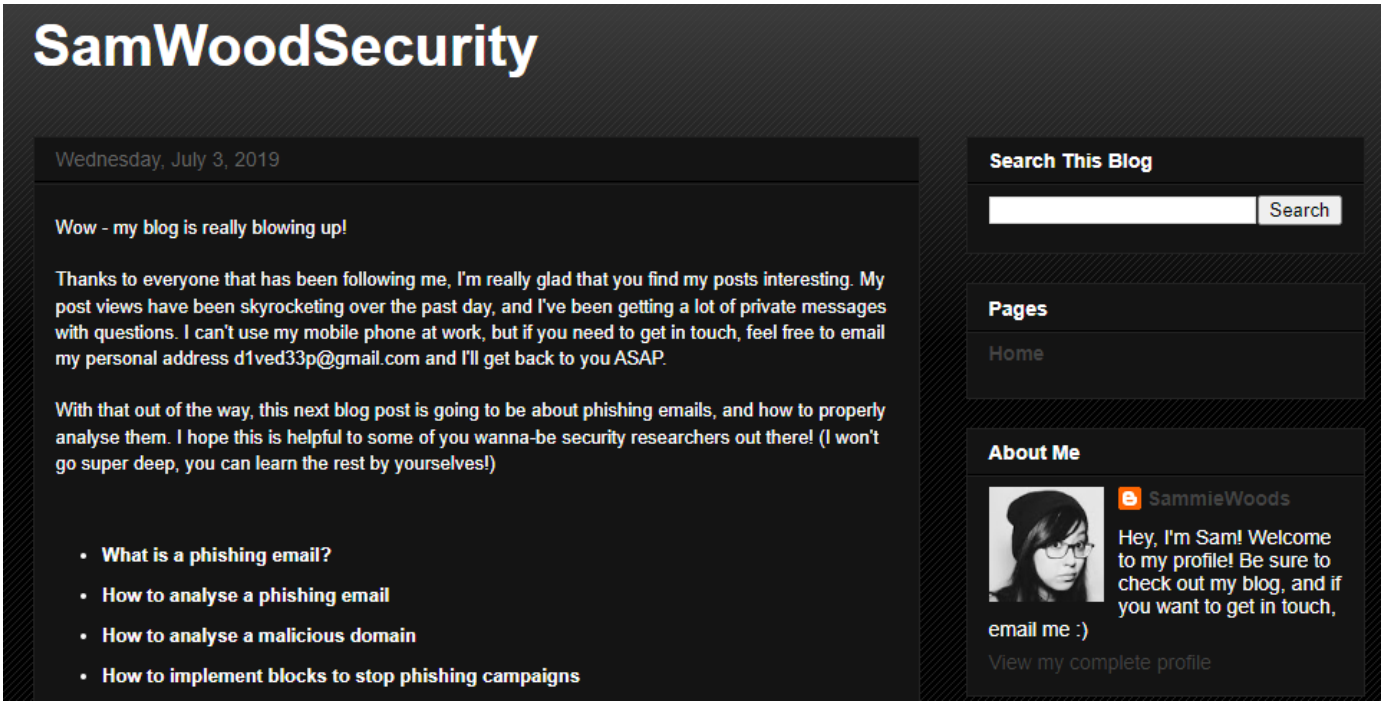
Hacker stories

Información sobre mí

Sexo	Mujer
Ubicación	68747470733a2f2f73616d6d6965776f6f647365632e626c6f6773706f742e636f6d

68747470733a2f2f73616d6d6965776f6f647365632e626c6f6773706f742e636f6d

- Hexadecimal decoder → https://sammiewoodsec.blogspot.com



Thursday, June 27, 2019

How I got into Cyber Security

Hey everyone, my name is Sam, I'm 23, and currently working within the Cyber Security industry. It's an amazing industry that is ever-changing, so no two days are the same! I wanted to share with you my story about how I jumped into this world.

I studied ICT in college, and really enjoyed it. Learning how applications work, how devices talk to each other. It was all crazy. Eventually our course covered a module focus on Security, and despite being very quick and basic, I found myself wanting to know more. I'd spend some free time researching different hacking groups, such as LizardSquad (I remember them taking down Dyn, and DoSing Xbox Live and PSN as a result, pretty cool!) as well as Anonymous, and started reading about state-sponsored groups such as APT 28, and Turla Team.

I went off to University at Plymouth, and studied for a degree in Cyber Security and Forensics. I passed with a 1st degree, and shortly after I started working at PhilmanSecurityInc. I'm currently a junior pen tester, as I realised I preferred breaking stuff (Responsibly!) rather than fixing it.

I love the team here, and both Zach and Dave are great mentors, and constantly help me to develop and expand on my existing skills.

Lots more blog posts coming soon! :)
~ Sammie

at June 27, 2019 No comments:

Ver tamaño completo

En Blogger desde junio de 2019

Vistas del perfil - 12964

Denunciar abuso

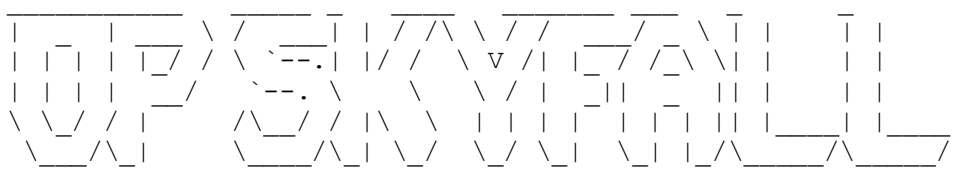
Mis blogs

SamWoodSecurity

Información sobre mí

Sexo	Mujer
Sector	Tecnología
Profesión	Junior Penetration Tester
Ubicación	Reading, Reino Unido
Introducción	Hey, I'm Sam! Welcome to my profile! Be sure to check out my blog, and if you want to get in touch, email me :)
Intereses	Security, Programming, Technology, Gaming, Photography, Camping
Películas favoritas	Ready Player One 2018
Música favorita	The Beatles, Rolling Stones, Queen
Libros favoritos	The Hunger Games series

SBT-OSINT-Challenge-Report.txt: (Answers)



```
Investigation into MSP data breach. Clear web investigation team.

================================++================================
Known Info:
=================
Twitter Handle: @sp1ritfyre

Required Info:
=================
[1] First Name: Sam
[2] Last Name: Woods
[3] Age: 23
[4] Country: United Kingdom
[5] Interests (5 minimum): Security, Programming, Technology, Gaming,
Photography, Camping, Malware Analysis.
[6] Hacker's employer (company name): PhilmanSecurityInc
[7] Hacker's position within company: Junior Penetration Tester

Online Presence:
================================
[8] Self-Owned Website (Hacker owns the domain):

https://redhunt.net

[9] Other Websites (Person does not own the domain, such as blogs):

https://sammiewoodsec.blogspot.com/
https://sp1ritfyrehackerstories.blogspot.com/
https://github.com/SammieWoodSec/Disrupt0r


Evidence Collection:
================================
[10] Any URLs of webpages that directly tie individual to MSP breach:

https://sammiewoodsec.blogspot.com/

Email Addresses Utilized:
================================
[11] What email addresses have been used by the hacker? (2)

d1ved33p@gmail.com

================================++================================
```

3 - Introduction to Digital Forensics

Digital Forensics Tools

3.11 - Evidence Collection Tools

1. **KAPE (Kroll Artifact Parser and Extractor)** = Open-source digital forensics tool designed to automate the collection and parsing of forensic artifacts from a computer's file system and memory.

    - Can be deployed locally or on remote systems to quickly gather key data.

2. **FTK Imager** = Forensic imaging proprietary software used for creating forensic images of storage media and analyzing digital evidence.

    - Can create disk images and memory images.
    - Can export acquired images in multiple formats.
    - Can import images for analysis.

3. **EnCase** = Digital forensics software suite used to conduct digital investigations.

    - **Data Acquisition** → Allows for the collection of digital evidence from various devices (computers, mobile devices, IoT devices, etc.).
    - **Data Analysis** → Software offers tools to analyze the collected data.
    - **Evidence Management** → Helps manage and organize digital evidence, maintaining a chain of custody and ensuring integrity of the data.
    - **Reporting** → Provides reporting features, enabling investigators to create detailed reports of their findings.

4. **Cellebrite** = Software suite of tools and services designed to extract, analyze, and manage digital data from mobile devices.

    - **Data Acquisition** → Allows for the collection of digital evidence from a wide range of mobile devices.
    - **Data Analysis** → Provides powerful analysis tools to interpret collected information (ability to reconstruct events, link contacts, and visualize communication patterns).
    - **Reporting** → Enables the creation of detailed court-admissible reports that document the findings of a digital investigation.

3.12 - Evidence Analysis Tools

1. **Autopsy** = Open-source digital forensics platform designed to assist investigators in the analysis and extraction of digital evidence from various data sources.

    - User-friendly interface & wide range of features to aid in examination and reporting.
    - Enables the retrieval of many different types of digital data (images, video, audio, email messages, deleted files, visited websites, etc.).
    - **Data Recovery** → Process of retrieving lost or deleted files and extracting information from damaged or corrupted media.

2. **Volatility** = Open-source memory forensics framework used for the analysis of volatile memory (RAM) dumps.

    - **Memory Dump** → Enables the capture a snapshot of a computer's memory.
    - **Memory Dump Analysis** → Can analyze memory dumps from various operating systems (Windows, Linux, and MacOS).

Linux Command-Line Interface

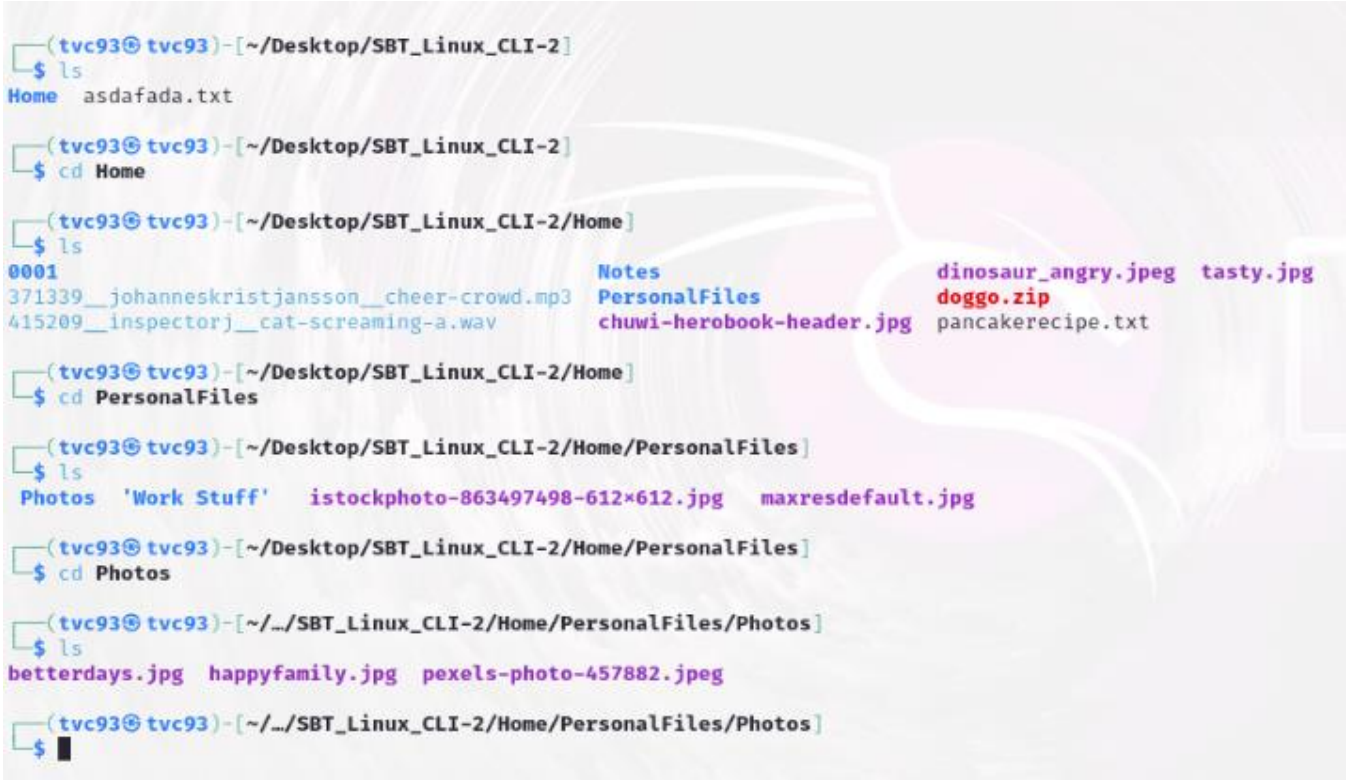
3.21 - Linux CLI Activity

1. **What is the phrase on line 8 of the first text file you come across?**

there's a snake in my boot

2. **How many images are in the /Home/PersonalFiles/Photos/ directory?**

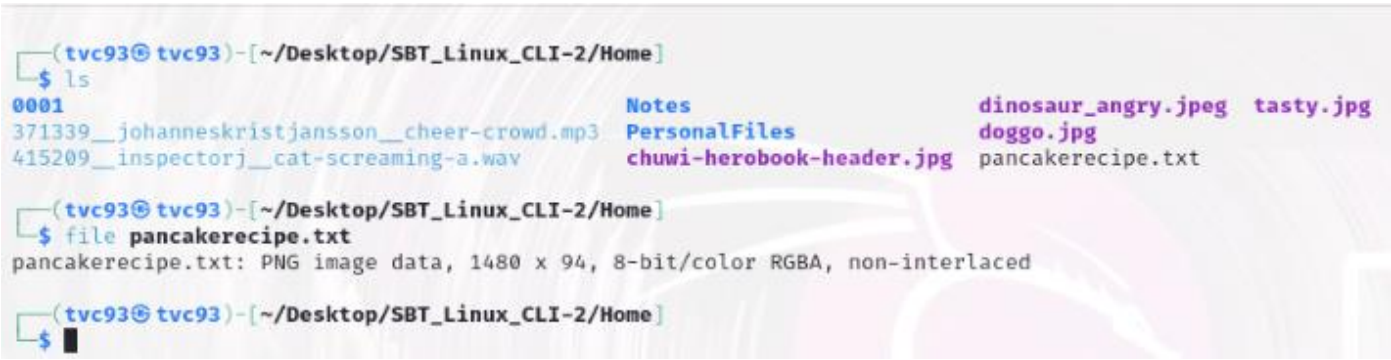
Three (3)



3. **There are two files with incorrect extensions, what are their filenames? (Without the file extensions)**

doggo.zip → JPEG

pancakerecipe.txt → PNG



4. **One of these incorrect extension files hides a message, what is it?**

```
┌──(tvc93㉿tvc93)-[~/Desktop/SBT_Linux_CLI-2/Home]
└─$ ls
0001                                    Notes                       dinosaur_angry.jpeg  tasty.jpg
371339__johanneskristjansson__cheer-crowd.mp3  PersonalFiles        doggo.jpg
415209__inspectorj__cat-screaming-a.wav        chuwi-herobook-header.jpg  pancakerecipe.txt

┌──(tvc93㉿tvc93)-[~/Desktop/SBT_Linux_CLI-2/Home]
└─$ mv pancakerecipe.txt pancakerecipe.png

┌──(tvc93㉿tvc93)-[~/Desktop/SBT_Linux_CLI-2/Home]
└─$ ls
0001                                    Notes                       dinosaur_angry.jpeg  tasty.jpg
371339__johanneskristjansson__cheer-crowd.mp3  PersonalFiles        doggo.jpg
415209__inspectorj__cat-screaming-a.wav        chuwi-herobook-header.jpg  pancakerecipe.png

┌──(tvc93㉿tvc93)-[~/Desktop/SBT_Linux_CLI-2/Home]
└─$
```

Open PNG file → SIERRA ECHO CHARLIE ROMEO ECHO TANGO

5. **There is a text file with the string "bankdetails" as part of the filename. What is the full filename?**

```
┌──(tvc93㉿tvc93)-[~/Desktop/SBT_Linux_CLI-2]
└─$ ls
Home  asdafada.txt

┌──(tvc93㉿tvc93)-[~/Desktop/SBT_Linux_CLI-2]
└─$ find Home -name "*bank*"
Home/PersonalFiles/Work Stuff/11_09_2019_statement_bankdetails.txt

┌──(tvc93㉿tvc93)-[~/Desktop/SBT_Linux_CLI-2]
└─$
```

11_09_2019_statement_bankdetails.txt

6. **What is the flag value inside the text file within the hidden directory?**

```
┌──(tvc93㉿tvc93)-[~/…/SBT_Linux_CLI-2/Home/PersonalFiles/Work Stuff]
└─$ ls
11_09_2019_statement_bankdetails.txt  'Meeting Notes'

┌──(tvc93㉿tvc93)-[~/…/SBT_Linux_CLI-2/Home/PersonalFiles/Work Stuff]
└─$ ls -a
.   ..   .Private   11_09_2019_statement_bankdetails.txt  'Meeting Notes'

┌──(tvc93㉿tvc93)-[~/…/SBT_Linux_CLI-2/Home/PersonalFiles/Work Stuff]
└─$ cd .Private

┌──(tvc93㉿tvc93)-[~/…/Home/PersonalFiles/Work Stuff/.Private]
└─$ ls
readme.txt

┌──(tvc93㉿tvc93)-[~/…/Home/PersonalFiles/Work Stuff/.Private]
└─$ cat readme.txt
106019BAL0S0A1

┌──(tvc93㉿tvc93)-[~/…/Home/PersonalFiles/Work Stuff/.Private]
└─$
```

106019BAL0S0A1

Steganography

3.31 - Steghide

Steghide = Steganography tool that allows users to embed and extract hidden data within various types of images and audio files.

- **Supports** → JPG, BMP, WAVA, and AU.

Steghide Command Syntax:

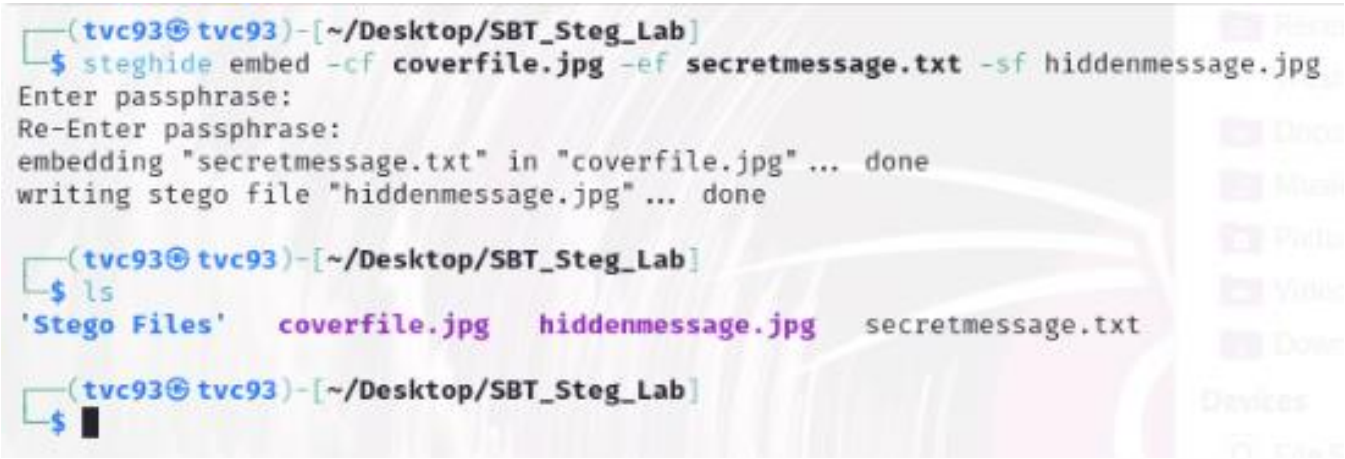
- **steghide** → selects the tool
- **embed** → selects the mode for embedding files
- **extract** → selects the mode for extracting files
- **-cf** → selects the cover file
- **-ef** → selects the embed file
- **-sf** → selects the steganography file

Embedding example: steghide embed –cd image.jpg –ef text.txt –sf image2.jpg

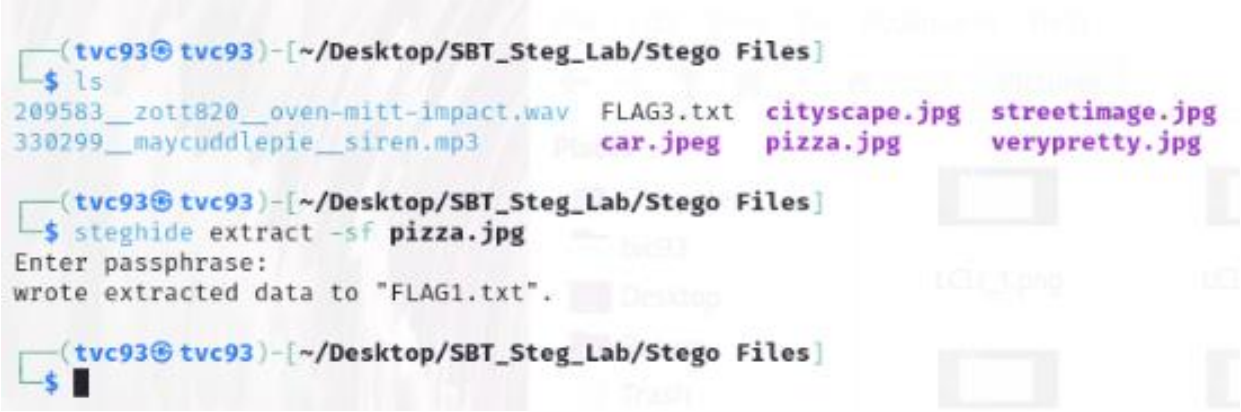
Extracting example: steghide extract –sf image2.jpg

3.32 - Steganography Activity

1. Embed the file “secretmessage.txt” inside the cover file “coverfile.jpg” and name the output stegofile “hiddenmessage.jpg”

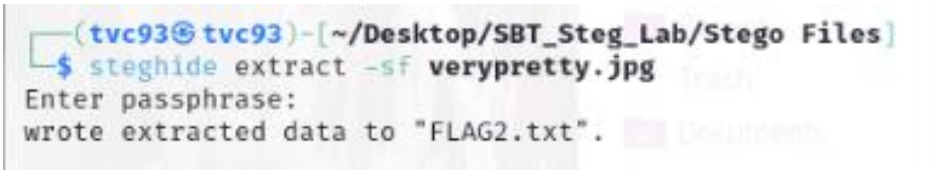


2. Flag 1 is hidden inside a text file in one of the steganography files. Which is the value?



Hidden text = kAN105KS

3. Flag 2 is hidden inside a text file in one of the steganography files. Which is the value?



Hidden text = 001JDANL

4. Flag 3 is hidden inside a text file in one of the steganography files. Which is the value?

Hidden text = 1LRBA9IU

Cracking ZIP Files

3.41 - Zip

Zip = Open-source command-line tool that allows users to compress files and directories into a single ZIP archive.

- **-r** → Recursively add directories to the ZIP archive.
- **-e** → Encrypt the contents of the ZIP file (adds password protection).
- **-q** → Quite mode (suppresses output messages).
- **-v** → Verbose mode (displays detailed information during the process).

Zip Command Syntax: zip [options] [zipfile] [files/directory]

Unzip Command Syntax: unzip [options] [zipfile]

3.42 - fcrackzip

Fcrackzip = Open-source command-line tool used to crack password-protected ZIP archives.

- **Brute Force Attack** → Attempts every possible combination of characters until the correct is found.
- **Dictionary Attack**→ Uses a list of potential passwords from a file and tries each one.

Fcrackzip Command Syntax: fcrackzip [options] [zipfile]

- **-b** → Brute force algorithm.
- **-c** → Specify the character set for brute force (a = lowercase letters, A = uppercase letters, 1 = numbers.
- **-l** → Specify the length of the password.
- **-u** → use unzip to weed out wrong passwords (enables cracking).
- **-D** → Use a dictionary file.
- **-p** → use STRING as the initial (or whole) password.

Brute Force Example: fcrackzip -b -u -c aA1 -l 4 file.zip

Dictionary Attack Example: fcrackzip -D -u -p dictionary.txt file.zip

3.43 - Cracking ZIP Files Activity

a) **BruteForceAttack.zip** – You are to brute-force this ZIP file using fcrackzip. Once you have the password, extract the text file ***FLAG1.txt*** and enter the text string as your answer for the quiz. For this file, you have been informed that the password is 6 characters long, and contains only lowercase letters, and numbers. *(Time to crack approx 5mins 30secs).*

b) **DictionaryAttack.zip** – You are to brute-force this ZIP file using fcrackzip and the ***rockyou.txt*** wordlist. Once you have the password, extract the text file ***FLAG2.txt*** and enter the text string as your answer for the quiz. *(Time to crack approx 3 mins)*.

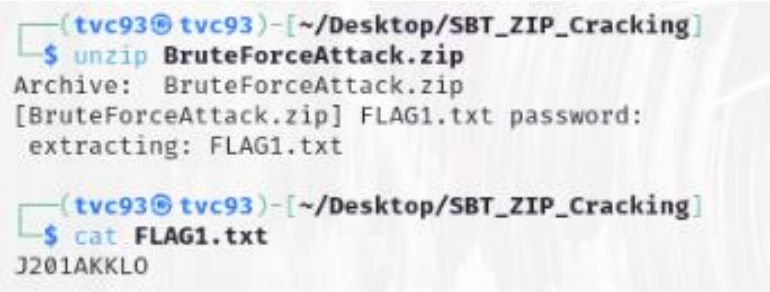
1. **What is the working password to unlock BruteForceAttack.zip?**

Password = a1b3c5

2. **What is the working password to unlock DictionaryAttack.zip?**

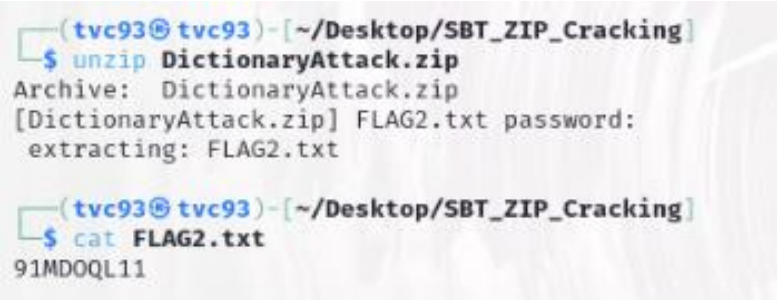
Password = FRIENDSHIPSTARS

3. **What is the text string inside FLAG1.txt?**



Text String = J201AKKLO

4. **What is the text string inside FLAG2.txt?**



Text String = 91MDOQL11

Introduction to Digital Forensics Challenge

3.51 - Introduction to Digital Forensics Challenge

The SOC has received an anonymous report that a user is potentially exfiltrating data from the company. An image of the user's hard drive has been taken, and you are responsible for analyzing the contents of a perfect copy to find any evidence of malicious activity. Using your newly developed skills, search through the folders and files using techniques to uncover 4 pieces of hidden information (**each piece of evidence will contain the string {1 of 4} or similar**). You will be tested on your ability to discover this information using all of the techniques taught in this course; *Linux CLI navigation, identifying incorrect file extensions, identifying hidden files/folders, steganography, and password cracking.*

1. **Evidence [1/4]**

```
┌──(tvc93㉿tvc93)-[~/…/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
└─$ ls -a
.  ..  .a0415ns.zip

┌──(tvc93㉿tvc93)-[~/…/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
└─$ unzip .a0415ns.zip
Archive:  .a0415ns.zip
[.a0415ns.zip] employeedump password:
   skipping: employeedump            incorrect password

┌──(tvc93㉿tvc93)-[~/…/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
└─$ fcrackzip -D -u -p rockyou.txt .a0415ns.zip


PASSWORD FOUND!!!!: pw == vendy13031988

┌──(tvc93㉿tvc93)-[~/…/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
└─$
```

```
┌──(tvc93㉿tvc93)-[~/…/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
└─$ unzip .a0415ns.zip
Archive:  .a0415ns.zip
[.a0415ns.zip] employeedump password:
  inflating: employeedump

┌──(tvc93㉿tvc93)-[~/…/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
└─$ ls
employeedump  rockyou.txt

┌──(tvc93㉿tvc93)-[~/…/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
└─$ cat employeedump
{Part 1 of 4}
,First Name,Last Name,Gender,Country,Age,Date,VPN UserID
1,Dulce,Abril,Female,United States,32,15/10/2017,1562
2,Mara,Hashimoto,Female,Great Britain,25,16/08/2016,1582
3,Philip,Gent,Male,France,36,21/05/2015,2587
```

a) **What is the name of the file where the evidence was found?**

Evidence file name = employeedump

b) **What is the name of the directory where this evidence was found?**

Directory name = /to-do/

c) **What piece of evidence have you found?**

Employee information

2. **Evidence [2/4]**

With ls -l you can look at the file size, helping with the steganography file identification process.

```
┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Images]
└─$ ls -l
total 560
-rw-r--r-- 1 tvc93 tvc93 163178 Oct 14  2019 'desk stock img.jpg'
-rw-r--r-- 1 tvc93 tvc93  41653 Oct 14  2019 'drupal 8 logo Stacked CMYK 300.png'
-rw-r--r-- 1 tvc93 tvc93  49025 Oct 14  2019  exploratory.jpg
-rw-r--r-- 1 tvc93 tvc93 119833 Oct 22  2019  laptop.jpg
-rw-r--r-- 1 tvc93 tvc93 107628 Oct 14  2019 'office 2.jpg'
-rw-r--r-- 1 tvc93 tvc93  25831 Oct 14  2019 'office pic1.jpg'
-rw-r--r-- 1 tvc93 tvc93  38769 Oct 14  2019  website-stock-photo.jpg
-rw-r--r-- 1 tvc93 tvc93  11802 Oct 14  2019  wireframe-design-guide.png

┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Images]
└─$ steghide extract -sf 'desk stock img.jpg'
Enter passphrase:
steghide: could not extract any data with that passphrase!

┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Images]
└─$ steghide extract -sf laptop.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!

┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Images]
└─$ steghide extract -sf 'office 2.jpg'
Enter passphrase:
steghide: could not extract any data with that passphrase!

┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Images]
└─$ █
```

Looking in the 'Saved Emails' directory, using **cat** on the file "Form1.jpg" exposes the following:

```
┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Saved Emails]
└─$ ls -l
total 288
-rw-r--r-- 1 tvc93 tvc93 288832 Oct 22  2019  Form1.jpg
-rwxrw-r-- 1 tvc93 tvc93   1221 Sep  8  2020 'Website Update Report 01_10_2019.eml'

┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Saved Emails]
└─$ cat Form1.jpg
◆PNG
▒
IHDRa◆◆gAMA◆◆
              ◆asRGB◆◆◆ cHRMz&◆◆◆◆◆u0◆`:◆p◆◆Q<EPLTE◆k◆◆◆◆◆◆UUUDDD◆◆◆◆"""◆◆◆fff◆◆333◆◆
UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
```

```
UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
2◆A◆H◆c%tEXtdate:create2016-06-27T08:26:44+00:00◆◆V◆%tEXtdate:modify2016-06-27T08:26:44+00:00◆◆◆PtEXtSoftwareGPL Ghostscript 8.64jN◆◆
tEXtgenerator◆2IEND◆B`◆

Simon, I have usernames and passwords for the VPN. Still on my work PC. Don't want to risk emailing them just yet. When I do, the file is a .jp
g image + password for extraction is 'password'. Use steghide. Talk again soon
```

```
┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Images]
└─$ steghide extract -sf laptop.jpg
Enter passphrase:
wrote extracted data to "passwords".

┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Images]
└─$ ls
'desk stock img.jpg'                    exploratory.jpg  'office 2.jpg'
'drupal 8 logo Stacked CMYK 300.png'    laptop.jpg       'office pic1.jpg'

┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Images]
└─$ cat passwords
{2/4}
a123456
vincent
```

a) **What is the name of the file where the evidence was found?**

Evidence file name = laptop.jpg

b) **What is the name of the directory where this evidence was found?**

Directory name = /Images/

c) **What piece of evidence have you found?**

List of employee passwords

3. **Evidence [3/4]**

```
┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Weekly Meeting Notes/Week 10]
└─$ ls -la
total 16
drwxr-xr-x 2 tvc93 tvc93 4096 Jan 11  2020 .
drwxr-xr-x 4 tvc93 tvc93 4096 Jan 11  2020 ..
-rw-r--r-- 1 tvc93 tvc93 2644 Oct 22  2019 posidon.xml
-rw-r--r-- 1 tvc93 tvc93  253 Oct 22  2019 tue

┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Weekly Meeting Notes/Week 10]
└─$ file *
posidon.xml: PNG image data, 162 x 147, 8-bit/color RGB, non-interlaced
tue:         ASCII text

┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Weekly Meeting Notes/Week 10]
└─$ mv posidon.xml posidon.png

┌──(tvc93㉿tvc93)-[~/Desktop/J Harrison Disk Image 10.09.2019/Weekly Meeting Notes/Week 10]
└─$ ls
posidon.png  tue
```

{3/4}
OFFICES//
UK LONDON
UK MANCHESTER
US WASHINGTON
UK EXETER
US TAMPA, FL

a) **What is the name of the file where the evidence was found?**

Evidence file name = posidon.xml

b) **What is the name of the directory where this evidence was found?**

Directory name = /Week 10/

c) **What piece of evidence have you found?**

Office locations

4. **Evidence [4/4]**

The “bootsrap.min.abc” file extension is suspicious, so we take a look:

```
┌──(tvc93㉿tvc93)-[~/…/WebDev work/unfinished webpages/templatemo_508_power/css]
└─$ file *
animate.css:          ASCII text, with very long lines (460)
bootstrap.min.abc:    ASCII text, with very long lines (65005)
bootstrap.min.css:    ASCII text, with very long lines (65019)
font-awesome.css:     troff or preprocessor input, ASCII text, with very long lines (305)
owl-carousel.css:     ASCII text, with CRLF line terminators
templatemo_misc.css:  ASCII text, with CRLF line terminators
templatemo_style.css: ASCII text, with CRLF line terminators

┌──(tvc93㉿tvc93)-[~/…/WebDev work/unfinished webpages/templatemo_508_power/css]
└─$ cat bootstrap.min.abc
/*!
 * Bootstrap v3.1.1 (http://getbootstrap.com)
 * Copyright 2011-2014 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 */

/*! {Part 4 of 4}
 * This is in case Colin tries to screw me. I'll expose him.
 * Colin Andrews
 * 31 years old
 * lives in Suffolk, UK
 * drives a Kia Sportage
 * buys and sells valid company credentials to hackers
 * phishing attacks, malware distribution

 * (still got his email addresses, domains, mobile no. and BTC wallet address on my personal PC)
 */
```

a) **What is the name of the file where the evidence was found?**

Evidence file name = bootstrap.min.abc

b) **What is the name of the directory where this evidence was found?**

Directory name = /css/

c) **What piece of evidence have you found?**

Colin’s information

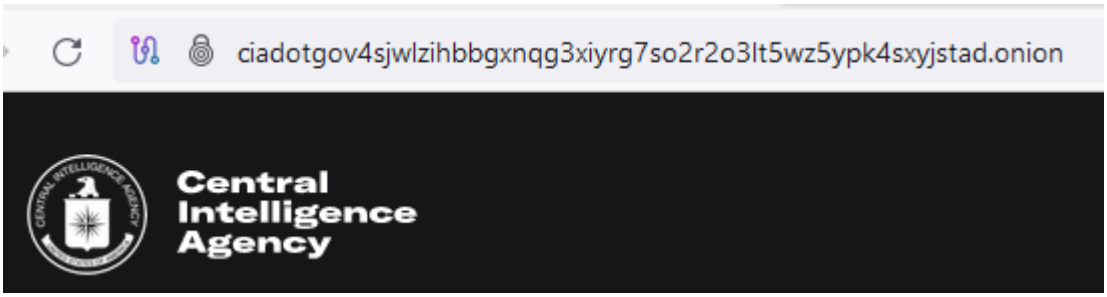
4 - Introduction to Dark Web Ops

Accessing the Dark Web

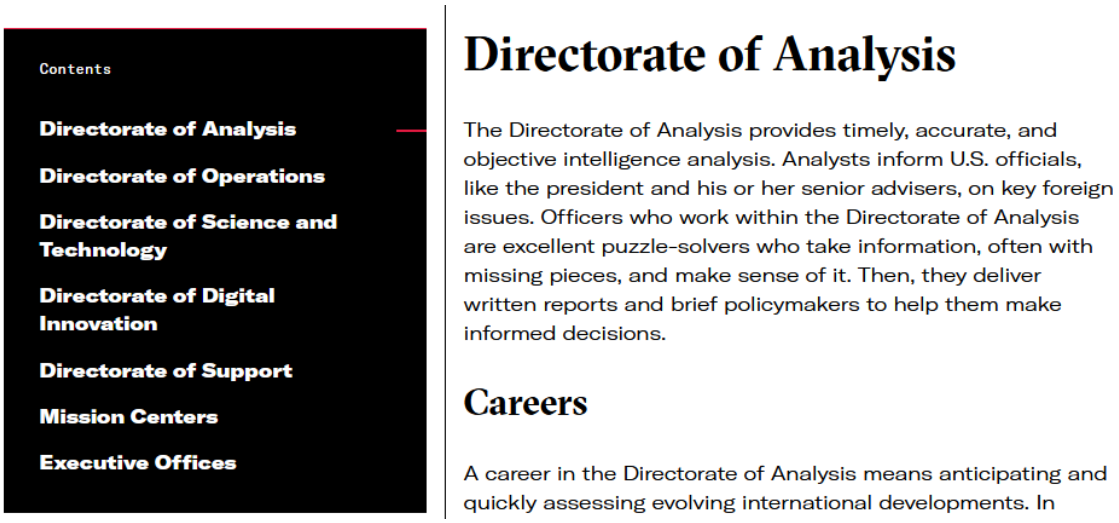
4.11 – Accessing the Dark Web

1. **What is the current URL for the CIA mirror website on the dark web?**

URL: http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/



2. **Visit the CIA mirror site and search for "Our Organization" and the "About" sub-menus. What is the first of the seven basic components of CIA?**



Directorate of Analysis, Directorate of Operations, Directorate of Science and Technology, Directorate of Digital Innovation, Directorate of Support, Mission Centers, and Executive Offices.

3. **What is the current URL for the ProPublica investigative journalism outlet?**

URL: http://p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyeznfu5uqd.onion/

4. **On the ProPublica site, click on "About" at the top. Copy and paste the first sentence under the heading "The Mission".**

The Mission:

"To expose abuses of power and betrayals of the public trust by government, business, and other institutions, using the moral force of investigative journalism to spur reform through the sustained spotlighting of wrongdoing."

Intro to Dark Web Ops Challenge

4.21 - Introduction to Dark Web Ops Challenge

In this scenario, you will be gaining access to a low-level dark website (hosted by SBT) and collecting intelligence about one of the users. You will play the role of a law enforcement officer, working to track a group of **drug traffickers**, after a tip that a large shipment will be coming into the seaport soon. Find intelligence that can be used to track the criminals and seize their illegal goods before they can hit the streets.

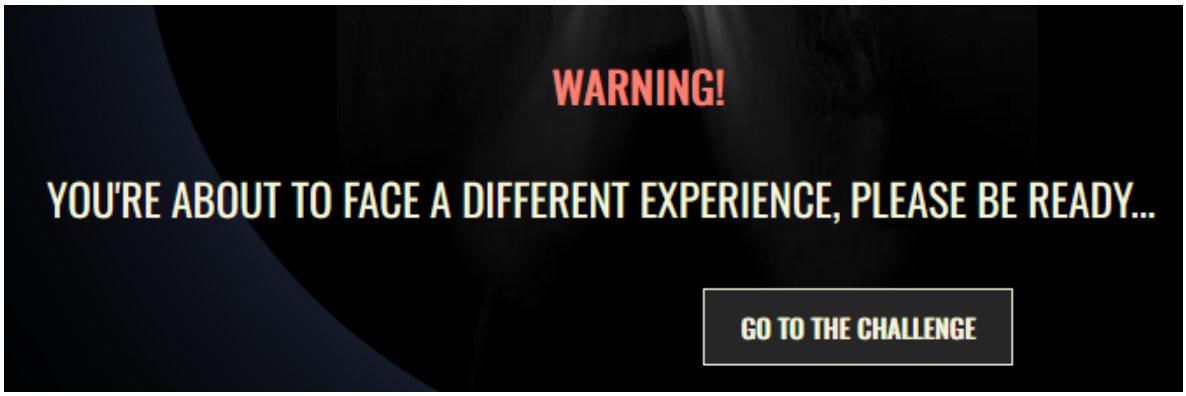
Last month we were informed about a huge drug trafficking network that was taking place in the UK through the TOR network, in response to this situation we set to work and managed to dismantle their main TOR marketplace to stop drugs from reaching the streets of the UK. However, we were informed that one of the creators of this network managed to evade us and is now continuing to carry out this type of activity. This is where you come in. We think we have found the site that this individual uses to "tell their stories" regarding criminal activity.

We need you to find evidence that will allow us to identify this subject, relate it to drug trafficking crimes, and bring them to justice. We know this is a difficult task, but we are confident in your abilities, and we are sure that you will succeed.

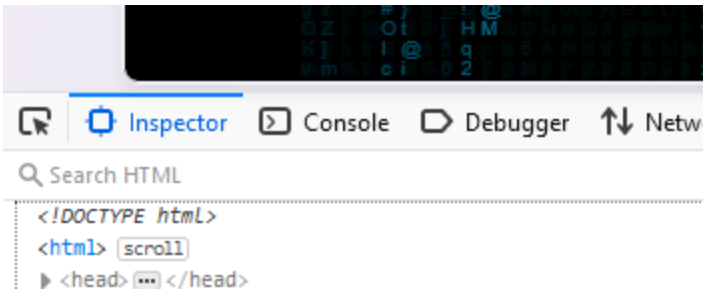
(1) Gain access to the site

a) Visit the URL, click on ‘Start Challenge’ button.

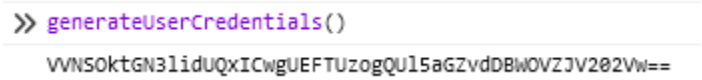
URL: 5xdv6dqxv2bsbmlgttsq3ma3nw6ffa2zhqbl7o4w46p32wsqulzrtsqd.onion



b) When presented with a login screen, right-click and select “Inspect Element”.



c) Select the ‘Console’ tab and enter in the command: generateUserCredentials().

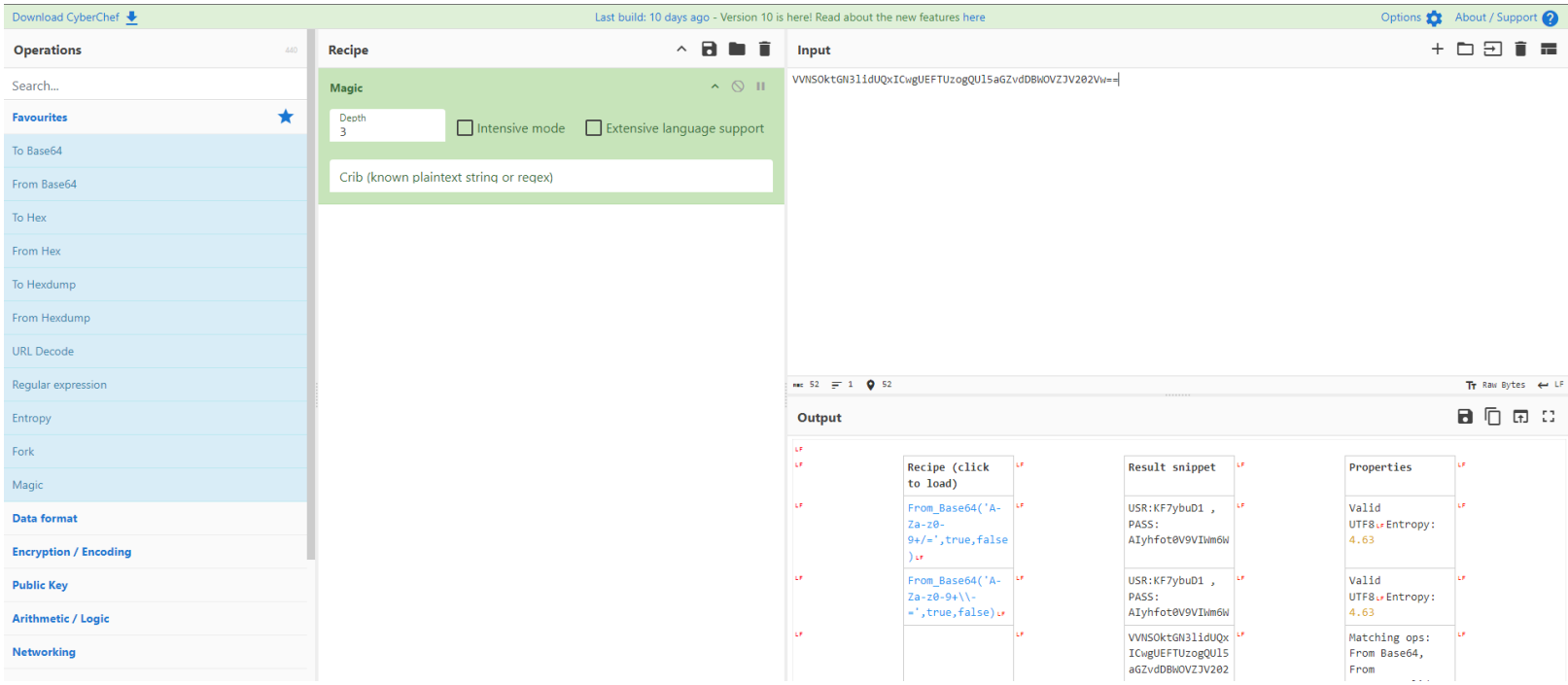


We got encrypted credentials.

d) Decode the answer

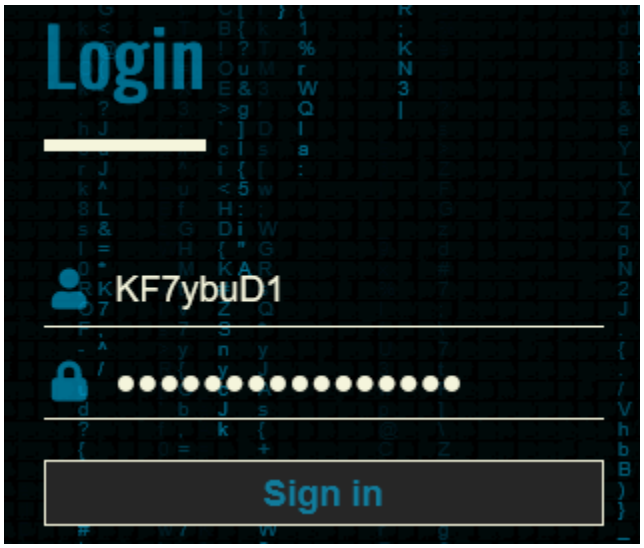
Go to cyberchef to decode the credentials:
https://gchq.github.io/CyberChef/#input=oEQ51QyX//8

- Using the magic mode for decoding:



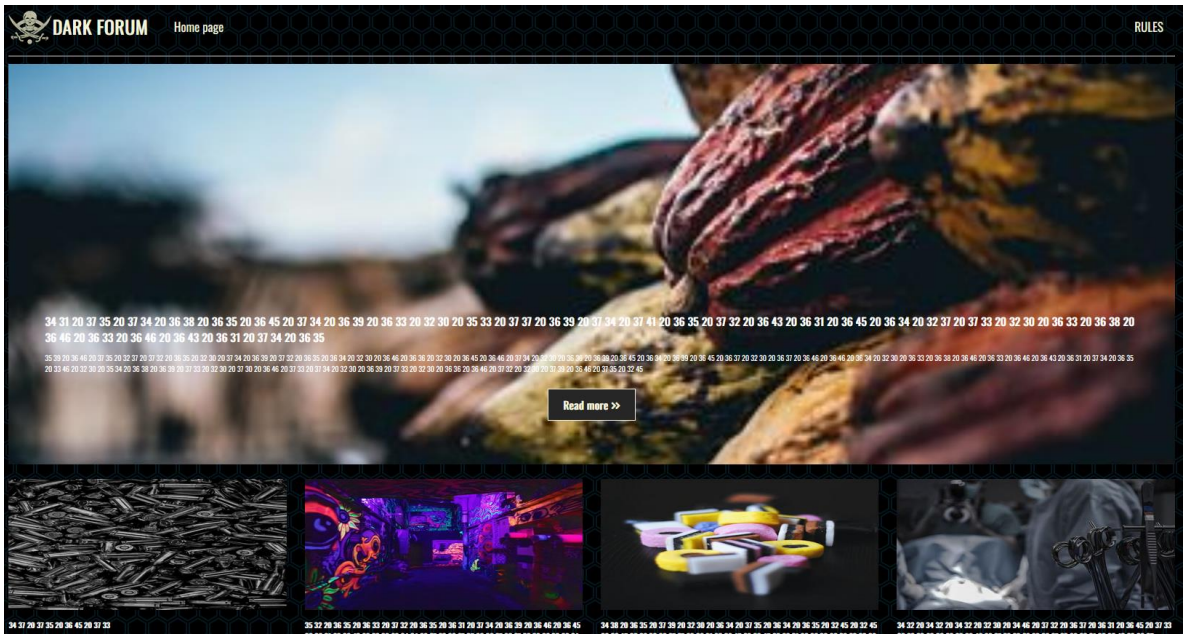
Username = KF7ybuD1

Password = AIyhfot0V9VIWm6W



(2) Find evidence that the individual is involved in drug trafficking

We find many posts with encoded text:



Using cyberchef we can decode the text of each post: (from hex decode)

First post: Authentic Switzerland's chocolateYou're tired of not finding good chocolate? This post is for you.

Second post: GunsWANNA KNOW HOW TO BUY YOUR GUNS? THIS IS FOR YOU

Third post: Recreational Drugs Buying/SellingLet the party begins! (Everything you wanna know about drug dealing)

Fourth post: Hey dude... wanna candy? (The real D king!) Deliver the package, collect the money and live like a king!

Fifth post: BBB Organs for saleAre you such an alcoholic that your kidney stopped working? Don't worry, we can get you a new one.

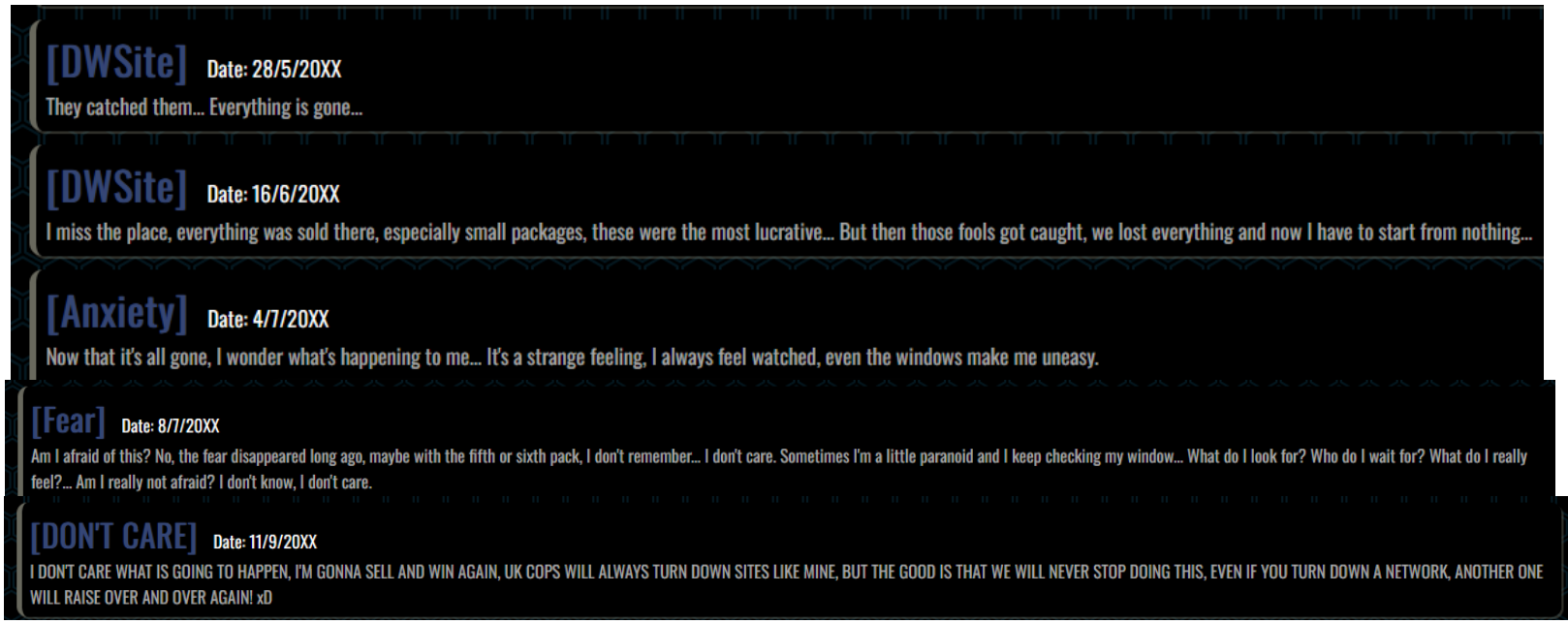
Sixth post: No more silence (Politics)THEY'LL NEVER SHUT US UP AGAIN, FREE THE COUNTRY!!!

Seventh post: Love Scales (Reptile Sales) We all love these little cute and beautiful reptiles, come and get one :3

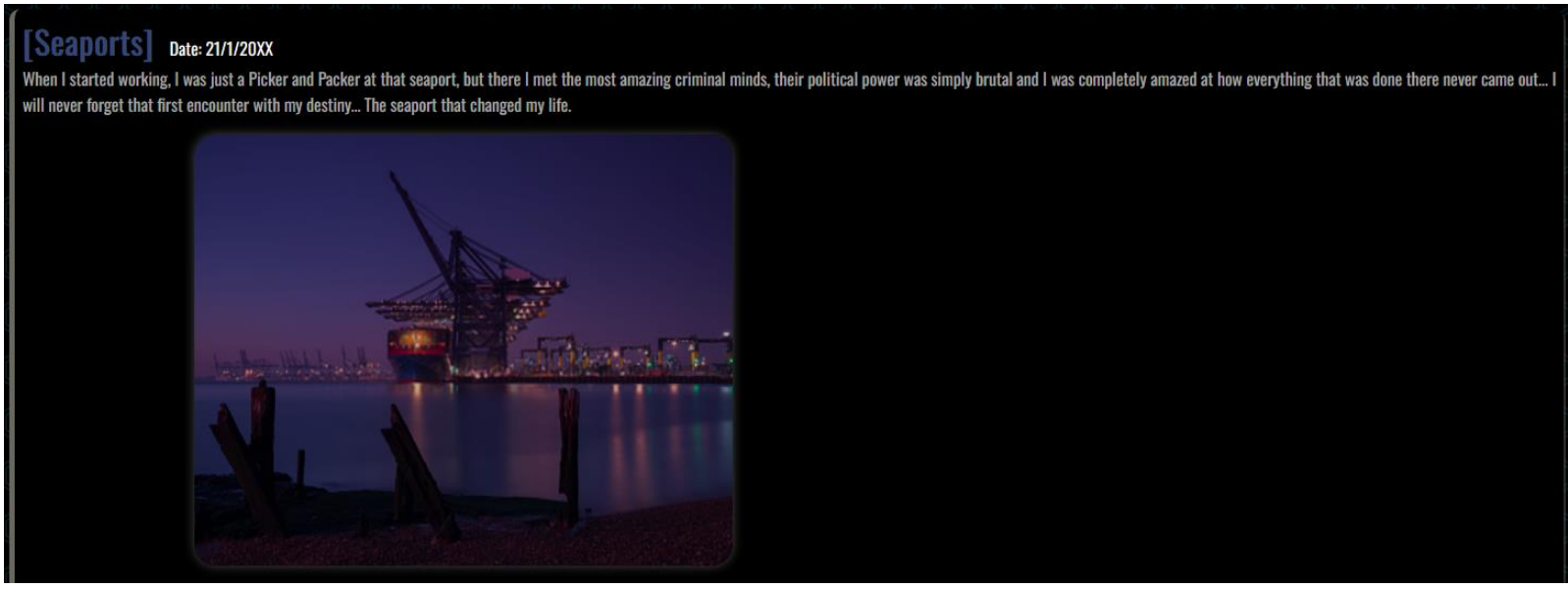
Only the third and fourth posts are related to drugs, specifically the subject we are looking for seems to be the one from the fourth post.

(3) Find any information about the next shipment that is coming in, so we can seize it

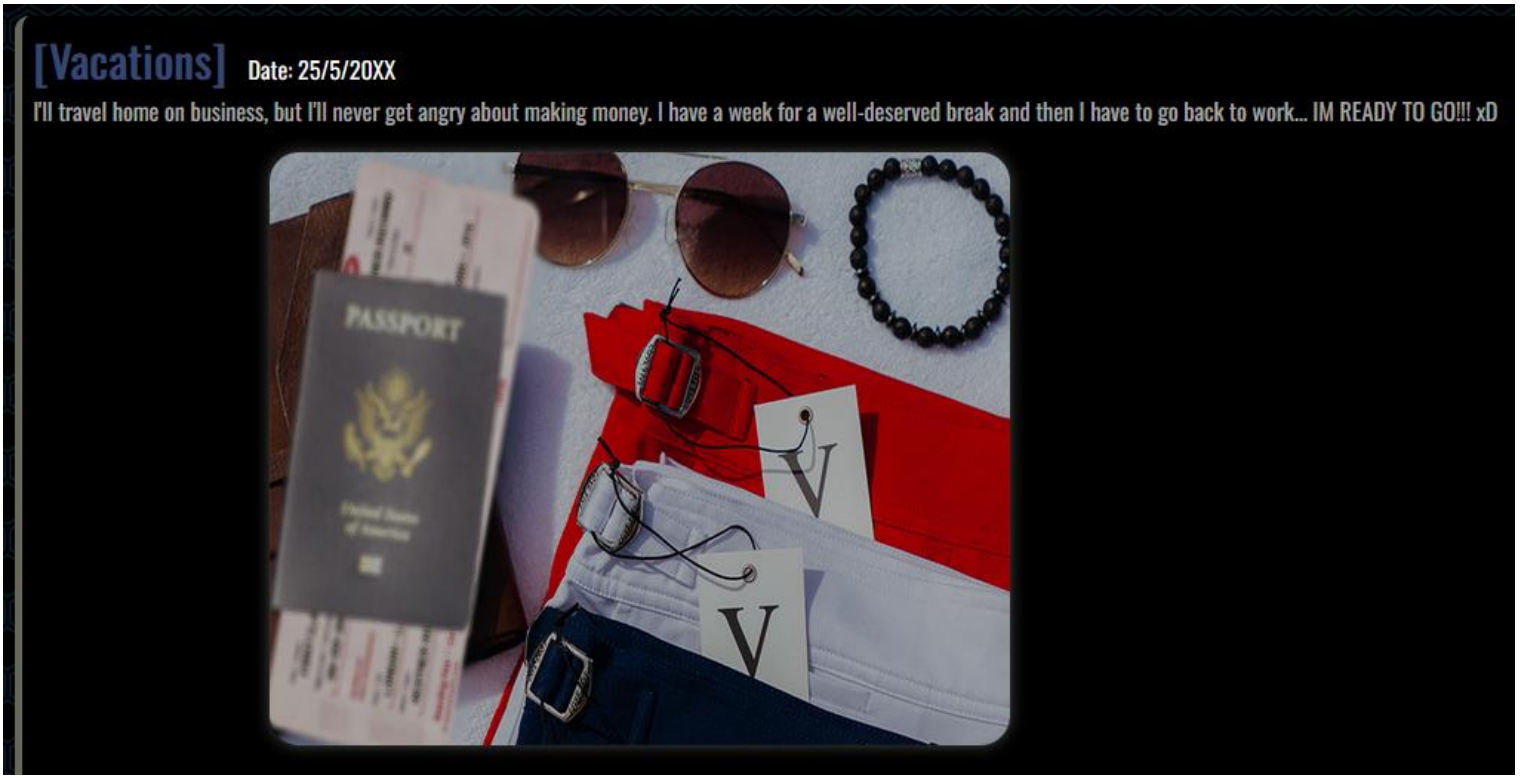
Criminal username = DarkChest984



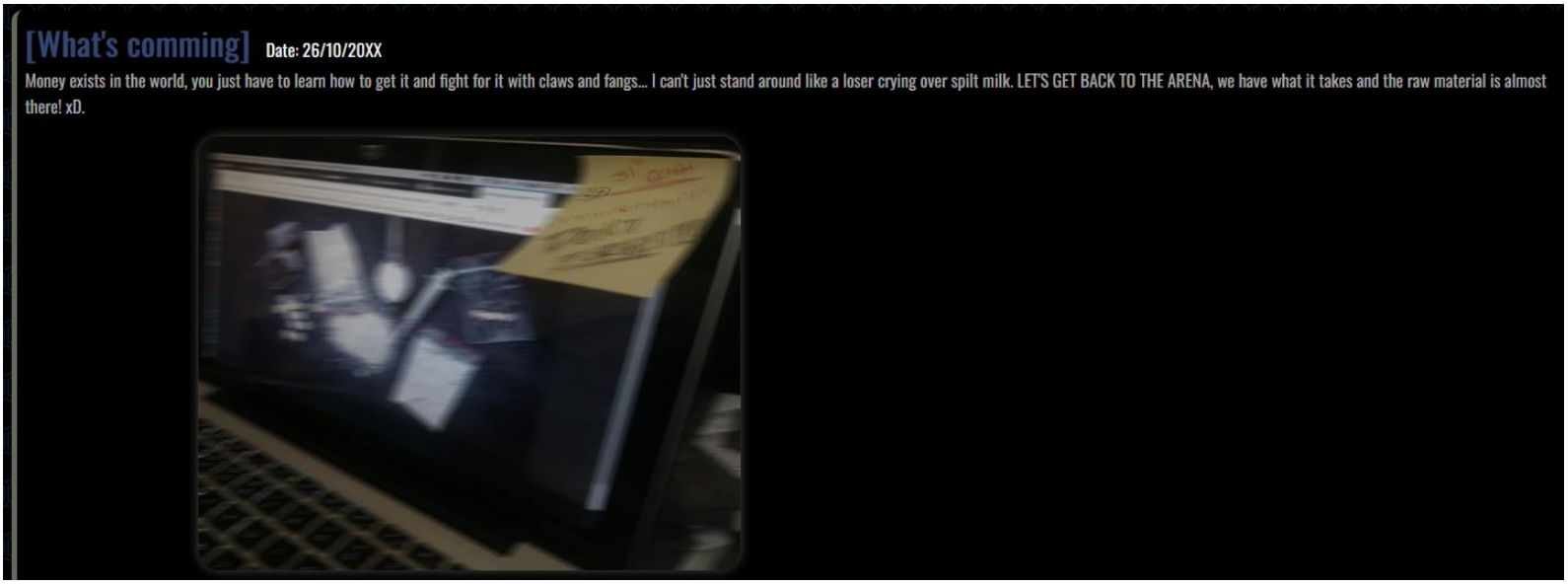
All the previous entries of the blog relate the subject with the given information about the case.



Searching for the image on the “Seaports” entry with google lens, we learn that the location is **Port of Felixstowe (Britain’s biggest & bussiest container port)**.



Analyzing the “Vacations” entry we can guess that the dealer is a US citizen. When upscaling the image and looking at the flight ticket, we learn that the name of the dealer is **KESTNER RICHARD** (flight ticket from London to New York).



Analyzing the **last post** of the criminal on the blog, by using an image enhancer we discover a location coordinates and the shipping date on the sticky note:

51° 56' 57.2"N 1° 19' 26.1"E → Port of Felixstowe (same location as the previous post) and shipping date for 31/10/20XX.

Challenge Questions:

1. **What is the username and password to gain access to the site?**

KF7ybuD1 AIyhfot0V9VIWm6W

2. **What is the suspect site username?**

DarkChest984

3. **What is the suspect first and last name?**

KESTNER RICHARD

4. **What country does the suspect currently live in?**

UK

5. **What is the date of the oldest post related to drug trafficking?**

26/11/20XX

6. **What is the date of the most recent post related to drug trafficking?**

26/10/20XX

7. **What type of encoding has been used on the site content?**

Hexadecimal

8. **What is the next drug shipment coming into the UK?**

31/10/20XX

9. **What are the GPS coordinates of the shipment delivery location?**

51° 56' 57.2"N 1° 19' 26.1"E

10. **What is the name of the seaport where the shipment is being delivered?**

Felixstowe

Last month we were informed about a huge drug trafficking network that was taking place in the UK through the TOR network, in response to this situation we set to work and managed to dismantle their main TOR marketplace to stop drugs reaching the streets of the UK. However, we were informed that one of the creators of this network managed to evade us and is now continuing to carry out this type of activity. This is where you come in. We think we have found the site that this individual uses to "tell their stories" regarding criminal activity.

We need you to find evidence that will allow us to identify this subject, relate it to the drug trafficking crimes, and bring them to justice. We know this is a difficult task, but we are confident in your abilities and we are sure that you will succeed.

1] Gain access to the site (We're sure there's some way for users to gain valid credentials fairly easily).
2] Find evidence that the individual is involved in drug trafficking.
3] Find any information about the next shipment that is coming in, so we can seize it.

```
-------------++---------------++---------------++---------------++-
                    _********************_
=================== \  CHALLENGE REPORT  / ====================
                     ******************
 _____________________________________________________
|                                                     |
|  |    \                                            |
|  | |\  \        / /     Â´  _ `Â´    __ `Â´   ___`     |
|  | | \  \  /\  / /     | | | | !_/ /! Â´--.      |
|  | | /  /\/  \/ /___   | | | |  __/  `--. Â¡     |
|  | !/  /\  /\  / Â´   ` ! !_! ! |    /`--Â´ !     |
|  !____/  \/  \/  `---Â´  `___Â´!_!    `----Â´      |
|                                          (SBT).|
 -----------------------------------------------
```

Known Info:
==========
[*] DWebsite:
5xdv6dqxv2bsbmlgttsq3ma3nw6ffa2zhqbl7o4w46p32wsqulzrtsqd.onion

Requested Info:
==========
1) What command is used in the Console to generate valid credentials?
generateUserCredentials()
2) What is the suspect's site username? DatkChest984
3) What is the suspect's first and last name? Kestner Richard
4) What country is the suspect currently living in? UK
5) What is the date of the first post related to drug trafficking?
26/11/20XX
6) What is the date of the latest post related to drug trafficking?
26/10/20XX
7) What type of encoding has been used on the site content? Hexadecimal
8) When is the next drug shipment coming into the UK? 31/10/20XX
9) What are the GPS coordinates of the shipment delivery location?
51° 56' 57.2"N 1° 19' 26.1"E
10) What is the name of the seaport where the shipment is being
delivered? Felixstowe

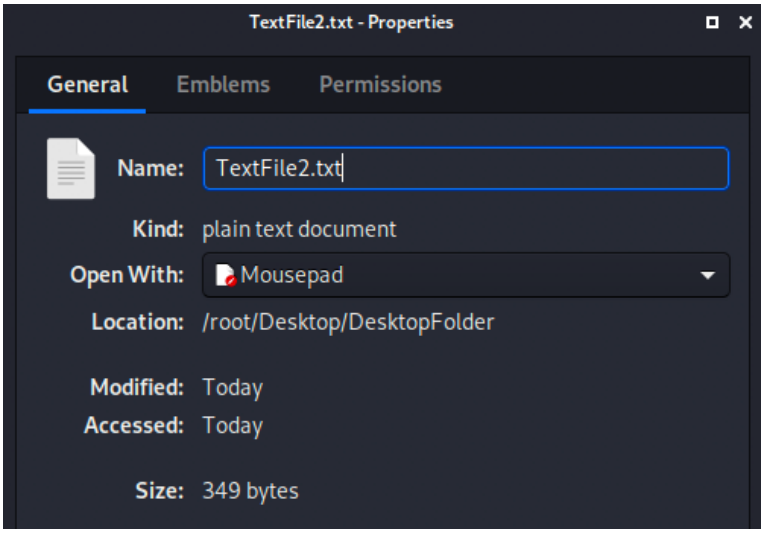
5 - Introduction to Threat Hunting

Generating Indicators of Compromise (IoCs)

5.11 - File Property IoCs

File Size & Name:

- Kilobytes (kb), megabytes (mb), gigabytes (gb), or terabytes (tb).
- **GUI** → Right-click > Properties > Size value & Name Value.
- **CLI** → "**ls -lh**" → Lists all files and their sizes.



5.12 - File Hash IoCs

Hashing = Process of converting input data into a unique fixed-length string of characters (Hash) using a hashing algorithm.

- **Hash Algorithm** → MD5, SHA-256, etc.

MD5 (Message-Digest Algorithm 5) = Cryptographic hash function that produces a 128-bit hash value.

- **md5sum** = Linux CLI command to generate MD5 hashes.
- **Command Syntax** → md5sum [options] [file]
- **-b** → Read in binary mode.
- **-t** → Read in text mode (default).
- **-c** → Check MD5 checksum files and reports if hash matches the expected value.

SHA-256 (Secure Hash Algorithm) = Cryptographic hash function that produces a 256-bit hash value.

- **Sha256sum** = Linux CLI command to generate SHA-256 hashes.
- **Command Syntax** → [options] [file]
- **-b** → Read in binary mode.
- **-t** → Read in text mode (default).
- **-c** → Check SHA-256 checksum files and reports if hash matches the expected value.

Windows PowerShell Hashing:

- **Command** → Get-FileHash [File]
- **Default Hashing Algorithm** → SHA-256
- **-algorithm** → Flag to specify what algorithm we want to use.
- **Example:** Get-FileHash -algorithm MD5 file.txt

5.13 - IoC Editor

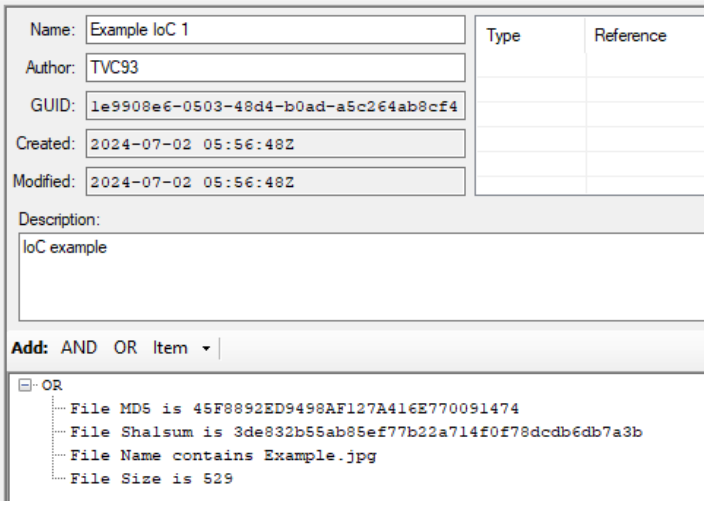
Mandiant IoC Editor = Software that provides an interface for creating, editing, and managing indicators of compromise (IoCs).

IoC File = XML file that can capture diverse information about threats

- **Create IoC File** → File > New > Indicator
- **OR Tree** → If any of the items in this tree is present in a file we get a notification.
- **AND Tree** → All items in this tree must be present in file to get a notification.

IoC File Item = Specific type of indicator within an IoC file that identifies and describes a file-related artifact that could indicate a security compromise.

- **Create IoC File Item** → Right-click > Add Item > FileItem > XXX



5.14 - Generating IoCs Activity

This activity will have you gathering IOCs from a number of files to make sure you understand everything we've covered so far. Remember, this is crucial so you can conduct your malware hunt later in the course.

1. **File Beginning With "1":**

    a) **What is the SHA-1 Hash value of this file?**
    1f221ebaee912b351ec703874f3a0aa8a019dfd9

    b) **What is the MD5 Hash value of this file?**
    cf49367f7c184ee0a9ec7bc8c1ba907f

    c) **What is the file size of this file?**
    86 bytes

    d) **What is the full file name of this file?**
    1HIGHLY_MALICIOUS.txt

2. **File Beginning With "1":**

    a) **What is the SHA-1 Hash value of this file?**
    90FFD2359008D82298821D16B21778C5C39AEC36

    b) **What is the MD5 Hash value of this file?**

    2942bfabb3d05332b66eb128e0842cff

    c) **What is the file size of this file?**
    13264 bytes

    d) **What is the full file name of this file?**
    2innocent.pdf

3. **File Beginning With "1":**

    a) **What is the SHA-1 Hash value of this file?**
    0ecd0e0a47d3a2a9e9a9c835994963f8f20ae191

    b) **What is the MD5 Hash value of this file?**
    3136fe5f1e43d07e8b509bbf710f5f31

    c) **What is the file size of this file?**
    1066208 bytes

d) **What is the full file name of this file?**
3Stock-Image-PANIC.jpg

4. **File Beginning With "1":**

a) **What is the SHA-1 Hash value of this file?**
BC371BB75B9CBBEC7819292BC3A380DF913111BE

b) **What is the MD5 Hash value of this file?**
daa5ffbcc4f371070fb8b17e87b747e6

c) **What is the file size of this file?**
43002 bytes

d) **What is the full file name of this file?**
4sales report july 2019.pdf

5. **Additional Questions:**

a) **When trying to add new IoC values, what is the first property available under the Network heading?**
Network DNS

b) **There is an option to add values from email, Snort, and Task items, True or False?**
True

c) **What does IoC stand for?**
IoC = Indicators of Compromise

d) **Which of the following are examples of IoCs?**

Email sending address, IP address, File name, File hash, String, Website URL.

Malware Hunting

5.21 - Malware Hunting

Malware Hunting → Collecting and using IoCs to identify any presence of malware within a system.

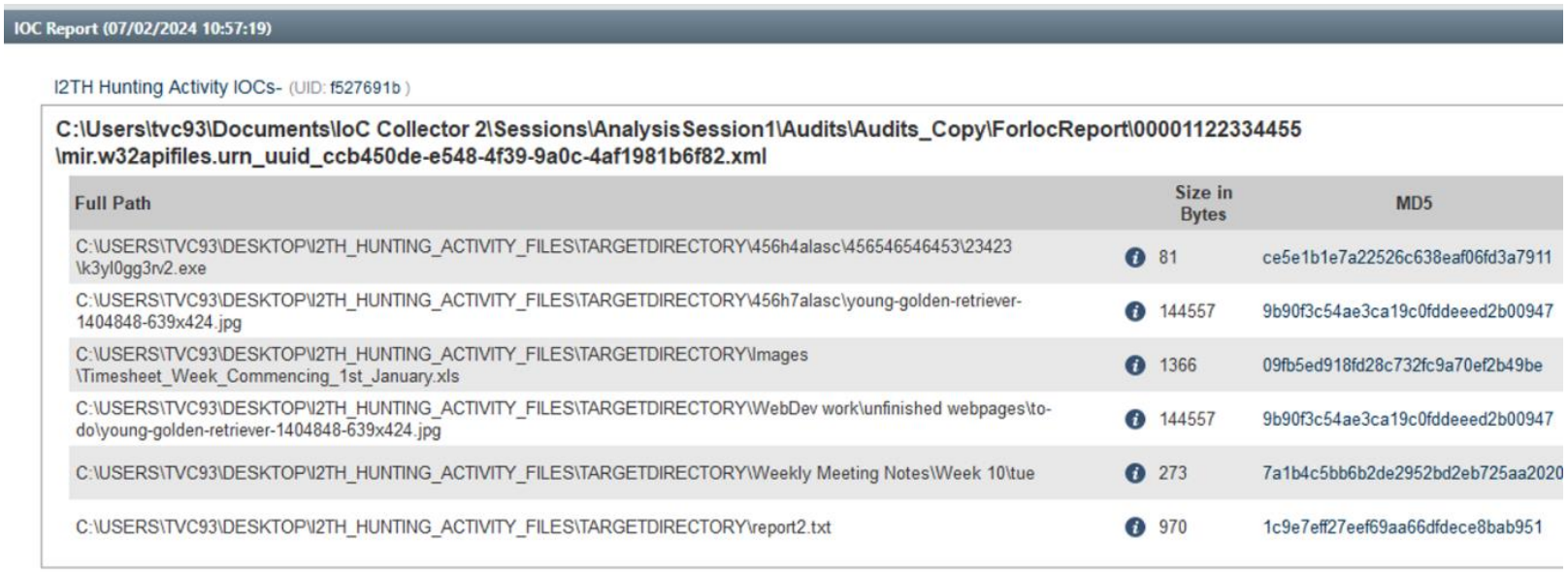
- (1) Covert malware found using IoCs.
- (2) Comparing known good values against systems to check for any differences (verifying integrity with hashes).

Mandiant Redline = Endpoint security software used for incident response and malware detection & analysis.

- Collection and analysis of RAM from Windows systems to identify IoCs (Indicator of compromise analysis).
- Give Redline an IoC file → Use audit system to search for the presence of any of the listed IoCs.
- **Create a Search Collector** → Configures a package which will collect only the data needed to search for the IoCs which you specify.

5.22 - Malware Hunting with IoCs Activity

In this activity you will be given an IOC file, and you will have to create an IOC Search Collector and use it to search for some specific files that we have hidden within a folder full of junk. You will then report on any files that have been discovered in the IOC Report generated by the .mans file by Redline.



IOC Report (07/02/2024 10:57:19)

I2TH Hunting Activity IOCs- (UID: f527691b)

C:\Users\tvc93\Documents\IoC Collector 2\Sessions\AnalysisSession1\Audits\Audits_Copy\ForIocReport\00001122334455\mir.w32apifiles.urn_uuid_ccb450de-e548-4f39-9a0c-4af1981b6f82.xml

Full Path	Size in Bytes	MD5
C:\USERS\TVC93\DESKTOP\I2TH_HUNTING_ACTIVITY_FILES\TARGETDIRECTORY\456h4alasc\456546546453\23423\k3yl0gg3rv2.exe	81	ce5e1b1e7a22526c638eaf06fd3a7911
C:\USERS\TVC93\DESKTOP\I2TH_HUNTING_ACTIVITY_FILES\TARGETDIRECTORY\456h7alasc\young-golden-retriever-1404848-639x424.jpg	144557	9b90f3c54ae3ca19c0fddeeed2b00947
C:\USERS\TVC93\DESKTOP\I2TH_HUNTING_ACTIVITY_FILES\TARGETDIRECTORY\Images\Timesheet_Week_Commencing_1st_January.xls	1366	09fb5ed918fd28c732fc9a70ef2b49be
C:\USERS\TVC93\DESKTOP\I2TH_HUNTING_ACTIVITY_FILES\TARGETDIRECTORY\WebDev work\unfinished webpages\to-do\young-golden-retriever-1404848-639x424.jpg	144557	9b90f3c54ae3ca19c0fddeeed2b00947
C:\USERS\TVC93\DESKTOP\I2TH_HUNTING_ACTIVITY_FILES\TARGETDIRECTORY\Weekly Meeting Notes\Week 10\tue	273	7a1b4c5bb6b2de2952bd2eb725aa2020
C:\USERS\TVC93\DESKTOP\I2TH_HUNTING_ACTIVITY_FILES\TARGETDIRECTORY\report2.txt	970	1c9e7eff27eef69aa66dfdece8bab951

1. **How many entries are there in the IoC Report?**

Number of entries in the IoC report = 6

2. **What is the file name that has the MD5 hash of "ce5e1b1e7a22526c638eaf06fd3a7911"?**

   File name = k3yl0gg3rv2.exe

3. **What is the file path that contains the file with a size of 144557 bytes?**

TARGETDIRECTORY\456h7alasc\young-golden-retriever-1404848-639x429.jpg

4. **Which of the following alerting file sizes are present in the IoC report?**

81 bytes, 144557 bytes, 1366 bytes, 144557 bytes, 273 bytes, 970 bytes.

5. **What is the file name that has MD5 hash of 7a1b4c5bb6b2de2952bd2eb725aa2020?**

   File name = tue

Introduction to Threat Hunting Challenge

5.31 - Introduction to Threat Hunting Challenge

In this challenge, you will need to complete two objectives:

- Collect IoCs from two samples files and generate two IoC files in Mandiant IOC Editor.
- Use the IoC file to audit a complete system using Mandiant Redline.

You are a Junior Threat Hunter working for an organization. Your Threat Intelligence team has obtained two malware samples, but they're too busy dealing with a data breach dump that includes employee credentials, so you'll need to hunt for any presence of the malware in any systems. As you're new to the role, the Senior Threat Hunter is using advanced tools to assess all systems company-wide, but he has given you permission to run a live hunt on one system. A disk image was taken, as the system is in a remote office. You have been told to gather your own IOCs from two malware samples, and conduct a hunt on the files using Mandiant IOC Editor and Mandiant Redline. You are to report on the findings generated by the IOC Reports.

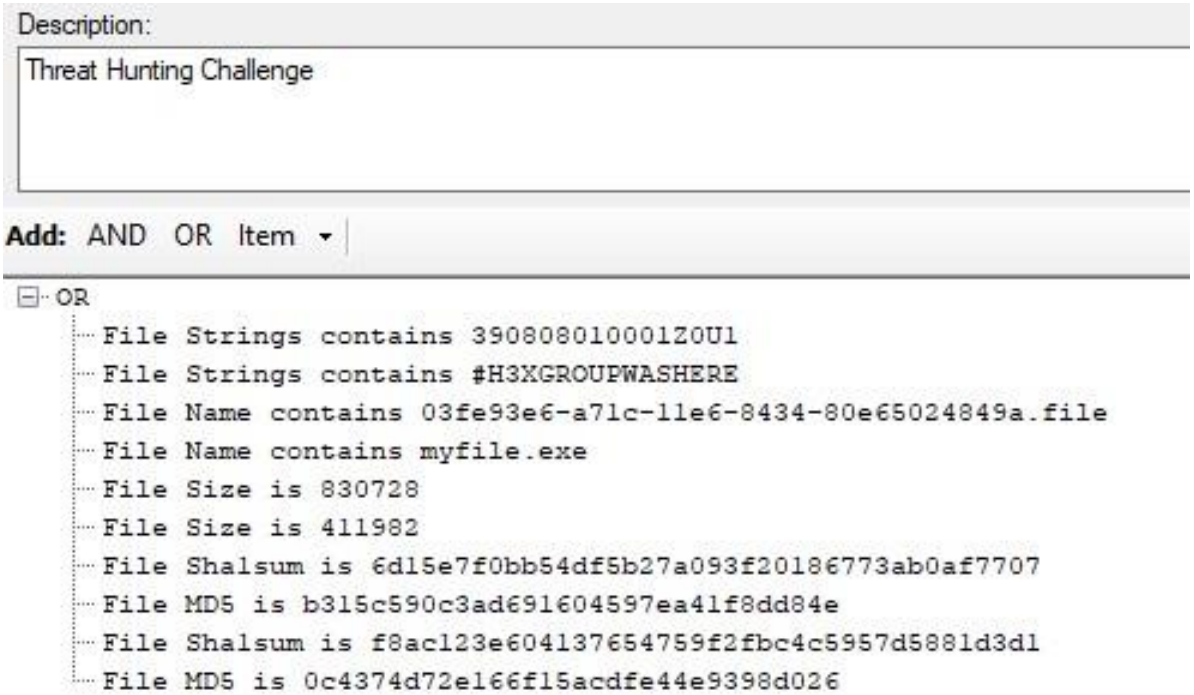
Challenge resources:

- .ZIP file containing the target directory for this challenge.
- *.ZIP file that contains two malware samples.*

CTI Team Note For Hunter - Notepad

File Edit Format View Help

```
Hey Hunter, Matt from the Threat Intel Team here. Got a few things that might help you.

> The two samples are in the folder "CTI Team - Malware Samples" on the Desktop. Grab your
IOCs from them.

> It goes without saying, but don't open the malware. Why? Because it's malware.

> We've saved you some work and identified the following strings that are present in
the samples, use them as IOCs (but make sure Redline is accepting Strings, see the
brief to enable them); 3908080100017Z0U1 , #H3XGROUPWASHERE

> We believe the User "DaveS" has potentially downloaded both samples, so limit Redline
to only search directories associated with this user, otherwise you'll miss your lunch
break ;)

> Good luck! Sorry to put this on you, we're just so busy today.


// Matt - Threat Intelligence Analyst
```



IOC Report (7/3/2024 9:07:12 AM)

Threat Hunting Challenge- (UID: af51bac7)

C:\Users\tvc93\Documents\IoC Collector Challenge\Sessions\AnalysisSession1\Audits\Audits_Copy\ForIocReport\00001122334455\mir.w32apifiles.urn_uuid_fb42901a-aa63-4eaf-92dc-be8f11284baf.xml

Full Path	Size in Bytes	MD5
C:\USERS\TVC93\DESKTOP\TH_CHALLENGE_TARGET-2\DAVES\3D Objects\3D\03fe93e6-a71c-11e6-8434-80e65024849a.file.exe	830721	9232e4cb2d0b17463351dc0aed0de01d
C:\USERS\TVC93\DESKTOP\TH_CHALLENGE_TARGET-2\DAVES\Documents\WindowsPowerShell\03fe93e6-a71c-11e6-8434-80e65024849a.file.exe	830719	2ca451f261e81cb84cc6a3a950ef49a0
C:\USERS\TVC93\DESKTOP\TH_CHALLENGE_TARGET-2\DAVES\Downloads\FREEdesktopWALLPAPERS\wallpaperHD.exe	411982	0c4374d72e166f15acdfe44e9398d026
C:\USERS\TVC93\DESKTOP\TH_CHALLENGE_TARGET-2\DAVES\Pictures\myfile.exe	411982	0c4374d72e166f15acdfe44e9398d026
C:\USERS\TVC93\DESKTOP\TH_CHALLENGE_TARGET-2\DAVES\Searches\Saved\234272a\indexed-search-history.exe	830728	b315c590c3ad691604597ea41f8dd84e

How many pieces of malware were detected using IoCs generated from the two samples?

Pieces of malware detected = 5

1. **What is the file name beginning with \"w\"?**

File name = wallpaperHD.exe

2. **Is there malware in the location "/DaveS/Pictures"? (True or False)**

True

3. **Which MD5 hash appears in two different files?**

0c4374d72e166f15acdfe44e9398d026

6 - Introduction to Vulnerability Management

Metasploitable 2

6.11 - Metasploit, Metasploitable, & Nmap

Metasploit = Open-source penetration testing framework that provides a suite of tools for developing and executing exploit code against a remote target machine.

- Includes exploitation modules for exploit development, payload generation, and post-exploitation.

Metasploitable = Deliberately vulnerable virtual machine created for testing and learning purposes.

- Includes various unpatched vulnerabilities, misconfigurations, and security flaws.

Nmap (Network mapper) = Open-source network scanner used to discover vulnerabilities on computer networks.

- **Host discovery** → Determine which hosts are active on a network.
- **Port Scanning** → Scan for open ports on target host.
- **Service detection** → Determine the version of services and applications running on open ports.
- **Operating System Detection** → Identify the running OS on the target host.

Nmap Command Syntax → nmap [scan type] [options] [IP Address]

a) **Scan Types:**
   - -sS → TCP SYN scan (default)
   - -sT → TCP connect scan
   - -sU → UDP scan
   - -sP → Ping scan
   - -sA → TCP ACK scan
   - -sW → TCP Windows scan
   - -sM → TCP Maimon scan

b) **Options:**

i. **Host Discovery:**
- -sn → Disable port scan, only perform port discovery.
- -Pn → Treat all hosts as online and skip host discovery.
- -PS → TCP SYN discovery on specified ports.
- -PA → TCP ACK discovery on specified ports.
- -PU → UDP discovery on specified ports.
- -PR → ARP discovery on local network.

ii. **Port Specification & Scan Order:**
- -p → Specify ports to scan (e.g: '-p 22,80,443' or '-p 1-65535')
- -F → Fast mode (scan fewer ports than default scan).

iii. **Service Version Detection:**
- - Sv → Probe open ports to determine service/version information.

iv. **OS Detection:**
- -O → Enable OS detection.

v. **Aggressive Scan Options:**
- -A → Enable OS detection, version detection, script scanning, and traceroute.

vi. **Miscellaneous Options:**
- --open → Only show open ports.
- --reason → Display the reason a port is in a particular state.
- --traceroute → Trace the path to the host.

6.12 - Metaspoiltable 2 Activity

1. **Which company created Metasploit and Metasploitable 2?**

Rapid7

2. **How many TCP ports are OPEN on MS2?**

23 OPEN TCP ports.

```
└─$ nmap -sT --open 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 03:01 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

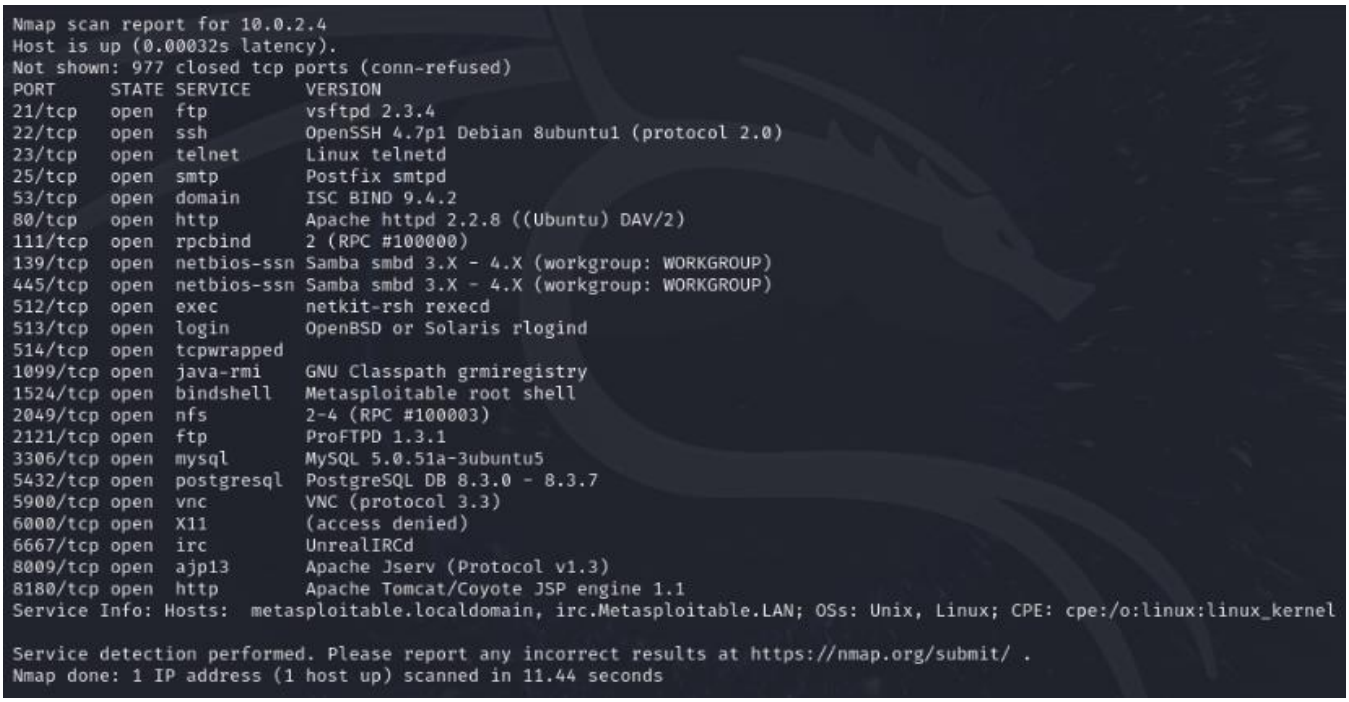
3. **How many UDP ports are OPEN on MS2?**
   7 UDP OPEN ports

```
┌──(tvc93㉿kali)-[~]
└─$ sudo nmap -sU --open 10.0.2.4
[sudo] password for tvc93:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 03:08 EDT
Stats: 0:02:20 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 15.28% done; ETC: 03:23 (0:12:56 remaining)
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 15.79% done; ETC: 03:24 (0:12:53 remaining)
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 15.80% done; ETC: 03:24 (0:12:58 remaining)
Stats: 0:04:42 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 28.74% done; ETC: 03:25 (0:11:42 remaining)
Stats: 0:07:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 44.10% done; ETC: 03:25 (0:09:32 remaining)
Stats: 0:16:26 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 94.93% done; ETC: 03:26 (0:00:53 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.00018s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 08:00:27:AD:9D:10 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1074.76 seconds
```

4. **What port is running a Metasploitable Root Shell?**

Command → nmap –sV 10.0.2.4

Port 1524



5. **What non-standard port is FTP running on (Not port 21)?**

Port 2121

6. **What version of FTP is running on the non-standard port?**

ProFTPD 1.3.1

Vulnerability Scanning

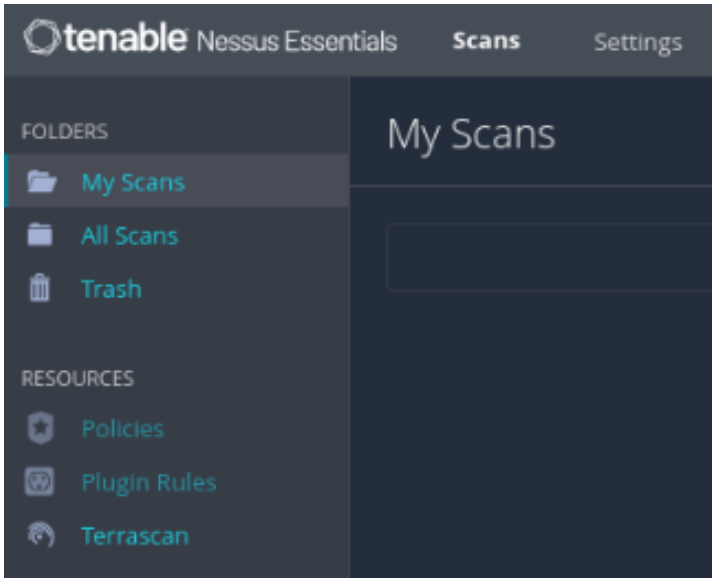
6.21 - Nessus

Tenable Nessus = Proprietary vulnerability scanner developed by Tenable designed to identify security vulnerabilities, configuration issues, and malware in computer systems, networks, and applications.

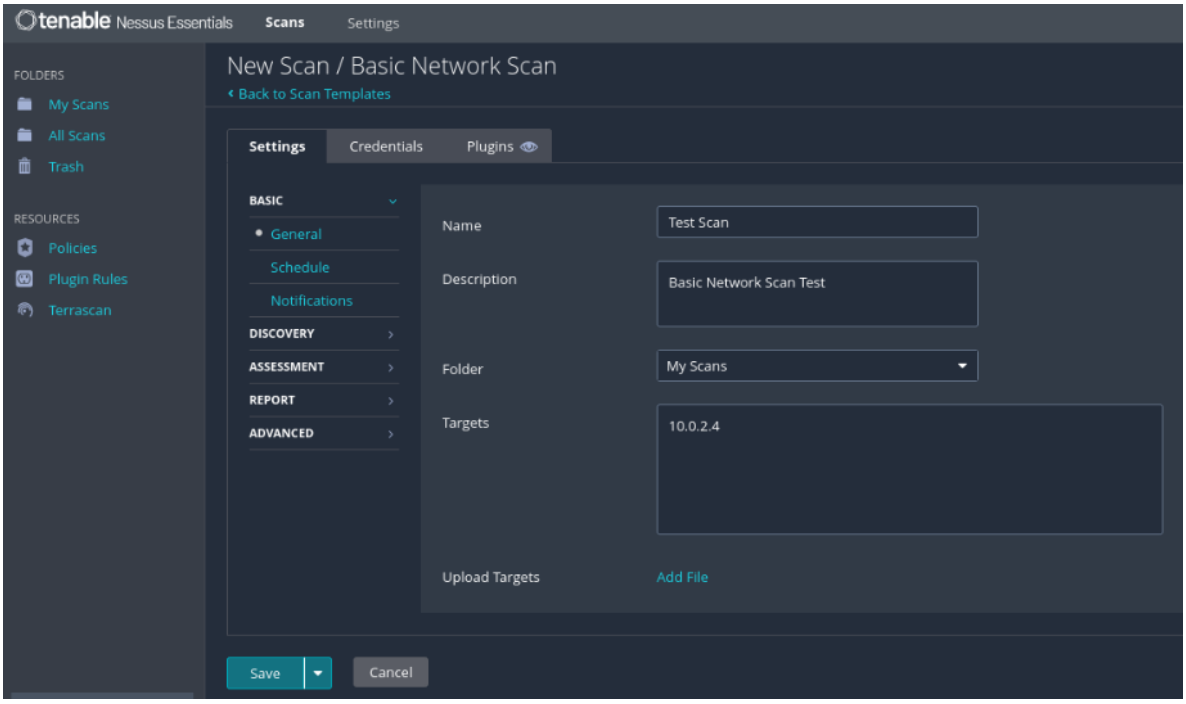
- **Nessus Essentials** = Free version of Nessus vulnerability scanner software that provides basic vulnerability assessment capabilities.

Nessus GUI:

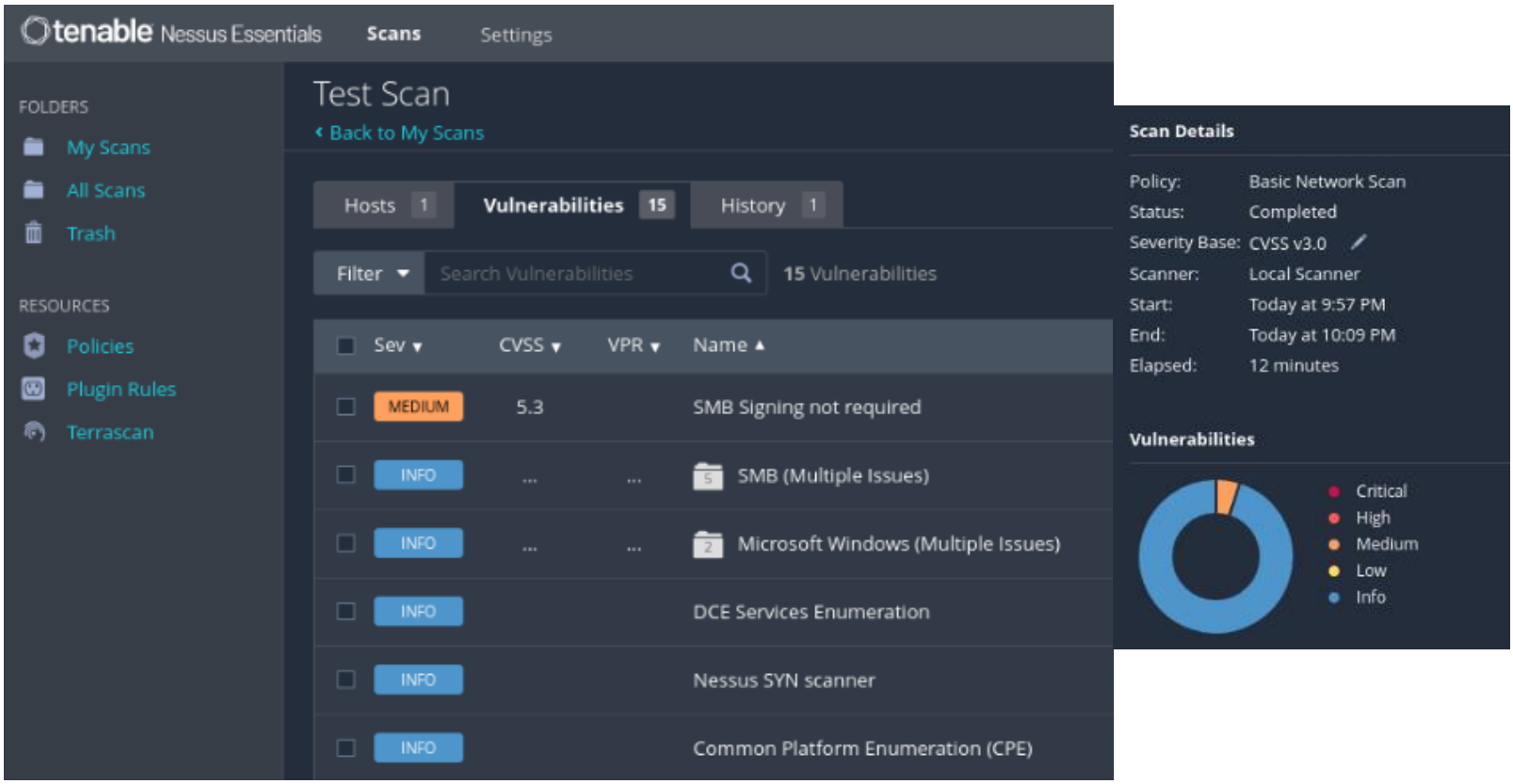
- **My Scans** – Any scans that have been conducted by the currently signed-in user. This includes completed, scheduled, pending, and failed scans.
- **All Scans** – Any scans that have been conducted by any users within an organization. This includes completed, scheduled, pending, and failed scans.
- **Trash** – Once you've got a scan template, you can send it to the Trash, so that it is no longer in the "My Scans" or "All Scans" tabs.
- **Policies** – Scans are conducted using a target and a policy, which is a list of settings and plugins that you use. Different plugins will identify and test different things (scan templates).
- **Plugin Rules** – Plugins are the part of Nessus that actually conduct the scanning and enumeration. Using different ones will provide different results, so this is where you can fine tune the scan to look for specific security issues.
- **Terrascan** – Open-source static code analyzer for infrastructure as a code (IaC) developed by Accurics and now owned by Tenable primarily used for scanning IaC files before deployment.



Nessus Test Scan:



10.0.2.4 → Metasploitable 2 VM

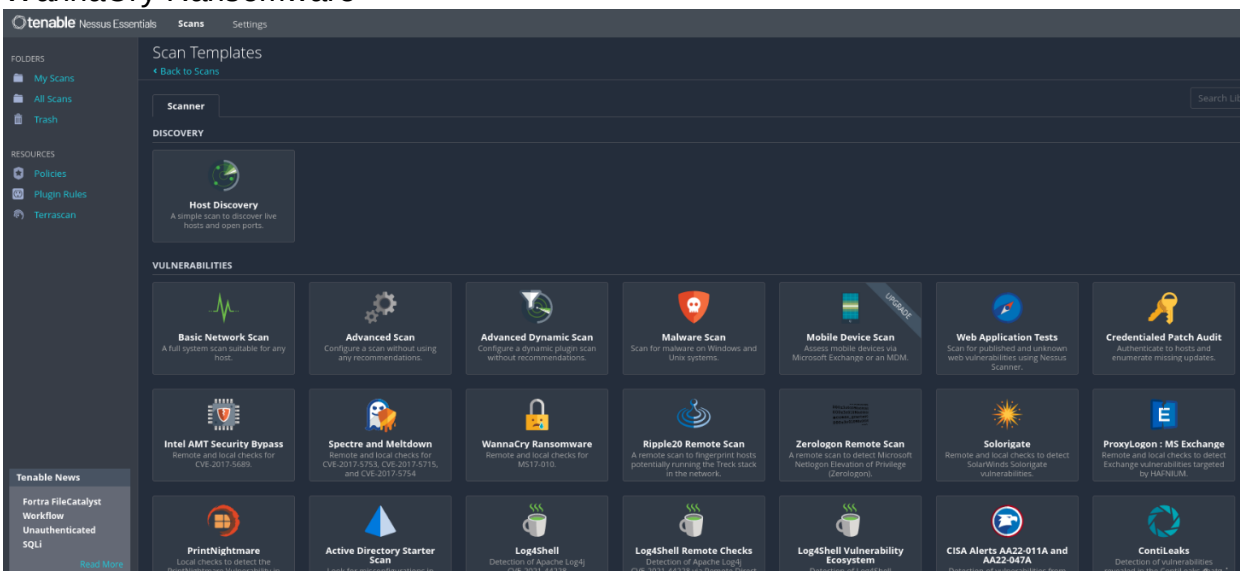


1. **Which Company created Nessus?**

Tenable

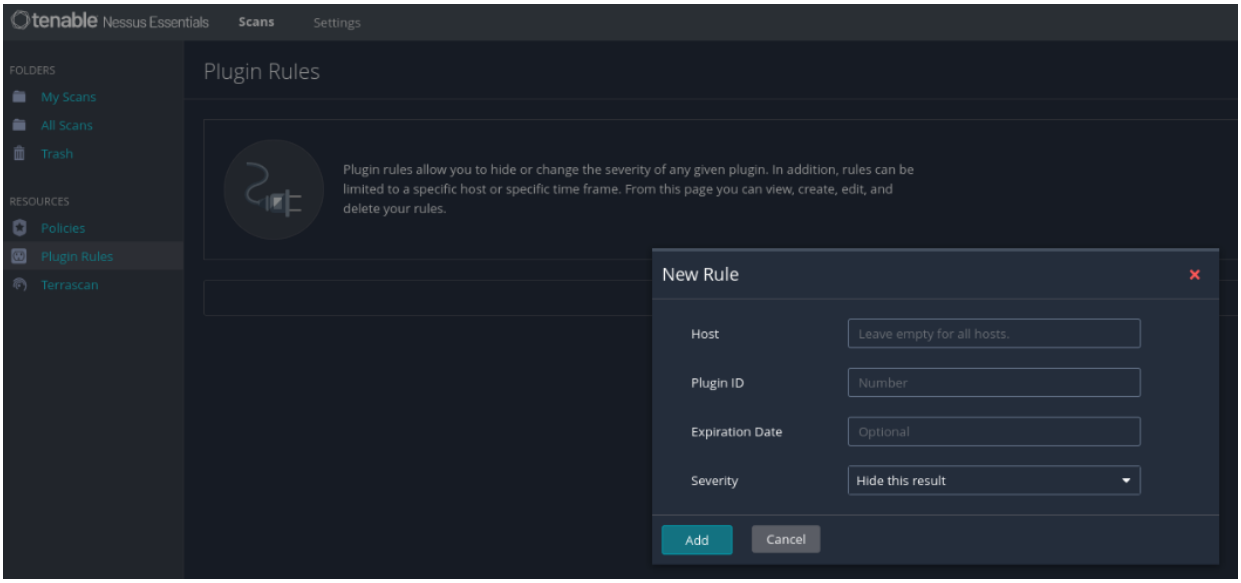
2. **Under Scan Templates in Nessus, there is a scan for what type of Ransomware?**

WannaCry Ransomware

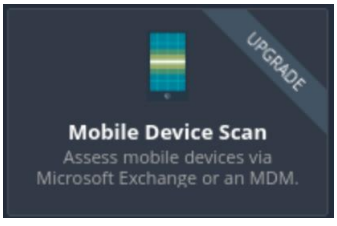


3. **When creating a new Plugin Rule, what 4 fields do you need to enter?**

Host, Plugin ID, Expiration date, and Severity.



4. **Is there a scan template specifically designed for mobile devices?**

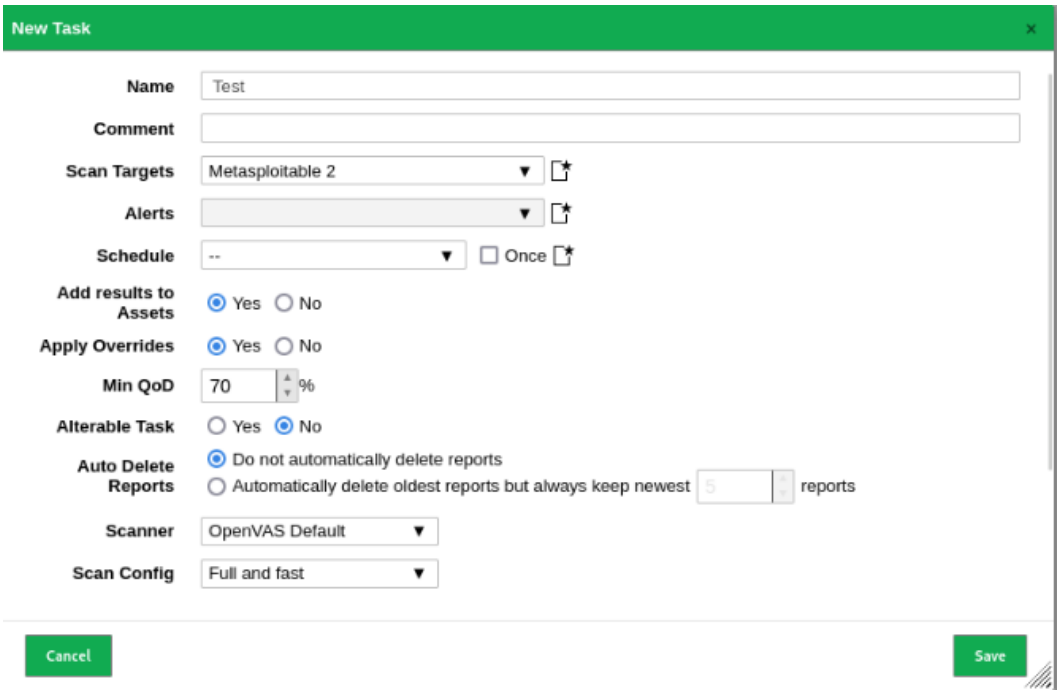


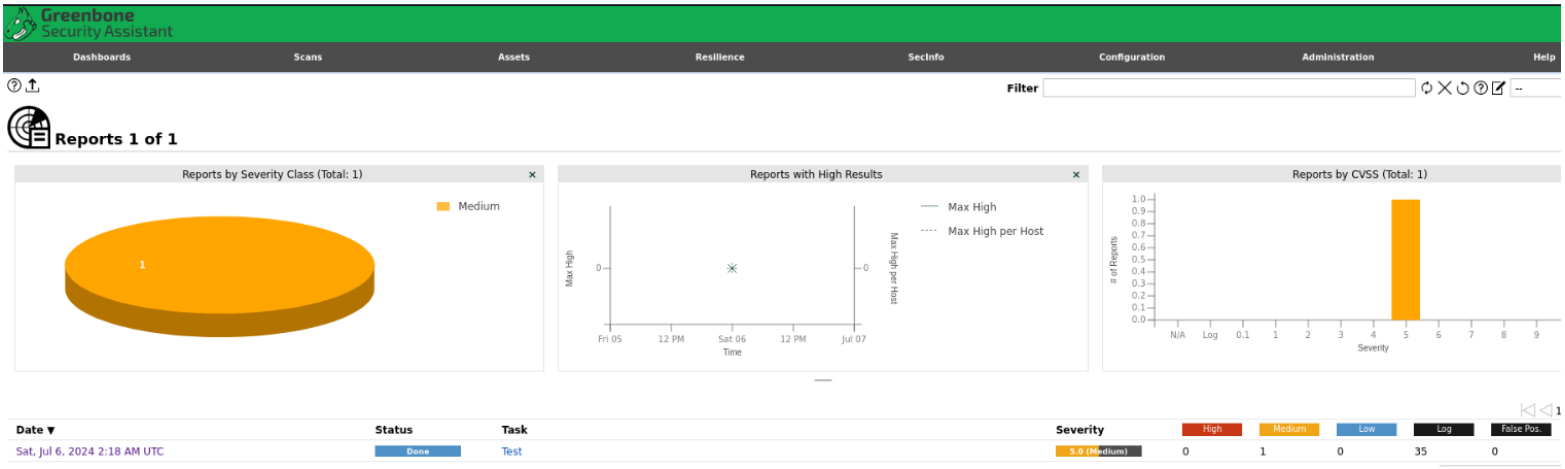
True

6.22 - OpenVAS

OpenVAS (Open Vulnerability Assessment System) = Open-source vulnerability scanner maintained by Greenbone.

OpenVAS Test Scan:





Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	10.0.2.4		135/tcp
Services	0.0 (Log)	80 %	10.0.2.4		1042/tcp
SSL/TLS: Collect and Report Certificate Details	0.0 (Log)	98 %	10.0.2.4		1043/tcp
SMB/CIFS Server Detection	0.0 (Log)	80 %	10.0.2.4		445/tcp
Service Detection with 'HELP' Request'	0.0 (Log)	80 %	10.0.2.4		2869/tcp
SSL/TLS: Version Detection	0.0 (Log)	80 %	10.0.2.4		1043/tcp
DCE/RPC and MSRPC Services Enumeration	0.0 (Log)	80 %	10.0.2.4		135/tcp
SSL/TLS: Hostname discovery from server certificate	0.0 (Log)	98 %	10.0.2.4		general/tcp
OS Detection Consolidation and Reporting	0.0 (Log)	80 %	10.0.2.4		general/tcp
Services	0.0 (Log)	80 %	10.0.2.4		1043/tcp

6.23 - WPScan

WPScan = Popular open-source vulnerability scanner specifically designed for WordPress websites.

- Identify security vulnerabilities in the many features that WordPress allows (plugins, themes, and users).

WordPress = Popular open-source content management system used for creating websites and blogs.

- **Plugins** = Pieces of software that can be added to a website to provide additional functionality.
- **Themes** = Combination of templates and stylesheets that change how a website looks.
- **Users** = WordPress allows for user registration so that members of your website can access specific areas.

WPScan Test (Done in owned domain):

```
[+] WordPress theme in use: salient
 | Location: https://infanciasegura.cl/wp-content/themes/salient/
 | Last Updated: 2024-06-26T03:44:34.000Z
 | Readme: https://infanciasegura.cl/wp-content/themes/salient/readme.txt
 | [!] The version is out of date, the latest version is 16.3.0
 | Style URL: https://infanciasegura.cl/wp-content/themes/salient/style.css
 | Style Name: Salient
 | Style URI: https://themeforest.net/item/salient-responsive-multipurpose-theme/4363266
 | Description: An Ultra Responsive Multi-Purpose Theme....
 | Author: ThemeNectar
 | Author URI: https://themeforest.net/user/themenectar
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 16.2.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://infanciasegura.cl/wp-content/themes/salient/style.css, Match: 'Version:    16.2.2'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
```

```
[i] Plugin(s) Identified:
```

```
[+] contact-form-7
 | Location: https://infanciasegura.cl/wp-content/plugins/contact-form-7/
 | Last Updated: 2024-06-17T08:11:00.000Z
 | [!] The version is out of date, the latest version is 5.9.6
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 5.9.5 (90% confidence)
 | Found By: Query Parameter (Passive Detection)
 |  - https://infanciasegura.cl/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.9.5
 | Confirmed By: Readme - Stable Tag (Aggressive Detection)
 |  - https://infanciasegura.cl/wp-content/plugins/contact-form-7/readme.txt

[+] js_composer
 | Location: https://infanciasegura.cl/wp-content/plugins/js_composer/
 | Last Updated: 2024-06-19T22:58:58.000Z
 | [!] The version is out of date, the latest version is 7.7.2
 |
 | Found By: Body Tag (Passive Detection)
 |
 | Version: 7.6 (60% confidence)
 | Found By: Body Tag (Passive Detection)
 |  - https://infanciasegura.cl/, Match: 'js-comp-ver-7.6'

[+] js_composer_salient
 | Location: https://infanciasegura.cl/wp-content/plugins/js_composer_salient/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | The version could not be determined.
```

```
[+] salient-core
 | Location: https://infanciasegura.cl/wp-content/plugins/salient-core/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | The version could not be determined.

[+] salient-portfolio
 | Location: https://infanciasegura.cl/wp-content/plugins/salient-portfolio/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | The version could not be determined.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:05 <==========================================> (137 / 137) 100.00% Time: 00:00:05

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jul  5 23:21:19 2024
[+] Requests Done: 192
[+] Cached Requests: 6
[+] Data Sent: 50.479 KB
[+] Data Received: 342.497 KB
[+] Memory used: 270.809 MB
[+] Elapsed time: 00:00:20
```

For this activity, you'll need to analyze the output of our scan against securityred.team (scan output is provided).

1. **What version of PHP is running?**

PHP Version → 7.2.17

```
[+] http://securityred.team/
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Powered-By: PHP/7.2.17
 |  - X-Mod-Pagespeed: 1.13.35.2-0
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

2. **What is the predicted version of the WordPress theme "mesmerize-pro"?**

Mesmerize-pro Version → 1.6.109

```
[+] WordPress theme in use: mesmerize-pro
 | Location: http://securityred.team/wp-content/themes/mesmerize-pro/
 | Readme: http://securityred.team/wp-content/themes/mesmerize-pro/readme.txt
 | Style URL: http://securityred.team/wp-content/themes/mesmerize-pro/style.css
 | Style Name: Mesmerize PRO
 | Style URI: https://extendthemes.com/go/mesmerize-home/
 | Description: Mesmerize is an incredibly flexible, multipurpose WordPress theme that can help you
 | Author: Horea Radu
 | Author URI: https://extendthemes.com/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.6.109 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://securityred.team/wp-content/themes/mesmerize-pro/style.css, Match: 'Version: 1.6.109'
```

3. **What username were discovered during the scan?**

Users identified → blackshard, user, bob, and spellcaster198.

```
[i] User(s) Identified:

[+] blackshard
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] user
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] bob
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] spellcaster198
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

4. **How did WPScan find the WordPress version 5.3.2?**

WordPress Version found by → Rss Generator (passive detection)

```
[+] WordPress version 5.3.2 identified (Latest, released on 2019-12-18).
 | Found By: Rss Generator (Passive Detection)
 |  - http://securityred.team/feed/, <generator>https://wordpress.org/?v=5.3.2</generator>
 |  - http://securityred.team/comments/feed/, <generator>https://wordpress.org/?v=5.3.2</generator>
```

Vulnerability Management Challenge

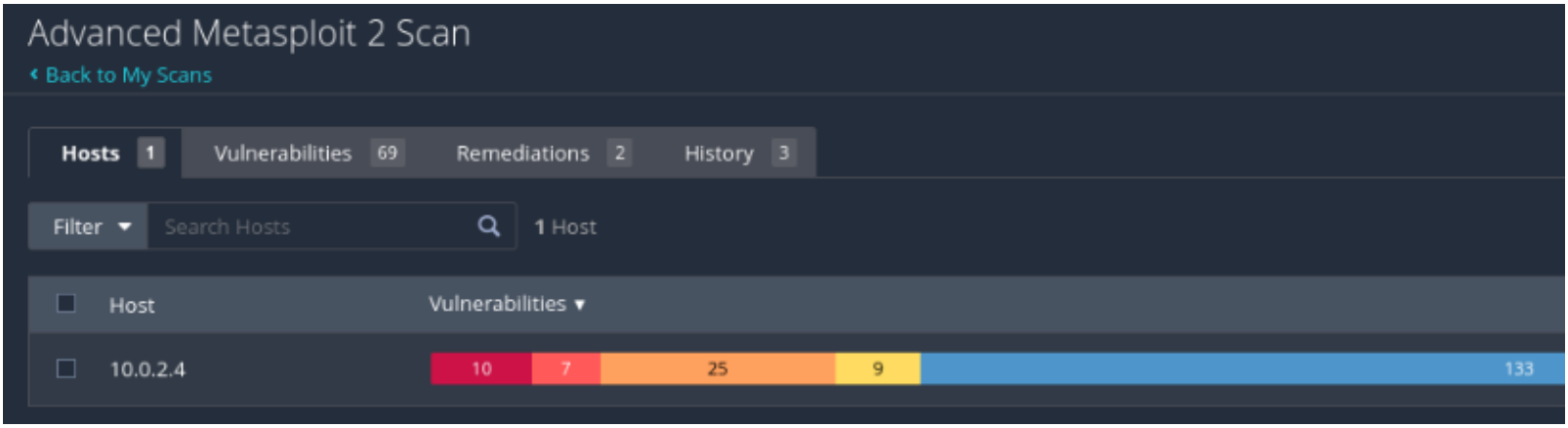
6.31 – Introduction to Vulnerability Management Challenge

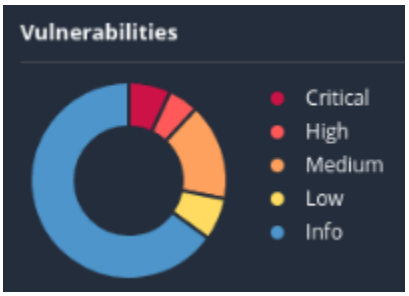
In this challenge, you will need to complete two objectives:

- Conduct a vulnerability scan using Nessus
- Analyze the results to determine critical issues, and suggest appropriate remediation steps

You are looking to move into a Vulnerability Analyst position within the security team, but first you have to prove your skills. You have been asked to conduct a vulnerability assessment of the intentionally vulnerable system, Metasploitable 2. You are required to work individually to conduct a scan of the system using Nessus (preferably within Kali Linux), you will host both systems yourself in virtual machines. You have been given a report template, which you must fill out completely and submit to be considered for the new role.

- Use the color-coding Nessus offers as well as CVSS scores to see the different severity ratings of each security flaw identified. By clicking on a vulnerability, Nessus will provide you with remediation steps – take note of these, as you'll need to include them in your report.
- DO NOT copy and paste these – rewrite them in your own words, and make it simple and easy to read.



Name of Individual Conducting Scanning:	Tomás Villaseca C.
Nessus Scanner IP (IP of Kali VM):	10.0.2.15
Date & Time Scan Started:	July 6 at 2:29 AM, 2024
Date & Time Scan Finished:	July 6 at 2:37 AM, 2024
Security Issues Identified: 	Multiple security vulnerabilities identified, including: • 10 critical vulnerabilities. • 7 high-risk vulnerabilities. • 25 medium-risk vulnerabilities. • 9 low-risk vulnerabilities. • 133 information findings

Instructions

1. Please refer to the Course Challenge Brief for instructions on what you are being asked to do.
2. Answer all questions mentioned below.

Overview

Vulnerability scanning was done against a Metasploit 2 VM using the "Advanced Scan" scan template.

The scan results indicate that this system is highly vulnerable and at significant risk. A total of 182 findings were identified, distributed across various severity levels:

- 10 Critical vulnerabilities
- 7 High-risk vulnerabilities
- 25 Medium-risk vulnerabilities
- 7 Low-risk vulnerabilities
- 133 Informational findings

The presence of 10 critical and 7 high-risk vulnerabilities suggests that the system has severe security weaknesses that could be readily exploited by attackers. These likely include outdated software versions, misconfigurations, and potentially exposed sensitive services. The substantial number of medium-risk vulnerabilities further compounds the system's overall vulnerability.

Given the nature of Metasploitable 2 as an intentionally vulnerable system for testing purposes, these results are not unexpected. However, in a real-world scenario, a system with this vulnerability profile would be considered extremely high-risk and would require immediate attention and remediation.

The large number of informational findings (133) suggests that there are many potential areas for system hardening and security improvement, even beyond addressing the more severe vulnerabilities.

In conclusion, this system exhibits a very high level of vulnerability and would be an easy target for various types of cyber-attacks if exposed to a hostile network environment.

Top 5 Most Serious Security Issues (In priority order - most important first):

1. **Apache Tomcat AJP Connector Request Injection (Ghostcat) (Critical – CVSS 9.8 – VPR 9.0)**

This vulnerability, also known as Ghostcat, affects Apache Tomcat servers. It allows an attacker to read or include files outside of the web root directory through the AJP connector.

If exploited, an attacker could:

- Read sensitive configuration files
- Obtain source code of web applications
- In some cases, execute arbitrary code on the server

The high VPR score (9.0) indicates this is actively exploited and poses an immediate threat.

2. **NFS Exported Share Information Disclosure (Critical – CVSS 10.0 – VPR 5.9).**

This vulnerability involves Network File System (NFS) shares that are improperly configured, allowing unauthorized access to sensitive information.

If exploited, an attacker could:

- Access and read sensitive files shared over the network
- Potentially modify or delete critical data
- Use the information gathered to plan further attacks

The high CVSS score (10.0) reflects its severity, while the VPR (5.9) suggests it's a significant but not necessarily the most actively exploited vulnerability.

3. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) (Critical – CVSS 10.0 – VPR 5.1)**

This vulnerability affects the random number generation in OpenSSL on Debian-based systems, potentially compromising the security of SSL/TLS connections.

If exploited, an attacker could:

- Predict cryptographic keys generated by the affected systems
- Decrypt encrypted communications
- Potentially impersonate secure websites or services

The high CVSS score (10.0) indicates its critical nature, while the VPR (5.1) suggests it's serious but may not be as actively exploited as some other vulnerabilities.

4. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (Critical – CVSS 10.0 – VPR 5.1)**

This is related to the previous vulnerability but specifically affecting OpenSSH. It stems from the same weak random number generation issue in Debian systems.

If exploited, an attacker could:

- Predict SSH keys generated on affected systems
- Potentially gain unauthorized access to SSH-secured systems
- Intercept or manipulate SSH-encrypted communications

The implications are similar to the SSL version, with the same critical CVSS score (10.0) and VPR (5.1).

5. **VNC Server ‘password’ Password (Critical – CVSS 10.0 – VPR N/A)**

This vulnerability indicates that the VNC (Virtual Network Computing) server is using a default or easily guessable password, specifically 'password'.

If exploited, an attacker could:

- Gain unauthorized remote access to the system
- View and control the desktop environment
- Potentially access sensitive information or install malware

The CVSS score of 10.0 reflects the critical nature of this issue.

Top 5 - Remediations (In priority order - most important first):

1. Update Apache Tomcat to the latest secure version and disable the AJP connector if not required. If AJP is necessary, implement strict access controls and configure a strong secret for the AJP connector to mitigate the Ghostcat vulnerability.

2. Review and reconfigure NFS share settings. Implement strict access controls, use NFSv4 with Kerberos authentication if possible, and ensure that only necessary directories are shared. Regularly audit NFS exports for any unintended information disclosure.

3. Update OpenSSL packages on all Debian-based systems to the latest patched versions. Regenerate all SSL/TLS keys and certificates that were created on potentially affected systems. Implement a process for regular security updates of cryptographic libraries.

4. Similar to the previous item, focus on OpenSSH. Update OpenSSH packages, regenerate all SSH keys on affected systems, and revoke old keys. Implement key rotation policies and consider using alternative sources of entropy for key generation.

5. Change the VNC server password immediately to a strong, unique password. Implement two-factor authentication for VNC access if possible. Consider using VPN or SSH tunneling for VNC connections, and restrict VNC access to specific IP addresses or networks.