Network Security Skills Assessment

Introduction

You have been hired as a security analyst. You were tasked to determine any malicious activity associated with a malware attack.

You will have access to the internet to learn more about the events. You can use websites, such as VirusTotal, to upload and verify threat existence.

The tasks below are designed to provide some guidance through the analysis process.

You will practice and be assessed on the following skills:

- Evaluate event alerts using Squil.
- Use Google search as a tool to obtain intelligence on a potential exploit.
- Use VirusTotal to upload and verify threat existence.

Name: ISMAIL HOSSAIN PRANTO

ID:19-41088-2

SEC: A

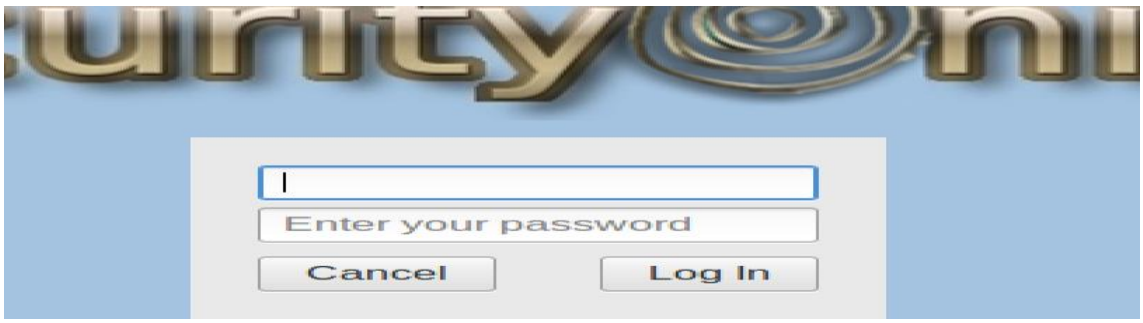
Instructions

Part 1: Gather the Basic Information

In this part, you will review the alerts listed in Security Onion VM and gather basic information for the interested time frame.

Step 1: Verify the status of services

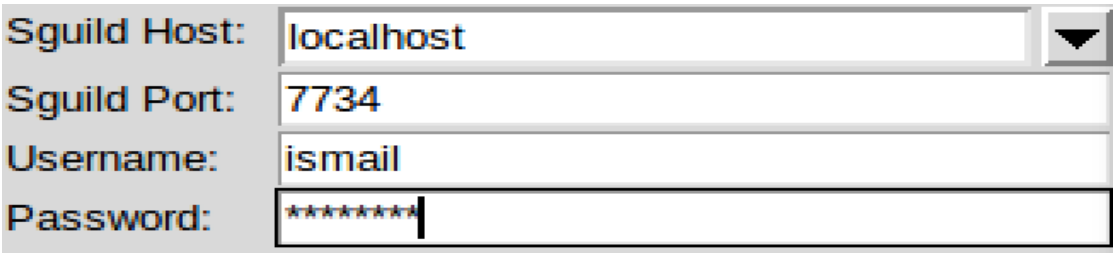
a. Log into Security Onion VM.



b. Open a terminal window. Enter the **sudo so-status** command to verify that all the services are ready.

```
ismail@ismail-VirtualBox:~$ sudo so-status
[sudo] password for ismail:
Status: securityonion
  * sguil server                                                    [  OK  ]
Status: HIDS
  * ossec_agent (sguil)                                             [  OK  ]
Status: Zeek
Name          Type        Host           Status    Pid    Started
zeek          standalone  localhost      running   2732   19 Aug 15:46:27
Status: ismail-virtualbox-enp0s3
  * netsniff-ng (full packet data)                                  [  OK  ]
  * pcap_agent (sguil)                                              [  OK  ]
  * snort_agent-1 (sguil)                                           [  OK  ]
  * snort-1 (alert data)                                            [  OK  ]
  * barnyard2-1 (spooler, unified2 format)                          [  OK  ]
Status: Elastic stack
  * so-elasticsearch                                                [  OK  ]
  * so-logstash
    Logstash API/stats not yet available...still initializing.      [ WARN ]
  * so-kibana                                                       [  OK  ]
  * so-freqserver                                                   [  OK  ]
  * so-curator                                                      [  OK  ]
```

c. When the nsm service is ready, log into Sguil.



d. Download the zip file from infected.zip and replay the malware packet capture. Password for the zip file: **cyberops**

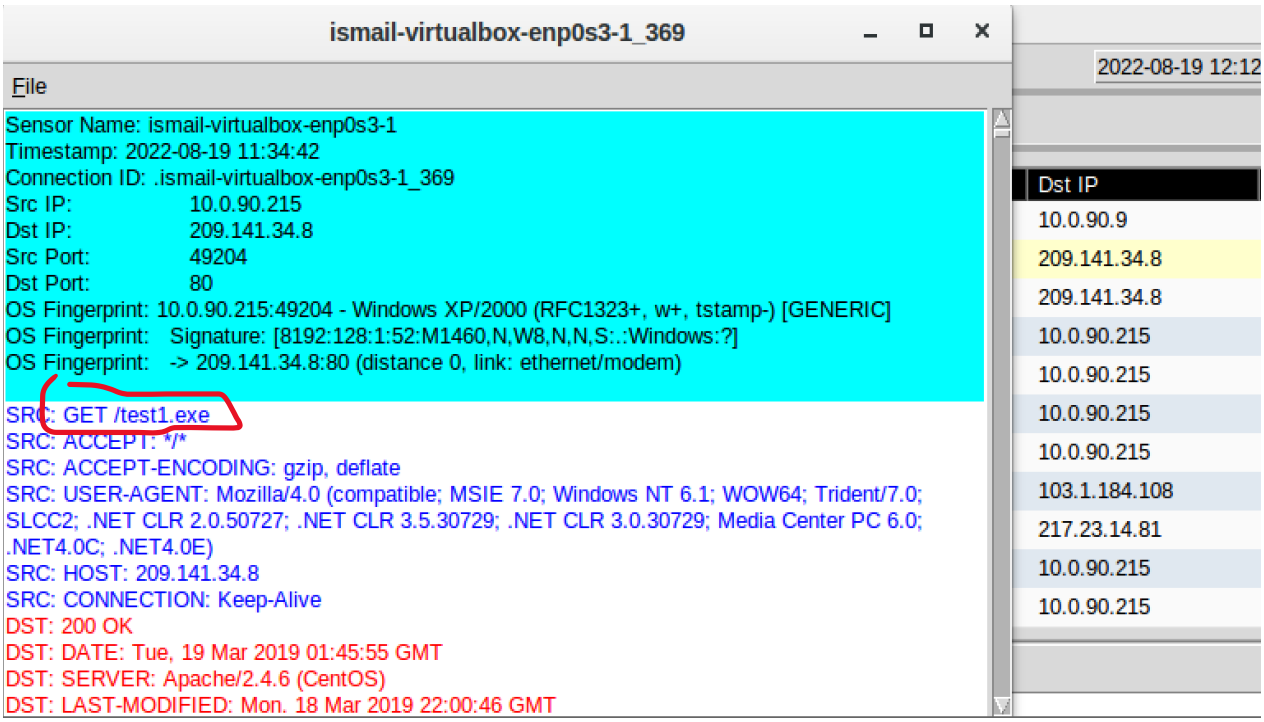
```
ismail@ismail-VirtualBox:~/Downloads$ sudo tcpreplay -i enp0s3 -M 10 infected.pcap
sending out enp0s3
processing file: infected.pcap
Actual: 13186 packets (7563934 bytes) sent in 11.49 seconds.            Rated: 6583
147.61 pps
Statistics for network device: enp0s3
        Attempted packets:         13186
        Successful packets:        13186
        Failed packets:            0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

Step 2: Gather basic information.

a. What is the name of the trojan? Identify the time frame of the attack, including the date and approximate time.

Ans: The name of the trojan is “**Ramcos RAT”**

At start the allert and then the allert open it by Bro. Findout the infected file by “Bro”

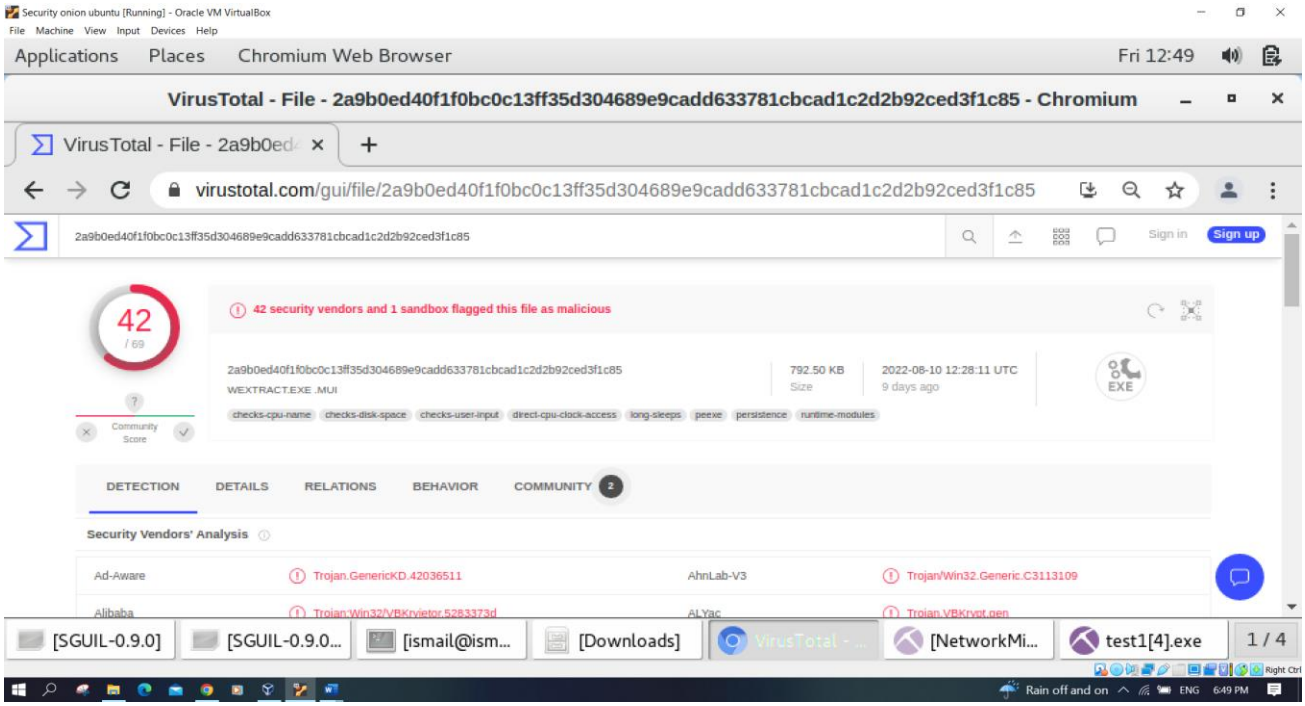

ismail-virtualbox-enp0s3-1_369
File
Sensor Name: ismail-virtualbox-enp0s3-1
Timestamp: 2022-08-19 11:34:42
Connection ID: .ismail-virtualbox-enp0s3-1_369
Src IP: 10.0.90.215
Dst IP: 209.141.34.8
Src Port: 49204
Dst Port: 80
OS Fingerprint: 10.0.90.215:49204 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint: -> 209.141.34.8:80 (distance 0, link: ethernet/modem)
SRC: GET /test1.exe
SRC: ACCEPT: */*
SRC: ACCEPT-ENCODING: gzip, deflate
SRC: USER-AGENT: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
SRC: HOST: 209.141.34.8
SRC: CONNECTION: Keep-Alive
DST: 200 OK
DST: DATE: Tue, 19 Mar 2019 01:45:55 GMT
DST: SERVER: Apache/2.4.6 (CentOS)
DST: LAST-MODIFIED: Mon, 18 Mar 2019 22:00:46 GMT
2022-08-19 12:12
Dst IP
10.0.90.9
209.141.34.8
209.141.34.8
10.0.90.215
10.0.90.215
10.0.90.215
10.0.90.215
103.1.184.108
217.23.14.81
10.0.90.215
10.0.90.215


Names
test1.exe
Wextract
WEXTRACT.EXE.MUI
test1.bin
myfile.exe
2019-03-19-test1.exe-from-209.141.34.8.exe

ST	...T	...	Alert ID	Date/Time △
RT	1	...	3.368	2022-08-19 11:34:42
RT	2	...	3.369	2022-08-19 11:34:42
RT	1	...	3.370	2022-08-19 11:34:42
RT	2	...	3.371	2022-08-19 11:34:42
RT	12	...	3.373	2022-08-19 11:34:42
RT	12	...	3.385	2022-08-19 11:34:42
RT	12	...	3.397	2022-08-19 11:34:42
RT	1	...	3.409	2022-08-19 11:34:43
RT	1	...	3.411	2022-08-19 11:34:43
RT	2	...	3.412	2022-08-19 11:34:43
RT	12	...	3.414	2022-08-19 11:34:43
RT	12	...	3.426	2022-08-19 11:34:43
RT	12	...	3.438	2022-08-19 11:34:43
RT	12	...	3.450	2022-08-19 11:34:43
RT	12	...	3.462	2022-08-19 11:34:43
RT	16	...	3.474	2022-08-19 11:34:44
RT	13	...	3.482	2022-08-19 11:34:46
RT	3	...	3.503	2022-08-19 11:34:53

List the alerts noted during this time frame associated with the trojan.

Ans:



b. List the internal IP addresses and external IP addresses involve

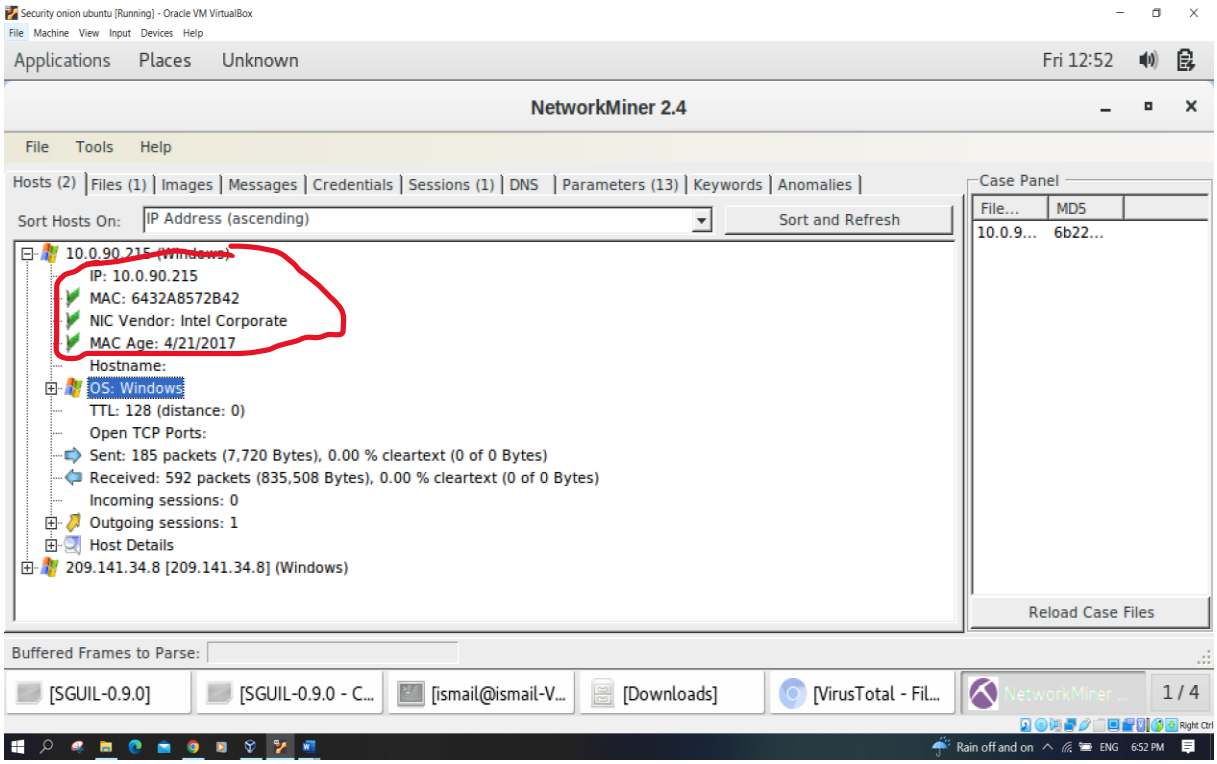
10.0.90.215	52609	10.0.90.9	53	17
10.0.90.215	49204	209.141.34.8	80	6
10.0.90.215	49204	209.141.34.8	80	6
209.141.34.8	80	10.0.90.215	49204	6
209.141.34.8	80	10.0.90.215	49204	6

Part 2: Learn about the Exploit

In this part, you will learn more about the exploit.

Step 1: Infected host

Based on the alerts, what is the IP and MAC addresses of the infected computer? Based on the MAC address, what is the vendor of the NIC chipset? (**Hint**: NetworkMiner or internet search)



a. Based on the alerts, when (date and time in UTC) and how was the PC infected? (Hint: Enter the command date in the terminal to determine the time zone for the displayed time

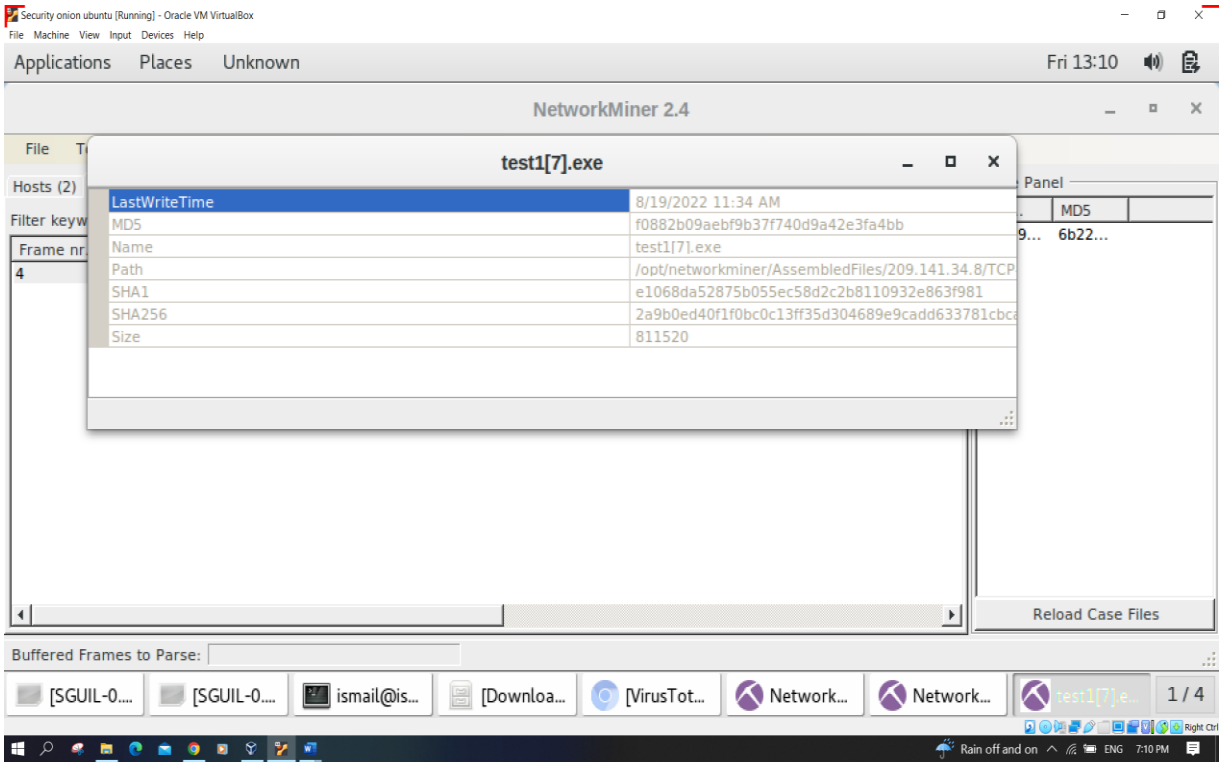
Ans:

```
ismail@ismail-VirtualBox:~/Downloads$ date
Fri Aug 19 12:57:05 UTC 2022
```

1. The client or user has visited a compromised site with an outdated and vulnerable flash version which allows remote code execution
2. The client downloaded a malicious executable file
3. After the user/client unzipped it
4. The executable file encrypted all the files of the user
5. And then the PC has infected

b. How did the malware infect the PC? Use an internet search as necessary.

Ans:



The client or user was visited the malicious site with the outdated flash version software. After the downloadede the infected file. This malware is an executable software which connects with the different public IP. It was downloaded but updating the DNS from External net.

Step 2: Examine the exploit.

a. **Based on the alerts associated with HTTP GET request, what files were downloaded? List the malicious domains observed and the files downloaded**

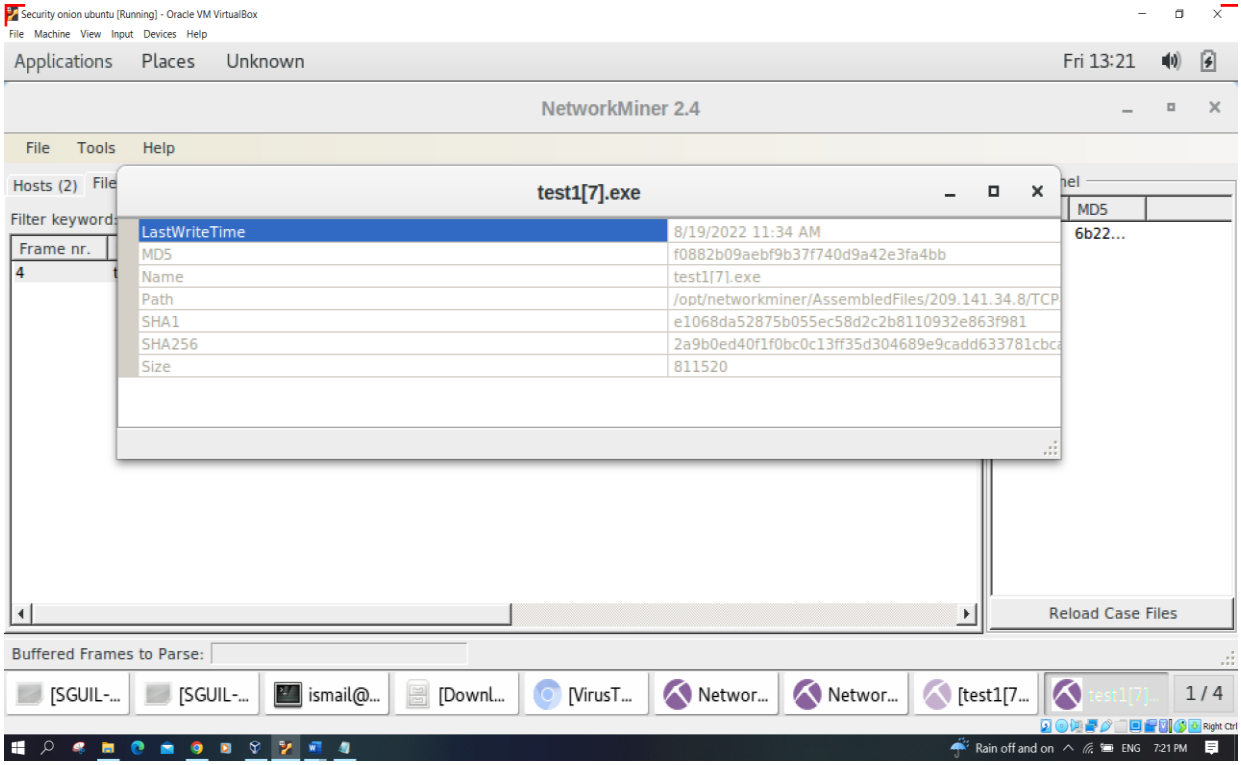
Ans:

Src IP	SPort	Dst IP	DPort	Pr
10.0.90.215	52609	10.0.90.9	53	17
209.141.34.8	80	10.0.90.215	49204	6
217.23.14.81	80	10.0.90.215	49206	6
10.0.90.215	49204	209.141.34.8	80	6
217.23.14.81	80	10.0.90.215	49206	6

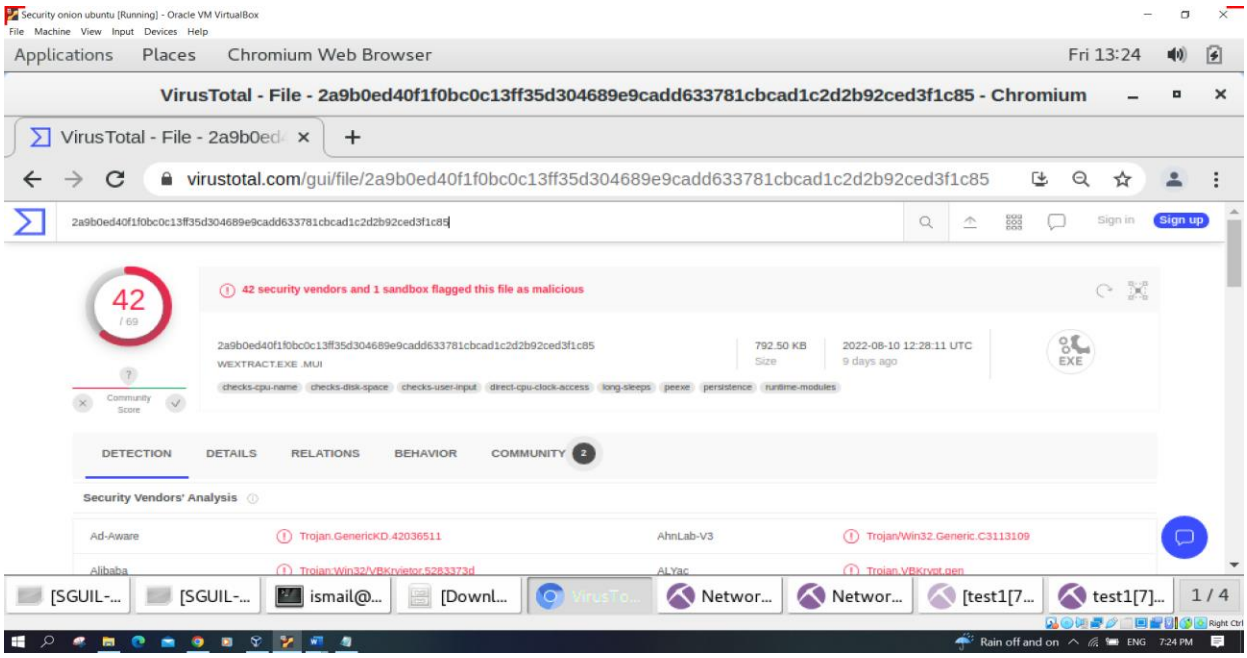
In these cases, all destination IP's are public IP. And they are using port 6 , it means they are using TCP.

b. Use any available tools in Security Onion VM, determine and record the SHA256 hash for the downloaded files that probably infected the computer?

Ans: We are using NetworkMiner to record the hash.

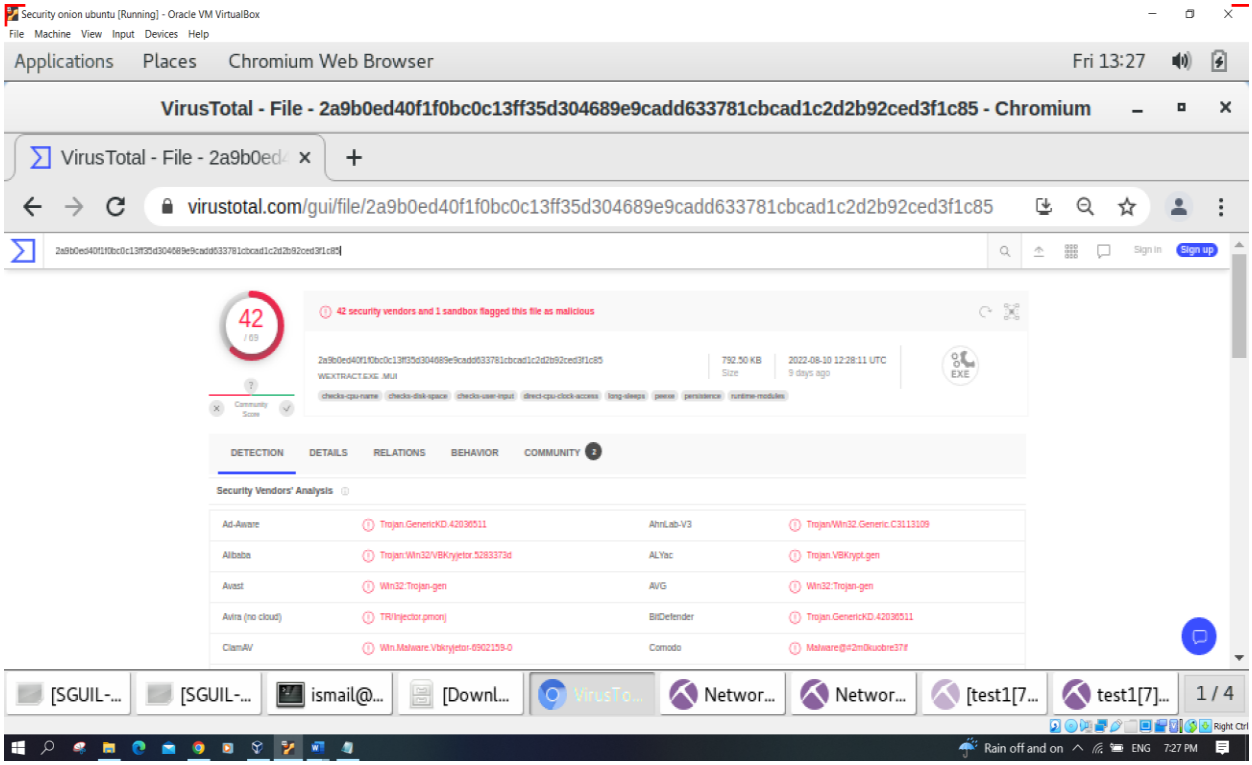


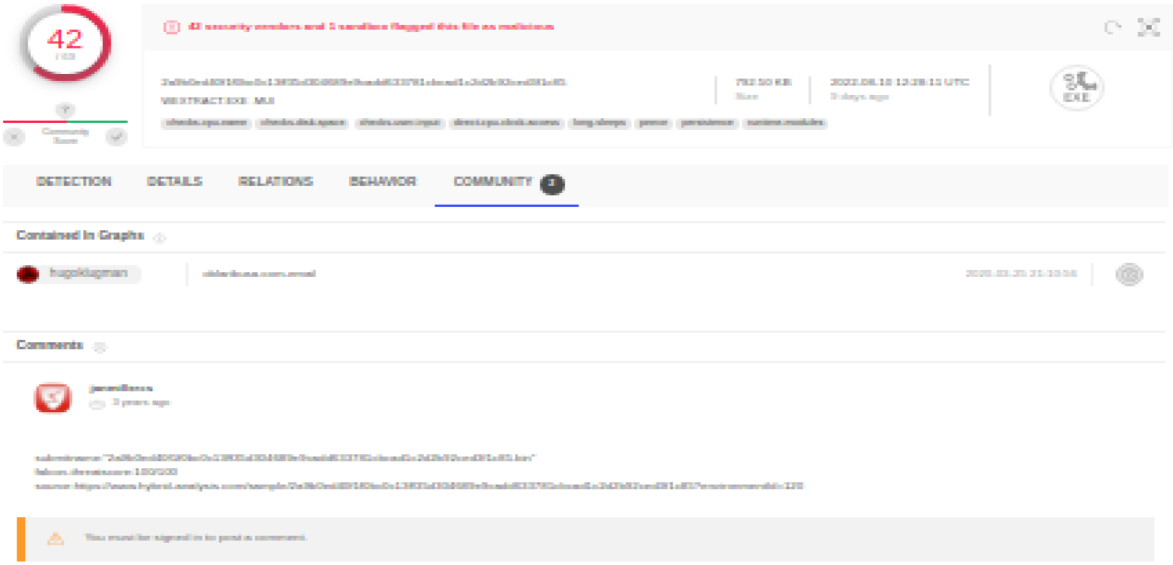
To determining the record with SHA256 hash for the downloaded file is it infected or not



c. Navigate to www.virustotal.com input the SHA256 hash to determine if these were detected as malicious files. Record your findings, such as file type and size, other names, and target machine. You can also include any information that is provided by the community posted in VirusTotal.

Ans:





d. Examine other alerts associated with the infected host during this timeframe and record your findings:

Ans:

The other alerts are same as **test1.exe**

Wextract

WEXTRACT.EXE.MUI

test1.bin

myfile.exe

2019-03-19-test1.exe-from-209.141.34.8.exe

The correlated event attack is that. Next will be the same way.

ST	...T	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	D...	Event Message
RT	1	ismail-...	3.369	2022-08-19 11:34:42	10.0.90.215	49204	209.141.34.8	80	ET INFO Executable Download from dotted-qua...
RT	1	ismail-...	3.410	2022-08-19 11:34:43	10.0.90.215	49206	217.23.14.81	80	ET INFO Executable Download from dotted-qua...

Secondary Attack:

Source IP:

31.22.4.176

203.45.1.75

115.112.43.81

RT	16	3.474	2022-08-19 11:34:44	31.22.4.176	3389	10.0.90.215	49213	6	ET TROJAN ABUS...
RT	13	3.482	2022-08-19 11:34:46	203.45.1.75	443	10.0.90.215	49218	6	ET TROJAN ABUS...
RT	3	3.503	2022-08-19 11:34:53	115.112.43.81	443	10.0.90.215	49289	6	ET TROJAN ABUS...

RT	16	3.474	2022-08-19 11:34:44	10.0...	.	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
RT	13	3.482	2022-08-19 11:34:46	10.0...	.	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
RT	3	3.503	2022-08-19 11:34:53	10.0...	.	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)

Step 3: Report Your Findings

Summarizes your findings based on the information you have gathered from the previous parts, summarize your findings.

Ans:

1. In first step the client update DNS from External Net with a outdated and vulnerable falsh version
2. A malicious flash file was sent from the compromised site to the browser of the victim
3. The malware was downloaded by and updating DNS from External Net
4. The downloaded file that was actually malicious files
5. The client was install it on his pc and then he has been affected by that file.

----------THANK YOU----------