



DIGITAL FORENSICS - INVESTIGATION OF A PCAP

Cybersecurity DFIR



**2025
MICHAEL MUSOKE**

Contents

PCAP Investigation using Security Onion2

Objectives.....2

Introduction2

Investigation in Security Onion2

Conclusion.....6

Lessons Learned7

PCAP Investigation using Security Onion

Objectives

1. Import .pcap file into Security Onion
2. Investigate .pcap file
3. Provide an analysis of what probably occurred

Introduction

Security Onion is a free open-source Linux distribution for network security monitoring, intrusion detection, and log management. It integrated powerful like Suricata, Zeek, Wazuh and the ELK stack to capture and analyse network traffic.

In the security industry, Security Onion plays a critical role by providing SOCs, incident responders and threat hunters with a comprehensive platform for real-time monitoring and forensic analysis. Its ability to correlate data from multiple sources enables organisations to quickly identify, investigate and mitigate potential threats, thereby enhancing their overall security posture.

In this demonstration, a .pcap will be ingested into security onion and an investigation will be done to determine the nature of the captured network traffic.

Investigation in Security Onion

Log on to the security onion console. Create a directory into which the pcap will be downloaded using mkdir command e.g. **mkdir Malware**

```
[mike@sec-onion ~]$ ll
total 4
drwxr-xr-x. 10 mike mike 4096 Feb 15 17:04 SecurityOnion
[mike@sec-onion ~]$ mkdir Malware
[mike@sec-onion ~]$
[mike@sec-onion ~]$
[mike@sec-onion ~]$ ll
total 4
drwxr-xr-x. 2 mike mike 6 Feb 16 09:24 Malware
drwxr-xr-x. 10 mike mike 4096 Feb 15 17:04 SecurityOnion
[mike@sec-onion ~]$ cd Malware/
[mike@sec-onion Malware]$ ll
total 0
[mike@sec-onion Malware]$ wget https://www.malware-traffic-analysis.net/2022/01/07/2022-01-07-traffic-analysis-exercise.pcap.zip
--2025-02-16 09:29:16-- https://www.malware-traffic-analysis.net/2022/01/07/2022-01-07-traffic-analysis-exercise.pcap.zip
Resolving www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)... 199.201.110.204
Connecting to www.malware-traffic-analysis.net (www.malware-traffic-analysis.net)|199.201.110.204|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2641838 (2.5M) [application/zip]
Saving to: '2022-01-07-traffic-analysis-exercise.pcap.zip'

2022-01-07-traffic-analy 100%[=====>] 2.52M 997KB/s in 2.6s

2025-02-16 09:29:20 (997 KB/s) - '2022-01-07-traffic-analysis-exercise.pcap.zip' saved [2641838/2641838]

[mike@sec-onion Malware]$ ll
total 2580
-rw-r--r--. 1 mike mike 2641838 May 9 2024 2022-01-07-traffic-analysis-exercise.pcap.zip
[mike@sec-onion Malware]$
```

Figure 1

use the command `wget` to download an infected pcap from the website as shown in figure 1
<https://www.malware-traffic-analysis.net/2022/01/07/2022-01-07-traffic-analysis-exercise.pcap.zip>

When the zipped pcap is downloaded use the `unzip` command to decompress the pcap. Visit the about page of Traffic analysis to obtain the password.

```
[mike@sec-onion Malware]$  
[mike@sec-onion Malware]$ unzip 2022-01-07-traffic-analysis-exercise.pcap.zip  
Archive: 2022-01-07-traffic-analysis-exercise.pcap.zip  
[2022-01-07-traffic-analysis-exercise.pcap.zip] 2022-01-07-traffic-analysis-exercise.pcap password:  
password incorrect--reenter:  
  inflating: 2022-01-07-traffic-analysis-exercise.pcap  
[mike@sec-onion Malware]$ ll  
total 7196  
-rw-r--r--. 1 mike mike 4722992 Jan  7 2022 2022-01-07-traffic-analysis-exercise.pcap  
-rw-r--r--. 1 mike mike 2641838 May  9 2024 2022-01-07-traffic-analysis-exercise.pcap.zip  
[mike@sec-onion Malware]$ _
```

Figure 2

Next is to import the pcap using the command `so-import-pcap <name of pcap>`

```
[mike@sec-onion Malware]$  
[mike@sec-onion Malware]$ sudo so-import-pcap 2022-01-07-traffic-analysis-exercise.pcap  
[sudo] password for mike:  
Processing Import: /home/mike/Malware/2022-01-07-traffic-analysis-exercise.pcap  
- verifying file  
- assigning unique identifier to import: e687298812366f48eab16e2676dd765a  
- analyzing traffic with Suricata  
- analyzing traffic with Zeek  
- found PCAP data spanning dates 1984-11-11 through 2022-01-07  
  
Import complete!  
  
Use the following hyperlink to view the imported data. Triple-click to quickly highlight the entire  
hyperlink and then copy it into a browser:  
https://172.20.10.4/#/dashboards?q=import.id:e687298812366f48eab16e2676dd765a%20%7C%20groupby%20event.module%20%7C%20groupby%20sankey%20event.module%20event.dataset%20%7C%20groupby%20event.dataset%20%7C%20groupby%20source.ip%20%7C%20groupby%20destination.ip%20%7C%20groupby%20destination.port%20%7C%20groupby%20network.protocol%20%7C%20groupby%20rule.name%20rule.category%20event.severity_label%20%7C%20groupby%20dns.query.name%20%7C%20groupby%20file.mime_type%20%7C%20groupby%20http.virtual_host%20http.uri%20%7C%20groupby%20notice.note%20notice.message%20notice.sub_message%20%7C%20groupby%20ssl.server_name%20%7C%20groupby%20source_geo.organization_name%20source_geo.country_name%20%7C%20groupby%20destination_geo.organization_name%20destination_geo.country_name&t=1984%2F11%2F11%2000%3A00%3A00%20AM%20-%202022%2F01%2F08%2000%3A00%3A00%20AM&z=UTC  
  
or, manually set the Time Range to be (in UTC):  
From: 1984-11-11 To: 2022-01-08  
  
Note: It can take 30 seconds or more for events to appear in Security Onion Console.  
[mike@sec-onion Malware]$ _
```

Figure 3

With the import complete log on the web console. To examine the pcap change time to a period the pcap was captured in this case 2022-01-07-2022-01-31

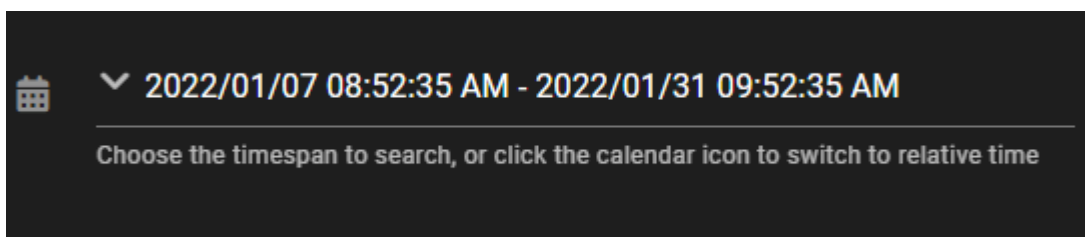


Figure 4

Take note of the query that was generated by changing the time. The wildcard * to select everything grouped by the different options

```

✓ * | groupby event.category | groupby -sankey event.category event.module | groupby event.module |
  groupby -sankey event.module event.dataset | groupby event.dataset | groupby observer.name |
  groupby host.name | groupby source.ip | groupby destination.ip | groupby destination.port
Specify a query in Onion Query Language (OQL)

```

Figure 5

Scrolling to the Event alerts by Suricata and Zeek at the time. Under event dataset Suricata and Zeek flagged some packets

Events					
			Fetch Limit 100		
	Timestamp	event.dataset	source.ip	source.port	destination.ip
>	2022-01-07 16:16:39.981 +00:00	suricata.alert	192.168.1.216	49763	192.168.1.2
>	2022-01-07 16:16:09.964 +00:00	suricata.alert	192.168.1.216	49761	192.168.1.2
>	2022-01-07 16:14:32.032 +00:00	zeek.dns	192.168.1.216	50116	192.168.1.2
>	2022-01-07 16:14:22.488 +00:00	zeek.pe			
>	2022-01-07 16:14:22.462 +00:00	zeek.software	192.168.1.216		
>	2022-01-07 16:14:22.343 +00:00	zeek.file	192.168.1.216	49748	184.50.62.43
>	2022-01-07 16:14:19.551 +00:00	zeek.ssl	192.168.1.216	49744	20.54.89.15
>	2022-01-07 16:14:18.247 +00:00	zeek.software	192.168.1.216		
>	2022-01-07 16:09:42.452 +00:00	zeek.file	192.168.1.216	49739	52.168.112.67
>	2022-01-07 16:07:35.790 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108

Figure 6

In the Alerts tab 9 counts Malware Vider are shown

	Count	rule.name	event.module	event.severity_label	rule.uuid
	9	ET MALWARE Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	suricata	high	2034813
	3	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response	suricata	medium	2021076
	2	GPL NETBIOS SMB IPC\$ unicode share access	suricata	low	2100538
	1	ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Chrome_Default.txt)	suricata	medium	2033886
	1	ET INFO PE EXE or DLL Windows file download HTTP	suricata	high	2018959

Figure 7

>	▲	2022-01-07 16:07:35.790 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108	80	ET MALWARE Vidar/Arkel/Megumin/Oski Stealer HTTP POST Pattern	A Ne
>	▲	2022-01-07 16:07:34.894 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108	80	ET MALWARE Vidar/Arkel/Megumin/Oski Stealer HTTP POST Pattern	A Ne
>	▲	2022-01-07 16:07:34.379 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108	80	ET MALWARE Vidar/Arkel/Megumin/Oski Stealer HTTP POST Pattern	A Ne
>	▲	2022-01-07 16:07:34.374 +00:00	zeek.pe						
>	▲	2022-01-07 16:07:34.079 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108	80	ET MALWARE Vidar/Arkel/Megumin/Oski Stealer HTTP POST Pattern	A Ne
>	▲	2022-01-07 16:07:33.909 +00:00	suricata.alert	192.168.1.216	49738	2.56.57.108	80	ET MALWARE Vidar/Arkel/Megumin/Oski Stealer HTTP POST Pattern	A Ne

Figure 8

The source IP address 2.56.57.108 could give some more information. Using OSINT tools to find out more about the source IP address.

Using AbuseIP.com, the source IP based in Singapore was reported several times. It was associated with multiple cases of misuse.

AbuseIPDB » 2.56.57.108

Check an IP Address, Domain Name, or Subnet
e.g. 2a01:b340:80:6ad1:7c8c:a5c3:5868:6b31,
microsoft.com, or 5.188.10.0/24

2.56.57.108

CHECK

2.56.57.108 was found in our database!
This IP was reported **7** times. Confidence of Abuse is **0%**: ?

0%

ISP

SingNet Pte Ltd

Usage Type

Fixed Line ISP


ASN

AS3758

Domain Name

singnet.com.sg

Country

 Singapore

City

Singapore

IP Info including ISP, Usage Type, and Location provided by [IPInfo](#). Updated biweekly.

Figure 9

Checking on Virus Total, 4 security vendors flagged the IP address.

4

/ 94

Community Score

1

4/94 security vendors flagged this IP address as malicious

2.56.57.108 (2.56.56.0/22)
AS 3758 (SingNet)

DETECTION DETAILS RELATIONS COMMUNITY 1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

CyRadar	ⓘ Malicious	Kaspersky	ⓘ Malware
SOCRadar	ⓘ Malware	Webroot	ⓘ Malicious

Figure 10

Expanding the event. Under network data decoded. Notice content Type jpeg

```
network.data.decoded HTTP/1.1 200 OK
Date: Fri, 07 Jan 2022 16:07:32 GMT
Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10
Last-Modified: Thu, 06 Jun 2019 04:01:52 GMT
ETag: "235d0-58a9fc6206c00"
Accept-Ranges: bytes
Content-Length: 144848
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpeg

MZ.....@.....!..L!This program cannot be run in DOS mode.
$......!$.JO.JO.JO.u.O.JO?oKN.JO?oIN.JO?oON.JO?oNN.JO.mKN.JO-nKN.JO.KO~JO-nNN.JO-nJN.JO-n.O.JO-nHN.JO
D.....F.....@..@.data.....@.....fsrc...X...0.....@..@.reloc..`....@.....@..B.....
u..\".].U..\".u.....t...].\".].U..\".u.....t3].\".].xU..\".u.....t...].\".].U..\".u.....[...u..\".].].U..\".u.;
u..\".].P..].U..\".u.....t...].\".].H...U..\".u.....t...].\".].X...U..\".u.....t...].\".].T..U..\".u.....H....t3].\".].hU..
```

Figure 11

But compared to Gary Kessler Magic number MZ are associated with .exe or DLLs. Jpegs are as shown in figure 12.

```
00 00 00 0C 6A 50 20 20      ....jP
0D 0A                        ..
JP2 Various JPEG-2000 image file formats
```

Figure 12

Further scrutiny shows that Suricata flagged a Privacy Violation, and this would warrant further investigation.

2022-01-07 16:07:32.605 +00:00	suricata.alert	2.56.57.108	80	192.168.1.216	49738	Potential Corporate Privacy Violation	ET INFO PE EXE or DLL Windows file download HTTP
timestamp	2022-01-07T16:07:32.605Z						
version	1						
container.id	eve-2025-02-16-09:47.json						

Figure 13

From the brief analysis, it would seem that the source IP address had access and was able to download a file.

Conclusion.

Multiple tools installed in Security Onion make the investigation of cases easier, enabling the security team to identify anomalies in the traffic flow, ultimately confirming the presence of suspicious behaviour. The Security team can have a comprehensive analysis of network traffic and underscores the importance of continuous network monitoring and reinforces the need for proactive threat detection and response measures

Lessons Learned

1. Importing a pcap into Security Onion
2. Searching for anomalies
3. Using OSINT tools to get more details
4. Using Gary Kessler Magic number to identify discrepancies in file extensions
5. Using Online tools e.g. Virus Total, AbuseIP