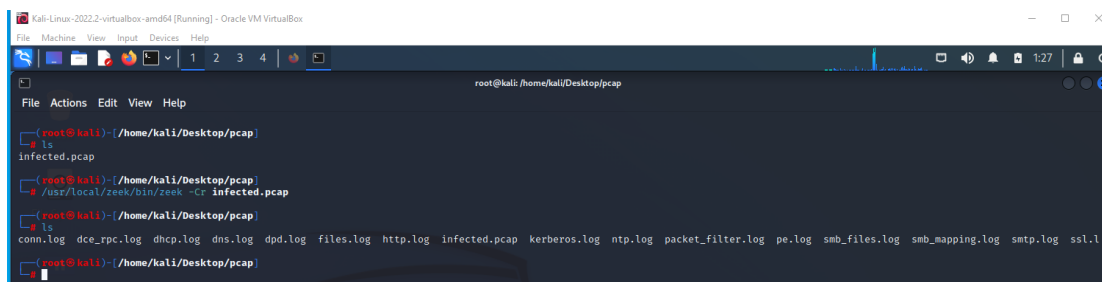


# PCAP File Investigation

By: Tamir Maidani

We will be using the zeek software in Linux in order to conduct this investigation.

1. splitting the ".log" files in order to allow zeek to work with them.

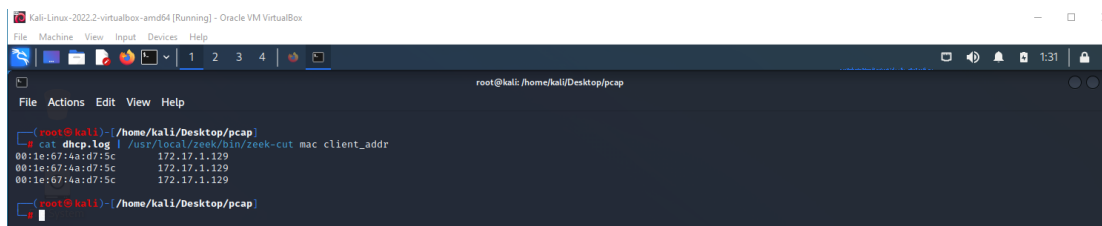


```

root@kali: ~/home/kali/Desktop/pcap
root@kali:~/home/kali/Desktop/pcap# ls
infected.pcap
root@kali:~/home/kali/Desktop/pcap# /usr/local/zeek/bin/zeek-cut infected.pcap
root@kali:~/home/kali/Desktop/pcap# ls
conn.log dce_rpc.log dhcp.log dns.log dpd.log files.log http.log infected.pcap kerberos.log ntp.log packet_filter.log pe.log smb_files.log smb_mapping.log smtp.log ssl.l
root@kali:~/home/kali/Desktop/pcap#

```

2. Extracting the MAC and IP addresses from the "dhcp.log" file.

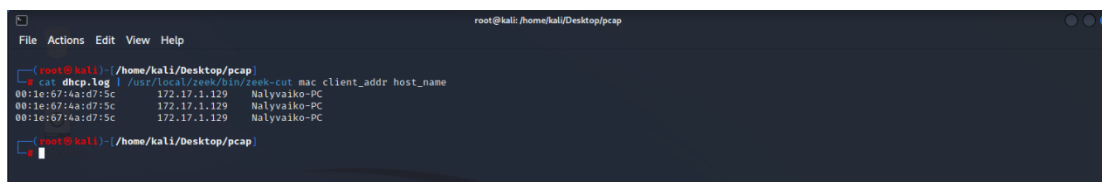


```

root@kali:~/home/kali/Desktop/pcap# cat dhcp.log | /usr/local/zeek/bin/zeek-cut mac client_addr
00:1e:07:4a:d7:5c 172.17.1.129
00:1e:07:4a:d7:5c 172.17.1.129
00:1e:07:4a:d7:5c 172.17.1.129
root@kali:~/home/kali/Desktop/pcap#

```

3. Extracting the host name from the "dhcp.log" file.

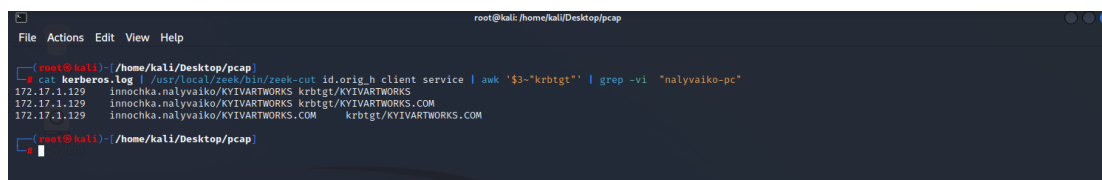


```

root@kali:~/home/kali/Desktop/pcap# cat dhcp.log | /usr/local/zeek/bin/zeek-cut mac client_addr host_name
00:1e:07:4a:d7:5c 172.17.1.129 Nalyvaiko-PC
00:1e:07:4a:d7:5c 172.17.1.129 Nalyvaiko-PC
00:1e:07:4a:d7:5c 172.17.1.129 Nalyvaiko-PC
root@kali:~/home/kali/Desktop/pcap#

```

4. Extracting the Windows User Name from the "Kerberos.log" file.



```

root@kali:~/home/kali/Desktop/pcap# cat kerberos.log | /usr/local/zeek/bin/zeek-cut id.orig.h client service | awk '{3~"krbtgt"}' | grep -vi "nalyvaiko-pc"
172.17.1.129 innochka.nalyvaiko/KYIVARTWORKS krbtgt/KYIVARTWORKS.COM
172.17.1.129 innochka.nalyvaiko/KYIVARTWORKS krbtgt/KYIVARTWORKS.COM
172.17.1.129 innochka.nalyvaiko/KYIVARTWORKS.COM krbtgt/KYIVARTWORKS.COM
root@kali:~/home/kali/Desktop/pcap#

```

5.Extracting the "file.log" from the infected **Microsoft Word** file.

```
root@kali: /home/kali/Desktop/pcap
File Actions Edit View Help
root@kali: /home/kali/Desktop/pcap
cat file.log | /usr/local/zeek/bin/zeek-cut mime_type filename | grep msword
application/msword 2018_11Details_zur_Transaktion.doc
root@kali: /home/kali/Desktop/pcap
```

6.Extracting the time and date on which the **Word** file was downloaded.

```
root@kali: /home/kali/Desktop/pcap
File Actions Edit View Help
root@kali: /home/kali/Desktop/pcap
cat http.log | /usr/local/zeek/bin/zeek-cut -d ts method host uri resp_filenames resp_mime_types | grep "2018_11Details_zur_Transaktion.doc"
2018-11-12T16:02:49-0500 GET ifcingenieria.cl /QpX8It/BIZ/Firmenkunden/ 2018_11Details_zur_Transaktion.doc application/msword
root@kali: /home/kali/Desktop/pcap
```

7.Extracting the name of the executable file that was downloaded via the "macro" in the **Word** file.

```
root@kali: /home/kali/Desktop/pcap
File Actions Edit View Help
root@kali: /home/kali/Desktop/pcap
cat http.log | /usr/local/zeek/bin/zeek-cut -d ts method host uri resp_filenames resp_mime_types | grep dosexec
2018-11-12T16:02:49-0500 GET timlinger.com /nmw/ 6169583.exe application/x-dosexec
root@kali: /home/kali/Desktop/pcap
```

8.Using the "Hybrid-Analysis" website to conduct further investigation.

The screenshot shows the Hybrid-Analysis website interface. The top navigation bar includes links for Sandbox, Quick Scans, File Collections, Resources, and Request Info. The main content area displays a report for a sample with a threat score of 100/100 and a detection rate of 82%. The 'Incident Response' section is highlighted, showing a 'Risk Assessment' with 'Persistence' and 'Network Behavior' indicators. The 'MITRE ATT&CK Techniques Detection' section shows 14 indicators mapped to 13 attack techniques and 7 tactics. The 'Latest News' section on the right features articles about PROPHET SPIDER exploits, CVE-2023-22940, and CrowdStrike Falcon.

Free Automated Malware Analysis

https://www.hybrid-analysis.com/sample/094be4229a74cdd11212671e6391742cc8b6e387b14da02974b07857b2779223

SandboxQuick ScansFile CollectionsResourcesRequest Info

Q IP, Domain, Hash

More

Analysis Overview

Submission name: Fimberlunden

Size: 7KB

Type: [doc](#) [office](#)

Mime: application/msword

SHA256: 094be4229a74cdd11212671e6391742cc8b6e387b14da02974b07857b2779223

Operating System: Windows

Last Anti-Virus Scan: 05/08/2022 19:09:23 (UTC)

Last Sandbox Report: 04/04/2019 13:22:34 (UTC)

Request Report Detection

malicious

Threat Score: 100/100

AI Detection: 92%

Labeled as: Trojan.Generic

amavise-on-ops

Like

Twitter

Facebook

Print

Analysis Overview

Anti-Virus Scanner Results

Falcon Sandbox Reports (2)

Incident Response

Community (0)

Back to top

Anti-Virus Results

Refresh

CrowdStrike Falcon

90%

Static Analysis and ML

Last Update: 05/08/2022 19:09:23 (UTC)

View Details: [N/A](#)

Visit Vendor: [Go](#)

GET STARTED WITH A FREE TRIAL

MetaDefender

N/A

Multi Scan Analysis

Last Update: 05/08/2022 19:09:23 (UTC)

View Details: [Go](#)

Visit Vendor: [Go](#)

VirusTotal

73%

Multi Scan Analysis

Last Update: 05/08/2022 19:09:23 (UTC)

View Details: [Go](#)

Visit Vendor: [Go](#)

Latest News

RIDOMET SPIDER Exploits Canva ShareFile Remote Code Execution Vulnerability CVE-2022-22941 to Deliver Webshell

Chris Nguyen - Evt Ldr - March 3, 2022

Decryptable Ransomware Reportedly Targeting Ukrainian Entities

CrowdStrike Intelligence Team - March 3, 2022

CrowdStrike Falcon Protects from New Wiper Malware Used in Ukraine Cyberattacks

William Thomas - Active Labs Analyst - Ford World - February 25, 2022

Access Breakers: Who Are the Targets, and What Are They Worth?

CrowdStrike Intelligence Team - February 23, 2022

CrowdStrike Research Investigates Exploit Behavior to Strengthen Customer Protection

Joseph Crockett - Agent Intelligence - February 12, 2022

[See More](#)

Falcon Sandbox Reports

This website uses cookies to enhance your browsing experience. Please note that by continuing to use this site you consent to the terms of our [Data Protection Policy](#).

ACCEPT

01:57 05/06/2022

ENG

14°C

הקל באן בדי לחט