Faculty of Computers and Data Science

Cyber Security department

Level 3

جامعة الإسكندرية
ALEXANDRIA
UNIVERSITY
كليـة الحاسبات وعلـوم البيـانات

Analyzing the Zeus Banking Trojan using various tools and techniques.

(https://github.com/omaribrahim44/Zeus-Banking-Trojan.git)

Prepared by:

Omar Ibrahim Ahmed	2206209
Marwan Gaber Ramadan	2206167
Mohamed Salah Fayad	22010448
Youssef Tamer Mohamed	2206208

Under supervision of:

Dr Hatem Abdelkadir

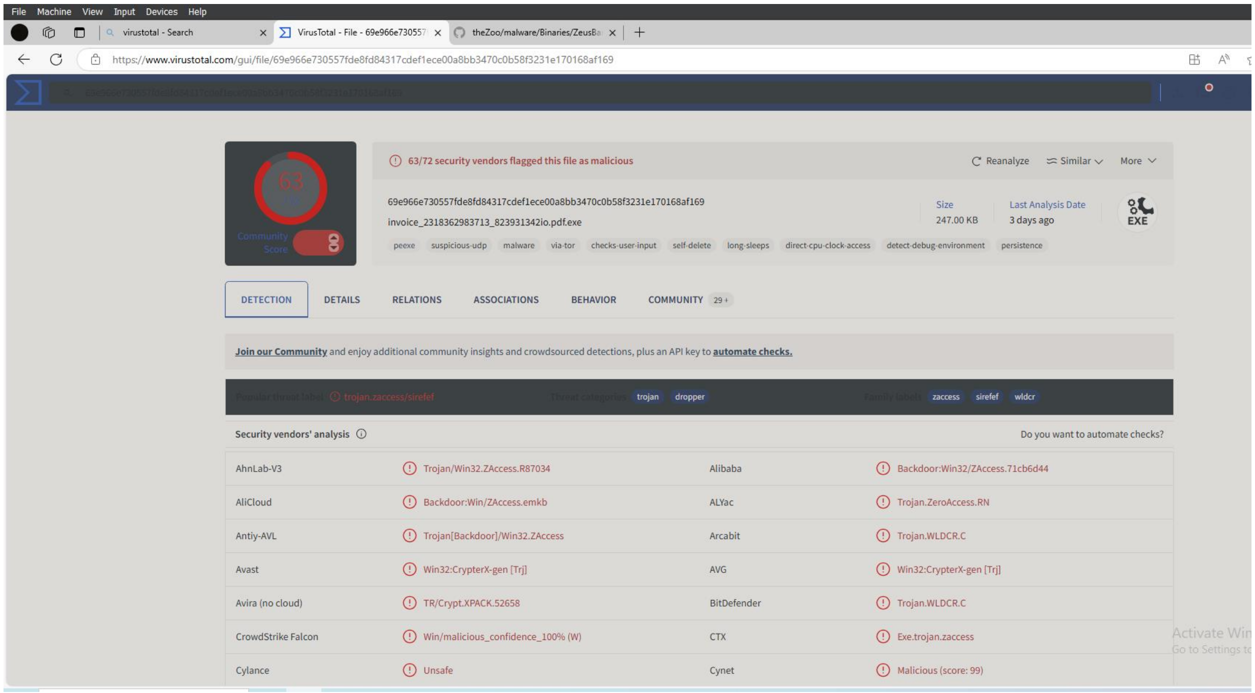
Proactive Computer Security

2024/2025

1] Static Analysis of the trojan

➢ VIRUSTOTAL

- File name : invoice_2318362983713_823931342io.pdf.exe


File Machine View Input Devices Help
virustotal - Search
VirusTotal - File - 69e966e730557
theZoo/malware/Binaries/ZeusBa
https://www.virustotal.com/gui/file/69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
63
Community Score
Reanalyze
Similar
More
Size
Last Analysis Date
EXE
DETECTION
DETAILS
RELATIONS
ASSOCIATIONS
BEHAVIOR
COMMUNITY 29 +

63/72 security vendors flagged this file as malicious

69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
invoice_2318362983713_823931342io.pdf.exe

Size: 247.00 KB
Last Analysis Date: 3 days ago

peexe · suspicious-udp · malware · via-tor · checks-user-input · self-delete · long-sleeps · direct-cpu-clock-access · detect-debug-environment · persistence

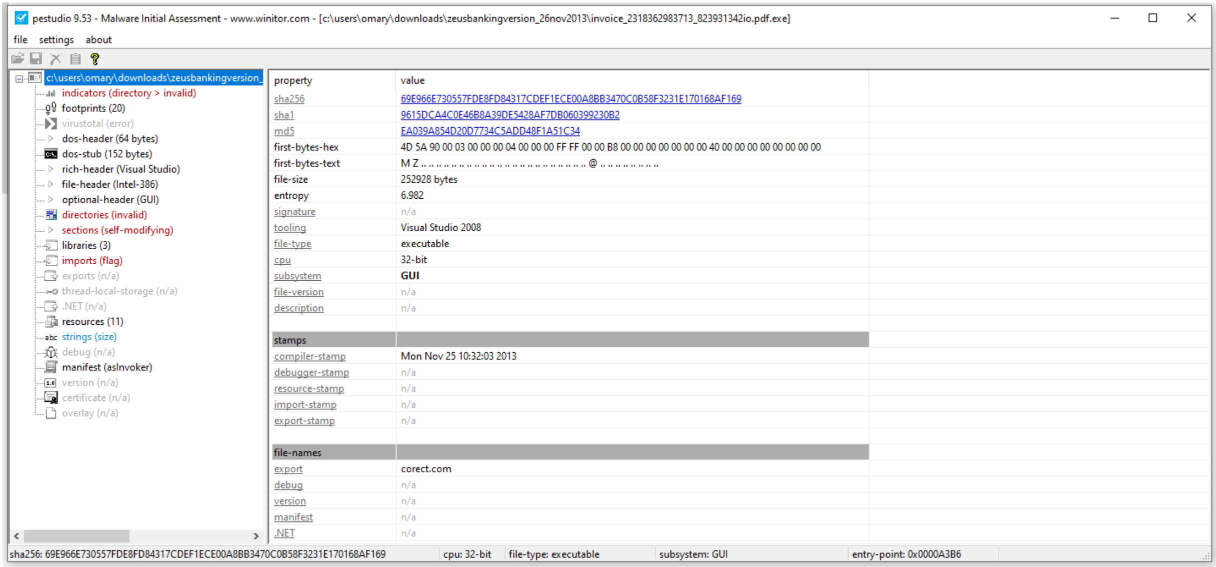
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.zaccess/sirefef · Threat categories: trojan, dropper · Family labels: zaccess, sirefef, wldcr

Security vendors' analysis · Do you want to automate checks?

AhnLab-V3	Trojan/Win32.ZAccess.R87034	Alibaba	Backdoor:Win32/ZAccess.71cb6d44
AliCloud	Backdoor:Win/ZAccess.emkb	ALYac	Trojan.ZeroAccess.RN
Antiy-AVL	Trojan[Backdoor]/Win32.ZAccess	Arcabit	Trojan.WLDCR.C
Avast	Win32:CrypterX-gen [Trj]	AVG	Win32:CrypterX-gen [Trj]
Avira (no cloud)	TR/Crypt.XPACK.52658	BitDefender	Trojan.WLDCR.C
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.zaccess
Cylance	Unsafe	Cynet	Malicious (score: 99)

➢ PE Studio



pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\omary\downloads\zeusbankingversion_26nov2013\invoice_2318362983713_823931342io.pdf.exe]

c:\users\omary\downloads\zeusbankingversion_
- indicators (directory > invalid)
- footprints (20)
- virustotal (error)
- dos-header (64 bytes)
- dos-stub (152 bytes)
- rich-header (Visual Studio)
- file-header (Intel-386)
- optional-header (GUI)
- directories (invalid)
- sections (self-modifying)
- libraries (3)
- imports (flag)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (11)
- strings (size)
- debug (n/a)
- manifest (asInvoker)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

property	value
sha256	69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169
sha1	9615DCA4C0E46B8A39DE5428AF7DB060399230B2
md5	EA039A854D20D7734C5ADD48F1A51C34
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	252928 bytes
entropy	6.982
signature	n/a
tooling	Visual Studio 2008
file-type	executable
cpu	32-bit
subsystem	GUI
file-version	n/a
description	n/a
stamps	
compiler-stamp	Mon Nov 25 10:32:03 2013
debugger-stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a
file-names	
export	corect.com
debug	n/a
version	n/a
manifest	n/a
.NET	n/a

sha256: 69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169 · cpu: 32-bit · file-type: executable · subsystem: GUI · entry-point: 0x0000A3B6

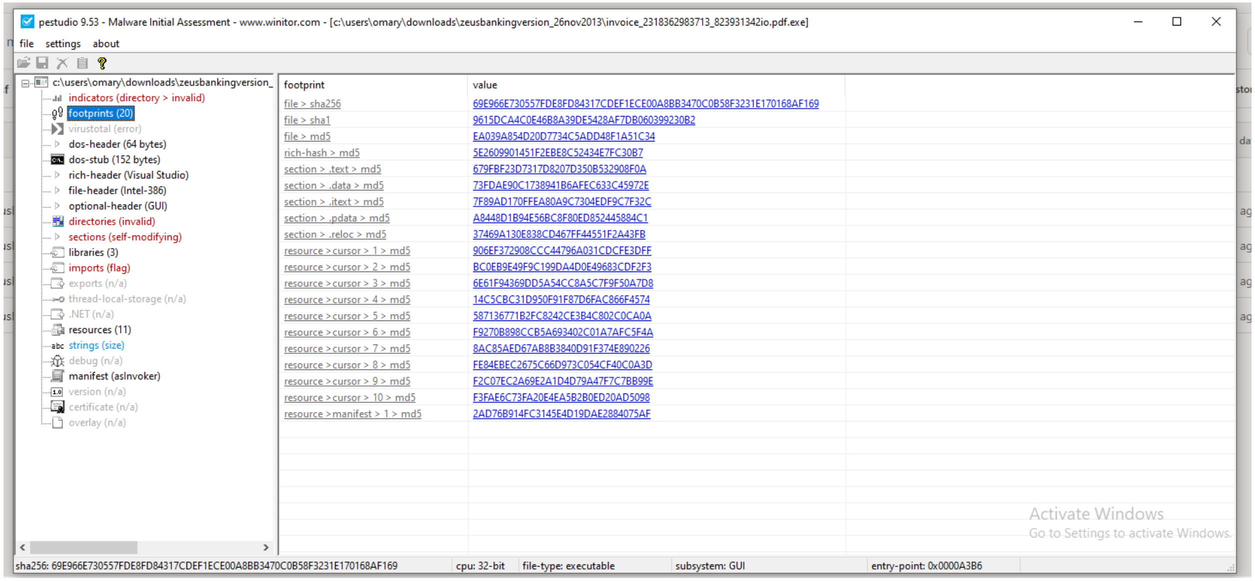
- Hashes

sha256,69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169

sha1,9615DCA4C0E46B8A39DE5428AF7DB060399230B2

md5,EA039A854D20D7734C5ADD48F1A51C34

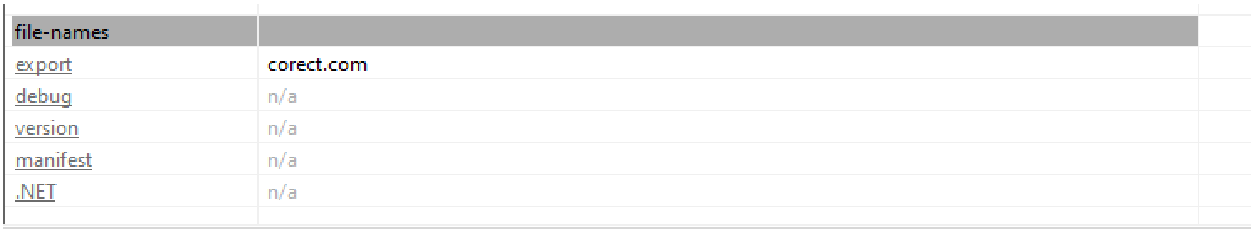
- footprints


pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\omary\downloads\zeusbankingversion_26nov2013\invoice_2318362983713_823931342io.pdf.exe]
file
settings
about
c:\users\omary\downloads\zeusbankingversion_
indicators (directory > invalid)
footprints (20)
virustotal (error)
dos-header (64 bytes)
dos-stub (152 bytes)
rich-header (Visual Studio)
file-header (Intel-386)
optional-header (GUI)
directories (invalid)
sections (self-modifying)
libraries (3)
imports (flag)
exports (n/a)
thread-local-storage (n/a)
.NET (n/a)
resources (11)
strings (size)
debug (n/a)
manifest (asInvoker)
version (n/a)
certificate (n/a)
overlay (n/a)
Activate Windows
Go to Settings to activate Windows.

footprint	value
file > sha256	69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169
file > sha1	9615DCA4C0E46B8A39DE5428AF7DB060399230B2
file > md5	EA039A854D20D7734C5ADD48F1A51C34
rich-hash > md5	5E2609901451F2EBE8C52434E7FC30B7
section > .text > md5	679FBF23D7317D8207D350B532908F0A
section > .data > md5	73FDAE90C1738941B6AFEC633C45972E
section > .itext > md5	7F89AD170FFEA80A9C7304EDF9C7F32C
section > .pdata > md5	A8448D1B94E56BC8F80ED852445884C1
section > .reloc > md5	37469A130E838CD467FF44551F2A43FB
resource > cursor > 1 > md5	906EF372908CCC44796A031CDCFE3DFF
resource > cursor > 2 > md5	BC0EB9E49F9C199DA4D0E49683CDF2F3
resource > cursor > 3 > md5	6E61F94369DD5A54CC8A5C7F9F50A7D8
resource > cursor > 4 > md5	14C5CBC31D950F91F87D6FAC866F4574
resource > cursor > 5 > md5	587136771B2FC8242CE3B4C802C0CA0A
resource > cursor > 6 > md5	F9270B898CCB5A693402C01A7AFC5F4A
resource > cursor > 7 > md5	8AC85AED67AB8B3840D91F374E890226
resource > cursor > 8 > md5	FE84EBEC2675C66D973C054CF40C0A3D
resource > cursor > 9 > md5	F2C07EC2A69E2A1D4D79A47F7C7BB99E
resource > cursor > 10 > md5	F3FAE6C73FA20E4EA5B2B0ED20AD5098
resource > manifest > 1 > md5	2AD76B914FC3145E4D19DAE2884075AF

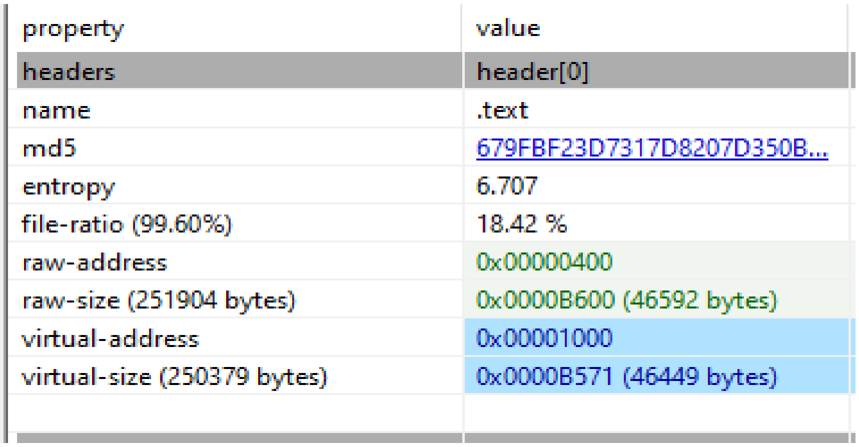
sha256: 69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169 cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x0000A3B6

-Incorrect url



file-names	
export	corect.com
debug	n/a
version	n/a
manifest	n/a
.NET	n/a

- Virtual size and raw size aren’t equal



property	value
headers	header[0]
name	.text
md5	679FBF23D7317D8207D350B...
entropy	6.707
file-ratio (99.60%)	18.42 %
raw-address	0x00000400
raw-size (251904 bytes)	0x0000B600 (46592 bytes)
virtual-address	0x00001000
virtual-size (250379 bytes)	0x0000B571 (46449 bytes)

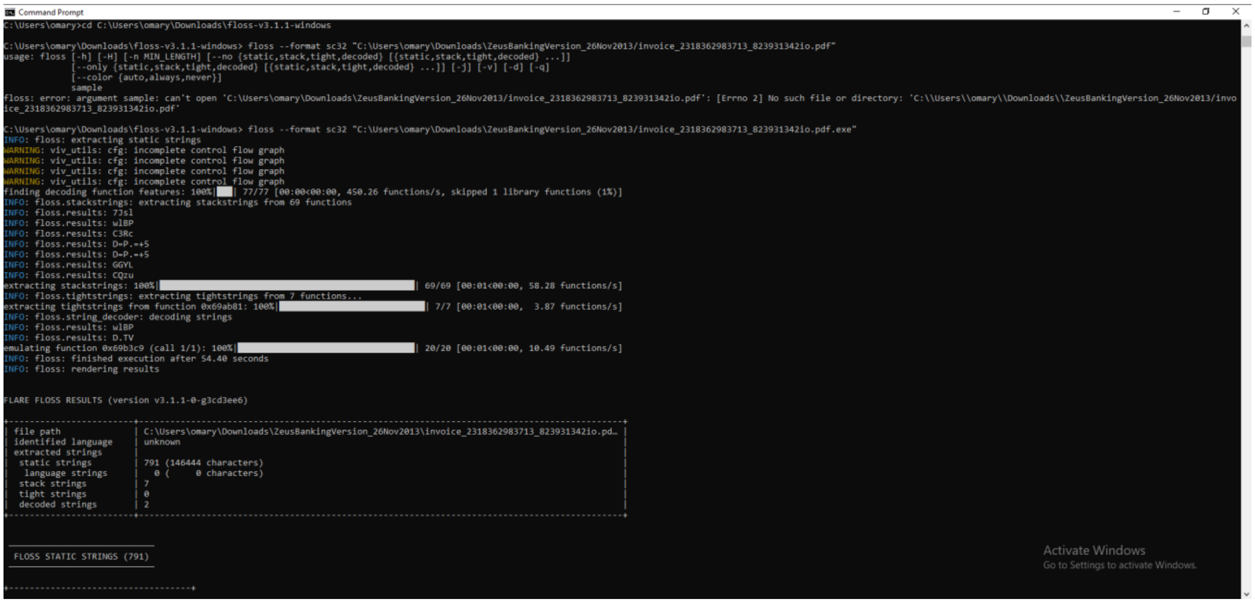
- Libraries

SHLWAPI.dll,-,-,-,0x00020208,0x00020078,implicit,21,-,Shell Light-weight Utility Library

KERNEL32.dll,-,-,-,0x00020190,0x00020000,implicit,29,-,Windows NT BASE API Client

USER32.dll,-,-,-,0x00020260,0x000200D0,implicit,27,-,Multi-User Windows USER API Client Library

➢ Floss



```
C:\Users\omary>cd C:\Users\omary\Downloads\floss-v3.1.1-windows

C:\Users\omary\Downloads\floss-v3.1.1-windows> floss --format sc32 "C:\Users\omary\Downloads\ZeusBankingVersion_26Nov2013/invoice_2318362983713_823931342io.pdf"
usage: floss [-h] [-H] [-n MIN_LENGTH] [--no {static,stack,tight,decoded} [{static,stack,tight,decoded} ...]]
             [--only {static,stack,tight,decoded} [{static,stack,tight,decoded} ...]] [-j] [-v] [-d] [-q]
             [--color {auto,always,never}]
             sample
floss: error: argument sample: can't open 'C:\Users\omary\Downloads\ZeusBankingVersion_26Nov2013/invoice_2318362983713_823931342io.pdf': [Errno 2] No such file or directory: 'C:\\Users\\omary\\Downloads\\ZeusBankingVersion_26Nov2013/invo
ice_2318362983713_823931342io.pdf'

C:\Users\omary\Downloads\floss-v3.1.1-windows> floss --format sc32 "C:\Users\omary\Downloads\ZeusBankingVersion_26Nov2013/invoice_2318362983713_823931342io.pdf.exe"
INFO: floss: extracting static strings
WARNING: viv_utils: cfg: incomplete control flow graph
WARNING: viv_utils: cfg: incomplete control flow graph
WARNING: viv_utils: cfg: incomplete control flow graph
WARNING: viv_utils: cfg: incomplete control flow graph
finding decoding function features: 100%|██| 77/77 [00:00<00:00, 450.26 functions/s, skipped 1 library functions (1%)]
INFO: floss.stackstrings: extracting stackstrings from 69 functions
INFO: floss.results: 7Jsl
INFO: floss.results: wlBP
INFO: floss.results: C3Rc
INFO: floss.results: D=P.=+5
INFO: floss.results: D=P.-+5
INFO: floss.results: GGYL
INFO: floss.results: CQzu
extracting stackstrings: 100%|████████████████████████| 69/69 [00:01<00:00, 58.28 functions/s]
INFO: floss.tightstrings: extracting tightstrings from 7 functions...
extracting tightstrings from function 0x69ab81: 100%|██████████████| 7/7 [00:01<00:00,  3.87 functions/s]
INFO: floss.string_decoder: decoding strings
INFO: floss.results: wlBP
INFO: floss.results: D.TV
emulating function 0x69b3c9 (call 1/1): 100%|█████████████████| 20/20 [00:01<00:00, 10.49 functions/s]
INFO: floss: finished execution after 54.40 seconds
INFO: floss: rendering results


FLARE FLOSS RESULTS (version v3.1.1-0-g3cd3ee6)

+------------------------+------------------------------------------------------------------------------------------+
| file path              | C:\Users\omary\Downloads\ZeusBankingVersion_26Nov2013\invoice_2318362983713_823931342io.pd… |
| identified language    | unknown                                                                                  |
| extracted strings      |                                                                                          |
|  static strings        | 791 (146444 characters)                                                                  |
|   language strings     |   0 (     0 characters)                                                                  |
|  stack strings         | 7                                                                                        |
|  tight strings         | 0                                                                                        |
|  decoded strings       | 2                                                                                        |
+------------------------+------------------------------------------------------------------------------------------+


 ─────────────────────────
  FLOSS STATIC STRINGS (791)
 ─────────────────────────

+----------------------------------+
```

2] Detection of the trojan

- **VM Setup:**

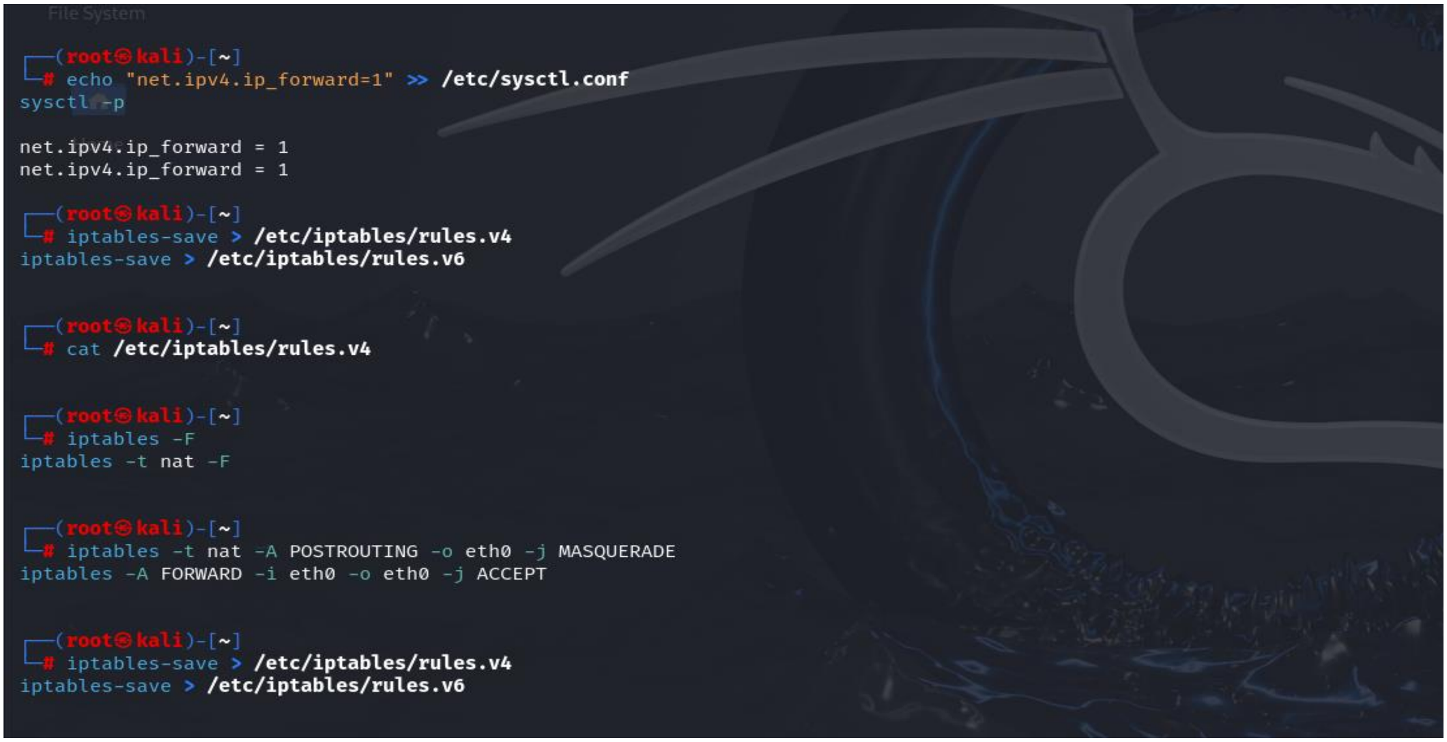
  - Kali Linux machine (Detection Machine) on Bridged Adapter 1

  - Windows 10 machine (Infected Machine) on Bridged Adapter 1

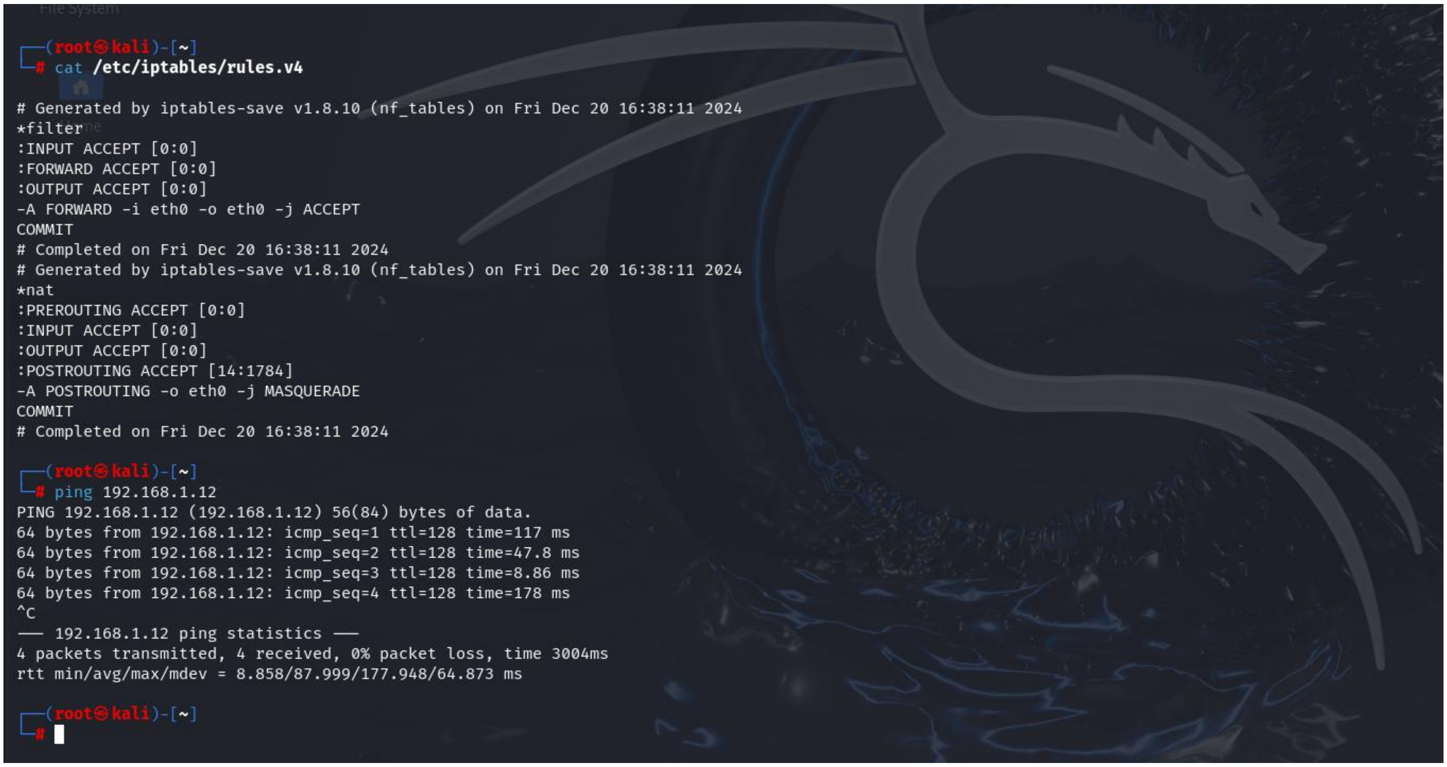
- **Network Configuration:**

  - Kali Linux Setup (192.168.1.9)

    Enabling IP Forwarding + Configuring NAT



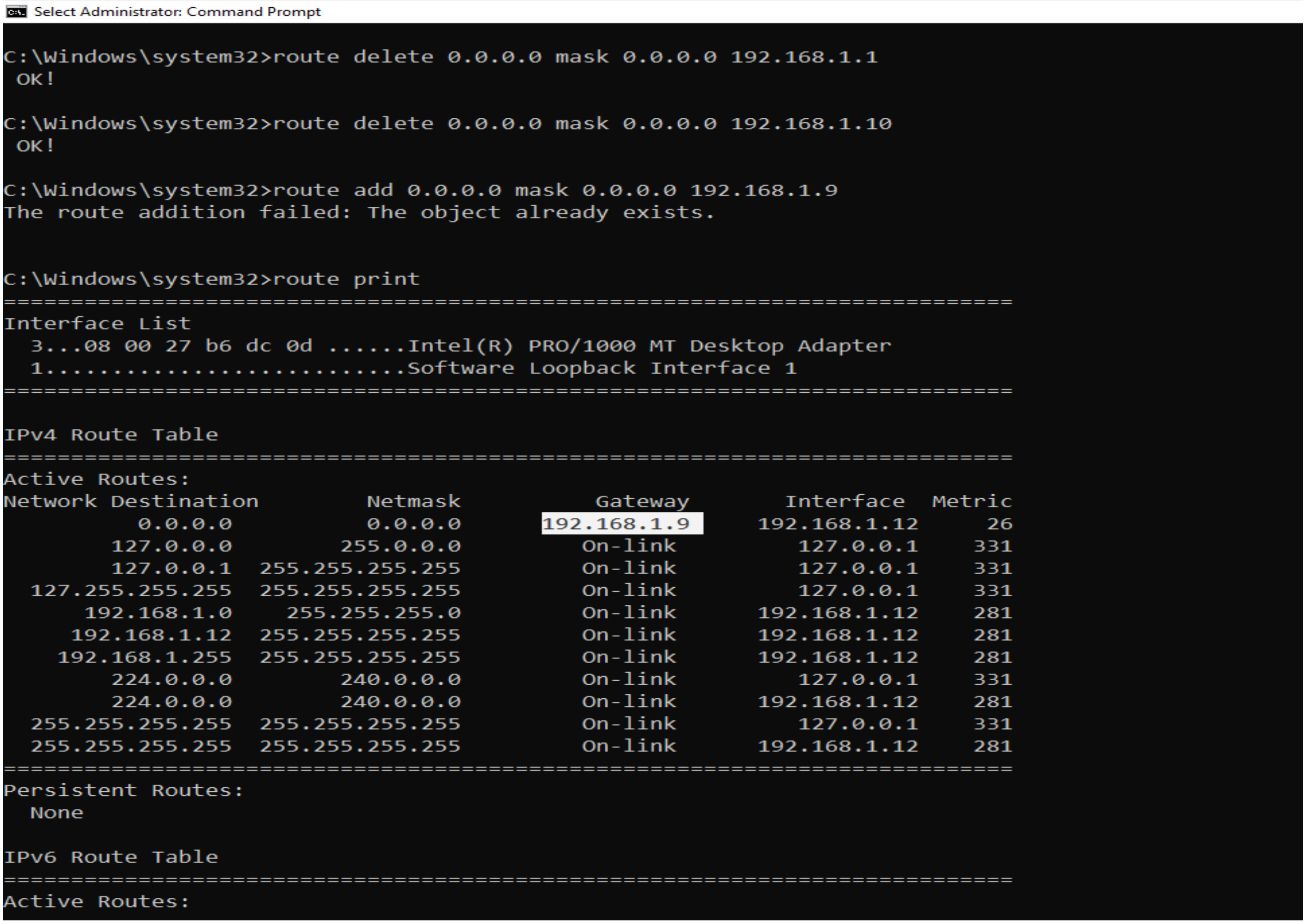
```
┌──(root㉿kali)-[~]
└─# echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
sysctl -p

net.ipv4.ip_forward = 1
net.ipv4.ip_forward = 1

┌──(root㉿kali)-[~]
└─# iptables-save > /etc/iptables/rules.v4
iptables-save > /etc/iptables/rules.v6


┌──(root㉿kali)-[~]
└─# cat /etc/iptables/rules.v4


┌──(root㉿kali)-[~]
└─# iptables -F
iptables -t nat -F


┌──(root㉿kali)-[~]
└─# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i eth0 -o eth0 -j ACCEPT


┌──(root㉿kali)-[~]
└─# iptables-save > /etc/iptables/rules.v4
iptables-save > /etc/iptables/rules.v6
```



```
┌──(root㉿kali)-[~]
└─# cat /etc/iptables/rules.v4

# Generated by iptables-save v1.8.10 (nf_tables) on Fri Dec 20 16:38:11 2024
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -i eth0 -o eth0 -j ACCEPT
COMMIT
# Completed on Fri Dec 20 16:38:11 2024
# Generated by iptables-save v1.8.10 (nf_tables) on Fri Dec 20 16:38:11 2024
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [14:1784]
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT
# Completed on Fri Dec 20 16:38:11 2024

┌──(root㉿kali)-[~]
└─# ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=128 time=117 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=128 time=47.8 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=128 time=8.86 ms
64 bytes from 192.168.1.12: icmp_seq=4 ttl=128 time=178 ms
^C
--- 192.168.1.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 8.858/87.999/177.948/64.873 ms

┌──(root㉿kali)-[~]
└─# 
```

- Windows VM Setup (192.168.1.12)

Setting the Kali machine as the default gateway.

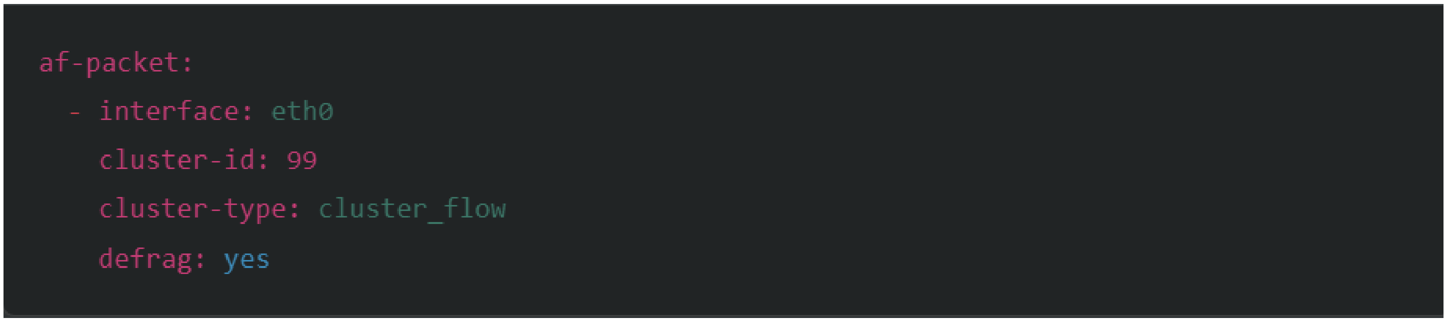


Select Administrator: Command Prompt

```
C:\Windows\system32>route delete 0.0.0.0 mask 0.0.0.0 192.168.1.1
 OK!

C:\Windows\system32>route delete 0.0.0.0 mask 0.0.0.0 192.168.1.10
 OK!

C:\Windows\system32>route add 0.0.0.0 mask 0.0.0.0 192.168.1.9
The route addition failed: The object already exists.


C:\Windows\system32>route print
===========================================================================
Interface List
  3...08 00 27 b6 dc 0d ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.9     192.168.1.12     26
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link      192.168.1.12    281
     192.168.1.12  255.255.255.255         On-link      192.168.1.12    281
    192.168.1.255  255.255.255.255         On-link      192.168.1.12    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.1.12    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.1.12    281
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
```

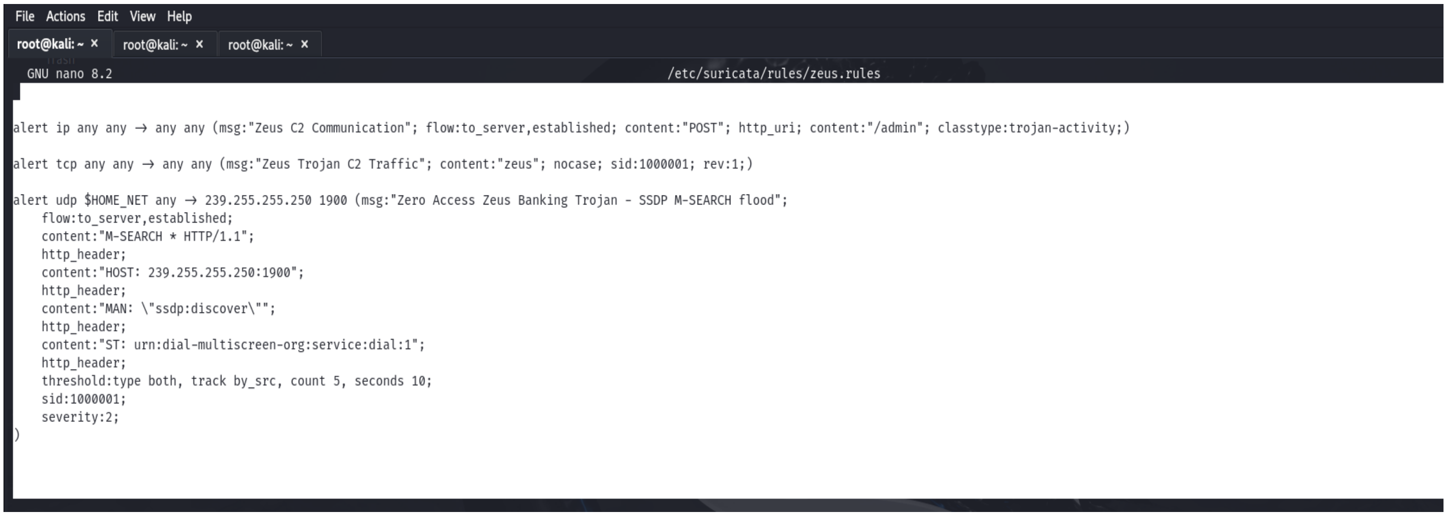
➢ Configure Suricata on Kali:

Ensuring suricata.yaml file is configured as



```
af-packet:
  - interface: eth0
    cluster-id: 99
    cluster-type: cluster_flow
    defrag: yes
```

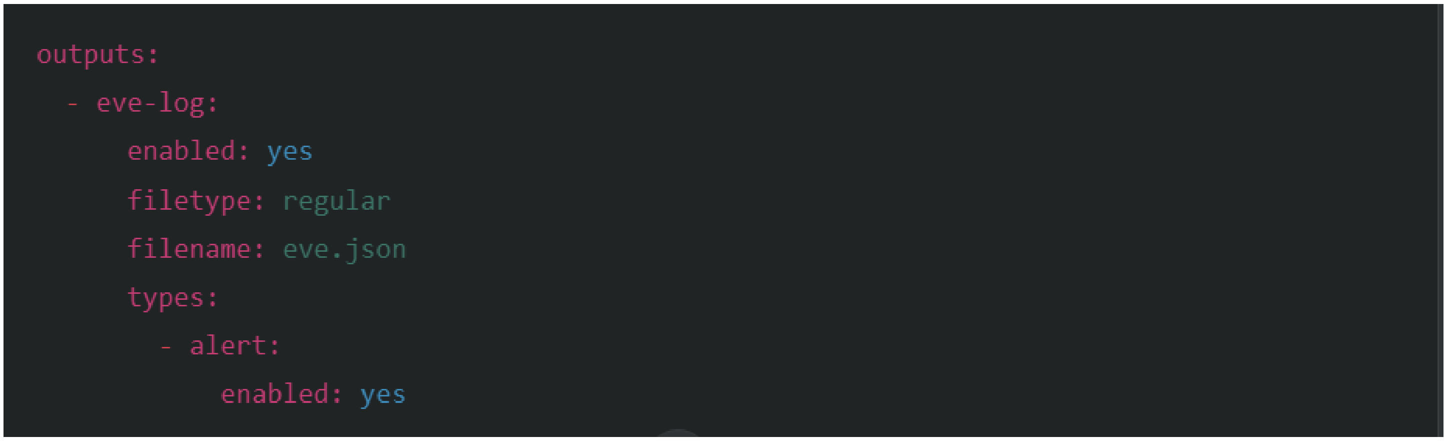
➢ Suricata Rules



```
  GNU nano 8.2                                        /etc/suricata/rules/zeus.rules

alert ip any any → any any (msg:"Zeus C2 Communication"; flow:to_server,established; content:"POST"; http_uri; content:"/admin"; classtype:trojan-activity;)

alert tcp any any → any any (msg:"Zeus Trojan C2 Traffic"; content:"zeus"; nocase; sid:1000001; rev:1;)

alert udp $HOME_NET any → 239.255.255.250 1900 (msg:"Zero Access Zeus Banking Trojan - SSDP M-SEARCH flood";
    flow:to_server,established;
    content:"M-SEARCH * HTTP/1.1";
    http_header;
    content:"HOST: 239.255.255.250:1900";
    http_header;
    content:"MAN: \"ssdp:discover\"";
    http_header;
    content:"ST: urn:dial-multiscreen-org:service:dial:1";
    http_header;
    threshold:type both, track by_src, count 5, seconds 10;
    sid:1000001;
    severity:2;
)
```

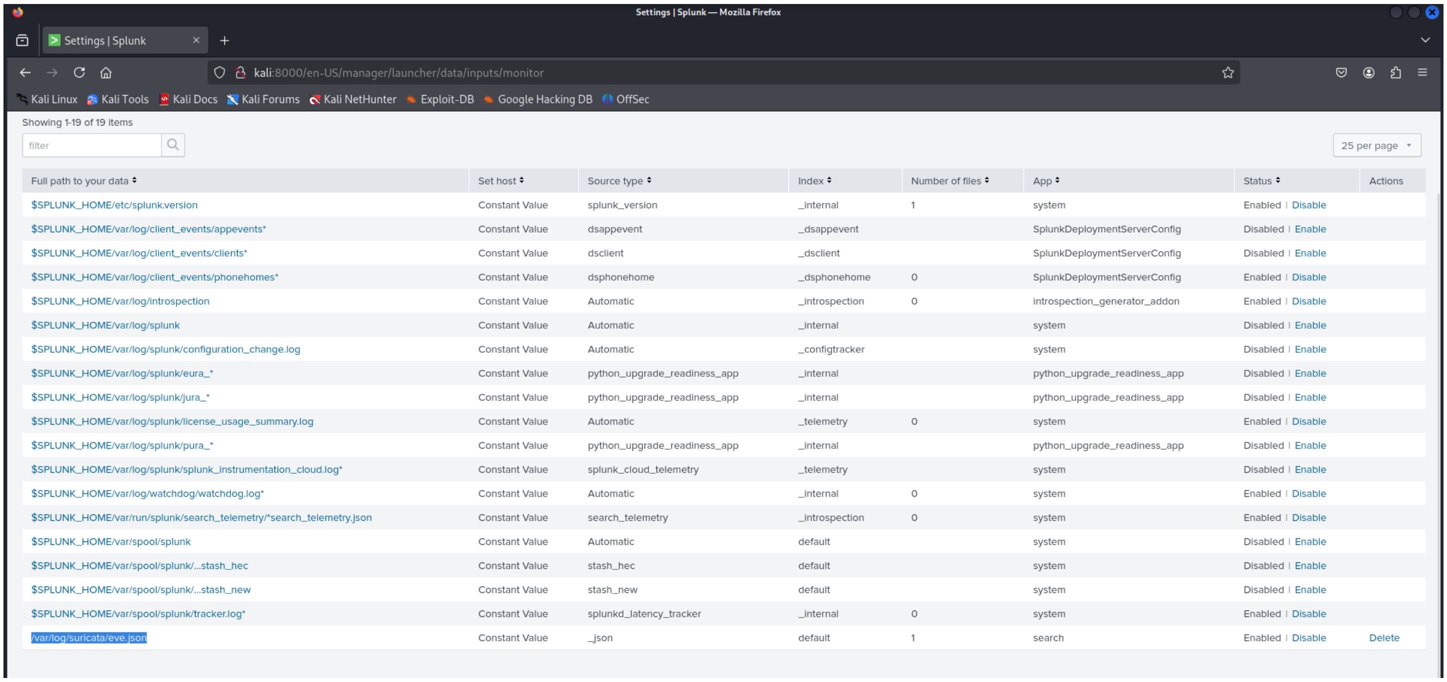
➢ Splunk Configuration:

Edit Suricata configuration to output logs in JSON format



```
outputs:
  - eve-log:
      enabled: yes
      filetype: regular
      filename: eve.json
      types:
        - alert:
            enabled: yes
```

- **Access splunk on localhost:8000**

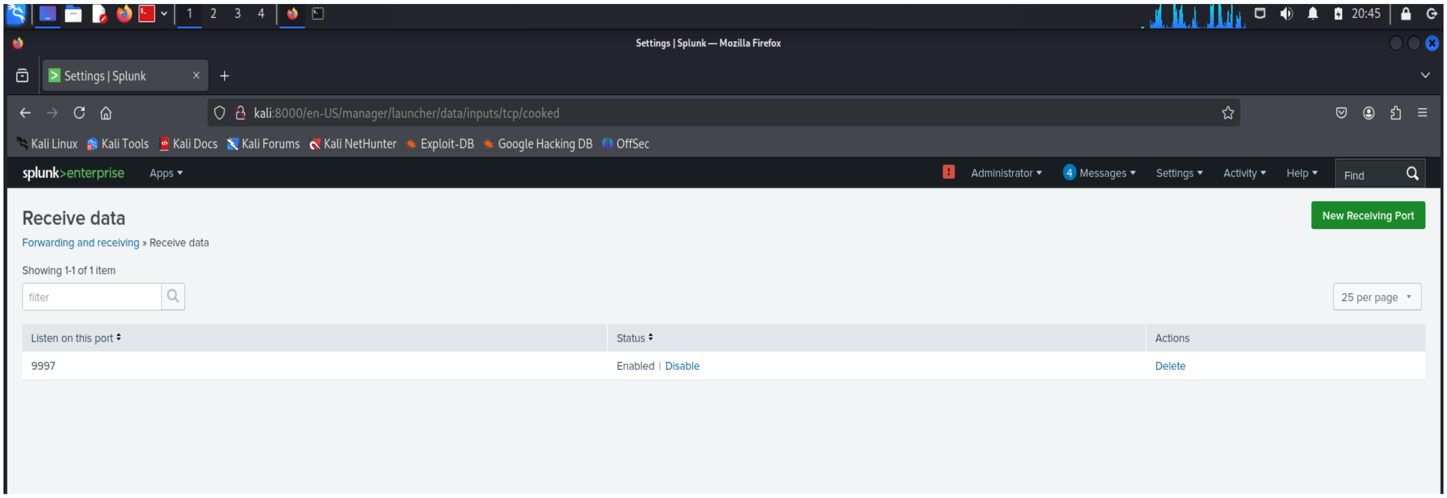


Showing 1-19 of 19 items

Full path to your data	Set host	Source type	Index	Number of files	App	Status	Actions
$SPLUNK_HOME/etc/splunk.version	Constant Value	splunk_version	_internal	1	system	Enabled | Disable	
$SPLUNK_HOME/var/log/client_events/appevents*	Constant Value	dsappevent	_dsappevent		SplunkDeploymentServerConfig	Disabled | Enable	
$SPLUNK_HOME/var/log/client_events/clients*	Constant Value	dsclient	_dsclient		SplunkDeploymentServerConfig	Disabled | Enable	
$SPLUNK_HOME/var/log/client_events/phonehomes*	Constant Value	dsphonehome	_dsphonehome	0	SplunkDeploymentServerConfig	Enabled | Disable	
$SPLUNK_HOME/var/log/introspection	Constant Value	Automatic	_introspection	0	introspection_generator_addon	Enabled | Disable	
$SPLUNK_HOME/var/log/splunk	Constant Value	Automatic	_internal		system	Disabled | Enable	
$SPLUNK_HOME/var/log/splunk/configuration_change.log	Constant Value	Automatic	_configtracker		system	Disabled | Enable	
$SPLUNK_HOME/var/log/splunk/eura_*	Constant Value	python_upgrade_readiness_app	_internal		python_upgrade_readiness_app	Disabled | Enable	
$SPLUNK_HOME/var/log/splunk/jura_*	Constant Value	python_upgrade_readiness_app	_internal		python_upgrade_readiness_app	Disabled | Enable	
$SPLUNK_HOME/var/log/splunk/license_usage_summary.log	Constant Value	Automatic	_telemetry	0	system	Enabled | Disable	
$SPLUNK_HOME/var/log/splunk/pura_*	Constant Value	python_upgrade_readiness_app	_internal		python_upgrade_readiness_app	Disabled | Enable	
$SPLUNK_HOME/var/log/splunk/splunk_instrumentation_cloud.log*	Constant Value	splunk_cloud_telemetry	_telemetry		system	Disabled | Enable	
$SPLUNK_HOME/var/log/watchdog/watchdog.log*	Constant Value	Automatic	_internal	0	system	Enabled | Disable	
$SPLUNK_HOME/var/run/splunk/search_telemetry/*search_telemetry.json	Constant Value	search_telemetry	_introspection	0	system	Enabled | Disable	
$SPLUNK_HOME/var/spool/splunk	Constant Value	Automatic	default		system	Disabled | Enable	
$SPLUNK_HOME/var/spool/splunk/...stash_hec	Constant Value	stash_hec	default		system	Disabled | Enable	
$SPLUNK_HOME/var/spool/splunk/...stash_new	Constant Value	stash_new	default		system	Disabled | Enable	
$SPLUNK_HOME/var/spool/splunk/tracker.log*	Constant Value	splunkd_latency_tracker	_internal	0	system	Enabled | Disable	
/var/log/suricata/eve.json	Constant Value	_json	default	1	search	Enabled | Disable	Delete

- **Install Splunk Forwarder:**

Set the receiver IP as 192.168.1.9 and port 9997



Receive data

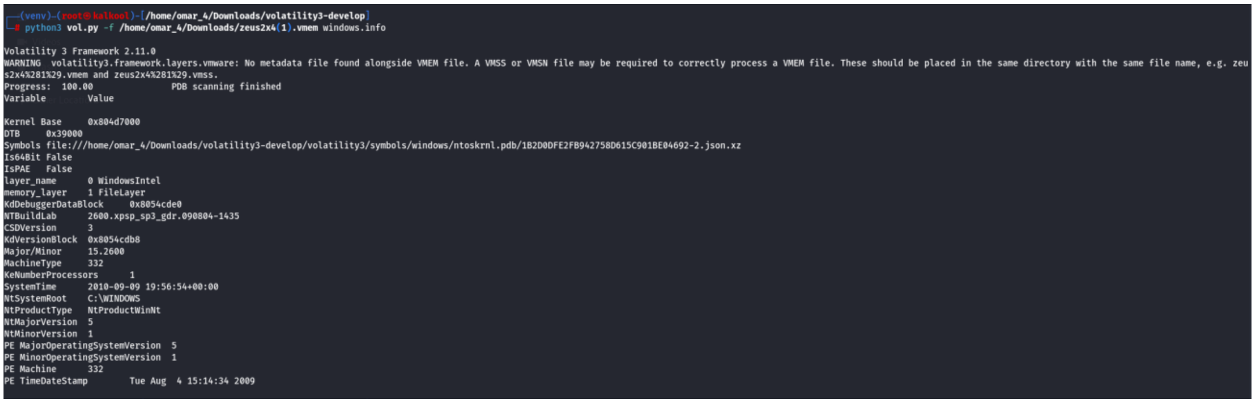
Forwarding and receiving » Receive data

Showing 1-1 of 1 item

Listen on this port	Status	Actions
9997	Enabled | Disable	Delete

3] Analyze Memory with Volatility

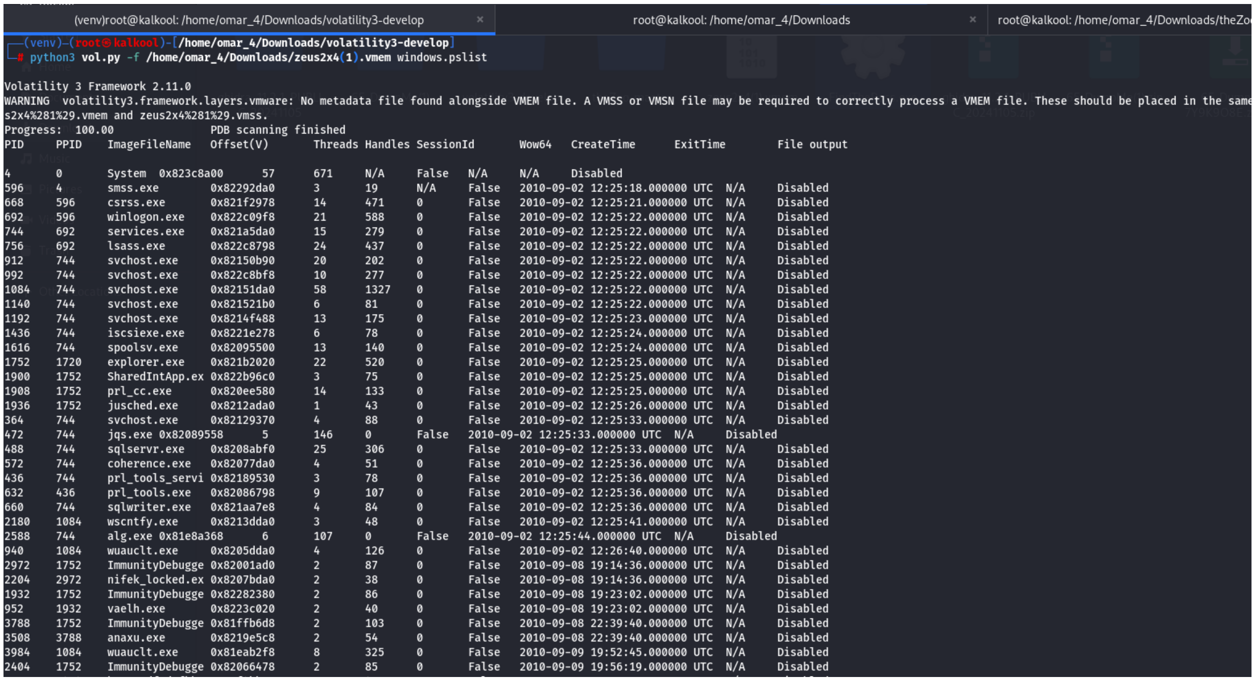
1- identify the OS and version of the memory dump



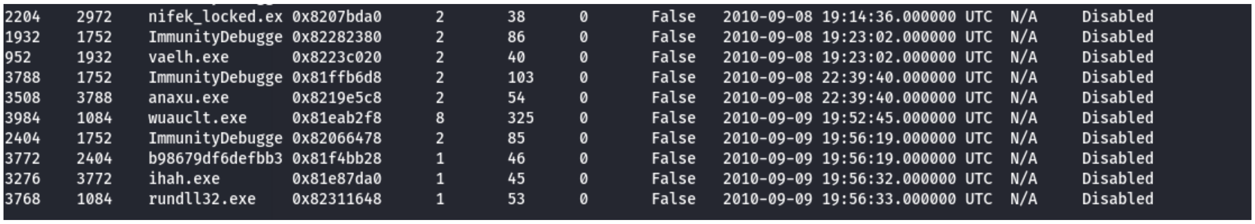
```
┌──(venv)─(root㉿kalkool)-[/home/omar_4/Downloads/volatility3-develop]
└─# python3 vol.py -f /home/omar_4/Downloads/zeus2x4(1).vmem windows.info

Volatility 3 Framework 2.11.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. zeu
s2x4%281%29.vmem and zeus2x4%281%29.vmss.
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0x804d7000
DTB     0x39000
Symbols file:///home/omar_4/Downloads/volatility3-develop/volatility3/symbols/windows/ntoskrnl.pdb/1B2D0DFE2FB942758D615C901BE04692-2.json.xz
Is64Bit False
IsPAE   False
layer_name      0 WindowsIntel
memory_layer    1 FileLayer
KdDebuggerDataBlock     0x8054cde0
NTBuildLab      2600.xpsp_sp3_gdr.090804-1435
CSDVersion      3
KdVersionBlock  0x8054cdb8
Major/Minor     15.2600
MachineType     332
KeNumberProcessors      1
SystemTime      2010-09-09 19:56:54+00:00
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  5
NtMinorVersion  1
PE MajorOperatingSystemVersion  5
PE MinorOperatingSystemVersion  1
PE Machine      332
PE TimeDateStamp        Tue Aug  4 15:14:34 2009
```

2- Identify active processes

(a list of processes running at the time of the memory capture)

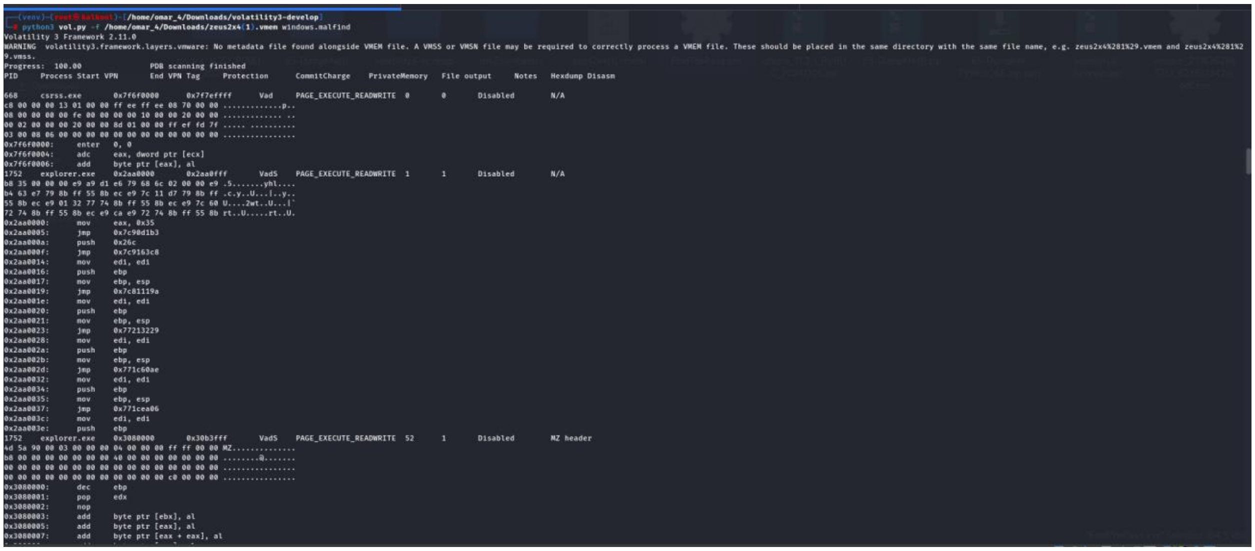

(venv)root@kalkool: /home/omar_4/Downloads/volatility3-develop
root@kalkool: /home/omar_4/Downloads
root@kalkool: /home/omar_4/Downloads/theZo

```
┌──(venv)─(root㉿kalkool)-[/home/omar_4/Downloads/volatility3-develop]
└─# python3 vol.py -f /home/omar_4/Downloads/zeus2x4(1).vmem windows.pslist

Volatility 3 Framework 2.11.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same
s2x4%281%29.vmem and zeus2x4%281%29.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x823c8a00      57      671     N/A     False   N/A     N/A     Disabled
596     4       smss.exe        0x82292da0      3       19      N/A     False   2010-09-02 12:25:18.000000 UTC  N/A     Disabled
668     596     csrss.exe       0x821f2978      14      471     0       False   2010-09-02 12:25:21.000000 UTC  N/A     Disabled
692     596     winlogon.exe    0x822c09f8      21      588     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
744     692     services.exe    0x821a5da0      15      279     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
756     692     lsass.exe       0x822c8798      24      437     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
912     744     svchost.exe     0x82150b90      20      202     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
992     744     svchost.exe     0x822c8bf8      10      277     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
1084    744     svchost.exe     0x82151da0      58      1327    0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
1140    744     svchost.exe     0x821521b0      6       81      0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
1192    744     svchost.exe     0x8214f488      13      175     0       False   2010-09-02 12:25:23.000000 UTC  N/A     Disabled
1436    744     iscsiexe.exe    0x8221e278      6       78      0       False   2010-09-02 12:25:24.000000 UTC  N/A     Disabled
1616    744     spoolsv.exe     0x82095500      13      140     0       False   2010-09-02 12:25:24.000000 UTC  N/A     Disabled
1752    1720    explorer.exe    0x821b2020      22      520     0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
1900    1752    SharedIntApp.ex 0x822b96c0      3       75      0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
1908    1752    prl_cc.exe      0x820ee580      14      133     0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
1936    1752    jusched.exe     0x8212ada0      1       43      0       False   2010-09-02 12:25:26.000000 UTC  N/A     Disabled
364     744     svchost.exe     0x82129370      4       88      0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
472     744     jqs.exe 0x82089558      5       146     0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
488     744     sqlservr.exe    0x8208abf0      25      306     0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
572     744     coherence.exe   0x82077da0      4       51      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
436     744     prl_tools_servi 0x82189530      3       78      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
632     436     prl_tools.exe   0x82086798      9       107     0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
660     744     sqlwriter.exe   0x821aa7e8      4       84      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
2180    1084    wscntfy.exe     0x8213dda0      3       48      0       False   2010-09-02 12:25:41.000000 UTC  N/A     Disabled
2588    744     alg.exe 0x81e8a368      6       107     0       False   2010-09-02 12:25:44.000000 UTC  N/A     Disabled
940     1084    wuauclt.exe     0x8205dda0      4       126     0       False   2010-09-02 12:26:40.000000 UTC  N/A     Disabled
2972    1752    ImmunityDebugge 0x82001ad0      2       87      0       False   2010-09-08 19:14:36.000000 UTC  N/A     Disabled
2204    2972    nifek_locked.ex 0x8207bda0      2       38      0       False   2010-09-08 19:14:36.000000 UTC  N/A     Disabled
1932    1752    ImmunityDebugge 0x82282380      2       86      0       False   2010-09-08 19:23:02.000000 UTC  N/A     Disabled
952     1932    vaelh.exe       0x8223c020      2       40      0       False   2010-09-08 19:23:02.000000 UTC  N/A     Disabled
3788    1752    ImmunityDebugge 0x81ffb6d8      2       103     0       False   2010-09-08 22:39:40.000000 UTC  N/A     Disabled
3508    3788    anaxu.exe       0x8219e5c8      2       54      0       False   2010-09-08 22:39:40.000000 UTC  N/A     Disabled
3984    1084    wuauclt.exe     0x81eab2f8      8       325     0       False   2010-09-09 19:52:45.000000 UTC  N/A     Disabled
2404    1752    ImmunityDebugge 0x82066478      2       85      0       False   2010-09-09 19:56:19.000000 UTC  N/A     Disabled
```



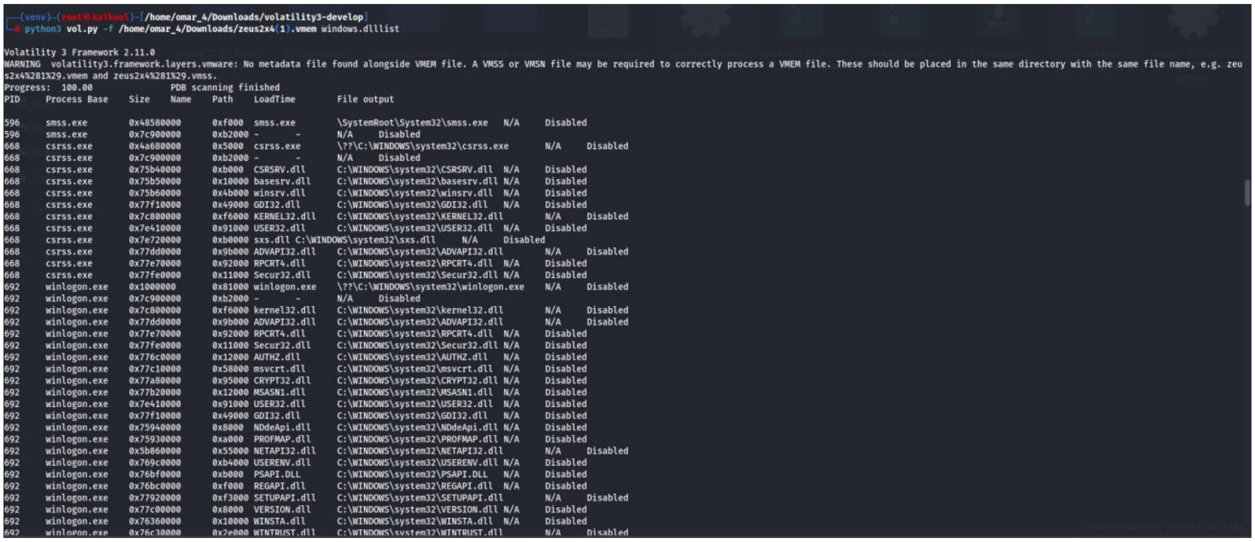
```
2204    2972    nifek_locked.ex 0x8207bda0      2       38      0       False   2010-09-08 19:14:36.000000 UTC  N/A     Disabled
1932    1752    ImmunityDebugge 0x82282380      2       86      0       False   2010-09-08 19:23:02.000000 UTC  N/A     Disabled
952     1932    vaelh.exe       0x8223c020      2       40      0       False   2010-09-08 19:23:02.000000 UTC  N/A     Disabled
3788    1752    ImmunityDebugge 0x81ffb6d8      2       103     0       False   2010-09-08 22:39:40.000000 UTC  N/A     Disabled
3508    3788    anaxu.exe       0x8219e5c8      2       54      0       False   2010-09-08 22:39:40.000000 UTC  N/A     Disabled
3984    1084    wuauclt.exe     0x81eab2f8      8       325     0       False   2010-09-09 19:52:45.000000 UTC  N/A     Disabled
2404    1752    ImmunityDebugge 0x82066478      2       85      0       False   2010-09-09 19:56:19.000000 UTC  N/A     Disabled
3772    2404    b98679df6defbb3 0x81f4bb28      1       46      0       False   2010-09-09 19:56:19.000000 UTC  N/A     Disabled
3276    3772    ihah.exe        0x81e87da0      1       45      0       False   2010-09-09 19:56:32.000000 UTC  N/A     Disabled
3768    1084    rundll32.exe    0x82311648      1       53      0       False   2010-09-09 19:56:33.000000 UTC  N/A     Disabled
```

3- identify potentially injected or hidden processes



```
┌──(venv)─(root㉿kalkool)-[/home/omar_4/Downloads/volatility3-develop]
└─# python3 vol.py -f /home/omar_4/Downloads/zeus2x4(1).vmem windows.malfind
Volatility 3 Framework 2.11.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. zeus2x4%281%29.vmem and zeus2x4%281%2
9.vmss.
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm

668     csrss.exe       0x7f6f0000      0x7f7effff      Vad     PAGE_EXECUTE_READWRITE  0       0       Disabled        N/A
c8 00 00 00 13 01 00 00 ff ee ff ee 08 70 00 00 .............p..
08 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00 ............. ..
00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f ..... ..........
03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x7f6f0000:     enter   0, 0
0x7f6f0004:     adc     eax, dword ptr [ecx]
0x7f6f0006:     add     byte ptr [eax], al
1752    explorer.exe    0x2aa0000       0x2aa0fff       VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled        N/A
b8 35 00 00 00 e9 a9 d1 e6 79 68 6c 02 00 00 e9 .5.......yhl....
b4 63 e7 79 8b ff 55 8b ec e9 7c 11 d7 79 8b ff .c.y..U...|..y..
55 8b ec e9 01 32 77 74 8b ff 55 8b ec e9 7c 60 U....2wt..U...|`
72 74 8b ff 55 8b ec e9 ca e9 72 74 8b ff 55 8b rt..U.....rt..U.
0x2aa0000:      mov     eax, 0x35
0x2aa0005:      jmp     0x7c90d1b3
0x2aa000a:      push    0x26c
0x2aa000f:      jmp     0x7c9163c8
0x2aa0014:      mov     edi, edi
0x2aa0016:      push    ebp
0x2aa0017:      mov     ebp, esp
0x2aa0019:      jmp     0x7c81119a
0x2aa001e:      mov     edi, edi
0x2aa0020:      push    ebp
0x2aa0021:      mov     ebp, esp
0x2aa0023:      jmp     0x77213229
0x2aa0028:      mov     edi, edi
0x2aa002a:      push    ebp
0x2aa002b:      mov     ebp, esp
0x2aa002d:      jmp     0x771c60ae
0x2aa0032:      mov     edi, edi
0x2aa0034:      push    ebp
0x2aa0035:      mov     ebp, esp
0x2aa0037:      jmp     0x771cea06
0x2aa003c:      mov     edi, edi
0x2aa003e:      push    ebp
1752    explorer.exe    0x3080000       0x30b3fff       VadS    PAGE_EXECUTE_READWRITE  52      1       Disabled        MZ header
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 ................
0x3080000:      dec     ebp
0x3080001:      pop     edx
0x3080002:      nop
0x3080003:      add     byte ptr [ebx], al
0x3080005:      add     byte ptr [eax], al
0x3080007:      add     byte ptr [eax + eax], al
```

4- Analyze the DLLs loaded by a suspicious process

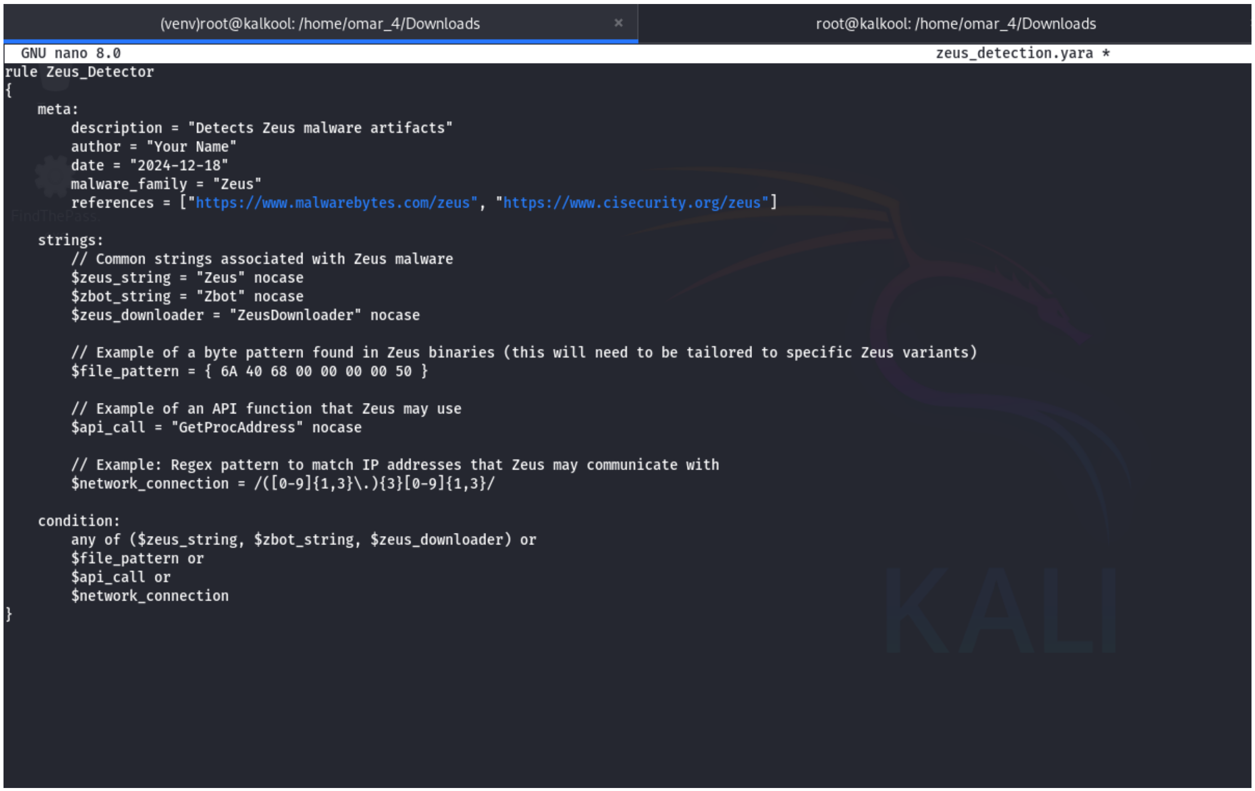


```
┌──(venv)─(root㉿kalkool)-[/home/omar_4/Downloads/volatility3-develop]
└─# python3 vol.py -f /home/omar_4/Downloads/zeus2x4(1).vmem windows.dlllist

Volatility 3 Framework 2.11.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. zeu
s2x4%281%29.vmem and zeus2x4%281%29.vmss.
Progress:  100.00               PDB scanning finished
PID     Process Base    Size    Name    Path    LoadTime        File output

596     smss.exe        0x48580000      0xf000  smss.exe        \SystemRoot\System32\smss.exe   N/A     Disabled
596     smss.exe        0x7c900000      0xb2000 -       -       N/A     Disabled
668     csrss.exe       0x4a680000      0x5000  csrss.exe       \??\C:\WINDOWS\system32\csrss.exe       N/A     Disabled
668     csrss.exe       0x7c900000      0xb2000 -       -       N/A     Disabled
668     csrss.exe       0x75b40000      0xb000  CSRSRV.dll      C:\WINDOWS\system32\CSRSRV.dll  N/A     Disabled
668     csrss.exe       0x75b50000      0x10000 basesrv.dll     C:\WINDOWS\system32\basesrv.dll N/A     Disabled
668     csrss.exe       0x75b60000      0x4b000 winsrv.dll      C:\WINDOWS\system32\winsrv.dll  N/A     Disabled
668     csrss.exe       0x77f10000      0x49000 GDI32.dll       C:\WINDOWS\system32\GDI32.dll   N/A     Disabled
668     csrss.exe       0x7c800000      0xf6000 KERNEL32.dll    C:\WINDOWS\system32\KERNEL32.dll        N/A     Disabled
668     csrss.exe       0x7e410000      0x91000 USER32.dll      C:\WINDOWS\system32\USER32.dll  N/A     Disabled
668     csrss.exe       0x7e720000      0xb0000 sxs.dll C:\WINDOWS\system32\sxs.dll     N/A     Disabled
668     csrss.exe       0x77dd0000      0x9b000 ADVAPI32.dll    C:\WINDOWS\system32\ADVAPI32.dll        N/A     Disabled
668     csrss.exe       0x77e70000      0x92000 RPCRT4.dll      C:\WINDOWS\system32\RPCRT4.dll  N/A     Disabled
668     csrss.exe       0x77fe0000      0x11000 Secur32.dll     C:\WINDOWS\system32\Secur32.dll N/A     Disabled
692     winlogon.exe    0x1000000       0x81000 winlogon.exe    \??\C:\WINDOWS\system32\winlogon.exe    N/A     Disabled
692     winlogon.exe    0x7c900000      0xb2000 -       -       N/A     Disabled
692     winlogon.exe    0x7c800000      0xf6000 kernel32.dll    C:\WINDOWS\system32\kernel32.dll        N/A     Disabled
692     winlogon.exe    0x77dd0000      0x9b000 ADVAPI32.dll    C:\WINDOWS\system32\ADVAPI32.dll        N/A     Disabled
692     winlogon.exe    0x77e70000      0x92000 RPCRT4.dll      C:\WINDOWS\system32\RPCRT4.dll  N/A     Disabled
692     winlogon.exe    0x77fe0000      0x11000 Secur32.dll     C:\WINDOWS\system32\Secur32.dll N/A     Disabled
692     winlogon.exe    0x776c0000      0x12000 AUTHZ.dll       C:\WINDOWS\system32\AUTHZ.dll   N/A     Disabled
692     winlogon.exe    0x77c10000      0x58000 msvcrt.dll      C:\WINDOWS\system32\msvcrt.dll  N/A     Disabled
692     winlogon.exe    0x77a80000      0x95000 CRYPT32.dll     C:\WINDOWS\system32\CRYPT32.dll N/A     Disabled
692     winlogon.exe    0x77b20000      0x12000 MSASN1.dll      C:\WINDOWS\system32\MSASN1.dll  N/A     Disabled
692     winlogon.exe    0x7e410000      0x91000 USER32.dll      C:\WINDOWS\system32\USER32.dll  N/A     Disabled
692     winlogon.exe    0x77f10000      0x49000 GDI32.dll       C:\WINDOWS\system32\GDI32.dll   N/A     Disabled
692     winlogon.exe    0x75940000      0x8000  NDdeApi.dll     C:\WINDOWS\system32\NDdeApi.dll N/A     Disabled
692     winlogon.exe    0x75930000      0xa000  PROFMAP.dll     C:\WINDOWS\system32\PROFMAP.dll N/A     Disabled
692     winlogon.exe    0x5b860000      0x55000 NETAPI32.dll    C:\WINDOWS\system32\NETAPI32.dll        N/A     Disabled
692     winlogon.exe    0x769c0000      0xb4000 USERENV.dll     C:\WINDOWS\system32\USERENV.dll N/A     Disabled
692     winlogon.exe    0x76bf0000      0xb000  PSAPI.DLL       C:\WINDOWS\system32\PSAPI.DLL   N/A     Disabled
692     winlogon.exe    0x76bc0000      0xf000  REGAPI.dll      C:\WINDOWS\system32\REGAPI.dll  N/A     Disabled
692     winlogon.exe    0x77920000      0xf3000 SETUPAPI.dll    C:\WINDOWS\system32\SETUPAPI.dll        N/A     Disabled
692     winlogon.exe    0x77c00000      0x8000  VERSION.dll     C:\WINDOWS\system32\VERSION.dll N/A     Disabled
692     winlogon.exe    0x76360000      0x10000 WINSTA.dll      C:\WINDOWS\system32\WINSTA.dll  N/A     Disabled
692     winlogon.exe    0x76c30000      0x2e000 WINTRUST.dll    C:\WINDOWS\system32\WINTRUST.dll        N/A     Disabled
```

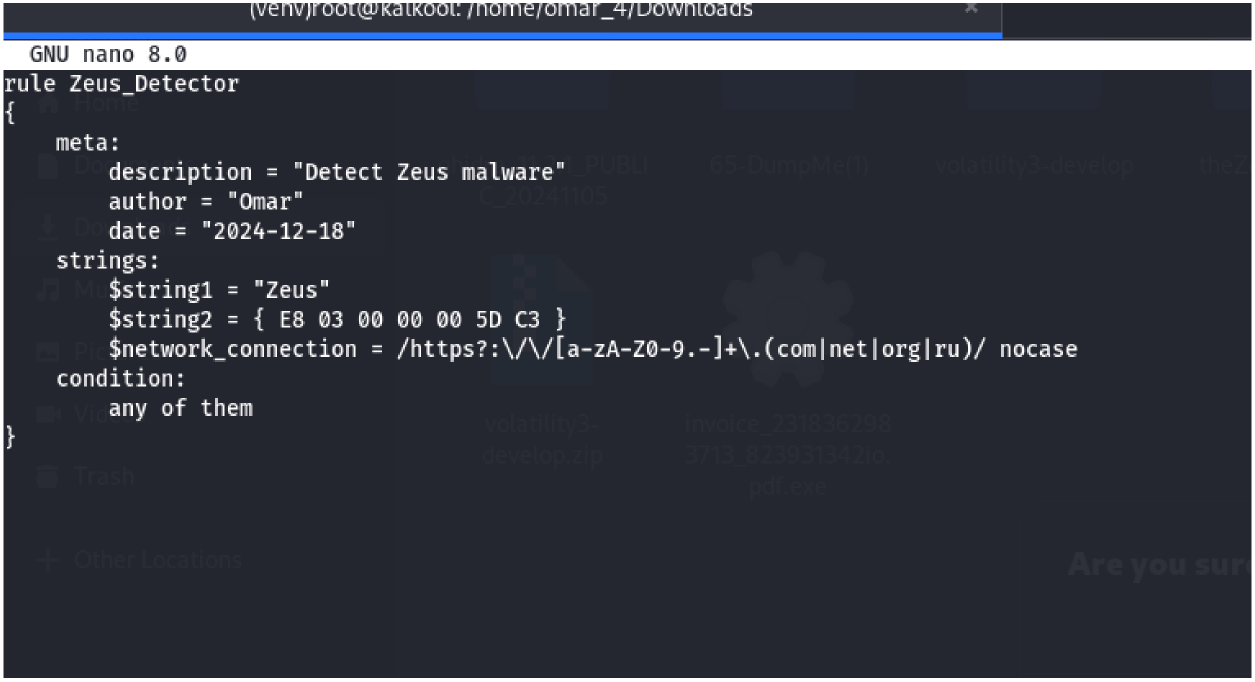
4] Detect Zeus with YARA Signatures

1- Yara Rules :

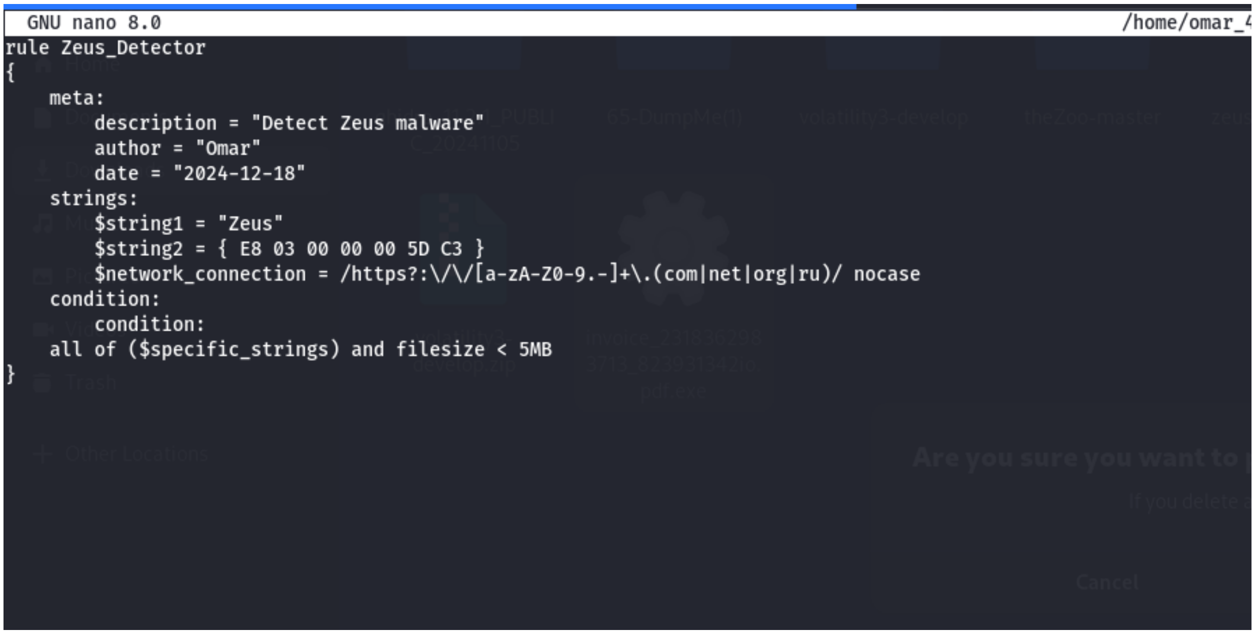
Rule Name: Zeus_Detector


(venv)root@kalkool: /home/omar_4/Downloads
root@kalkool: /home/omar_4/Downloads
GNU nano 8.0
zeus_detection.yara *

```
rule Zeus_Detector
{
    meta:
        description = "Detects Zeus malware artifacts"
        author = "Your Name"
        date = "2024-12-18"
        malware_family = "Zeus"
        references = ["https://www.malwarebytes.com/zeus", "https://www.cisecurity.org/zeus"]

    strings:
        // Common strings associated with Zeus malware
        $zeus_string = "Zeus" nocase
        $zbot_string = "Zbot" nocase
        $zeus_downloader = "ZeusDownloader" nocase

        // Example of a byte pattern found in Zeus binaries (this will need to be tailored to specific Zeus variants)
        $file_pattern = { 6A 40 68 00 00 00 00 50 }

        // Example of an API function that Zeus may use
        $api_call = "GetProcAddress" nocase

        // Example: Regex pattern to match IP addresses that Zeus may communicate with
        $network_connection = /([0-9]{1,3}\.){3}[0-9]{1,3}/

    condition:
        any of ($zeus_string, $zbot_string, $zeus_downloader) or
        $file_pattern or
        $api_call or
        $network_connection
}
```



```
rule Zeus_Detector
{
   meta:
      description = "Detect Zeus malware"
      author = "Omar"
      date = "2024-12-18"
   strings:
      $string1 = "Zeus"
      $string2 = { E8 03 00 00 00 5D C3 }
      $network_connection = /https?:\/\/[a-zA-Z0-9.-]+\.(com|net|org|ru)/ nocase
   condition:
      any of them
}
```

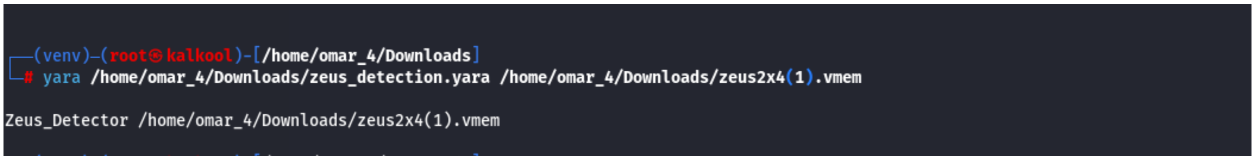


```
  GNU nano 8.0                                                                          /home/omar_4
rule Zeus_Detector
{
    meta:
        description = "Detect Zeus malware"
        author = "Omar"
        date = "2024-12-18"
    strings:
        $string1 = "Zeus"
        $string2 = { E8 03 00 00 00 5D C3 }
        $network_connection = /https?:\/\/[a-zA-Z0-9.-]+\.(com|net|org|ru)/ nocase
    condition:
        condition:
    all of ($specific_strings) and filesize < 5MB
}
```

2- Testing memory dump

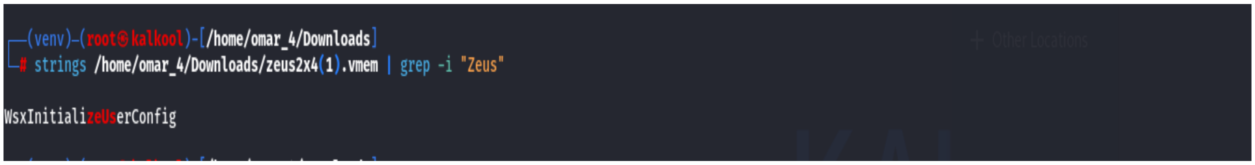
Matches:

rule matched content in the file



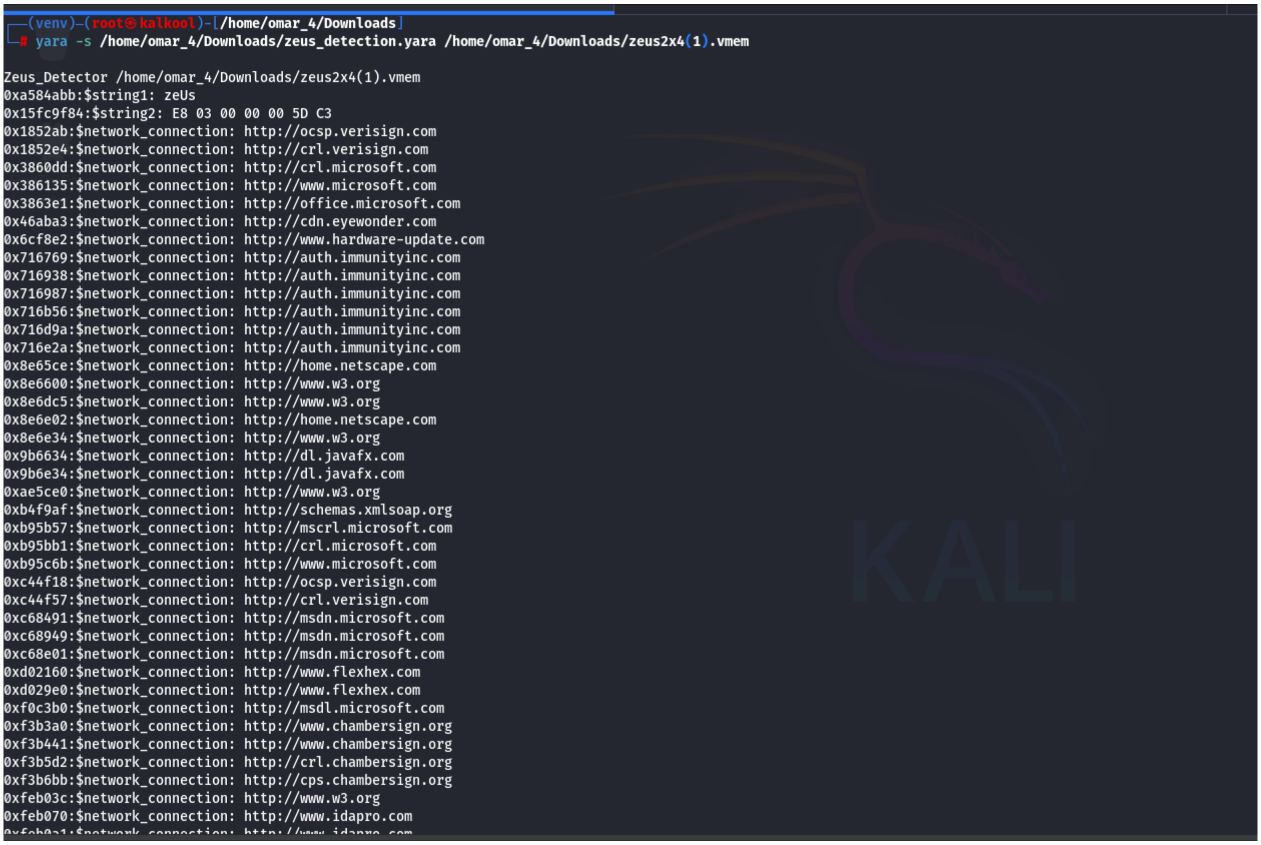
```
┌──(venv)─(root㉿kalkool)-[/home/omar_4/Downloads]
└─# yara /home/omar_4/Downloads/zeus_detection.yara /home/omar_4/Downloads/zeus2x4(1).vmem

Zeus_Detector /home/omar_4/Downloads/zeus2x4(1).vmem
```

3- Running strings with a filter for "Zeus"



```
┌──(venv)─(root㉿kalkool)-[/home/omar_4/Downloads]
└─# strings /home/omar_4/Downloads/zeus2x4(1).vmem | grep -i "Zeus"

WsxInitializeUserConfig
```

4- Matching strings for each rule.



```
┌──(venv)─(root㉿kalkool)-[/home/omar_4/Downloads]
└─# yara -s /home/omar_4/Downloads/zeus_detection.yara /home/omar_4/Downloads/zeus2x4(1).vmem

Zeus_Detector /home/omar_4/Downloads/zeus2x4(1).vmem
0xa584abb:$string1: zeUs
0x15fc9f84:$string2: E8 03 00 00 00 5D C3
0x1852ab:$network_connection: http://ocsp.verisign.com
0x1852e4:$network_connection: http://crl.verisign.com
0x3860dd:$network_connection: http://crl.microsoft.com
0x386135:$network_connection: http://www.microsoft.com
0x3863e1:$network_connection: http://office.microsoft.com
0x46aba3:$network_connection: http://cdn.eyewonder.com
0x6cf8e2:$network_connection: http://www.hardware-update.com
0x716769:$network_connection: http://auth.immunityinc.com
0x716938:$network_connection: http://auth.immunityinc.com
0x716987:$network_connection: http://auth.immunityinc.com
0x716b56:$network_connection: http://auth.immunityinc.com
0x716d9a:$network_connection: http://auth.immunityinc.com
0x716e2a:$network_connection: http://auth.immunityinc.com
0x8e65ce:$network_connection: http://home.netscape.com
0x8e6600:$network_connection: http://www.w3.org
0x8e6dc5:$network_connection: http://www.w3.org
0x8e6e02:$network_connection: http://home.netscape.com
0x8e6e34:$network_connection: http://www.w3.org
0x9b6634:$network_connection: http://dl.javafx.com
0x9b6e34:$network_connection: http://dl.javafx.com
0xae5ce0:$network_connection: http://www.w3.org
0xb4f9af:$network_connection: http://schemas.xmlsoap.org
0xb95b57:$network_connection: http://mscrl.microsoft.com
0xb95bb1:$network_connection: http://crl.microsoft.com
0xb95c6b:$network_connection: http://www.microsoft.com
0xc44f18:$network_connection: http://ocsp.verisign.com
0xc44f57:$network_connection: http://crl.verisign.com
0xc68491:$network_connection: http://msdn.microsoft.com
0xc68949:$network_connection: http://msdn.microsoft.com
0xc68e01:$network_connection: http://msdn.microsoft.com
0xd02160:$network_connection: http://www.flexhex.com
0xd029e0:$network_connection: http://www.flexhex.com
0xf0c3b0:$network_connection: http://msdl.microsoft.com
0xf3b3a0:$network_connection: http://www.chambersign.org
0xf3b441:$network_connection: http://www.chambersign.org
0xf3b5d2:$network_connection: http://crl.chambersign.org
0xf3b6bb:$network_connection: http://cps.chambersign.org
0xfeb03c:$network_connection: http://www.w3.org
0xfeb070:$network_connection: http://www.idapro.com
0xfeb0a1:$network_connection: http://www.idapro.com
```