

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training



Co-funded by
the European Union

Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training



Co-funded by
the European Union

Acknowledgement

- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Network Protection for Energy Control Systems

These slides outline the essential offensive tools that will be used in this course.

These tools are intended for use within this course to demonstrate how different tools can be employed for various cyberattack activities and address existing security weaknesses to avoid or mitigate related cyber risks. Therefore, all these practical activities are solely intended for educational purposes ONLY and not for any other malicious or unauthorized activities.

Detection of Cyberattacks

Detection of Cyberattacks

- Detecting ARP Poisoning Attacks on the network
- We consider the Windows machine to act as a network administration machine within the network. If any suspicious activities are occurring on the network, the network administrator should detect them. How?

On the windows machine

Arp -a

Before

```

Command Prompt
Interface: 192.168.122.21 --- 0x4
Internet Address    Physical Address    Type
192.168.122.1      52-54-00-1f-18-ec  dynamic
192.168.122.103    08-00-27-30-20-e0  dynamic
192.168.122.255    ff-ff-ff-ff-ff-ff  static
224.0.0.22         01-00-5e-00-00-16  static
224.0.0.251        01-00-5e-00-00-fb  static
224.0.0.252        01-00-5e-00-00-fc  static
239.255.255.250    01-00-5e-7f-ff-fa  static
255.255.255.255    ff-ff-ff-ff-ff-ff  static
  
```

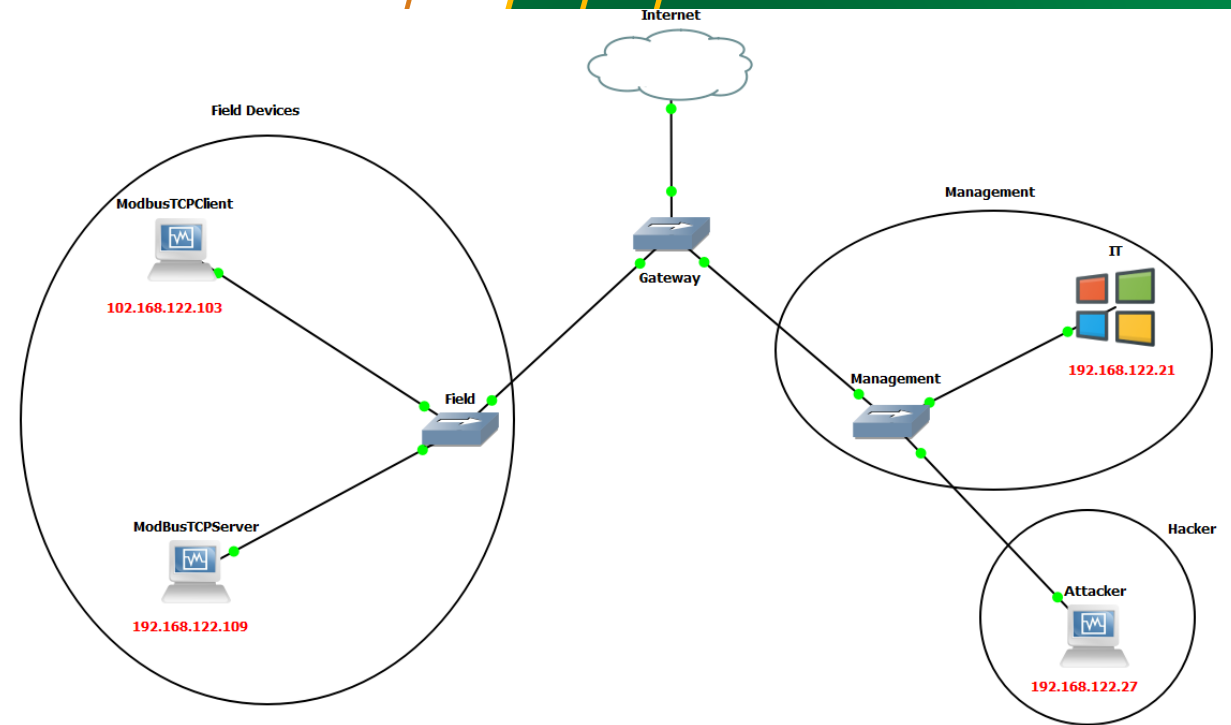
C:\Users\User>arp -a

After

```

Command Prompt
Interface: 192.168.122.21 --- 0x4
Internet Address    Physical Address    Type
192.168.122.1      08-00-27-27-29-8c  dynamic
192.168.122.27     08-00-27-27-29-8c  dynamic
192.168.122.103    08-00-27-30-20-e0  dynamic
192.168.122.255    ff-ff-ff-ff-ff-ff  static
224.0.0.22         01-00-5e-00-00-16  static
224.0.0.251        01-00-5e-00-00-fb  static
224.0.0.252        01-00-5e-00-00-fc  static
239.255.255.250    01-00-5e-7f-ff-fa  static
255.255.255.255    ff-ff-ff-ff-ff-ff  static
  
```

C:\Users\User>



Detection of Cyberattacks

ARP Poisoning Attacks

- The "arp -a" command should be executed manually every time to detect such suspicious activities.
- The xarp tool can automatically detect any such activities.

Before

XArp - unregistered version
File XArp Professional Help
Status: no ARP attacks
Security level set to: basic

IP	MAC	Host	Vendor	Interface	Online	Cache	First seen
192.168.122.1	52-54-00-1f-18-ec	gns3vm	Realtek (uptec...	0x4 - Intel(R) P...	unkno...	yes	4/3/2024 09:42
192.168.122.21	08-00-27-ab-32-d8	WinDev2401Eval	Cadmus Com...	0x4 - Intel(R) P...	unkno...	no	4/3/2024 09:42
192.168.122.27	08-00-27-27-29-8c	kali	Cadmus Com...	0x4 - Intel(R) P...	unkno...	yes	4/3/2024 09:42
192.168.122.103	08-00-27-30-20-e0	192.168.122.103	Cadmus Com...	0x4 - Intel(R) P...	unkno...	yes	4/3/2024 09:42
192.168.122.109	08-00-27-52-a4-8f	raspberrypi	Cadmus Com...	0x4 - Intel(R) P...	unkno...	no	4/3/2024 09:42

XArp 2.2.2 - 5 mappings - 1 interface - 0 alerts

After

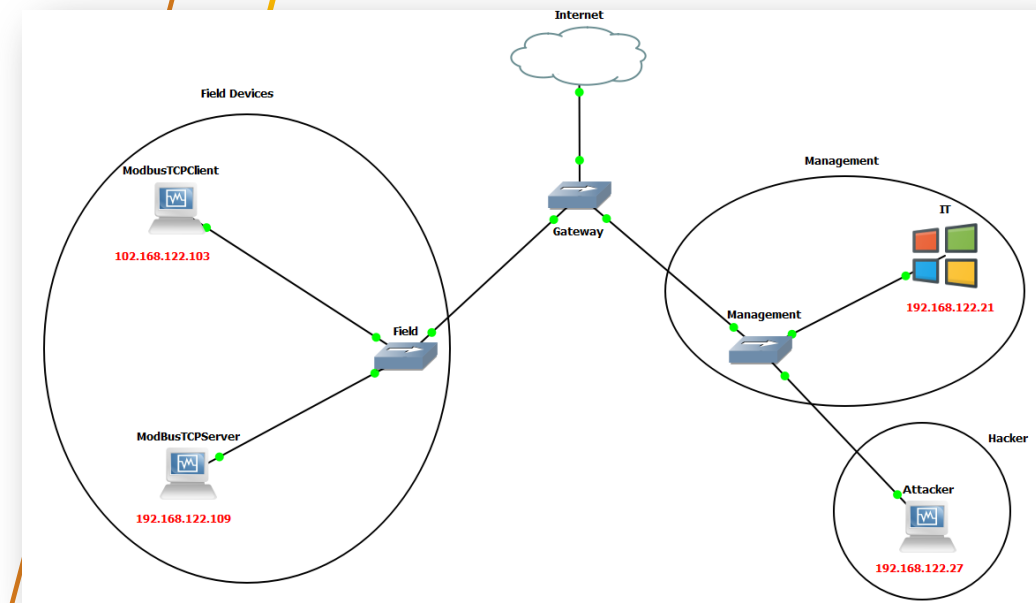
Windows 11 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
XArp - unregistered version
File XArp Professional Help
Status: ARP attacks detected!
Security level set to: basic

IP	MAC	Host	Vendor	Interface	Online	Cache	First seen
192.168.122.1	52-54-00-1f-18-ec	gns3vm	Realtek (uptec...	0x4 - Intel(R) P...	unkno...	no	4/3/2024 09:42
192.168.122.21	08-00-27-ab-32-d8	WinDev2401Eval	Cadmus Com...	0x4 - Intel(R) P...	unkno...	no	4/3/2024 09:42
192.168.122.27	08-00-27-27-29-8c	kali	Cadmus Com...	0x4 - Intel(R) P...	unkno...	yes	4/3/2024 09:42
192.168.122.103	08-00-27-30-20-e0	192.168.122.103	Cadmus Com...	0x4 - Intel(R) P...	unkno...	yes	4/3/2024 09:42
192.168.122.109	08-00-27-27-29-8c	raspberrypi	Cadmus Com...	0x4 - Intel(R) P...	unkno...	yes	4/3/2024 09:42

Alert 1 of 10
4/3/2024 09:44:26
ChangeFilter: MAC address for IP: 192.168.122.1 changed from 52-54-00-1f-18-ec to 08-00-27-27-29-8c

Interface : 0x4
(ethzerns)
source mac: 08-00-27-27-29-8c
dest mac: 08-00-27-52-a4-8f
type: 0x806
(arp)
direction: in
type: reply
source ip: 192.168.122.1
dest ip: 192.168.122.109
source mac: 08-00-27-27-29-8c
dest mac: 08-00-27-52-a4-8f

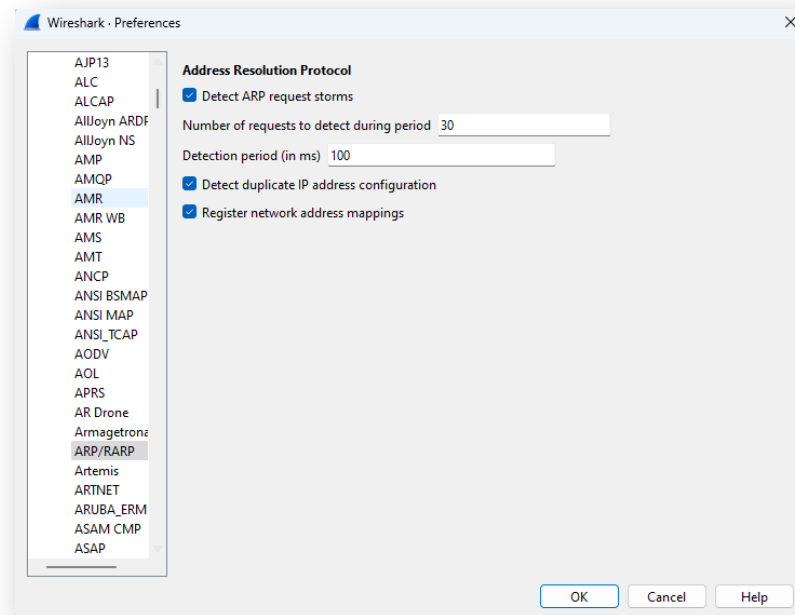
XArp 2.2.2 - 5 mappings - 1 interface - 10 alerts



Detection of Cyberattacks

Detecting suspicious Activities In The Network using Wireshark

- Run wireshark on windows device, and let the tool detect an ARP request packets through the network.
- To do so, do the following:
 - Select preferences from Edit, then select Protocols → ARP/RARP
 - Keep the “Detect ARP request storms” selected. Then press ok

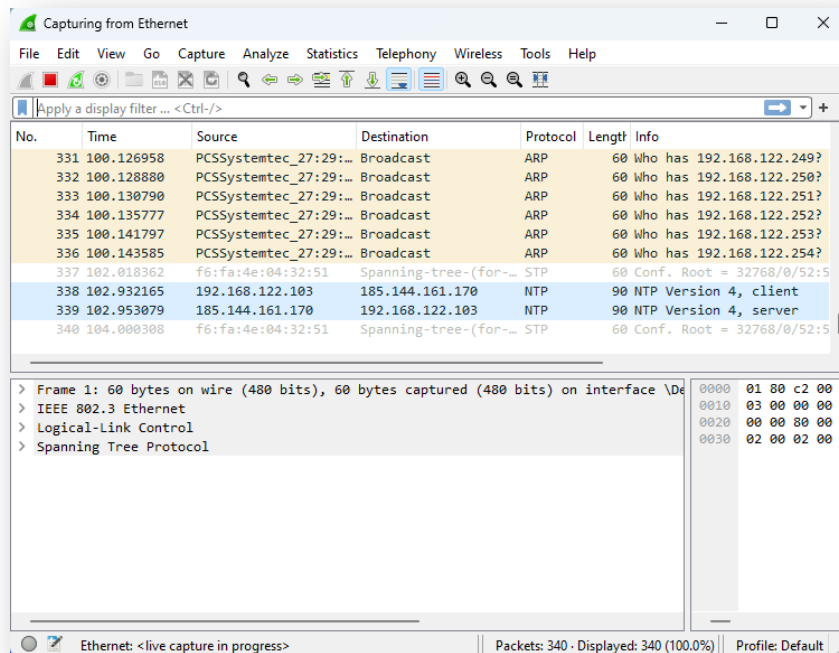


Detection of Cyberattacks

Detecting suspicious Activities In The Network using Wireshark

- Run the Wireshark tool using the proper connection.
- In order to test the ARP poisoning attack, we will start discovering the connected devices on the network using the netdiscover command on the kali linux

Netdiscover -i eth0 -r 192.168.122.1/24



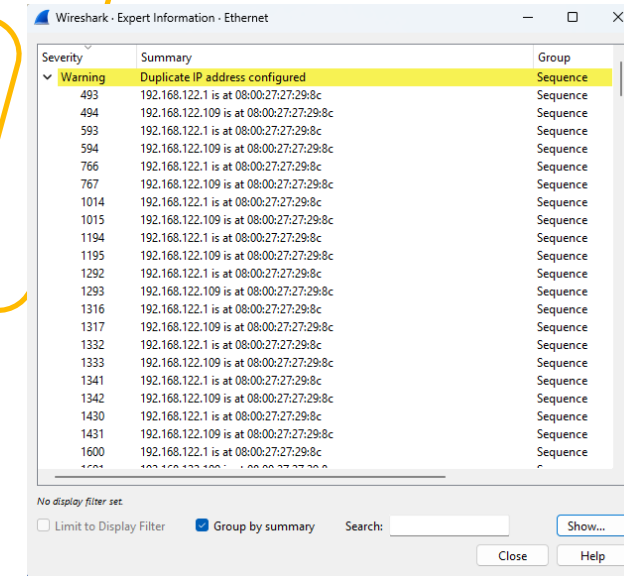
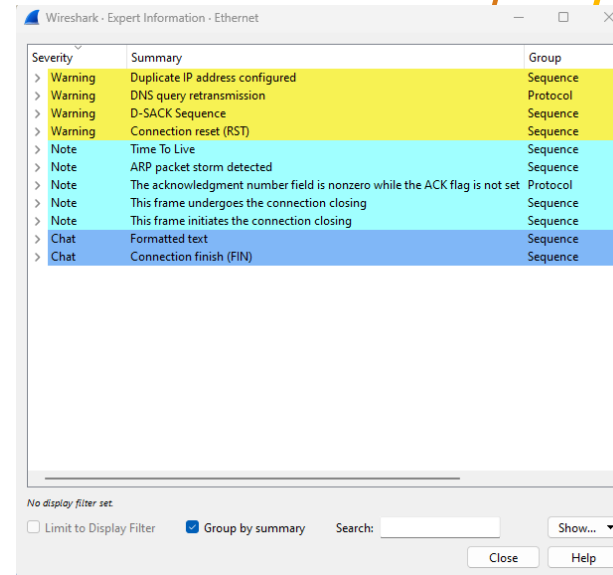
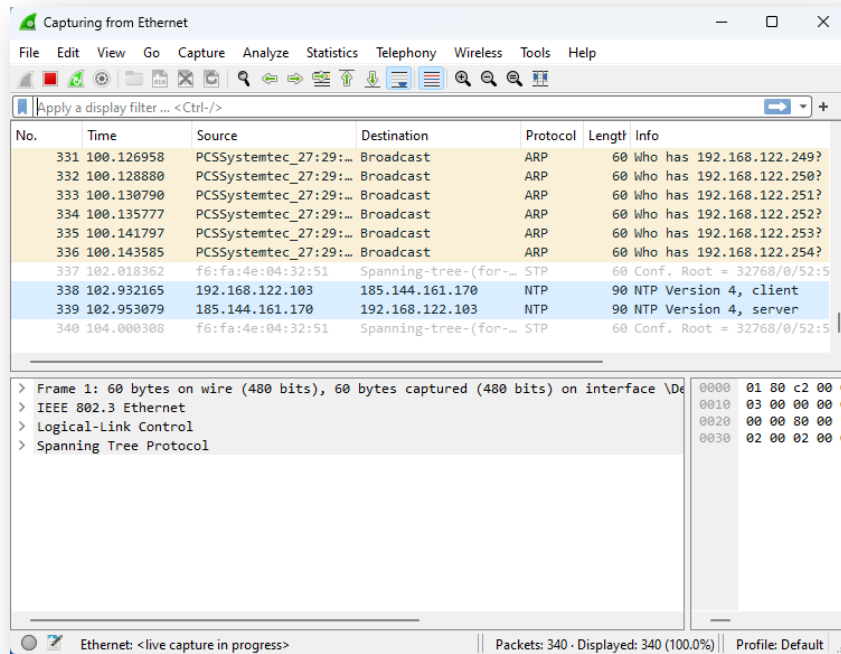
Wireshark start detecting ARP request over the network

Detection of Cyberattacks

Detecting suspicious Activities In The Network using Wireshark

- Run the arp spoofing attack using any of the previously discussed too (bettercap or arpspoof)

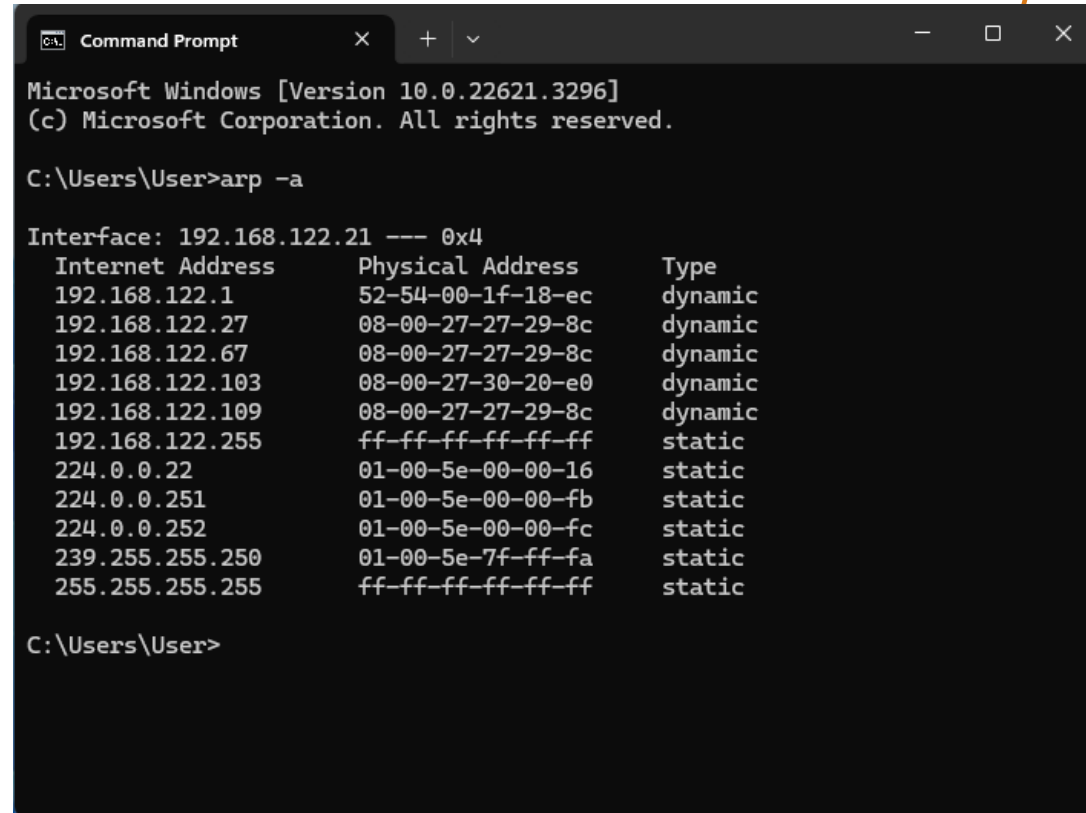
Bettercap `-iface eth0 -caplet spoof.cap`



Wireshark start detecting ARP poisoning request over the network. Formore analysis, select Expert Infromation from the Analyze Menue

Prevention of ARP Poisoning Attack

Prevention of ARP Poisoning Attack



```
Command Prompt
Microsoft Windows [Version 10.0.22621.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>arp -a

Interface: 192.168.122.21 --- 0x4
Internet Address      Physical Address      Type
192.168.122.1         52-54-00-1f-18-ec    dynamic
192.168.122.27        08-00-27-27-29-8c    dynamic
192.168.122.67        08-00-27-27-29-8c    dynamic
192.168.122.103       08-00-27-30-20-e0    dynamic
192.168.122.109       08-00-27-27-29-8c    dynamic
192.168.122.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\User>
```

"Dynamic" could be changed to "static," but when a new device is added to the network, you must configure it manually.

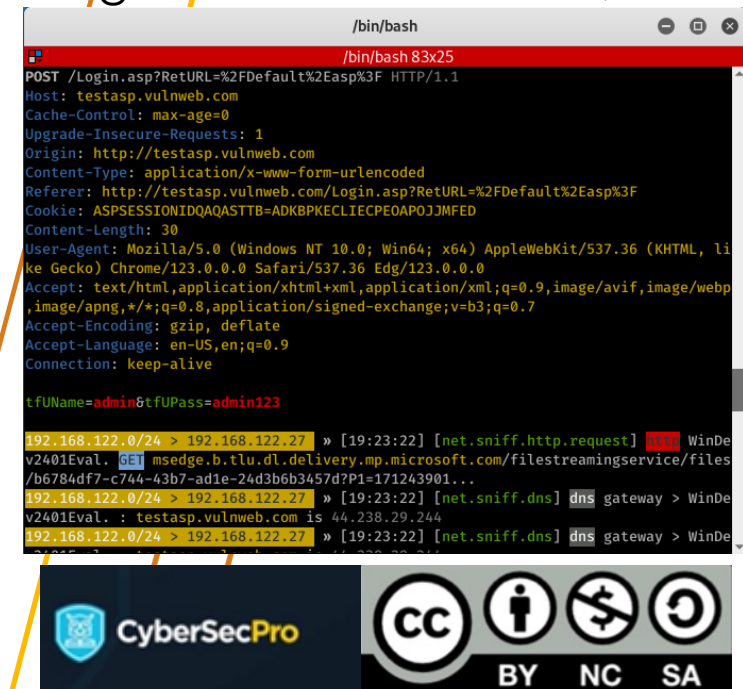
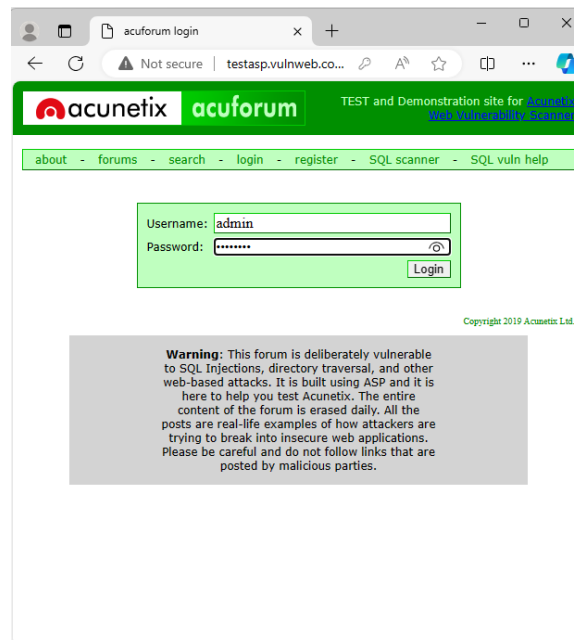
Prevention of MITM

- Detection is not considered a prevention action.
- The previously discussed detection approaches were used only for detecting ARP spoofing attacks.
- To ensure network security, encrypt traffic using HTTPS (browser plugins). Most recent versions of web browsers support services that warn when visiting HTTP websites.
- Some plugins can redirect from HTTP to HTTPS, but hackers can still obtain information about your insecure communication.
- VPN is the best solution for preventing MITM attacks.

VPN

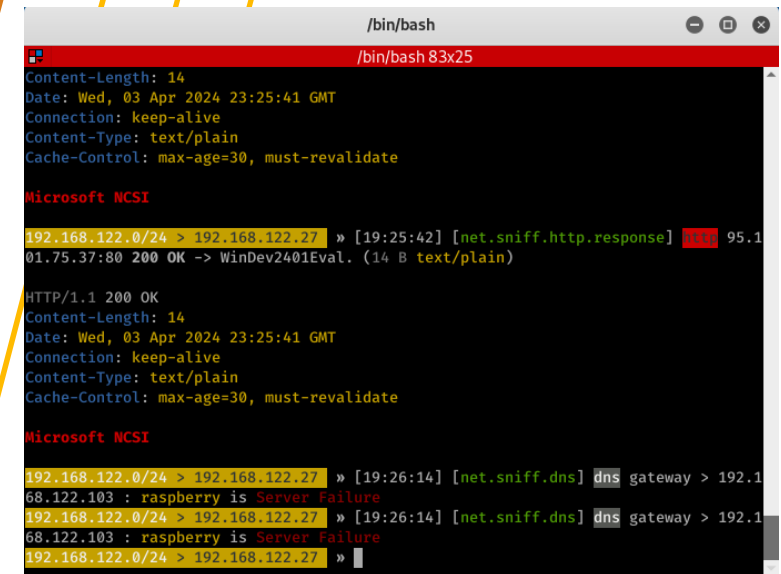
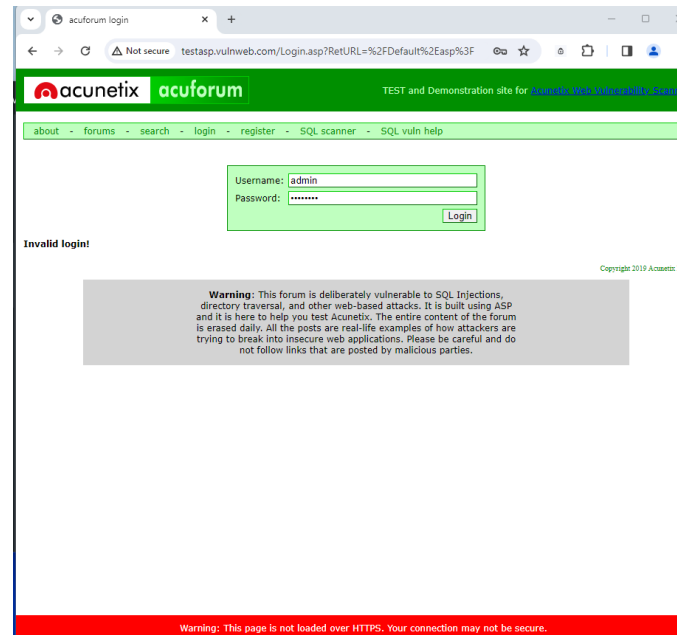
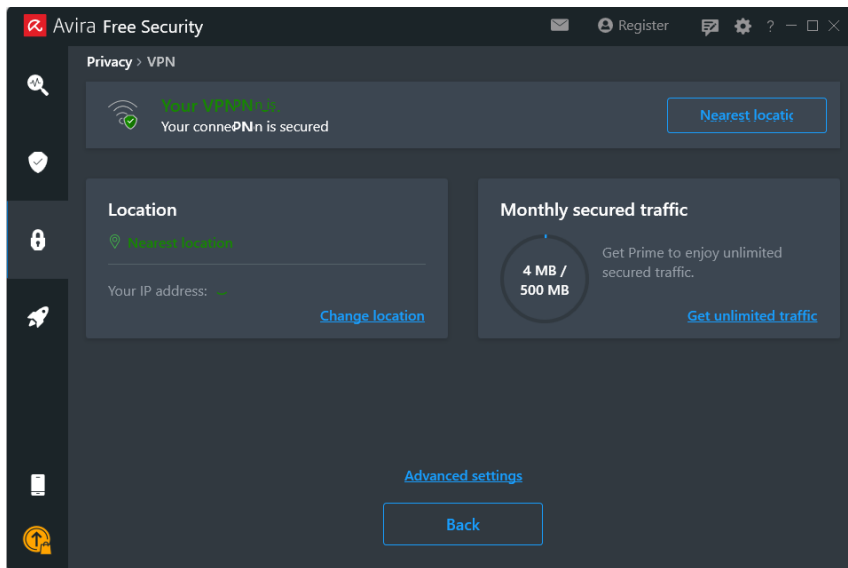
VPN for Prevention of MITM

- Use any preferred VPN tool for your test.
- I use Avira VPN, the free version, for testing.
- There is a free version available with about 500 MB of data stream.
- Installed it on my Windows machine.
- Before turning the VPN on, visit testasp.vulnweb.com and insert your login credentials (username and password).
- At the same time, check Bettercap for collecting all visiting website information, including the credentials.



VPN for Prevention of MITM

- Turn on the VPN on your windows machine (victim machine), and then reload the same page and insert your access credentials
- Observe the difference



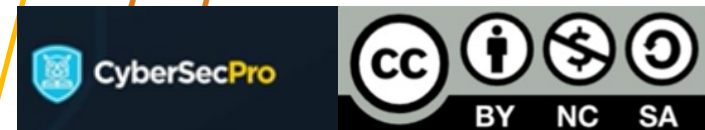
SURICATA

SURICATA

- Suricata is an open-source-based intrusion detection system and intrusion prevention system
- Suricata analyzes all traffic on the interface, searching for known attacks and anomalies
- When an attack or anomaly is detected, the system can decide whether to block traffic or simply save the event on a log (/var/log/suricata/fast.log)
- Suricata can be configured using sets of rules organized in uniform categories. Each category can be set to:
 - **Enable**: traffic matching rules from these categories will be reported
 - **Block**: traffic matching rules from this category will be dropped
 - **Disable**: rules from this category are ignored

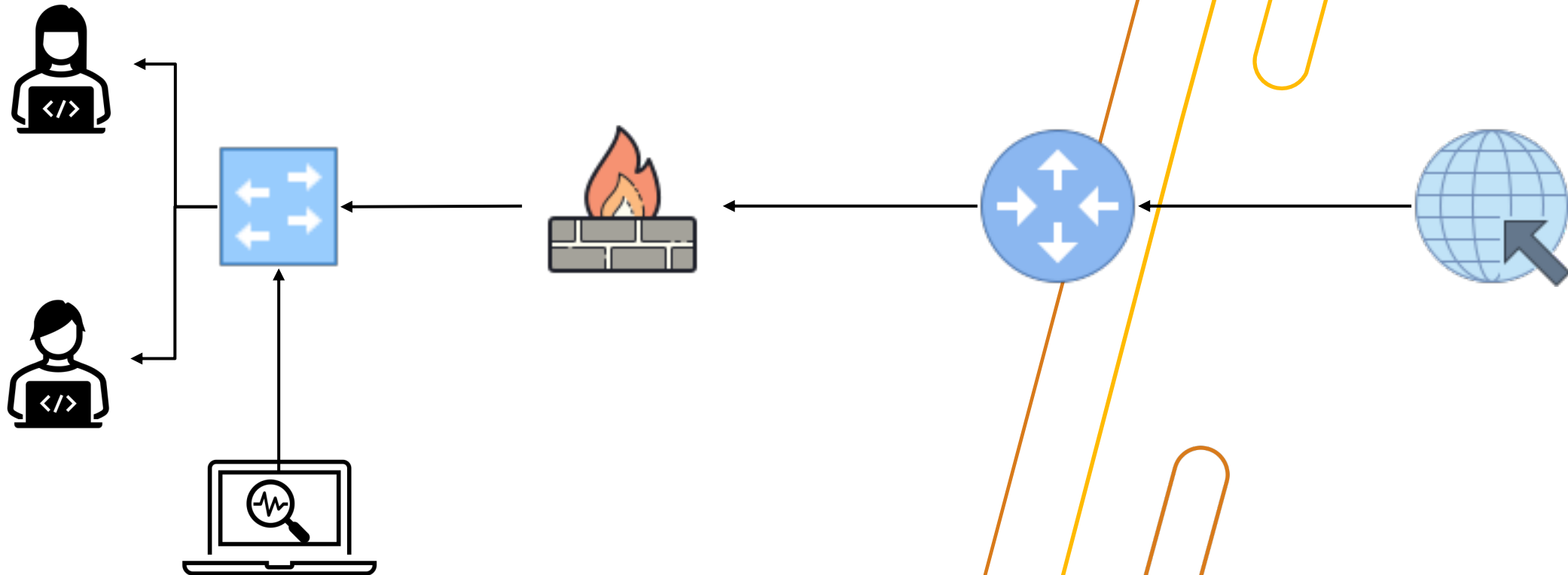


SURICATA



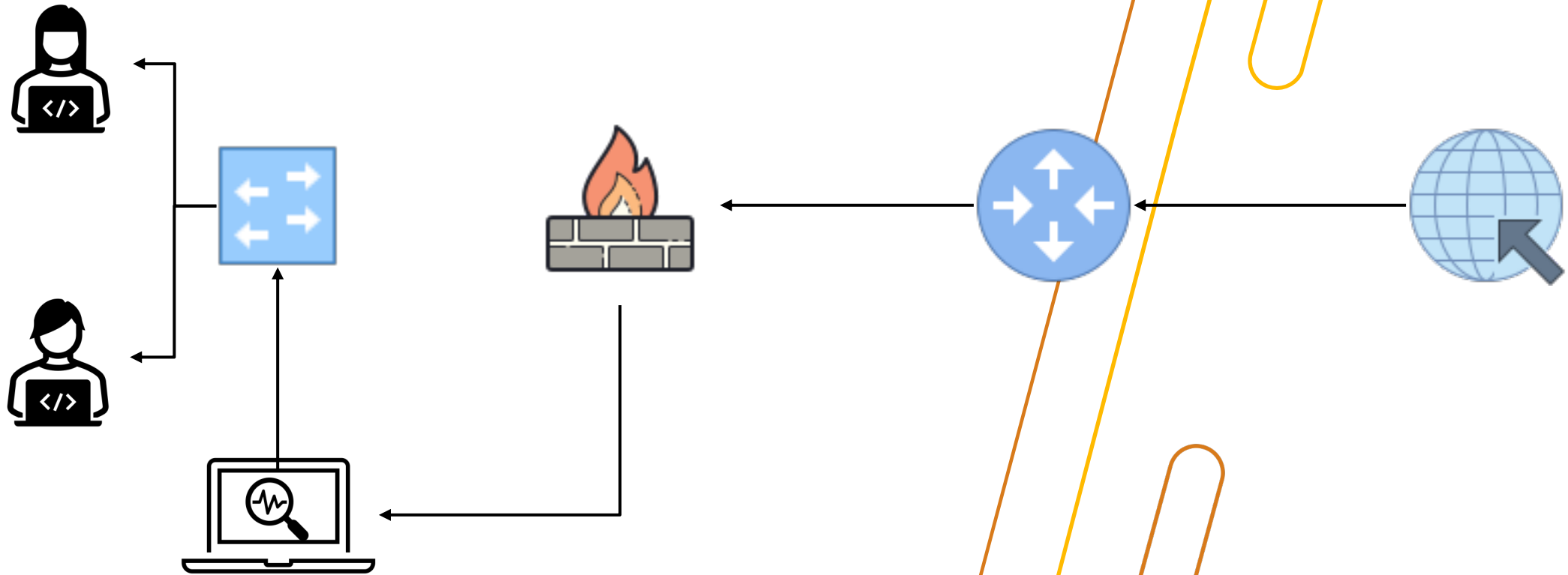
SURICTA Modes

IDS



SURICTA Modes

IPS



SURICATA Installation

- Sudo apt-get update
- Sudo apt -y install suricata

```
kali@kali: ~  
File Actions Edit View Help  
Setting up librt-net-bond24:amd64 (23.11-1) ...  
Setting up suricata (1:7.0.3-1) ...  
update-rc.d: We have no instructions for the suricata init script.  
update-rc.d: It looks like a network service, we disable it.  
suricata.service is a disabled or a static unit, not starting it.  
Processing triggers for libc-bin (2.37-12) ...  
Processing triggers for man-db (2.12.0-3) ...  
Processing triggers for kali-menu (2023.4.7) ...  
  
(kali@kali)-[~]  
└─$ suricata  
Suricata 7.0.3  
USAGE: suricata [OPTIONS] [BPF FILTER]  
  
-c <path>           : path to configuration file  
-T                 : test configuration file (use with -c)  
-i <dev or ip>     : run in pcap live mode  
-F <bpf filter file> : bpf filter file  
-r <path>         : run in pcap file/offline mode  
-q <qid[:qid]>     : run in inline nfqueue mode (use colon to specify a  
-s <path>         : path to signature file loaded in addition to suric  
(optional)  
-S <path>         : path to signature file loaded exclusively (optiona  
-l <dir>          : default log directory  
-D                : run as daemon  
-k [all|none]     : force checksum check (all) or disabled it (none)  
-V                : display Suricata version  
-v                : be more verbose (use multiple times to increase ve
```

Suricata Rules and Configurations

Suricata list of Rules

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ls -al /etc/suricata
total 116
drwxr-xr-x  3 root root  4096 Apr  8 17:44 .
drwxr-xr-x 182 root root 12288 Apr  8 17:44 ..
-rw-r--r--  1 root root  3327 Feb  8 04:35 classification.config
-rw-r--r--  1 root root  1375 Feb  8 04:35 reference.config
drwxr-xr-x  2 root root  4096 Apr  8 17:44 rules
-rw-r--r--  1 root root 85175 Feb  8 17:22 suricata.yaml
-rw-r--r--  1 root root  1643 Feb  8 04:35 threshold.config

(kali@kali)-[~]
└─$
  
```

Suricata Configurations and Rules

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ls -al /etc/suricata/rules
total 152
drwxr-xr-x  2 root root  4096 Apr  8 17:44 .
drwxr-xr-x  3 root root  4096 Apr  8 17:44 ..
-rw-r--r--  1 root root  1858 Feb  8 04:35 app-layer-events.rules
-rw-r--r--  1 root root 20880 Feb  8 04:35 decoder-events.rules
-rw-r--r--  1 root root   468 Feb  8 04:35 dhcp-events.rules
-rw-r--r--  1 root root  1221 Feb  8 04:35 dnp3-events.rules
-rw-r--r--  1 root root  1198 Feb  8 04:35 dns-events.rules
-rw-r--r--  1 root root  4005 Feb  8 04:35 files.rules
-rw-r--r--  1 root root   446 Feb  8 04:35 ftp-events.rules
-rw-r--r--  1 root root 14256 Feb  8 04:35 http-events.rules
-rw-r--r--  1 root root  3311 Feb  8 04:35 http2-events.rules
-rw-r--r--  1 root root  2832 Feb  8 04:35 ipsec-events.rules
-rw-r--r--  1 root root   585 Feb  8 04:35 kerberos-events.rules
-rw-r--r--  1 root root  2077 Feb  8 04:35 modbus-events.rules
-rw-r--r--  1 root root  2187 Feb  8 04:35 mqtt-events.rules
-rw-r--r--  1 root root   729 Feb  8 04:35 nfs-events.rules
-rw-r--r--  1 root root   558 Feb  8 04:35 ntp-events.rules
-rw-r--r--  1 root root   544 Feb  8 04:35 quic-events.rules
-rw-r--r--  1 root root   926 Feb  8 04:35 rfb-events.rules
-rw-r--r--  1 root root  4607 Feb  8 04:35 smb-events.rules
-rw-r--r--  1 root root  5393 Feb  8 04:35 smtp-events.rules
-rw-r--r--  1 root root   719 Feb  8 04:35 ssh-events.rules
-rw-r--r--  1 root root 14311 Feb  8 04:35 stream-events.rules
-rw-r--r--  1 root root  6861 Feb  8 04:35 tls-events.rules

(kali@kali)-[~]
└─$
  
```

Suricata Rules and Configurations

Update the configuration file
Sudo vim /etc/suricata/suricata.yaml

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ls -al /etc/suricata
total 116
drwxr-xr-x  3 root root  4096 Apr  8 17:44 .
drwxr-xr-x 182 root root 12288 Apr  8 17:44 ..
-rw-r--r--  1 root root  3327 Feb  8 04:35 classification.config
-rw-r--r--  1 root root  1375 Feb  8 04:35 reference.config
drwxr-xr-x  2 root root  4096 Apr  8 17:44 rules
-rw-r--r--  1 root root 85175 Feb  8 17:22 suricata.yaml
-rw-r--r--  1 root root  1643 Feb  8 04:35 threshold.config

(kali@kali)-[~]
└─$
```

Suricata Configurations and Rules

```
kali@kali: ~
File Actions Edit View Help

YAML 1.1

# Suricata configuration file. In addition to the comments describing a
# ll
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.3.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"

<etc/suricata/suricata.yaml" 2173L, 85175B          1,1          Top
```

Suricata Rules and Configurations

Update the configuration file
Sudo vim /etc/suricata/suricata.yaml

We need to configure the HOME_NET that we want to monitor and ensure the correct interface name is defined.

So we need to know the subnet

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.122.203 netmask 255.255.255.0 broadcast 192.168.122.255
    inet6 fe80::1a9:e34d:3f15:b318 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:fa:75:14 txqueuelen 1000 (Ethernet)
    RX packets 53707 bytes 77874681 (74.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22955 bytes 1632538 (1.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
└─$
```

Interface name

192.168.122.0/24

```
kali@kali: ~
File Actions Edit View Help
YAML 1.1
# Suricata configuration file. In addition to the comments describing a
ll
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.3.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
# more specific is better for alert accuracy and performance
address-groups:
HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
#HOME_NET: "[192.168.0.0/16]"
#HOME_NET: "[10.0.0.0/8]"
#HOME_NET: "[172.16.0.0/12]"
#HOME_NET: "any"

EXTERNAL_NET: "!$HOME_NET"
#EXTERNAL_NET: "any"

HTTP_SERVERS: "$HOME_NET"
SMTP_SERVERS: "$HOME_NET"
SQL_SERVERS: "$HOME_NET"
DNS_SERVERS: "$HOME_NET"
TELNET_SERVERS: "$HOME_NET"
AIM_SERVERS: "$EXTERNAL_NET"
<etc/suricata/suricata.yaml" 2173L, 85175B 1,1 Top
```

Suricata Rules and Configurations

You could directly open the .yaml configuration file, make any updates you want, then store the file again.

We need to configure the HOME_NET that we want to monitor

So we need to know the subnet

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.122.203 netmask 255.255.255.0 broadcast 192.168.122.255
    inet6 fe80::1a79:e34d:3f15:b318 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:fa:75:14 txqueuelen 1000 (Ethernet)
    RX packets 53707 bytes 77874681 (74.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22955 bytes 1632538 (1.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
└─$
  
```

Interface name

192.168.122.0/24

```

~/Desktop/suricata.yaml - Mousepad
File Edit Search View Document Help
# This configuration file generated by Suricata 7.0.3
9 suricata-version: "7.0"
10
11 ##
12 ## Step 1: Inform Suricata about your network
13 ##
14
15 vars:
16 # more specific is better for alert accuracy and performance
17 address-groups:
18 HOME_NET: "[192.168.122.0/24]"
19 #HOME_NET: "[192.168.0.0/16]"
20 #HOME_NET: "[10.0.0.0/8]"
21 #HOME_NET: "[172.16.0.0/12]"
22 #HOME_NET: "any"
23
24 EXTERNAL_NET: "!$HOME_NET"
25 #EXTERNAL_NET: "any"
26
27 HTTP_SERVERS: "$HOME_NET"
28 SMTP_SERVERS: "$HOME_NET"
29 SQL_SERVERS: "$HOME_NET"
30 DNS_SERVERS: "$HOME_NET"
31 TELNET_SERVERS: "$HOME_NET"
32 AIM_SERVERS: "$EXTERNAL_NET"
33 DC_SERVERS: "$HOME_NET"
34 DNP3_SERVER: "$HOME_NET"
35 DNP3_CLIENT: "$HOME_NET"
36 MODBUS_CLIENT: "$HOME_NET"
37 MODBUS_SERVER: "$HOME_NET"
38 ENIP_CLIENT: "$HOME_NET"
39 ENIP_SERVER: "$HOME_NET"
40
41 port-groups:
42 HTTP_PORTS: "80"
43 SHELLCODE_PORTS: "!80"
44 ORACLE_PORTS: 1521
45 SSH_PORTS: 22
  
```

Suricata Rules and Configurations

Update suricata using: `sudo suricata-update`

```
File Actions Edit View Help

(kali@kali)-[~/Desktop]
└─$ sudo suricata-update
8/4/2024 -- 18:39:51 - <Info> -- Using data-directory /var/lib/suricata.
8/4/2024 -- 18:39:51 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
8/4/2024 -- 18:39:51 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
8/4/2024 -- 18:39:51 - <Info> -- Found Suricata version 7.0.3 at /usr/bin/suricata.
8/4/2024 -- 18:39:51 - <Info> -- Loading /etc/suricata/suricata.yaml
8/4/2024 -- 18:39:51 - <Info> -- Disabling rules for protocol postgres
8/4/2024 -- 18:39:51 - <Info> -- Disabling rules for protocol modbus
8/4/2024 -- 18:39:51 - <Info> -- Disabling rules for protocol dnp3
8/4/2024 -- 18:39:51 - <Info> -- Disabling rules for protocol enip
8/4/2024 -- 18:39:51 - <Info> -- No sources configured, will use Emerging Threats Open
8/4/2024 -- 18:39:51 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.3/emerging.rules.tar.gz.
100% - 4239199/4239199
8/4/2024 -- 18:39:53 - <Info> -- Done.
8/4/2024 -- 18:39:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
```

Suricata Rules and Configurations

To test the configuration file of Suricata; `sudo suricata -T -c /etc/suricata/suricata.yaml -v`

All intrusion activities are in the .log file; the .json contains the same collected/detected intrusions but in JSON format.

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 37120 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 37123 signatures processed. 1182 are IP-only rules, 4910 are inspecting packet payload, 30819 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
(kali@kali)-[~]
└─$
```

Running on the test mode

There are 37120 rules successfully loaded, and 0 failed

Suricata Run

- Run as a daemon
 - Sudo systemctl start suricata.service
- Check the status of the Suricata tool
 - Sudo systemctl status suricata.service

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo systemctl status suricata.service
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-04-10 06:34:37 EDT; 2min 4s ago
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://suricata.io/documentation/
   Process: 3618 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml
   Main PID: 3619 (Suricata-Main)
    Tasks: 10 (limit: 4611)
   Memory: 460.6M (peak: 461.1M)
      CPU: 22.847s
   CGroup: /system.slice/suricata.service
           └─3619 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml

Apr 10 06:34:37 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon:
Apr 10 06:34:37 kali suricata[3618]: i: suricata: This is Suricata version 4.0.0
Apr 10 06:34:37 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon:
lines 1-17/17 (END)
```

```
kali@kali: ~
File Actions Edit View Help
└─$ ls -al /var/log/suricata
total 1504
drwxr-xr-x  2 root root   4096 Apr  8 18:44 .
drwxr-xr-x 22 root root   4096 Apr 10 06:28 ..
-rw-r--r--  1 root root 833985 Apr 10 06:39 eve.json
-rw-r--r--  1 root root     0 Apr  8 19:14 fast.log
-rw-r--r--  1 root root 676745 Apr 10 06:39 stats.log
-rw-r--r--  1 root root 11307 Apr 10 06:34 suricata.log

(kali@kali)-[~]
└─$
```

- Now it means that the tool is running on the background

Detect ID Attack using Suricata

- Default rules are stored:
 - `sudo ls -al /var/lib/suricata/rules/`

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ sudo ls -al /var/lib/suricata/rules
[sudo] password for kali:
total 27672
drwxr-xr-x 2 root root    4096 Apr  8 18:39 .
drwxr-xr-x 4 root root    4096 Apr  8 18:39 ..
-rw-r--r-- 1 root root    3228 Apr  8 18:39 classification.config
-rw-r--r-- 1 root root 28320075 Apr  8 18:39 suricata.rules

(kali@kali)-[~]
└─$
```

- Test Suricata
 - Visit: <http://testmynids.org/uid/index.html>

testmynids.org

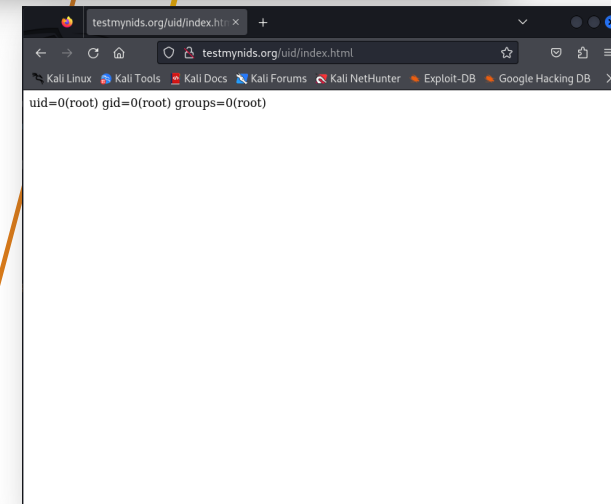
- Check the log:
 - `sudo cat /var/log/suricata/fast.log`

```
kali@kali: ~
File Actions Edit View Help

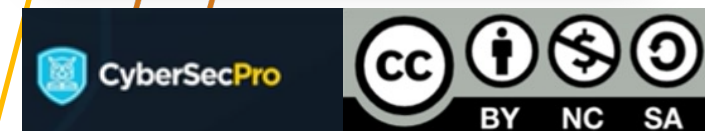
drwxr-xr-x 4 root root    4096 Apr  8 18:39 ..
-rw-r--r-- 1 root root    3228 Apr  8 18:39 classification.config
-rw-r--r-- 1 root root 28320075 Apr  8 18:39 suricata.rules

(kali@kali)-[~]
└─$ sudo cat /var/log/suricata/fast.log
04/10/2024-06:55:53.676719  [**] [1:2100498:7] GPL ATTACK_RESPONSE id c
heck returned root [**] [Classification: Potentially Bad Traffic] [Prio
rity: 2] {TCP} 13.32.110.51:80 → 192.168.122.203:37862

(kali@kali)-[~]
└─$
```



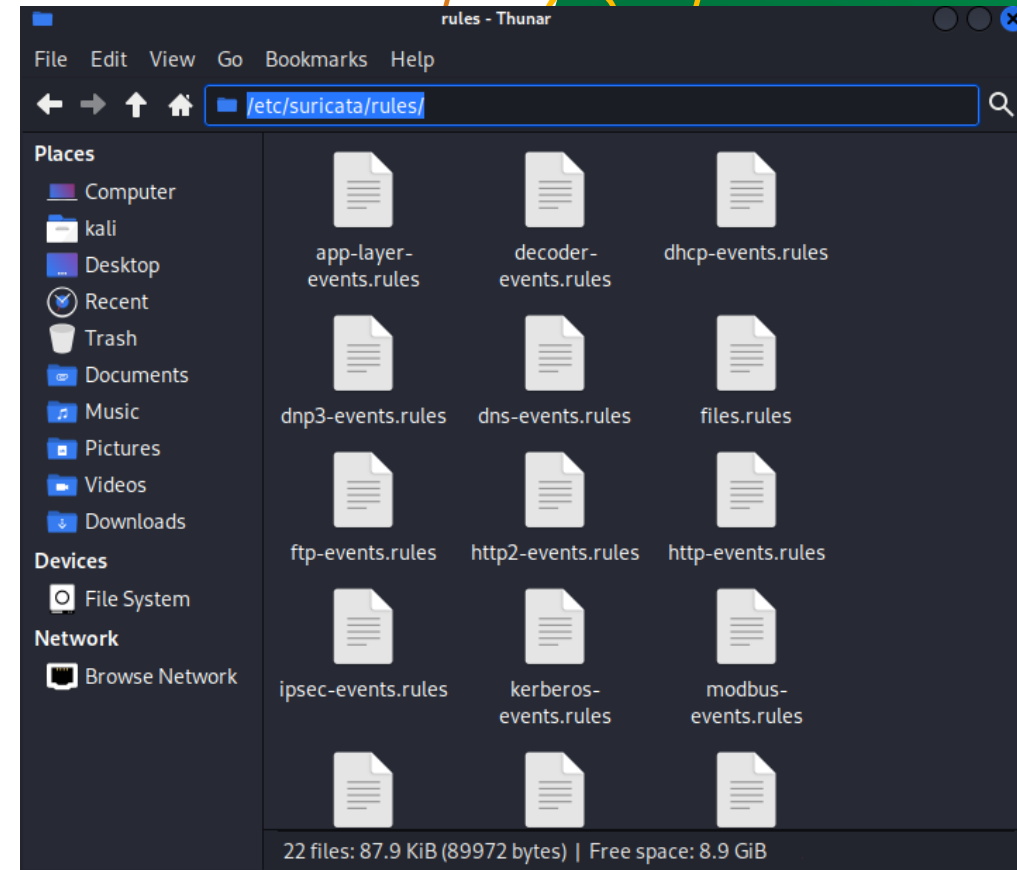
[GitHub - 3CDRESec/testmynids.org](https://github.com/3CDRESec/testmynids.org): A website and framework for testing NIDS detection



Customize Rules for Suricata

- Stop Suricata
 - Sudo systemctl stop suricata.service

- All rules are store on: /etc/suricata/rules



Customize Rules for Suricata

- Create a file „My.rules“ and store the file on /etc/suricata/
alert icmp any any -> \$HOME_NET any (msg: "Ping ICMP"; sid: 1; rev: 1;)

```
~/Desktop/My.rules - Mousepad
File Edit Search View Document Help
1 alert icmp any any -> $HOME_NET any (msg: "Ping ICMP"; sid:1; rev:1;)
2
```

- Update the .yaml configuration file

```
rule-files:
- suricata.rules
- /etc/suricata/rules/My.rules
```

It seems that
everything running
well

Check the configuration file

```
kali@kali: ~/Desktop
File Actions Edit View Help
priority: 1] {UDP} 192.168.122.27:68 -> 192.168.122.1:67

(kali@kali)-[~/Desktop]
└─$ sudo cp -f suricata.yaml /etc/suricata

(kali@kali)-[~/Desktop]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 37121 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 37124 signatures processed. 1183 are IP-only rules, 4910 are inspecting packet payload, 30819 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.

(kali@kali)-[~/Desktop]
└─$
```

Run Customize Rules

- Run Suricata
 - Sudo systemctl start suricata.service

```

/bin/bash
/bin/bash 83x25
64 bytes from 192.168.122.203: icmp_seq=20 ttl=64 time=3.02 ms
64 bytes from 192.168.122.203: icmp_seq=21 ttl=64 time=1.08 ms
64 bytes from 192.168.122.203: icmp_seq=22 ttl=64 time=1.14 ms
64 bytes from 192.168.122.203: icmp_seq=23 ttl=64 time=1.15 ms
64 bytes from 192.168.122.203: icmp_seq=24 ttl=64 time=1.58 ms
64 bytes from 192.168.122.203: icmp_seq=25 ttl=64 time=4.11 ms
64 bytes from 192.168.122.203: icmp_seq=26 ttl=64 time=2.65 ms
64 bytes from 192.168.122.203: icmp_seq=27 ttl=64 time=4.11 ms
64 bytes from 192.168.122.203: icmp_seq=28 ttl=64 time=3.29 ms
64 bytes from 192.168.122.203: icmp_seq=29 ttl=64 time=1.69 ms
64 bytes from 192.168.122.203: icmp_seq=30 ttl=64 time=1.50 ms
64 bytes from 192.168.122.203: icmp_seq=31 ttl=64 time=1.04 ms
64 bytes from 192.168.122.203: icmp_seq=32 ttl=64 time=1.85 ms
64 bytes from 192.168.122.203: icmp_seq=33 ttl=64 time=1.48 ms
64 bytes from 192.168.122.203: icmp_seq=34 ttl=64 time=1.78 ms
64 bytes from 192.168.122.203: icmp_seq=35 ttl=64 time=5.25 ms
64 bytes from 192.168.122.203: icmp_seq=36 ttl=64 time=1.28 ms
64 bytes from 192.168.122.203: icmp_seq=37 ttl=64 time=1.35 ms
64 bytes from 192.168.122.203: icmp_seq=38 ttl=64 time=1.19 ms
64 bytes from 192.168.122.203: icmp_seq=39 ttl=64 time=1.36 ms
64 bytes from 192.168.122.203: icmp_seq=40 ttl=64 time=2.51 ms
64 bytes from 192.168.122.203: icmp_seq=41 ttl=64 time=3.49 ms
64 bytes from 192.168.122.203: icmp_seq=42 ttl=64 time=2.92 ms
64 bytes from 192.168.122.203: icmp_seq=43 ttl=64 time=3.22 ms

```

```

kali@kali: ~/Desktop
File Actions Edit View Help
rity: 3] {ICMP} 192.168.122.203:0 → 192.168.122.27:0

(kali@kali)~[~/Desktop]
$ sudo cat /var/log/suricata/fast.log
04/10/2024-06:55:53.676719 [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned r
oot [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 13.32.110.51:80
→ 192.168.122.203:37862
04/10/2024-06:58:36.038441 [**] [1:2022973:1] ET POLICY Possible Kali Linux hostname
in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [P
riority: 1] {UDP} 192.168.122.203:68 → 192.168.122.1:67
04/10/2024-06:58:51.122740 [**] [1:2022973:1] ET POLICY Possible Kali Linux hostname
in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [P
riority: 1] {UDP} 192.168.122.27:68 → 192.168.122.1:67
04/10/2024-07:53:57.321030 [**] [1:2022973:1] ET POLICY Possible Kali Linux hostname
in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [P
riority: 1] {UDP} 192.168.122.27:68 → 192.168.122.1:67
04/10/2024-07:54:40.040137 [**] [1:2022973:1] ET POLICY Possible Kali Linux hostname
in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [P
riority: 1] {UDP} 192.168.122.203:68 → 192.168.122.1:67
04/10/2024-08:02:22.900291 [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.27:8 → 192.168.122.203:0
04/10/2024-08:02:22.900332 [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.203:0 → 192.168.122.27:0
04/10/2024-08:09:07.448926 [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.27:8 → 192.168.122.203:0
04/10/2024-08:09:07.449032 [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.203:0 → 192.168.122.27:0

(kali@kali)~[~/Desktop]
$

```

Attacker Linux
My Linux

Run Customize Rules

- Test Ping from the Client to Server devices

```

pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~$ ping 192.168.122.109
PING 192.168.122.109 (192.168.122.109) 56(84) bytes of data:
64 bytes from 192.168.122.109: icmp_seq=1 ttl=64 time=4.51 ms
64 bytes from 192.168.122.109: icmp_seq=2 ttl=64 time=3.47 ms
64 bytes from 192.168.122.109: icmp_seq=3 ttl=64 time=2.63 ms
64 bytes from 192.168.122.109: icmp_seq=4 ttl=64 time=6.77 ms
64 bytes from 192.168.122.109: icmp_seq=5 ttl=64 time=2.24 ms
64 bytes from 192.168.122.109: icmp_seq=6 ttl=64 time=1.91 ms
64 bytes from 192.168.122.109: icmp_seq=7 ttl=64 time=2.53 ms
64 bytes from 192.168.122.109: icmp_seq=8 ttl=64 time=2.93 ms
64 bytes from 192.168.122.109: icmp_seq=9 ttl=64 time=2.67 ms
64 bytes from 192.168.122.109: icmp_seq=10 ttl=64 time=1.11 ms
64 bytes from 192.168.122.109: icmp_seq=11 ttl=64 time=1.59 ms
64 bytes from 192.168.122.109: icmp_seq=12 ttl=64 time=1.01 ms
64 bytes from 192.168.122.109: icmp_seq=13 ttl=64 time=3.45 ms
64 bytes from 192.168.122.109: icmp_seq=14 ttl=64 time=2.66 ms
64 bytes from 192.168.122.109: icmp_seq=15 ttl=64 time=2.56 ms
64 bytes from 192.168.122.109: icmp_seq=16 ttl=64 time=2.57 ms
64 bytes from 192.168.122.109: icmp_seq=17 ttl=64 time=1.26 ms
64 bytes from 192.168.122.109: icmp_seq=18 ttl=64 time=3.21 ms
64 bytes from 192.168.122.109: icmp_seq=19 ttl=64 time=1.23 ms
64 bytes from 192.168.122.109: icmp_seq=20 ttl=64 time=1.16 ms
64 bytes from 192.168.122.109: icmp_seq=21 ttl=64 time=1.36 ms
64 bytes from 192.168.122.109: icmp_seq=22 ttl=64 time=1.94 ms
  
```

```

kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
└─$ sudo cat /var/log/suricata/fast.log
04/10/2024-06:55:53.676719  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned r
oot [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 13.32.110.51:80
→ 192.168.122.203:37862
04/10/2024-06:58:36.038441  [**] [1:2022973:1] ET POLICY Possible Kali Linux hostname
in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [P
riority: 1] {UDP} 192.168.122.203:68 → 192.168.122.1:67
04/10/2024-06:58:51.122740  [**] [1:2022973:1] ET POLICY Possible Kali Linux hostname
in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [P
riority: 1] {UDP} 192.168.122.27:68 → 192.168.122.1:67
04/10/2024-07:53:57.321030  [**] [1:2022973:1] ET POLICY Possible Kali Linux hostname
in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [P
riority: 1] {UDP} 192.168.122.27:68 → 192.168.122.1:67
04/10/2024-07:54:40.040137  [**] [1:2022973:1] ET POLICY Possible Kali Linux hostname
in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [P
riority: 1] {UDP} 192.168.122.203:68 → 192.168.122.1:67
04/10/2024-08:02:22.900291  [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.27:8 → 192.168.122.203:0
04/10/2024-08:02:22.900332  [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.203:0 → 192.168.122.27:0
04/10/2024-08:09:07.448926  [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.27:8 → 192.168.122.203:0
04/10/2024-08:09:07.449032  [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.203:0 → 192.168.122.27:0
04/10/2024-08:12:57.931674  [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.1:8 → 192.168.122.103:0
04/10/2024-08:15:36.973197  [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.103:8 → 192.168.122.109:0
04/10/2024-08:15:36.973995  [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Prio
rity: 3] {ICMP} 192.168.122.109:0 → 192.168.122.103:0
  
```

Server (kali@kali)-[~/Desktop]
Client

Connect with CyberSecPro: How to register and other practical information

1. Website:
www.cybersecpro-project.eu
2. X (Twitter):
https://twitter.com/CyberSecPro_eu
3. LinkedIn:
<https://www.linkedin.com/company/cybersecpro-euproject/>



**Co-funded by
the European Union**

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

 ACEEU ACCREDITATION COUNCIL FOR ENTREPRENEURIAL & ENGAGED UNIVERSITIES	 AIT AUSTRIAN INSTITUTE OF TECHNOLOGY	 APIROPLUS SOLUTIONS	 SINTEF	 SOCIAL ENGINEERING ACADEMY	 TAL TECH
ACEEU GmbH Germany Visit Website	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH Austria Visit Website	APIROPLUS SOLUTIONS LTD Cyprus Visit Website	SINTEF AS Norway Visit Website	Social Engineering Academy GmbH Germany Visit Website	Tallin University of Technology Estonia Visit Website
Logo missing	 COFAC COOPERATIVA DE FORMAÇÃO E ANIMACÃO CULTURAL C.R.L.	 Consiglio Nazionale delle Ricerche	 Technische Universität Braunschweig	 TECHNICAL UNIVERSITY OF CRETE	 trustilio Enhance your Trustworthiness
C2B CONSULTING Italy Visit Website	COFAC Portugal Visit Website	Consiglio Nazionale delle Ricerche Italy Visit Website	Technical University of Braunschweig Germany Visit Website	Technical University of Crete Greece Visit Website	trustilio B.V. The Netherlands Visit Website
 focal point Cyber Defence Exercises as a Service	 GOETHE UNIVERSITÄT FRANKFURT AM MAIN	 ITML	 UNINOVA	 UNIVERSIDAD DE MÁLAGA	 NOVA UNIVERSIDADE NOVA DE LISBOA
FOCAL POINT Belgium Visit Website	Goethe University Frankfurt Germany Visit Website	Information Technology for Market Leadership Greece Visit Website	Uninova Portugal Visit Website	Universidad de Malaga Spain Visit Website	Universidade Nova De Lisboa Portugal Visit Website
 Institut Mines-Télécom	 LAUREA	 GRUPPO Maggioli	 University of Cyprus	 FACULTY OF SCIENCES NOVI SAD 1969 SERBIA	 UNIVERSITY OF PIRAEUS RESEARCH CENTER
Institut Mines-Télecom France Visit Website	Laurea University of Applied Sciences Finland Visit Website	Maggioli S.p.A. Italy Visit Website	University of Cyprus Cyprus Visit Website	University of Novi Sad Faculty of Sciences Serbia Visit Website	University of Piraeus Research Center Greece Visit Website
 PDMFC	 Security Labs Consulting Ltd	 SGI	 Zelus		
PDMFC Portugal Visit Website	Security Labs Consulting Ltd Ireland (Republic) Visit Website	Serious Games Interactive Denmark Visit Website	ZELUS P.C. Greece Visit Website		

Thank you

Please send all questions to:
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at
Stefan Schauer
Stefan.Schauer@ait.ac.at