INFOTACT SOLUTIONS

INFOTACT
SOLUTIONS

Network Intrusion Detection System (NIDS) Implementation

Group Members:

Abhishek M S

Akanksha K J

Mridul Chamoli

Suraj Balanagouda Nadagoudra

Submitted To:

Mr. Vasudev Jha

Project Report: Network Intrusion Detection System (NIDS) Implementation

Introduction

Project Goal

The primary goal of this project was to develop and implement a robust Network Intrusion Detection System using Suricata to detect and alert on various types of cyber attacks in real-time. The system was designed to identify reconnaissance scans, brute-force attempts, and suspicious network activities to reduce the mean time to detect threats within a network environment.

Importance of NIDS

Network Intrusion Detection Systems are critical components of modern cybersecurity infrastructure. They provide:

- ✓ Real-time monitoring of network traffic
- ✓ Early detection of malicious activities
- ✓ Alerting capabilities for security teams
- ✓ Forensic data for incident response
- ✓ Compliance with security frameworks and regulations

Lab Setup

Virtual Environment Configuration

- ✓ **Host System**: Windows/Mac/Linux with virtualization support
- ✓ **Virtualization Platform**: VirtualBox/VMware
- ✓ **Guest OS**: Kali Linux 2024.1
- ✓ **Network Mode**: Bridged Adapter
- ✓ **IP Address**: 192.168.0.0

Suricata Installation and Configuration

# Installation commands executed

- ✓ sudo apt update && sudo apt upgrade -y
- ✓ sudo apt install suricata -y
- ✓ sudo systemctl enable suricata
- ✓ sudo systemctl start suricata
- ✓ sudo systemctl status suricata

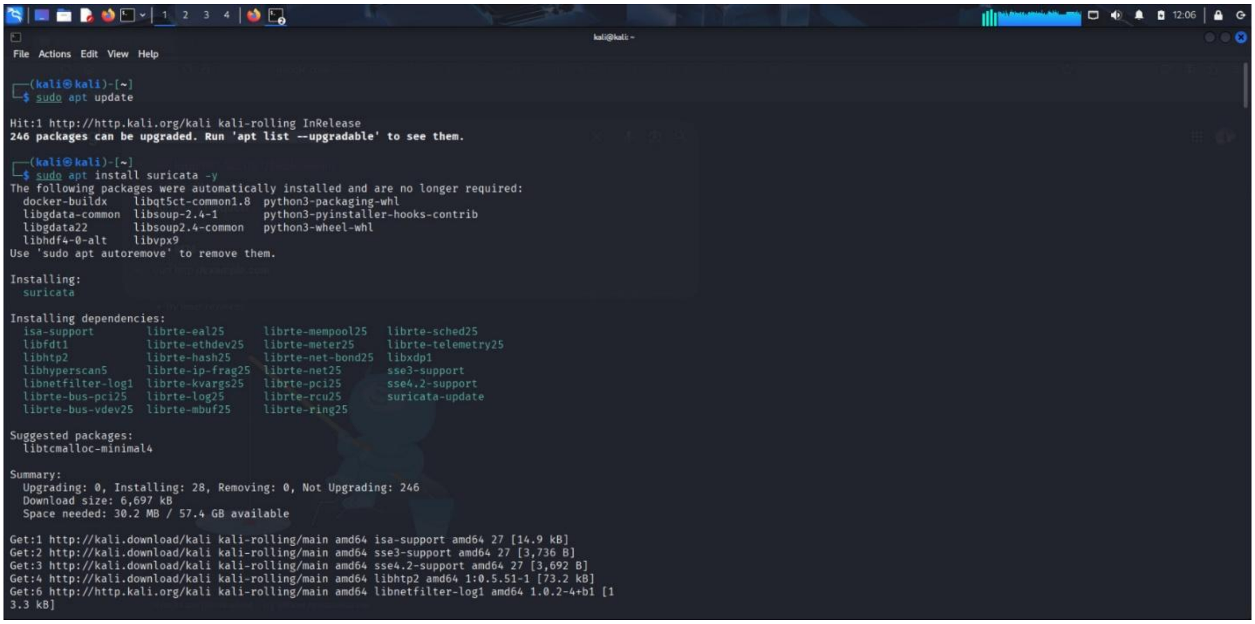
# Network interface configuration

✓ ip a *# Identified interface: eth0,usb0*

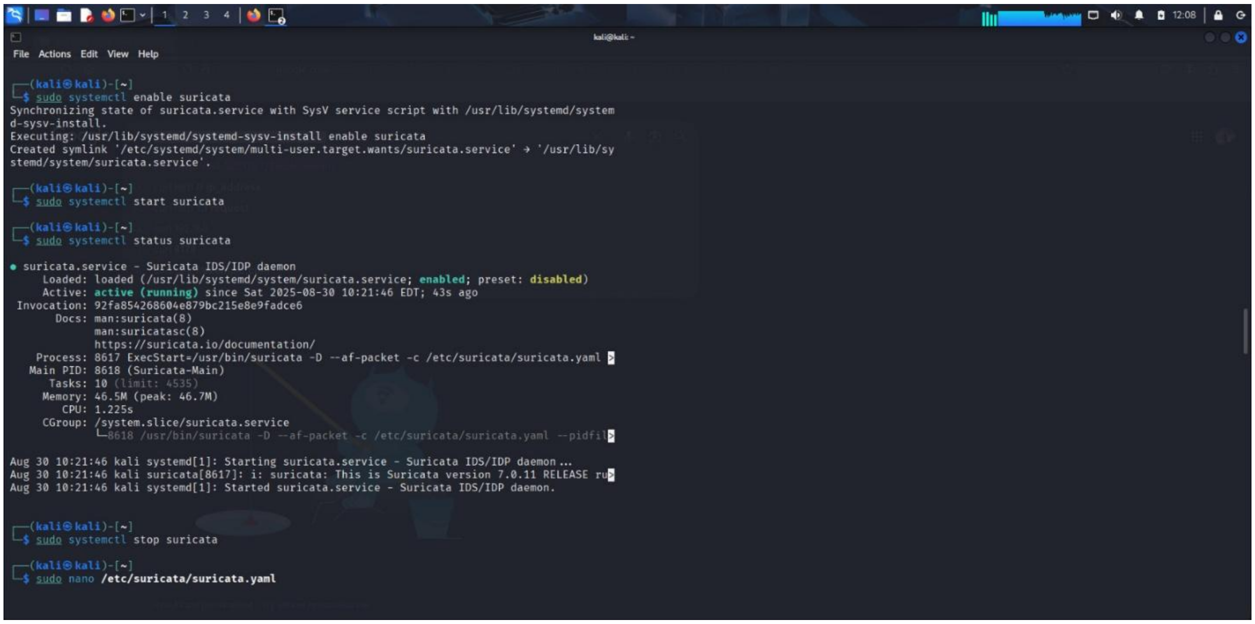
# Suricata configuration

✓ sudo nano /etc/suricata/suricata.yaml

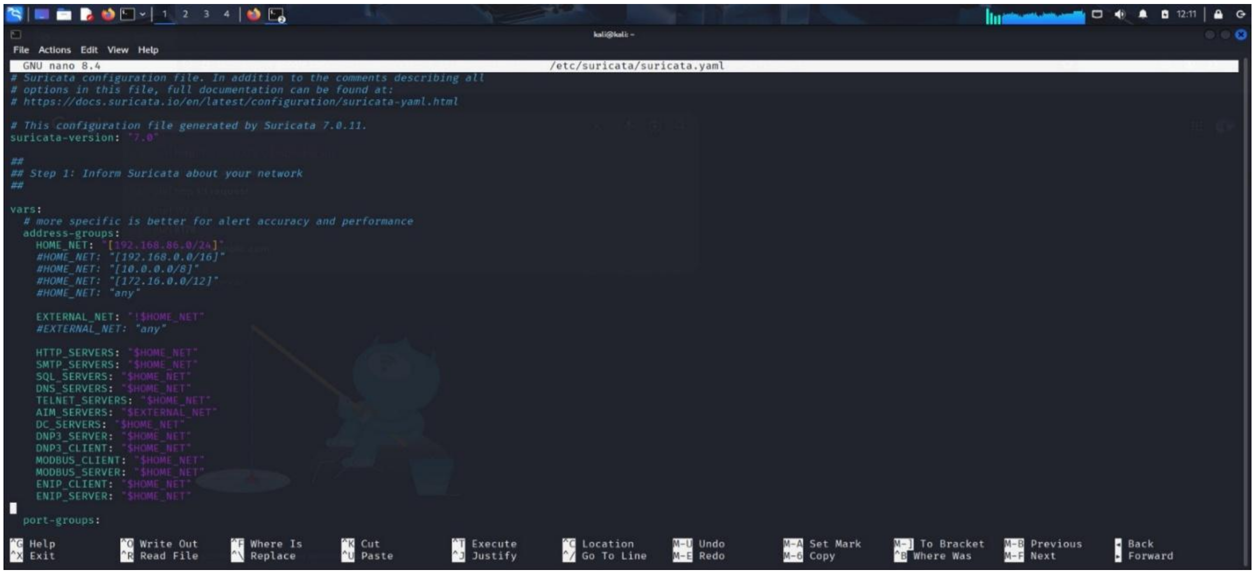
Screenshots:



```
┌──(kali㉿kali)-[~]
└─$ sudo apt update

Hit:1 http://http.kali.org/kali kali-rolling InRelease
246 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)-[~]
└─$ sudo apt install suricata -y
The following packages were automatically installed and are no longer required:
  docker-buildx    libqt5ct-common1.8  python3-packaging-whl
  libgdata-common  libsoup-2.4-1       python3-pyinstaller-hooks-contrib
  libgdata22       libsoup2.4-common   python3-wheel-whl
  libhdf4-0-alt    libvpx9
Use 'sudo apt autoremove' to remove them.

Installing:
  suricata

Installing dependencies:
  isa-support        librte-eal25      librte-mempool25   librte-sched25
  libfdt1            librte-ethdev25   librte-meter25     librte-telemetry25
  libhtp2            librte-hash25     librte-net-bond25  libxdp1
  libhyperscan5      librte-ip-frag25  librte-net25       sse3-support
  libnetfilter-log1  librte-kvargs25   librte-pci25       sse4.2-support
  librte-bus-pci25   librte-log25      librte-rcu25       suricata-update
  librte-bus-vdev25  librte-mbuf25     librte-ring25

Suggested packages:
  libtcmalloc-minimal4

Summary:
  Upgrading: 0, Installing: 28, Removing: 0, Not Upgrading: 246
  Download size: 6,697 kB
  Space needed: 30.2 MB / 57.4 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 isa-support amd64 27 [14.9 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 sse3-support amd64 27 [3,736 B]
Get:3 http://kali.download/kali kali-rolling/main amd64 sse4.2-support amd64 27 [3,692 B]
Get:4 http://kali.download/kali kali-rolling/main amd64 libhtp2 amd64 1:0.5.51-1 [73.2 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 libnetfilter-log1 amd64 1.0.2-4+b1 [1
3.3 kB]
```



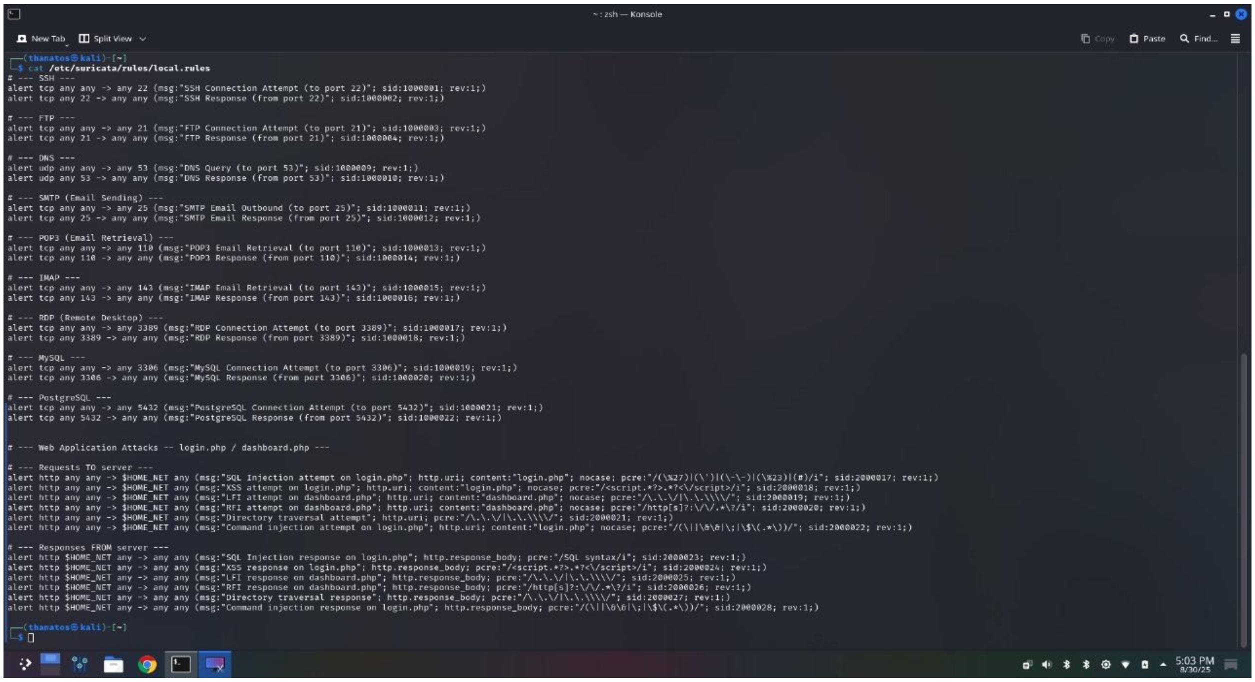
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable suricata
Synchronizing state of suricata.service with SysV service script with /usr/lib/systemd/system
d-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable suricata
Created symlink '/etc/systemd/system/multi-user.target.wants/suricata.service' → '/usr/lib/sy
stemd/system/suricata.service'.

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start suricata

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status suricata

● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: disabled)
     Active: active (running) since Sat 2025-08-30 10:21:46 EDT; 43s ago
 Invocation: 92fa854268604e879bc215e8e9fadce6
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 8617 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml >
   Main PID: 8618 (Suricata-Main)
      Tasks: 10 (limit: 4535)
     Memory: 46.5M (peak: 46.7M)
        CPU: 1.225s
     CGroup: /system.slice/suricata.service
             └─8618 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfil>

Aug 30 10:21:46 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Aug 30 10:21:46 kali suricata[8617]: i: suricata: This is Suricata version 7.0.11 RELEASE ru>
Aug 30 10:21:46 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.


┌──(kali㉿kali)-[~]
└─$ sudo systemctl stop suricata

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/suricata/suricata.yaml
```



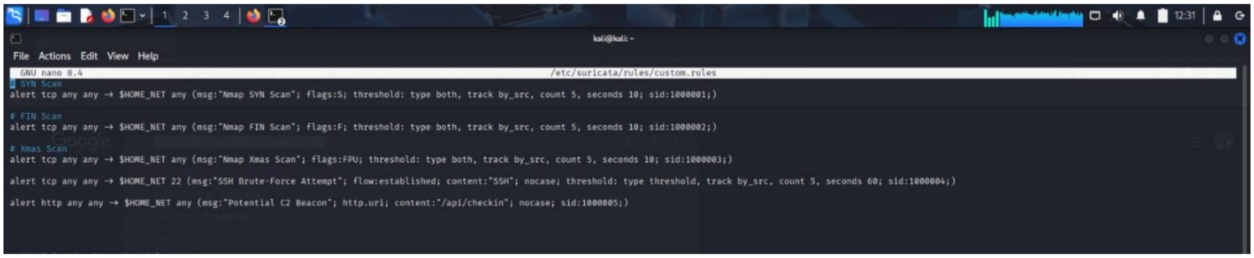
```
GNU nano 8.4                    /etc/suricata/suricata.yaml
# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.11.
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: "[192.168.86.0/24]"
    #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"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"

  port-groups:
```

Custom Rule Development:

sudo nano /etc/suricata/rules/custom.rules

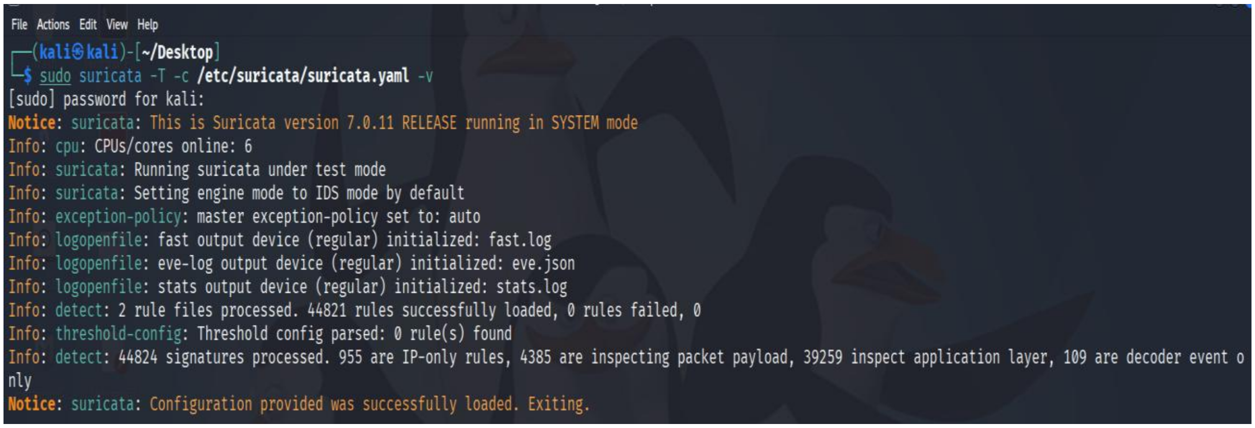


```
┌──(thanatos㉿kali)-[~]
└─$ cat /etc/suricata/rules/local.rules
# --- SSH ---
alert tcp any any -> any 22 (msg:"SSH Connection Attempt (to port 22)"; sid:1000001; rev:1;)
alert tcp any 22 -> any any (msg:"SSH Response (from port 22)"; sid:1000002; rev:1;)

# --- FTP ---
alert tcp any any -> any 21 (msg:"FTP Connection Attempt (to port 21)"; sid:1000003; rev:1;)
alert tcp any 21 -> any any (msg:"FTP Response (from port 21)"; sid:1000004; rev:1;)

# --- DNS ---
alert udp any any -> any 53 (msg:"DNS Query (to port 53)"; sid:1000009; rev:1;)
alert udp any 53 -> any any (msg:"DNS Response (from port 53)"; sid:1000010; rev:1;)

# --- SMTP (Email Sending) ---
alert tcp any any -> any 25 (msg:"SMTP Email Outbound (to port 25)"; sid:1000011; rev:1;)
alert tcp any 25 -> any any (msg:"SMTP Email Response (from port 25)"; sid:1000012; rev:1;)

# --- POP3 (Email Retrieval) ---
alert tcp any any -> any 110 (msg:"POP3 Email Retrieval (to port 110)"; sid:1000013; rev:1;)
alert tcp any 110 -> any any (msg:"POP3 Response (from port 110)"; sid:1000014; rev:1;)

# --- IMAP ---
alert tcp any any -> any 143 (msg:"IMAP Email Retrieval (to port 143)"; sid:1000015; rev:1;)
alert tcp any 143 -> any any (msg:"IMAP Response (from port 143)"; sid:1000016; rev:1;)

# --- RDP (Remote Desktop) ---
alert tcp any any -> any 3389 (msg:"RDP Connection Attempt (to port 3389)"; sid:1000017; rev:1;)
alert tcp any 3389 -> any any (msg:"RDP Response (from port 3389)"; sid:1000018; rev:1;)

# --- MySQL ---
alert tcp any any -> any 3306 (msg:"MySQL Connection Attempt (to port 3306)"; sid:1000019; rev:1;)
alert tcp any 3306 -> any any (msg:"MySQL Response (from port 3306)"; sid:1000020; rev:1;)

# --- PostgreSQL ---
alert tcp any any -> any 5432 (msg:"PostgreSQL Connection Attempt (to port 5432)"; sid:1000021; rev:1;)
alert tcp any 5432 -> any any (msg:"PostgreSQL Response (from port 5432)"; sid:1000022; rev:1;)


# --- Web Application Attacks -- login.php / dashboard.php ---

# --- Requests TO server ---
alert http any any -> $HOME_NET any (msg:"SQL Injection attempt on login.php"; http.uri; content:"login.php"; nocase; pcre:"/(\%27)|(\')|(\-\-)|(\%23)|(#)/i"; sid:2000017; rev:1;)
alert http any any -> $HOME_NET any (msg:"XSS attempt on login.php"; http.uri; content:"login.php"; nocase; pcre:"/<script.*?>.*?<\/script>/i"; sid:2000018; rev:1;)
alert http any any -> $HOME_NET any (msg:"LFI attempt on dashboard.php"; http.uri; content:"dashboard.php"; nocase; pcre:"/\.\.\/|\.\.\\\\/"; sid:2000019; rev:1;)
alert http any any -> $HOME_NET any (msg:"RFI attempt on dashboard.php"; http.uri; content:"dashboard.php"; nocase; pcre:"/http[s]?:\/\/.*\?/i"; sid:2000020; rev:1;)
alert http any any -> $HOME_NET any (msg:"Directory traversal attempt"; http.uri; pcre:"/\.\.\/|\.\.\\\\/"; sid:2000021; rev:1;)
alert http any any -> $HOME_NET any (msg:"Command injection attempt on login.php"; http.uri; content:"login.php"; nocase; pcre:"/(\||\&\&|\;|\$\(.*\))/"; sid:2000022; rev:1;)

# --- Responses FROM server ---
alert http $HOME_NET any -> any any (msg:"SQL Injection response on login.php"; http.response_body; pcre:"/SQL syntax/i"; sid:2000023; rev:1;)
alert http $HOME_NET any -> any any (msg:"XSS response on login.php"; http.response_body; pcre:"/<script.*?>.*?<\/script>/i"; sid:2000024; rev:1;)
alert http $HOME_NET any -> any any (msg:"LFI response on dashboard.php"; http.response_body; pcre:"/\.\.\/|\.\.\\\\/"; sid:2000025; rev:1;)
alert http $HOME_NET any -> any any (msg:"RFI response on dashboard.php"; http.response_body; pcre:"/http[s]?:\/\/.*\?/i"; sid:2000026; rev:1;)
alert http $HOME_NET any -> any any (msg:"Directory traversal response"; http.response_body; pcre:"/\.\.\/|\.\.\\\\/"; sid:2000027; rev:1;)
alert http $HOME_NET any -> any any (msg:"Command injection response on login.php"; http.response_body; pcre:"/(\||\&\&|\;|\$\(.*\))/"; sid:2000028; rev:1;)

┌──(thanatos㉿kali)-[~]
└─$ 
```



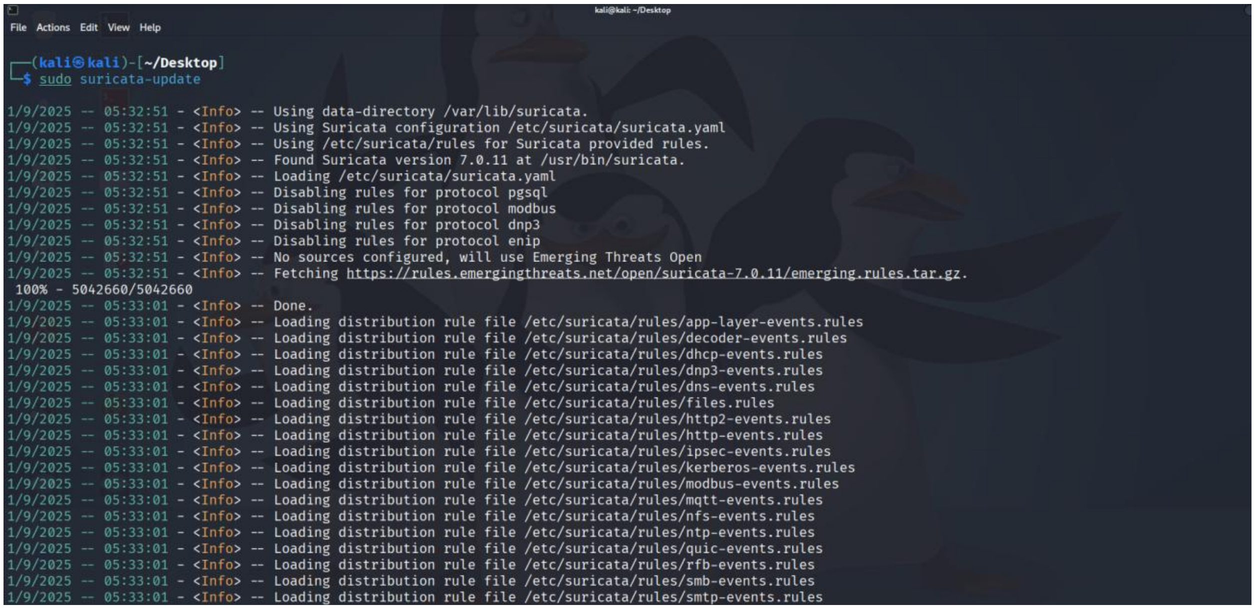
```
GNU nano 8.4                    /etc/suricata/rules/custom.rules
# SYN Scan
alert tcp any any -> $HOME_NET any (msg:"Nmap SYN Scan"; flags:S; threshold: type both, track by_src, count 5, seconds 10; sid:1000001;)

# FIN Scan
alert tcp any any -> $HOME_NET any (msg:"Nmap FIN Scan"; flags:F; threshold: type both, track by_src, count 5, seconds 10; sid:1000002;)

# Xmas Scan
alert tcp any any -> $HOME_NET any (msg:"Nmap Xmas Scan"; flags:FPU; threshold: type both, track by_src, count 5, seconds 10; sid:1000003;)

alert tcp any any -> $HOME_NET 22 (msg:"SSH Brute-Force Attempt"; flow:established; content:"SSH"; nocase; threshold: type threshold, track by_src, count 5, seconds 60; sid:1000004;)

alert http any any -> $HOME_NET any (msg:"Potential C2 Beacon"; http.uri; content:"/api/checkin"; nocase; sid:1000005;)
```

sudo suricata -T -c /etc/suricata/suricata.yaml -v

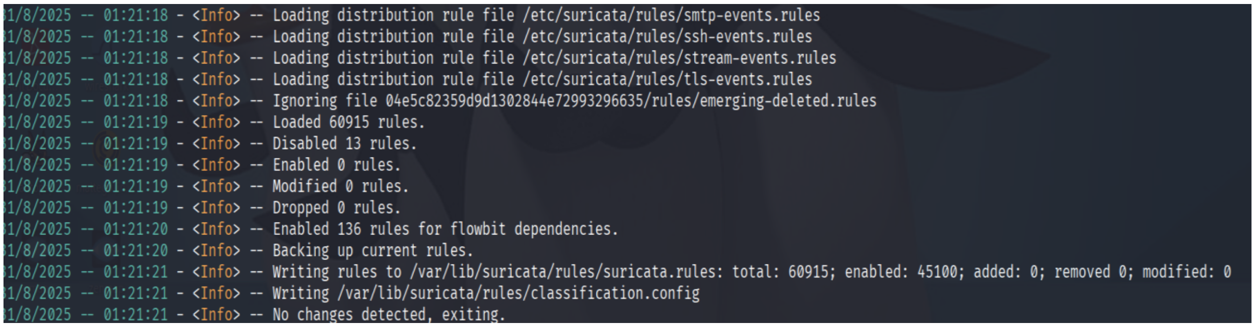


```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
[sudo] password for kali:
Notice: suricata: This is Suricata version 7.0.11 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 6
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine 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. 44821 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 44824 signatures processed. 955 are IP-only rules, 4385 are inspecting packet payload, 39259 inspect application layer, 109 are decoder event o
nly
Notice: suricata: Configuration provided was successfully loaded. Exiting.
```

sudo suricata-update



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo suricata-update

1/9/2025 -- 05:32:51 - <Info> -- Using data-directory /var/lib/suricata.
1/9/2025 -- 05:32:51 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
1/9/2025 -- 05:32:51 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
1/9/2025 -- 05:32:51 - <Info> -- Found Suricata version 7.0.11 at /usr/bin/suricata.
1/9/2025 -- 05:32:51 - <Info> -- Loading /etc/suricata/suricata.yaml
1/9/2025 -- 05:32:51 - <Info> -- Disabling rules for protocol pgsql
1/9/2025 -- 05:32:51 - <Info> -- Disabling rules for protocol modbus
1/9/2025 -- 05:32:51 - <Info> -- Disabling rules for protocol dnp3
1/9/2025 -- 05:32:51 - <Info> -- Disabling rules for protocol enip
1/9/2025 -- 05:32:51 - <Info> -- No sources configured, will use Emerging Threats Open
1/9/2025 -- 05:32:51 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.11/emerging.rules.tar.gz.
 100% - 5042660/5042660
1/9/2025 -- 05:33:01 - <Info> -- Done.
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/http2-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/mqtt-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/quic-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/rfb-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
1/9/2025 -- 05:33:01 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
```



```
31/8/2025 -- 01:21:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
31/8/2025 -- 01:21:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/ssh-events.rules
31/8/2025 -- 01:21:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
31/8/2025 -- 01:21:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
31/8/2025 -- 01:21:18 - <Info> -- Ignoring file 04e5c82359d9d1302844e72993296635/rules/emerging-deleted.rules
31/8/2025 -- 01:21:19 - <Info> -- Loaded 60915 rules.
31/8/2025 -- 01:21:19 - <Info> -- Disabled 13 rules.
31/8/2025 -- 01:21:19 - <Info> -- Enabled 0 rules.
31/8/2025 -- 01:21:19 - <Info> -- Modified 0 rules.
31/8/2025 -- 01:21:19 - <Info> -- Dropped 0 rules.
31/8/2025 -- 01:21:20 - <Info> -- Enabled 136 rules for flowbit dependencies.
31/8/2025 -- 01:21:20 - <Info> -- Backing up current rules.
31/8/2025 -- 01:21:21 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 60915; enabled: 45100; added: 0; removed 0; modified: 0
31/8/2025 -- 01:21:21 - <Info> -- Writing /var/lib/suricata/rules/classification.config
31/8/2025 -- 01:21:21 - <Info> -- No changes detected, exiting.
```

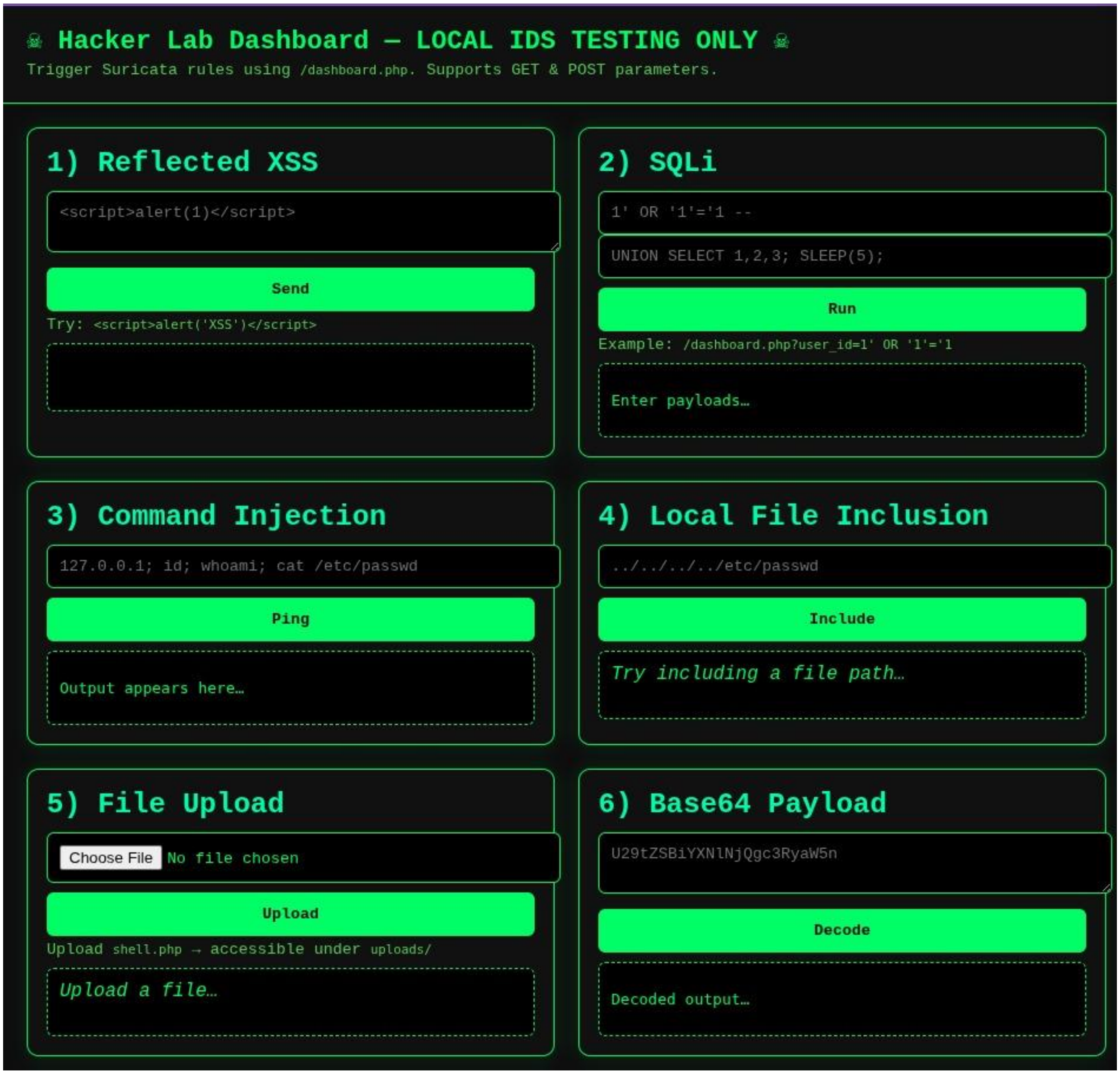
Dashboard creation for testing:

Install Apache and PHP:

sudo apt install apache2 php libapache2-mod-php -y

Commands need to be used:

- ✓ Open the terminal where the dashboard.php file is located.
- ✓ Then run: sudo cp ~/Downloads/dashboard.php /var/www/html/
- ✓ sudo chown www-data:www-data /var/www/html/dashboard.php
- ✓ sudo chmod 644 /var/www/html/dashboard.php
- ✓ Go to the browser and open: http://localhost/dashboard.php



☠ Hacker Lab Dashboard — LOCAL IDS TESTING ONLY ☠

Trigger Suricata rules using /dashboard.php. Supports GET & POST parameters.

1) Reflected XSS

<script>alert(1)</script>

Try: <script>alert('XSS')</script>

2) SQLi

1' OR '1'='1 --

UNION SELECT 1,2,3; SLEEP(5);

Example: /dashboard.php?user_id=1' OR '1'='1

Enter payloads…

3) Command Injection

127.0.0.1; id; whoami; cat /etc/passwd

Output appears here…

4) Local File Inclusion

../../../../etc/passwd

Try including a file path…

5) File Upload

No file chosen

Upload shell.php → accessible under uploads/

Upload a file…

6) Base64 Payload

U29tZSBiYXNlNjQgc3RyaW5n

Decoded output…

Testing & Results

Reconnaissance Scans Testing

Rule Tested: SYN Scan Detection (SID: 1000001)
Attack Command:

```
nmap -sS <ip address>
```

SSH Connection Testing

Rule Tested: SSH Connection Attempt (SID: 1000001, 1000002)
Attack Command:

```
nmap -p 22 <ip address>
```

DNS Query/Response Testing

Rule Tested: DNS Query/Response (SID: 1000007, 1000008)
Attack Command:

```
dig @<ip address>google.com
```

Web Application Attacks Testing

Rule Tested: SQL Injection, XSS, Directory Traversal, Command Injection (SID: 2000017–2000022)

✓ **SQL Injection Test**

```
curl "http:// <ip address>/login.php?id=1' OR '1'='1"
```

✓ **XSS Test**

```
curl "http:// <ip address>/login.php?q=<script>alert('XSS')</script>"
```

✓ **Directory Traversal Test**

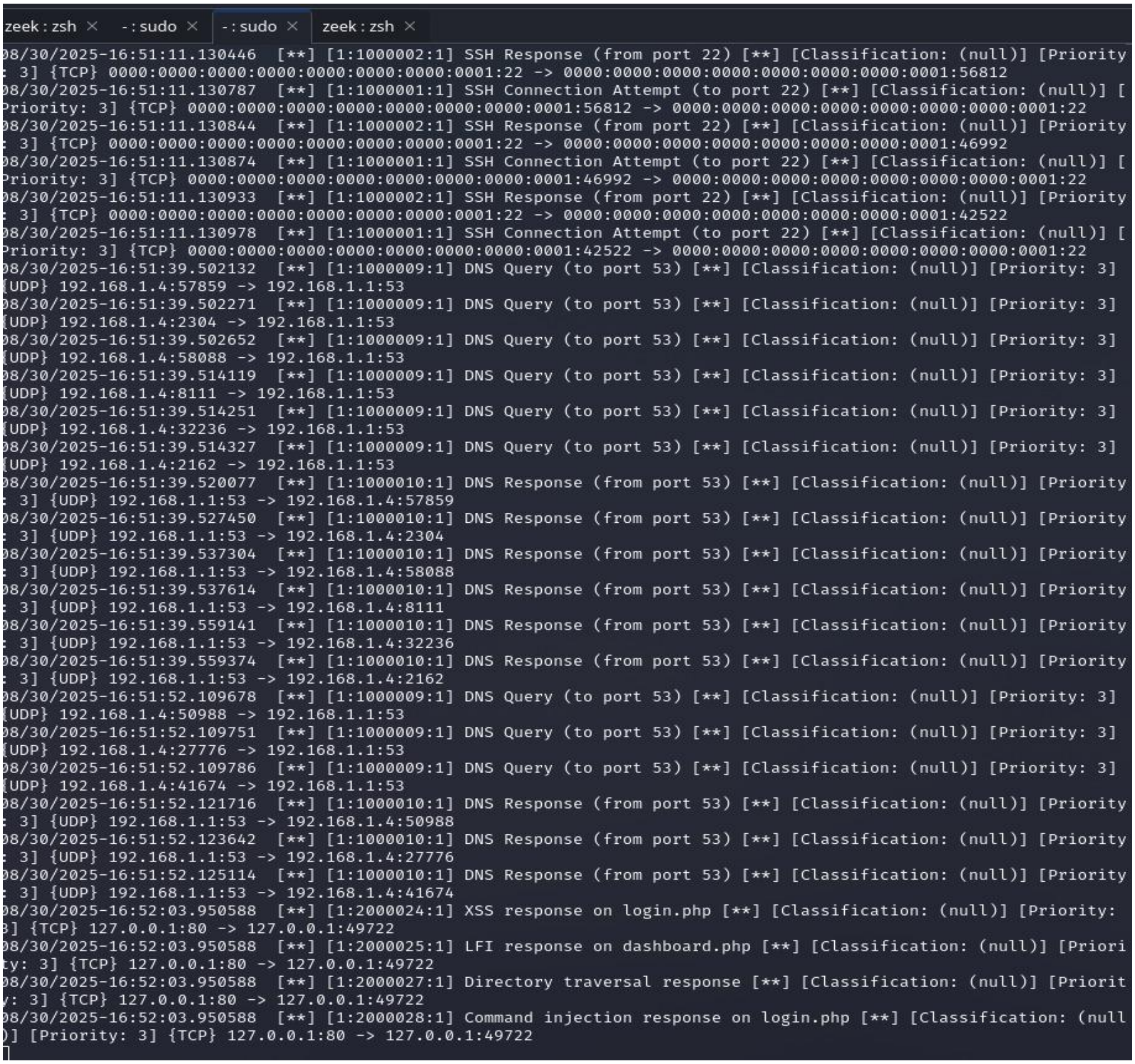
```
curl "http:// <ip address>/login.php?page=../../../../etc/passwd"
```

✓ **Command Injection Test**

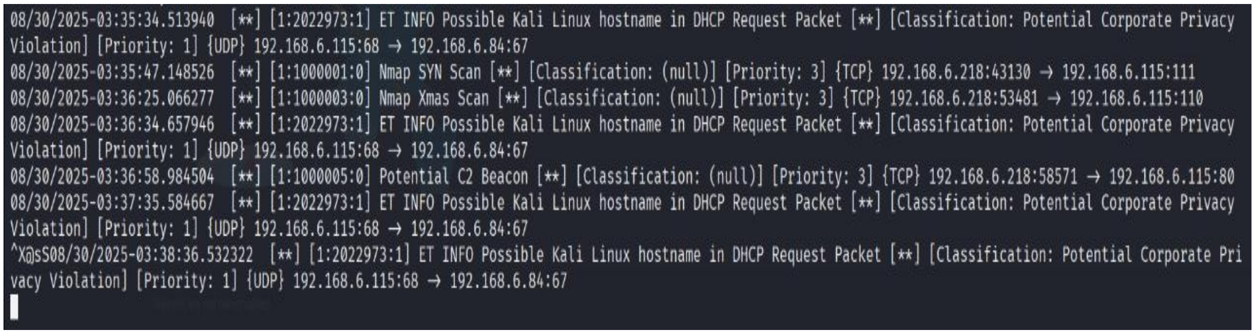
```
curl http://<ip address>/login.php?cmd=ls%20-al
```

To check the logs, use command:

```
tail -f /var/log/suricata/fast.log
```



```
08/30/2025-16:51:11.130446  [**] [1:1000002:1] SSH Response (from port 22) [**] [Classification: (null)] [Priority
: 3] {TCP} 0000:0000:0000:0000:0000:0000:0000:0001:22 -> 0000:0000:0000:0000:0000:0000:0000:0001:56812
08/30/2025-16:51:11.130787  [**] [1:1000001:1] SSH Connection Attempt (to port 22) [**] [Classification: (null)] [
Priority: 3] {TCP} 0000:0000:0000:0000:0000:0000:0000:0001:56812 -> 0000:0000:0000:0000:0000:0000:0000:0001:22
08/30/2025-16:51:11.130844  [**] [1:1000002:1] SSH Response (from port 22) [**] [Classification: (null)] [Priority
: 3] {TCP} 0000:0000:0000:0000:0000:0000:0000:0001:22 -> 0000:0000:0000:0000:0000:0000:0000:0001:46992
08/30/2025-16:51:11.130874  [**] [1:1000001:1] SSH Connection Attempt (to port 22) [**] [Classification: (null)] [
Priority: 3] {TCP} 0000:0000:0000:0000:0000:0000:0000:0001:46992 -> 0000:0000:0000:0000:0000:0000:0000:0001:22
08/30/2025-16:51:11.130933  [**] [1:1000002:1] SSH Response (from port 22) [**] [Classification: (null)] [Priority
: 3] {TCP} 0000:0000:0000:0000:0000:0000:0000:0001:22 -> 0000:0000:0000:0000:0000:0000:0000:0001:42522
08/30/2025-16:51:11.130978  [**] [1:1000001:1] SSH Connection Attempt (to port 22) [**] [Classification: (null)] [
Priority: 3] {TCP} 0000:0000:0000:0000:0000:0000:0000:0001:42522 -> 0000:0000:0000:0000:0000:0000:0000:0001:22
08/30/2025-16:51:39.502132  [**] [1:1000009:1] DNS Query (to port 53) [**] [Classification: (null)] [Priority: 3]
{UDP} 192.168.1.4:57859 -> 192.168.1.1:53
08/30/2025-16:51:39.502271  [**] [1:1000009:1] DNS Query (to port 53) [**] [Classification: (null)] [Priority: 3]
{UDP} 192.168.1.4:2304 -> 192.168.1.1:53
08/30/2025-16:51:39.502652  [**] [1:1000009:1] DNS Query (to port 53) [**] [Classification: (null)] [Priority: 3]
{UDP} 192.168.1.4:58088 -> 192.168.1.1:53
08/30/2025-16:51:39.514119  [**] [1:1000009:1] DNS Query (to port 53) [**] [Classification: (null)] [Priority: 3]
{UDP} 192.168.1.4:8111 -> 192.168.1.1:53
08/30/2025-16:51:39.514251  [**] [1:1000009:1] DNS Query (to port 53) [**] [Classification: (null)] [Priority: 3]
{UDP} 192.168.1.4:32236 -> 192.168.1.1:53
08/30/2025-16:51:39.514327  [**] [1:1000009:1] DNS Query (to port 53) [**] [Classification: (null)] [Priority: 3]
{UDP} 192.168.1.4:2162 -> 192.168.1.1:53
08/30/2025-16:51:39.520077  [**] [1:1000010:1] DNS Response (from port 53) [**] [Classification: (null)] [Priority
: 3] {UDP} 192.168.1.1:53 -> 192.168.1.4:57859
08/30/2025-16:51:39.527450  [**] [1:1000010:1] DNS Response (from port 53) [**] [Classification: (null)] [Priority
: 3] {UDP} 192.168.1.1:53 -> 192.168.1.4:2304
08/30/2025-16:51:39.537304  [**] [1:1000010:1] DNS Response (from port 53) [**] [Classification: (null)] [Priority
: 3] {UDP} 192.168.1.1:53 -> 192.168.1.4:58088
08/30/2025-16:51:39.537614  [**] [1:1000010:1] DNS Response (from port 53) [**] [Classification: (null)] [Priority
: 3] {UDP} 192.168.1.1:53 -> 192.168.1.4:8111
08/30/2025-16:51:39.559141  [**] [1:1000010:1] DNS Response (from port 53) [**] [Classification: (null)] [Priority
: 3] {UDP} 192.168.1.1:53 -> 192.168.1.4:32236
08/30/2025-16:51:39.559374  [**] [1:1000010:1] DNS Response (from port 53) [**] [Classification: (null)] [Priority
: 3] {UDP} 192.168.1.1:53 -> 192.168.1.4:2162
08/30/2025-16:51:52.109678  [**] [1:1000009:1] DNS Query (to port 53) [**] [Classification: (null)] [Priority: 3]
{UDP} 192.168.1.4:50988 -> 192.168.1.1:53
08/30/2025-16:51:52.109751  [**] [1:1000009:1] DNS Query (to port 53) [**] [Classification: (null)] [Priority: 3]
{UDP} 192.168.1.4:27776 -> 192.168.1.1:53
08/30/2025-16:51:52.109786  [**] [1:1000009:1] DNS Query (to port 53) [**] [Classification: (null)] [Priority: 3]
{UDP} 192.168.1.4:41674 -> 192.168.1.1:53
08/30/2025-16:51:52.121716  [**] [1:1000010:1] DNS Response (from port 53) [**] [Classification: (null)] [Priority
: 3] {UDP} 192.168.1.1:53 -> 192.168.1.4:50988
08/30/2025-16:51:52.123642  [**] [1:1000010:1] DNS Response (from port 53) [**] [Classification: (null)] [Priority
: 3] {UDP} 192.168.1.1:53 -> 192.168.1.4:27776
08/30/2025-16:51:52.125114  [**] [1:1000010:1] DNS Response (from port 53) [**] [Classification: (null)] [Priority
: 3] {UDP} 192.168.1.1:53 -> 192.168.1.4:41674
08/30/2025-16:52:03.950588  [**] [1:2000024:1] XSS response on login.php [**] [Classification: (null)] [Priority:
3] {TCP} 127.0.0.1:80 -> 127.0.0.1:49722
08/30/2025-16:52:03.950588  [**] [1:2000025:1] LFI response on dashboard.php [**] [Classification: (null)] [Priori
ty: 3] {TCP} 127.0.0.1:80 -> 127.0.0.1:49722
08/30/2025-16:52:03.950588  [**] [1:2000027:1] Directory traversal response [**] [Classification: (null)] [Priorit
y: 3] {TCP} 127.0.0.1:80 -> 127.0.0.1:49722
08/30/2025-16:52:03.950588  [**] [1:2000028:1] Command injection response on login.php [**] [Classification: (null
)] [Priority: 3] {TCP} 127.0.0.1:80 -> 127.0.0.1:49722
```



```
08/30/2025-03:35:34.513940  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy
Violation] [Priority: 1] {UDP} 192.168.6.115:68 → 192.168.6.84:67
08/30/2025-03:35:47.148526  [**] [1:1000001:0] Nmap SYN Scan [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.6.218:43130 → 192.168.6.115:111
08/30/2025-03:36:25.066277  [**] [1:1000003:0] Nmap Xmas Scan [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.6.218:53481 → 192.168.6.115:110
08/30/2025-03:36:34.657946  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy
Violation] [Priority: 1] {UDP} 192.168.6.115:68 → 192.168.6.84:67
08/30/2025-03:36:58.984504  [**] [1:1000005:0] Potential C2 Beacon [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.6.218:58571 → 192.168.6.115:80
08/30/2025-03:37:35.584667  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy
Violation] [Priority: 1] {UDP} 192.168.6.115:68 → 192.168.6.84:67
^X@sS08/30/2025-03:38:36.532322  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Pri
vacy Violation] [Priority: 1] {UDP} 192.168.6.115:68 → 192.168.6.84:67
```

Challenges Faced

- ✓ **Rule Syntax Errors**: Initial rules had syntax issues with threshold declarations and content formatting
- ✓ **Network Configuration**: Required multiple attempts to configure bridged networking correctly
- ✓ **Alert Verification**: Some rules required specific traffic patterns to trigger alerts
- ✓ **Suricata Version Compatibility**: Certain rule syntax elements behaved differently in Suricata 7.0.11

Areas for Improvement:

- ✓ **Reduce False Positives:** Refine rules using stricter thresholds and whitelists to prevent benign traffic from triggering alerts.
- ✓ **Minimize False Negatives:** Expand ruleset coverage with updated threat intelligence to detect evasive and advanced attacks.
- ✓ **Implement Automated Testing:** Develop a pipeline using malicious/benign traffic samples to quantitatively measure detection accuracy and reduce alert fatigue.

Conclusion

This project successfully demonstrated the implementation of a robust Network Intrusion Detection System using Suricata on Kali Linux, which effectively detected various cyber threats including reconnaissance scans, web application attacks, and suspicious network activities through a carefully crafted custom ruleset. Despite initial challenges with rule syntax and network configuration, the system achieved its core objective of real-time threat detection, reducing the mean time to identify potential security incidents, while highlighting the critical importance of custom rule tuning for minimizing false positives and addressing organization-specific security needs. The hands-on experience gained in configuring, testing, and optimizing the NIDS provides a solid foundation for practical network security monitoring and underscores the value of tailored detection rules in enhancing overall cybersecurity posture.