Project Report: WordPress Hosting, Security Monitoring, and Attack Simulation on Ubuntu Server

Report Issued : 26/06/2025

Submitted by : Rashid Ok

Table of Contents

1. Introduction

This project focuses on deploying a secure WordPress hosting environment using Ubuntu 24.04 on VirtualBox. Key security integrations include Splunk for centralized logging, Snort for intrusion detection, Fail2Ban for automated IP banning, and the ELK stack (Elasticsearch, Logstash, Kibana) for comprehensive log analysis. The project concludes with attack simulations (Brute Force, SQL Injection, XSS) to validate monitoring and defense mechanisms.

1.1 Project Overview

This project demonstrates the deployment and security monitoring of a self-hosted WordPress website on an Ubuntu 24.04 server. The goal is to simulate a production-like environment with layered security and logging mechanisms to detect and prevent cyberattacks such as brute force, SQL injection (SQLi), and cross-site scripting (XSS).

Security solutions like **Snort** (Intrusion Detection System), **Fail2Ban** (Intrusion Prevention System), **Splunk**, and the **ELK Stack** (Elasticsearch, Logstash, Kibana, Filebeat) were configured to collect, analyze, and visualize logs from Apache, WordPress, MySQL, and Snort.

Additionally, various simulated attacks were executed to validate the effectiveness of the detection and prevention systems.

1.2 Objectives

- **Deploy a functional WordPress site** using Apache, MySQL, and PHP.
- **Configure Snort IDS** with custom rules to detect specific attack patterns (SQLi, XSS, Command Injection, brute force).
- **Implement Fail2Ban** to automatically ban IPs based on Snort alerts and Apache logs.
- **Set up Splunk and ELK Stack** to collect and visualize logs from WordPress, Apache, and Snort for real-time monitoring.

- **Perform attack simulations** (e.g., SQLi, brute force, XSS) and verify detection and prevention mechanisms.
- **Build hands-on experience** in Linux server administration, log forwarding, IDS/IPS tuning, and SIEM dashboard usage.

2. Tools and Sub-Tools Overview

2.1 ELK Stack

- **Elasticsearch**: Stores and indexes logs collected from various sources (syslog, Apache logs, Snort alerts) for fast searching and analytics.
- **Logstash**: Acts as a data processing pipeline, ingesting logs from multiple files, parsing, and forwarding them into Elasticsearch.
- **Kibana**: Provides a web-based user interface to visualize and analyze log data stored in Elasticsearch.
- **Filebeat** (optional, if used): Lightweight log shipper installed on Ubuntu to forward system and application logs to Logstash or Elasticsearch.

2.2 Splunk

- **Splunk Enterprise (Windows)**: Centralized platform for collecting, indexing, and visualizing logs forwarded from Ubuntu server.
- **Splunk Universal Forwarder (Ubuntu)**: Installed on Ubuntu to monitor key log files (auth.log, syslog, Apache access/error logs, Snort alerts) and forward them securely to Splunk Enterprise for centralized analys

2.3 Snort IDS

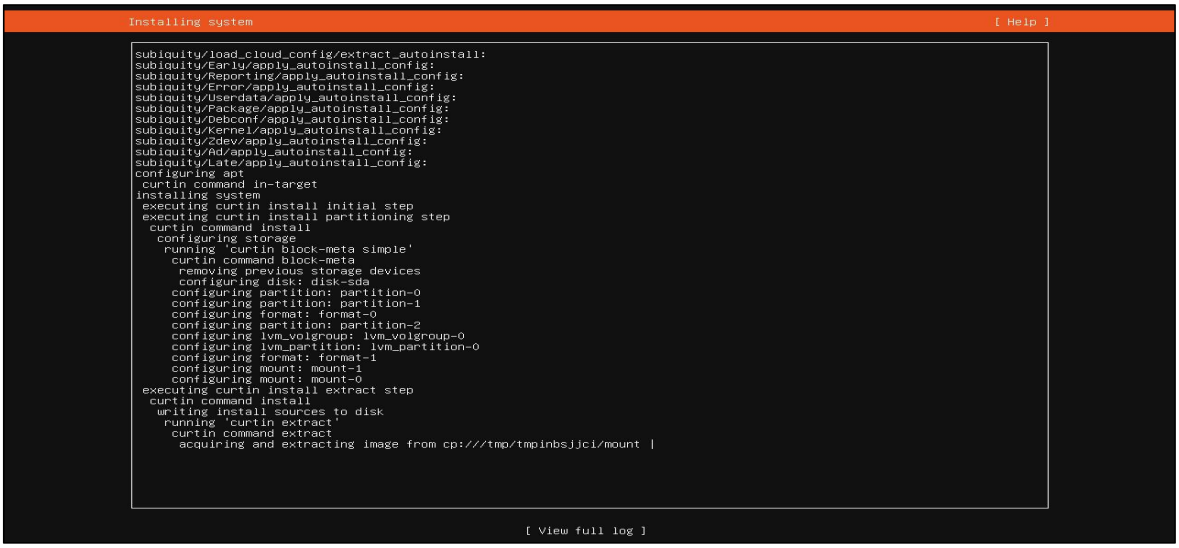
- Network Intrusion Detection System monitoring traffic on the server.
- Detects various attacks (ICMP scanning, SSH attempts, HTTP access, WordPress login attempts, SQL injection, XSS, command injection).
- Custom Snort rules written to identify specific threats relevant to WordPress and SSH.
- Outputs alerts logged locally and forwarded to Splunk/ELK for monitoring.

2.4 Fail2Ban

- Monitors log files for suspicious patterns (using custom filters based on Snort alerts and Apache logs).
- Filters located in /etc/fail2ban/filter.d/ define patterns for brute force and web attacks (WordPress brute force, SQLi, XSS).
- Jails configured in /etc/fail2ban/jail.local specify which logs to monitor and ban policies (ban time, retry limits).
- Automatically bans IP addresses exhibiting malicious behavior to prevent continued attacks.

3. Environment Setup

Insatalling Ubuntu server in VirtualBox/Vmware



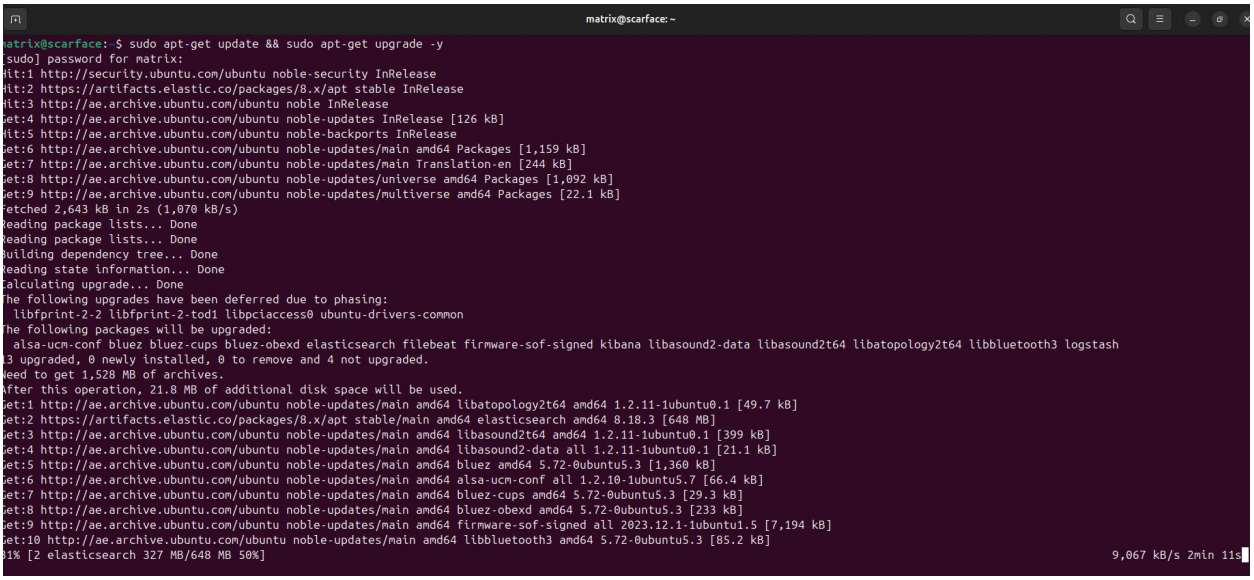
3.1 Updating and Upgrading Ubuntu Packages

- **Update package lists** – Fetches the latest list of available packages.

  sudo apt-get update

- **Upgrade installed packages** – Installs latest versions of installed software.

  sudo apt-get upgrade -y



```
matrix@scarface: ~
matrix@scarface:~$ sudo apt-get update && sudo apt-get upgrade -y
[sudo] password for matrix:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:3 http://ae.archive.ubuntu.com/ubuntu noble InRelease
Get:4 http://ae.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:5 http://ae.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:6 http://ae.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,159 kB]
Get:7 http://ae.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [244 kB]
Get:8 http://ae.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,092 kB]
Get:9 http://ae.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [22.1 kB]
Fetched 2,643 kB in 2s (1,070 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following upgrades have been deferred due to phasing:
  libfprint-2-2 libfprint-2-tod1 libpciaccess0 ubuntu-drivers-common
The following packages will be upgraded:
  alsa-ucm-conf bluez bluez-cups bluez-obexd elasticsearch filebeat firmware-sof-signed kibana libasound2-data libasound2t64 libatopology2t64 libbluetooth3 logstash
13 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
Need to get 1,528 MB of archives.
After this operation, 21.8 MB of additional disk space will be used.
Get:1 http://ae.archive.ubuntu.com/ubuntu noble-updates/main amd64 libatopology2t64 amd64 1.2.11-1ubuntu0.1 [49.7 kB]
Get:2 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.18.3 [648 MB]
Get:3 http://ae.archive.ubuntu.com/ubuntu noble-updates/main amd64 libasound2t64 amd64 1.2.11-1ubuntu0.1 [399 kB]
Get:4 http://ae.archive.ubuntu.com/ubuntu noble-updates/main amd64 libasound2-data all 1.2.11-1ubuntu0.1 [21.1 kB]
Get:5 http://ae.archive.ubuntu.com/ubuntu noble-updates/main amd64 bluez amd64 5.72-0ubuntu5.3 [1,360 kB]
Get:6 http://ae.archive.ubuntu.com/ubuntu noble-updates/main amd64 alsa-ucm-conf all 1.2.10-1ubuntu5.7 [66.4 kB]
Get:7 http://ae.archive.ubuntu.com/ubuntu noble-updates/main amd64 bluez-cups amd64 5.72-0ubuntu5.3 [29.3 kB]
Get:8 http://ae.archive.ubuntu.com/ubuntu noble-updates/main amd64 bluez-obexd amd64 5.72-0ubuntu5.3 [233 kB]
Get:9 http://ae.archive.ubuntu.com/ubuntu noble-updates/main amd64 firmware-sof-signed all 2023.12.1-1ubuntu1.5 [7,194 kB]
Get:10 http://ae.archive.ubuntu.com/ubuntu noble-updates/main amd64 libbluetooth3 amd64 5.72-0ubuntu5.3 [85.2 kB]
31% [2 elasticsearch 327 MB/648 MB 50%]                                                                    9,067 kB/s 2min 11s
```

4. Apache and Wordpress Installation and Configuration

Installing Apache, PHP, MySQL, and Required Modules

Install Apache, PHP, MySQL and required modules – Provides the web and database server environment for WordPress.

```
sudo apt install apache2 php libapache2-mod-php mysql-server php-mysql -y
```

4.1 Starting and Enabling Apache Service

- Enable Apache to start at boot – Ensures Apache runs after system reboots.

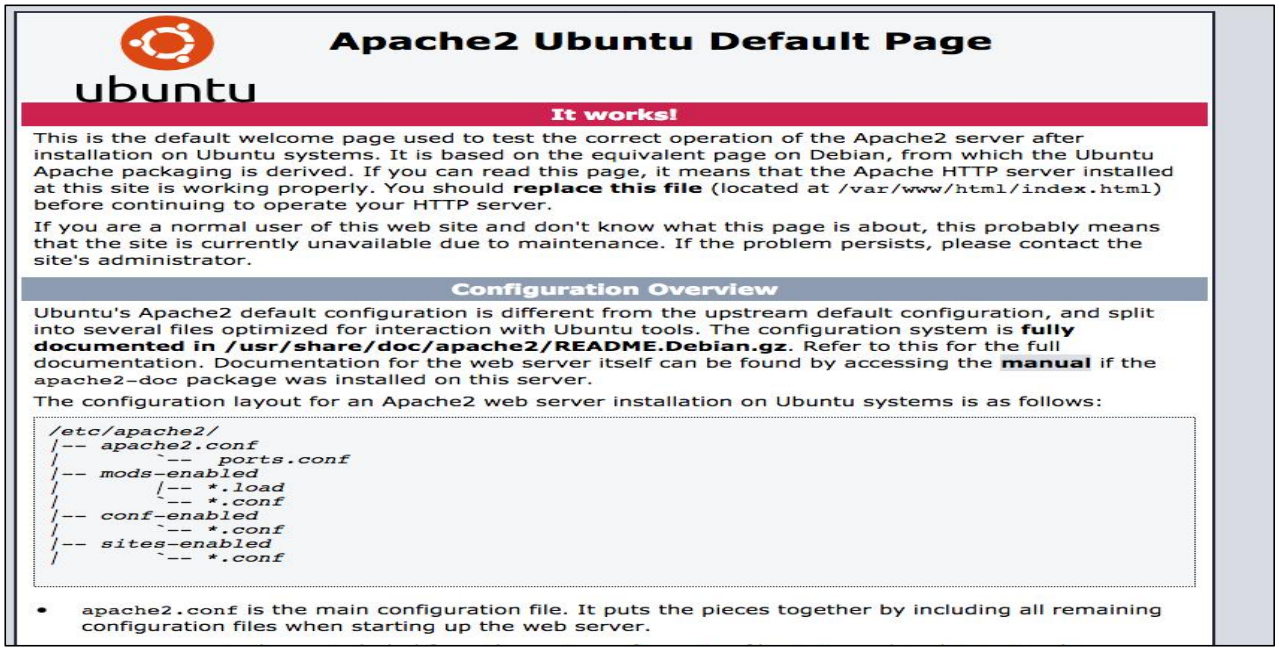
```
sudo systemctl enable apache2
```

- Start Apache service immediately.

```
sudo systemctl start apache2
```

- Check Apache service status.

```
sudo systemctl status apache2
```



4.3 WordPress Download and Setup

Navigate to web root directory.

- Download latest WordPress package.

```
sudo wget https://wordpress.org/latest.tar.gz
```

- Extract WordPress archive.

```
sudo tar -xvzf latest.tar.gz
```

- Move WordPress files to web root.

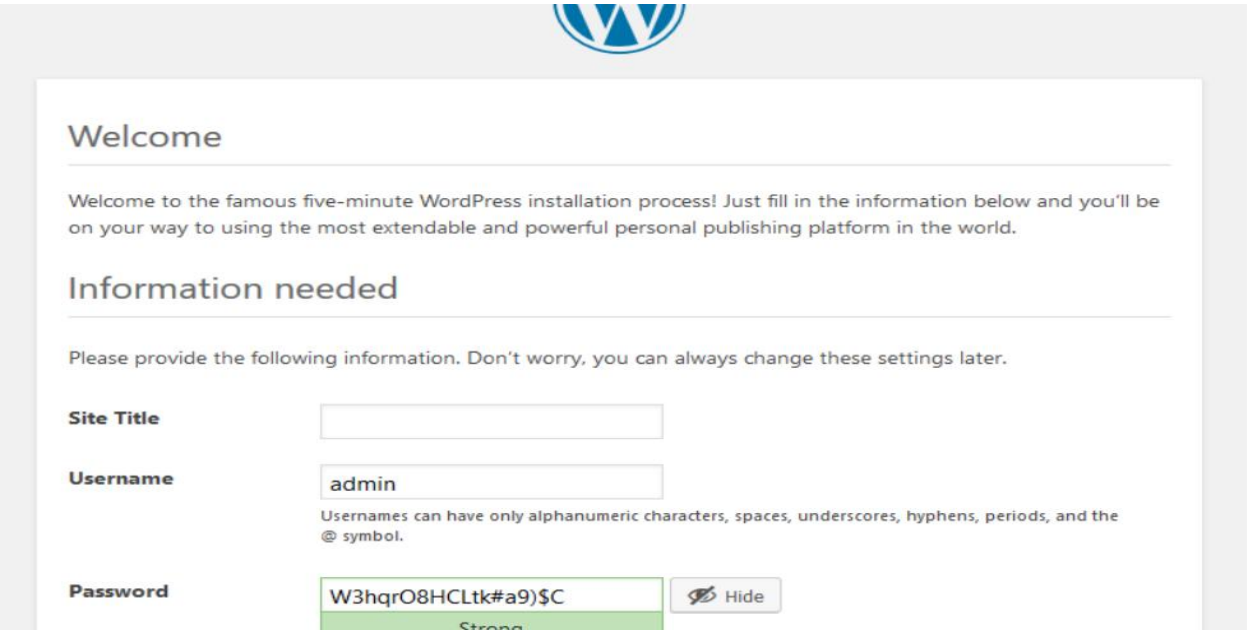
```
sudo mv wordpress/* ./
```

- Set ownership to Apache user (www-data).

```
sudo chown -R www-data:www-data /var/www/html
```

- Set appropriate file permissions.

```
sudo chmod -R 755 /var/www/html
```



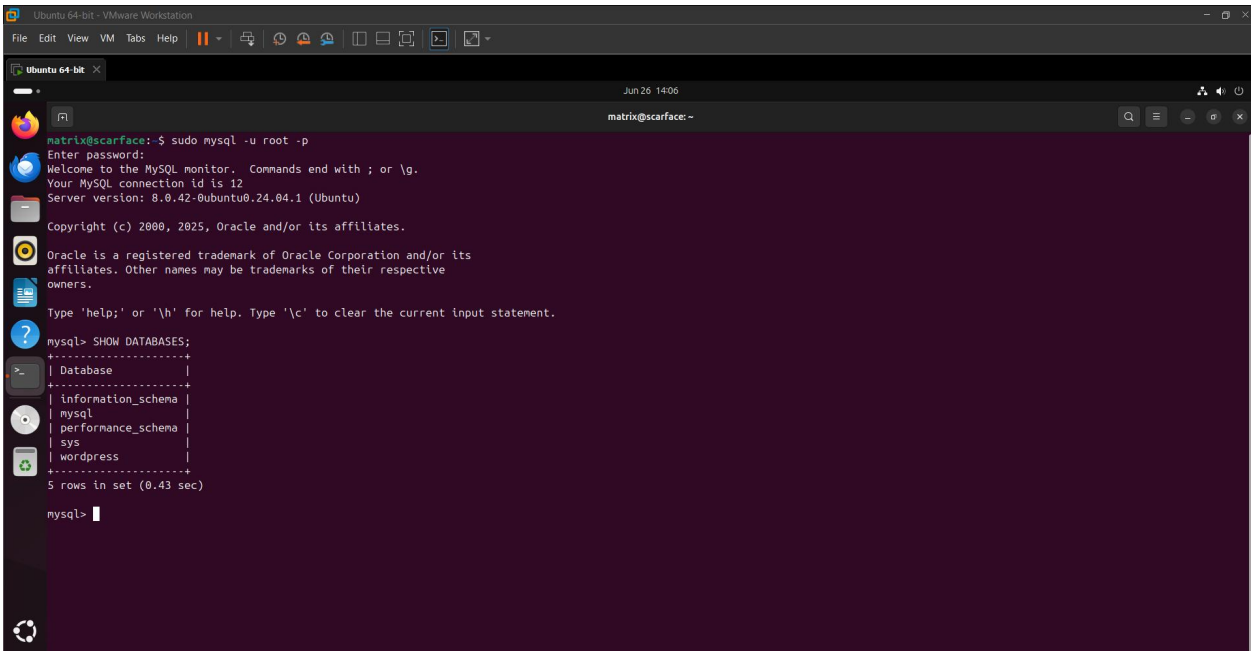
4.4 Configuring MySQL for WordPress

- Access MySQL shell.

```
sudo mysql -u root -p
```

- Create WordPress database and user with privileges.

```
CREATE DATABASE wordpress;
CREATE USER 'wpuser'@'localhost' 'wpuser'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```



4.5 Apache Virtual Host Configuration

- Create virtual host configuration file.

```
sudo nano /etc/apache2/sites-available/wordpress.conf
```

- Paste the following virtual host configuration.

```
<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html
  ServerName yourdomain.com
  <Directory /var/www/html>
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
  </Directory>
  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

- Enable the new site and reload Apache.

```
sudo a2ensite wordpress.conf
sudo systemctl reload apache2
```

4.6 WordPress Configuration File Setup

- Rename sample config file.

```
sudo mv wp-config-sample.php wp-config.php
```

- Edit database connection details.

```
sudo nano wp-config.php
```

- Update DB settings.

```
define('DB_NAME',   'wordpress');define('DB_USER',   'wpuser');define('DB_PASSWORD',
'password');define('DB_HOST', 'localhost');
```

5. Splunk Enterprise on Windows

Purpose

Splunk Enterprise acts as a centralized log collection and analysis platform. Itreceives logs forwarded from the Ubuntu server and provides a user-friendly Interface for searching, alerting, and visualizing data.

Steps and Commands

5.1 Accessing Splunk Web Interface

- Access Splunk Web Interface

Open your browser and navigate to:

http://127.0.0.1:8000

Login with your credentials

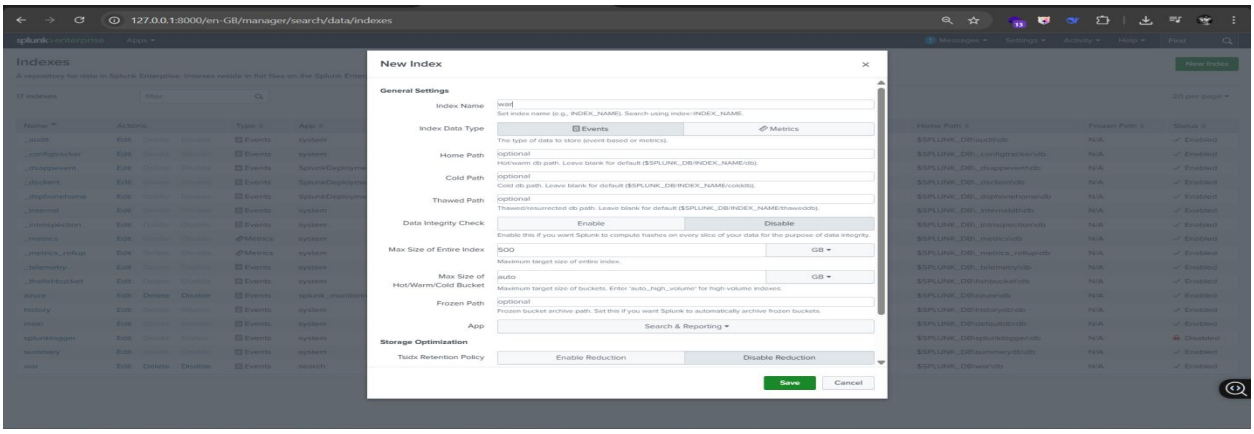
5.2 Creating Index for Log Storage

Create a new index named "war"

This index stores logs forwarded from Ubuntu.

Navigate to:

Settings > Indexes > New Index Enter “war” and save.

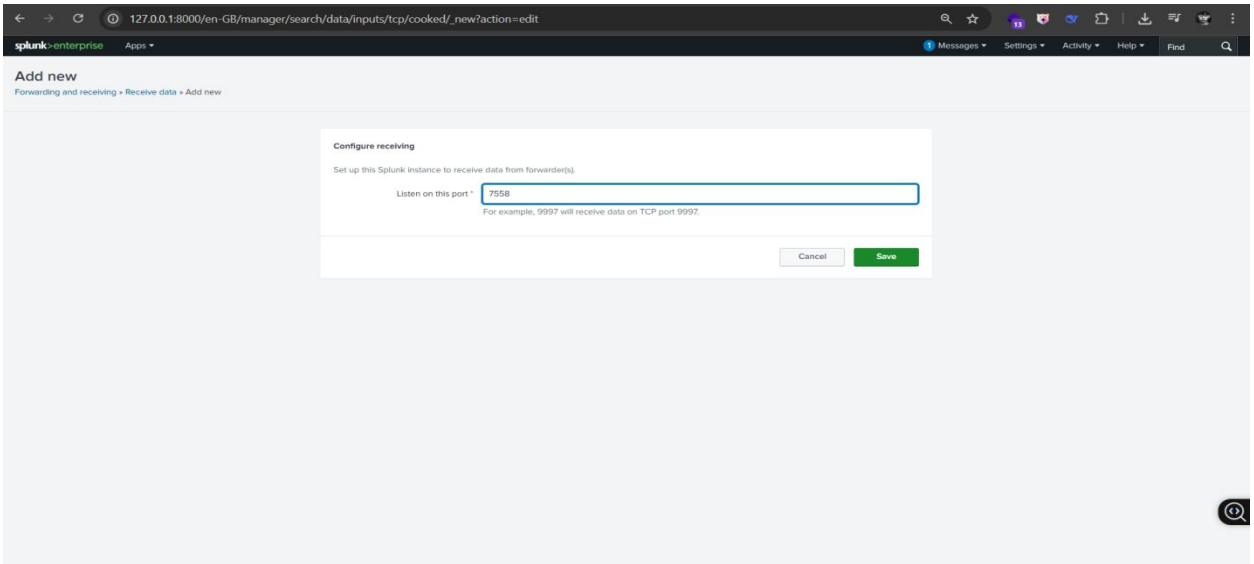


5.3 Configuring Receiving Port for Log Forwarding

Navigate to:

Settings > Forwarding and Receiving > Configure Receiving > Add New

Enter port 7558 and enable.



6. Splunk Universal Forwarder on Ubuntu

Purpose

Splunk Universal Forwarder runs on Ubuntu to monitor critical log files and securely forward them to Splunk Enterprise for central analysis.

Installation and Configuration Steps

6.1 **Installation and Extraction**

- Extract Splunk Forwarder package (adjust filename accordingly)

```
sudo tar xvzf /tmp/splunkforwarder--Linux--bit.tgz -C /opt
```

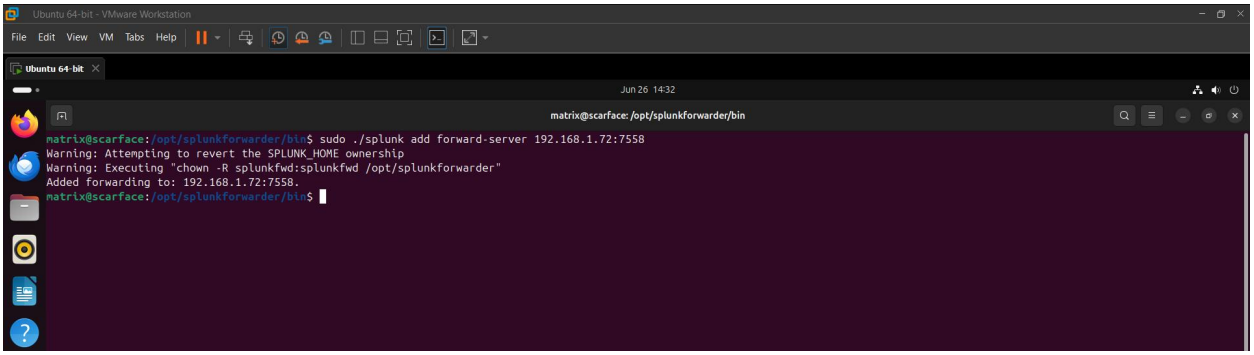
- Starting Forwarder and Accepting License

```
sudo ./splunk start --accept-license
```

6.3 Configuring Forward Server Connection

- Add Splunk Enterprise server as forward-server (replace <Windows_IP> with actual IP):

```
sudo ./splunk add forward-server <Windows_IP>:7558
```



6.4 Adding Log File Monitors

- Add monitors for critical logs:

```
sudo ./splunk add monitor /var/log/auth.log -index war
sudo ./splunk add monitor /var/log/syslog -index war
Sudo ./splunk add monitor /var/log/apache2/access.log -index war
sudo ./splunk add monitor /var/log/apache2/error.log -index war
sudo ./splunk add monitor /var/log/snort/snort.alert.fast -index war
```

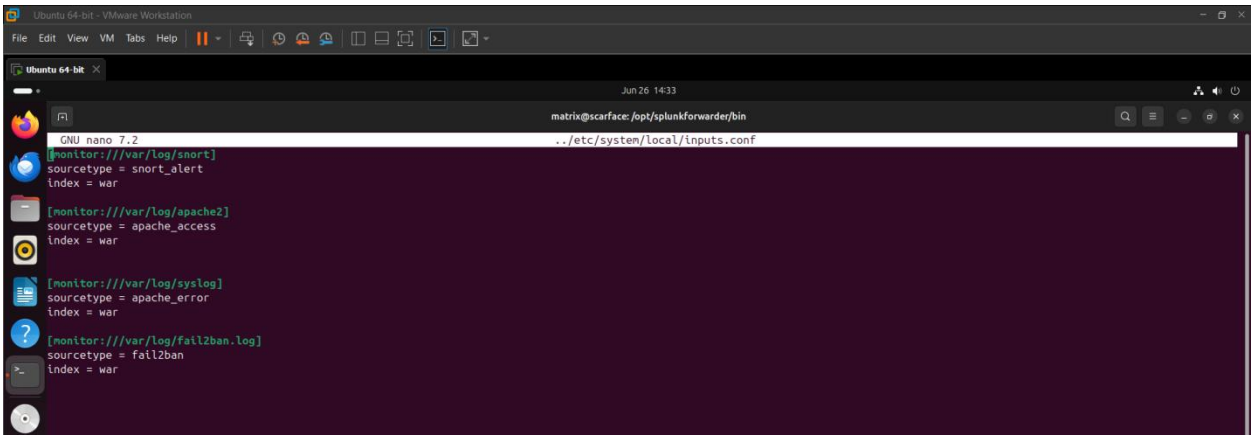
6.5 Manual Configuration via inputs.conf

- Alternative: Manual inputs.conf editing

```
sudo nano /opt/splunkforwarder/etc/system/local/inputs.conf
```

- Example content:

```
[monitor:///var/log/auth.log]
index = war

[monitor:///var/log/syslog]
index = war

[monitor:///var/log/apache2/access.log]
index = war

[monitor:///var/log/apache2/error.log]
index = war

[monitor:///var/log/snort/snort.alert.fast]
index = war
```


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Ubuntu 64-bit
Jun 26 14:33
matrix@scarface: /opt/splunkforwarder/bin
GNU nano 7.2 ../etc/system/local/inputs.conf
[monitor:///var/log/snort]
sourcetype = snort_alert
index = war
[monitor:///var/log/apache2]
sourcetype = apache_access
index = war
[monitor:///var/log/syslog]
sourcetype = apache_error
index = war
[monitor:///var/log/fail2ban.log]
sourcetype = fail2ban
index = war

7. ELK Stack Installation and Configuration on Ubuntu

Purpose

The ELK stack collects, processes, and visualizes logs locally on the Ubuntu server, providing another method for detailed log analysis and dashboarding.

Installation and Commands

7.1 Installing Elasticsearch

- Install Elasticsearch

```
sudo apt update
sudo apt install elasticsearch -y
sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch
```

- Configuring elasticsearch.yml hosts

```
Sudo nano /etc/elasticsearch/elasticsearch.yml
```

7.2 Installing and Configuring Logstash

- Install Logstash

```
sudo apt install logstash -y
```

Create Logstash configuration

```
sudo nano /etc/logstash/conf.d/logstash.conf
```

Add:

```
input {
 file {
   path => [
     "/var/log/syslog",
     "/var/log/apache2/access.log",
     "/var/log/apache2/error.log",
     "/var/log/snort/snort.alert.fast"
   ]
   start_position => "beginning"
   sincedb_path => "/dev/null"
 }
}

output {
 elasticsearch {
   hosts => ["localhost:9200"]
   index => "logs-%{+YYYY.MM.dd}"
 }
 stdout { codec => rubydebug }
}
```

- Start and enable Logstash

```
sudo systemctl enable logstash
sudo systemctl start logstash
```

7.3 Installing and Starting Kibana

- Install Kibana

```
sudo apt install kibana -y
sudo systemctl enable kibana
sudo systemctl start kibana
```

Configuring kibana.yml hosts

7.4 Installing and Filebeat

Filebeat was installed using the official APT repository:

```
sudo apt-get update
sudo apt-get install filebeat -y
```

Configuration Steps

- Enable Required Modules

To monitor Apache access/error logs and system authentication logs:

```
sudo filebeat modules enable apache
sudo filebeat modules enable system
```

You can view all available modules with:

filebeat modules list

Edit Filebeat Configuration

Filebeat's main configuration file was updated:

```
sudo nano /etc/filebeat/filebeat.yml
```

- **Option A – Output to Logstash:**

```
filebeat.inputs:
```

```
 - type: log
   enabled: true
   paths:
     - /var/log/auth.log
     - /var/log/apache2/*.log
output.logstash:
  hosts: ["localhost:5044"]
```

- **Option B – Output directly to Elasticsearch:**

```
output.elasticsearch:
  hosts: ["http://localhost:9200"]
```

If authentication is enabled:

```
  username: "elastic"
  password: "your_password"
```

- Start and Enable Filebeat

```
sudo systemctl enable filebeat
sudo systemctl start filebeat
sudo systemctl status filebeat
```

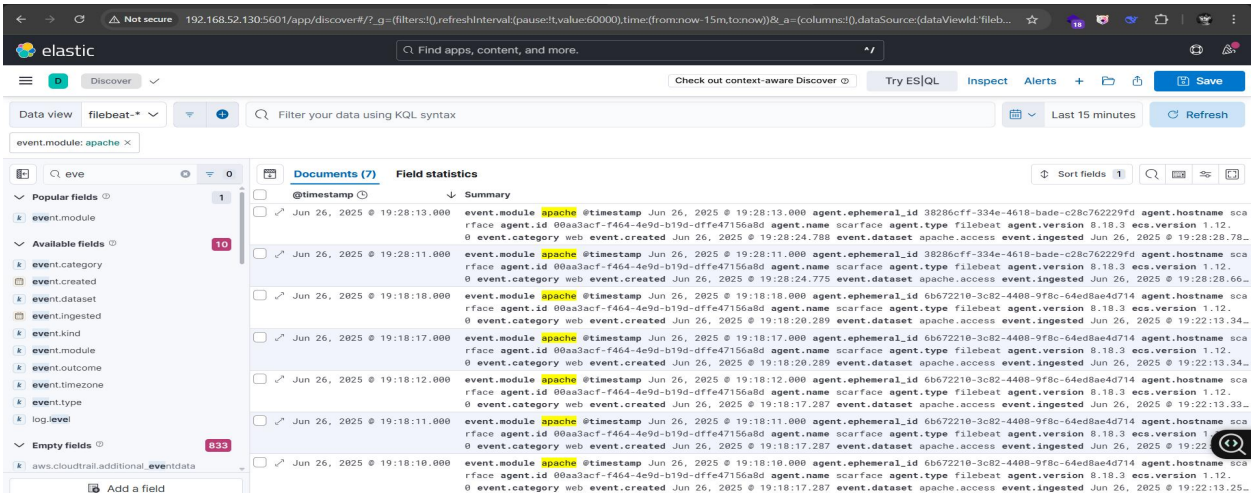
7.5 Accessing and Using Kibana Dashboard

Access Kibana Dashboard

Open browser and navigate to:

http://<your-ubuntu-ip>:5601

Configure index patterns to start visualizing the logs.


Not secure 192.168.52.130:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now-15m,to:now))&_a=(columns:!(),dataSource:(dataViewId:'fileb...
elastic
Find apps, content, and more.
Discover
Check out context-aware Discover
Try ES|QL
Inspect
Alerts
Save
Data view
filebeat-*
Filter your data using KQL syntax
Last 15 minutes
Refresh
event.module: apache
eve
Popular fields
event.module
Available fields
event.category
event.created
event.dataset
event.ingested
event.kind
event.module
event.outcome
event.timezone
event.type
log.level
Empty fields
aws.cloudtrail.additional_eventdata
Add a field
Documents (7)
Field statistics
Sort fields
@timestamp
Summary
Jun 26, 2025 @ 19:28:13.000 event.module apache @timestamp Jun 26, 2025 @ 19:28:13.000 agent.ephemeral_id 38286cff-334e-4618-bade-c28c762229fd agent.hostname scarface agent.id 00aa3acf-f464-4e9d-b19d-dffe47156a8d agent.name scarface agent.type filebeat agent.version 8.18.3 ecs.version 1.12.0 event.category web event.created Jun 26, 2025 @ 19:28:24.788 event.dataset apache.access event.ingested Jun 26, 2025 @ 19:28:28.78
Jun 26, 2025 @ 19:28:11.000 event.module apache @timestamp Jun 26, 2025 @ 19:28:11.000 agent.ephemeral_id 38286cff-334e-4618-bade-c28c762229fd agent.hostname scarface agent.id 00aa3acf-f464-4e9d-b19d-dffe47156a8d agent.name scarface agent.type filebeat agent.version 8.18.3 ecs.version 1.12.0 event.category web event.created Jun 26, 2025 @ 19:28:24.775 event.dataset apache.access event.ingested Jun 26, 2025 @ 19:28:28.66
Jun 26, 2025 @ 19:18:18.000 event.module apache @timestamp Jun 26, 2025 @ 19:18:18.000 agent.ephemeral_id 6b672210-3c82-4408-9f8c-64ed8ae4d714 agent.hostname scarface agent.id 00aa3acf-f464-4e9d-b19d-dffe47156a8d agent.name scarface agent.type filebeat agent.version 8.18.3 ecs.version 1.12.0 event.category web event.created Jun 26, 2025 @ 19:18:20.289 event.dataset apache.access event.ingested Jun 26, 2025 @ 19:22:13.34
Jun 26, 2025 @ 19:18:17.000 event.module apache @timestamp Jun 26, 2025 @ 19:18:17.000 agent.ephemeral_id 6b672210-3c82-4408-9f8c-64ed8ae4d714 agent.hostname scarface agent.id 00aa3acf-f464-4e9d-b19d-dffe47156a8d agent.name scarface agent.type filebeat agent.version 8.18.3 ecs.version 1.12.0 event.category web event.created Jun 26, 2025 @ 19:18:20.289 event.dataset apache.access event.ingested Jun 26, 2025 @ 19:22:13.34
Jun 26, 2025 @ 19:18:12.000 event.module apache @timestamp Jun 26, 2025 @ 19:18:12.000 agent.ephemeral_id 6b672210-3c82-4408-9f8c-64ed8ae4d714 agent.hostname scarface agent.id 00aa3acf-f464-4e9d-b19d-dffe47156a8d agent.name scarface agent.type filebeat agent.version 8.18.3 ecs.version 1.12.0 event.category web event.created Jun 26, 2025 @ 19:18:17.287 event.dataset apache.access event.ingested Jun 26, 2025 @ 19:22:13.33
Jun 26, 2025 @ 19:18:11.000 event.module apache @timestamp Jun 26, 2025 @ 19:18:11.000 agent.ephemeral_id 6b672210-3c82-4408-9f8c-64ed8ae4d714 agent.hostname scarface agent.id 00aa3acf-f464-4e9d-b19d-dffe47156a8d agent.name scarface agent.type filebeat agent.version 8.18.3 ecs.version 1 0 event.category web event.created Jun 26, 2025 @ 19:18:17.287 event.dataset apache.access event.ingested Jun 26, 2025 @ 19:22
Jun 26, 2025 @ 19:18:10.000 event.module apache @timestamp Jun 26, 2025 @ 19:18:10.000 agent.ephemeral_id 6b672210-3c82-4408-9f8c-64ed8ae4d714 agent.hostname scarface agent.id 00aa3acf-f464-4e9d-b19d-dffe47156a8d agent.name scarface agent.type filebeat agent.version 8.18.3 ecs.version 1.12.0 event.category web event.created Jun 26, 2025 @ 19:18:17.287 event.dataset apache.access event.ingested Jun 26, 2025 @ 19:22:13.25

8. Snort IDS Installation and Configuration

Purpose

Snort analyzes network traffic to detect malicious activities based on custom and standard rules, alerting when suspicious packets are seen.

Commands and Setup

8.1 Directory Setup for Snort

- Create necessary directories

```
sudo mkdir -p /etc/snort/rules /etc/snort/preproc_rules /var/log/snort /usr/local/lib/snort_dynamicrules
```

8.2 Editing Snort Configuration

- Edit Snort configuration

```
sudo nano /etc/snort/snort.conf
```

Set variables:

```
var HOME_NET 192.168.1.0/24var
 EXTERNAL_NET anyvar
 RULE_PATH    /etc/snort/rules
```

Include rules:

```
include $RULE_PATH/local.rules
include $RULE_PATH/community.rules
```

8.3 Adding and Customizing Snort Rules

Add custom rules to /etc/snort/rules/local.rules

Examples (including your new rules):

- alert tcp any any -> any 80 (msg:"Web Attack - Command Injection system("; content:"system("; nocase; sid:1002009; rev:1;)

- alert tcp any any -> $HOME_NET 80 (msg:"WordPress Bruteforce Attempt"; content:"POST"; content:"/wp-login.php"; threshold:type threshold, track by_src, count 5, seconds 30; sid:1006001; rev:1;)

- alert tcp any any -> $HOME_NET 80 (msg:"SQL Injection Attempt - ' OR 1=1"; content:"' OR 1=1"; nocase; sid:1002101; rev:1;)

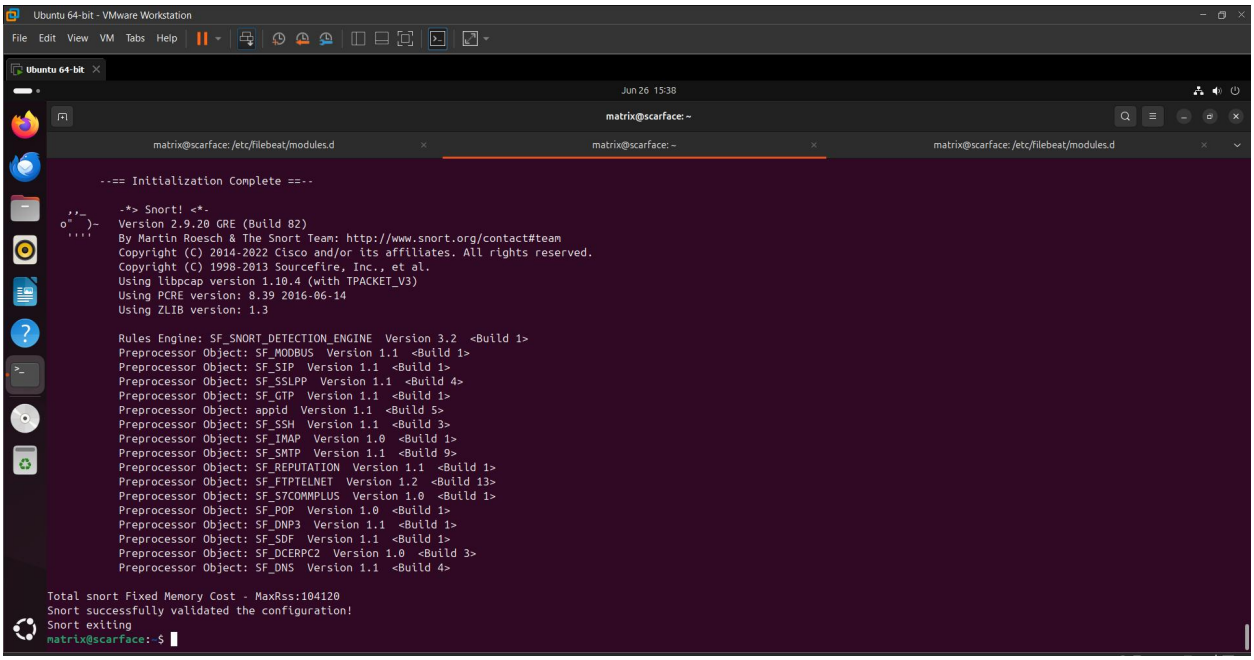
- alert tcp any any -> $HOME_NET 80 (msg:"XSS Attack Attempt - <script>"; content:"<script>"; nocase; sid:1002001; rev:1;)

- alert tcp any any -> $HOME_NET 22 (msg:"SSH Brute Force Attempt"; flags:S; threshold:type threshold, track by_src, count 5, seconds 30; sid:1003008; rev:1;)

8.4 Testing Snort Configuration

Test Snort configuration

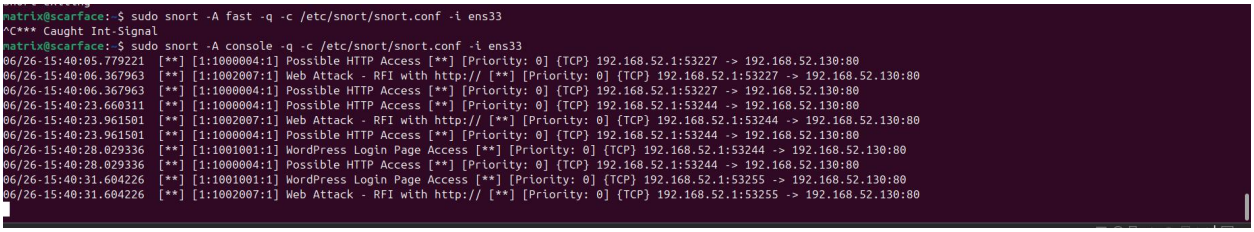
```
sudo snort -T -c /etc/snort/snort.conf
```



8.5 Running Snort in Alert Mode

Run Snort in alert mode

```
sudo snort -A console -q -c /etc/snort/snort.conf -i ens33
```



9. Fail2Ban Configuration

Purpose

Fail2Ban monitors logs (including Snort alerts and Apache logs) and bans IPs that exhibit suspicious behavior such as brute force attacks or injections.

Commands and Configuration

9.1 Installing Fail2Ban

- Install Fail2Ban

```
sudo apt install fail2ban -y
```

9.2 Creating Custom Filters for WordPress and Snort Alerts

Create filter files in /etc/fail2ban/filter.d/

Example: wordpress.conf

```
[Definition]
failregex = <HOST> -.*"(POST|GET).*wp-login.php.*" 200
ignoreregex =
```

Example: snort-sql-injection.conf

```
[Definition]
failregex = \[\*\*\] \[.*\] Web Attack - SQL   Injection.*\[\*\*\].*{.*-><HOST>}
ignoreregex =
```

Example: snort-xss.conf

```
[Definition]
failregex = \[\*\*\] \[.*\] Web Attack -XSS.*\[\*\*\].*{.*-    ><HOST>}
ignoreregex =
```

9.3 Configuring Jails for SSH, WordPress, and Snort Filters

Edit the jail.local file using the command Sudo nano /etc/fail2ban/jail.local

```
[sshd]

enabled = true

port = ssh

logpath = /var/log/auth.log

maxretry = 5

findtime = 60

bantime = 1800



[wordpress]

enabled = true

filter = wordpress

port = http,https

logpath = /var/log/apache2/access.log

maxretry = 5
```

```
findtime = 60

bantime = 1800



[snort-sql-injection]

enabled = true

filter = snort-sql-injection

logpath = /var/log/snort/snort.alert.fast

maxretry = 5

findtime = 600

bantime = 1800

[snort-xss]

enabled = true

filter = snort-xss

logpath = /var/log/snort/snort.alert.fast

maxretry = 5

findtime = 600

bantime = 3600
```

9.4 Restarting Fail2Ban and Monitoring Logs

- Restart Fail2Ban

```
sudo systemctl restart fail2ban
sudo systemctl status fail2ban
```

- View Fail2Ban logs to verify bans

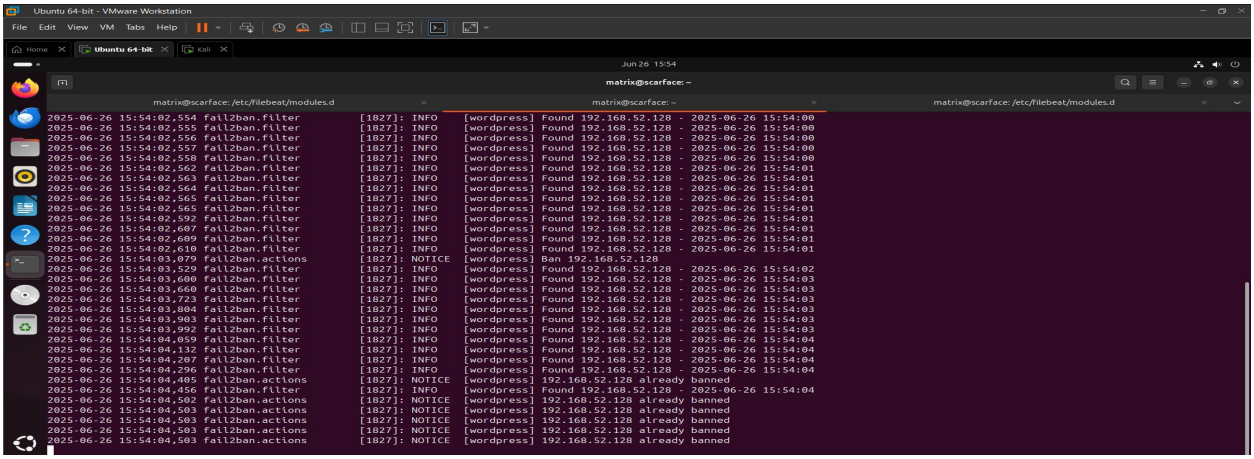
```
sudo tail -f /var/log/fail2ban.log
```

- Restart Fail2Ban

```
sudo systemctl restart fail2ban
sudo systemctl status fail2ban
```

- View Fail2Ban logs to verify bans

```
sudo tail -f /var/log/fail2ban.log
```



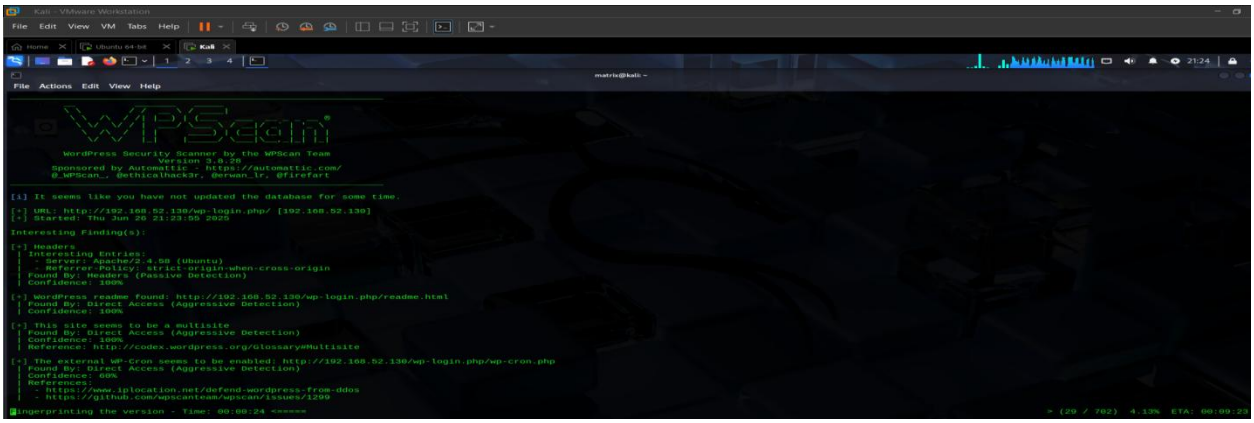
10. Attack Simulation and Verification

Executing Brute Force Attack Simulations

Perform brute force login attempts

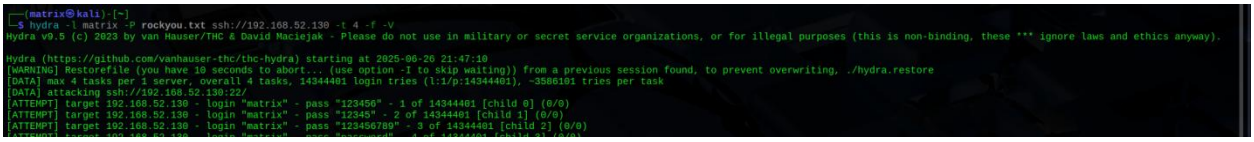
Wordpress

wpscan --url http://<target-ip>/wp-login.php --usernames matrix --passwords /path/to/wordlist.txt



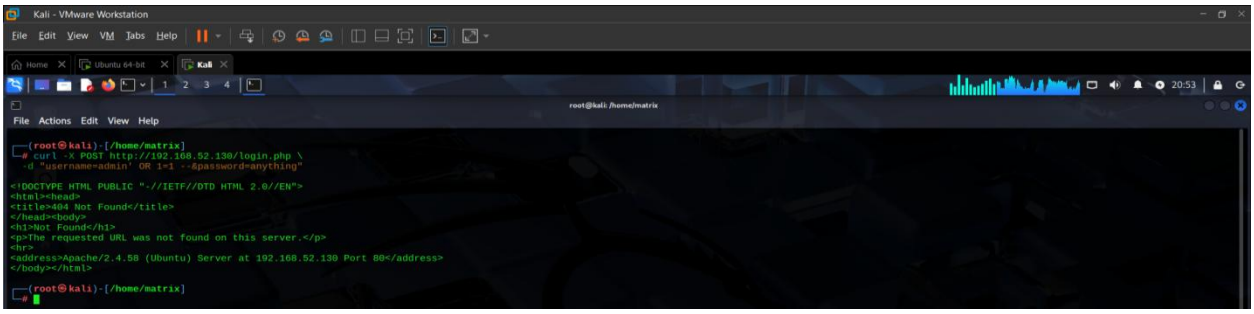
- Ssh

hydra -l matrix -P rockyou.txt ssh://192.168.52.130 -t 4 -f -V



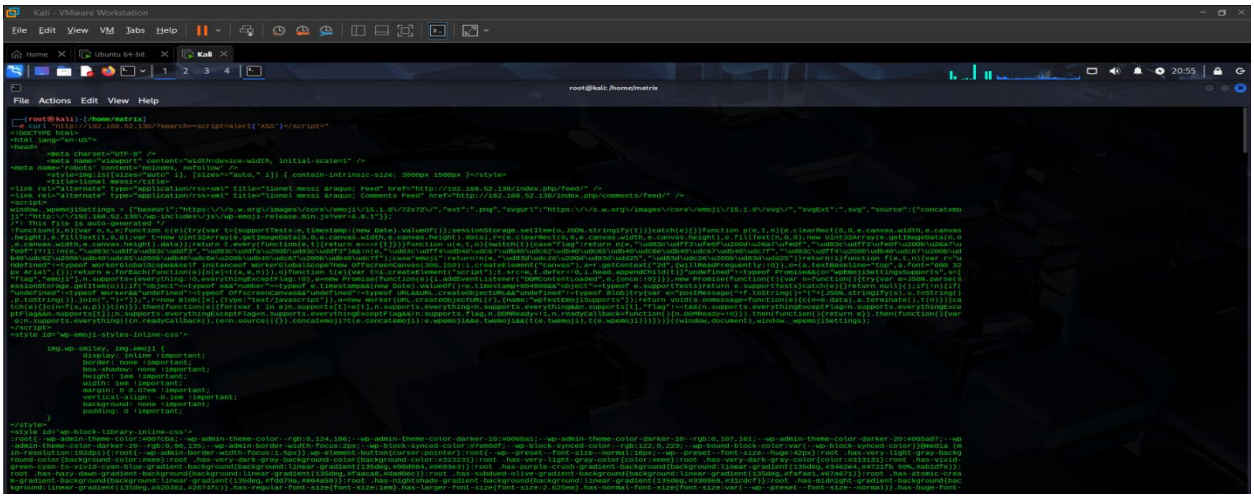
- SQL Injection and XSS Attacking

Curl -X POST http://192.168.52.130/login.php \ -d "username=admin' OR 1=1 --&password=anything"



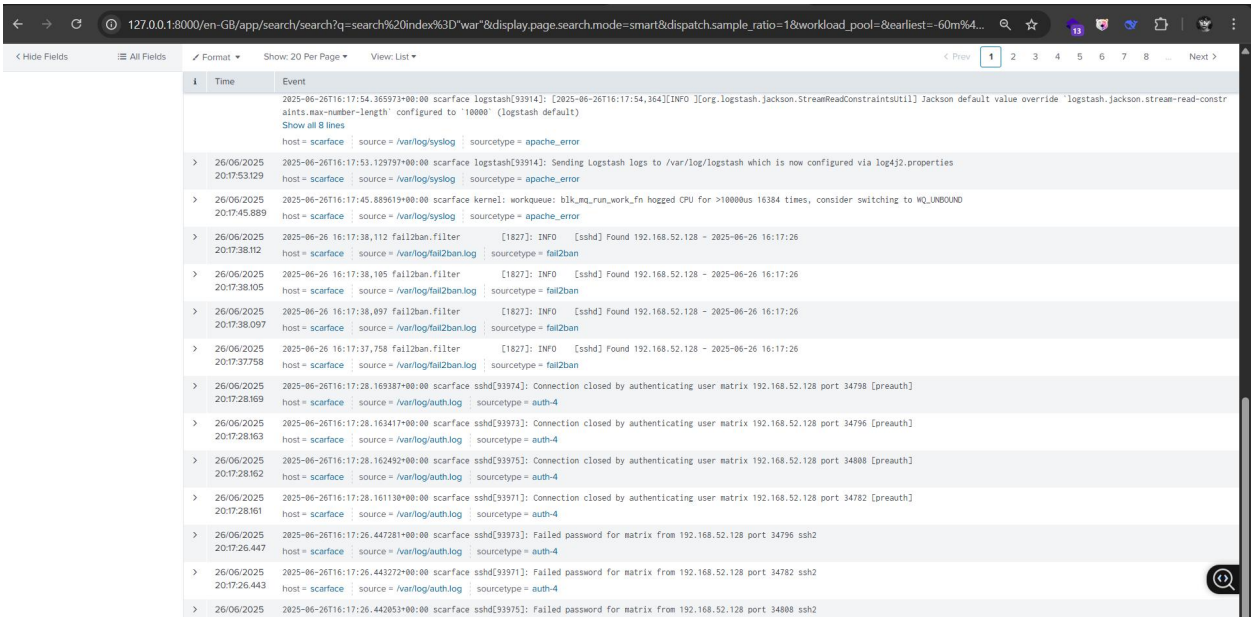
```
┌──(root㉿kali)-[/home/matrix]
└─# curl -X POST http://192.168.52.130/login.php \
  -d "username=admin' OR 1=1 --&password=anything"

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at 192.168.52.130 Port 80</address>
</body></html>

┌──(root㉿kali)-[/home/matrix]
└─#
```

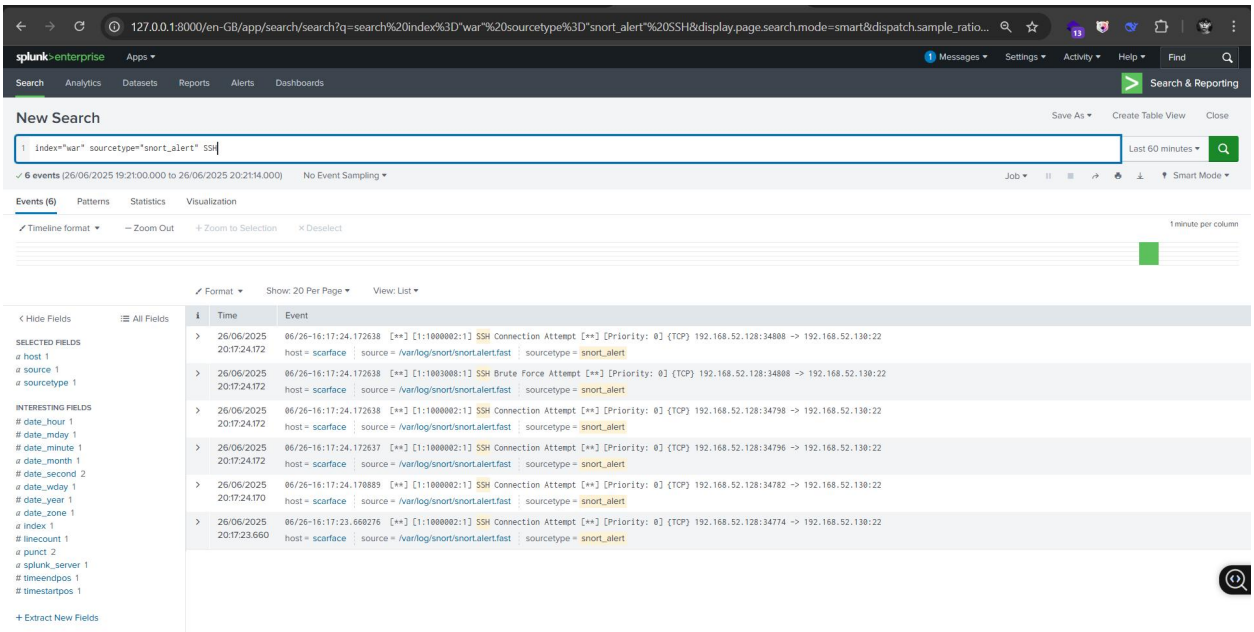
curl "http://192.168.52.130/?search=<script>alert('XSS')</script>"

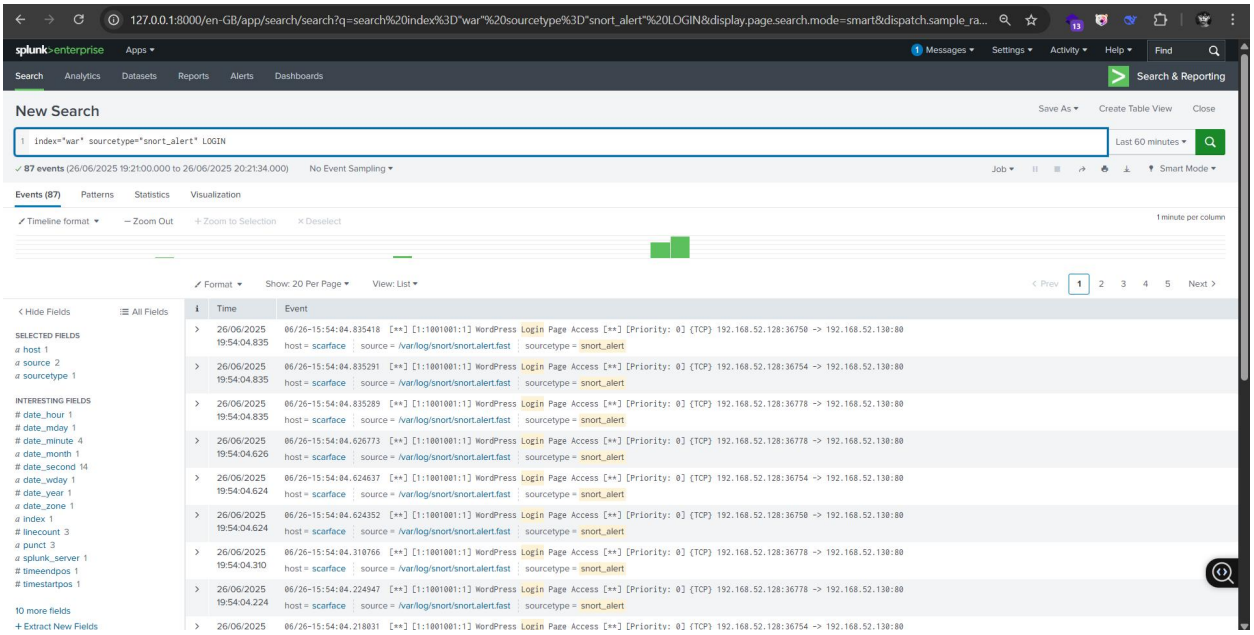


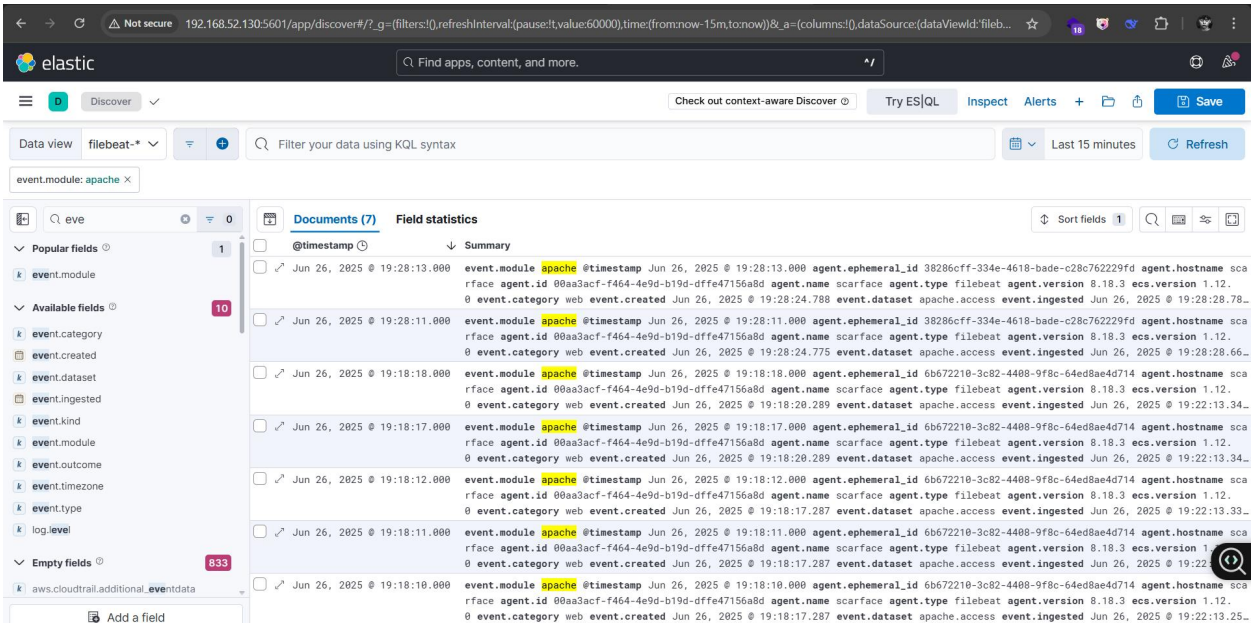
```
┌──(root㉿kali)-[/home/matrix]
└─# curl "http://192.168.52.130/?search=<script>alert('XSS')</script>"
<!DOCTYPE html>
<html lang="en-US">
<head>
        <meta charset="UTF-8" />
        <meta name="viewport" content="width=device-width, initial-scale=1" />
<meta name='robots' content='noindex, nofollow' />
        <style>img:is([sizes="auto" i], [sizes^="auto," i]) { contain-intrinsic-size: 3000px 1500px }</style>
        <title>lionel messi</title>
<link rel="alternate" type="application/rss+xml" title="lionel messi &raquo; Feed" href="http://192.168.52.130/index.php/feed/" />
<link rel="alternate" type="application/rss+xml" title="lionel messi &raquo; Comments Feed" href="http://192.168.52.130/index.php/comments/feed/" />
<script>
window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/15.1.0\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/15.1.0\/svg\/","svgExt":".svg","source":{"concatemo
ji":"http:\/\/192.168.52.130\/wp-includes\/js\/wp-emoji-release.min.js?ver=6.8.1"}};
/*! This file is auto-generated */
!function(i,n){var o,s,e;function c(e){try{var t={supportTests:e,timestamp:(new Date).valueOf()};sessionStorage.setItem(o,JSON.stringify(t))}catch(e){}}function p(e,t,n){e.clearRect(0,0,e.canvas.width,e.canvas
.height),e.fillText(t,0,0);var t=new Uint32Array(e.getImageData(0,0,e.canvas.width,e.canvas.height).data),r=(e.clearRect(0,0,e.canvas.width,e.canvas.height),e.fillText(n,0,0),new Uint32Array(e.getImageData(0,0
,e.canvas.width,e.canvas.height).data));return t.every(function(e,t){return e===r[t]})}function u(e,t,n){switch(t){case"flag":return n(e,"\ud83c\udff3\ufe0f\u200d\u26a7\ufe0f","\ud83c\udff3\ufe0f\u200b\u26a7\u
fe0f")?!1:!n(e,"\ud83c\uddfa\ud83c\uddf3","\ud83c\uddfa\u200b\ud83c\uddf3")&&!n(e,"\ud83c\udff4\udb40\udc67\udb40\udc62\udb40\udc65\udb40\udc6e\udb40\udc67\udb40\udc7f","\ud83c\udff4\u200b\udb40\udc67\u200b\ud
b40\udc62\u200b\udb40\udc65\u200b\udb40\udc6e\u200b\udb40\udc67\u200b\udb40\udc7f");case"emoji":return!n(e,"\ud83d\udc26\u200d\ud83d\udd25","\ud83d\udc26\u200b\ud83d\udd25")}return!1}function f(e,t,n){var r="u
ndefined"!=typeof WorkerGlobalScope&&self instanceof WorkerGlobalScope?new OffscreenCanvas(300,150):i.createElement("canvas"),a=r.getContext("2d",{willReadFrequently:!0}),o=(a.textBaseline="top",a.font="600 32
px Arial",{});return e.forEach(function(e){o[e]=t(a,e,n)}),o}function t(e){var t=i.createElement("script");t.src=e,t.defer=!0,i.head.appendChild(t)}"undefined"!=typeof Promise&&(o="wpEmojiSettingsSupports",s=[
"flag","emoji"],n.supports={everything:!0,everythingExceptFlag:!0},e=new Promise(function(e){i.addEventListener("DOMContentLoaded",e,{once:!0})}),new Promise(function(t){var n=function(){try{var e=JSON.parse(s
essionStorage.getItem(o));if("object"==typeof e&&"number"==typeof e.timestamp&&(new Date).valueOf()<e.timestamp+604800&&"object"==typeof e.supportTests)return e.supportTests}catch(e){}return null}();if(!n){if(
"undefined"!=typeof Worker&&"undefined"!=typeof OffscreenCanvas&&"undefined"!=typeof URL&&URL.createObjectURL&&"undefined"!=typeof Blob)try{var e="postMessage("+f.toString()+"("+[JSON.stringify(s),u.toString()
,p.toString()].join(",")+"));",r=new Blob([e],{type:"text/javascript"}),a=new Worker(URL.createObjectURL(r),{name:"wpTestEmojiSupports"});return void(a.onmessage=function(e){c(n=e.data),a.terminate(),t(n)})}ca
tch(e){}c(n=f(s,u,p))}t(n)}).then(function(e){for(var t in e)n.supports[t]=e[t],n.supports.everything=n.supports.everything&&n.supports[t],"flag"!==t&&(n.supports.everythingExceptFlag=n.supports.everythingExce
ptFlag&&n.supports[t]);n.supports.everythingExceptFlag=n.supports.everythingExceptFlag&&!n.supports.flag,n.DOMReady=!1,n.readyCallback=function(){n.DOMReady=!0}}).then(function(){return e}).then(function(){var
 e;n.supports.everything||(n.readyCallback(),(e=n.source||{}).concatemoji?t(e.concatemoji):e.wpemoji&&e.twemoji&&(t(e.twemoji),t(e.wpemoji)))}))}((window,document),window._wpemojiSettings);
</script>
<style id='wp-emoji-styles-inline-css'>

        img.wp-smiley, img.emoji {
                display: inline !important;
                border: none !important;
                box-shadow: none !important;
                height: 1em !important;
                width: 1em !important;
                margin: 0 0.07em !important;
                vertical-align: -0.1em !important;
                background: none !important;
                padding: 0 !important;
        }
</style>
<style id='wp-block-library-inline-css'>
:root{--wp-admin-theme-color:#007cba;--wp-admin-theme-color--rgb:0,124,186;--wp-admin-theme-color-darker-10:#006ba1;--wp-admin-theme-color-darker-10--rgb:0,107,161;--wp-admin-theme-color-darker-20:#005a87;--wp
-admin-theme-color-darker-20--rgb:0,90,135;--wp-admin-border-width-focus:2px;--wp-block-synced-color:#7a00df;--wp-block-synced-color--rgb:122,0,223;--wp-bound-block-color:var(--wp-block-synced-color)}@media (m
in-resolution:192dpi){:root{--wp-admin-border-width-focus:1.5px}}.wp-element-button{cursor:pointer}:root{--wp--preset--font-size--normal:16px;--wp--preset--font-size--huge:42px}:root .has-very-light-gray-backg
round-color{background-color:#eee}:root .has-very-dark-gray-background-color{background-color:#313131}:root .has-very-light-gray-color{color:#eee}:root .has-very-dark-gray-color{color:#313131}:root .has-vivid-
green-cyan-to-vivid-cyan-blue-gradient-background{background:linear-gradient(135deg,#00d084,#0693e3)}:root .has-purple-crush-gradient-background{background:linear-gradient(135deg,#34e2e4,#4721fb 50%,#ab1dfe)}:
root .has-hazy-dawn-gradient-background{background:linear-gradient(135deg,#faaca8,#dad0ec)}:root .has-subdued-olive-gradient-background{background:linear-gradient(135deg,#fafae1,#67a671)}:root .has-atomic-crea
m-gradient-background{background:linear-gradient(135deg,#fdd79a,#004a59)}:root .has-nightshade-gradient-background{background:linear-gradient(135deg,#330968,#31cdcf)}:root .has-midnight-gradient-background{bac
kground:linear-gradient(135deg,#020381,#2874fc)}.has-regular-font-size{font-size:1em}.has-larger-font-size{font-size:2.625em}.has-normal-font-size{font-size:var(--wp--preset--font-size--normal)}.has-huge-font-
```

10.1 Monitoring Attack Logs in Splunk and Kibana

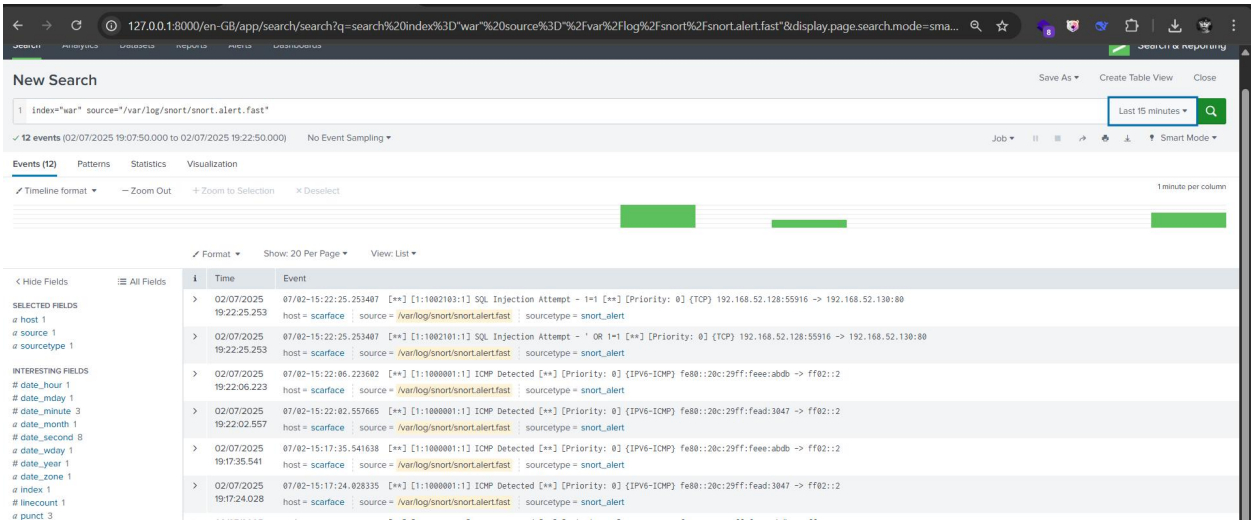




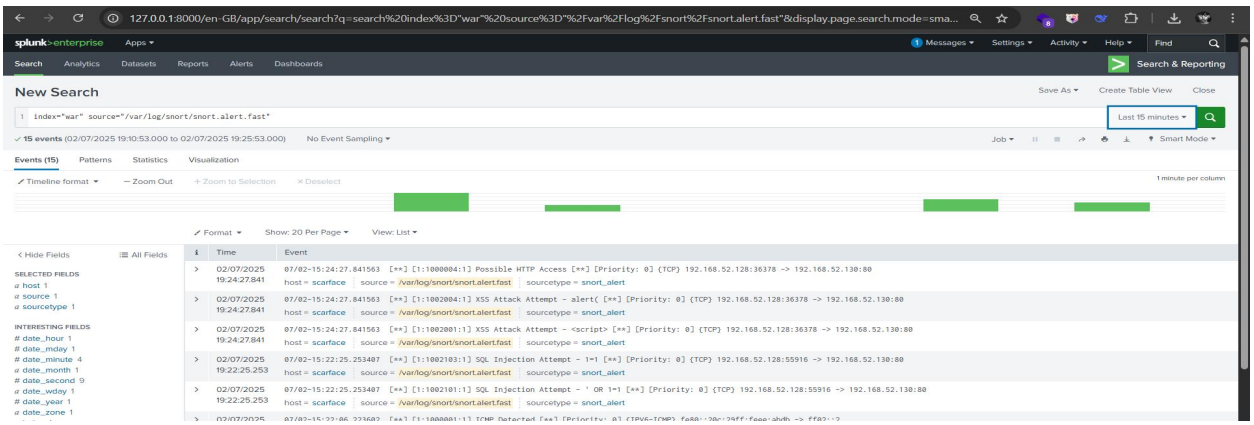

splunk>enterprise
Search & Reporting
New Search
index="war" sourcetype="snort_alert" LOGIN
87 events (26/06/2025 19:21:00.000 to 26/06/2025 20:21:34.000)
Events (87)
Patterns
Statistics
Visualization
Time
Event


elastic
Discover
Data view
filebeat-*
Filter your data using KQL syntax
Last 15 minutes
Refresh
event.module: apache
Documents (7)
Field statistics
@timestamp
Summary
Popular fields
Available fields
Empty fields
Add a field

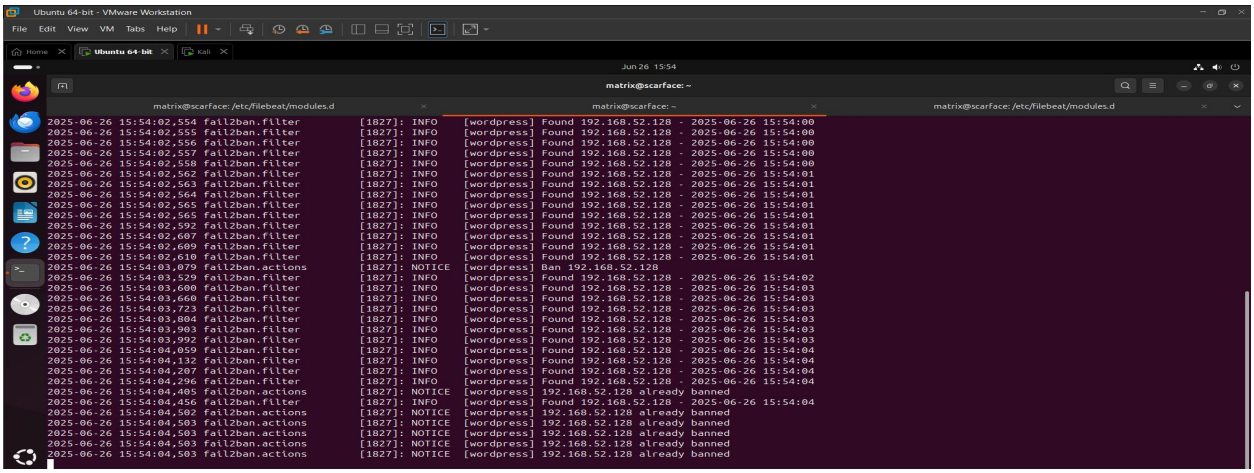
SQL Injection log



XSS attack log



10.2 Verifying IP Bans with Fail2Ban


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu 64-bit
Kali
Jun 26 15:54
matrix@scarface: ~
matrix@scarface: /etc/filebeat/modules.d
matrix@scarface: ~
matrix@scarface: /etc/filebeat/modules.d
2025-06-26 15:54:02,554 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:00
2025-06-26 15:54:02,555 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:00
2025-06-26 15:54:02,556 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:00
2025-06-26 15:54:02,557 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:00
2025-06-26 15:54:02,558 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:00
2025-06-26 15:54:02,562 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:01
2025-06-26 15:54:02,563 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:01
2025-06-26 15:54:02,564 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:01
2025-06-26 15:54:02,565 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:01
2025-06-26 15:54:02,565 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:01
2025-06-26 15:54:02,592 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:01
2025-06-26 15:54:02,607 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:01
2025-06-26 15:54:02,609 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:01
2025-06-26 15:54:02,610 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:01
2025-06-26 15:54:03,079 fail2ban.actions [1827]: NOTICE [wordpress] Ban 192.168.52.128
2025-06-26 15:54:03,529 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:02
2025-06-26 15:54:03,600 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:03
2025-06-26 15:54:03,660 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:03
2025-06-26 15:54:03,723 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:03
2025-06-26 15:54:03,804 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:03
2025-06-26 15:54:03,903 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:03
2025-06-26 15:54:03,992 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:03
2025-06-26 15:54:04,059 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:04
2025-06-26 15:54:04,132 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:04
2025-06-26 15:54:04,207 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:04
2025-06-26 15:54:04,296 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:04
2025-06-26 15:54:04,405 fail2ban.actions [1827]: NOTICE [wordpress] 192.168.52.128 already banned
2025-06-26 15:54:04,456 fail2ban.filter [1827]: INFO [wordpress] Found 192.168.52.128 - 2025-06-26 15:54:04
2025-06-26 15:54:04,502 fail2ban.actions [1827]: NOTICE [wordpress] 192.168.52.128 already banned
2025-06-26 15:54:04,503 fail2ban.actions [1827]: NOTICE [wordpress] 192.168.52.128 already banned
2025-06-26 15:54:04,503 fail2ban.actions [1827]: NOTICE [wordpress] 192.168.52.128 already banned
2025-06-26 15:54:04,503 fail2ban.actions [1827]: NOTICE [wordpress] 192.168.52.128 already banned
2025-06-26 15:54:04,503 fail2ban.actions [1827]: NOTICE [wordpress] 192.168.52.128 already banned

11. Conclusion

This project demonstrates a fully integrated cybersecurity setup for a WordPress hosting environment on Ubuntu, employing Apache, MySQL, Snort IDS, Splunk, ELK stack, and Fail2Ban for multi-layered protection. Attack simulations validate the effectiveness of detection, alerting, and automatic mitigation mechanisms, offering a solid foundation for real-world web server defense.