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 analysis.

2.3 Snort IDS

- Network Intrusion Detection System monitoring traffic on the server.

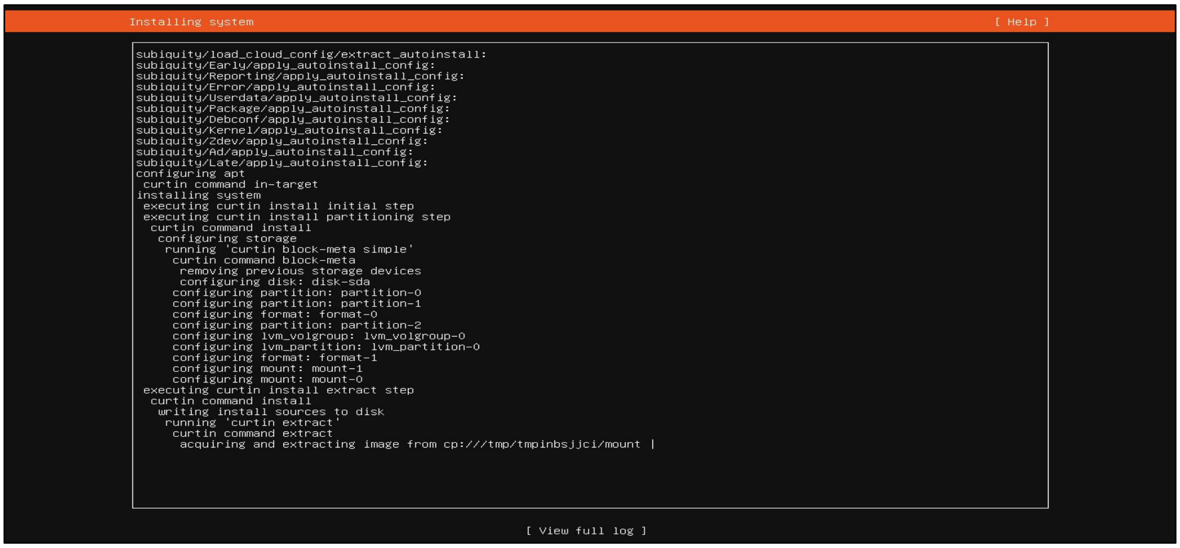
- Detects various attacks (ICMP scanning, SSH attempts, HTTP access, WordPress login attempts, SQL injection, XSS, command injection).
- Custom Snort rules written to identify specific threats relevant to WordPress and SSH.
- Outputs alerts logged locally and forwarded to Splunk/ELK for monitoring.

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



```
subiquity/load_cloud_config/extract_autoinstall:
subiquity/Early/apply_autoinstall_config:
subiquity/Reporting/apply_autoinstall_config:
subiquity/Error/apply_autoinstall_config:
subiquity/Userdata/apply_autoinstall_config:
subiquity/Package/apply_autoinstall_config:
subiquity/Debconf/apply_autoinstall_config:
subiquity/Kernel/apply_autoinstall_config:
subiquity/Zdev/apply_autoinstall_config:
subiquity/Ad/apply_autoinstall_config:
subiquity/Late/apply_autoinstall_config:
configuring apt
 curtin command in-target
installing system
 executing curtin install initial step
 executing curtin install partitioning step
  curtin command install
   configuring storage
    running 'curtin block-meta simple'
     curtin command block-meta
      removing previous storage devices
      configuring disk: disk-sda
     configuring partition: partition-0
     configuring partition: partition-1
     configuring format: format-0
     configuring partition: partition-2
     configuring lvm_volgroup: lvm_volgroup-0
     configuring lvm_partition: lvm_partition-0
     configuring format: format-1
     configuring mount: mount-1
     configuring mount: mount-0
 executing curtin install extract step
  curtin command install
   writing install sources to disk
    running 'curtin extract'
     curtin command extract
      acquiring and extracting image from cp:///tmp/tmpinbsjjci/mount |
```

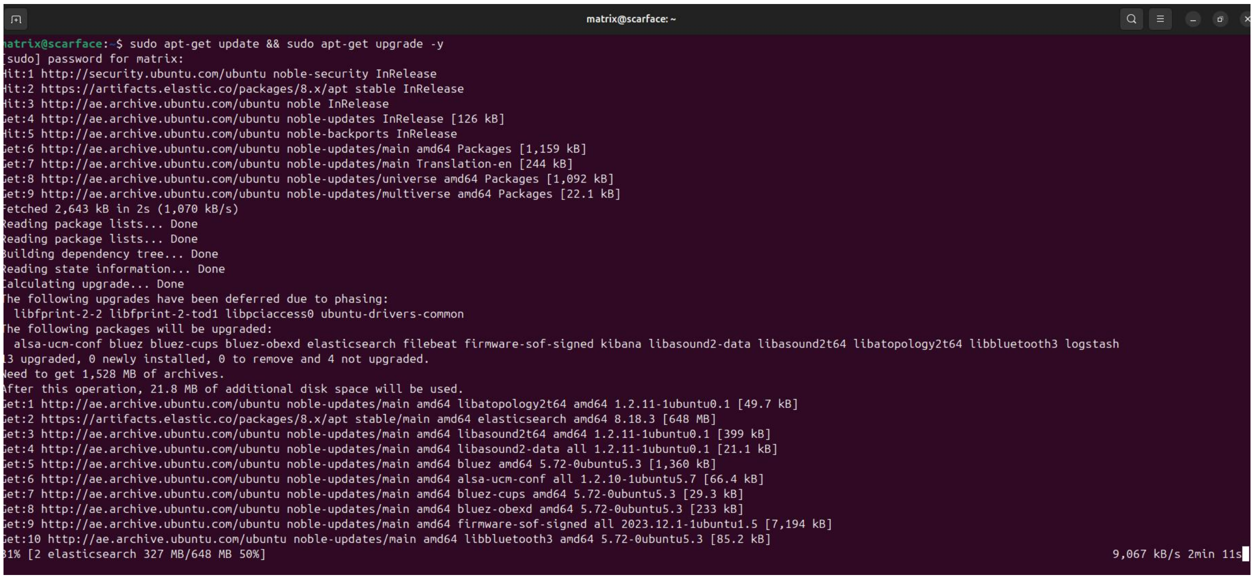
3.1 Updating and Upgrading Ubuntu Packages

- **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:~$ 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

4.1 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

4.2 Starting and Enabling Apache Service

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

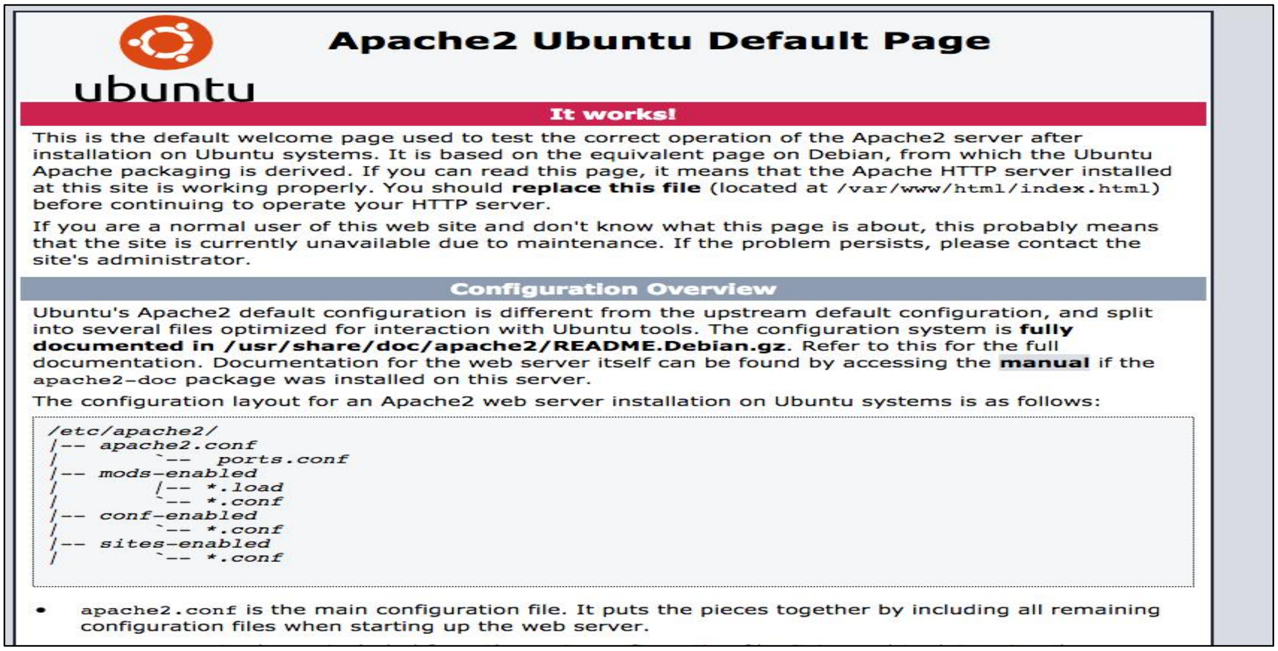
```
sudo systemctl enable apache2
```

- Start Apache service immediately.

```
sudo systemctl start apache2
```

- Check Apache service status.

```
sudo systemctl status apache2
```



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

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.

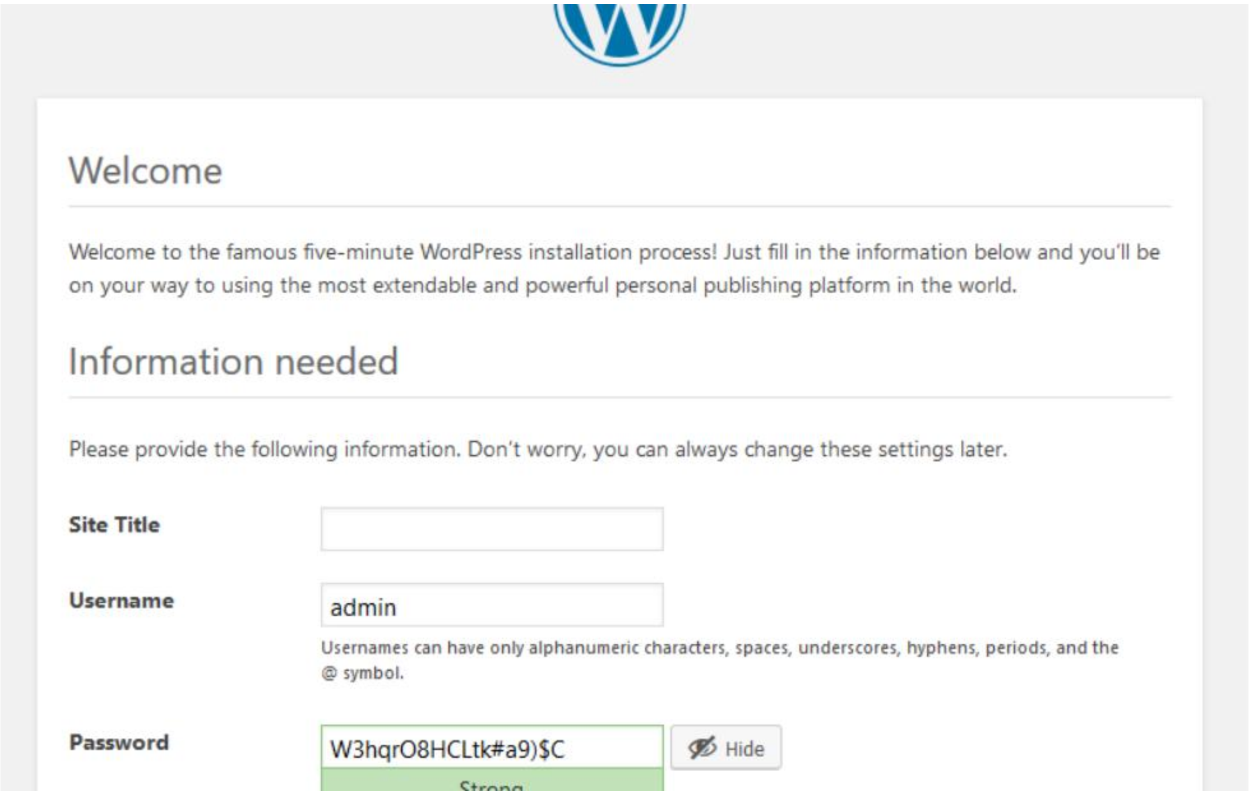
```
sudo mv wordpress/* ./
```

- 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
```



Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title

Username admin

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password W3hqrO8HCLtk#a9)$C

4.4 Configuring MySQL for WordPress

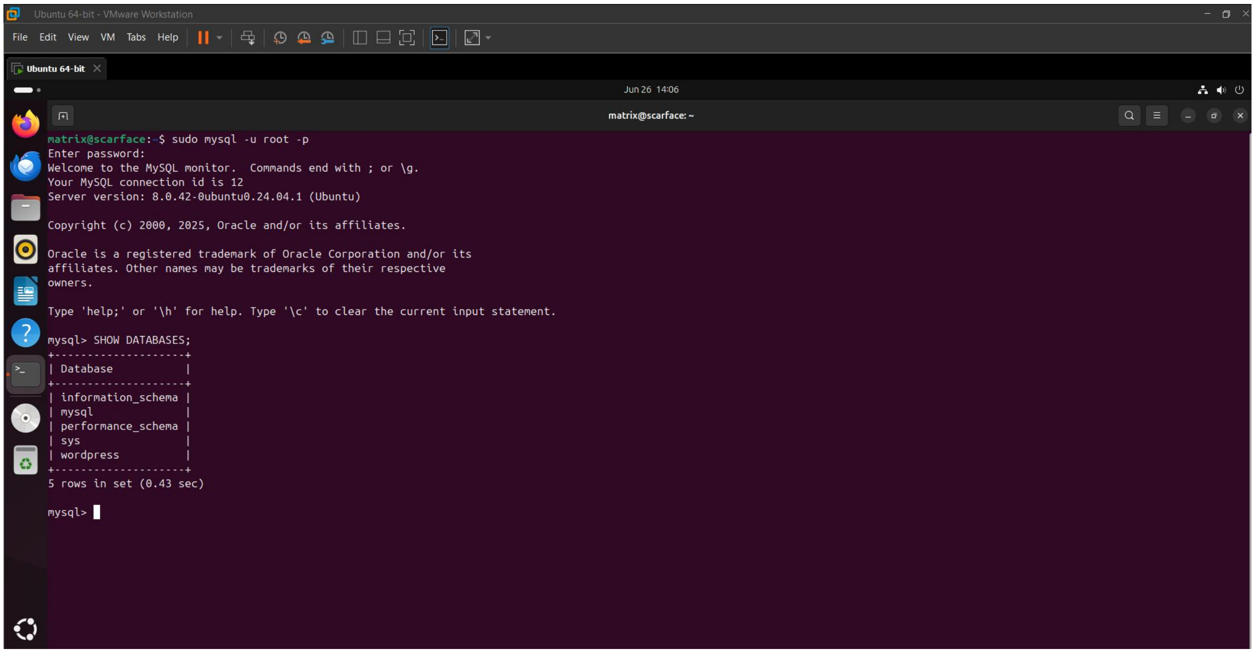
- **Access MySQL shell**.

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

- **Create WordPress database and user with privileges**.

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

(i'am done already)



Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Ubuntu 64-bit
Jun 26 14:06
matrix@scarface: ~

```
matrix@scarface:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.42-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wordpress          |
+--------------------+
5 rows in set (0.43 sec)

mysql> 
```

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.

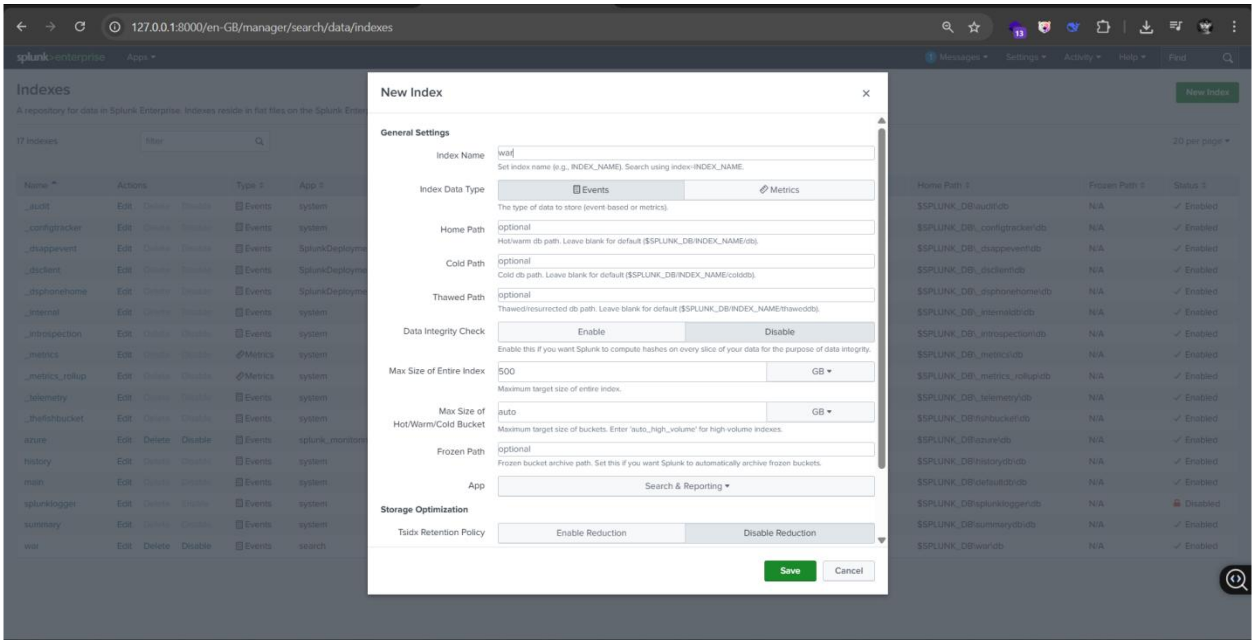
5.2 Creating Index for Log Storage

Create a new index named "war"

This index stores logs forwarded from Ubuntu.

Navigate to:

Settings > Indexes > New Index
Enter war and save.



127.0.0.1:8000/en-GB/manager/search/data/indexes

New Index

General Settings

Index Name: war
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable | Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path: optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App: Search & Reporting

Storage Optimization

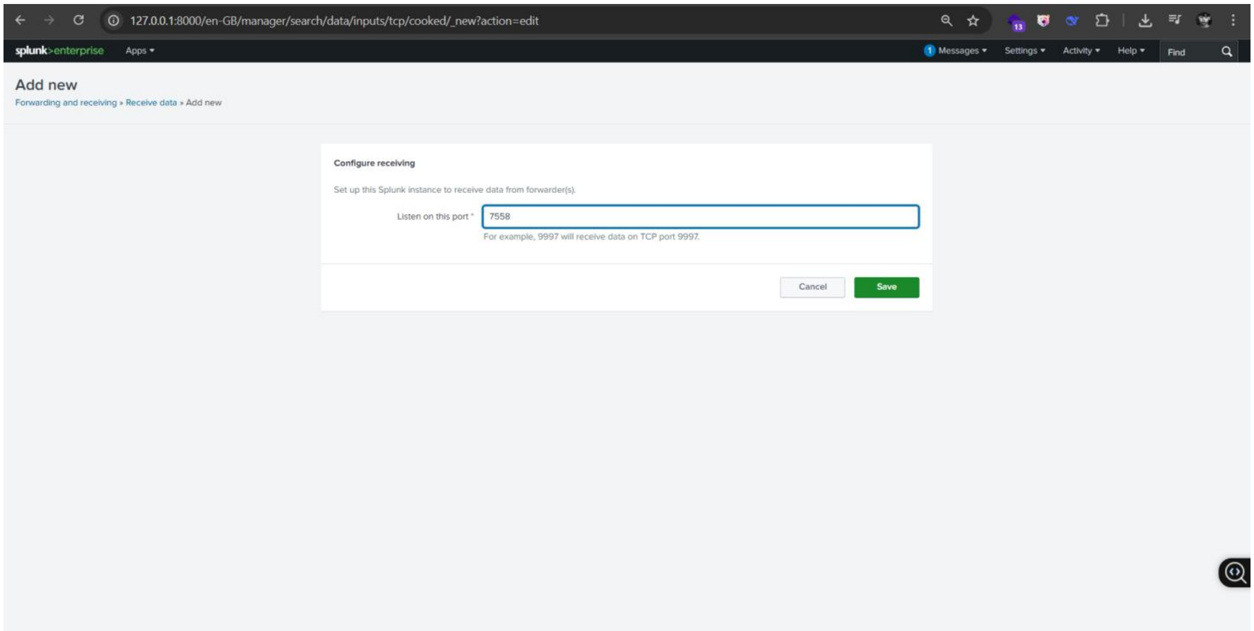
Tsidx Retention Policy: Enable Reduction | Disable Reduction

5.3 Configuring Receiving Port for Log Forwarding

Navigate to:

Settings > Forwarding and Receiving > Configure Receiving > Add New

Enter port 7558 and enable.



127.0.0.1:8000/en-GB/manager/search/data/inputs/tcp/cooked/_new?action=edit

Add new

Forwarding and receiving » Receive data » Add new

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *: 7558
For example, 9997 will receive data on TCP port 9997.

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
```

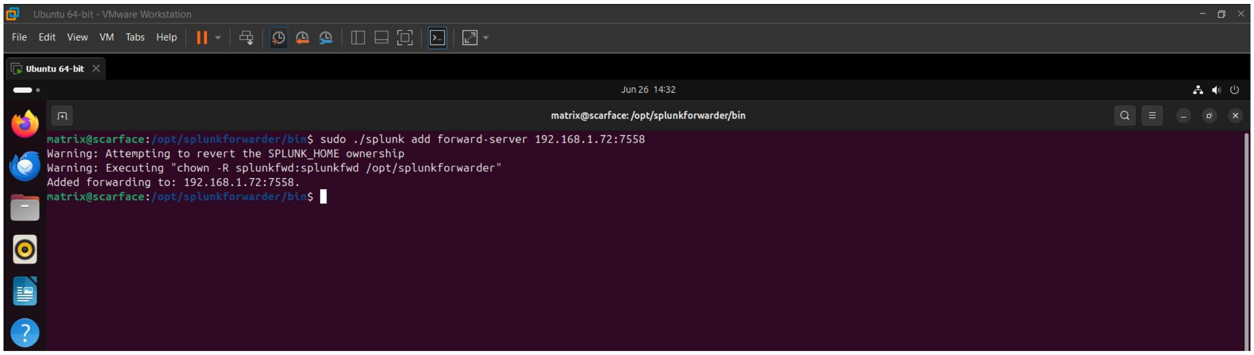
6.2 Starting Forwarder and Accepting License

```
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
```



Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Ubuntu 64-bit
Jun 26 14:32
matrix@scarface: /opt/splunkforwarder/bin

```
matrix@scarface:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 192.168.1.72:7558
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 192.168.1.72:7558.
matrix@scarface:/opt/splunkforwarder/bin$ 
```

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

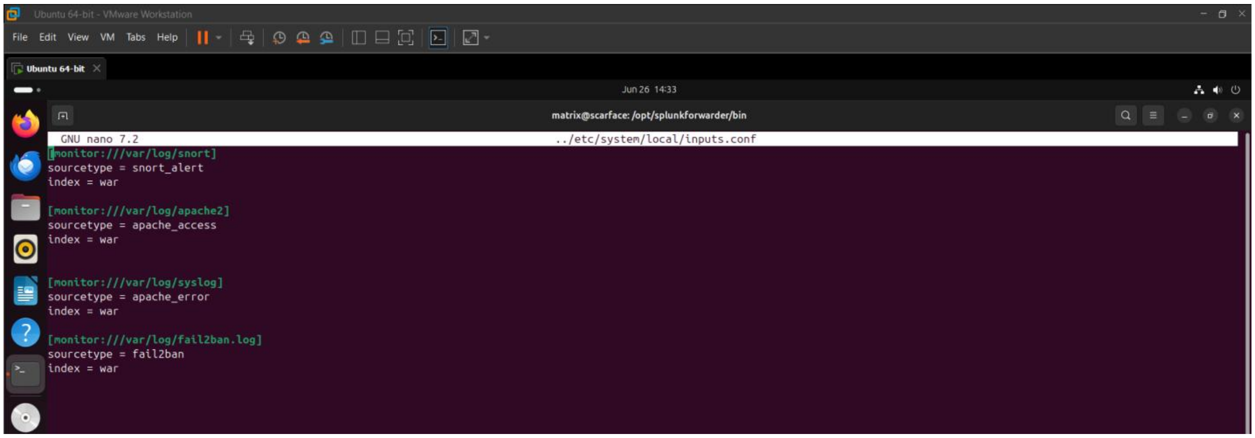
Alternative: Manual inputs.conf editing

```
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

1. **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
```

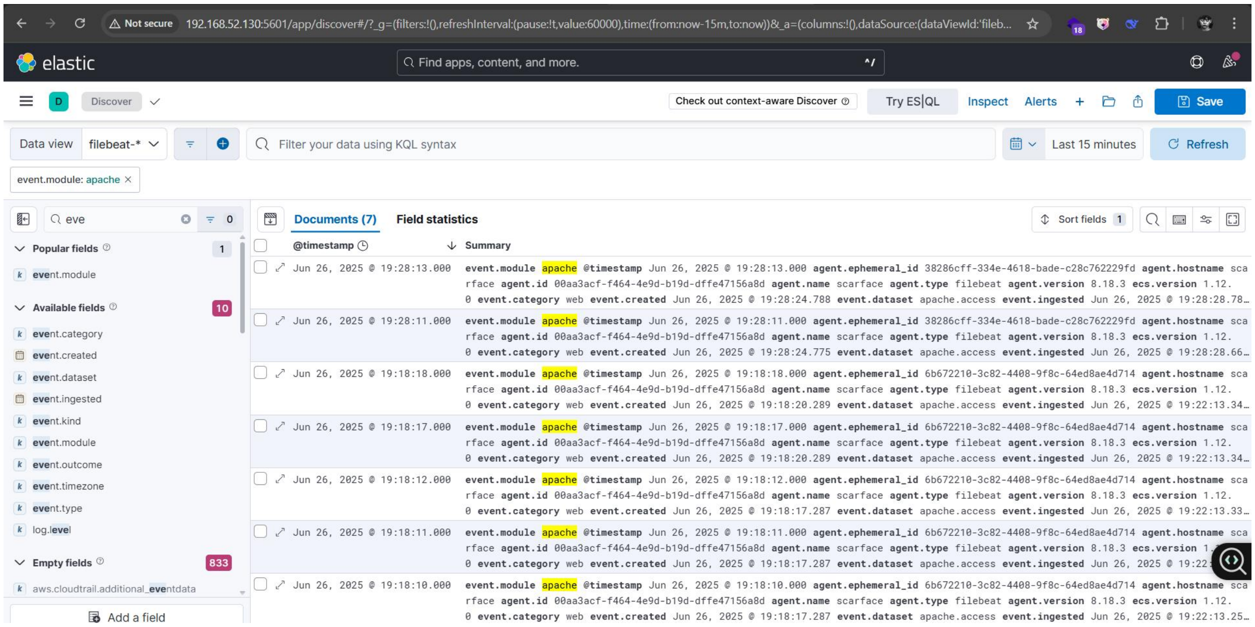
7.5 Accessing and Using Kibana Dashboard

Access Kibana Dashboard

Open browser and navigate to:

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

Configure index patterns to start visualizing the logs.



```
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 sca
                              rface 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 sca
                              rface 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 sca
                              rface 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 sca
                              rface 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 sca
                              rface 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 sca
                              rface 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 sca
                              rface 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;)

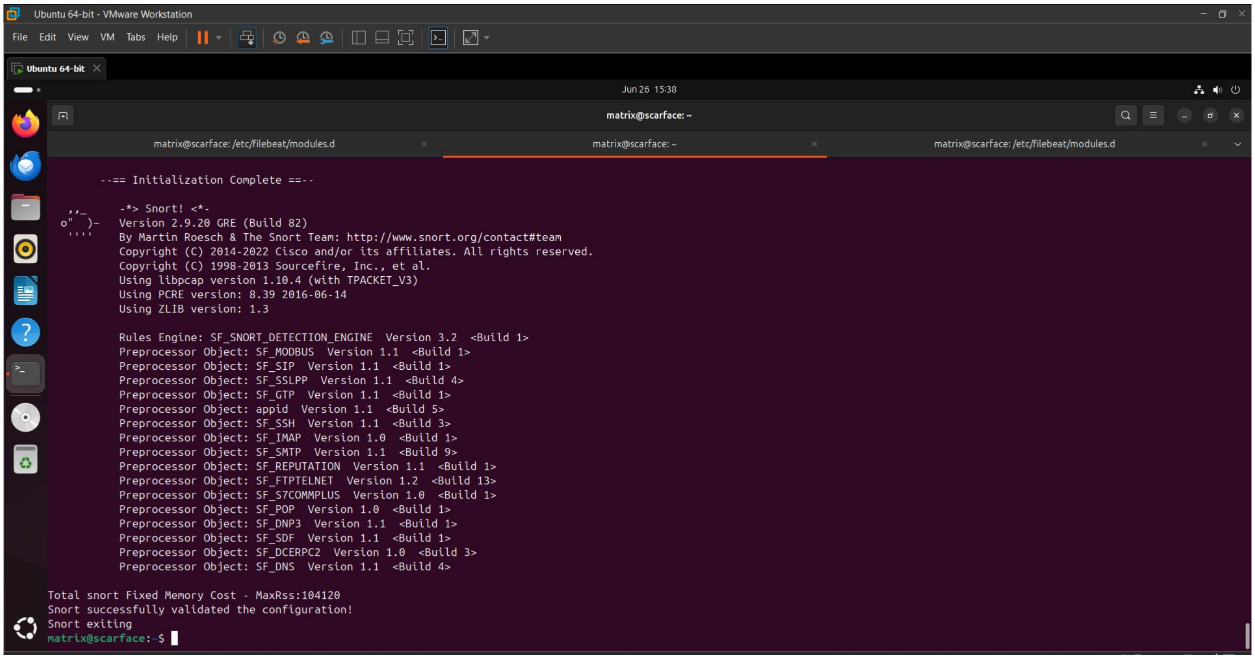
- alert tcp any any -> $HOME_NET 80 (msg:"XSS Attack Attempt - <script>"; content:"<script>"; nocase; sid:1002001; rev:1;)

- 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
```

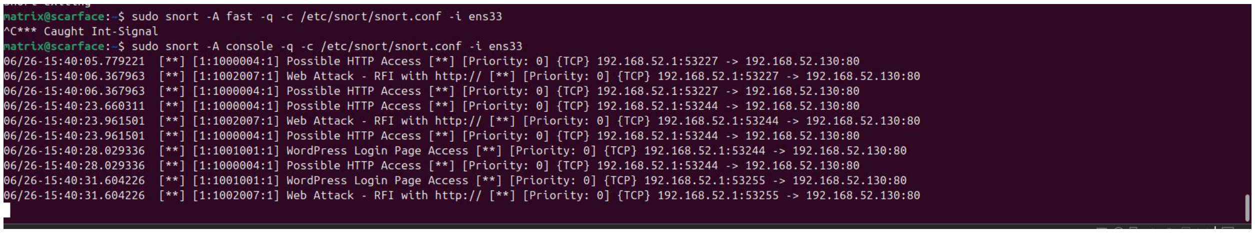

Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Ubuntu 64-bit
Jun 26 15:38
matrix@scarface: ~
matrix@scarface: /etc/filebeat/modules.d
matrix@scarface: ~
matrix@scarface: /etc/filebeat/modules.d

```
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>

Total snort Fixed Memory Cost - MaxRss:104120
Snort successfully validated the configuration!
Snort exiting
matrix@scarface:~$
```

8.5 Running Snort in Alert Mode

Run Snort in alert mode

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



```
matrix@scarface:~$ sudo snort -A fast -q -c /etc/snort/snort.conf -i ens33
^C*** Caught Int-Signal
matrix@scarface:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i ens33
06/26-15:40:05.779221  [**] [1:1000004:1] Possible HTTP Access [**] [Priority: 0] {TCP} 192.168.52.1:53227 -> 192.168.52.130:80
06/26-15:40:06.367963  [**] [1:1002007:1] Web Attack - RFI with http:// [**] [Priority: 0] {TCP} 192.168.52.1:53227 -> 192.168.52.130:80
06/26-15:40:06.367963  [**] [1:1000004:1] Possible HTTP Access [**] [Priority: 0] {TCP} 192.168.52.1:53227 -> 192.168.52.130:80
06/26-15:40:23.660311  [**] [1:1000004:1] Possible HTTP Access [**] [Priority: 0] {TCP} 192.168.52.1:53244 -> 192.168.52.130:80
06/26-15:40:23.961501  [**] [1:1002007:1] Web Attack - RFI with http:// [**] [Priority: 0] {TCP} 192.168.52.1:53244 -> 192.168.52.130:80
06/26-15:40:23.961501  [**] [1:1000004:1] Possible HTTP Access [**] [Priority: 0] {TCP} 192.168.52.1:53244 -> 192.168.52.130:80
06/26-15:40:28.029336  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.1:53244 -> 192.168.52.130:80
06/26-15:40:28.029336  [**] [1:1000004:1] Possible HTTP Access [**] [Priority: 0] {TCP} 192.168.52.1:53244 -> 192.168.52.130:80
06/26-15:40:31.604226  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.1:53255 -> 192.168.52.130:80
06/26-15:40:31.604226  [**] [1:1002007:1] Web Attack - RFI with http:// [**] [Priority: 0] {TCP} 192.168.52.1:53255 -> 192.168.52.130:80
```

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 /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

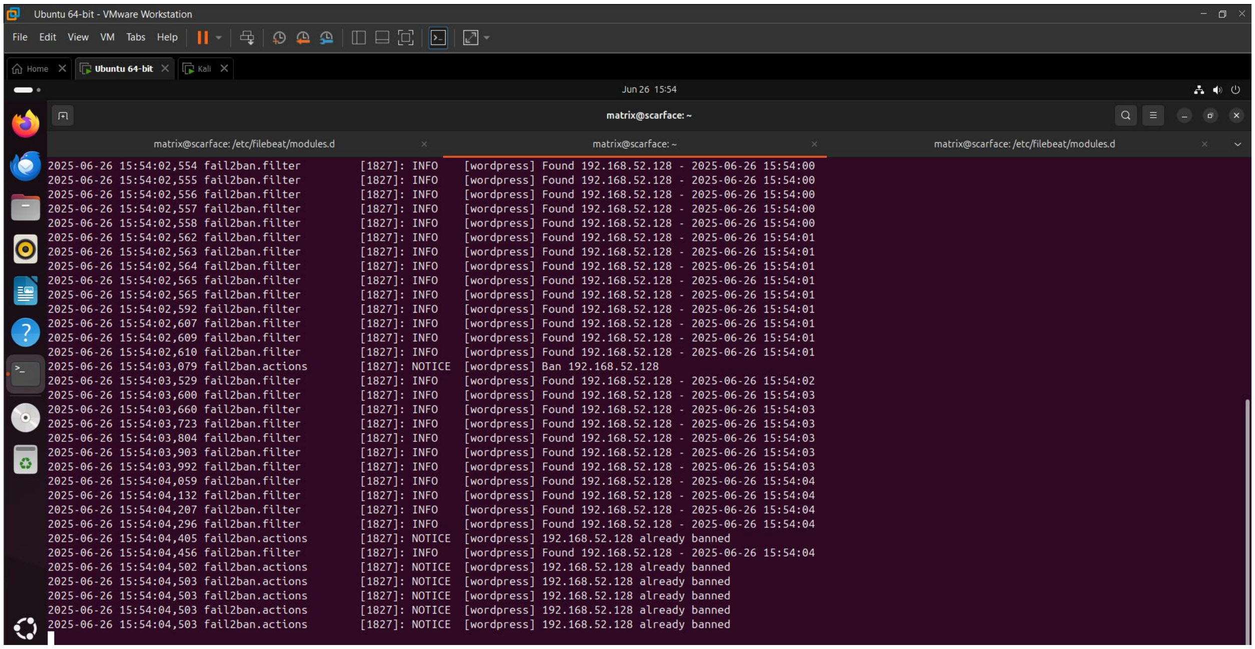
```
sudo tail -f /var/log/fail2ban.log
```

Restart Fail2Ban

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

View Fail2Ban logs to verify bans

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



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
```

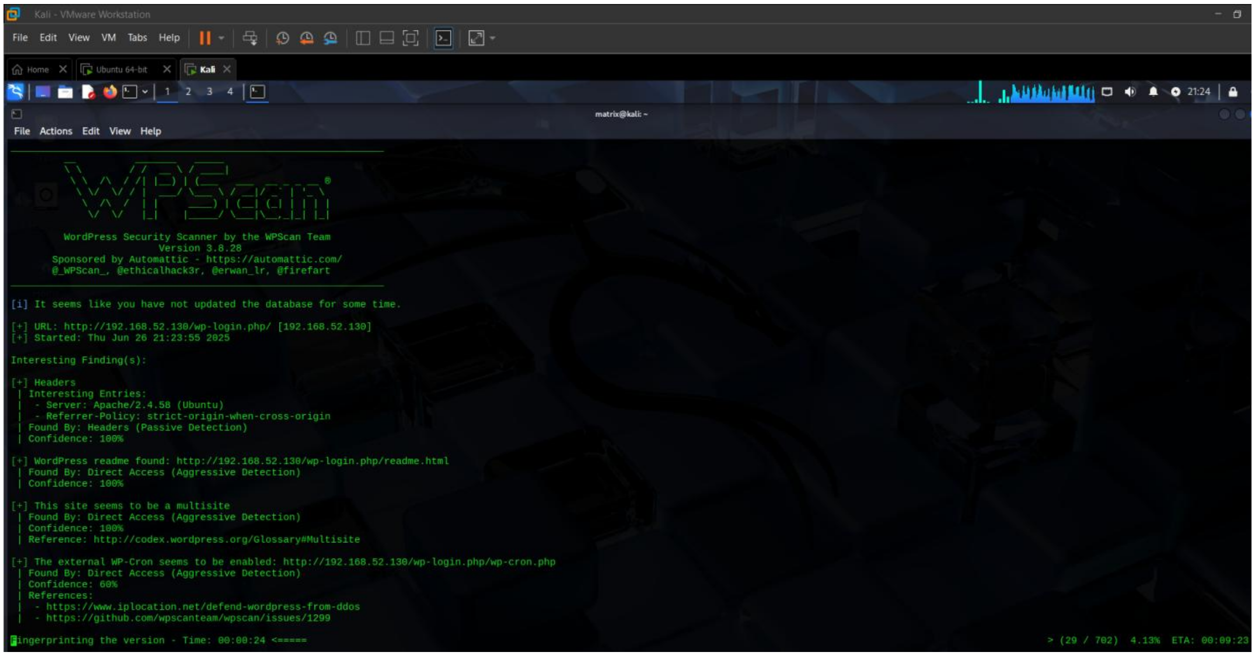
10. Attack Simulation and Verification

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
```

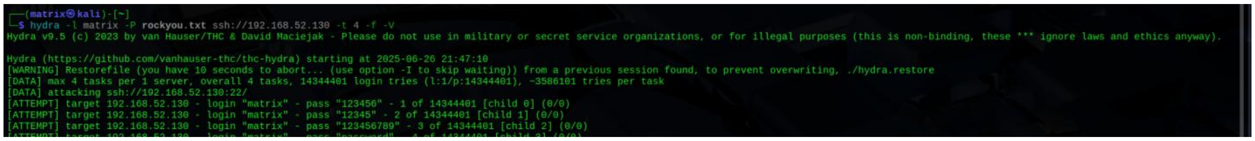


Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu 64-bit
Kali
21:24
matrix@kali: ~
File Actions Edit View Help

```
WordPress Security Scanner by the WPScan Team
                Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] It seems like you have not updated the database for some time.

[+] URL: http://192.168.52.130/wp-login.php/ [192.168.52.130]
[+] Started: Thu Jun 26 21:23:55 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.58 (Ubuntu)
 |  - Referrer-Policy: strict-origin-when-cross-origin
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] WordPress readme found: http://192.168.52.130/wp-login.php/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] This site seems to be a multisite
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | Reference: http://codex.wordpress.org/Glossary#Multisite

[+] The external WP-Cron seems to be enabled: http://192.168.52.130/wp-login.php/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

Fingerprinting the version - Time: 00:00:24 <=====                          > (29 / 702)  4.13%  ETA: 00:09:23
```

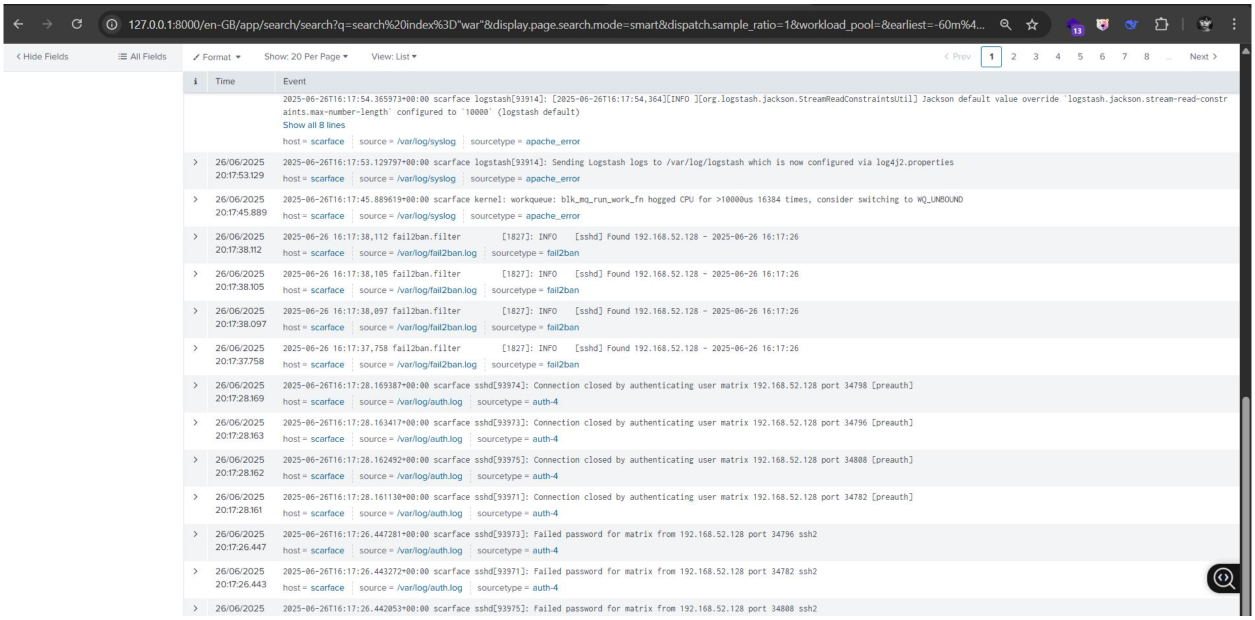
Ssh

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



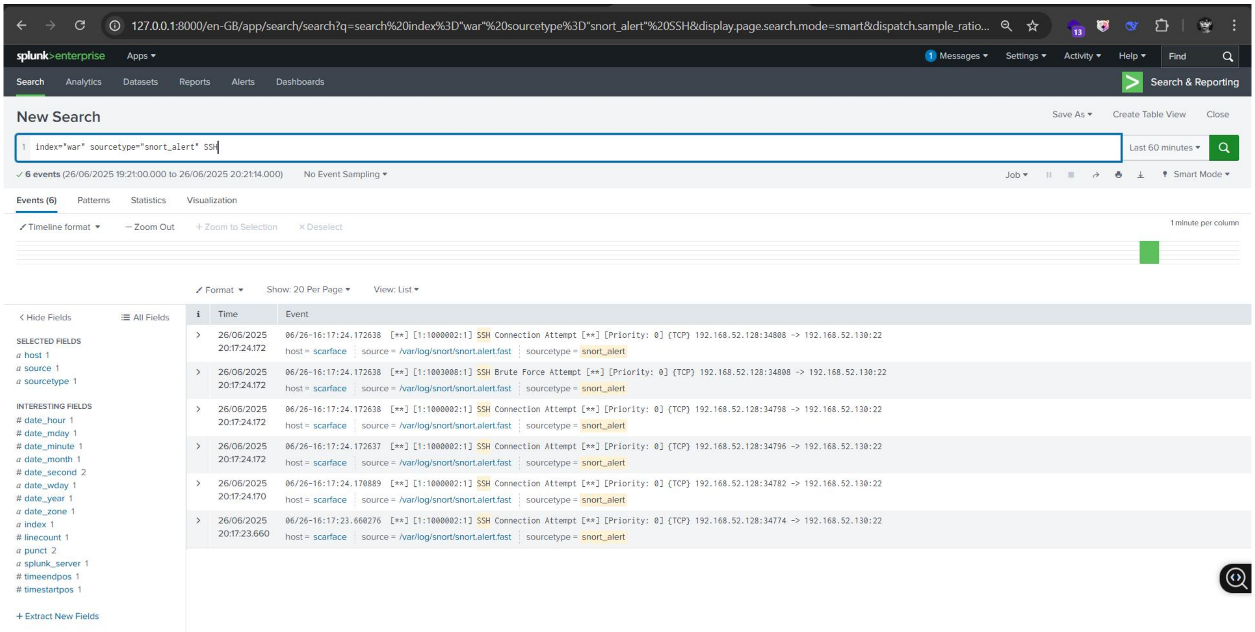
```
┌──(matrix㉿kali)-[~]
└─$ hydra -l matrix -P rockyou.txt ssh://192.168.52.130 -t 4 -f -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-26 21:47:10
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344401 login tries (l:1/p:14344401), ~3586101 tries per task
[DATA] attacking ssh://192.168.52.130:22/
[ATTEMPT] target 192.168.52.130 - login "matrix" - pass "123456" - 1 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.52.130 - login "matrix" - pass "12345" - 2 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.52.130 - login "matrix" - pass "123456789" - 3 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.52.130 - login "matrix" - pass "password" - 4 of 14344401 [child 3] (0/0)
```

10.1 Monitoring Attack Logs in Splunk and Kibana



```
127.0.0.1:8000/en-GB/app/search/search?q=search%20index%3D"war"&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=-60m%4...
```

```
                   2025-06-26T16:17:54.365973+00:00 scarface logstash[93914]: [2025-06-26T16:17:54,364][INFO ][org.logstash.jackson.StreamReadConstraintsUtil] Jackson default value override `logstash.jackson.stream-read-constr
                   aints.max-number-length` configured to `10000` (logstash default)
                   host = scarface | source = /var/log/syslog | sourcetype = apache_error
26/06/2025         2025-06-26T16:17:53.129797+00:00 scarface logstash[93914]: Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties
20:17:53.129       host = scarface | source = /var/log/syslog | sourcetype = apache_error
26/06/2025         2025-06-26T16:17:45.889619+00:00 scarface kernel: workqueue: blk_mq_run_work_fn hogged CPU for >10000us 16384 times, consider switching to WQ_UNBOUND
20:17:45.889       host = scarface | source = /var/log/syslog | sourcetype = apache_error
26/06/2025         2025-06-26 16:17:38,112 fail2ban.filter         [1827]: INFO    [sshd] Found 192.168.52.128 - 2025-06-26 16:17:26
20:17:38.112       host = scarface | source = /var/log/fail2ban.log | sourcetype = fail2ban
26/06/2025         2025-06-26 16:17:38,105 fail2ban.filter         [1827]: INFO    [sshd] Found 192.168.52.128 - 2025-06-26 16:17:26
20:17:38.105       host = scarface | source = /var/log/fail2ban.log | sourcetype = fail2ban
26/06/2025         2025-06-26 16:17:38,097 fail2ban.filter         [1827]: INFO    [sshd] Found 192.168.52.128 - 2025-06-26 16:17:26
20:17:38.097       host = scarface | source = /var/log/fail2ban.log | sourcetype = fail2ban
26/06/2025         2025-06-26 16:17:37,758 fail2ban.filter         [1827]: INFO    [sshd] Found 192.168.52.128 - 2025-06-26 16:17:26
20:17:37.758       host = scarface | source = /var/log/fail2ban.log | sourcetype = fail2ban
26/06/2025         2025-06-26T16:17:28.169387+00:00 scarface sshd[93974]: Connection closed by authenticating user matrix 192.168.52.128 port 34798 [preauth]
20:17:28.169       host = scarface | source = /var/log/auth.log | sourcetype = auth-4
26/06/2025         2025-06-26T16:17:28.163417+00:00 scarface sshd[93973]: Connection closed by authenticating user matrix 192.168.52.128 port 34796 [preauth]
20:17:28.163       host = scarface | source = /var/log/auth.log | sourcetype = auth-4
26/06/2025         2025-06-26T16:17:28.162492+00:00 scarface sshd[93975]: Connection closed by authenticating user matrix 192.168.52.128 port 34808 [preauth]
20:17:28.162       host = scarface | source = /var/log/auth.log | sourcetype = auth-4
26/06/2025         2025-06-26T16:17:28.161130+00:00 scarface sshd[93971]: Connection closed by authenticating user matrix 192.168.52.128 port 34782 [preauth]
20:17:28.161       host = scarface | source = /var/log/auth.log | sourcetype = auth-4
26/06/2025         2025-06-26T16:17:26.447281+00:00 scarface sshd[93973]: Failed password for matrix from 192.168.52.128 port 34796 ssh2
20:17:26.447       host = scarface | source = /var/log/auth.log | sourcetype = auth-4
26/06/2025         2025-06-26T16:17:26.443272+00:00 scarface sshd[93971]: Failed password for matrix from 192.168.52.128 port 34782 ssh2
20:17:26.443       host = scarface | source = /var/log/auth.log | sourcetype = auth-4
26/06/2025         2025-06-26T16:17:26.442053+00:00 scarface sshd[93975]: Failed password for matrix from 192.168.52.128 port 34808 ssh2
```

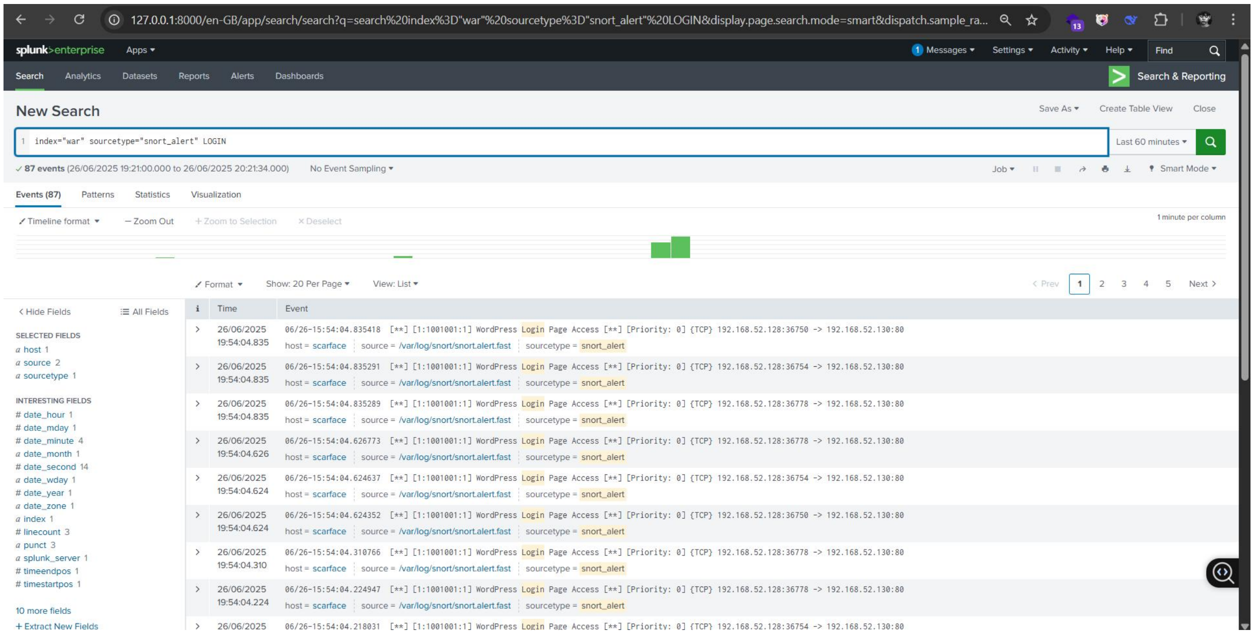


```
127.0.0.1:8000/en-GB/app/search/search?q=search%20index%3D"war"%20sourcetype%3D"snort_alert"%20SSH&display.page.search.mode=smart&dispatch.sample_ratio...
```

```
index="war" sourcetype="snort_alert" SSH
```

✓ 6 events (26/06/2025 19:21:00.000 to 26/06/2025 20:21:14.000)

```
26/06/2025         06/26-16:17:24.172638  [**] [1:1000002:1] SSH Connection Attempt [**] [Priority: 0] {TCP} 192.168.52.128:34808 -> 192.168.52.130:22
20:17:24.172       host = scarface | source = /var/log/snort/snort.alert.fast | sourcetype = snort_alert
26/06/2025         06/26-16:17:24.172638  [**] [1:1003008:1] SSH Brute Force Attempt [**] [Priority: 0] {TCP} 192.168.52.128:34808 -> 192.168.52.130:22
20:17:24.172       host = scarface | source = /var/log/snort/snort.alert.fast | sourcetype = snort_alert
26/06/2025         06/26-16:17:24.172638  [**] [1:1000002:1] SSH Connection Attempt [**] [Priority: 0] {TCP} 192.168.52.128:34798 -> 192.168.52.130:22
20:17:24.172       host = scarface | source = /var/log/snort/snort.alert.fast | sourcetype = snort_alert
26/06/2025         06/26-16:17:24.172637  [**] [1:1000002:1] SSH Connection Attempt [**] [Priority: 0] {TCP} 192.168.52.128:34796 -> 192.168.52.130:22
20:17:24.172       host = scarface | source = /var/log/snort/snort.alert.fast | sourcetype = snort_alert
26/06/2025         06/26-16:17:24.170889  [**] [1:1000002:1] SSH Connection Attempt [**] [Priority: 0] {TCP} 192.168.52.128:34782 -> 192.168.52.130:22
20:17:24.170       host = scarface | source = /var/log/snort/snort.alert.fast | sourcetype = snort_alert
26/06/2025         06/26-16:17:23.660276  [**] [1:1000002:1] SSH Connection Attempt [**] [Priority: 0] {TCP} 192.168.52.128:34774 -> 192.168.52.130:22
20:17:23.660       host = scarface | source = /var/log/snort/snort.alert.fast | sourcetype = snort_alert
```



```
index="war" sourcetype="snort_alert" LOGIN
```

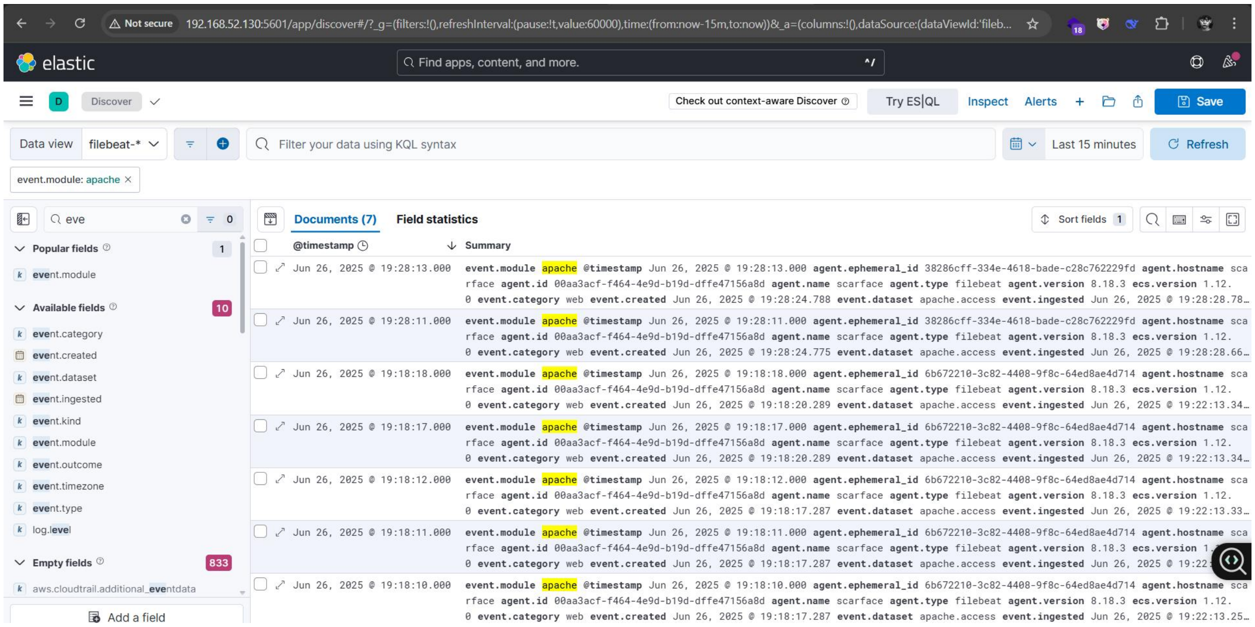
✓ 87 events (26/06/2025 19:21:00.000 to 26/06/2025 20:21:34.000)   No Event Sampling

SELECTED FIELDS
a host 1
a source 2
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 4
a date_month 1
# date_second 14
a date_wday 1
# date_year 1
a date_zone 1
a index 1
# linecount 3
a punct 3
a splunk_server 1
# timeendpos 1
# timestartpos 1

10 more fields
+ Extract New Fields

```
i  Time                     Event
>  26/06/2025               06/26-15:54:04.835418  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.128:36750 -> 192.168.52.130:80
   19:54:04.835             host = scarface   source = /var/log/snort/snort.alert.fast   sourcetype = snort_alert
>  26/06/2025               06/26-15:54:04.835291  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.128:36754 -> 192.168.52.130:80
   19:54:04.835             host = scarface   source = /var/log/snort/snort.alert.fast   sourcetype = snort_alert
>  26/06/2025               06/26-15:54:04.835289  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.128:36778 -> 192.168.52.130:80
   19:54:04.835             host = scarface   source = /var/log/snort/snort.alert.fast   sourcetype = snort_alert
>  26/06/2025               06/26-15:54:04.626773  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.128:36778 -> 192.168.52.130:80
   19:54:04.626             host = scarface   source = /var/log/snort/snort.alert.fast   sourcetype = snort_alert
>  26/06/2025               06/26-15:54:04.624637  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.128:36754 -> 192.168.52.130:80
   19:54:04.624             host = scarface   source = /var/log/snort/snort.alert.fast   sourcetype = snort_alert
>  26/06/2025               06/26-15:54:04.624352  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.128:36750 -> 192.168.52.130:80
   19:54:04.624             host = scarface   source = /var/log/snort/snort.alert.fast   sourcetype = snort_alert
>  26/06/2025               06/26-15:54:04.310766  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.128:36778 -> 192.168.52.130:80
   19:54:04.310             host = scarface   source = /var/log/snort/snort.alert.fast   sourcetype = snort_alert
>  26/06/2025               06/26-15:54:04.224947  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.128:36778 -> 192.168.52.130:80
   19:54:04.224             host = scarface   source = /var/log/snort/snort.alert.fast   sourcetype = snort_alert
>  26/06/2025               06/26-15:54:04.218031  [**] [1:1001001:1] WordPress Login Page Access [**] [Priority: 0] {TCP} 192.168.52.128:36754 -> 192.168.52.130:80
```


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.
D
Discover
Check out context-aware Discover
Try ES|QL
Inspect
Alerts
Save
Data view
Filter your data using KQL syntax
Refresh
Documents (7)
Field statistics
Sort fields 1
Add a field

Data view: filebeat-*   Last 15 minutes

event.module: apache

eve

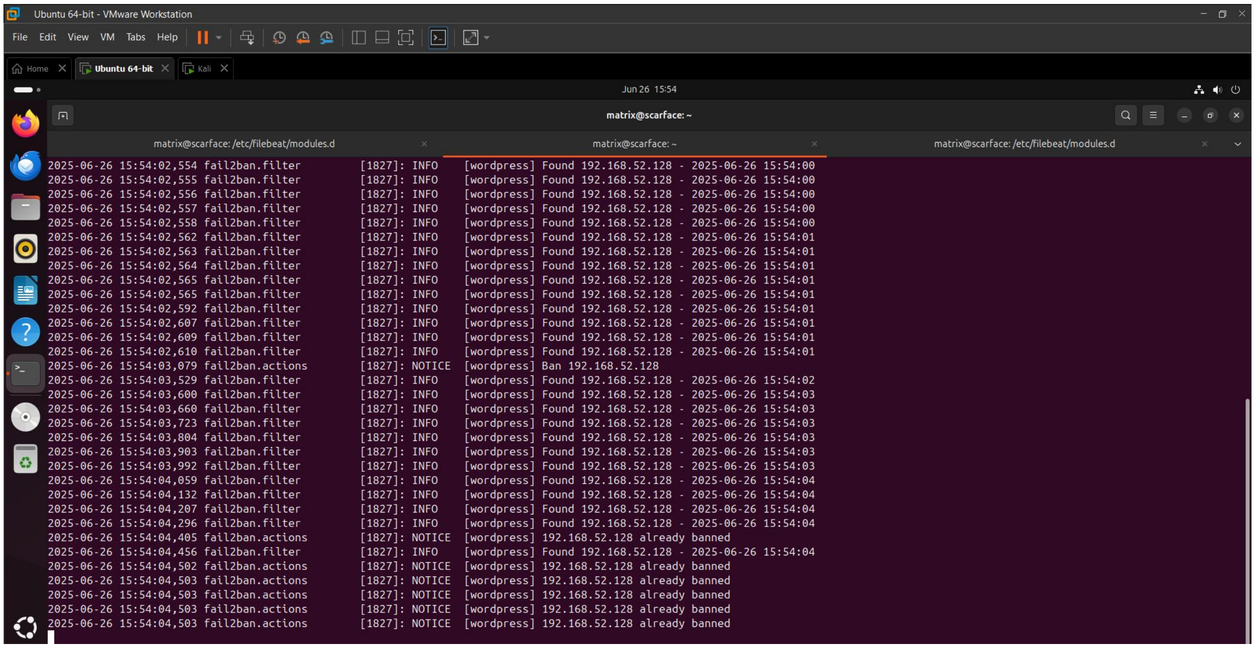
Popular fields 1
event.module

Available fields 10
event.category
event.created
event.dataset
event.ingested
event.kind
event.module
event.outcome
event.timezone
event.type
log.level

Empty fields 833
aws.cloudtrail.additional_eventdata

```
@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 sca
                             rface 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 sca
                             rface 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 sca
                             rface 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 sca
                             rface 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 sca
                             rface 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 sca
                             rface 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 sca
                             rface 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…
```

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.