BOOTCAMP PROJECT REPORT

Project Title	:	**Integrated Intrusion Detection Systems: Monitoring and Response to Network and Host Anomalies**
Bootcamp Client	:	**PT Square Gate One**
Concentration	:	**Cybersecurity**

By:

Alghazali Winet Abdurrahman	001202300125
Ahmad Akbar Sidiq. N	001202300017
Ida Bagus Wahyudha Gautama	001202300107
Zaidan Mahfudz Azzam Saidi	001202300144

INFORMATICS STUDY PROGRAM
FACULTY OF COMPUTER SCIENCE
PRESIDENT UNIVERSITY

ABSTRACT

This project focuses on simulating and detecting cyberattacks using Host-Based Intrusion Detection Systems (HIDS) and Network-Based Intrusion Detection Systems (NIDS). The implementation utilizes **Wazuh** for HIDS and **Suricata** for NIDS, integrated within a local environment featuring an Ubuntu-based Wazuh manager, a Windows victim machine, and a Kali Linux attacker. The goal was to monitor and identify security breaches such as brute-force logins, port scans, and file upload attacks through custom rules and alert mechanisms. We configured Suricata to capture real-time network traffic and send alerts via Wazuh, while the Windows agent monitored host activity and Apache logs. Alerts were fine-tuned to trigger email notifications for critical threats. The project successfully demonstrated the practical value of HIDS and NIDS in detecting simulated attacks, offering insights into building low-cost, real-time detection systems.

INTRODUCTION

Background & Current Trends

Cybersecurity remains a core concern in today's digital ecosystem. As threats like malware, phishing, and brute-force attacks grow more sophisticated, Intrusion Detection Systems (IDS) offer crucial protection. HIDS and NIDS, especially open-source ones like Wazuh and Suricata, provide cost-effective solutions for real-time monitoring.

Problem Statement

Many systems lack centralized, real-time threat visibility across host and network levels, leading to undetected intrusions and delayed responses.

Objectives

1. Implement HIDS using Wazuh to monitor endpoint activities.
2. Implement NIDS using Suricata to detect network-based threats.
3. Simulate attacks and verify system detection and response.
4. Set up follow up action (email alerting) for critical events.

Scope & Limitations

This project runs within a local network setup using virtual machines. Internet-based real-world testing was not included. The email alerting is limited to local SMTP (Postfix), and automatic IP blocking was not implemented.

Relevance to Real-World Problems

This setup demonstrates how organizations can monitor threats in real time, reducing breach response time, and can be scaled for use in SMEs, SOCs, or education labs.

METHODS

Approach

We configured a secure network with:

1. Wazuh for log collection, agent monitoring, and rule correlation.
2. Suricata for deep packet inspection and traffic monitoring.
3. Simulated attacks were launched from Kali Linux to trigger alerts.

Development Tools

OS: Ubuntu 22.04, Windows 11, Kali Linux

IDS Tools: Wazuh 4.7, Suricata 7.0.3

Web Stack: XAMPP (Apache, PHP, MySQL)

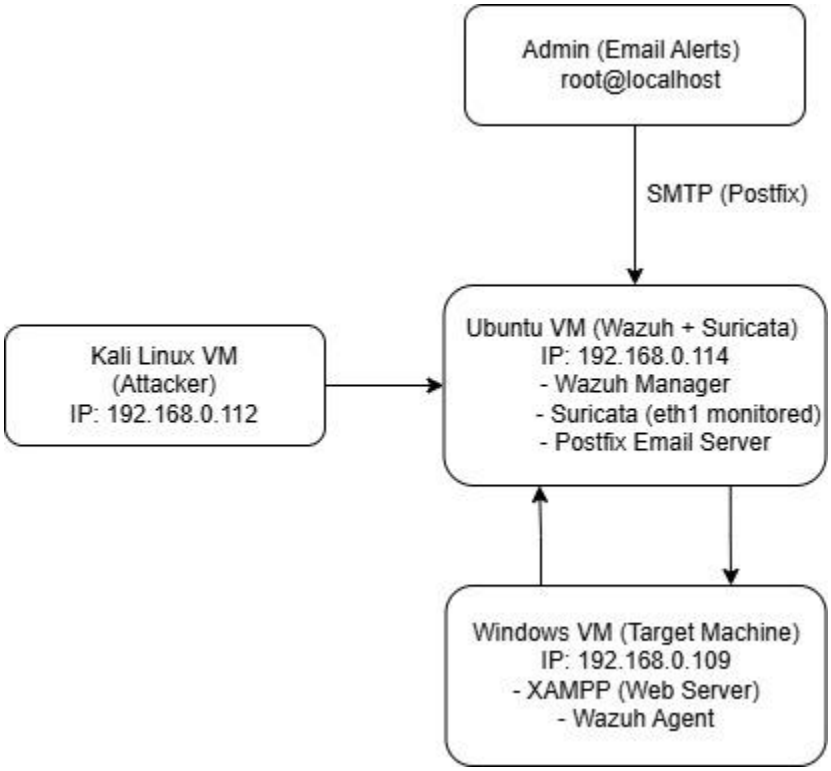
Attack Tools: Hydra, Nikto, Nmap

Follow-up Alerting: Postfix (local mail server)

Design Diagrams

3-Node Architecture:

1. Ubuntu Wazuh Manager (192.168.0.114)
2. Windows Agent/XAMPP (192.168.0.109)
3. Kali Attacker (192.168.0.112)



Teamwork / Workflow

- Installed on each our device, but testing mainly on Alghazali's Laptop
- Discord for collaboration and troubleshooting

RESULTS

Main Features Developed

1. Real-time detection of brute-force logins using custom Wazuh rules
2. Detection of web shell uploads via Apache access logs
3. Suricata alerts triggered by Nikto and Nmap scans
4. Email alerting configured via Postfix for alerts ≥ level 7

Screenshots & Logs

1. Suricata JSON alerts (NIDS) and triggered custom rules

    - Nmap scan (Rule 100008)

timestamp per 30 minutes

Time	rule.description	data.alert.signature	data.alert.category
May 1, 2025 @ 03:18:48.977	HIGH LEVEL - Nmap Port Scan Detected	-	-
May 1, 2025 @ 03:18:4	HIGH LEVEL - Nmap Port Scan Detected	-	-
May 1, 2025 @ 03:18:48.977	HIGH LEVEL - Nmap Port Scan Detected	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack
May 1, 2025 @ 03:18:48.977	HIGH LEVEL - Nmap Port Scan Detected	-	-
May 1, 2025 @ 03:18:48.977	HIGH LEVEL - Nmap Port Scan Detected	-	-
May 1, 2025 @ 03:18:48.977	HIGH LEVEL - Nmap Port Scan Detected	-	-
May 1, 2025 @ 03:18:48.977	HIGH LEVEL - Nmap Port Scan Detected	-	-
May 1, 2025 @ 03:18:48.977	HIGH LEVEL - Nmap Port Scan Detected	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack
May 1, 2025 @ 03:18:48.977	HIGH LEVEL - Nmap Port Scan Detected	-	-
May 1, 2025 @ 03:18:48.977	HIGH LEVEL - Nmap Port Scan Detected	-	-
May 1, 2025 @ 03:18:48.977	HIGH LEVEL - Nmap Port Scan Detected	ET SCAN Possible Nmap User-Agent Obs	Web Application Attac

t	input.type	log
t	location	/var/log/suricata/eve.json
t	manager.name	cathzer-VirtualBox
t	rule.description	HIGH LEVEL - Nmap Port Scan Detected
#	rule.firedtimes	74
t	rule.groups	local, customnetwork, scan, portscan
t	rule.id	100008
#	rule.level	8
	rule.mail	true
	timestamp	May 15, 2025 @ 09:17:45.020

- Nikto (taken from matching with “Successful Credential Theft Detected” and using custom rule 100007)

›	May 15, 2025 @ 09:20:13.357	Attempted Administrator Privilege Gain	3	ET EXPLOIT D-Link DSL-2750B Command Injection Attempt (CVE-2016-20017)	Suricata: Alert - ET EXPLOIT D-Link DSL-2750B Command Injection Attempt (CVE-2016-20017)
›	May 15, 2025 @ 09:20:09.357	Web Application Attack	3	ET WEB_SERVER ColdFusion componentutils access	Suricata: Alert - ET WEB_SERVER Cold Fusion componentutils access
›	May 15, 2025 @ 09:20:07.337	Successful Credential Theft Detected	8	ET WEB_SPECIFIC_APPS Wordpress LiteSpeed Cache Plugin debug.log Access Attempt (CVE-2024-44000)	HIGH LEVEL - Nikto Scan Detected
›	May 15, 2025 @ 09:20:07.332	Generic Protocol Command Decode	3	SURICATA Applayer Detect protocol only one direction	Suricata: Alert - SURICATA Applayer Detect protocol only one direction

t	manager.name	cathzer-VirtualBox
t	rule.description	HIGH LEVEL - Nikto Scan Detected
#	rule.firedtimes	1
t	rule.groups	local, customnetwork, attack
t	rule.id	100007
#	rule.level	8
	rule.mail	true
	timestamp	May 15, 2025 @ 09:20:07.337

2. Wazuh HIDS logs and triggered rules

- Brute-Forcing using Hydra

Security Alerts

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
May 15, 2025 @ 09:24:09.249	002	MSI			IDS event.	6	20101
May 15, 2025 @ 09:24:09.245	002	MSI			Brute-force login detected: 10 failed attempts within 60s	10	100010
May 15, 2025 @ 09:24:09.242	002	MSI			IDS event.	6	20101
May 15, 2025 @ 09:24:09.240	002	MSI			IDS event.	6	20101
May 15, 2025 @ 09:24:09.237	002	MSI			IDS event.	6	20101
May 15, 2025 @ 09:24:09.234	002	MSI			IDS event.	6	20101
May 15, 2025 @ 09:24:09.231	002	MSI			IDS event.	6	20101

rule.description	Brute-force login detected: 10 failed attempts within 60s
rule.firedtimes	39
rule.frequency	10
rule.groups	local, custombrute_force, ids, authentication_failed
rule.id	100010
rule.level	10
rule.mail	true
timestamp	2025-05-15T09:24:09.245+0700

- Web Shell Upload and Execution

Security Alerts

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
May 15, 2025 @ 09:27:04.981	002	MSI			HIGH LEVEL - Shell.php Command Execution Detected	8	100009
May 15, 2025 @ 09:27:00.947	002	MSI			HIGH LEVEL - Shell.php Command Execution Detected	8	100009

rule.description	HIGH LEVEL - Shell.php Command Execution Detected
rule.firedtimes	2
rule.groups	local, customweb, attack, shell
rule.id	100009
rule.level	8
rule.mail	true
timestamp	2025-05-15T09:27:04.981+0700

3. Logs confirming alert mail follow-up

rule.groups	local, customweb, attack, shell
rule.id	100009
rule.level	8
rule.mail	true
timestamp	2025-05-15T09:27:04.981+0700

Security Test Reports

Nmap detected: Port scan → Suricata → Wazuh (alert level: 7+)

```
Return-Path: <wazuh@localhost>
X-Original-To: root@localhost
Delivered-To: root@localhost
Received: from notify.ossec.net (localhost [127.0.0.1])
        by cathzer-VirtualBox (Postfix) with SMTP id 153561000E7
        for <root@localhost>; Wed, 14 May 2025 18:53:04 +0700 (WIB)
To: <root@localhost>
From: Wazuh <wazuh@localhost>
Date: Wed, 14 May 2025 18:53:04 +0700
Subject: Wazuh notification - cathzer-VirtualBox - Alert level 8
Message-Id: <20250514115304.153561000E7@cathzer-VirtualBox>


Wazuh Notification.
2025 May 14 18:52:51

Received From: cathzer-VirtualBox->/var/log/suricata/eve.json
Rule: 100008 fired (level 8) -> "HIGH LEVEL - Nmap Port Scan Detected"
Portion of the log(s):

{"timestamp":"2025-05-14T18:52:49.790921+0700","flow_id":523868780458745,"in_ifa
ce":"enp0s9","event_type":"alert","src_ip":"192.168.0.112","src_port":51596,"des
t_ip":"192.168.0.114","dest_port":9080,"proto":"TCP","pkt_src":"wire/pcap","tx_i
```

Nikto detected: Vulnerability scan on NGINX container

```
Return-Path: <wazuh@localhost>
X-Original-To: root@localhost
Delivered-To: root@localhost
Received: from notify.ossec.net (localhost [127.0.0.1])
        by cathzer-VirtualBox (Postfix) with SMTP id 8F57C1000E7
        for <root@localhost>; Wed, 14 May 2025 18:45:03 +0700 (WIB)
To: <root@localhost>
From: Wazuh <wazuh@localhost>
Date: Wed, 14 May 2025 18:45:03 +0700
Subject: Wazuh notification - cathzer-VirtualBox - Alert level 8
Message-Id: <20250514114503.8F57C1000E7@cathzer-VirtualBox>


Wazuh Notification.
2025 May 14 18:44:52

Received From: cathzer-VirtualBox->/var/log/suricata/eve.json
Rule: 100007 fired (level 8) -> "HIGH LEVEL - Nikto Scan Detected"
Portion of the log(s):

{"timestamp":"2025-05-14T18:44:52.286945+0700","flow_id":1150060424733428,"in_if
ace":"enp0s9","event_type":"alert","src_ip":"192.168.0.112","src_port":59326,"de
st_ip":"192.168.0.114","dest_port":9080,"proto":"TCP","pkt_src":"wire/pcap","tx_
--More--
```

Hydra attack: Repeated login attempts → email alert

```
Return-Path: <wazuh@localhost>
X-Original-To: root@localhost
Delivered-To: root@localhost
Received: from notify.ossec.net (localhost [127.0.0.1])
        by cathzer-VirtualBox (Postfix) with SMTP id E7F6C1000E7
        for <root@localhost>; Wed, 14 May 2025 18:06:05 +0700 (WIB)
To: <root@localhost>
From: Wazuh <wazuh@localhost>
Date: Wed, 14 May 2025 18:06:05 +0700
Subject: Wazuh notification - (MSI) any - Alert level 10
Message-Id: <20250514110605.E7F6C1000E7@cathzer-VirtualBox>


Wazuh Notification.
2025 May 14 18:05:42

Received From: (MSI) any->C:\wazuh_logs\login_attempts.log
Rule: 100010 fired (level 10) -> "Brute-force login detected: 10 failed attempts
 within 60s"
Portion of the log(s):

2025-05-14 13:05:40|192.168.0.112|admin|failed
2025-05-14 13:05:40|192.168.0.112|admin|failed
```

Web shell execution: Triggered rule via Apache log (Windows agent)

```
Return-Path: <wazuh@localhost>
X-Original-To: root@localhost
Delivered-To: root@localhost
Received: from notify.ossec.net (localhost [127.0.0.1])
        by cathzer-VirtualBox (Postfix) with SMTP id 3FD0D1000E7
        for <root@localhost>; Wed, 14 May 2025 17:55:35 +0700 (WIB)
To: <root@localhost>
From: Wazuh <wazuh@localhost>
Date: Wed, 14 May 2025 17:55:35 +0700
Subject: Wazuh notification - (MSI) any - Alert level 8
Message-Id: <20250514105535.3FD0D1000E7@cathzer-VirtualBox>


Wazuh Notification.
2025 May 14 17:55:19

Received From: (MSI) any->C:\xampp\apache\logs\access.log
Rule: 100009 fired (level 8) -> "HIGH LEVEL - Shell.php Command Execution Detect
ed"
Src IP: 192.168.0.109
Portion of the log(s):

192.168.0.109 - - [14/May/2025:17:55:18 +0700] "GET /Wazuh_Demo/uploads/shell.ph
```

DISCUSSION

What Went Well :

Throughout the project, several key components were implemented successfully. One of the major achievements was the smooth integration of Wazuh and Suricata, which allowed for effective monitoring of both host and network activities in a local simulated environment. We were also able to simulate various types of attacks—such as brute-force login attempts, shell upload exploits, port scans, and web application scanning—demonstrating the flexibility and detection capabilities of both HIDS and NIDS. The creation and application of custom rules proved to be effective in identifying specific threats. Additionally, configuring email notifications helped ensure that critical alerts were delivered in real time, providing immediate awareness of security incidents.

Challenges

One of the initial hurdles involved understanding and troubleshooting Wazuh's rule syntax, particularly realizing that certain options like `<email_alert>` are unsupported, which led to configuration errors. Another issue emerged during Suricata's setup, where file permission problems prevented Wazuh from reading the `eve.json` log correctly. Furthermore, designing correlation rules to detect repeated brute-force login attempts required fine-tuning to avoid both false positives and missed alerts.

Improvements

One valuable improvement would be the implementation of Wazuh's Active Response feature to automatically block IP addresses after suspicious activity is detected, thereby reducing the response time to threats. Additionally, forwarding email alerts via a trusted external SMTP server such as Gmail would make the alerting mechanism more reliable for real deployments. Finally, expanding the attack simulation library to include threats like Cross-Site Scripting (XSS) and Remote Code Execution (RCE) would strengthen the system's ability to handle a broader range of real-world attack scenarios.

Ethical/Security Considerations

All testing was done in isolated local environments. These tools are powerful and must be used responsibly under legal boundaries.

CONCLUSION

We successfully demonstrated the detection of host-based and network-based intrusions using open-source tools Wazuh and Suricata. Through simulated attacks such as brute-force, shell uploads, and port scans, our system accurately identified and alerted us in real time. We gained hands-on experience configuring IDS, writing rules, and interpreting logs. This project has real-world implications for enhancing organizational security monitoring on a budget and can be expanded with auto-response mechanisms in future work.

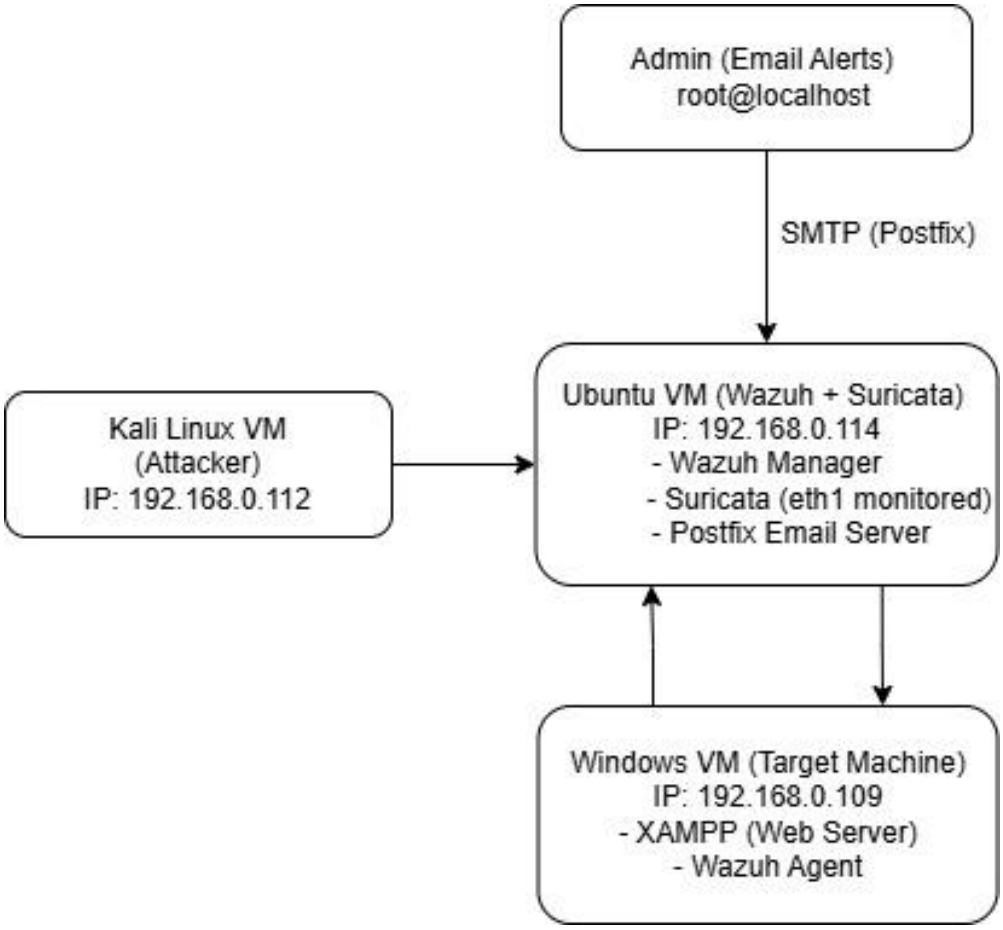
APPENDICES

Full code
- Only local_rules.xml was modified for detection logic

```
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,custom">

  <!-- Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 > -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

  <!-- Shell.php webshell detection -->
  <rule id="100005" level="8">
    <program_name>apache</program_name>
    <match>shell.php</match>
    <description>Possible shell.php upload or execution</description>
    <group>web, attack, shell</group>
  </rule>

  <!-- Brute-force login detection -->
  <rule id="100006" level="8">
    <program_name>apache</program_name>
    <match>Invalid credentials</match>
    <description>Brute-force login attempt detected</description>
    <group>authentication_failed, brute_force</group>  </rule>

  <!-- Suricata detects Successful Credential Theft (ex. Nikto or others) -->
  <rule id="100007" level="8">
    <if_group>ids,suricata</if_group>
    <match>Successful Credential Theft Detected</match>
    <description>HIGH LEVEL - Nikto Scan Detected</description>
    <group>network, attack</group>
  </rule>
<!-- Suricata detects Nmap -->
  <rule id="100008" level="8">
    <if_group>ids,suricata</if_group>
    <match>Nmap</match>
    <description>HIGH LEVEL - Nmap Port Scan Detected</description>
    <group>network, scan, portscan</group>
  </rule>
```

```
  <rule id="100009" level="8">
    <if_sid>31514</if_sid>
    <description>HIGH LEVEL - Shell.php Command Execution Detected</description>
    <group>web, attack, shell</group>
  </rule>

  <rule id="100010" level="10" frequency="10" timeframe="60">
    <if_matched_sid>20101</if_matched_sid>
    <description>Brute-force login detected: 10 failed attempts within 60s</des>
    <group>brute_force, ids, authentication_failed</group>
  </rule>
</group>
```

Diagram



User Manual

Installation Summary

- **Wazuh installed on Ubuntu using installation script:**

  curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh

  sudo bash ./wazuh-install.sh --ignore-check -a

- **Suricata installed:**

  sudo apt install suricata

- Suricata eve.json log enabled and linked in Wazuh config.

- Wazuh agent installed on Windows and configured with manager IP.

- Config Files Edited:
  1. /var/ossec/etc/ossec.conf — enabled email alert
  2. /var/ossec/etc/rules/local_rules.xml — added rules and adjusted rule level

- Email notifications setup:
  1. **Installed Postfix:**

  sudo apt install postfix

  2. **Configured Wazuh with:**

  <email_notification>yes</email_notification>

  <email_to>your-email@gmail.com</email_to>

  <email_from>wazuh@yourdomain.com</email_from>

  <smtp_server>localhost</smtp_server>

  <email_maxperhour>10</email_maxperhour>

- Attack Simulations
  1. **Nmap (NIDS) :**

     nmap -sV 192.168.0.114

  2. **Nikto (NIDS) :**

     nikto -h http://192.168.0.114:9080 (But we need to docker NGINX on the 9080 or other port before simulate the attack)

  3. **Hydra Brute Force (HIDS)** :

     hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.109 http-post-form "/Wazuh_Demo/login.php:name=^USER^&password=^PASS^:Invalid credentials" -s 8080

  4. **Web Shell Upload & Access (HIDS) :**
     - upload.php uploaded shell.php with command inside the file (`<?php system($_GET['cmd']); ?>`)
     - **Accessed via:** http://192.168.0.109:8080/Wazuh_Demo/uploads/shell.php?cmd=whoami

Risk Assessment

Threat	Risk	Impact	Mitigation
Unauthorized Shell Access	High	Remote execution	Detect via Apache logs + rule 31514
Brute-force Login	Medium	Password theft	Throttling via rule correlation (100010)
Nmap/Nikto Reconnaissance	Medium–High	Vulnerability intel	Alerting enabled for scan patterns
Log Overload / Alert Fatigue	Medium	Storage issues	Limited alert levels, hourly email cap

Video Demonstration

https://drive.google.com/drive/folders/1XP2HwC4L0lWx9ygUNljkEMsA6jOsKdH2?usp=sharing