Mini SIEM with ELK Stack — Project Report

1. Executive Summary:

This project demonstrates the design and implementation of a Security Information and Event Management (SIEM) solution using the ELK Stack (Elasticsearch, Logstash, Kibana). The system ingests logs from multiple sources, detects simulated attacks, and provides actionable insights for incident response.

Outcome: A functional mini-SIEM capable of log centralization, visualization, and detection of web application attacks (DVWA), authentication anomalies, and system events.

2. Objectives:

- Centralize logs from Apache, DVWA, and system authentication sources.
- Detect and visualize suspicious activity (SQL injection, brute force, command injection).
- Simulate incident response workflows (containment, lockout, forensic analysis).
- Provide recommendations for improving detection and response capabilities.

3. Environment Setup:

- Tools: Elasticsearch, Logstash, Kibana, Filebeat, Apache2, DVWA
- Architecture:
  - Filebeat → Logstash → Elasticsearch → Kibana
- Log Sources:
  - Apache access/error logs
  - /var/log/auth.log (SSH login attempts)
  - DVWA application logs

4. Methodology:

- Log Ingestion: Configured Filebeat to forward logs into Logstash pipelines.
- Parsing & Indexing: Applied Grok filters for structured fields (IP, timestamp, request type).
- Visualization: Built Kibana dashboards for authentication events, HTTP requests, and DVWA activity.
- Attack Simulation: Executed SQL injection and command injection attacks on DVWA.

- Detection: Verified alerts and anomalies in Kibana dashboards.

- Response Simulation: Disabled compromised accounts and reconstructed incident timeline.

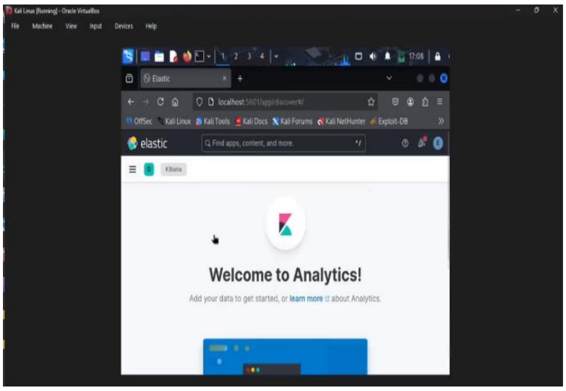
5. Findings:

Finding 1: Successful Log Ingestion

- Evidence: Apache logs ingested and indexed in Elasticsearch.

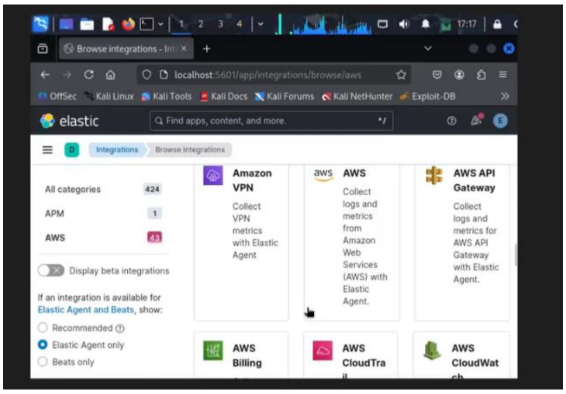
- Impact: Validates pipeline configuration.

- Screenshot Placeholder: Kibana dashboard showing live Apache logs.



Welcome to Analytics!

Add your data to get started, or learn more about Analytics.



localhost:5601/app/integrations/browse/aws

All categories	424
APM	1
AWS	43

Display beta integrations

If an integration is available for Elastic Agent and Beats, show:

○ Recommended

● Elastic Agent only

○ Beats only

Amazon VPN: Collect VPN metrics with Elastic Agent

AWS: Collect logs and metrics from Amazon Web Services (AWS) with Elastic Agent.

AWS API Gateway: Collect logs and metrics for AWS API Gateway with Elastic Agent.

AWS Billing

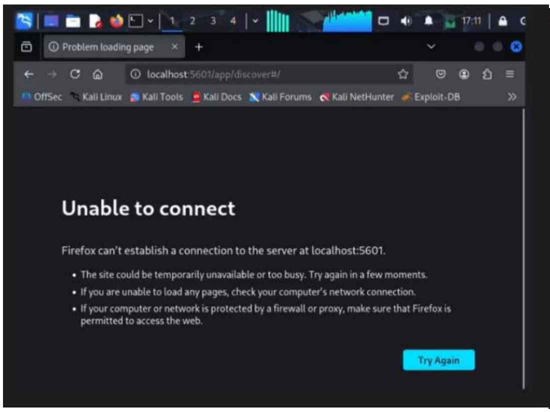
AWS CloudTrail

AWS CloudWatch

Finding 2: Authentication Events Tracked

- Evidence: Failed SSH login attempts visualized in Kibana.

- Impact: Enables brute-force detection.



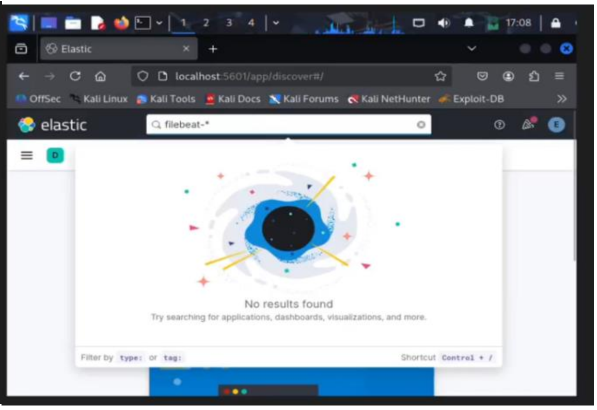
localhost:5601/app/discover#/

Unable to connect

Firefox can't establish a connection to the server at localhost:5601.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again



localhost:5601/app/discover#/

filebeat-*

No results found

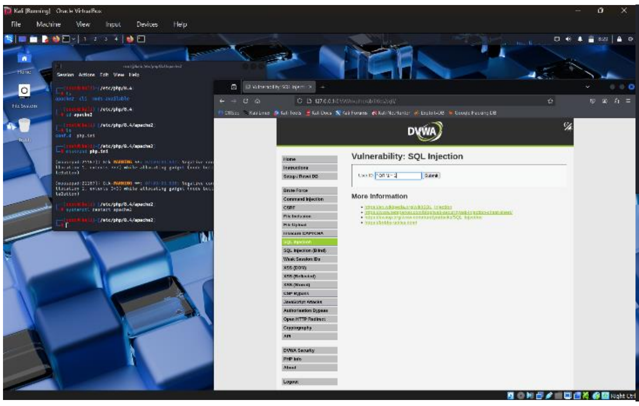
Try searching for applications, dashboards, visualizations, and more.

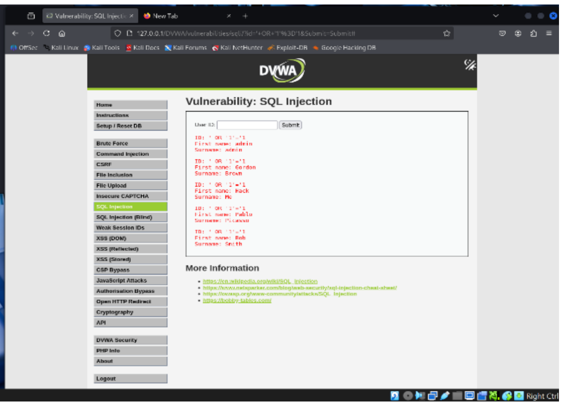
Filter by type: or tag: Shortcut Control + /

Finding 3: SQL Injection Detected

- Evidence: DVWA logs captured malicious payloads (' OR '1'='1).

- Impact: Confirms SIEM’s ability to detect web-based injection attacks.





Vulnerability: SQL Injection

```
ID: ' OR '1'='1
First name: admin
Surname: admin

ID: ' OR '1'='1
First name: Gordon
Surname: Brown

ID: ' OR '1'='1
First name: Hack
Surname: Me

ID: ' OR '1'='1
First name: Pablo
Surname: Picasso

ID: ' OR '1'='1
First name: Bob
Surname: Smith
```

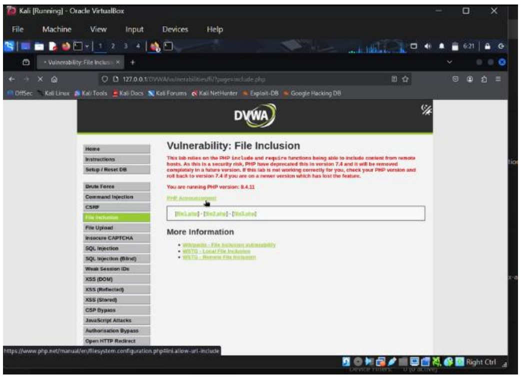
More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

Finding 4: Command Injection Detected

- Evidence: Logs show suspicious system command execution via DVWA input.

- Impact: Demonstrates OS-level exploitation detection.



Vulnerability: File Inclusion

This lab relies on the PHP include and require functions being able to include content from remote hosts. As this is a security risk, PHP have deprecated this in version 7.4 and it will be removed completely in a future version. If this lab is not working correctly for you, check your PHP version and roll back to version 7.4 if you are on a newer version which has lost the feature.

You are running PHP version: 8.4.11

PHP Announcement

[file1.php] - [file2.php] - [file3.php]

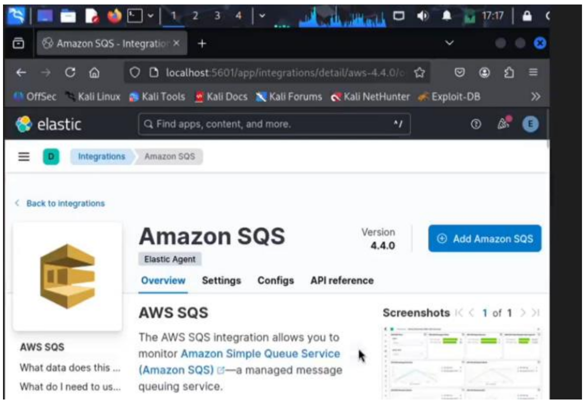
More Information

- Wikipedia - File inclusion vulnerability
- WSTG - Local File Inclusion
- WSTG - Remote File Inclusion

Finding 5: Incident Response Simulation

- Evidence: User account disabled post-detection; incident timeline reconstructed.

- Impact: Validates containment and forensic capabilities.



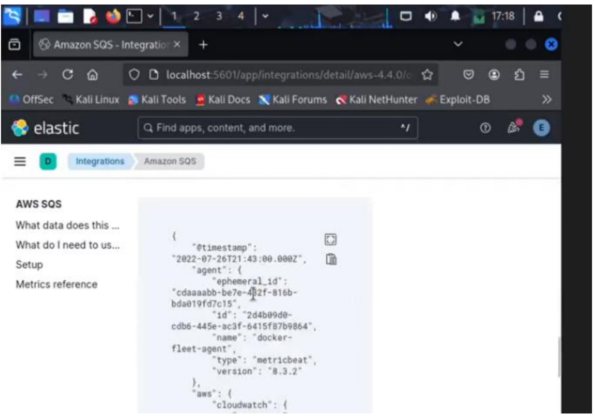
Amazon SQS

Elastic Agent

Version 4.4.0

AWS SQS

The AWS SQS integration allows you to monitor Amazon Simple Queue Service (Amazon SQS)—a managed message queuing service.



```
{
    "@timestamp":
"2022-07-26T21:43:00.000Z",
    "agent": {
        "ephemeral_id":
"cdaaaabb-be7e-4b2f-816b-
bda019fd7c15",
        "id": "2d4b09d0-
cdb6-445e-ac3f-6415f87b9864",
        "name": "docker-
fleet-agent",
        "type": "metricbeat",
        "version": "8.3.2"
    },
    "aws": {
        "cloudwatch": {
```

6. Risk Rating Summary:

Event/Attack	Severity	Detection Status	Response Action
SQL Injection	High	Detected	Alert + Timeline
Command Injection	High	Detected	Containment
Failed SSH Logins	Medium	Detected	Account Lockout
Apache Misconfigurations	Medium	Observed Hardening	Config

7. Recommendations:

- Configure alert thresholds for failed logins.
- Integrate GeoIP filtering for suspicious regions.
- Automate email/SMS alerts for critical events.
- Harden DVWA and Apache configurations.
- Extend SIEM to include IDS/IPS logs for broader coverage.

8. Conclusion:

The Mini SIEM project successfully demonstrates the feasibility of using ELK Stack for centralized log management, attack detection, and incident response. While limited in scale, the system provides a strong foundation for enterprise-level SIEM deployment and highlights the importance of proactive monitoring in cybersecurity.