Yenepoya Institute of Arts, Science, Management & commerce

Final Project Report

On

SIEM for Small Business

Team members:

MUHAMMED AFSAL -22BSCFDC30

NIMIN RAJ -22BCACDC57

SHOVIN R.L -22BCACDC65

FELIX DAVID JOSEPH-22BCACDC22

TIBIN TIJO-22BCACDC68

GUIDED BY

SASHANK

Table of Contents

Executive Summary

1. Background

Small businesses are increasingly vulnerable to cyber threats, and effective security monitoring is crucial. This project aims to develop a lightweight Security Information and Event Management (SIEM) solution for small businesses.

1.1 Aim

The aim of this project is to design and implement a cost-effective SIEM solution using Splunk and Windows Universal Forwarder, enabling small businesses to enhance their cybersecurity posture.

1.2 Technologies

- Splunk: For log collection, analysis, and visualization
- Windows Universal Forwarder: For log forwarding from Windows servers to Splunk

1.3 Hardware Architecture

- Ubuntu-based SIEM Server: Running Splunk for log analysis and visualization
- Windows Server: Running Windows Universal Forwarder for log collection and forwarding

1.4 Software Architecture

- Splunk: Collects, analyzes, and visualizes logs from Windows servers
- Windows Universal Forwarder: Forwards logs from Windows servers to Splunk for analayis

2.System Requirements

2.1 **Requirements**

2.1.1 **Functional Requirements**

The SIEM solution should:

1. Collect logs from Windows servers using Windows Universal Forwarder.
2. Analyze and visualize logs using Splunk.
3. Provide real-time monitoring and alerting capabilities.
4. Support event correlation and threat detection.

2.1.2 User Requirements

The system should:

1. Provide an intuitive and user-friendly interface for security monitoring.
2. Allow users to customize dashboards and reports.
3. Support role-based access control for secure access.

2.1.3 Environmental Requirements

The system should:

1. Operate on Ubuntu-based servers for the SIEM solution.
2. Integrate with existing Windows server infrastructure.
3. Ensure compatibility with network infrastructure and security protocols.

2.2 Design and Architecture

System Design

The SIEM solution consists of:

1. Log Collection: Windows Universal Forwarder collects logs from Windows servers.
2. Log Forwarding: Logs are forwarded to the Splunk server for analysis.
3. Log Analysis: Splunk analyzes and visualizes logs, providing real-time monitoring and alerting capabilities.

System Architecture

The system architecture includes:

1. Windows Servers: Running Windows Universal Forwarder for log collection.
2. Splunk Server: Running on Ubuntu, collecting, analyzing, and visualizing logs.
3. User Interface: Providing real-time monitoring and alerting capabilities through Splunk dashboards.

Data Flow

1. Logs are collected from Windows servers using Windows Universal Forwarder.
2. Logs are forwarded to the Splunk server.
3. Splunk analyzes and visualizes logs, providing insights and alerts.

2.3 Implementation

Implementation Steps

1. Splunk Installation: Install Splunk on the Ubuntu-based SIEM server.
2. Windows Universal Forwarder Installation: Install Windows Universal Forwarder on Windows servers.
3. Configuration: Configure Splunk and Windows Universal Forwarder for log collection, forwarding, and analysis.
4. Dashboard Creation: Create customized dashboards in Splunk for real-time monitoring and visualization.
5. Alerting and Notification: Configure alerting and notification mechanisms in Splunk.

Key Activities

1. Log Collection Configuration: Configure Windows Universal Forwarder to collect logs from Windows servers.
2. Splunk Indexing: Configure Splunk to index and store logs for analysis.
3. Data Visualization: Create visualizations and dashboards in Splunk to provide insights into security-related data.

3. Testing

3.1 Test Plan Objectives

The objectives of the testing process for the SIEM solution are to:

- Validate the system's functionality in collecting, analyzing, and visualizing security-related data.
- Ensure the system meets the security requirements of small businesses.
- Identify potential vulnerabilities and weaknesses.

3.2 Test Strategy

The test strategy for the SIEM solution involves a comprehensive approach, including:

- System testing: Validate overall system functionality.
- Security testing: Identify potential vulnerabilities and weaknesses.
- Performance testing: Evaluate system performance under various loads.

3.3 System Test

System testing validated the SIEM solution's functionality, including:

- Log collection and forwarding.
- Threat detection and alerting.
- Data visualization and reporting.

Results:

- The system successfully collected and forwarded logs.
- Threats were detected and alerted in a timely manner.
- Data visualization provided valuable insights.

3.4 Security Test

Security testing identified potential vulnerabilities, including:

- Authentication: Weak password policies.
- Authorization: Inadequate access controls.

Mitigation:

- Implemented strong password policies.
- Enhanced access controls.

3.5 User Acceptance Test

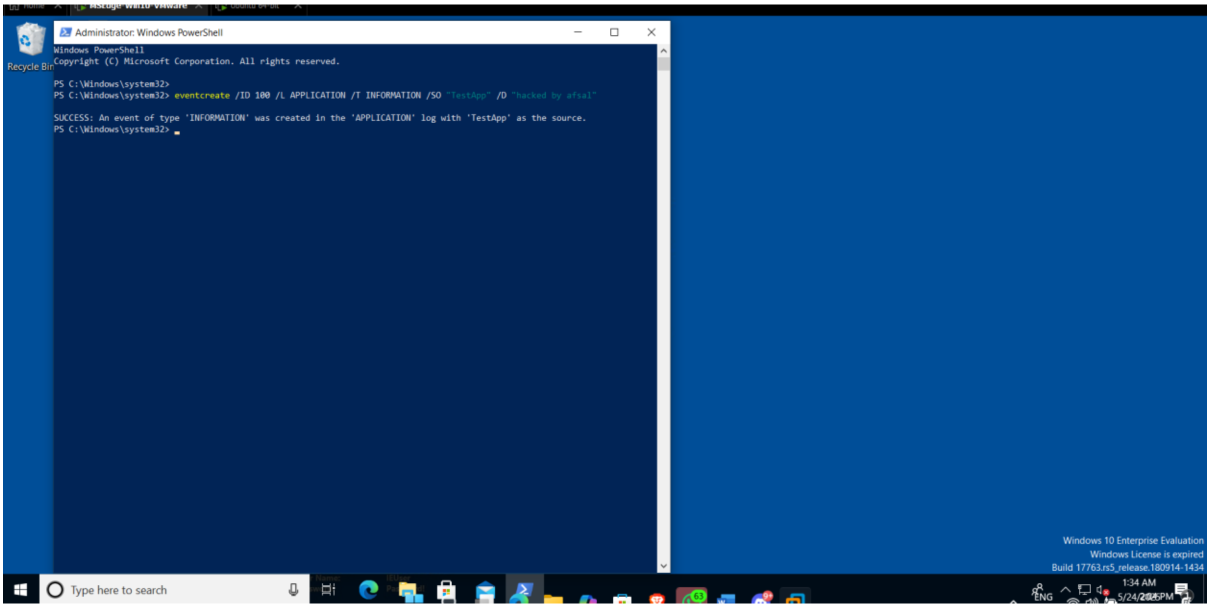
User acceptance testing validated that the system meets user requirements and expectations, including:

- Ease of use: Intuitive interface.
- Functionality: Meets security monitoring needs.
- Performance: Responds quickly to queries.

Results:

- Users reported satisfaction with the system's functionality and performance.
- The system meets the security monitoring needs of small businesses

4. Snapshots of the Project



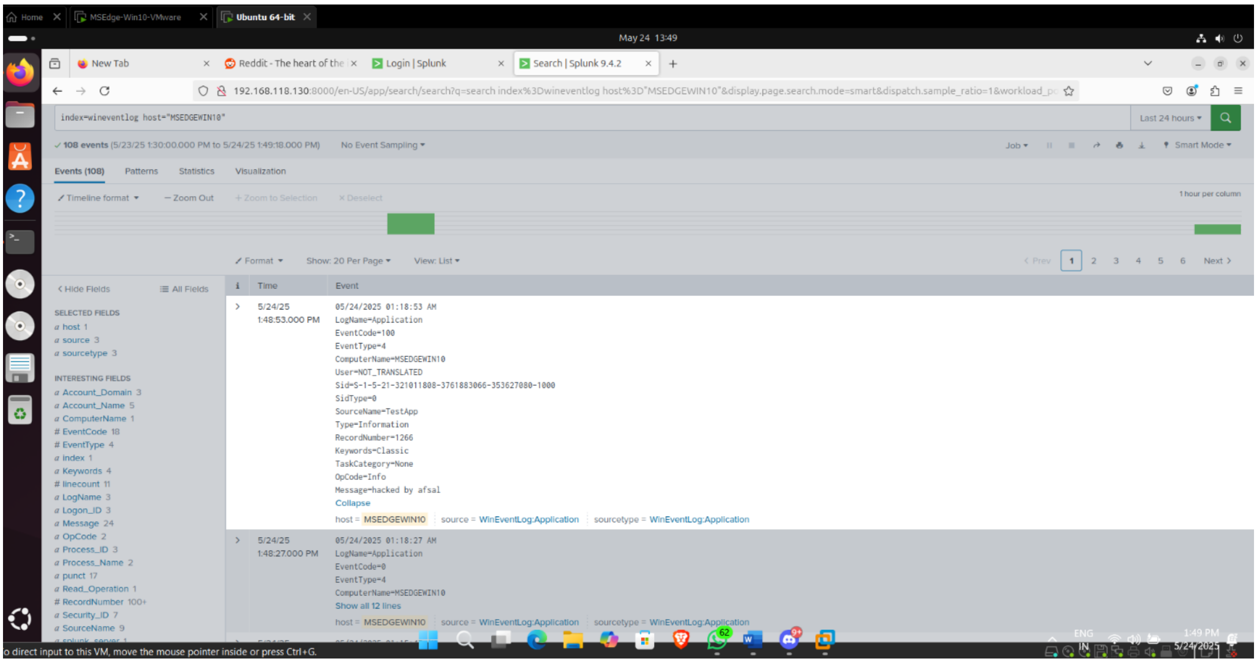
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
PS C:\Windows\system32> eventcreate /ID 100 /L APPLICATION /T INFORMATION /SO "TestApp" /D "hacked by afsal"

SUCCESS: An event of type 'INFORMATION' was created in the 'APPLICATION' log with 'TestApp' as the source.
PS C:\Windows\system32> _
```

Administrator: Windows PowerShell
Recycle Bin
Type here to search
Windows 10 Enterprise Evaluation
Windows License is expired
Build 17763.rs5_release.180914-1434

Created an event through windows powershell



```
index=wineventlog host="MSEDGEWIN10"
```

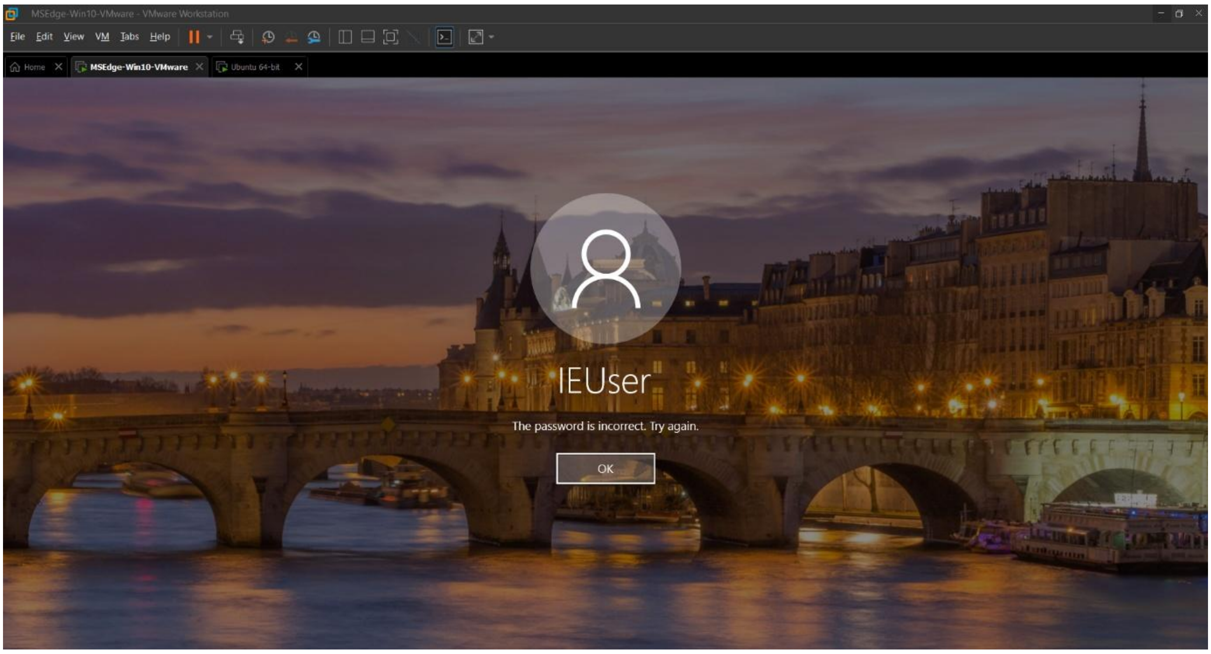
108 events (5/23/25 1:30:00.000 PM to 5/24/25 1:49:18.000 PM)

```
5/24/25              05/24/2025 01:18:53 AM
1:48:53.000 PM       LogName=Application
                     EventCode=100
                     EventType=4
                     ComputerName=MSEDGEWIN10
                     User=NOT_TRANSLATED
                     Sid=S-1-5-21-321011808-3761883066-353627080-1000
                     SidType=0
                     SourceName=TestApp
                     Type=Information
                     RecordNumber=1266
                     Keywords=Classic
                     TaskCategory=None
                     OpCode=Info
                     Message=hacked by afsal
                     Collapse
                     host = MSEDGEWIN10   source = WinEventLog:Application   sourcetype = WinEventLog:Application

5/24/25              05/24/2025 01:18:27 AM
1:48:27.000 PM       LogName=Application
                     EventCode=0
                     EventType=4
                     ComputerName=MSEDGEWIN10
                     Show all 12 lines
                     host = MSEDGEWIN10   source = WinEventLog:Application   sourcetype = WinEventLog:Application
```

Log generated in splunk dashboard

Entered incorrect password

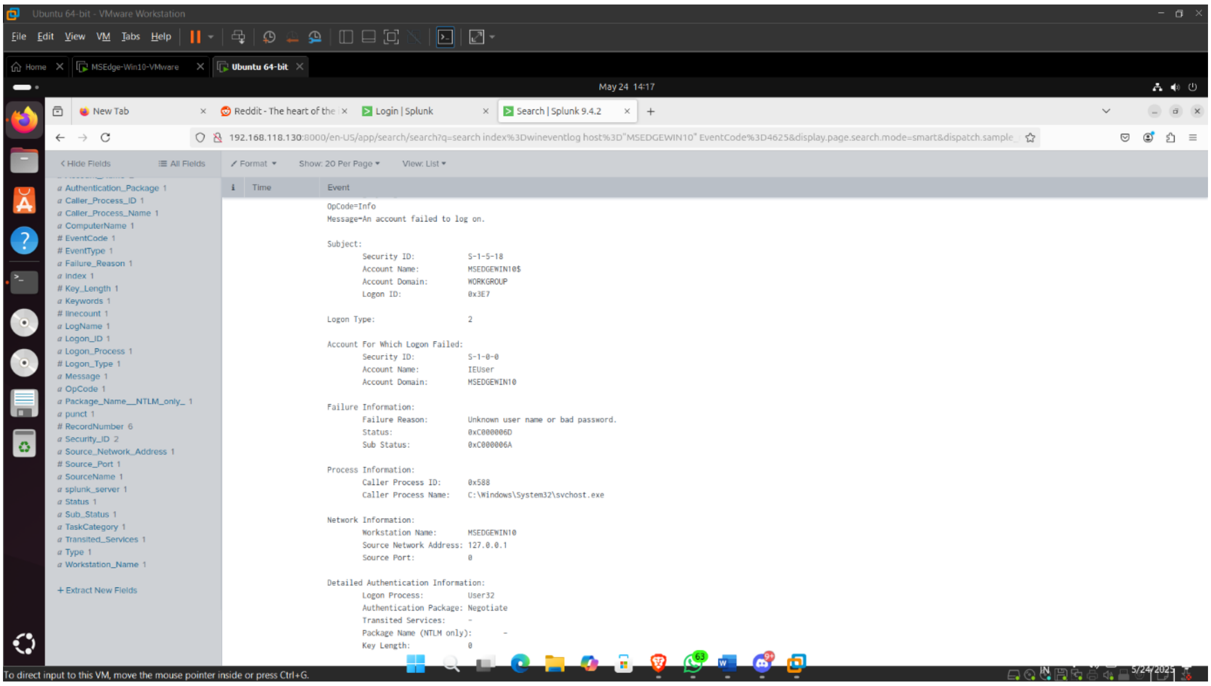

MSEdge-Win10-VMware - VMware Workstation
File Edit View VM Tabs Help
Home
MSEdge-Win10-VMware
Ubuntu 64-bit

IEUser

The password is incorrect. Try again.

OK

Log generated in splunk



192.168.118.130:8000/en-US/app/search/search?q=search index%3Dwineventlog host%3D"MSEDGEWIN10" EventCode%3D4625&display.page.search.mode=smart&dispatch.sample_

a Authentication_Package 1
a Caller_Process_ID 1
a Caller_Process_Name 1
a ComputerName 1
EventCode 1
EventType 1
a Failure_Reason 1
a index 1
Key_Length 1
a Keywords 1
# linecount 1
a LogName 1
a Logon_ID 1
a Logon_Process 1
Logon_Type 1
a Message 1
a OpCode 1
a Package_Name__NTLM_only_ 1
a punct 1
RecordNumber 6
a Security_ID 2
a Source_Network_Address 1
Source_Port 1
a SourceName 1
a splunk_server 1
a Status 1
a Sub_Status 1
a TaskCategory 1
a Transited_Services 1
a Type 1
a Workstation_Name 1

```
OpCode=Info
Message=An account failed to log on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           MSEDGEWIN10$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Type:                     2

Account For Which Logon Failed:
        Security ID:            S-1-0-0
        Account Name:           IEUser
        Account Domain:         MSEDGEWIN10

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A

Process Information:
        Caller Process ID:      0x588
        Caller Process Name:    C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:       MSEDGEWIN10
        Source Network Address: 127.0.0.1
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          User32
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
```

5. Conclusion

This project has successfully designed and implemented a Security Information and Event Management (SIEM) solution tailored to the specific needs of small businesses. The solution provides real-time monitoring and alerting capabilities, enabling prompt detection and response to security threats. It integrates seamlessly with existing infrastructure, leveraging current investments and minimizing additional costs. The solution's intuitive interface and customizable dashboards facilitate effective security monitoring and analysis. Regular review and updates are recommended to ensure the solution remains aligned with evolving security requirements and threats. Overall, the SIEM solution developed in this project provides a robust and effective security monitoring capability for small businesses, enhancing their security posture and enabling prompt response to security incidents

6. Further Development or Research

To further enhance the SIEM solution and address emerging security challenges, the following areas of development or research could be explored:

1. Machine Learning and Artificial Intelligence: Integrate machine learning and AI capabilities to improve threat detection and incident response.

2. Cloud Integration: Develop cloud-based SIEM solutions for greater scalability and flexibility.

3. Advanced Threat Intelligence: Incorporate advanced threat intelligence feeds to enhance threat detection and response.

4. Automation and Orchestration: Implement automation and orchestration capabilities to streamline incident response and improve efficiency.

5. User Behavior Analytics: Develop user behavior analytics capabilities to detect insider threats and anomalous activity

7. References

[1]. Splunk Documentation. Retrieved from https://docs.splunk.com/Documentation/Splunk

[2]. NIST Special Publication 800-137. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

[3].SentinelOne: Offers a comprehensive SIEM solution with advanced threat detection and response capabilities, designed for small businesses with limited IT resources.

[4].Logmanager: Provides a lightweight SIEM solution for small businesses, offering real-time threat detection, log management, and compliance reporting features.

[5].CrowdStrike: Offers a next-gen SIEM solution with advanced security analytics, threat detection, and response capabilities, tailored for small businesses with limited security expertise.

[6]. Comparitech: A review website that provides in-depth comparisons of various SIEM tools, including ManageEngine Log360, Datadog Security Monitoring, and Graylog.

8. Appendix

A. Additional Resources

- SIEM Solution Configuration Files: Sample configuration files for the SIEM solution, including settings for log collection, threat detection, and alerting.

- SIEM Solution Troubleshooting Guide: A comprehensive guide for troubleshooting common issues with the SIEM solution, including error messages and potential solutions.

B. Glossary of Terms

- SIEM: Security Information and Event Management

- Log Collection: The process of gathering and storing log data from various sources.

- Threat Detection: The process of identifying potential security threats based on log data and other security-related information.

- Alerting: The process of generating notifications when potential security threats are detected.

C. Detailed System Architecture

- System Components: A detailed list of the components that make up the SIEM solution, including hardware and software requirements.

- System Diagram: A diagram illustrating the architecture of the SIEM solution, including data flows and system interaction