Innovation Center for Education

PHEMESOFT
Software That Matters
TRUSTED DELIVERY PARTNER for IBM ICE

Yenepoya Institute of Arts, Science, Management & commerce

PROJECT SYNOPSIS

SIEM for Small Business

BACHELOR OF SCIENCE

COMPUTER SCIENCE

SUBMITTED BY

MUHAMMED AFSAL -22BSCFDC30

NIMIN RAJ -22BCACDC57

SHOVIN R.L -22BCACDC65

FELIX DAVID JOSEPH-22BCACDC22

TIBIN TIJO-22BCACDC68

GUIDED BY

SASHANK

Table of Contents

Introduction

This project focuses on building a lightweight Security Information and Event Management (SIEM) solution tailored for small business environments. The setup includes a Windows machine functioning as the business server and an Ubuntu machine acting as the SIEM server. Logs from the Windows server are collected and forwarded to the Ubuntu-based SIEM for centralized monitoring and analysis.

Technology Used

- SIEM Solution: Splunk

- Log Forwarder: Windows Universal Forwarder

- Operating Systems: Windows (business server) and Ubuntu (SIEM server)

Field of Project

This project falls under the field of Cybersecurity, specifically focusing on providing small businesses with a cost-effective solution for enhancing their cybersecurity posture through centralized log monitoring and analysis.

Special Technical Terms

- SIEM (Security Information and Event Management): A system that monitors and analyzes security-related data from various sources.

- Log Collection: Gathering logs from various systems and applications for analysis and monitoring.

- Event Correlation: Analyzing multiple events to identify potential security threats or incidents.

Project Goal

The goal of this project is to demonstrate the effectiveness of a lightweight SIEM solution in small business environments, providing a cost-effective way to enhance cybersecurity posture through log collection, event correlation, and basic threat detection using Splunk and Windows Universal Forwarder.

Methodology/Planning of Work

Project Development Steps

1. **Requirement Gathering**: Identify the requirements for the SIEM solution, including log collection, event correlation, and threat detection.

2. **System Design**: Design the architecture of the SIEM solution, including the Ubuntu-based SIEM server and Windows Universal Forwarder.

3. **Splunk Configuration:** Configure Splunk to collect, analyze, and visualize logs from the Windows server.

4. **Log Collection and Forwarding:** Set up the Windows Universal Forwarder to collect and forward logs to the Splunk server.

5. **Event Correlation and Threat Detection:** Configure Splunk to perform event correlation and basic threat detection.

6. **Testing and Validation**: Test and validate the SIEM solution to ensure it meets the requirements.

7. **Deployment and Maintenance**: Deploy the SIEM solution and plan for ongoing maintenance and updates.

Tools and Resources

- Splunk

- Windows Universal Forwarder

- Ubuntu-based SIEM server

- Windows server

Timeline

- Week 1-2: Requirement gathering and system design

- Week 3-4: Splunk configuration and log collection setup

- Week 5-6: Event correlation and threat detection configuration

- Week 7-8: Testing, validation, and deployment

Facilities Required for Proposed Work

Hardware Requirements

- Servers:
  - Ubuntu-based SIEM server
  - Windows server (for log generation and testing)
- Computing Resources:
  - Adequate CPU, RAM, and storage for Splunk and Windows Universal Forwarder

Software Requirements

- Splunk Enterprise: For log collection, analysis, and visualization
- Windows Universal Forwarder: For log forwarding from Windows server to Splunk
- Ubuntu Operating System: For the SIEM server
- Windows Operating System: For the Windows server

Additional Requirements

- Network Connectivity: Stable network connection for communication between servers
- Storage: Adequate storage for log data and Splunk indexes

References

Study Materials

The following study materials were referenced for the development of this SIEM solution:

1. Splunk Documentation: Official Splunk documentation for setup, configuration, and usage.

2. Windows Universal Forwarder Documentation: Microsoft documentation for Windows Universal Forwarder setup and configuration.

3. Ubuntu Documentation: Official Ubuntu documentation for server setup and configuration.

4. Cybersecurity Resources: Online resources and articles on cybersecurity, threat detection, and log analysis.

Online Resources

The following online resources were also utilized:

1. Splunk Community Forum: For community support and troubleshooting.

2. Stack Overflow: For Splunk and Windows-related questions and solutions.

3. Cybersecurity blogs and websites: For staying up-to-date with the latest cybersecurity trends and best practices.