SOC Task 1

Submitted by : Asna P K
Date : 26/12/2025

1. Introduction

This report documents the completion of assigned SOC Theoretical Knowledge and Practical Application tasks.

The objective of these tasks was to build a strong foundation in Security Operations Center (SOC) concepts, understand commonly used security tools and workflows, and gain hands-on experience with log analysis, monitoring, alerting, and documentation.

2. Theoretical Knowledge

The following sections were completed through structured study, tool familiarization, and workflow understanding.

2.1 SOC Fundamentals and Operations

Purpose of a SOC

- A Security Operations Center (SOC) is responsible for proactive threat detection, incident response, and continuous monitoring of organizational systems and networks.
- SOC alerts and detections were linked to MITRE ATT&CK techniques to understand how attackers behave and carry out attacks.

SOC Roles

- Tier 1 Analyst: Initial alert monitoring and triage
- Tier 2 Analyst: In-depth investigation and correlation
- Tier 3 Analyst: Advanced threat hunting and incident handling
- SOC Manager: Oversight, reporting, and coordination
- Threat Hunter: Proactive search for hidden threats

Key SOC Functions

- Log analysis
- Alert triage
- Threat intelligence integration

Learning Outcome

- Understood SOC workflows and alert-to-response lifecycle.
- Gained conceptual understanding of SOAR and playbooks using Splunk Phantom.

2.2 Security Monitoring Basics

Objectives

- Detect anomalies
- Identify unauthorized access
- Detect policy violations

Monitoring Tools

- SIEM tools (Splunk, Elastic)
- Network traffic analyzers (Wireshark)

Key Metrics

- False positives and false negatives
- Mean Time To Detect (MTTD)

Learning Outcome

- Understood how SIEM platforms correlate logs and generate alerts.
- Studied attack detection using sample datasets.

2.3 Log Management Fundamentals

Log Lifecycle

- Collection
- Normalization
- Storage
- Retention
- Analysis

Common Log Types

- Windows Event Logs
- Syslog
- HTTP server logs

Learning Outcome

- Learned how Fluentd and Logstash are used for log collection and normalization.
- Understood querying techniques using SQL-like syntax (KQL/SPL).

2.4 Security Tools Overview

Tools Studied

- SIEM: Splunk, QRadar
- EDR: CrowdStrike
- IDS/IPS: Snort
- Vulnerability Scanners: Nessus

Learning Outcome

- Understood the role of each tool within a SOC environment.
- Learned where detection, prevention, and response tools fit in the security architecture.

2.5 Basic Security Concepts

Concepts Covered

- CIA Triad (Confidentiality, Integrity, Availability)
- Threat vs Vulnerability vs Risk
- Defense-in-Depth
- Zero Trust

Learning Outcome

- Gained clarity on core security principles and their real-world relevance.
- Studied real-world breach examples for context.

2.6 Security Operations Workflow

Stages

1. Detection
2. Triage
3. Investigation
4. Response

Learning Outcome

- Understood end-to-end SOC workflow.
- Designed a flowchart for phishing incident handling.

2.7 Incident Response Basics

Incident Response Lifecycle

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Learning Outcome

- Studied NIST SP 800-61 framework.
- Performed tabletop simulation exercises conceptually.

2.8 Documentation Standards

Documents Studied

- Incident reports
- SOPs
- Runbooks
- Post-incident reviews

Learning Outcome

- Practiced writing structured security documentation using standard templates.

3. Practical Application

The following tasks were completed hands-on with evidence and outputs.

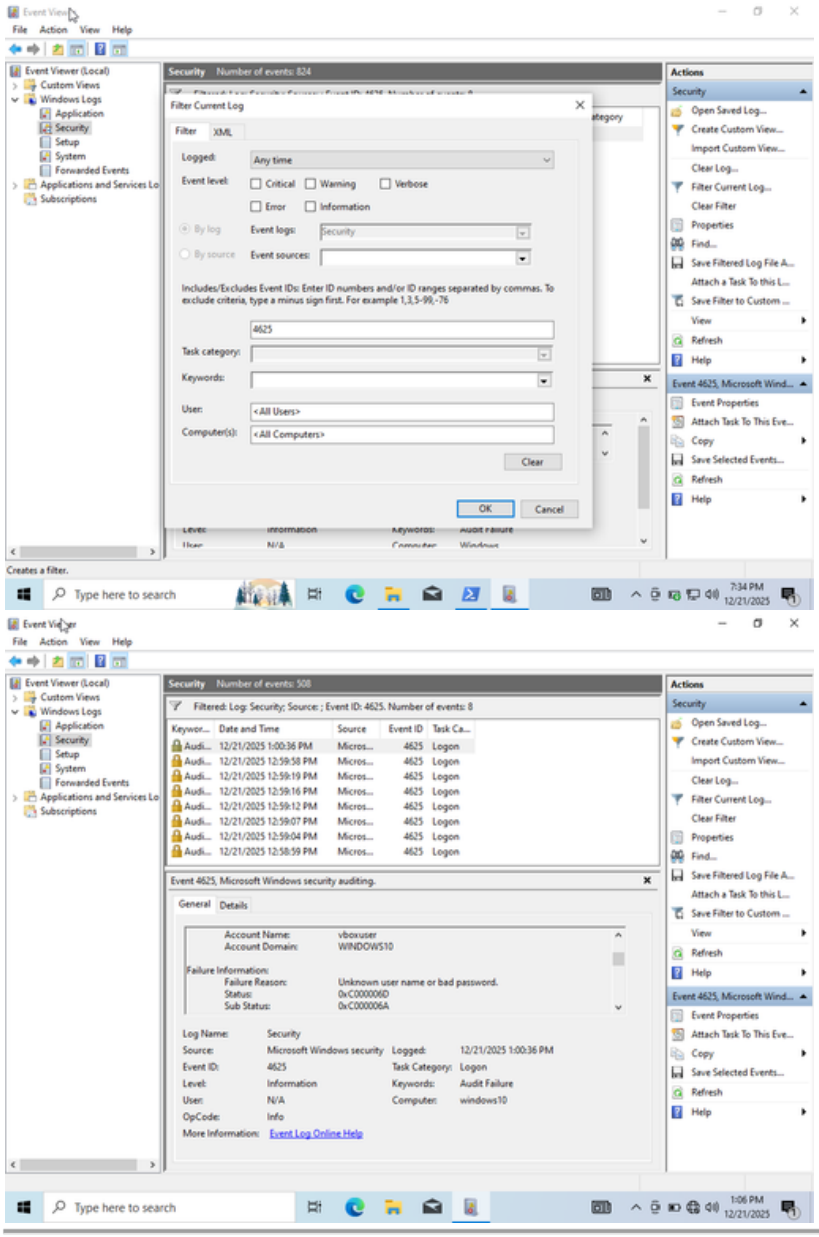
3.1 Log Analysis Practice

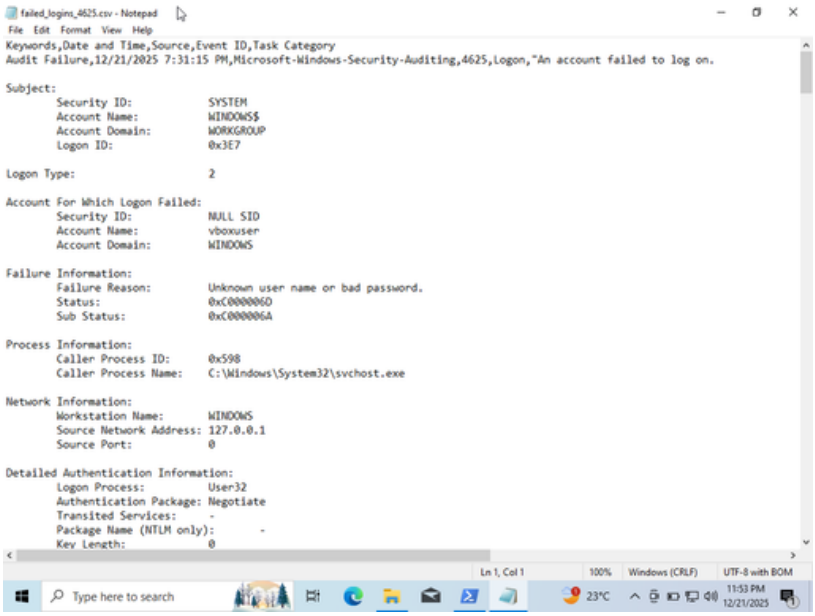
Activities Performed

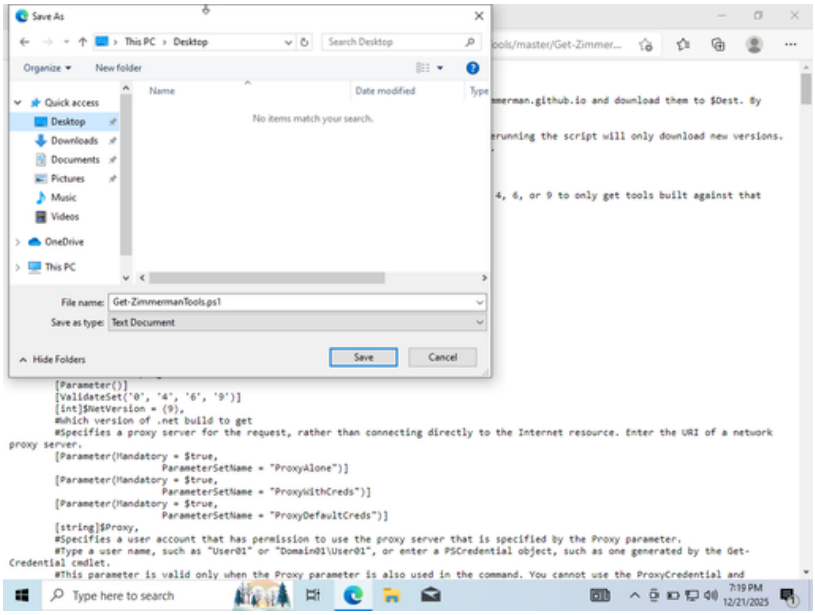
- Filtered Windows Event Logs for:
  - Event ID 4625 (Failed Logins)
- Identified potential brute-force attempts.
- Exported results to CSV.
- Used Eric Zimmerman's LECmd tool to analyze browser history for suspicious URLs.

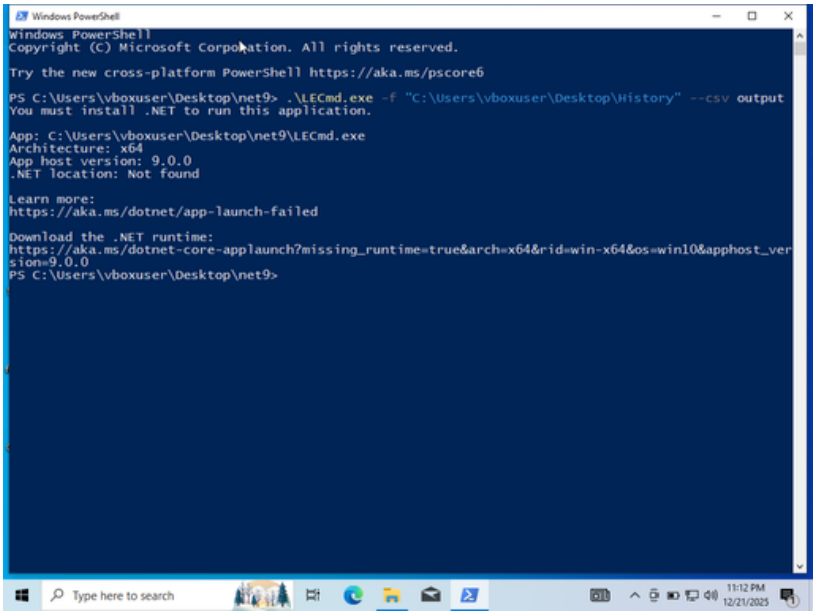
Outcome

- Successfully identified suspicious login behavior.




failed_logins_4625.csv - Notepad
File Edit Format View Help
Keywords,Date and Time,Source,Event ID,Task Category
Audit Failure,12/21/2025 7:31:15 PM,Microsoft-Windows-Security-Auditing,4625,Logon,"An account failed to log on.
Subject:
Security ID: SYSTEM
Account Name: WINDOWS$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Logon Type: 2
Account For Which Logon Failed:
Security ID: NULL SID
Account Name: vboxuser
Account Domain: WINDOWS
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A
Process Information:
Caller Process ID: 0x598
Caller Process Name: C:\Windows\System32\svchost.exe
Network Information:
Workstation Name: WINDOWS
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
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8 with BOM
Type here to search
23°C
11:53 PM
12/21/2025


Save As
This PC > Desktop
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Name
Date modified
Type
No items match your search.
File name: Get-ZimmermanTools.ps1
Save as type: Text Document
Hide Folders
Save
Cancel
[Parameter()]
[ValidateSet('0', '4', '6', '9')]
[int]$NetVersion = (9),
#Which version of .net build to get
#Specifies a proxy server for the request, rather than connecting directly to the Internet resource. Enter the URI of a network proxy server.
[Parameter(Mandatory = $true,
ParameterSetName = "ProxyAlone")]
[Parameter(Mandatory = $true,
ParameterSetName = "ProxyWithCreds")]
[Parameter(Mandatory = $true,
ParameterSetName = "ProxyDefaultCreds")]
[string]$Proxy,
#Specifies a user account that has permission to use the proxy server that is specified by the Proxy parameter.
#Type a user name, such as "User01" or "Domain01\User01", or enter a PSCredential object, such as one generated by the Get-Credential cmdlet.
#This parameter is valid only when the Proxy parameter is also used in the command. You cannot use the ProxyCredential and
Type here to search
7:19 PM
12/21/2025


Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\vboxuser\Desktop\net9> .\LECmd.exe -f "C:\Users\vboxuser\Desktop\History" --csv output
You must install .NET to run this application.
App: C:\Users\vboxuser\Desktop\net9\LECmd.exe
Architecture: x64
App host version: 9.0.0
.NET location: Not found
Learn more:
https://aka.ms/dotnet/app-launch-failed
Download the .NET runtime:
https://aka.ms/dotnet-core-applaunch?missing_runtime=true&arch=x64&rid=win-x64&os=win10&apphost_version=9.0.0
PS C:\Users\vboxuser\Desktop\net9>
Type here to search
11:12 PM
12/21/2025

3.2 Document Security Events

Task:

- Created a security event documentation template with:
  - Date/Time
  - Source IP
  - Event ID
  - Description
  - Action Taken

Event Documentation Template

Date/Time	Source IP	Event ID	Description	Action Taken
21-12-2025 07:30:39 pm	127.0.0.1	4625	Multiple failed login attempts detected indicating possible brute-force activity	Activity monitored and no successful unauthorized access observed

- Multiple failed login attempts were detected on a Windows system using Event ID 4625. This activity may indicate incorrect credential usage or a possible brute-force attempt.

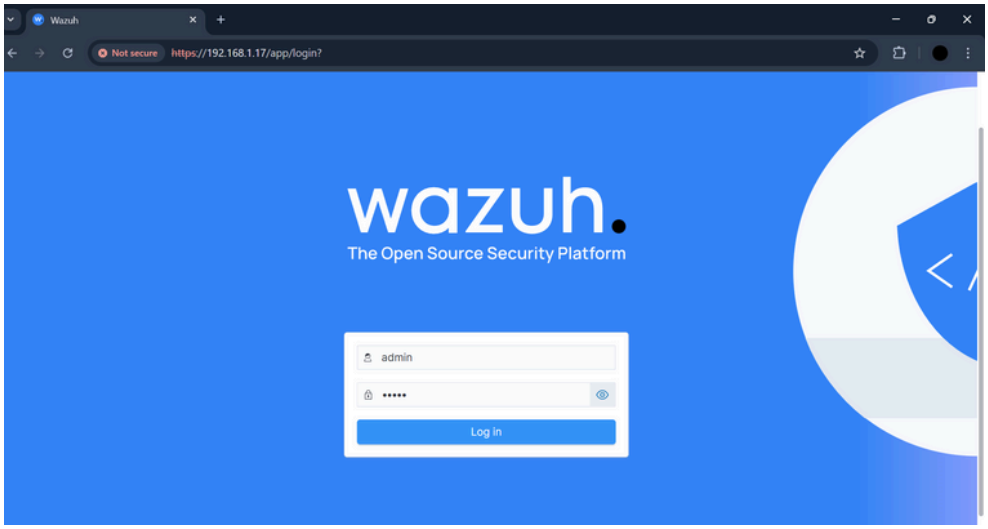
3.3 Set Up Monitoring Dashboards (Using Wazuh)

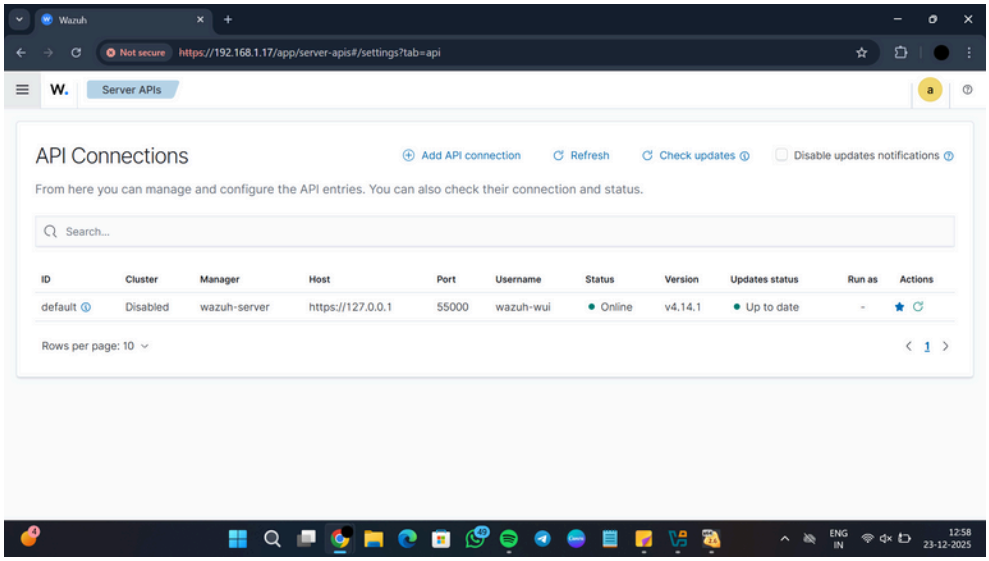
Activities Performed

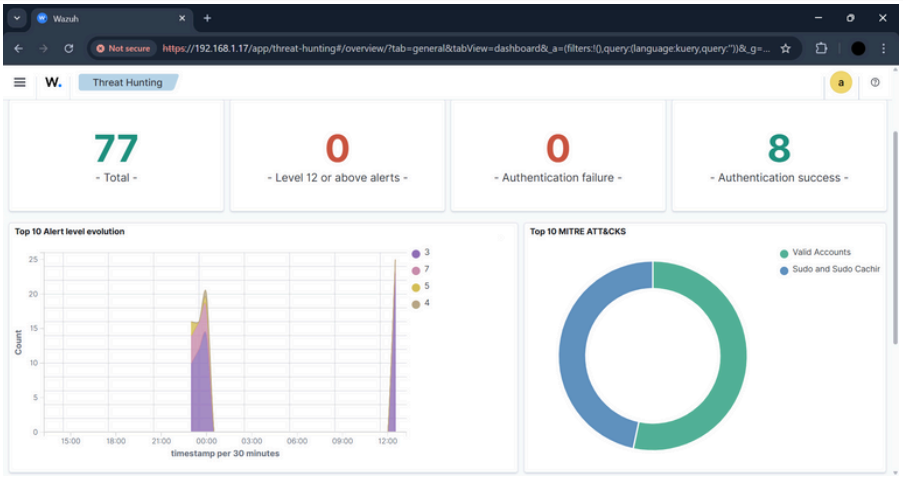
- Used the Wazuh Dashboard to monitor security events.
- Created and reviewed visualizations for:
  - Top source IP addresses generating alerts
  - Frequency of critical security event IDs
- Analyzed alert trends and severity levels to understand SOC visibility.

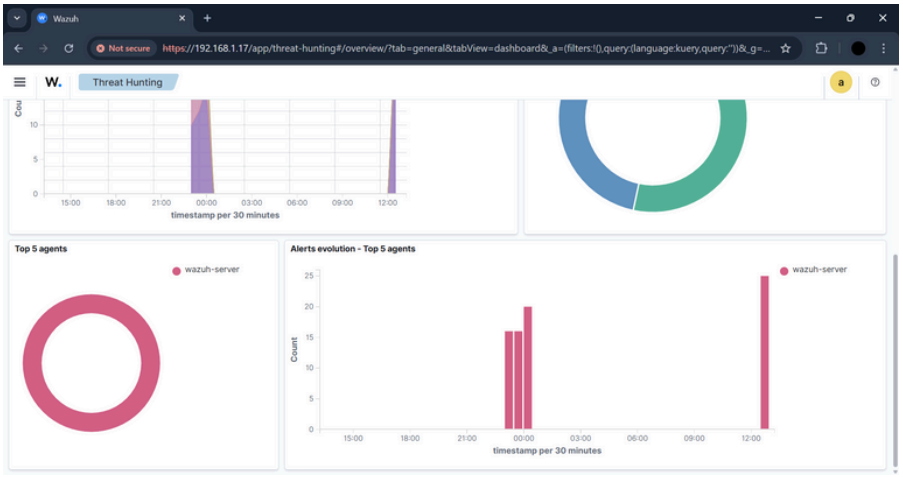
Outcome

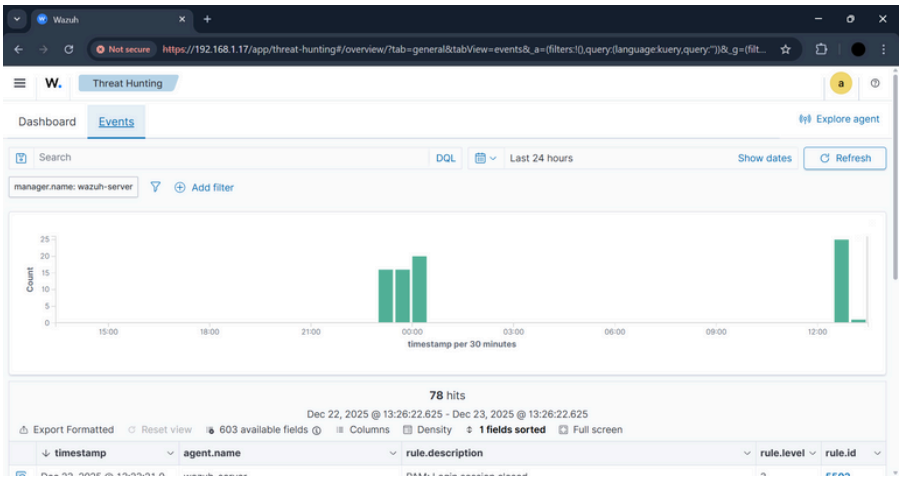
- Gained hands-on experience with dashboard-based security monitoring.
- Understood how Wazuh dashboards help SOC analysts quickly identify suspicious activity and prioritize alerts.

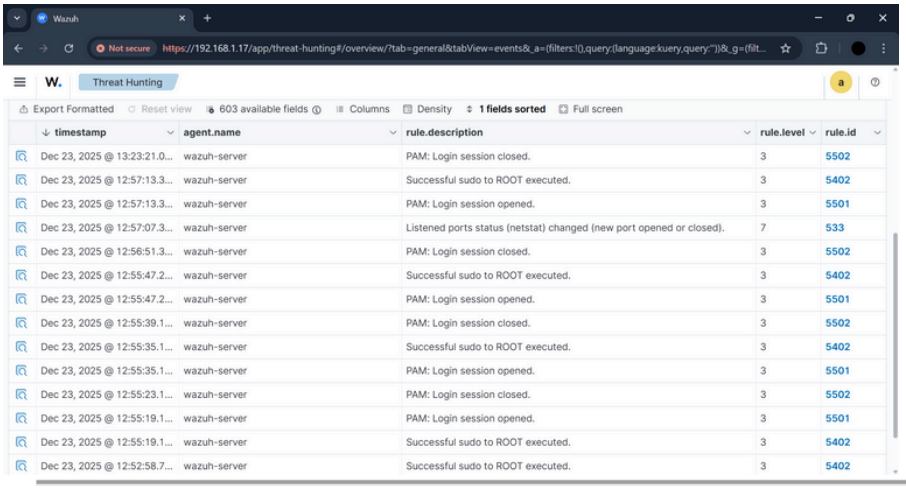





Wazuh
Not secure
https://192.168.1.17/app/threat-hunting#/overview/?tab=general&tabView=dashboard&_a=(filters:!(),query:(language:kuery,query:''))&_g=...
Threat Hunting
77
- Total -
0
- Level 12 or above alerts -
0
- Authentication failure -
8
- Authentication success -
Top 10 Alert level evolution
Count
timestamp per 30 minutes
Top 10 MITRE ATT&CKS
Valid Accounts
Sudo and Sudo Cachir


Wazuh
Not secure
https://192.168.1.17/app/threat-hunting#/overview/?tab=general&tabView=dashboard&_a=(filters:!(),query:(language:kuery,query:''))&_g=...
Threat Hunting
timestamp per 30 minutes
Top 5 agents
wazuh-server
Alerts evolution - Top 5 agents
wazuh-server
Count
timestamp per 30 minutes


Wazuh
Not secure
https://192.168.1.17/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filt...
Threat Hunting
Dashboard
Events
Explore agent
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
Add filter
Count
timestamp per 30 minutes
78 hits
Dec 22, 2025 @ 13:26:22.625 - Dec 23, 2025 @ 13:26:22.625
Export Formatted
Reset view
603 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id


Wazuh
Not secure
https://192.168.1.17/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filt...
Threat Hunting
Export Formatted
Reset view
603 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id
Dec 23, 2025 @ 13:23:21.0... wazuh-server PAM: Login session closed. 3 5502
Dec 23, 2025 @ 12:57:13.3... wazuh-server Successful sudo to ROOT executed. 3 5402
Dec 23, 2025 @ 12:57:13.3... wazuh-server PAM: Login session opened. 3 5501
Dec 23, 2025 @ 12:57:07.3... wazuh-server Listened ports status (netstat) changed (new port opened or closed). 7 533
Dec 23, 2025 @ 12:56:51.3... wazuh-server PAM: Login session closed. 3 5502
Dec 23, 2025 @ 12:55:47.2... wazuh-server Successful sudo to ROOT executed. 3 5402
Dec 23, 2025 @ 12:55:47.2... wazuh-server PAM: Login session opened. 3 5501
Dec 23, 2025 @ 12:55:39.1... wazuh-server PAM: Login session closed. 3 5502
Dec 23, 2025 @ 12:55:35.1... wazuh-server Successful sudo to ROOT executed. 3 5402
Dec 23, 2025 @ 12:55:35.1... wazuh-server PAM: Login session opened. 3 5501
Dec 23, 2025 @ 12:55:23.1... wazuh-server PAM: Login session closed. 3 5502
Dec 23, 2025 @ 12:55:19.1... wazuh-server PAM: Login session opened. 3 5501
Dec 23, 2025 @ 12:55:19.1... wazuh-server Successful sudo to ROOT executed. 3 5402
Dec 23, 2025 @ 12:52:58.7... wazuh-server Successful sudo to ROOT executed. 3 5402

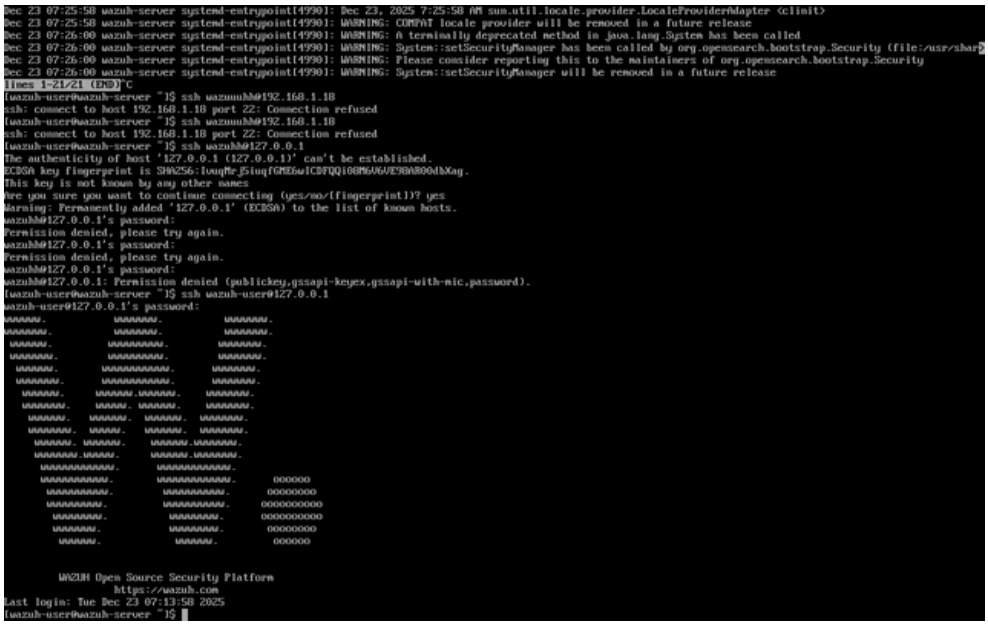
3.4 Configure Alert Rules (Using Wazuh)

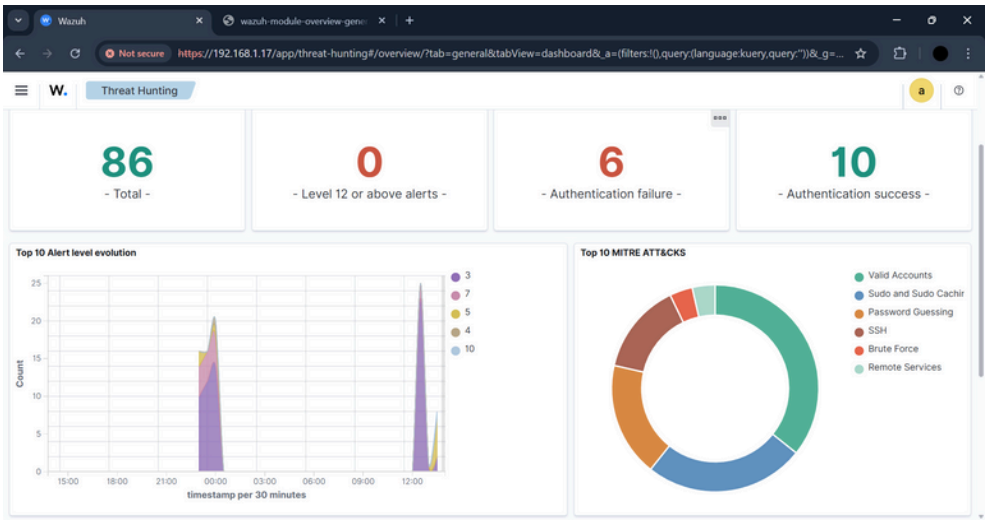
Activities Performed

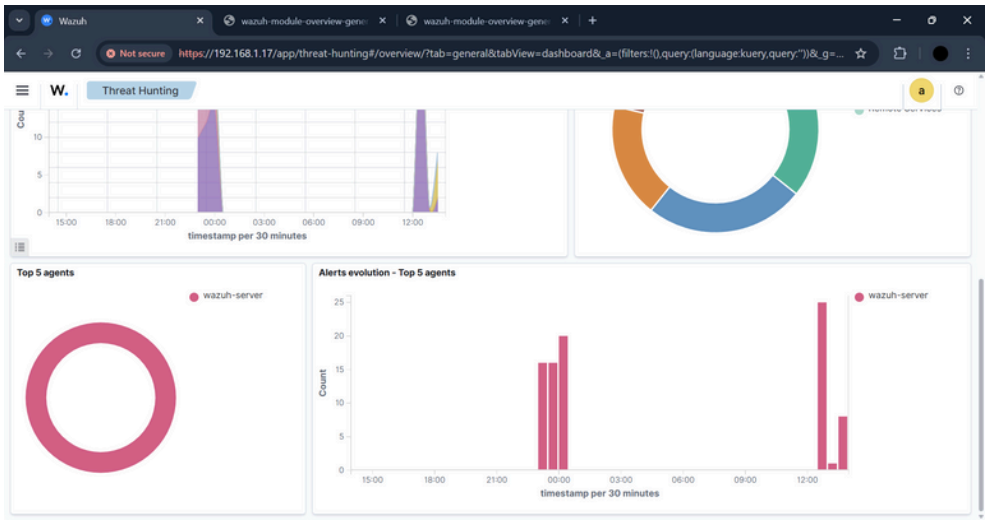
- Configured alert rules in Wazuh SIEM to detect multiple failed login attempts.
- Simulated failed authentication attempts to trigger alerts.
- Verified alert generation in the Wazuh dashboard.
- Reviewed alert details such as rule ID, severity level, and source information.

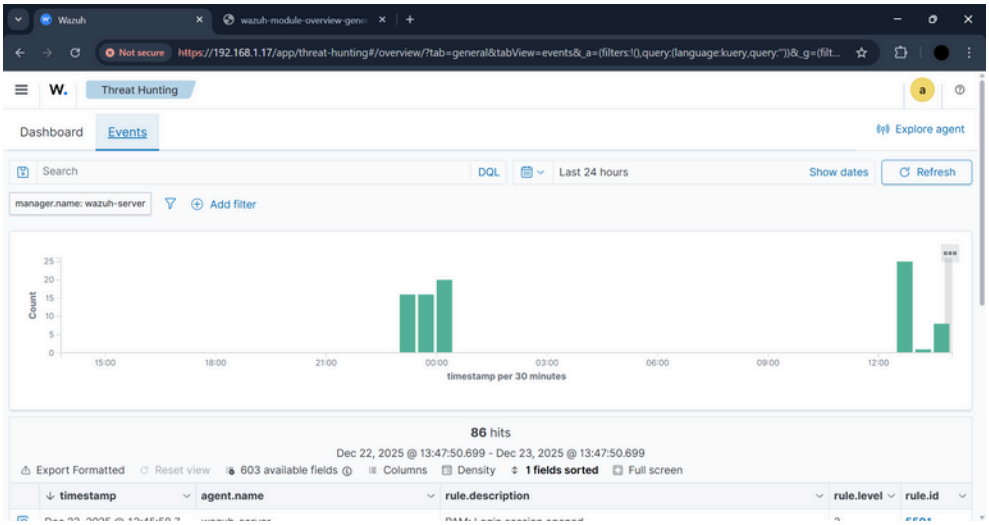
Outcome

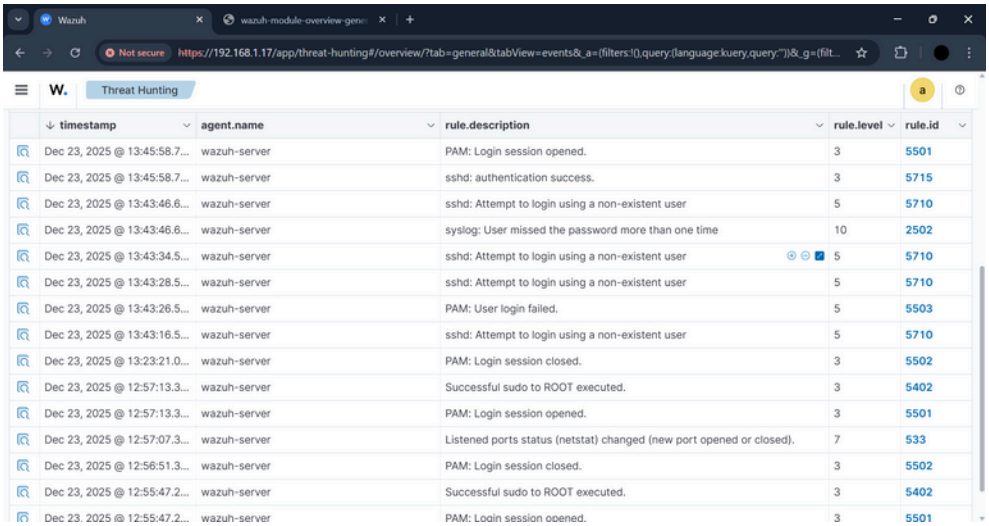
- Successfully validated alert logic and detection accuracy.
- Understood how SIEM alert rules support real-time detection and incident response.






Wazuh
Not secure
https://192.168.1.17/app/threat-hunting#/overview/?tab=general&tabView=dashboard&_a=(filters:!(),query:(language:kuery,query:''))&_g=...
Threat Hunting
timestamp per 30 minutes
Top 5 agents
wazuh-server
Alerts evolution - Top 5 agents
wazuh-server
Count
timestamp per 30 minutes


Wazuh
Not secure
https://192.168.1.17/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filt...
Threat Hunting
Dashboard
Events
Explore agent
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
Add filter
Count
timestamp per 30 minutes
86 hits
Dec 22, 2025 @ 13:47:50.699 - Dec 23, 2025 @ 13:47:50.699
Export Formatted
Reset view
603 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id


Wazuh
Not secure
https://192.168.1.17/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filt...
Threat Hunting
timestamp
agent.name
rule.description
rule.level
rule.id
Dec 23, 2025 @ 13:45:58.7... wazuh-server PAM: Login session opened. 3 5501
Dec 23, 2025 @ 13:45:58.7... wazuh-server sshd: authentication success. 3 5715
Dec 23, 2025 @ 13:43:46.6... wazuh-server sshd: Attempt to login using a non-existent user 5 5710
Dec 23, 2025 @ 13:43:46.6... wazuh-server syslog: User missed the password more than one time 10 2502
Dec 23, 2025 @ 13:43:34.5... wazuh-server sshd: Attempt to login using a non-existent user 5 5710
Dec 23, 2025 @ 13:43:28.5... wazuh-server sshd: Attempt to login using a non-existent user 5 5710
Dec 23, 2025 @ 13:43:26.5... wazuh-server PAM: User login failed. 5 5503
Dec 23, 2025 @ 13:43:16.5... wazuh-server sshd: Attempt to login using a non-existent user 5 5710
Dec 23, 2025 @ 13:23:21.0... wazuh-server PAM: Login session closed. 3 5502
Dec 23, 2025 @ 12:57:13.3... wazuh-server Successful sudo to ROOT executed. 3 5402
Dec 23, 2025 @ 12:57:13.3... wazuh-server PAM: Login session opened. 3 5501
Dec 23, 2025 @ 12:57:07.3... wazuh-server Listened ports status (netstat) changed (new port opened or closed). 7 533
Dec 23, 2025 @ 12:56:51.3... wazuh-server PAM: Login session closed. 3 5502
Dec 23, 2025 @ 12:55:47.2... wazuh-server Successful sudo to ROOT executed. 3 5402
Dec 23, 2025 @ 12:55:47.2... wazuh-server PAM: Login session opened. 3 5501

4.Key Learnings

- Gained a clear understanding of SOC roles, responsibilities, and workflows, including alert detection, triage, investigation, and response.
- Learned how SIEM platforms collect, correlate, and analyze security logs to detect suspicious activity.
- Developed hands-on experience in log analysis by investigating Windows Event IDs such as 4625 (failed login) and identifying potential brute-force attempts.
- Understood the importance of accurate security event documentation and practiced recording incidents using a structured template.
- Acquired practical exposure to monitoring dashboards using Wazuh, enabling quick visibility into alert trends, source IPs, and event severity.
- Learned how to configure and validate alert rules in a SIEM by simulating failed login attempts and confirming alert generation.
- Osquery was studied conceptually as part of endpoint visibility in a SOC, though hands-on execution was not performed in this task.
- Gained awareness of tool dependencies and environmental limitations, such as .NET runtime compatibility issues encountered while using LECmd.
- Improved understanding of incident response processes and the significance of timely detection and proper escalation in a SOC environment.
- Learned how theoretical security concepts (CIA triad, threat vs risk, defense-in-depth) connect to real-world SOC operations.

5.Conclusion

This task provided a strong foundation in Security Operations Center (SOC) concepts and practices. Through a combination of theoretical learning and hands-on practical activities, I gained valuable insight into how security events are monitored, analyzed, documented, and responded to in a SOC environment.

The practical tasks, particularly log analysis, dashboard monitoring, and alert configuration using Wazuh SIEM, helped translate theoretical knowledge into real-world application. Challenges encountered during tool execution were documented and used as learning opportunities to better understand system dependencies and troubleshooting in security operations.

Overall, this experience enhanced my analytical skills, improved my familiarity with industry-standard security tools, and strengthened my understanding of SOC workflows, preparing me for further hands-on roles in cybersecurity and security operations.