A Major Project Report On

"Attack, Detect and Secure a Cloud-Based Enterprise Infrastructure Using Azure and SIEM"

Submitted to
CHHATTISGARH SWAMI VIVEKANAND TECHNICAL UNIVERSITY, BHILAI

In partial fulfillment of the requirement for the award of degree of

Bachelor of Technology
in
Computer Science & Engineering (Data Science)
5th Semester

Submitted By

Mohammad Kaif
CSVTU Roll No.: 301311023071
Enrollment No.: 6604750

Under the Guidance of Mr. ANSHUL KAUNDAL

ETHICAL HACKING Technical Trainer

RUNGTA EDUCATIONAL FOUNDATION
BHILAI-CHHATTISGARH

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Rungta College of Engineering & Technology
Kohka–Kurud Road, Bhilai (C.G.), India

Session: 2025–2026

DECLARATION

I, the undersigned, solemnly declare that this report on the project entitled
"Attack, Detect and Secure a Cloud-Based Enterprise Infrastructure Using Azure and SIEM"
is based on my own work carried out during the course of my study under the guidance of
Mr. ANSHUL KAUNDAL

I assert that the statements made and conclusions drawn are an outcome of the project work. I further declare that to the best of my knowledge and belief, the report does not contain any part of any work which has been submitted for the award of any other degree or diploma in this University or any other University.

Signature: _____
Name: Mohammad Kaif
CSVTU Roll No.: 301311023071
Enrollment No.: 6604750

CERTIFICATE

This is to certify that the project entitled
"Attack, Detect and Secure a Cloud-Based Enterprise Infrastructure Using Azure and SIEM"
submitted by **Mohammad Kaif** is a bonafide work carried out under my guidance and supervision for the award of Bachelor of Technology in Computer Science & Engineering of Chhattisgarh Swami Vivekanand Technical University, Bhilai.

To the best of my knowledge, the report:

1. Embodies the work of the student
2. Has been completed satisfactorily
3. Fulfills the academic requirements of the University
4. Is up to the desired standard

Guide's Signature
Name & Designation

This project work as mentioned above is hereby being recommended and forwarded for examination and evaluation by the University,

Signature

Dr. AJAY KUSHWAHA
Head,
Department of Computer Science and Engineering,
Rungta College of Engineering & Technology,
Kohka - Kurud Road, Bhilai(C.G.), India

ACKNOWLEDGEMENT

It is a matter of profound privilege and pleasure to extend my sense of respect and deepest gratitude to my project guide _____ , Department of Computer Science and Engineering under whose precise guidance and gracious encouragement I had the privilege to work.

Iavail this opportunity to thank respected **Dr. Ajay Kushwaha**, Head of the Department of Computer Science and Engineering for facilitating such a pleasant environment in the department and also for providing everlasting encouragement and support throughout.

I acknowledge with the deep sense of responsibility and gratitude the help rendered by respected Dr. Manish Manoria, Director General, Rungta Educational Foundation, Bhilai, Dr. Y. M. Gupta, Director(Academics), and Dr. Chinmay Chandrakar, Dean(Academics), of Rungta College of Engineering and Technology, Bhilai for infusing endless enthusiasm & instilling a spirit of dynamism.

I would also like to thank all faculty members of my department, and the supporting staff for always being helpful over the years.

Last but not the least, I would like to express my deepest gratitude to my parents and the management of Rungta College of Engineering and Technology, Bhilai, respected Shri Santosh Ji Rungta, Chairman, respected Dr. Sourabh Rungta, Vice Chairman, and respected Shri Sonal Rungta, Secretary, of Rungta Educational Foundation, Bhilai for their continuous moral support and encouragement.

I hope that I will make everybody proud of my achievements..

Mohammad Kaif

C E R T I F I C A T E B Y T H E E X A M I N E R S

This is to certify that this project work entitled "_____

_____", submitted by…

Mohammad Kaif,

CSVTU Roll No. : 301311023071,

Enrollment No. : 6604750

is duly examined by the undersigned as a part of the examination for the award of Bachelor of Technology degree in Rungta College of Engineering and Technology of Chhattisgarh Swami Vivekanand Technical University, Bhilai.

Internal Examiner **External Examiner**

Name & Signature **Name & Signature**

Date: **Date:**

TABLE OF CONTENTS

ABSTRACT

With the rapid adoption of cloud computing, organizations face increasing cybersecurity threats targeting misconfigured and vulnerable cloud infrastructures. This project focuses on designing, attacking, monitoring, and securing a simulated enterprise environment deployed on Microsoft Azure.

The project is divided into two phases. In the first phase, a vulnerable cloud infrastructure consisting of internal servers, a web server, and a SIEM system is deployed. Ethical hacking techniques such as network scanning, brute-force attacks, web-based attacks, and privilege escalation attempts are simulated to generate real-world security events.

In the second phase, security events are analyzed using the Wazuh SIEM platform. Identified vulnerabilities and misconfigurations are mitigated through systematic hardening techniques, including firewall configuration, SSH hardening, access control enforcement, and enhanced logging. The effectiveness of the applied security measures is validated through re-attack simulations.

This project provides hands-on experience in ethical hacking, security monitoring, incident response, and cloud security hardening aligned with industry practices.

LIST OF ABBREVIATIONS

Abbreviation	Description
SIEM	Security Information and Event Management
VM	Virtual Machine
NSG	Network Security Group
SSH	Secure Shell
DMZ	Demilitarized Zone
IDS	Intrusion Detection System

CHAPTER 1: INTRODUCTION

Cloud computing has transformed how organizations deploy and manage IT infrastructure. However, improper configuration and lack of security controls can expose cloud environments to severe cyber threats.

This project demonstrates a complete security lifecycle by simulating attacks on a cloud-based infrastructure, detecting malicious activities using SIEM tools, and applying appropriate security hardening measures.

CHAPTER 2: LITERATURE REVIEW

The literature review provides an overview of existing research, technologies, and methodologies related to cloud security, ethical hacking, and Security Information and Event Management (SIEM) systems. This chapter establishes the theoretical foundation for the project by examining prior work in these domains and identifying how the present project aligns with and extends existing approaches.

2.1 Cloud Computing and Security Challenges

Cloud computing has become the backbone of modern IT infrastructure due to its scalability, flexibility, and cost efficiency. According to multiple studies, platforms such as Microsoft Azure enable organizations to deploy resources rapidly without the need for extensive on-premise infrastructure. However, literature also highlights that improper configuration of cloud resources is one of the leading causes of security breaches.

Researchers emphasize that cloud environments introduce shared responsibility models, where cloud providers secure the underlying infrastructure, while customers are responsible for securing operating systems, applications, and access controls. Misunderstanding this responsibility often results in exposed services, weak authentication mechanisms, and insufficient monitoring, making cloud deployments attractive targets for attackers.

2.2 Ethical Hacking as a Security Assessment Technique

Ethical hacking is widely recognized as an effective approach for identifying vulnerabilities before they can be exploited by malicious attackers. Several studies describe ethical hacking as a proactive security assessment method that involves controlled attacks on systems to evaluate their resilience against real-world threats.

Literature shows that common attack techniques such as network scanning, brute-force authentication attacks, web application exploitation, and privilege escalation are frequently used during penetration testing exercises. These techniques help security teams understand attacker behavior and uncover weaknesses in system configuration, network design, and application logic. The use of ethical hacking in academic and enterprise environments has proven to significantly improve security awareness and preparedness.

2.3 Network Security and Web Application Attacks

Numerous research papers focus on network-based attacks such as port scanning and service enumeration as the initial stage of cyber-attacks. Tools like Nmap are extensively discussed in literature for their ability to identify open ports, services, and operating system fingerprints. Such reconnaissance techniques are often followed by targeted exploitation.

Web application security has also been a major focus area in cybersecurity research. The OWASP Top 10 list identifies SQL injection and directory traversal as some of the most critical web vulnerabilities. Studies highlight that poorly validated user inputs and improper server configurations allow attackers to manipulate database queries or access restricted system files. These findings reinforce the importance of securing web servers deployed in publicly accessible zones such as DMZs.

2.4 Security Information and Event Management (SIEM) Systems

SIEM systems play a crucial role in modern cybersecurity by providing centralized log collection, correlation, and real-time alerting. Literature describes SIEM platforms as essential tools for Security Operations Centers (SOCs), enabling organizations to detect, analyze, and respond to security incidents efficiently.

Open-source SIEM solutions such as **Wazuh** have gained popularity due to their flexibility, cost effectiveness, and strong community support. Research highlights Wazuh's capabilities in log analysis, intrusion detection, file integrity monitoring, and compliance reporting. Several studies demonstrate that integrating SIEM systems with cloud environments significantly enhances visibility into security events and improves incident response capabilities.

2.5 Importance of Security Hardening and Continuous Monitoring

Security hardening is frequently emphasized in literature as a necessary step after vulnerability identification. Studies show that implementing measures such as firewall rules, secure authentication mechanisms, least privilege access, and enhanced logging drastically reduces the attack surface of systems.

Researchers also stress that security is not a one-time process but an ongoing cycle involving monitoring, detection, response, and improvement. Continuous monitoring through SIEM systems enables organizations to adapt to evolving threats and maintain a strong security posture over time. Re-attack validation, where previously successful attacks are attempted again after hardening, is identified as an effective method to measure the success of applied security controls.

2.6 Summary of Literature Review

The reviewed literature clearly establishes that cloud environments require proactive security assessment, continuous monitoring, and systematic hardening to remain secure. Ethical hacking provides practical insight into system vulnerabilities, while SIEM platforms enable effective detection and analysis of security events. The findings from existing research strongly support the methodology adopted in this project, which integrates ethical hacking, SIEM-based monitoring, and security hardening to enhance cloud infrastructure security.

.

CHAPTER 3: PROBLEM IDENTIFICATION

With the increasing adoption of cloud computing platforms, organizations are rapidly migrating critical applications and data to cloud environments. While cloud platforms provide scalability and flexibility, they also introduce new security challenges, especially when systems are deployed without proper security controls and monitoring mechanisms.

One of the primary problems identified in cloud-based infrastructures is **misconfiguration**. Improperly configured network services, open ports, and weak access control policies often expose systems to unauthorized access. In many cases, default configurations are used without considering security implications, making systems vulnerable to basic reconnaissance and exploitation techniques.

Another significant issue is the presence of **weak authentication mechanisms**. Password-based authentication without proper restrictions allows attackers to perform brute-force and password-guessing attacks. The absence of strong authentication policies, such as key-based access and login attempt limitations, increases the risk of unauthorized system access.

The lack of **centralized monitoring and logging** further complicates security management. Without a Security Information and Event Management (SIEM) system, organizations struggle to detect suspicious activities in real time. Distributed logs across multiple systems make it difficult to correlate events, resulting in delayed detection and response to security incidents.

Web servers deployed in publicly accessible zones, such as DMZs, often suffer from **inadequate application security**. Poor input validation, insecure configurations, and excessive permissions expose web applications to common attacks such as SQL injection and directory traversal. These vulnerabilities can lead to data exposure and compromise of internal systems.

Finally, the absence of **systematic security hardening** leaves cloud infrastructures vulnerable even after vulnerabilities are identified. Without applying firewall rules, access restrictions, and secure configurations, identified weaknesses continue to exist, increasing the likelihood of successful attacks.

This project addresses these identified problems by designing a vulnerable cloud infrastructure, performing ethical hacking simulations to expose weaknesses, monitoring security events using a SIEM platform, and applying structured security hardening measures to improve the overall security posture of the system.

CHAPTER 4:

METHODOLOGY

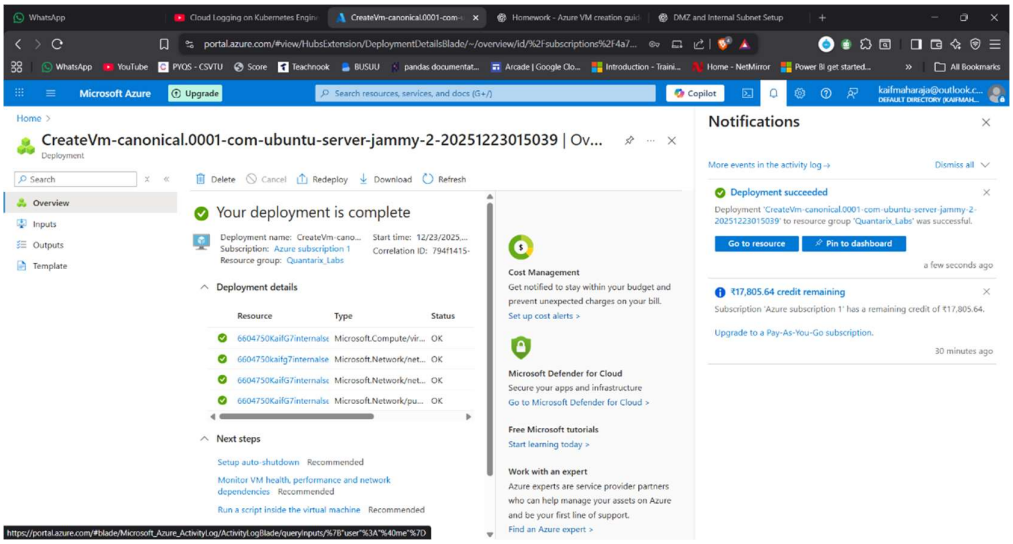
This chapter explains the systematic methodology followed to design, implement, attack, monitor, and secure a cloud-based enterprise infrastructure. The approach closely mirrors real-world cybersecurity practices, where systems are first deployed, then tested against threats, monitored using centralized tools, and finally hardened to improve overall security posture.

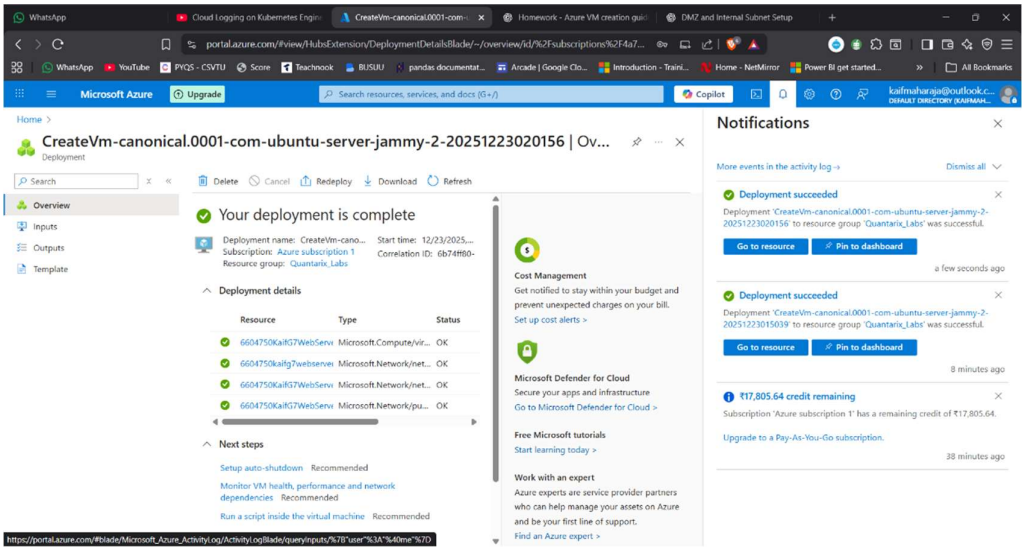
4.1 Infrastructure Deployment

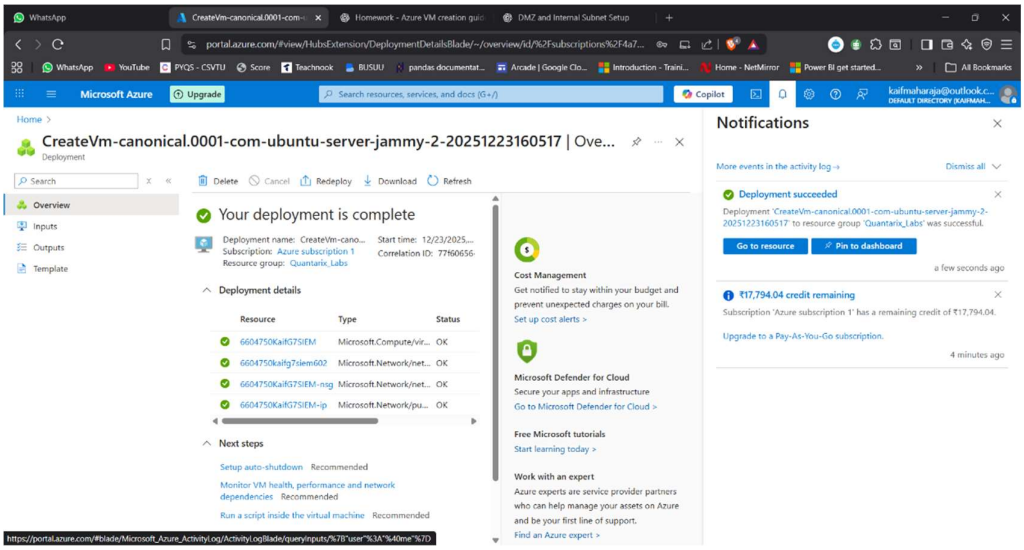
The infrastructure deployment phase focused on creating a realistic enterprise-like environment using **Microsoft Azure cloud services**. A dedicated **Azure Virtual Network (VNet)** was configured to provide logical isolation and controlled communication between different components of the system. To simulate real organizational network architecture, the VNet was divided into two subnets: an **Internal Subnet** and a **Demilitarized Zone (DMZ) Subnet**. The Internal Subnet was designed to host sensitive internal resources, while the DMZ Subnet was used to place externally accessible services, thereby increasing the realism of the deployment.

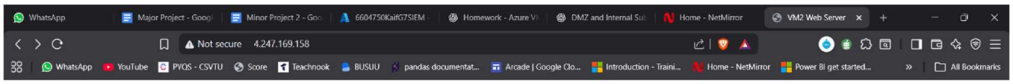
Three **Linux-based virtual machines** were deployed within this network. **VM1 (Internal Server)** was placed in the Internal Subnet and configured to simulate internal enterprise services such as identity management and file handling. **VM2 (Web Server)** was deployed in the DMZ Subnet and hosted a web application using Apache/Nginx, intentionally kept vulnerable to allow controlled attack simulations. **VM3 (SIEM Server)** was also placed in the Internal Subnet and dedicated to centralized log collection, analysis, and monitoring.

All virtual machines were deployed using Ubuntu Server, ensuring consistency and compatibility across the environment. Basic network security groups were configured only to allow necessary communication, while advanced security hardening was intentionally avoided at this stage. This ensured that the infrastructure remained vulnerable enough for ethical hacking simulations in later phases of the project.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home
CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20251223015039 | Ov...
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name: CreateVm-cano...
Subscription: Azure subscription 1
Resource group: Quantarix_Labs
Start time: 12/23/2025,...
Correlation ID: 794f1415-
Deployment details
Resource
Type
Status
6604750KaifG7internalse
Microsoft.Compute/vir...
OK
6604750kaifg7internalse
Microsoft.Network/net...
OK
6604750KaifG7internalse
Microsoft.Network/net...
OK
6604750KaifG7internalse
Microsoft.Network/pu...
OK
Next steps
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >
Notifications
More events in the activity log →
Dismiss all
Deployment succeeded
Deployment 'CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20251223015039' to resource group 'Quantarix_Labs' was successful.
Go to resource
Pin to dashboard
a few seconds ago
₹17,805.64 credit remaining
Subscription 'Azure subscription 1' has a remaining credit of ₹17,805.64.
Upgrade to a Pay-As-You-Go subscription.
30 minutes ago
https://portal.azure.com/#blade/Microsoft_Azure_ActivityLog/ActivityLogBlade/queryInputs/%7B"user"%3A"%40me"%7D

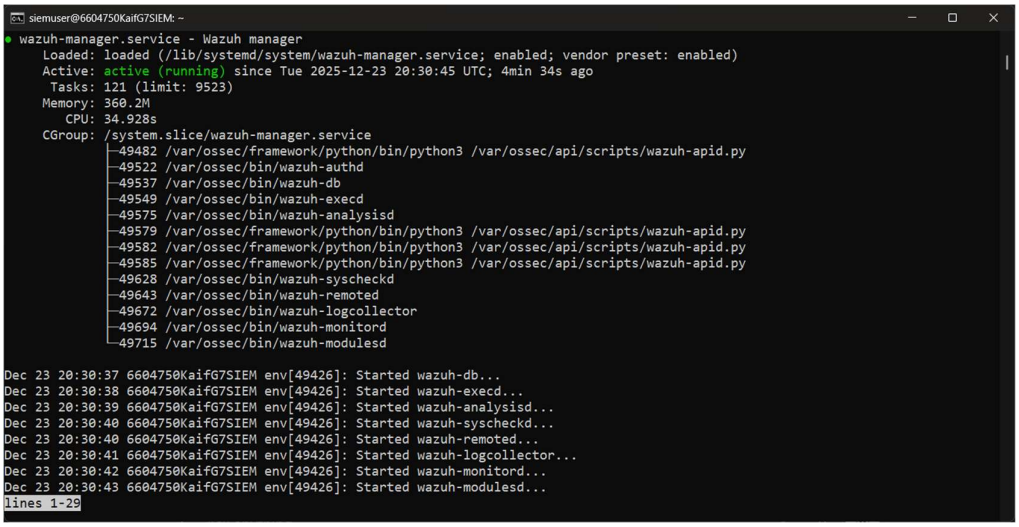

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home
CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20251223020156 | Ov...
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name: CreateVm-cano...
Subscription: Azure subscription 1
Resource group: Quantarix_Labs
Start time: 12/23/2025,...
Correlation ID: 6b74ff80-
Deployment details
Resource
Type
Status
6604750KaifG7WebServe
Microsoft.Compute/vir...
OK
6604750kaifg7webserve
Microsoft.Network/net...
OK
6604750KaifG7WebServe
Microsoft.Network/net...
OK
6604750KaifG7WebServe
Microsoft.Network/pu...
OK
Next steps
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >
Notifications
More events in the activity log →
Dismiss all
Deployment succeeded
Deployment 'CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20251223020156' to resource group 'Quantarix_Labs' was successful.
Go to resource
Pin to dashboard
a few seconds ago
Deployment succeeded
Deployment 'CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20251223015039' to resource group 'Quantarix_Labs' was successful.
Go to resource
Pin to dashboard
8 minutes ago
₹17,805.64 credit remaining
Subscription 'Azure subscription 1' has a remaining credit of ₹17,805.64.
Upgrade to a Pay-As-You-Go subscription.
38 minutes ago
https://portal.azure.com/#blade/Microsoft_Azure_ActivityLog/ActivityLogBlade/queryInputs/%7B"user"%3A"%40me"%7D


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home
CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20251223160517 | Ove...
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name: CreateVm-cano...
Subscription: Azure subscription 1
Resource group: Quantarix_Labs
Start time: 12/23/2025,...
Correlation ID: 77f60656-
Deployment details
Resource
Type
Status
6604750KaifG7SIEM
Microsoft.Compute/vir...
OK
6604750kaifg7siem602
Microsoft.Network/net...
OK
6604750KaifG7SIEM-nsg
Microsoft.Network/net...
OK
6604750KaifG7SIEM-ip
Microsoft.Network/pu...
OK
Next steps
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >
Notifications
More events in the activity log →
Dismiss all
Deployment succeeded
Deployment 'CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20251223160517' to resource group 'Quantarix_Labs' was successful.
Go to resource
Pin to dashboard
a few seconds ago
₹17,794.04 credit remaining
Subscription 'Azure subscription 1' has a remaining credit of ₹17,794.04.
Upgrade to a Pay-As-You-Go subscription.
4 minutes ago
https://portal.azure.com/#blade/Microsoft_Azure_ActivityLog/ActivityLogBlade/queryInputs/%7B"user"%3A"%40me"%7D



Welcome to VM2 â€“ Web Server

This server is intentionally vulnerable for ethical hacking practice.



4.2 Attack Simulation

After successfully deploying the infrastructure, controlled **attack simulations** were conducted to emulate real-world cyber threats. The objective of this phase was not to cause damage but to generate realistic security events and logs that could later be analyzed using a SIEM platform. All attacks were performed ethically within the scope of the deployed environment.

The first category of attacks involved **network scanning using Nmap**. These scans were executed to identify open ports, running services, and potential misconfigurations on the target systems, particularly the web server in the DMZ. Network scanning helped simulate the reconnaissance phase typically performed by attackers before launching further exploits.

Next, **SSH brute-force attacks** were simulated using the Hydra tool. These attacks targeted the SSH service on internal and web servers to test the effectiveness of authentication mechanisms and password policies. Multiple failed login attempts were intentionally generated to observe authentication logs and intrusion alerts.

Web-based attacks were also performed on the DMZ web server. These included **SQL injection attempts** and **directory traversal attacks**, which are common techniques used to exploit insecure web applications. Even when these attacks failed, they successfully generated suspicious request patterns and error logs, which are critical for monitoring and detection.

Finally, **privilege escalation reconnaissance** was carried out on compromised systems to identify misconfigurations such as weak permissions, vulnerable services, and improperly configured binaries. This step helped highlight how attackers might attempt to gain higher privileges after initial access.

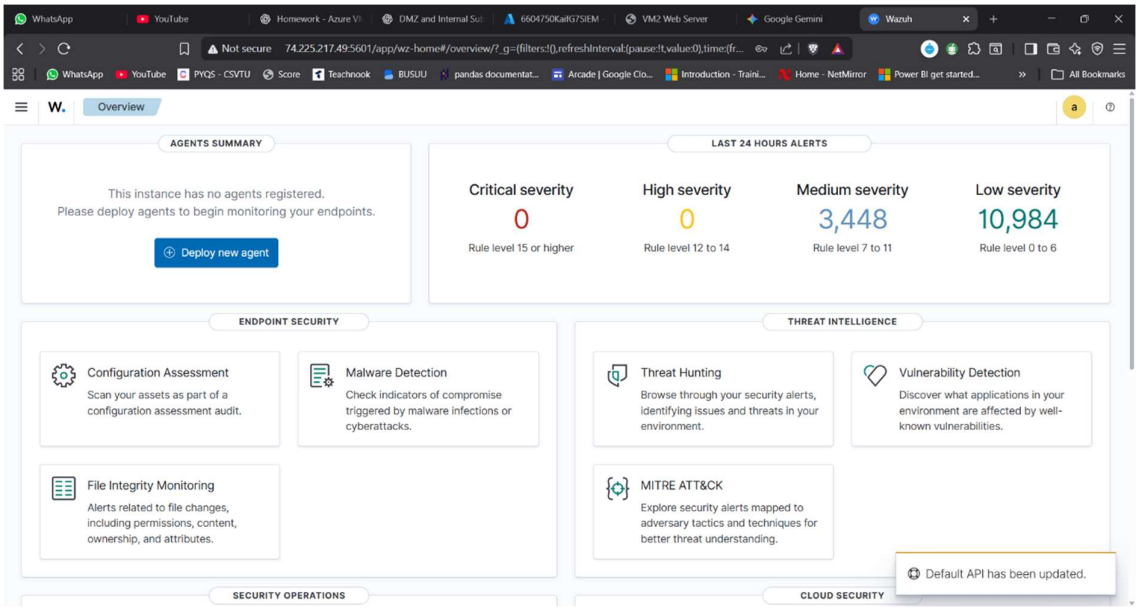
4.3 Monitoring and Detection

The monitoring and detection phase focused on observing and analyzing the security events generated during attack simulations. For this purpose, the **Wazuh SIEM platform** was deployed on **VM3**, which acted as the centralized monitoring and analysis server. Wazuh was chosen due to its open-source nature, powerful log analysis capabilities, and suitability for academic projects.

Wazuh agents were installed and configured on **VM1 and VM2** to forward system logs, authentication logs, and application logs to the SIEM server. Important log sources included system logs, SSH authentication logs, audit logs, and web server access and error logs. These logs were transmitted in real time to the Wazuh manager running on VM3.

The Wazuh dashboard was used to visualize and analyze incoming events. During attack simulations, alerts related to brute-force attempts, port scanning, suspicious web requests, and policy violations were observed. The real-time alerting mechanism allowed quick identification of malicious activities and source IP addresses.

This phase demonstrated the importance of centralized monitoring in modern cybersecurity environments and provided hands-on experience in correlating attack activities with generated alerts and logs.



4.4 Security Hardening

Based on the findings from the monitoring and detection phase, systematic **security hardening measures** were applied to improve the overall security posture of the infrastructure. The primary objective of this phase was to reduce the attack surface and prevent the success of previously executed attacks.

One of the key measures implemented was **SSH hardening**. Password-based authentication was disabled, and **key-based authentication** was enforced to prevent brute-force login attempts. Additional SSH configurations such as limiting authentication attempts and disabling root login were also applied.

Network-level security was enhanced using **UFW (Uncomplicated Firewall)**. Firewall rules were configured to restrict unnecessary inbound traffic, allowing only required ports such as SSH and HTTP/HTTPS. Access to sensitive services was limited to trusted internal sources, significantly reducing exposure.

The **web server** hosted on the DMZ VM was hardened by disabling directory listing, adding security headers, and restricting access to sensitive files and directories. These changes reduced the effectiveness of web-based attacks such as directory traversal and information disclosure.

Finally, **enhanced logging and access control mechanisms** were implemented to ensure better visibility and accountability. After applying all hardening measures, selected attacks were re-executed to validate improvements. The results showed a clear reduction in successful attack attempts and improved alert quality, confirming the effectiveness of the applied security controls.

CHAPTER 5: RESULTS

This chapter presents the results obtained from the attack simulations, monitoring activities, and security hardening processes performed on the cloud-based enterprise infrastructure. The results clearly demonstrate the differences in system behavior, security posture, and alert patterns before and after the implementation of security controls. The observations are based on system logs, SIEM alerts, and the outcomes of repeated attack attempts.

5.1 Results of Attack Simulation (Before Hardening)

During the initial phase, the infrastructure was intentionally kept vulnerable to observe how common cyber-attacks impact an unsecured cloud environment. Network scanning using Nmap successfully identified multiple open ports and exposed services on the target systems, particularly the web server deployed in the DMZ. These scans confirmed the absence of strict firewall rules and highlighted the increased attack surface.

SSH brute-force attacks generated a large number of failed authentication attempts on both the internal server and the web server. The authentication logs recorded repeated login failures, indicating weak password-based authentication mechanisms. These attempts were clearly visible in system logs and later detected by the SIEM platform.

Web-based attacks such as SQL injection and directory traversal produced abnormal HTTP requests in the web server access and error logs. Although some attacks did not result in data disclosure, they successfully generated suspicious activity patterns that are typically associated with exploitation attempts. Privilege escalation reconnaissance further revealed misconfigurations such as excessive permissions and vulnerable system settings.

Overall, the results of the attack simulation phase confirmed that the infrastructure was highly susceptible to common attack techniques when no security hardening measures were applied.

5.2 SIEM Detection and Log Analysis

The Wazuh SIEM platform played a critical role in collecting and analyzing logs generated during the attack simulations. Logs from VM1 and VM2 were successfully forwarded to the SIEM server (VM3), providing centralized visibility into system activities.

The SIEM dashboard displayed multiple alerts related to authentication failures, port scanning behavior, and suspicious web requests. Alerts were categorized based on severity, enabling easy identification of high-risk events. The correlation of logs allowed the identification of attack sources, affected systems, and attack timelines.

One key observation was the clear mapping between attack actions and SIEM alerts. For example, SSH brute-force attempts resulted in repeated authentication failure alerts, while network scanning triggered warnings related to abnormal connection attempts. This confirmed the effectiveness of centralized monitoring in detecting malicious behavior in real time.

5.3 Results After Security Hardening

After implementing security hardening measures, the same set of attacks was re-executed to evaluate improvements. The results showed a significant reduction in successful attack attempts. SSH brute-force attacks failed due to the enforcement of key-based authentication and restricted login attempts. Authentication logs showed fewer failed login entries, indicating improved access control.

Firewall configurations using UFW successfully limited network exposure. Nmap scans revealed a reduced number of open ports, demonstrating effective network-level protection. Web-based attacks such as directory traversal attempts were blocked or logged with restricted access, preventing information disclosure.

The SIEM alerts after hardening showed a noticeable change in pattern. While some alerts were still generated, their severity and frequency were significantly reduced. This indicated that attacks were being detected early and mitigated before causing impact.

5.4 Comparative Analysis (Before vs After Hardening)

A comparative analysis of the results before and after hardening highlights the effectiveness of the applied security measures. Before hardening, the infrastructure exhibited high exposure and vulnerability, with frequent alerts and successful reconnaissance. After hardening, the attack surface was minimized, and the infrastructure demonstrated improved resilience against common threats.

The number of SIEM alerts related to brute-force attempts and network scanning decreased, and the system logs reflected stricter access control policies. This comparison clearly validates the importance of proactive security hardening in cloud environments.

5.5 Summary of Observations

The results obtained from this project demonstrate that:

- Unsecured cloud environments are highly vulnerable to basic attacks.
- Centralized monitoring using SIEM provides valuable visibility into security events.
- Systematic hardening significantly improves security posture.
- Re-attack validation is essential to confirm the effectiveness of security measures.

Overall, the results confirm that the adopted methodology successfully achieved the project objectives and provided practical insight into ethical hacking, monitoring, and cloud security.

CHAPTER 6: CONCLUSION

This project successfully demonstrates a complete cloud security workflow, from deployment and attack simulation to detection and hardening. The applied security measures significantly improved the overall security posture of the cloud infrastructure.

The project enhanced practical knowledge of ethical hacking, SIEM operations, and cloud security best practices.

BIBLIOGRAPHY

1. Wazuh Documentation, https://documentation.wazuh.com
2. Microsoft Azure Security Documentation
3. OWASP Top 10 Web Application Security Risks

APPENDIX

APPENDIX A: ATTACK SCREENSHOTS AND OBSERVATIONS

Figure A.1: Nmap Port Scanning on VM2 (Before Hardening)

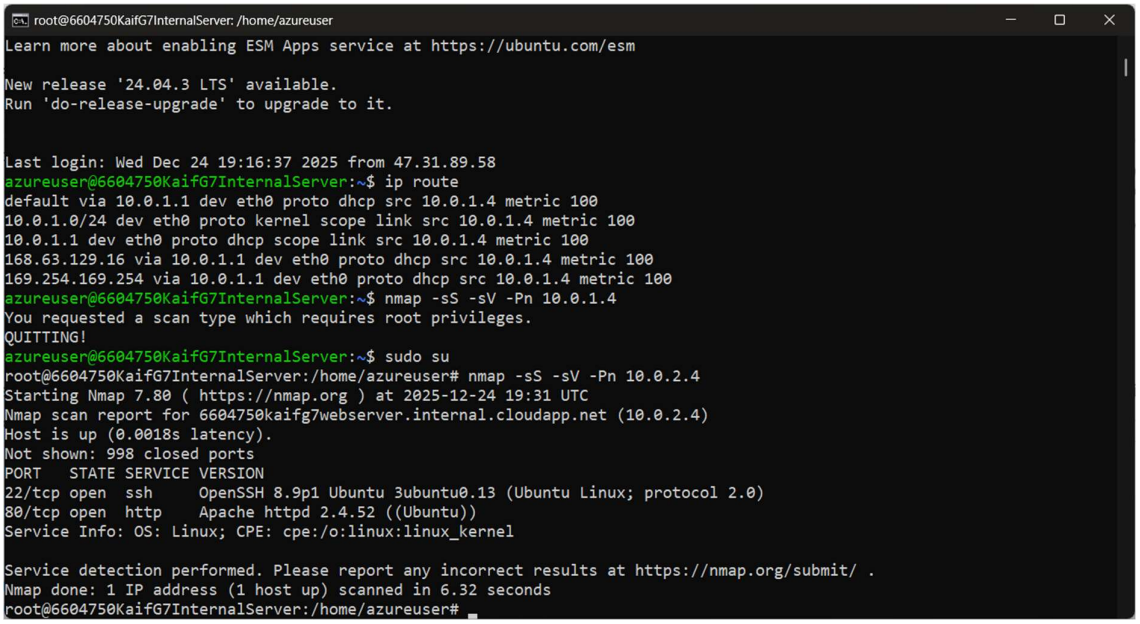


Figure A.2: SSH Brute Force Attempts Using Hydra

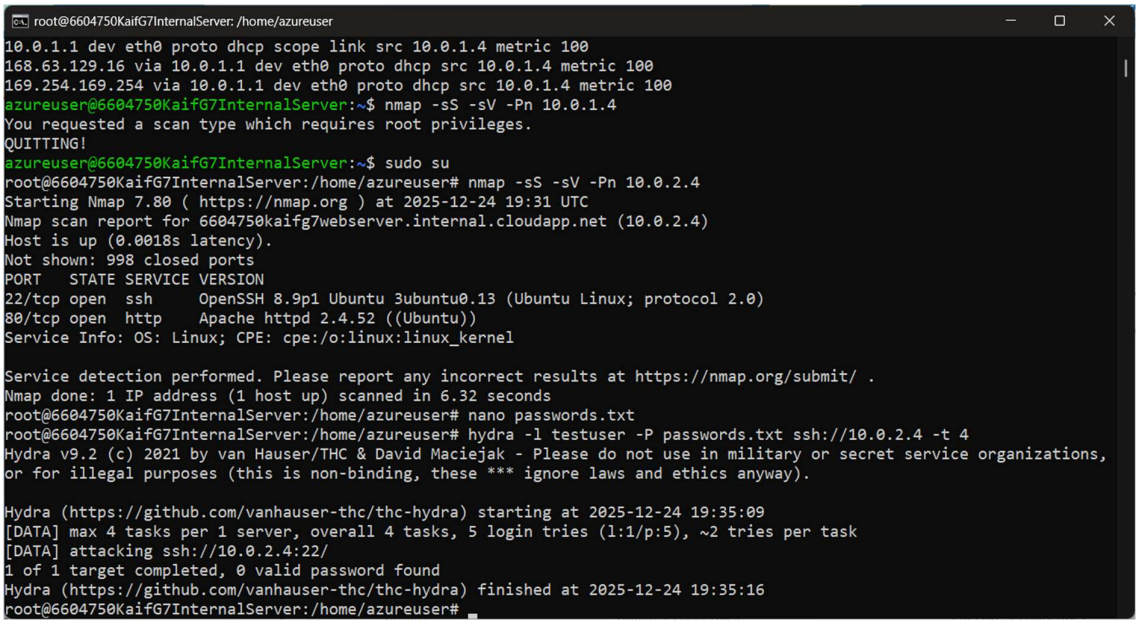


Figure A.3: SQL Injection Attempts on Web Server

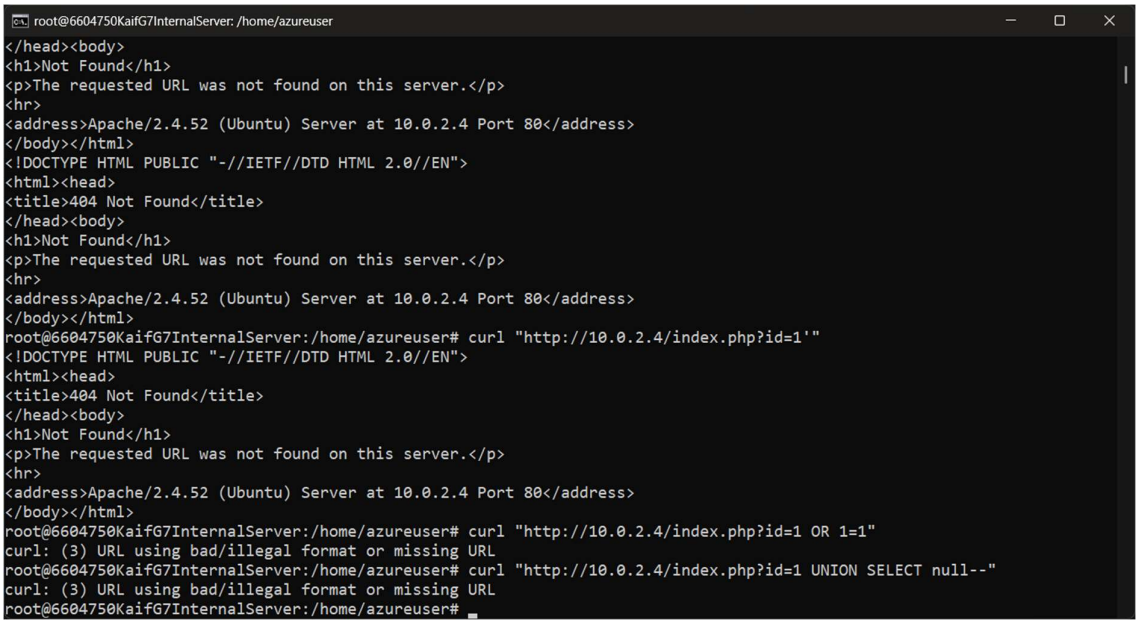
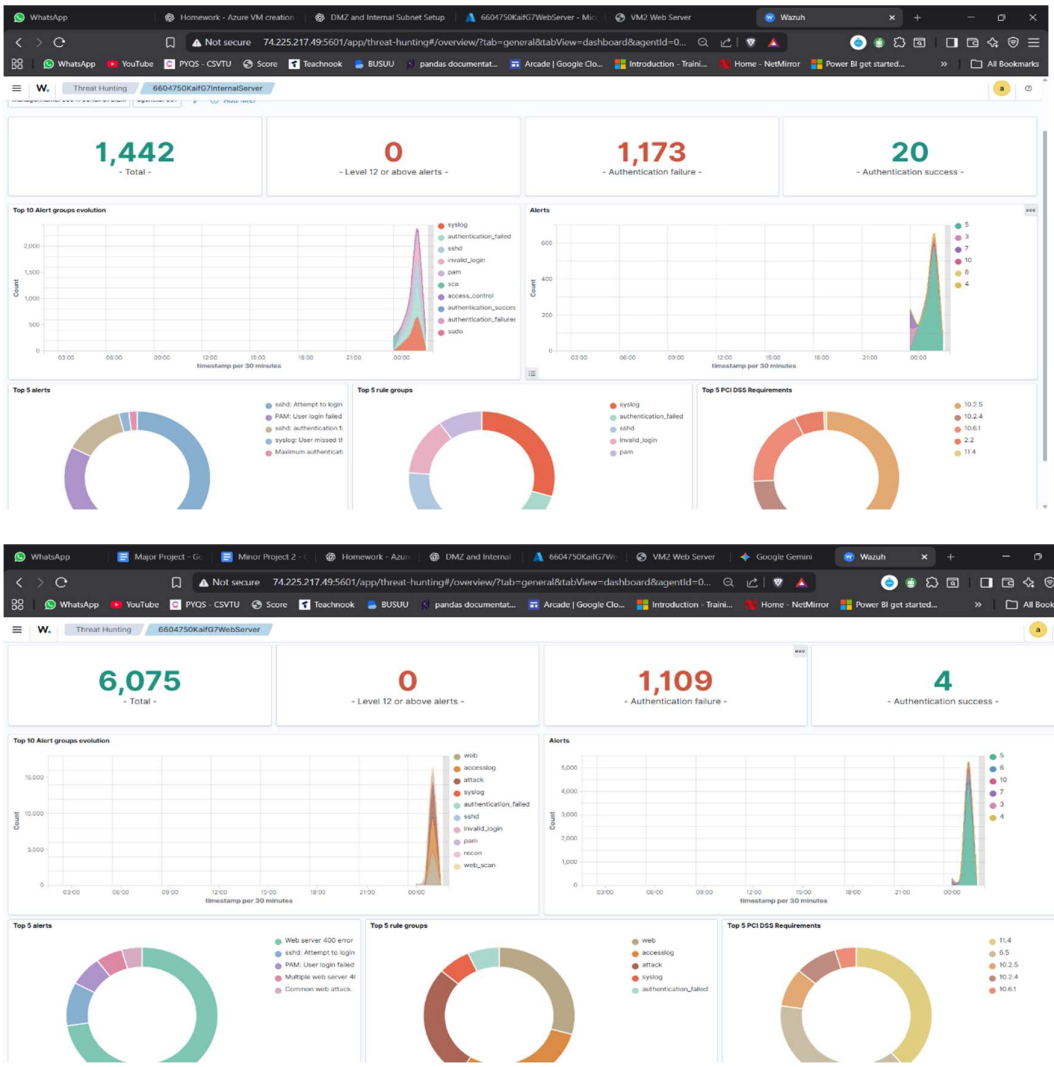


Figure A.4: Directory Traversal Attempts

```
root@6604750KaifG7InternalServer: /home/azureuser
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-24 19:35:16
root@6604750KaifG7InternalServer:/home/azureuser# curl http://10.0.2.4
<!DOCTYPE html>
<html>
<head>
  <title>VM2 Web Server</title>
</head>
<body>
  <h1>Welcome to VM2 - Web Server</h1>
  <p>This server is intentionally vulnerable for ethical hacking practice.</p>
</body>
</html>
root@6604750KaifG7InternalServer:/home/azureuser# nikto -h http://10.0.2.4
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.0.2.4
+ Target Hostname:    6604750kaifg7webserver.internal.cloudapp.net
+ Target Port:        80
+ Start Time:         2025-12-24 19:38:54 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.52 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0xd5 0x646a1962bb50b
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ 6544 items checked: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2025-12-24 19:38:58 (GMT0) (4 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@6604750KaifG7InternalServer:/home/azureuser#
```

Figure A.5: Wazuh Alerts Generated Before Hardening



APPENDIX B: POST-HARDENING VALIDATION

Figure B.1: Reduced Open Ports After Firewall Configuration

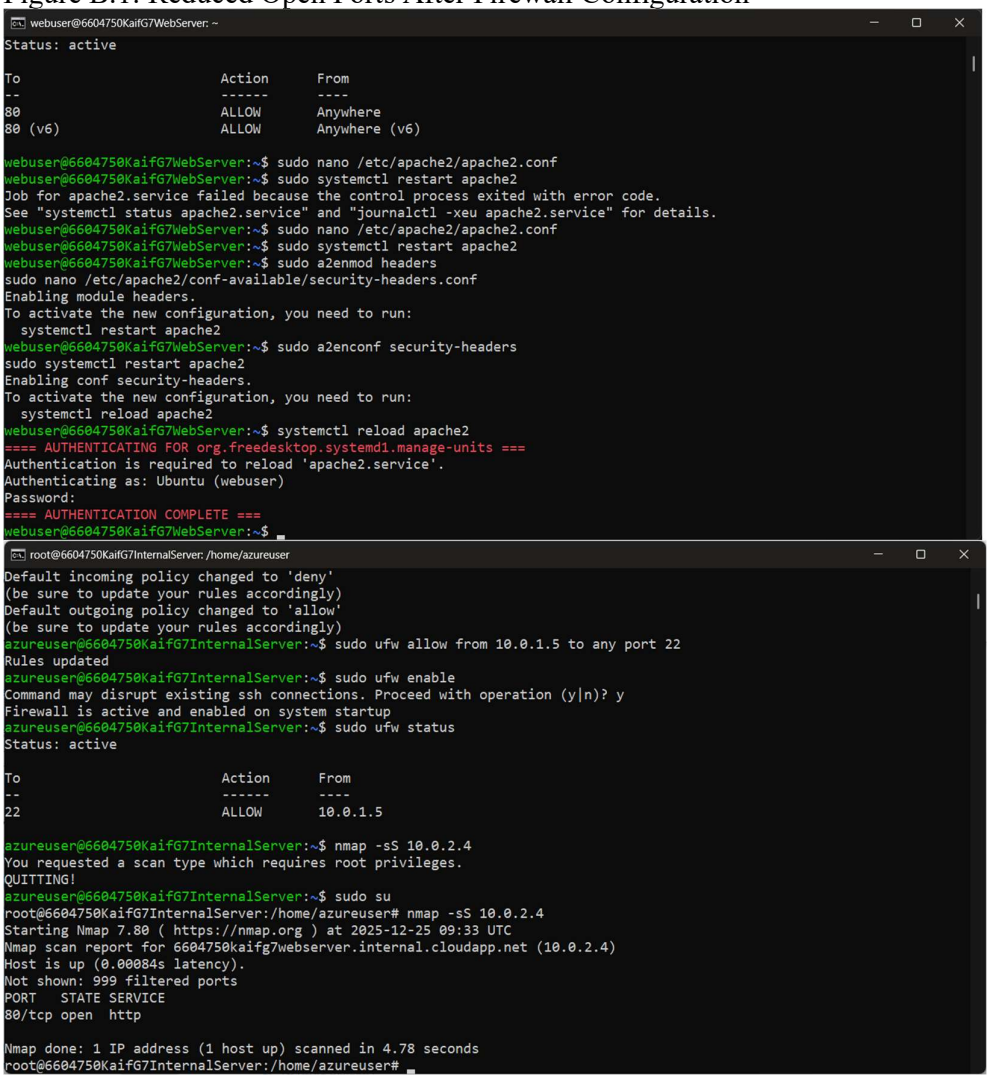


Figure B.2: Failed SSH Brute Force After Hardening

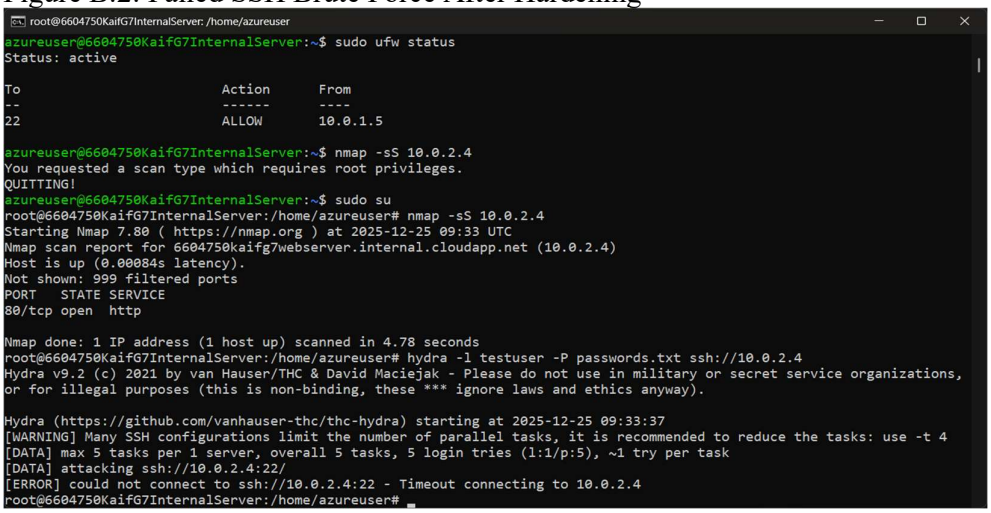
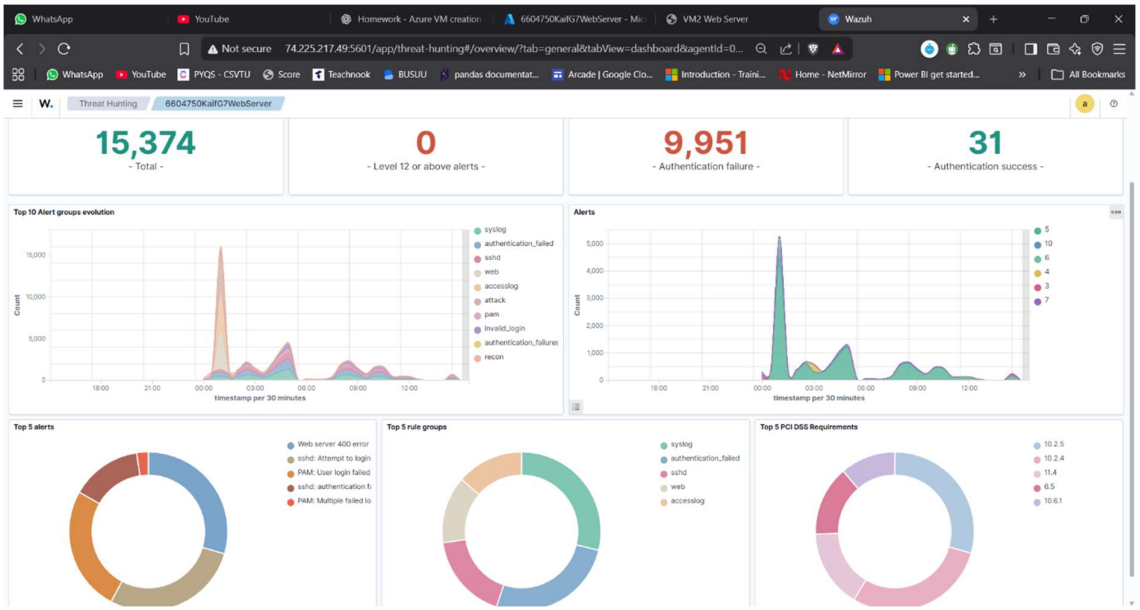
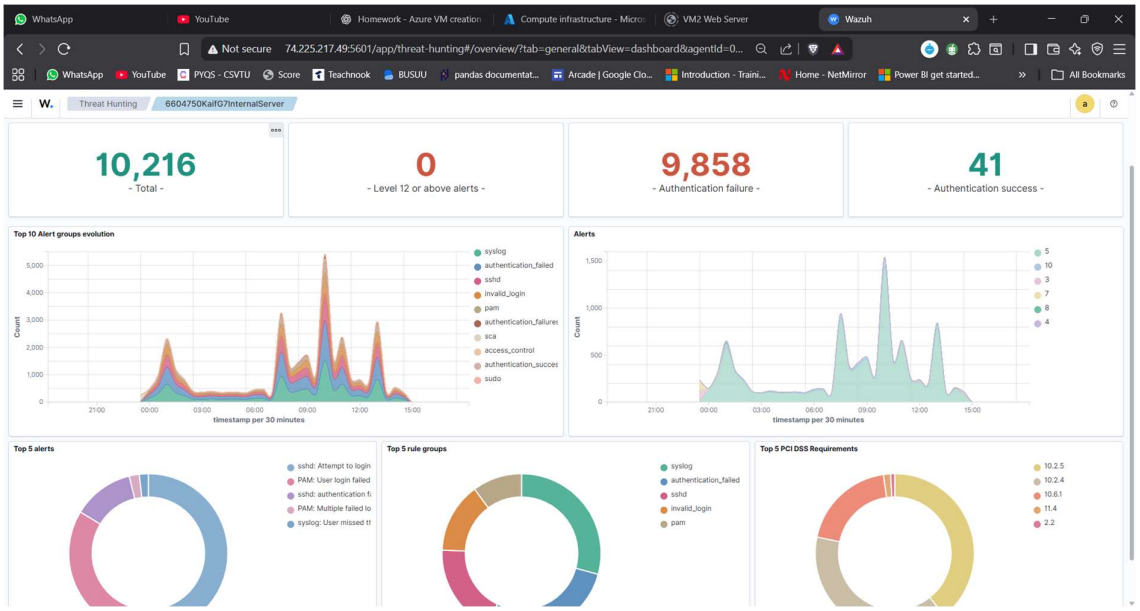


Figure B.3: Wazuh Alerts After Security Hardening




WhatsApp
YouTube
Homework - Azure VM creation
Compute infrastructure - Micros
VM2 Web Server
Wazuh
Not secure
74.225.217.49:5601/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=0...
WhatsApp
YouTube
PYQS - CSVTU
Score
Teachnook
BUSUU
pandas documentat...
Arcade | Google Clo...
Introduction - Traini...
Home - NetMirror
Power BI get started...
All Bookmarks
W.
Threat Hunting
6604750KaifG7InternalServer
10,216
- Total -
0
- Level 12 or above alerts -
9,858
- Authentication failure -
41
- Authentication success -
Top 10 Alert groups evolution
Count
timestamp per 30 minutes
syslog
authentication_failed
sshd
invalid_login
pam
authentication_failures
sca
access_control
authentication_succes
sudo
Alerts
Count
timestamp per 30 minutes
5
10
3
7
8
4
Top 5 alerts
sshd: Attempt to login
PAM: User login failed
sshd: authentication fi
PAM: Multiple failed lo
syslog: User missed th
Top 5 rule groups
syslog
authentication_failed
sshd
invalid_login
pam
Top 5 PCI DSS Requirements
10.2.5
10.2.4
10.6.1
11.4
2.2