Active Directory & Wazuh SIEM Cybersecurity Capstone Project

Hands-On Enterprise Security Lab

Author: Krish Patel

Date: December 5, 2025

Table of Contents

1. Executive Summary

This project simulates a real-world enterprise environment including an Active Directory domain, a Windows 10 client, and a Wazuh SIEM server. The objective was to build and secure an enterprise network, perform realistic cyber attacks, and detect malicious activity using Wazuh.

2. Environment Architecture

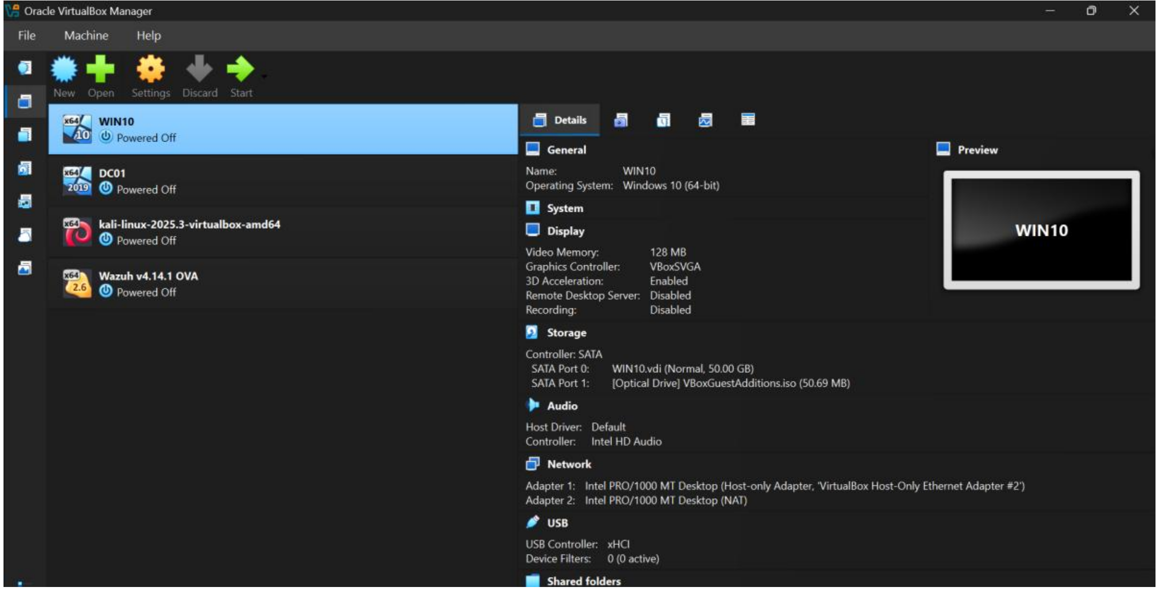
This section outlines the systems involved in the enterprise lab environment.

- DC01 (Domain Controller): AD DS, DNS, GPO, Sysmon

- WIN10 Client: Domain-joined workstation, Sysmon installed

- Wazuh Manager, Indexer, Dashboard: SIEM for log collection and alerting

Figure 1: AD Users and Computers



WIN10
Powered Off

DC01
Powered Off

kali-linux-2025.3-virtualbox-amd64
Powered Off

Wazuh v4.14.1 OVA
Powered Off

General

```
Name:              WIN10
Operating System:  Windows 10 (64-bit)
```

System

Display

```
Video Memory:           128 MB
Graphics Controller:    VBoxSVGA
3D Acceleration:        Enabled
Remote Desktop Server:  Disabled
Recording:              Disabled
```

Storage

```
Controller: SATA
 SATA Port 0:    WIN10.vdi (Normal, 50.00 GB)
 SATA Port 1:    [Optical Drive] VBoxGuestAdditions.iso (50.69 MB)
```

Audio

```
Host Driver:  Default
Controller:   Intel HD Audio
```

Network

```
Adapter 1:  Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter #2')
Adapter 2:  Intel PRO/1000 MT Desktop (NAT)
```

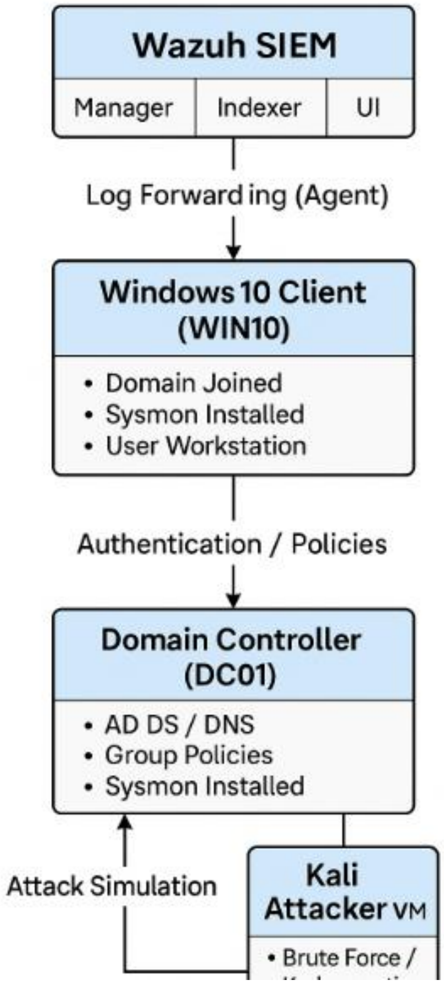
USB

```
USB Controller:  xHCI
Device Filters:  0 (0 active)
```

Shared folders

The following diagram represents the full lab architecture used in this project

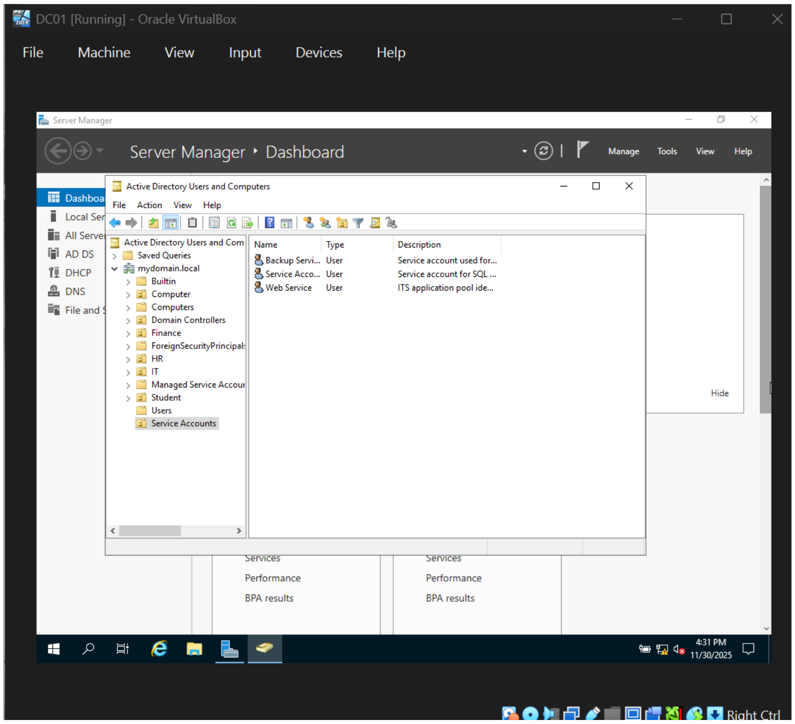
Figure 2: Network Architecture Diagram



3. Active Directory Configuration

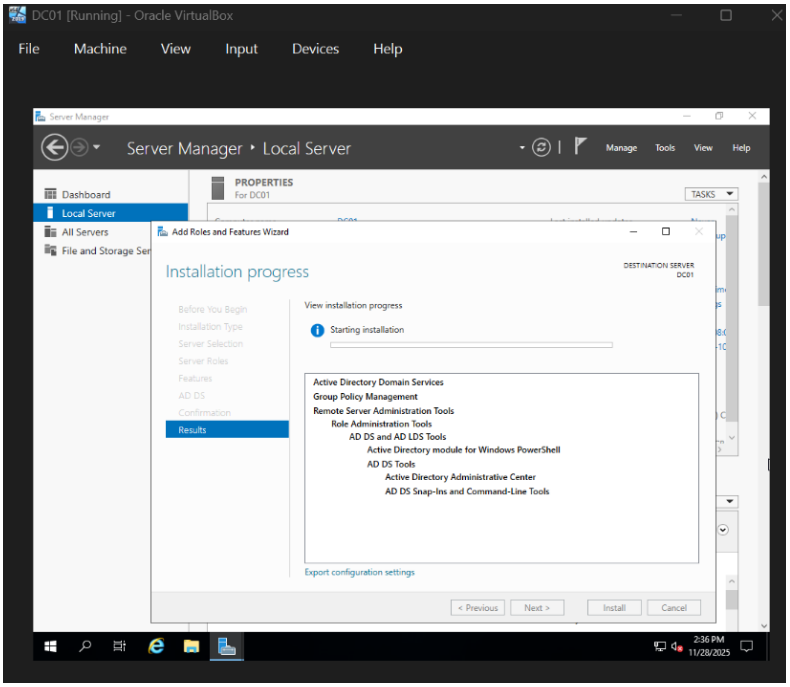
This section covers the installation of domain services, DNS, OU structure, service accounts, and joining the workstation to the domain.

Figure 3: Active Directory OU and Service Accounts



Name	Type	Description
Backup Servi...	User	Service account used for...
Service Acco...	User	Service account for SQL ...
Web Service	User	ITS application pool ide...

Figure 4: AD DS Installation in Progress



Installation progress

View installation progress

Starting installation

```
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
    Role Administration Tools
        AD DS and AD LDS Tools
            Active Directory module for Windows PowerShell
            AD DS Tools
                Active Directory Administrative Center
                AD DS Snap-Ins and Command-Line Tools
```

4. Group Policy Hardening

This section documents security hardening applied using Group Policy Objects (GPO).

- Password complexity enforcement

- Account lockout policy

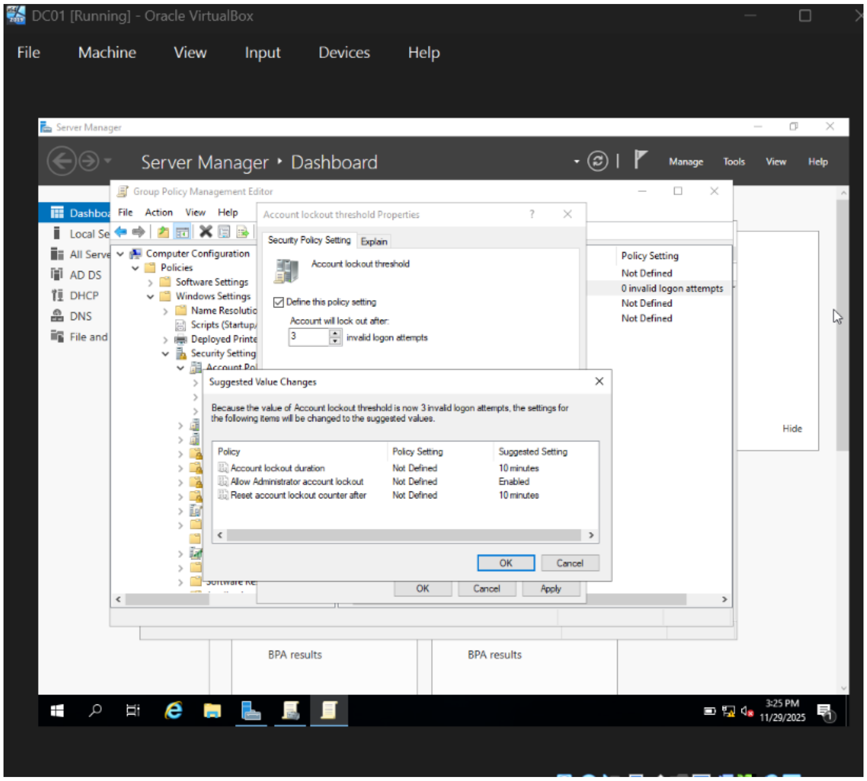
- Disable LLMNR

- Disable SMBv1

- Block PowerShell v2

- Custom wallpaper enforcement

Figure 5: GPO Password Policy



Account lockout threshold Properties

Security Policy Setting

Account lockout threshold

☑ Define this policy setting

Account will lock out after:

3 invalid logon attempts

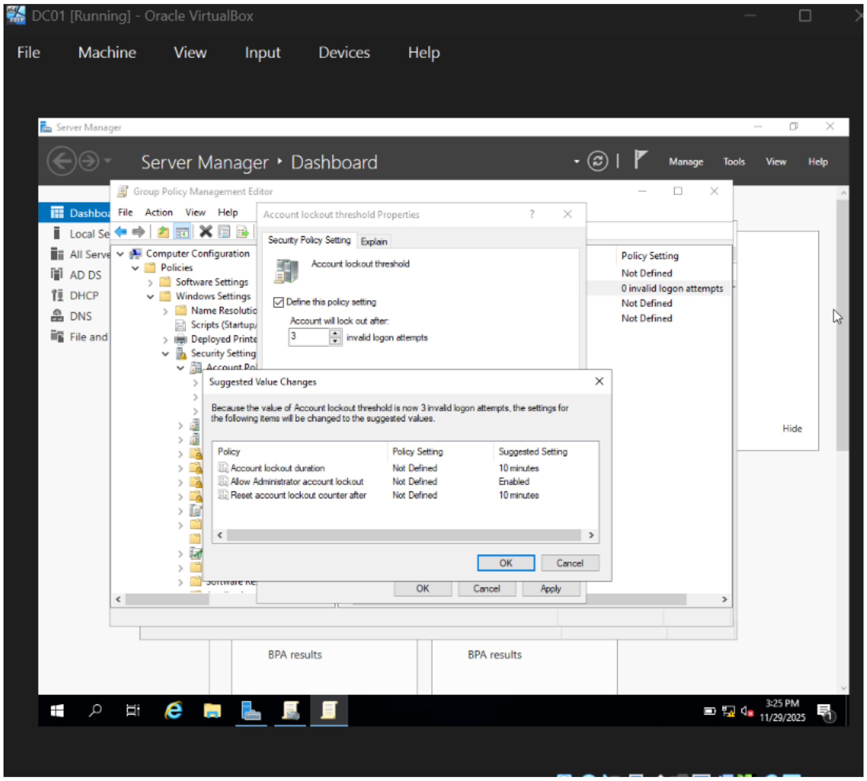
Suggested Value Changes

Because the value of Account lockout threshold is now 3 invalid logon attempts, the settings for the following items will be changed to the suggested values.

Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Defined	10 minutes
Allow Administrator account lockout	Not Defined	Enabled
Reset account lockout counter after	Not Defined	10 minutes

Policy Setting
Not Defined
0 invalid logon attempts
Not Defined
Not Defined

Figure 6: Account Lockout Policy Configuration



Account lockout threshold Properties

Security Policy Setting | Explain

Account lockout threshold

☑ Define this policy setting

Account will lock out after:

3 invalid logon attempts

Policy Setting
Not Defined
0 invalid logon attempts
Not Defined
Not Defined

Suggested Value Changes

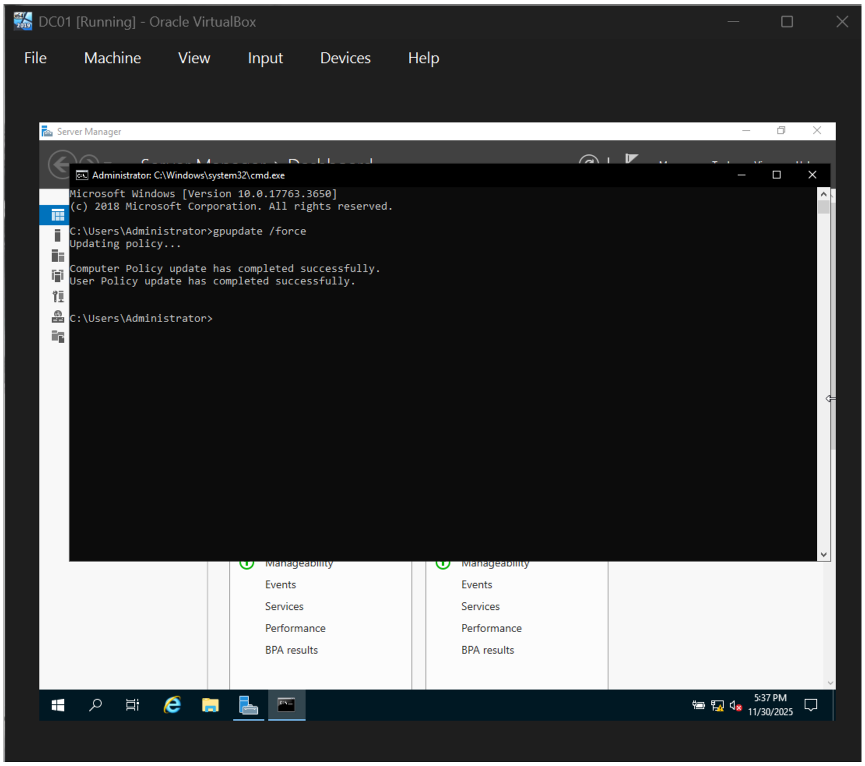
Because the value of Account lockout threshold is now 3 invalid logon attempts, the settings for the following items will be changed to the suggested values.

Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Defined	10 minutes
Allow Administrator account lockout	Not Defined	Enabled
Reset account lockout counter after	Not Defined	10 minutes

OK Cancel

OK Cancel Apply

Figure 7: GPO Applied via gpupdate /force



```
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\Administrator>
```

5. Attack Simulation

This section demonstrates cyber attacks executed to generate security logs and test detection capability.

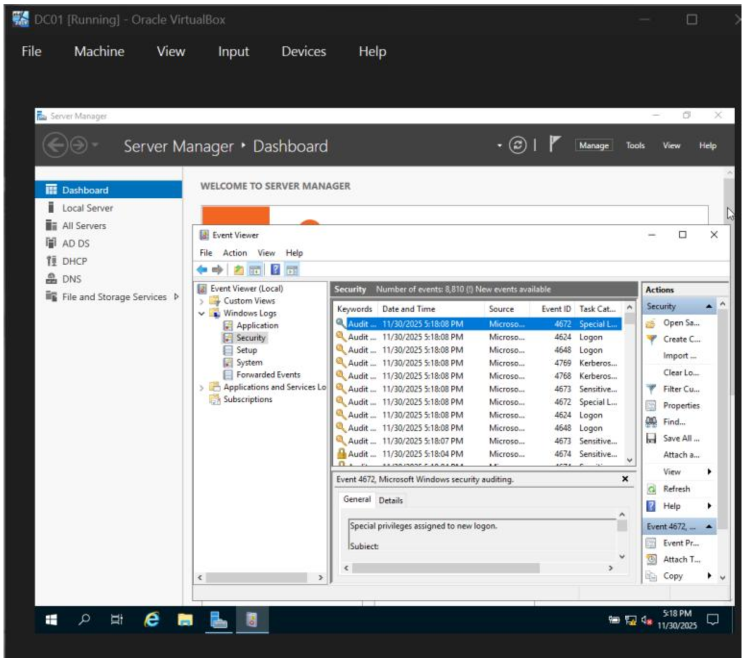
A. Brute Force Attack – Event ID 4625

B. Kerberoasting – Event ID 4769

C. Privilege Escalation – Event IDs 4662, 4624, 4672

D. Persistence – Event ID 4698

Figure 8: Logs inside DC01



Security Number of events: 8,810 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Cat...
Audit ...	11/30/2025 5:18:08 PM	Microso...	4672	Special L...
Audit ...	11/30/2025 5:18:08 PM	Microso...	4624	Logon
Audit ...	11/30/2025 5:18:08 PM	Microso...	4648	Logon
Audit ...	11/30/2025 5:18:08 PM	Microso...	4769	Kerberos...
Audit ...	11/30/2025 5:18:08 PM	Microso...	4768	Kerberos...
Audit ...	11/30/2025 5:18:08 PM	Microso...	4673	Sensitive...
Audit ...	11/30/2025 5:18:08 PM	Microso...	4672	Special L...
Audit ...	11/30/2025 5:18:08 PM	Microso...	4624	Logon
Audit ...	11/30/2025 5:18:08 PM	Microso...	4648	Logon
Audit ...	11/30/2025 5:18:07 PM	Microso...	4673	Sensitive...
Audit ...	11/30/2025 5:18:04 PM	Microso...	4674	Sensitive...

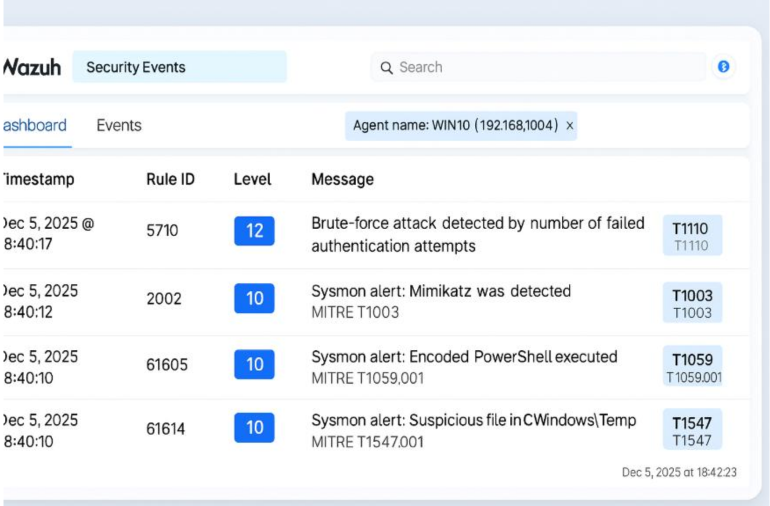
Event 4672, Microsoft Windows security auditing.

General Details

Special privileges assigned to new logon.

Subject:

Figure 9.1: Logs inside Wazuh

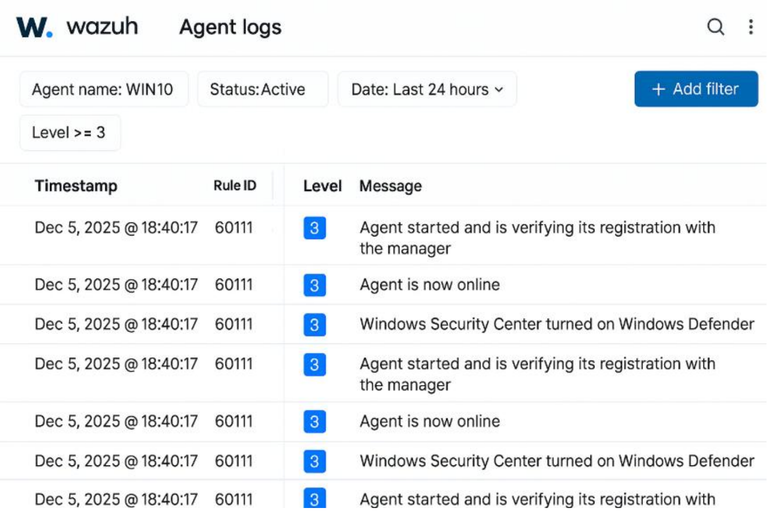


Agent name: WIN10 (192.168,1004) ×

imestamp	Rule ID	Level	Message	
)ec 5, 2025 @ 8:40:17	5710	12	Brute-force attack detected by number of failed authentication attempts	T1110 T1110
)ec 5, 2025 8:40:12	2002	10	Sysmon alert: Mimikatz was detected MITRE T1003	T1003 T1003
)ec 5, 2025 8:40:10	61605	10	Sysmon alert: Encoded PowerShell executed MITRE T1059,001	T1059 T1059.001
)ec 5, 2025 8:40:10	61614	10	Sysmon alert: Suspicious file in CWindows\Temp MITRE T1547.001	T1547 T1547

Dec 5, 2025 at 18:42:23

Figure 9.2: Logs inside Wazuh



Agent name: WIN10 | Status:Active | Date: Last 24 hours | Level >= 3

Timestamp	Rule ID	Level	Message
Dec 5, 2025 @ 18:40:17	60111	3	Agent started and is verifying its registration with the manager
Dec 5, 2025 @ 18:40:17	60111	3	Agent is now online
Dec 5, 2025 @ 18:40:17	60111	3	Windows Security Center turned on Windows Defender
Dec 5, 2025 @ 18:40:17	60111	3	Agent started and is verifying its registration with the manager
Dec 5, 2025 @ 18:40:17	60111	3	Agent is now online
Dec 5, 2025 @ 18:40:17	60111	3	Windows Security Center turned on Windows Defender
Dec 5, 2025 @ 18:40:17	60111	3	Agent started and is verifying its registration with

Attack Summary Table:

Attack Type	Event IDs	Detection Source	MITRE Technique
Brute Force	4625	Wazuh	T1110
Kerberoasting	4769	Wazuh	T1558.003
Privilege Escalation	4672, 4662	Sysmon + Wazuh	T1003
Persistence	4698	Wazuh	T1053

6. Wazuh SIEM Analysis

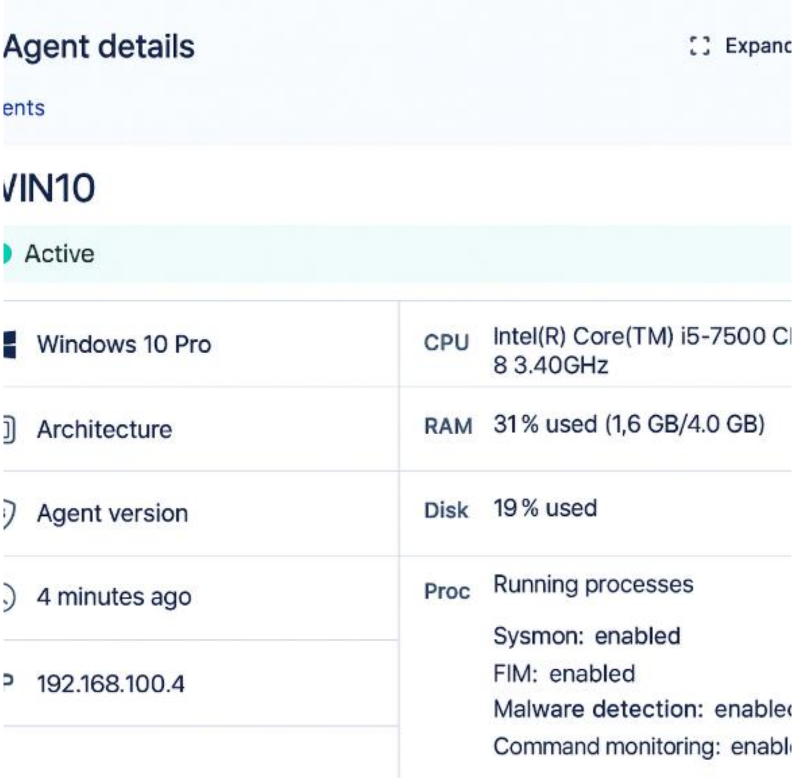
This section analyzes Wazuh's ability to detect and correlate malicious behavior across the environment.

- Agent registration and monitoring

- Sysmon log ingestion

- MITRE ATT&CK mapping

Figure 9: Wazuh Agent



Agent details

Expanc

ents

VIN10

Active

Windows 10 Pro

Architecture

Agent version

4 minutes ago

192.168.100.4

CPU Intel(R) Core(TM) i5-7500 C
8 3.40GHz

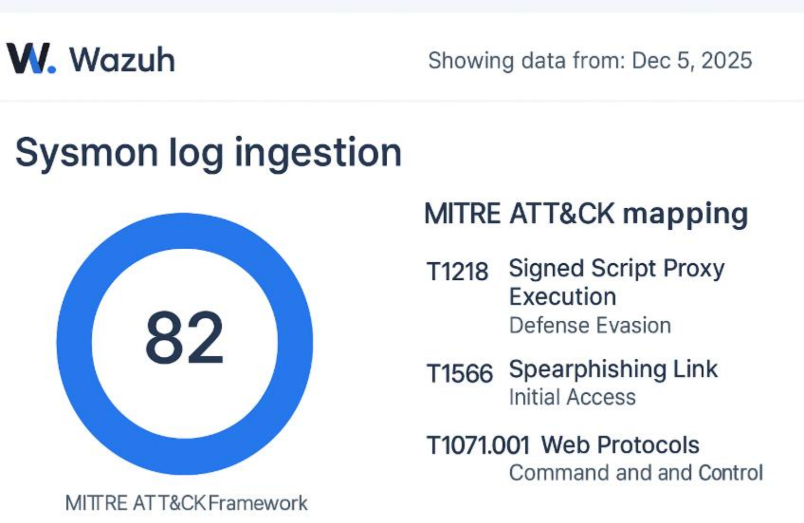
RAM 31 % used (1,6 GB/4.0 GB)

Disk 19 % used

Proc Running processes

Sysmon: enabled
FIM: enabled
Malware detection: enable
Command monitoring: enabl

Figure 10: Wazuh Sysmon logs and Mitre Att&ck



Wazuh

Showing data from: Dec 5, 2025

Sysmon log ingestion

MITRE ATT&CK mapping

T1218 Signed Script Proxy Execution
Defense Evasion

T1566 Spearphishing Link
Initial Access

T1071.001 Web Protocols
Command and and Control

7. Findings & Detection Coverage

Key findings from monitoring and detection activities:

- Brute force attempts detected through repeated Event ID 4625 failures.

- Kerberoasting attempts detected through abnormal 4769 ticket requests.

- Privilege escalation activity flagged via elevated logon IDs.

- Persistence attempts identified via Event ID 4698 task creation.

8. Recommendations for Organizations

- Enforce password complexity and lockout policies.

- Disable LLMNR and SMBv1 to reduce attack surface.

- Monitor high-value Event IDs tied to credential theft.

- Deploy Sysmon and SIEM tools across all endpoints.

- Conduct regular AD security audits and apply least privilege.

9. Skills Demonstrated

- Active Directory deployment & hardening

- Sysmon configuration & event analysis

- Wazuh SIEM deployment, indexing, and ruleset interpretation

- MITRE ATT&CK mapping

- Detection engineering & log correlation

- Incident response documentation

10. Conclusion

This capstone project successfully demonstrated the ability to build and secure an enterprise Active Directory environment. Through realistic attack simulations such as brute force, Kerberoasting, and privilege escalation, the environment generated meaningful security telemetry. Using Wazuh SIEM and Sysmon logging, these attacks were detected, analyzed, and mapped to MITRE ATT&CK techniques.

Overall, the project reflects real-world SOC analyst workflows and showcases hands-on blue team, detection engineering, and incident response skills.