Configuring SIEM with Wazuh

16.04.2025 - 07.05.2025

Authors:

- Bakina Sofia
- Andrey Boronin
- Ivan Sannikov
- Alexander Tomashov

Table of Contents

1. Introduction

1.1 Rationale for the choice of topic

Modern organizations are increasingly facing the need to efficiently detect and respond to cybersecurity incidents. One of the key tools in this field are Security Information and Event Management (SIEM) systems.

This project focuses on the deployment and configuration of the Wazuh SIEM solution — an open-source and powerful framework based on the Elastic Stack. The project aims to create a fully isolated virtual environment where the Wazuh server is deployed, along with agents operating on both Windows and Linux systems.

1.2 Aims and objectives of the project

The goal of the project is to create a secure virtual infrastructure using the Wazuh SIEM system for monitoring, detecting attacks, and ensuring integrity control. The project involves deploying a system that will include:

- Deploying a virtual infrastructure using VMware vSphere and configuring network segmentation through MikroTik.
- Deploying Wazuh on a server for security event monitoring and configuring agents on workstations and servers (Windows and Linux).
- Implementing several use cases for attack detection, such as:
  - Detecting suspicious processes using Sysmon.
  - Detecting process creation and termination events.
- Simulating attacks on vulnerable applications (Juice Shop), analyzing protection results, and adjusting security policies.

1.3 Description of the initial idea

At the start of the project, a basic virtual environment is in place, which will be used to deploy the components. The virtual infrastructure includes services with varying levels of security, including test vulnerable applications (e.g., Juice Shop), which will serve as targets for attacks.
Wazuh will be used for monitoring, with agents configured on servers and workstations. The system will be integrated with external threat sources for improved threat processing and analysis. During the implementation, attacks will be simulated using standard tools like Linux to test defenses and adjust rules accordingly.

---

2. Infrastructure Design

2.1 Overall architecture

The infrastructure of the project is deployed in an isolated virtual environment based on VMware ESXi/vSphere. The virtual infrastructure includes:

- **Wazuh** — the core SIEM component.
- **Windows Agent** — simulates a user workstation.
- **Linux Agent** — a server or host in the exploitation segment.
- **Juice Shop** — a vulnerable web application for attack simulation.
- **MikroTik Router** — used for network segmentation and traffic filtering.

2.2 Network segmentation

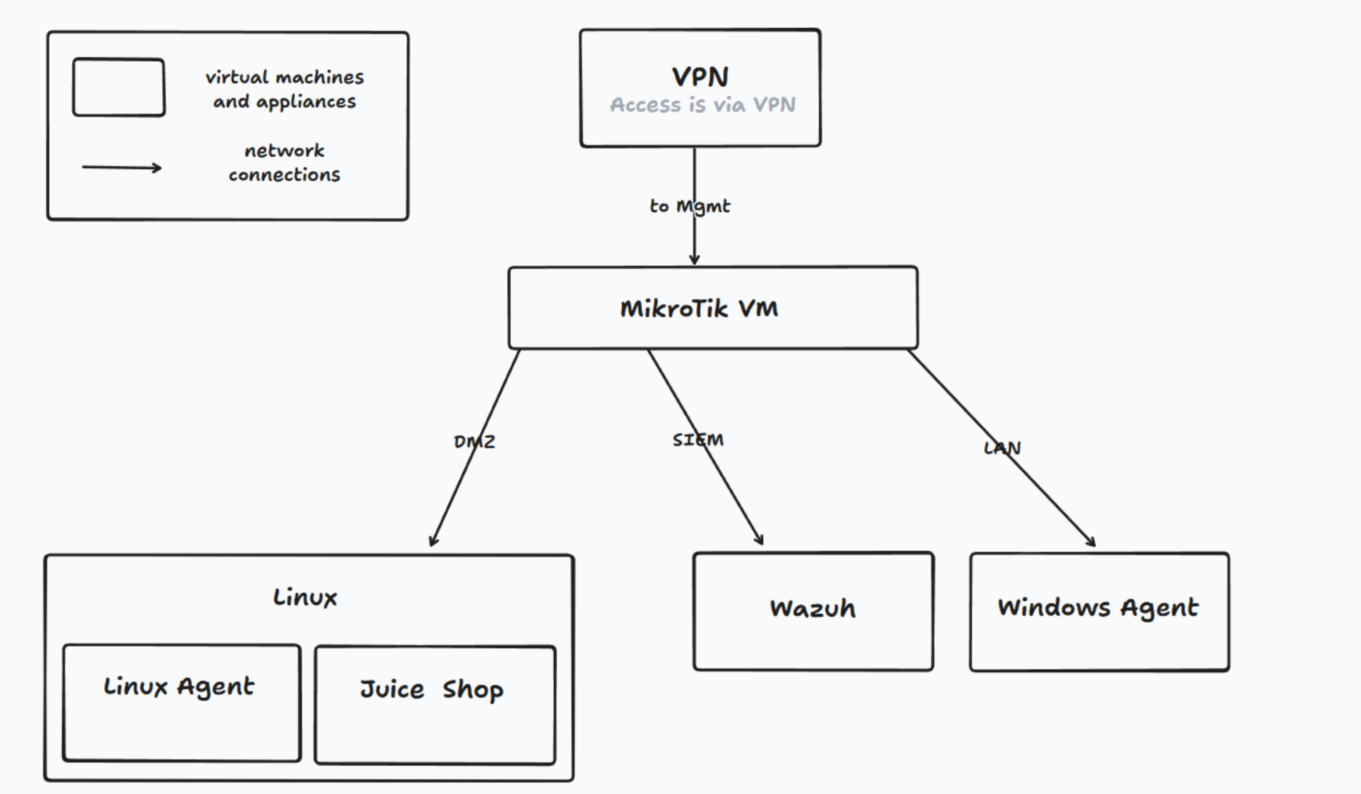
For security and access management, the entire infrastructure is divided into several logical zones (VLAN/port group):

- **Segment | Purpose**

- **MGMT** | Management and administration
- **DMZ** | Public or semi-public services
- **DMZ** | Servers isolated from the internal infrastructure

2.3 Network topology

The project includes setting up a virtual infrastructure, network segmentation using MikroTik and VMware, which allows isolating different subnets and services for enhanced security. Access to services is configured via secure channels, and VPN is also set up.



Example of interaction:

- VPN connects to MikroTik and other VMs (via the Mgmt VLAN).
- Agents (Windows/Linux) send logs to the Wazuh server via SIEM.
- MikroTik controls inter-network communication, e.g., allows LAN → DMZ but blocks DMZ → LAN.

2.4 Technologies

The infrastructure of the diploma project is deployed in an isolated virtual environment based on VMware ESXi/vSphere (or a similar platform). The virtual infrastructure includes:

- **Component** | **Technology / Product**
- **Virtualization** | VMware ESXi
- **Segmentation / Routing** | MikroTik RouterOS
- **SIEM** | Wazuh (Elastic Stack: Elasticsearch, Kibana)
- **Agents** | Wazuh Agent (Windows, Linux)
- **Vulnerable Application** | OWASP Juice Shop
- **Threat Monitoring** | Wazuh Rules, YARA
- **Testing** | Linux

2.5 Security and isolation

Firewall and access rules are implemented on MikroTik.
Strict isolation is applied between subnets.
The Wazuh server is only accessible from the Management segment.
The User segment cannot interact directly with SIEM or other zones except the DMZ.
NAT and VPN are implemented through MikroTik (for external access and traffic forwarding).
Firewall and access rules are managed by MikroTik, which controls routing and isolation between VLANs.

---

3. Deployment and Configuration

This chapter will describe the process of installing and configuring basic components such as the Wazuh server and agents, as well as configuring other services and infrastructure for effective monitoring and security.

3.1 Configuring MikroTik

What was done:

- Subnets for Management, LAN, DMZ were configured, and IP addresses were assigned via DHCP.
- Access to the Management subnet is provided only via VPN, isolating it from other network segments. Other devices cannot access the Management network without VPN.
- Routing was configured to direct traffic through correct paths, and firewall rules ensure necessary security and isolation between segments.

3.2 Setting up secure tunnels

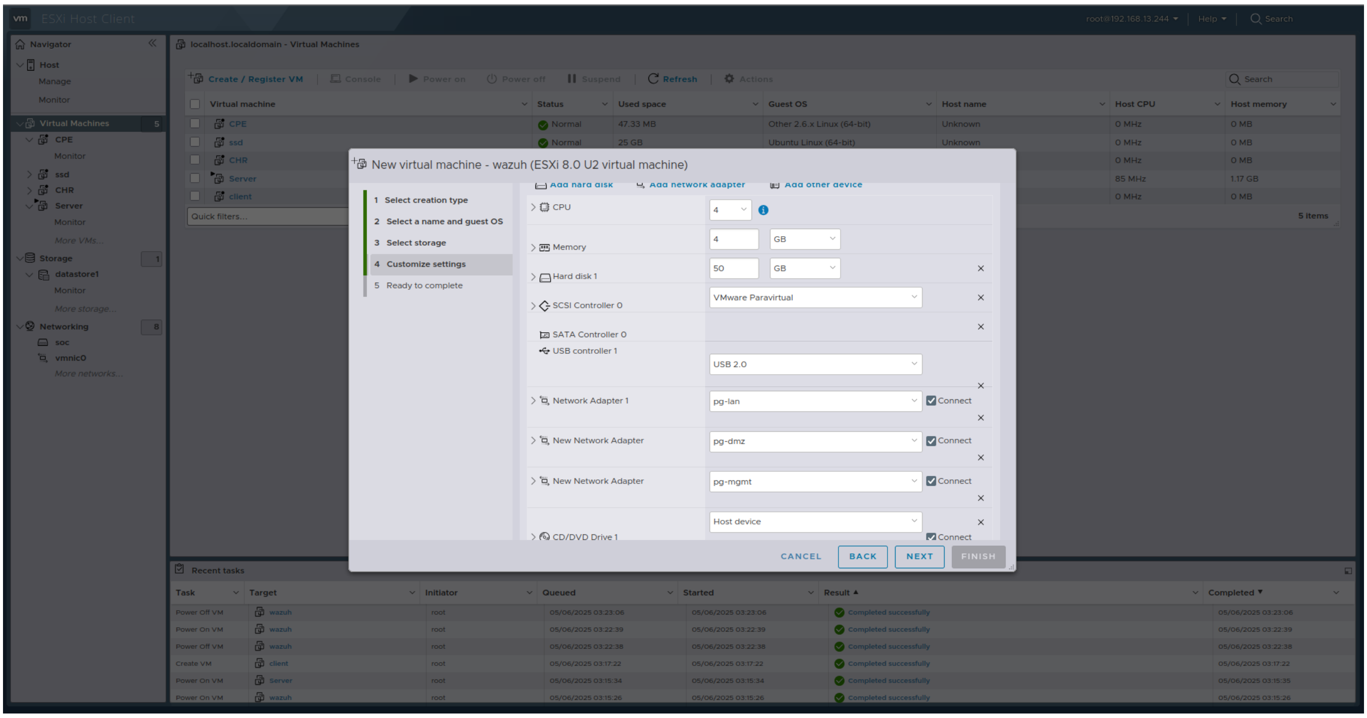
For secure connections between infrastructure components, VPN tunnels were configured using IPsec and OpenVPN.
What was done:

- VPN via IPsec was set up for secure connections between subnets and infrastructure components.
- OpenVPN was also configured as an additional VPN connection system, ensuring secure data transfer.
- MikroTik was set up to work with VPN to ensure segmentation and secure interaction between clients and services, including the Management subnet.

3.3 Deploying the Wazuh

Preparation:

- Wazuh is deployed on a virtual machine located in two subnets: pg-LAN and pg-DMZ.
  Requirements:
- Operating system: Ubuntu 20.04 or later.
- At least 4GB of RAM and 2 virtual CPUs.
- 50GB of disk space for data storage.



Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
CPE	Normal	47.33 MB	Other 2.6.x Linux (64-bit)	Unknown	0 MHz	0 MB
ssd	Normal	25 GB	Ubuntu Linux (64-bit)	Unknown	0 MHz	0 MB
CHR					0 MHz	0 MB
Server					85 MHz	1.17 GB
client					0 MHz	0 MB

New virtual machine - wazuh (ESXi 8.0 U2 virtual machine)

1 Select creation type
2 Select a name and guest OS
3 Select storage
4 Customize settings
5 Ready to complete

CPU	4
Memory	4 GB
Hard disk 1	50 GB
SCSI Controller 0	VMware Paravirtual
SATA Controller 0	
USB controller 1	USB 2.0
Network Adapter 1	pg-lan ☑ Connect
New Network Adapter	pg-dmz ☑ Connect
New Network Adapter	pg-mgmt ☑ Connect
CD/DVD Drive 1	Host device ☑ Connect

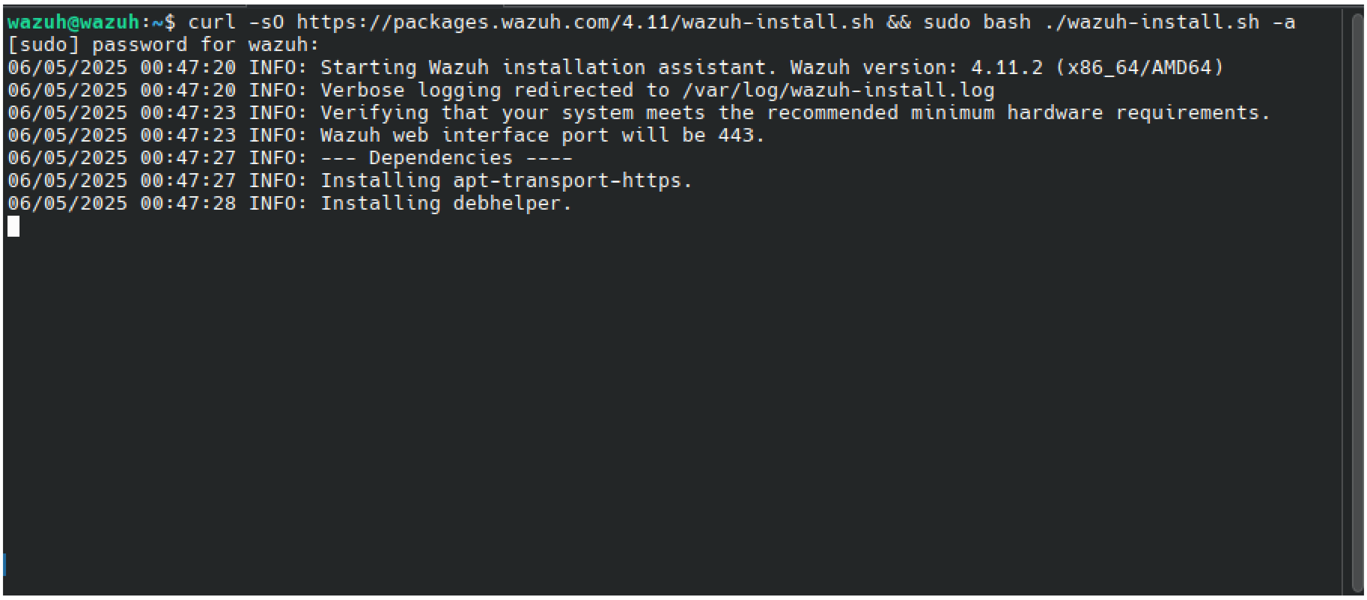
Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼
Power Off VM	wazuh	root	05/06/2025 03:23:06	05/06/2025 03:23:06	Completed successfully	05/06/2025 03:23:06
Power On VM	wazuh	root	05/06/2025 03:22:39	05/06/2025 03:22:39	Completed successfully	05/06/2025 03:22:39
Power Off VM	wazuh	root	05/06/2025 03:22:38	05/06/2025 03:22:38	Completed successfully	05/06/2025 03:22:38
Create VM	client	root	05/06/2025 03:17:22	05/06/2025 03:17:22	Completed successfully	05/06/2025 03:17:22
Power On VM	Server	root	05/06/2025 03:15:34	05/06/2025 03:15:34	Completed successfully	05/06/2025 03:15:35
Power On VM	wazuh	root	05/06/2025 03:15:26	05/06/2025 03:15:26	Completed successfully	05/06/2025 03:15:26

Installation:

- Update the system:

```
sudo apt-get update
```

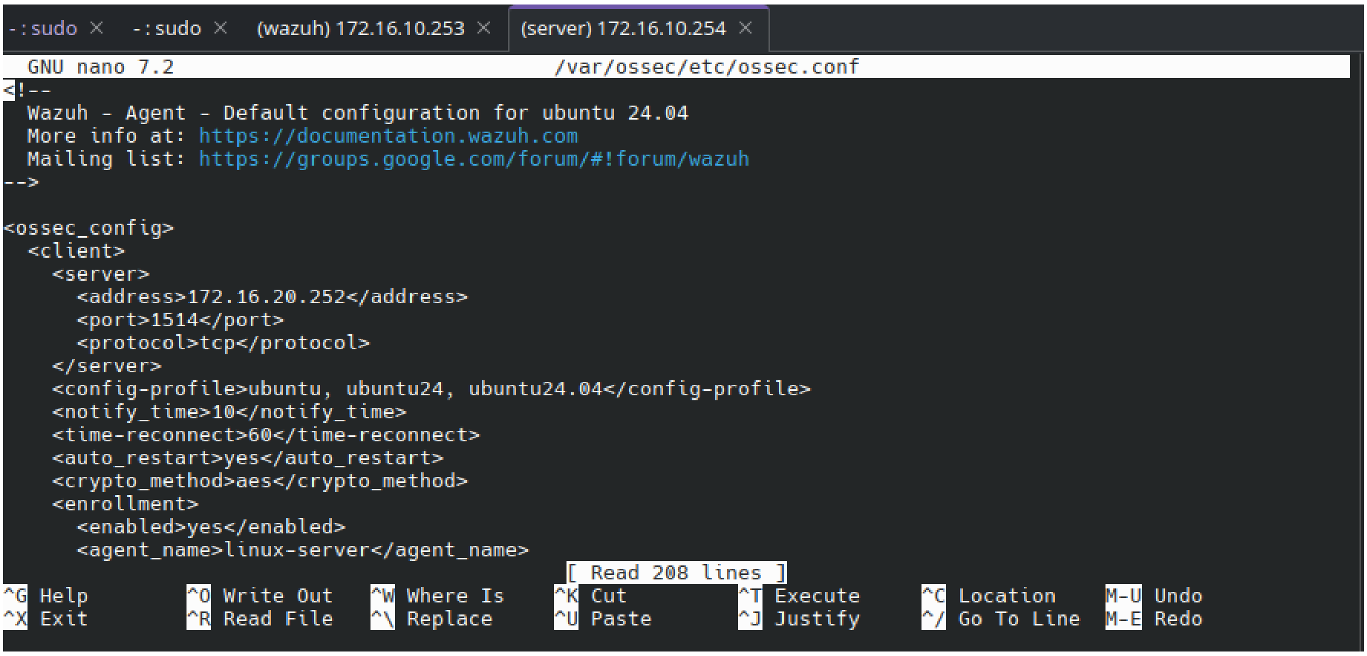
- Install Wazuh by following the instructions in the official Wazuh quickstart guide.



```
wazuh@wazuh:~$ curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
[sudo] password for wazuh:
06/05/2025 00:47:20 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.2 (x86_64/AMD64)
06/05/2025 00:47:20 INFO: Verbose logging redirected to /var/log/wazuh-install.log
06/05/2025 00:47:23 INFO: Verifying that your system meets the recommended minimum hardware requirements.
06/05/2025 00:47:23 INFO: Wazuh web interface port will be 443.
06/05/2025 00:47:27 INFO: --- Dependencies ----
06/05/2025 00:47:27 INFO: Installing apt-transport-https.
06/05/2025 00:47:28 INFO: Installing debhelper.
```

Configuration:

- After installation, configure Wazuh for log collection and processing. This can be done via the configuration file: `/var/ossec/etc/ossec.conf`. In this file, security rules, agent settings, file integrity monitoring, etc., can be configured.



```
  GNU nano 7.2                            /var/ossec/etc/ossec.conf
<!--
  Wazuh - Agent - Default configuration for ubuntu 24.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>172.16.20.252</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>ubuntu, ubuntu24, ubuntu24.04</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
    <enrollment>
      <enabled>yes</enabled>
      <agent_name>linux-server</agent_name>
                                              [ Read 208 lines ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```

3.4 Installing and configuring agents

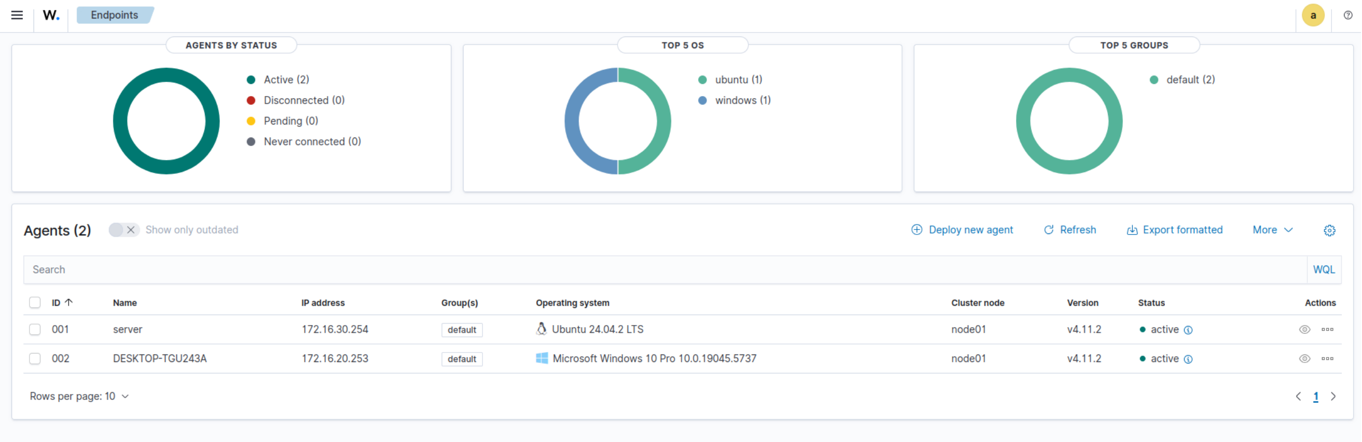
After setting up the Wazuh server, agents need to be installed on both Windows and Linux systems to collect and send data for analysis.

Installing Wazuh agent on Windows:

1. Download the latest Wazuh agent version from the official website.
2. Run the installer and follow the instructions.
3. Add the server address to the configuration file.
4. Restart the agent service.

Installing Wazuh agent on Linux:

1. Add the Wazuh repository and install the agent.
2. Configure the agent.
3. Start the agent service.



ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	server	172.16.30.254	default	Ubuntu 24.04.2 LTS	node01	v4.11.2	● active	
002	DESKTOP-TGU243A	172.16.20.253	default	Microsoft Windows 10 Pro 10.0.19045.5737	node01	v4.11.2	● active	

3.5 Implementing Use Cases

In this section, we will implement and configure at least three use cases as described in the Wazuh documentation. We will work on:

- Detecting suspicious processes using Sysmon.
- Detecting process creation and termination events.

3.5.1 Detecting Suspicious Processes

Objective:
Configure Wazuh to detect suspicious processes such as unauthorized or unusual processes (e.g., **lsass.exe**, **svchost.exe**, etc.).

Sysmon Rules Installation and Configuration:

1. To monitor processes such as **lsass.exe** and others, rules have been added to the Wazuh configuration.

   Example configuration for detecting suspicious processes:

   ```
   <group name="windows,sysmon,sysmon_process-anomalies,">
      <rule id="61625" level="12">
         <if_group>sysmon_event1</if_group>
         <field name="win.eventdata.image">lsass.exe</field>
         <description>Sysmon - Suspicious Process - lsass</description>
         <mitre>
            <id>T1055</id>
         </mitre>
         <group>pci_dss_10.6.1,pci_dss_11.4,gdpr_IV_35.7.d,</group>
      </rule>

      <rule id="61626" level="0">
         <if_sid>61625</if_sid>
         <field name="win.eventdata.parentImage">wininit.exe</field>
         <description>Sysmon - Legitimate Parent Image -
   lsass.exe</description>
      </rule>
   </group>
   ```

2. To ensure Sysmon logs are collected, the following configuration has been added to the Windows configuration:

   ```
   <localfile>
      <location>Microsoft-Windows-Sysmon/Operational</location>
      <log_format>eventchannel</log_format>
   </localfile>
   ```

Verification:

To verify the rule, create a copy of **lsass.exe** (or another suspicious process) and check Wazuh logs. If the process is suspicious, Wazuh should generate an alert indicating the process and its parent (e.g., `wininit.exe`).

3.5.2 Detecting Process Creation and Termination Events

Objective: Monitor process creation and termination events, such as the starting and stopping of critical system processes.

Sysmon Event Rules for Process Creation and Termination:

1. Additional rules for monitoring process creation and termination have been added in the Wazuh configuration:

   ```
   <rule id="61603" level="5">
      <if_sid>61600</if_sid>
      <field name="win.system.eventID">^1$</field>
      <description>Sysmon - Event 1: Process creation $(win.eventdata.description)</description>
   </rule>

   <rule id="61605" level="0">
      <if_sid>61600</if_sid>
      <field name="win.system.eventID">^5$</field>
      <description>Sysmon - Event 5: Process terminated $(win.eventdata.image)</description>
   </rule>
   ```

2. These rules help to track processes that are created or terminated and ensure that no unauthorized processes are running or exiting without notification.

Verification:

To verify this use case, simulate the creation and termination of a process and check the Wazuh alerts:

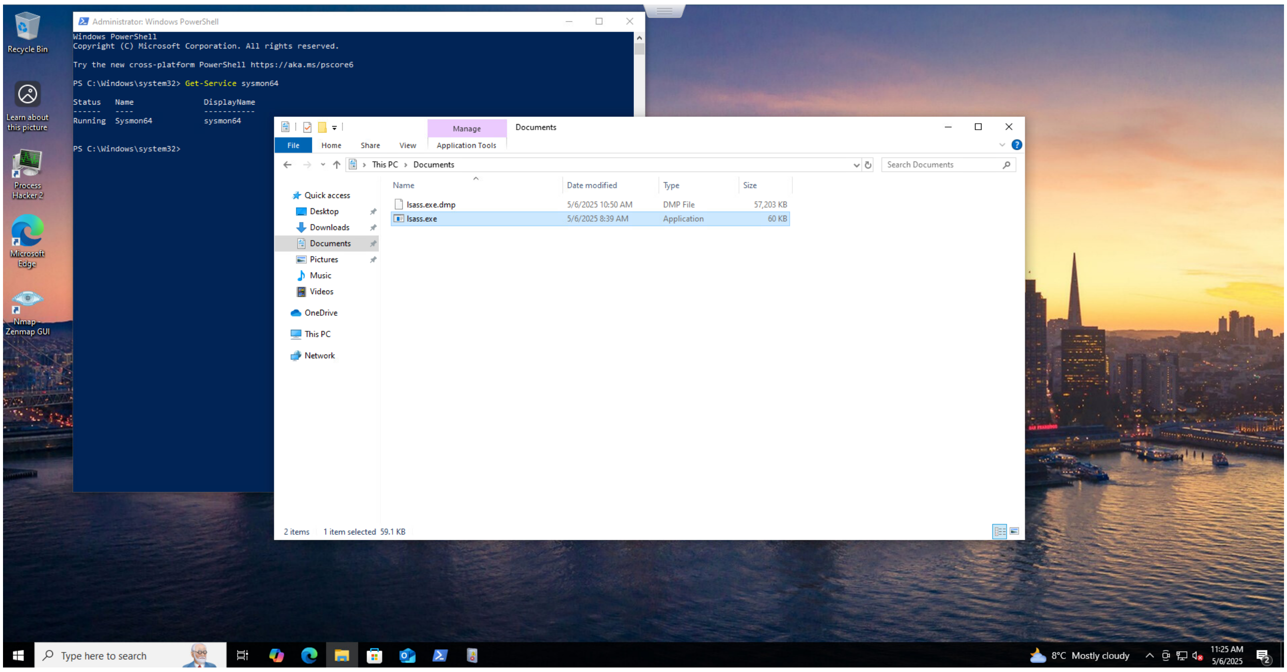
- For a suspicious process like **csrss.exe**, Wazuh should trigger an alert.
- Similarly, on process termination, Wazuh should log an event indicating the process was terminated.

4. Attack Modelling, Analysis and Improvements

4.1 Attack Testing

Description of conducted attacks:

- **Detecting Suspicious Processes:**
  - A **process hacker** was used to simulate the launching of suspicious processes such as **lsass.exe**.
  - Result: Wazuh detected the suspicious process and identified the parent process (`wininit.exe`).



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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Get-Service sysmon64

Status   Name               DisplayName
------   ----               -----------
Running  Sysmon64           sysmon64


PS C:\Windows\system32>
```

This PC › Documents

Name	Date modified	Type	Size
lsass.exe.dmp	5/6/2025 10:50 AM	DMP File	57,203 KB
lsass.exe	5/6/2025 8:39 AM	Application	60 KB

2 items 1 item selected 59.1 KB

- **Detecting Process Creation and Termination Events:**
  - The creation and termination of processes were simulated using **Sysmon**.
  - Result: Wazuh detected the creation and termination events correctly.

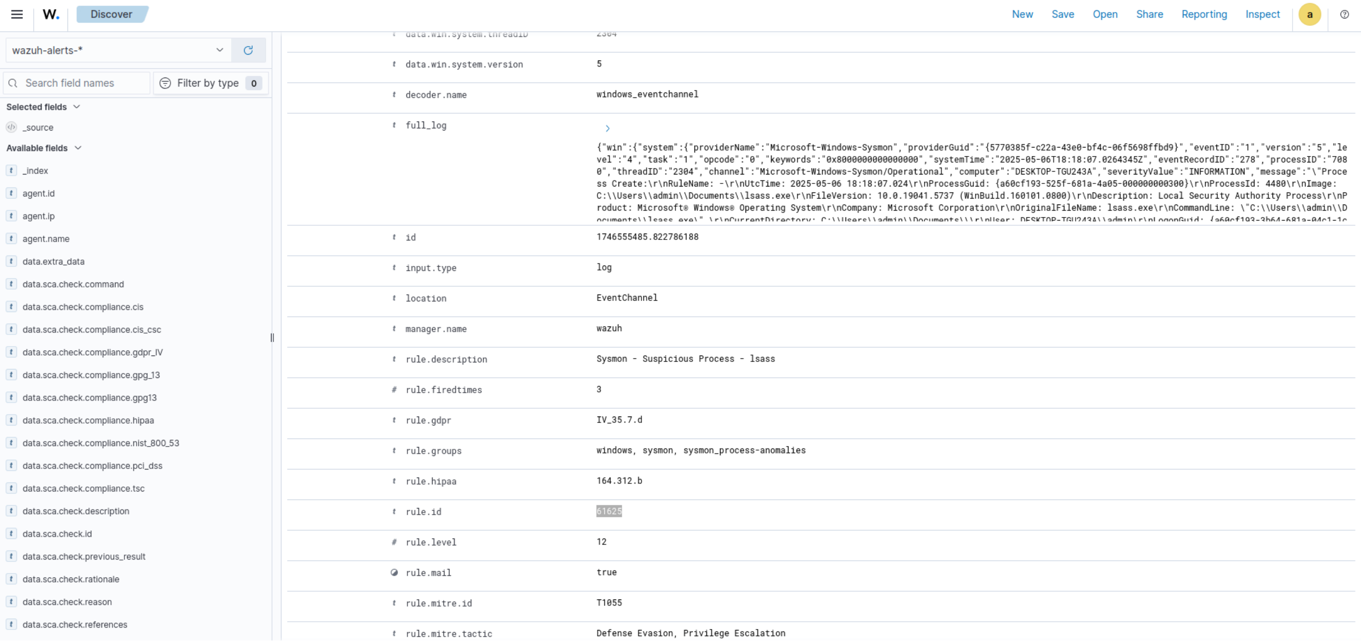
Software used for attacks:

- **Process Hacker** (for simulating process creation)
- **Sysmon** (for event logging)
- **Test files** (for process termination events)

4.2 Wazuh System Response

Screenshots and logs of triggered alerts:

- **Suspicious Process Alert:**



```
data.win.system.threadID    2304
data.win.system.version     5
decoder.name                windows_eventchannel
full_log                    {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-06f5698ffbd9}","eventID":"1","version":"5","le
                            vel":"4","task":"1","opcode":"0","keywords":"0x8000000000000000","systemTime":"2025-05-06T18:18:07.0264345Z","eventRecordID":"278","processID":"708
                            0","threadID":"2304","channel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-TGU243A","severityValue":"INFORMATION","message":"\"Proce
                            ss Create:\r\nRuleName: -\r\nUtcTime: 2025-05-06 18:18:07.024\r\nProcessGuid: {a60cf193-525f-681a-4a05-000000000300}\r\nProcessId: 4480\r\nImage:
                            C:\\Users\\admin\\Documents\\lsass.exe\r\nFileVersion: 10.0.19041.5737 (WinBuild.160101.0800)\r\nDescription: Local Security Authority Process\r\nP
                            roduct: Microsoft® Windows® Operating System\r\nCompany: Microsoft Corporation\r\nOriginalFileName: lsass.exe\r\nCommandLine: \"C:\\Users\\admin\\D
                            ocuments\\lsass.exe\" \r\nCurrentDirectory: C:\\Users\\admin\\Documents\\\r\nUser: DESKTOP-TGU243A\\admin\r\nLogonGuid: {a60cf193-3b64-681a-04c1-1c
id                          1746555485.822786188
input.type                  log
location                    EventChannel
manager.name                wazuh
rule.description            Sysmon - Suspicious Process - lsass
rule.firedtimes             3
rule.gdpr                   IV_35.7.d
rule.groups                 windows, sysmon, sysmon_process-anomalies
rule.hipaa                  164.312.b
rule.id                     61625
rule.level                  12
rule.mail                   true
rule.mitre.id               T1055
rule.mitre.tactic           Defense Evasion, Privilege Escalation
```

W.
Discover
New
Save
Open
Share
Reporting
Inspect
a
wazuh-alerts-*
Search field names
Filter by type 0
Selected fields
_source
Available fields
_index
agent.id
agent.ip
agent.name
data.extra_data
data.sca.check.command
data.sca.check.compliance.cis
data.sca.check.compliance.cis_csc
data.sca.check.compliance.gdpr_IV
data.sca.check.compliance.gpg_13
data.sca.check.compliance.gpg13
data.sca.check.compliance.hipaa
data.sca.check.compliance.nist_800_53
data.sca.check.compliance.pci_dss
data.sca.check.compliance.tsc
data.sca.check.description
data.sca.check.id
data.sca.check.previous_result
data.sca.check.rationale
data.sca.check.reason
data.sca.check.references

Description of Each Alert and Its Significance:

- **Suspicious Process Alert:** This alert indicates that an unauthorized or suspicious process was detected. Wazuh flagged the process and identified the legitimate parent process.

4.3 Recommendations

Based on the test results, the following recommendations are made:

- **Suspicious Process Detection:**
  - Regularly update the list of processes to track and ensure that new threats are detected.
  - Consider adding more specific rules for new suspicious processes that may emerge.
- **Process Creation and Termination Events:**
  - Enable automatic actions based on alert levels (e.g., terminate processes with a high-level alert).
  - Optimize the balance between alert accuracy and system performance.

Conclusion

This section demonstrates how to configure Wazuh to detect suspicious processes, such as **lsass.exe**, and monitor process creation and termination events using **Sysmon**. With these configurations in place, Wazuh can effectively monitor for unusual behavior in the system, providing enhanced security and monitoring capabilities.

---

5. Applications

5.1 Team

- **Alexander Tomashov** - Infrastructure and architecture design
- **Andrey Boronin** - Deployment and configuration of components
- **Ivan Sannikov** - Monitoring, security, and integration setup
- **Bakina Sofia** - Testing, attack modelling, analysis, reporting, and presentation preparation

5.2 Configuration files

Link to the repository with configuration files.

5.3 Screenshots

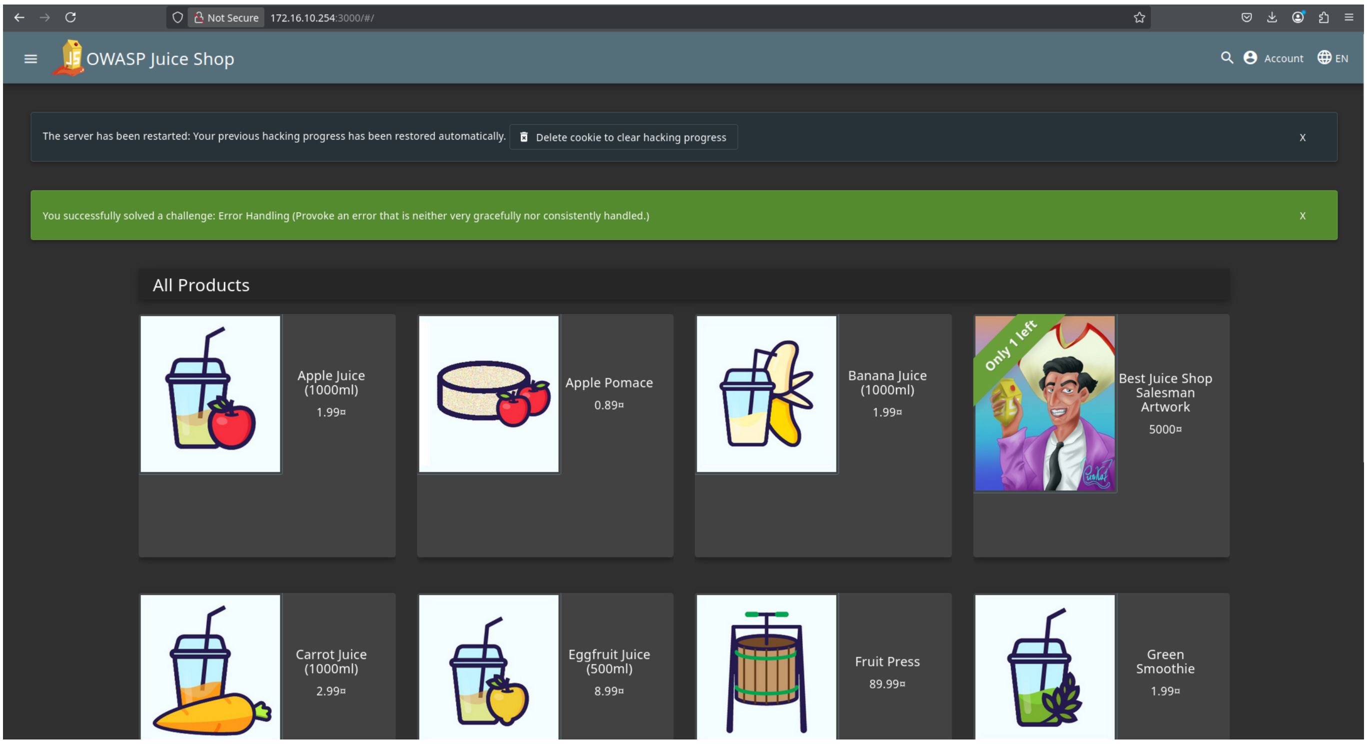
Link to the archive with screenshots of the system in action.

5.4 Video

Link to the demo video of the system.

5.5 Settings that were also made

Juiceshop



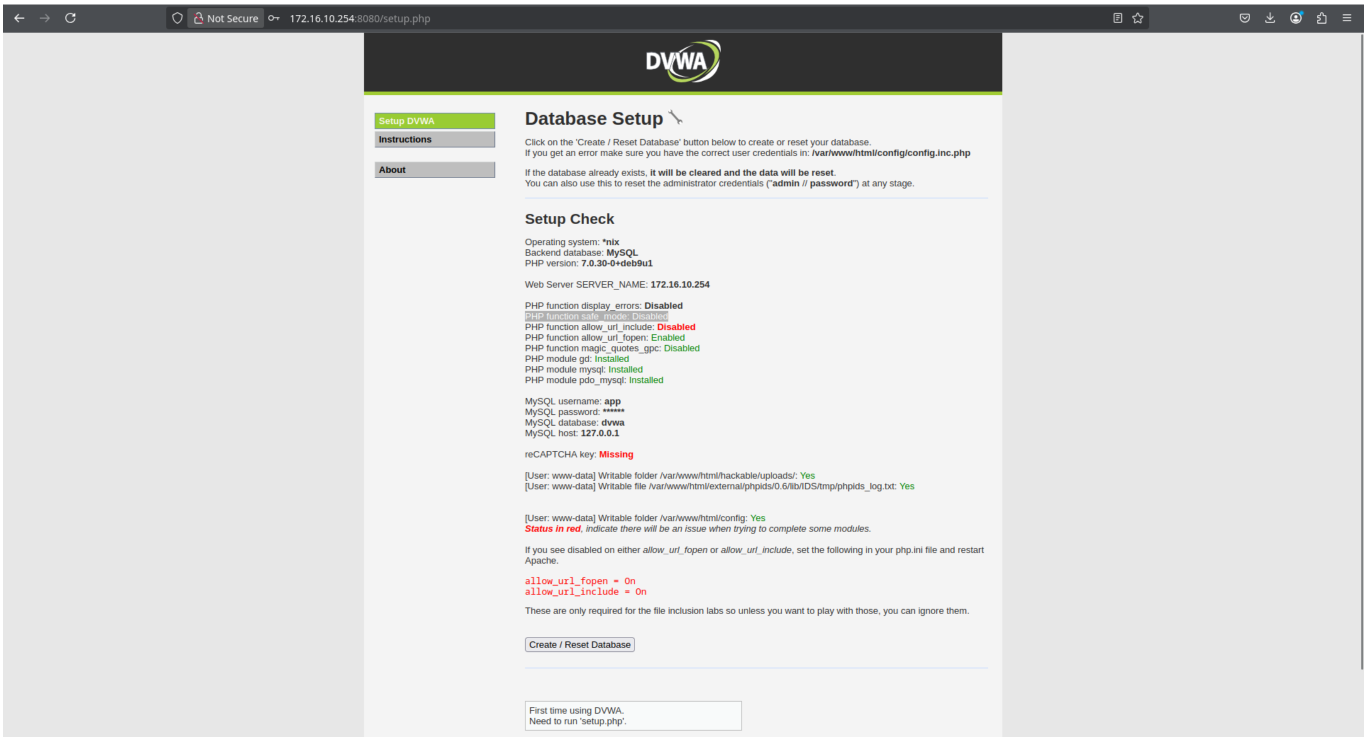
The server has been restarted: Your previous hacking progress has been restored automatically.

Delete cookie to clear hacking progress

You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)

All Products

Dvwa



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: ***nix**
Backend database: **MySQL**
PHP version: **7.0.30-0+deb9u1**

Web Server SERVER_NAME: **172.16.10.254**

PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **app**
MySQL password: **********
MySQL database: **dvwa**
MySQL host: **127.0.0.1**

reCAPTCHA key: **Missing**

[User: www-data] Writable folder /var/www/html/hackable/uploads/: Yes
[User: www-data] Writable file /var/www/html/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes

[User: www-data] Writable folder /var/www/html/config: Yes
Status in red*, indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

First time using DVWA.
Need to run 'setup.php'.