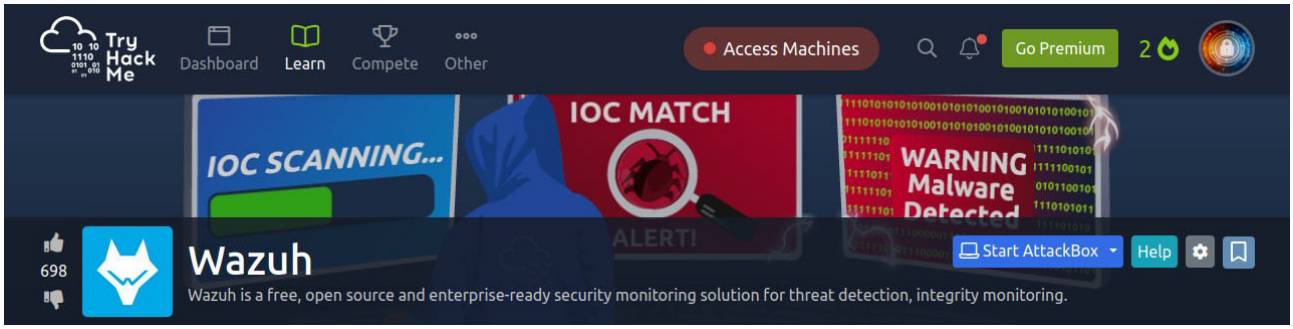
Eric Mwenda

Wazuh

https://tryhackme.com/p/Ericm



First step was to explain what EDR solutions are exactly.

Endpoint detection and response (EDR) are a series of tools and applications that monitor devices for an activity that could indicate a threat or security breach.

These tools and applications have features that include:

- Auditing a device for common vulnerabilities

- Proactively monitoring a device for suspicious activity such as unauthorised logins, brute-force attacks or privilege escalations

- Visualizing complex data and events into neat and trendy graphs

- Recording a device's normal operating behaviour to help with detecting anomalies

Wazuh was created on 2015 and it is an open-source, freely available and extensive EDR solution. It can be used in all scales of environments. Wazuh operates on a management and agent module.

Simply, a device is dedicated to running Wazuh named a manager, where Wazuh operates on a management and agent model where the manager is responsible for managing agents installed on the devices you'd like to monitor

Answer the questions below

When was Wazuh released?

2015

What is the term that Wazuh calls a device that is being monitored for suspicious activity and potential security threats?

Agent

Lastly, what is the term for a device that is responsible for managing these devices?

Manager

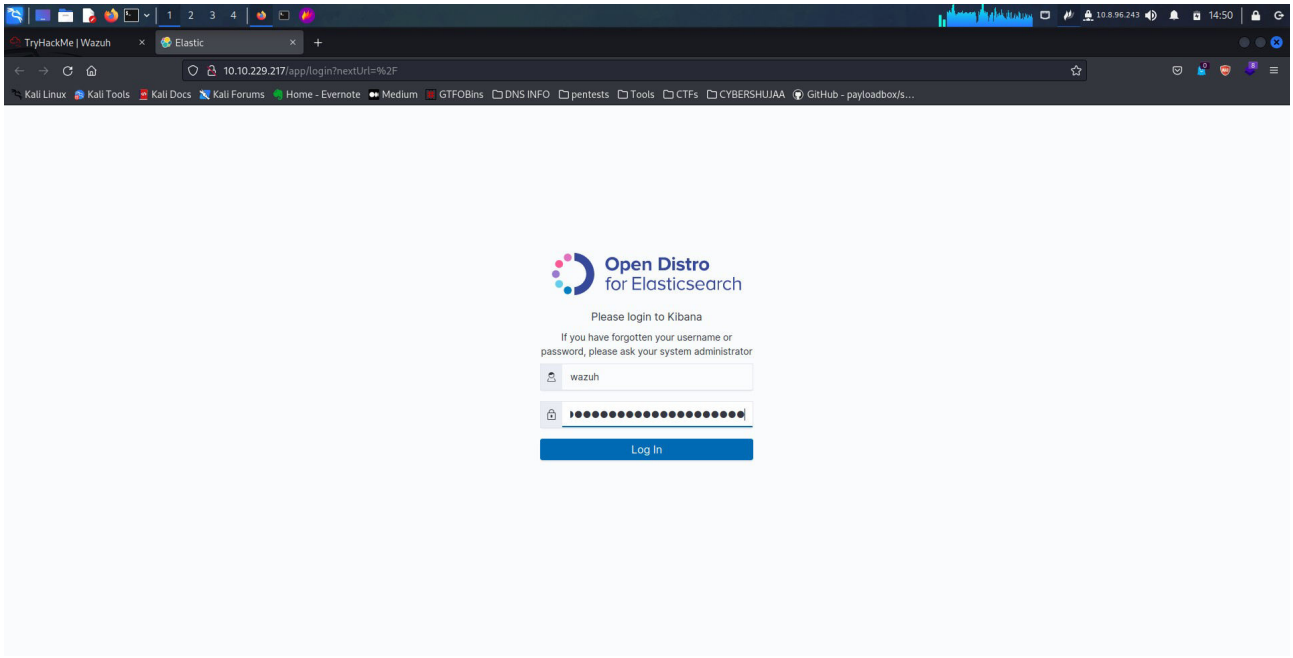
Required: Deploy Wazuh Serve

Next step was to connect to the TryHackMe network and deploy the Wazuh management server attached to the task.

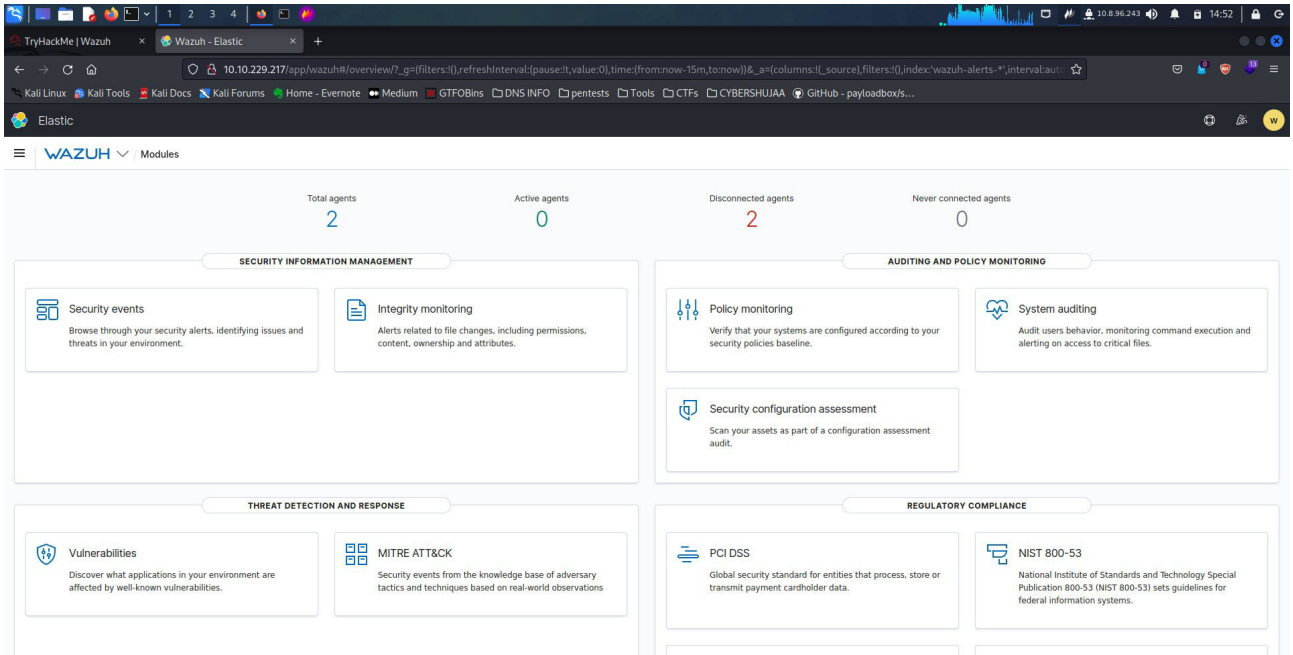
Once it has started, log in using the following credentials:

Username: **wazuh (make sure that this is lowercase!)**

Password: **eYa0M1-hG0e7rjGi-lRB2qGYVoonsG1K**



Am in



Wazuh Agents

Devices that record the events and processes of a system are called agents. Agents monitor the processes and events that take place on the device, such as authentication and user management. Agents will offload these logs to a designated collector for processing, such as Wazuh.

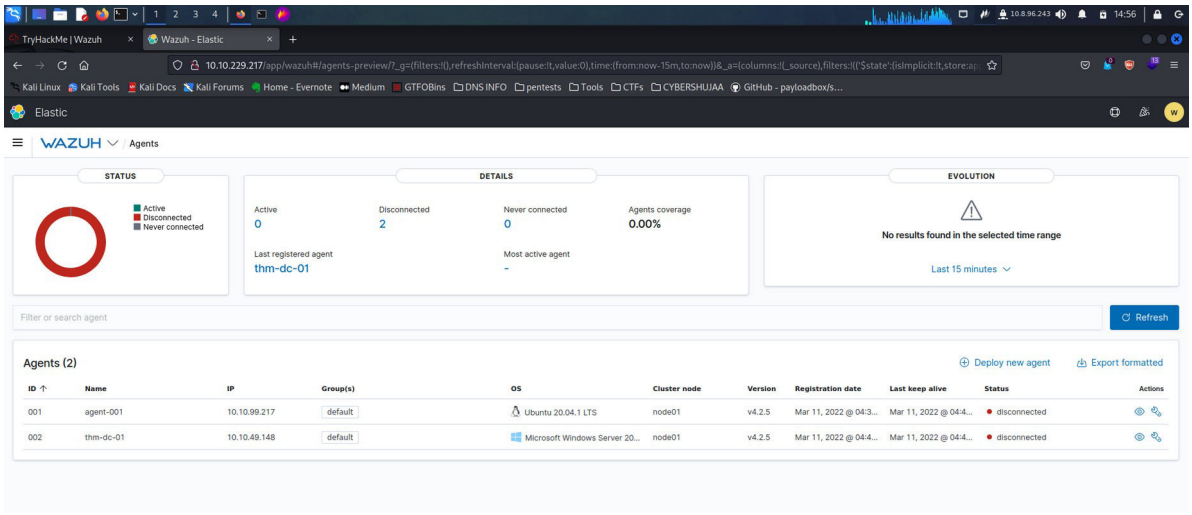
Answer the questions below

Ensure that you are logged in to the Wazuh management server on HTTPS://10.10.229.217

Done

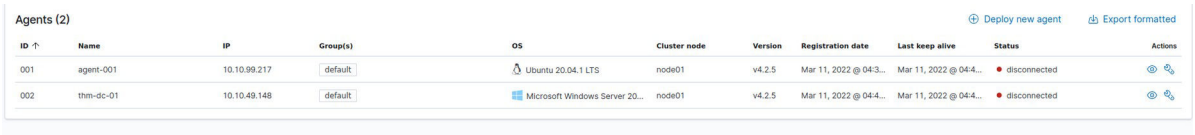
Navigate to the "Agents" tab by pressing Wazuh -> Agents

Done

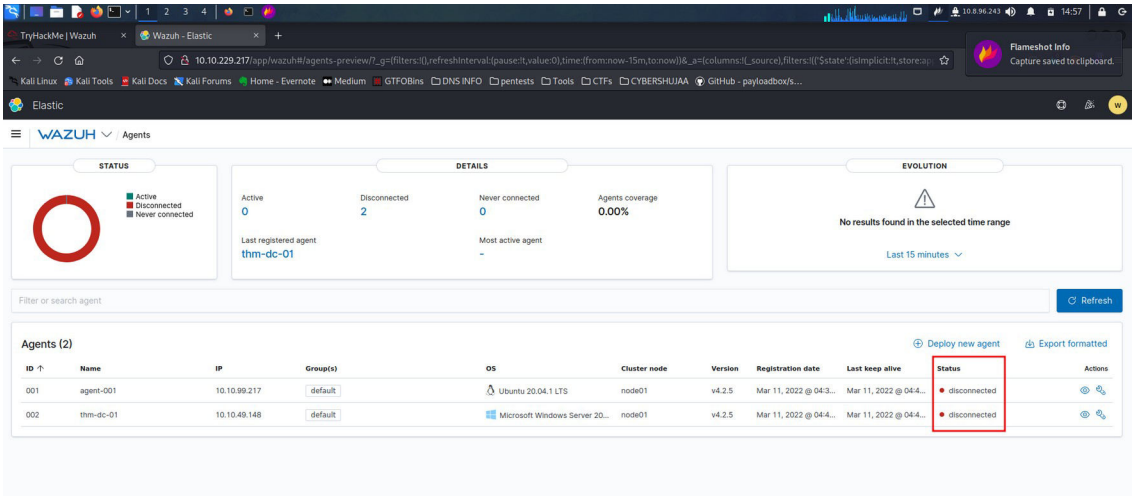


How many agents does this Wazuh management server manage?

2



What are the status of the agents managed by this Wazuh management server? **Disconnected**



Wazuh Vulnerability Assessment & Security Events

Wazuh's Vulnerability Assessment module is a powerful tool that can be used to periodically scan an agent's operating system for installed applications and their version numbers.

Once this information has been gathered, it is sent back to the Wazuh server and compared against a database of CVEs to discover potential vulnerabilities.

The vulnerability scanner module will perform a full scan when the Wazuh agent is first installed on a device and must be configured to run at a set interval then after (by default, this is set to 5 minute intervals when enabled) like so:

```
<vulnerability-detector>
  <enabled>no</enabled>
  <interval>5m</interval>
  <ignore_time>6h</ignore_time>
  <run_on_start>yes</run_on_start>
```

Answer the questions below

Ensure that you are logged in to the Wazuh management server on HTTPS://10.10.229.217

Done

Navigate to the Agents tab by pressing Wazuh -> Agents like so

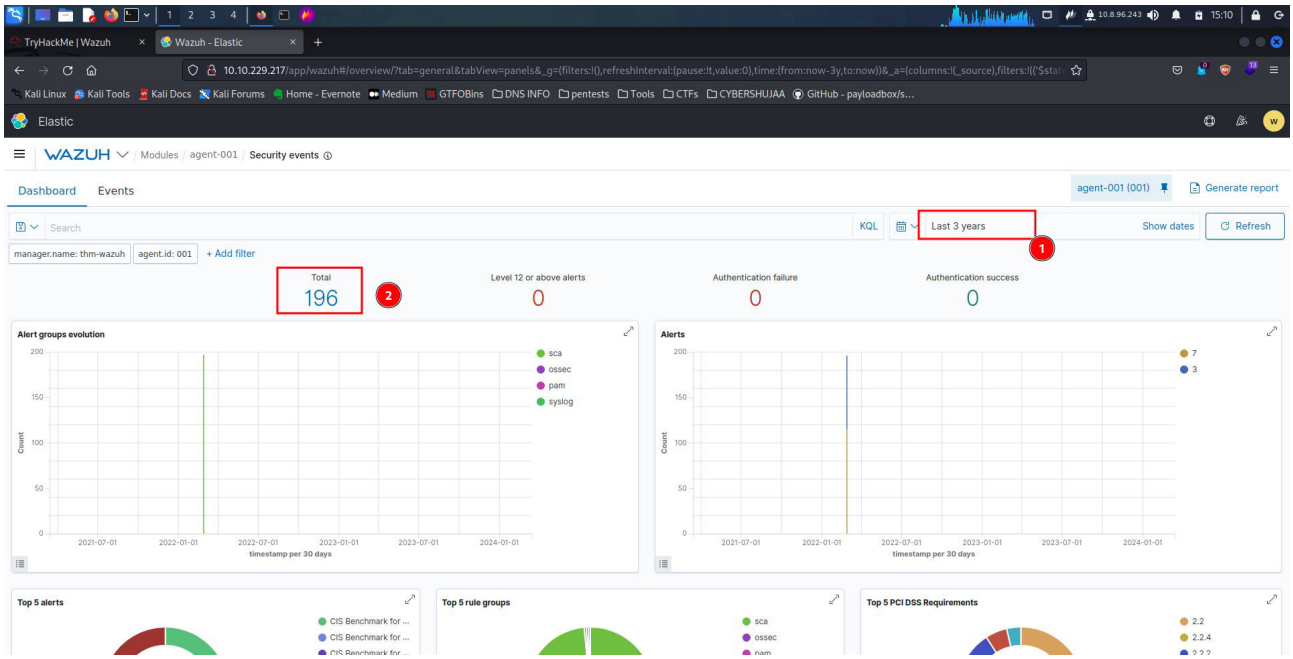
Done

Select the agent named "AGENT-001"

Done

How many "Security Event" alerts have been generated by the agent "AGENT-001"?

Results:



Note: You will need to make sure that your time range includes the 11th of March 2022

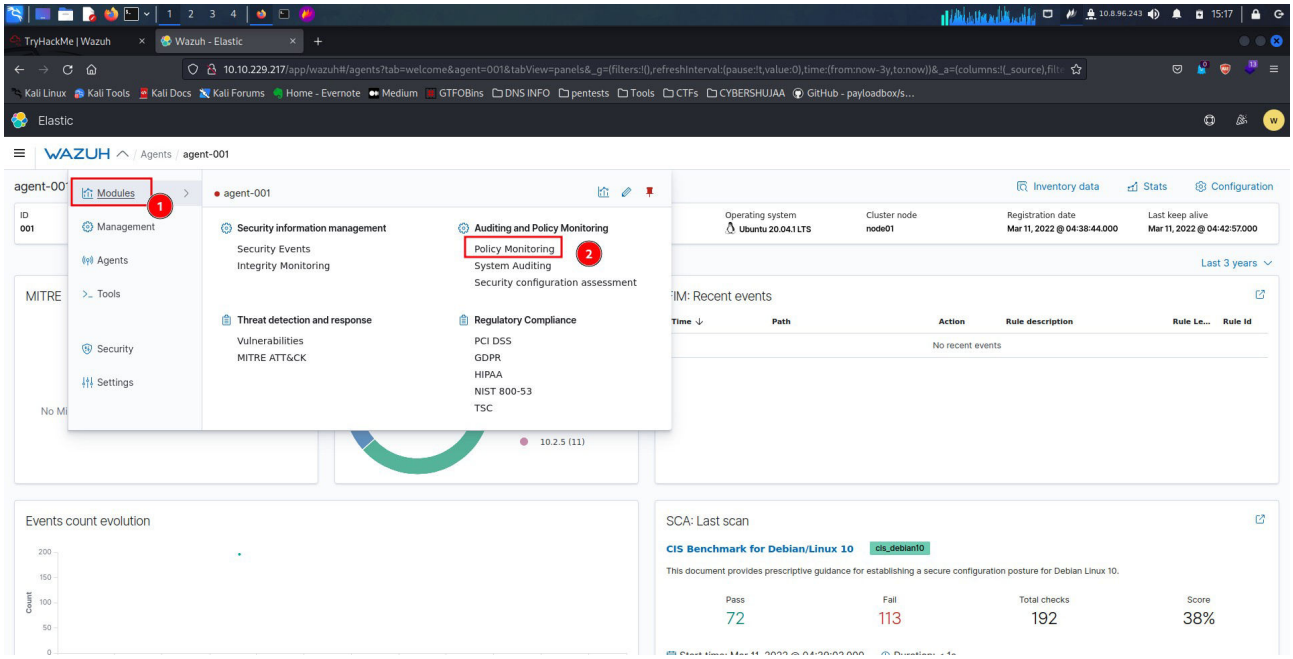
To get the number of events I had to turn back time since the machine was added, that is 3 years back.

Ans: 196

Wazuh Policy Auditing

Wazuh is capable of auditing and monitoring an agent's configuration whilst proactively recording event logs. When the Wazuh agent is installed, an audit is performed where a metric is given using multiple frameworks and legislations such as NIST, MITRE and GDPR.

To do so we click Modules > Policy Monitoring



Monitoring Logons with Wazuh

Wazuh's security event monitor is capable to actively record both successful and unsuccessful authentication attempts.

While using wazuh it can be set to send an alert when someone tries to log onto the agent with wrong credentials and store this information on a specific file.

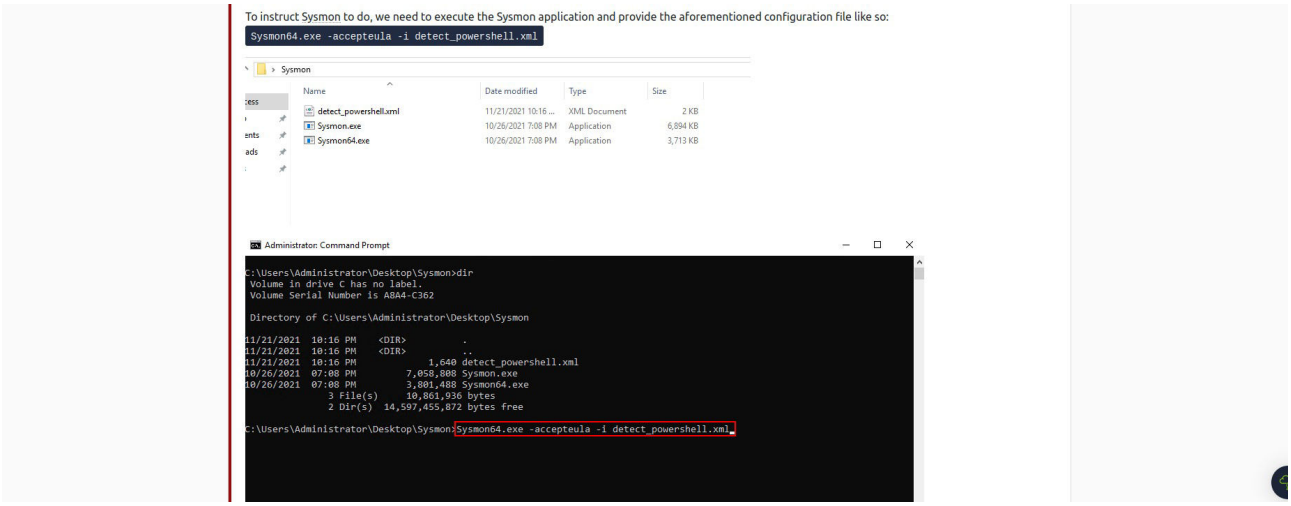
Collecting Windows Logs with Wazuh

All sorts of actions and events are captured and recorded on a Windows operating system. This includes authentication attempts, networking connections, files that were accessed, and the behaviours of applications and services. This information is stored in the Windows event log using a tool called Sysmon.

We can use the Wazuh agent to aggregate these events recorded by Sysmon for processing to the Wazuh manager. Now, we will need to configure both the Wazuh agent and the Sysmon application. Sysmon uses rules that are made in XML formatting to be triggered.

we can configure Sysmon to monitor for the event of the powershell.exe process starting using command:-

Sysmon64.exe -accepteula -i detect_powershell.xml



We can verify that Sysmon has accepted our configuration file by navigating to the Event Viewer and searching for the “Sysmon”

After this is done, we need to configure the Wazuh agent on this Window Server to instruct it to send these events to the Wazuh management server. To do so, we need to open the Wazuh agent file located at: **C:\Program Files (x86)\ossec-agent\ossec.conf**

Once you open the file on the not pad you add this snippet.

<localfile>

<location>Microsoft-Windows-Sysmon/Operational</location>

<log_format>eventchannel</log_format>

</localfile>

```
    <events_per_second>500</events_per_second>
  </client_buffer>

  <!-- Log analysis -->
  <localfile>
    <location>Application</location>
    <log_format>eventchannel</log_format>
  </localfile>

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


  <localfile>
    <location>Security</location>
    <log_format>eventchannel</log_format>
    <query>Event/System[EventID != 5145 and EventID != 5156 and Eve
      EventID != 4656 and EventID != 4658 and EventID != 4663 and E
      EventID != 4670 and EventID != 4690 and EventID != 4703 and E
      EventID != 5152 and EventID != 5157]</query>
  </localfile>

  <localfile>
```

Next is to restart Wazuh agent to be sure changes have been made.

Once this is done, we need to tell the Wazuh Management server to add Sysmon as a rule to visualize these events. This can be done by adding an XML file to the local rules located in **/var/ossec/etc/rules/local_rules.xml**

To do so we add this statements to the file:

<group name="sysmon,">

<rule id="255000" level="12">

<if_group>sysmon_event1</if_group>

<field name="sysmon.image">\\powershell.exe|\\.ps1|\\.ps2</field>

<description>Sysmon - Event 1: Bad exe: $(sysmon.image)</description>

<group>sysmon_event1,powershell_execution,</group>

</rule>

</group>

Answer the questions below

What is the name of the tool that we can use to monitor system events?

Sysmon

What standard application on Windows do these system events get recorded to?

Event Viewer

Collecting Linux Logs with Wazuh

Capturing logs from a Linux agent is a simple process similar to capturing events from a Windows agent. We will be using Wazuh's log collector service to create an entry on the agent to instruct what logs should be sent to the Wazuh management server.

Wazuh comes with many rules that enable Wazuh to analyze log files and can be found in **/var/ossec/ruleset/rules**. Some common applications include:

- Docker

- FTP

- WordPress

- SQL Server

- MongoDB

- Firewalld

And many, many more (approximately 900), However, you can always make your own rules.

An Example of Wazuh digesting Apache2 logs using the **0250-apache_rules.xml ruleset.**

This ruleset can analyze apache2 logs for warnings and error messages like so: We will need to insert this into the Wazuh's agent that is sending logs to the Wazuh management servers configuration file located in **/var/ossec/etc/ossec.conf:**

<!-- Apache2 Log Analysis -->

<localfile>

<location>/var/log/example.log</location>

<log_format>syslog</log_format>

</localfile>

After this we need to restart the Linux agent running the Apache2 service.

Answer the questions below

What is the full file path to the rules located on a Wazuh management server?

Ans: /var/ossec/ruleset/rules

Auditing Commands on Linux with Wazuh

Wazuh utilises the auditd package that can be installed on Wazuh agents running on Debian/Ubuntu and CentOS operating systems.

Auditd monitors the system for certain actions and events and will write this to a log file.

Answer the questions below

What application do we use on Linux to monitor events such as command execution?

Auditd

What is the full path & filename for where the aforementioned application stores rules?

Ans: /etc/audit/rules.d/audit.rules

Wazuh API

The Wazuh management server features a rich and extensive API to allow the Wazuh management server to be interacted with using the command line. Because the Wazuh management server requires authentication, we must first authenticate our client.

Using a Linux machine with the curl tool installed we can interact with the Wazuh management server API. First, we will need to authenticate ourselves by providing a valid set of credentials to the authentication endpoint.

First is to get a token using the JWT tool

snippet below:

(replacing *WAZUH_MANAGEMENT_SERVER_IP* with the IP address of the Wazuh management server (i.e. 10.10.229.217):

```
TOKEN=$(curl -u : -k -X GET "https://WAZUH_MANAGEMENT_SERVER_IP:55000/security
/user/authenticate?raw=true")
```

Let's confirm that we have authenticated okay and have been given a token by the Wazuh management server:

```
curl -k -X GET "https://10.10.229.217:55000/" -H "Authorization: Bearer $TOKEN"
```

We can use the standard HTTP request methods such as GET/POST/PUT/DELETE by providing the relevant option after a -X i.e. -X GET

Using Wazuh's API Console

Wazuh has a powerful, integrated API console within the Wazuh website to query management servers and agents. Whilst it is not as extensive as using your own environment (where you can create and run scripts using python, for example), it is convenient.

To find this API console, we need to open the "Tools" category within the Wazuh heading at the top:

Answer the questions below

What is the name of the standard Linux tool that we can use to make requests to the Wazuh management server?

Curl

What HTTP method would we use to retrieve information for a Wazuh management server API?

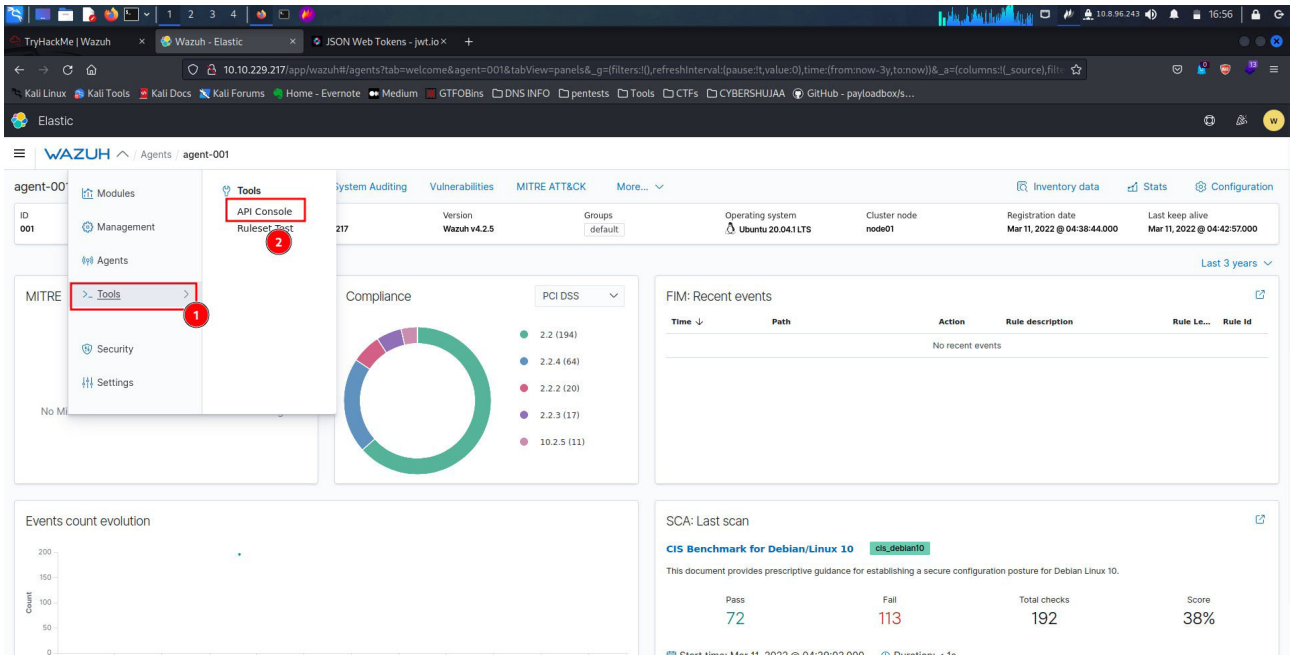
Get

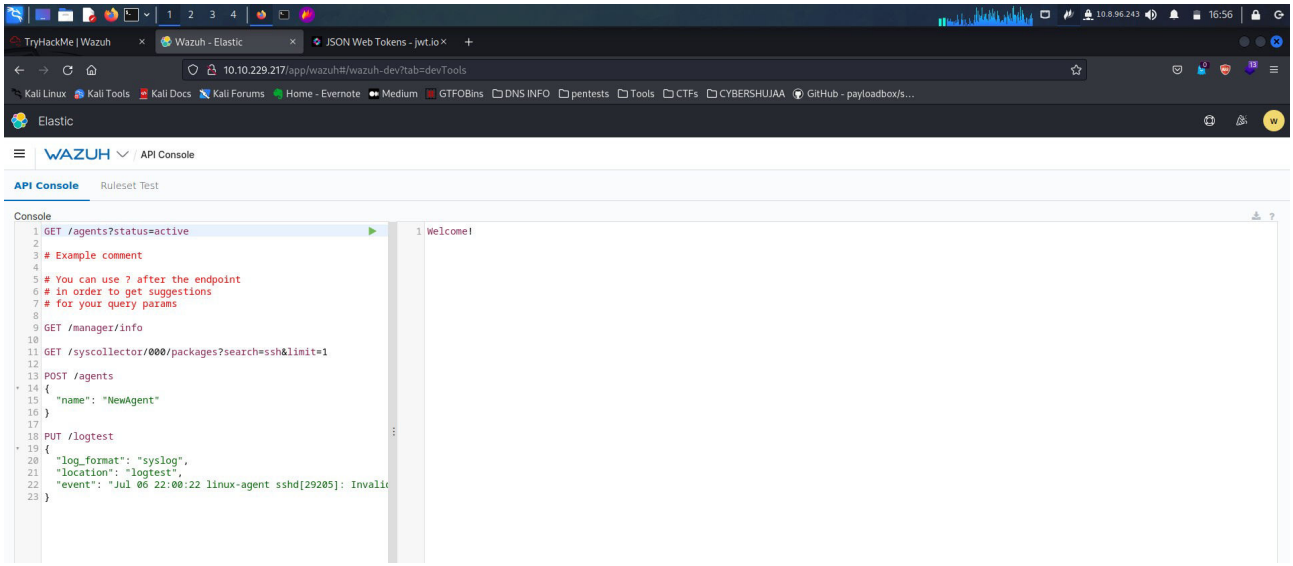
What HTTP method would we use to perform an action on a Wazuh management server API?

Put

Navigate to Wazuh's API console.

Done



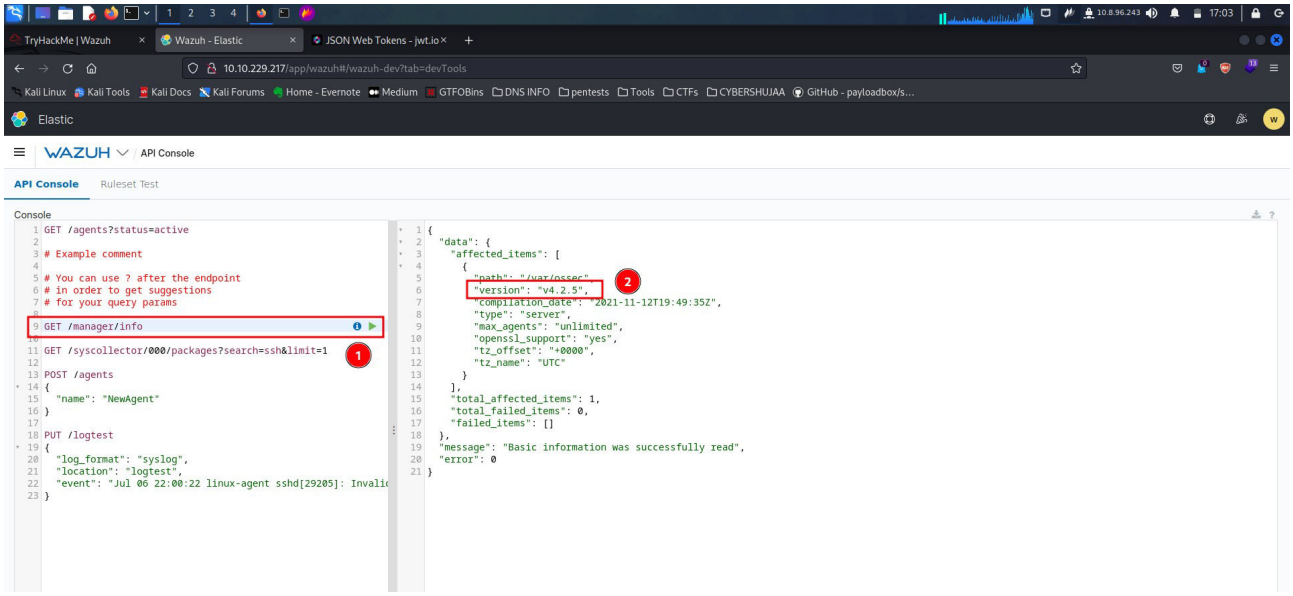


Use the API console to find the Wazuh server's version.

Note: You will need to add the "v" prefix to the number for this answer. For example v1.2.3

Ans: v4.2.5

To execute a line of code, we click on the line with the code you want to execute and a play button should appear. After clicking a few I was able to find the version number.



Generating Reports with Wazuh

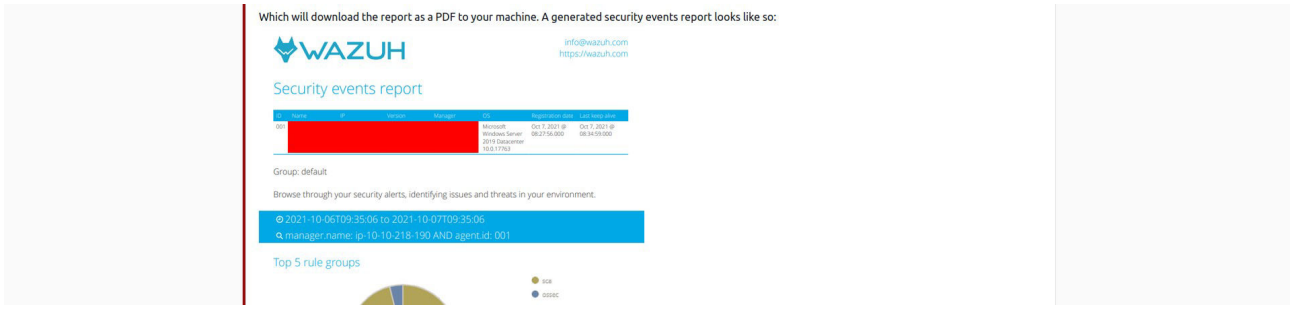
Wazuh features a reporting module that allows you to view a summarised breakdown of events that have occurred on an agent.

First, we will need to select a view to generate reports from. In this example, I want to generate a report of the security events in the last 24 hours. To do so, I will need to open the view: 1. Modules -> 2. Security Events

The report may take between a couple of seconds to a few minutes to generate (depending on the amount of data needed to be processed). After allowing some time, we will navigate to the report overview dashboard within Wazuh.

First, press on the "Wazuh" heading at the top of the screen and select "Management", and then click on the "Reporting" text located under the "Status and Reports" sub-heading:

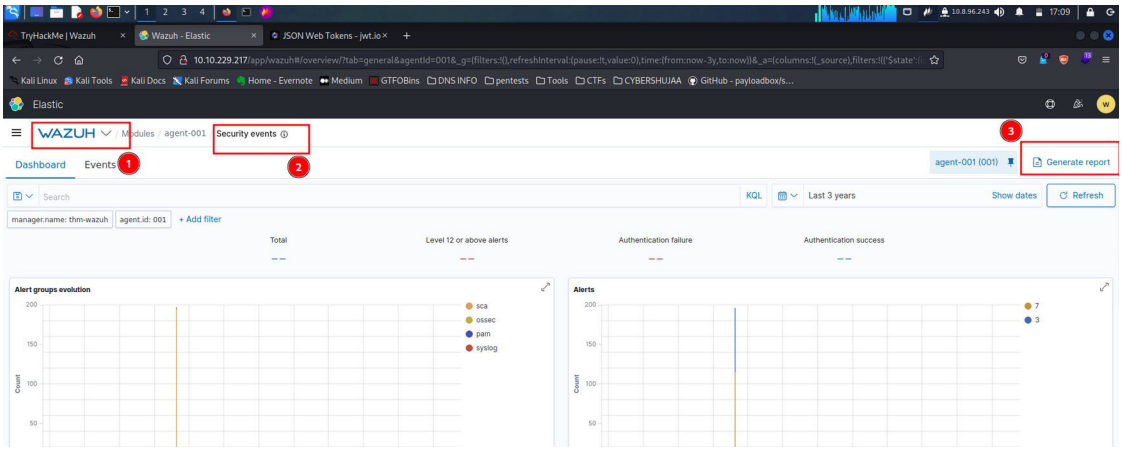
The report overview dashboard lists all generated reports. To download a report, press the save icon on the right of the report located under the "Actions" heading, which downloads the report as a PDF to your machine.



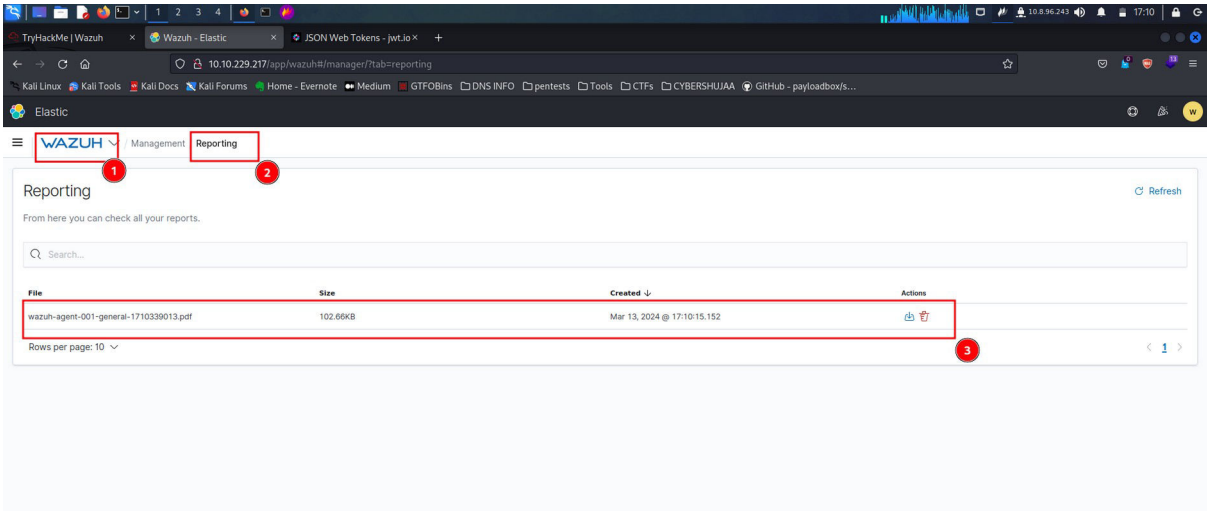
Answer the questions below

Use Wazuh's "Report" feature to generate a report of an agent.

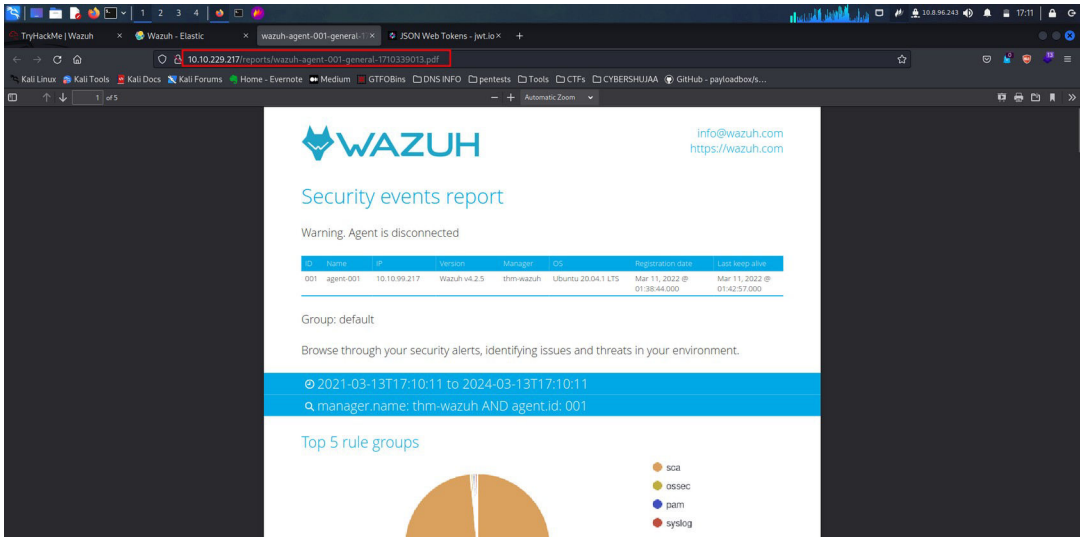
Done



Navigate to the Wazuh "Report" dashboard



Downloading



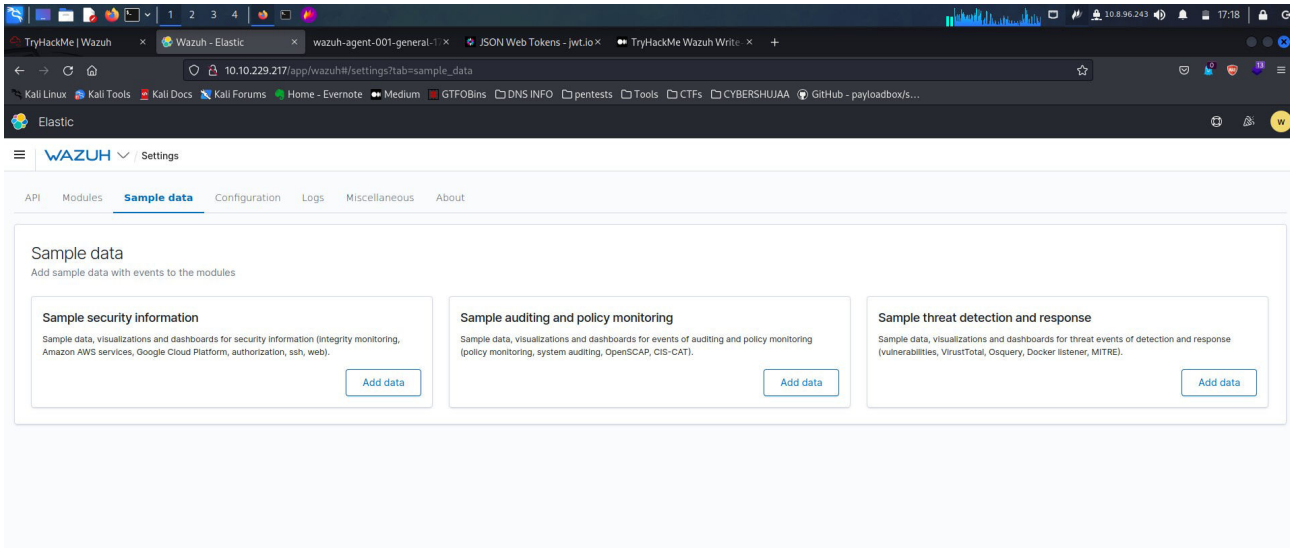
Analyse the report. What is the name of the agent that has generated the most alerts?

Ans: agent-001

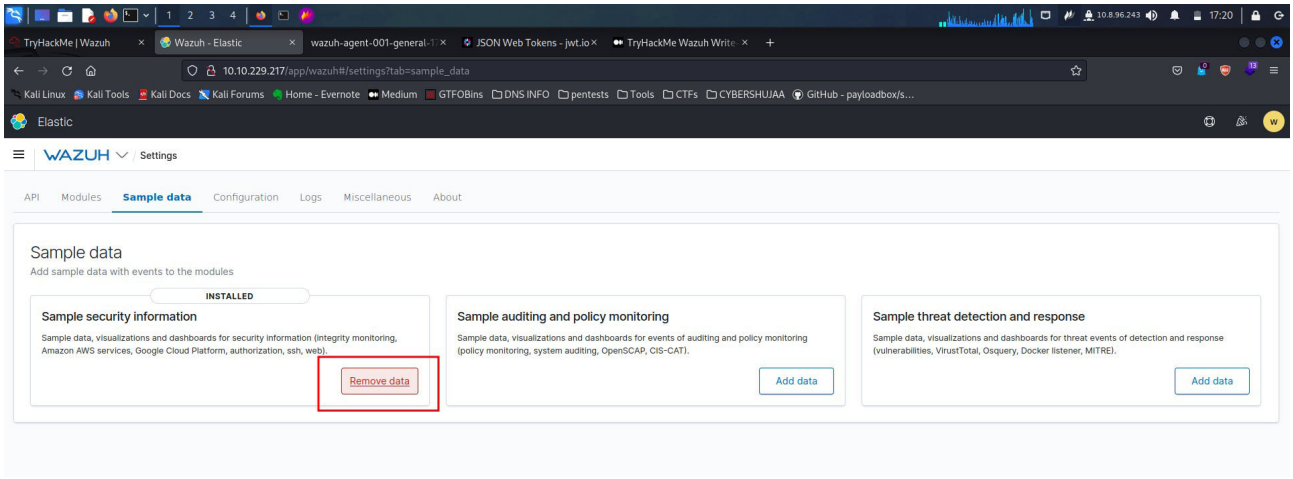
Loading Sample Data

The Wazuh management server comes with sample data bundled with the installation that can be loaded at your convenience. I have not enabled this by default to improve the performance of the server. However, if you wish to import much more data to showcase the extensibility of Wazuh further, follow the steps below. Navigate to the module to load the sample data:

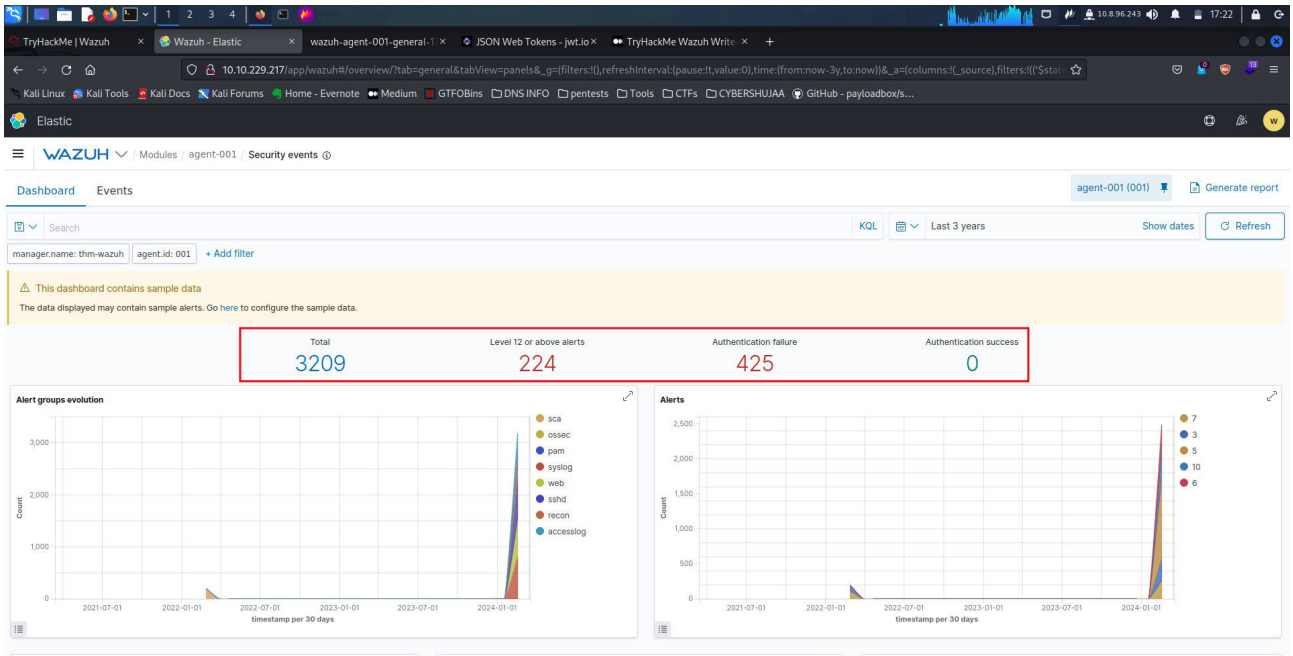
1. Open the "Wazuh" tab in the heading.
2. Highlight over "Settings".
3. Select the "Sample Data" heading.
4. Press the "Add Data" button on the respective three cards to import the data.



The data will have successfully imported when the button on the card says "Remove data"



Return to the Wazuh dashboard to see the newly imported data. we can now see that the "Security Events" module has a tonne more data for us to explore.



The absolute minimum required to show the sample will need to be Last 7 days+ and refresh the dashboard for this to apply.

Conclusion.

In my conclusion this room has introduced me to a new tool that I was not quite open to what it entails that is the Wazuh tool which is an open-source security information and event management (SIEM) tool designed to provide intrusion detection, vulnerability detection and log analysis on a variety of platforms. Wazuh helps organizations monitor and analyze security events in real-time, enabling them to detect and respond to potential threats.

The key features of Wazuh include log analysis, intrusion detection, vulnerability detection and threat intelligence. It can collect and analyze data from various sources, such as logs, network traffic, and endpoint data, to identify security incidents and potential weaknesses in the infrastructure.

Wazuh also offers centralized management through a web-based interface, making it easier for security teams to monitor and manage their security posture. The tool is highly extensible and can be integrated with other security solutions, making it a versatile choice for organizations looking to enhance their Cybersecurity capabilities.

With the basics that I have learnt from this room am quite confident I am well able to work around this tool.

Thank You.