The final room before we head over to the SIEM rooms. I've already done the Splunk rooms so I won't have a write-up for those. I remember that I didn't struggle too much in them though. I just did a lot of clicking around when I found something interesting.

Task 1 Introduction

1: When was Wazuh released?

Found in the introduction.

Answer: 2015

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

This was in the reading. It's the relationship between this and manager.

Answer: Agent

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

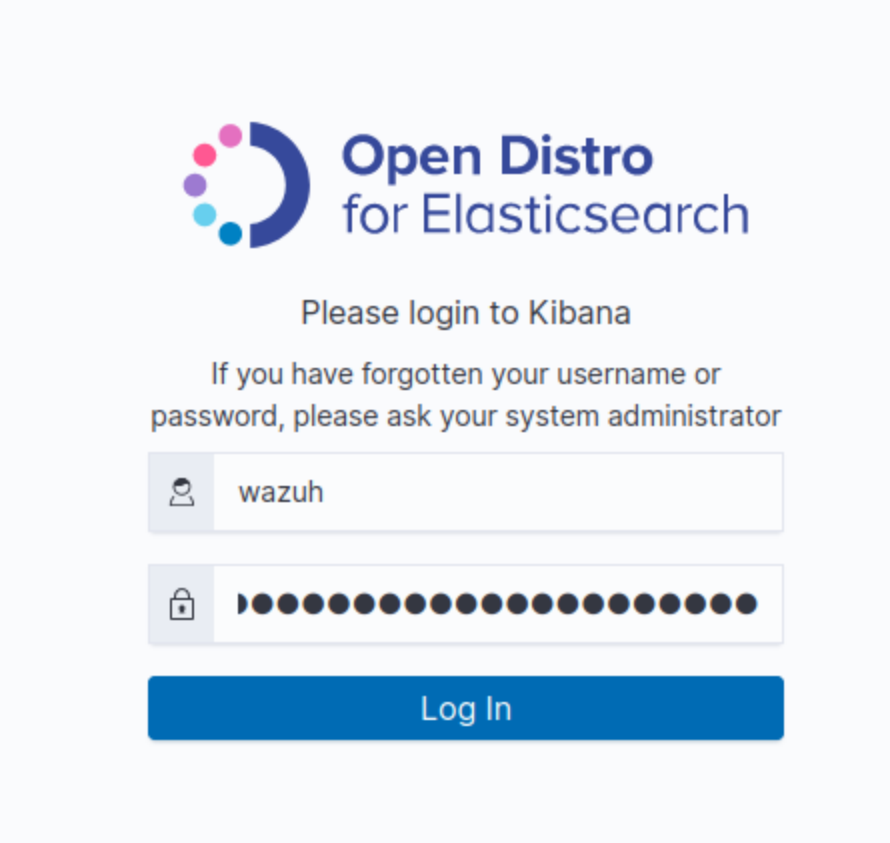
I wasn't able to really find it in the readings so I checked the hint.

Answer: Manager

Task 2 Required: Deploy Wazuh Server

While I can't RDP here, it said to connect to TryHackMe's network then type the IP address. If you don't know how to, my RDP guide will at least tell you how to get your open vpn profile and get on TryHackMe's network.

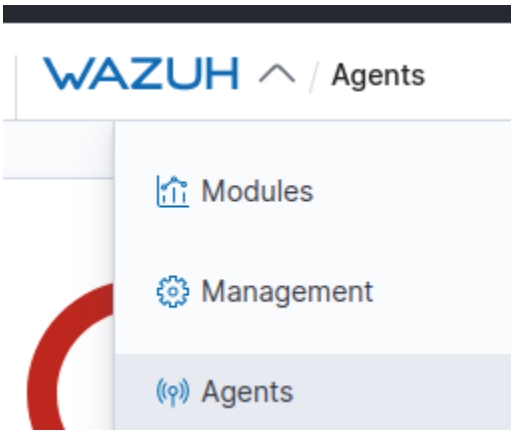
Once you get in the network, open your virtual machine's browser and type in the IP address. It should be listed in the question for task 2. The IP is different every time you start it up. Then enter the credentials obtained from the reading.



Task 3 Wazuh Agents

1: How many agents does this Wazuh management server manage?

We can find this by clicking on the Wazuh icon on the top left and then clicking on “Agents.”



You should be able to see a list of agents attached to this manager.

Answer: 2

2: What are the status of the agents managed by this Wazuh management server?

On the screenshot above, look to the right to see the status.

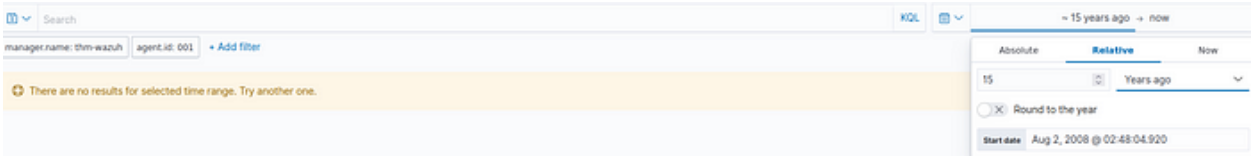
Answer: disconnected

Task 4 Wazuh Vulnerability Assessment & Security Events

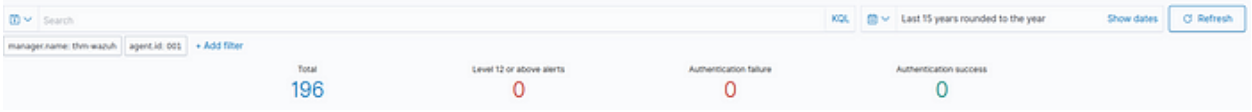
1: How many “Security Event” alerts have been generated by the agent “AGENT-001”?

First, we will navigate to the agent page again. This time, we will click on the agent named “agent-001.” Then we will click on “Security events” at the top left.

Next, we will be presented with a search bar. On the right side of it, we will edit the time. I simply changed it to “Years ago” instead.



After changing it and updating it, it should display the security events alert.



Answer: 196

Task 7 Collecting Windows Logs with Wazuh

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

From the reading, Sysmon is used.

Answer: Sysmon

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

From the reading, and the Sysmon room we did, you can find these events in Event Viewer.

Answer: Event Viewer.

Task 8 Collecting Linux Logs with Wazuh

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

This one can be found within the reading.

Answer: /var/ossec/ruleset/rules

Task 9 Auditing Commands on Linux with Wazuh

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

This can be found in the reading.

Answer: Auditd

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

This can be found in the reading.

Answer: /etc/audit/rules.d/audit.rules

Task 10 Wazuh API

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

This is found in the reading, near the beginning.

Answer: curl

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

I already knew this, but I checked and it is also found in the reading.

Answer: GET

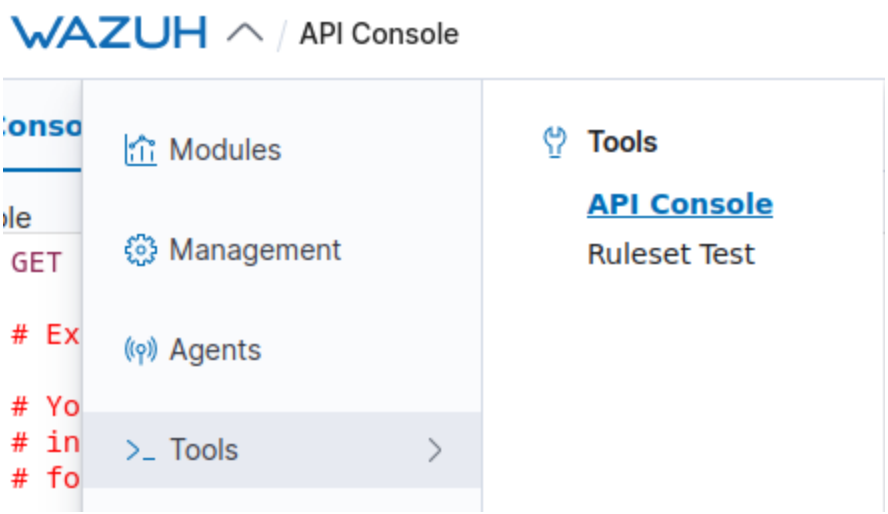
3: What HTTP method would we use to perform an action on a Wazuh management server API?

This one I did not know but it is found in the reading.

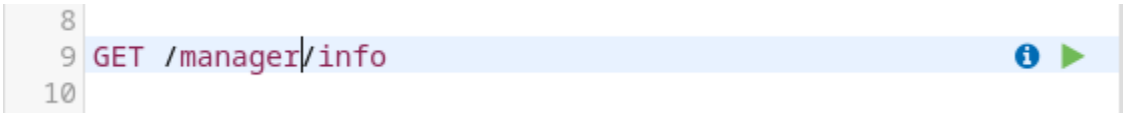
Answer: PUT

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

First, we need to get to the API Console. This can be done by going to the top left and clicking on the Wazuh icon, clicking on tools, and then clicking on API Console.



After that, we are presented with some queries already! To execute a line of code, we click on the line with the code you want to execute and a play button should appear.



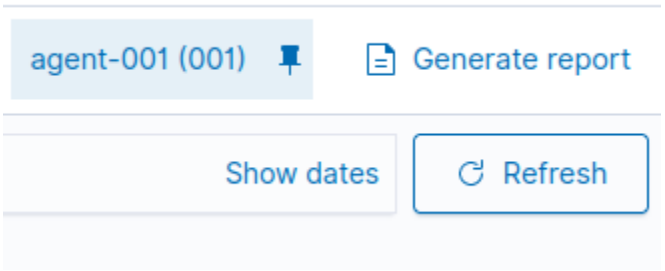
Clicking play will execute the command. Then we just look at the output. I clicked through all of them to find the server information.

Answer: v4.2.5

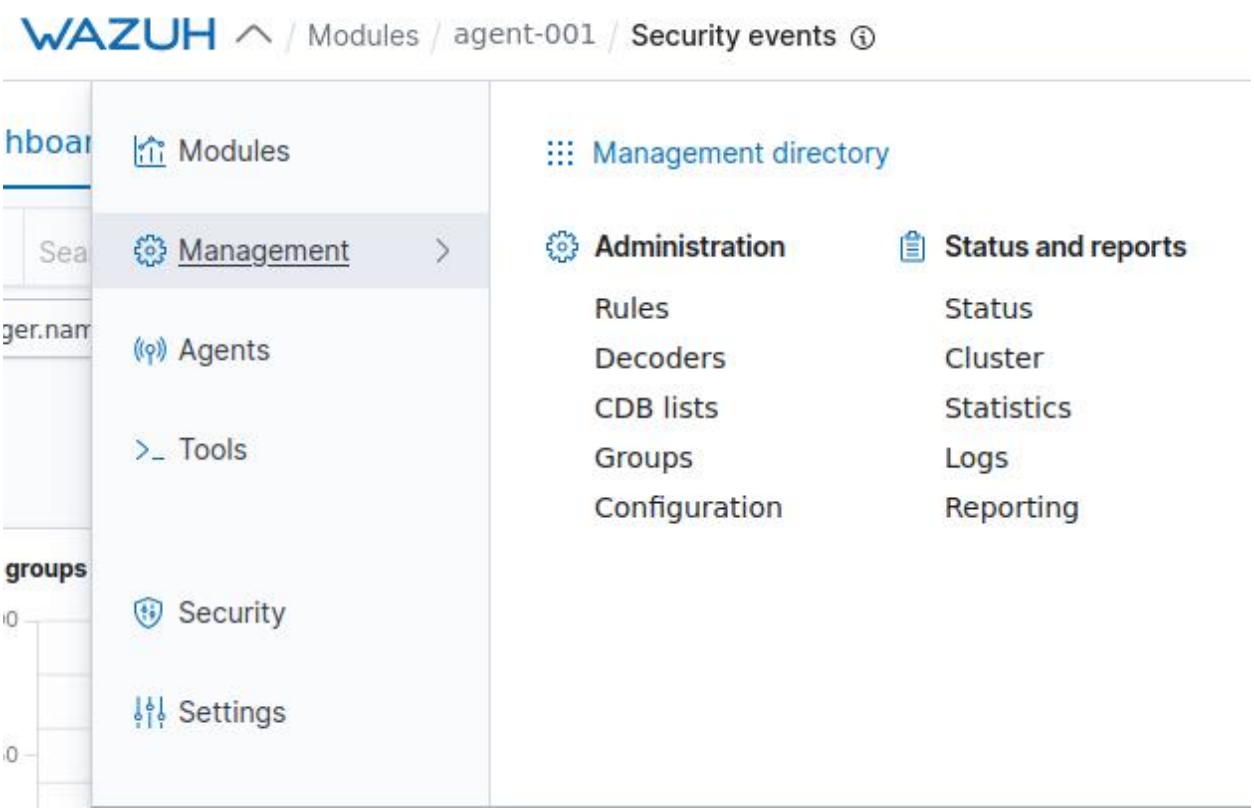
Task 11 Generating Reports with Wazuh

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

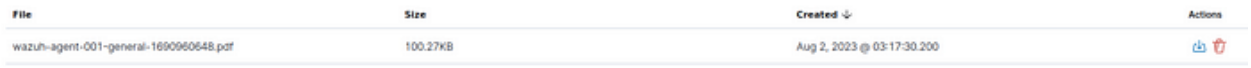
First we need to generate a report. We will go back to the Security Events section. Click on the Wazuh logo on the top left, then click Modules, then click Security Event. On this page, we generate the report by clicking on “Generate report” on the top right.



Now that we generated the report, we will download the file to view it. We do this by going to the Wazuh logo again, then to Management, then finally Reporting.



When we find the report we want, we go to the Actions column and click either download or delete.



Since we know we only have one agent, we already know the answer of the name of the agent that generated the most alert. We found the names back in Task 4.

Answer: agent-001

Thoughts:

Wow. That was another fun room. I suppose I think fun rooms are easy rooms. I did enjoy it because Wazuh seemed like an extensive EDR and also a SIEM together. I did enjoy how easy to use it was. I never heard of Wazuh but I'm glad I was exposed to it!