Wazuh

Introduction

Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring.

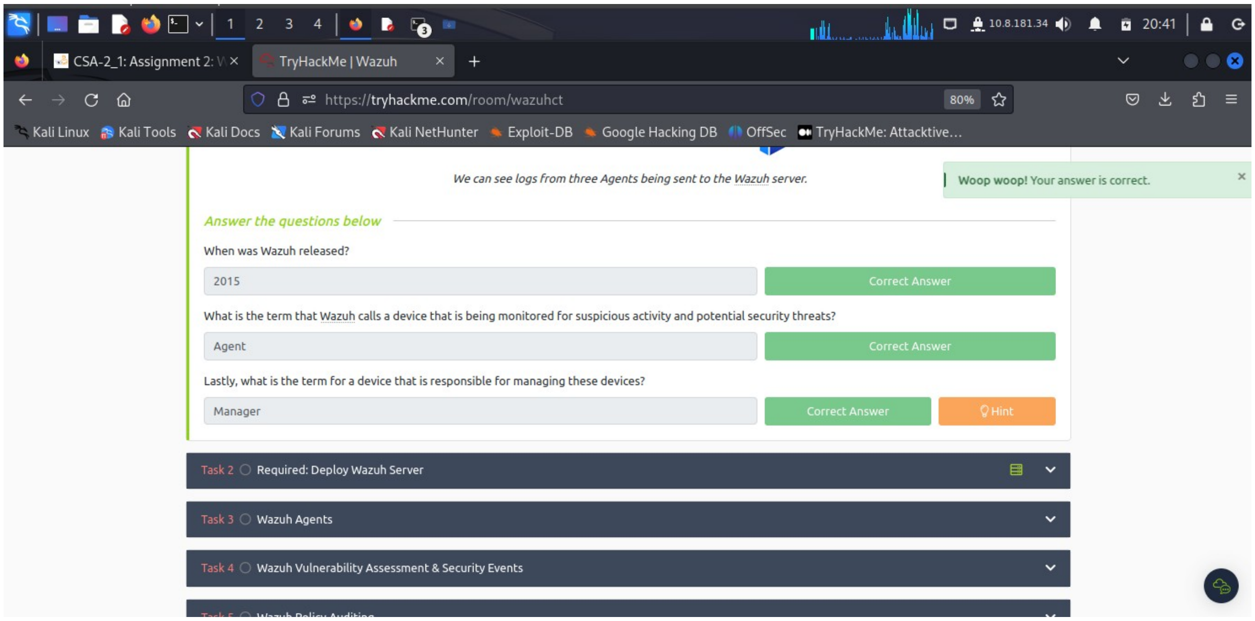
Activities

Task 1: Introduction

Endpoint detection and response (EDR) is a series of tools that monitor devices for activity that could indicate a threat.

The 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
- Visualising complex data and events into neat and trendy graphs
- Recording a device's normal operating behaviour to help with detecting anomalies



We can see logs from three Agents being sent to the Wazuh server.

Woop woop! Your answer is correct.

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

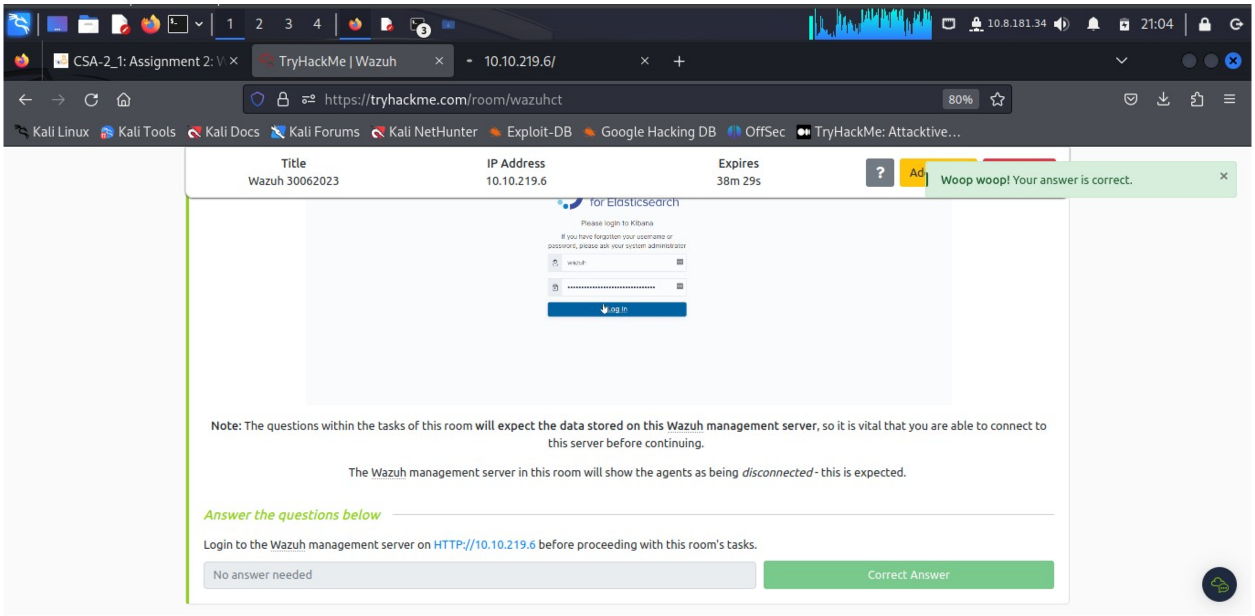
Lastly, what is the term for a device that is responsible for managing these devices?

Manager

Correct Answer
Hint
Task 2 Required: Deploy Wazuh Server
Task 3 Wazuh Agents
Task 4 Wazuh Vulnerability Assessment & Security Events
Task 5 Wazuh Policy Auditing

Task 2: Required: Deploy Wazuh Server

Now **Connect** to the TryHackMe network and deploy the Wazuh management server attached to this task and wait a **minimum of five minutes** before visiting the Wazuh server on HTTP://10.10.219.6.(IP at that particular time.



Title	IP Address	Expires
Wazuh 30062023	10.10.219.6	38m 29s

Woop woop! Your answer is correct.

Note: The questions within the tasks of this room **will expect the data stored on this Wazuh management server**, so it is vital that you are able to connect to this server before continuing.

The Wazuh management server in this room will show the agents as being *disconnected* - this is expected.

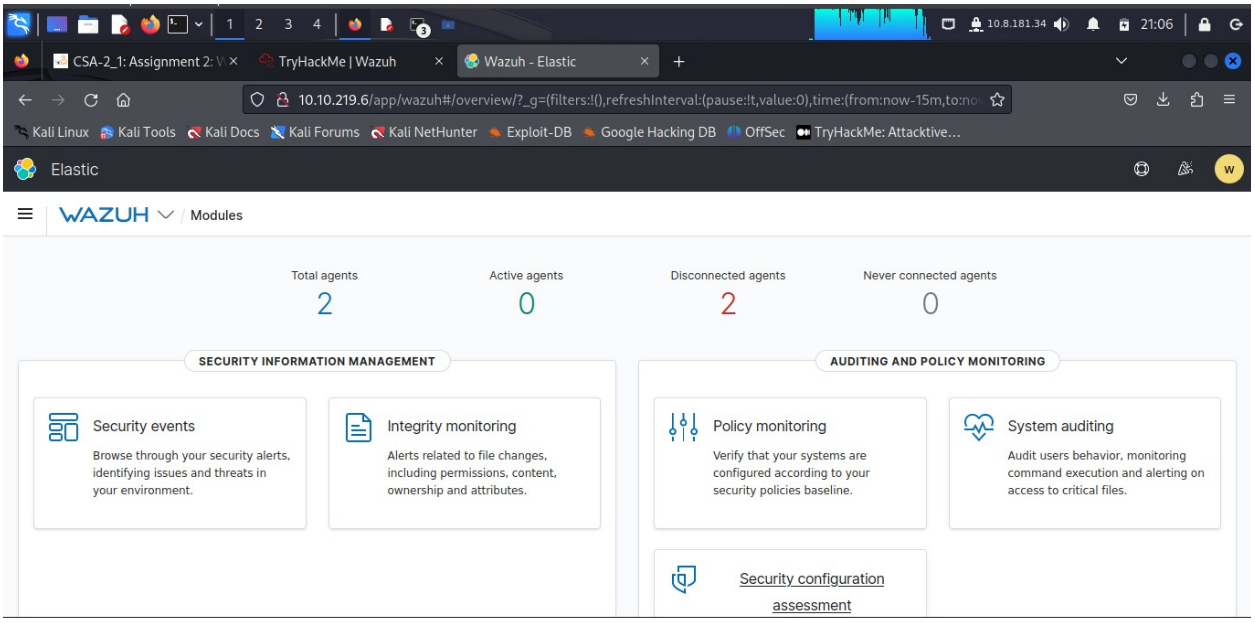
Answer the questions below

Login to the Wazuh management server on HTTP://10.10.219.6 before proceeding with this room's tasks.

No answer needed

Correct Answer

Successful login into **wazuh.**



Total agents	Active agents	Disconnected agents	Never connected agents
2	0	2	0

SECURITY INFORMATION MANAGEMENT

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

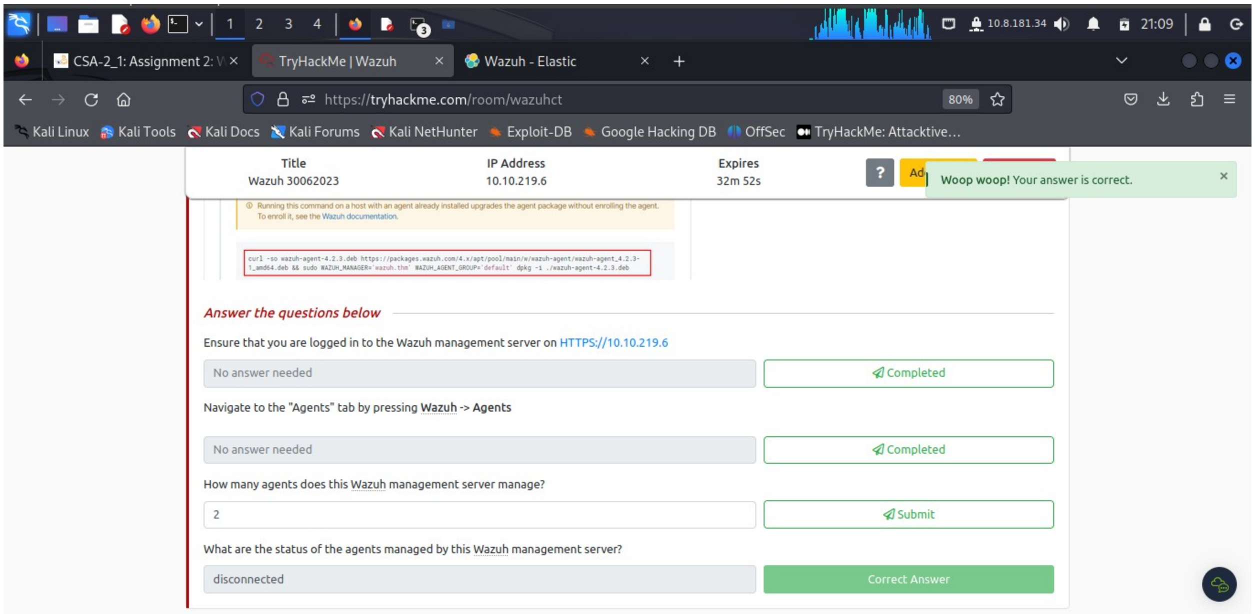
Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment

Task 3: 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.



Title	IP Address	Expires
Wazuh 30062023	10.10.219.6	32m 52s

Woop woop! Your answer is correct.

Running this command on a host with an agent already installed upgrades the agent package without enrolling the agent. To enroll it, see the Wazuh documentation.

```
curl -so wazuh-agent-4.2.3.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.2.3-
1_amd64.deb && sudo WAZUH_MANAGER='wazuh.thm' WAZUH_AGENT_GROUP='default' dpkg -i ./wazuh-agent-4.2.3.deb
```

Answer the questions below

Ensure that you are logged in to the Wazuh management server on HTTPS://10.10.219.6

No answer needed — Completed

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

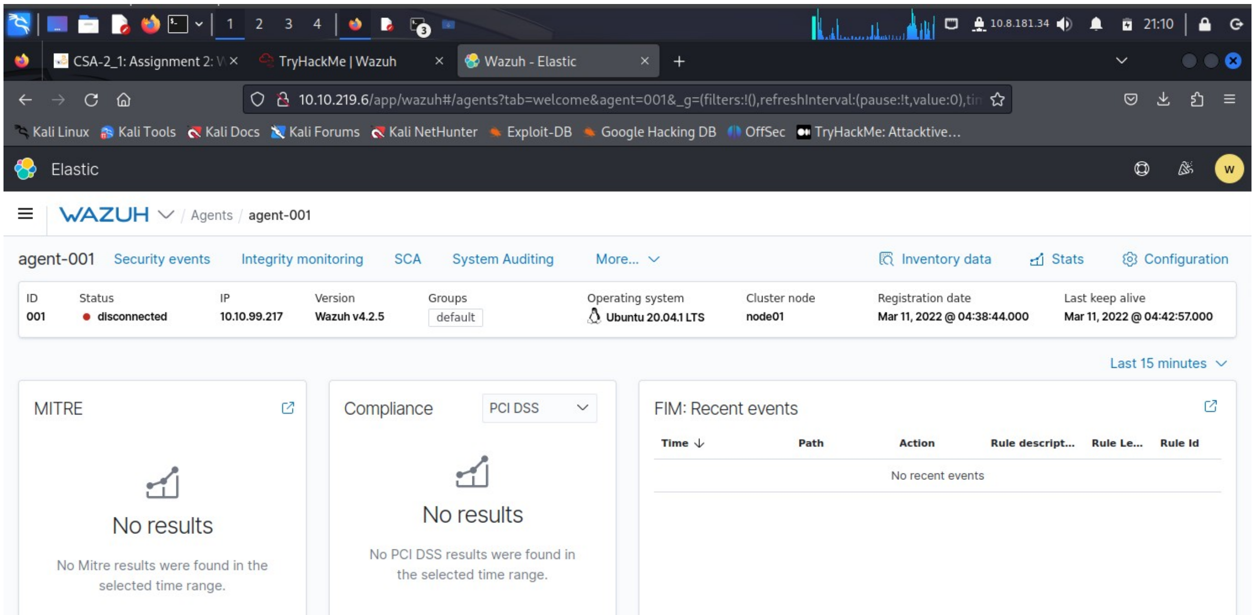
No answer needed — Completed

How many agents does this Wazuh management server manage?

2 — Submit

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

disconnected — Correct Answer



agent-001

ID	Status	IP	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
001	● disconnected	10.10.99.217	Wazuh v4.2.5	default	Ubuntu 20.04.1 LTS	node01	Mar 11, 2022 @ 04:38:44.000	Mar 11, 2022 @ 04:42:57.000

MITRE

No results

No Mitre results were found in the selected time range.

Compliance — PCI DSS

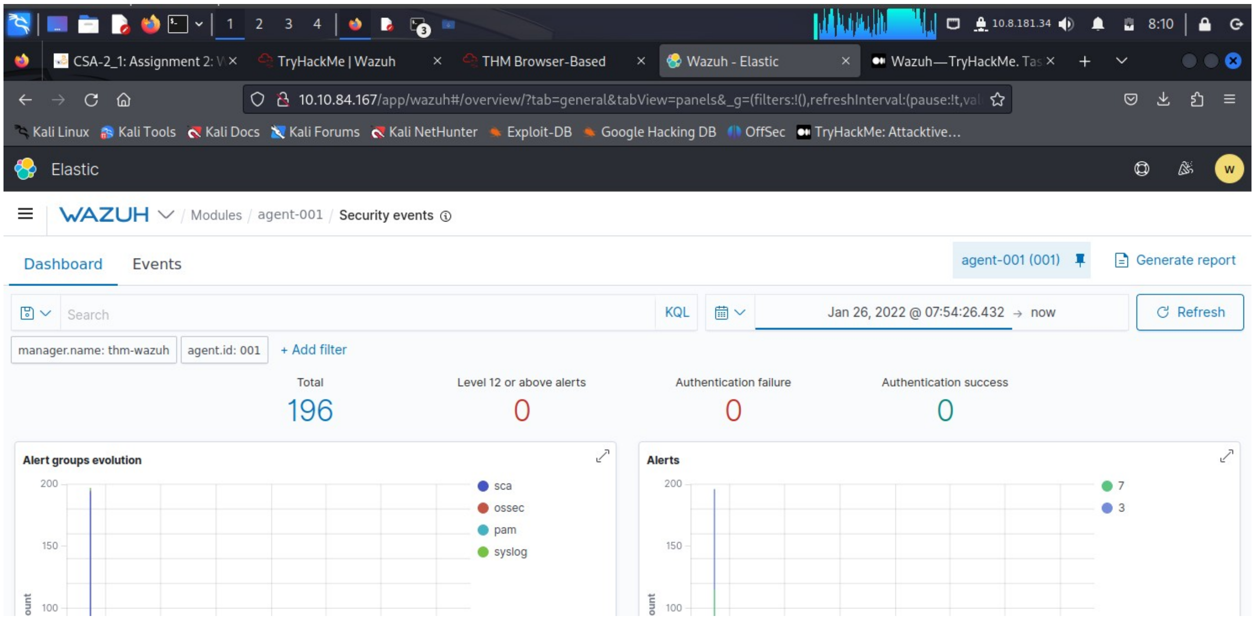
No results

No PCI DSS results were found in the selected time range.

FIM: Recent events

Time	Path	Action	Rule descript...	Rule Le...	Rule Id
No recent events					

Task 4: Wazuh Vulnerability Assessment & Security Events



10.10.84.167/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,val

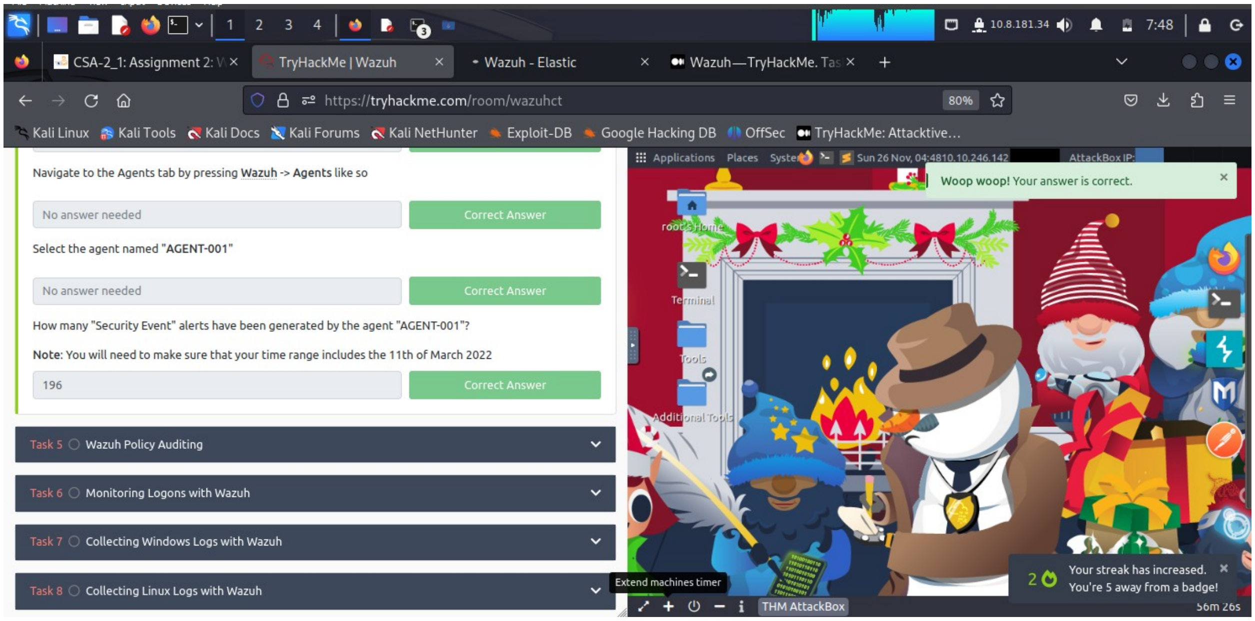
WAZUH / Modules / agent-001 / Security events

agent-001 (001)

Jan 26, 2022 @ 07:54:26.432 → now

manager.name: thm-wazuh | agent.id: 001

Total	Level 12 or above alerts	Authentication failure	Authentication success
196	0	0	0



https://tryhackme.com/room/wazuhct

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

No answer needed

Correct Answer

Select the agent named "AGENT-001"

No answer needed

Correct Answer

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

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

196

Correct Answer

Task 5 Wazuh Policy Auditing

Task 6 Monitoring Logons with Wazuh

Task 7 Collecting Windows Logs with Wazuh

Task 8 Collecting Linux Logs with Wazuh

Woop woop! Your answer is correct.

Your streak has increased. You're 5 away from a badge!

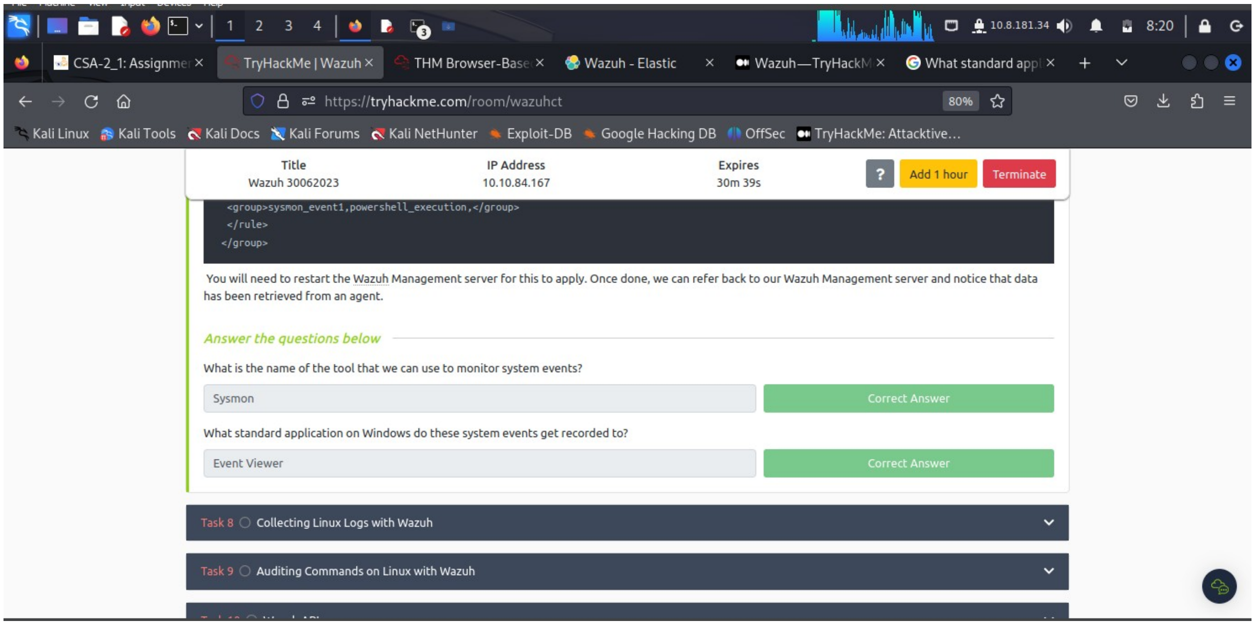
Task 5: Wazuh Policy Auditing

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.

Task 6: Monitoring Logons with Wazuh

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

Task 7: Collecting Windows Logs with Wazuh



Title	IP Address	Expires
Wazuh 30062023	10.10.84.167	30m 39s

```
  <group>sysmon_event1,powershell_execution,</group>
  </rule>
</group>
```

You will need to restart the Wazuh Management server for this to apply. Once done, we can refer back to our Wazuh Management server and notice that data has been retrieved from an agent.

Answer the questions below

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

Sysmon — Correct Answer

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

Event Viewer — Correct Answer

Task 8 ○ Collecting Linux Logs with Wazuh

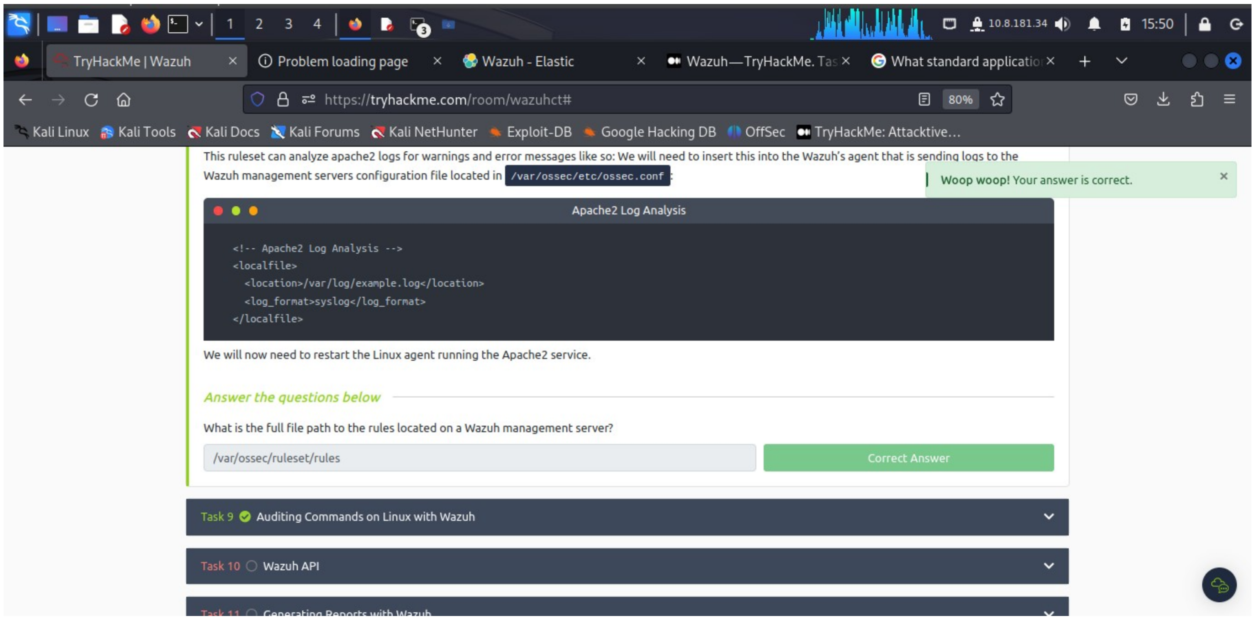
Task 9 ○ Auditing Commands on Linux with Wazuh

Task 8: Collecting Linux Logs with Wazuh

Capturing logs from a Linux agent is a simple process similar to capturing events from a Windows agent.

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



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`:

Woop woop! Your answer is correct.

Apache2 Log Analysis

```
<!-- Apache2 Log Analysis -->
<localfile>
  <location>/var/log/example.log</location>
  <log_format>syslog</log_format>
</localfile>
```

We will now 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?

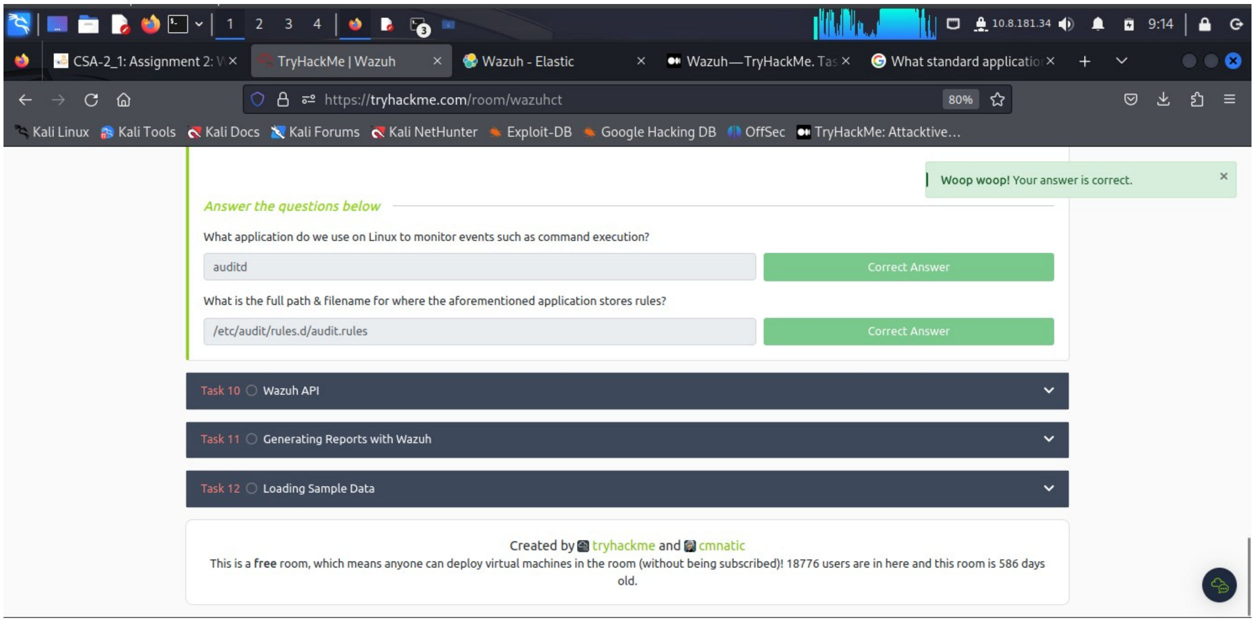
/var/ossec/ruleset/rules

Correct Answer
Task 9 Auditing Commands on Linux with Wazuh
Task 10 Wazuh API
Task 11 Generating Reports with Wazuh

Task 9: 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.



Woop woop! Your answer is correct.

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?

/etc/audit/rules.d/audit.rules

Correct Answer
Correct Answer
Task 10 Wazuh API
Task 11 Generating Reports with Wazuh
Task 12 Loading Sample Data

Created by tryhackme and cmnatic

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 18776 users are in here and this room is 586 days old.

Task 10: 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.

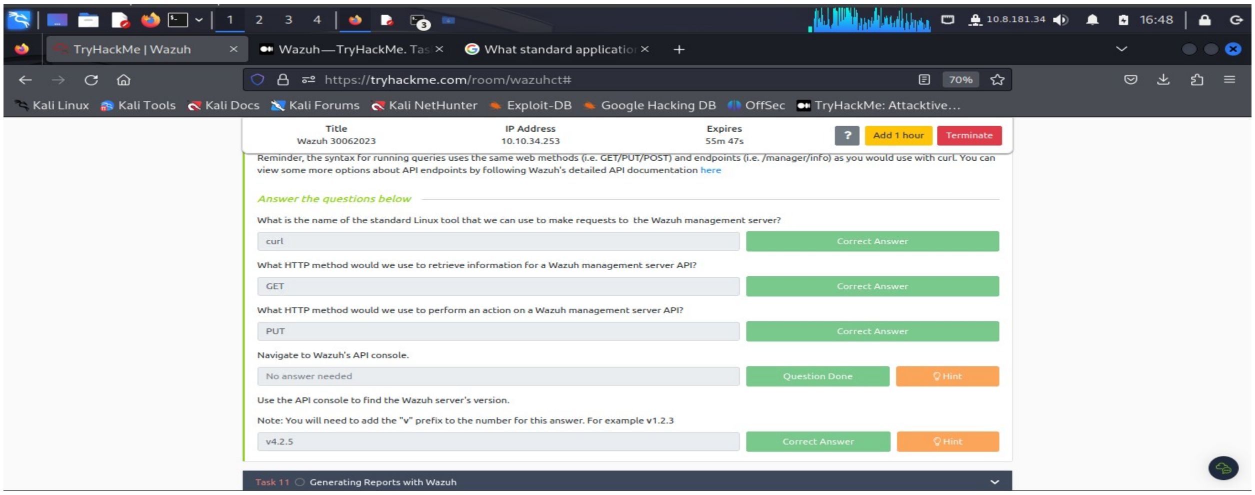
curl tool installed to interact with the Wazuh management server API.

We can store this token as an environment variable on our Linux machine like the snippet below:

(replacing *WAZUH_MANAGEMENT_SERVER_IP* with the IP address of the Wazuh management server (i.e. 10.10.84.167):

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

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



Title	IP Address	Expires
Wazuh 30062023	10.10.34.253	55m 47s

? Add 1 hour Terminate

Reminder, the syntax for running queries uses the same web methods (i.e. GET/PUT/POST) and endpoints (i.e. /manager/info) as you would use with curl. You can view some more options about API endpoints by following Wazuh's detailed API documentation here

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 — Correct Answer

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

GET — Correct Answer

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

PUT — Correct Answer

Navigate to Wazuh's API console.

No answer needed — Question Done — Hint

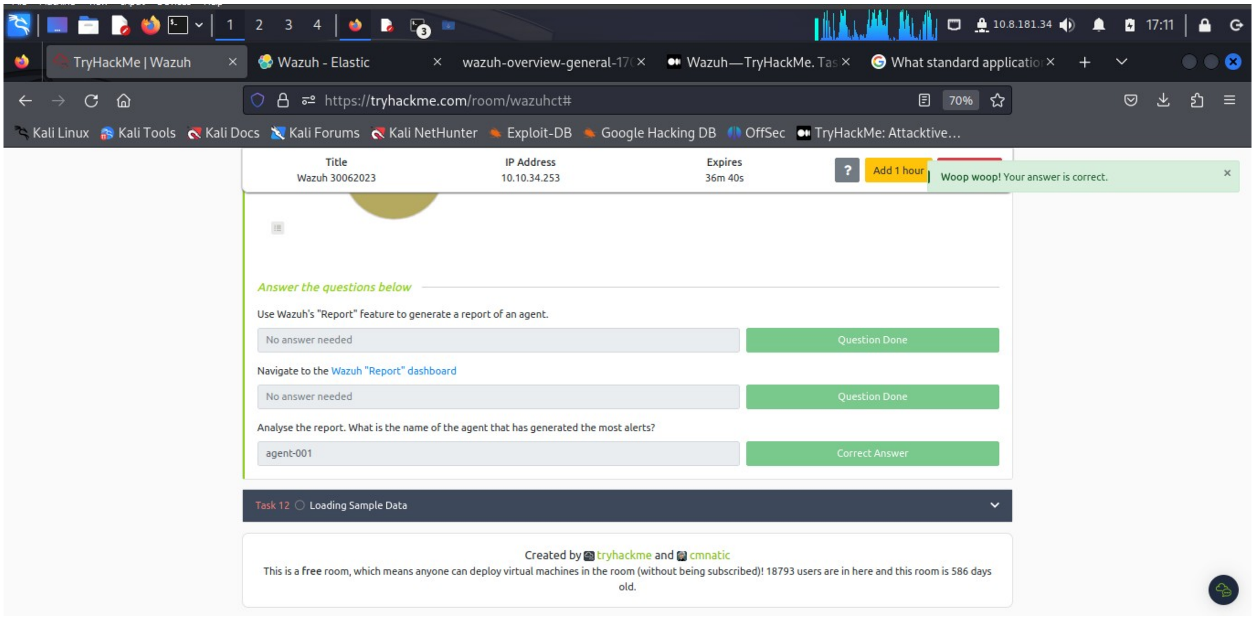
Use the API console to find the Wazuh server's version.

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

v4.2.5 — Correct Answer — Hint

Task 11 ○ Generating Reports with Wazuh

Task 11: Generating Reports with Wazuh



Title	IP Address	Expires
Wazuh 30062023	10.10.34.253	36m 40s

? Add 1 hour

Woop woop! Your answer is correct.

Answer the questions below

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

No answer needed — Question Done

Navigate to the Wazuh "Report" dashboard

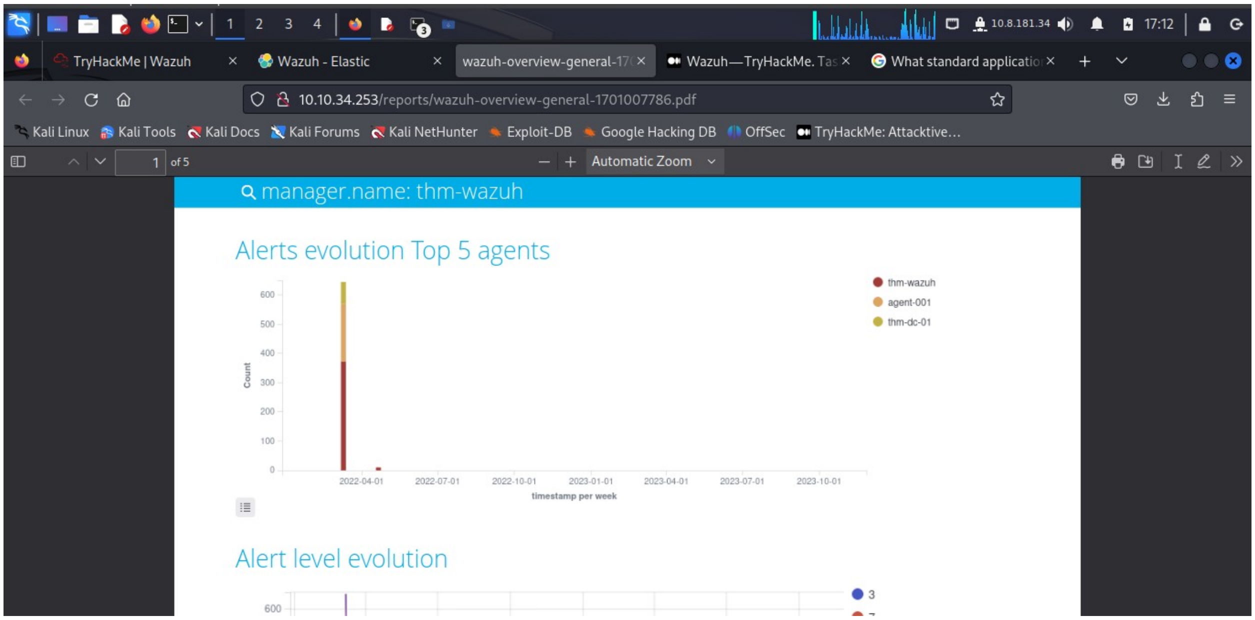
No answer needed — Question Done

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

agent-001 — Correct Answer

Task 12 ○ Loading Sample Data

Created by tryhackme and cmnatic
This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 18793 users are in here and this room is 586 days old.



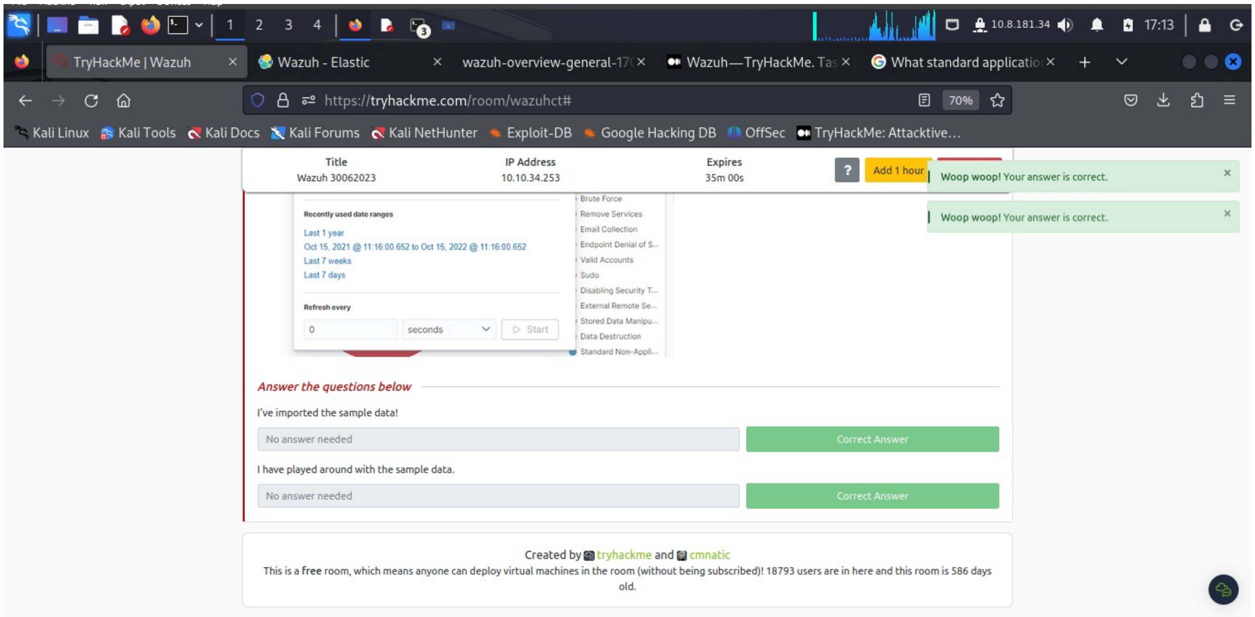
10.10.34.253/reports/wazuh-overview-general-1701007786.pdf

manager.name: thm-wazuh

Alerts evolution Top 5 agents

Alert level evolution

Task 12: Loading Sample Data



https://tryhackme.com/room/wazuhct#

Title	IP Address	Expires
Wazuh 30062023	10.10.34.253	35m 00s

Woop woop! Your answer is correct.

Woop woop! Your answer is correct.

Answer the questions below

I've imported the sample data!

No answer needed

Correct Answer

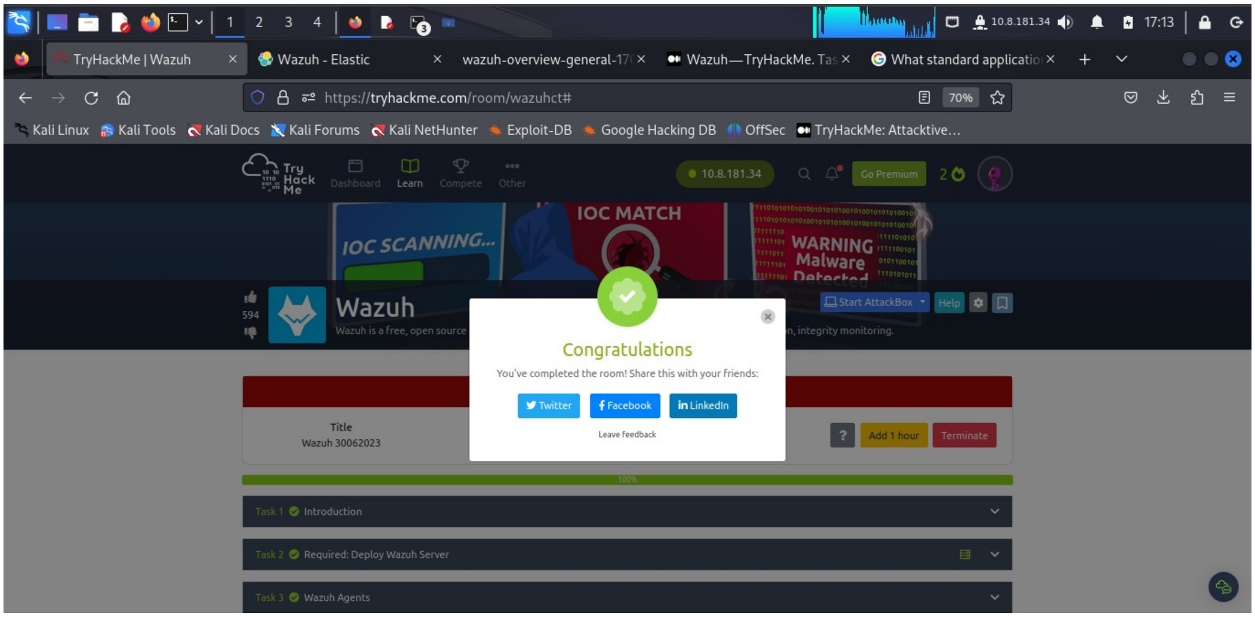
I have played around with the sample data.

No answer needed

Correct Answer

Created by tryhackme and cmnatic

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 18793 users are in here and this room is 586 days old.



Congratulations

You've completed the room! Share this with your friends:

Title
Wazuh 30062023

Task 1 Introduction

Task 2 Required: Deploy Wazuh Server

Task 3 Wazuh Agents

Conclusion

In these activities the security analyst capitalizes on the Wazuh Tool to conduct security monitoring solution for threat detection, integrity monitoring.

Completion Link: https://tryhackme.com/room/wazuhct#