**Wazuh**

**Introduction**

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

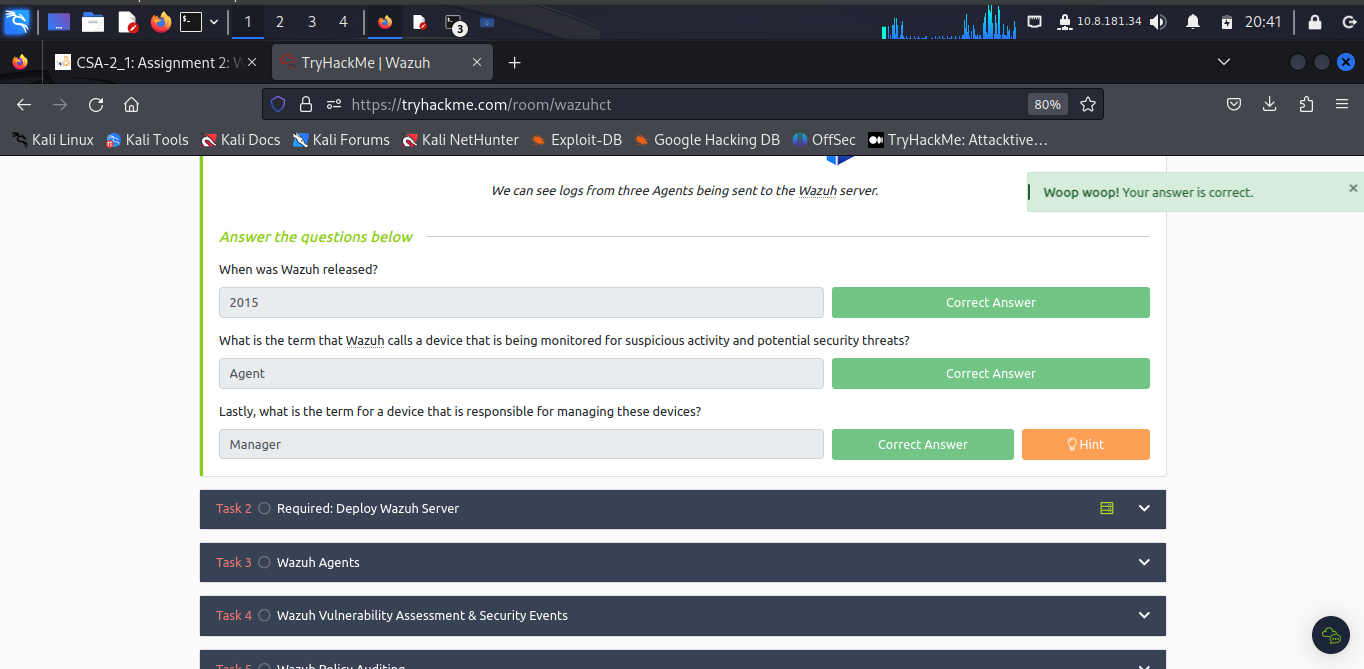
***Activities***

***Task 1: Introduction***

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

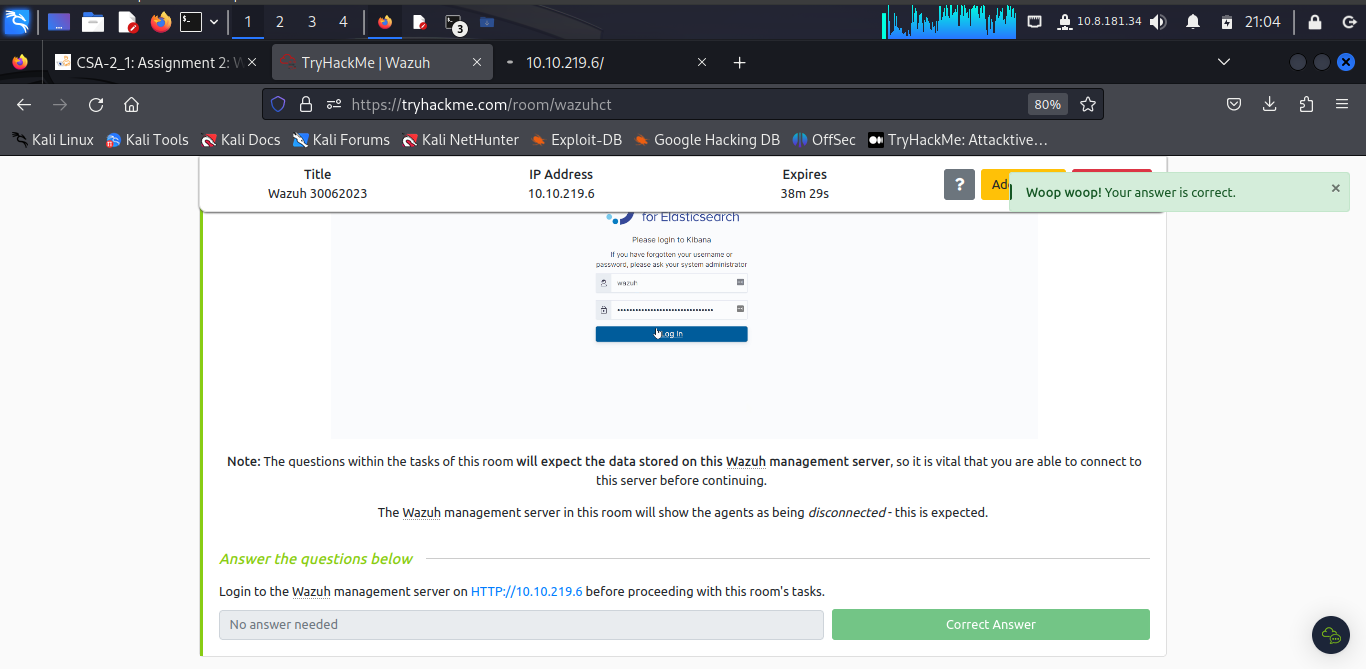
The tools and applications have features that include:

* 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

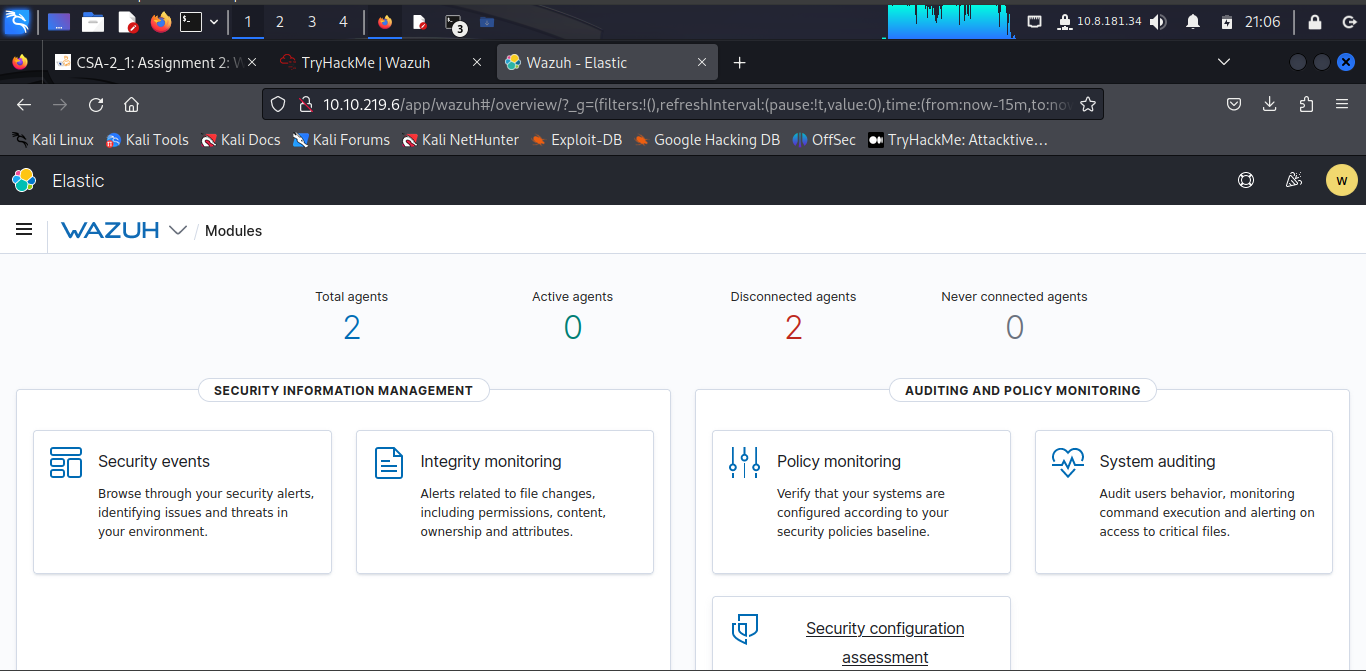


***Task 2: Required: Deploy Wazuh Server***

Now [**Connect**](https://tryhackme.com/access) 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.

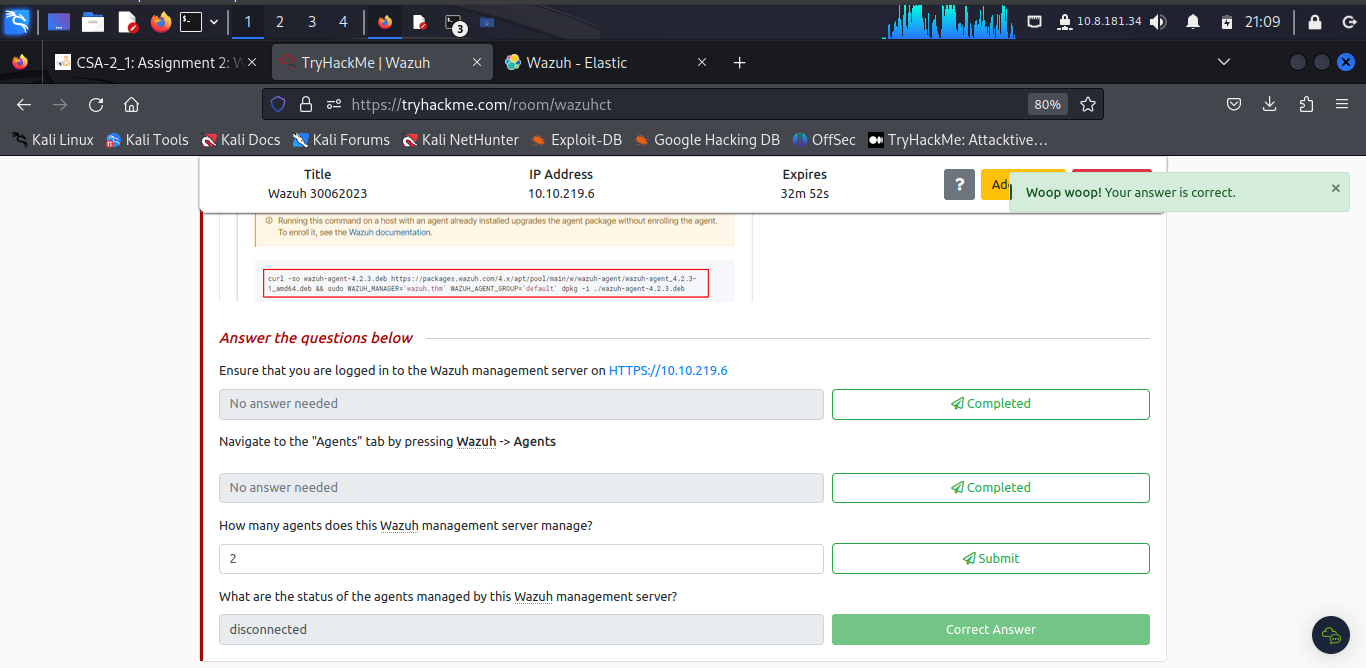


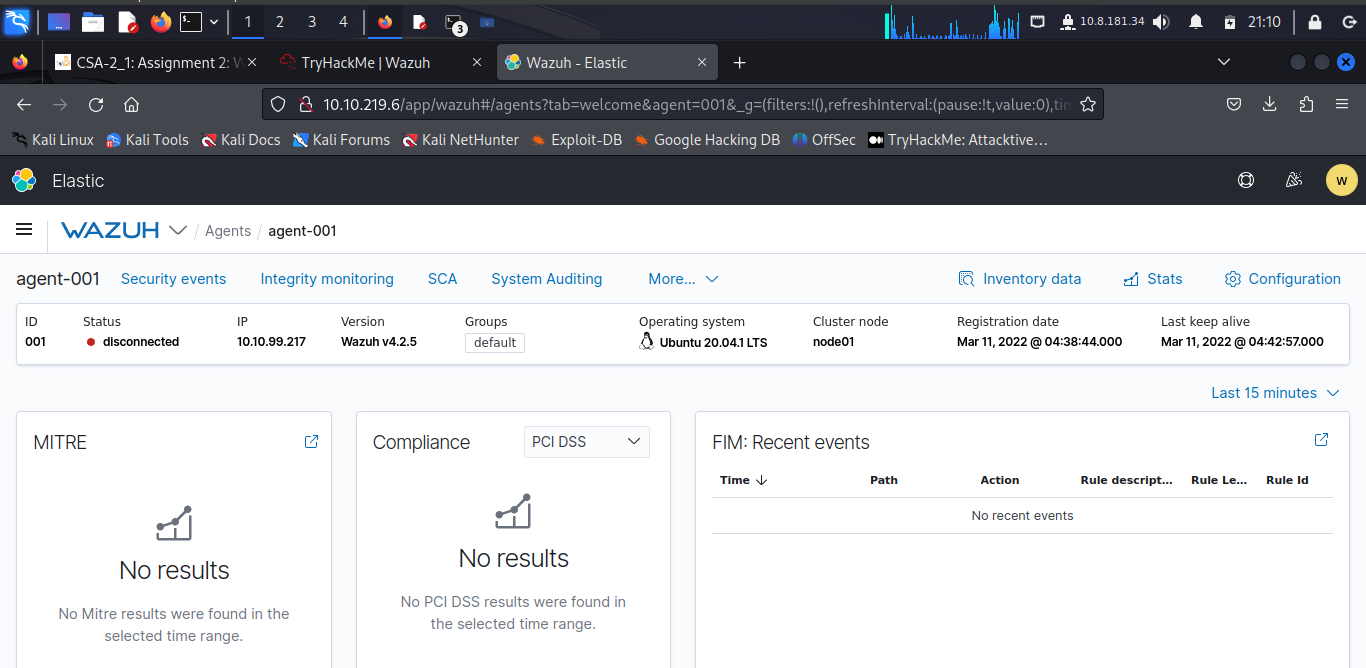
Successful login into **wazuh.**



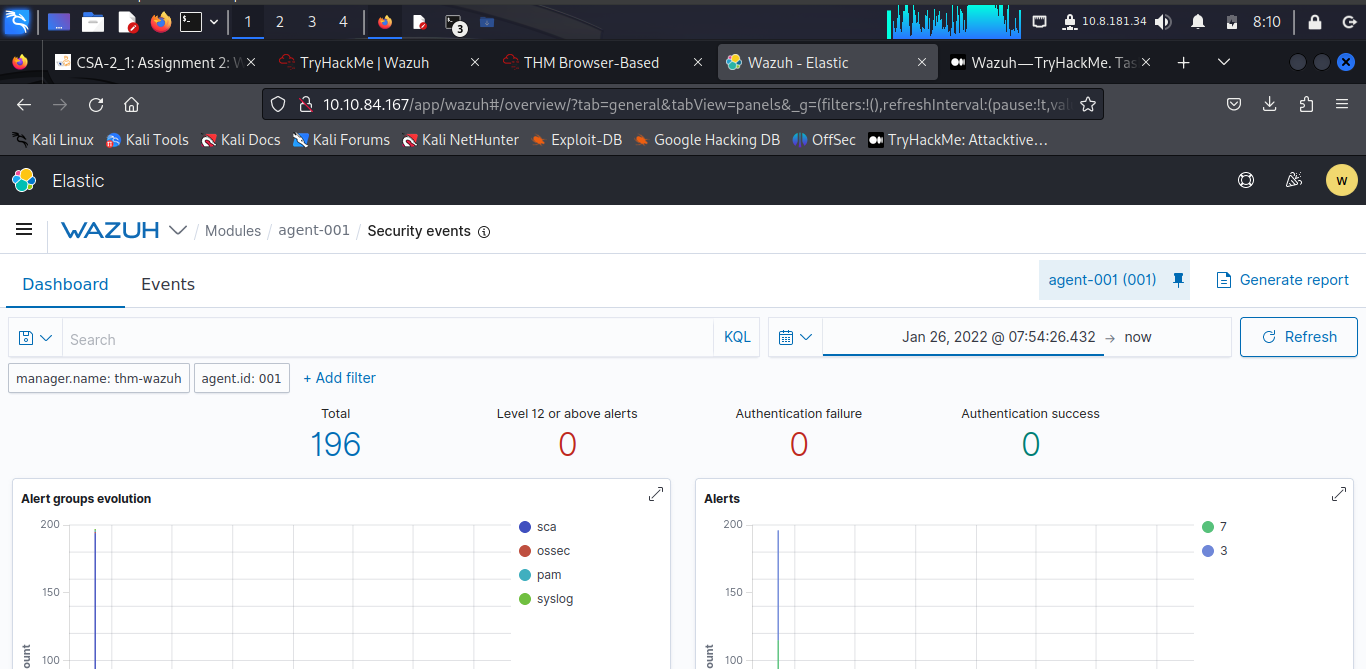
***Task 3: Wazuh Agents***

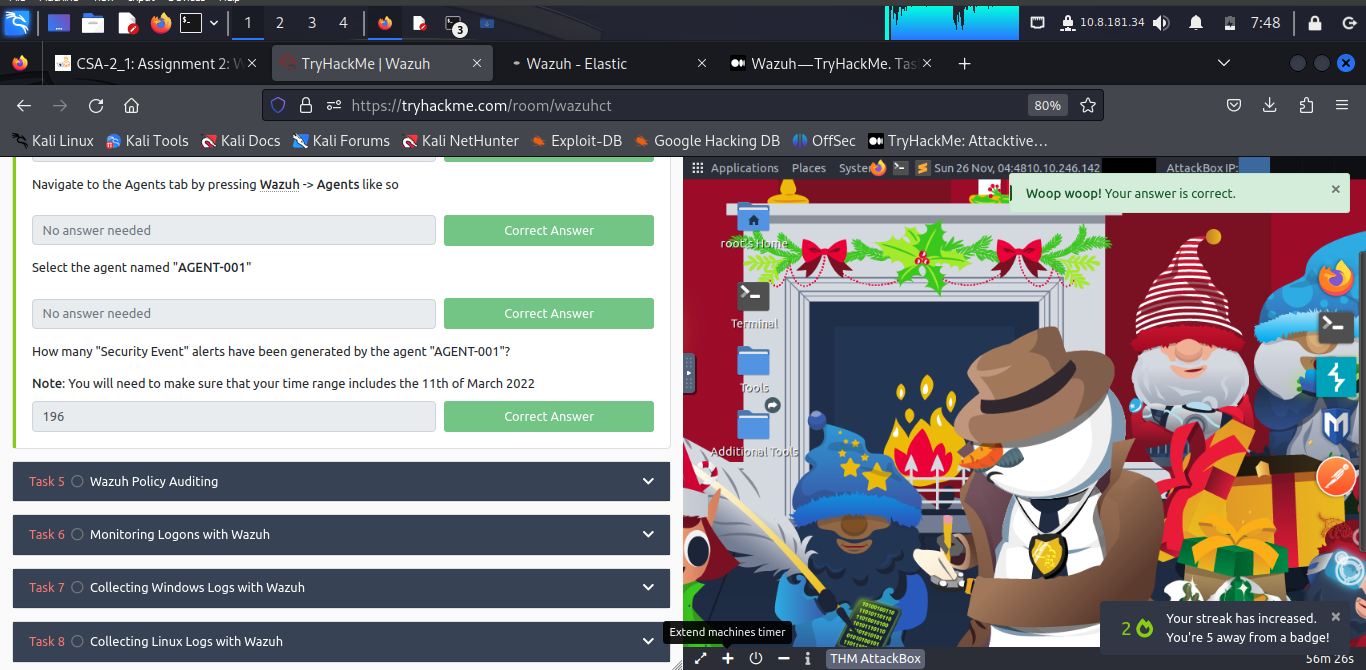
Devices that record the events and processes of a system are called **agents**. Agents monitor the processes and events that take place on the device, such as authentication and user management. Agents will offload these logs to a designated collector for processing, such as Wazuh.





***Task 4: Wazuh Vulnerability Assessment & Security Events***





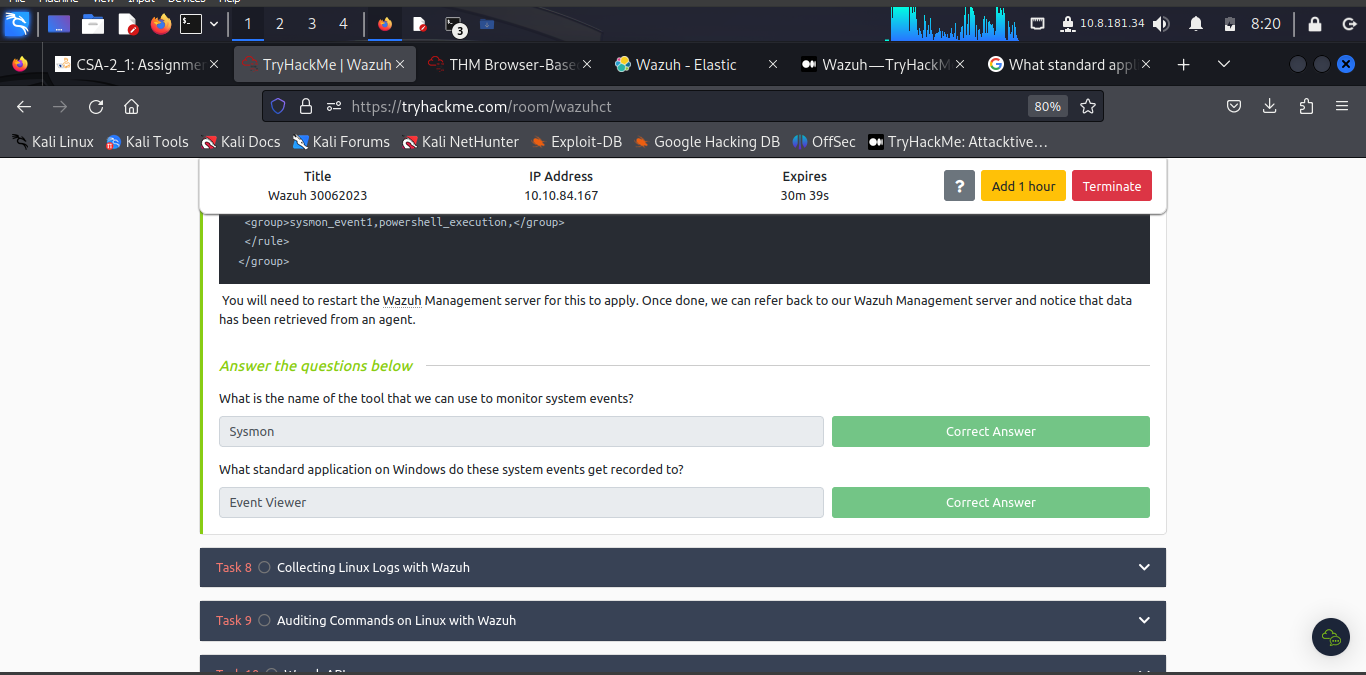
***Task 5: Wazuh Policy Auditing***

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***

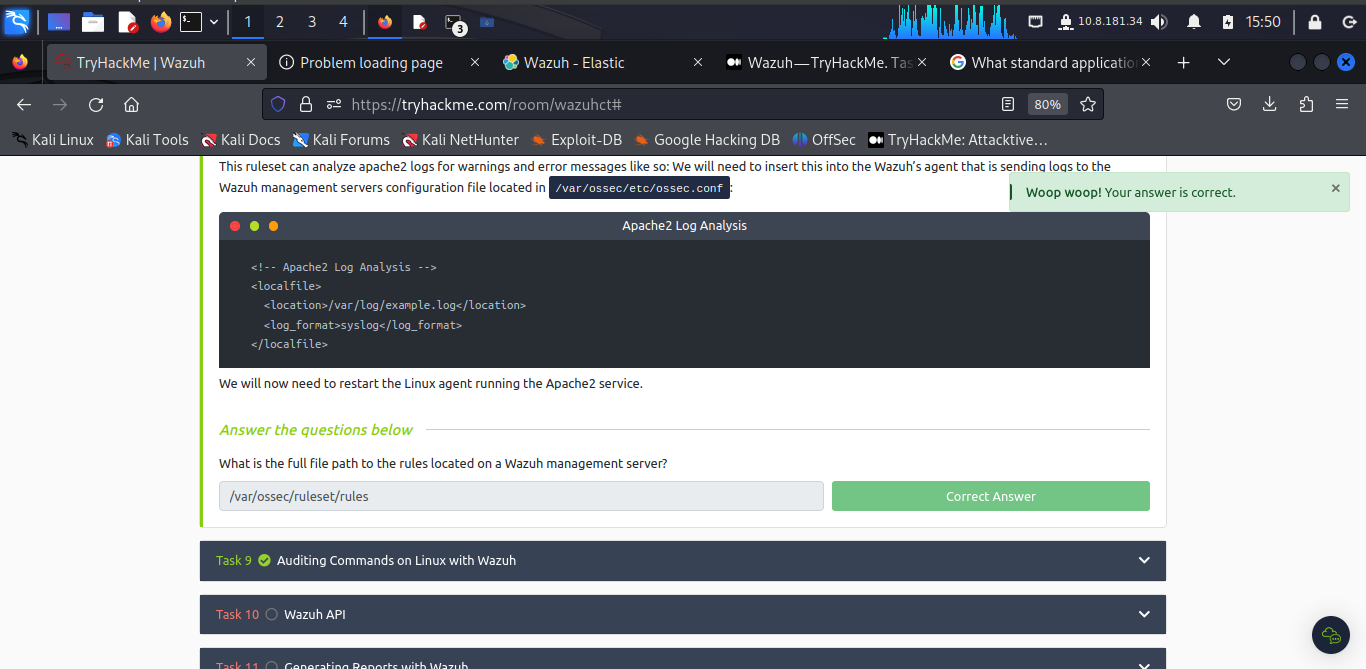


***Task 8: Collecting Linux Logs with Wazuh***

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:

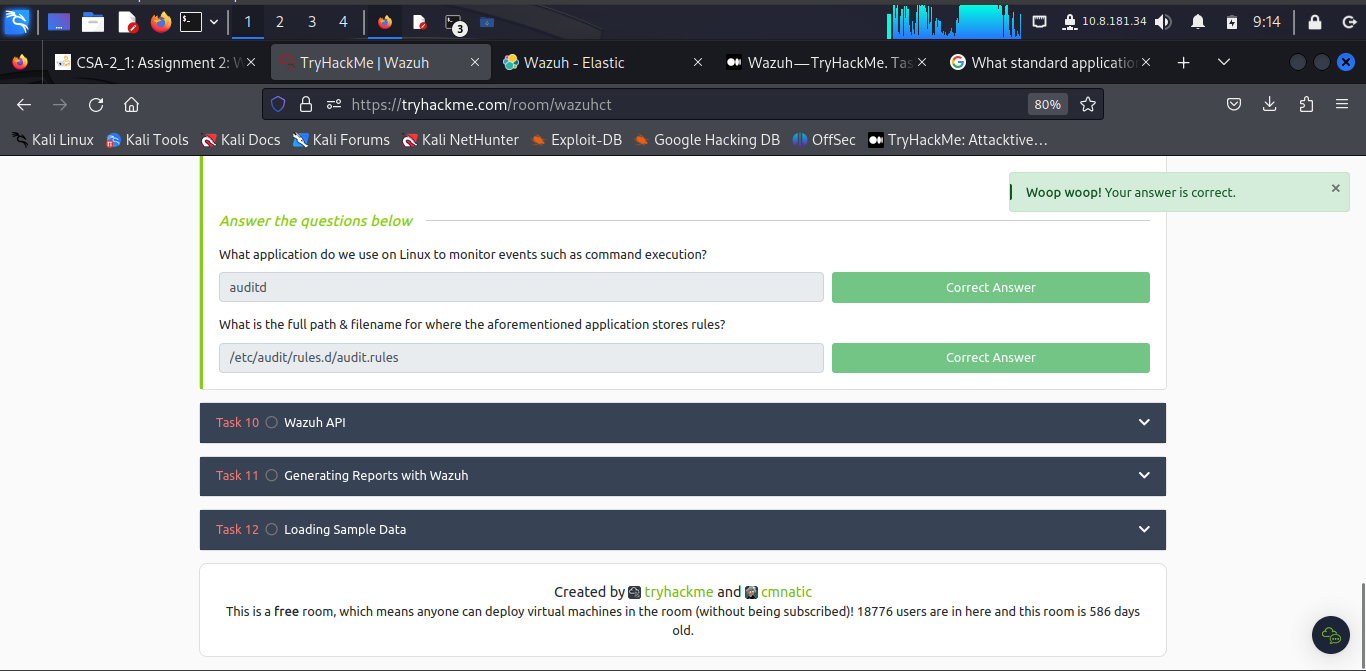
* Docker
* FTP
* WordPress
* SQL Server
* MongoDB
* Firewalld



***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.



***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.

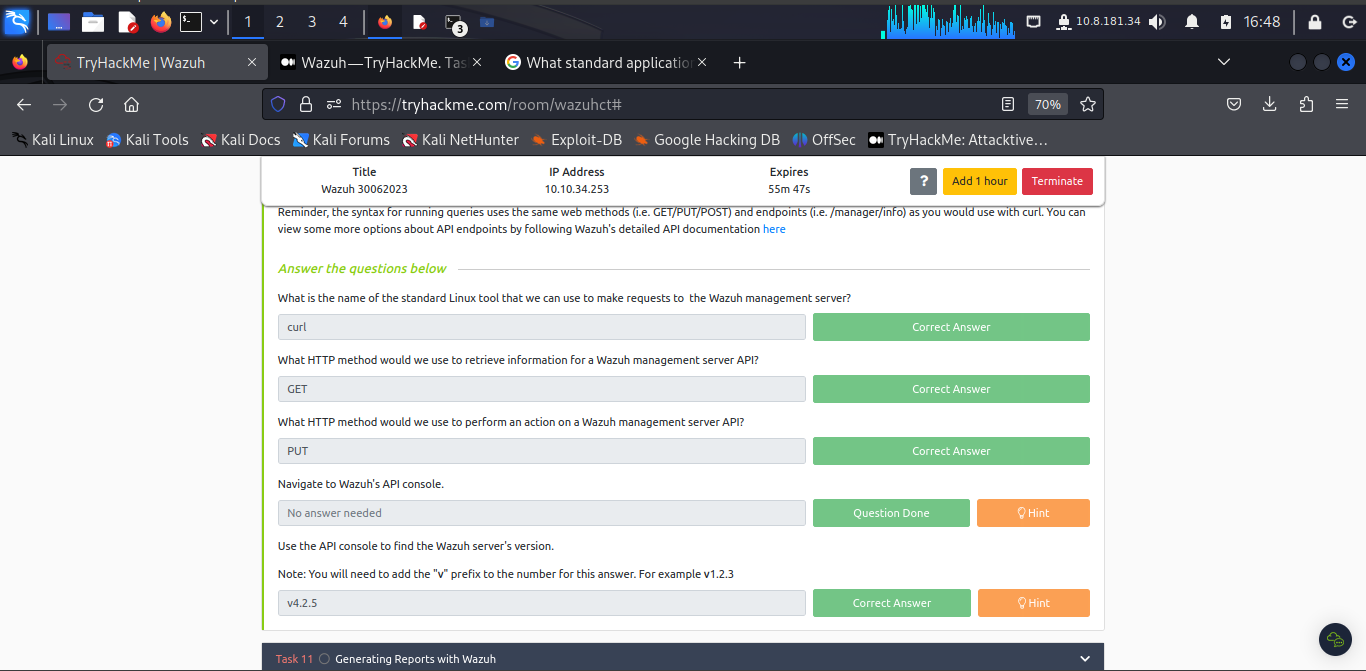
**curl** tool installed to interact with the Wazuh management server API.

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

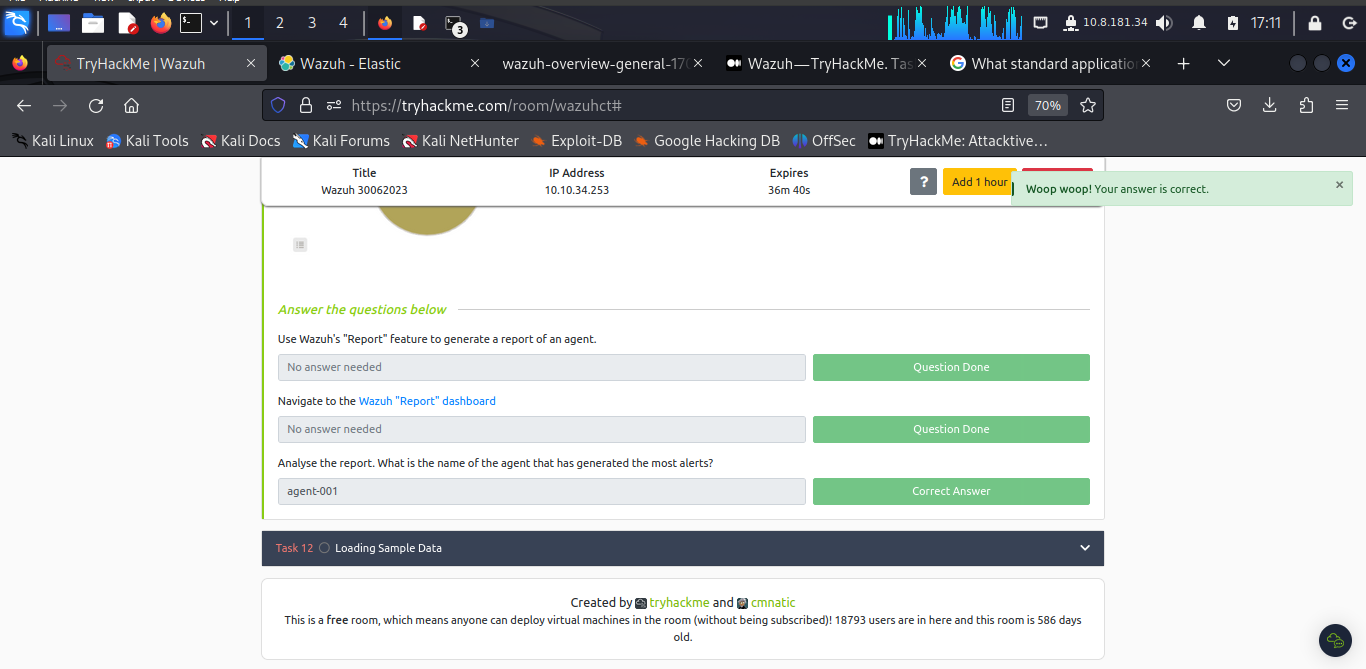
(replacing *WAZUH\_MANAGEMENT\_SERVER\_IP* with the IP address of the Wazuh management server (i.e. 10.10.84.167):

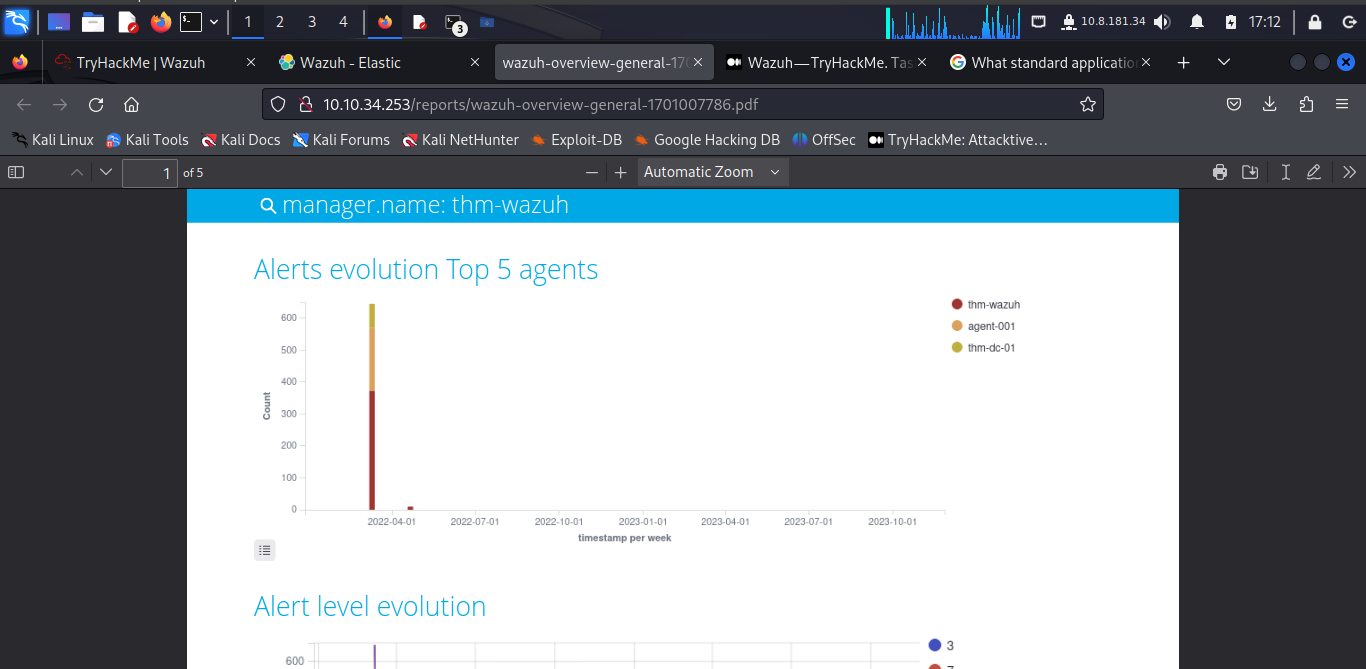
**TOKEN=$(curl -u : -k -X GET "https://WAZUH\_MANAGEMENT\_SERVER\_IP:55000/security/user/authenticate?raw=true")**

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

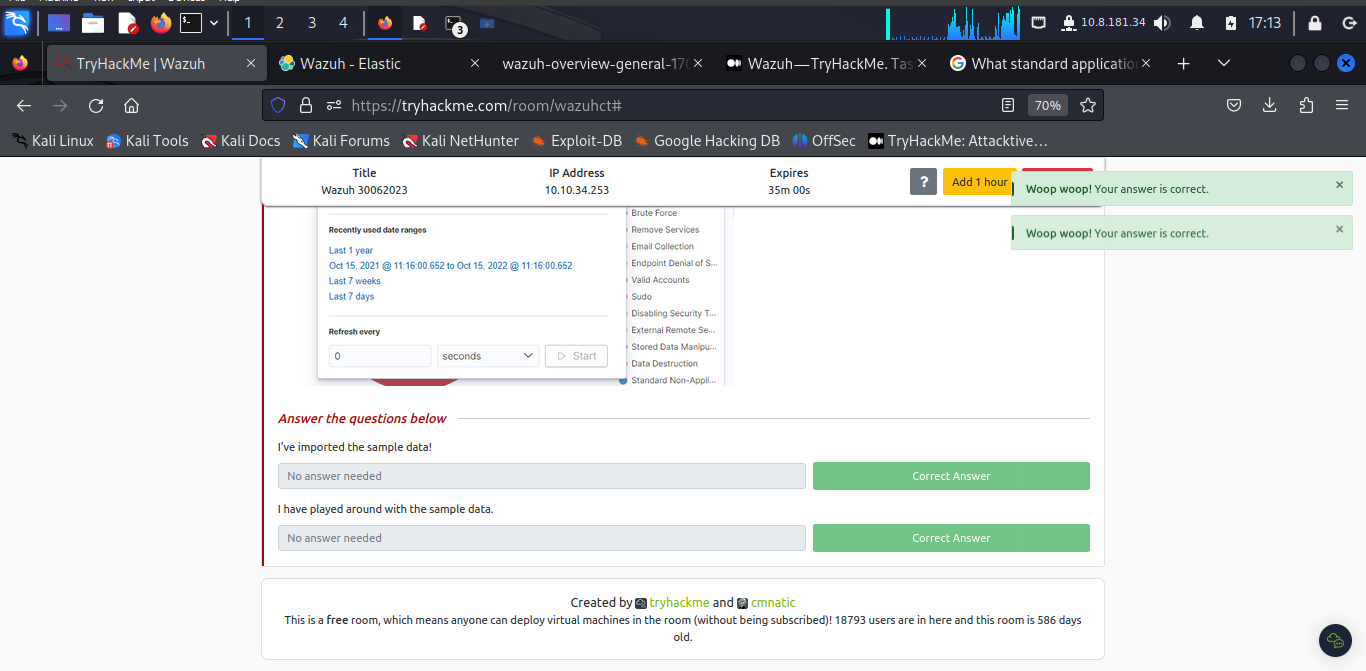


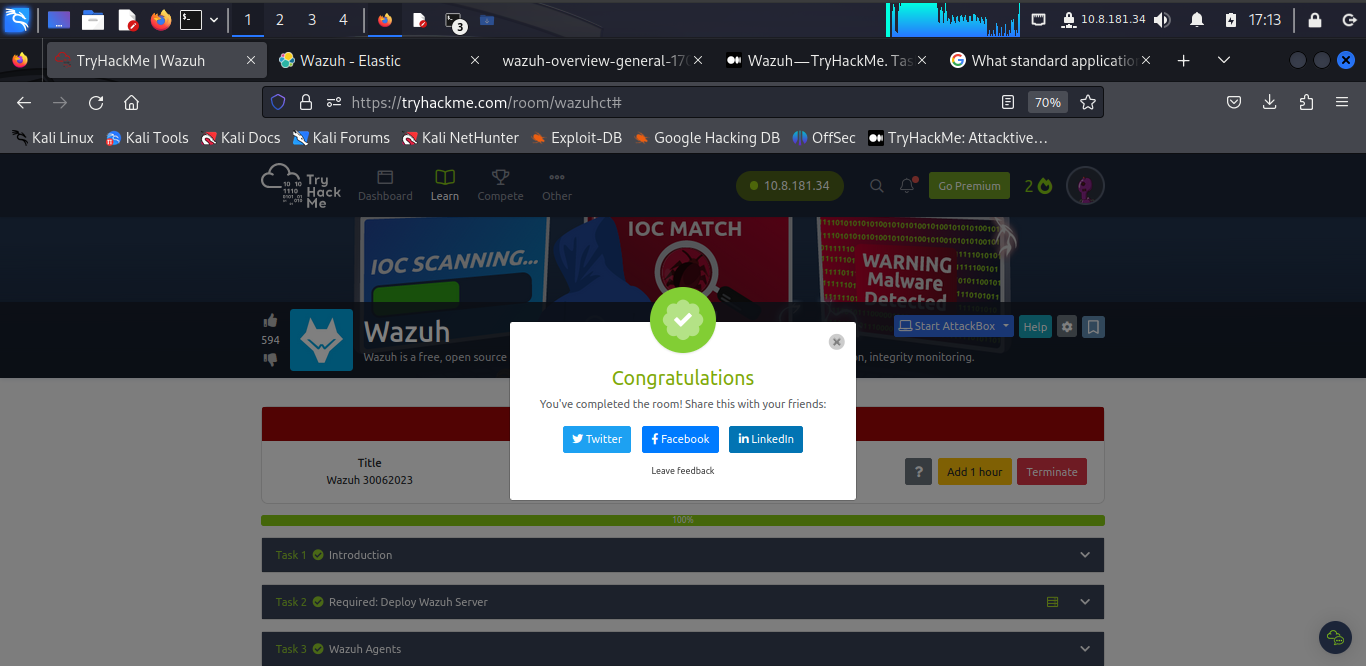
***Task 11: Generating Reports with Wazuh***





***Task 12: Loading Sample Data***





**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#>