

CodemanBD Internship (December-2023 to January-2024)

Topic: Task-4 (Project-1)

Submitted By:

Student's Id: 213/48

Student's Name: Teresa Jency Bala

Submitted to:

Instructor: Sanin Ahammed Sifat (Shuvo Ahmed)

Date: 04-01-2024

Day: Thursday

Project-1: Mix tasks 1-2-3 and make a fresh report about Wazuh as SIEM & EDR. **(without installation steps)**

Wazuh:

Wazuh is a **free** and **open-source** security monitoring tool that helps organizations detect, respond to, and mitigate cyber threats. It is a **host-based intrusion detection system** (HIDS) that monitors system files, processes, and network traffic for suspicious activity. Wazuh also includes a security information and event management (SIEM) system that collects and analyzes logs from various sources to provide a centralized view of security events.

Wazuh is a popular security monitoring tool because it is:

Free and open-source: Wazuh is available to download and use without any licensing fees. This makes it a cost-effective solution for organizations of all sizes.

Comprehensive: Wazuh provides a wide range of security monitoring capabilities, including HIDS, SIEM, and log management. This makes it a one-stop shop for security monitoring needs.

Powerful: Wazuh is powered by a variety of powerful detection engines, including Random Cut Forest, Local Outlier Factor, and K-Means Clustering. This allows it to detect a wide range of threats, including zero-day attacks and advanced persistent threats (APTs).

Easy to use: Wazuh has a user-friendly interface that makes it easy to configure and manage. It also has a large community of users and developers who can provide support and assistance.

Wazuh is used by a variety of organizations, including government agencies, financial institutions, and healthcare providers. It is a trusted security monitoring tool that can help organizations protect their systems and data from cyber threats.

In addition to the features listed above, Wazuh also includes the following:

Real-time monitoring: Wazuh monitors system activity in real-time, so it can detect threats as they are happening.

Threat intelligence: Wazuh includes a threat intelligence feed that provides information about the latest threats and vulnerabilities.

Incident response: Wazuh provides tools to help organizations respond to security incidents, such as playbooks and runbooks.

Compliance reporting: Wazuh can generate reports that help organizations comply with security regulations, such as PCI DSS and HIPAA.

Wazuh is a comprehensive and powerful security monitoring tool that can help organizations protect their systems and data from cyber threats. It is free and open-source, easy to use, and has a large community of users and developers.

Wazuh Dashboard before integrating agents(hosts) for monitoring:

The screenshot displays the Wazuh Dashboard web interface in a browser. The address bar shows the URL `https://192.168.68.110/app/wazuh#/overview/?_g=(filters:!,refreshInterval:(pause:!t,value:0),time:(from:no`. The dashboard header includes the Wazuh logo, a 'Modules' tab, and a user profile icon labeled 'a'. The main content area features five agent status cards: 'Total agents' (0), 'Active agents' (0), 'Disconnected agents' (0), 'Pending agents' (0), and 'Never connected agents' (0). Below these is a yellow notification bar stating 'No agents were added to this manager. Add agent'. The dashboard is divided into two main sections: 'SECURITY INFORMATION MANAGEMENT' and 'AUDITING AND POLICY MONITORING'. The first section contains 'Security events' (Browse through your security alerts, identifying issues and threats in your environment.) and 'Integrity monitoring' (Alerts related to file changes, including permissions, content, ownership and attributes.). The second section contains '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.), and 'Security configuration assessment'.

Wazuh - Wazuh

https://192.168.68.110/app/wazuh#/overview/?_g=(filters:!,refreshInterval:(pause:!t,value:0),time:(from:no

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Using Burp to Test for ...

wazuh. Modules

Total agents 0

Active agents 0

Disconnected agents 0

Pending agents 0

Never connected agents 0

⚠ No agents were added to this manager. [Add agent](#)

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

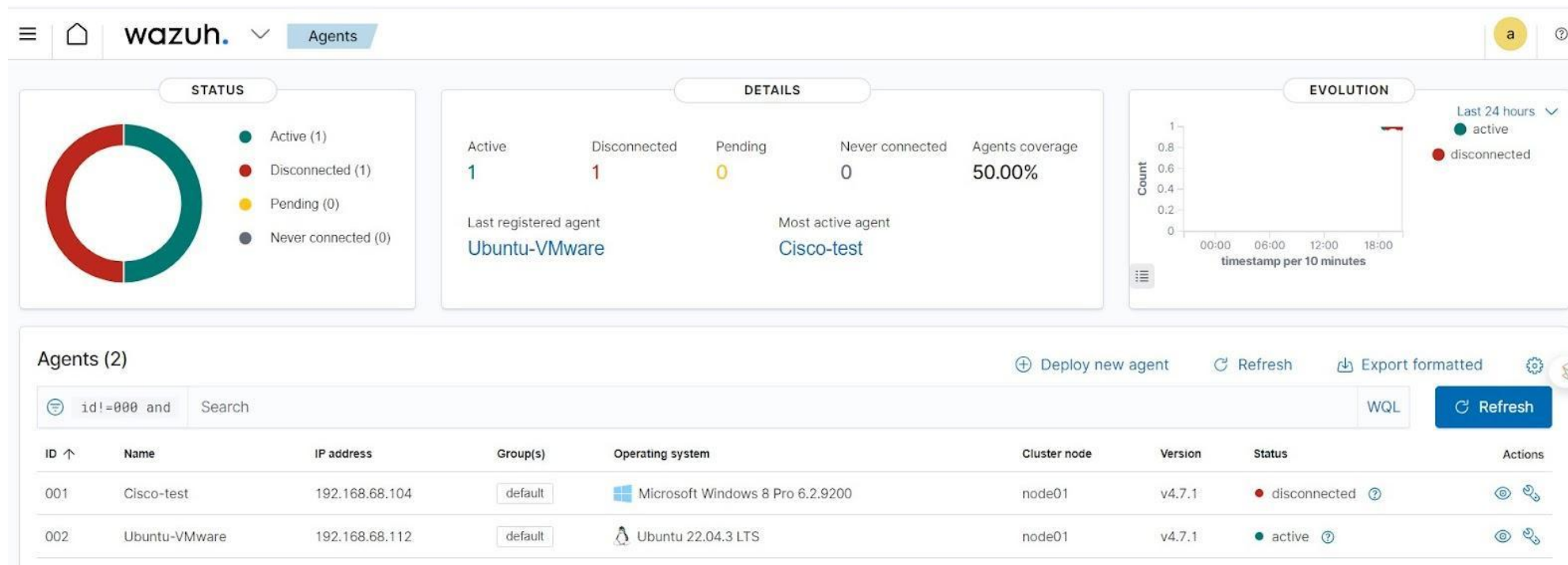
Policy monitoring
Verify that your systems are configured according to your security policies baseline.

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

Security configuration assessment

ove the mouse pointer inside or press Ctrl+G.

Wazuh Dashboard after integrating agents(hosts) for monitoring: Here One agent (ubuntu) active



Wazuh Dashboard after integrating agents(hosts) for monitoring: Here both Linux and Windows Host active

The screenshot displays a Kali Linux virtual machine environment. In the background, a terminal window shows the execution of Wazuh agent commands and system logs. In the foreground, a web browser displays the Wazuh Dashboard interface, specifically the 'Agents' page. The dashboard shows two active agents: 'Cisco-test' (Windows) and 'Ubuntu-VMware' (Ubuntu).

Terminal Output:

```
3393 /var/ossec/bin/wazuh-agentd
3406 /var/ossec/bin/wazuh-syscheckd
3860 /bin/sh active-response/bin/restart.sh agent
3864 /bin/sh /var/ossec/bin/wazuh-control restart
4625

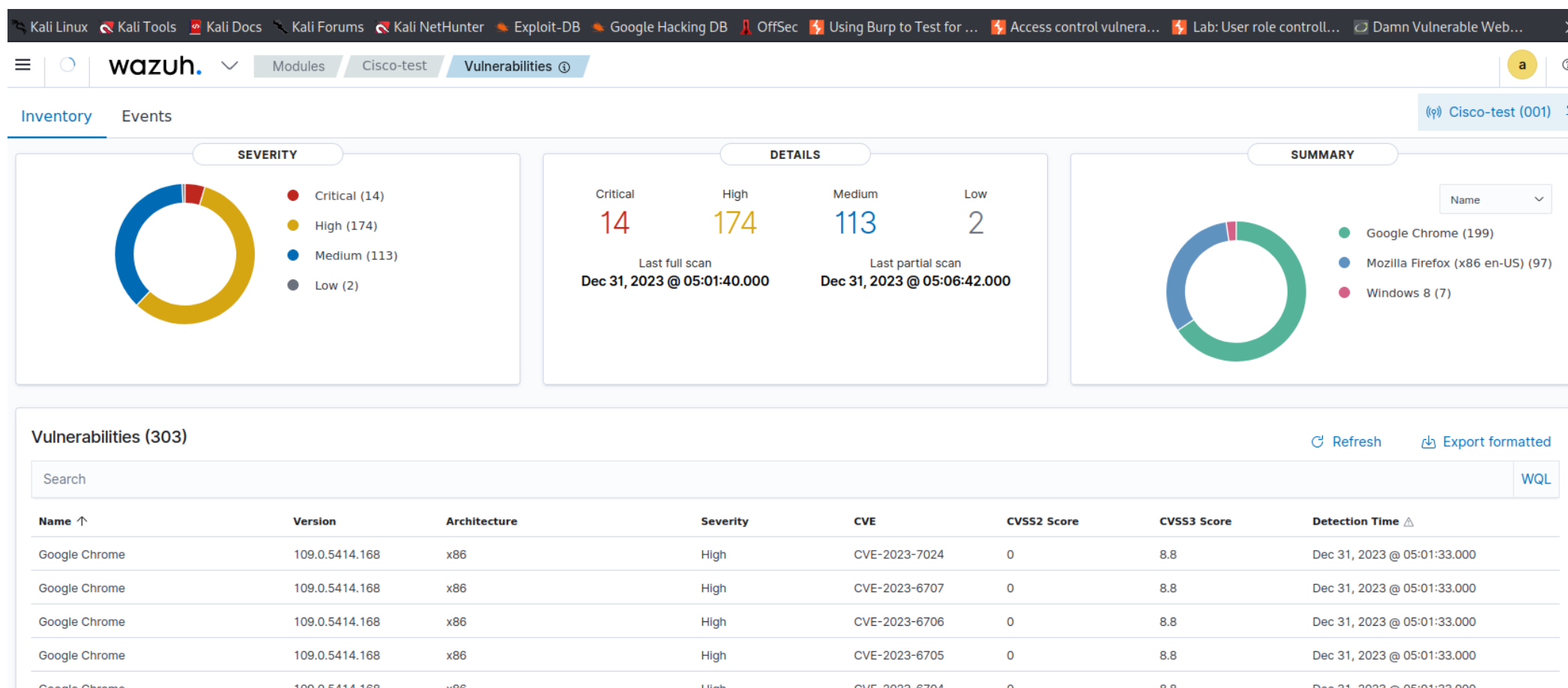
Dec 30 09:29:20 teresa-virtual-machine systemd[1]: Starting Wazuh agent...
Dec 30 09:29:20 teresa-virtual-machine env[3360]: Starting Wazuh v4.7.1...
Dec 30 09:29:22 teresa-virtual-machine env[3360]: Started wazuh-execd...
Dec 30 09:29:23 teresa-virtual-machine env[3360]: Started wazuh-agentd...
Dec 30 09:29:24 teresa-virtual-machine env[3360]: Started wazuh-syscheckd...
Dec 30 09:29:25 teresa-virtual-machine env[3360]: Started wazuh-logcollector...
Dec 30 09:29:26 teresa-virtual-machine env[3360]: Started wazuh-modulesd...
```

Wazuh Dashboard Agents Table:

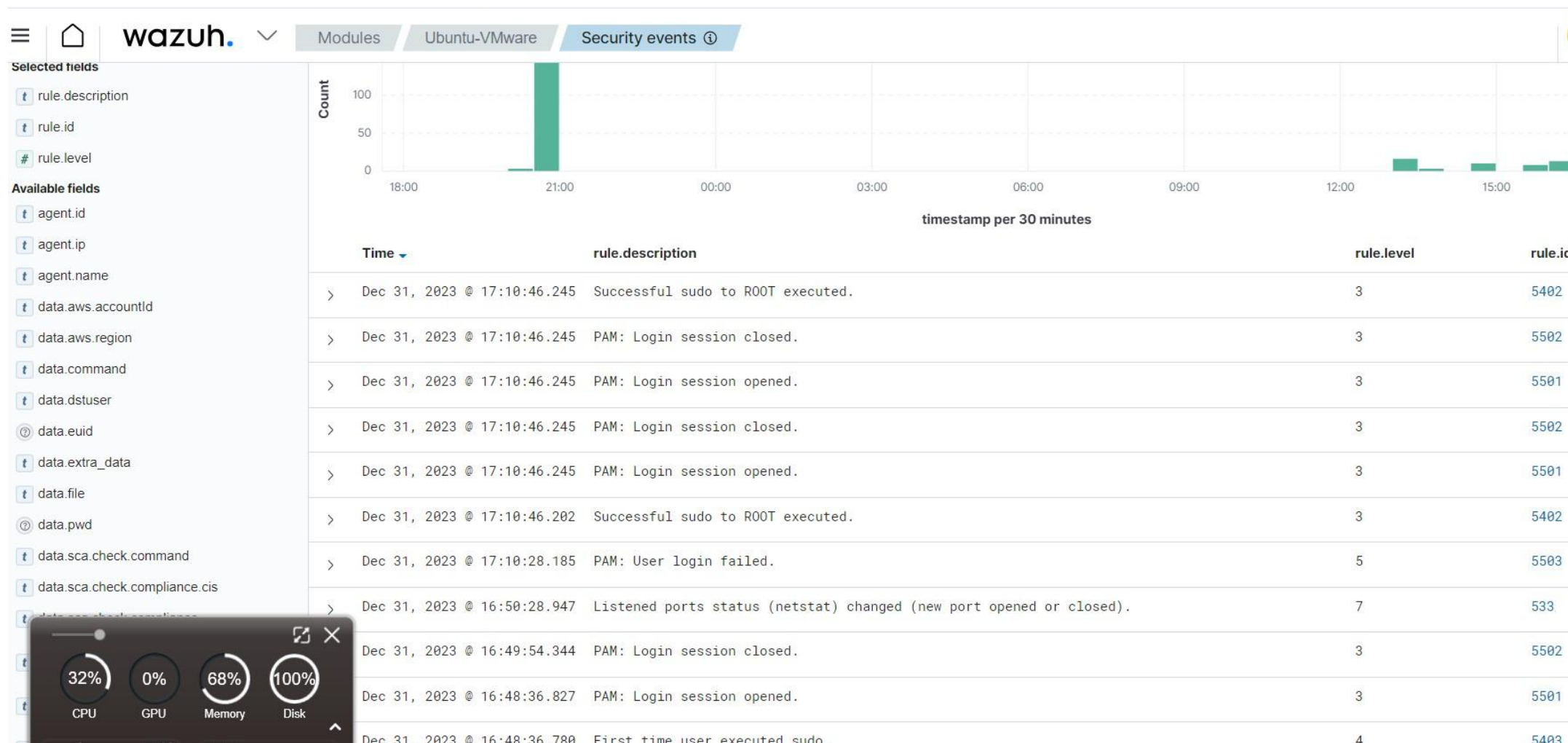
ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Cisco-test	192.168.68.104	default	Microsoft Windows 8 Pro 6.2.9200	node01	v4.7.1	active	View Refresh
002	Ubuntu-VMware	192.168.68.112	default	Ubuntu 22.04.3 LTS	node01	v4.7.1	active	View Refresh

After enabling the vulnerability detector in the Wazuh configuration files through wazuh dashboard we are able to detect vulnerabilities and do study on information from all the agent devices.

For example the windows 8 device has many vulnerabilities in the Chrome exe file. So it has to be updated to latest release:



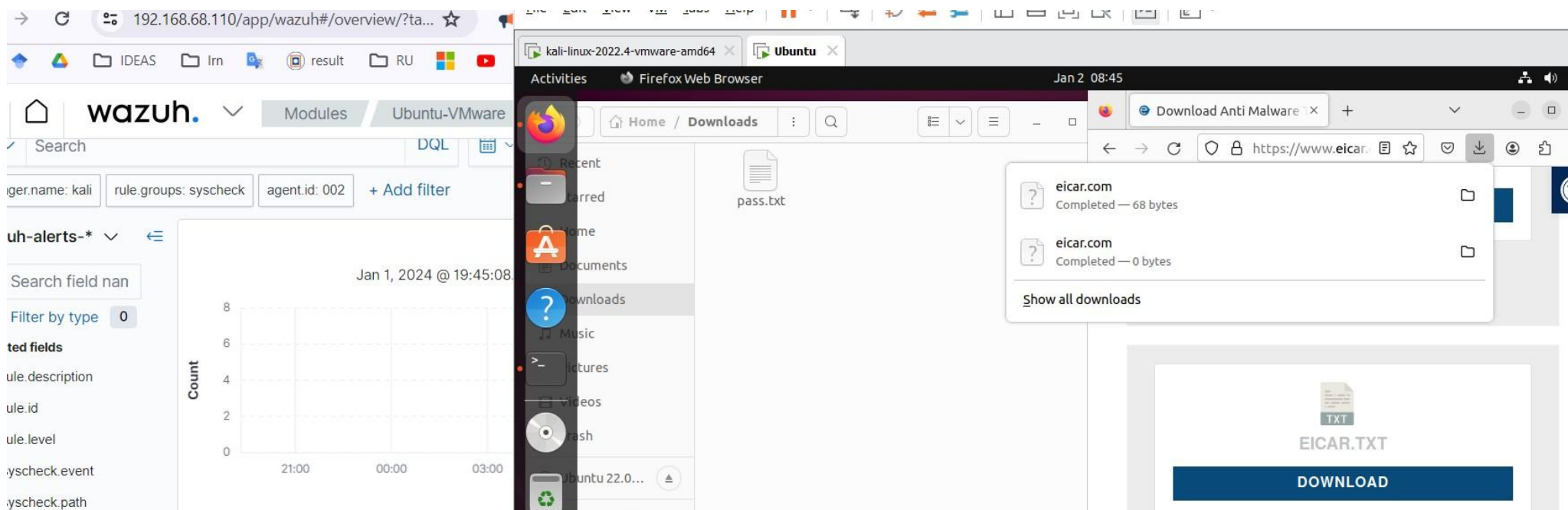
For the **Ubuntu device** since there we didn't find any vulnerabilities we can use AtomicRedTeam to apply some tactics on the device and those will also get monitored on the wazuh. Any sort of operations getting executed in the agent devices will get recorded in real time in the wazuh dashboard.



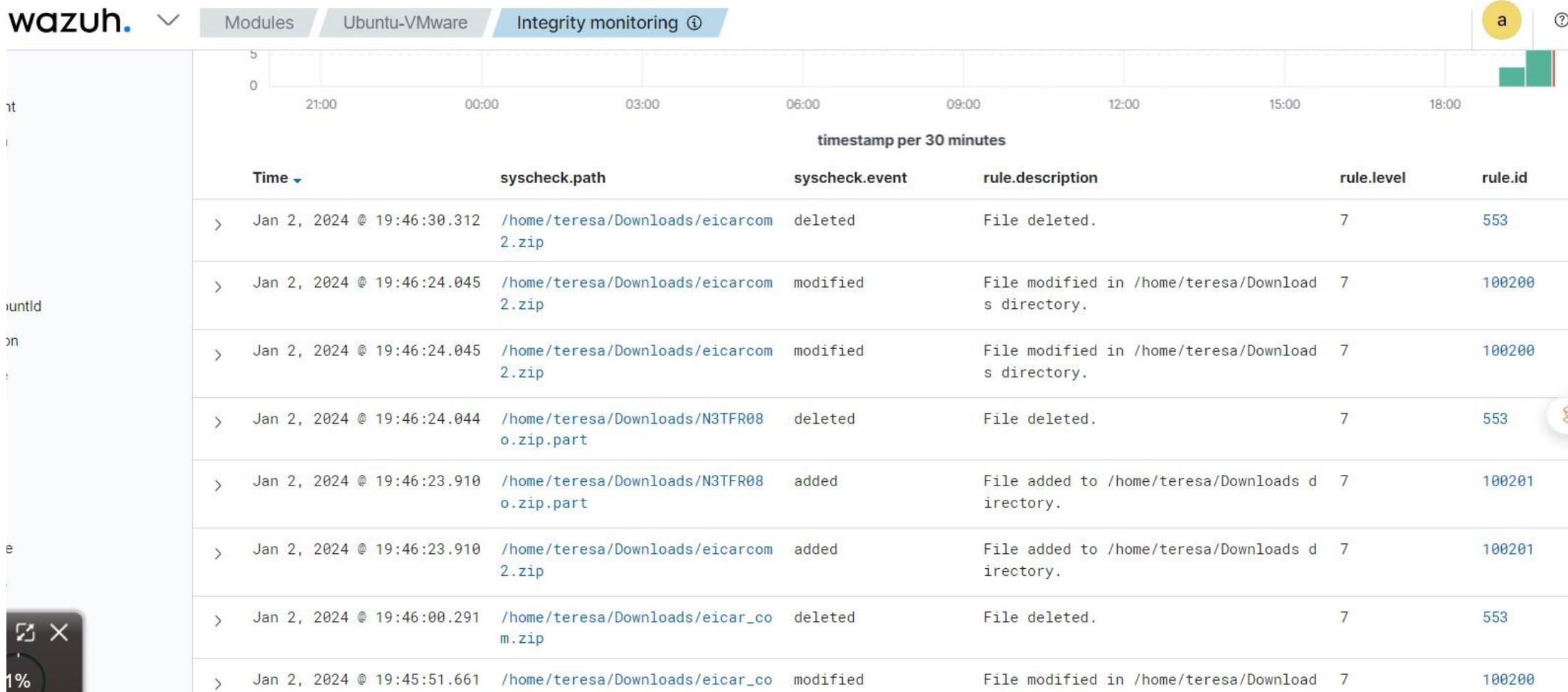
For getting **real-time updates** and Setting up **Active Responses** for the whole system or for a specific directory in Ubuntu we can integrate **Virustotal API** for malware detection and realtime removal.

For demonstration purpose here in the Ubuntu (Linux system) we will set up VirusTotal API and have Real-time Active response for downloading Malicious softwares.

After following directives and completing the setup following the Wazuh Virustotal API integration system from the Official website for the Server and the wazuh-agent device here is an example of how Wazuh with VirusTotal API integration, instantly removes malicious files downloaded from the web.



Files after downloading from eicar. com website are automatically getting deleted within seconds as they contain malicious codes and are listed in Virustotal as malicious files.



Wazuh is an SIEM solution where we can monitor, collect, and analyze logs from various sources to provide a centralized view of security events. It can be used for threat prevention, detection, and response. Our work here is done with the Wazuh- server being installed in Kali Linux device and we have two agents - ubuntu and Windows 8. Furthermore, Wazuh is capable of protecting workloads across on-premises, virtualized, containerized, and cloud-based environments.