# WAZUH

## ( PROJECT SUBMISSION )

**SUBMITTED TO:**
**SAURAV SHA**

**SUBMITTED BY:**
**MOHAMMED YASEEN V.A**

# INDEX

# INTRODUCTION

Wazuh is a threat prevention, detection, and response platform that is free and open source. It safeguards workloads on-premises, in virtualized, containerized, and cloud settings. Wazuh is utilized by hundreds of companies worldwide, ranging from tiny firms to major corporations. Wazuh is a security data collection, aggregation, indexing, and analysis tool that aids businesses in detecting intrusions, threats, and suspicious behavior.

Wazuh's platform includes security capabilities for cloud, container, and server applications. Log data analysis, intrusion and malware detection, file integrity monitoring, configuration assessment, vulnerability detection, and regulatory compliance help are examples of these services.

# UNDERSTANDING WAZUH

Understanding Wazuh begins with realizing that it is a free and open source security platform designed to provide extended detection and response (XDR) capabilities, with features such as security monitoring for endpoints and cloud workloads, threat detection and response, compliance management, log management and analysis, and vulnerability detection.

# OVERVIEW OF WAZUH AS A SECURITY PLATFORM

Wazuh is a comprehensive security information and event management (SIEM) platform designed to provide organizations with the tools and capabilities needed to monitor, detect, and respond to security threats. Here's an overview of Wazuh as a security platform:

1. **Log Management:**
    - Wazuh collects and centralizes log data from various sources, including system logs, application logs, and network logs.
    - The platform uses decoders to normalize and parse log data, making it easier to analyze and correlate security events.
2. **Intrusion Detection:**
    - The intrusion detection system (IDS) component analyzes log data in real-time, triggering alerts based on rule matches.
3. **Vulnerability Detection:**
    - Wazuh helps identify vulnerabilities in monitored systems by comparing configurations and software versions against known vulnerabilities.
    - Vulnerability detection contributes to proactive security measures and risk mitigation.

4. **Real-time Threat Detection:**
    - The Wazuh manager provides real-time monitoring and analysis of security events, enabling rapid detection of malicious activities.
5. **Scalability:**
    - Wazuh is designed to scale horizontally, allowing organizations to deploy multiple managers to handle a large number of agents and data sources.
6. **Integration with ELK Stack:**
    - Wazuh integrates with the ELK stack, utilizing Elasticsearch for data storage, Logstash for data processing, and Kibana for visualization and analysis.
    - The integration with ELK provides a powerful and flexible platform for exploring and visualizing security data.
7. **Agent-Based Architecture:**
    - Wazuh agents are deployed on monitored systems, collecting and forwarding log data to the Wazuh manager.
    - Agents perform local log analysis, integrity checking, and rootkit detection, enhancing the platform's ability to detect threats at the endpoint level.
8. **Customizable Rules and Decoders:**
    - Organizations can customize rules and decoders to adapt Wazuh to their specific security requirements and environment.
9. **Active Responses:**
    - Wazuh supports active responses that enable automated reactions to security events.
    - Active responses can include blocking IP addresses, executing custom scripts, or sending notifications to security personnel.
10. **Compliance Monitoring:**
    - Wazuh provides features to help organizations monitor and maintain compliance with industry regulations and security standards.
11. **Threat Intelligence Integration:**
    - Wazuh can be configured to integrate with threat intelligence feeds, enhancing its ability to identify and respond to known malicious activity.

# KEY FEATURES OF WAZUH

Wazuh offers a range of features including endpoint and cloud workload security monitoring, threat detection and response, compliance management, log analysis, and vulnerability detection explore these features further to see how Wazuh can benefit your organization.

# SECURITY MONITORING FOR ENDPOINTS AND CLOUD WORKLOADS

Wazuh provides a comprehensive security monitoring solution for endpoints and cloud workloads. It allows users to monitor all activity, including file changes, network connections, user behavior, and privileged account access. With Wazuh, you can detect threats in real-time and respond quickly to mitigate any risks.

For example, let's say an employee is working remotely using their laptop. Wazuh can monitor the device for any unauthorized access attempts or malware infections. If it detects any suspicious activity like multiple failed login attempts from different IP addresses or unusual data transfers outside of regular business hours, it will alert the security team immediately so they can investigate further.

Similarly, if your organization uses cloud services like Amazon Web Services (AWS) or Microsoft Azure Wazuh provides an agent that integrates with these platforms to provide enhanced protection for your cloud workloads. This ensures that you are always aware of who is accessing your resources and what they're doing once inside

# THREAT DETECTION AND RESPONSE

Wazuh provides a robust platform for threat detection and response, allowing organizations to monitor, analyze, and respond to security events in real-time. Here's an overview of how Wazuh facilitates threat detection and response:

**Threat Detection:**

1. Intrusion Detection:
2. Log Analysis:
3. Vulnerability Detection:
4. File Integrity Monitoring (FIM):
5. User Activity Monitoring:
6. Network Security Monitoring:
7. Threat Intelligence Integration:

**Threat Response:**

1. Active Responses:
2. Automated Incident Response:
3. Integration with External Tools:
4. Incident Response Planning:
5. Incident Investigation and Forensics:
6. Real-time Alerting:
7. Dashboard and Reporting:
8. Continuous Monitoring:

By combining threat detection and response capabilities, Wazuh provides organizations with a comprehensive security solution to proactively identify and mitigate potential threats. Regular updates, continuous monitoring, and collaboration between security teams enhance the effectiveness of Wazuh in threat detection and response scenarios.

# COMPLIANCE MANAGEMENT

Compliance management is one of the core features of Wazuh, making it an ideal solution for organizations that need to meet regulatory and compliance requirements. Wazuh provides a range of tools to help you manage compliance, including policy templates, automated scans, and alerts that notify you when there are potential issues.

Using Wazuh's compliance management feature can save your organization a lot of time and effort by automating many routine tasks. For example, you can use the pre-configured policies included with Wazuh or create custom ones that match your organization's specific needs. These policies automatically scan endpoints and cloud workloads for security vulnerabilities and deviations from best practices related to various regulations like SOC 2, GDPR or HIPAA so you can identify gaps in your security posture quickly.

# LOG MANAGEMENT AND ANALYSIS

Log management and analysis is a crucial component of the Wazuh security platform. In short, it involves collecting and analyzing logs generated by various systems and applications to detect potential security threats. With Wazuh, log data can be gathered from endpoints, cloud workloads, and other sources, providing valuable insights for incident response and compliance management.

One benefit of log management with Wazuh is that it allows for real-time monitoring of system activity. By aggregating logs in a central location, potential issues can be identified quickly instead of having to sift through individual device or application logs separately. Additionally, advanced analytics capabilities are built into the platform which allow for automated detection of suspicious behavior or patterns within log data. Overall, proper use of log management and analysis through Wazuh can greatly enhance overall cybersecurity posture.

# VULNERABILITY DETECTION

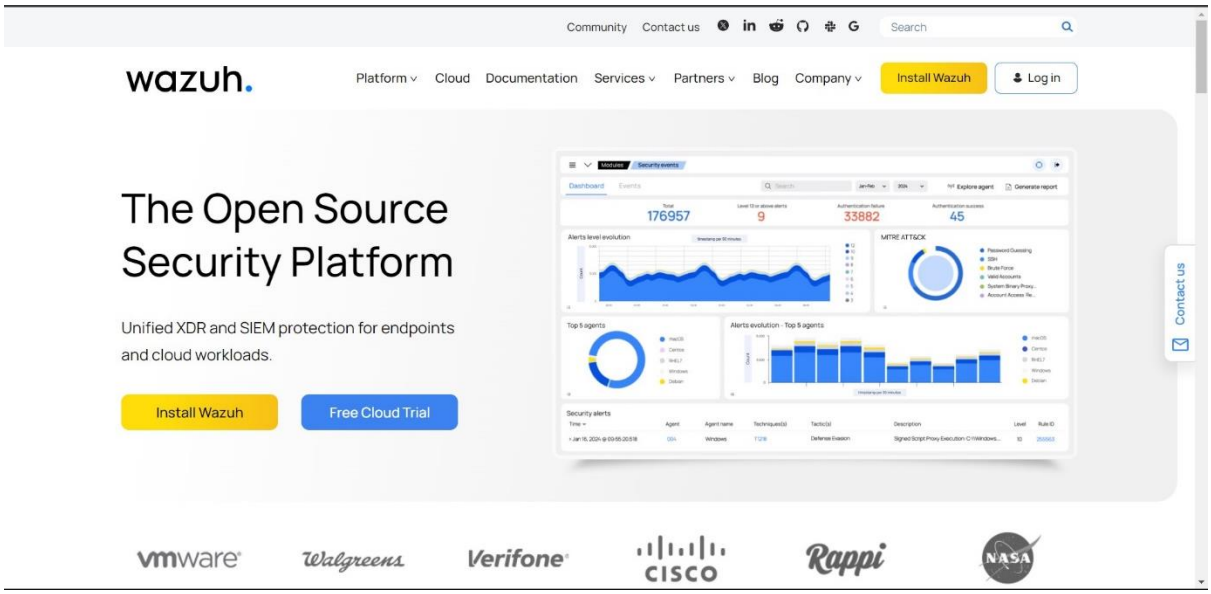
Vulnerability detection is a key feature of Wazuh that helps to identify and mitigate any vulnerabilities in your system. With Wazuh, you can detect known vulnerabilities in applications, operating systems or network services before they are exploited by attackers. This feature allows you to prioritize remediation efforts and reduce the risk of exploitation.

Wazuh uses active scanning techniques to conduct vulnerability assessments on both cloud workloads and endpoints. The platform also provides continuous monitoring of your systems for new vulnerabilities so that you can stay on top of any potential security risks. Additionally, Wazuh's compliance management feature ensures that your organization stays compliant with industry regulations such as PCI DSS or HIPAA.

Overall, vulnerability detection is just one of many powerful features offered by the open-source security platform Wazuh. By using this tool, businesses can be proactive in identifying potential vulnerabilities before they become major issues which could lead to costly damage or breaches.

# WAZUH INSTALLING PROCESS

**Open wazuh site in browser [https://wazuh.com/](https://wazuh.com/)**

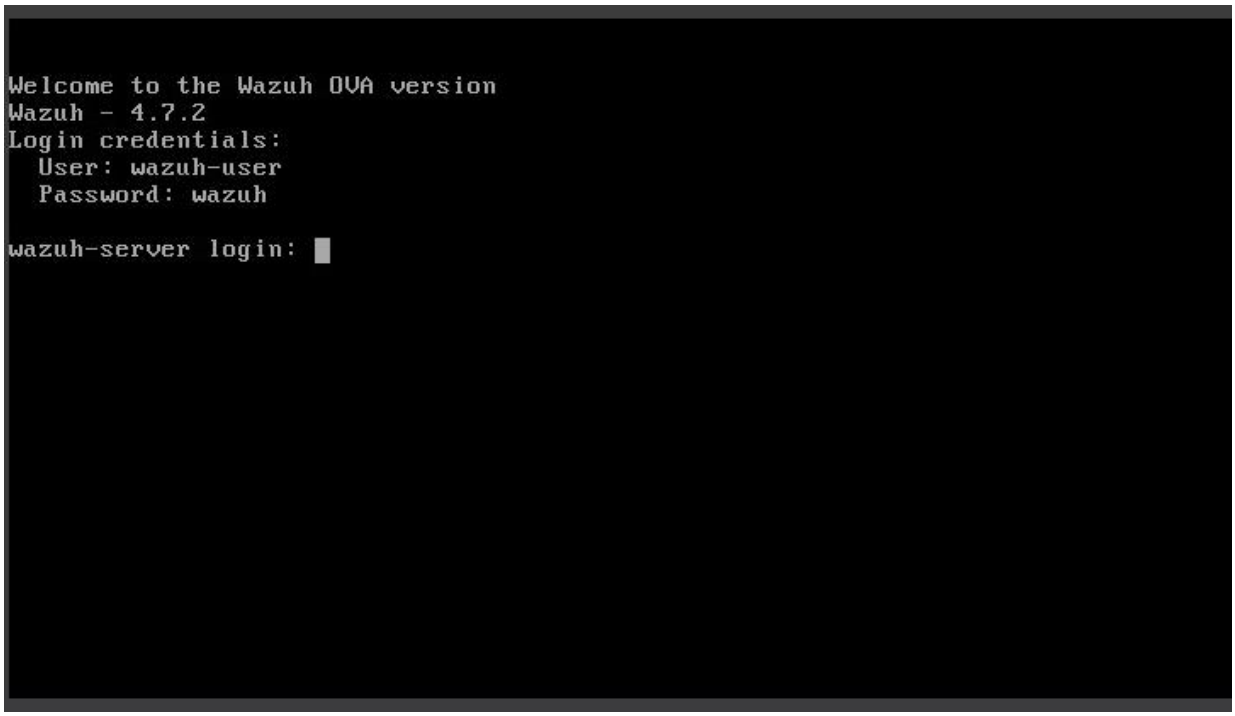



Go to Install wazuh  - Quickstart – Installation alternatives.

From there download the virtual machine (OVA) file.

Import the downloaded ova file to the virtual box and start the machine. Before starting the machine we need to configure its display settings to VMSVGA option.

Then we will get a login Screen.




Login with given credentials.

Root privilege escalation can be achieved by executing the following command: sudo -i.

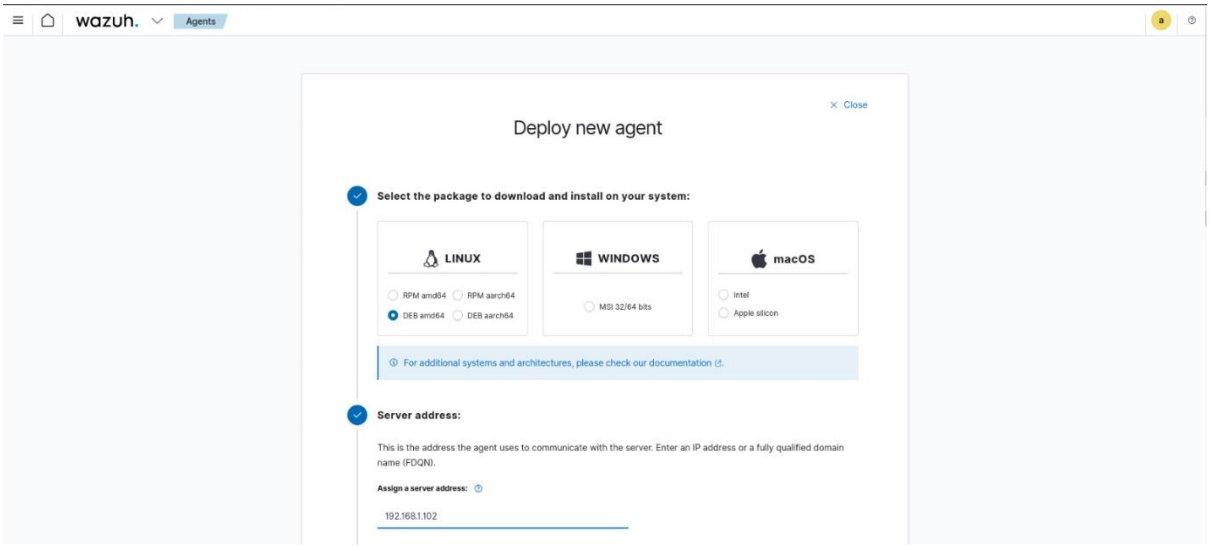
We can find <wazuh_server_ip> by typing the following command: ifconfig.

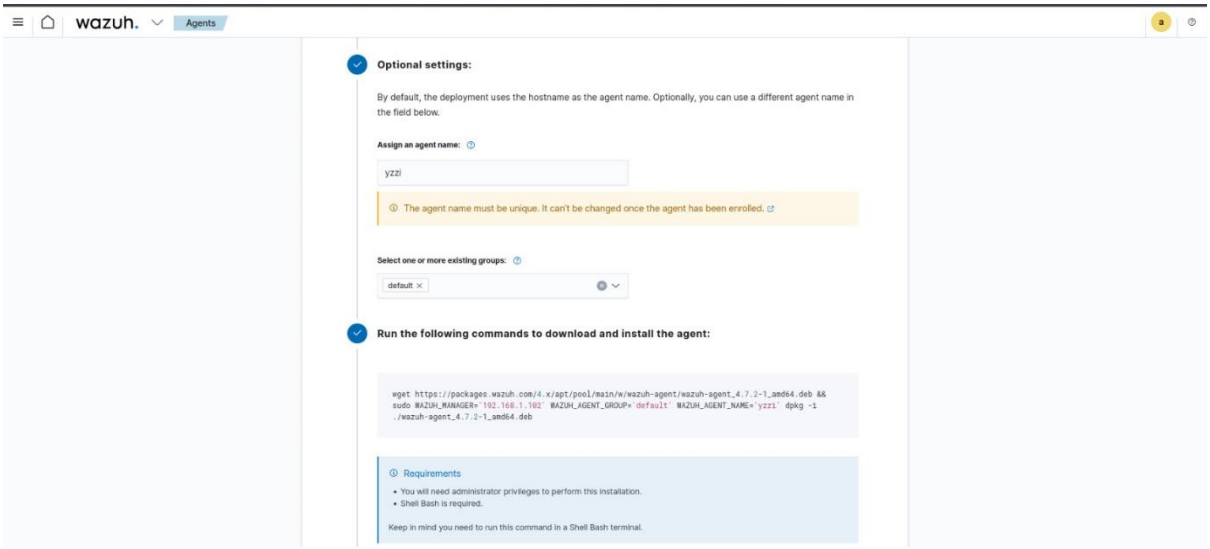
```
        WAZUH Open Source Security Platform
                https://wazuh.com


[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.102  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fecc:e32e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cc:e3:2e  txqueuelen 1000  (Ethernet)
        RX packets 106  bytes 22633 (22.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 149  bytes 12734 (12.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 686  bytes 138114 (134.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 686  bytes 138114 (134.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

`[root@wazuh-server ~]#
```

Now open a browser in kali and paste the server ip, then we will get login page of a wazuh. Login with username and password admin:admin respectively.

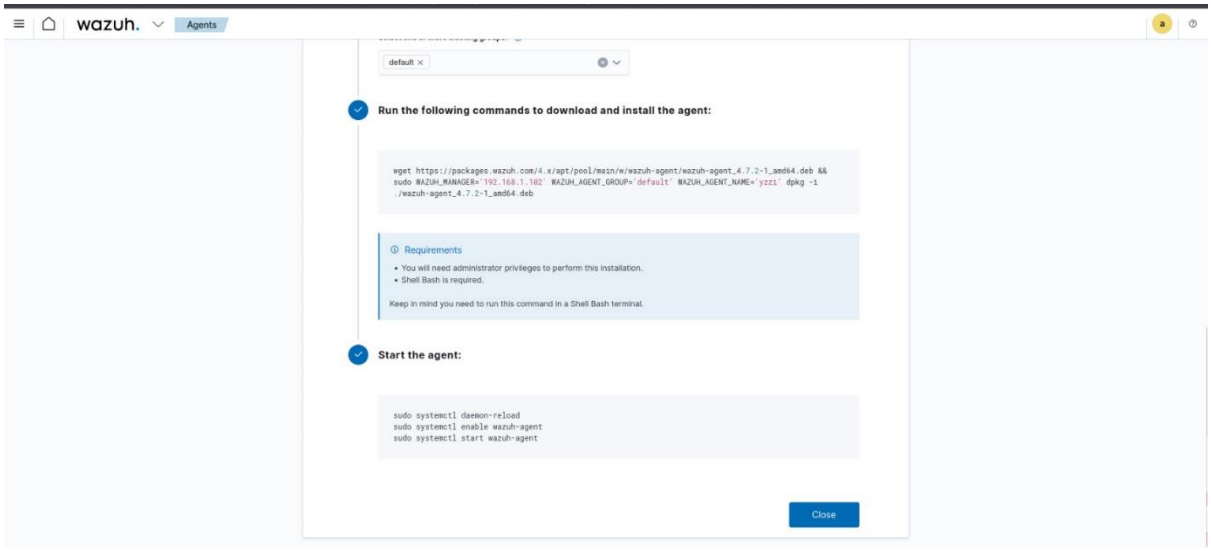

To add the agent, select Agents from the dropdown list.

Now we will get a page to configure the agent. Select the options according to our system.

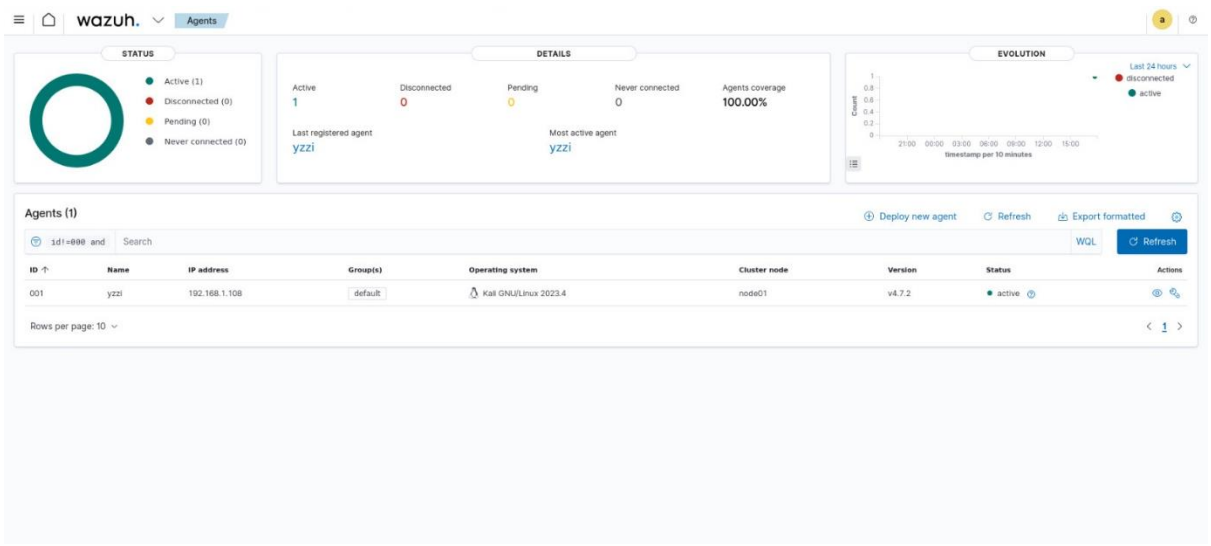


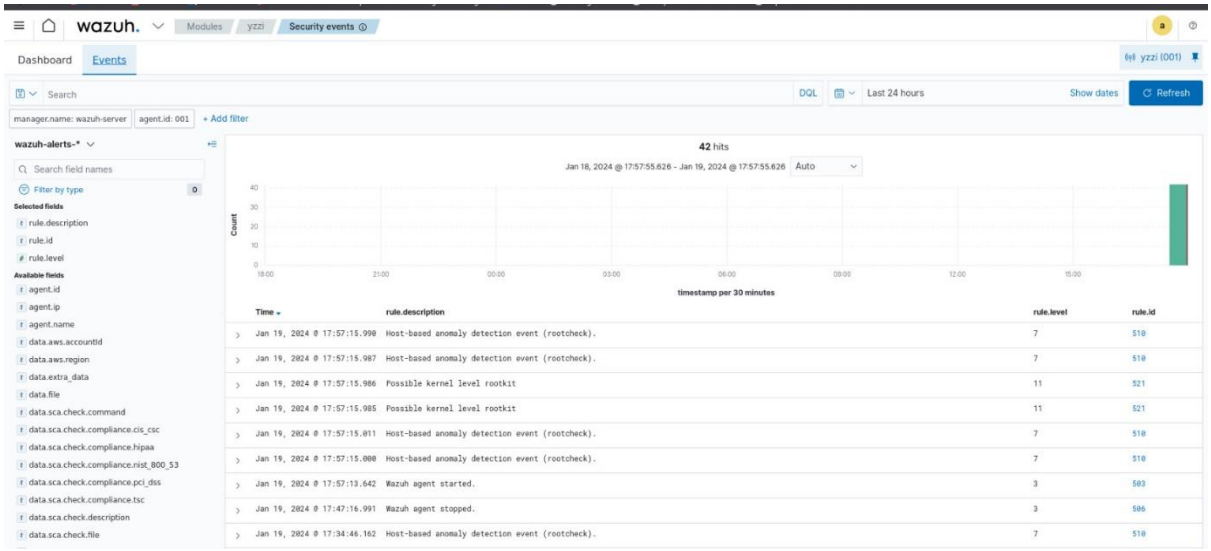

Run the following commands to download and install the agent.




Start the agent,




Here we see added agent is active also we can check the security events. To check the logs select modules in dropdown list and select security events.


wazuh.
Modules
yzzi
Security events
Dashboard
Events
yzzi (001)
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
agent.id: 001
+ Add filter
wazuh-alerts-*
Search field names
Filter by type
Selected fields
rule.description
rule.id
rule.level
Available fields
agent.id
agent.ip
agent.name
data.aws.accountId
data.aws.region
data.extra_data
data.file
data.sca.check.command
data.sca.check.compliance.cis_csc
data.sca.check.compliance.hipaa
data.sca.check.compliance.nist_800_53
data.sca.check.compliance.pci_dss
data.sca.check.compliance.tsc
data.sca.check.description
data.sca.check.file
42 hits
Jan 18, 2024 @ 17:57:55.626 - Jan 19, 2024 @ 17:57:55.626
Auto
Count
timestamp per 30 minutes
Time
rule.description
rule.level
rule.id
Jan 19, 2024 @ 17:57:15.990 Host-based anomaly detection event (rootcheck). 7 510
Jan 19, 2024 @ 17:57:15.987 Host-based anomaly detection event (rootcheck). 7 510
Jan 19, 2024 @ 17:57:15.986 Possible kernel level rootkit 11 521
Jan 19, 2024 @ 17:57:15.985 Possible kernel level rootkit 11 521
Jan 19, 2024 @ 17:57:15.011 Host-based anomaly detection event (rootcheck). 7 510
Jan 19, 2024 @ 17:57:15.000 Host-based anomaly detection event (rootcheck). 7 510
Jan 19, 2024 @ 17:57:13.642 Wazuh agent started. 3 503
Jan 19, 2024 @ 17:47:16.991 Wazuh agent stopped. 3 506
Jan 19, 2024 @ 17:34:46.162 Host-based anomaly detection event (rootcheck). 7 510

# WAZUH TRYHACKME

1.When was Wazuh released?

2015

Explanation: Given on introduction.

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

Agent

Explanation: This was in the reading. It’s the relationship between this and manager.

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

Manager

Explanation: Manager is responsible for managing devices

4. How many agents does this Wazuh management server manage?

2

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

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

Disconnected

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

6. 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

Explanation: 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.

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

Sysmon

Explanation: From the reading, Sysmon is used.

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

Event Viewer.

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

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

/var/ossec/ruleset/rules

Explanation: This one can be found within the reading.

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

Audit

Explanation: This can be found in the reading.

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

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

Explanation: This can be found in the reading.

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

Curl

Explanation: This is found in the reading, near the beginning.

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

Get

Explanation: This can be found in the reading.

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

Put

Explanation: This can be found in the reading.

15. 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

Explanation: 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.

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

agent-001

Explanation: 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.

# CONCLUSION

In conclusion, Wazuh is a powerful and versatile security platform that offers protection for endpoints and cloud workloads. Its key features include threat detection and response, compliance management, log management and analysis, and vulnerability detection. With the help of its all-in-one dashboard and user-friendly WUI, users can easily register agents, monitor events in realtime, and implement best practices to secure their systems. As an open-source software with no licensing fees attached, Wazuh offers businesses of all sizes a cost-effective solution for their cybersecurity needs. So, whether you're a road warrior or working within your organization's security operations centre (SOC), consider giving Wazuh a try to stay ahead of cyber threats today!