Wazuh Brute Force Detection Test Report

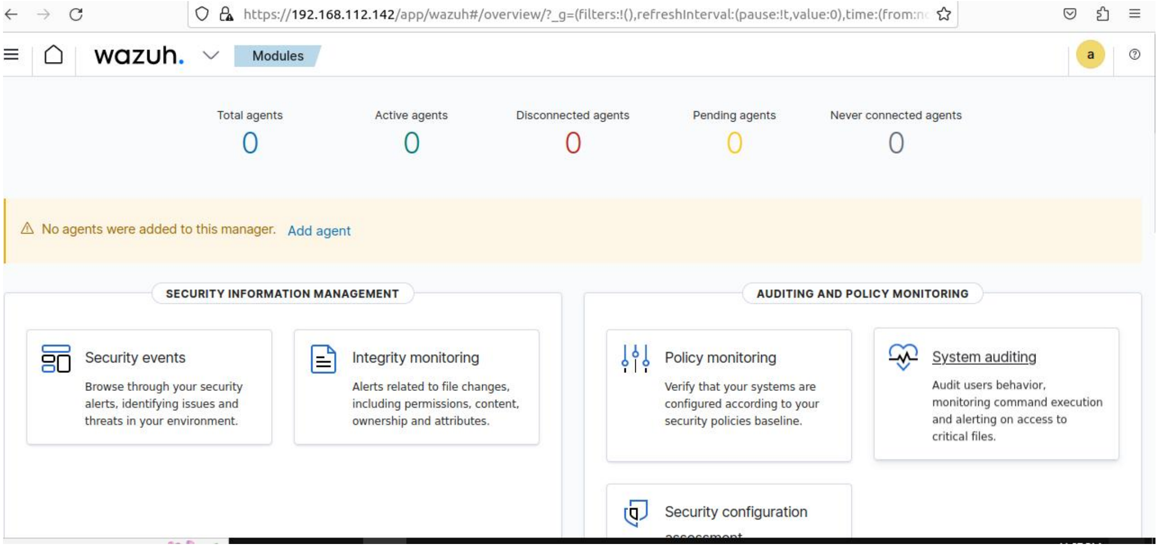
1. Introduction

This report documents the process of setting up a Wazuh SIEM environment with a Windows agent, simulating a brute force attack, and verifying alert generation and email notifications.

2. Environment Setup

The following components were used:

- - Wazuh Manager (Ubuntu 20.04, version 4.7)
- - Wazuh Dashboard
- - Windows Agent (Windows 10)



https://192.168.112.142/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:n

Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
0	0	0	0	0

⚠ No agents were added to this manager. Add agent

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.

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.

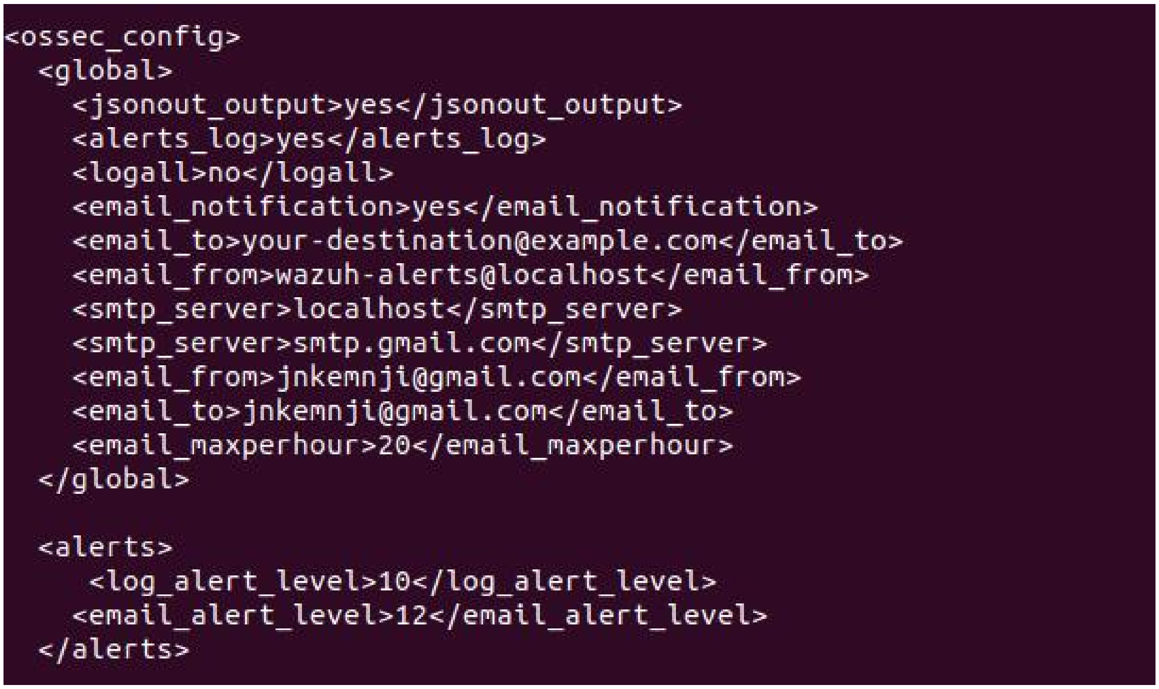
wazuh.
Modules
a
SECURITY INFORMATION MANAGEMENT
AUDITING AND POLICY MONITORING
Security configuration assessment

Figure 2.1: Wazuh Dashboard Overview (screenshot placeholder)

3. Configuration

Key configuration steps included:

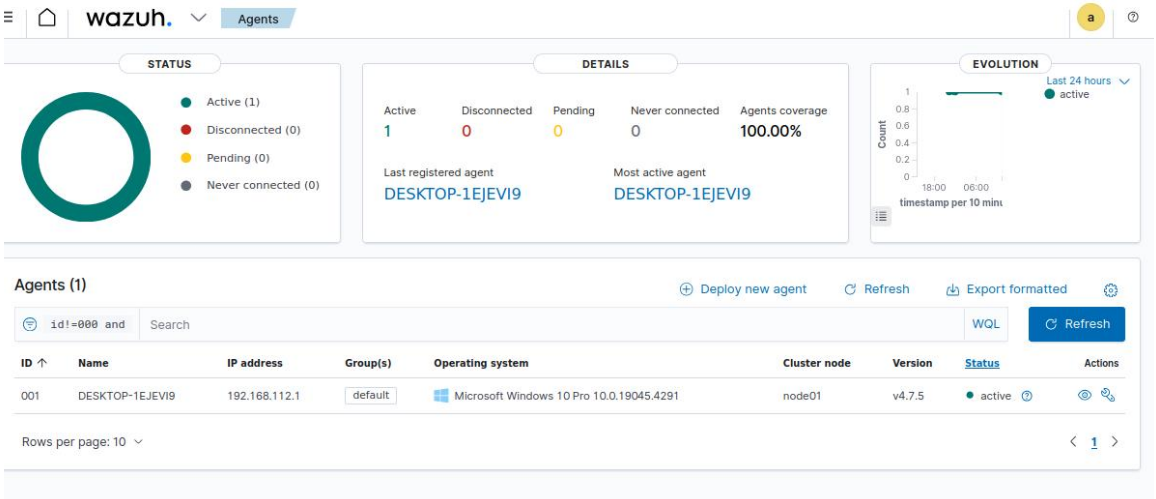
- - Setting up email alerts in ossec.conf
- - Registering and verifying the Windows agent



```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <email_notification>yes</email_notification>
    <email_to>your-destination@example.com</email_to>
    <email_from>wazuh-alerts@localhost</email_from>
    <smtp_server>localhost</smtp_server>
    <smtp_server>smtp.gmail.com</smtp_server>
    <email_from>jnkemnji@gmail.com</email_from>
    <email_to>jnkemnji@gmail.com</email_to>
    <email_maxperhour>20</email_maxperhour>
  </global>

  <alerts>
     <log_alert_level>10</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>
```

Figure 3.1: ossec.conf Email Configuration (screenshot placeholder)



Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

Last registered agent: DESKTOP-1EJEVI9

Most active agent: DESKTOP-1EJEVI9

Agents (1)

id!=000 and Search

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	DESKTOP-1EJEVI9	192.168.112.1	default	Microsoft Windows 10 Pro 10.0.19045.4291	node01	v4.7.5	● active	

Figure 3.2: Windows Agent Registration Output (screenshot placeholder)

4. Attack Simulation and Testing

A brute force attack was simulated on the Windows agent by performing multiple failed login attempts. Event ID 4625 was triggered repeatedly to mimic an unauthorized access attempt.

5. Results

The Wazuh Manager successfully detected the brute force pattern and triggered an alert. The alert was visible on the Wazuh Dashboard and classified with an appropriate rule ID and severity.

6. Conclusion

The simulation demonstrated that Wazuh can effectively detect brute force attacks from a Windows agent. This validates the alerting and monitoring capability of the Wazuh SIEM system.