

Wazuh SIEM Lab - Threat Detection Project

Name: Blaze

Date Completed: April 02, 2025

Overview:

Built and configured a Wazuh-based open-source SIEM lab using Ubuntu Server and Elastic Stack. Simulated real-world attacks such as SSH brute-force attempts and privilege escalation. Verified detection through real-time alerts and rule matches, mapped to MITRE ATT&CK techniques.

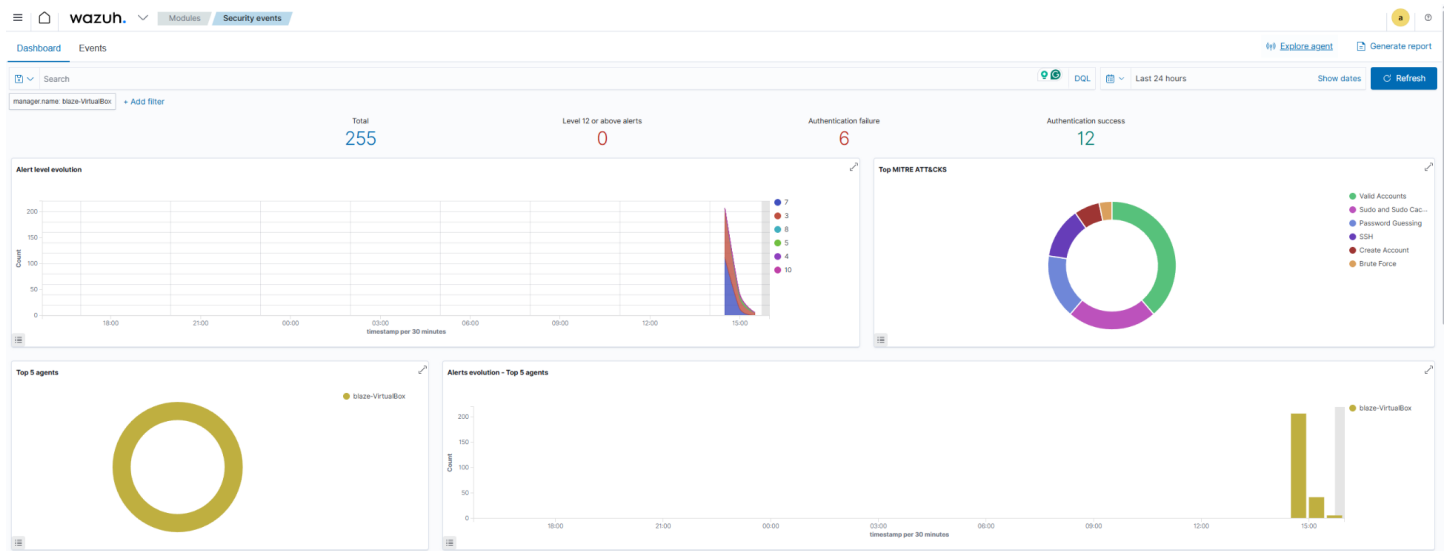
Threats Simulated:

- SSH brute-force (invalid user attempts)
- Privilege escalation (/etc/shadow access)
- File access and sudo command logging

Highlighted Features:

- Real-time alerting in Wazuh Dashboard
- MITRE-aligned detections (T1110.001, T1548.003)
- Visual correlation of system activity and alerts

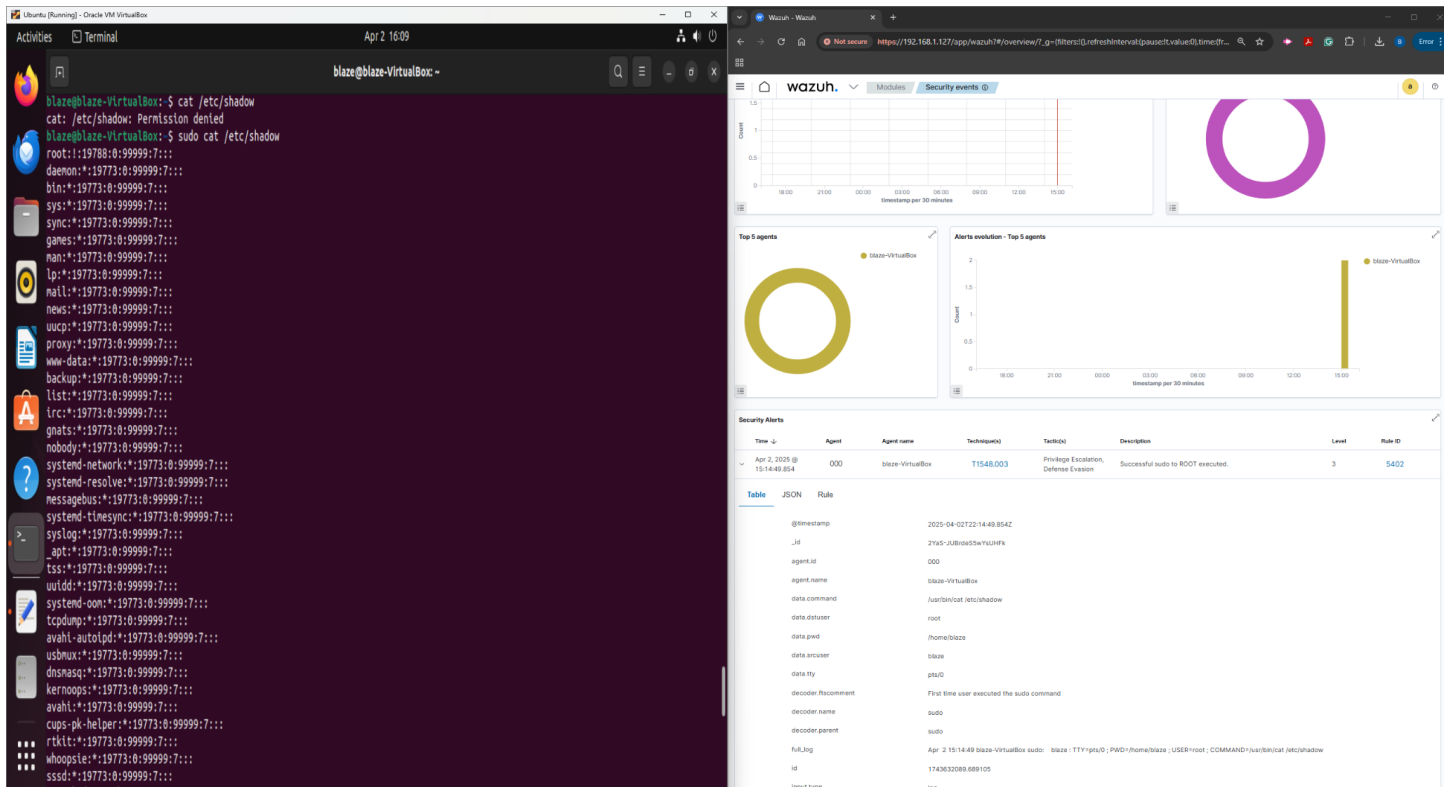
Wazuh SIEM Lab - Threat Detection Project



Screenshot 1 - Wazuh System Overview:

Wazuh dashboard showing active agent (blaze-VirtualBox), real-time alerts, top MITRE techniques triggered, and authentication statistics from the simulated attack scenarios.

Wazuh SIEM Lab - Threat Detection Project



Screenshot 2 - Privilege Escalation via `/etc/shadow`:

Attempted to access a protected file without permissions, followed by a successful ``sudo`` read. Wazuh detected the event and logged it as a successful escalation to root - MITRE technique T1548.003.

The image shows a Kali Linux virtual machine environment. On the left, a terminal window displays the installation and configuration of OpenSSH. The user is at the prompt `blaze@blaze-VirtualBox:~`. The terminal output shows the installation of `openssh-server` and `openssh-client` packages, followed by the configuration of the `ssh` service. The user attempts to connect to `localhost` using `ssh`, but the connection is denied because the host is not known. The user is prompted to add the host to the list of known hosts.

On the right, the Wazuh dashboard is visible. It shows the following sections:

- Alert level evolution:** A line graph showing the count of alerts over time. The count is 0 for most of the day, with a spike to 3 at 15:00.
- Top MITM ATTACKS:** A donut chart showing the distribution of MITM attacks. The chart is divided into two segments: Password Cracking (blue) and SSH (purple).
- Top 5 agents:** A donut chart showing the distribution of agents. The chart is divided into two segments: Blaze-VirtualBox (yellow) and another agent (blue).
- Alerts evolution - Top 5 agents:** A line graph showing the count of alerts over time for the top 5 agents. The count is 0 for most of the day, with a spike to 4 at 15:00.
- Security Alerts:** A table listing security alerts. The table has columns for Time, Agent, Agent name, Technique(s), Tactic(s), Description, Level, and Rule ID.

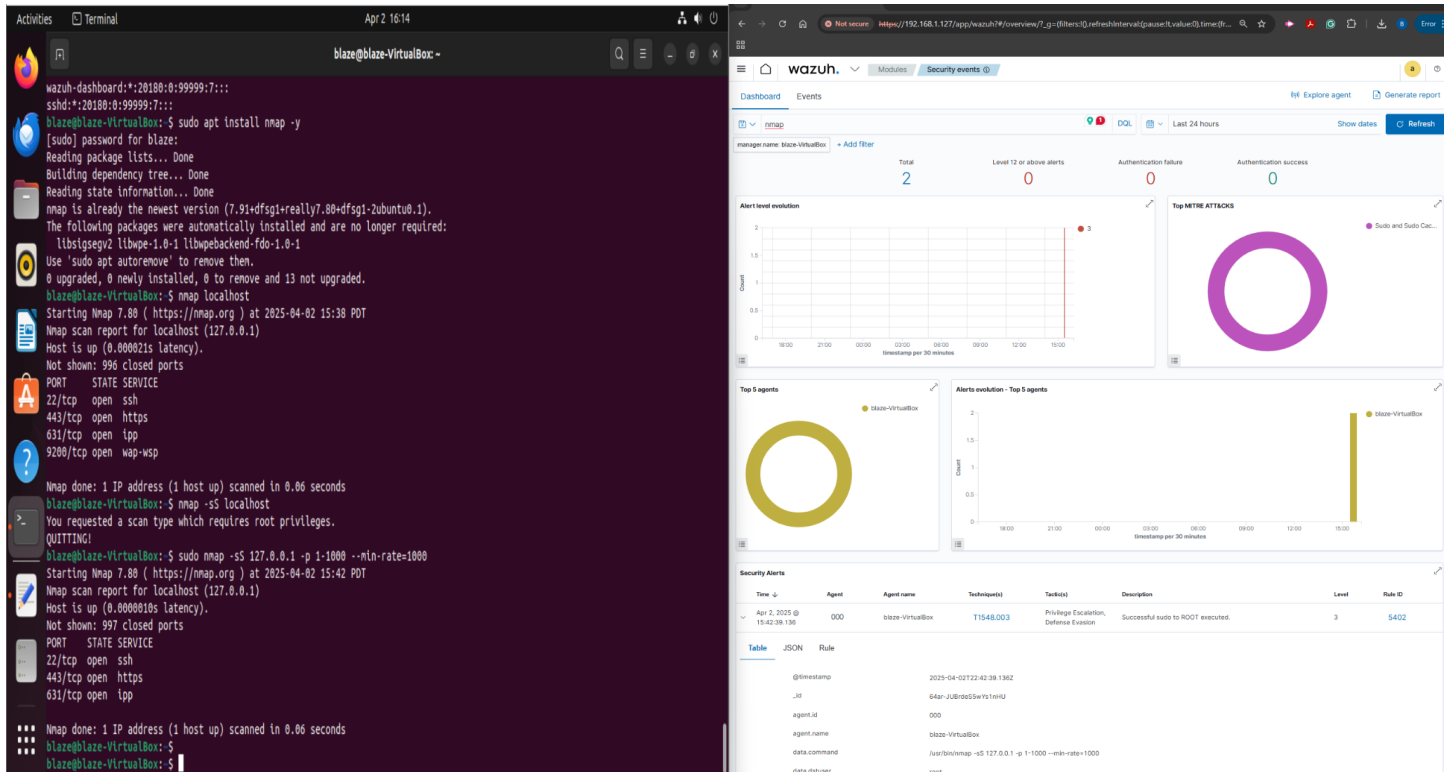
Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 2, 2023 @ 15:02:58.592	000	blaze-VirtualBox	T1110.001 T1021.004	Credential Access, Lateral Movement	ssh: Attempt to login using a non-existent user	5	5710

The table also includes a section for the alert details, showing the following information:

- @timestamp:** 2023-04-02T12:03:58.592Z
- _id:** zoe-Ju8d85wrxn0g
- agent.id:** 000
- agent.name:** blaze-VirtualBox
- data.origin:** 127.0.0.1
- data.processor:** invaliduser
- decoder.name:** sshd
- decoder.namespace:** sshd

Simulated multiple failed SSH login attempts using a non-existent user ('invaliduser'). Wazuh logged the activity and correlated it to MITRE T1110.001 (Password Guessing) and T1021.004 (Lateral Movement).

Wazuh SIEM Lab - Threat Detection Project



Screenshot 4 - Nmap Recon Scan:

Terminal shows `nmap` being installed and executed against localhost with custom flags to simulate aggressive scanning behavior. Wazuh detected the scan and logged a privilege escalation alert (MITRE T1548.003).