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.

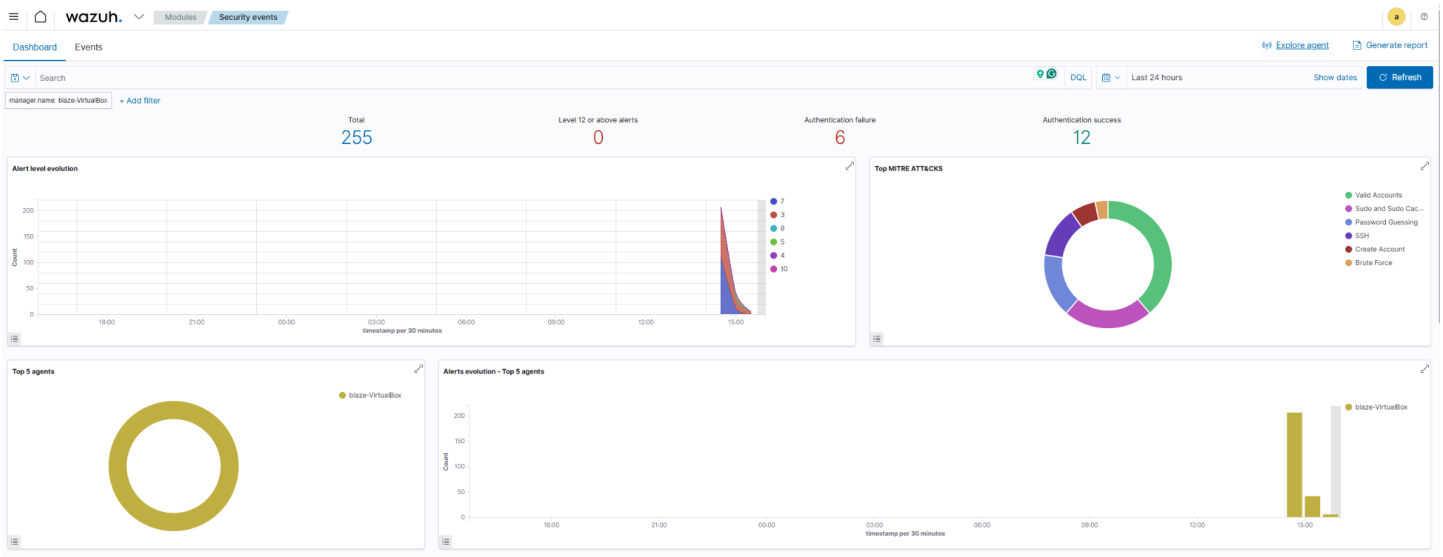
Threats Simulated:

- 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

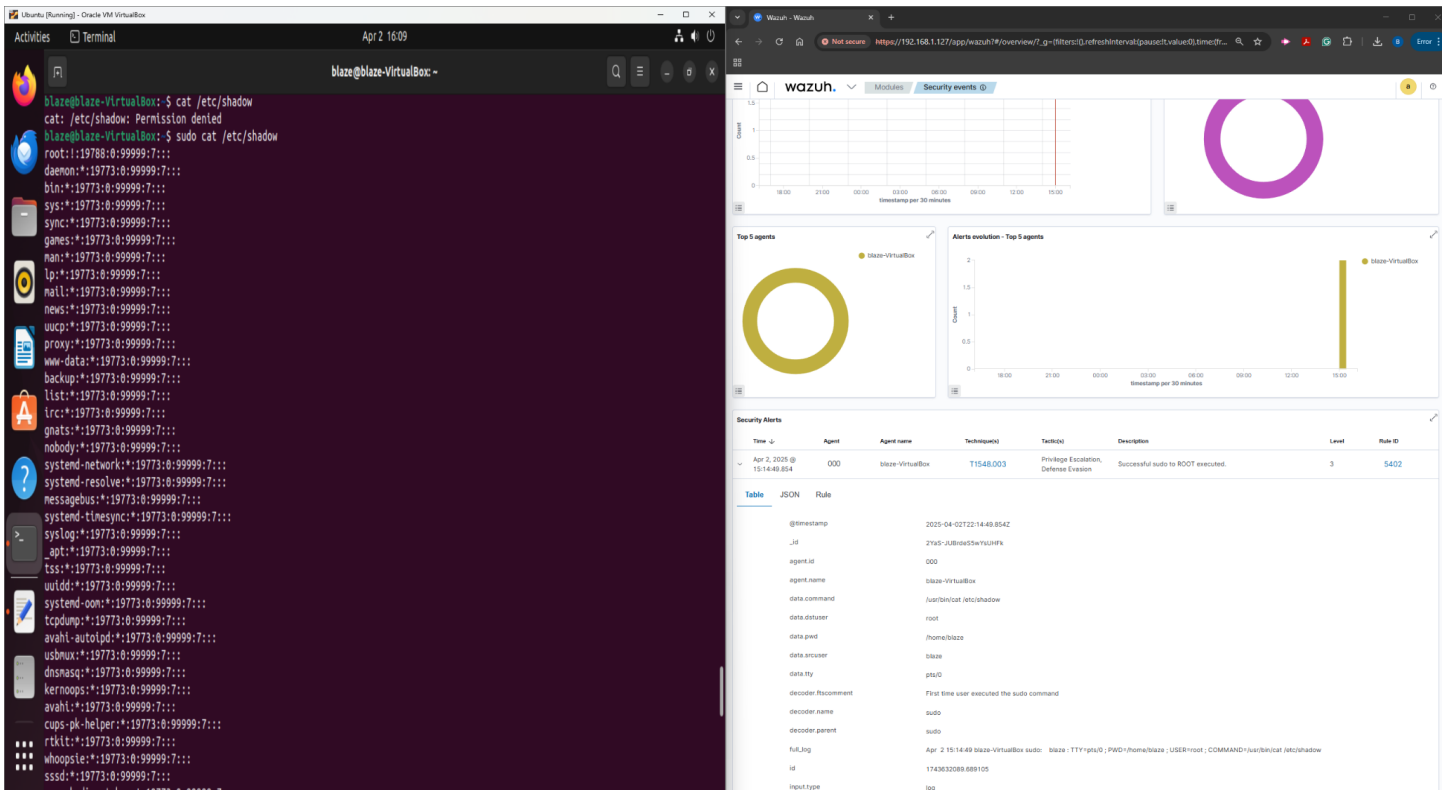
Wazuh SIEM Lab - Threat Detection Project



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.

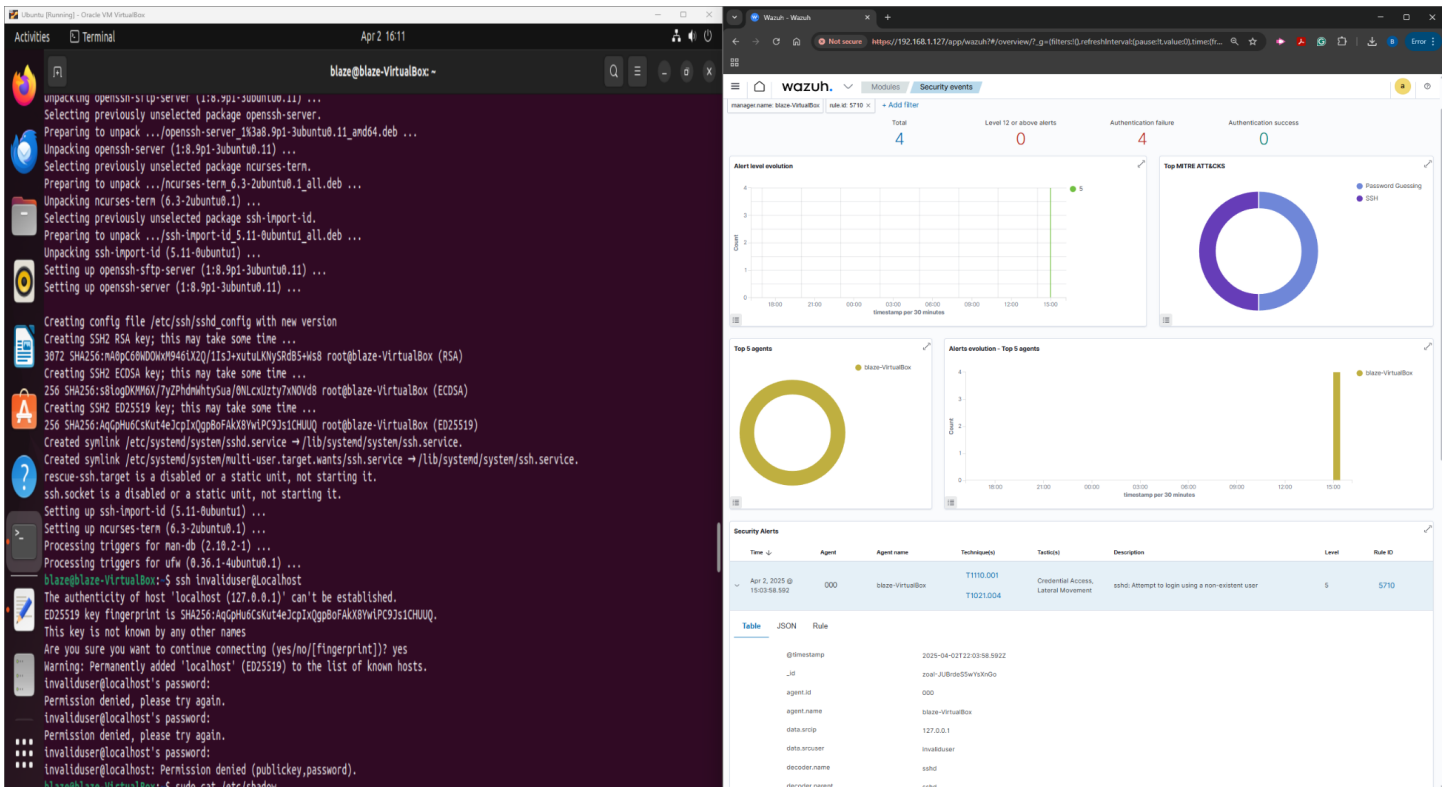
Wazuh SIEM Lab - Threat Detection Project



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.

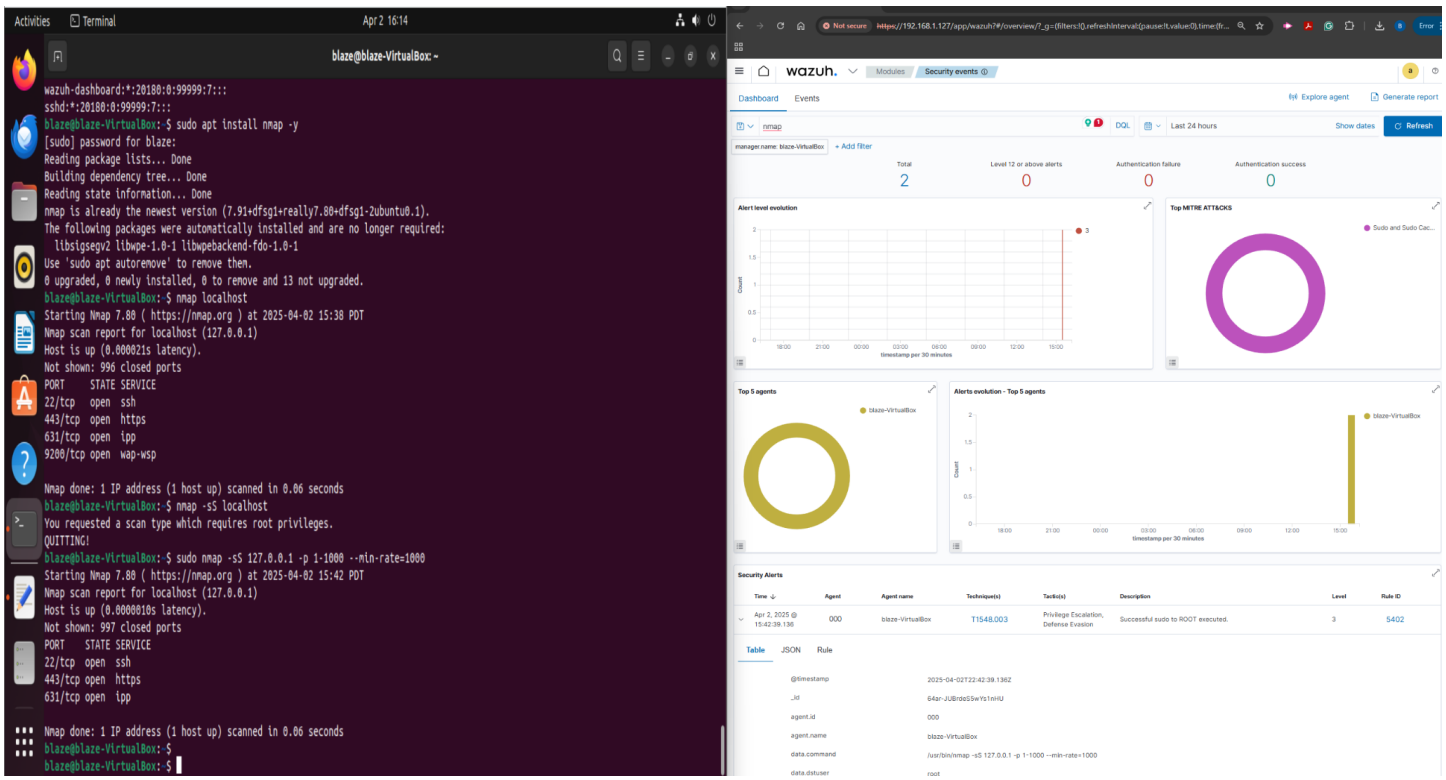
Wazuh SIEM Lab - Threat Detection Project



Screenshot 3 - SSH Brute-Force Attempt:

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).