Case Study: Detecting and Analysing SSH Authentication Failures Using Wazuh SIEM

---

1. Introduction

This case study documents the deployment and use of the Wazuh SIEM platform in an all-in-one lab environment to detect, analyse, and contextualize SSH authentication failures. The objective of this project was to understand how host-based logs are ingested, parsed, correlated, and visualized by a SIEM, and how such events are mapped to adversary behaviour using the MITRE ATT&CK framework.

---

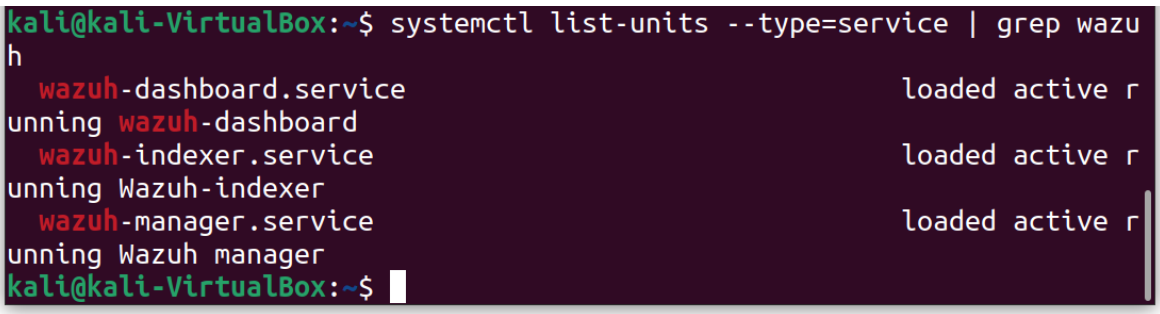
2. Lab Environment

The lab was set up using a single virtual machine running Ubuntu in an all-in-one Wazuh deployment.

Environment details:

- Operating System: Ubuntu (all-in-one deployment)
- Wazuh components: Manager, Indexer, Dashboard
- Log source: Local system logs (/var/log/auth.log)
- Access method: SSH

In an all-in-one deployment, the Wazuh manager monitors the local system directly, therefore no additional Wazuh agent was installed on the same machine.

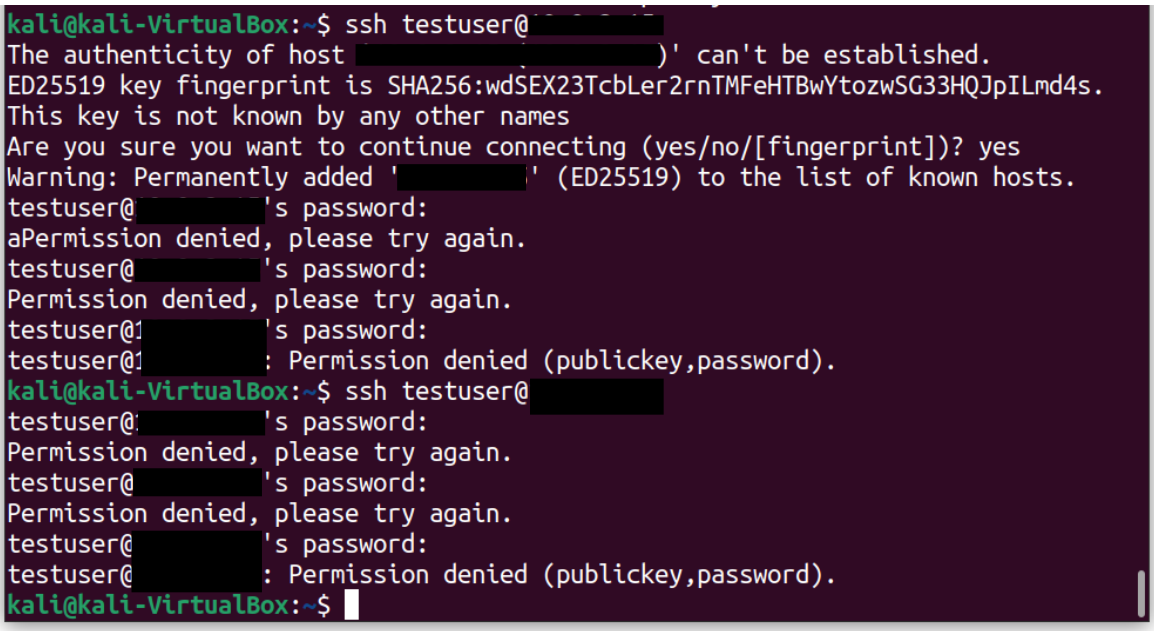


---

3. Attack Simulation: SSH Authentication Failures

To simulate a common attack scenario, repeated failed SSH login attempts were generated using a non-existent user account. This behaviour is representative of password guessing or brute-force attempts often observed in real-world environments.

Multiple SSH login attempts were intentionally made with incorrect credentials, causing authentication failures to be logged by the system.

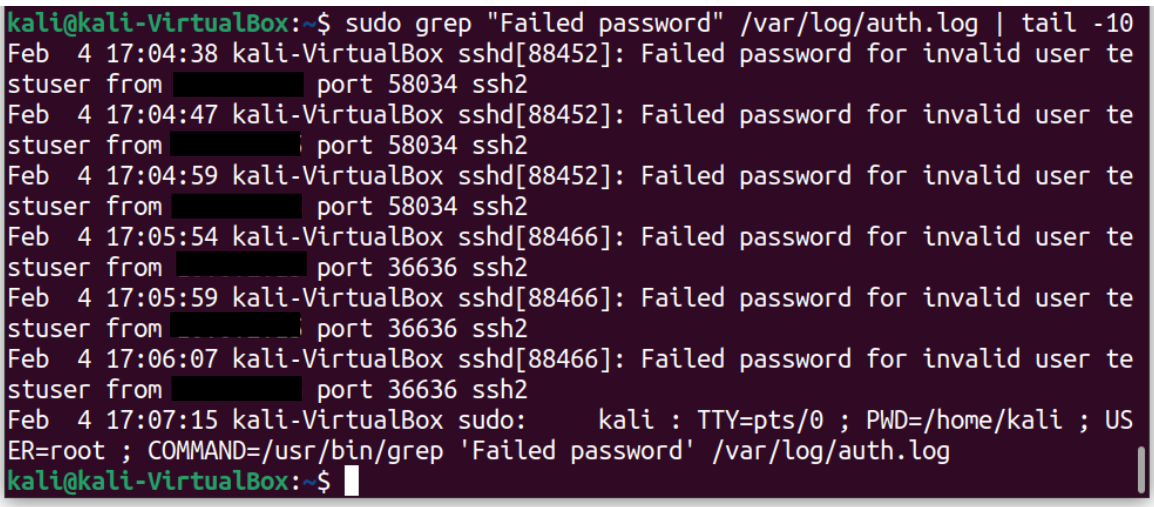


---

4. Log Verification at Host Level

Before analyzing alerts in Wazuh, the underlying system logs were verified to ensure that the failed authentication attempts were being recorded correctly. The SSH daemon logs clearly showed repeated “Failed password” entries, confirming that the activity was captured at the operating system level.

This step validated that any subsequent SIEM alerts were based on real log data rather than simulated events.



---

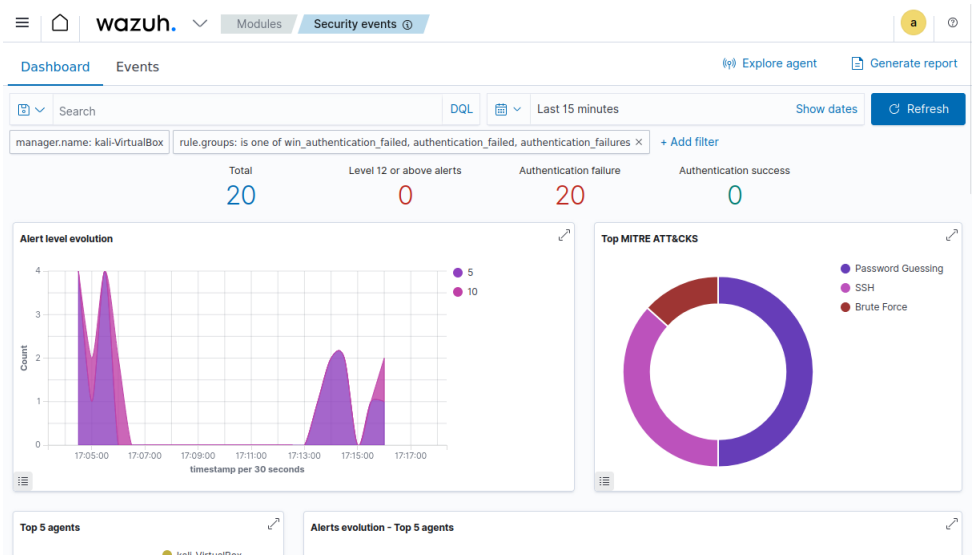
5. Detection in Wazuh SIEM

After generating the failed SSH attempts, the Wazuh Dashboard was refreshed to observe how the SIEM processed the new log entries. The Security Events view showed an increase in authentication failure alerts, confirming successful log ingestion and rule matching.

This confirmed that Wazuh rules correctly parsed SSH authentication logs and generated alerts without requiring custom rule modifications.

The dashboard displayed:

- An increase in authentication failure counts
- Time-correlated alert spikes
- Classification under SSH-related rule groups

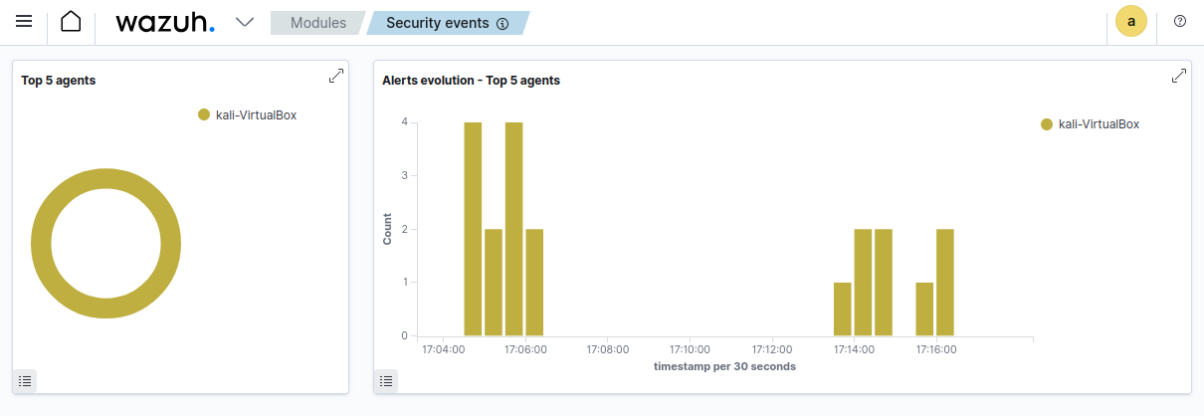


---

6. Timeline and Behavioural Analysis

The alert evolution graph showed distinct spikes corresponding to the times when repeated SSH login attempts were made. This temporal clustering is characteristic of brute-force or password-guessing behaviour, where multiple attempts occur within a short time window.

Analysing the timeline helped correlate attacker behaviour with detection output, an important skill in SOC investigations.



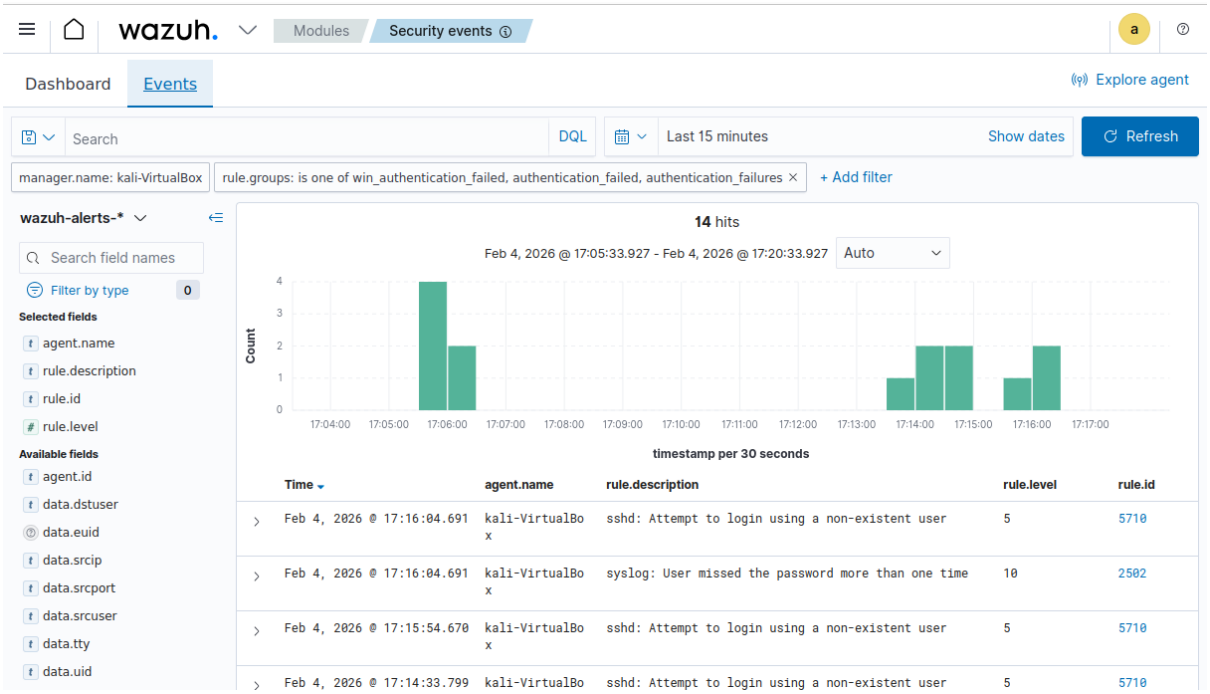
---

7. MITRE ATT&CK Mapping

Wazuh automatically mapped the detected events to relevant MITRE ATT&CK techniques. The failed SSH authentication attempts were associated with techniques such as:

- T1110: Brute Force
- T1110.001: Password Guessing

This mapping adds context to raw log data and helps analysts understand attacker intent rather than just individual events.



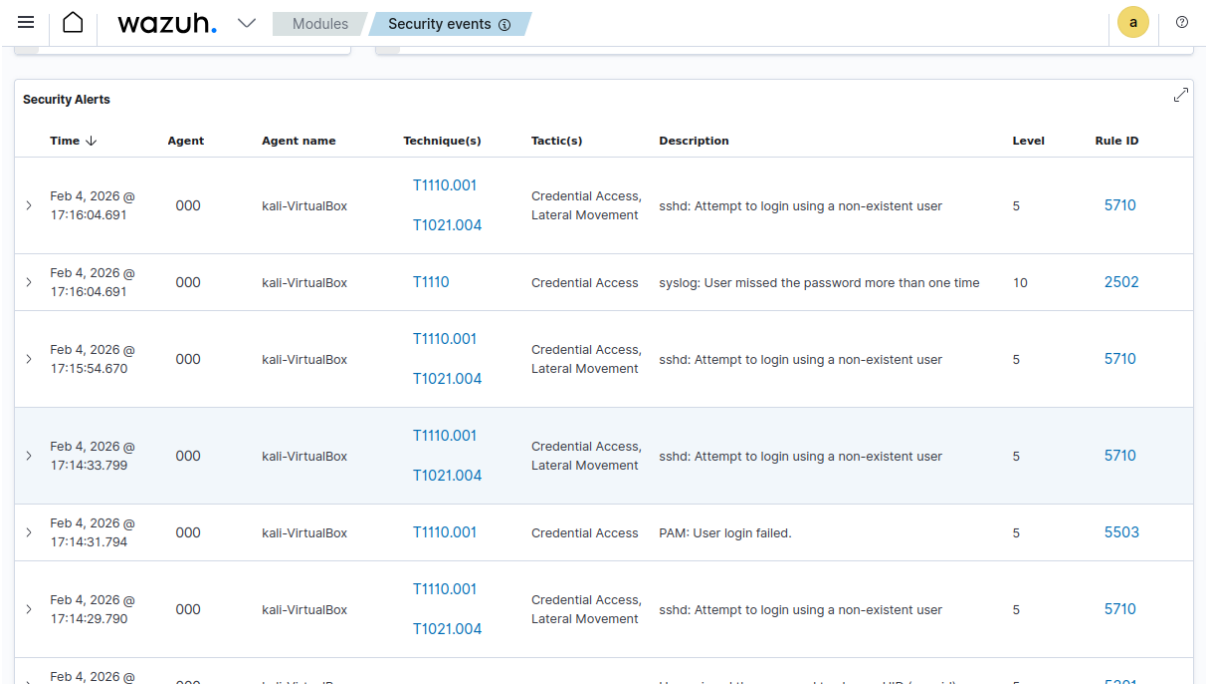
---

8. Rule-Level Analysis

To understand the detection logic in detail, one representative alert was analysed at the rule level. The expanded alert showed:

- Rule ID and description
- Severity level
- Associated MITRE techniques
- Original log message

Rather than reviewing every alert, analysing a single representative rule provided sufficient insight into how Wazuh detects and classifies SSH authentication failures.



---

9. Severity Interpretation

The detected alerts were classified as medium severity. This classification is appropriate because:

- Authentication failures were detected
- No successful login was observed
- No privilege escalation or lateral movement occurred

This demonstrates that Wazuh differentiates between suspicious activity and confirmed compromise, helping reduce alert fatigue.

---

10. Limitations

This lab intentionally focused on authentication failures only. The following limitations were identified:

- All activity originated from the same host
- No correlation rule for extended brute-force thresholds was tested
- No active response or blocking was configured

These limitations were accepted to keep the scope focused and the analysis clear.

---

11. Conclusion

This case study demonstrated how Wazuh SIEM can effectively detect and analyse SSH authentication failures using host-based logs. Through controlled attack simulation, log verification, alert analysis, and MITRE ATT&CK mapping, the project showcased a complete detection pipeline from raw logs to actionable security insights.

The exercise also reinforced the importance of understanding SIEM deployment models, alert severity interpretation, and honest documentation of limitations.

---

12. Key Learnings

- Practical understanding of Wazuh all-in-one deployment
- Detection of SSH brute-force style behaviour
- Log-to-alert correlation and timeline analysis
- MITRE ATT&CK contextualization of security events
- Importance of scoped and focused case studies