INCIDENT REPORT – USE CASE 5
Malicious Command Execution Detection (Ubuntu Agent)

Incident ID: SOC-CMD-005
Incident Title: Suspicious Command Execution Detected on Ubuntu System
Date & Time: Jan 19, 2026 @ 10:25:11.619
Detection Source: Wazuh SIEM – Audit Log Monitoring

Affected Asset

Host: Ubuntu Agent
Asset Type: Linux Server
Severity: Medium

Incident Summary

Wazuh SIEM detected the execution of suspicious system commands on an Ubuntu Linux host through audit log monitoring. Such activity may indicate post-access attacker behavior, including system enumeration, privilege misuse, or preparation for further malicious actions. The detection demonstrates the SOC's ability to identify potentially malicious command execution at the host level.

Detection Details

Detection Tool: Wazuh SIEM
Detection Type: Host-based Command Execution Monitoring
Log Source: auditd
Operating System: Ubuntu Linux
Alert Type: Suspicious Command Execution
User Context: Local User (Lab Simulation)

Investigation and Analysis

The SOC analyst reviewed the command execution alert in the Wazuh dashboard and analyzed the executed command, associated user account, and timestamp. The activity was correlated with recent authentication events to determine whether the execution followed a legitimate login. No additional indicators such as privilege escalation, unauthorized file modifications, or network anomalies were observed. The command execution was confirmed to be part of a controlled lab simulation.

Classification

True Positive – Authorized Activity (Test Case Validation)

Root Cause

Intentional execution of commands on the Ubuntu system to validate audit logging and malicious command execution detection capabilities.

Impact Assessment

No service disruption occurred.
No system compromise or unauthorized privilege escalation was identified.
The activity did not result in persistence or data exposure.

Response Actions

The alert was reviewed and validated by the SOC analyst.
Executed commands and user activity were documented.
No remediation actions were required due to the controlled test scenario.
Continued monitoring was maintained for related activity.

Lessons Learned

Command execution monitoring using audit logs is effective for identifying suspicious post-access activity. Correlating command execution events with authentication and file integrity alerts helps SOC analysts distinguish between legitimate administrative actions and malicious behavior.

MITRE ATT&CK Mapping
Tactic: TA0002 – Execution
Technique ID: T1059
Technique Name: Command and Scripting Interpreter

Incident Status
Closed – Informational (Test Case Validation)