SOC Incident Report and Executive Summary : Task 3

Web Reconnaissance Attempt (MITRE T1595.002)

Abishek V

August 7, 2025

Executive Summary

On August 7, 2025, a simulated web reconnaissance activity targeting a Linux web server was detected and analyzed using Wazuh SIEM. The reconnaissance was performed using the Nmap scripting engine against an Apache HTTP server running on the monitored host (‘soc‘). Wazuh generated multiple alerts due to a series of HTTP 404/405 error codes, indicating potential probing for hidden or vulnerable paths. The activity was mapped to the MITRE ATT&CK technique **T1595.002 - Vulnerability Scanning** under the Reconnaissance tactic.

This report summarizes the incident, detection methods, analysis, and suggested actions from a SOC Level 1 analyst perspective.

1 Incident Overview

- **Date/Time:** August 7, 2025 @ 01:08 UTC
- **Attacker IP:** 192.168.1.5
- **Target Host:** SOC Linux Server (Agent name: `soc`)
- **Tool Used:** Nmap Scripting Engine
- **Attack Method:** Multiple malformed or invalid HTTP requests
- **Detection:** Apache access log monitored by Wazuh agent, alerts triggered based on HTTP error codes (404, 405, 501)

2 Detection Details

The Wazuh agent on the ‘soc‘ machine monitored the Apache logs and reported multiple suspicious HTTP requests with the following characteristics:

- Paths like `/.git/HEAD`, `/HNAP1`, `/evox/about`, and `/sdk` were probed.
- User-Agent string identified as: `Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)`

- Multiple Wazuh rules triggered: 31101 (Web server 400 error), 31121 (501 errors), and 31151 (Recon activity)

Sample Alert (Wazuh)

```
Rule: 31151 (level 10) -> "Multiple web server 400 error codes from same source ip."
srcip: 192.168.1.5
url: /.git/HEAD
rule.groups: web, accesslog, web_scan, recon
mitre.id: T1595.002 (Vulnerability Scanning)
```

3 MITRE ATT&CK Mapping

- **Tactic:** Reconnaissance
- **Technique:** T1595.002 - Vulnerability Scanning
- **Description:** The adversary used a network scanning tool (Nmap NSE) to enumerate accessible directories and probe server responses.

4 Impact Assessment

- No known exploitation occurred during the recon phase.
- Repeated 404/405/501 errors confirm enumeration activity.
- Activity was limited to scanning and did not result in any privilege escalation or data access.

5 Recommended Actions

- **Alert Threshold Tuning:** Customize Wazuh rule thresholds to generate alerts when multiple 404s occur within a short timeframe.
- **GeoIP Filtering (Optional):** Enable GeoIP resolution to flag anomalous countries if relevant.
- **Web App Hardening:** Disable directory listing, remove unused endpoints, and audit exposed paths.
- **Threat Intelligence Integration:** Correlate scanning IP with threat feeds (e.g., AbuseIPDB, AlienVault OTX).

6 Conclusion

This simulation demonstrates how early detection of reconnaissance attempts using simple log-based alerts can empower SOC teams to proactively identify potential threats before exploitation. This report reflects how a SOC L1 analyst would document and escalate such an event for review.

Note: This incident is part of a simulated lab series for learning SIEM tools using open-source Wazuh. No real systems were harmed.