WorkFlow

1. Executive Summary

On December 19, 2025, a high-severity security incident was detected involving unauthorized remote access to a vulnerable Metasploitable2 system. The attacker exploited the Samba usermap script vulnerability using Metasploit, gaining root-level command execution. The activity was detected by Wazuh and mapped to MITRE ATT&CK technique T1210. Immediate containment actions were taken by isolating the affected virtual machine and blocking the attacker's IP address using CrowdSec. The incident was escalated to Tier 2 via TheHive for further investigation. No lateral movement, persistence, or data exfiltration was observed.

2. Attack Simulation (Metasploit)

Tool: Metasploit Framework
Exploit Module: exploit/multi/samba/usermap_script
Target System: 10.0.2.18
Attacker IP: 10.0.2.19
The attacker exploited the Samba usermap script vulnerability, allowing arbitrary command execution as root. A shell (/bin/sh) was spawned, confirming successful exploitation.
MITRE Mapping: T1210 – Exploitation of Remote Services

3. Alert Triage

Wazuh detected suspicious Samba activity using custom detection rules and raised a high-severity alert.

Triage Actions

- Verified alert source and log authenticity
- Confirmed remote command execution via Samba
- Checked for known false positives
- Classified alert as **True Positive**
- Assessed severity as **High**

4. Scope Assessment

The affected asset was identified as a single machine. Network and system logs were reviewed to determine the extent of compromise. No evidence of lateral movement, additional compromised hosts, or outbound connections beyond the initial attack source was observed. The incident impact was confirmed to be limited to one system at this stage.

5. Evidence Collection

Relevant evidence was preserved for investigation and escalation. This included Wazuh alert logs, Samba service logs, source IP information, and MITRE technique mapping. The attacker IP and exploitation method were documented as IOCs and attached to the case for further analysis by L2.

6. Containment and Isolation

VM Isolation

- Compromised Metasploitable2 VM was immediately isolated.
- Network interface disabled to prevent lateral movement.

CrowdSec IP Blocking

- Attacker IP 10.0.2.19 blocked using CrowdSec.
- Firewall enforcement applied automatically.

Verification

- Ping and connection attempts from attacker failed.
- No further malicious traffic observed.

7. Evidence Collection

Relevant evidence was preserved for investigation and escalation. This included Wazuh alert logs, Samba service logs, source IP information, and MITRE technique mapping. The attacker IP and exploitation method were documented as IOCs and attached to the case for further analysis by L2.

8. Escalation to SOC L2 (TheHive)

The incident was escalated to SOC L2 using TheHive for deeper investigation.

SOC L2 Case

A confirmed exploitation of a vulnerable Samba service resulted in root-level shell access on a Metasploitable2 system. The alert was detected by Wazuh and mapped to MITRE T1210. Containment was achieved through VM isolation and IP blocking via CrowdSec. No evidence of lateral movement or persistence was identified. The case is escalated for forensic validation and security hardening.

9. Incident Response Documentation

Prepare a report for the incident in SANS template.

10. Non-Technical Management Briefing

A simulated cyberattack exploited a known software weakness on a test system. Our security tools detected the activity quickly, isolated the affected system, and blocked the attacker. No data was compromised, and the issue was fully contained. This exercise confirmed that our security monitoring and response processes work effectively and are aligned with industry best practices.