CAPSTONE PROJECT

Notes

- **Task Title:** Samba Backdoor Detected
- **Case ID:** ~8294592
- **Assignee:** SOC Analyst
- **Severity:** Medium
- **TLP:** Amber
- **Status:** Completed
- **Observables:** MITRE T1210
- **Exploit:** Metasploit usermap_script
- **Source IP:** 192.168.1.39
- **Destination IP:** 192.168.1.36
- **Protocol:** SMB (port 139)
- **Zeek Notice:** Samba_Backdoor
- **Detection:** Zeek logs in /opt/zeek/logs/current/notice.log
- **Actions Taken:**
  - Verified Zeek detection of Samba usermap_script exploit.
  - Created a case in TheHive using an authorized admin user.
  - Added observables from the UI (source and destination IPs).
  - Initiated containment using CrowdSec:
  - Blocked the attacker IP (192.168.1.39) via firewall-bouncer.
  - Task marked as complete in TheHive.

- **Observations:**
  - Zeek successfully logged multiple Samba backdoor attempts.
  - TheHive case creation and observables management were functional after using an account with proper manageCase/create permissions.

- Containment via CrowdSec wa tested manually and confirmed active.
- Alerts from Zeek did not automatically populate in TheHive; only the case was visible.
- Attempted calculation of MTTD (Mean Time to Detect), MTTR (Mean Time to Respond), and dwell time in Elastic Security dashboards was unsuccessful due to:
- Inconsistent or missing timestamp fields for attack start and detection times (attack_start_time field absent).
- Runtime field scripts in Kibana returning errors (Cannot cast from [double] to [void]) despite multiple iterations.
- Dashboard lens could only display raw event timelines, not calculated metrics.

- **Root Cause Summary:**
  - The Samba exploit succeeded due to exposed legacy SMB services and incomplete system hardening.
  - Lack of automated detection and enforcement workflows initially allowed the attack attempt.
  - Recommendations / Follow-up:
  - Disable legacy SMB scripts and restrict SMB traffic to trusted hosts.
  - Ensure proper patch management and vulnerability scanning.
  - Integrate Zeek, TheHive, and CrowdSec for automated detection, alerting, and containment.
  - Investigate alternative ways to capture MTTD/MTTR metrics for reporting purposes.