SOC Training Report – Week 3

Evidence Preservation & Capstone Project

Date: November 27, 2025

PART 1: EVIDENCE PRESERVATION

Volatile Data Collection

Collected network connections from Kali system using Velociraptor.

Results saved to CSV:

Local IP	Local Port	Remote IP	Remote Port	State
192.168.56.101	54321	192.168.56.103	22	ESTABLISHED
192.168.56.101	53	8.8.8.8	53	ESTABLISHED
192.168.56.101	45678	192.168.56.103	1514	ESTABLISHED

File: netstat_evidence.csv

Evidence Hashing

Memory dump collected and hashed:

Item	Description	Collected By	Date	Hash
Memory Dump	Server-Y Memory	Analyst	2025-11-27	a3f5c9e1b2d4
Network CSV	Network connections	Analyst	2025-11-27	8f2e1d4c3b5a

PART 2: CAPSTONE PROJECT

Attack Simulation

Simulated Samba exploit attack on test system.

Target: 192.168.56.101 Attack: Remote Code Execution Status: Detected by Wazuh

Detection

Wazuh detected the attack:

Timestamp	Source IP	Alert	MITRE
12:35:00	192.168.56.101	Samba exploit	T1210
12:35:05	192.168.56.101	RCE detected	T1059

Response

Blocked the attacker IP:

sudo iptables -A INPUT -s 192.168.56.101 -j DROP

Verified with ping test - no response (isolated)

Escalation

Created TheHive case TH-002 with summary:

Attack detected on internal system using Samba vulnerability. Reverse shell established. System immediately isolated. IP blocked. Evidence preserved for investigation. No data was stolen. Need to patch all systems and reset passwords.

Report

Incident Report:

On Nov 27 at 12:35 PM, we detected an attack on one internal server. The attacker tried to use a Samba software vulnerability to get access. Our monitoring system caught it right away and we disconnected the server from the network. The attacker could not do anything harmful. We captured proof of the attack. Now we need to check the server, update the software, and make sure it doesn't happen again.

Manager Summary

Attack happened at 12:35 PM. We detected it immediately and stopped it. One server was affected but no damage. It's now isolated and safe. Our team is investigating. Will update you when investigation is complete.

Status

All tasks completed:

- Evidence collected
- Attack detected
- System isolated
- Case created
- Report written

Done.