Purple Team Field Report: AD Cyber Range Operations

Incident ID: PRPL-2026-001

Date: February 03, 2026

Analyst: Charles Beane **Security Clearance:** Lab Admin

Environment: Air-Gapped Host-Only Network (VirtualBox)

1. Executive Summary

This report documents a controlled "Purple Team" exercise conducted within a virtualized Active Directory environment. The objective was to validate the detection capabilities of a deployed **Splunk Enterprise** SIEM against two specific attack vectors: **Network-Based Credential Access** and **Post-Exploitation Data Destruction**.

The exercise confirmed that the implemented telemetry pipeline (Sysmon + Splunk Universal Forwarder) successfully captured high-fidelity Indicators of Compromise (IoCs) in real-time. All malicious activities were detected, logged, and analyzed, proving the efficacy of the current monitoring configuration.

2. Infrastructure & Scope

- **Target Endpoint:** Windows 11 Enterprise (192.168.56.104)
  - *Defensive Stack:* Sysmon (SwiftOnSecurity Config), Audit Policy (Logon Failures), Splunk Universal Forwarder.
- **Threat Actor Node:** Kali Linux 2025.4
  - *Offensive Stack:* Hydra, Nmap, PowerShell.
- **Analysis Node:** Splunk Enterprise 9.x (Ubuntu Server)

3. Incident 001: SMB Credential Brute Force

Severity: Critical **MITRE ATT&CK Tactic:** T1110.001 (Credential Access: Password Guessing)

3.1 Threat Actor Methodology (Red Team)

The attacker attempted to gain unauthorized access to the Victim user account by exploiting the SMB (Server Message Block) protocol. Due to Windows 11's default security posture disabling SMBv1, the attacker was forced to utilize specific protocol flags to execute the attack.

- **Attack Vector:** Network Service Scanning & Brute Force.

- **Tooling:** Hydra (v9.5).
- **Payload Execution:**
  hydra -l Victim -P /usr/share/wordlists/fasttrack.txt smb2://192.168.56.104

3.2 Detection & Forensic Analysis (Blue Team)

Detection Logic: High-frequency generation of Windows Security Event ID 4625 (An account failed to log on).

- **SIEM Query:** index=main EventCode=4625
- **Forensic Evidence:**
  - **Volume:** 262 authentication failures recorded in < 2 seconds.
  - **Log Analysis:**
    - **Subject User Name:** Victim
    - **Failure Reason:** %%2313 (Unknown user name or bad password)
    - **Workstation Name:** Kali-Linux (Attacker hostname leaked in logs)

Root Cause: The endpoint lacked an "Account Lockout Policy," allowing unlimited authentication attempts without triggering a temporary ban.

4. Incident 002: Ransomware Simulation (Data Encrypted for Impact)

Severity: High **MITRE ATT&CK Tactic:** T1486 (Impact: Data Encrypted for Impact)

4.1 Threat Actor Methodology (Red Team)

Simulating a post-compromise scenario, the attacker executed a custom PowerShell script designed to mimic ransomware behavior: bulk file modification and ransom note creation.

- **Delivery Method:** Local Execution (simulating a downloaded payload).
- **Payload:** malware.ps1
- **Defense Evasion:**
  The attacker encountered a default Restricted execution policy. To proceed, they manually lowered the local security posture:
  Set-ExecutionPolicy Unrestricted -Scope CurrentUser

4.2 Detection & Forensic Analysis (Blue Team)

Detection Logic: Sysmon Event ID 1 (Process Creation) and file system anomalies.

- **SIEM Query:** index=main "malware.ps1"
- **Forensic Evidence:**
  1. **Process Creation:** Splunk captured the explicit invocation of the malicious script:
     - ParentImage: explorer.exe

    - CommandLine: ...powershell.exe -file "C:\Users\Victim\Desktop\malware.ps1"
2. **File Artifacts:** Telemetry confirmed the creation of READ_ME_NOW.txt immediately following the script execution, confirming intent.

Root Cause: The user account possessed Local Administrative privileges, allowing the modification of the Execution Policy without triggering a User Account Control (UAC) denial.

5. Strategic Recommendations & Hardening

Based on the analysis of these incidents, the following remediation steps are recommended for the production environment:

1. **Identity Protection (Identity):** Implement a Group Policy Object (GPO) enforcing an **Account Lockout Threshold** of 5 failed attempts within 15 minutes to mitigate brute-force efficacy.
2. **Attack Surface Reduction (ASR):** Restrict PowerShell execution to **Signed Scripts Only** (Set-ExecutionPolicy AllSigned) to prevent the execution of untrusted, ad-hoc malware scripts.
3. **Automated Response (SOAR):** Configure a Splunk Alert to trigger when EventCode=4625 exceeds 20 events per minute, enabling rapid IP blocking at the firewall level.

6. Conclusion

This exercise demonstrated successful implementation of a "Defense-in-Depth" monitoring strategy. By correlating network-level logs (SMB traffic) with endpoint-level telemetry (Sysmon), the security posture provided full visibility into the attack lifecycle, from initial access attempts to final impact.