Active Directory & SIEM Cyber Range: Implementation Guide

Project Lead: Charles Beane **Date:** February 2026 **Platform:** Oracle VirtualBox 7.0+ **Environment:** Air-Gapped Host-Only Network

1. Executive Summary

This document outlines the technical specifications and provisioning steps for a "Purple Team" home lab environment. The architecture consists of three distinct nodes: an attacker (Kali Linux), a victim endpoint (Windows 11 Enterprise), and a centralized SIEM (Splunk on Ubuntu). The primary objective is to simulate realistic credential-based attacks (SMB Brute Force) and validate detection capabilities using Sysmon telemetry.

2. Infrastructure Prerequisites

Ensure the following ISO images and resources are available prior to deployment:

- **SIEM Host:** Ubuntu Server 24.04 LTS (ISO)
- **Endpoint:** Windows 11 Enterprise Evaluation (ISO)
- **Attack Platform:** Kali Linux 2025.4 (ISO)

2.1 Host Hardware Resource Strategy

The lab is hosted on a high-performance workstation designed to handle simultaneous multi-VM workloads without latency.

- **Processor: AMD Ryzen 7 7800X3D** (8 Cores / 16 Threads)
  - *Allocation Strategy:* 8 vCPUs assigned total (4 SIEM + 2 Victim + 2 Attacker), leaving 8 logical threads for the Host OS to prevent freezing.
- **Memory: 32GB DDR5 RAM (6000MT/s)**
  - *Allocation Strategy:* 16GB committed to the lab (8GB SIEM + 4GB Victim + 4GB Attacker), leaving 16GB buffer for Host operations.
- **Storage: 1TB NVMe M.2 SSD**
  - *Role:* High-speed NVMe I/O is critical for Splunk log ingestion to prevent "write-lock" delays during brute-force simulations.
- **Graphics: Gigabyte RTX 3080 Ti**
  - *Role:* Supports multi-monitor workflow for simultaneous visualization of the Attack Terminal (Kali), Victim Desktop (Windows), and Blue Team Dashboard (Splunk Web).

3. Node 1: Security Information & Event Management (SIEM)

Hostname: Blue-Splunk-Server **OS:** Ubuntu Server 24.04 LTS (Headless)

3.1 Hardware Allocation

- **vCPU:** 4 Cores (Required for high-volume log indexing)
- **RAM:** 8GB (Minimum requirement for Splunk Enterprise 9.x+)
- **Storage:** 50GB (Dynamic allocation)

3.2 Network Segmentation Strategy

The server utilizes a dual-adapter configuration to balance management access with network isolation.

- **Adapter 1 (NAT):** Dedicated management interface for package repository updates (apt update) and Splunk software downloads.
- **Adapter 2 (Host-Only):** A strictly internal, air-gapped interface (192.168.56.x). This interface listens for incoming log data from the victim machine.

3.3 Provisioning & Configuration

1. **Remote Access:** OpenSSH Server was selected during installation to facilitate remote administration via PowerShell on the host machine.
2. **Splunk Deployment:**
   - Package retrieval via wget.
   - Installation command: sudo dpkg -i splunk-installer.deb
   - Service initialization: sudo /opt/splunk/bin/splunk start --accept-license --answer-yes --run-as-root
3. **Ingestion Configuration:**
   - Configured a **Receiver** on TCP Port **9997** to accept incoming forwarder traffic.

4. Node 2: The Victim Endpoint

Hostname: Windows-11-Victim **OS:** Windows 11 Enterprise Evaluation

4.1 Hardware Allocation

- **vCPU:** 2 Cores
- **RAM:** 4GB
- **Security Modules:** TPM 2.0 and Secure Boot enabled (VirtualBox Passthrough).

4.2 Network Configuration

- **Adapter 1 (Host-Only):** Configured strictly on the internal network range to simulate an enterprise intranet endpoint. No direct internet access is permitted during attack simulations.

4.3 OS Provisioning & OOBE Bypass

To bypass the mandatory Microsoft Account requirement during the Out-of-Box Experience (OOBE):

1. **Network Disconnection:** The virtual network cable was disconnected during setup.
2. **Bypass Command:** Executed `OOBE\BYPASSNRO` via the Shift+F10 command prompt.
3. **Result:** Forced the creation of a local "Offline Account," simulating a domain-joined user environment.

4.4 Telemetry & Monitoring Implementation

To enable high-fidelity detection, the endpoint was hardened with the following agents:

A. Advanced System Monitor (Sysmon)

- **Configuration:** Deployed the SwiftOnSecurity configuration (`sysmonconfig-export.xml`) to filter noise and target critical events (Process Creation, Network Connections).
- **Deployment:** `sysmon64.exe -i sysmonconfig-export.xml -accepteula`

B. Splunk Universal Forwarder

- **Destination:** Configured to forward logs to the Ubuntu SIEM IP (`192.168.56.x`) on port 9997.
- **Service Principal Configuration:**
  - *Issue:* The default `NT SERVICE` account lacks permissions to read the `Microsoft-Windows-Sysmon/Operational` log channel.
  - *Resolution:* The **SplunkForwarder** service was reconfigured to run as **Local System**, granting full read access to all event channels.

C. Audit Policy Enforcement

- **Policy Path:** Local Security Policy > Audit Policy > Audit Logon Events
- **Setting:** Enabled logging for **Failure** events.
- **Objective:** To generate Event ID 4625 records during brute-force attempts.

5. Node 3: The Threat Actor

Hostname: `Kali-Linux` **OS:** Kali Linux 2025.4 (Rolling)

5.1 Hardware Allocation

- **vCPU:** 2 Cores
- **RAM:** 4GB

5.2 Network Configuration

- **Adapter 1 (Host-Only):** Placed on the same subnet as the Victim (`192.168.56.x`) to facilitate direct Layer 3 connectivity without routing through a firewall.

5.3 Attack Tool Configuration

Tool: Hydra (Network Logon Cracker)

- **Target Protocol:** SMB (Server Message Block)
- **Protocol Negotiation Issue:** Initial attacks failed due to Hydra defaulting to SMBv1, which is deprecated and blocked by default on Windows 11.
- **Remediation:** The attack syntax was modified to explicitly force **SMBv2**.
- **Final Payload:**
  `hydra -l Victim -P /usr/share/wordlists/fasttrack.txt smb2://[Target_IP]`

6. System Validation

The environment was validated via a full "Kill Chain" simulation:

1. **Attack:** Kali successfully executed 262 login attempts against the target using the `fasttrack.txt` wordlist.
2. **Detection:** Splunk successfully indexed 262 corresponding `Event Code 4625` logs in real-time.
3. **Latency:** Detection latency was measured at <1 second.