Manual de Implementación de Simulación de Adversarios en Máquinas Virtuales

Este manual describe el procedimiento paso a paso para implementar un laboratorio de simulación de adversarios (Adversary Simulation) utilizando únicamente software existente y seguro: MITRE CALDERA, SIEM (Wazuh/ELK) y agentes de telemetría. El objetivo es ejecutar simulaciones de ciberataques en entornos controlados sin necesidad de desarrollar código ofensivo.

1. Preparación del entorno de máquinas virtuales

- Instalar VirtualBox o VMware en la máquina host.
- Crear al menos 3–4 VMs: (1) Control con Linux (CALDERA), (2) Windows Target, (3) Linux Target, (4) SIEM.
- Configurar todas las VMs en una red interna aislada sin acceso a Internet.

2. Instalación de CALDERA (VM Control - Linux)

- Actualizar dependencias: sudo apt update && sudo apt install git python3-pip -y
- Clonar repositorio: git clone https://github.com/mitre/caldera.git --recursive
- Instalar requisitos: cd caldera && pip3 install -r requirements.txt
- Ejecutar: python3 server.py --insecure
- Acceder desde navegador: http://:8888 (admin/admin).

3. Instalación de agentes en máquinas objetivo

- Windows Target: instalar Sysmon, Winlogbeat y el agente Sandcat desde CALDERA.
- Linux Target: instalar auditd, osquery, Filebeat y el agente Sandcat desde CALDERA.

4. Configuración del SIEM (VM SIEM)

- Instalar Wazuh (recomendado) o ELK Stack.
- Wazuh: curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh && sudo bash wazuh-install.sh -a
- Configurar agentes para enviar logs al SIEM.
- Acceder a la consola de Wazuh: https://:5601

5. Ejecución de simulaciones con CALDERA

- Acceder a CALDERA → Campaigns → Create New.
- Seleccionar agentes conectados (Windows/Linux).
- Elegir un perfil de adversario (ej. Discovery, Credential Access).
- Ejecutar campaña y observar ejecución de TTPs benignos.
- Validar en SIEM (Wazuh/ELK) que se recibieron los eventos.

6. Validación y documentación

- En CALDERA: revisar técnicas ejecutadas y mapeo ATT&CK.;
- En SIEM: verificar eventos recibidos y reglas de correlación.

- Documentar evidencias: técnicas probadas, eventos generados, tiempos de detección.
- Generar un reporte en HTML/CSV o manual con métricas y hallazgos.

Este laboratorio académico permite realizar simulaciones de adversarios en un entorno seguro. La combinación de CALDERA, agentes de telemetría y un SIEM (Wazuh/ELK) facilita la evaluación continua de seguridad, sin necesidad de desarrollar código ofensivo, cumpliendo con el enfoque de 'Pruebas Continuas de Seguridad'.