MANUAL DE USUARIO

Proyecto: Simulación de Ataques Persistentes Avanzados (APTs) para Pruebas de Seguridad Continuas

Autores: Salamar Barre Antonio Jeremías; Freddy Antonio Torres Benítez
Fecha: Octubre 2025
Versión: 1.0

INDICE

Introducción

Este manual de usuario describe los pasos necesarios para utilizar el laboratorio de simulación APT. Está orientado a operadores y evaluadores que ejecutarán campañas controladas usando MITRE CALDERA y monitorearán telemetría con Wazuh/ELK.

Requisitos del Sistema

Requisitos	Detalle
Host físico (mínimo)	Windows/Linux con 16 GB RAM, 4 vCPU, 250 GB disco
Virtualización	Oracle VirtualBox 7.x o VMware Workstation
Red	Host-only 192.168.56.0/24 configurada en VirtualBox
SO VMs	Ubuntu 22.04 (CALDERA, Wazuh), Windows 10/11 (Cliente)
Software	CALDERA 5.3.0, Wazuh 4.7.x, Elasticsearch/Kibana compatibles

Información de Acceso

A continuación un ejemplo de credenciales y puertos. Modifique por valores seguros en producción.

Sistema	Dirección IP	Usuario	Contraseña	Puerto
CALDERA (Web)	192.168.56.50	admin	CalderaAdmin2025!	8888
Wazuh / Kibana	192.168.56.51	admin	WazuhAdmin2025!	5601 / 443
Windows Client (Agente)	192.168.56.100	UsuarioLocal	Passw0rd!	RDP 3389
HTTP Receiver (Flask)	192.168.56.51	n/a	n/a	8080

Inicio del Laboratorio

Pasos para arrancar el laboratorio en el orden recomendado:

1. Iniciar WAZUH-ELK (192.168.56.51).

2. Iniciar CALDERA (192.168.56.50).

3. Iniciar WINDOWS-CLIENT (192.168.56.100).

Verificar conectividad con ping entre las IPs. Asegurarse de que los agentes estén activos en Wazuh antes de ejecutar campañas en CALDERA.

Acceso a Interfaces Web

1. Acceder a las consolas desde el host (o navegador con acceso a la red host-only):
2. CALDERA: http://192.168.56.50:8888
3. Wazuh/Kibana: https://192.168.56.51:5601 (o 443 según configuración)
4. HTTP Receiver (validación): http://192.168.56.51:8080/ping

Ejecución de Simulaciones

1. En CALDERA, ir a Campaigns -> Create New.
2. Seleccionar los agentes disponibles y un adversary profile.
3. Configurar parámetros (timeout, output, etc.) y presionar 'Start Operation'.
4. Supervisar steps y logs en la interfaz de CALDERA.

Monitoreo de Eventos

1. En Wazuh Dashboard -> Agents: verificar agente activo.
2. En Kibana, abrir índices 'wazuh-alerts-*' y filtrar por host o técnica ATT&CK.
3. Consultar dashboards preconfigurados para procesos, conexiones de red y exfiltración.

Generación de Reportes

Exportar hallazgos y métricas:

1. En CALDERA: exportar operation logs (JSON/CSV).
2. En Wazuh/Kibana: exportar dashboards como CSV o PDF.
3. Consolidar reporte con: técnicas ejecutadas, eventos detectados, MTTD y recomendaciones.

Detención del Laboratorio

1. Detener operaciones en CALDERA.
2. Apagar Windows Client.
3. Apagar CALDERA.
4. Por último, apagar Wazuh-ELK.
5. Crear snapshots después de obtener evidencia si se requiere recuperación.

Solución de Problemas

Problema: Agente no aparece en CALDERA

Solución: Verificar que sandcat esté ejecutándose en el cliente y que éste tenga conectividad con 192.168.56.50:8888.

Problema: Agente no se registra en Wazuh

Solución: Revisar clave de autenticación generada por /var/ossec/bin/manage_agents y que la IP del manager sea 192.168.56.51.

Problema: No llegan eventos a Kibana

Solución: Verificar Logstash y Elasticsearch; revisar índices y espacio en disco.

Referencias Rápidas

1. Comprobar conectividad: ping 192.168.56.50
2. Reiniciar Wazuh Manager: sudo systemctl restart wazuh-manager
3. Reiniciar CALDERA: detener server.py y ejecutar python3 server.py –insecure