# MANUAL TÉCNICO

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

Autor: Salamar Barre Antonio Jeremías; Fredy Antonio Torres Benítez
Fecha: Octubre 2025
Versión: 1.1

**INDICE**

## Introducción

Este manual técnico detalla la instalación, configuración, topología y especificaciones técnicas de cada componente del laboratorio APT. Está dirigido a administradores e ingenieros que desplegarán y mantendrán el entorno.

## Requisitos del Sistema

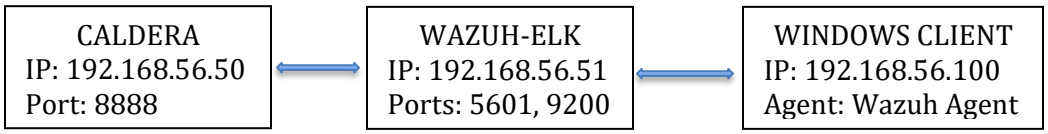
| ELEMENTO | ESPECIFICACIÓN |
|---|---|
| Host físico | 16 GB RAM mínimo, 4vCPU, 250GB disco |
| Red | Host-Only 192.168.56.0/24 + NAT para actualizaciones |
| VMs mínimas | CALDERA, WAZUH-ELK, WINDOWS-CLIENT, OPTIONAL: LINUX-CLIENT |
| Sistemas operativos | Ubuntu Server 22.04 LTS, Windows 10/11 |

## Topología de Red

Topología propuesta (host-only):

CALDERA (192.168.56.50) -- WAZUH-ELK (192.168.56.51) -- WINDOWS-CLIENT (192.168.56.100)

**Diagrama de arquitectura**




## Flujo de datos:

1. CALDERA ejecuta abilities -> envía órdenes al agente sandcat en Windows.
2. Windows genera eventos (Sysmon) -> Wazuh Agent los envía al Wazuh Manager.
3. Wazuh Manager procesa y envía a Logstash/Elasticsearch -> Kibana visualiza.
4. Si hay exfil, Windows realiza POST a Flask receiver alojado en 192.168.56.51:8080 (aislado).

## Especificaciones Técnicas de VMs

| VM | vCPU | RAM | Disco (GB) |
|---|---|---|---|
| CALDERA1 (Ubuntu 22.04) | 2 | 4 GB | 50 |
| WAZUH-ELK1 (Ubuntu 22.04) | 4 | 8 GB | 100 |
| WINDOWS-CLIENT1 (Win10/11) | 2 | 4 GB | 50 |
| HTTP-RECEIVER (Flask) | 1 | 1 GB | 10 |

## Configuración de Red (Ejemplo)

| Adaptador | Modo | Dirección IPv4 / Máscara |
|---|---|---|
| Adapter 1 (CALDERA) | Host-Only | 192.168.56.50 / 255.255.255.0 |
| Adapter 1 (WAZUH-ELK) | Host-Only | 192.168.56.51 / 255.255.255.0 |
| Adapter 1 (WINDOWS-CLIENT) | Host-Only | 192.168.56.100 / 255.255.255.0 |

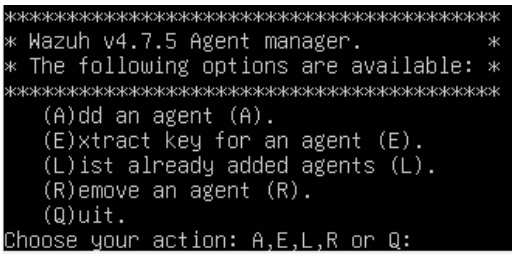
## Instalación y Configuración (paso a paso)

**CALDERA:**

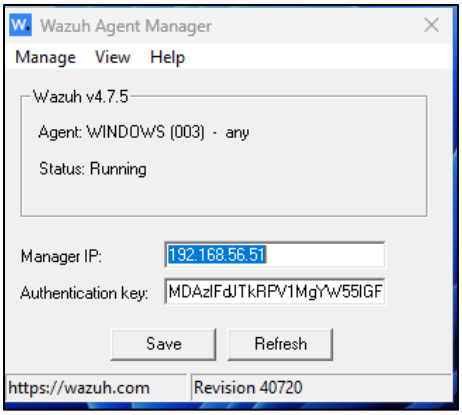
1) Actualizar sistema: sudo apt update && sudo apt upgrade -y
2) Instalar dependencias: sudo apt install git python3-pip -y
3) Clonar repo y ejecutar: *git clone https://github.com/mitre/caldera.git && pip3 install -r requirements.txt && python3 server.py --insecure*

**WAZUH (resumen):**

1) Instalar Wazuh manager y Elastic Stack (usar instalador oficial o docker-compose)
2) Configurar agente registración: /var/ossec/bin/manage_agents
   *Seleccionar (A) ad dan agent*
   *Seleccionar (E) Extract key for an agent*



3) En cliente Windows, pegar auth key y registrar agente




## Flujo de Datos

Detalle técnico del flujo de datos entre componentes:

1. **CALDERA** ejecuta abilities (ordenes) -> agente sandcat en Windows recibe la orden.
2. **Windows** ejecuta comandos benignos; Sysmon genera eventos -> Wazuh Agent los envía al manager en 192.168.56.51.
3. **Wazuh** aplica reglas y genera alertas -> Filebeat/Logstash indexan en Elasticsearch -> Kibana muestra dashboards.
4. **Logs y evidencias** se almacenan en /var/ossec/archives o en índices Elasticsearch (wazuh-alerts-*).

## Pautas de Seguridad y Hardening

- Mantener red host-only aislada y no conectar VMs a Internet durante pruebas.
- Aplicar contraseñas seguras y rotarlas tras cada sesión.
- Restringir acceso a puertos de administración desde la red física.
- Hacer snapshots antes y después de pruebas.

## Solución de Problemas Avanzada

Logs críticos y comandos de diagnóstico:

- Ver logs Wazuh: /var/ossec/logs/ossec.log
- Ver estado services: sudo systemctl status wazuh-manager
- Ver índices Elastic: GET _cat/indices?v
- Revisar conectividad: tcpdump -i any host 192.168.56.100 and port 8888

## Referencias Rápidas

1. CALDERA UI: http://192.168.56.50:8888
2. Wazuh/Kibana: https://192.168.56.51:5601
3. Comandos: /var/ossec/bin/manage_agents, sudo systemctl restart wazuh-manager