Guía de Ejecución y Diagnóstico

OpenSorry Toolkit - Guía de Ejecución

Este paquete contiene scripts de autodiagnóstico para auditorías de ciberseguridad (CIS v8.1).
Todos los scripts están escritos en Python estándar para Windows y no requieren instalación de librerías extra (usamos módulos nativos como json, subprocess, socket).

Instrucciones de Uso

1. **Descomprimir** este archivo en la máquina objetivo.
2. Ejecutar cada script haciendo doble clic o desde terminal (`python nombre_script.py`).

Lista de Herramientas

1. **inventario_activos.py**
- **Qué hace:** Lista información del sistema hardware y todo el software instalado.
- **Salida:** `inventario_[hostname].json`
- **CIS Control:** 1 (Inventario de Activos) y 2 (Inventario de Software).

2. **auditoria_politicas.py** (Reemplaza chequeo_mfa.py)
- **Qué hace:** Extrae la política de contraseñas local (longitud mínima, bloqueo) y crea placeholder para MFA.
- **Salida:** `auditoria_identidad_local.json`
- **CIS Control:** 5 (Gestión de Cuentas) y 6 (Gestión de Control de Acceso).

3. **auditoria_red.py** (Reemplaza vulnerabilidades_pcap_mock.py)
- **Qué hace:** Escanea los puertos locales (TCP) más comunes para detectar servicios expuestos.
- **Salida:** `auditoria_red_puertos.json`
- **CIS Control:** 4 (Gestión Segura de Configuración).

4. **auditoria_av.py** [NUEVO]
- **Qué hace:** Verifica que exista un producto Antivirus registrado en el Centro de Seguridad de Windows (ej. Defender).
- **Salida:** `auditoria_antivirus.json`
- **CIS Control:** 10 (Defensas contra Malware).

Subida de Evidencias

Una vez generados los archivos JSON:
1. Revíselos para asegurar que no contienen datos PII no deseados.
2. Súbalos a la carpeta compartida de OneDrive indicada en el portal web de OpenSorry.
3. Para capturas de pantalla o logs adicionales, use las carpetas "Visuales" y "Logs_Sensibles".