OpenLock Security Suite

Guia Tecnica de Ejecucion y Diagnostico CIS v8.1

Introduccion

Este documento detalla el procedimiento tecnico para la recoleccion de evidencia de ciberseguridad. Las herramientas suministradas (OpenLock Toolkit) son scripts de auditoria de solo lectura disenados para evaluar la postura de seguridad frente a los Controles CIS v8.1 sin impactar la disponibilidad del servicio.

1. Analisis de Inventario (CIS 1 & 2)

El primer paso para la defensa es conocer que se esta defendiendo. El script 'inventario_activos.py' realiza un levantamiento detallado del hardware y software.

Detalle Tecnico

- Software: Lista todas las aplicaciones instaladas via WMI/Registry.
- Objetivo: Detectar software no autorizado, versiones obsoletas o 'Shadow IT'.
- Archivo generado: inventario_[hostname].json

2. Auditoria de Identidad (CIS 5 & 6)

Los ataques de identidad son el vector mas comun actual. 'auditoria_politicas.py' examina la configuracion local de seguridad de Windows.

Detalle Tecnico

- Politicas Password: Verifica longitud minima, complejidad y bloqueo de cuentas.
- Interpretacion: Si la longitud es < 14 caracteres o no hay bloqueo, el riesgo de fuerza bruta es Alto.
- Archivo generado: auditoria_identidad_local.json

3. Superficie de Ataque de Red (CIS 4)

Es critico minimizar los servicios expuestos. 'auditoria_red.py' realiza un escaneo de puertos TCP en la interfaz local (loopback) para identificar servicios escuchando.

Detalle Tecnico

- Escaneo: Top 1000 puertos + puertos criticos (RDP 3389, SQL 1433, SMB 445).
- Riesgo: Puertos como 3389 (RDP) abiertos innecesariamente aumentan el riesgo de Ransomware.
- Archivo generado: auditoria_red_puertos.json

4. Estado de Proteccion Malware (CIS 10)

Verificacion de la eficacia de las herramientas EDR/Antivirus instaladas mediante 'auditoria_av.py'.

Detalle Tecnico

- Consulta WMI root\SecurityCenter2.
- Verifica: Que el AV este registrado, habilitado y con firmas actualizadas.
- Archivo generado: auditoria_antivirus.json

Instrucciones de Entrega

Una vez ejecutados los 4 scripts, siga estos pasos para asegurar la cadena de custodia de la evidencia:

```
1. Verifique que se hayan generado los 4 archivos .json en la carpeta del toolkit.
2. Comprima los archivos JSON en un unico archivo ZIP llamado
'Evidencia_[NombreCliente].zip'.
3. Acceda al portal OpenLock y navegue a la Mision 4.
4. Use el enlace seguro de OneDrive para cargar el archivo ZIP.
5. Haga clic en 'Notificar Finalizacion' para alertar a nuestro SOC.
```

Si encuentra errores durante la ejecucion (ej. 'Access Denied'), asegurese de estar ejecutando los scripts con privilegios de Administrador (Clic derecho -> Ejecutar como Administrador).