

## **Guía Completa de Uso de Screen Crab por Hak5**

### **Parte I: Fundamentos y Mecanismo de Funcionamiento**

#### **1. Screen Crab Basics (Conceptos Básicos)**

- **Propósito:** Capturar imágenes (instantáneas) de la pantalla de un ordenador sin depender del software del sistema operativo, su CPU o sus drivers.
- **Mecanismo:** El Screen Crab actúa como un **interceptor de video**. Se conecta en línea entre la tarjeta gráfica del ordenador (salida HDMI, DisplayPort, DVI, etc.) y el monitor.
- **Modo de Operación:** Una vez conectado y encendido, el dispositivo escucha pasivamente la señal de video digital. Cuando se activa, toma la señal de video que está pasando en ese momento, la procesa y la guarda internamente en su memoria como una imagen (generalmente JPEG o PNG).
- **Ventaja Forense:** Dado que solo interactúa con el flujo de video, es completamente **indetectable** por *firewalls*, software antivirus o sistemas de detección de intrusiones a nivel de software.

#### **2. Specifications (Especificaciones) y Advertencias**

- **Especificaciones:** El dispositivo incluye una pequeña placa de procesamiento capaz de manejar resoluciones de video modernas, una memoria interna para almacenar las capturas y, a menudo, una batería para operar de forma autónoma.
- **Importante Safety Information And Warnings (Advertencias):** El uso del Screen Crab está restringido a **pruebas de penetración autorizadas** y operaciones forenses o de auditoría en equipos propios o con permiso explícito. El uso no autorizado constituye espionaje.

### **Parte II: Configuración y Control**

#### **3. Configuring The Screen Crab (Configuración del Screen Crab)**

La configuración se realiza generalmente conectando el dispositivo a un ordenador a través de un puerto de control USB (o MicroSD) y editando un archivo de configuración o accediendo a un shell básico.

- **Parámetros Clave:**

- **Frecuencia de Captura:** Establecer cada cuánto tiempo debe tomar una captura (ej: cada 30 segundos, cada 5 minutos, o solo bajo demanda).
- **Formato de Imagen:** Definir el formato de la captura (JPEG para ahorrar espacio, PNG para mejor calidad).
- **Resolución:** Asegurarse de que el dispositivo está configurado para manejar la resolución nativa de la pantalla de destino.

#### 4. Led Status Indications (Indicadores de Estado LED)

El Screen Crab utiliza un sistema de LEDs para indicar su estado de operación al auditor:

- **LED de Encendido:** Indica que el dispositivo está recibiendo energía (de la batería o de la conexión USB/video).
- **LED de Grabación/Captura:** Parpadea brevemente cuando se realiza una captura de pantalla exitosa.
- **LED de Error:** Puede indicar un fallo en el almacenamiento o que la señal de video no es compatible.

#### 5. Configuring Cloud C2 (Configuración de Cloud C2)

- **Propósito:** Permite la gestión y exfiltración de las capturas de pantalla de forma remota.
- **Mecanismo:** El Screen Crab, si tiene conectividad de red, puede configurarse para conectarse a la plataforma **Cloud C2** de Hak5. Esto permite al auditor ver las capturas en tiempo real o descargar los archivos almacenados sin tener que recuperar el dispositivo físicamente.

### Parte III: Mantenimiento y Solución de Problemas

#### 6. 2024 SSL Update (Actualización SSL 2024)

- **Propósito:** Esta es una actualización específica para asegurar las comunicaciones del dispositivo.
- **Necesidad:** Garantiza que la comunicación con el servidor **Cloud C2** o con el panel de administración web se realice de forma segura mediante protocolos SSL/TLS actualizados,

evitando que las credenciales de administración sean interceptadas.

## 7. Troubleshooting (Solución de Problemas)

Los problemas comunes con un interceptor de video se centran en:

- **Incompatibilidad de Resolución o Señal:** Si la pantalla de destino utiliza un modo de video inusual o una resolución no compatible, el Screen Crab puede fallar al capturar o pasar la señal. La solución es actualizar el *firmware* o ajustar la configuración.
- **Fallo en la Energía:** Si la batería se agota o el puerto HDMI no suministra suficiente energía (si está diseñado para ser alimentado por el puerto), el dispositivo dejará de grabar.
- **Memoria Llena:** El dispositivo podría detener la captura si su almacenamiento interno se llena de imágenes. La solución es descargar los archivos y limpiar la memoria.

En resumen, el **Screen Crab** es una herramienta de nicho de auditoría visual que ofrece un método silencioso para documentar la actividad de un sistema al interceptar el flujo de video a nivel de *hardware*.