Guía Completa de Uso del Shark Jack por Hak5

Parte I: Fundamentos y Configuración Inicial

1. Specifications, Safety and Warnings (Especificaciones y Seguridad)

- **Especificaciones:** Es un dispositivo pequeño con una batería recargable incorporada, lo que le permite operar de forma autónoma durante un tiempo limitado (generalmente para completar un *payload* de reconocimiento rápido).
- **Seguridad:** El uso del Shark Jack debe ser estrictamente para **pruebas de penetración autorizadas** o auditorías en entornos controlados, debido a su capacidad para ejecutar código automáticamente al conectarse a una red.

2. Shark Jack Basics y Default Settings (Conceptos Básicos y Configuración por Defecto)

- El Shark Jack funciona como un pequeño ordenador Linux.
- **Configuración por Defecto:** Al igual que otras herramientas de Hak5, el Shark Jack se conecta inicialmente a través de una dirección IP estática (como **172.16.84.1** o similar) y utiliza **SSH** para la configuración y el acceso remoto.
- **Modo de Operación:** El dispositivo está diseñado para ser conectado a un puerto Ethernet de la red de destino. Su batería le permite ejecutar un *payload* incluso si el puerto no suministra alimentación PoE (Power over Ethernet).

3. Unboxing And Setup (Desembalaje y Configuración)

1. **Carga Inicial:** El primer paso es cargar completamente la batería.
2. **Conexión SSH:** Conecte el Shark Jack a su PC vía USB y acceda a la interfaz de administración mediante un cliente SSH (ej: ssh root@172.16.84.1).
3. **Cambio de Contraseña:** Es crucial cambiar la contraseña predeterminada por motivos de seguridad.
4. **Actualización:** Ejecute la actualización inicial del *firmware* si es necesario.

Parte II: Operación, Comandos Clave y Payloads

El Shark Jack utiliza una lógica basada en *scripts* de *payload* (archivos de *script* que se ejecutan automáticamente).

4. Two Key Commands (Dos Comandos Clave)

El Shark Jack opera en dos modos clave que se cambian mediante el interruptor físico del dispositivo (SWITCH).

- **1. Carga (Armar):** El dispositivo está en modo de escucha y espera a ser conectado. El *payload* no se ejecuta.
- **2. Ataque (Ejecutar):** Cuando se conecta a la red de destino, el *payload* se activa inmediatamente.

5. Using Sharkjack.sh (Uso del Script de Ayuda)

- sharkjack.sh es una utilidad de línea de comandos en la computadora del atacante que facilita la interacción con el Shark Jack, como montarlo como un dispositivo USB o transferir archivos.

6. Writing A Simple Payload (Escribir un Payload Simple)

Los *payloads* son *scripts* de Bash que se ejecutan secuencialmente cuando el Shark Jack detecta una conexión de red.

Un *payload* simple se enfoca en la acción principal:

Bash

```
# Ejemplo de Payload Simple (Reconocimiento Rápido)

LED RÁPIDO # Muestra que el payload se está ejecutando

NETMODE DHCP # Obtiene una IP de la red

nmap -sn 192.168.1.0/24 > /root/loot/network_scan.txt # Escanea la red

LED LENTO # Indica que ha finalizado
```

Parte III: Comandos de Desarrollo y NETMODE

Estos comandos se utilizan dentro del *script* de *payload* para controlar el hardware y la red.

Comando	Descripción	Uso en Payload
The NETMODE Command	Controla cómo el Shark Jack interactúa con la red, definiendo su rol (DHCP, Estático, MiTM).	NETMODE DHCP (obtener IP de la red para escanear).
The LED Command	Controla el LED de estado para dar *feedback* visual sobre el progreso del *payload*.	LED RÁPIDO (ejecutando), LED LENTO (finalizado), LED ROJO (error).
The SWITCH Command	Lee el estado del interruptor físico para ejecutar diferentes lógicas de *payload* (aunque la función principal es armar/ejecutar).	Se usa para ramificar el *script* si se desea añadir lógica compleja.
The BATTERY Command	Permite verificar el estado de carga de la batería antes de comenzar una tarea.	Útil para garantizar que hay suficiente energía para completar un escaneo largo.
The SERIAL_WRITE Command	Envía datos a través del puerto USB en modo serie.	Se utiliza para el *debugging* o para comunicarse con otro *hardware* conectado (ej: un teléfono, si está configurado).
The Cloud C2 Commands	Habilita la comunicación remota con la plataforma **Cloud C2** de Hak5.	Permite al Shark Jack conectarse a un servidor en Internet para descargar *payloads* actualizados o exfiltrar datos de forma remota.
Included Tools	La lista de herramientas preinstaladas en la pequeña distribución	Se utilizan directamente en los *payloads* para realizar el trabajo real

Comando	Descripción	Uso en Payload
	Linux (ej: **Nmap**, **tcpdump**, **netcat**).	(escaneo, *sniffing*, etc.).

Parte IV: Gestión de Payloads y Mantenimiento

7. Payload Management (Gestión de Payloads)

Comando	Descripción
The UPDATE_PAYLOADS Command	Descarga la última colección de *payloads* de la comunidad o del repositorio oficial de Hak5.
The LIST Command	Muestra una lista de todos los *payloads* instalados actualmente en la memoria del Shark Jack.
The ACTIVATE Command	Permite al analista seleccionar y establecer cuál de los *payloads* listados se ejecutará la próxima vez que el dispositivo pase al modo "Ataque".

8. Firmware Update and Recovery (Actualización y Recuperación)

- **Over The Air Upgrade (Actualización OTA):** El método preferido. Se conecta el Shark Jack a Internet y se ejecuta el comando de actualización desde la consola SSH.
- **Manual Upgrade:** Si la OTA falla, el *firmware* se descarga manualmente y se carga a través de SSH o la conexión USB.
- **Firmware Recovery:** Es el último recurso. Permite restablecer el dispositivo si el *firmware* se ha dañado, generalmente a través de un proceso de *bootloader* o puenteo de pines.

Parte V: Casos de Uso Avanzados

9. Advanced Usage (Uso Avanzado)

- **Charge The Shark Jack From Your Phone (Carga desde el Teléfono):** Es una característica de portabilidad que permite usar un teléfono Android con capacidad OTG (On-

The-Go) para suministrar energía de carga al Shark Jack cuando no hay un puerto USB disponible.

- **Using The Shark Jack With The Plunder Bug As A Simple Switch:** El Plunder Bug es otro dispositivo Hak5. Al usarlo junto con el Shark Jack, el Plunder Bug puede actuar como un simple *switch* (*hub* de red pasivo), permitiendo que el Shark Jack intercepte el tráfico sin ser el único intermediario.
- **Android Serial Setup:** Permite una conexión de consola directa entre el Shark Jack y un dispositivo Android para *debugging* y control, lo que elimina la necesidad de una laptop.

En resumen, el Shark Jack es la herramienta de bolsillo ideal para el auditor que necesita **automatizar el reconocimiento** y la recolección de datos en un entorno físico de forma rápida y discreta.