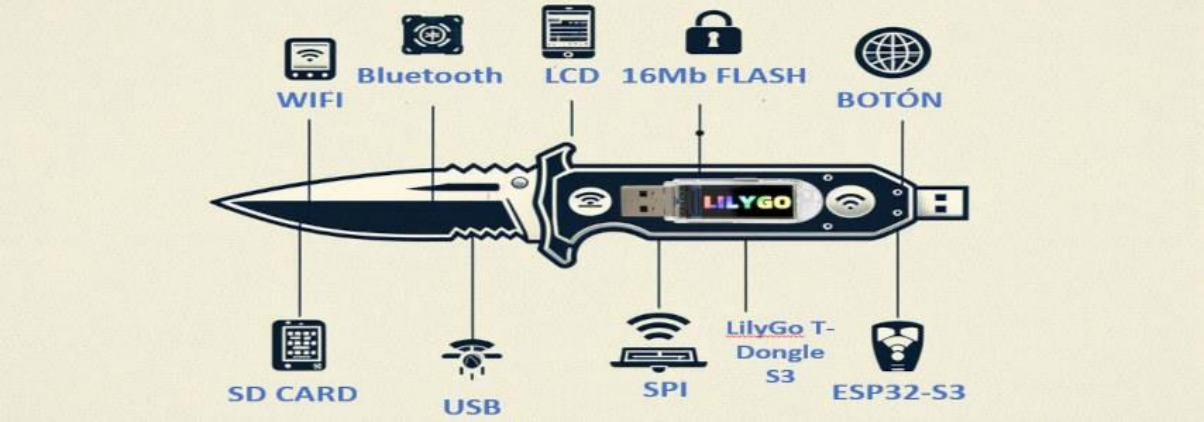


USBArmyKnife

Herramienta Definitiva para Pruebas de Penetración

Los ataques de acceso físico/USB actuales presentan limitaciones. Cada ataque individualmente no ofrece una solución completa para alcanzar la mayoría de los objetivos.

Los ataques de teclado USB (como los de Ducky) requieren que la máquina esté desbloqueada, y ni siquiera las mejores herramientas resuelven este problema. Los ataques de red pueden obtener hashes de contraseñas, pero a menudo requieren dispositivos voluminosos conectados a puertos Ethernet para la extracción de datos y el posterior descifrado offline.

Cuando se obtiene acceso a un sistema, las opciones para la exfiltración de datos se ven limitadas si cualquier conexión de socket es detectada.

Lo que se necesitaba era una plataforma de acceso físico que permitiera combinar las mejores características de cada tipo de ataque, superando sus limitaciones mediante la sinergia entre ellos. Idealmente, esta plataforma sería económica y discreta, de modo que la pérdida de un dispositivo no representara un problema significativo.

Esta es la razón de ser del *USBArmyKnife*.

¿Necesitas un adaptador Ethernet USB para capturar tráfico (PCAP) y extraerlo a través de WiFi? *USBArmyKnife*.

¿Quieres personalizar la interfaz de tus ataques o mostrar una interfaz espectacular cuando tu ataque tenga éxito? *USBArmyKnife*.

¿Necesitas un dispositivo de almacenamiento encubierto? *USBArmyKnife*.

Podéis encontrar el repositorio original de **i-am-shodam** aquí:

https://github.com/i-am-shodan/USBArmyKnife

USBArmyKnife: La navaja suiza para pruebas de seguridad USB

En el mundo de la ciberseguridad, las pruebas de penetración son esenciales para identificar y mitigar vulnerabilidades. USBArmyKnife se presenta como una herramienta versátil y poderosa para evaluar la seguridad de dispositivos USB y sistemas que interactúan con ellos.

¿Qué es USBArmyKnife?

USBArmyKnife es un conjunto de scripts y herramientas diseñadas para realizar una amplia gama de pruebas de seguridad relacionadas con USB. Su objetivo principal es ayudar a los profesionales de la seguridad a identificar posibles puntos débiles en la implementación de USB, tanto en hardware como en software.

Características principales:

- **Diversidad de ataques:** USBArmyKnife incluye scripts para realizar diversos tipos de ataques, como ataques de inyección de pulsaciones de teclado, ataques de almacenamiento masivo y ataques de dispositivos HID (Human Interface Device).
- **Flexibilidad:** La herramienta está diseñada para ser flexible y adaptable a diferentes escenarios de prueba. Los usuarios pueden personalizar los scripts y configuraciones para satisfacer sus necesidades específicas.
- **Facilidad de uso:** A pesar de su potencia, USBArmyKnife se ha creado con la facilidad de uso en mente. Los scripts están bien documentados y la herramienta cuenta con una interfaz de línea de comandos intuitiva.
- **Plataforma cruzada:** USBArmyKnife es compatible con múltiples sistemas operativos, lo que permite a los usuarios realizar pruebas en diferentes entornos.
- **Orientado a T-Dongle-S3:** La herramienta esta diseñada para usarse en conjunto con el hardware T-Dongle-S3, un dispositivo que expande las capacidades de la herramienta.

Casos de uso:

- **Pruebas de penetración:** USBArmyKnife se puede utilizar para simular ataques reales y evaluar la resistencia de los sistemas a las amenazas USB.
- **Análisis de vulnerabilidades:** La herramienta puede ayudar a identificar vulnerabilidades en la implementación de USB de dispositivos y sistemas.
- **Auditorías de seguridad:** USBArmyKnife se puede utilizar para realizar auditorías de seguridad exhaustivas y garantizar el cumplimiento de las normas de seguridad.

- **Investigación y desarrollo:** La herramienta es una valiosa herramienta para investigadores y desarrolladores que trabajan en el campo de la seguridad USB.

Hardware soportado

LilyGo T-Dongle S3 (Recomendado)

El LilyGo T-Dongle S3 es un tablero de desarrollo ESP32-S3 con forma de pen drive USB. Cuenta con una pantalla LCD en color, botón físico, adaptador de tarjeta SD micro oculto/tapado (dentro del conector USB-A) así como un adaptador SPI. Tiene 16MB de flash. Se basa en el chipset ESP32-S3, que le permite albergar una estación WiFi, así como soportar una gama de ataques con WiFi y Bluetooth. Es increíblemente barato. Hay dos versiones de este dispositivo con y sin la pantalla. Sólo la versión con la pantalla ha sido probada.

Waveshare ESP32-S3 1.47inch

Este dispositivo es similar en diseño, tamaño y características del LilyGo T-Dongle S3 y utiliza el mismo chipset. Es claramente un tablero de dev, ya que no viene con carcasa y lleva expuesto circuitos en la parte inferior. Donde este dispositivo mejora el T-Dongle S3 es que tiene una pantalla de alta calidad muy grande y 8MB de RAM adicional.

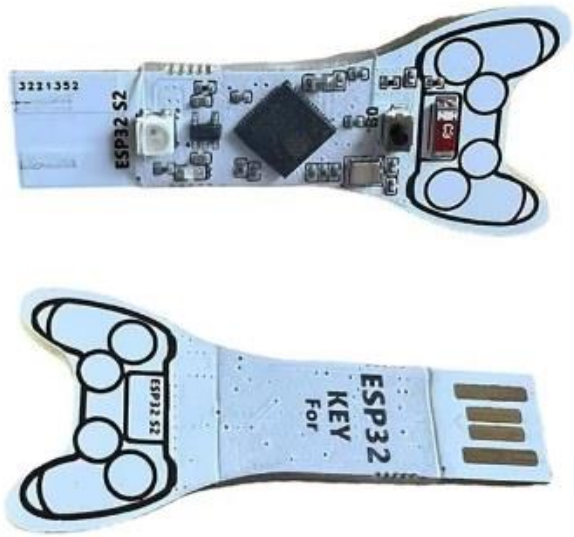
M5Stack AtomS3U

Este es un tablero de desarrollo ESP32-S3 con dos interfaz externa en la parte trasera. No cuenta con una pantalla o una tarjeta SD, pero sí tiene un LED y un botón. En lugar de una tarjeta SD, la memoria flash se utiliza para almacenar archivos. Inusualmente también contiene un micrófono digital y un LED IR que actualmente no son compatibles. Para poner el dispositivo en modo de arranque mantenga pulsar RESET (el botón en el lado del dispositivo) hasta que se encienda un LED verde.

ESP32 Udisk

El dispositivo más básico que puede ejecutar el código USB Army Knife es un chip ESP32-S2 conectado a un puerto USB. A menudo puedes encontrar estos vendidos en un sitios similares al T-Dongle S3 y tiende a anunciarse en sitios como AliExpress como Playstation 4 jailbreaks bajo el nombre de 'USB Dongle Udisk para P4'. Estos dispositivos carecen de memoria RAM, una pantalla, tarjeta SD, Bluetooth, LEDs y un buen botón de hardware. En lugar de una tarjeta SD, la memoria flash se utiliza para almacenar archivos diminutos. Estos dispositivos son increíblemente baratos y a menudo son buenos en la ejecución de cargas útiles HID-WiFi (como el rick roll).

Advertencia: Son demasiado concurridos para dirigir el servidor web. Al comprar estos, cuidado de que a menudo se pueden confundir con un dispositivo de aspecto muy similar que incluye un chipset CH343P y no hay botón de reinicio. Asegúrese de que el dispositivo que compra tiene un botón que se puede pulsar. Asegúrese de flashear este dispositivo con la configuración Generic-ESP32-S2.



ESP32 Key

Muy similar al ESP32 UDisk este es un ESP32-S2 en una placa de circuito. Es probablemente el dispositivo más barato que puede casi ejecutar USBArmyKnife y tiene un de precio igual. Tendrás que mantener pulsado el botón cuando lo enchufe para poner el dispositivo en modo flash. Asegúrese de flash de este dispositivo con la configuración Generic-ESP32-S2.

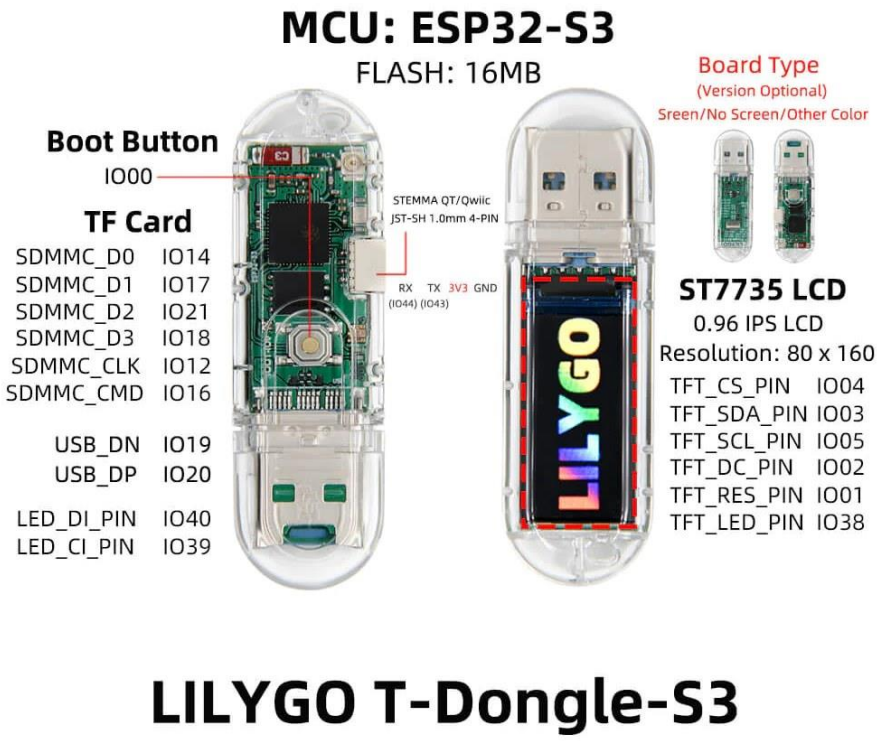
Waveshare-RP2040-GEEK

RP2040-GEEK es una tabla de desarrollo diseñada por Waveshare. Tiene pantalla LCD USB-A, 1.14-inch , una tarjeta SD y cuenta con puertos externos (SWD, UART e I2C). Este tablero no ejecuta el chipset ESP32. El modo USB ethernet (NCM) está actualmente sin soporte. ESP32 Maurader no puede trabajar en este dispositivo. En Windows también puede necesitar configurar este dispositivo para usar un controlador WinUSB usando Zadig. Mantenga el botón cuando lo conecte para poner el dispositivo en modo parpadeo.

LilyGo T-Dongle S3

De entre los dispositivos compatibles, los ejemplos de configuración, uso y capturas siguientes están probados en una LilyGo T-Dongle S3.

Este modelo muestra gran versatilidad por un precio inferior a los 20€



Instalación

Hay dos opciones para cargar el firmware de USBArmyKnife en su dispositivo:

- Flasheando con el firmware preconstruido usando su navegador web (ruta más fácil)
- Construyendo y flasheando el código usando VisualStudio.

Preparación de su tarjeta SD

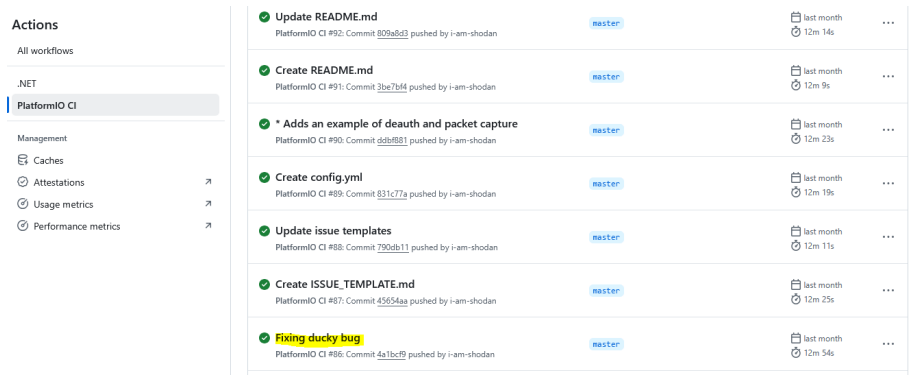
USBArmyKnife puede no funcionar correctamente con grandes tarjetas SD o aquellas con sistemas de archivos más nuevos. Recomendamos usar una con una partición FAT32 de 32 GB para la máxima compatibilidad. También se pueden utilizar capacidades más pequeñas.

Si una tarjeta SD no se puede encontrar con un sistema de archivos soportado, el dispositivo le ofrecerá opción para formatearlo. Si utiliza esta opción, el sistema de archivos creado en la tarjeta SD puede no funcionar bajo Windows. Como tal, se aconseja crear una tarjeta SD adecuada desactivada.

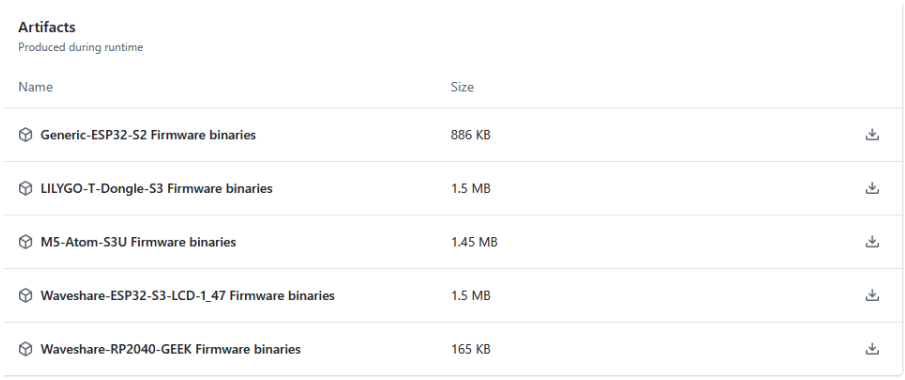
Archivos necesarios

En primer lugar vamos a preparar los archivos necesarios.

Tienes que descargar la última versión para tu dispositivo, para ello tienes que ir a esta **página**, y haces clic en la primera opción que aparezca como **Fixing ducky bug**

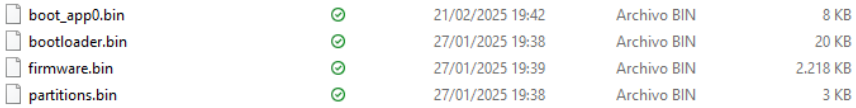


- En la sección Artifacts haz clic en descargar junto al modelo de dispositivo que tienes (sólo los dispositivos basados en ESP32 son compatibles actualmente)
- Extraer los archivos descargados



El siguiente archivo que vamos a descargar es boot.app0.bin. Asegúrate de pulsar el botón 'Descargar archivo raw'.

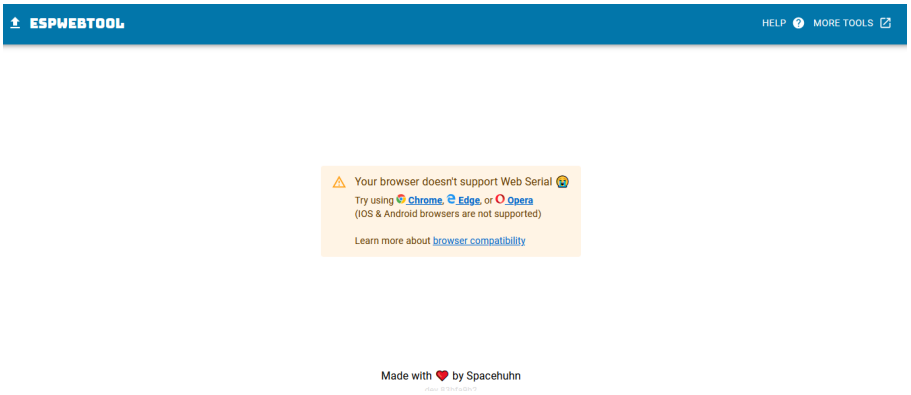
Ya tenemos los archivos que necesitamos:



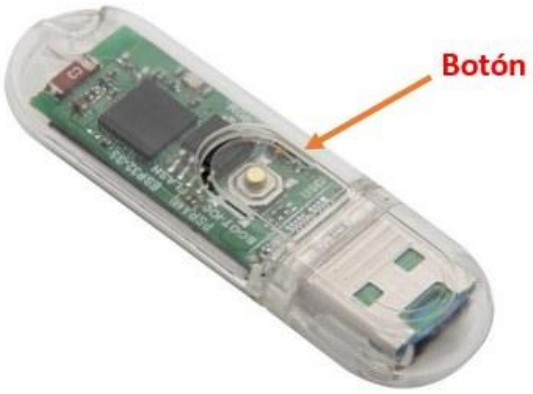
Flasheando con el navegador web

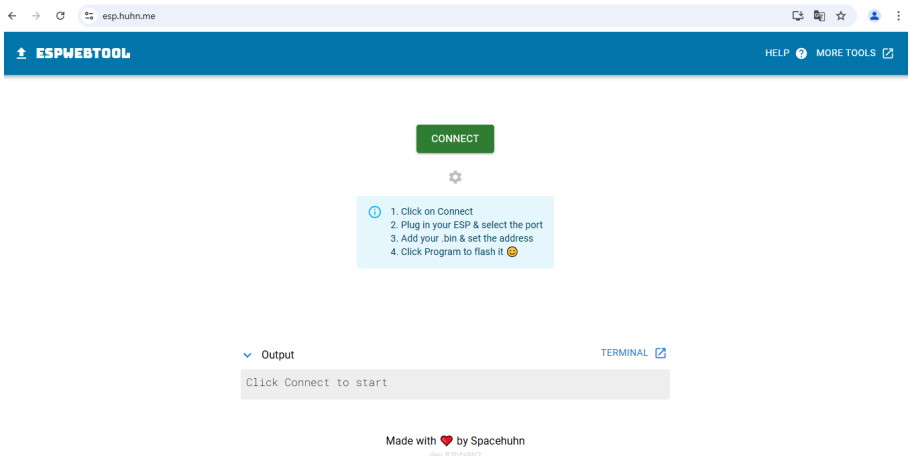
Ahora vamos a visitar esta página: https://esp.huhn.me/

Algunos navegadores como Firefox no están soportados, puedes utilizar Chrome



Conecta tu dispositivo, manteniendo pulsado el botón de arranque para que inicie en modo bootloader.

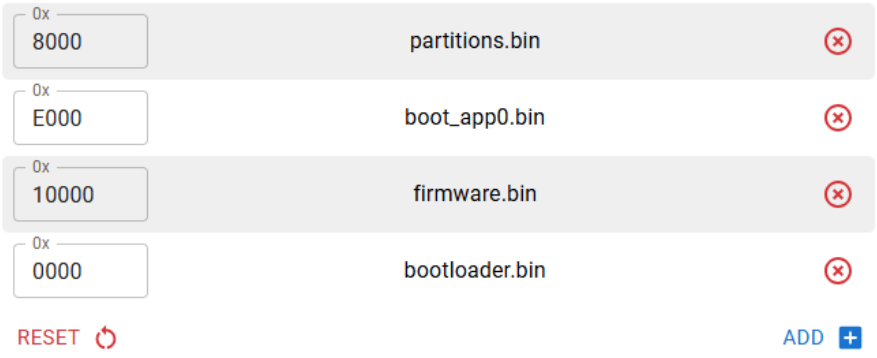




Haz clic en **Conecta**, selecciona tu dispositivo ESP32 y selecciona **Conecta** de nuevo.

Una vez que estamos conectados vamos a cargar y configurar los archivos que tenemos preparados.

Lo dejaremos todo tal cual se aprecia en la siguiente imagen:



Hacemos clic en **CONNECT** y en la venta de abajo veremos como empieza a flashear el dispositivo.

Si todo ha ido bien veremos que nos indica que para ejecutar el nuevo firmware, el dispositivo debe ser reseteado:

Desconectamos y volvemos a insertar el dispositivo pero esta vez sin pulsar el botón.

Ya tenemos nuestro dispositivo listo.

Si no puedes flashear tu dispositivo de esta manera, vas a necesitar usar el método **VSCode**

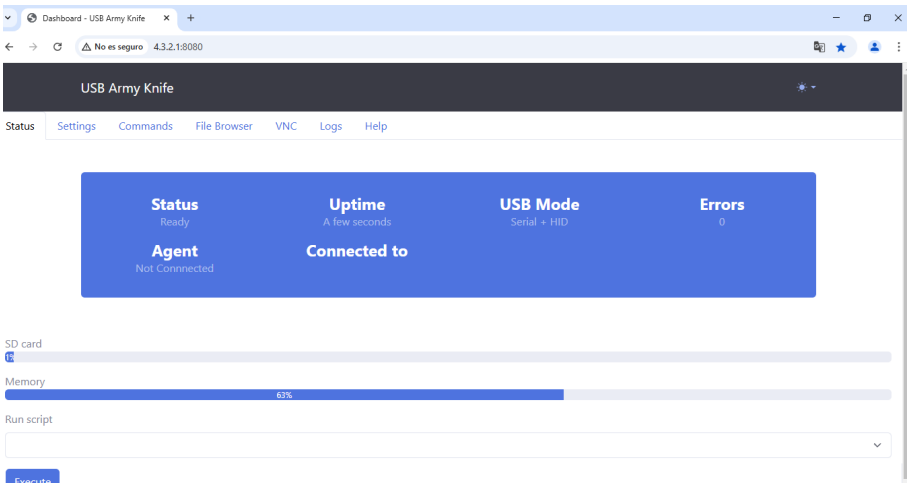
Probando el dispositivo

Conecta el dongle USB a tu equipo. Conéctate al punto de acceso WiFi (**iPhone14**) que se ha creado al conectar el **USBArmyKnife**, con la contraseña de '**password**'

Acceda a la interfaz web (http://4.3.2.1:8080) navegando a la URL con tu navegador.

Asegúrate de que la interfaz web se haya cargado correctamente. Deberías ver el estado actual y el tiempo de actividad. Si no es así refresca la página.

Utiliza la interfaz web para crear y administrar tus ataques usando DuckyScript.



Los dispositivos basados en ESP-S2 tienen soporte WiFi, pero no tienen una interfaz web. Los ataques se gestionan a través de archivos DuckyScript. Los dispositivos RP2040 no tienen capacidad ESP32 Maurader

Ejecución de comandos y scripting

El USB Army Knife ofrece una robusta función de ejecución de comandos, permitiendo a los usuarios ejecutar una variedad de comandos en la máquina de destino sobre HID o en sí mismo como los Rubber Ducky scripts, Marauder y controlar la pantalla y la luz led.

La lista completa de comandos está disponible en el GitHub.

Para poder empezar tienes unos cuantos ejemplos en el repositorio de **GitHub,** algunos realmente interesantes.

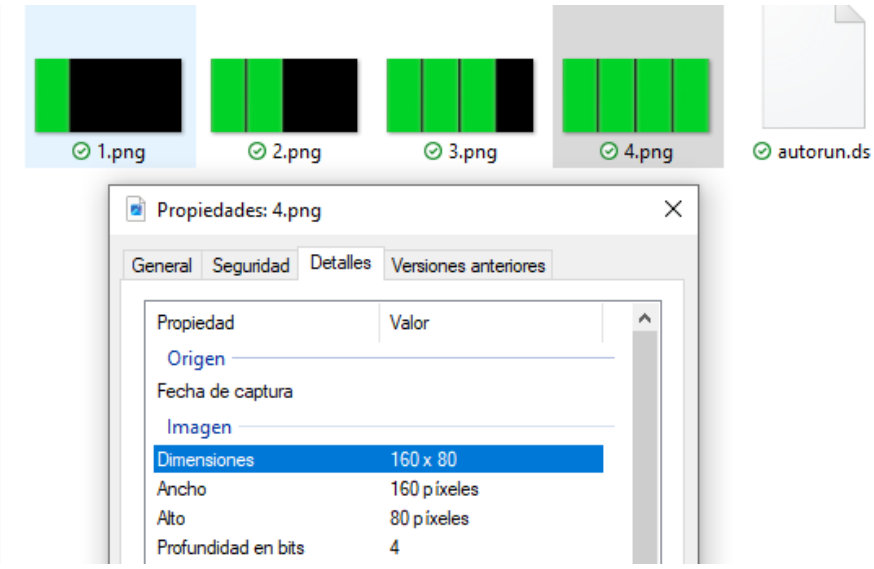
.

Personalización

Ejemplo de cómo mostrar una sencilla barra de progreso al estilo de Hollywood, útil para ataques multietapa.

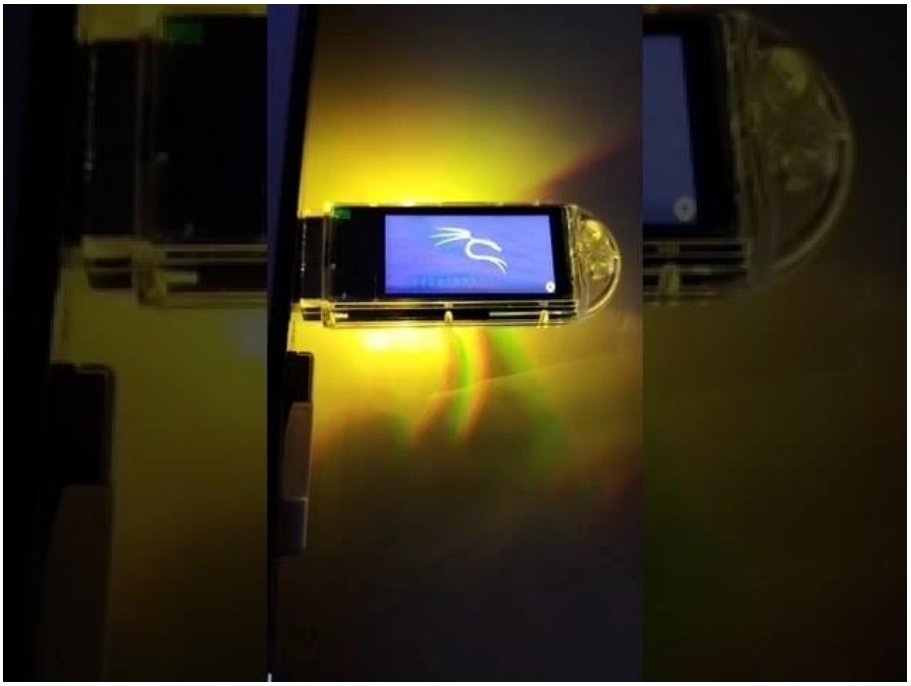
Las imágenes a mostrar se han desarrollado para la pantalla más pequeña soportada (160x80 píxeles). Si estás usando un dispositivo con una pantalla más grande encontrarás áreas sin llenar de la pantalla; tendrás que re-dimensionar las imágenes al tamaño de tu pantalla.

- Descarga el ejemplo
- Copia autorun.ds en la tarjeta SD
- Copia todos los archivos de PNG en la tarjeta SD
- Enchufa el dispositivo




1.png
2.png
3.png
4.png
autorun.ds


1.png
2.png
3.png
4.png
autorun.ds



Rickroll

Rickroll o Rickrolling es un meme de Internet que hace referencia al cantante Rick Astley. Consiste en un enlace trampa disfrazado como algo de interés para que el usuario haga clic sobre él, pero lo redirige hacia el vídeo musical de Rick Astley “Never Gonna Give You Up” (1987).

Esta carga útil de DuckyScript está diseñada para ofrecer la mejor experiencia de Rick Roll. Abre un navegador web, navega al clásico video de Rick Roll, utiliza un ESP32 Marauder para transmitir las letras a través de WiFi, y muestra la imagen icónica de Rick Astley en una pantalla LCD.

Las imágenes a mostrar se han desarrollado para la pantalla más pequeña soportada. Si estás usando un dispositivo con una pantalla más grande encontrarás áreas sin llenar de la pantalla.

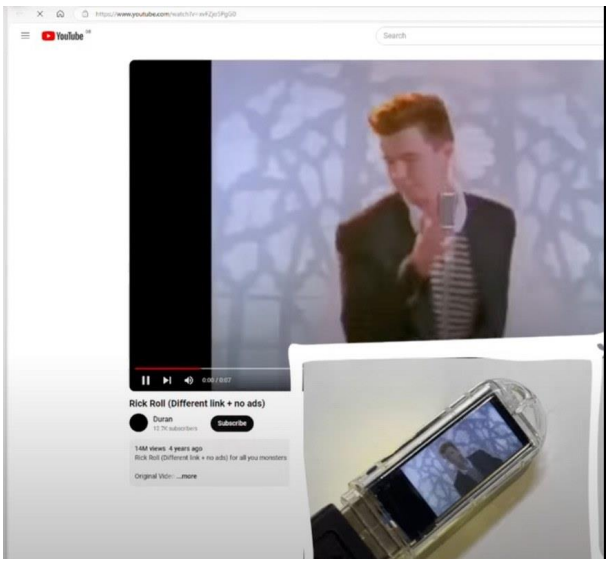
Lo único que necesitas es descargar los archivos desde **aquí** y copiarlos a la tarjeta SD:

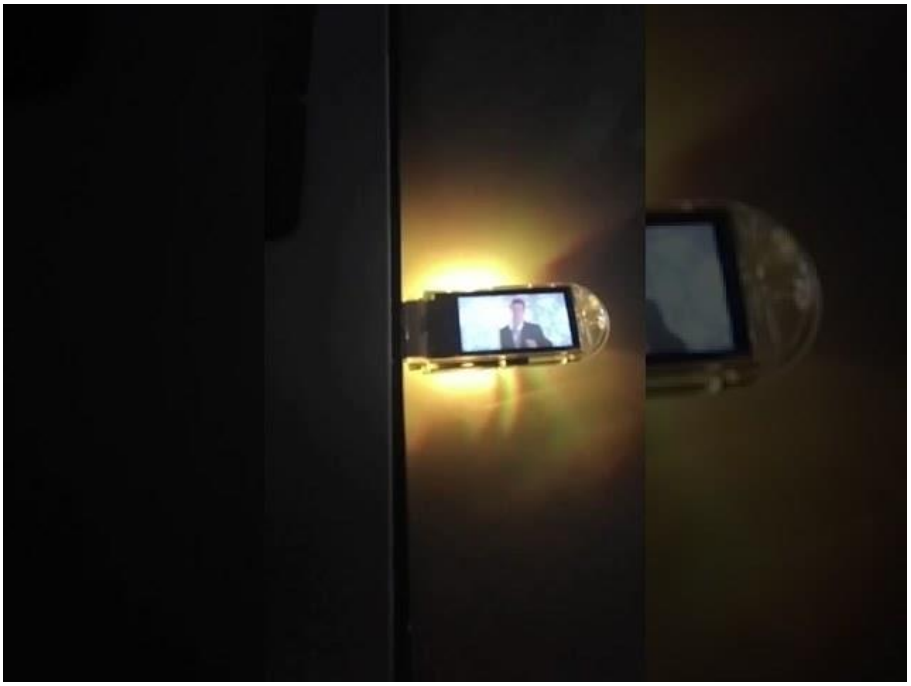
1.png	✓	22/02/2025 6:49	Archivo PNG	10 KB
2.png	✓	22/02/2025 6:49	Archivo PNG	10 KB
3.png	✓	22/02/2025 6:49	Archivo PNG	10 KB
autorun.ds	✓	22/02/2025 6:49	Archivo DS	1 KB

Enchufa el dispositivo.

Observa las redes wifi creadas:


Vodafone-C01610103
01 Never gonna give you up
02 Never gonna let you down
03 Never gonna run around
04 and desert you
05 Never gonna make you cry
06 Never gonna say goodbye
07 Never gonna tell a lie
Configuración de red e Internet
Cambia los ajustes de configuración, como hacer que una conexión sea de uso medido.
Wi-Fi
Modo avión
Zona con cobertura


YouTube
Rick Roll (Different link + no ads)
Duran
Subscribe



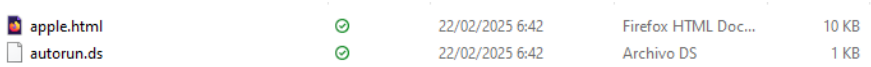
EvilAP

Un "evil portal" (portal malvado) es un tipo de ataque de seguridad informática que engaña a los usuarios para que se conecten a una red Wi-Fi falsa que parece legítima. Una vez conectados, los atacantes pueden robar información confidencial, como contraseñas, información de tarjetas de crédito o datos personales.

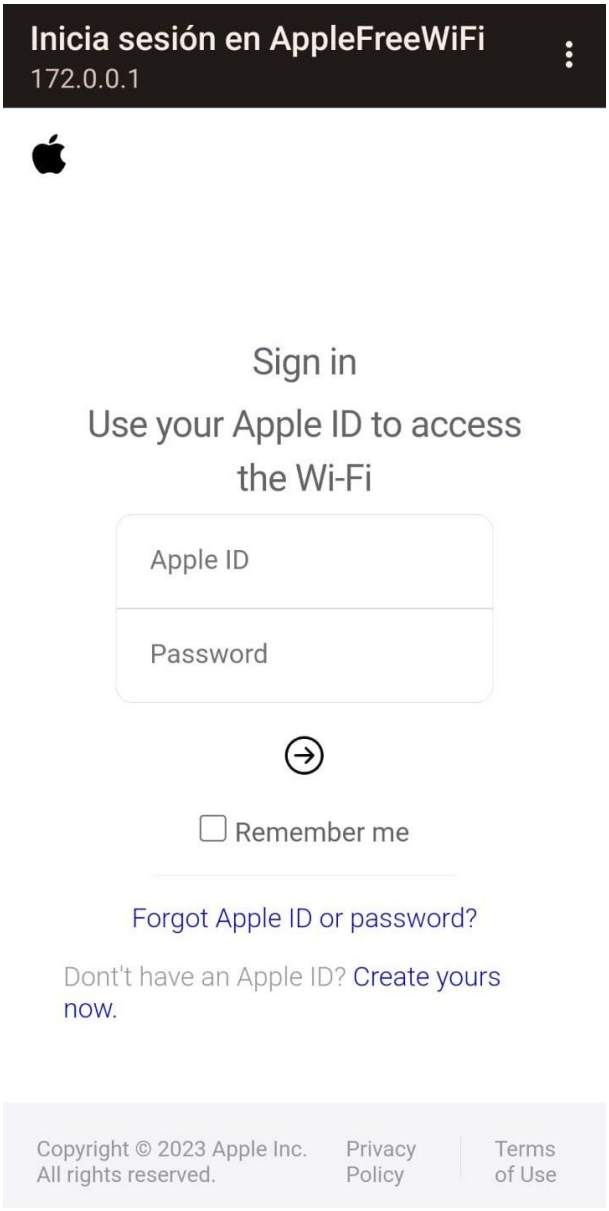
¿Cómo funciona un evil portal?

1. **Creación de una red Wi-Fi falsa:** El atacante configura un punto de acceso Wi-Fi que tiene un nombre similar o idéntico a una red legítima, como la de un café, un aeropuerto o un hotel.
2. **Atracción de víctimas:** Los usuarios que buscan conectarse a Wi-Fi ven la red falsa y, creyendo que es legítima, se conectan a ella.
3. **Captura de información:** Una vez conectados, el atacante puede interceptar todo el tráfico de la red, incluyendo las credenciales de inicio de sesión y otra información confidencial.
4. **Redirección a páginas web falsas:** En algunos casos, el atacante puede redirigir a los usuarios a páginas web falsas que imitan sitios legítimos, como bancos o redes sociales, para robar aún más información.

Para probarlo solo tienes que descargar estos dos archivos desde aquí y copiarlos a tu tarjeta SD

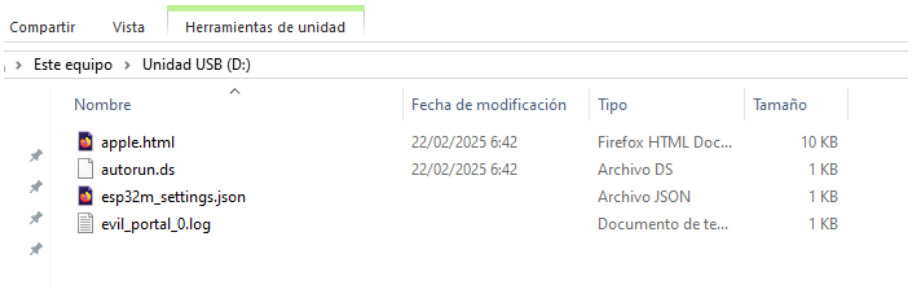


Conectas el dispositivo y se crea una red wifi llamada **AppleFreeWiFi:**

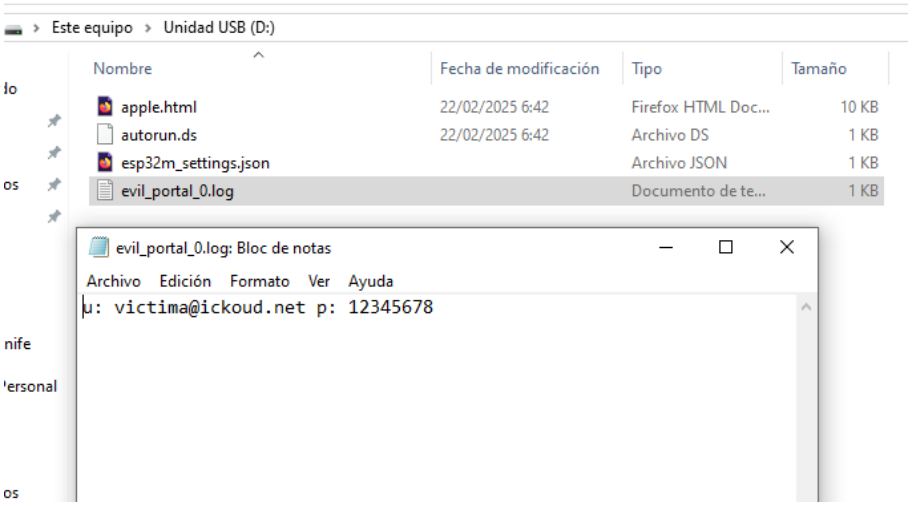


La víctima visita el punto de acceso libre y teclea sus credenciales.

Esas credenciales quedan grabadas en un archivo que se crea en la tarjeta SD llamado *evil_portal_0.log:*



En ese archivo tenemos las credenciales capturadas:



Requisitos

Para ejecutar Evil Portal, el usuario deberá proporcionar dos configuraciones:

- Nombre de punto de acceso: Puede ser proporcionado por la lista SSID, lista AP o archivo SD
- index.html: Sólo se puede proporcionar por archivo SD

Nombre de punto de acceso

El nombre del punto de acceso puede fijarse en la siguiente lista de prioridades:

1. El primer SSID en la lista de los SSID
2. La primera instancia de una AP "seleccionada" en la lista de AP
3. De /ap.config.txten la tarjeta SD acoplada a su ESP32

Usando SSIDs

Puede crear una lista de los SSID usando ssid, Add SSID o Generar SSID

Usando APs de escaneo

Puedes obtener una lista de puntos de acceso usando escaneo o Scan APs. Esta opción esencialmente clon un punto de acceso pre-escaneado y lo usarán para EvilPortal.

Usando ap.config.txt

Sólo tienes que poner el nombre deseado de tu punto de acceso en el archivo como...

FreeWifi

index.html

Por el momento, index.html sólo se puede proporcionar a través de /index.html en la raíz de la tarjeta SD adjunta al ESP32.

Puedes encontrar muchos archivos HTML diferentes aquí en bigbrodude6119 's EvilPortal repo. Una vez que hayas elegido tu archivo HTML, cambia el nombre a index.html y colócalo en la raíz de tu tarjeta ESP32 SD. Si deseas almacenar varios archivos HTML en tu tarjeta SD, puedes utilizar el sethtml subcomando de evil portal para seleccionar un archivo HTML específico antes de iniciar el ataque o al iniciar el ataque. También puedes utilizar Select EP HTML File para seleccionar cualquiera de los archivos HTML de tu tarjeta SD si está utilizando hardware oficial de Marauder.

Uso

evilportal [-c start [-w <html.html>]/sethtml <html.html>]

Argumentos

Argumentos	Requerido/opcional	Descripción
`-c`	Opcional	Ejecute un comando contra el módulo del portal malvado. `start` / `sethtml` -
`-w`	Opcional	Especifique un archivo HTML para usar. Sólo se usa cuando se usa `-c start`

Ejemplos

- `evilportal -c start` : Iniciar el portal malvado con predeterminado `index.html` archivo como el HTML
- `evilportal -c sethtml apple.html` : Establezca el HTML activo como `apple.html`
- `evilportal -c start -w CoxWifi.html` : Empieza malvado portal con `CoxWifi.html` como el HTML

USB Ethernet PCAP

Convierte el dispositivo en un adaptador de red USB y captura los primeros segundos de tráfico de red en un archivo PCAP.

Puedes descargar el archivo de ejemplo **aquí**

Lo único que debes hacer es copiar el archivo autorun.ds a la tarjeta SD

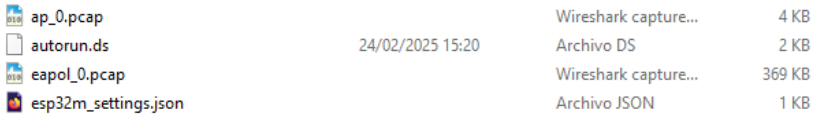
Conecta el dispositivo por el puerto USB en algún equipo que esté conectado a alguna red.

Cuando te lo indique aprieta el botón.

Espera unos segundos hasta capturar unos paquetes

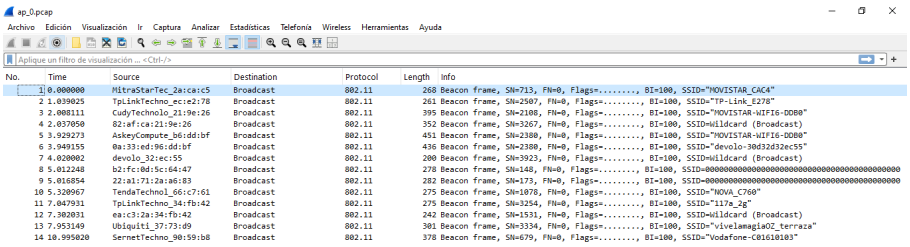
Vuelve a apretar el botón para terminar.

Desconecta el dispositivo y analiza el contenido de la tarjeta SD:



Abrimos las capturas con Wireshark.

La captura ap_0.pcap muestra todas las redes que pueden ser accesibles por la conexión wifi del equipo:

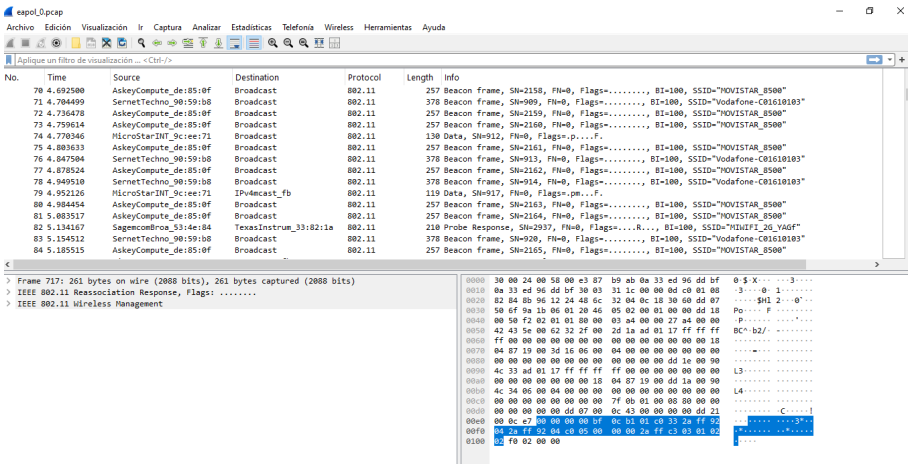


La captura eapol_0.pcap es mucho más completa.

Resumen de la Captura

- Se observa principalmente tráfico **802.11** (Wi-Fi), en particular:
    - **Probe Requests** (solicitudes de sondeo) de la dirección AzureWaveTec_51:47:c4 buscando la red MOVISTAR_PLUS_B37A.
    - **Beacon Frames** (tramas de baliza) de distintos APs anunciando redes como MOVISTAR_8500 y Vodafone-C01610103.
    - **Data Frames** con direcciones multicast (IPv6mcast_fb, IPv4mcast_fc).
- AzureWaveTec_51:47:c4 está enviando repetidas **solicitudes de sondeo (Probe Requests)** para MOVISTAR_PLUS_B37A, lo cual sugiere que es un cliente buscando conectarse a esa red Wi-Fi.
- AskeyCompute_de:85:0f y SernetTechno_90:59:b8 envían **tramas de baliza (Beacon Frames)** anunciando la disponibilidad de redes Wi-Fi.
- MicroStarINT_9c:ee:71 está enviando tramas de **datos multicast**, lo cual podría estar relacionado con comunicación en una red local.
- **Comportamiento Repetitivo de Probe Requests**:

- AzureWaveTec_51:47:c4 está enviando muchas solicitudes de sondeo en poco tiempo. Esto indica un ataque de escaneo pasivo para detectar redes disponibles.



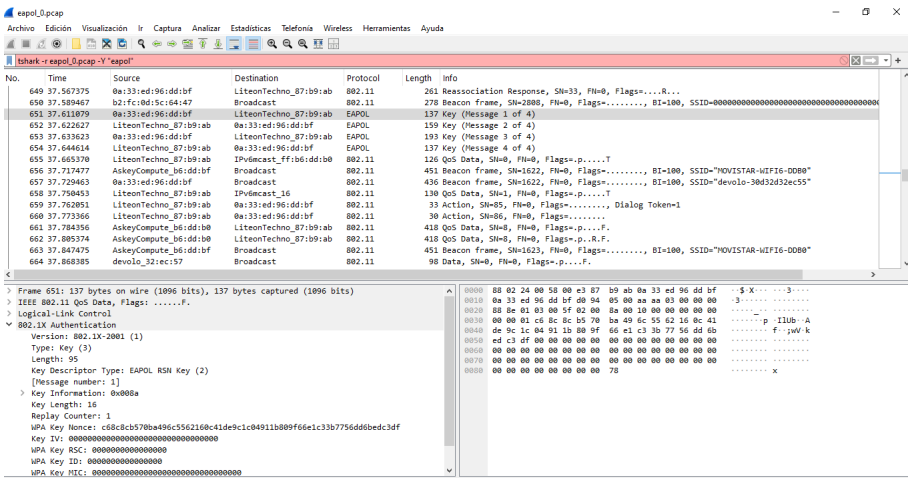
Si buscas el **handshake** en la captura, específicamente el **4-Way Handshake de WPA/WPA2**, debemos buscar paquetes EAPOL (Extensible Authentication Protocol over LAN), que son los que se intercambian entre el cliente y el punto de acceso durante la autenticación.

En la captura se ha registrado el **4-Way Handshake** de WPA/WPA2. Se encuentran los cuatro mensajes EAPOL clave:

1. **Mensaje 1 de 4** (Frame 651 y 674)
    a. **Fuente:** 0a:33:ed:96:dd:bf
    b. **Destino:** LiteonTechno_87:b9:ab
    c. **Protocolo:** EAPOL
    d. **Función:** El AP envía el primer mensaje con un nonce aleatorio al cliente.
2. **Mensaje 2 de 4** (Frame 652)
    a. **Fuente:** LiteonTechno_87:b9:ab
    b. **Destino:** 0a:33:ed:96:dd:bf
    c. **Función:** El cliente responde con su propio nonce y el MIC (Message Integrity Code).
3. **Mensaje 3 de 4** (Frame 653)
    a. **Fuente:** 0a:33:ed:96:dd:bf
    b. **Destino:** LiteonTechno_87:b9:ab
    c. **Función:** El AP envía una clave PTK (Pairwise Transient Key).

4. **Mensaje 4 de 4** (Frame 654)
    a. **Fuente:** LiteonTechno_87:b9:ab
    b. **Destino:** 0a:33:ed:96:dd:bf
    c. **Función:** El cliente confirma la recepción de la clave y finaliza el proceso.

Esto significa que el handshake se ha capturado correctamente, lo cual podría ser útil si estás analizando seguridad o realizando auditorías de red



Consideraciones importantes:

- Es fundamental utilizar USBArmyKnife de manera ética y responsable. Solo se debe utilizar la herramienta en sistemas y dispositivos para los que se tenga permiso explícito.

- El uso indebido de USBArmyKnife puede tener consecuencias legales.
- Es importante comprender los riesgos asociados con las pruebas de seguridad USB y tomar las precauciones necesarias para proteger los sistemas y datos.

Conclusión:

USBArmyKnife es una herramienta esencial para cualquier profesional de la seguridad que necesite evaluar la seguridad de dispositivos USB y sistemas relacionados. Su diversidad de ataques, flexibilidad y facilidad de uso la convierten en una opción poderosa para pruebas de penetración, análisis de vulnerabilidades y auditorías de seguridad.

Si te interesa la ciberseguridad y las pruebas de penetración, te recomiendo explorar el repositorio USBArmyKnife en GitHub.