***El Arsenal Del Hacker***

***Raspberry pi 4***

*Precio: a partir de 35 dólares*

*Link: https://www.raspberrypi.org/products/raspberry-pi-4-model-b/*

*Los miniordenadores Raspberry Pi de la última gama de modelos funcionan con chips Armovy de cuatro núcleos, están equipados con 1, 2 o 4 GB de RAM, son compatibles con Wi-Fi y Bluetooth y tienen dos puertos micro HDMI y cuatro USB. Casi pueden sustituir a una mesa de oficina de bajo coste, a menudo utilizada para crear centros multimedia y servidores domésticos, así como una gran variedad de proyectos diferentes, desde instrumentos musicales hasta robots.*

*Pero a nosotros nos interesa algo más: raspberry puede convertirse en un sistema portátil para pentests. Y carcasas listas para usar, pantallas, baterías y otros kits de carrocería, muchos más. Por cierto, en la revisión 1.2 han solucionado el problema de compatibilidad con algunos tipos de USB-C, tened en cuenta.*

Un circuito electrónico

Descripción generada automáticamente con confianza media

***Proxmark 3***

*Precio: 100-300 euros*

*Link: https://www.kickstarter.com/projects/1408815241/proxmark3-rdv-40*

*Uno de los mejores ayudantes para realizar ataques con tarjetas sin contacto ha sido y es un dispositivo para hackers llamado Proxmark3.*

*Está disponible en varias versiones.*

*RDV1 es una versión antigua del dispositivo, que rara vez se encuentra en el mercado, y no tiene ninguna ventaja especial.*

*RDV2: La ventaja de esta versión es la disponibilidad de un conector para una antena externa.*

*RDV3 es el modelo más popular (y más barato) del mercado, existen clones chinos con las mismas características, pero no siempre con un rendimiento estable.*

*RDV4 es la última versión de Proxmark, que al mismo tiempo incluye hardware y software para trabajar con tarjetas inteligentes. Es el modelo más caro de la lista.*

*Proxmark reemplazará todos los dispositivos similares para usted, pero vale la pena señalar que si usted va a estudiar sólo las tarjetas Mifare, es mejor mirar hacia el Chameleon Mini.*

Interfaz de usuario gráfica

Descripción generada automáticamente

***APImote***

*Precio: 150 dólares*

*Link: http://apimote.com*

*Si te has topado con una casa inteligente, probablemente hayas oído hablar del protocolo ZigBee. Tiene muchos años, pero no hay tantos dispositivos preparados para probar la seguridad de la red. Entre ellos se encuentra el tablero APImote, que funciona junto con el framework killerbee. El dispositivo viene listo para usar, pero para los aficionados a la soldadura, los desarrolladores han publicado los esquemas de KiCad en GitHub.*

Un circuito electrónico

Descripción generada automáticamente con confianza media

***E-mate x***

*Precio: 100 dólares*

*Link: https://gsmserver.es/e-mate-x-emmc-bga-13-in-1/*

*El kit E-Mate X será un regalo muy útil para quienes trabajan a menudo con sistemas integrados o smartphones. Consiste en trece adaptadores de chips de memoria no volátil en el paquete BGA a diferentes programadores e incluso a la entrada SD (que en algunos casos permite leer la memoria sin necesidad de un programador).*

*El coste de los análogos con sólo uno de los adaptadores puede superar el coste del E-Mate X dos veces, o incluso más.*

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

***Magspof***

*Precio: 60 dólares*

*Link: https://samy.pl/magspoof/*

*Cuando se trabaja con tarjetas magnéticas, muchos se enfrentan al mismo problema: un lector de tarjetas de tres vías con capacidad de escritura a veces cuesta cinco veces más que el mismo lector sin capacidad de escritura.*

*Para estas tareas se desarrolló la tarjeta MagSpoof, en la que se pueden grabar los datos de tres bandas magnéticas y falsificarlos. Por tanto, el dispositivo sustituye a la propia tarjeta. Y junto con un lector de tarjetas magnéticas, se ahorrará la mitad del dinero y obtendrá un dispositivo completo para probar la seguridad de acceso o el sistema de pago.*

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

***Cable O.MG***

*Precio: 120 dólares*

*Link : http://mg.lol/blog/omg-cable/*

*El cable para hackers O.MG se dio a conocer principalmente por la actuación de sus desarrolladores en DEFCON 2019. En este cable, se cose un Rubber Ducky completo con Wi-Fi, que permite introducir remotamente comandos de teclado en el dispositivo conectado. Y la principal ventaja de O.MG es que su apariencia es indistinguible de un cable de carga convencional. Hay varias opciones: Tipo-C, micro-USB y Lightning.*

Imagen que contiene cable

Descripción generada automáticamente

***DSLogic***

*Precio: 60-150 dólares*

*Link : https://www.dreamsourcelab.com*

*Un analizador lógico ayuda a depurar los circuitos digitales. Y los analizadores de la serie DSLogic se han establecido como uno de los mejores en términos de precio y calidad. Además, a diferencia de los productos de la empresa Saleae, son compatibles con proyectos de código abierto como PulseView.*

*En total, hay tres modelos de DSLogic disponibles en el sitio web oficial: Plus, U3Pro16 y U3Pro32. Y si eres aficionado a la fabricación de soldaduras, puedes buscar DSLogic Basic en AliExpress. Este modelo no se diferencia del DSLogic Plus, salvo por su menor precio y su memoria. Por cierto, habrá un reto adicional si quieres actualizarlo.*

Imagen que contiene electrónica, circuito

Descripción generada automáticamente

***FacerDancer21***

*Precio: 85 dólares*

*Link: http://goodfet.sourceforge.net/hardware/facedancer21/*

*El dispositivo de hacking FaceDancer21 es imprescindible para un probador de terminales de pago. Con él, puede hacer lo siguiente.*

*Emular diferentes dispositivos USB. Por ejemplo, puede crear un dispositivo con un ID específico y omitir la lista de dispositivos conectados permitidos.*

*Determinar qué tipos de dispositivos admite el puerto USB. Útil cuando se trabaja con cajeros automáticos y cargadores inalámbricos (en caso de que la carga inalámbrica sea el puerto de un ordenador pequeño).*

*Fuzz: conveniente para encontrar 0 días en los controladores USB.*

*Interactuar a través de USB utilizando la biblioteca de Python.*

*Debido a que la placa es de código abierto, su precio varía según la codicia del fabricante*



***Yard Stick One***

*Precio: 100 dólares*

*Link: https://greatscottgadgets.com/yardstickone/*

*Si has intentado desbloquear la cerradura de tu coche repitiendo la señal de desbloqueo, entonces tal vez evalúes este dispositivo. Yard Stick One le permite enviar y recibir tráfico en frecuencias populares (hasta 1 GHz). Su característica distintiva es el uso del chip CC1111, que permite al hardware demodular o modular la señal, lo que mejora la calidad de recepción y transmisión. Para utilizar el Yard Stick, es necesario instalar la utilidad gratuita RFCat.*

Un circuito electrónico

Descripción generada automáticamente con confianza media

***NFC Kill***

*Precio: 180/250 dólares*

*Link: https://nfckill.com*

*Pocos pueden sorprenderse ahora con dispositivos para probar las tarjetas sin contacto. Pero el dispositivo NFC Kill definitivamente le interesará: En primer lugar, está destinado a las pruebas difusas de los sistemas de lectura sin contacto. Y las funciones adicionales le permiten desactivar tanto los lectores como las tarjetas sin contacto.*

*El dispositivo funciona en tres frecuencias: baja frecuencia (125-134 kHz), alta frecuencia (13,56 MHz) y ultra alta frecuencia (850-930 MHz). Se presenta en dos versiones: estándar y profesional. La diferencia entre ellas es la posibilidad de realizar pruebas sin interacción física con el dispositivo.*

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

***Bash Bunny***

*Precio: 100 dólares*

*Link: https://shop.hak5.org/products/bash-bunny*

*Es probable que ya conozca el Rubber Ducky, un dispositivo que emula un teclado e inyecta automáticamente comandos maliciosos en el ordenador de la víctima. El dispositivo Bash Bunny es una versión más sofisticada del dispositivo para ataques HID.*

*Además del teclado, puede emular cualquier puerto serie, almacenamiento de archivos y adaptadores USB - Ethernet. Este dispositivo es perfecto para probar el Equipo Rojo y le ahorra dinero y espacio en el equipo de acampada.*

Imagen de la pantalla de un celular

Descripción generada automáticamente con confianza baja

***Hydrabus***

*Precio: 75 euros*

*Link: https://hydrabus.com/?v=3acf83834396*

*HydraBus fue diseñado originalmente como un reemplazo completo para el anticuado BusPirate. Esta es una lista de las principales ventajas de HydraBus:*

*proporciona una interfaz de usuario completa para trabajar con interfaces de hardware populares (I2C, SPI, UART, 1-3 hilos, JTAG / SWD);*

*HydraBus se puede utilizar junto con PulseView para operar en modo analizador lógico;*

*Hay una biblioteca en Python, que simplifica el uso;*

*Hay una ranura microSD para almacenar información mientras se trabaja.*

Imagen que contiene electrónica, circuito

Descripción generada automáticamente

***OpticSpy***

*Precio: 65-100 dólares.*

*Link: http://opticspy.org*

*Los dispositivos como los routers a menudo transmiten mucha información valiosa usando LEDs parpadeantes, especialmente cuando están encendidos. Sucede que estos LEDs están conectados a una línea de datos, por ejemplo, al pin TX del bus UART.*

*Para recibir información de este canal de datos sin soldaduras ni costosos analizadores lógicos, hemos desarrollado un pañuelo llamado OpticSpy. Para que funcione, tendrás que instalar la librería de Python, conectar OpticSpy al ordenador vía USB, y llevar tu fotodiodo a la fuente de luz.*

Control de video juego

Descripción generada automáticamente con confianza baja

***Hunter Cat***

*Precio: 35 dólares*

*Link: https://hunter.electroniccats.com*

*En 2019 apareció en el mercado un interesante dispositivo de hacking: Hunter Cat. Aunque es más para protección que para piratería y pentest. Fue desarrollado para buscar bancos y otros skimmers. Su esencia es sencilla: lo introducimos en el lector de tarjetas, lo sacamos y miramos el LED. Si se ilumina en verde, no se detecta el skimmer, de lo contrario es mejor no utilizar este cajero. El tamaño del Hunter Cat es ligeramente mayor que el de una tarjeta bancaria, y su coste es de unos 35 dólares.*

Imagen de la pantalla de un celular con letras

Descripción generada automáticamente con confianza media

***dongle nRF52840***

*Precio: 18 dólares*

*Link: https://www.nordicsemi.com/Software-and-tools/Development-Kits/nRF52840-Dongle*

*Tiene muchas oportunidades, entre las cuales hay dos. En primer lugar, puedes actualizarlo y conseguir un completo sniffer Bluetooth de bajo consumo con un bonito plugin para Wireshark. En segundo lugar, con el proyecto de código abierto LOGITacker, puedes convertir este dispositivo de seguridad en un aparato para probar los periféricos inalámbricos del ordenador: ratón, teclado, etc.*

Imagen que contiene electrónica, circuito

Descripción generada automáticamente

* ***github.com/AngelSecurityTeam***