Hacking con hardware

Boletín No. 80
1o. de septiembre de 2020

Hernandez Acosta Juan Jose
kiral.jhn@gmail.com

Méndez Lozano Oscar Geovani
mendezlozanoog@gmail.com

Vicario Solórzano Claudia Marina
marina.vicario@gmail.com#

RESUMEN

El pirateo de hardware es una forma de poder ingresar de manera no autorizada a algunas CPU con la ayuda de diferentes dispositivos electrónicos que facilitan la entrada de este. Esto lo hacen personas llamadas hackers de sombrero negro que tienen intenciones maliciosas para robar, destruir o crear información dentro de las CPU. En la industria es común encontrar muchos dispositivos infiltrados y ocultos con la intención de ejercer este delito. Las personas que ejercen este delito tienen un amplio conocimiento de la electrónica y la programación para poder maniobrar bien con estos dispositivos electrónicos. Se recomienda realizar una inspección de mantenimiento del hardware y el software de forma rutinaria para evitar ser víctima de este delito.

Palabras Clave: hacking, hardware, seguridad informática, software.

ABSTRACT

The hardware hacking is a way to be able to enter in an unauthorized way to some CPU with the help of different electronic devices that facilitate the entry of this. This is done by people called black hat hackers who have malicious intentions in order to steal, destroy, or create information within the CPUs. In the industry it is common to find many infiltrated and hidden devices with the intention of exercising this crime. People who exercise this crime have extensive knowledge of electronics and programming to be able to maneuver well with these electronic devices. It is recommended that a maintenance inspection of the hardware and software be routinely done to avoid being a victim of this crime.

Key-words: hacking, hardware, informatic security, software.

INTRODUCCION

Hacker: persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora sobre los mismos encontrando vulnerabilidades dentro de este. (Erickson G, 2008, p. 57).

Existen varias áreas de hacking dentro de la industria de la información, como es el de software y el de hardware. El hardware hacking trata de que con dispositivos externos, anteriormente cargados con

algún software, logre infiltrarse dentro del hardware que desea hackear. Para el hardware hacking se necesita anteriormente un conocimiento de electrónica, de comunicaciones entre componentes de circuitería impresa, de sistemas operativos e ingeniería inversa de software; lo que dificulta mucho su realización.

Una vez que tenemos la definición clara de lo que es un hacker y su función dentro del mundo virtual, podemos hablar del tipo de hacker que representa nuestro protagonista de este artículo.

1 .El hacker de Black Hat: Es un tipo de hacker, llamado “Hacker de sombrero negro”, es el que usa técnicas sofisticada para acceder a sistemas, apoderarse de ellos y de sus datos, para después, venderlos, destruirlos, etc. (Kypke J. 2017)

Es importante decir que nos centramos en solo definir a esta categoría de hackers, por que es la única que utiliza el método de USB killer, ya que es un método considerado ilícito y con fines no justificables. (Reyes R. 2005, p. 72)

Dispositivos de hardware hacking

1. Dispositivos de hardware hacking

2. USB killer: Se conecta a un equipo a través de su puerto USB y acumula parte de la energía generada por éste en unos condensadores. Después, descarga toda esa electricidad almacenada en la placa base del PC, “friendo” el equipo en cuestión de segundos. Esta descarga puede alcanzar los 220 voltios, prácticamente “matando” el aparato donde se conecte. (Wilhelm S. 2011, p. 32).

Figura 1.1 Fuente: Sancristan, L, (2018), USB killer. Recuperado de http://www.revista-gadget.es Figura 1.1 Fuente: Sancristan, L, (2018), USB killer. Recuperado de http://www.revista-gadget.es

3. Rubber Ducky: Normalmente cuando conectamos un dispositivo USB a un ordenador, no lo analizamos con un antivirus, y lo único que queremos es acceder a los archivos que este contiene. Rubber Ducky, un dispositivo que nos va a permitir robar datos fácilmente del ordenador al cual lo conectemos. (Álvarez Á. 2018, p.1).

Figura 1.2 Fuente: De Luz, S, (2018), Rubber Ducky. Recuperado de https://www.redeszone.net/

4. Bus Pirate: Es una herramienta electrónica universal y abierta que sirve para interactuar entre una computadora y la mayoría de los chipsets de una PC, ayudando a reducir los esfuerzos cuando se trabaja con chips desconocidos. Entre sus principales capacidades, Bus Pirate permite medir frecuencias entre 1 Hz y 40 MHz, escuchar tráfico en el puerto y muchas otras cosas más. (Joe Grand,Kevin Mitnick,Ryan Russel,2018)

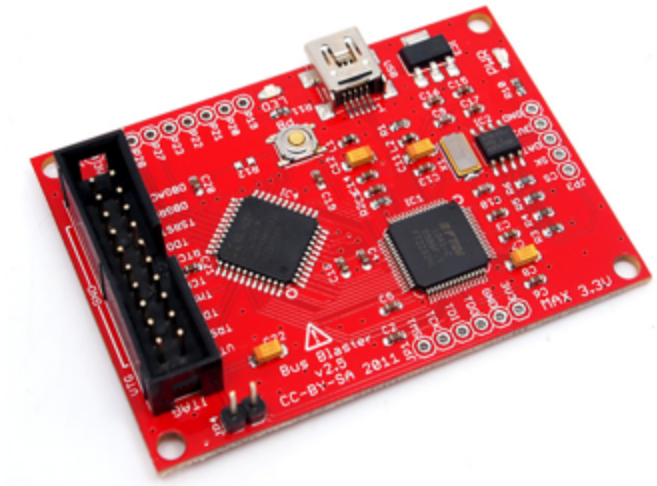

Figura 1.3 Fuente: Manuel, J, (2018), Bus Pirate. Recuperado de https://www.welivesecurity.com

5. Facedancer: Este gadget es un emulador USB de código abierto y una herramienta de fuzzing de dispositivos USB. Permite a una computadora o host enmascararse como un dispositivo USB para comunicarse con otros dispositivos USB o USB anfitriones. El propósito de este dispositivo es vincular estaciones de trabajo, de tal forma que los controladores de dispositivo USB de una estación de trabajo anfitriona puedan ser testeados mediante fuzzing en otra estación de trabajo.

Figura 1.4 Fuente: Manuel, J, (2018), Facedancer. Recuperado de https://www.welivesecurity.com

6. Adaptador inalámbrico USB Alfa AWUS036NHA: Se trata de un USB inalámbrico de largo alcance. Permite escuchar el tráfico y realizar otras tareas inalámbricas sin necesidad de deshabilitar el adaptador inalámbrico de una laptop. En este sentido, permite continuar navegando por Internet a través de la tarjeta inalámbrica principal mientras se mantenga el adaptador USB en el modo escaneo. (Joe Grand, Frank Thornton, Albert Yarusso, Lee Barken, Tom Owad, Ryan Russell, Bobby Kinstle, Marcus Brown, Job de Haas Deborah Kaplan,2006)

Figura 1.5 Fuente: Manuel, J, (2018), Adaptador inalambrico usb Alfa. Recuperado de https://www.welivesecurity.com

7. YARD Stick One: El YARD Stick One es una poderosa herramienta para pruebas inalámbricas. Puede enviar y recibir señales digitales inalámbricas permitiendo auditar fácilmente dispositivos inalámbricos que funcionan de manera remota, como sistemas de entradas sin llave (keyless entry systems). Se trata de una gran herramienta para realizar auditorías e investigaciones en transceptores inalámbricos. (Joshua Brashars, 2007). Figura 1.6 YARD Stick One.

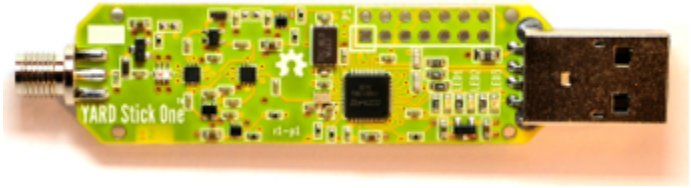

Figura 1.5 Fuente: Manuel, J, (2018), YARD Stick One. Recuperado de https://www.welivesecurity.com

En la industria es frecuente encontrarse con chips multipropósito, con diseños de uso general y utilizados en diferentes dispositivos específicos. Esto es una ventaja para el fabricante a la hora de producirlos, pero también es una ventaja a la hora de analizarlo. Esto facilita su estudio y el seguimiento de descubrimientos, por parte de personas dedicadas al “Hardware Hacking”.Conocer y controlar las entradas y salidas, tanto digitales como analógicas, que acepta un chip permite modificar el comportamiento normal del dispositivo, simular reseteados, forzar reinicios, etc. (Wutka, M. 1997, p. 45). Los análisis estáticos y dinámicos de todas las funciones que intervienen permiten descubrir los argumentos empleados, así como la existencia o no de validaciones de entrada o salida.

Problemas y medidas preventivas en la industria

El fabricante, desde la fase inicial de diseño, es el encargado de construir un producto robusto. La visión del cliente final debe estar recogida en el ciclo de producción, o al menos tenida en cuenta para introducir demandas y mejoras. Hasta el espacio de usuario (Aplicaciones) gestión de usuarios, roles, permisos; sin olvidar en ningún momento el aspecto físico y los mecanismos Anti-Tampering.

A nivel de hardware, el fabricante del dispositivo dispone de medios para evitar ciertas técnicas de hardware hacking. La lectura directa de señales en los pines de un chip puede ser evitada mediante el uso de resina epoxy cubriendo dichas patillas; si un atacante intenta quitar la resina, la placa se daña impidiendo establecer las comunicaciones. La existencia de puertos de prueba (debug), JTAG, SPI, I2C UART, en placas de producción podrían ser aprovechados por los especialistas en hardware hacking: si no son necesarios, o no van a ser usado en el cliente final, deben desaparecer. (Wellick,T. 2015).

Referencias

1. Álvarez, Á. (**2018**). *A Wearable Device and System for Movement and Biometric* Data Acquisition for Sports Applications.

2. De Luz, S, (**2015**).Rubber Ducky. Recuperado de https://www.redeszone.net/2018/03/17/rubber-ducky-usb-atacar-ordenador/

3. Erickson, G. (**2008**). *Hacking: The art of exploitation (2).* Northern California: No Starch Press.

4. Joe Grand, Frank Thornton, Albert Yarusso, Lee Barken, Tom Owad, Ryan Russell, Bobby Kinstle, Marcus Brown, Job de Haas Deborah Kaplan (**2006**). *Joe Grand's Best of HardwareWireless, and Game Console Hacking*KANSAS.

5. Joe Grand ,Kevin Mitnick, Ryan Russel, (**2018**). *welive security. Communications*Sitio web https://www.welivesecurity.com/

6. Joshua Brashars (**2007**). *Asterisk Hacking. (1). Illinois, Springfield.* 100-120.

7. Autor (**año**). *Título del artículolibro,revista o nombre de la página web*texto restante https://www.lipsum.com/feed/html