ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACIÓN

UNIVERSIDAD DE CANTABRIA

Trabajo Fin de Grado

PLATAFORMA PORTÁTIL DE PENTESTING BASADA EN RASPBERRY PI

(Portable platform for pentesting using Raspberry Pi)

Para acceder al Título de

Graduado en

Ingeniería de Tecnologías de Telecomunicación

Autor: Cristina Secada Carral

Junio-2019

GRADUADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

CALIFICACIÓN DEL TRABAJO FIN DE GRADO

Realizado por: Cristina Secada Carral
Director del TFG: Roberto Sanz Gil
Título: "Plataforma portátil de pentesting basada en Raspberry Pi"
Title: "Portable plataform for pentesting using Raspberry Pi**"**

Presentado a examen el día:

para acceder al Título de

GRADUADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

Composición del Tribunal:
Presidente (Apellidos, Nombre): Tomás Fernández Ibáñez
Secretario (Apellidos, Nombre): Alberto Eloy García Gutiérrez
Vocal (Apellidos, Nombre): Roberto Sanz Gil

Este Tribunal ha resuelto otorgar la calificación de: .....

Fdo.: El Presidente	Fdo.: El Secretario
Fdo.: El Vocal	Fdo.: El Director del TFG (sólo si es distinto del Secretario)
Vº Bº del Subdirector	Trabajo Fin de Grado Nº (a asignar por Secretaría)

Agradecimientos

En primer lugar, a mis padres por su apoyo, confianza y cariño que me han brindado durante mi etapa en la universidad y siempre. A mi familia por confiar siempre en mí, gracias.

A mis amigos de siempre, que como yo, han estado en mi misma situación y nos hemos ayudado, apoyado en los buenos y malos momentos.

A mis compañeros de universidad, que muchos de ellos son y serán amigos, gracias por la ayuda brindada durante estos años. Por hacer que los años de universidad hayan sido los mejores, porque nuestras anécdotas, risas, lágrimas y clases no se olvidaran nunca.

Por último a mi tutor, Roberto, por su ayuda y su paciencia, gracias porque haya sido posible este Trabajo de Fin de Grado.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

LISTA DE ACRÓNIMOS

AES	Advanced Encryption Standard
AP	Access Point
CCMP	Counter-Mode Cipher Block Chaining Message Authentication Code Protocol
CPU	Central Processing Unit
DB	Database
FTP	File Transfer Protocol
HDMI	High Definition Multimedia Interface
HTML	HyperText Markup Language
ICMP	Internet Control Message Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
LAN	Local Area Network
LTS	Long term support
MIB	Management Information Base
MTU	Maximum Transmission Unit
NFC	Near Field Communications
NOOBS	New Out of Box Software
OS	Operating System
PBC	Push Button Configuration
PIN	Personal Identification Number
PING	Packet Internet Groper
RAM	Random Access Memory
SLA	Service Level Agreement
SSH	Secure Shell
TCP	Transmission control protocol
TKIP	Temporal Key Integrity Protocol
TSN	Transition Security Network
UDP	User Datagram Protocol
USB	Universal Serial Bus

WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Lan
WMI	Windows Management Instrumentation
WPA	Wifi Protect Access
WPS	Wi-Fi Protected Setup

Resumen

La práctica de penetrar en redes y atacar para encontrar debilidades de seguridad a otros usuarios, empresas y a sí mismos es conocido como prueba de penetración, conocido en inglés como pentest. La finalidad de estas acciones es poder asegurar y prevenir los equipos antes estos ataques.

Se ha utilizado la Raspberry Pi 3 modelo B, ordenador de placa simple, para realizar pruebas de penetración mediante varias herramientas, además del sistema operativo Ubuntu.

Kali Linux, distribución basada en Debian GNU/Linux, es un sistema operativo el cual se ha instalado en la Raspberry Pi, incluye herramientas basadas en la penetración y auditoria de redes. Está posee muchas aplicaciones basadas en pruebas de penetración, por eso se trata de una herramienta para profesionales de la seguridad.

Por último, Ubuntu es un sistema operativo de código abierto. Es un sistema pensado en la seguridad. En él es instalada herramientas capaces de explotar vulnerabilidades como Routersploit y Metasploit.

Palabras claves

Penetración, redes, prueba, seguridad, herramientas, Raspberry PI, Kali Linux, Ubuntu, sistema operativo.

Abstract

The practice of penetrating networks and attacking to find security weaknesses to other users, companies and themselves is known as penetration test, known in English as pentest. The purpose of these actions is to be able to secure and prevent equipment before these attacks.

The Raspberry Pi 3 model B, single-board computer, has been used to perform penetration tests using various tools, in addition to the Ubuntu operating system.

Kali Linux, distribution based on Debian GNU / Linux, is an operating system which has been installed on the Raspberry Pi, includes tools based on penetration and network auditing. It has many applications based on penetration tests, so it is a tool for security professionals.

Finally, Ubuntu is an open source operating system. It is a system designed for security. It is installed tools capable of exploiting vulnerabilities such as Routersploit and Metasploit.

Keywords

Penetration, networking, testing, security, tools, Raspberry PI, Kali Linux, Ubuntu, operating system.

1. INTRODUCCIÓN

1.1 MOTIVACIÓN

La seguridad en las redes y equipos ha evolucionado a pasos agigantados. Las personas son capaces de utilizar la tecnología con una buena finalidad, o con una mala, conocido como hacker. Por este motivo, cada vez son más las personas que se dedican más al ámbito de la seguridad de las redes.

El "pentesting" o "test de penetración" consiste en atacar un sistema informático para identificar fallos, vulnerabilidades y demás errores de seguridad existentes, para así poder prevenir los ataques externos. [1]

Muchos de estos ataques son dirigidos a empresas, pero también son realizados en los propios equipos para poder identificar los posibles fallos de su seguridad.

El pentesting realmente es una forma de hacking, solo que esta práctica es totalmente legal, ya que cuenta con el consentimiento de los propietarios de los equipos que se van a testear, además de tener la intención de causar un daño real. [1]

Hoy en día, el número de aplicaciones o herramientas capaces de realizar o trastear sobre la seguridad de redes es enorme, y seguirá creciendo.

Por ello, estas son probadas en ordenadores y en Raspberry Pi, esta última no muy conocida, pero se va abriendo hueco en el mercado.

La Raspberry Pi es una computadora de muy bajo costo que se conecta a un monitor mediante la Interfaz multimedia de alta definición (HDMI) y utiliza su propio teclado y mouse USB. Raspberry Pi proporciona un entorno para aprender informática y programación a un precio extremadamente asequible. Las personas han utilizado la portabilidad y el bajo costo del dispositivo para construir dispositivos de aprendizaje, cámaras remotas, sistemas de seguridad, detectores de terremotos y muchos otros proyectos. [2]

Utilizar otra opción que no sea un ordenador, pero actúa como el, también hace que amplié nuestro conocimiento y se tenga una gama más amplia de trabajo.

1.2 OBJETIVOS

En este trabajo se van a estudiar herramientas capaces de vulnerar o atacar la red sobre Raspberry Pi, para conocerla, o sobre un ordenador.

Primero se va a hablar sobre la plataforma Raspberry Pi, describiéndola y viendo sus especificaciones para conocerla. Esta herramienta, utilizada en otros países de forma académica, ahora es estudiada también en una asignatura de la universidad de Cantabria, ya que actúa como un ordenador.

El propósito del trabajo era realizar todas las pruebas sobre la Raspberry Pi, pero debido a problemas de instalación, no ha sido posible.

Se va a hablar sobre el desarrollo de los sistemas operativos, para después instalar sobre ellos las herramientas o aplicaciones. Se van a conocer estas herramientas mediantes sus descripciones y se van a realizar pruebas. La finalidad es ver las posibles vulnerabilidades de una red.

El objetivo es realizar pruebas y comprobar si disponemos de un equipo seguro.

1.3 CONTENIDO DE LA MEMORIA

La memoria está dividida en tres capítulos. El primer capítulo hace referencia a la plataforma Raspberry Pi. En este capítulo se hará una breve introducción, historia y especificaciones de ella. La instalación de un sistema operativo en ella para la realización de pruebas de penetración. Y el resultado de una prueba de hackeo de wifi.

En los dos últimos capítulos se hablara sobre el desarrollo de dos sistemas operativos, Kali Linux y Ubuntu. Dentro de estos dos capítulos se hará una breve introducción. Sobre ellos, la instalación de herramientas y aplicaciones, con sus resultados obtenidos para encontrar vulnerabilidades en sus redes y ejemplos visuales mediantes fotos. Además de la descripción de estas herramientas.

El último capítulo incluirá las conclusiones donde se realiza un breve resumen de las herramientas utilizadas y los resultados. Y una valoración de líneas futuras sobre el tema de la seguridad de las redes y su evolución.

2. PLATAFORMA DE DESARROLLO: RASPBERRY PI

2.1 INTRODUCCIÓN

Raspberry Pi se describe como un ordenador simple o placa reducida que fue creado en el 2011 en Reino Unido por la Fundación Raspberry PI. Su fin era la enseñanza de informática en las escuelas. Es una propiedad registrada, pero no se conoce ciertamente si su hardware es libre o tiene derechos.

Su software si lo es, ya que es una versión adaptada del Debían, Raspbian. Está permite el uso de sistemas operativos. Su principal uso es el sistema operativo GNU/Linux.

Raspbian, una distribución derivada de Debian que está optimizada para el hardware de Raspberry Pi, el cual se lanzó en julio de 2012. Se considera una distribución recomendada por la fundación para iniciarse.

Slackware ARM (también llamada ARMedslack) versión 13.37 y posteriores arranca sin ninguna modificación. Los 128-496 MiB de memoria RAM disponible en la Raspberry Pi, cubren los necesarios 64 MiB de RAM para arrancar esta distribución en sistemas ARM y i386 sin usar interfaz gráfica (el administrador de ventanas Fluxbox que funciona bajo X WindowSystem requiere 48 MiB de memoria RAM adicional). Por otro lado, se están creando distribuciones más específicas y ligeras como IPfire (distribución para ser usada como firewall), u OpenELEC y OSMC (distribuciones con el centro multimedia Kodi). [3]

A la GPU se accede mediante una imagen del firmware de código cerrado, que se carga dentro de la GPU al arrancar desde la tarjeta SD. El archivo está asociado a los controladores del núcleo Linux que también son de código cerrado. Las aplicaciones hacen llamadas a las bibliotecas de tiempo de ejecución que son de código abierto, y las mismas hacen llamadas a unos controladores de código abierto en el núcleo Linux. La API del controlador del núcleo es específica para estas bibliotecas. Las aplicaciones que usan vídeo hacen uso de OpenMAX, las aplicaciones tridimensionales usan OpenGL ES y las aplicaciones 2D usan OpenVG; OpenGL ES y OpenVG hacen uso de EGL y este último, del controlador de código abierto del núcleo. [3]

2.2 HISTORIA

El 19 de febrero de 2012, la fundación lanzó un prototipo de imagen de tarjeta SD que almacenaba un sistema operativo y que podía ser cargado en una tarjeta SD. La imagen se basaba en Debian 6.0 (Squezze), con el escritorio LXDE y el navegador Midori, más algunas herramientas de programación. La imagen funcionaba bajo QEMU permitiendo que el Raspberry Pi pudiera ser emulado en otros sistemas. [3]

El 8 de marzo de 2012, la fundación lanzó Raspberry Pi Fedora Remix (actualmente llamada Pidora), que en el momento de era la distribución recomendada por la fundación, y fue desarrollada en la universidad de Séneca, en Canadá. También se propuso crear una tienda de aplicaciones para que la gente intercambiara programas. [3]

El 24 de octubre de 2012, Alex Bradbury, director de desarrollo Linux de la fundación, anunció que todo el código del controlador de la GPU Videocore que se ejecuta en ARM sería de código abierto, mediante licencia BSD modificada de 3 cláusulas. El código fuente está disponible en un repositorio de la fundación en GitHub. [3]

El 5 de noviembre de 2012, Eben Upton anunció el lanzamiento del sistema operativo RISC OS 5 para Raspberry Pi a la comunidad, pudiéndose descargar la imagen de forma gratuita desde la web de la fundación. Su relación con la comunidad RISC OS se remontaba a julio de 2011, cuando habló en ella de una hipotética versión. El sistema operativo incluye una gran cantidad de aplicaciones como NetSurf para la navegación web, StrongED para editar texto, Maestro para editar música, Packman para la gestión de paquetes o una tienda de aplicaciones llamada *Store* donde se puede encontrar aplicaciones gratuitas o de pago. Además, se incluyen manuales para crear aplicaciones en BASICpara el sistema operativo. [3]

El 24 de noviembre de 2012, se anunció en la Minecon de París, el juego Minecraft: *Pi* Edition para Raspberry Pi, basado en la versión Minecraft: Pocket Edition para teléfonos inteligentes y tabletas. La descarga se hizo disponible de forma oficial y gratuita por primera vez el 12 de febrero de 2013 desde el blog del juego, como versión 0.1.1 alpha, junto a instrucciones para ejecutarlo en Raspbian Wheezy. Una de las características

principales de este lanzamiento es poder interaccionar con el juego mediante programación, con la intención de motivar a los niños a aprender a programar. [3]

El 25 de mayo de 2013, la fundación informó de que se estaba trabajando en una versión del servidor gráfico Wayland para Raspberry Pi, para sustituir al sistema de ventanas X. Con este cambio se lograría suavidad al usar la interfaz gráfica del escritorio, ya que el procesamiento lo realizaría el núcleo de video de la GPU y no la CPU, sin interferir en el renderizado 3D. [3]

El 3 de junio de 2013, fue lanzado en la web de la fundación para su descarga la aplicación NOOBS, utilidad que facilita la instalación de diferentes sistemas operativos para Raspberry Pi. Se distribuye en forma de archivo zip que se copia descomprimido a una tarjeta SD de 4 o más GB, y una vez arrancada la placa con la tarjeta por primera vez, aparece un menú en que se da la opción de instalar una de las diferentes distribuciones en el espacio libre de la tarjeta de memoria, o acceder a internet con el navegador Arora integrado. Más adelante si se desea, es posible acceder a este menú apretando la tecla shift durante el arranque para reinstalar el sistema operativo, elegir otro, o editar el archivo config.txt. NOOBS contiene las distribuciones GNU/Linux de carácter general Raspbian, Arch Linux ARM y Pidora; las distribuciones para mediacenter con Kodi Openelec y RaspBMC; y el sistema operativo Risc OS 5. [3]

El 26 de septiembre de 2013, se añadió a los repositorios de Raspbian una versión oficial de Oracle Java JDK ARM con soporte para coma flotante por hardware, que ofrece bastante más rendimiento que la versión OpenJDK ARM ya existente hasta ese momento y más compatibilidad con aplicaciones. También se anunció que esta versión de Oracle Java JDK se incluiría dentro de la distribución en futuras versiones de Raspbian. [3]

2.3 ESPECIFICACIONES

La Raspberry consta de las siguientes especificaciones:

- Dimensiones: 85.60mm × 53.98mm (3.370 × 2.125 inch)

- Un Chipset Broadcom BCM2837, que contiene un CPU, GPU, DSP, SDRAM y puerto USB

- Un procesador central (CPU) de 1.2GHz 64-bit quad-core ARMv8

- Un procesador gráfico (GPU) Broadcom VideoCore IV, OpenGL ES 2.0, MPEG-2 y VC-1 (con licencia),[56] 1080p30 H.264/MPEG-4 AVC
- Memoria (SDRAM) de 1 GB (compartidos con la GPU)
- Un módulo de 512 MB de memoria RAM
- Un conector de RJ45 conectado a un integrado lan9512 -jzx de SMSC que nos proporciona conectividad a 10/100 Mbps
- 4 puertos USB
- Salida analógica de audio estéreo de 3.5mm.
- Salida digital de video + audio HDMI
- Salida analógica de video RCA
- Pines de entrada y salida de propósito general
- Almacenamiento MicroSD
- Conector de alimentación microUSB
- Conectividad de red de 10/100 Ethernet(RJ-45) vía hub USB, Wifi 802.11n, Bluetooth 4.1
- Una fuente de alimentación de 5 V vía Micro USB o GPIO header
- Un consumo energético de 800 mA, (4.0 W)
- Lector de tarjetas SD
- Soporta los sistemas operativos
  GNU/Linux: Debian (Raspbian), Fedora (Pidora), Arch Linux (Arch Linux ARM), Slackware Linux, SUSE Linux Enterprise Server for ARM [3][4]

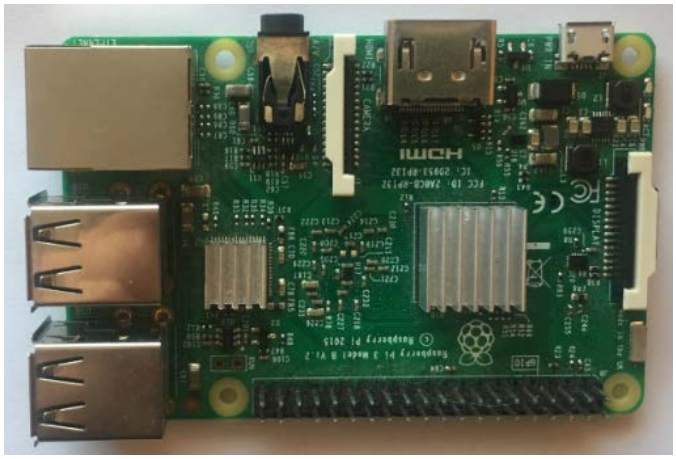


Figura 2.1. Modelo Raspberry Pi 3

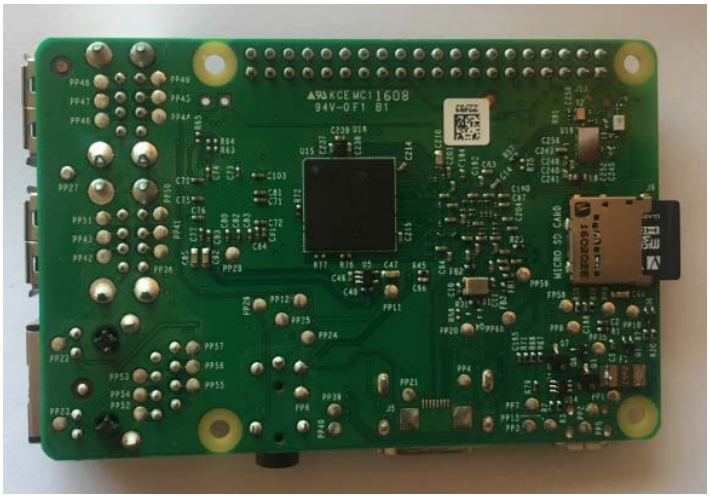


Figura 2.2. Modelo Raspberry Pi 3 (1)

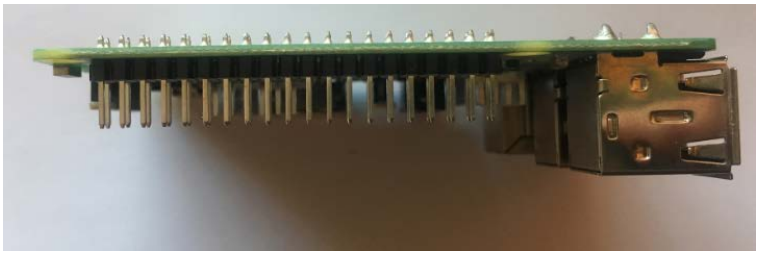


Figura 2.3. Modelo Raspberry Pi 3 (2)

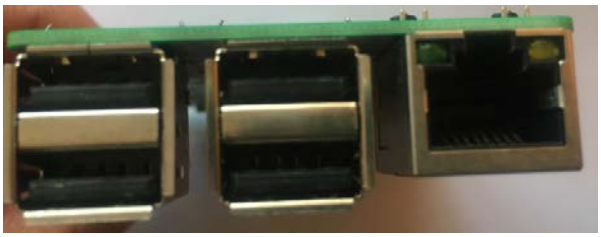


Figura 2.4. Modelo Raspberry Pi 3 (3)

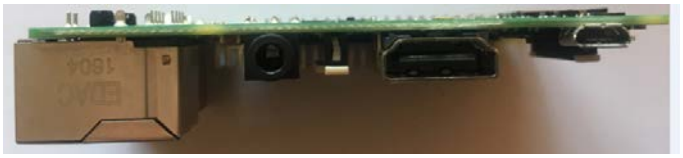


Figura 2.5. Modelo Raspberry Pi 3 (4)

Figura 2.6. Modelo Raspberry Pi 3 (5)

Figura 2.7. Modelo Raspberry Pi 3 (6)

3. DESARROLLO SOBRE KALI LINUX

3.1 INTRODUCCIÓN

Kali Linux se lanzó el 13 de marzo de 2013 como una reconstrucción completa e integral de BackTrack Linux, respetando completamente los estándares de desarrollo de Debian. [5]

El sistema operativo Kali Linux, es una distribución Linux que te permite obtener las herramientas necesarias para poder auditar sistemas y asegurar que nuestros equipos informáticos puedan acceder a Internet sin ningún riesgo de sufrir un ataque de hackeo. [6]

Su principal objetivo es poner a disposición del usuario, las mejores herramientas para trabajar la auditoría en internet y contar con un potente sistema de seguridad informática ante los peligros que puedan existir. [6]

Se incluyeron más de 600 herramientas de prueba de penetración: después de revisar todas las herramientas que se incluyeron en BackTrack, eliminaron una gran cantidad de herramientas que simplemente no funcionaban o que duplicaban otras herramientas que proporcionaban la misma o similar funcionalidad. Los detalles sobre lo que se incluye están en el sitio de Kali Tools. Este sistema es gratuito. [5]

Árbol de Git de código abierto: Esta comprometido con el modelo de desarrollo de código abierto y el árbol de desarrollo está disponible para que todos lo vean. Todo el código fuente que se incluye en Kali Linux está disponible para cualquier persona que quiera modificar o reconstruir paquetes para satisfacer sus necesidades específicas. [5]

Compatible con FHS: Kali se adhiere al estándar de jerarquía del sistema de archivos, lo que permite a los usuarios de Linux localizar fácilmente archivos binarios, archivos de soporte, bibliotecas, etc. [5]

Amplia compatibilidad con dispositivos inalámbricos: se admite un punto de bloqueo regular con las distribuciones de Linux para las interfaces inalámbricas. Se ha construido Kali Linux para que sea compatible con la mayor cantidad de dispositivos inalámbricos

que se pueda, lo que permite que se ejecute correctamente en una amplia variedad de hardware y que sea compatible con numerosos dispositivos USB y otros dispositivos inalámbricos. [5]

Kernel personalizado, parcheado para inyección: como evaluadores de penetración, el equipo de desarrollo a menudo necesita hacer evaluaciones inalámbricas, por lo que kernel tiene los últimos parches de inyección incluidos. [5]

Desarrollado en un entorno seguro: el equipo de Kali Linux está formado por un pequeño grupo de personas que son las únicas en las que se confía para enviar paquetes e interactuar con los repositorios, todo lo cual se realiza mediante múltiples protocolos seguros. [5]

Paquetes y repositorios firmados por GPG: Cada paquete en Kali Linux está firmado por cada desarrollador individual que lo construyó y confirmó, y los repositorios también firman los paquetes. [5]

Soporte en múltiples idiomas: aunque las herramientas de penetración tienden a estar escritas en inglés, se asegura que Kali incluya un verdadero soporte multilingüe, lo que permite que más usuarios operen en su idioma nativo y localicen las herramientas que necesitan para el trabajo. [5]

Soporte ARMEL y ARMHF: dado que los sistemas de placa única basados en ARM como Raspberry Pi y BeagleBone Black, entre otros, son cada vez más frecuentes y económicos, sabiendo que el soporte ARM de Kali tendría que ser tan sólido como se pudiera manejar, con instalaciones totalmente operativas para los sistemas ARMEL y ARMHF. Kali Linux está disponible en una amplia gama de dispositivos ARM y tiene repositorios ARM integrados con la distribución de línea principal, por lo que las herramientas para ARM se actualizan junto con el resto de la distribución. [5]

Kali Linux está específicamente diseñado para las necesidades de los profesionales de pruebas de penetración y, por lo tanto, toda la documentación en el sitio asume el conocimiento previo y la familiaridad con el sistema operativo Linux en general. [5]

3.1.1 INSTALACIÓN DE KALI LINUX EN LA RASPBERRY PI

Este sistema se ha instalado mediante el programa Etcher, una herramienta gráfica de escritura de tarjetas SD que funciona en Mac OS, Linux y Windows. Para ello se ha descargado la imagen de Linux, en la página oficial, y se ha instalado mediante esta herramienta.

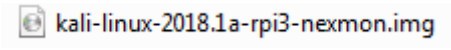


Figura 3.1. Archivo Kali-Linux

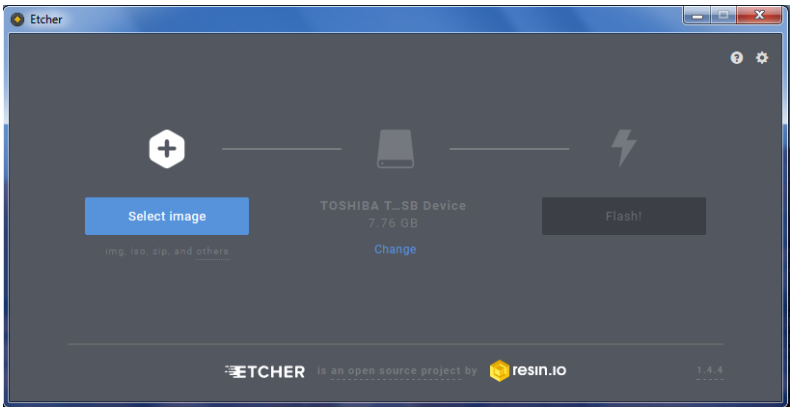


Figura 3.2. Programa Etcher

Una vez se haya instalado la imagen en la Raspberry se puede proceder a ejecutarla.

Conectada a una salida se puede ver un sistema operativo, parecido a Windows.

Figura 3.3. Ejecución Kali-Linux en Raspberry

Kali Linux manda meter un usuario, root, y contraseña, toor.

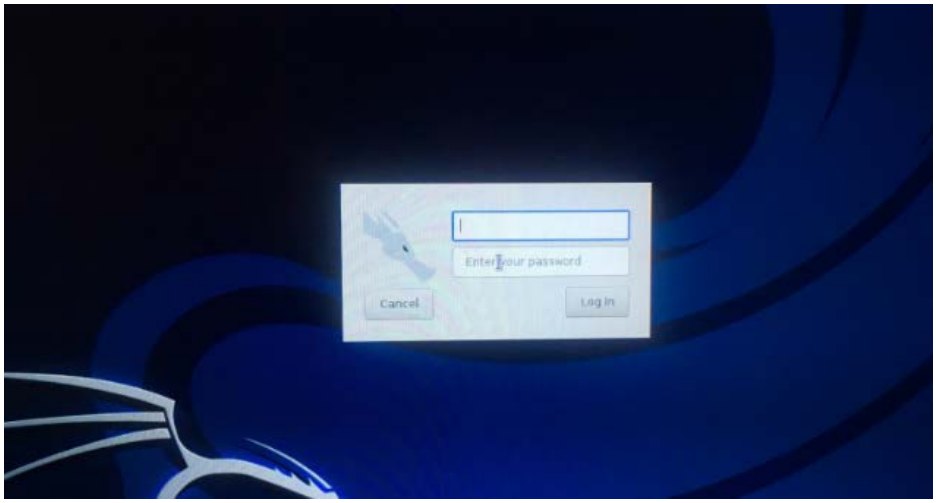


Figura 3.4. Registro de usuario en Kali-Linux

Figura 3.5. Visualización del monitor

3.2 WIFITE

Sirve para el ataque de redes encriptadas. Con ella se consigue hackear el wifi, con lo que se extrae su clave. Esta herramienta es personalizable para ser automatizada con solo unos pocos argumentos. Pretende ser una herramienta de auditoría inalámbrica.

3.2.1 CARACTERISTICAS

- Ordena objetivos por potencia de señal (en dB), primero crackea los puntos de acceso más cercanos.
- Automáticamente de-autentica clientes de redes ocultas para mostrar el Ssid.
- Numerosos filtros para especificar exactamente que atacar (Wep/Wpa o ambos sobre potencia de señal, canales, etc).
- Configuraciones parametrizables (timeouts, paquetes/sec, etc).
- Característica “anónima”, cambia la dirección Mac aleatoriamente antes de realizar un ataque.
- Todos los handshakes Wpa capturados son resguardados en el directorio “wifite.py”.
- De-autenticación inteligente sobre Wpa, a un cliente o toda una red.
- Detiene cualquier ataque con “Ctrl+” con opción de continuar al siguiente objeto, omitir el crackeo o salir de la ejecución.
- Muestra un resumen de la sesión al salir, informa contraseñas obtenidas.
- Todas las contraseñas son almacenadas a “cracked.txt” [7]

Está ataca múltiples redes encriptadas (Wep / Wpa / Wpa2/Wps).

3.2.2 WIFI

Tecnologías de comunicación inalámbrica mediante ondas, también llamada WLAN o estándar IEEE 802.11. WI-FI no es una abreviatura de Wireless Fidelity, simplemente es un nombre comercial. [8]

En abril de 2000 se establece la primera norma: WiFi 802.11b, que utilizaba la banda de los 2.4 Ghz y que alcanzaba una velocidad de 11 Mbps. Tras esta especificación llegó 802.11a, que generó algunos problemas entre Estados Unidos y Europa por la banda que se utilizaba. Mientras que en Estados Unidos la banda de los 5 GHz estaba libre, en Europa estaba reservada a fines militares, situación que paralizó un tanto esta tecnología inalámbrica, sobre todo teniendo en cuenta que la mayoría de los fabricantes de dispositivos, norteamericanos en su mayor parte, tardaron en reaccionar ante la imposibilidad de vender sus productos en el viejo continente. [8]

Tras muchos debates se aprobó una nueva especificación, 802.11g, que al igual que la "b" utilizaba la banda de los 2,4 GHz, pero multiplicaba la velocidad hasta los 54 Mbps. Llegado el momento en que tres especificaciones diferentes conviven en el mercado, se da el caso de que son incompatibles, por lo que el siguiente paso fue crear equipos capaces de trabajar con las tres, saltando “en caliente” de unas a otras, y lanzado soluciones que se etiquetaban como “multipunto”. Cuando se da este caso la banda de los 5 GHz, anteriormente reservada para usos militares, se habilitó para usos civiles, lo que fue un gran adelanto no sólo porque es ese momento ofrecía la mayor velocidad, sino porque no existían otras Tecnologías inalámbricas, como Bluetooth, Wireless USB o ZigBee que utilicen la misma frecuencia. [8]

Se pueden encontrar con dos tipos de comunicación WI-FI: 802.11b, que emite a 11 Mb/seg, y 802.11 g, más rápida, a 54 MB/seg. Su velocidad y alcance (100-150 metros en hardware asequible) lo convierten en una fórmula perfecta para el acceso a Internet sin cables. Una de las curiosidades de la especificación 802.11n es que los productos han llegado al mercado antes de aprobarse el estándar, denominándose Draft-N, lo que hace referencia a que están sujetos al borrador y no al estándar definitivo. [8]

Cuando se trata de Conexiones inalámbricas, no es difícil que cualquier persona intercepte la comunicación y tenga acceso a nuestro flujo de información. Por esto, es recomendable la encriptación de transmisión para emitir en entorno seguro. Esto es posible gracias al WPA, mucho más seguro que su predecesor WEP y con nuevas características de seguridad, como la generación dinámica de la clave de acceso. Para usuarios más avanzados existe la posibilidad de configurar el punto de acceso para que

emita sólo a ciertos dispositivos. Usando la dirección MAC, un identificador único de los dispositivos asignados durante su construcción, y permitiendo el acceso solamente a dispositivos instalados. [8]

Un muy elevado porcentaje de redes son instalados sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o completamente vulnerables a los crackers), sin proteger la información que por ellas circulan. [8]

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes: [8]

- WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire. Este tipo de cifrado no está muy recomendado, debido a las grandes vulnerabilidades que presenta, ya que cualquier cracker puede conseguir sacar la clave. [8]

- WPA: Presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud. [8]

- IPSEC (túneles IP): En el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios. [8]

- Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos. [8]

- Ocultación del punto de acceso: Se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios. [8]

- El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en

este momento. Sin embargo, requieren hardware y software compatibles, ya que los antiguos no lo son. [8]

No existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas. [8]

3.2.3 WEP

Fue el primer estándar de seguridad para redes Wi-Fi. El sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada, es el acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. [9]

WEP es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas. En ningún caso es compatible con IPSec. [9]

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida. El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado. [9]

Como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos. Hacia 2003, la Wi-Fi Alliance anunció que WEP había sido reemplazado por WPA. A pesar de sus debilidades, WEP sigue siendo utilizado, ya que es a menudo la primera opción de seguridad que se presenta a los usuarios por las herramientas de configuración de los routers aun cuando sólo

proporciona un nivel de seguridad que puede disuadir del uso sin autorización de una red privada, pero sin proporcionar verdadera protección. [9]

3.2.4 WPA

Abreviatura de Wifi Protect Access, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN. [10]

Es el sistema más simple de control de acceso tras WEP, a efectos prácticos tiene la misma dificultad de configuración que WEP, una clave común compartida, sin embargo, la gestión dinámica de claves aumenta notoriamente su nivel de seguridad. PSK se corresponde con las iniciales de PreShared Key y viene a significar clave compartida previamente, es decir, a efectos del cliente basa su seguridad en una contraseña compartida. WPA-PSK usa una clave de acceso de una longitud entre 8 y 63 caracteres, que es la clave compartida. Al igual que ocurría con WEP, esta clave hay que introducirla en cada una de las estaciones y puntos de acceso de la red inalámbrica. Cualquier estación que se identifique con esta contraseña, tiene acceso a la red. Las características de WPA-PSK lo definen como el sistema, actualmente, más adecuado para redes de pequeñas oficinas o domésticas, la configuración es muy simple, la seguridad es aceptable y no necesita ningún componente adicional. Utiliza TKIP para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. [10]

La principal debilidad de WPA-PSK es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en una contraseña siempre es susceptible de sufrir un ataque de fuerza bruta, es decir ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería plantear mayores problemas. [10]

3.2.5 WPA2

Una vez finalizado el nuevo estándar 802.11ie se crea el WPA2 basado en este. WPA se podría considerar de migración, mientras que WPA2 es la versión certificada del estándar de la IEEE.5 6. El estándar 802.11i fue ratificado en junio de 2004. [11]

La Wi-Fi Alliance llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise. Los fabricantes comenzaron a producir la nueva generación de puntos de acceso apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES. Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 les dan a los gerentes de TI la seguridad de que la tecnología cumple con estándares de interoperatividad" declaró Frank Hazlik Managing director de la Wi-Fi Alliance. [11]

WPA2 incluye el nuevo algoritmo de cifrado AES desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2. [11]

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP en lugar de los códigos MIC. Otra mejora respecto a WPA es que WPA2 incluye soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc). [10]

Tanto la versión 1 de WPA, como la denominada versión 2, se basan en la transmisión de las autenticaciones soportadas en el elemento de información correspondiente. En el caso caso de WPA2 en el tag estándar 802.11i RSN. Durante el intercambio de información en el proceso de conexión RSN, si el cliente no soporta las autenticaciones que especifica el AP (punto de acceso), será desconectado pudiendo sufrir de esta manera un ataque dos específico a WPA. [11]

Además, también existe la posibilidad de capturar el 4-way handshake que se intercambia durante el proceso de autenticación en una red con seguridad robusta. Las

claves PSK (precompartidas) son vulnerables a ataques de diccionario (no así las empresariales, ya que el servidor RADIUS generará de manera aleatoria dichas claves), existen proyectos libres que utilizan GPU con lenguajes específicos como CUDA (NVIDIA) y Stream (AMD) para realizar ataques de fuerza bruta hasta cien veces más rápido que con computadoras ordinarias. [11]

Tanto la especificación WPA como IEEE 802.11i solucionan todos los fallos conocidos de WEP y, en estos momentos, se consideran soluciones fiables. La ventaja de WPA es que no requiere de actualizaciones de hardware en los equipos. Mientras no se descubran problemas de seguridad en WPA, esta implementación puede ser suficiente en los dispositivos para los próximos meses. La apuesta de seguridad del IEEE para sustituir al desafortunado WEP, 802.11i y al WPA es el nuevo Wi-Fi Protected Access 2 (WPA2). [11]

3.2.5 WPS

WPS es un estándar de 2007, promovido por la Wi-Fi Alliance para facilitar la creación de redes WLAN. [13] Es un método para establecer una conexión entre un dispositivo inalámbrico y el router inalámbrico. Permite conectar rápidamente un dispositivo (móvil, computadora con tarjeta de red inalámbrica, tableta, etc.) a la red inalámbrica del router. [12] En otras palabras, WPS no es un mecanismo de seguridad de por sí, se trata de la definición de diversos mecanismos para facilitar la configuración de una red WLAN segura con WPA2, pensados para minimizar la intervención del usuario en entornos domésticos o pequeñas oficinas. Concretamente, WPS define los mecanismos a través de los cuales los diferentes dispositivos de la red obtienen las credenciales (SSID y PSK) necesarias para iniciar el proceso de autenticación. [13]

WPS define una arquitectura con tres elementos con roles diferentes:

- Registrar (matriculador): dispositivo con la autoridad de generar o revocar las credenciales en la red. Tanto un AP como cualquier otra estación o PC de la red pueden tener este rol. Puede haber más de un registra*r* en una red. [13]
- Enrollee (matriculado): dispositivo que solicita el acceso a la red WLAN. [13]

- Authenticator (autenticador): AP funcionando de proxy entre el registrar y el enrollee. [13]

WPS contempla cuatro tipos de configuraciones diferentes para el intercambio de credenciales, PIN, PBC, NFC y USB:

- PIN: tiene que existir un PIN asignado a cada elemento que vaya a asociarse a la red. Este PIN tiene que ser conocido tanto por el *Registrar*, como por el usuario. Es necesaria la existencia de una interfaz, pantalla y teclado, para que el usuario pueda introducir el mencionado PIN. [13]
- PBC: la generación y el intercambio de credenciales son desencadenados a partir que el usuario presiona un botón (físico o virtual) en el AP (o en otro elemento *Registrar*) y otro en el dispositivo. Notar que en el corto lapso de tiempo entre que se presiona el botón en el AP y se presiona en el dispositivo, cualquier otra estación próxima puede ganar acceso a la red. [13]
- NFC: intercambio de credenciales a través de comunicación NFC. La tecnología NFC, basada en RFID permite la comunicación sin hilos entre dispositivos próximos (0 - 20 cm). Entonces, el dispositivo enrollee se tiene que situar al lado del *Registrar* para desencadenar la autenticación. De esta manera, cualquier usuario que tenga acceso físico al *Registrar*, puede obtener credenciales válidas. [13]
- USB: con este método, las credenciales se transfieren mediante un dispositivo de memoria flash, como pendrive, desde el *Registrar* al enrollee. [13]

Los métodos PBC, NFC y USB pueden usarse para configurar dispositivos sin pantalla ni teclado, como impresoras, pero aunque el estándar contempla NFC y USB, todavía no se certifican estos mecanismos. Actualmente sólo el método PIN es obligatorio en todas las estaciones para obtener la certificación WPS; PBC es obligatorio sólo en APs. [13]

WPS sólo trabaja con seguridad WPA o WPA2, no soporta dispositivos viejos con WEP. [12]

Existe un fallo de seguridad que Stefan Viehböck descubrió en diciembre del 2011. Afecta a routers inalámbricos que tienen la función WPS (también llamada QSS), que en

dispositivos actuales se encuentra habilitada en forma preestablecida. Como todos los dispositivos WPS tienen un pin de 8 dígitos único, el fallo permite a un atacante recuperar el PIN WPS y, con él, la clave pre-compartida de la red WPA/WPA2 usando ataques de fuerza bruta en pocas horas. [13]

3.2.7 INSTALACIÓN

Se abre un terminal y programa para ponerlo en modo monitor primero, para utilizar la herramienta wifite, si no, no se habría podido ejecutar el comando.

Se ha utilizado para ello el siguiente código:

Iwconfig: Identifica los dispositivos inalámbricos que están en modo monitor.

Monstart

Iwconfig

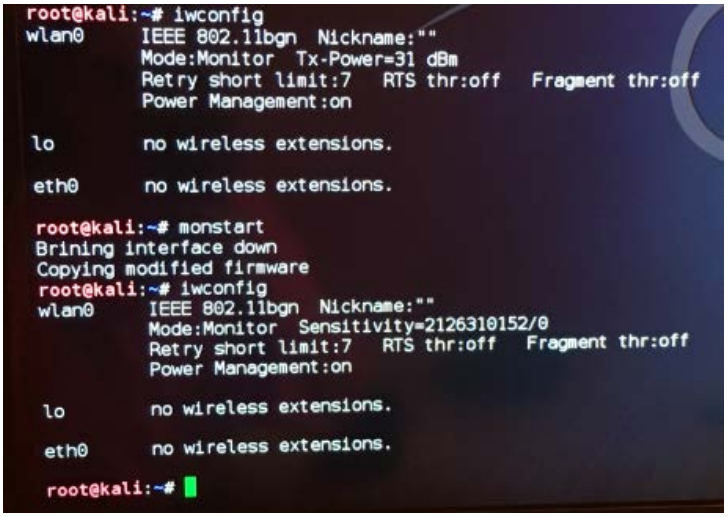


Figura 3.6. Modo monitor

Una vez que se haya conseguido estar en este modo, se ejecuta el wifite ya que, si no se pone en este modo, no se puede ejecutar.

Wifite

3.2.8 RESULTADOS

Figura 3.7. Ejecución Wifite

Una vez muestre las redes que tenemos cerca, se pulsa “CTRL+C” para que deje de capturar redes y se pueda seleccionar la red a la que se quiere atacar con el fin de poder sacar la clave.

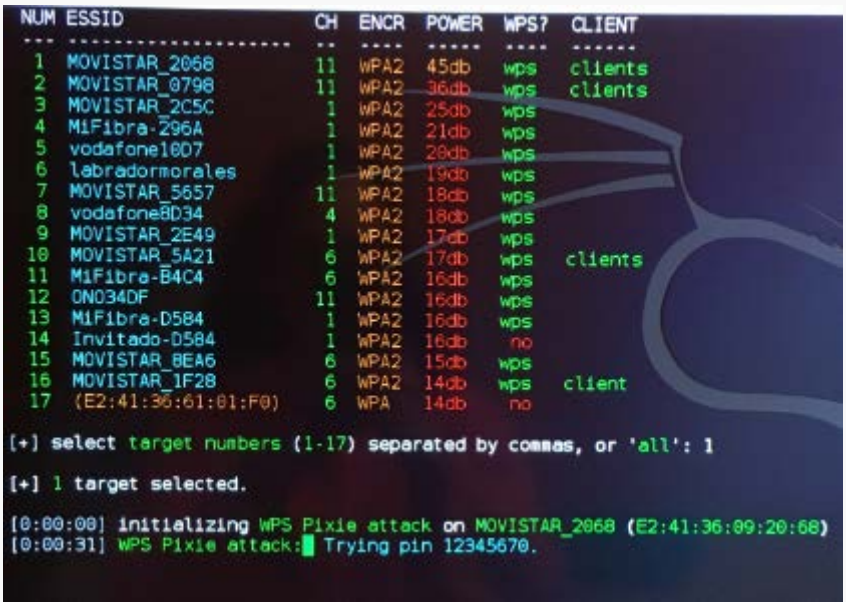


Figura 3.8. Captura de redes disponibles

Se solicita el número del wifi el cual se quiere atacar, en mi caso el 1, y comienza a realizar el ataque.

Figura 3.9. Inicio del ataque

Se puede comprobar que no deja hackear este tipo de redes, ya que la seguridad es mayor.

3.2.8 INSTALACIÓN DE ROUTERSPLOIT EN UBUNTU

Debido al problema que nos encontramos en la Raspberry, el cual no ha sido capaz de poder descargarse programas en él, se ha optado por utilizar Ubuntu, otro sistema operativo donde se han realizado las otras pruebas.

4. DESARROLLO SOBRE UBUNTU

4.1 INTRODUCCIÓN

Ubuntu es una distribución Linux que ofrece un sistema operativo predominantemente enfocado a ordenadores de escritorio, aunque también proporciona soporte para servidores. [14]

Basada en Debian GNU/Linux, esté concentra su objetivo en la facilidad de uso, la libertad en la restricción de uso, los lanzamientos regulares y la facilidad en la instalación. Ubuntu es patrocinado por Canonical Ltd., una empresa privada fundada y financiada por el empresario sudafricano Mark Shuttleworth. [14]

4.1 HISTORIA

El nombre de la distribución proviene del concepto zulú y xhosa de ubuntu, que significa "humanidad hacia otros" o "yo soy porque nosotros somos". Ubuntu es un movimiento sudafricano encabezado por el obispo Desmond Tutu, quien ganó el Premio Nobel de la Paz en 1984 por sus luchas en contra del *Apartheid* en Sudáfrica. El sudafricano Mark Shuttleworth, mecenas del proyecto, se encontraba muy familiarizado con la corriente. Tras ver similitudes entre los ideales de los proyectos GNU, Debian y en general con el movimiento del software libre, decidió aprovechar la ocasión para difundir los ideales de *Ubuntu*. El eslogan de Ubuntu – "Linux para seres humanos" (en inglés "Linux for Human Beings") resume una de sus metas principales: hacer de Linux un sistema operativo más accesible y fácil de usar. [14]

Mark Shuttleworth de la Fundación Ubuntu en la WSIS 2005 de Túnez. [14]

El 8 de julio de 2004, Mark Shuttleworth y la empresa Canonical Ltd. anunciaron la creación de la distribución Ubuntu. Ésta tuvo una financiación inicial de 10 millones de dólares (US$). El proyecto nació por iniciativa de algunos programadores de los proyectos Debian, Gnome porque se encontraban decepcionados con la manera de

operar del proyecto Debian, la distribución Linux sin ánimo de lucro más popular del mundo. [14]

De acuerdo con sus fundadores, Debian era un proyecto demasiado burocrático donde no existían responsabilidades definidas y donde cualquier propuesta interesante se ahogaba en un mar de discusiones. Asimismo, Debian no ponía énfasis en estabilizar el desarrollo de sus versiones de prueba y sólo proporcionaba auditorías de seguridad a su versión estable, la cual era utilizada sólo por una minoría debido a la poca o nula vigencia que poseía en términos de la tecnología Linux actual. [14]

Tras formar un grupo multidisciplinario, los programadores decidieron buscar el apoyo económico de Mark Shuttleworth, un emprendedor sudafricano que vendió la empresa Thawte a VeriSign, cuatro años después de fundarla en el garaje de su domicilio, por 575 millones de dólares estadounidenses. [14]

Shuttleworth vio con simpatía el proyecto y decidió convertirlo en una iniciativa autosostenible, combinando su experiencia en la creación de nuevas empresas con el talento y la experiencia de los programadores de la plataforma Linux. De esta forma nació la empresa Canonical, la cual se encarga de sostener económicamente el proyecto mediante la comercialización de servicios y soporte técnico a otras empresas. Mientras los programadores armaban el sistema, Shuttleworth aprovechó la ocasión para aplicar una pequeña campaña de mercadotecnia para despertar interés en la *distribución sin nombre* (en inglés: the no-name-distro). [14]

Tras varios meses de trabajo y un breve período de pruebas, la primera versión de Ubuntu (Warty Warthog) fue lanzada el 20 de octubre de 2004. [14]

4.3 CARACTERISTICAS

Basada en la distribución Debian. [14]

-Disponible en 4 arquitecturas: Intel x86, AMD64, SPARC (para esta última sólo existe la versión servidor). [14]

-Los desarrolladores de Ubuntu se basan en gran medida en el trabajo de las comunidades de Debian y GNOME, siendo este último el entorno de escritorio oficial. [14]

-Las versiones estables se liberan cada 6 meses y se mantienen actualizadas en materia de seguridad hasta 18 meses después de su lanzamiento. [14]

-La nomenclatura de las versiones no obedece principalmente a un orden de desarrollo, se compone del dígito del año de emisión y del mes en que esto ocurre. La versión 4.10 es de octubre de 2004, la 5.04 es de abril de 2005, la 5.10 de octubre de 2005, la 6.06 es de junio de 2006, la 6.10 es de octubre de 2006 y la 7.04 es de abril de 2007. [14]

-Para centrarse en solucionar rápidamente los bugs, conflictos de paquetes, etc. se decidió eliminar ciertos paquetes del componente main, ya que no son populares o simplemente se escogieron de forma arbitraria por gusto o sus bases de apoyo al software libre. Por tales motivos inicialmente KDE no se encontraba con más soporte de lo que entregaban los mantenedores de Debian en sus repositorios, razón por la que se sumó la comunidad de KDE distribuyendo la distro llamada Kubuntu. [14]

-De forma sincronizada a la versión 6.06 de Ubuntu, apareció por primera vez la distribución Xubuntu, basada en el entorno de escritorio XFce. [14]

-El sistema incluye funciones avanzadas de seguridad y entre sus políticas se encuentra el no activar, de forma predeterminada, procesos latentes al momento de instalarse. Por eso mismo, no hay un firewall predeterminado, ya que no existen servicios que puedan atentar a la seguridad del sistema. [14]

-Para labores/tareas administrativas en terminal incluye una herramienta llamada sudo (similar al Mac OS X), con la que se evita el uso del usuario root (administrador). [14]

-Mejora la accesibilidad y la internacionalización, de modo que el software está disponible para tanta gente como sea posible. En la versión 5.04, el UTF-8 es la codificación de caracteres en forma predeterminada. [14]

-No sólo se relaciona con Debian por el uso del mismo formato de paquetes deb, también tiene uniones muy fuertes con esa comunidad, contribuyendo con cualquier cambio directa e inmediatamente, y no solo anunciándolos. Esto sucede en los tiempos de lanzamiento. Muchos de los desarrolladores de Ubuntu son también responsables de los paquetes importantes dentro de la distribución de Debian. [14]

-Todos los lanzamientos de Ubuntu se proporcionan sin coste alguno. Los CDs de la distribución se envían de forma gratuita a cualquier persona que los solicite mediante el servicio ShipIt (la versión 6.10 no se llegó a distribuir de forma gratuita en CD, pero la versión 7.04 sí). También es posible descargar las imágenes ISO de los discos por transferencia directa o bajo la tecnología Bittorrent. [14]

4.4 ORGANIZACIÓN DE PAQUETES

Ubuntu divide todo el software en cuatro secciones, llamadas componentes**,** para mostrar diferencias en licencias y la prioridad con la que se atienden los problemas que informen los usuarios. Estos componentes son: main, restricted, universe y multiverse. [14]

Por defecto, se instala una selección de paquetes que cubre las necesidades básicas de la mayoría de los usuarios de computadoras. Los paquetes de Ubuntu generalmente se basan en los paquetes de la rama inestable (*Sid*) de Debian. [14]

-Componente main

El componente main contiene solamente los paquetes que cumplen los requisitos de la licencia de Ubuntu, y para los que hay soporte disponible por parte de su equipo. Éste está pensado para que incluya todo lo necesario para la mayoría de los sistemas Linux

de uso general. Los paquetes de este componente poseen ayuda técnica garantizada y mejoras de seguridad oportunas. [14]

-Componente restricted

El componente restricted contiene el programa soportado por los desarrolladores de Ubuntu debido a su importancia, pero que no está disponible bajo ningún tipo de licencia libre para incluir en main. En este lugar se incluyen los paquetes tales como los controladores propietarios de algunas tarjetas gráficas, como, por ejemplo, los de nVIDIA. El nivel de la ayuda es más limitado que para main, puesto que los desarrolladores puede que no tengan acceso al código fuente. [14]

-Componente universe

El componente universe contiene una amplia gama del programa, que puede o no tener una licencia restringida, pero que no recibe apoyo por parte del equipo de Ubuntu. Esto permite que los usuarios instalen toda clase de programas en el sistema guardándolos en un lugar aparte de los paquetes soportados: main y restricted. [14]

-Componente comercial

Como lo indica su clasificación, contiene programas comerciales. [14]

-Componente multiverse

Finalmente, se encuentra el componente multiverse, que contiene los paquetes sin soporte debido a que no cumplen los requisitos de Software Libre. [14]

4.5 LANZAMIENTOS

Cada lanzamiento de Ubuntu posee un nombre en clave, como también un número de versión basado en el año y el mes del lanzamiento. Por ejemplo, la versión *5.04* fue lanzada en abril de 2005. Cada versión de Ubuntu es lanzada con seis meses de diferencia con respecto al último lanzamiento, aunque el lanzamiento de la versión 6.06 se demoró más de seis meses, debido a que Canonical Ltd. quería desarrollar una

distribución a la que fuera posible dar ayuda técnica durante tres años en el escritorio y cinco años en el servidor. [14]

Canonical provee ayuda técnica y actualizaciones de la seguridad para la mayoría de las versiones de Ubuntu durante 18 meses, a partir de la fecha del lanzamiento. Actualmente existen tres versiones de Ubuntu que cuentan con soporte técnico: la versión 6.06 LTS, la versión 6.10 y la versión 7.04. [14]

4.6 VARIANTES

Existen diversas variantes de Ubuntu disponibles, las cuales poseen lanzamientos simultáneos con Ubuntu. Las más significativas son: [14]

-Kubuntu, el cual utiliza KDE en vez de GNOME. [14]

-Edubuntu, diseñado para entornos escolares. [14]

-Xubuntu, el cual utiliza el entorno de escritorio Xfce. [14]

Kubuntu, Edubuntu y Xubuntu son proyectos oficiales de la Ubuntu Foundation. Kubuntu y Edubuntu se encuentran incluidos dentro del programa ShipIt. [14]

Mark Shuttleworth también ha apoyado la creación de una distribución derivada de Ubuntu que utilizaría sólo software aprobado por la Free Software Foundation. Hasta ahora no ha sido lanzada ninguna versión oficial de 'Ubuntu-Libre', debido a dificultades en la gestión de paquetes de software. gNewSense, un proyecto algo similar al propuesto 'Ubuntu-Libre', fue lanzado el 2 de noviembre de 2006. Sin embargo, no es una versión oficial de Ubuntu. [14]

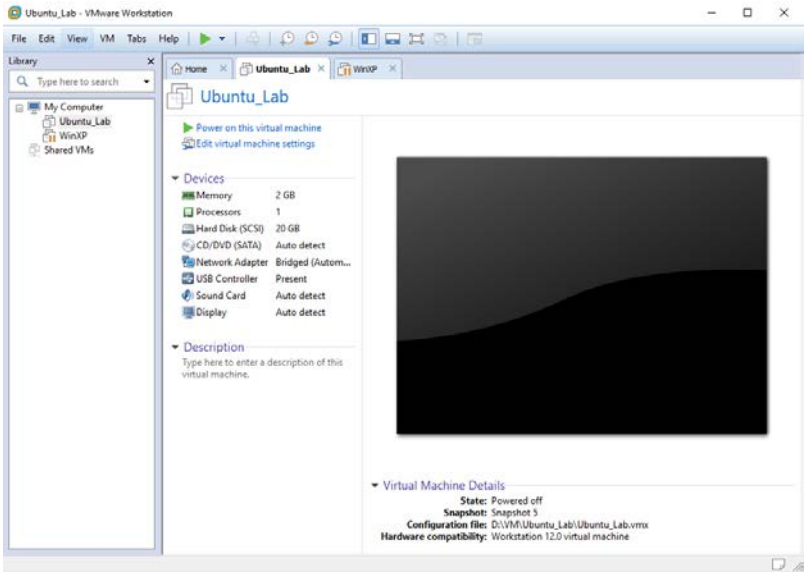


Figura 4.1. Ejecución Ubuntu

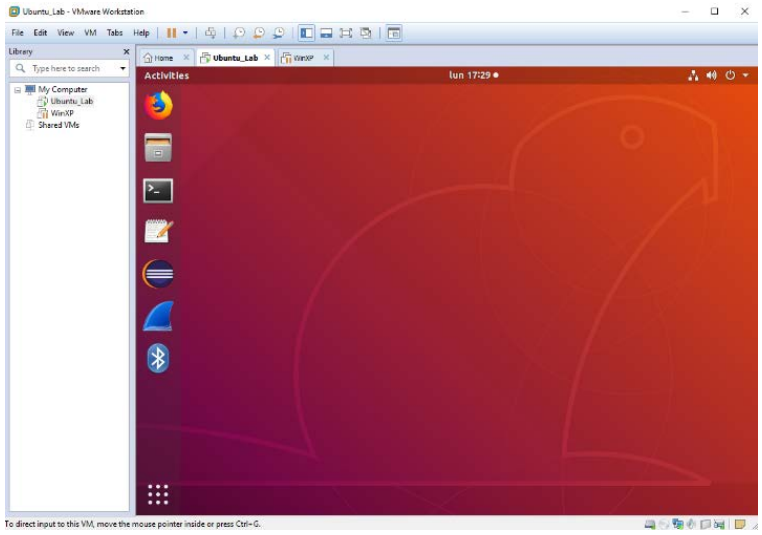


Figura 4.2. Visualización del monitor

4.7 ROUTERSPLOIT

Routersploit es un framework que permite explotar vulnerabilidades en dispositivos como routers, puntos de acceso, NAS y otros dispositivos embebidos. Este framework es de código libre, y no se paga por él.

Esté nos recuerda mucho al conocido Metasploit, el framework para explotar una gran cantidad de vulnerabilidades en sistemas operativos. RouterSploit se centra principalmente en tres módulos: [15]

-Exploits: Es el módulo encargado de explotar las vulnerabilidades encontradas en un dispositivo, como por ejemplo un router. [15]

-Creds: Es un módulo diseñado específicamente para probar credenciales por defecto de un router, e intentar entrar directamente en su administración. [15]

-Scanners: Es un módulo diseño para buscar y encontrar objetivos vulnerables, al reconocer un objetivo, nos mostrará si es vulnerable a algún exploit que tengamos en el módulo de Exploits. [15]

También se puede hablar de dos módulos más.

- payloads: módulos para generar cargas útiles en diversas arquitecturas. [16]

-generic: módulos que realizan ataques genéricos. [16]

4.7.1 INSTALACIÓN DE ROUTERSPLOIT EN UBUNTU

Para su instalación, se ha utilizado el siguiente código:

sudo add-apt-repository universe

sudo apt-get install git python3-pip

git clone https://www.github.com/threat9/routersploit
cd routersploit
python3 –m pip install –r requirement.txt
python3 rsf.py

Lanzado RouterSploit, se realiza una prueba para mostrar alguna vulnearabilidad sobre nuestro router.

Se selecciona el módulo scanner con autopwn (lanza contra el objetivo todos los exploits)

use scanner/autopwn

Se marca el target poniendo la IP del ordenador

Set target (IP del dispositivo)

Se lanza el ataque

Run [17]

4.7.2 RESULTADOS

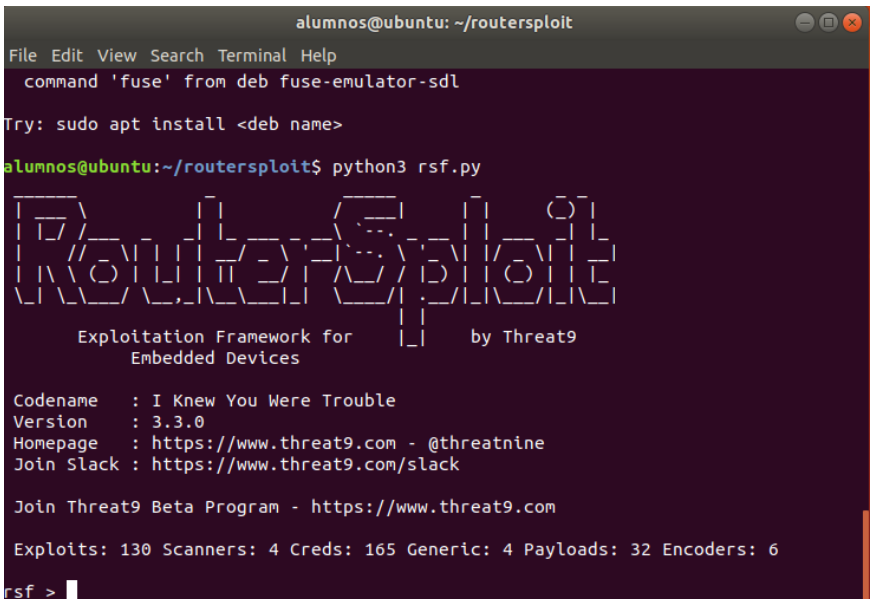


Figura 4.3. Ejecución RouterSploit

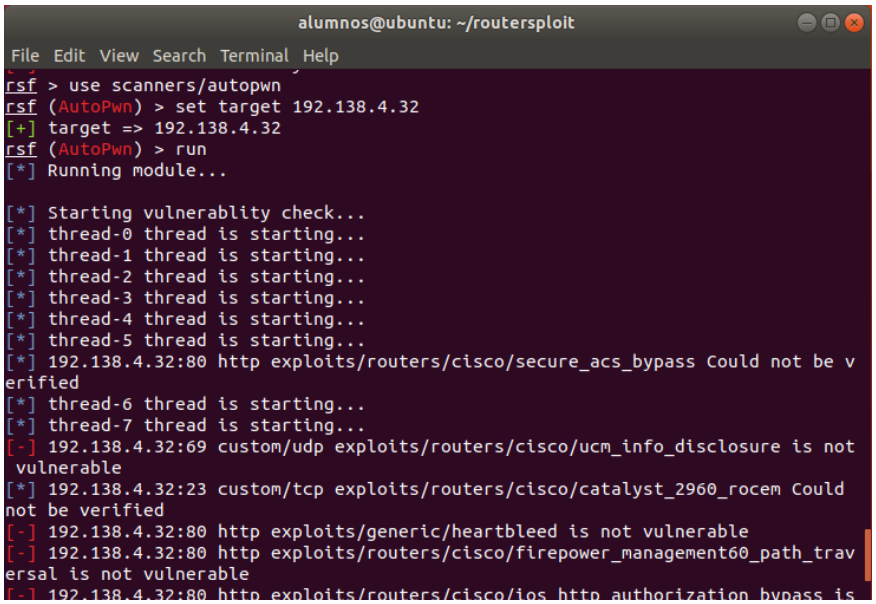


Figura 4.4. Realización de prueba de vulnerabilidad

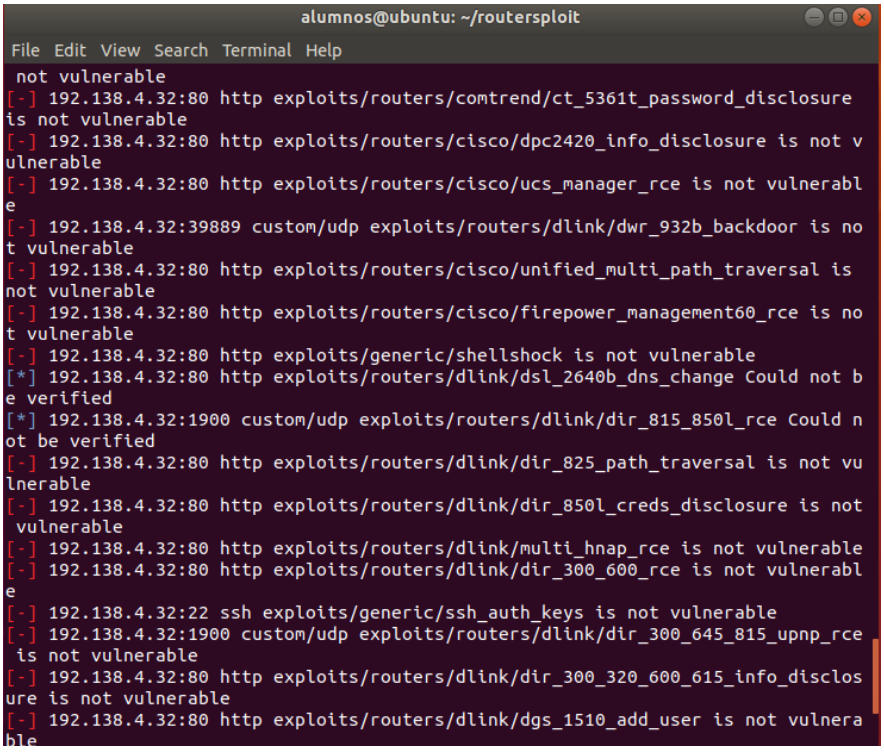


Figura 4.5. Realización de prueba de vulnerabilidad (1)

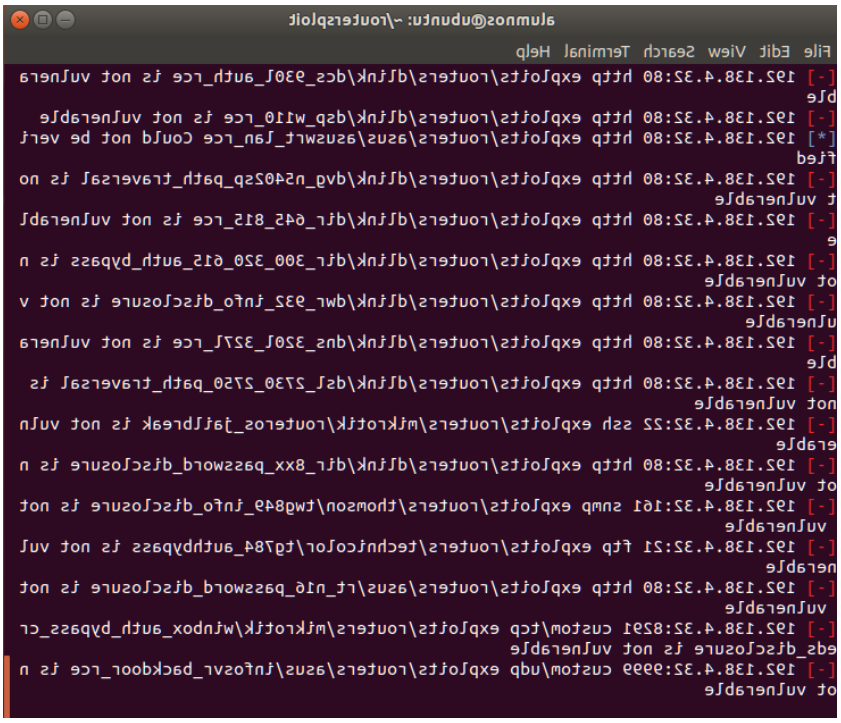


Figura 4.6. Realización de prueba de vulnerabilidad (2)

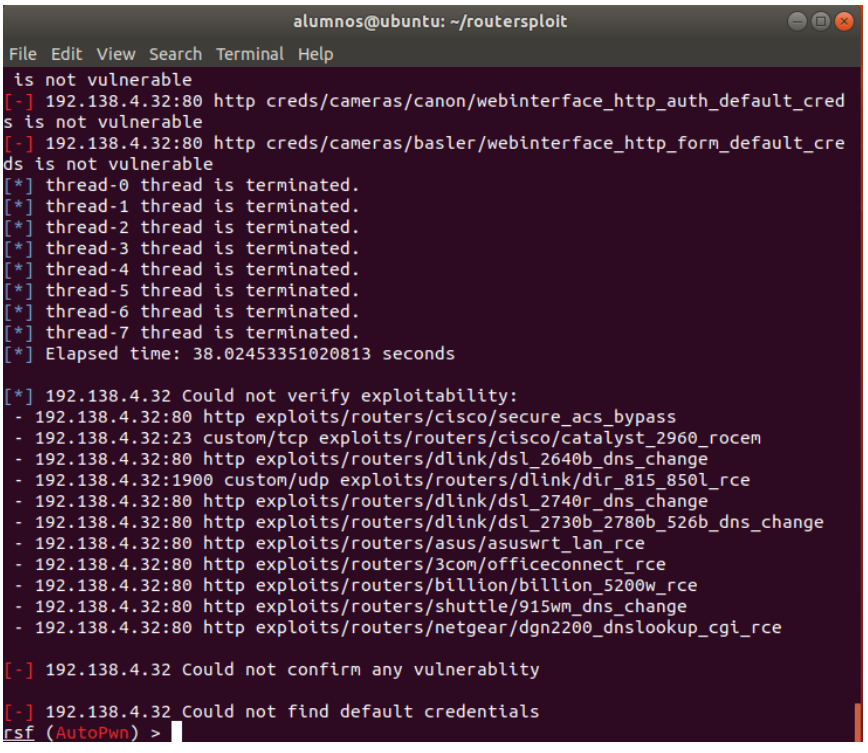


Figura 4.7. Resultado de la prueba

Después se lanzarse el ataque sobre el router de la Universidad de Cantabria, se genera un informe por pantalla y, se comprueba que no tiene ninguna vulnerabilidad.

4.8 METASPLOIT

Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos. [18]

Su subproyecto más conocido es el Metasploit Framework, una herramienta para desarrollar y ejecutar exploits contra una máquina remota. Otros subproyectos importantes son las bases de datos de opcodes (códigos de operación), un archivo de shellcodes, e investigación sobre seguridad. Inicialmente fue creado utilizando el lenguaje de programación de scripting Perl aunque actualmente el Metasploit Framework ha sido escrito de nuevo completamente en el lenguaje Ruby. [18]

Varios términos utilizados son:

-Exploit

Un exploit es el medio por el cual un atacante, o pentester, toma ventaja de una falla en un sistema, una aplicación o un servicio. Un atacante utiliza un exploit para atacar a un sistema de una manera que da lugar a un resultado particular. Exploits comunes son desbordamientos de búfer, vulnerabilidades de las aplicaciones web (como la inyección SQL) y errores de configuración. [19]

-Payload

Una payload es el código que queremos que el sistema se ejecute y que se va a seleccionar y entregado por el marco. Por ejemplo, un reverse shell es un payload que crea una conexión desde el equipo de destino del atacante como un símbolo del sistema (commmad prompt) de Windows, mientras que un bind shell es unpayload que “une (binds)” un símbolo del sistema (command prompt) para un puerto de escucha (listenning) en la máquina de destino, que el atacante puede conectarse. Una carga útil también podría ser algo tan simple como un par de comandos que se ejecutan en el sistema operativo de destino. [19]

-Shellcode

Shellcode es un conjunto de instrucciones utilizadas como payload cuando se produce la explotación. Shellcode normalmente se escribe en lenguaje ensamblador. En la mayoría de los casos, se proporcionará un shell de comandos o un shell Meterpreter después de la serie de instrucciones ha sido realizado por el equipo de destino, de ahí el nombre. [19]

-Module

Un módulo en el contexto es una pieza de software que puede ser utilizado por el Metasploit Framewor. A veces, se puede requerir el uso de un exploit module, un componente de software que lleva a cabo el ataque. Otras veces, un módulo auxiliar puede ser necesario para llevar a cabo una acción como el escaneado o la enumeración del sistema. Estos módulos intercambiables son el núcleo de lo que hace el Framework tan poderoso. [19]

-Listener

Un listener es un componente dentro de Metasploit que espera a una conexión entrante de algún tipo. Por ejemplo, después de que el equipo de destino ha sido explotado, puede llamar a la máquina de atacar a través de Internet. El listener se encarga de esa conexión, a la espera en la máquina atacante para ser contactado por el sistema de explotación. [19]

Los pasos básicos para la explotación de un sistema que utiliza el Sistema incluyen: [18]

1. La selección y configuración de un código el cual se va a explotar. El cual entra al sistema objetivo, mediante el aprovechamiento de una de bugs. Existen cerca de 900 exploits incluidos para Windows, Unix / Linux y Mac OS X. [18]
2. Opción para comprobar si el sistema destino es susceptible a los bugs elegidos. [16]
3. La técnica para codificar el sistema de prevención de intrusiones (IPS) e ignore la carga útil codificada. [18]
4. Visualización a la hora de ejecutar el exploit. [18]

Metasploit se ejecuta en Unix (incluyendo Linux y Mac OS X) y en Windows. El Sistema se puede extender y es capaz utilizar complementos en varios idiomas. [18]

Para elegir un exploit y la carga útil, se necesita un poco de información sobre el sistema objetivo, como la versión del sistema operativo y los servicios de red instalados. Esta información puede ser obtenida con el escaneo de puertos y "OS fingerprinting", puedes obtener esta información con herramientas como Nmap, NeXpose o Nessus, estos programas, pueden detectar vulnerabilidades del sistema de destino. Metasploit puede importar los datos de la exploración de vulnerabilidades y comparar las vulnerabilidades identificadas. [18]

Consta de los siguientes módulos:

-Módulo auxiliary: Permite la interacción de herramientas externas como pueden ser escaners de vulnerabilidades, sniffers, etc… con el framework de Metasploit. [20]

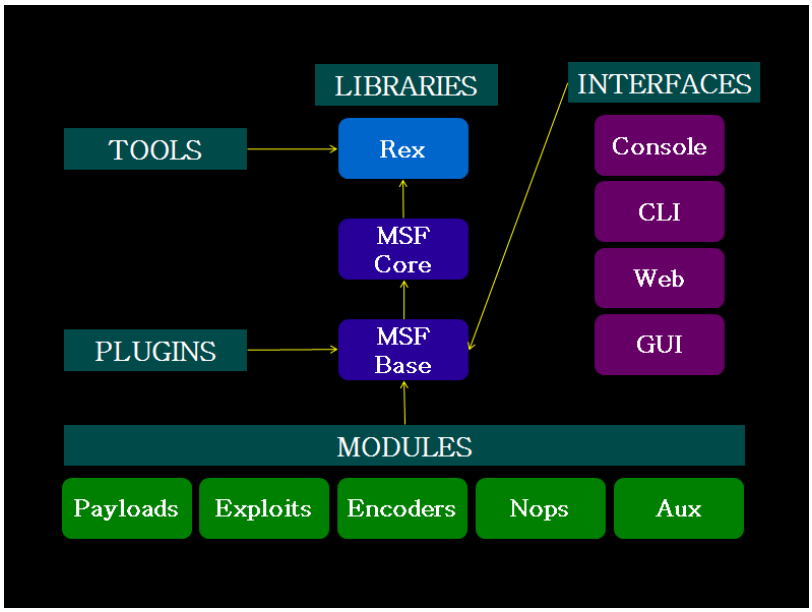
- Módulo encoders: Proporciona algoritmos para codificar y ofuscar los payloads que utilizaremos tras haber tenido exito el exploit. [20]

-Módulo exploits: Aquí es donde se encuentran todos los exploits disponibles en el framework para conseguir acceso a los diferentes SOs. [20]

-Módulo payloads: Nos proporciona gran cantidad de códigos “maliciosos” que podremos ejecutar una vez haya tenido éxito el exploit. [20]

- Módulo post: Nos proporciona funcionalidades para la fase de post explotación. [20]

-Módulo nops: Nos permite realizar u obtener operaciones nop. [20]



[19]

Figura 4.8. Arquitectura Metasploit

Instalación de Metasploit en Linux:

Curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \ chmod 755 msfinstall && \ ./msfinstall [21]

5. CONCLUSIONES

En este trabajado se han realizado pruebas de penetración mediantes varias herramientas sobre la Raspberry Pi, el cual actúa como un ordenador, y un ordenador normal. Y a su vez, ejecutar y conocer las herramientas más utilizadas en el ámbito de la seguridad.

Sobre la Raspberry Pi, se ha instalado el sistema operativo Kali Linux, uno muy conocido por su gran variedad de herramientas y para la realización de pruebas de seguridad mediante el programa Etcher.

Sobre Kali Linux se ha ejecutado wifite para el ataque de redes encriptadas como Wep, Wpa, Wpa2 y Wps. Su finalidad es extraer la clave wifi hackeandola. Se trata de una herramienta inalámbrica. Esta prueba se ha realizado sobre la red de un hogar. La red no pudo ser hackeada porque la seguridad era mayor.

Routersploit no pudo ser instalado por problemas de descarga.

Sobre un ordenador, se ha instalado el sistema operativo Ubuntu, un sistema parecido a Windows, de fácil manejo. La herramienta que se ha instalado en él es Routersploit, un framework que permite explorar las vulnerabilidades, en este caso del router de la universidad de Cantabria. Se ha comprobado que el router no tiene ninguna vulnerabilidad.

Otra herramienta que se ha estudiado es Metasploit. Está realiza test de penetración, pentesting, explora las vulnerabilidades de seguridad, como Routersploit, y el desarrollo de firmas para sistemas para la detección de intrusos. Esta aplicación se puede ejecutar tanto en Linux como en Ubuntu.

Estas herramientas son utilizadas de una forma sencilla, pero con ellas si conoces muy bien el manejo y el lenguaje puedes atacar a otros equipos. Por eso, se utiliza para conocer bien las vulnerabilidades de tus redes y con ello poder realizar test de penetración para tener un equipo más seguro.

5.1 LÍNEAS FUTURAS

La tecnología evoluciona rápidamente, muchos hackers seguirán intentando encontrar vulnerabilidades en redes y atacando a otros equipos, ya sea a través de un ordenador o mediante la Raspberry Pi.

Los medios por los que lo hacen, aplicaciones y herramientas son infinitas. Por esta razón, la realización de pruebas para encontrar vulnerabilidades y prevenir esos ataques son muy importantes para la seguridad de redes y cada vez más frecuentes.

Esta área cada vez tiene más peso y está más solicitada porque nunca un equipo será seguro del todo.

REFERENCIAS

[1] https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/

[2]https://subscription.packtpub.com/book/networking_and_servers/9781784396435/1

[3] https://es.wikipedia.org/wiki/Raspberry_Pi#Raspberry_Pi_3_Modelo_B

[4] http://histinf.blogs.upv.es/2013/12/18/raspberry-pi/

[5] https://docs.kali.org/introduction/what-is-kali-linux

[6] https://iciberseguridad.es/kali-linux-descargar-instalar/

[7] https://tools.kali.org/wireless-attacks/wifite

[8] https://www.ecured.cu/Tecnolog%C3%ADa_Wi-Fi

[9] https://www.ecured.cu/WEP

[10] https://www.ecured.cu/WPA

[11] https://www.ecured.cu/WPA2

[12] http://www.alegsa.com.ar/Dic/wps.php

[13] https://es.wikipedia.org/wiki/Wi-Fi_Protected_Setup

[14] https://linuxzone.es/distribuciones-principales/ubuntu

[15] https://www.redeszone.net/2016/11/12/routersploit-conoce-este-completo-framework-realizar-auditorias-seguridad-routers/

[16] https://hackpuntes.com/routersploit-comprueba-si-tu-router-es-vulnerable/

[17] https://github.com/threat9/routersploit (instalar)

[18] https://es.wikipedia.org/wiki/Metasploit

[19] https://widrogo.wordpress.com/tag/metasploit/

[20] http://highsec.es/2013/07/conociendo-metasploit-parte-i-exploit-basico/

[21] https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers