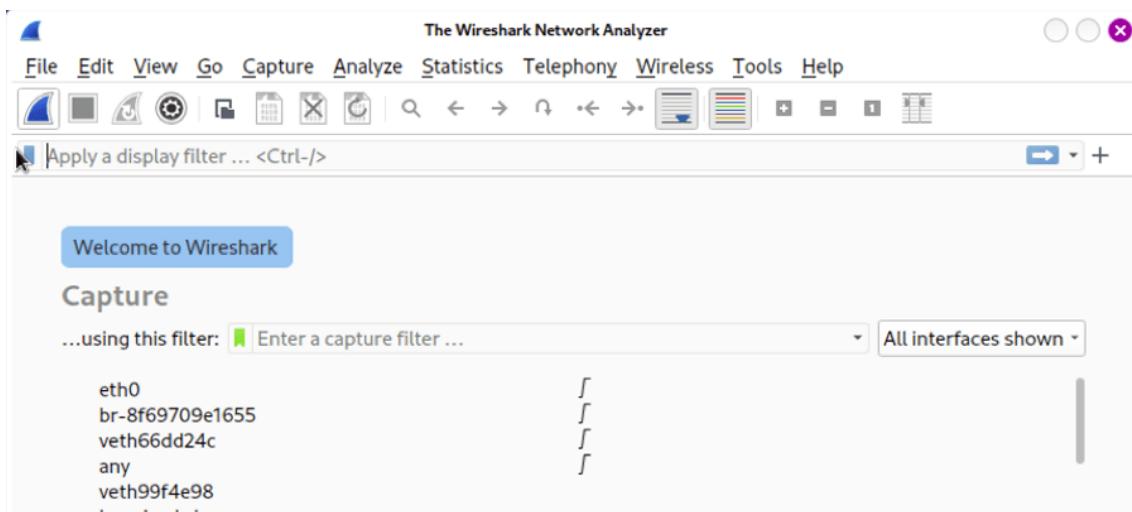


# Herramientas de monitoreo de red

Las herramientas de monitoreo de red son útiles para capturar, analizar y mostrar el tráfico de red en tiempo real. Permiten a los administradores de red y a los profesionales de seguridad obtener información sobre el comportamiento de los dispositivos de red, solucionar problemas y **detectar posibles amenazas de seguridad**.

## Wireshark



Wireshark es un analizador de protocolos de red ampliamente utilizado que **captura y muestra el tráfico de red en tiempo real**. Esta herramienta de código abierto es esencial para que los administradores de red y los profesionales de seguridad supervisen y analicen las actividades de red, solucionen problemas e identifiquen posibles amenazas de seguridad.

Gratis (código abierto)

Wireshark proporciona una interfaz fácil de usar con funciones avanzadas como filtrado, reglas de colores y vistas personalizables que facilitan la comprensión y el análisis del tráfico de la red.

### Características únicas:

- Captura y análisis del tráfico de red en tiempo real

- Interfaz personalizable con opciones de filtrado y coloración.
- Amplio soporte para varios protocolos

Preinstalado en Kali Purple.

## Nmap

```
└$ sudo nmap -Pn -T4 --traceroute www.example.com
[sudo] password for andrew:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 11:50 CDT
Nmap scan report for www.example.com (93.184.216.34)
Host is up (0.00042s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

TRACEROUTE (using port 9666/tcp)
HOP RTT      ADDRESS
1  0.34 ms  93.184.216.34

Nmap done: 1 IP address (1 host up) scanned in 28.41 seconds
```

Nmap, abreviatura de Network Mapper, es un potente escáner de red de código abierto que se utiliza para descubrir hosts y servicios en una red. Es una herramienta esencial para administradores de red y profesionales de seguridad, que proporciona información sobre los dispositivos y servicios presentes en una red, sus sistemas operativos y posibles vulnerabilidades.

Gratis (código abierto)

Nmap es muy versátil y ofrece una amplia gama de opciones de escaneo, incluido el descubrimiento de host, escaneo de puertos, detección de versiones e interacciones programables con los sistemas de destino.

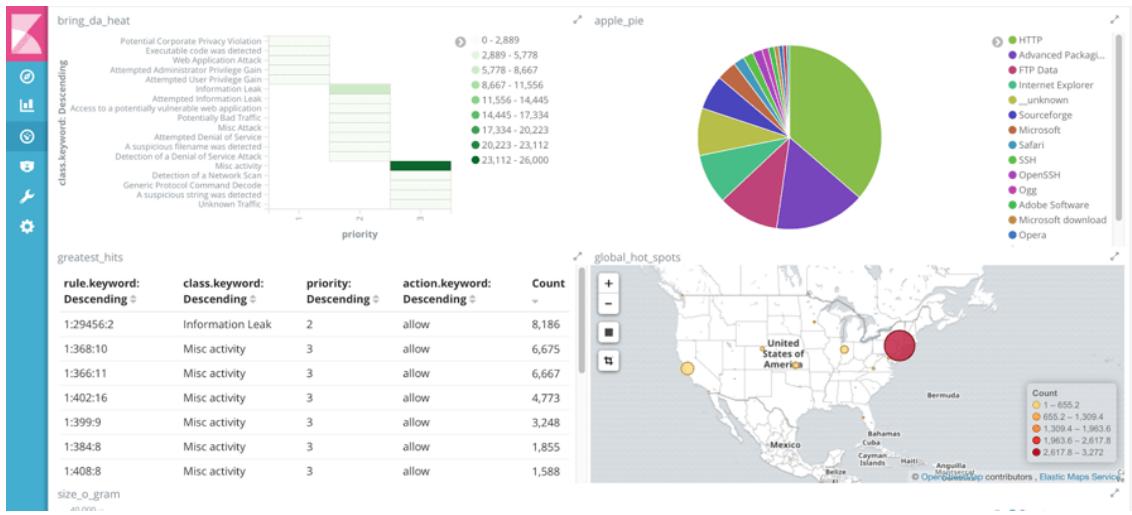
### Características únicas:

- Capacidades integrales de descubrimiento de host y escaneo de puertos

- Opciones de escaneo versátiles para diferentes tareas de seguridad de red
- Interacciones programables con sistemas de destino mediante el motor de scripts Nmap (NSE)

Preinstalado en Kali Purple.

## Snort



Snort es un popular sistema de detección de intrusiones (IDS) de código abierto que monitorea el tráfico de red para detectar actividades sospechosas. Al analizar los paquetes de red y aplicar reglas predefinidas, Snort puede detectar posibles amenazas de seguridad, como ataques, intrusiones o violaciones de políticas, y brindar alertas o tomar medidas preventivas.

Opciones gratuitas y de pago

Snort admite una amplia gama de protocolos de red y se puede ampliar con complementos para mejorar su funcionalidad.

### Características únicas:

- Análisis de tráfico en tiempo real y detección de intrusiones
- Conjuntos de reglas personalizables para una supervisión de seguridad personalizada
- Soporte para varios protocolos de red

- Arquitectura extensible con complementos para mayor funcionalidad

Descárguelo aquí: <https://www.snort.org/downloads>

## Herramientas forenses

Las herramientas de análisis forense digital son fundamentales para investigar incidentes, analizar evidencias y descubrir actividades maliciosas. Ayudan a los profesionales de seguridad y a los investigadores a examinar imágenes de disco, volcados de memoria y otras fuentes de datos para revelar información oculta y reconstruir eventos.

## Autopsy

The screenshot shows the Autopsy interface with the following details:

- Header:** localhost:9999/autopsy?mod=1&submod=4&case=stationxdemo&host=host1&... (with a star icon)
- Navigation:** Back, Forward, Home, Search, Help, Close
- Links:** Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec
- Toolbar:** FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, CLOSE
- Left Panel (Search Results):**
  - Searching for ASCII: Done
  - Saving: Done
  - 21 hits - [link to results](#)
  - [New Search](#)
  - 21 occurrences of [0-2]?[[:digit:]]{1,2}\[0-2]?[[:digit:]]{1,2}\[0-2]?[[:digit:]]{1,2}\[0-2]?[[:digit:]]{1,2} were found**
  - Search Options:
    - ASCII
    - Case Insensitive
    - Regular Expression
  - [Unit 103 \(Hex - Ascii\)](#)
  - 1: 478
- Right Panel (File Type: data):**
  - Unit: 103
  - Hex Contents of Unit 103 in autopsy.db-disk
  - Table showing hex dump from 0 to 113:
 

Hex	ASCII	File Contents
0	00000000	00000000 00000000 00000000
16	00000000	00000000 00000000 00000000
32	00000000	00000000 00000000 00000000
48	00000000	00000000 00000000 00000000
64	00000000	00000000 00000000 00000000
80	00000000	00000000 00000000 00000000
96	00000000	00000000 00000000 00000029
112	7F	4506 67..

Autopsy es una potente plataforma de análisis forense digital que proporciona una interfaz gráfica para [The Sleuth Kit](#) y ofrece funciones adicionales de análisis y análisis forense digital. Es ampliamente utilizada por investigadores, agentes de la ley y profesionales de seguridad para analizar imágenes de discos y otras fuentes de datos con el fin de descubrir información oculta y reconstruir eventos.

Gratis (código abierto)

El diseño modular de Autopsy permite a los usuarios ampliar sus capacidades con complementos y admite una amplia gama de sistemas de archivos y formatos de imagen.

### **Características únicas:**

- Interfaz gráfica para The Sleuth Kit
- Compatibilidad con varios sistemas de archivos y formatos de imagen.
- Arquitectura extensible con complementos para mayor funcionalidad
- Análisis de línea de tiempo, búsqueda de palabras clave y funciones de extracción de datos

Preinstalado en Kali Purple.

## **Volatility**

```
$ python vol.py -f Win2K3SP2x64-6f1bedec.vmem --profile=Win2003SP2x64 kdbgscan
Volatility Foundation Volatility Framework 2.4
*****
Instantiating KDBG using: Kernel AS Win2003SP2x64 (5.2.3791 64bit)
Offset (V)           : 0xf80001172cb0
Offset (P)           : 0x1172cb0
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win2003SP2x64
Version64           : 0xf80001172c70 (Major: 15, Minor: 3790)
Service Pack (CmNtCSDVersion) : 0
Build string (NtBuildLab)   : T?
PsActiveProcessHead    : 0xfffffff800011947f0 (0 processes)
PsLoadedModuleList     : 0xfffffff80001197ac0 (0 modules)
KernelBase            : 0xfffffff80001000000 (Matches MZ: True)
Major (OptionalHeader) : 5
```

Volatility es una potente herramienta de análisis forense de memoria de código abierto que puede analizar volcados de memoria para identificar posibles programas maliciosos u otras amenazas de seguridad. Los investigadores de seguridad y los encargados de responder a incidentes la utilizan ampliamente para investigar datos de memoria volátil de sistemas activos o volcados de memoria, lo que proporciona información valiosa sobre procesos en ejecución, conexiones de red y otros artefactos.

Gratis (código abierto)

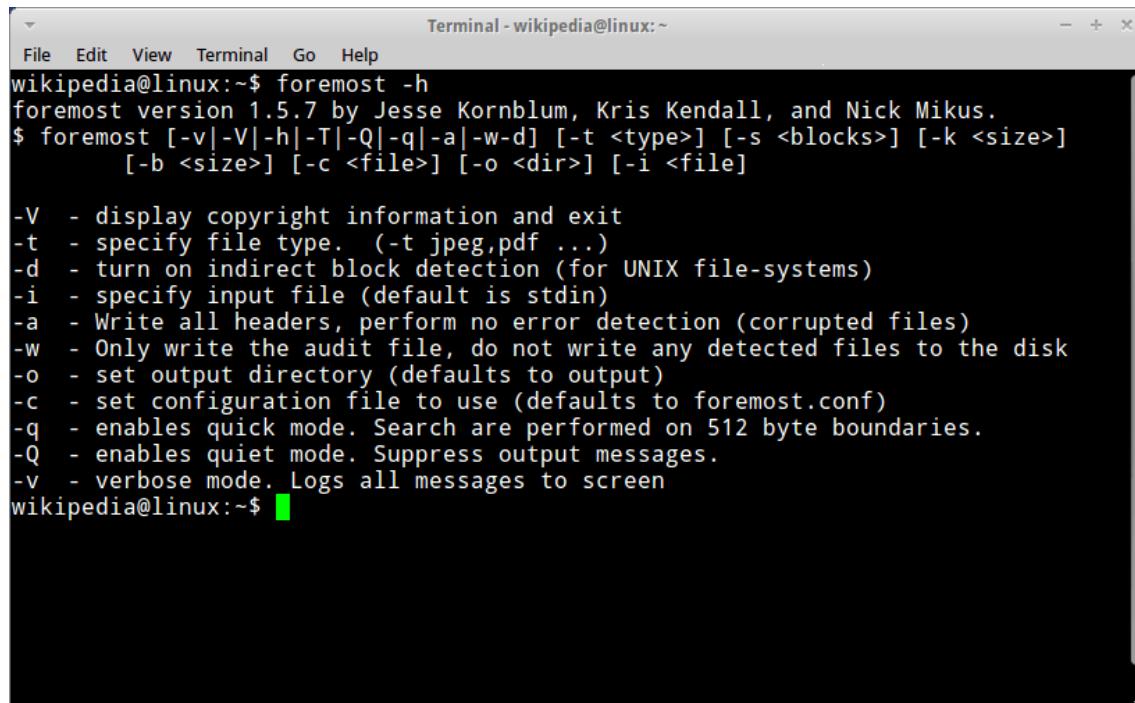
Volatility admite una amplia gama de plataformas y formatos de volcado de memoria, lo que lo hace muy versátil para diversas investigaciones.

### **Características únicas:**

- Análisis en profundidad de datos de memoria volátil
- Compatibilidad con múltiples plataformas y formatos de volcado de memoria
- Arquitectura extensible basada en complementos
- Extracción de artefactos valiosos como procesos en ejecución, conexiones de red y credenciales de usuario.

Descarga aquí: <https://www.volatilityfoundation.org/releases>

## **Foremost**



The screenshot shows a terminal window titled "Terminal - wikipedia@linux:~". The window contains the following text output from the "foremost" command:

```
wikipedia@linux:~$ foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
      [-b <size>] [-c <file>] [-o <dir>] [-i <file>]

-V  - display copyright information and exit
-t  - specify file type. (-t jpeg,pdf ...)
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
wikipedia@linux:~$
```

Foremost es una herramienta eficaz de extracción de archivos que puede extraer tipos de archivos específicos de imágenes de disco, sistemas activos y otras fuentes de datos. Es ampliamente utilizada por investigadores y profesionales de la ciencia forense digital para recuperar archivos perdidos o eliminados, lo que proporciona información valiosa sobre los datos almacenados en un dispositivo.

Gratis (código abierto)

Foremost admite una amplia gama de tipos de archivos, incluidos documentos, imágenes y archivos multimedia, y se puede personalizar para extraer tipos de archivos adicionales si es necesario.

## **Características únicas:**

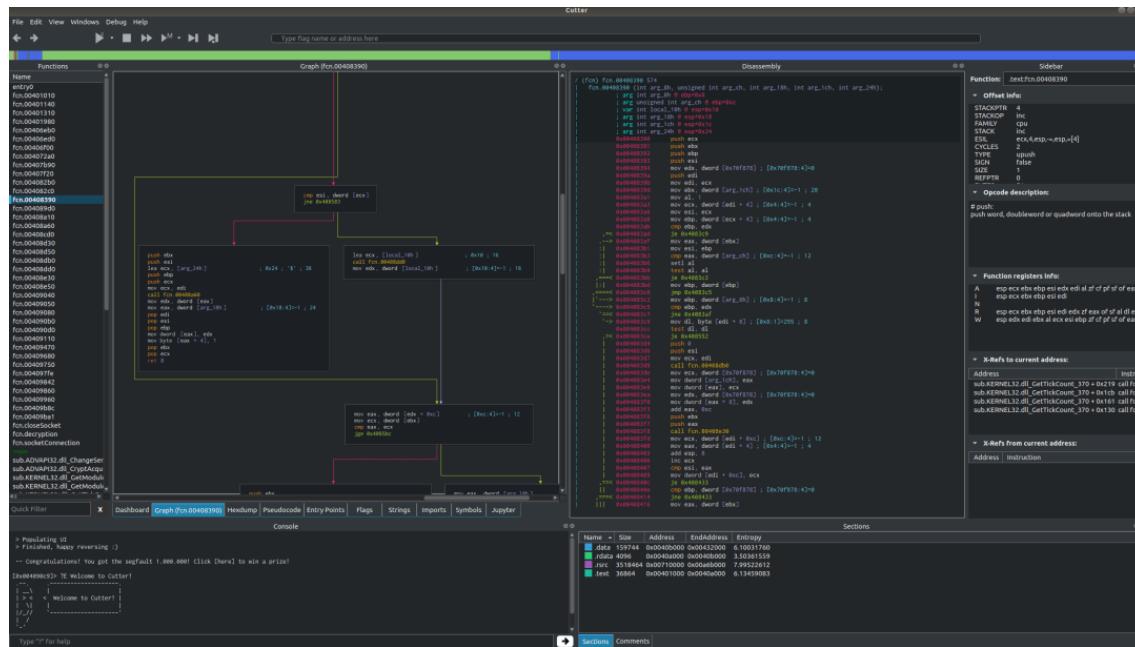
- Tallado de archivos rápido y eficiente
  - Compatibilidad con una amplia gama de tipos de archivos
  - Firmas de tipos de archivos personalizables para extracción de archivos adicionales

Preinstalado en Kali Purple.

# Herramientas de ingeniería inversa

Las herramientas de ingeniería inversa permiten a los investigadores de seguridad, analistas de malware y desarrolladores de software analizar y desensamblar código binario para comprender su funcionalidad y descubrir posibles vulnerabilidades. Estas herramientas son increíblemente útiles para diseccionar programas compilados, aplicar ingeniería inversa a malware y explorar vulnerabilidades de software.

# Radare2



Radare2 es un marco integral de ingeniería inversa de línea de comandos que puede analizar y desensamblar código binario. Es ampliamente adoptado por investigadores de seguridad, analistas de malware e ingenieros inversos para tareas como análisis binario, depuración y aplicación de parches.

Gratis (código abierto)

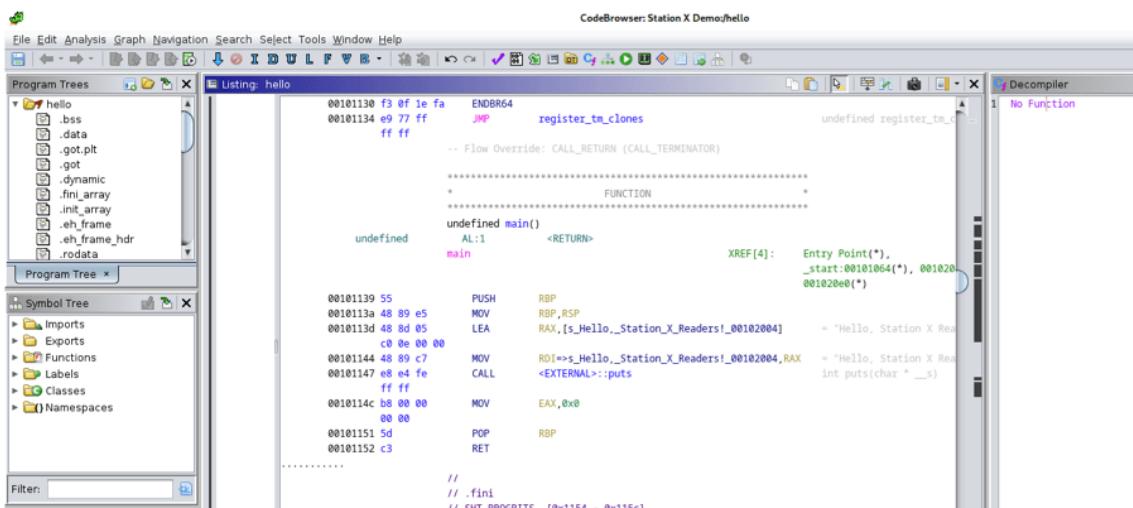
Radare2 ofrece un amplio conjunto de funciones y admite una amplia gama de arquitecturas, formatos de archivos y sistemas operativos, lo que lo hace adecuado para diversas tareas de ingeniería inversa.

### Características únicas:

- Marco de ingeniería inversa de línea de comandos versátil
- Compatibilidad con diversas arquitecturas, formatos de archivos y sistemas operativos.
- Flujo de trabajo de análisis personalizable y programable
- Capacidades integradas de depuración y aplicación de parches

Preinstalado en Kali Purple.

## Ghidra



The screenshot shows the Ghidra software interface. The top menu bar includes File, Edit, Analysis, Graph, Navigation, Search, Select, Tools, Window, Help. The main window has several panes:

- Program Trees**: Shows the file structure of 'hello' with sections like .bss, .data, .got.plt, .got, .dynamic, .fini\_array, .init\_array, .eh\_frame, .eh\_frame\_hdr, and .rodata.
- Symbol Tree**: Shows categories like Imports, Exports, Functions, Labels, Classes, and Namespaces.
- Listing: hello**: Displays assembly code for the 'hello' program. The code starts with an ENDBR64 instruction at address 00101130, followed by a jump to 'register\_tm\_clones'. The main function is defined at address 00101139, starting with a PUSH RBP instruction. The assembly code continues with various instructions like MOV, LEA, CALL, and RET, along with comments explaining the purpose of each section.
- CodeBrowser: Station X Demo/hello**: A smaller pane showing the same assembly code.
- Decompiler**: A pane on the right showing the decompiled C code for the program.

Ghidra es una potente herramienta de ingeniería inversa desarrollada por la Agencia de Seguridad Nacional (NSA) que se puede utilizar para analizar y desensamblar código binario. Ofrece una interfaz gráfica intuitiva y funciones avanzadas, lo que la convierte en una excelente opción para investigadores de seguridad, analistas de malware e ingenieros inversos.

Gratis (código abierto)

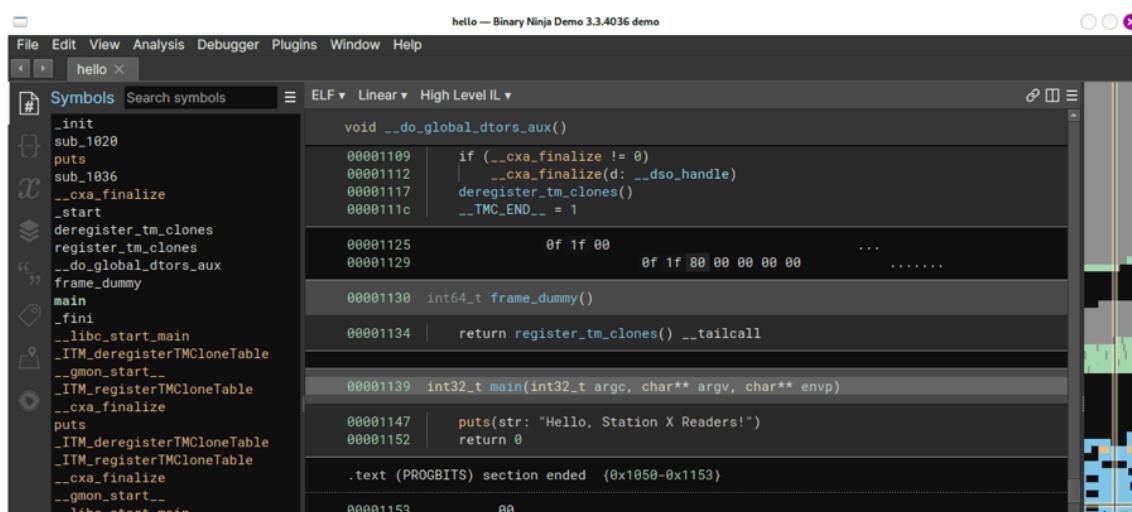
Ghidra ofrece funciones avanzadas como descompilación, creación de scripts y capacidades de parcheo, lo que lo hace adecuado para diversas tareas de ingeniería inversa.

### Características únicas:

- Interfaz gráfica intuitiva para tareas de ingeniería inversa
- Capacidades avanzadas de descompilación y desensamblaje
- Arquitectura de complemento extensible para funcionalidad adicional
- Compatibilidad con diversas arquitecturas, formatos de archivos y sistemas operativos.

Preinstalado en Kali Purple.

## Binary Ninja



Binary Ninja es una herramienta comercial de ingeniería inversa con una interfaz fácil de usar para analizar código binario. Su potente motor de análisis y su amplio conjunto de funciones lo convierten en una excelente opción para investigadores de seguridad, analistas de malware e ingenieros inversos que buscan una alternativa más accesible a las herramientas de línea de comandos.

Pago, prueba gratuita

El potente motor de análisis de Binary Ninja puede identificar automáticamente funciones, bucles y otras estructuras de código, lo que facilita la comprensión y la navegación por binarios complejos.

#### **Características únicas:**

- Interfaz fácil de usar para tareas de ingeniería inversa
- Potente motor de análisis con identificación automática de la estructura del código
- Compatibilidad con scripts y complementos para personalización

Descárgalo aquí: <https://binary.ninja/>

## **Herramientas de evaluación y gestión de vulnerabilidades**

Las herramientas de esta categoría ayudan a las organizaciones a identificar, priorizar y abordar posibles vulnerabilidades de seguridad en sus sistemas y redes. Realizan análisis automatizados, detectan fallas de seguridad y generan informes detallados sobre las vulnerabilidades y sus posibles impactos.

## GVM (anteriormente OpenVAS)

The screenshot shows the Greenbone Security Assistant interface. At the top, there are navigation tabs: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the tabs, a search bar is present with a filter placeholder. The main content area displays a scan report for a host named "Repor" (ID: 10bb72df-acd0-4edc-9741-635d22d5edf8) from Friday, March 17, 2023, at 10:42 AM UTC. The report includes sections for Information, Results, Hosts, Ports, Applications, Operating Systems, CVEs, Closed CVEs, TLS Certificates, Error Messages, and User Tags. A table below lists the vulnerabilities found, including their severity (e.g., 10.0 (High)), QoD (Quality of Detection), Host IP, Name, Location, and Creation date.

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
CVE-2012-2688	10.0 (High)	75 %	192.168.201.9			Fri, Mar 17, 2023 10:42 AM UTC
CVE-2015-0235	10.0 (High)	75 %	192.168.201.9			Fri, Mar 17, 2023 10:42 AM UTC
CVE-2014-9912	9.8 (High)	75 %	192.168.201.9			Fri, Mar 17, 2023 10:42 AM UTC

Greenbone Vulnerability Manager, anteriormente OpenVAS, es un escáner de vulnerabilidades de código abierto que puede identificar posibles vulnerabilidades de seguridad en una red. Es ampliamente utilizado por profesionales de seguridad y administradores de sistemas para evaluar la situación de seguridad de sus redes y priorizar los esfuerzos de reparación.

Gratis (código abierto)

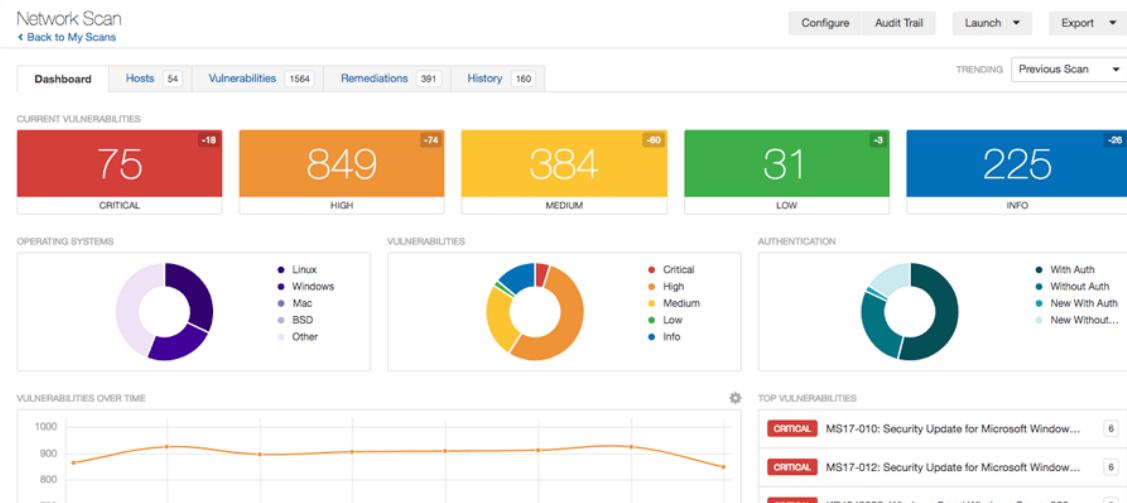
GVM ofrece una solución integral de escaneo de vulnerabilidades con una extensa base de datos de controles de seguridad, lo que la hace altamente efectiva para identificar vulnerabilidades potenciales.

### Características únicas:

- Solución integral de escaneo de vulnerabilidades
- Amplia base de datos de controles de seguridad
- Interfaz basada en web para la gestión y generación de informes de escaneo
- Integración con otras herramientas y plataformas de seguridad

Preinstalado en Kali Purple.

# Nessus



Nessus es un escáner de vulnerabilidades comercial ampliamente utilizado y con muchas funciones que puede identificar y priorizar posibles vulnerabilidades de seguridad. Los profesionales de seguridad y los administradores de sistemas de todo el mundo confían en él para evaluar la situación de seguridad de sus redes y ayudar a priorizar los esfuerzos de reparación. También aparece en nuestro artículo [Los mejores escáneres de vulnerabilidades para Kali Linux](#).

## Pago

Nessus ofrece una amplia base de datos de controles de seguridad y es conocido por su precisión en la identificación de vulnerabilidades.

## Características únicas:

- Solución de escaneo de vulnerabilidades precisa y completa
- Amplia base de datos de controles de seguridad
- Interfaz intuitiva basada en web para la gestión y generación de informes de escaneo
- Integración con otras herramientas y plataformas de seguridad

Descárguelo aquí: <https://www.tenable.com/products/nessus>

# Metasploit

```
[+] metasploit v6.3.14-dev
+ -- ---=[ 2311 exploits - 1206 auxiliary - 412 post      ]
+ -- ---=[ 975 payloads - 46 encoders - 11 nops          ]
+ -- ---=[ 9 evasion                                ]

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search eternalblue

Matching Modules
=====
#  Name
-  --
0  exploit/windows/smb/ms17_010_永恒之蓝      Disclosure Date  Rank   Check  Description
Blue SMB Remote Windows Kernel Pool Corruption 2017-03-14    average Yes    MS17-010 Eternal
1  exploit/windows/smb/ms17_010_psexec        2017-03-14    normal  Yes    MS17-010 Eternal
Romance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command       2017-02-14    normal  No     MS17-010 Eternal
```

Metasploit es un marco de trabajo ampliamente utilizado para desarrollar y ejecutar exploits contra sistemas vulnerables. Proporciona una amplia biblioteca de exploits, cargas útiles y módulos auxiliares, lo que lo convierte en una herramienta poderosa para que los profesionales de seguridad, los evaluadores de penetración y los investigadores evalúen y validen la seguridad de sus redes y aplicaciones. Puede encontrar nuestra [hoja de referencia aquí](#).

Gratis (código abierto), pago (Metasploit Pro)

La extensa biblioteca de exploits y cargas útiles de Metasploit permite a los usuarios probar de forma rápida y eficaz la seguridad de sus sistemas.

Descargue Metasploit Pro aquí: <https://www.metasploit.com/>

## Características únicas:

- Amplia biblioteca de exploits, cargas útiles y módulos auxiliares
- Arquitectura modular para una fácil personalización e integración.
- Interfaces de línea de comandos y basadas en web para diversas preferencias de usuario

Preinstalado en Kali Purple.

## Herramientas de análisis de malware

Las herramientas de análisis de malware son fundamentales para detectar, examinar y comprender el comportamiento del software malicioso. Permiten a los investigadores y analistas de seguridad analizar el malware, estudiar su funcionalidad y desarrollar contramedidas para protegerse contra él.

### Total de virus

The screenshot shows the VirusTotal analysis interface. At the top, there's a search bar and various navigation icons. Below it, a large green circle indicates a 'Community Score' of 0 out of 57. To the right, a message says 'No security vendors and no sandboxes flagged this file as malicious'. Underneath, the file name '9aca7b142890a5aae7ef79c75fe9fbda4428bbc836437042069a6ec7074ca33 virustotal1.png' is listed along with its type 'png', size '185.27 KB', and upload date '2023-05-04 00:15:47 UTC' (1 minute ago). On the far right is a 'PNG' file preview icon. Below this, there are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'. The 'DETECTION' tab is selected, showing a table of vendor analysis results:

Security vendors' analysis	Do you want to automate checks?			
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected	
ALYac	Undetected	Antiy-AVL	Undetected	
Arcabit	Undetected	Avast	Undetected	
AVG	Undetected	Avira (no cloud)	Undetected	
Baidu	Undetected	BitDefender	Undetected	

VirusTotal es un popular servicio de análisis de malware en línea que permite a los usuarios cargar archivos y URL para analizarlos con varios motores antivirus y otras herramientas de seguridad. Agrega los resultados para brindar información completa sobre amenazas potenciales, lo que lo convierte en un recurso valioso para investigadores de seguridad, analistas de malware y personal de respuesta ante incidentes.

Gratis (Web)

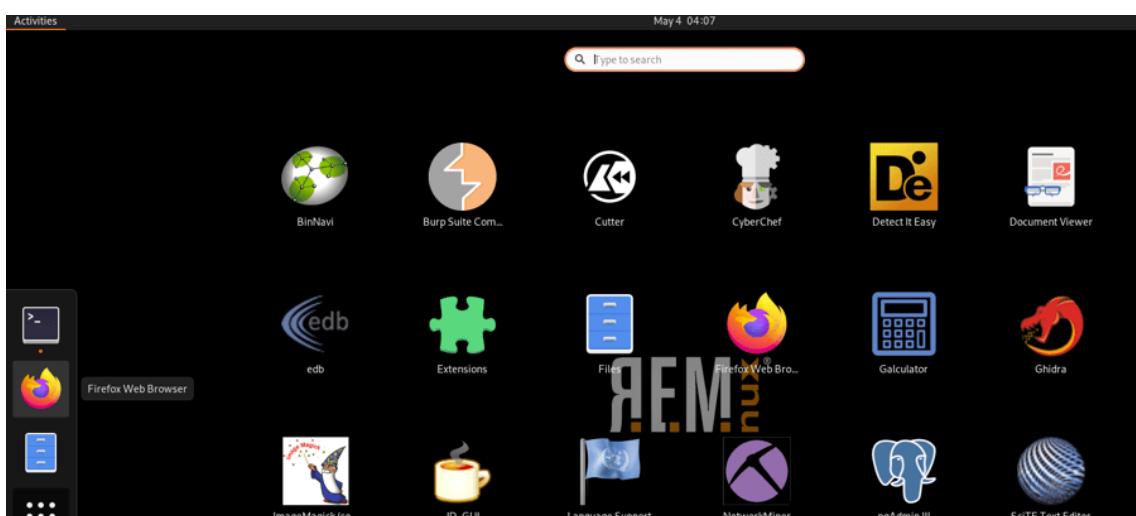
VirusTotal ofrece una forma rápida y sencilla de analizar archivos y URL sospechosos sin tener que configurar un entorno de análisis de malware dedicado. El uso de múltiples motores antivirus y herramientas de seguridad garantiza una alta tasa de detección y ayuda a los usuarios a identificar falsos positivos.

## Características únicas:

- Servicio de análisis de malware en línea con múltiples motores antivirus y herramientas de seguridad
- Alta tasa de detección e identificación de falsos positivos
- Interfaz basada en web, reglas personalizadas de Yara y compatibilidad con API para una fácil accesibilidad e integración
- Plataforma impulsada por la comunidad para compartir y obtener información sobre amenazas

Accede aquí: <https://www.virustotal.com/gui/home/upload>

## REMnux



REMnux es una distribución de Linux diseñada específicamente para el análisis de malware y la ingeniería inversa. Viene precargada con una amplia gama de herramientas y utilidades, lo que facilita a los investigadores de seguridad, analistas de malware y encargados de la respuesta a incidentes diseccionar y analizar archivos sospechosos y tráfico de red.

Soporte gratuito (código abierto), pago

REMnux proporciona un entorno optimizado diseñado específicamente para tareas de análisis de malware, con una colección seleccionada de herramientas que simplifican la disección y la comprensión del software malicioso.

## Características únicas:

- Entorno personalizado para análisis de malware e ingeniería inversa
- Colección seleccionada de herramientas y utilidades preinstaladas
- Fácil implementación como máquina virtual
- Entorno seguro para analizar archivos potencialmente dañinos

Descárguelo aquí: <https://docs.remnux.org/install-distro/get-virtual-appliance>

## YARA

```
josh@REVOLUTION:~$ yara
usage: yara [OPTION]... [RULEFILE]... FILE | PID
options:
  -t <tag>           print rules tagged as <tag> and ignore the rest.
  -i <identifier>     print rules named <identifier> and ignore the rest.
  -n                 print only not satisfied rules (negate).
  -g                 print tags.
  -m                 print metadata.
  -s                 print matching strings.
  -l <number>         abort scanning after a <number> of rules matched.
  -d <identifier>=<value> define external variable.
  -r                 recursively search directories.
  -f                 fast matching mode.
  -v                 show version information.

Report bugs to: <vmalvarez@virustotal.com>
```

YARA es una herramienta versátil de comparación de patrones que identifica y clasifica el malware en función de atributos específicos. Permite a los investigadores de seguridad y analistas de malware crear reglas personalizadas que describen las características únicas de una familia de malware en particular, lo que la convierte en una herramienta eficaz para detectar y categorizar software malicioso.

Gratis (código abierto)

La simplicidad y eficiencia de YARA lo convierten en una herramienta esencial para investigadores de seguridad y analistas de malware que buscan comprender integralmente las amenazas que enfrentan.

## Características únicas:

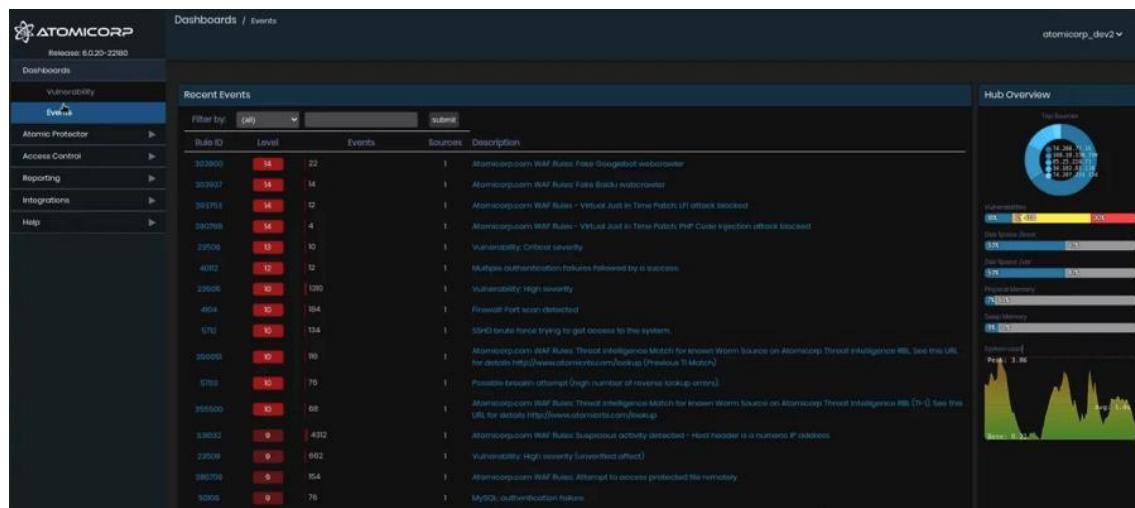
- Herramienta versátil de comparación de patrones para la identificación de malware
- Reglas personalizadas para describir características únicas del malware
- Eficaz para detectar y categorizar software malicioso
- Integración con otras herramientas y plataformas de seguridad

Preinstalado en Kali Purple.

## Herramientas de seguridad de puntos finales

Las herramientas de seguridad de endpoints se centran en supervisar, analizar y proteger dispositivos individuales (endpoints) dentro de una red. Las organizaciones las utilizan para proteger sus sistemas de accesos no autorizados, malware y otras amenazas de seguridad.

## OSSEC



OSSEC es un sistema de detección de intrusiones basado en host de código abierto que monitorea y analiza la actividad en un punto final. Proporciona análisis de registros completos,

verificación de integridad de archivos, monitoreo de políticas y capacidades de detección de rootkits, lo que lo convierte en una herramienta valiosa para administradores de sistemas y profesionales de seguridad que buscan proteger sus sistemas.

Gratis (código abierto), pago (OSSEC+)

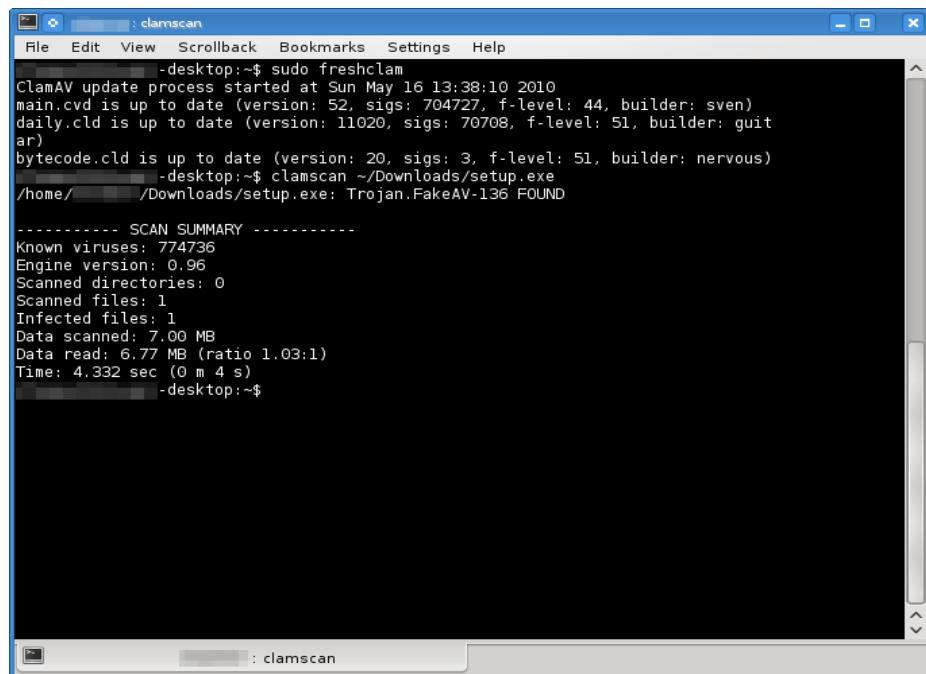
Su escalabilidad y soporte para diversas plataformas lo hacen adecuado para diversos entornos, mientras que su función de respuesta activa permite la remediación automatizada de las amenazas detectadas.

#### Características únicas:

- Análisis de registros exhaustivo y verificación de integridad de archivos
- Capacidades de detección de rootkits y monitoreo de políticas
- Escalable y adecuado para diversos entornos.
- Función de respuesta activa para la remediación automatizada

Descárguelo aquí: <https://www.ossec.net/ossec-downloads/>

## ClamAV



```
-desktop:~$ sudo freshclam
ClamAV update process started at Sun May 16 13:38:10 2010
main.cvd is up to date (version: 52, sigs: 704727, f-level: 44, builder: sven)
daily.cld is up to date (version: 11020, sigs: 70708, f-level: 51, builder: guit
ar)
bytecode.cld is up to date (version: 20, sigs: 3, f-level: 51, builder: nervous)
/home/ /Downloads/setup.exe: Trojan.FakeAV-136 FOUND

----- SCAN SUMMARY -----
Known viruses: 774736
Engine version: 0.96
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 7.00 MB
Data read: 6.77 MB (ratio 1.03:1)
Time: 4.332 sec (0 m 4 s)
-deSKTOP:~$
```

ClamAV es un software antivirus de código abierto que puede escanear y detectar malware en un punto final. Ofrece un demonio de escaneo multiproceso, utilidades de línea de comandos para escaneo de archivos a pedido y actualizaciones automáticas de la base de datos para garantizar que se mantenga actualizado con las últimas amenazas de malware.

Gratis (código abierto)

ClamAV proporciona una solución liviana y confiable para detectar malware en puntos finales, lo que lo convierte en una herramienta esencial para administradores de sistemas y profesionales de seguridad.

#### **Características únicas:**

- Daemon de escáner multiproceso para un escaneo eficiente
- Utilidades de línea de comandos para escaneo de archivos a pedido
- Actualizaciones automáticas de la base de datos para la detección de malware actualizada
- Compatibilidad con varios formatos de archivos y archivos

Preinstalado en Kali Purple.

## **Herramientas de seguridad para aplicaciones web**

Las herramientas de seguridad de aplicaciones web están diseñadas para descubrir y abordar vulnerabilidades en aplicaciones web. Ayudan a los desarrolladores y profesionales de seguridad a probar aplicaciones web para detectar problemas como **inyección SQL**, **secuencias de comandos entre sitios** y otras vulnerabilidades basadas en la web.

## Nikto

```
> nikto -h example.com
- Nikto v2.1.6
-----
+ Target IP:      93.184.216.34
+ Target Hostname: example.com
+ Target Port:    80
+ Start Time:    2023-05-03 20:56:01 (GMT-5)
-----
+ Server: ECS (dab/4B67)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-cache' found, with contents: HIT
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'ECS (dab/4B67)' to 'EOS (vny/044E)' which may suggest a WAF, load balancer or proxy is in place
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
```

Nikto es un escáner de vulnerabilidades de aplicaciones web de código abierto que puede identificar posibles problemas de seguridad en servidores y aplicaciones web. Comprueba si hay configuraciones incorrectas, software desactualizado y otras vulnerabilidades comunes, lo que lo convierte en una herramienta valiosa para desarrolladores web, evaluadores de penetración y profesionales de la seguridad.

Gratis (código abierto)

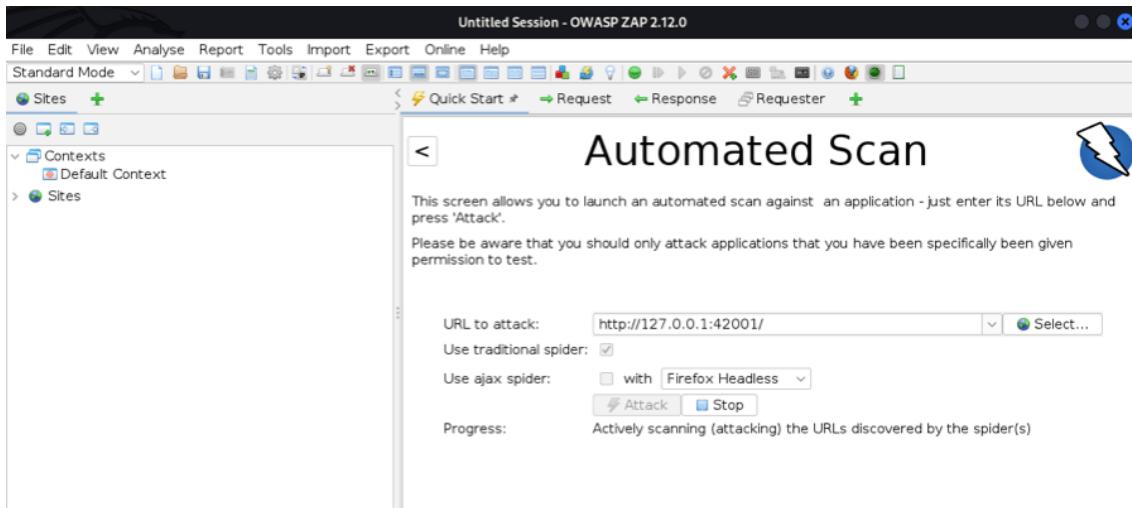
Nikto ofrece una solución integral para escanear aplicaciones web y servidores en busca de posibles problemas de seguridad, lo que lo convierte en una herramienta esencial para cualquiera que busque identificar y remediar vulnerabilidades en su infraestructura web.

### Características únicas:

- Análisis integral de vulnerabilidades de aplicaciones web
- Comprueba configuraciones incorrectas, software desactualizado y otros problemas comunes
- Actualizaciones periódicas para mantenerse al día con la información más reciente sobre vulnerabilidades
- Compatibilidad con diversas tecnologías de servidores web

Preinstalado en Kali Linux.

## ZAP OWASP



OWASP ZAP es un escáner de seguridad de aplicaciones web de código abierto desarrollado por el **Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP)**. Proporciona una interfaz fácil de usar para realizar escaneos de vulnerabilidades manuales y automatizados y herramientas para interceptar y modificar el tráfico web, lo que lo convierte en una herramienta poderosa para desarrolladores web, evaluadores de penetración y profesionales de la seguridad.

Gratis (código abierto)

OWASP ZAP ofrece una amplia gama de funciones, participación activa de la comunidad e integración con otras herramientas de seguridad, lo que lo convierte en una valiosa adición a cualquier kit de herramientas de seguridad web.

### Características únicas:

- Análisis de vulnerabilidades automatizado y manual
- Herramientas para interceptar y modificar el tráfico web
- Integración con otras herramientas y plataformas de seguridad

Preinstalado en Kali Purple.

# Wapiti

## Vulnerability found in /n\_sql-simpl-get.php

Description    **HTTP Request**    cURL command line

```
GET /n_sql-simpl-get.php?search=%3C%2Fscript%3E%3CScRiPt%3Ealert%28%2Fwj3n56ujrg%2F%29%3C%2FsCrIpT%3E&enter=submit HTTP/1.1
Host: sites.vulns.pentestit.ru
Referer: http://sites.vulns.pentestit.ru/n_sql-simpl-get.php
```

## Vulnerability found in /index.php

Description    **HTTP Request**    cURL command line

```
XSS vulnerability found via injection in the parameter login
```

## Vulnerability found in /index2.php

Description    **HTTP Request**    cURL command line

```
POST /index2.php HTTP/1.1
Host: sites.vulns.pentestit.ru
Referer: http://sites.vulns.pentestit.ru/index2.php
Content-Type: multipart/form-data; boundary=-----boundarystring

-----boundarystring
Content-Disposition: form-data; name="form_file_22"; filename=<Img src=z oNeRrror=alert('wxm1jpwhwf')>"

GIF89a
-----boundarystring--
```

Wapiti es un escáner de vulnerabilidades de código abierto para aplicaciones web que puede identificar y solucionar problemas de seguridad en aplicaciones web. Realiza un escaneo de «caja negra» analizando las páginas web de la aplicación en busca de posibles vulnerabilidades, como inyección SQL, secuencias de comandos entre sitios (XSS) e inclusión de archivos, lo que lo convierte en una herramienta útil para desarrolladores web, evaluadores de penetración y profesionales de la seguridad.

Gratis (código abierto)

Wapiti ofrece soporte para varios tipos de ataques, facilidad de uso y la capacidad de generar informes, lo que lo convierte en una herramienta valiosa para evaluaciones y auditorías de seguridad web.

## Características únicas:

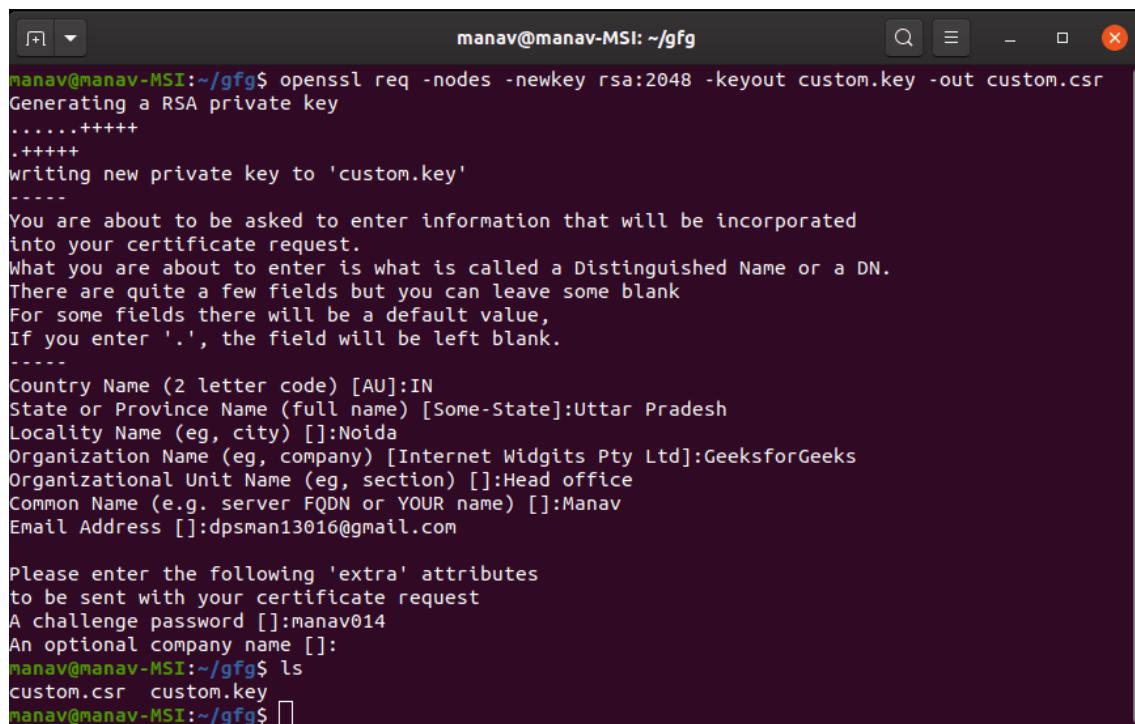
- Análisis de vulnerabilidades de aplicaciones web de tipo «caja negra»
- Identifica inyección SQL, XSS, inclusión de archivos y otras vulnerabilidades comunes
- Soporte para varios tipos de ataques
- Genera informes en múltiples formatos.

Preinstalado en Kali Purple.

## Otras herramientas de seguridad

Esta categoría incluye herramientas de seguridad adicionales que no encajan perfectamente en las categorías anteriores, pero que siguen siendo esenciales para mantener un entorno seguro y que los miembros del Equipo Azul deberían tener en cuenta. Estas herramientas cubren diversas funciones, como el cifrado, la comprobación de la integridad de los archivos y el control de acceso.

## OpenSSL



```
manav@manav-MSI:~/gfg$ openssl req -nodes -newkey rsa:2048 -keyout custom.key -out custom.csr
Generating a RSA private key
.....+++++
.....+
writing new private key to 'custom.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Uttar Pradesh
Locality Name (eg, city) []:Noida
Organization Name (eg, company) [Internet Widgits Pty Ltd]:GeeksforGeeks
Organizational Unit Name (eg, section) []:Head office
Common Name (e.g. server FQDN or YOUR name) []:Manav
Email Address []:dpsman13016@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:manav014
An optional company name []:
manav@manav-MSI:~/gfg$ ls
custom.csr  custom.key
manav@manav-MSI:~/gfg$ 
```

OpenSSL es un conjunto de herramientas de código abierto que se puede utilizar para implementar protocolos SSL/TLS y cifrado. Proporciona herramientas sólidas para crear y administrar certificados, pares de claves y funciones criptográficas. Es una herramienta esencial para administradores de sistemas, desarrolladores y profesionales de seguridad que buscan proteger las comunicaciones de red.

Gratis (código abierto)

El amplio conjunto de características de OpenSSL, su desarrollo activo y su soporte para varios algoritmos criptográficos lo convierten en una opción confiable para proteger datos y comunicaciones.

#### **Características únicas:**

- Implementa protocolos SSL/TLS y encriptación
- Herramientas para crear y gestionar certificados y pares de claves
- Admite varios algoritmos criptográficos
- Desarrollo activo y actualizaciones periódicas.

Preinstalado en Kali Purple.

## **GPG (protección de privacidad GNU)**

```
root@SAMBASF:~# gpg --gen-key
gpg (GnuPG) 1.4.12; Copyright (C) 2012 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Por favor seleccione tipo de clave deseado:
 (1) RSA and RSA (default)
 (2) DSA and Elgamal
 (3) DSA (sólo firmar)
 (4) RSA (sólo firmar)
Su elección: _
```

GPG es una herramienta de cifrado de código abierto que se puede utilizar para proteger datos y comunicaciones. Basada en el estándar OpenPGP, permite a los usuarios cifrar, descifrar y

firmar datos, garantizando la confidencialidad, integridad y autenticidad de la información. GPG se utiliza ampliamente para el cifrado de correo electrónico, la protección de archivos y la distribución segura de software, lo que la convierte en una herramienta valiosa para personas y organizaciones que buscan proteger sus activos digitales.

Gratis (código abierto)

El soporte de GPG para varios algoritmos de cifrado, capacidades de administración de claves e integración con clientes y herramientas de correo electrónico populares lo hacen versátil para proteger datos y comunicaciones confidenciales.

#### **Características únicas:**

- Basado en el estándar OpenPGP
- Cifrar, descifrar y firmar datos
- Soporte para varios algoritmos de cifrado
- Capacidades de gestión de claves e integración con herramientas y clientes de correo electrónico populares
- Capacidades de gestión de claves e integración con herramientas y clientes de correo electrónico populares

Preinstalado en Kali Purple.

## **AIDE (Entorno de detección de intrusiones avanzado)**

---

The attributes of the (uncompressed) database(s):

---

```
/var/lib/aide/aide.db
MD5      : XIH/j+OPD5l6qLFJBYbbJA==
SHA1     : u82I3oyYjPpZW+ZxK5tsSVVP9XU=
SHA256   : JffrD11AXKaEUFrK/FjkgII0NwqIufXO
           lgxp/RfiB0Q=
SHA512   : cGat1bDtjoE6+DIEUMtMcBqaEbNG51q0
           v60Pfcsg4Kfa0+gM2OB7e5R+3XqnTZvC
           OryJpmSeNSYnRZlxelPc0g=
RMD160   : UYMaabXiv1CLt4q70+NmSzDvYNs=
TIGER    : gCHL5ovHKcyUUVGIVqh9daZp9cyPJ0eC
```

AIDE es un verificador de integridad de archivos que detecta cambios no autorizados en los archivos del sistema. Crea una base de datos de atributos de archivos, como permisos, propiedad y hashes, y los compara con una línea base para identificar discrepancias. AIDE se utiliza habitualmente para supervisar archivos y directorios críticos del sistema en busca de signos de compromiso o manipulación, lo que lo convierte en una herramienta esencial para administradores de sistemas y profesionales de seguridad.

Gratis (código abierto)

AIDE proporciona una solución sencilla y eficiente para supervisar la integridad de los archivos y directorios del sistema.

#### **Características únicas:**

- Comprobador de integridad de archivos para detectar cambios no autorizados en los archivos del sistema
- Crea una base de datos de atributos de archivo para compararlos con una línea base
- Opciones de configuración flexibles
- Compatibilidad con varios algoritmos hash

Preinstalado en Kali Purple.

## Lynis

```
Enterprise support and plugins available via CISOfy - http://cisofty.com
#####
[+] Initializing program
-----
- Detecting OS...
- Clearing log file (/var/log/lynis.log)... [ DONE ] [ DONE ]

-----
Program version: 1.6.0
Operating system: Linux
Operating system name: Debian
Operating system version: Kali Linux 1.0.7
Kernel version: 3.14-kali1-686-pae
Hardware platform: i686
Hostname: sideswipe
Auditor: [Unknown]
Profile: ./default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: ./plugins

-----
[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

Lynis es una herramienta de auditoría de seguridad de código abierto que puede evaluar la situación de seguridad de un sistema basado en Linux, macOS o Unix. Realiza un análisis profundo del sistema para identificar posibles vulnerabilidades, configuraciones incorrectas y software desactualizado, y proporciona un informe completo con recomendaciones prácticas para mejorar la seguridad del sistema. Lynis es ampliamente utilizado por administradores de sistemas, profesionales de seguridad y auditores para mantener un entorno seguro y compatible.

Gratis (código abierto)

La amplia gama de controles, los perfiles de escaneo personalizables y los informes detallados de Lynis lo convierten en una herramienta valiosa para mantener un entorno seguro y compatible.

### Características únicas:

- Auditoría de seguridad exhaustiva de sistemas basados en Linux, macOS y Unix
- Identifica posibles vulnerabilidades, configuraciones erróneas y software obsoleto.

- Proporciona recomendaciones prácticas para mejorar la seguridad del sistema.
- Perfiles de escaneo personalizables e informes detallados

Preinstalado en Kali Purple.