



Blog Ethical Hacking Consultores (<https://blog.ehcgroup.io/>)

Encuentra noticias recientes de seguridad.



Cómo usar SearchSploit para encontrar exploits

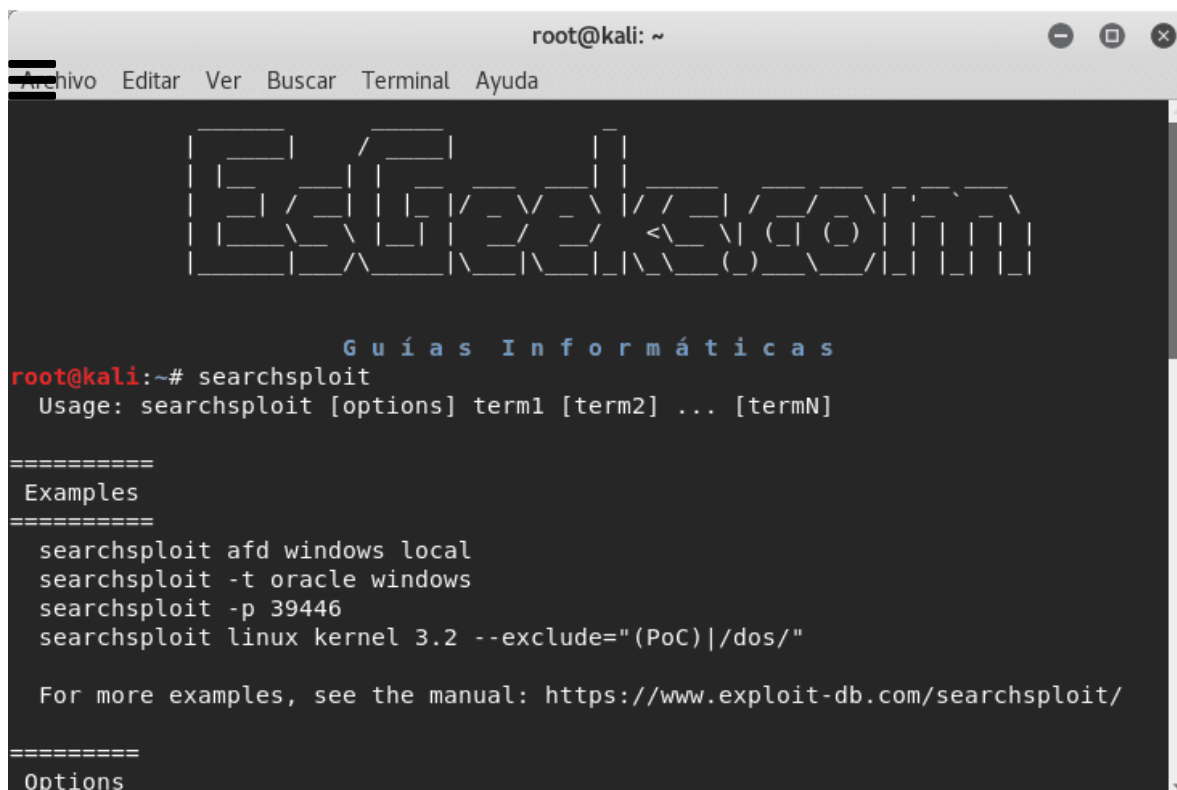
27 noviembre, 2018 (<https://blog.ehcgroup.io/index.php/2018/11/27/como-usar-searchsploit-para-encontrar-exploits/>) / [ehacking](https://blog.ehcgroup.io/index.php/author/ehacking/) (<https://blog.ehcgroup.io/index.php/author/ehacking/>) / [Hacking](https://blog.ehcgroup.io/index.php/category/hacking/) (<https://blog.ehcgroup.io/index.php/category/hacking/>), [Herramientas de Seguridad](https://blog.ehcgroup.io/index.php/category/herramientas-de-seguridad/) (<https://blog.ehcgroup.io/index.php/category/herramientas-de-seguridad/>), [Noticias de Seguridad](https://blog.ehcgroup.io/index.php/category/noticias-de-seguridad/) (<https://blog.ehcgroup.io/index.php/category/noticias-de-seguridad/>), [Noticias EHC](https://blog.ehcgroup.io/index.php/category/noticias-ehc/) (<https://blog.ehcgroup.io/index.php/category/noticias-ehc/>), [Novedades](https://blog.ehcgroup.io/index.php/category/novedades/) (<https://blog.ehcgroup.io/index.php/category/novedades/>), [Seguridad Informática](https://blog.ehcgroup.io/index.php/category/seguridad-informatica/) (<https://blog.ehcgroup.io/index.php/category/seguridad-informatica/>), [Sistemas Operativos](https://blog.ehcgroup.io/index.php/category/sistemas-operativos/) (<https://blog.ehcgroup.io/index.php/category/sistemas-operativos/>), [Vulnerabilidades](https://blog.ehcgroup.io/index.php/category/seguridad-informatica/vulnerabilidades/) (<https://blog.ehcgroup.io/index.php/category/seguridad-informatica/vulnerabilidades/>)



En este artículo vamos a discutir Searchsploit en detalle: Comandos y usos con ejemplos.

Si estás utilizando la versión estándar de Kali Linux, el paquete “exploitdb” ya está incluido de forma predeterminada. Sin embargo, si estás utilizando la variante **Kali Light** o tu propia ISO personalizada, puedes instalar el paquete manualmente de la siguiente manera:

```
apt update && apt -y install exploitdb
```

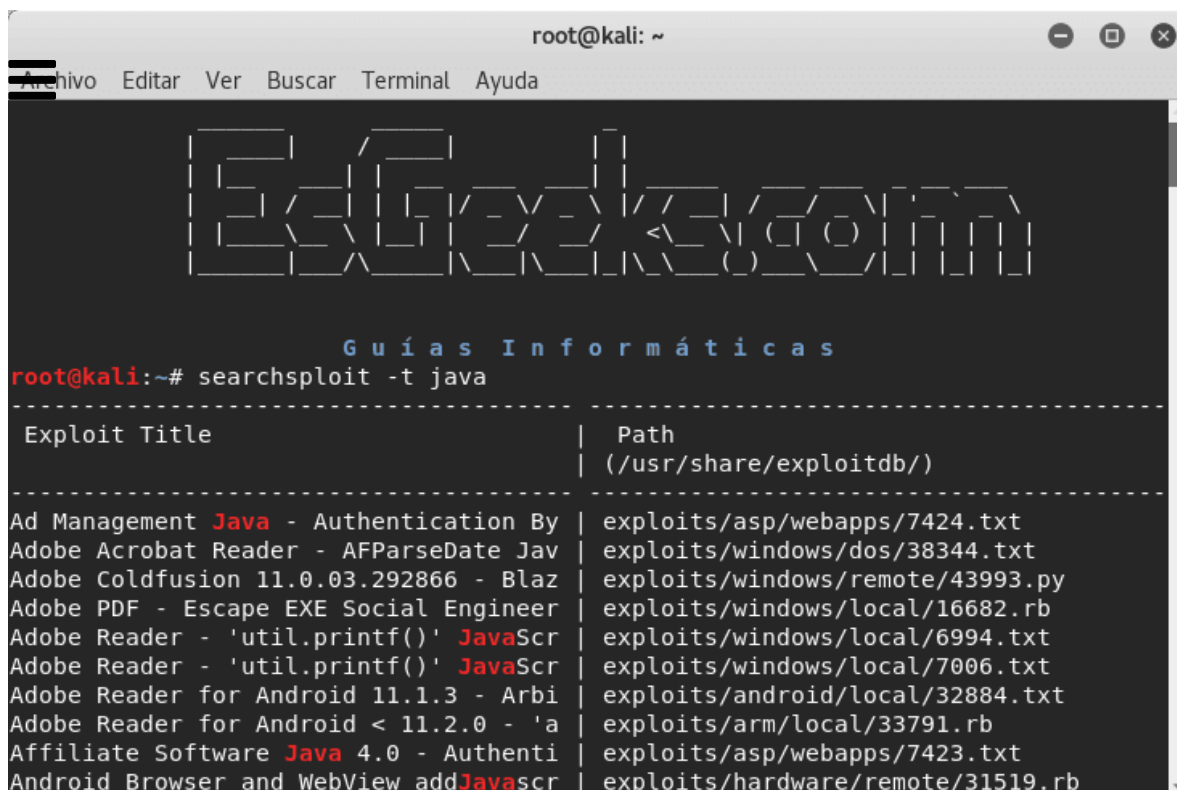
A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal content shows the ASCII art logo for 'Searchsploit', followed by the text 'Guías Informáticas'. Below this, the command 'root@kali:~# searchsploit' is entered, and the usage information is displayed: 'Usage: searchsploit [options] term1 [term2] ... [termN]'. This is followed by a section of examples: 'searchsploit afd windows local', 'searchsploit -t oracle windows', 'searchsploit -p 39446', and 'searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"'. A link to the manual is provided: 'https://www.exploit-db.com/searchsploit/'. The section ends with 'Options'.

Tutorial con Searchsploit

1. Búsqueda de título

El uso de la opción `-t` habilita el parámetro "título" para buscar un exploit con un título específico. Porque por defecto, **searchsploit** intentará tanto el título del exploit como la ruta. La búsqueda de un exploit con un título específico da resultados rápidos y ordenados.

```
searchsploit -t java
```



```
root@kali:~# searchsploit -t java
```

Exploit Title	Path (/usr/share/exploitdb/)
Ad Management Java - Authentication By	exploits/asp/webapps/7424.txt
Adobe Acrobat Reader - AFParseDate Jav	exploits/windows/dos/38344.txt
Adobe Coldfusion 11.0.03.292866 - Blaz	exploits/windows/remote/43993.py
Adobe PDF - Escape EXE Social Engineer	exploits/windows/local/16682.rb
Adobe Reader - 'util.printf()' JavaScr	exploits/windows/local/6994.txt
Adobe Reader - 'util.printf()' JavaScr	exploits/windows/local/7006.txt
Adobe Reader for Android 11.1.3 - Arbi	exploits/android/local/32884.txt
Adobe Reader for Android < 11.2.0 - 'a	exploits/arm/local/33791.rb
Affiliate Software Java 4.0 - Authenti	exploits/asp/webapps/7423.txt
Android Browser and WebView add JavaScr	exploits/hardware/remote/31519.rb

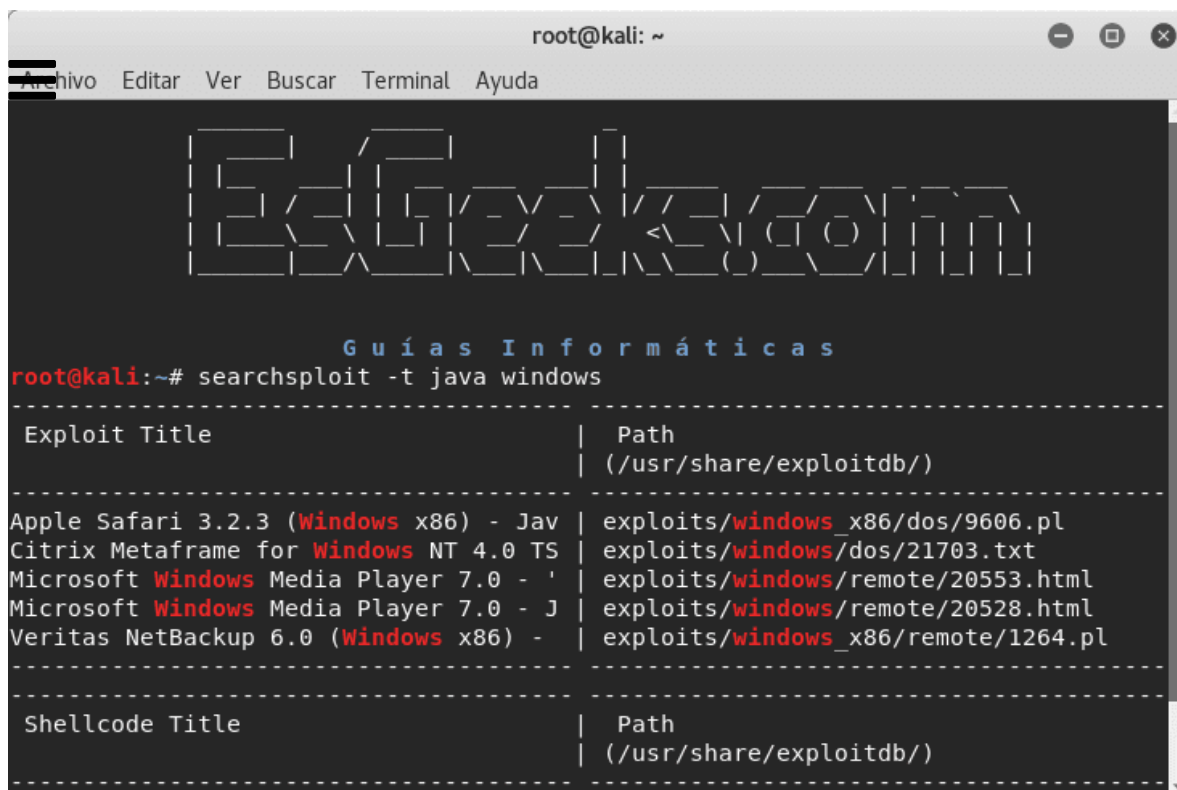
Búsqueda de exploits por título

El comando anterior buscará un exploit relacionado con la plataforma *java* y mostrará todos los exploits disponibles en la base de datos exploit-db.

2. Búsqueda avanzada de títulos

Incluso puede usar la opción `-t`, para obtener un resultado más preciso al encontrar la vulnerabilidad de cualquier plataforma en particular. Por ejemplo, si deseas descubrir el exploit de Java para la plataforma de Windows, puedes considerar el siguiente comando.

```
searchsploit -t java windows
```



```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda

Guías Informáticas
root@kali:~# searchsploit -t java windows

-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Apple Safari 3.2.3 (Windows x86) - Jav | exploits/windows_x86/dos/9606.pl
Citrix Metaframe for Windows NT 4.0 TS | exploits/windows/dos/21703.txt
Microsoft Windows Media Player 7.0 - ' | exploits/windows/remote/20553.html
Microsoft Windows Media Player 7.0 - J | exploits/windows/remote/20528.html
Veritas NetBackup 6.0 (Windows x86) - | exploits/windows_x86/remote/1264.pl
-----

Shellcode Title | Path
                | (/usr/share/exploitdb/)
```

Searchsploit para buscar títulos de exploits

Ahora puedes comparar el resultado de la salida actual con el resultado anterior.

3. Copiar al portapapeles

Al usar la opción `-p`, se muestra la ruta completa de un exploit. Esta opción proporciona más información relacionada con el exploit, así como también copia la ruta completa del exploit al portapapeles, todo lo que se necesitas es presionar las teclas `Ctrl + v` para pegar.

```
searchsploit 39166
searchsploit -p 39166
```

```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
Guías Informáticas  
root@kali:~# searchsploit Linux Kernel 4.3.3  
-----  
Exploit Title | Path  
-----  
| (/usr/share/exploitdb/)  
-----  
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10 | exploits/linux/local/39166.c  
Linux Kernel 4.3.3 - 'overlayfs' Local | exploits/linux/local/39230.c  
-----  
Shellcodes: No Result  
root@kali:~# searchsploit 39166  
-----  
Exploit Title | Path  
-----  
| (/usr/share/exploitdb/)  
-----  
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10 | exploits/linux/local/39166.c  
-----  
Shellcodes: No Result  
root@kali:~# searchsploit -p 39166  
Exploit: Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege  
Escalation (1)  
URL: https://www.exploit-db.com/exploits/39166/  
Path: /usr/share/exploitdb/exploits/linux/local/39166.c  
File Type: C source, ASCII text, with CRLF line terminators  
Copied EDB-ID #39166's path to the clipboard.
```

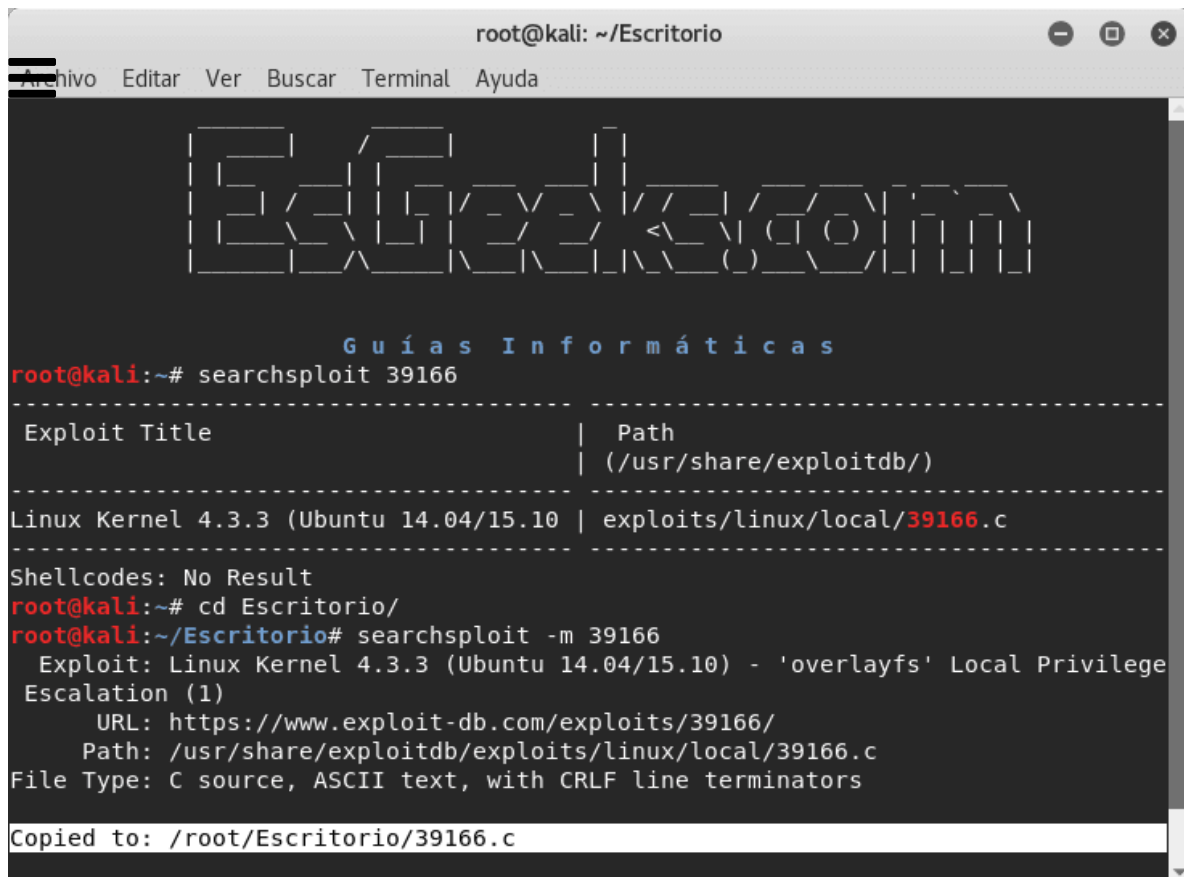
Ruta del exploit con searchsploit

En la siguiente imagen, hemos mostrado que el resultado predeterminado varía cuando usamos la opción `-p`. Por cierto, 39166 es el EDB-ID del título 'Linux Kernel'.

4. Copiar al directorio

La opción `-m` copia un exploit en el directorio de trabajo actual. Esta opción proporciona la misma información que la anterior relacionada con el exploit, pero también copia la vulnerabilidad en tu directorio actual de trabajo.

```
searchsploit 39166  
searchsploit -m 39166
```



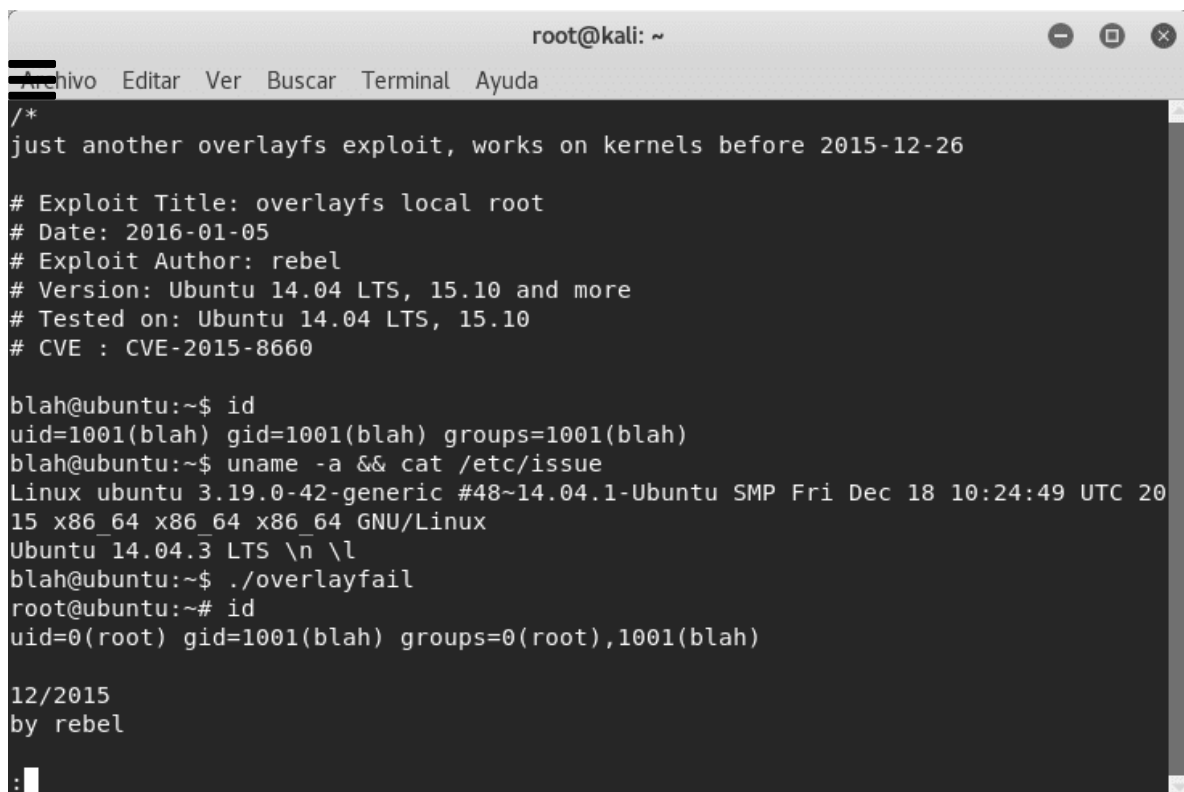
Copiar un exploit a un directorio con Searchsploit

5. Examiner un Exploit

Con la opción `--examine`, se puede leer la funcionalidad de ese exploit con la ayuda de `$PAGER`.

```
searchsploit 39166 --examine
searchsploit -x 39166
```

El comando anterior abrirá el archivo de texto del exploit para revisar su funcionalidad, código y otra información.

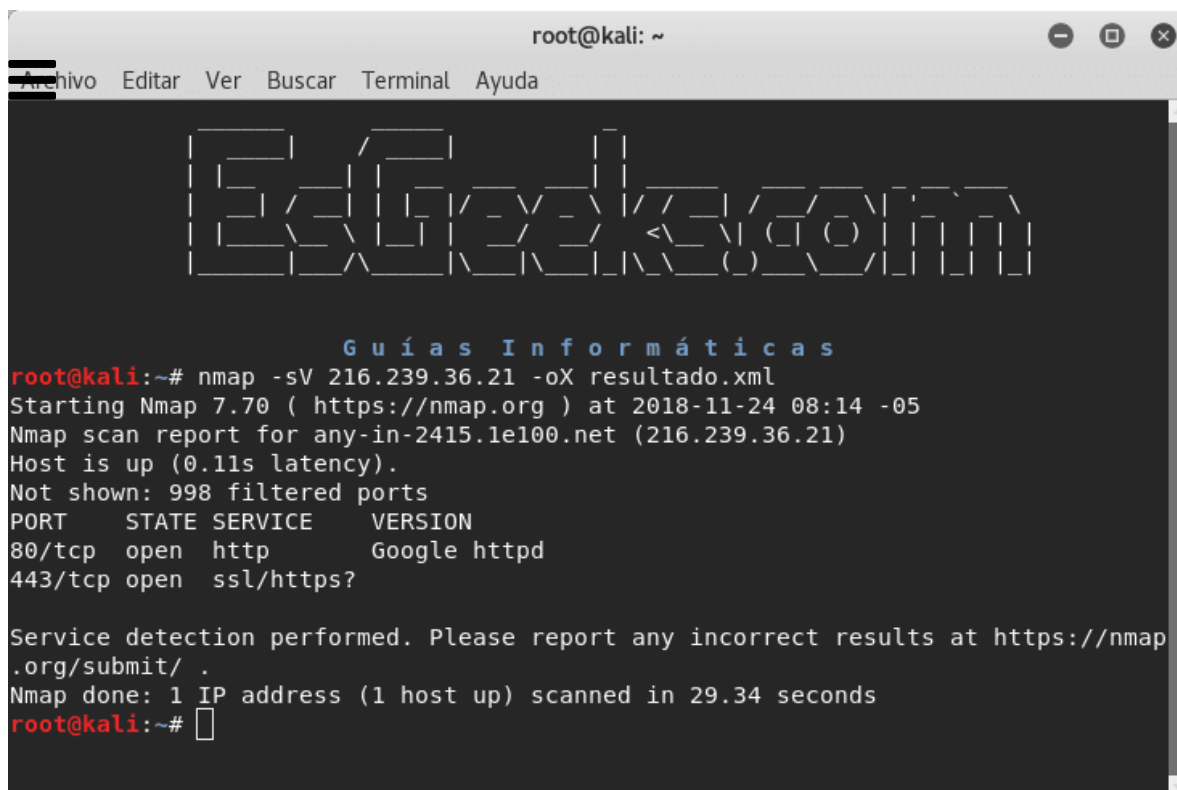
A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal content shows a comment: '/* just another overlayfs exploit, works on kernels before 2015-12-26'. This is followed by metadata: '# Exploit Title: overlayfs local root', '# Date: 2016-01-05', '# Exploit Author: rebel', '# Version: Ubuntu 14.04 LTS, 15.10 and more', '# Tested on: Ubuntu 14.04 LTS, 15.10', and '# CVE : CVE-2015-8660'. Then, a user 'blah' runs 'id' showing they are a regular user. Next, they run 'uname -a && cat /etc/issue' showing system details. Finally, they run './overlayfail', which results in a root shell. The user runs 'id' again, showing they are now root. The script ends with '12/2015' and 'by rebel'.

Examinar un exploit con Searchsploit

6. Examinar un resultado de Nmap

Como todos sabemos, Nmap tiene una característica muy notable que te permite guardar el resultado de salida en formato .xml y podemos identificar cada vulnerabilidad asociada con el archivo xml de nmap.

```
nmap -sV [IP] -oX resultado.xml
```

```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
  
Guías Informáticas  
root@kali:~# nmap -sV 216.239.36.21 -oX resultado.xml  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 08:14 -05  
Nmap scan report for any-in-2415.1e100.net (216.239.36.21)  
Host is up (0.11s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Google httpd  
443/tcp    open  ssl/https?  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 29.34 seconds  
root@kali:~#
```

Guardar resultado Nmap en XML

Con la ayuda del comando anterior, hemos guardado el resultado del escaneo de nmap en un archivo XML, para que podamos buscar el exploit relacionado con los puertos/servicios escaneados.

Usando la opción `-x` podemos examinar y con la opción `-nmap` comprobar todos los resultados en la salida XML de Nmap para averiguar el exploit relacionado con ello.

```
searchsploit -x --nmap resultado.xml
```

Aquí se puede observar que está utilizando el modo detallado para examinar el archivo xml y ha mostrado todas las posibles vulnerabilidades de los servicios en ejecución:

```

root@kali: ~
Archivo  Editor  Ver  Buscar  Terminal  Ayuda

  Guías Informáticas

root@kali:~# searchsploit -x --nmap resultado.xml
[i] SearchSploit's XML mode (without verbose enabled).  To enable: searchsploit
    -v --xml...
[i] Reading: 'resultado.xml'

[i] /usr/bin/searchsploit -t google httpd
[i] /usr/bin/searchsploit -t https
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Apache Tomcat 6.0.16 - 'HttpServletRes | exploits/multiple/remote/32138.txt
BugHunter HTTP Server 1.6.2 - 'httpsv. | exploits/windows/dos/9478.pl
GeoHttpServer - Remote Denial of Servi | exploits/windows/dos/12531.pl
GeoVision (GeoHttpServer) Webcams - Re | exploits/hardware/webapps/37258.py

```

Uso de searchsploit con nmap

7. Exploit-DB en línea

Con la opción `-w`, se muestra la URL de Exploit-DB.com en lugar de la ruta local. En dicho sitio web obtendrás información más detallada, como CVE-ID, archivos de configuración, etiquetas y asignaciones de vulnerabilidad que no se incluyen en **searchsploit**.

```
searchsploit ubuntu 14.04 -w
```

El comando anterior mostrará todos los enlaces disponibles del sitio web de Exploit DB para el exploit relacionado con Ubuntu 14.04.

```

root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Exploit-DB

Guías Informáticas
root@kali:~# searchsploit ubuntu 14.10 -w
-----
Exploit Title | URL
-----
Apport (Ubuntu 14.04/14.10/15.04) | https://www.exploit-db.com/exploits/37088/
Linux Kernel 3.13.0 < 3.19 (Ubuntu | https://www.exploit-db.com/exploits/37292/
Linux Kernel 3.13.0 < 3.19 (Ubuntu | https://www.exploit-db.com/exploits/37293/
usb-creator 0.2.x (Ubuntu 12.04/14 | https://www.exploit-db.com/exploits/36820/
-----
Shellcodes: No Result
root@kali:~# searchsploit ubuntu 14.04 -w
-----
Exploit Title | URL
-----
Apport (Ubuntu 14.04/14.10/15.04) | https://www.exploit-db.com/exploits/37088/

```

searchsploit y Exploit-DB en línea

8. Excluir resultados no deseados

Al usar la opción `--exclude`, se habilita el parámetro de exclusión para eliminar los resultados no deseados dentro de la lista de exploits. También puedes eliminar varios términos separando los términos con un `"|"` (pipe). Esto se puede considerar en lo siguiente:

```

searchsploit ubuntu 14.10 -w
searchsploit ubuntu 14.10 -w --exclude="Linux Kernel"

```

En la siguiente imagen, apreciamos que el resultado predeterminado varía cuando usamos la opción `--exclude`. Incluso puedes eliminar más términos con la ayuda de `"|"` (pipe).


```

root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Guías Informáticas
root@kali:~# searchsploit xss
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Apple macOS HelpViewer 10.12.1 - XSS Le | exploits/macos/remote/41443.html
CA BrightStor ARCserve for Laptops & Des | exploits/windows/remote/16415.rb
CodeIgniter 2.1 - 'xss_clean()' Filter S | exploits/php/webapps/37521.txt
Joomla! Component xstream-dm 0.01b - SQ | exploits/php/webapps/5587.pl
Microsoft AntiXSS 3/4.0 Library Sanitiza | exploits/windows/remote/36507.txt
Microsoft Indexing Service - 'ixsso.dll' | exploits/windows/dos/37673.html
-----
Shellcodes: No Result
root@kali:~# searchsploit -c XSS
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Apple macOS HelpViewer 10.12.1 - XSS Le | exploits/macos/remote/41443.html
Microsoft AntiXSS 3/4.0 Library Sanitiza | exploits/windows/remote/36507.txt
-----
Shellcodes: No Result
root@kali:~#

```

Búsqueda insensitive con searchsploit

Puedes considerar el siguiente ejemplo:

```

searchsploit xss
searchsploit --c XSS

```

Como se puede observar por defecto, muestra todos los exploits disponibles relacionados con xss/XSS, pero en el siguiente comando solo muestra el resultado para XSS.

Espero que este pequeño tutorial te haya sido útil, y que puedas compartir este artículo en tus redes sociales. Saludos :')

Fuente: esgeeks.com (<https://esgeeks.com/searchsploit-para-encontrar-exploits/>)

Please follow and like us:

(<http://twitter.com/share>)

Etiquetado con exploit (<https://blog.ehcgroup.io/index.php/tag/exploit/>), exploits

(<https://blog.ehcgroup.io/index.php/tag/exploits/>), hacking

(<https://blog.ehcgroup.io/index.php/tag/hacking-2/>), herramientas de Seguridad

(<https://blog.ehcgroup.io/index.php/tag/herramientas-de-seguridad-2/>), Java

(<https://blog.ehcgroup.io/index.php/tag/java/>), nmap (<https://blog.ehcgroup.io/index.php/tag/nmap/>),

scripts (<https://blog.ehcgroup.io/index.php/tag/scripts/>), searchsploit

(<https://blog.ehcgroup.io/index.php/tag/searchsploit/>), Ubuntu

(<https://blog.ehcgroup.io/index.php/tag/ubuntu/>), vulnerabilidades

(<https://blog.ehcgroup.io/index.php/tag/vulnerabilidades/>)




Cómo funciona TLS 1.3

(<https://blog.ehcgroup.io/index.php/2018/11/26/como-funciona-tls-1-3/>)

SMWYG: Buscar entre 1.4 billones de credenciales en texto plano

(<https://blog.ehcgroup.io/index.php/2018/11/27/smwyg-buscar-entre-1-4-billones-de-credenciales-en-texto-plano/>)



Creado con WordPress (<http://es.wordpress.org/>) | Tema: Oblique (<http://themeisle.com/themes/oblique/>) por Themeisle.