Máquina Knife HTB Easy

Ping inicial

```
┌──(jouker㉿joukerm)-[~]
└─$ ping 10.10.10.242 -R
PING 10.10.10.242 (10.10.10.242) 56(124) bytes of data.
64 bytes from 10.10.10.242: icmp_seq=1 ttl=63 time=37.4 ms
RR:     10.10.16.5
        10.10.10.2
        10.10.10.242
        10.10.10.242
        10.10.16.1
        10.10.16.5

64 bytes from 10.10.10.242: icmp_seq=2 ttl=63 time=39.3 ms      (same route)
64 bytes from 10.10.10.242: icmp_seq=3 ttl=63 time=40.2 ms      (same route)
64 bytes from 10.10.10.242: icmp_seq=4 ttl=63 time=413 ms       (same route)
64 bytes from 10.10.10.242: icmp_seq=5 ttl=63 time=37.5 ms      (same route)
^C
--- 10.10.10.242 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 37.367/113.461/412.999/149.772 ms
```

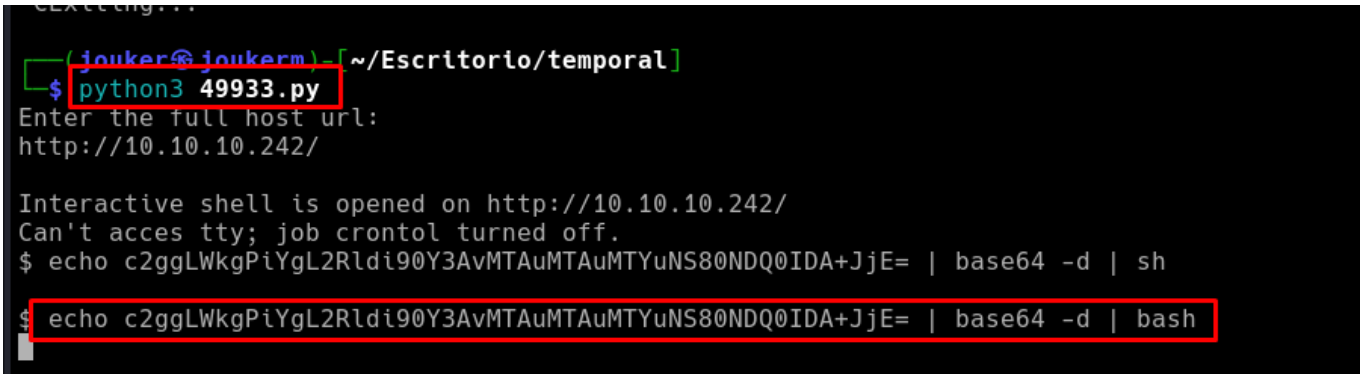
Realización de NMAP:

```
┌──(jouker㉿joukerm)-[~]
└─$ sudo nmap -p- --min-rate 2000 -n -Pn -sV -sC -vvv 10.10.10.242 -oN scan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-22 23:33 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:33
Completed NSE at 23:33, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:33
Completed NSE at 23:33, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:33
Completed NSE at 23:33, 0.00s elapsed
Initiating SYN Stealth Scan at 23:33
Scanning 10.10.10.242 [65535 ports]
Discovered open port 22/tcp on 10.10.10.242
Discovered open port 80/tcp on 10.10.10.242
Increasing send delay for 10.10.10.242 from 0 to 5 due to 181 out of 601 dropped probes since last increase.
Increasing send delay for 10.10.10.242 from 5 to 10 due to 291 out of 969 dropped probes since last increase.
Increasing send delay for 10.10.10.242 from 10 to 20 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.10.242 from 20 to 40 due to max_successful_tryno increase to 5
```

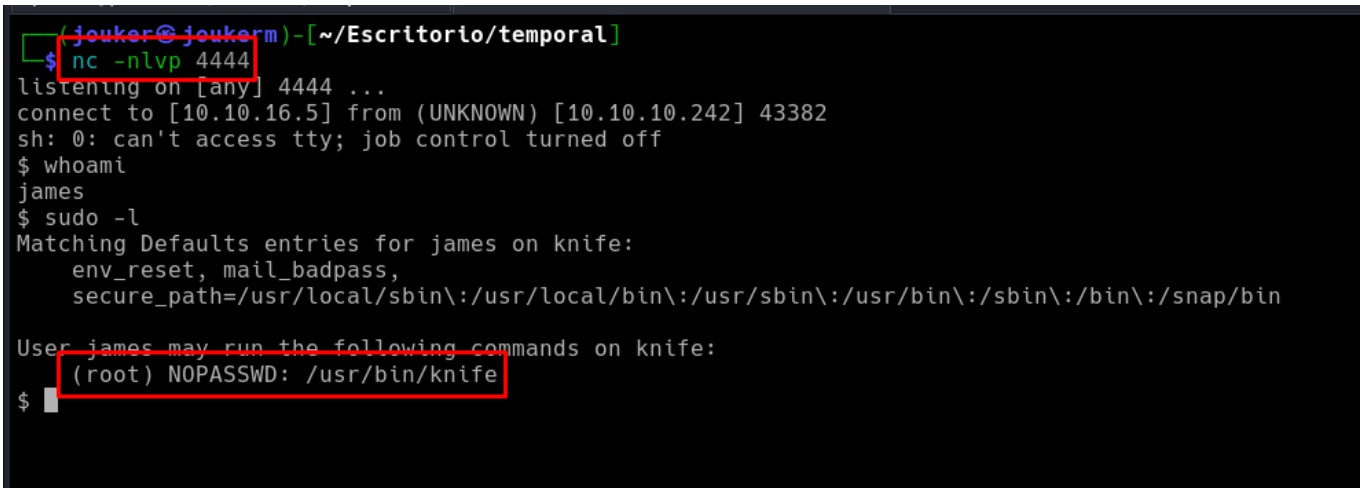
El whatweb nos dice una serie de caracteres, si pasamos la versión de PHP al searchsploit nos marca un exploit a descargar.

```
┌──(jouker㉿joukerm)-[~]
└─$ whatweb 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 Medica
l Idea], X-Powered-By[PHP/8.1.0-dev]
```

Ejecutamos el script, nos crea una shell. La shell no es completamente interactiva por lo que nos la enviamos a traves de netcat y base64

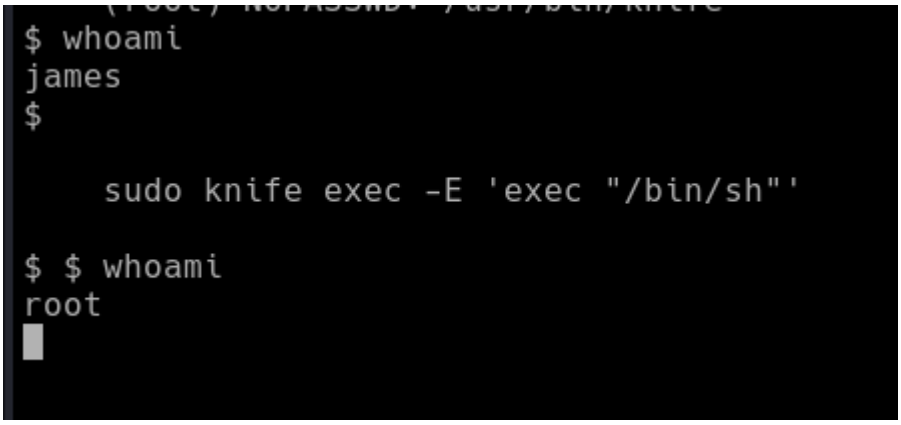


Recibimos la Shell y hacemos tratamiento de la TTY



Miramos knife en GTFOBINS, esta así de simple.

Hacemos la comanda adecuada y somos el usuario root.



Fácil de vd la máquina