0️⃣

HTB writeup - Starting Point tier0

Created By	
Created time	@February 10, 2022 2:13 PM
Last Edited	@February 13, 2022 10:08 PM
Tags	HTB Sec tier0 writeup
Author	
URL	https://app.hackthebox.com/starting-point
Topic	
Property	@February 10, 2022 2:13 PM

::Starting Point
- Setting
  - use pwnbox
  - VPN
  - SSH

Meow - Account Misconfiguration (FTP)
- use nmap -Pn to ping it
- 靶機有時候會不正常
- port 23 is open
- get flag

Fawn - Account Misconfiguration (FTP)
- -F 會址掃描 100個 port
- -Pn assume target is alive
- -T5 最快速度
- get flag
- Dancing
- Tasks
  - What does the 3-letter acronym SMB stand for? → `Server Message Block`
  - What port does SMB use to operate at? → `445` , `137 138 UDP, 139 TCP`
  - What is the service name for port 445 that came up in our nmap scan → `microsoft-ds`
  - What is the tool we use to connect to SMB shares from our Linux distribution? → `smbclient`
  - flag

Explosion (RDP)

::Starting Point

基本上這篇比較像是熟悉 HTB 的使用方式，難度是 very easy，就是基本知識的等級

官方也有附上 writeup

Setting

use pwnbox

不用設定，直接用瀏覽器連到測試環境

也可以在 pwnbox instance 產生後再從 host 用 VNC (or xRDP) 連到到 pwnbox

VPN

use openvpn in your VM or host machine to connect to HTB network

記得用 `sudo`

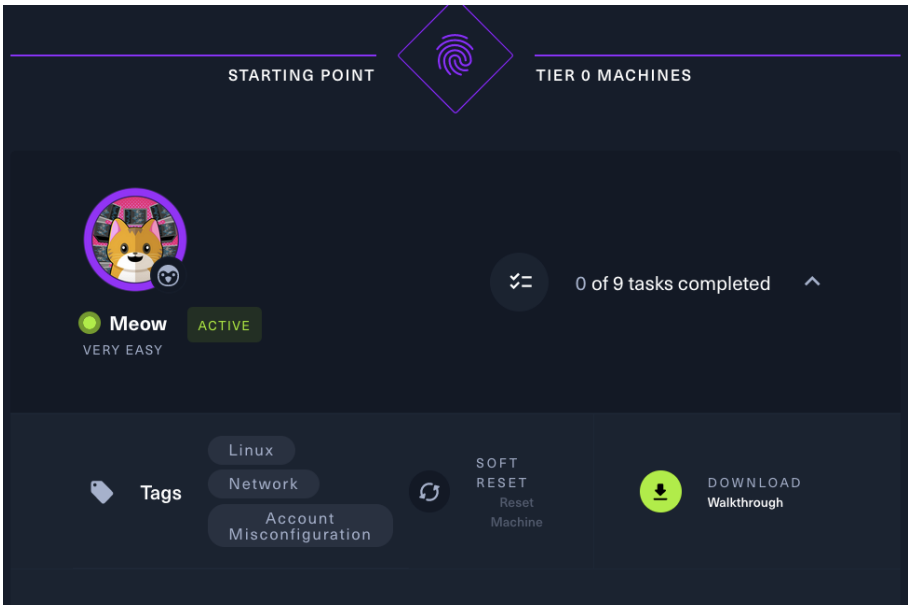
```
sudo openvpn <your-downloaded-openvpn-pack>.ovpn
```

SSH

用他們提供的密碼登入

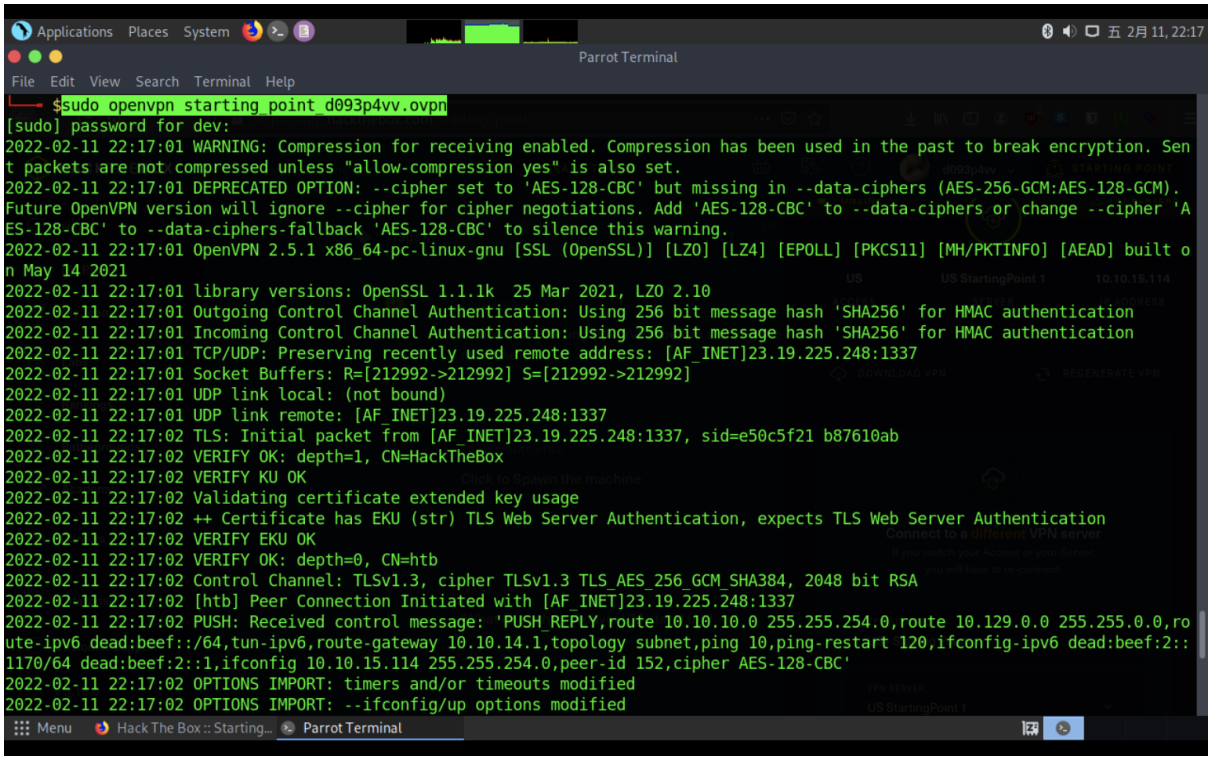
GS: Introduction to Pwnbox | Hack The Box Help Center
https://help.hackthebox.com/en/articles/5185608-gs-introduction-to-pwnbox

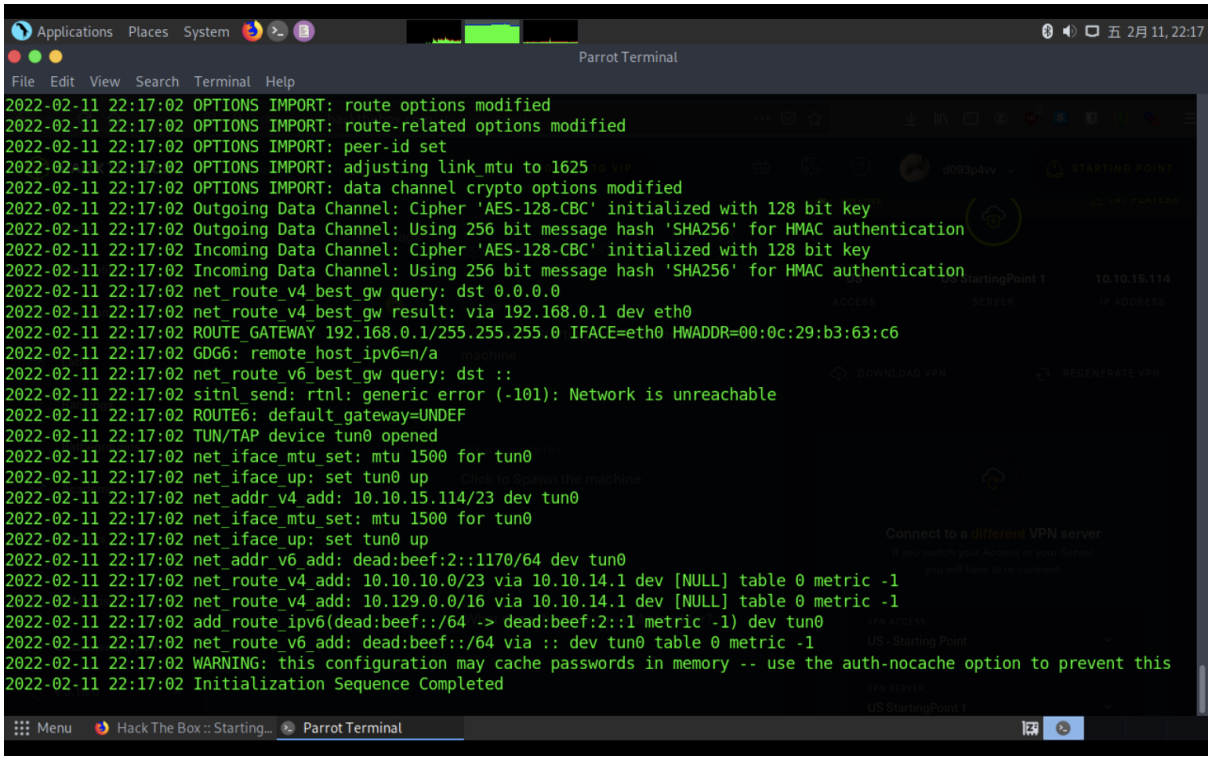
Meow - Account Misconfiguration (FTP)

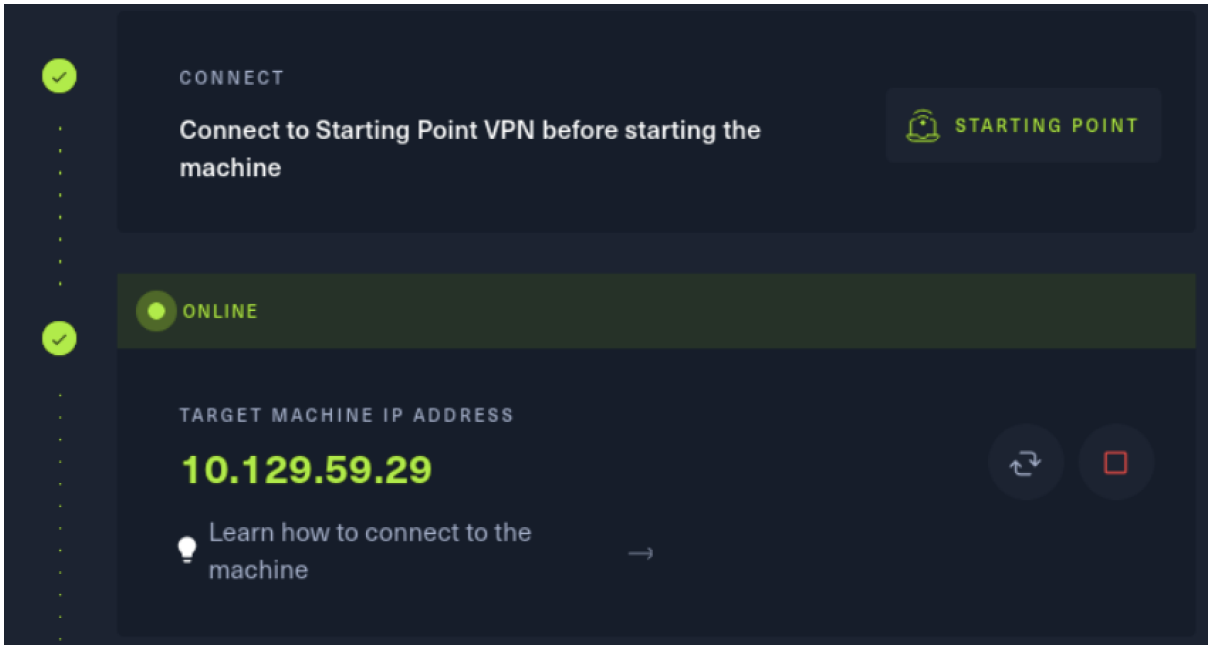


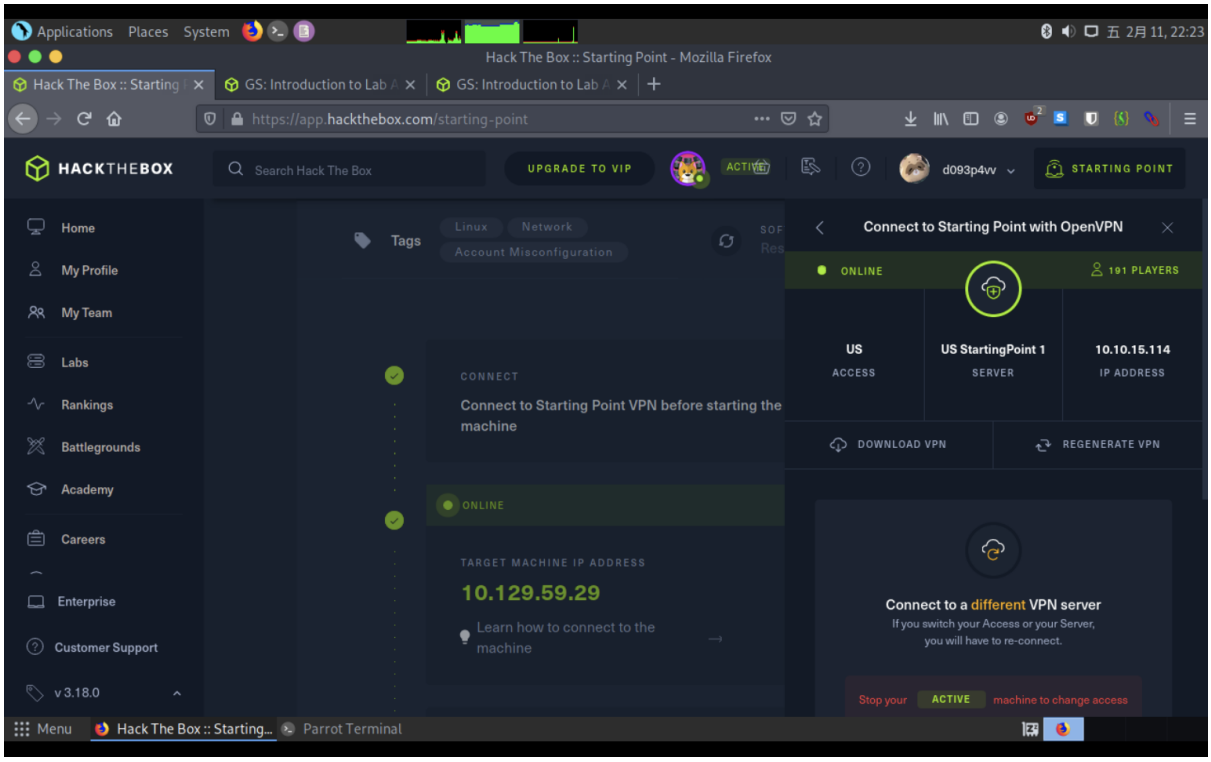
Hack The Box

https://app.hackthebox.com/starting-point

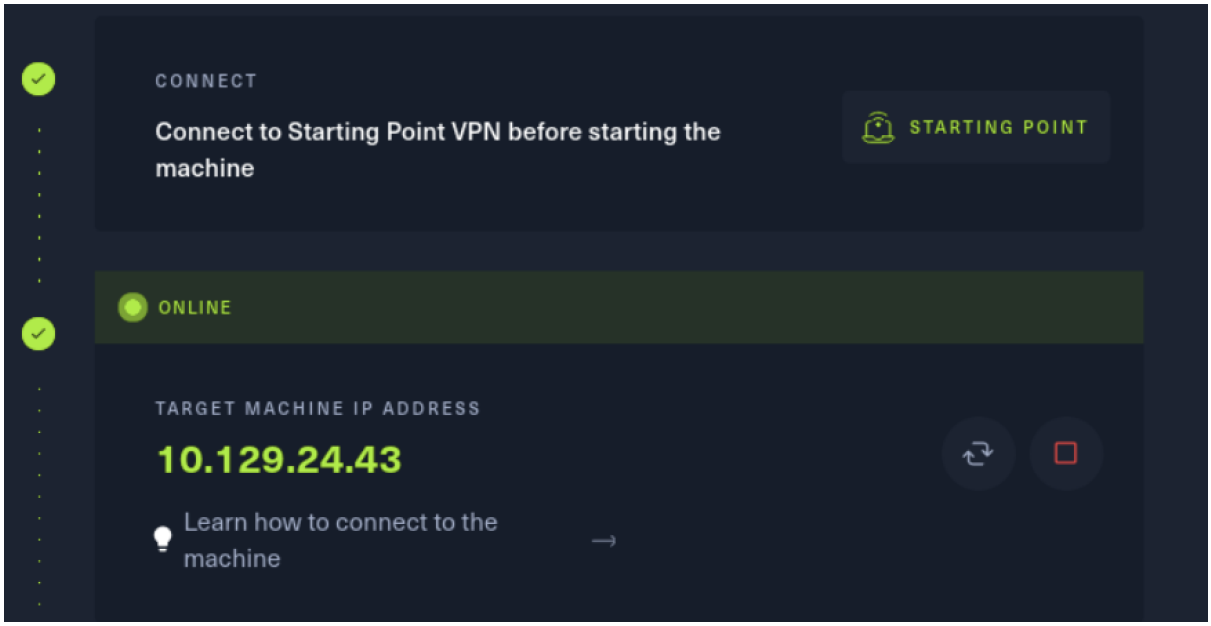

Applications Places System
五 2月 11, 22:17
Parrot Terminal
File Edit View Search Terminal Help
$sudo openvpn starting_point_d093p4vv.ovpn
[sudo] password for dev:
2022-02-11 22:17:01 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2022-02-11 22:17:01 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphers or change --cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warning.
2022-02-11 22:17:01 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2022-02-11 22:17:01 library versions: OpenSSL 1.1.1k 25 Mar 2021, LZO 2.10
2022-02-11 22:17:01 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-11 22:17:01 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-11 22:17:01 TCP/UDP: Preserving recently used remote address: [AF_INET]23.19.225.248:1337
2022-02-11 22:17:01 Socket Buffers: R=[212992->212992] S=[212992->212992]
2022-02-11 22:17:01 UDP link local: (not bound)
2022-02-11 22:17:01 UDP link remote: [AF_INET]23.19.225.248:1337
2022-02-11 22:17:02 TLS: Initial packet from [AF_INET]23.19.225.248:1337, sid=e50c5f21 b87610ab
2022-02-11 22:17:02 VERIFY OK: depth=1, CN=HackTheBox
2022-02-11 22:17:02 VERIFY KU OK
2022-02-11 22:17:02 Validating certificate extended key usage
2022-02-11 22:17:02 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2022-02-11 22:17:02 VERIFY EKU OK
2022-02-11 22:17:02 VERIFY OK: depth=0, CN=htb
2022-02-11 22:17:02 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2022-02-11 22:17:02 [htb] Peer Connection Initiated with [AF_INET]23.19.225.248:1337
2022-02-11 22:17:02 PUSH: Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-ipv6 dead:beef::/64,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::1170/64 dead:beef:2::1,ifconfig 10.10.15.114 255.255.254.0,peer-id 152,cipher AES-128-CBC'
2022-02-11 22:17:02 OPTIONS IMPORT: timers and/or timeouts modified
2022-02-11 22:17:02 OPTIONS IMPORT: --ifconfig/up options modified
Menu
Hack The Box :: Starting...
Parrot Terminal


Applications Places System
五 2月 11, 22:17
Parrot Terminal
File Edit View Search Terminal Help
2022-02-11 22:17:02 OPTIONS IMPORT: route options modified
2022-02-11 22:17:02 OPTIONS IMPORT: route-related options modified
2022-02-11 22:17:02 OPTIONS IMPORT: peer-id set
2022-02-11 22:17:02 OPTIONS IMPORT: adjusting link_mtu to 1625
2022-02-11 22:17:02 OPTIONS IMPORT: data channel crypto options modified
2022-02-11 22:17:02 Outgoing Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
2022-02-11 22:17:02 Outgoing Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-11 22:17:02 Incoming Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
2022-02-11 22:17:02 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-11 22:17:02 net_route_v4_best_gw query: dst 0.0.0.0
2022-02-11 22:17:02 net_route_v4_best_gw result: via 192.168.0.1 dev eth0
2022-02-11 22:17:02 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:b3:63:c6
2022-02-11 22:17:02 GDG6: remote_host_ipv6=n/a
2022-02-11 22:17:02 net_route_v6_best_gw query: dst ::
2022-02-11 22:17:02 sitnl_send: rtnl: generic error (-101): Network is unreachable
2022-02-11 22:17:02 ROUTE6: default_gateway=UNDEF
2022-02-11 22:17:02 TUN/TAP device tun0 opened
2022-02-11 22:17:02 net_iface_mtu_set: mtu 1500 for tun0
2022-02-11 22:17:02 net_iface_up: set tun0 up
2022-02-11 22:17:02 net_addr_v4_add: 10.10.15.114/23 dev tun0
2022-02-11 22:17:02 net_iface_mtu_set: mtu 1500 for tun0
2022-02-11 22:17:02 net_iface_up: set tun0 up
2022-02-11 22:17:02 net_addr_v6_add: dead:beef:2::1170/64 dev tun0
2022-02-11 22:17:02 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
2022-02-11 22:17:02 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2022-02-11 22:17:02 add_route_ipv6(dead:beef::/64 -> dead:beef:2::1 metric -1) dev tun0
2022-02-11 22:17:02 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2022-02-11 22:17:02 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2022-02-11 22:17:02 Initialization Sequence Completed
Menu
Hack The Box :: Starting...
Parrot Terminal

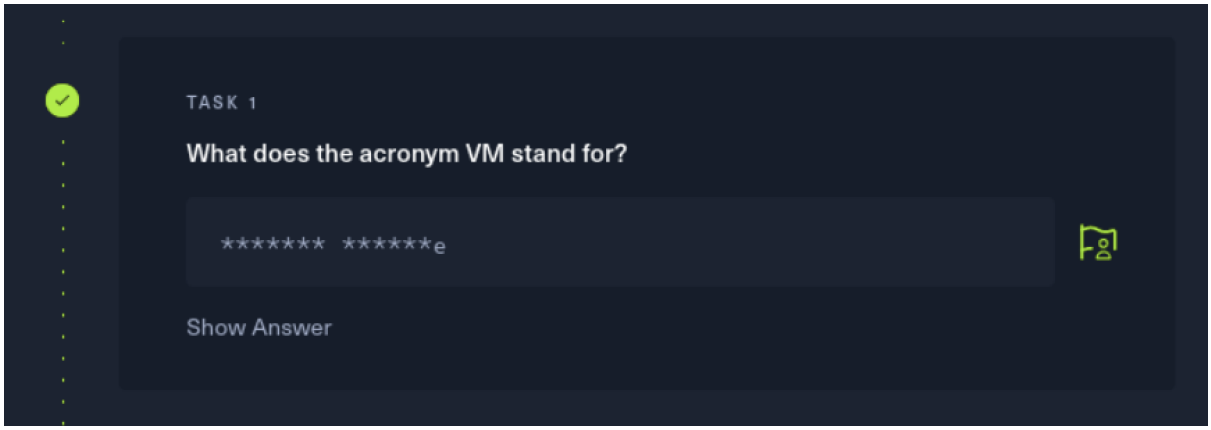


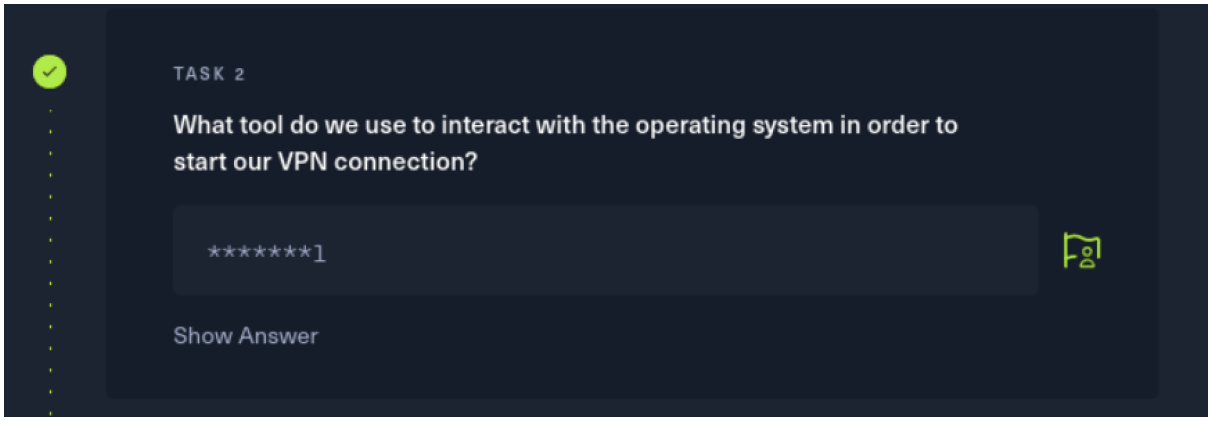


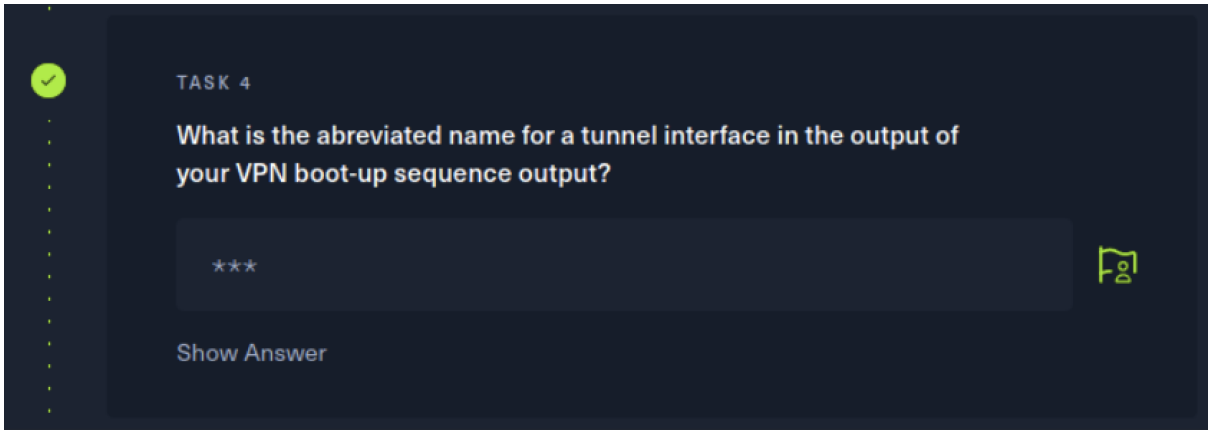
好像出了些問題，無法繼續下一關，所以重來一次．就可以繼續回答接下來的問題了，這關只是確認你會用 openvpn or pwnbox 連線，還有回答一些基本問題而已


CONNECT
Connect to Starting Point VPN before starting the machine
STARTING POINT
ONLINE
TARGET MACHINE IP ADDRESS
10.129.24.43
Learn how to connect to the machine

```
10.129.24.43
```

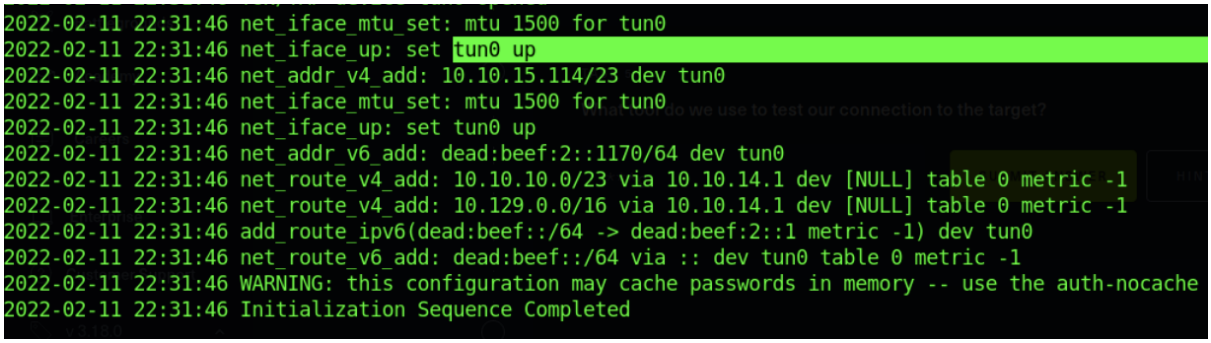

TASK 1
What does the acronym VM stand for?
******* ******e
Show Answer


TASK 2
What tool do we use to interact with the operating system in order to start our VPN connection?
*******l
Show Answer

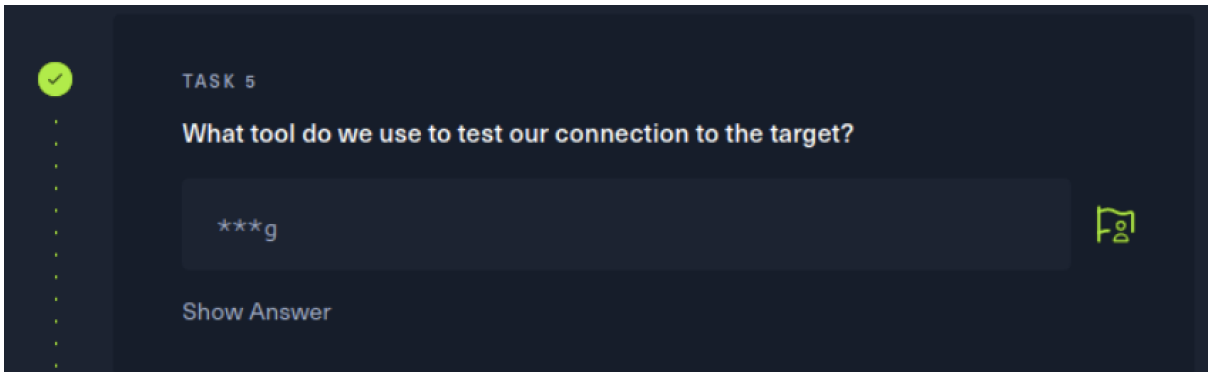


openvpn network interface 通常都是 tun開頭，e.g `tun0`, `tun1`

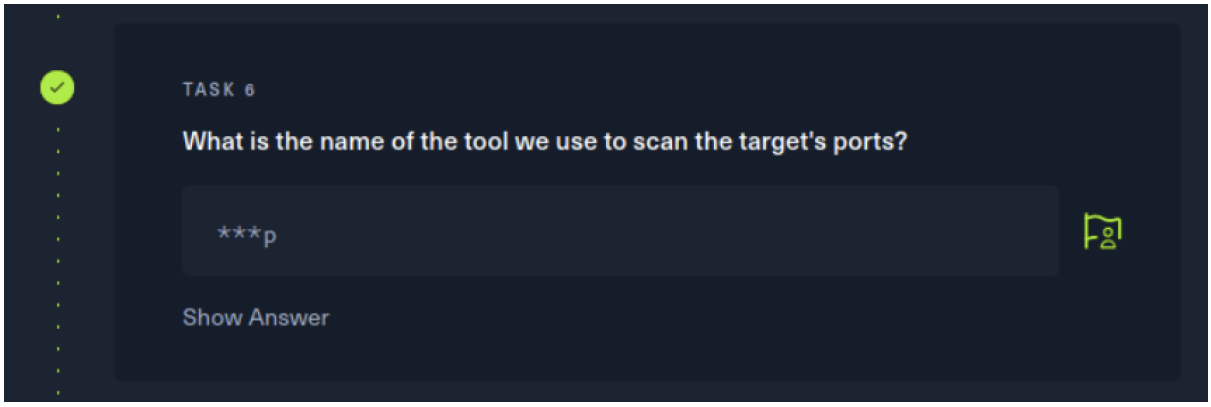
```
tun
```



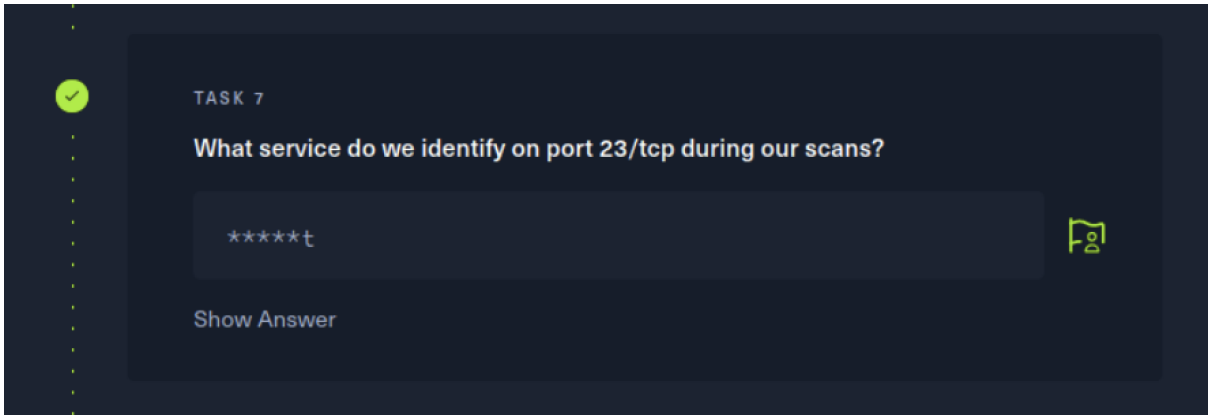
接下來是一連串的小 task，這邊都是常識題



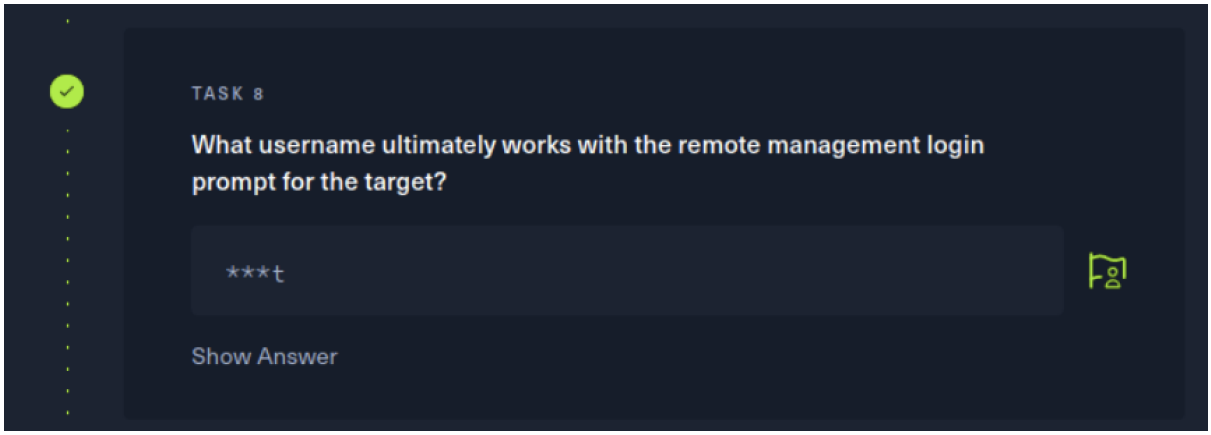

```
ping
```


TASK 6
What is the name of the tool we use to scan the target's ports?
***p
Show Answer

```
nmap
```


TASK 7
What service do we identify on port 23/tcp during our scans?
******t
Show Answer

```
telnet
```

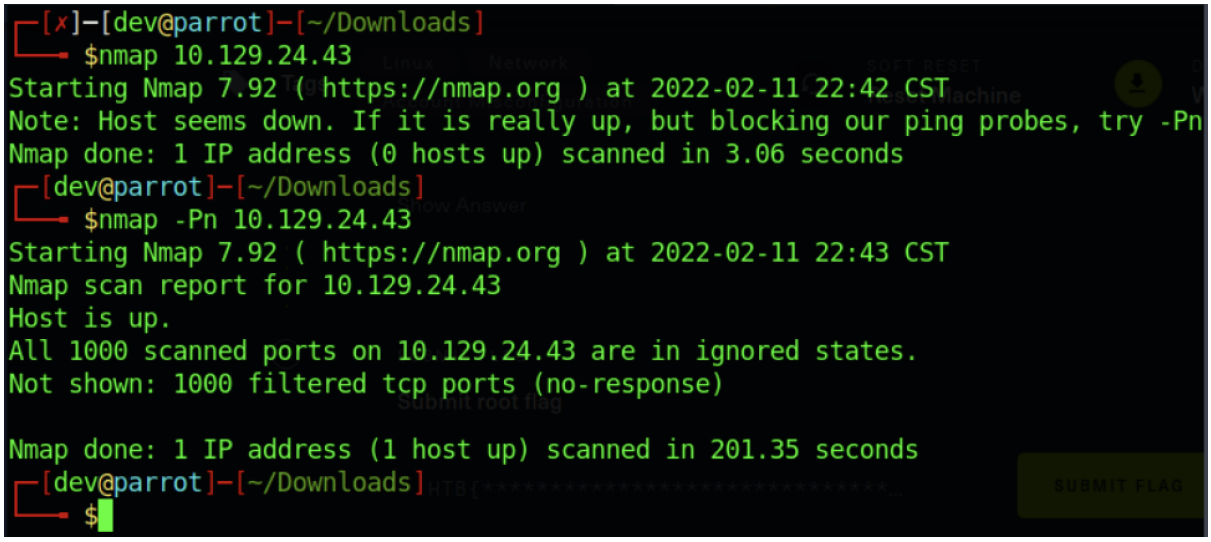



```
root
```

最後一個 task 就是暗示你用 telnet 連進靶機，取得 flag

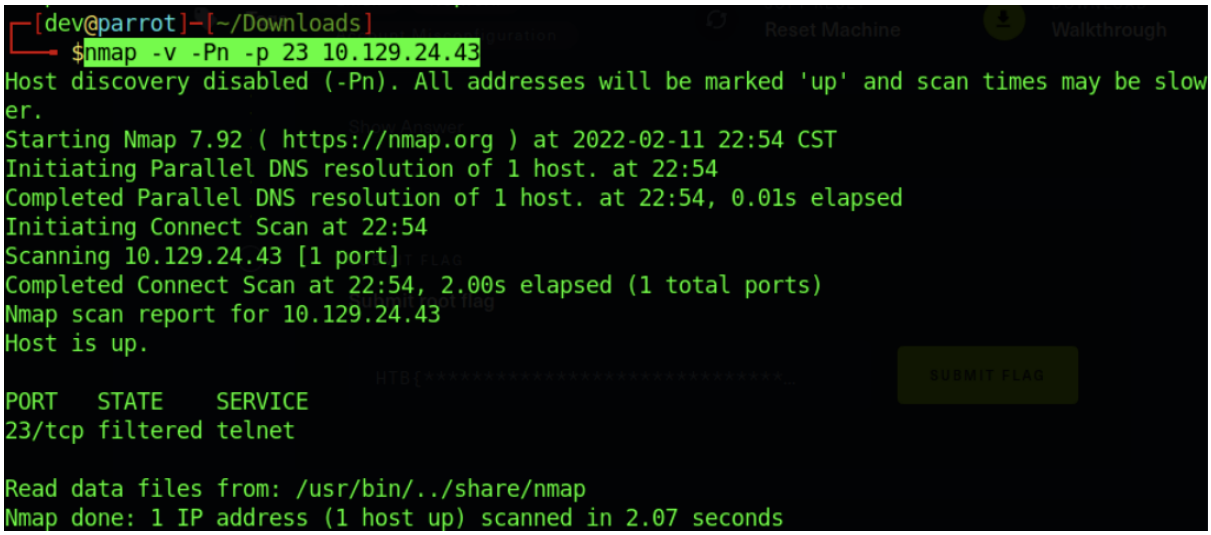
use nmap -Pn to ping it

```
nmap -Pn 10.129.24.43
```



看起來機器活著，那接下來是著 test port 23

```
nmap -v -Pn -p 23 10.129.24.43
```



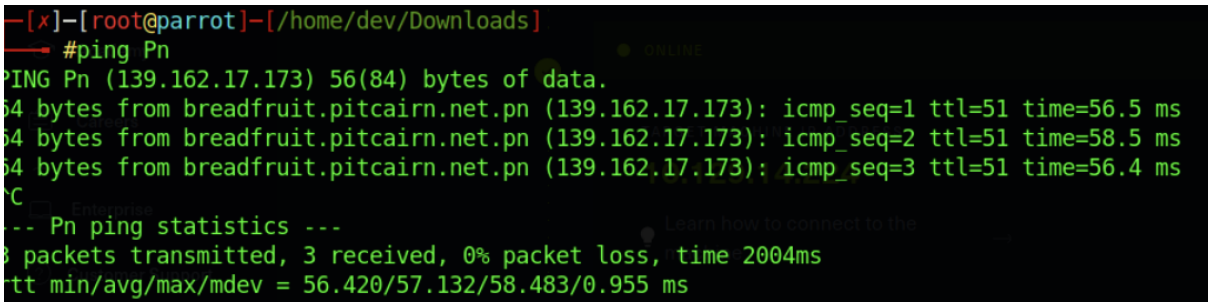
靶機有時候會不正常

不過後來發現怪怪的，因為所有 port 都是 filterd，reset 靶機和重新連線也無效，最後切換成歐洲的線路，靶機才正常運作 QQ

現在恢復正常了...

疑 等等 有點奇怪，我忘了加 `-` 在 `Pn` 前面，所以 nmap 掃描的主機是一台叫 `Pn` 的 server @@

```
nmap -v Pn 10.129.14.224
```



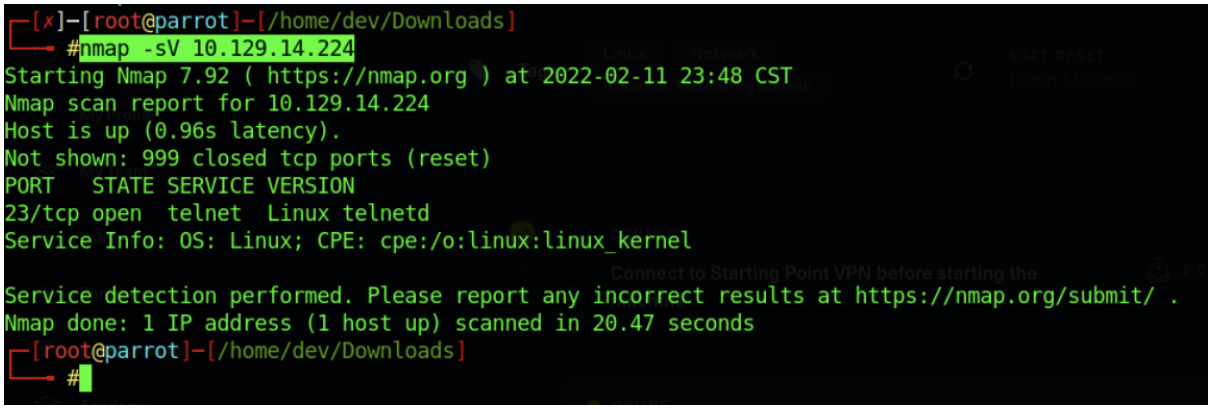
拍照留念一下

繼續回來練習

```
nmap -v -Pn 10.129.14.224
```

port 23 is open

```
nmap -sV 10.129.14.224
```




```
telnet 10.129.14.224
```

用 telenet 連線，直接用 root 登入不用密碼

```
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 11 Feb 2022 04:11:32 PM UTC

  System load:           0.02
  Usage of /:            41.7% of 7.75GB
  Memory usage:          4%
  Swap usage:            0%
  Processes:             135
  Users logged in:       0
  IPv4 address for eth0: 10.129.14.224
  IPv6 address for eth0: dead:beef::250:56ff:feb9:92f7

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~#
```

```
root@Meow:~# uname -a
Linux Meow 5.4.0-77-generic #86-Ubuntu SMP Thu Jun 17 02:35:03 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
root@Meow:~#
```

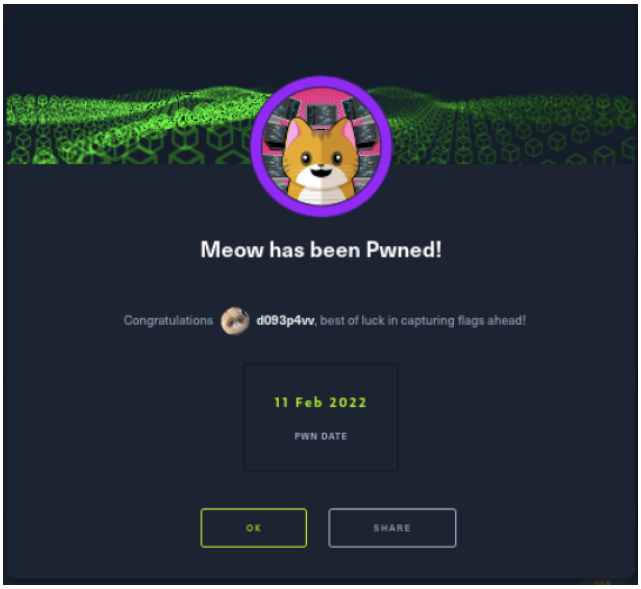
```
root@Meow:~# ll
total 36
drwx------  5 root root 4096 Jun 18  2021 ./
drwxr-xr-x 20 root root 4096 Jul  7  2021 ../
lrwxrwxrwx  1 root root    9 Jun  4  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3132 Oct  6  2020 .bashrc
drwx------  2 root root 4096 Apr 21  2021 .cache/
-rw-r--r--  1 root root   33 Jun 17  2021 flag.txt
drwxr-xr-x  3 root root 4096 Apr 21  2021 .local/
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r--r--  1 root root   75 Mar 26  2021 .selected_editor
drwxr-xr-x  3 root root 4096 Apr 21  2021 snap/
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~#
```

get flag

```
b40abdfe23665f766f9c61ecba8a4c19
```

提交時要用加上 `HTB{...}` 在外面

```
HTB{b40abdfe23665f766f9c61ecba8a4c19}
```



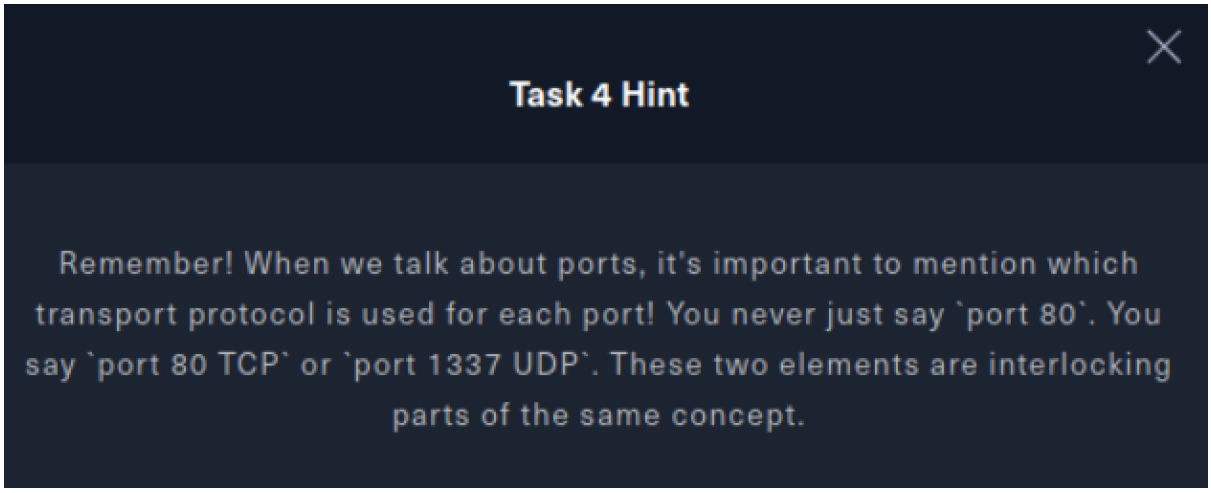
https://www.hackthebox.com/achievement/machine/929350/394

Fawn - Account Misconfiguration (FTP)

這題單純讓你練習 FTP

```
10.129.200.227
```

有一些常識題，可以幫你複習一些知識，因為太基礎，有些 task 就不做紀錄

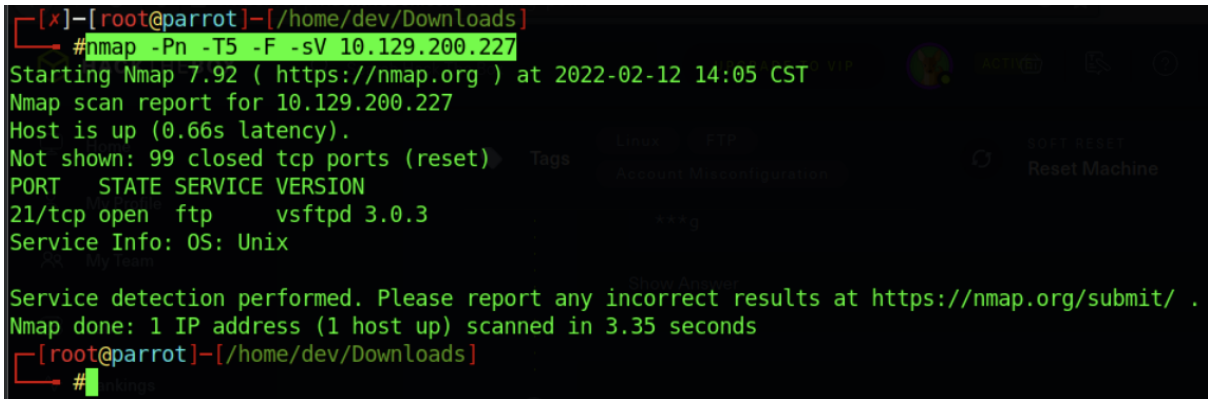


確認靶機 FTP version，用 `-sV` (scan port and service) scan 就可以看出來

答案是 `ftp vsftpd 3.0.3`


```
nmap -Pn -T5 -F -sV 10.129.200.227
```

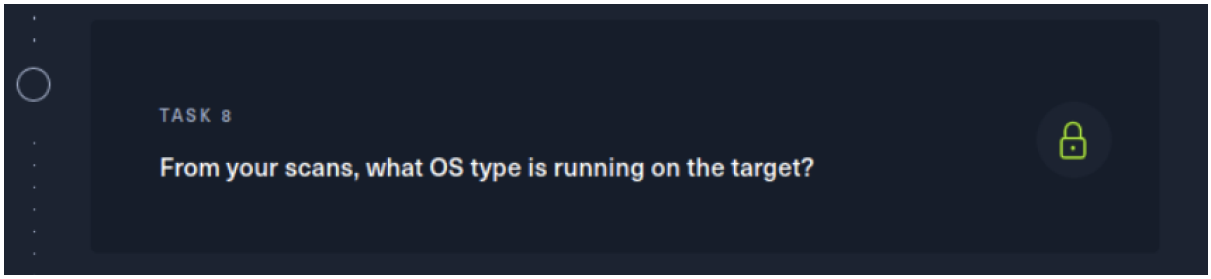
```
nmap -Pn -T5 -p21 -sV 10.129.200.227
```



```
21/tcp open  ftp vsftpd 3.0.3
Service Info: OS: Unix
```

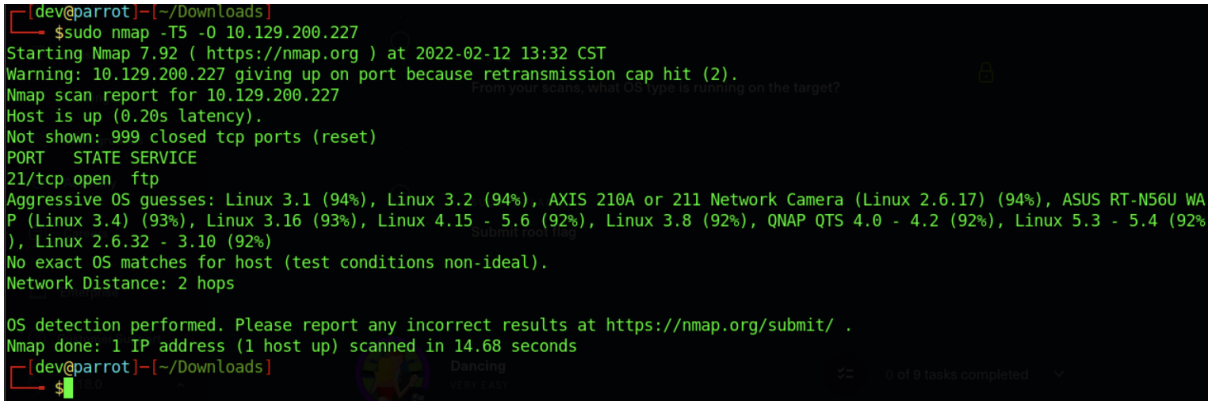
找出 OS type，用 nmap scan 即可

答案是 `Unix`




```
sudo nmap -T4 -A 10.129.200.227
```

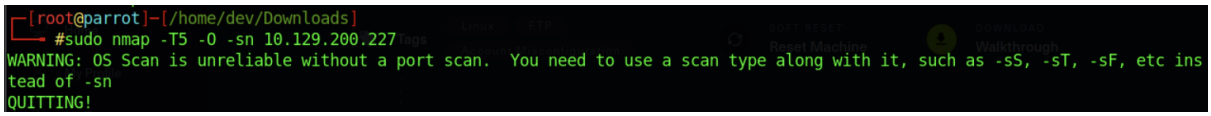
```
sudo nmap -T5 -O 10.129.200.227
```



可以看出是 Linux

可以趁機熟悉一下 nmap 預設的行為，例如 我只想 fingerprint OS，但不想掃 port

但沒辦法，因為 port scan 是它用來判斷 OS 的方式之一

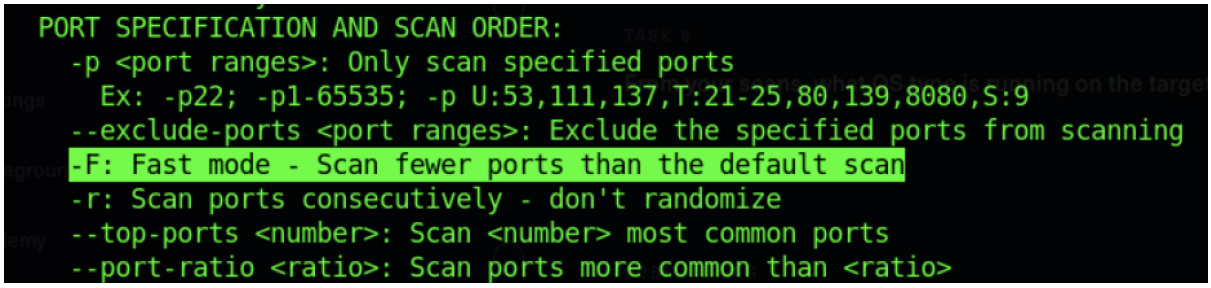


在你很了解環境的情況下，可以用 `-F -Pn -T5` 來減少不必要的掃描和加快速度

-F 會址掃描 100個 port

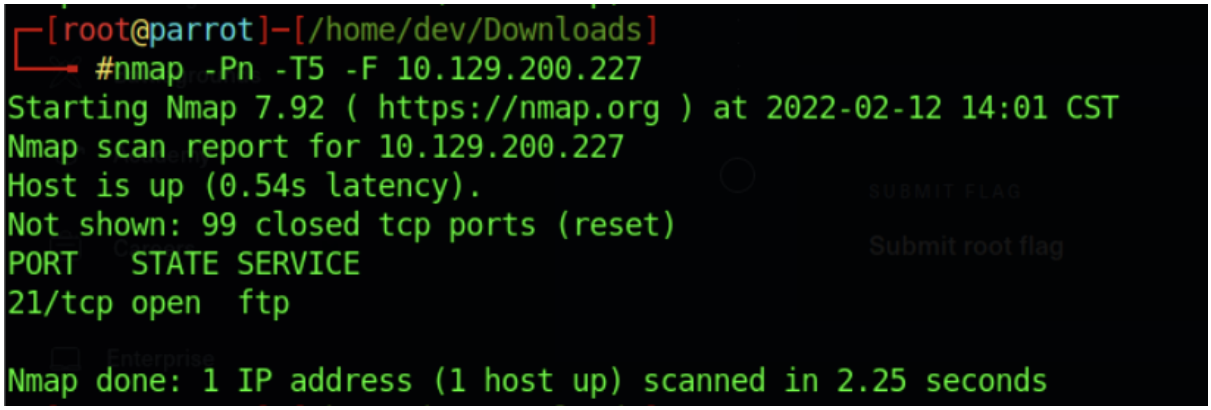
-Pn assume target is alive

-T5 最快速度



不猜測 OS 的話，scan 100 ports 約 2~2 秒

```
nmap -Pn -T5 -F 10.129.200.227
```



加上 guess OS 約 9~15 秒

```
nmap -Pn -T5 -F -O 10.129.200.227
```

```
┌──[root@parrot]─[/home/dev/Downloads]
└─── #nmap -Pn -T5 -F -O 10.129.200.227
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 14:02 CST
Nmap scan report for 10.129.200.227
Host is up (0.20s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.3 (95%), Linux 3.1 (94
%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%
), Linux 5.0 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.90 seconds
```

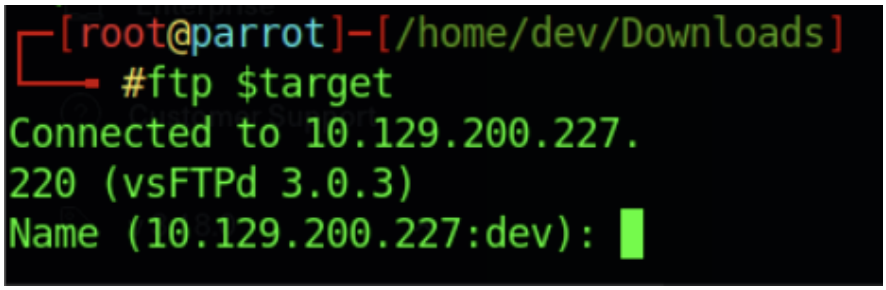
get flag

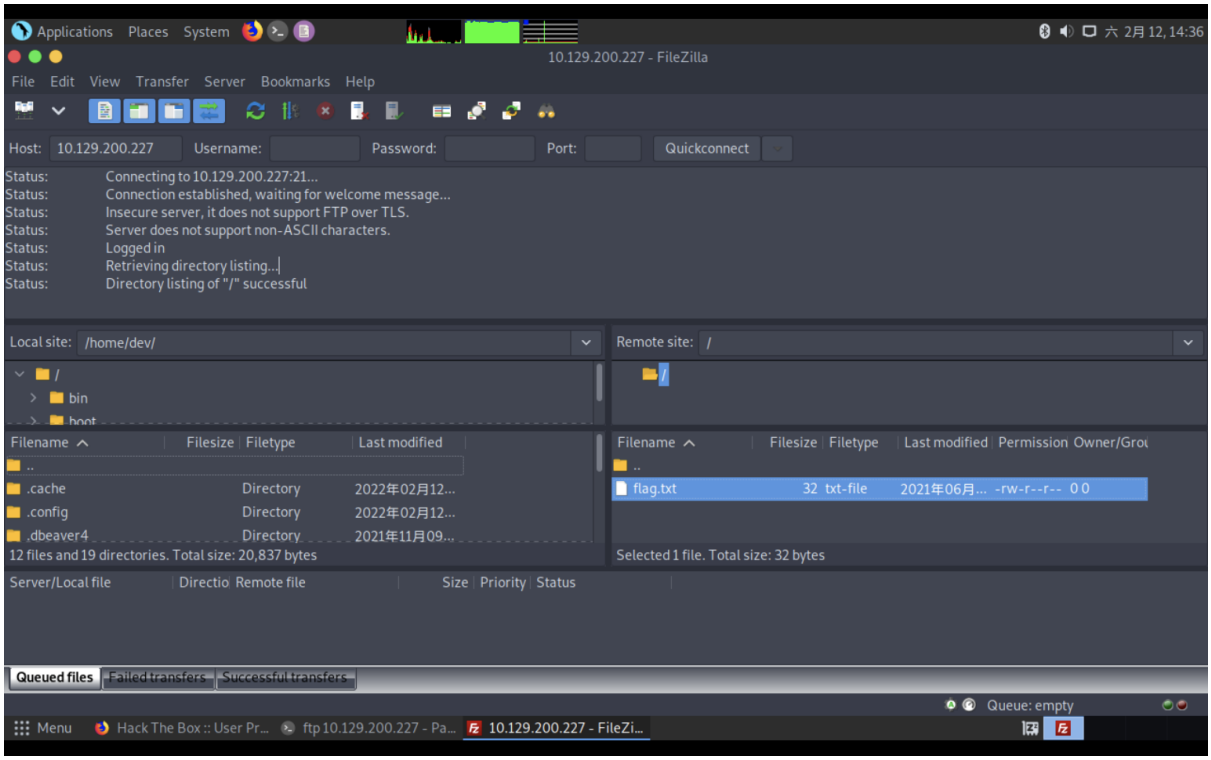
```
sudo apt install ftp -y
ftp $target
```

用 ftp 指令需要輸入帳密，沒什麼頭緒，後來改用 filezilla 就順定進去了 @@，因為前面有暗示 filezilla 這套 ftp app

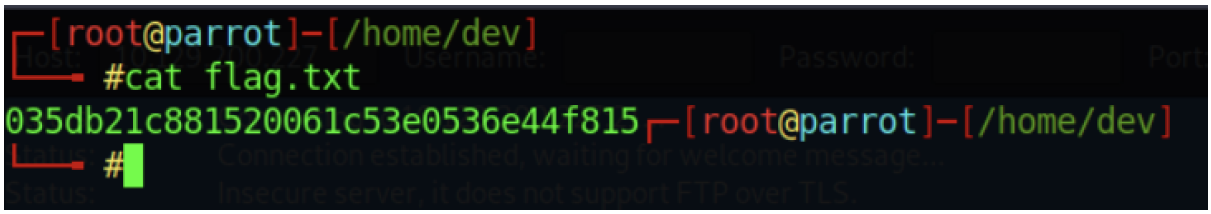
```
sudo apt install filezilla -y
```

```
ftp -v -p -n 10.129.187.227
```

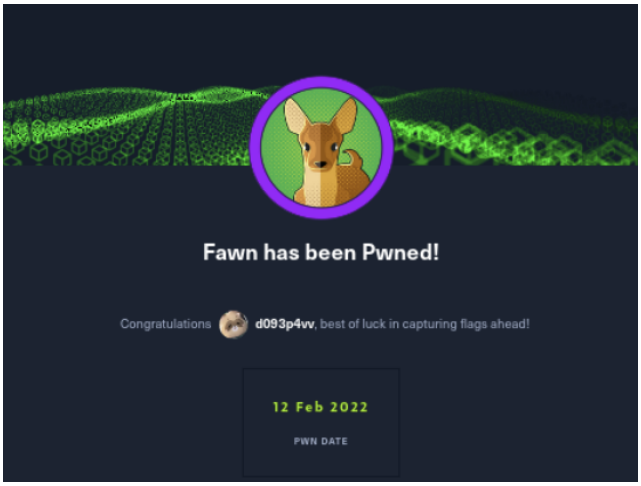





```
Status: Connecting to 10.129.200.227:21...
Status: Connection established, waiting for welcome message...
Status: Insecure server, it does not support FTP over TLS.
Status: Server does not support non-ASCII characters.
Status: Logged in
Status: Retrieving directory listing...
Status: Directory listing of "/" successful
Status: Connecting to 10.129.200.227:21...
Status: Connection established, waiting for welcome message...
Status: Insecure server, it does not support FTP over TLS.
Status: Server does not support non-ASCII characters.
Status: Logged in
Status: Starting download of /flag.txt
Status: File transfer successful, transferred 32 bytes in 1 second
Status: Disconnected from server
Status: Connection closed by server
```




```
035db21c881520061c53e0536e44f815
```



https://www.hackthebox.com/achievement/machine/929350/393

Dancing

Windows SMB 題

SMB runs at the Application or Presentation layers of the OSI model,

The Transport layer protocol that Microsoft SMB Protocol is most often used with is NetBIOS over TCP/IP (NBT). This is why, during scans, we will most likely see both protocols with open ports running on the target.

```
10.129.112.127
```

Tasks

What does the 3-letter acronym SMB stand for? → `Server Message Block`

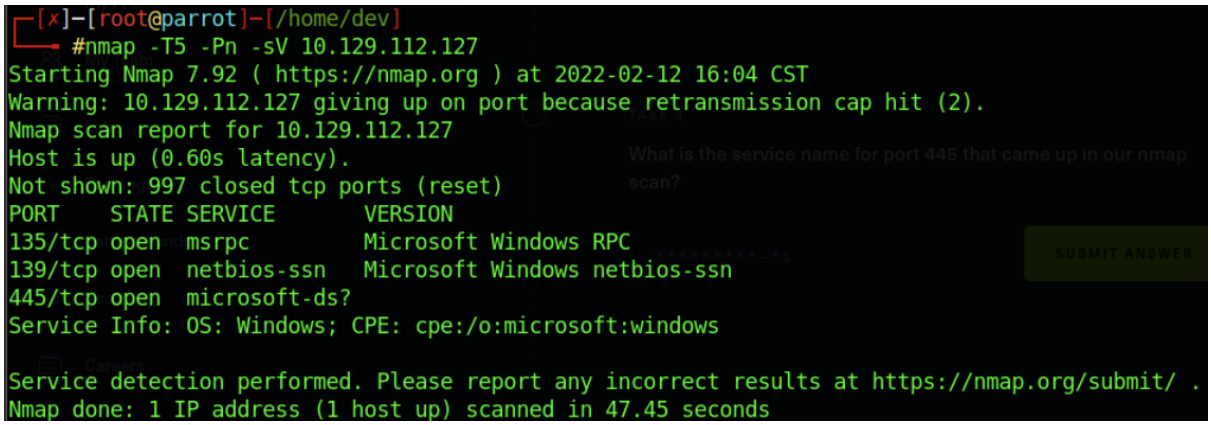
What port does SMB use to operate at? → `445` , `137 138 UDP, 139 TCP`

Windows: `445`

for communicate with Non-Windows (NetBIOS Name Service): `137 138 UDP, 139 TCP`

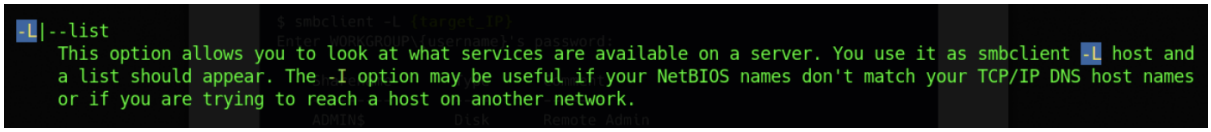
What is the service name for port 445 that came up in our nmap scan → `microsoft-ds`

```
nmap -T5 -Pn -sV 10.129.112.127
```

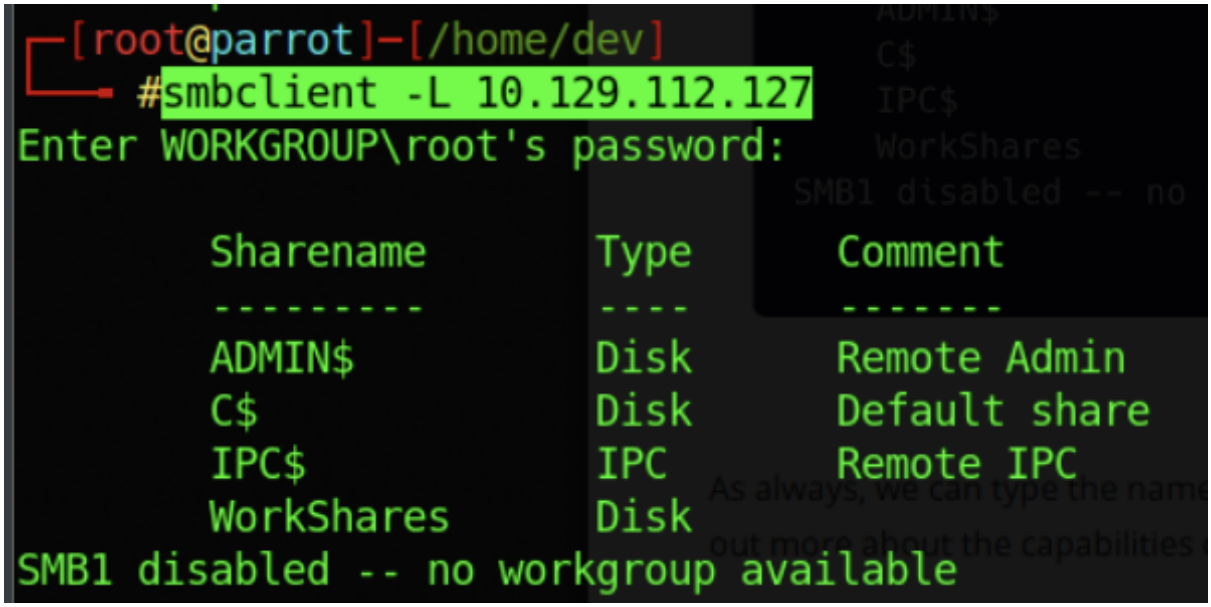


What is the tool we use to connect to SMB shares from our Linux distribution? → `smbclient`

```
smbclient -L 10.129.112.127
```

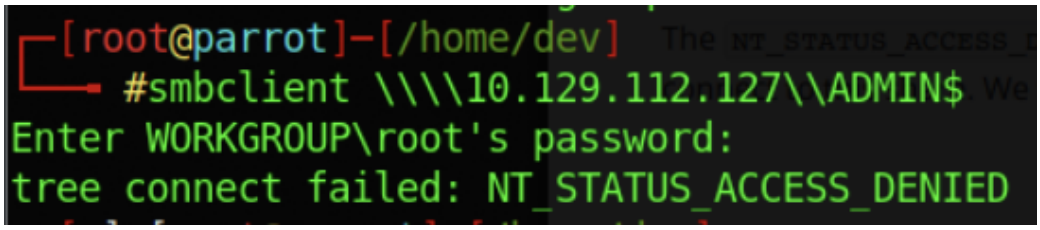


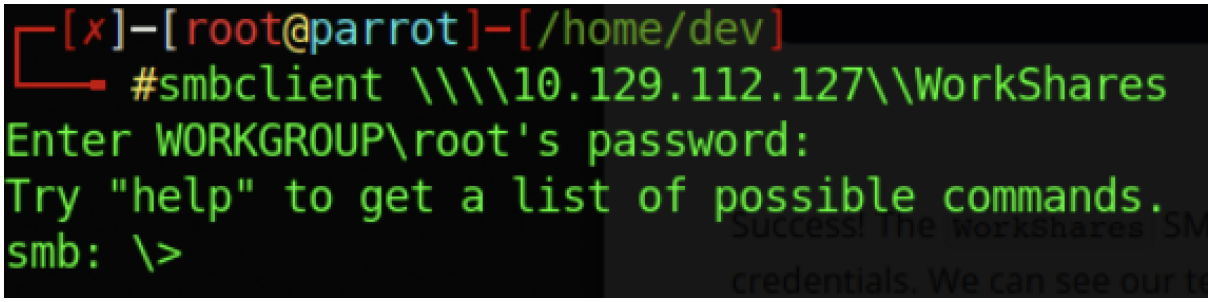
列出 server 分享的資源，有些需要帳密進不去




```
Enter WORKGROUP\root's password:

  Sharename       Type      Comment
  ---------       ----      -------
  ADMIN$          Disk      Remote Admin
  C$              Disk      Default share
  IPC$            IPC       Remote IPC
  WorkShares      Disk
SMB1 disabled -- no workgroup available
```

try to connect to ADMIN$ but failed





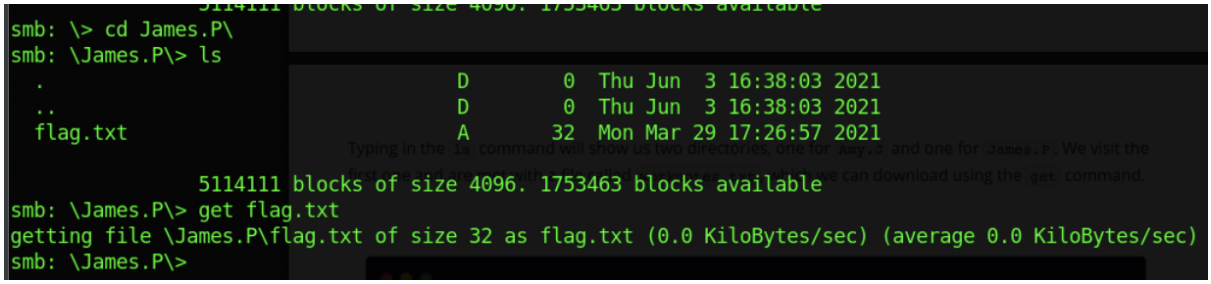
試著瀏覽 `WorkSpace$`

```
┌──[x]─[root@parrot]─[/home/dev]
└──╼ #smbclient \\\\10.129.112.127\\WorkShares
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \>
```

```
smb: \> ls
  .                                   D        0  Mon Mar 29 16:22:01 2021
  ..                                  D        0  Mon Mar 29 16:22:01 2021
  Amy.J                               D        0  Mon Mar 29 17:08:24 2021
  James.P                             D        0  Thu Jun  3 16:38:03 2021

                5114111 blocks of size 4096. 1753463 blocks available
smb: \>
```

D 代表資料夾，所以可以進去裡面逛逛

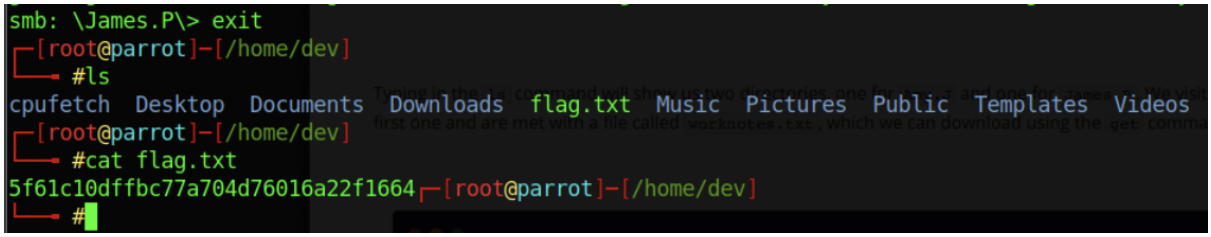
```
smb: \> cd Amy.J
smb: \Amy.J\> ls
  .                                   D        0  Mon Mar 29 17:08:24 2021
  ..                                  D        0  Mon Mar 29 17:08:24 2021
  worknotes.txt                       A       94  Fri Mar 26 19:00:37 2021

                5114111 blocks of size 4096. 1753463 blocks available
smb: \Amy.J\>
```



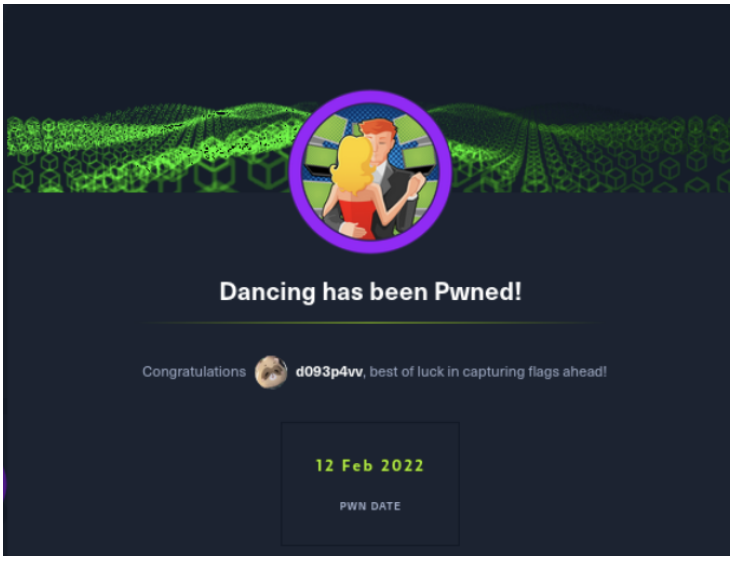
flag

Use `get` to download a file from remote or `mget` to download multiple files

```
get Amy.J
```




```
5f61c10dffbc77a704d76016a22f1664
```



https://www.hackthebox.com/achievement/machine/929350/395

Explosion (RDP)

```
10.129.197.50
```

Tasks

What is the concept used to verify the identity of the remote host with SSH connections?

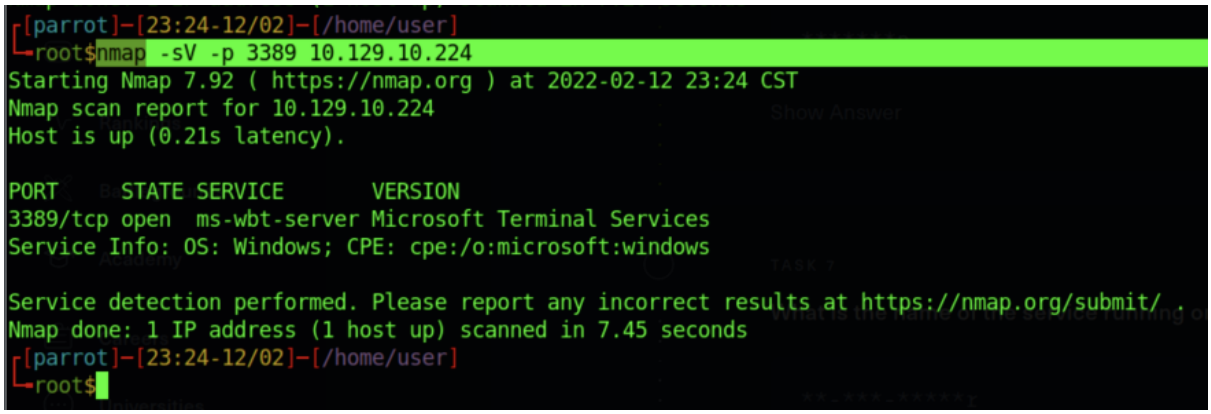
`public-key cryptography` aka Asymmetric cryptography

What is the name of the tool that we can use to initiate a desktop projection to our host using the terminal?

`xfreerdp`

What is the name of the service running on port 3389 TCP?

`ms-wbt-server`



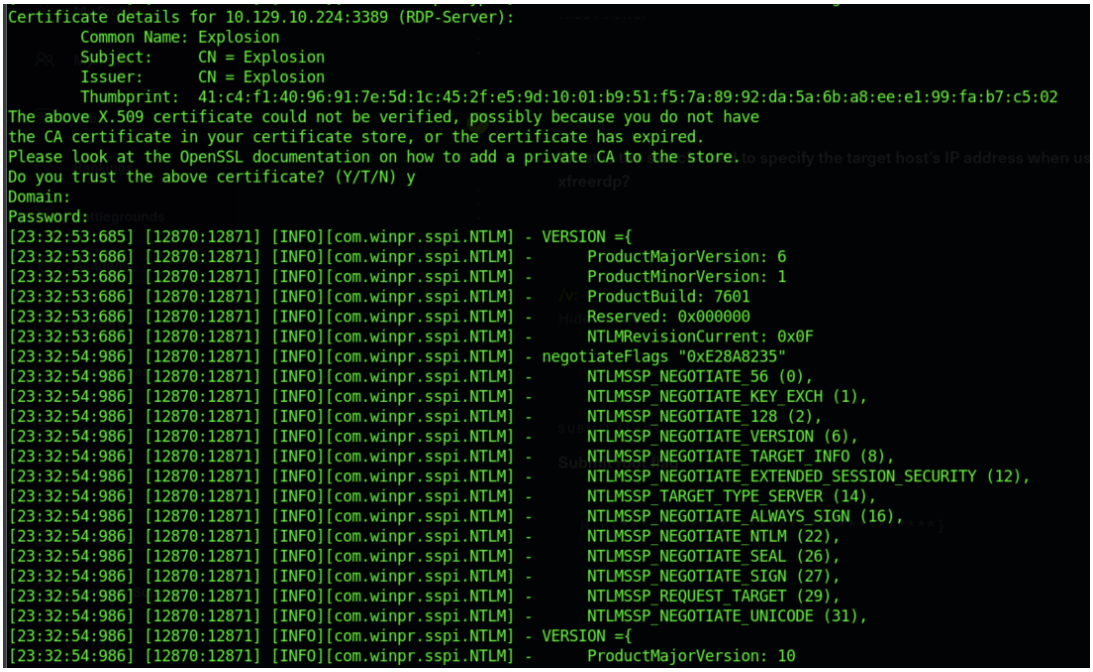

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 23:24 CST
Nmap scan report for 10.129.10.224
Host is up (0.21s latency).

PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.45 seconds
```

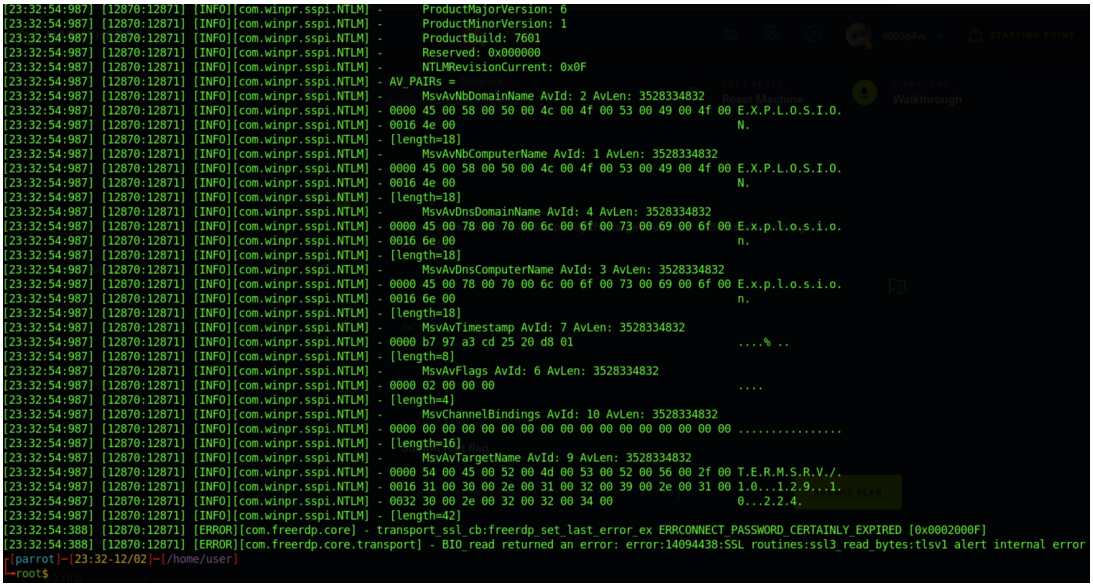
What is the switch used to specify the target host's IP address when using xfreerdp? → `/v:`

```
                                    settings, use with extreme caution!
/tune-list                          Print options allowed for /tune
/u:[[<domain>\]<user>|<user>[@<domain>]]
                                    Username
+unmap-buttons                      Enable Let server see real physical pointer
                                    button
/usb:[dbg,][id:<vid>:<pid>#...,][addr:<bus>:<addr>#...,][auto]
                                    Redirect USB device
/v:<server>[:port]                  Server hostname
/vc:<channel>[,<options>]           Static virtual channel
/version                            Print version
/video                              Video optimized remoting channel
/vmconnect[:<vmid>]                 Hyper-V console (use port 2179, disable
                                    negotiation)
```

嘗試失敗

```
For Gateways, the https_proxy environment variable is respected:
    export https_proxy=http://proxy.contoso.com:3128/
    xfreerdp /g:rdp.contoso.com ...

More documentation is coming, in the meantime consult source files

┌[parrot]─[23:26-12/02]─[/home/user]
└─root$xfreerdp 10.129.10.224
[23:32:32:959] [12870:12870] [WARN][com.freerdp.client.common.cmdline] - Using deprecated command-line interface!
[23:32:32:960] [12870:12870] [WARN][com.freerdp.client.common.compatibility] - 10.129.10.224 -> /v:10.129.10.224
[23:32:32:960] [12870:12870] [WARN][com.freerdp.client.common.compatibility] -
[23:32:32:960] [12870:12871] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[23:32:32:960] [12870:12871] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[23:32:32:960] [12870:12871] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[23:32:32:960] [12870:12871] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[23:32:32:960] [12870:12871] [INFO][com.freerdp.client.x11] - No user name set. - Using login name: user
[23:32:32:270] [12870:12871] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[23:32:32:280] [12870:12871] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[23:32:32:280] [12870:12871] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[23:32:33:717] [12870:12871] [INFO][com.freerdp.crypto] - creating directory /root/.config/freerdp
[23:32:33:717] [12870:12871] [INFO][com.freerdp.crypto] - creating directory [/root/.config/freerdp/certs]
[23:32:33:717] [12870:12871] [INFO][com.freerdp.crypto] - created directory [/root/.config/freerdp/server]
[23:32:33:176] [12870:12871] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[23:32:33:176] [12870:12871] [WARN][com.freerdp.crypto] - CN = Explosion
[23:32:33:176] [12870:12871] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[23:32:33:176] [12870:12871] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[23:32:33:176] [12870:12871] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[23:32:33:176] [12870:12871] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.129.10.224:3389)
[23:32:33:176] [12870:12871] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[23:32:33:176] [12870:12871] [ERROR][com.freerdp.crypto] - Common Name (CN):
[23:32:33:176] [12870:12871] [ERROR][com.freerdp.crypto] -     Explosion
[23:32:33:176] [12870:12871] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.129.10.224:3389 (RDP-Server):
        Common Name: Explosion
        Subject:     CN = Explosion
        Issuer:      CN = Explosion
        Thumbprint:  41:c4:f1:40:96:91:7e:5d:1c:45:2f:e5:9d:10:01:b9:51:f5:7a:89:92:da:5a:6b:a8:ee:e1:99:fa:b7:c5:02
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N)
```



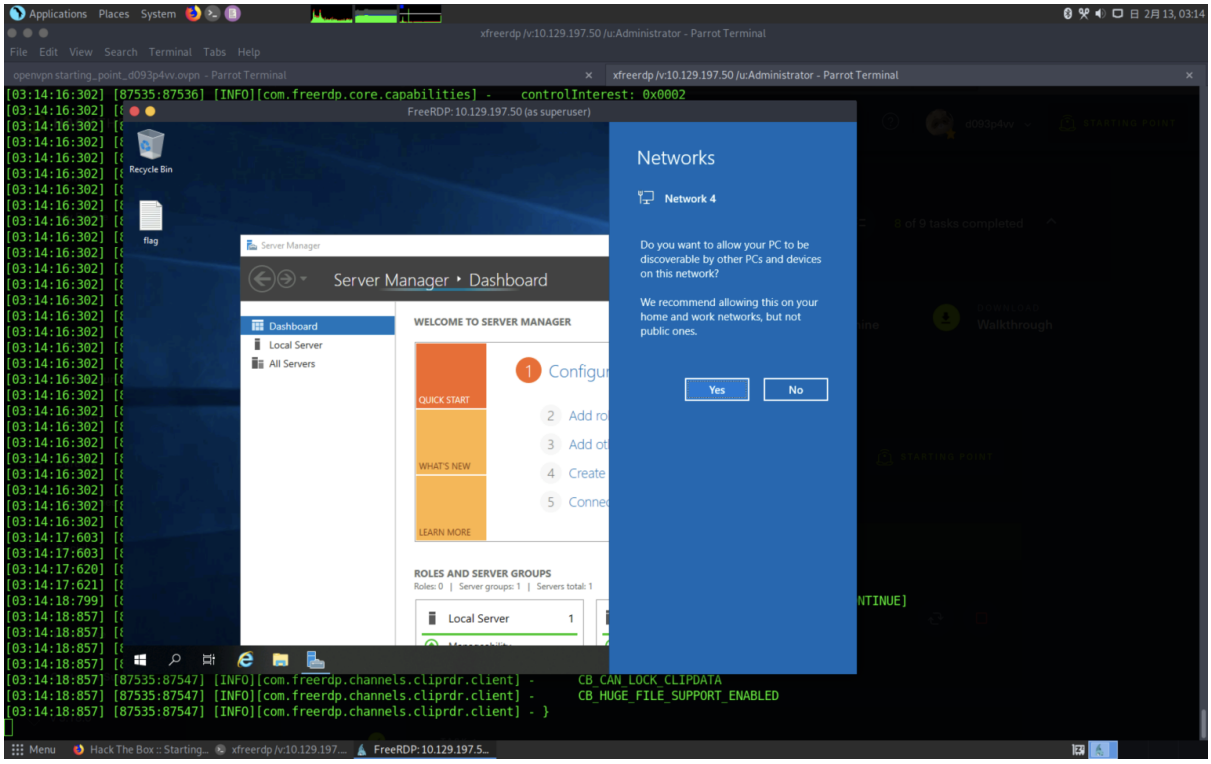


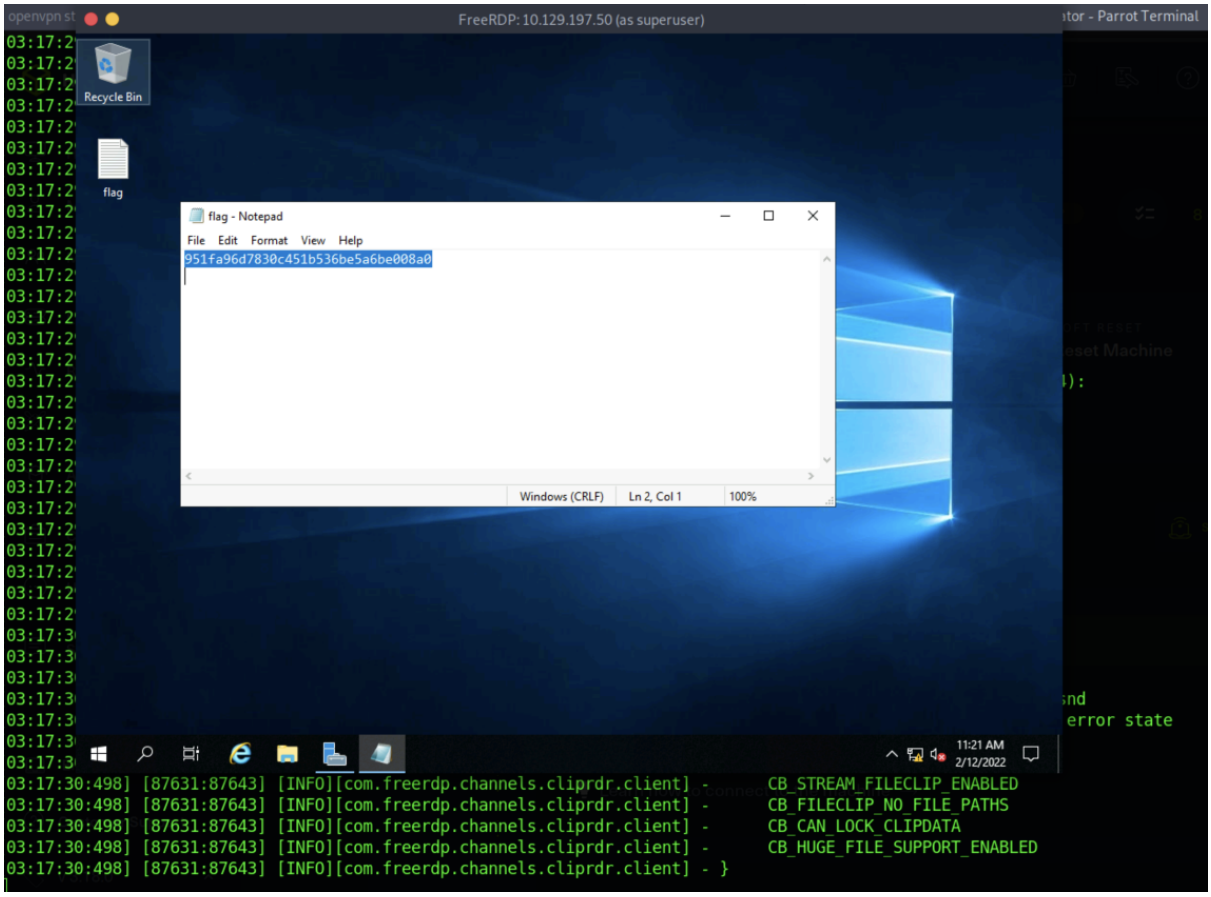
看 writeup 是使用 `/u:` 指定 user，可以先 try `user` `admin` `Administrator` 這類預設的帳號

使用 Administrator，password 直接 enter 不輸入

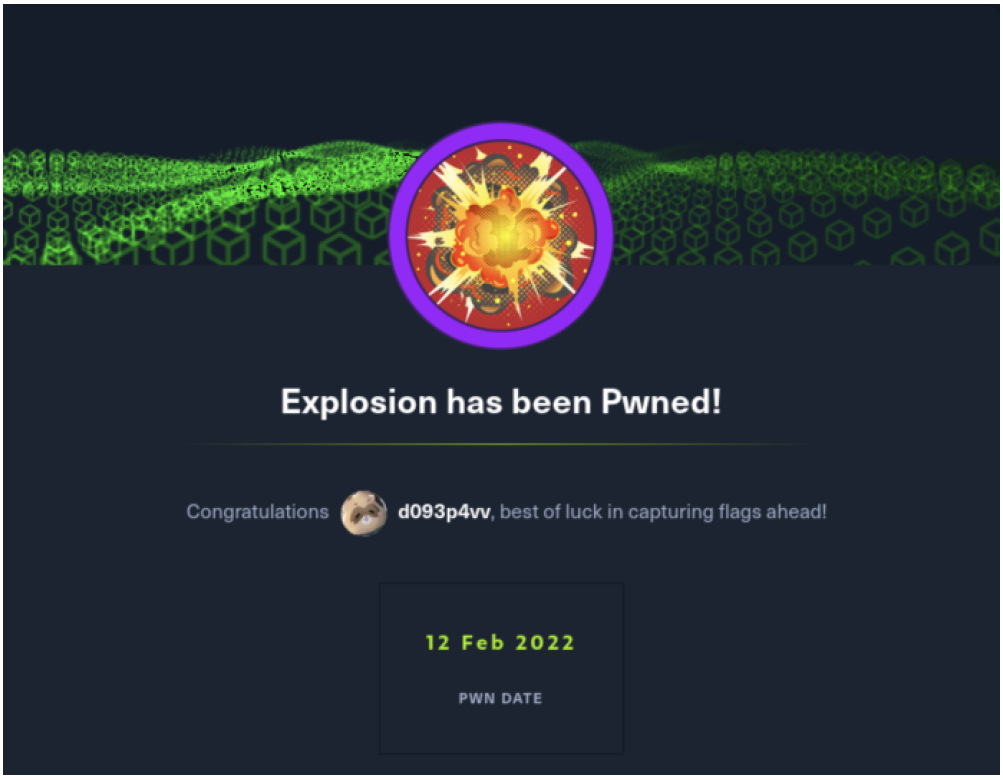
```
xfreerdp /v:10.129.197.50 /u:Administrator
```

```
┌[parrot]-[03:14-13/02]-[/home/user]
└─root$xfreerdp /v:10.129.197.50 /u:Administrator
[03:14:11:988] [87535:87536] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[03:14:11:988] [87535:87536] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[03:14:11:988] [87535:87536] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[03:14:11:988] [87535:87536] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[03:14:11:300] [87535:87536] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[03:14:11:307] [87535:87536] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[03:14:11:307] [87535:87536] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[03:14:12:130] [87535:87536] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[03:14:12:130] [87535:87536] [WARN][com.freerdp.crypto] - CN = Explosion
Password:
[03:14:13:391] [87535:87536] [INFO][com.winpr.sspi.NTLM] - VERSION ={
[03:14:13:391] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      ProductMajorVersion: 6
[03:14:13:391] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      ProductMinorVersion: 1
[03:14:13:391] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      ProductBuild: 7601
[03:14:13:391] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      Reserved: 0x000000
[03:14:13:391] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMRevisionCurrent: 0x0F
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] - negotiateFlags "0xE28A8235"
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_56 (0),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_KEY_EXCH (1),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_128 (2),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_VERSION (6),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_TARGET_INFO (8),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_EXTENDED_SESSION_SECURITY (12),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_TARGET_TYPE_SERVER (14),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_ALWAYS_SIGN (16),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_NTLM (22),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_SEAL (26),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_SIGN (27),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_REQUEST_TARGET (29),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMSSP_NEGOTIATE_UNICODE (31),
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] - VERSION ={
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      ProductMajorVersion: 10
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      ProductMinorVersion: 0
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      ProductBuild: 17763
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      Reserved: 0x000000
[03:14:14:692] [87535:87536] [INFO][com.winpr.sspi.NTLM] -      NTLMRevisionCurrent: 0x0F
```






```
951fa96d7830c451b536be5a6be008a0
```



https://www.hackthebox.com/achievement/machine/929350/396

Preignition (dir busting)

這關主要是體驗 dir busting，使用 gobuster

```
10.129.109.218
```

gobuster

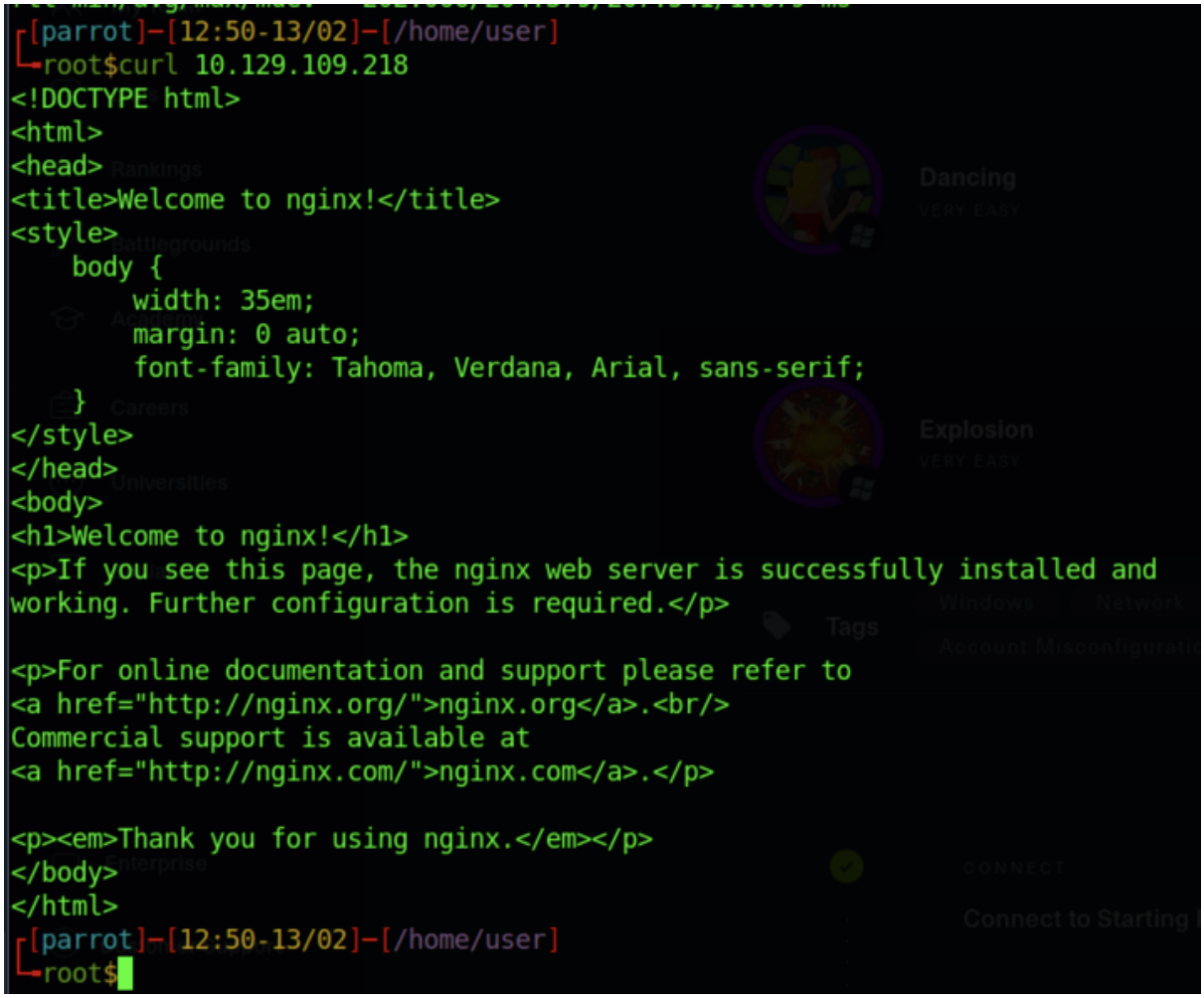
OJ/gobuster: Directory/File, DNS and VHost busting tool written in Go
https://github.com/OJ/gobuster

Tasks

用 nmap scan 基本資訊

```
80/tcp http nginx 1.14.2
```

```
curl 10.129.109.218
```




```
nmap -Pn -sV -T5 10.129.109.218
```

```
┌[parrot]-[12:55-13/02]-[/home/user]
└─root$nmap -Pn -sV -T5 10.129.109.218
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 12:55 CST
Nmap scan report for 10.129.109.218
Host is up (0.21s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.43 seconds
┌[parrot]-[12:55-13/02]-[/home/user]
└─root$
```

```
gobuster
```

```
┌[parrot]-[13:00-13/02]-[/home/user]
└─root$gobuster
Usage:
  gobuster [command]

Available Commands:
  dir         Uses directory/file enumeration mode
  dns         Uses DNS subdomain enumeration mode
  fuzz        Uses fuzzing mode
  help        Help about any command
  s3          Uses aws bucket enumeration mode
  version     shows the current version
  vhost       Uses VHOST enumeration mode

Flags:
      --delay duration    Time each thread waits between requests (e.g. 1500ms)
  -h, --help              help for gobuster
      --no-error          Don't display errors
  -z, --no-progress       Don't display progress
  -o, --output string     Output file to write results to (defaults to stdout)
  -p, --pattern string    File containing replacement patterns
  -q, --quiet             Don't print the banner and other noise
  -t, --threads int       Number of concurrent threads (default 10)
  -v, --verbose           Verbose output (errors)
  -w, --wordlist string   Path to the wordlist

Use "gobuster [command] --help" for more information about a command.
┌[parrot]-[13:00-13/02]-[/home/user]
└─root$
```

What switch do we use to specify to gobuster we want to perform dir busting specifically? → `dir`

```
gobuster dir --help
```

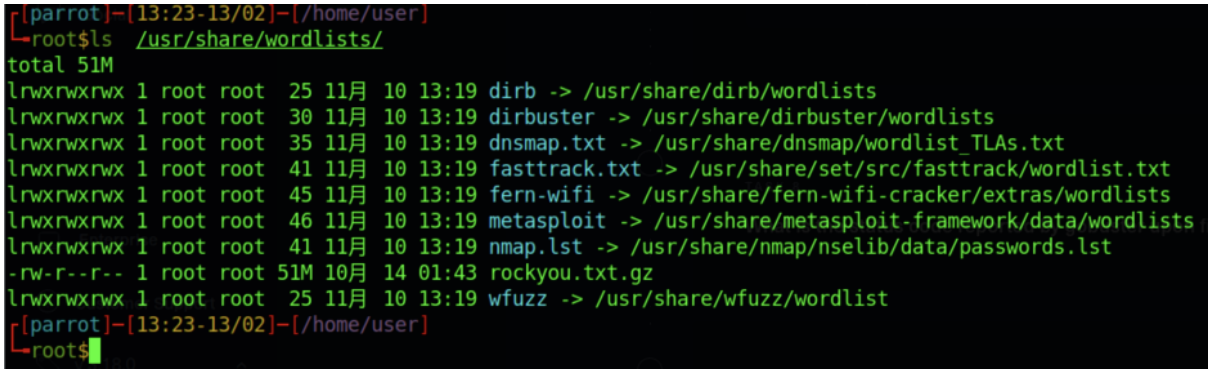
基本上用到的就這是個 options

```
dir : specify we are using the directory busting mode of the tool
-w : specify a wordlist, a collection of common directory names that are typically used
for sites
-u : specify the target's IP address
```

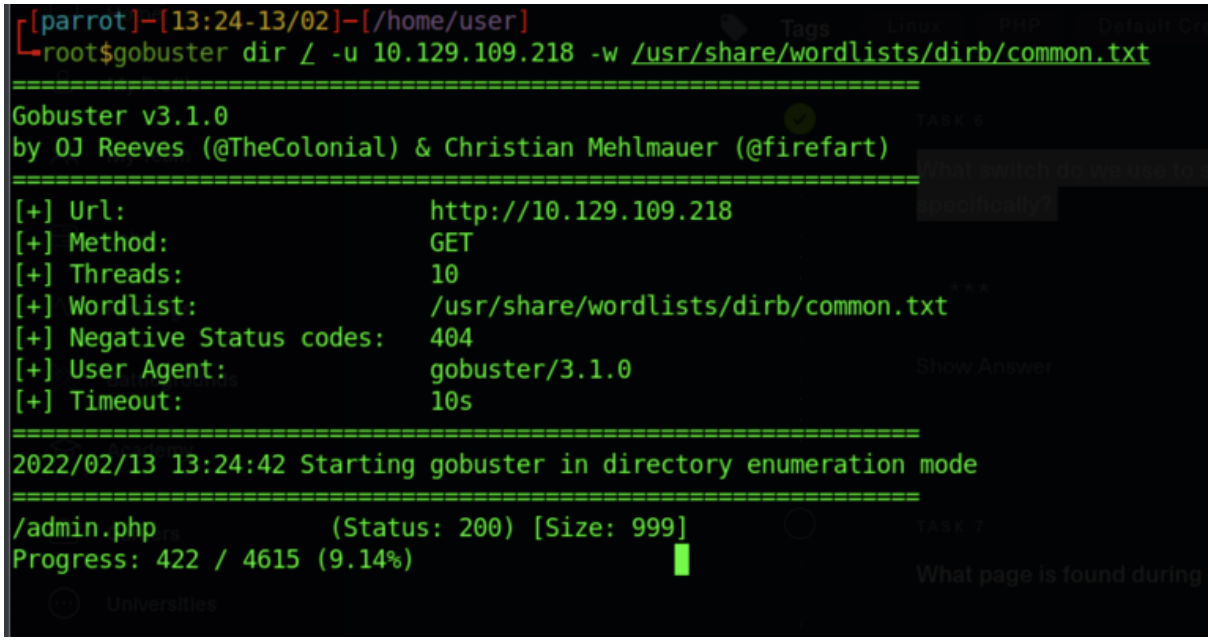
shared wordlist

```
/usr/share/wordlists
```

```
/usr/share/wordlists/dirb/common.txt
```

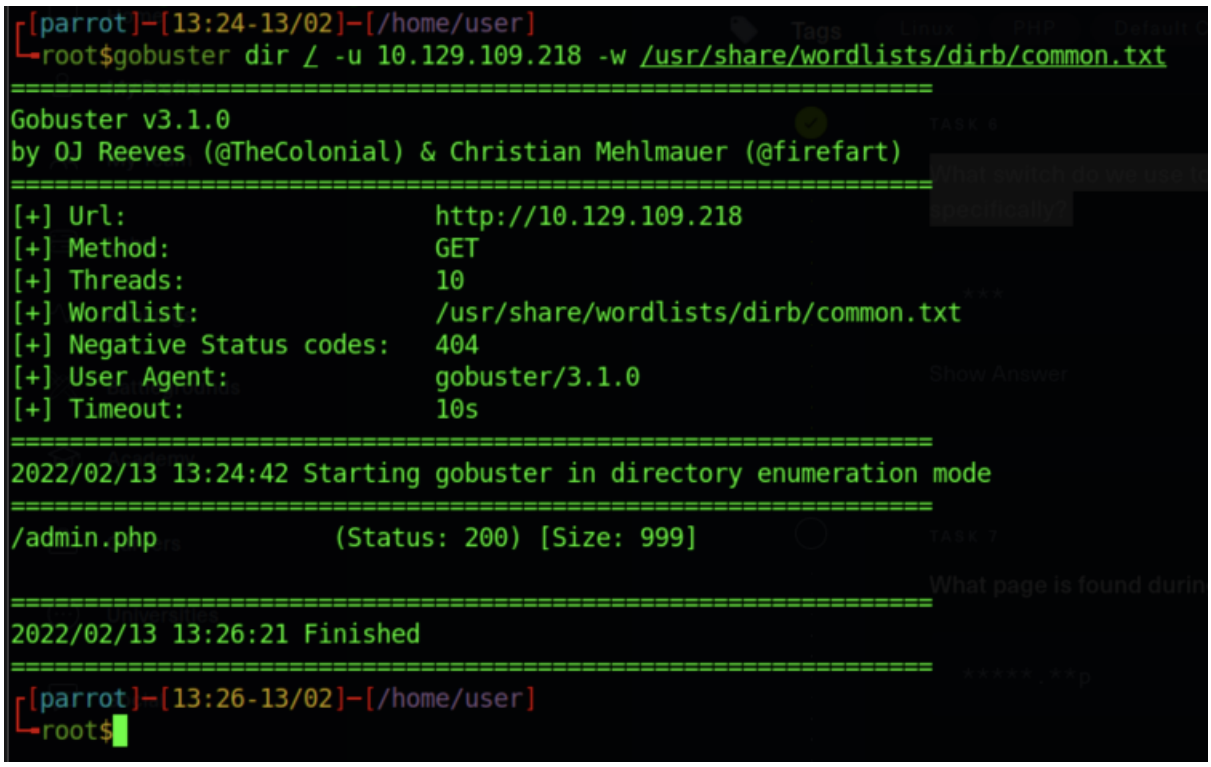


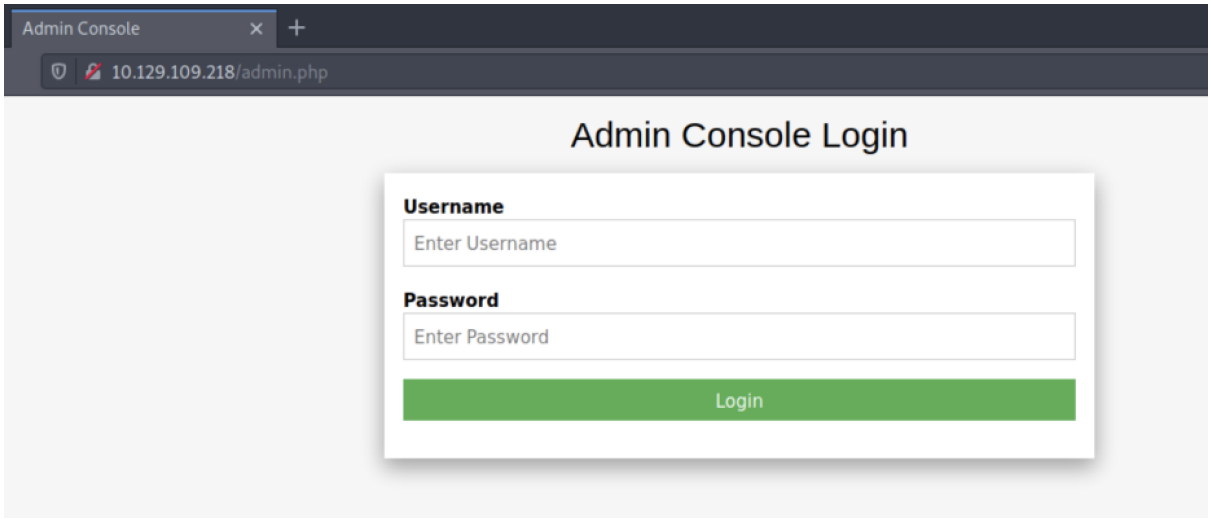

```
gobuster dir / -u 10.129.109.218 -w /usr/share/wordlists/dirb/common.txt
```



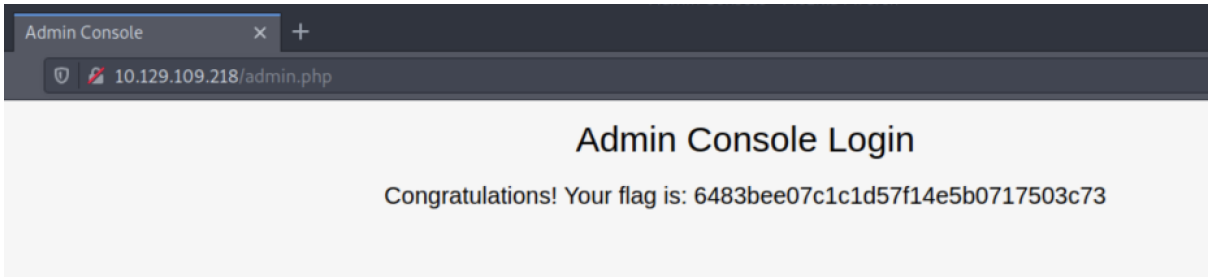
found a path

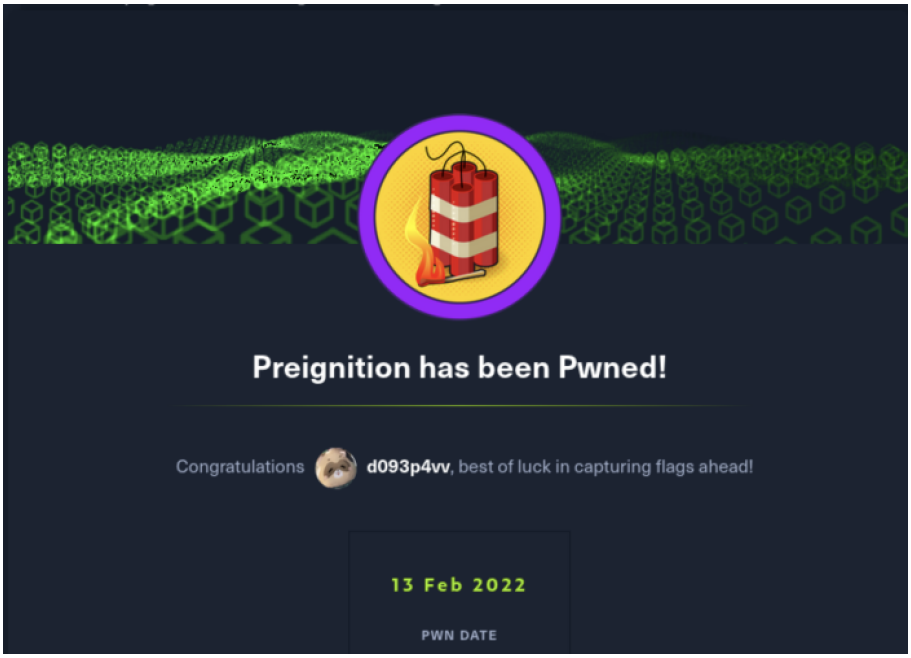
```
/admin.php            (Status: 200) [Size: 999]
```



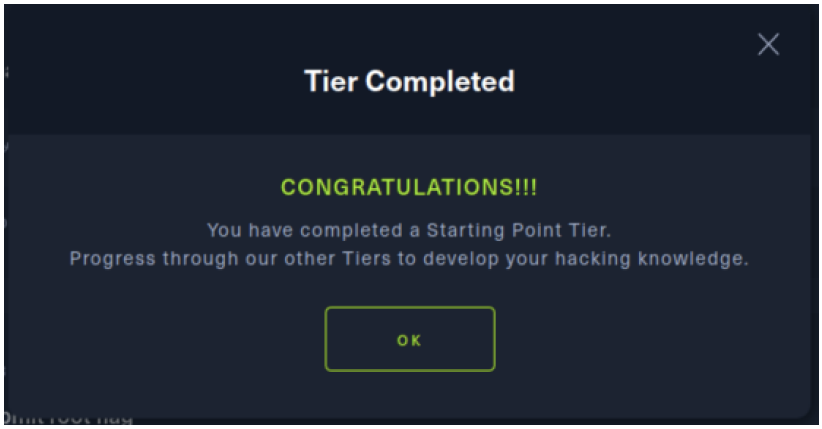


用 admin:admin try try 看就登入了





https://www.hackthebox.com/achievement/machine/929350/397



Ref

- Hack The Box :: Login
- GS: Introduction to Pwnbox | Hack The Box Help Center
- OJ/gobuster: Directory/File, DNS and VHost busting tool written in Go