



# 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	<a href="https://app.hackthebox.com/starting-point">https://app.hackthebox.com/starting-point</a>
☰ 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)

## Tasks

- What is the concept used to verify the identity of the remote host with SSH connections?
- What is the name of the tool that we can use to initiate a desktop projection to our host using the terminal?
- What is the name of the service running on port 3389 TCP?
- What is the switch used to specify the target host's IP address when using xfreerdp? → **/v:**

## Preignition (dir busting)

### Tasks

- What switch do we use to specify to gobuster we want to perform dir busting specifically? → **dir**
- shared wordlist

## Ref

---

# ::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
```

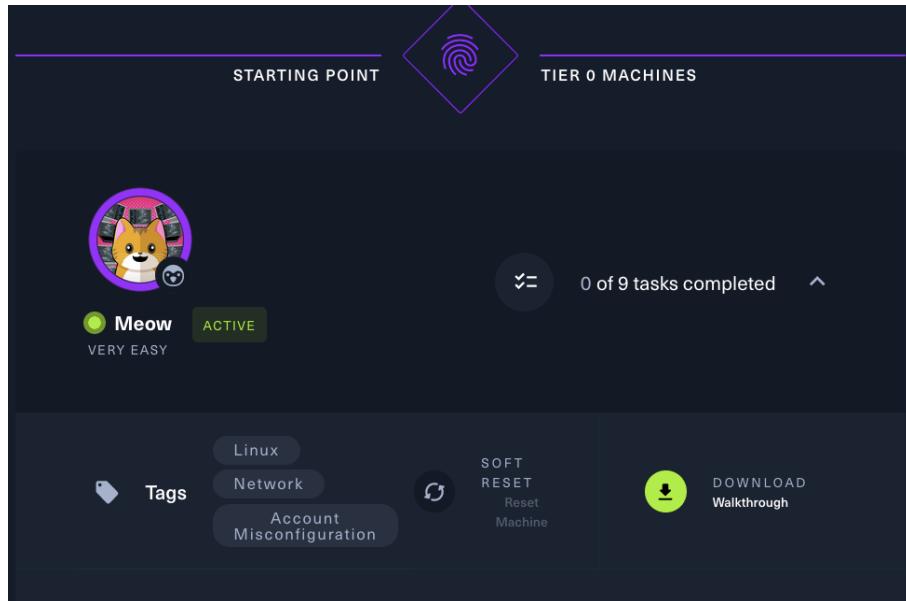
## SSH

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)

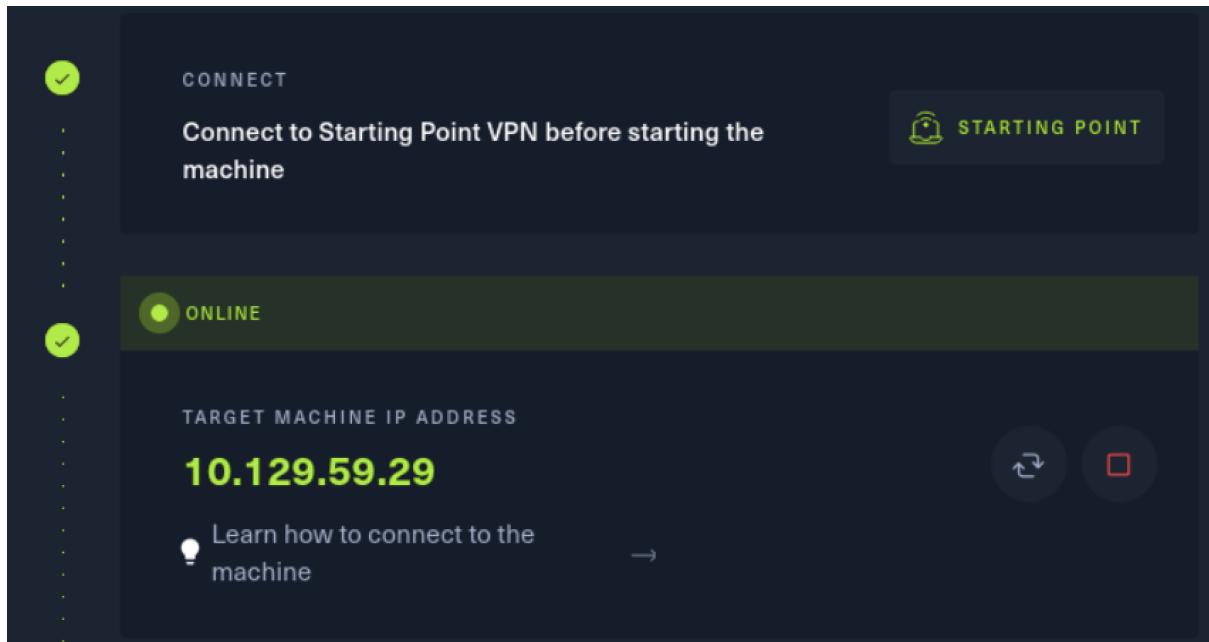


Hack The Box

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

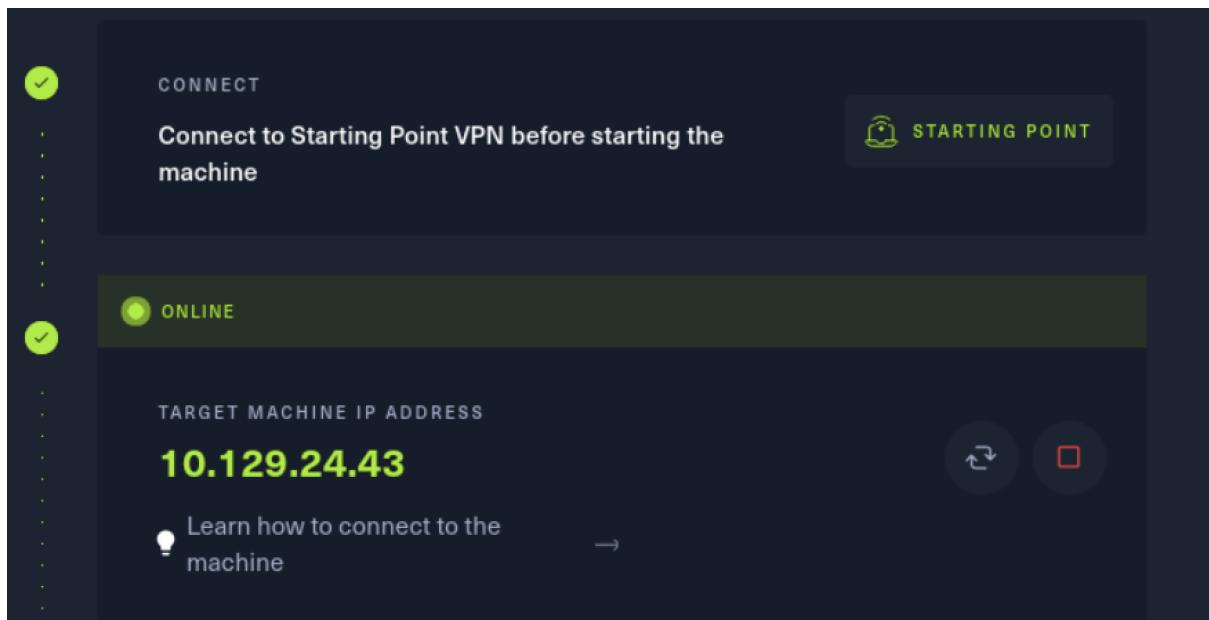
```
$ sudo openvpn starting_point d093p4vv.ovpn
[sudo] password for dev:
2022-02-11 22:17:01 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2022-02-11 22:17:01 DEPRECATED 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::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
```

```
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 TO VPN
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_mtus_set: mtu 1500 for tun0
2022-02-11 22:17:02 net_iface_up: set tun0 up Click to Spawn the machine
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_mtus_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
```

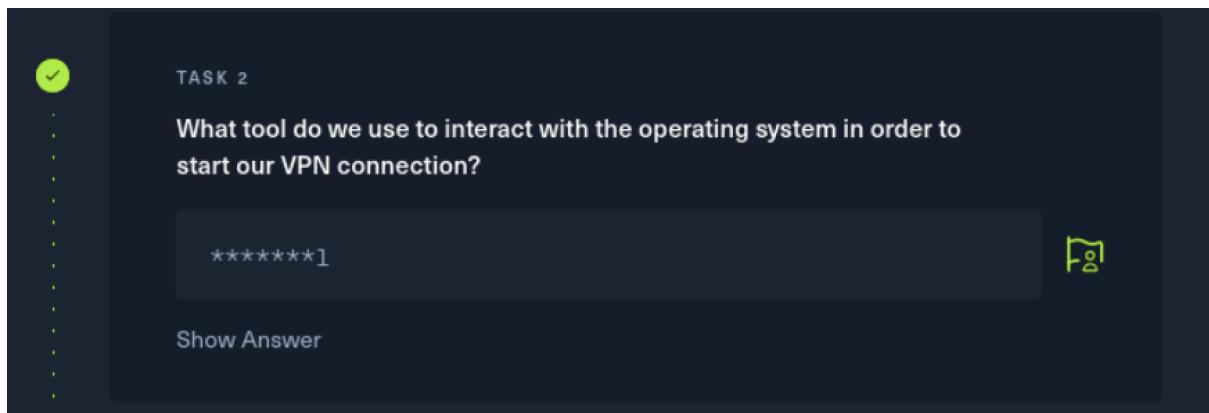
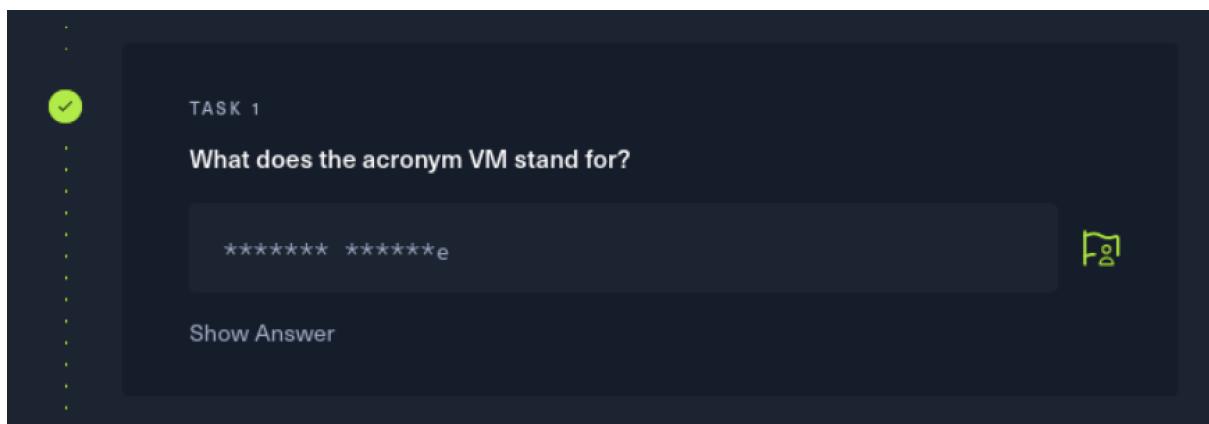


A screenshot of the HackTheBox interface. On the left, a sidebar lists various sections like Home, My Profile, My Team, Labs, Rankings, Battlegrounds, Academy, Careers, Enterprise, and Customer Support. The main content area shows a 'CONNECT' section with the message 'Connect to Starting Point VPN before starting the machine'. It displays an 'ONLINE' status with a checkmark icon. Below it, the 'TARGET MACHINE IP ADDRESS' is listed as '10.129.59.29'. A 'Learn how to connect to the machine' link with a right-pointing arrow is shown. To the right, there's a 'Connect to Starting Point with OpenVPN' section. It shows '191 PLAYERS' online, 'US ACCESS', 'US StartingPoint 1 SERVER', and '10.10.15.114 IP ADDRESS'. Buttons for 'DOWNLOAD VPN' and 'REGENERATE VPN' are available. A note at the bottom says 'Connect to a different VPN server' and 'If you switch your Access or your Server, you will have to re-connect.' A 'Stop your ACTIVE machine to change access' button is at the bottom right. The browser toolbar at the top shows the URL 'https://app.hackthebox.com/starting-point' and the date '2月 11, 22:23'.

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



10.129.24.43



 TASK 4

What is the abbreviated name for a tunnel interface in the output of your VPN boot-up sequence output?

\*\*\*

Show Answer

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

```
tun
```

```
2022-02-11 22:31:46 net_iface_mtu_set: mtu 1500 for tun0
2022-02-11 22:31:46 net_iface_up: set tun0 up
2022-02-11 22:31:46 net_addr_v4_add: 10.10.15.114/23 dev tun0
2022-02-11 22:31:46 net_iface_mtu_set: mtu 1500 for tun0
2022-02-11 22:31:46 net_iface_up: set tun0 up
2022-02-11 22:31:46 net_addr_v6_add: dead:beef:2::1170/64 dev tun0
2022-02-11 22:31:46 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
2022-02-11 22:31:46 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2022-02-11 22:31:46 add_route_ipv6(dead:beef::/64 -> dead:beef:2::1 metric -1) dev tun0
2022-02-11 22:31:46 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2022-02-11 22:31:46 WARNING: this configuration may cache passwords in memory -- use the auth-nocache
2022-02-11 22:31:46 Initialization Sequence Completed
```

接下來是一連串的小 task，這邊都是常識題

 TASK 5

What tool do we use to test our connection to the target?

\*\*\*g

Show Answer

```
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

 TASK 8

What username ultimately works with the remote management login prompt for the target?

\*\*\*t



Show Answer

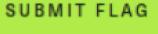
root

最後一個 task 就是暗示你用 telnet 連進靶機，取得 flag

 SUBMIT FLAG

Submit root flag

HTB{\*\*\*\*\*...}



**use nmap -Pn to ping it**

```
nmap -Pn 10.129.24.43
```

```
[x]-[dev@parrot]-[~/Downloads]
└─$ nmap 10.129.24.43
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-11 22:42 CST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds
[dev@parrot]-[~/Downloads]
└─$ nmap -Pn 10.129.24.43
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-11 22:43 CST
Nmap scan report for 10.129.24.43
Host is up.
All 1000 scanned ports on 10.129.24.43 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.35 seconds
[dev@parrot]-[~/Downloads] HTB{*****}
└─$
```

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
```

```
[dev@parrot]-[~/Downloads]
└─$ nmap -v -Pn -p 23 10.129.24.43
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-11 22:54 CST
Initiating Parallel DNS resolution of 1 host. at 22:54
Completed Parallel DNS resolution of 1 host. at 22:54, 0.01s elapsed
Initiating Connect Scan at 22:54
Scanning 10.129.24.43 [1 port]
Completed Connect Scan at 22:54, 2.00s elapsed (1 total ports)
Nmap scan report for 10.129.24.43
Host is up.

PORT      STATE      SERVICE
23/tcp    filtered  telnet

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.07 seconds
[dev@parrot]-[~/Downloads] HTB{*****}
└─$
```

## 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 filtered，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 -Pn 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
```

```
[-x]-[root@parrot]-[/home/dev/Downloads]
└─#ping Pn
PING Pn (139.162.17.173) 56(84) bytes of data.
64 bytes from breadfruit.pitcairn.net.pn (139.162.17.173): icmp_seq=1 ttl=51 time=56.5 ms
64 bytes from breadfruit.pitcairn.net.pn (139.162.17.173): icmp_seq=2 ttl=51 time=58.5 ms
64 bytes from breadfruit.pitcairn.net.pn (139.162.17.173): icmp_seq=3 ttl=51 time=56.4 ms
...
└─# Enterprise
--- Pn ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 56.420/57.132/58.483/0.955 ms
└─# Learn how to connect to the machine
```

拍照留念一下

繼續回來練習

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

```
[-x]-[root@parrot]-[/home/dev/Downloads]
└─#nmap -v -Pn 10.129.14.224
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-11 23:41 CST
Initiating Parallel DNS resolution of 1 host. at 23:41
Completed Parallel DNS resolution of 1 host. at 23:41, 0.05s elapsed
Initiating SYN Stealth Scan at 23:41
Scanning 10.129.14.224 [1000 ports]
Discovered open port 23/tcp on 10.129.14.224
Completed SYN Stealth Scan at 23:41, 7.03s elapsed (1000 total ports)
Nmap scan report for 10.129.14.224
Host is up (0.62s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
TARGET MACHINE IP ADDRESS
10.129.14.224
└─# Enterprise
Read data files from: /usr/bin/../share/nmap
└─# Learn how to connect to the machine
Nmap done: 1 IP address (1 host up) scanned in 7.17 seconds
└─# Customer support available at https://nmap.org/support/
Raw packets sent: 1129 (49.676KB) | Rcvd: 1129 (45.164KB)
```

port 23 is open

```
nmap -sV 10.129.14.224
```

```
[x]-[root@parrot]-[/home/dev/Downloads]
└─# nmap -sV 10.129.14.224
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-11 23:48 CST
Linux Network
Nmap scan report for 10.129.14.224
Host is up (0.96s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Connect to Starting Point VPN before starting the
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.47 seconds
[root@parrot]-[/home/dev/Downloads]
└─#
```

```
telnet 10.129.14.224
```

用 telenet 連線，直接用 root 登入不用密碼

```
[x]-[root@parrot]-[/home/dev/Downloads]
└─# telnet 10.129.14.224
Trying 10.129.14.224...
Connected to 10.129.14.224.
Escape character is '^]'.
```

Careers

# Hack the Box

Customer Support

Meow login:  
Password:

```
* Support: https://ubuntu.com/advantage
HACKTHEBOX System information as of Fri 11 Feb 2022 04:11:32 PM UTC UPGRADE TO VIP
System load: 0.02 Linux Network
Usage of /: 41.7% of 7.75GB Tags Account Misconfiguration
Memory usage: 4%
Swap usage: 0%
Processes: 135
Users logged in: 0
IPv4 address for eth0: 10.129.14.224 Connect to Starting Point VPN be
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.

Battlegrounds https://ubuntu.com/blog/microk8s-memory-optimisation
Academy ONLINE
75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
10.129.14.224

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:~#
```

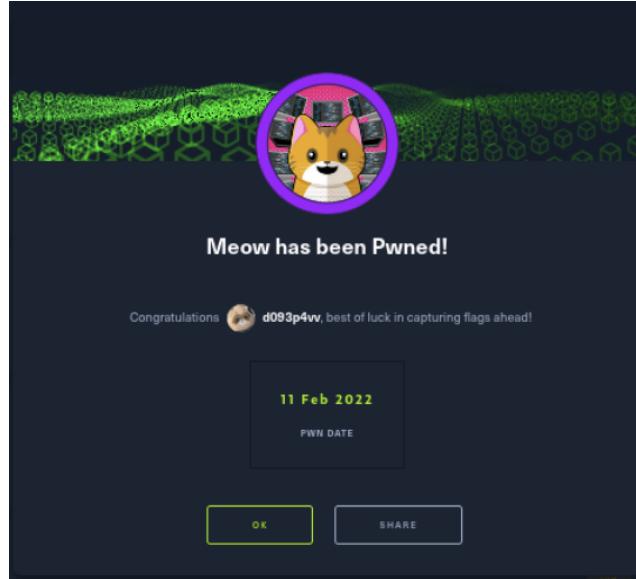
```
root@Meow:~# ll
total 36
drwxr-xr-x 20 root root 4096 Jul 7 2021 ..
drwxr-xr-x  5 root root 4096 Jun 18 2021 .
lrwxrwxrwx  1 root root   9 Jun  4 2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3132 Oct  6 2020 .bashrc
drwxr-xr-x  2 root root 4096 Apr 21 2021 .cache/
-rw-r--r--  1 root root   3 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
b40abdfc23665f766f9c61ecba8a4c19
root@Meow:~#
```

## get flag

```
b40abdf2e23665f766f9c61ecba8a4c19
```

提交時要用加上 `HTB{...}` 在外面

```
HTB{b40abdf2e23665f766f9c61ecba8a4c19}
```



<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



## Task 4 Hint

Remember! When we talk about ports, it's important to mention which transport protocol is used for each port! You never just say 'port 80'. You say 'port 80 TCP' or 'port 1337 UDP'. These two elements are interlocking parts of the same concept.

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`

TASK 7

From your scans, what version is FTP running on the target?

\*\*\*\*\* \*.\*.3

SUBMIT ANSWER

HINT

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

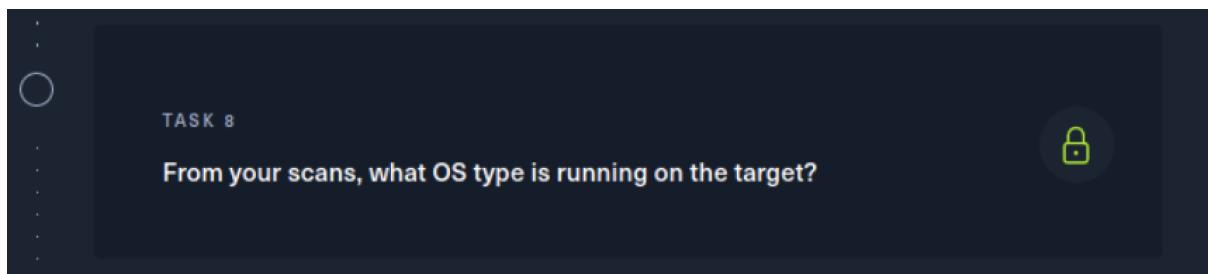
```
nmap -Pn -T5 -p21 -sV 10.129.200.227
```

```
[x]-[root@parrot]-[/home/dev/Downloads]
└─#nmap -Pn -T5 -F -sV 10.129.200.227
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 14:05 CST
Nmap scan report for 10.129.200.227
Host is up (0.66s latency).
Not shown: 99 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
Service Info: OS: Unix
                ***g
Show Answer
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 3.35 seconds
[root@parrot]-[/home/dev/Downloads]
└─#
```

```
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
```

```
[dev@parrot]~[~/Downloads]
$ sudo nmap -T5 -O 10.129.200.227
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 13:32 CST
Warning: 10.129.200.227 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.129.200.227
Host is up (0.20s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
Aggressive OS guesses: Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WA P (Linux 3.4) (93%), Linux 3.16 (93%), Linux 4.15 - 5.6 (92%), Linux 3.8 (92%), QNAP QTS 4.0 - 4.2 (92%), Linux 5.3 - 5.4 (92%), Linux 2.6.32 - 3.10 (92%)
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 14.68 seconds
[dev@parrot]~[~/Downloads]
```

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

```
[root@parrot]~[~/home/dev/Downloads]
# sudo nmap -T5 -O -sn 10.129.200.227
WARNING: OS Scan is unreliable without a port scan. You need to use a scan type along with it, such as -sS, -sT, -sF, etc instead of -sn
QUITTING!
```

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**

```
PORT SPECIFICATION AND SCAN ORDER: TASK 8
-p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports consecutively - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
```

不猜測 OS 的話，scan 100 ports 約 2~2 秒

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

```
[root@parrot]~[/home/dev/Downloads]
└─#nmap -Pn -T5 -F 10.129.200.227
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 14:01 CST
Nmap scan report for 10.129.200.227
Host is up (0.54s latency).
Not shown: 99 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
```

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

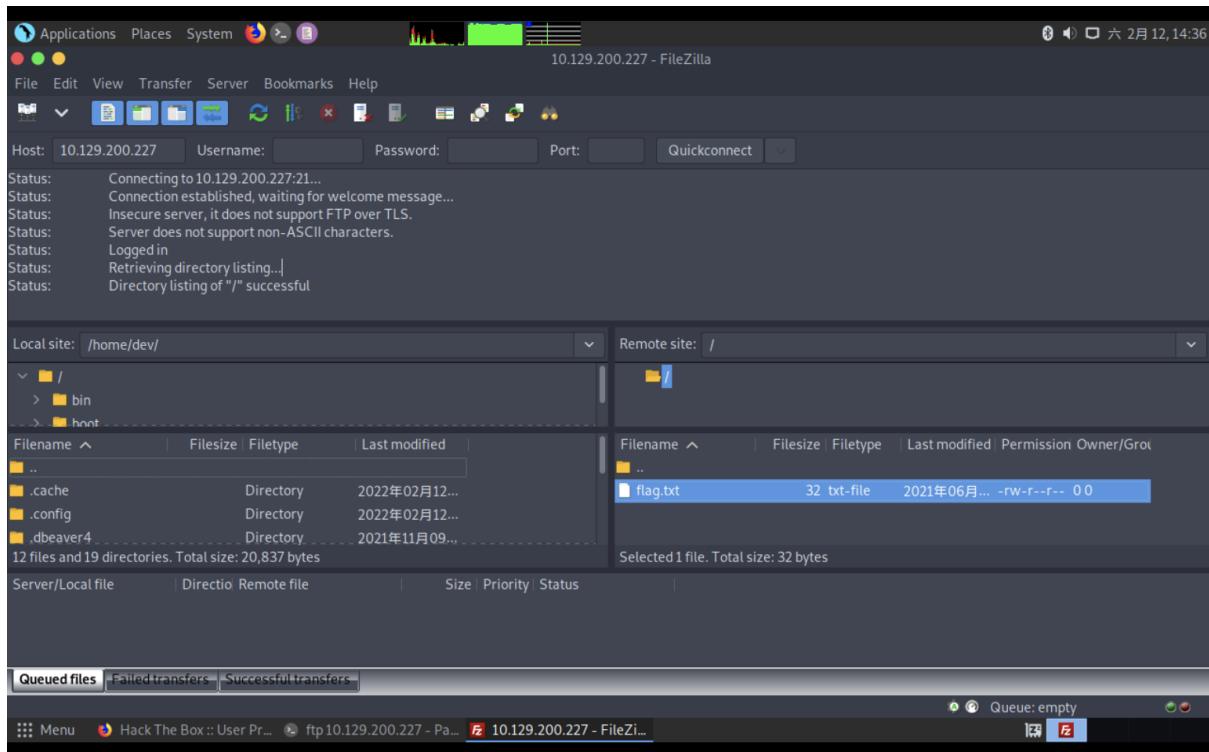
```
sudo apt install ftp -y
ftp $target
```

用 ftp 指令需要輸入帳密，沒什麼頭緒，後來改用 filezilla 就順利進去了 @@，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
```

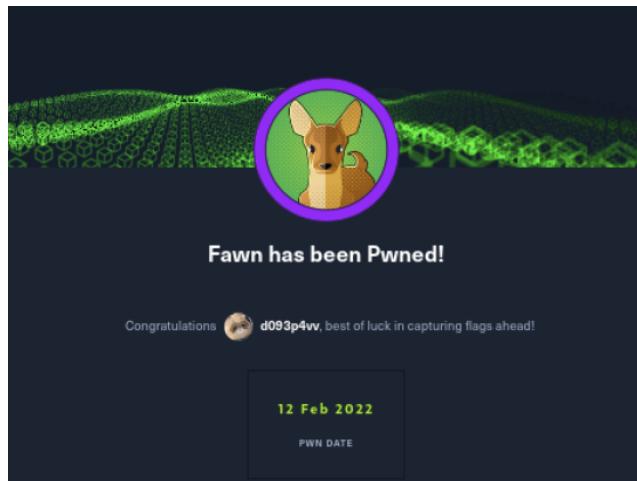
```
[root@parrot]~[/home/dev/Downloads]
└─#ftp $target
Connected to 10.129.200.227.
220 (vsFTPd 3.0.3)
Name (10.129.200.227:dev): █
```



```
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
```

```
[root@parrot]~[~/home/dev]
└─# cat flag.txt
035db21c881520061c53e0536e44f815
[root@parrot]~[~/home/dev]
└─# Connection established, waiting for welcome message...
Insecure server, it does not support FTP over TLS.
```

```
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
```

```
[x]-[root@parrot]-[/home/dev]
└─#nmap -T5 -Pn -sV 10.129.112.127
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 16:04 CST
Warning: 10.129.112.127 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.129.112.127
Host is up (0.60s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
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 47.45 seconds
```

What is the service name for port 445 that came up in our nmap scan?

SUBMIT ANSWER

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

```
smbclient -L 10.129.112.127
```

```
-L|--list          $ smbclient -L [target_IP]
                   Enter [USERGROUP] username's password:
This option allows you to look at what services are available on a server. You use it as smbclient -L host and
a list should appear. The -I option may be useful if your NetBIOS names don't match your TCP/IP DNS host names
or if you are trying to reach a host on another network.
```

列出 server 分享的資源，有些需要帳密進不去

```
[root@parrot]~[/home/dev]
└─# smbclient -L 10.129.112.127
Enter WORKGROUP\root's password:
ADMIN$          C$          IPC$          WorkShares
C$              SMB1 disabled -- no workgroup available
SMB1 disabled -- no workgroup available
```

Sharename	Type	Comment
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share
IPC\$	IPC	Remote IPC
WorkShares	Disk	As always, we can type the name of the share to learn more about the capabilities.

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

```
[root@parrot]~[/home/dev]
└─# smbclient \\\\10.129.112.127\\\\ADMIN$.We
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

```
[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: \>
```

試著瀏覽 WorkShares\$

```

[x]-[root@parrot]-/home/dev] operating systems that allow system administrators to have rem
└─# smbclient \\\\10.129.112.127\\WorkShares
Enter WORKGROUP\root's password: cs - Administrative share for the C:\ disk volume. This is where t
Try "help" to get a list of possible commands. The process communication share. Used for inter-p
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       showacl   setea    setmode
scopy      stat         symlink   tar      tarmode
timeout    translate   unlock    volume  vuid
wdel       logon       listconnect showconnect tcon
tdis        tid         utimes   logoff   ..
!
smb: \>

```

```

smb: \> ls
.
..
Amy.J
James.P
We will try to connect to each of the shares except for the ricks one, wh
not browsable D 0 Mon Mar 29 16:22:01 2021
D 0 Mon Mar 29 16:22:01 2021
D 0 Mon Mar 29 16:22:01 2021
proper creden D 0 Mon Mar 29 17:08:24 2021
ADMIN.S 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
.
..
worknotes.txt
D 0 Mon Mar 29 17:08:24 2021
D 0 Mon Mar 29 17:08:24 2021
A 94 Fri Mar 26 19:00:37 2021
Typing in the ls command will show us two directo
first one and are met with a warning about
5114111 blocks of size 4096. 1753463 blocks available
smb: \Amy.J\>

```

```

      5114111 blocks of size 4096. 1753463 blocks available
smb: \> cd James.P\
smb: \James.P\> ls
.
..
flag.txt
              D      0 Thu Jun  3 16:38:03 2021
              D      0 Thu Jun  3 16:38:03 2021
              A    32 Mon Mar 29 17:26:57 2021
Typing in the ls command will show us two directories, one for Amy.J and one for James.P. We visit the first one and are greeted with a file named worknotes.txt which we can download using the get command.
5114111 blocks of size 4096. 1753463 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \James.P\>

```

## flag

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

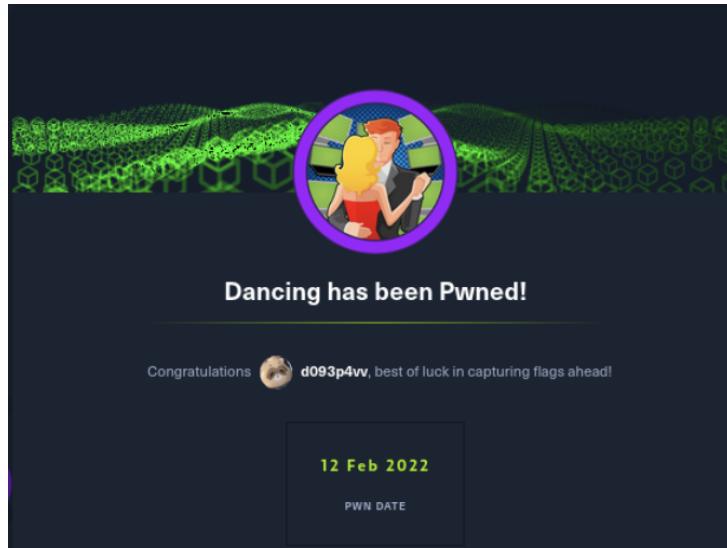
```
get Amy.J
```

```

smb: \James.P\> exit
[root@parrot]~[/home/dev]
└─#ls
cpufetch Desktop Documents Downloads flag.txt Music Pictures Public Templates Videos
[root@parrot]~[/home/dev]
└─#cat flag.txt
5f61c10dffbc77a704d76016a22f1664
[root@parrot]~[/home/dev]
└─#

```

```
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`

```
[parrot]-[23:24-12/02]-[/home/user]
└─root$ nmap -sV -p 3389 10.129.10.224
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).                                         Show Answer
PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
                TASK 7
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
[parrot]-[23:24-12/02]-[/home/user]
└─root$
```

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 What is the switch used to
/v:<server>[:port]	Server hostname xfreerdp?
/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.compatiblity] - 10.129.10.224 -> /v:10.129.10.224
[23:32:32:960] [12870:12870] [WARN][com.freerdp.client.common.compatiblity] -
[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: userP address when using
[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] - @XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX @
[23:32:33:176] [12870:12871] [ERROR][com.freerdp.crypto] - @ WARNING: CERTIFICATE NAME MISMATCH! @
[23:32:33:176] [12870:12871] [ERROR][com.freerdp.crypto] - @XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX @
[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] - SubjExpl
[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) [
```

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. to specify the target host's IP address when using this command.

Do you trust the above certificate? (Y/T/N) y xfreerdp?

Password: degrounds

```
[23:32:53:685] [12870:12871] [INFO][com.winpr.sspi.NTLM] - VERSION ={[23:32:53:686] [12870:12871] [INFO][com.winpr.sspi.NTLM] - ProductMajorVersion: 6[23:32:53:686] [12870:12871] [INFO][com.winpr.sspi.NTLM] - ProductMinorVersion: 1[23:32:53:686] [12870:12871] [INFO][com.winpr.sspi.NTLM] - ProductBuild: 7601[23:32:53:686] [12870:12871] [INFO][com.winpr.sspi.NTLM] - Reserved: 0x000000[23:32:53:686] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMRevisionCurrent: 0x0F[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - negotiateFlags "0xE28A8235"  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_56 (0),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_KEY_EXCH (1),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_128 (2),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_VERSION (6),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_TARGET_INFO (8),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_EXTENDED_SESSION_SECURITY (12),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_TARGET_TYPE_SERVER (14),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_ALWAYS_SIGN (16),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_NTLM (22),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_SEAL (26),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_SIGN (27),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_REQUEST_TARGET (29),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_UNICODE (31),  
[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - VERSION ={[23:32:54:986] [12870:12871] [INFO][com.winpr.sspi.NTLM] - ProductMajorVersion: 10
```

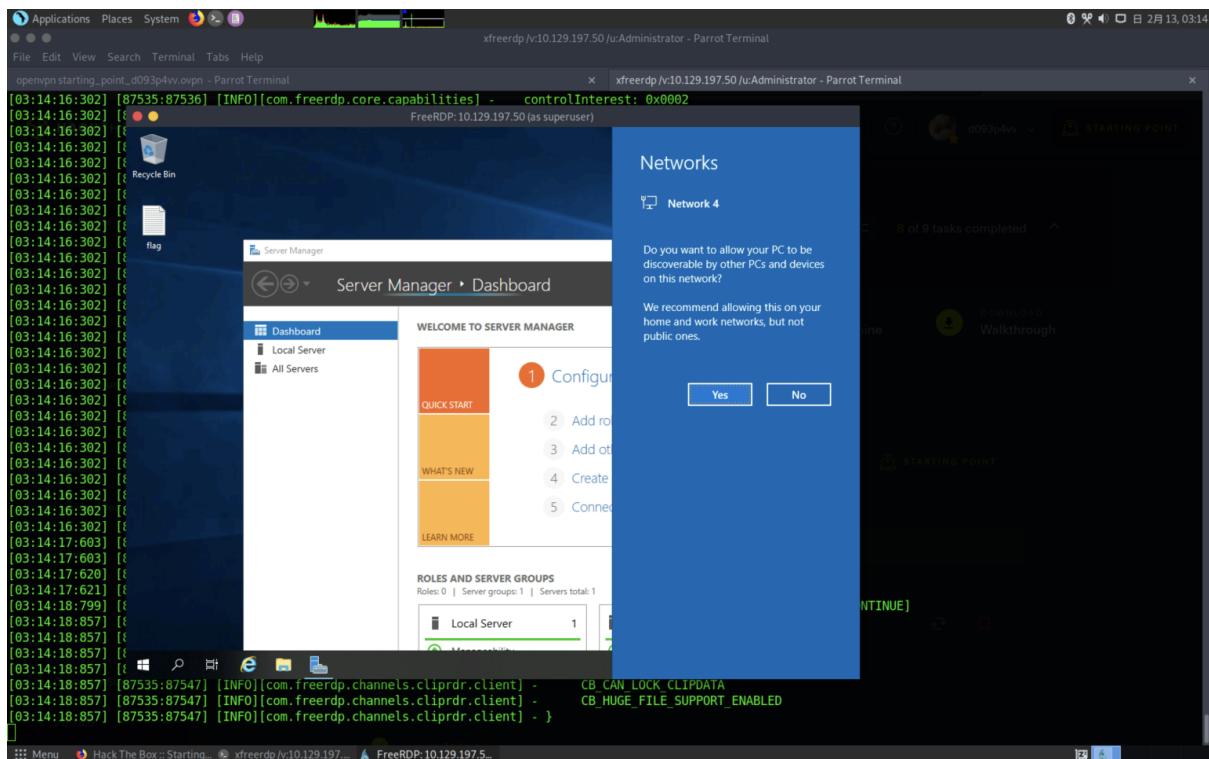
  

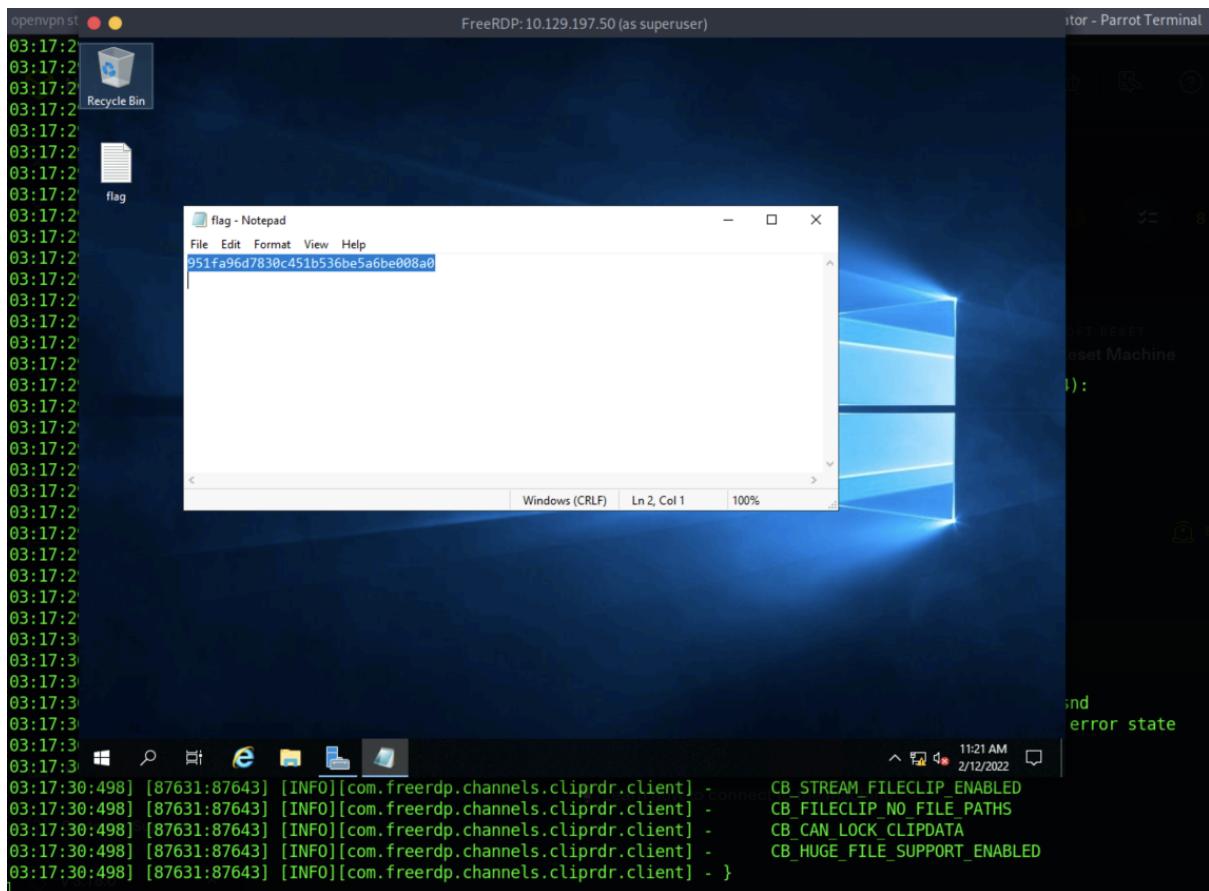
```
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - ProductMajorVersion: 6  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - ProductMinorVersion: 1  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - ProductBuild: 7601  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - Reserved: 0x000000  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - NTLMRevisionCurrent: 0x0F  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - AV_PAIRs =  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - MsvAvNbDomainName AvId: 2 AvLen: 3528334832 Reset Machine  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 00 00 45 00 58 00 50 00 4c 00 4f 00 53 00 49 00 4f 00 E.X.P.L.O.S.I.O.  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 0016 4e 00 N.  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - [length=18]  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - MsvAvNbComputerName AvId: 1 AvLen: 3528334832  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 00 00 45 00 58 00 50 00 4c 00 4f 00 53 00 49 00 4f 00 E.X.P.L.O.S.I.O.  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 0016 4e 00 N.  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - [length=18]  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - MsvAvNsDomainName AvId: 4 AvLen: 3528334832  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 00 00 45 00 78 00 70 00 6c 00 6f 00 73 00 69 00 6f 00 E.x.p.l.o.s.i.o.  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 0016 6e 00 N.  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - [length=18]  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - MsvAvNsComputerName AvId: 3 AvLen: 3528334832  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 00 00 45 00 78 00 70 00 6c 00 6f 00 73 00 69 00 6f 00 E.x.p.l.o.s.i.o.  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 0016 6e 00 N.  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - [length=18]  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - MsvAvTimestamp AvId: 7 AvLen: 3528334832  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 0000 b7 97 a5 cd 25 20 d8 01 .....% ..  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - [length=8]  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - MsvAvFlags AvId: 6 AvLen: 3528334832  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 0000 02 00 00 00 .....  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - [length=4]  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - MsvChannelBindings AvId: 10 AvLen: 3528334832  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - [length=16]  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - MsvAvTargetName AvId: 9 AvLen: 3528334832  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 0000 54 00 45 00 52 00 4d 00 53 00 52 00 56 00 2f 00 T.E.R.M.S.R.V./.  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 0016 31 30 30 00 2e 00 31 00 32 00 39 00 2e 00 31 00 1.0..1.2.9..1. ....PLAN  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - 0032 30 00 2e 00 32 00 32 00 34 00 0...2.2.4.  
[23:32:54:987] [12870:12871] [INFO][com.winpr.sspi.NTLM] - [length=42]  
[23:32:54:388] [12870:12871] [ERROR][com.freerdp.core] - transport_ssl_cb:freerdp_set_last_error_ex ERRORCONNECT_PASSWORD_CERTAINLY_EXPIRED [0x002000F]  
[23:32:54:388] [12870:12871] [ERROR][com.freerdp.core.transport] - BIO_read returned an error: error:14094438:SSL routines:ssl3_read_bytes:tls1 alert internal error  
[parrot] -[23:32:12/02 -| /home/user]  
-root$
```

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

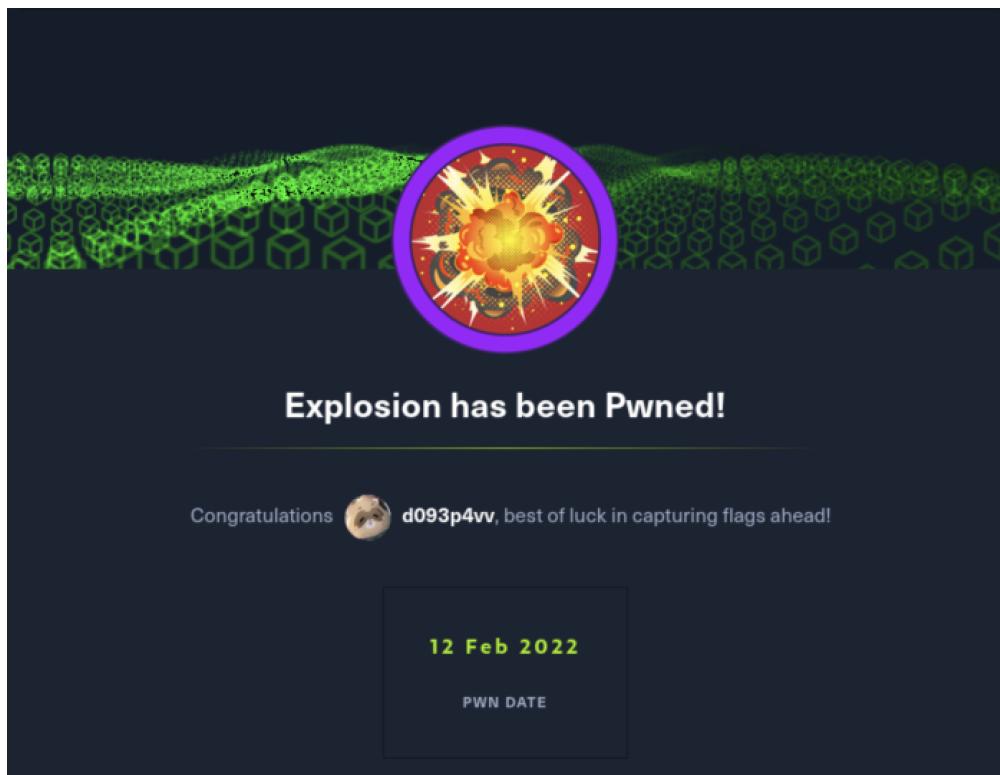
```
xfreerdp /v:10.129.197.50 /u:Administrator
```

```
[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 rdpr
[03:14:11:988] [87535:87536] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpnsd
[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
```

```
[parrot]-[12:50-13/02]-[/home/user]
└─root$curl 10.129.109.218
<!DOCTYPE html>
<html>
<head> Rankings
<title>Welcome to nginx!</title>
<style>
body {
    width: 35em;
    margin: 0 auto;
    font-family: Tahoma, Verdana, Arial, sans-serif;
}
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>
<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>
<p><em>Thank you for using nginx.</em></p>
</body>
</html>
[parrot]-[12:50-13/02]-[/home/user]
└─root$
```

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

```
[parrot]-[12:55-13/02]-[/home/user]
└─$ 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]
└─$
```

gobuster

```
[parrot]-[13:00-13/02]-[/home/user]
└─$ gobuster
Usage: HACKTHEBOX Search Hack The Box
[parrot]-[13:00-13/02]-[/home/user]
Available Commands:
dir      Uses directory/file enumeration mode
dns     My Profile Uses DNS subdomain enumeration mode
fuzz     Uses fuzzing mode
help    My Team Help about any command
s3       Uses aws bucket enumeration mode
version   shows the current version
vhost    abs     Uses VHOST enumeration mode
Flags: Rankings
--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]
└─$
```

**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
```

```
[parrot]-(13:23-13/02)-[/home/user]  
└─root$ls /usr/share/wordlists/  
total 51M  
lrwxrwxrwx 1 root root 25 11月 10 13:19 dirb -> /usr/share/dirb/wordlists  
lrwxrwxrwx 1 root root 30 11月 10 13:19 dirbuster -> /usr/share/dirbuster/wordlists  
lrwxrwxrwx 1 root root 35 11月 10 13:19 dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAs.txt  
lrwxrwxrwx 1 root root 41 11月 10 13:19 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt  
lrwxrwxrwx 1 root root 45 11月 10 13:19 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists  
lrwxrwxrwx 1 root root 46 11月 10 13:19 metasploit -> /usr/share/metasploit-framework/data/wordlists  
lrwxrwxrwx 1 root root 41 11月 10 13:19 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst  
-rw-r--r-- 1 root root 51M 10月 14 01:43 rockyou.txt.gz  
lrwxrwxrwx 1 root root 25 11月 10 13:19 wfuzz -> /usr/share/wfuzz/wordlist  
[parrot]-(13:23-13/02)-[/home/user]  
└─root$
```

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

```
[parrot]-(13:24-13/02)-[/home/user]
└─$ gobuster dir -u 10.129.109.218 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.129.109.218
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
=====
2022/02/13 13:24:42 Starting gobuster in directory enumeration mode
=====
/admin.php      (Status: 200) [Size: 999]
Progress: 422 / 4615 (9.14%)
=====
Universities
```

found a path

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

```
[parrot]-(13:24-13/02)-[/home/user]
└─$ gobuster dir -u 10.129.109.218 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.129.109.218
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
=====
2022/02/13 13:24:42 Starting gobuster in directory enumeration mode
=====
/admin.php      (Status: 200) [Size: 999]
=====
2022/02/13 13:26:21 Finished
=====
[parrot]-(13:26-13/02)-[/home/user]
└─$ ****.**p
```

Admin Console

10.129.109.218/admin.php

### Admin Console Login

**Username**  
Enter Username

**Password**  
Enter Password

**Login**

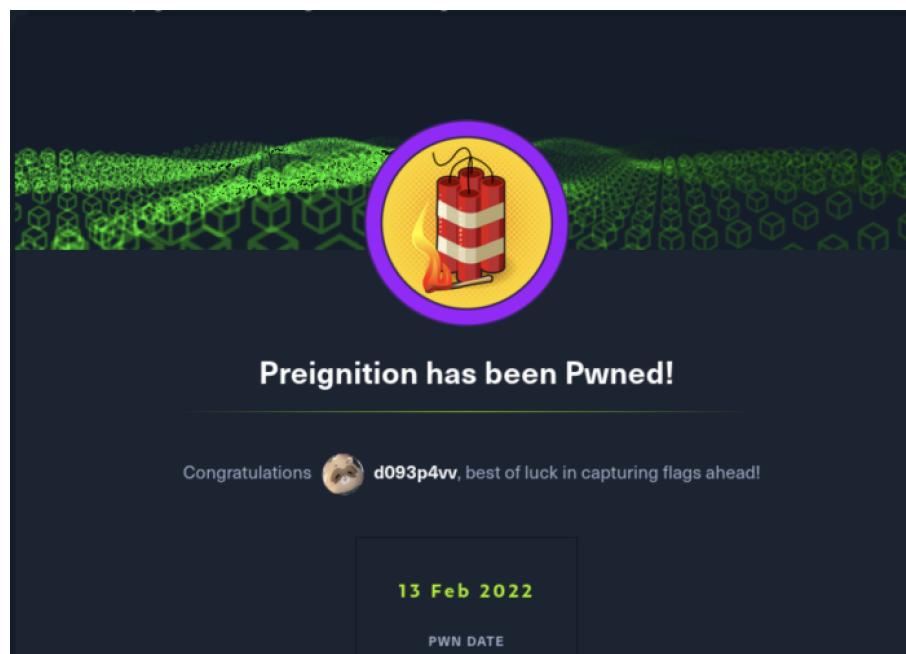
用 admin:admin try try 看就登入了

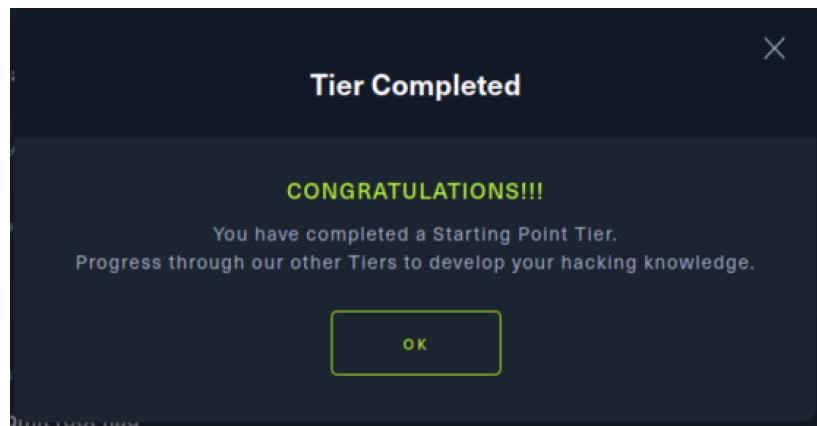
Admin Console

10.129.109.218/admin.php

### Admin Console Login

Congratulations! Your flag is: 6483bee07c1c1d57f14e5b0717503c73





## 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](#)