

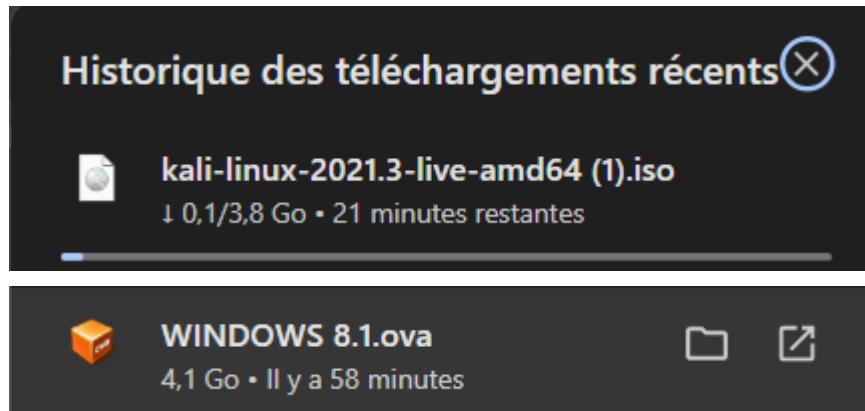
DEL CERRO
Lucas
MANIE
Mathis

TP SAE 1.01

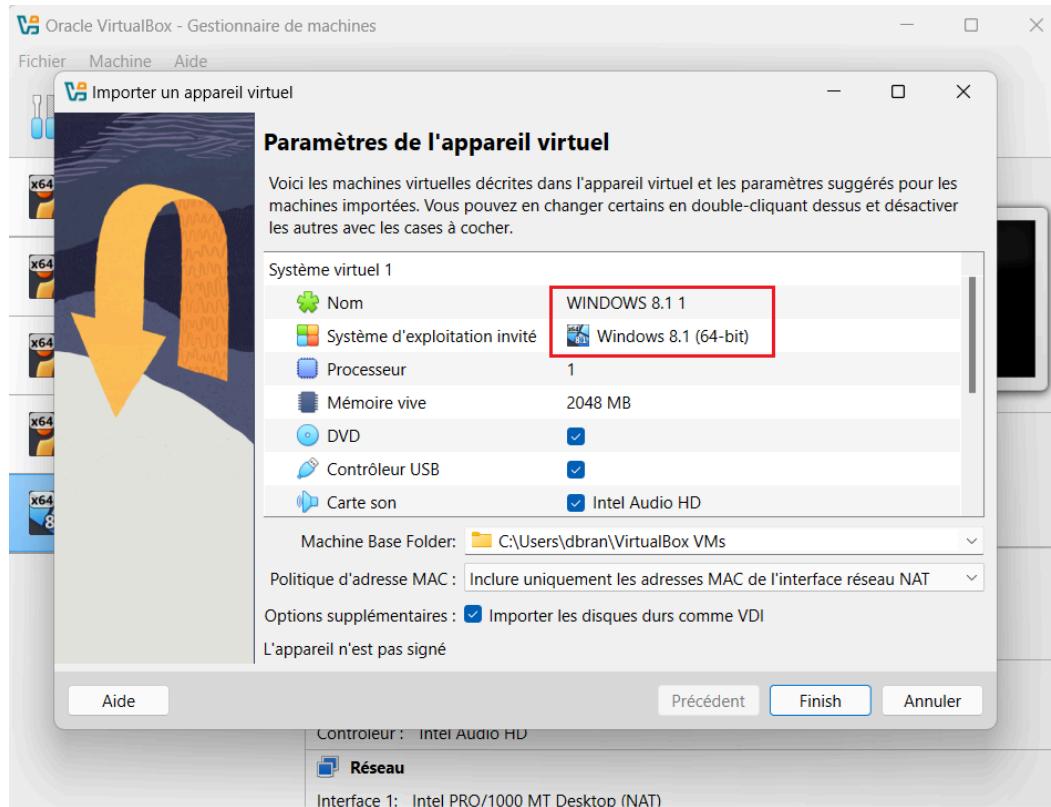
Partie 1:

Le but est de réaliser des tests d'interception des données d'authentification circulant entre une machine virtuelle sous Windows 8 et un environnement Kali Linux, afin d'extraire les mots de passe associés aux comptes utilisateur de la session Windows 8.

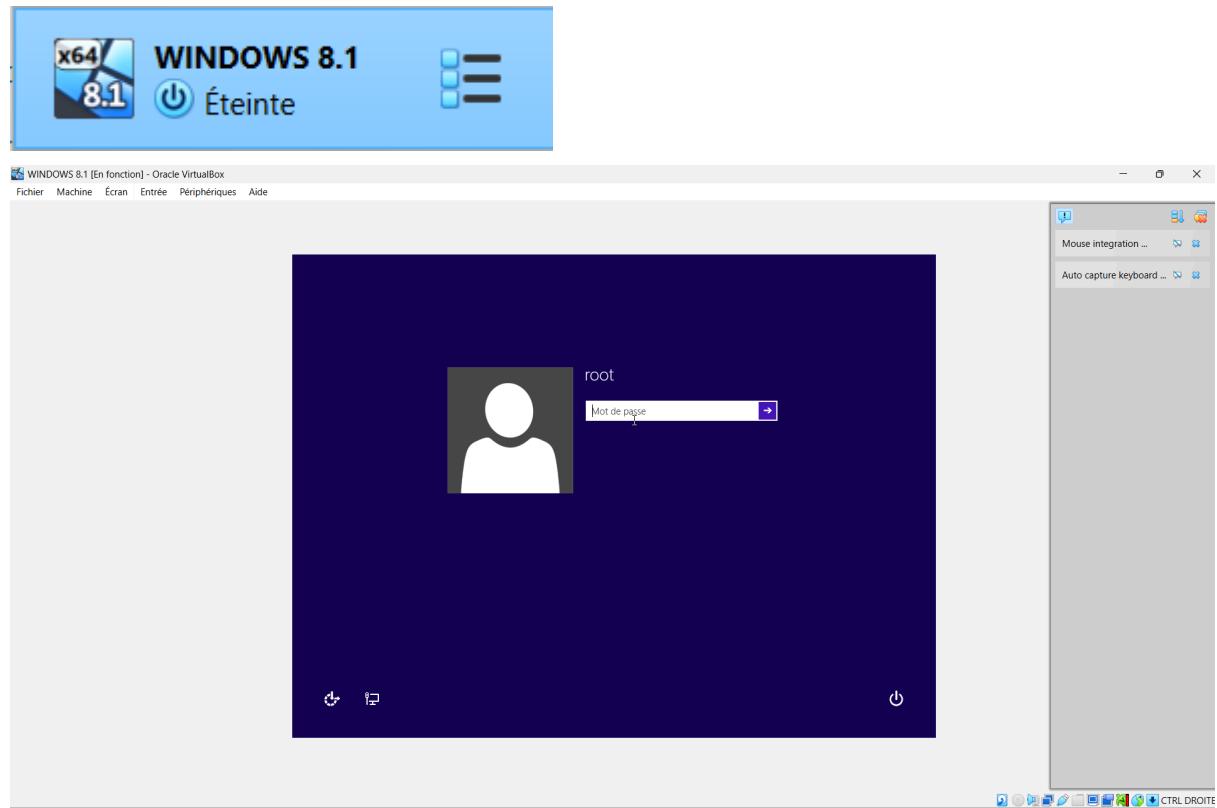
Tout d'abord nous installons les .iso des 2 systèmes d'exploitations requis



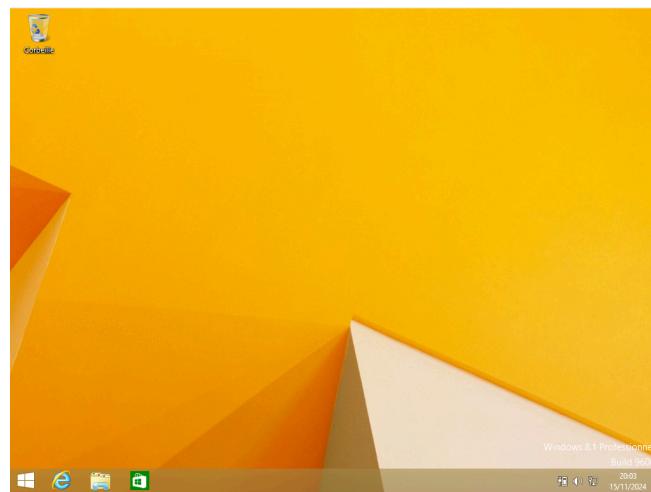
Par la suite nous créons la machine virtuelle Windows 8 .



Une fois installée dans la machine virtuel, nous pouvons le démarrer, avec comme mot de identifiant “root”, et comme mot de passe “toor”.



Maintenant, nous avons accès à notre environnement Windows 8.

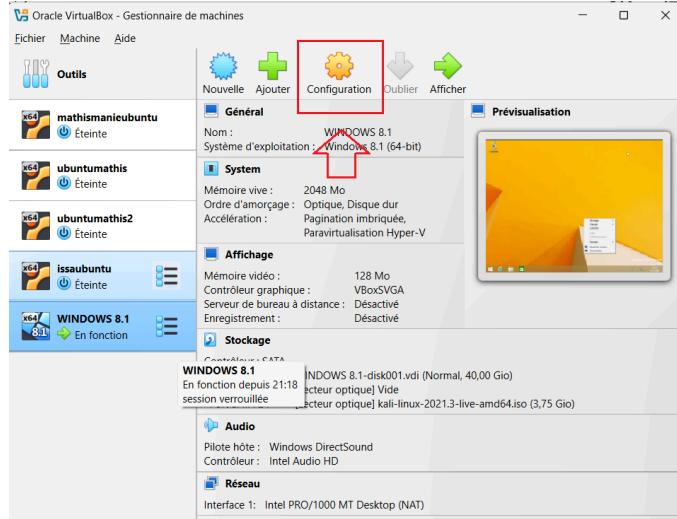


Pour ajouter un second utilisateur, nous sommes passés par les options « Paramètres », puis « Comptes », « Gérer les autres utilisateurs » et « Ajouter un compte ». Le nouvel utilisateur a été créé avec le nom d'identifiant « BUTRT1SAE11 » et le mot de passe défini comme « Roanne123 »

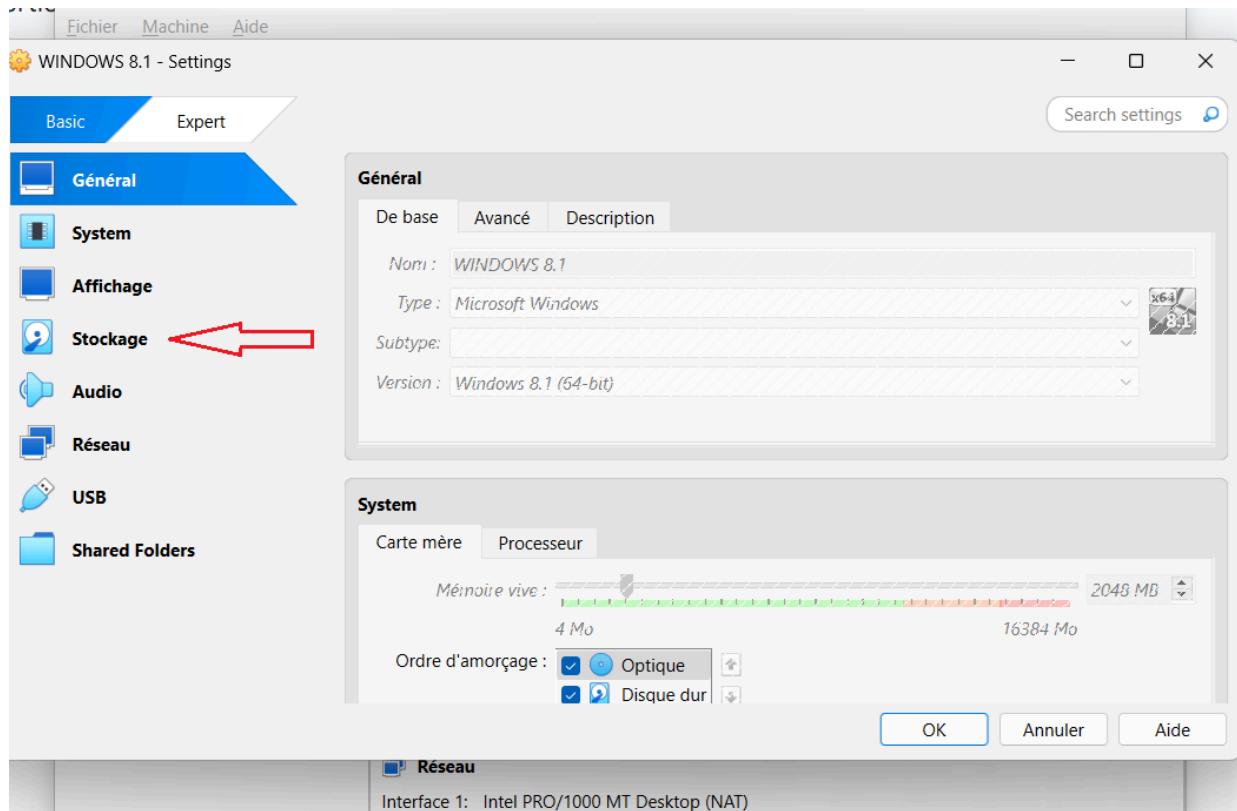


Nous avons par la suite joint le fichier .iso de Kali Linux dans notre machine virtuelle Windows 8. Pour cette tâche, nous avons procédé en plusieurs étapes.

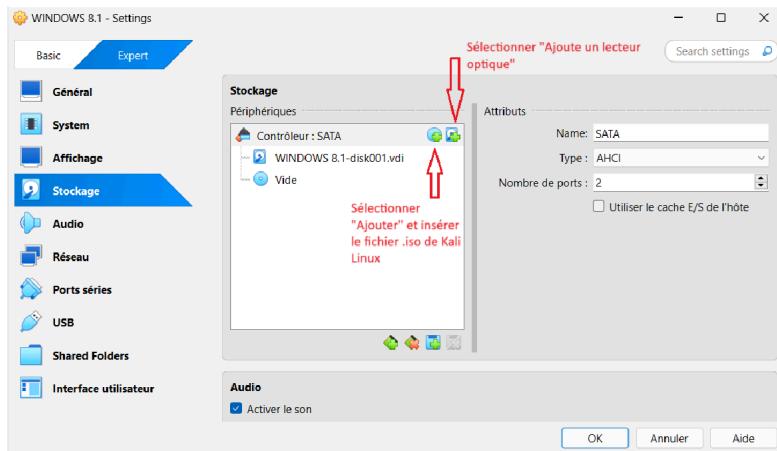
Nous rentrons dans le menu configuration



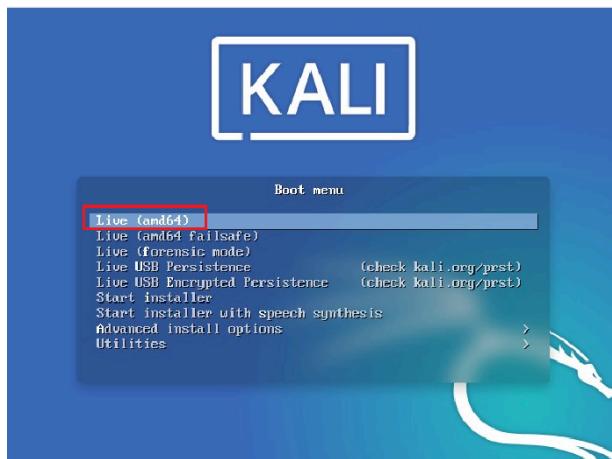
Nous rentrons ensuite dans l'onglet "stockage"



Nous sélectionnons “Ajouter un lecteur optique” puis “Ajouter” et nous joignons le fichier .iso de Kali Linux



Nous redémarrons ensuite la machine virtuelle Windows 8, et à son lancement, nous sélectionnons « Live (amd64) »



Nous ouvrons par la suite un terminal et joignons « setxkbmap fr » afin d'avoir accès au clavier en mode AZERTY

```
(kali㉿kali)-[~]
$ setxkbmap fr
```

Nous avons ensuite exécuté la commande « sudo fdisk -l » pour afficher la liste des partitions présentes sur la machine virtuelle. Cela nous a permis d'identifier celle contenant notre environnement Windows 8, qui correspond ici à « sda2 »

```
(kali㉿kali)-[~]
└─$ sudo fdisk -l
```

Disk /dev/sda: 40 GiB, 42949672960 bytes, 83886080 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x6c9b8b46

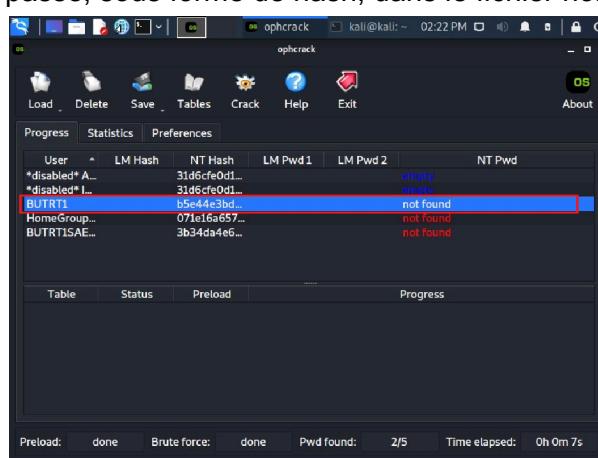
Device Boot Start End Sectors Size Id Type
/dev/sda1 * 2048 718847 716800 350M 7 HPFS/NTFS/exFAT
/dev/sda2 718848 83884031 83165184 39.7G 7 HPFS/NTFS/exFAT

Disk /dev/loop0: 3.33 GiB, 3574292480 bytes, 6981040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Nous avons ensuite utilisé la commande « mount » pour monter la partition Windows détectée précédemment dans Kali. Au préalable, nous avions créé le répertoire sda2 à l'aide de la commande « mkdir »

```
(kali㉿kali)-[~]
└─$ sudo mount /dev/sda2 /mnt/dev/sda2
The disk contains an unclean file system (0, 0).
The file system wasn't safely closed on Windows. Fixing.
```

À l'aide de l'outil « ophcrack », nous avons spécifié le chemin des répertoires associés à l'environnement Windows 8 ainsi que sa partition. Cela nous a permis d'extraire les mots de passe, sous forme de hash, dans le fichier nommé mdp.txt



On constate que les utilisateurs BUTRT1 et BUTRT1SAE11 apparaissent, accompagnés de leurs mots de passe sous forme de hash.

```
GNU nano 5.4                               /mnt/mdp.txt
*disabled* Administrateur:500::31d6cfe0d16ae931b73c59d7e0c089c0 :::
*disabled* Invité:501::31d6cfe0d16ae931b73c59d7e0c089c0 :::
BUTRT1:1001::b5e44e3bdb1ec33cf798364e49bd1efb :::
HomeGroupUser$:1003::071e16a657cce089693f5fc97b4e1ed6 :::
BUTRT1SAE11:1004::3b34da4e6c4a6c09c597264d6808e24c :::
```

À l'aide de l'outil « John the Ripper » et du dictionnaire « rockyou.txt », nous avons réussi à déchiffrer le mot de passe de l'utilisateur « BUTRT1 », qui s'avère être « Roanne ».

```
(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt /mnt/mdp.txt      1 ×
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Remaining 3 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Roanne          (BUTRT1)
1g 0:00:00:00:00 DONE (2024-10-28 14:43) 1.785g/s 25613Kp/s 25613Kc/s 54974KC/s
_ 09 .. *7;Vamos!
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords
reliably
Session completed
```

Suite à l'échec de récupération du second mot de passe, nous avons utilisé la bibliothèque "Vista Free" avec Ophcrack. Après son installation, nous avons configuré Ophcrack avec les chemins de la partition Windows 8 et lancé l'analyse, permettant ainsi la visualisation directe des mots de passe dans l'interface.

The screenshot shows the Ophcrack graphical user interface. At the top, there is a menu bar with 'Load', 'Delete', 'Save', 'Tables', 'Crack', 'Help', and 'Exit'. To the right of the menu is an 'OS' button and an 'About' link. Below the menu is a toolbar with three buttons: 'Progress', 'Statistics', and 'Preferences'. The 'Progress' tab is selected. A progress bar at the bottom indicates '100% in RAM'. The main area is a table showing password cracking results:

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
disabled A...	31d6cfe0d1...				empty
disabled I...	31d6cfe0d1...				empty
BUTRT1	b5e44e3bd...				Roanne
HomeGroup...	071e16a657...				not found
BUTRT1SAE...	3b34da4e6...				Roanne123

Three red arrows point from the 'Roanne' entries in the LM Pwd 1 and NT Pwd columns to a callout box containing the password 'Roanne'. Another red arrow points from the 'Roanne123' entry in the NT Pwd column to a callout box containing the password 'Roanne123'.

Comme on peut le constater, grâce à cette bibliothèque nous avons pu avoir les mots de passe de nos 2 utilisateurs Windows 8.

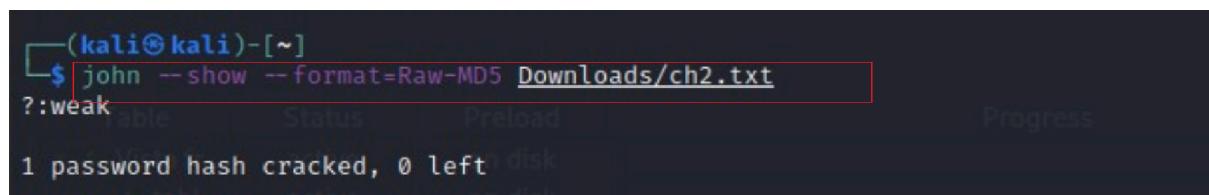
- BUTRT1 : "Roanne"
- BUTRTSAE11 : "Roanne123"

Exercice Root.me

2.1 Hash - Message Digest 5

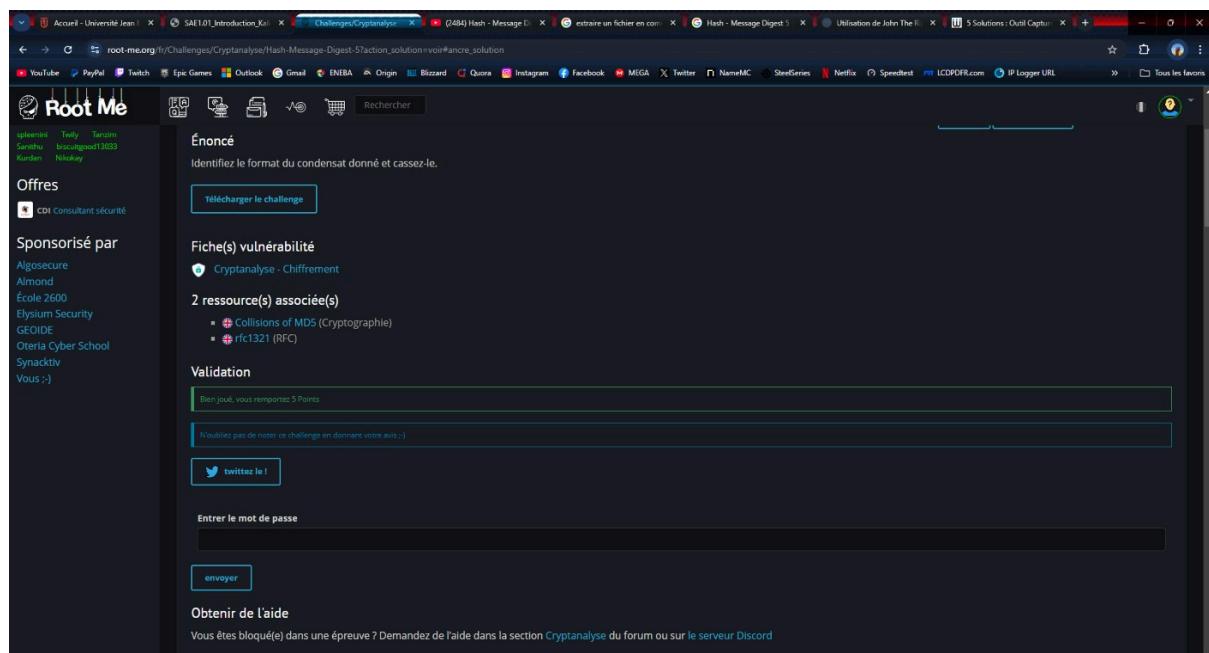
Pour casser le hash fourni, nous avons créé un fichier .txt contenant celui-ci, puis utilisé John the Ripper pour l'identifier et le déchiffrer.

Voici le hash : 7ecc19e1a0be36ba2c6f05d06b5d3058



```
(kali㉿kali)-[~]
$ john --show --format=Raw-MD5 Downloads/ch2.txt
?:weak
1 password hash cracked, 0 left
```

Donc le mot de passe est "weak"

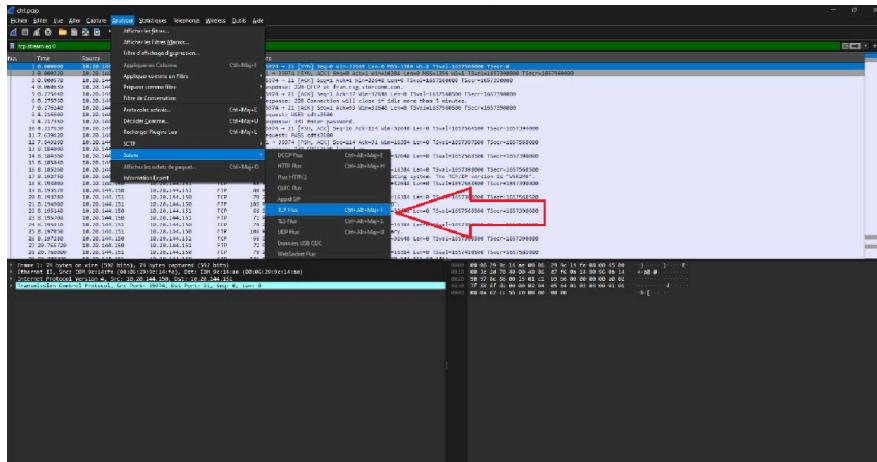


The screenshot shows a challenge page from the Root Me platform. The challenge title is "Hash - Message Digest 5". The challenge details mention "Identifiez le format du condensat donné et cassez-le." Below this, there's a "Télécharger le challenge" button. The challenge description includes sections for "Fiche(s) vulnérabilité" (mentioning Cryptanalysis - Chiffrement), "2 ressource(s) associée(s)" (Collisions of MD5 (Cryptographie) and rfc1321 (RFC)), and "Validation" (indicating 5 points have been awarded). There's also a "Twitter" sharing button and a text input field for entering the password. At the bottom, there's a link to "Obtenir de l'aide".

2.2 Hash - FTP – Authentification

Le but de l'exercice est de trouver le mot de passe de l'utilisateur à partir de la trame FTP

Pour cela nous allons installé Wireshark, ensuite nous allons analysé la trame avec le flux TCP.



On voit donc le mot de passe dans l'analyse de la trame, le mot de passe est donc : « cdts3500 ».

```

220-QTCP at fran.csg.stercomm.com.
220 Connection will close if idle more than 5 minutes.

USER cdts3500

331 Enter password.
PASS cdts3500
230 CDT3500 logged on.

SYST

215 OS/400 is the remote operating system. The TCP/IP version is "V5R2M0".

SITE NAMEFMT

250 Now using naming format "0".

PWD

257 "CDTS3500" is current library.

PASV

227 Entering Passive Mode (10,20,144,151,62,141).

RETR qgpl/apkeyf.apkeyf

150 Retrieving member APKEYF in file APKEYF in library QGPL.
250 File transfer completed successfully.

QUIT

221 QUIT subcommand received.

```

Root Me

HOME / CHALLENGES / RÉSEAU

FTP - Authentification

5 Points

Analyse de capture réseau

Auteur: gouZ, 30 août 2010 | Niveau:  | Validations: 101192 Challengeurs | Note: ★★★★☆ 9827 votes

Énoncé

Un échange authentifié de fichier réalisé grâce au protocole FTP. Retrouvez le mot de passe utilisé par l'utilisateur.

Télécharger le challenge

2 vulnérabilités

- Wireshark - TELNET et FTP
- Outil - Wireshark

1 ressource(s) associée(s)

- rfc595 (RFC)

Validation

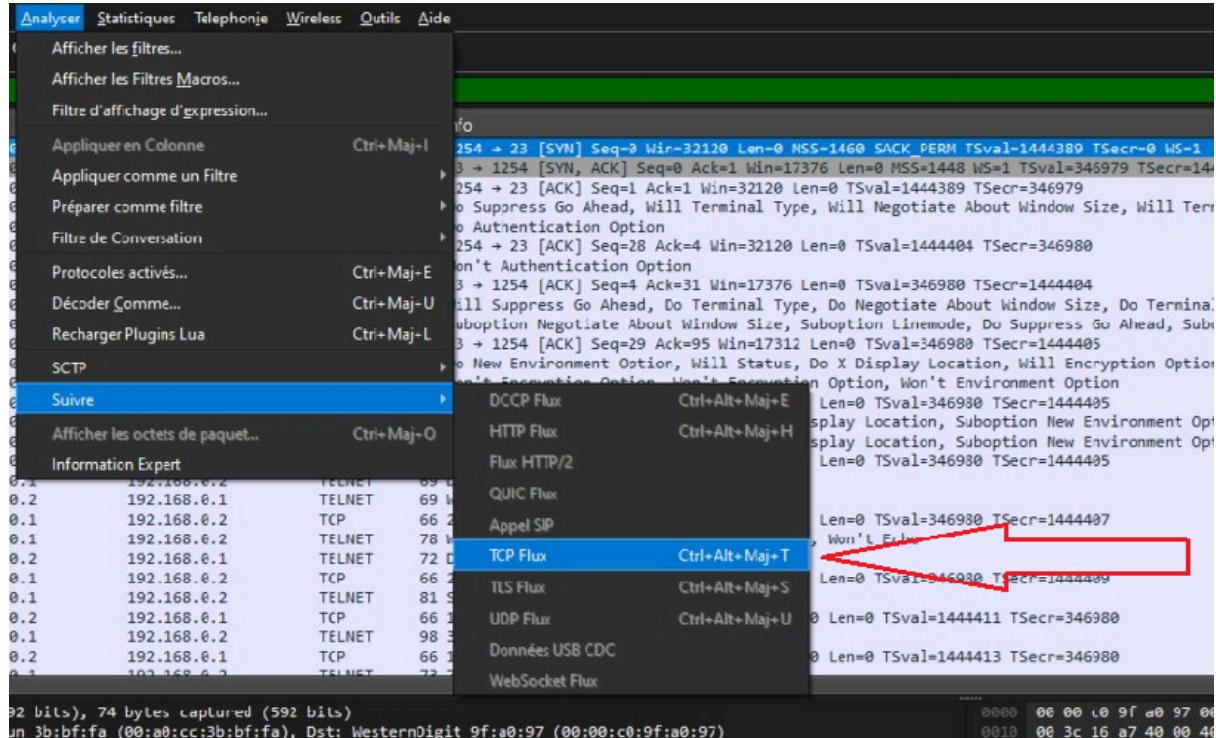
Bien joué, vous remportez 5 Points

N'oubliez pas de noter ce challenge en donnant votre avis :)

2-3 TELNET – authentification

Le but de cet exercice est de retrouver le mdp de l'utilisateur dans cette capture réseau de session TELNET.

En analysant le flux TCP de la capture réseau TELNET via Wireshark, nous avons pu extraire le mot de passe de l'utilisateur.



Puis nous trouvons le mot de passe dans l'analyse de la trame

```
Wireshark - Suivre le flux TCP (tcp.stream eq 0) - ch2.pcap

[...]
P.....b.....b.....B.
'#, 8, 8, 5
8, 8, 5
#.....]
..9600,9600...#.bam.zing.org:0.0...'.DISPLAY.bam.zing.org:0.0.....xterm-color..
[...]
OpenBSD/1.386 (oof) (tty1)

login:
t
f
a
a
k
k
e
e
.

Password: user ➡
Last login: Thu Dec  2 21:32:59 on ttys0 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code. With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ 1
1
5
5
.
$ 1
1
```

Le mot de passe est donc “user” .



Root Me

[Home](#) [About](#) [Contact](#) [Logout](#)

Rechercher

1343 visiteurs en ce moment

derniers inscrits :

- Artemar yDk Nmon6200
- Arieli H Zuken PanTrister
- mathis

Offres

 CDI Consultant sécurité

Sponsorié par

- Algosecure
- Almond
- École 2600
- Elysium Security
- GEOIDE
- Oteria Cyber School
- Synactiv
- Vous ;-)

Auteur

g0uZ, 30 août 2010

Niveau

①

Validations

90398 Challenger

Partager

Note

①

5565 votes

J'aime

Je n'aime pas

Énoncé

Retrouvez le mot de passe de l'utilisateur dans cette capture réseau de session TELNET.

Télécharger le challenge

2 vulnérabilités

-  Wireshark - TELNET et FTP
-  Outil - Wireshark

1 ressource(s) associée(s)

-  rfc854 (RFC)

Validation

Bien joué, vous remportez 5 Points

N'oubliez pas de noter ce challenge en donnant votre avis ;-)

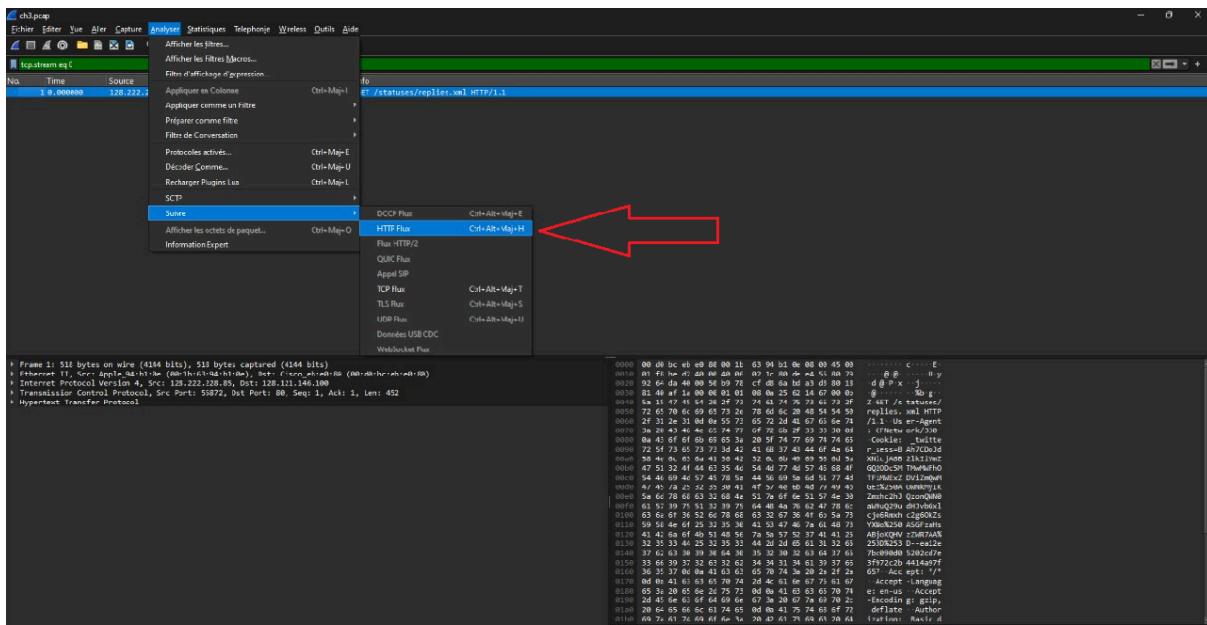
 twitez le !

Entrer le mot de passe

2-3 Authentification Twitter

Le but de cette mission est de retrouver le mot de passe d'un l'utilisateur Twitter dans une capture réseau.

Pour y parvenir, nous avons analysé la trame avec le fux HTTP via Wireshark



Puis nous apercevons le mot de passe dans l'analyse de la trame, mais cette fois ci, il est hashé.

```
GET /statuses/replies.xml HTTP/1.1
User-Agent: CFNetwork/3.0
Cookie: _twitter_sess=BAh7CDoJxNlcjA6B2lkIiVmZGQ20c5MTIw!%FhOTF1M!ExZDV1zmqw!Gez%250AO!Nk!yIKZmxhc2hJQzonQ!n8uQ29udHJvbGxlcjo6Rmxhc2g6OkzsYXNo%250ASGFzaHsAbjoKQHVz!r7AA%253D%253D-e12e7bc090d05202c7de3f972c2b441a97f657
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Authorization: Basic dXNlcnRlc3Q6cGFzc3dvcmQ=
Connection: keep-alive
Host: twitter.com
```

Nous avons décodé le mot de passe en utilisant un décodeur base64, le hash étant identifié dans ce format.

Décodage à partir du format Base64

Il suffit de saisir vos données et d'appuyer sur le bouton de décodage.

dXNlcnRlc3Q6cGFzc3dvcmQ=

Pour les binaires encodés (comme les images, les documents, etc.), utilisez le formulaire de téléchargement de fichiers un peu plus bas sur cette page.

UTF-8 Jeu de caractères source.

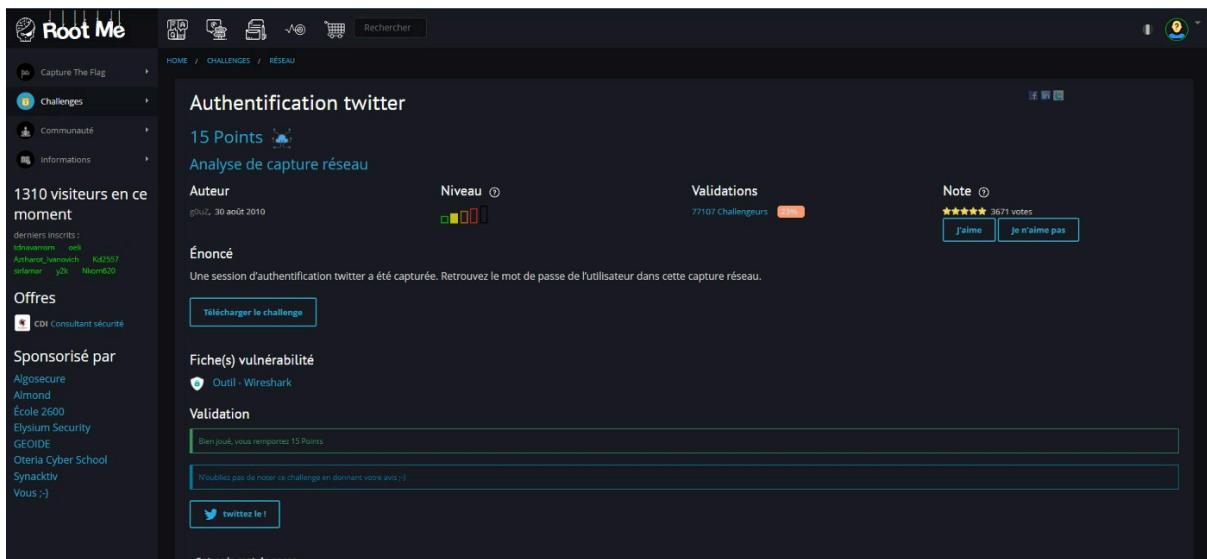
Décoder chaque ligne séparément (utile lorsque vous avez plusieurs entrées).

Mode direct OFF Décodage en temps réel alors que vous tapez ou collez (prenant en charge uniquement le jeu de caractères UTF-8).

< DÉCODAGE > Décodage de vos données dans la zone ci-dessous.

user: test:password

Donc le mot de passe est password



Royal Mail (janvier 2023)

- **Vulnérabilité exploitée** : Attaque par ransomware du groupe LockBit, exploitant des systèmes Windows mal protégés.
- **Dommages** : Suspension des services d'exportation internationaux, retards dans la distribution du courrier national, fuite de données sensibles du personnel. Royal Mail a choisi de ne pas payer la rançon et a dépensé 10 millions de livres pour renforcer sa cybersécurité

ABB (mai 2023)

- **Vulnérabilité exploitée** : Attaque par ransomware du groupe Black Basta, ciblant les vulnérabilités de l'Active Directory Windows.
- **Dommages** : Arrêt des opérations et fuite de données sensibles de l'entreprise. ABB a dû suspendre temporairement les connexions VPN avec ses clients

MGM Resorts (septembre 2023)

- **Vulnérabilité exploitée** : Exploitation de vulnérabilités dans les systèmes internes utilisés par les casinos et hôtels, notamment sur les infrastructures Windows.
- **Dommages** : Suspension des services essentiels tels que les clés de chambre, les machines à sous et les réservations, coûtant à MGM plus de 100 millions de dollars. Les données personnelles des clients, incluant des informations sensibles comme des numéros de carte d'identité, ont été compromises

ICMR - Indian Council of Medical Research (octobre 2023)

- **Vulnérabilité exploitée** : Fuite de données en raison de la mauvaise protection d'une base de données de tests Covid.
- **Dommages** : Exposition des données personnelles de 815 millions d'individus, incluant des identifiants sensibles comme le numéro Aadhaar

Violation MOVEit Transfer (2023)

- **Vulnérabilité exploitée** : Exploitation des failles du logiciel MOVEit Transfer, entraînant d'importantes violations de données.
- **Dommages** : Exposition des informations personnelles de santé de plus de 3,4 millions de personnes, avec des menaces de publication publique des données si la rançon n'était pas payée