**B3.3 - SEQ1-S2**

**Réalisation des tests d’intrusion**

**Situation professionnelle**

Vous êtes chargé de réaliser des tests d’intrusion, au niveau des éléments d’authentification, auprès de la société Calypso. Pour pouvoir accomplir cette tâche, vous devez disposer d’une machine virtuelle sous Windows 7 et d’une distribution Kali Linux.

**Vos missions**

Vous devez accomplir trois missions à l’aide des documents (1, 2, 3 et 4) contenant les informations de configuration nécessaires.

**Mission 1 : Préparation des tests (Documents 1 et 2)**

La réalisation des tests nécessite de passer par les étapes suivantes :

* Présenter le type d’audit que vous devez réaliser ;
* Préparer la machine virtuelle Windows 7 ;
* Configurer l’environnement de travail Kali Linux.

**Mission 2 : Réalisation des tests (Document 3 et 4)**

Vous allez réaliser deux types de test « Force brute » et « Dictionnaire » qui vont vous permettre de trouver ou non les identifiants et mots de passe de chaque compte, après avoir récupéré la base SAM (Security Account Manager : Gestionnaire des comptes de sécurité).

Suivez les étapes ci-dessous en utilisant Kali :

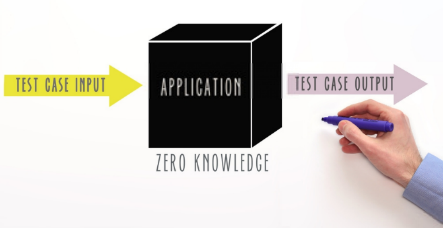
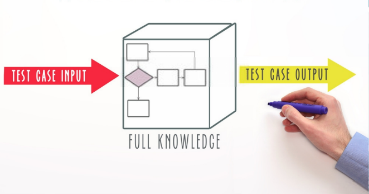
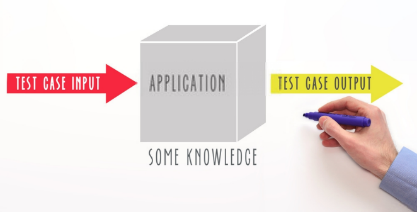
* Exécuter le test proposé par Ophcrack ;
* Exécuter les différents tests proposés par l’outil John The Ripper ;
* Exécuter le test à l’aide de Hashcat ;
* Noter les identifiants et mots de passe trouvés et tirer les conclusions qui en découlent. (Répondre aux questions 1 à 7).

**Mission 3 : Mesures de sécurité à prendre**

* Modifier le mot de passe du compte en prenant les mesures pour renforcer la sécurité de l’authentification ;
* Réaliser à nouveau les deux types de tests faits auparavant ;
* Proposer les critères permettant d’améliorer la sécurité des mots de passe, en répondant à la question 8).

**Document 1 : Pentest ou test d’intrusion**

|  |
| --- |
| Un **test d'intrusion** (« *penetration test* » ou « *pentest* », en anglais) est une méthode d'évaluation (« [audit](https://fr.wikipedia.org/wiki/Audit) », en anglais) de la [sécurité](https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_du_syst%C3%A8me_d%27information) d'un [système d'information](https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27information) ou d'un [réseau informatique](https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique) ; il est réalisé par un testeur « *pentester* ».  La méthode consiste généralement à analyser l'infrastructure d'un [réseau informatique](https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique), afin de simuler l'attaque d'un utilisateur mal intentionné, voire d'un [logiciel malveillant](https://fr.wikipedia.org/wiki/Logiciel_malveillant) (« [malware](https://fr.wikipedia.org/wiki/Logiciel_malveillant) »). Le consultant (« *pentester* ») analyse alors les risques potentiels dus à une mauvaise [configuration](https://fr.wikipedia.org/wiki/Configuration_(informatique)) d'un [système d'information](https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27information), d'un défaut de configuration, de [programmation informatique](https://fr.wikipedia.org/wiki/Programmation_informatique) ou encore d'une [vulnérabilité](https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9_(informatique)) liée à la solution testée. |



|  |  |  |
| --- | --- | --- |
| Dans une mission de test de boîte noire, le testeur de pénétration est placé dans le rôle du pirate informatique, sans aucune connaissance interne du système cible. Les testeurs n’ont aucune information sur le système d’information sauf celles déjà publiquement disponible | Le second niveau des tests est le test en boîte grise, ou Gray Box. Alors que le testeur en boite noire n’a presque aucune information sur le système d’information ciblé, celui pratiquant un test en boite grise dispose des niveaux d’accès et de connaissances d’un utilisateur du SI, voire même avec des privilèges élevés sur un système. | Les tests en boîte blanche portent plusieurs noms différents, y compris les tests de boîte transparente, de boîte ouverte, auxiliaire et logique. Il se situe à l’opposé des tests en boîte noire et les testeurs de pénétration bénéficient d’un accès complet au code source, schémas d’architecture, etc. |

**Document 2 : Environnement de travail Windows 7 & Kali**

* Importer la machine virtuelle Windows 7 dans VirtualBox ;
* Démarrer la MV Windows 7 ;
* S’authentifier sur Windows 7 :

Identifiant : pergaud

Mot de passe : louis

* Créer sept utilisateurs et leurs mots de passe :
* User1 avec un mot de passe de cinq caractères en lettres minuscules :

(Exemple btsio) ;

* User2 avec un mot de passe de cinq caractères en lettres minuscules incluant un chiffre et un caractère spécial : (exemple bts1#) ;
* User3 avec un mot de passe de six caractères en lettres minuscule :

Exemple btssio ;

* User4 avec un mot de passe de six caractères incluant une majuscule :

Exemple Btssio.

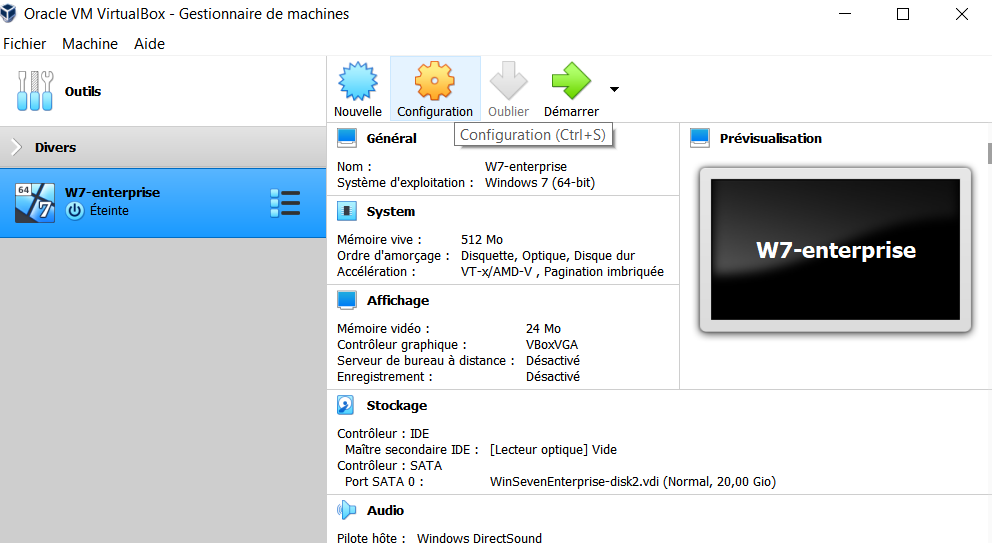
* User5 avec un mot de passe de six caractères plus un chiffre :

Exemple btssio1.

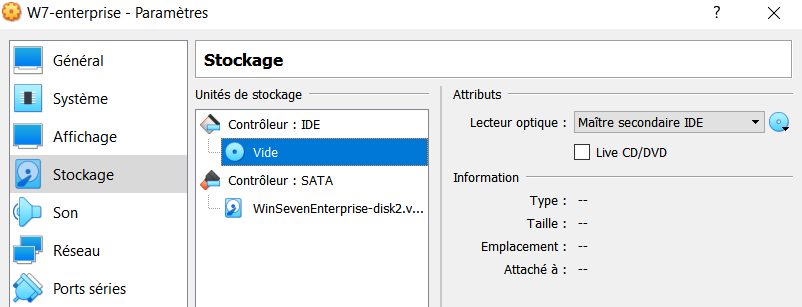
* User6 avec le mot de passe : harrypotter
* User7 avec le mot de passe : TheMatrix#1

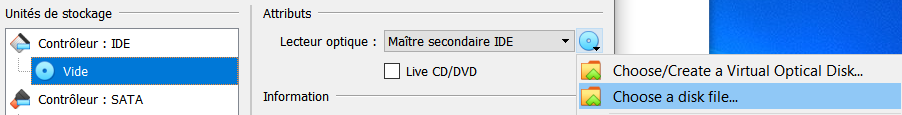


* Importer la machine virtuelle Kali.
* Pour démarrer Windows 7 à partir de la machine virtuelle Kali, il faut suivre les étapes suivantes :
* Etape 1 : Dans les paramètres « Configuration » de Windows 7, choisir « Stockage » puis ajouter un disque dur ;

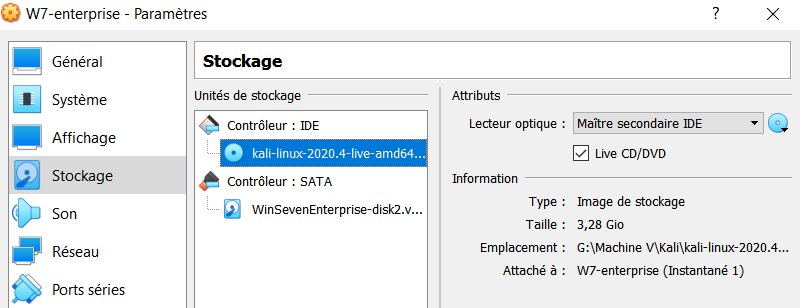
**o**

* Etape 2 : Sélectionner l’emplacement « vide », puis « choisir un disque » ;

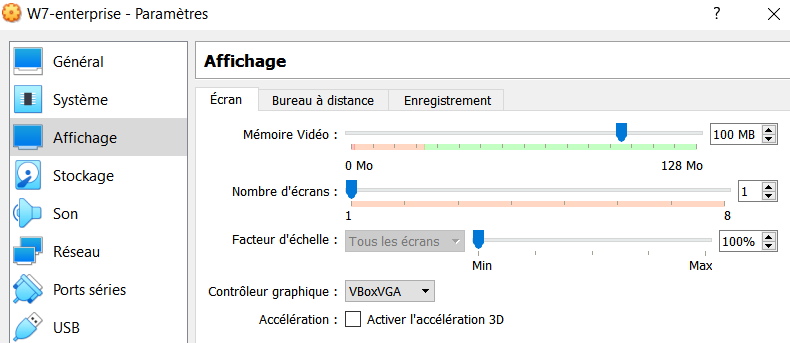
****

****

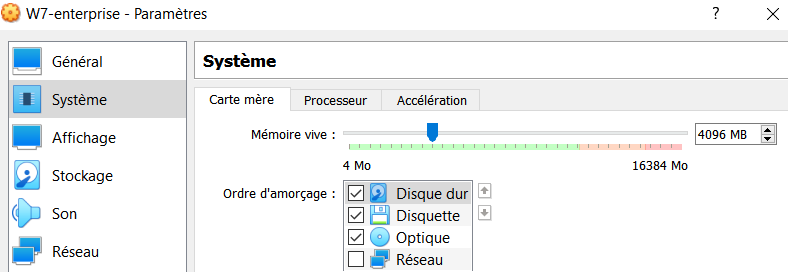
Etape 3 : Cocher la case « Live CD/DVD » ;

****

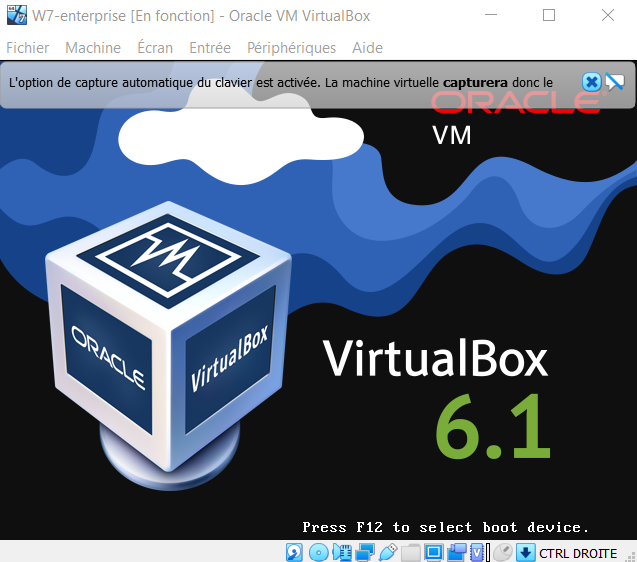
Etape 4 : Dans le paramètre « Affichage », augmenter la mémoire vidéo à 100 MB ;

****

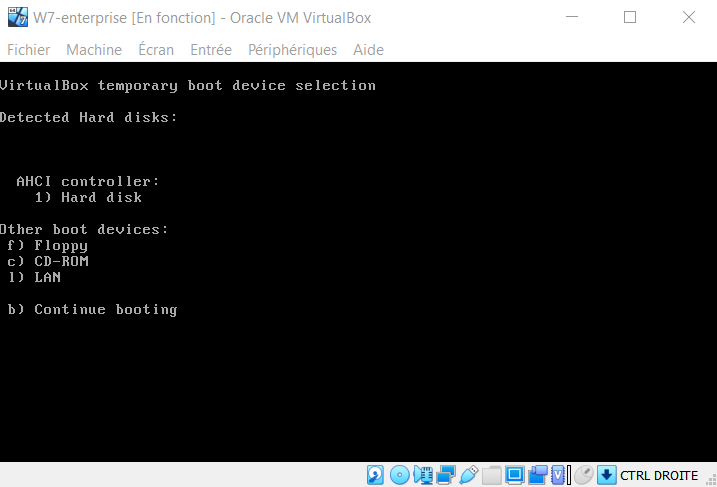
Etape 5 : Changer l’ordre d’amorçage en mettant « Disque dur » en premier.

****

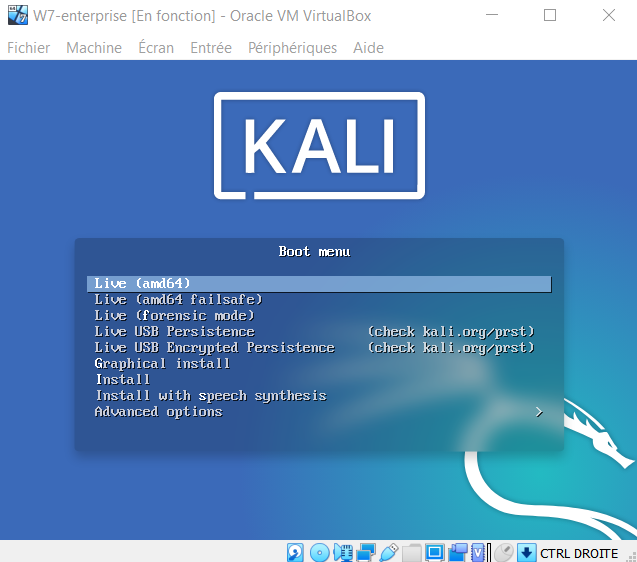
Etape 6 : Démarrer la MV Windows 7, puis appuyer **rapidement** sur la touche « F12 ».



Etape 7 : Appuyer sur la touche « c » pour choisir le démarrage à partir du Live CD.



Etape 8 : Choisir la première option « Live (amd64) »



**Kali Linux** est une [distribution GNU/Linux](https://fr.wikipedia.org/wiki/Distribution_Linux) basée sur [Debian](https://fr.wikipedia.org/wiki/Debian), elle est financée et maintenue à jour par [Offensive Security](https://en.wikipedia.org/wiki/Offensive_Security) (société internationale américaine active dans les [domaines de la sécurité de l'information](https://en.wikipedia.org/wiki/Information_security) , des [tests d'intrusion](https://en.wikipedia.org/wiki/Penetration_testing) et de [la criminalistique numérique](https://en.wikipedia.org/wiki/Digital_forensics)).

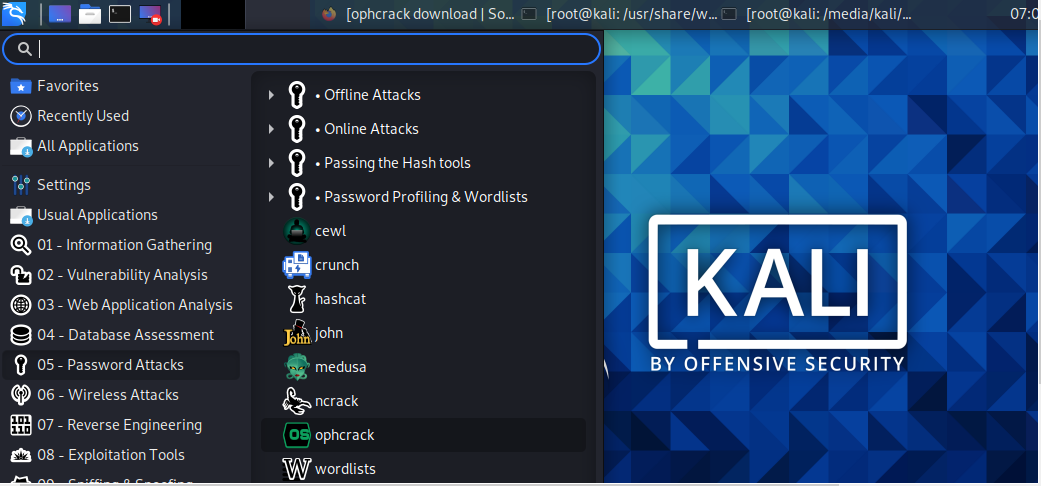
L'objectif de Kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de [sécurité d'un système d'information](https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27information), notamment le [test d'intrusion](https://fr.wikipedia.org/wiki/Test_d%27intrusion).

**Document 3 : Utilisation du logiciel Ophcrack**

Ophcrack est un [logiciel libre](https://fr.wikipedia.org/wiki/Logiciel_libre) permettant de [casser les mots de passe](https://fr.wikipedia.org/wiki/Cassage_de_mot_de_passe) des utilisateurs de systèmes d'exploitation Windows stockés en [LM hash](https://fr.wikipedia.org/wiki/LM_hash) et aussi en NT hash en utilisant les [tables arc-en-ciel](https://fr.wikipedia.org/wiki/Table_arc-en-ciel). Il permet de récupérer la base SAM qui contient les identifiants des comptes utilisateurs ainsi que leur mot de passe sous forme de hash : algorithme MD5, LM ou NTLM.

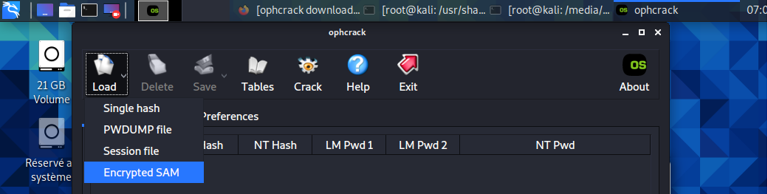
**Utilisation d’Ophcrack à l’aide des figures ci-dessous :**

* Chercher le logiciel Ophcrack dans le menu des applications de Kali, puis dans l’onglet « Password Attacks » **(fig1) ;**

**Figure 1**

* Dans le menu Ophcrack, aller dans l’onglet « Load » puis « Encrypted SAM » (**fig 2**);

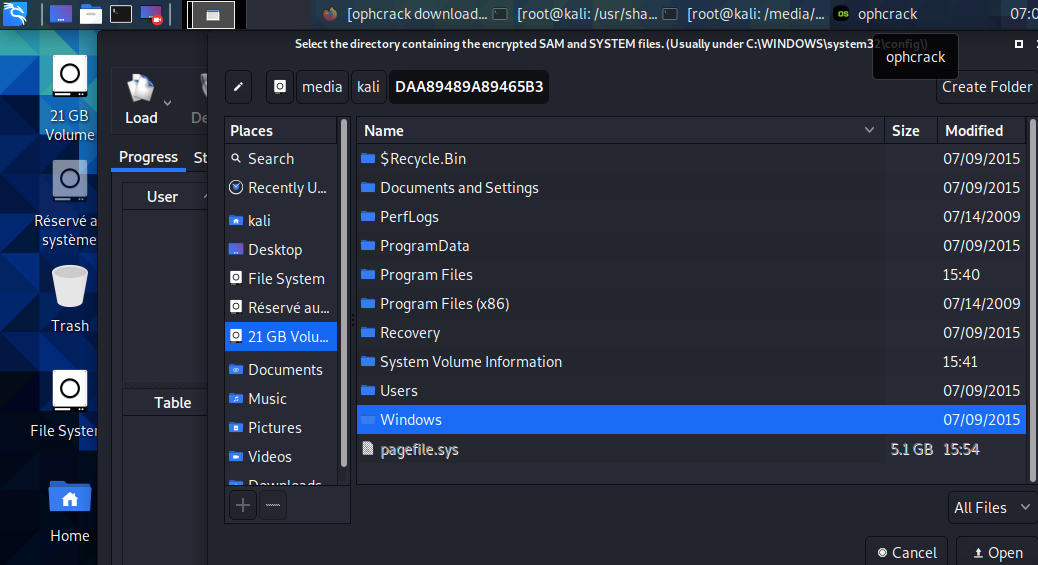
**Figure 2**



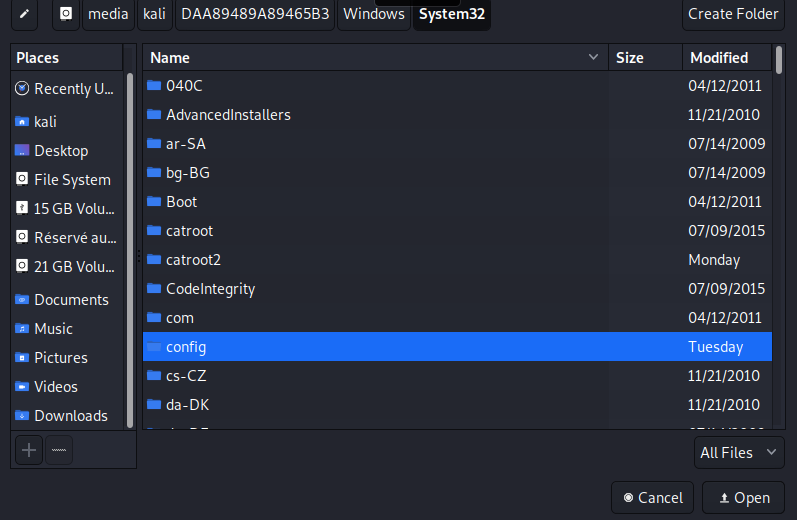
* Chercher le répertoire « **config »** en suivant le chemin suivant :

=> **/media/kali/.. /Windows/System32/config**, puis cliquer sur **Open** (**fig 3, fig 4 et fig 5**);

**Figure 3**

****

**Figure 4**

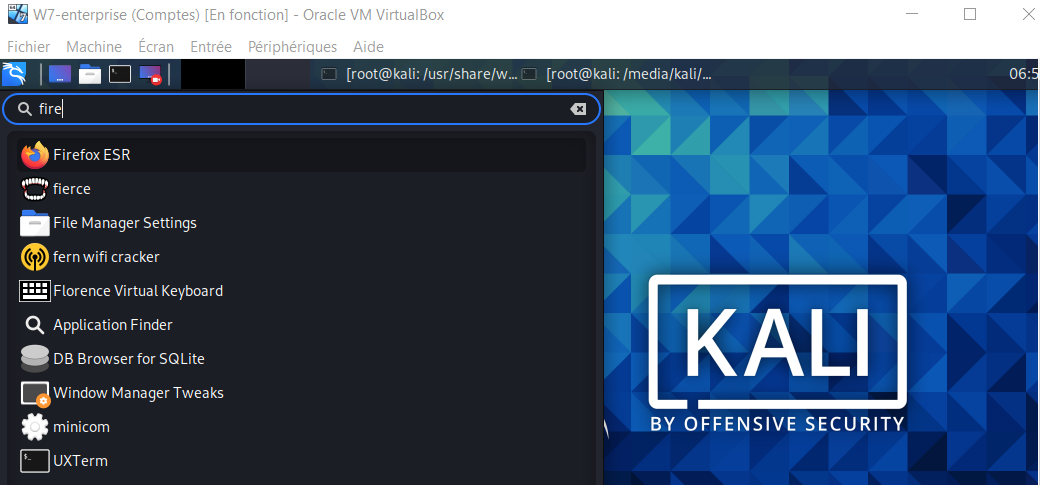
****

**Figure 5**

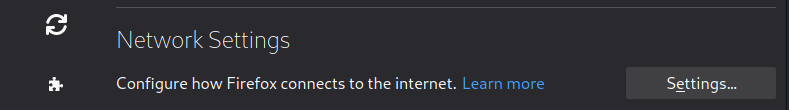
****

* Configurer le navigateur Firefox en y intégrant l’adresse IP et le port du proxy **(fig 6, fig 7 et fig 8)** ;
* Aller dans « **Menu** » => « **Préférences** », puis tout en bas dans « **Network settings** », cliquer sur « **Settings** » ;
* Renseigner l’adresse IP et le port du proxy, sans oublier de cocher la case : « **Also use this proxy for FTP and HTTPS**» ;

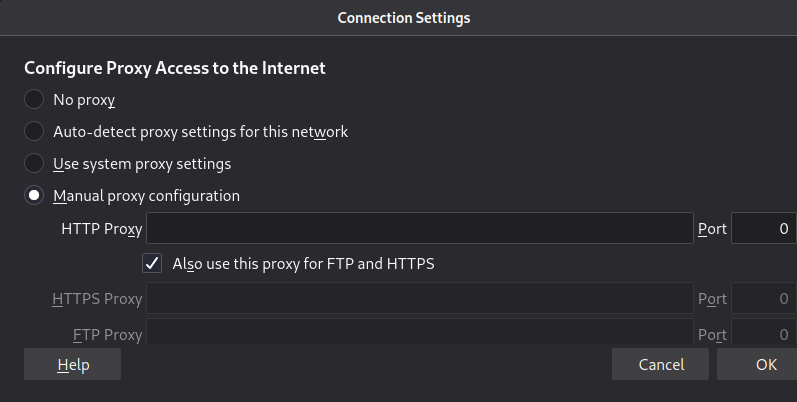
**Figure 6**



**Figure 7**



**Figure 8**

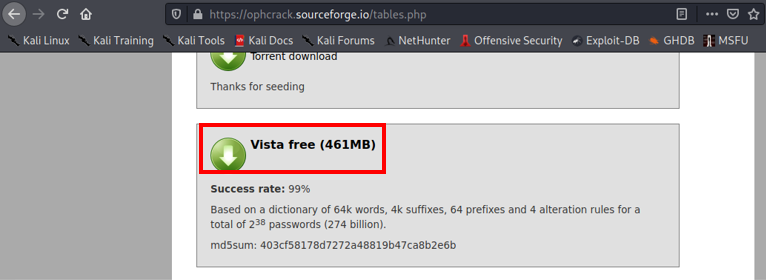


* Télécharger la table Vista free sur le site : <https://ophcrack.sourceforge.io>, à partir du navigateur Firefox**(fig 9 et fig 10**).

**Figure 9**

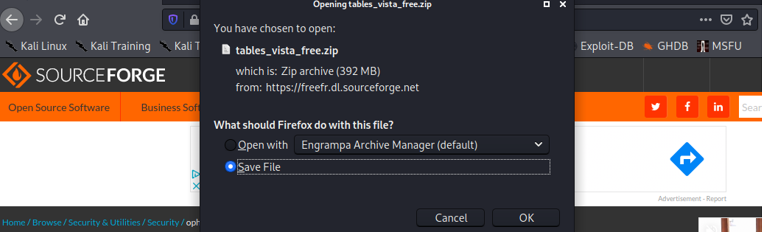
****

**Figure 10**

****

* Enregistrer puis extraire la table **(fig 11 et fig 12)** ;

**Figure 11**

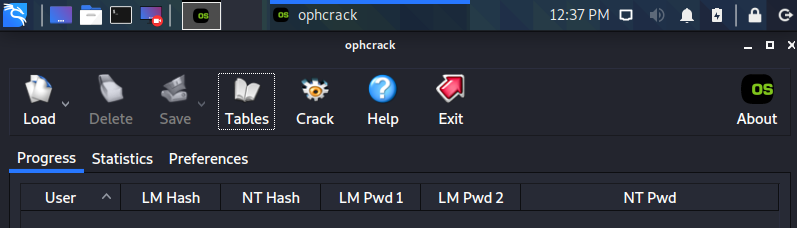
****

**Figure 12**

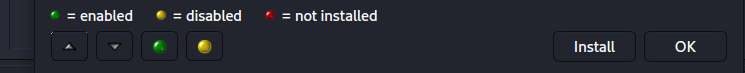
****

* Installer la table Vista free (**fig 13, fig 14, fig 15 et fig 16**);

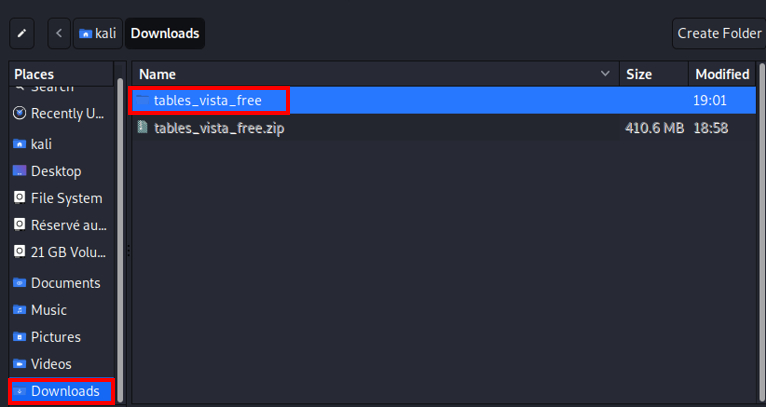
**Figure 13**

****

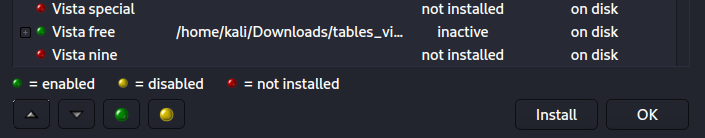
**Figure 14**

****

**Figure 15**

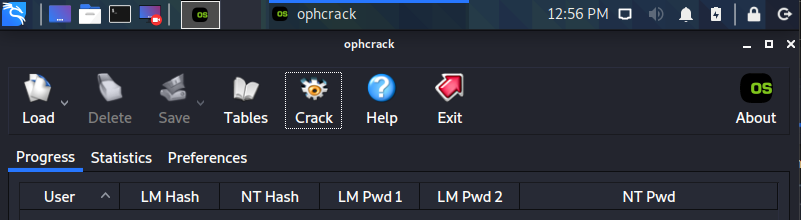
****

**Figure 16**

****

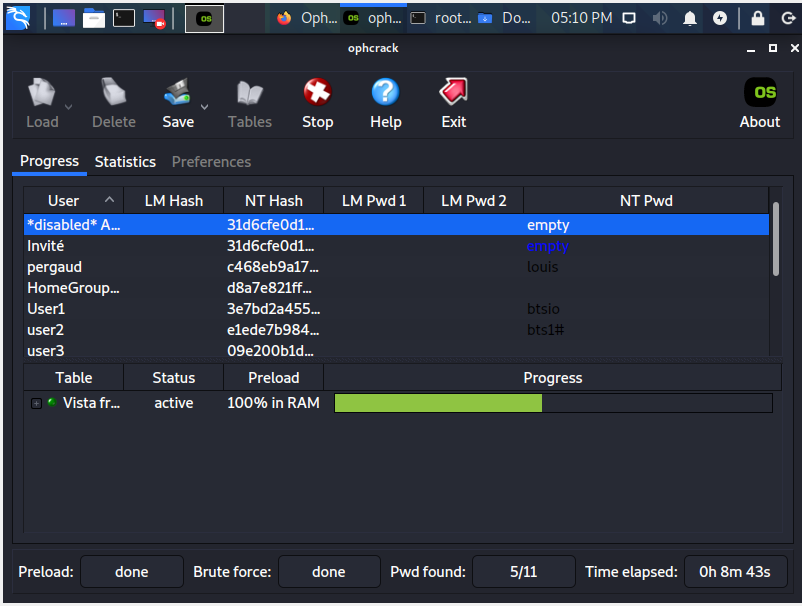
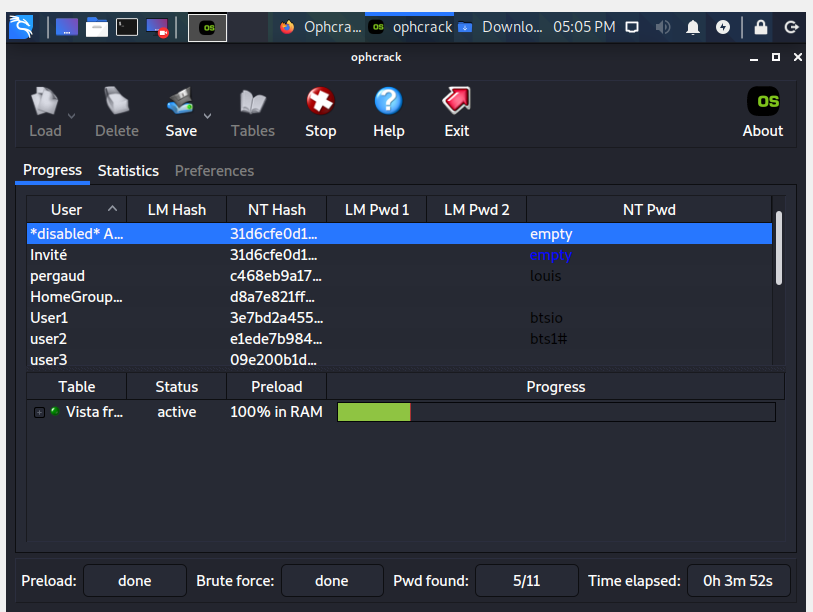
* Lancer le crack **(fig 17).**

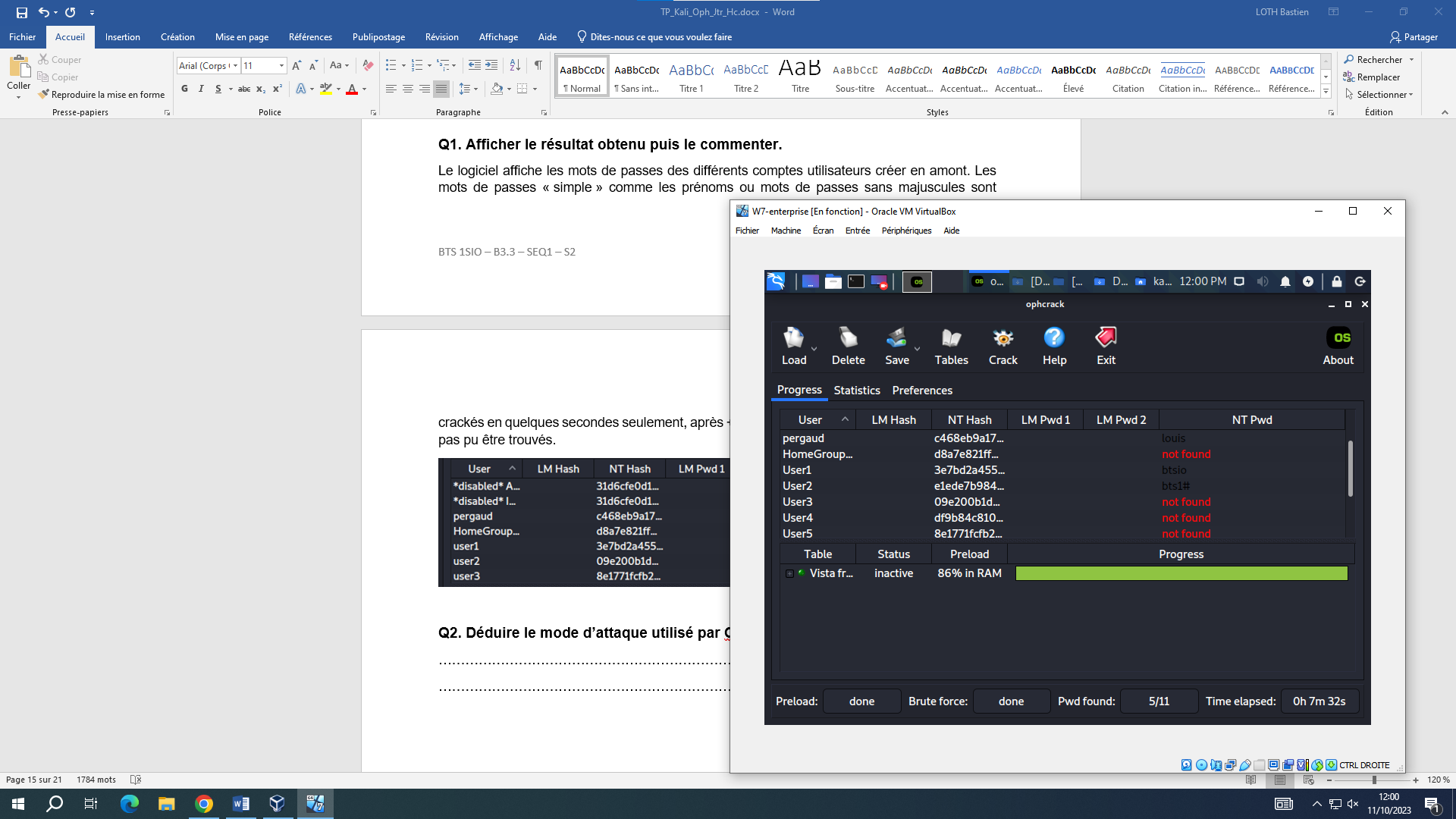
**Figure 17**

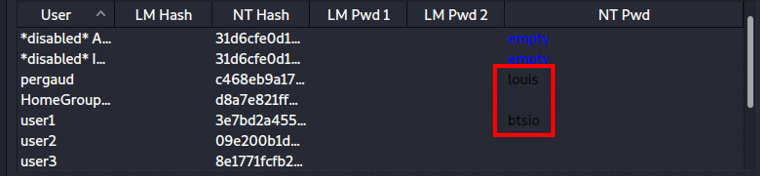
****

**Q1. Afficher le résultat obtenu puis le commenter.**

Le logiciel affiche les mots de passes des différents comptes utilisateurs créer en amont. Les mots de passes « simple » comme les prénoms ou mots de passes sans majuscules sont crackés en quelques secondes seulement, après +7min les mots de passes plus sécurisés n’ont pas pu être trouvés

. 





**Q2. Déduire le mode d’attaque utilisé par Ophcrack.**

En vue du temps nécessaire au craquage des mots de passes, on peut en déduire que Ophcrack utilise la méthode du dictionnaire car les prénoms et autres mots clés ont été trouvés très rapidement.

**Document 4 : Utilisation de John The Ripper et Hashcat**

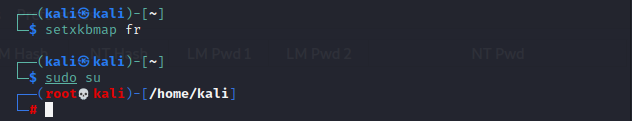
*John the Ripper* (ou *JTR*, ou *John*) est un [logiciel libre](https://fr.wikipedia.org/wiki/Logiciel_libre)  utilisé notamment pour tester la sécurité d'un mot de passe ([audit](https://fr.wikipedia.org/wiki/Audit_informatique), [crack](https://fr.wikipedia.org/wiki/Crack_(informatique))). John est capable d'attaquer les mots de passe hachés avec différentes fonctions de hachage, notamment les algorithmes suivants : [*MD5*](https://fr.wikipedia.org/wiki/MD5), *[Blowfish](https://fr.wikipedia.org/wiki/Blowfish" \o "Blowfish)*, [*Kerberos*](https://fr.wikipedia.org/wiki/Kerberos_(protocole)), [AFS](https://fr.wikipedia.org/wiki/Andrew_File_System), et les [*LM hashes*](https://fr.wikipedia.org/wiki/LM_hash) des anciennes versions de Windows ainsi que les mots de passe [NTLM](https://fr.wikipedia.org/wiki/NTLM), pour les dernières versions de Windows. Il utilise plusieurs types d’attaque : Single (simple), Wordlist (dictionnaire) ou Incremental(incrémental).

**Les étapes en ligne de commande :**

* Au démarrage de Kali, le clavier est en « Querty », il faudra le mettre en « Azerty » :
* Ouvrir le terminal puis mettre le clavier en français avec la commande :

 setxkbmap fr ;

* Passer en mode root avec la commande : **sudo su**.
* En cas de mise en veille de Kali, l’identifiant est « **kali** » et le mot de passe est « **kali**». Attention le clavier est en « Querty » !



* Récupérer la base SAM (fichiers SAM et SYSTEM) :

|  |
| --- |
| * Se positionner dans le répertoire config : * En copiant le chemin à partir de l’explorateur ;      * Ou avec un clic droit sur le répertoire « config » ;      * Passer en mode root.      * Extraire les hashs et les copier dans un fichier texte :      * Afficher les hashs récupérés :      * **Lancer l’attaque à l’aide de JTR** * **Utilisation du dictionnaire par défaut :**   John utilise par défaut le dictionnaire password.lst qui se trouve dans le dossier :  /usr/share/john/password.lst.    **Q3. Que constatez-vous ?**  On voit le type d’encodage utiliser et la clés pour le déverrouiller     * **Utilisation du type de hachage :**     **Q4. Afficher le résultat obtenu à l’aide de la commande appropriée.**     * **Utilisation d’un dictionnaire externe (exemple rockyou.txt) :**   Il existe un autre dictionnaire nommé rockyou.txt qui se trouve dans le dossier :  wordlists => /usr/share/wordlists.  Il doit être dézippé pour être utilisé à l’aide de la commande gunzip.  La commande « ls » permet d’afficher le contenu du répertoire « wordlists »    Utilisation du dictionnaire rockyou.txt :    **Q5. Quel résultat obtenez-vous ?**  **On vois que l’on obtient le mots de passe qui a première vue sembler difficile a trouver**     * **Utilisation de l’attaque incrémentale**     **Q6. Commenter puis afficher le résultat obtenu.**  **Cette façon et long et elle fait toutes les combinaisons possibles jusqu’à trouver un mots de passe puis continue jusqu’à trouver tous les mots de passe.**  **Avec plus de temps j’aurai pu trouver plus de code.**    **Lancer l’attaque à l’aide de Hashcat**  Hashcat est un utilitaire de récupération de mots de passe réputé pour son efficacité. Il est très utilisé par les pen-testeurs et les administrateurs systèmes. Il peut prendre en charge cinq modes d'attaque uniques pour près de 300 algorithmes de hachage hautement optimisés. Il permet d’utiliser un ou plusieurs CPU ou GPU.    Explication des options :  -m : type de hash => 1000 correspond au hash NTLM  -a : mode d’attaque => 3 correspond à la force brute  **Q7. Commenter puis afficher le résultat obtenu.**  Remarque : pour afficher les résultats, utiliser la commande --show :      **Q8. Quels critères proposez-vous afin d’optimiser la sécurité d’un mot de passe ?** |

Les critères pour optimiser un mot de passe sont : le nombre de caractère, le nombre de chiffre, le nombre de caractère présent.

