CHAPITRE 4

Travaux en laboratoire informatique

1 Informer les utilisateurs sur les risques et promouvoir les bons usages à adopter

> Fiche savoirs technologiques 4

M. Brillat souhaite réaliser un audit sur la robustesse des identifiants de connexion des différents partenaires, afin de s'assurer que la sensibilisation des utilisateurs a été efficace. Pour cela, il décide de faire réaliser des tests d'usurpation des éléments de connexion. Pour réaliser cette tâche, vous devez disposer d'une machine virtuelle sous Windows 10 et d'une distribution live Kali Linux en fichier ISO.

ÉTAPE 1 Préparation des tests

Plusieurs étapes sont préalables à la réalisation des tests : préparer les différents environnements de test, extraire les fichiers SYSTEM et SAM, accéder aux dossiers et fichiers de la partition Windows à partir de la distribution live Kali et ajouter la table vista_proba_free.

1. **Préparez la machine virtuelle Windows 10 en reprenant les éléments mentionnés dans le guide de configuration.**
   > Document 1
   > Logiciel : www.lienmini.fr/882-03
2. **Configurez l'environnement de travail Kali selon les commandes fournies dans le document.**
   > Document 2
   > Machine virtuelle : www.lienmini.fr/882-04

ÉTAPE 2 Première réalisation des tests

Votre environnement de travail est maintenant opérationnel. Vous allez réaliser trois types de tests (« simple », « dictionnaire » et « force brute ») qui vous permettront de trouver ou non les identifiants et mots de passe de chaque compte présent dans le fichier 127.0.0.1.pwdump.

3. **Exécutez les différents tests proposés par l'outil John the Ripper. Pour cela, appuyez-vous sur les indications détaillées fournies.**
   > Document 3
4. **Notez les identifiants trouvés et tirez les conclusions qui en découlent.**

ÉTAPE 3 Seconde réalisation des tests

Vous utilisez l'outil Ophcrack pour réaliser un test grâce à une table arc-en-ciel (*rainbow table*) et ainsi tenter de trouver les mots de passe manquants.

5. **Exécutez le test à partir d'Ophcrack.**
6. **Proposez, d'après vos observations, plusieurs critères qui permettent d'améliorer la sécurité des mots de passe.**

> Voir lexique BTS SIO, p. 221

Document 1 Guide de configuration de la machine virtuelle Windows de test

❶ Sur la machine virtuelle Windows 10, s'authentifier avec le compte administrateur (défini lors de l'installation de la VM) et créer trois comptes appartenant au groupe Administrateurs :
- ENEDIS, avec un mot de passe de moins de huit caractères alphanumériques (exemple : judo63) ;
- MSA, avec un mot de passe de plus de 8 caractères alphanumériques (exemple : aurillac15) ;
- CLIC, avec un mot de passe selon votre choix.

❷ Désactiver la protection en temps réelle et le contrôle des applications.

❸ Télécharger, décompresser et exécuter l'outil FGDUMP en tant qu'administrateur sur votre bureau. Il permet d'extraire le contenu des fichiers SYSTEM et SAM dans un fichier nommé 127.0.0.1.pwdump.

❹ Télécharger et installer Notepad++. Ouvrir le fichier 127.0.0.1.pwdump et conserver uniquement les identifiants des utilisateurs créés précédemment.

❺ Télécharger et décompresser sur votre bureau le fichier zippé « vista_proba_free.zip ».

Document 2 Commandes pour la préparation de l'environnement Kali

Commandes à réaliser :

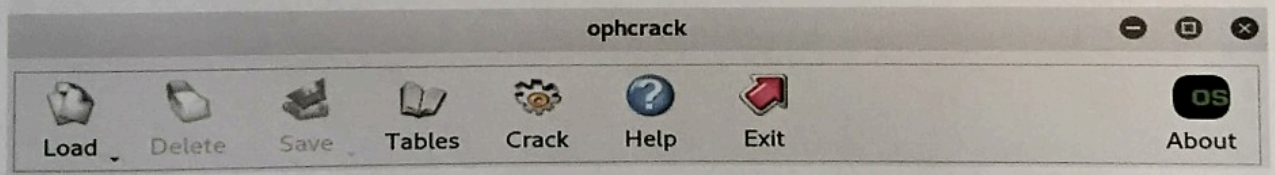
❶ Au lancement de la machine virtuelle Windows 10, le *boot* (démarrage) sera réalisé sur le lecteur de disque avec l'ISO du live CD Kali comme support.

❷ Modifier le clavier QWERTY en AZERTY avec la commande **setxkbmap fr**.

❸ Repérer la partition Windows à utiliser pour les tests, avec la commande **fdisk -l**. Généralement, les différentes partitions sont représentées par le mot « **sdax** » ou « **nvme0n1px** » où **x** représente un numéro. Il est probable que la partition la plus volumineuse soit celle recherchée. Noter le nom de la partition.

❹ Vous pouvez maintenant accéder aux dossiers et fichiers de la partition Windows : pour réaliser les tests, vous devez utiliser le fichier **127.0.0.1.pwdump** présent sur le bureau de l'utilisateur administrateur créé lors de l'installation de la VM. Le chemin de ce fichier sera : **/media/kali/UUID_Partition/Users/nom_utilisateur/Desktop/** (UUID est affiché lors de l'ouverture du dossier).

❺ Notez ce chemin, il vous sera utile lorsque que vous utiliserez l'outil **Ophcrack** (**Applications ➔ 05 - Password Attacks**) et que vous demanderez à charger « **Load** » le fichier **PWDUMP** (127.0.0.1.pwdump), afin de réaliser l'attaque avec la table arc-en-ciel (bouton « **Table** », puis bouton « **Install** »).



© DR

Document 3 Tests à l'aide de l'outil John the Ripper

John the Ripper permet de tester la robustesse des mots de passe en utilisant plusieurs types d'attaques :
- en transformant le nom des utilisateurs pour définir un mot de passe ;
- à l'aide d'un dictionnaire qui correspond à un fichier avec un ensemble de mots de passe prédéfinis ;
- en testant l'ensemble des combinaisons possibles (une attaque en force brute).

Commandes	Explications
john --single /chemin/nom-fichier	Transforme les identifiants présents dans le fichier Exemple : ENEDIS devient enedis12, enedis1234...
john --wordlist /chemin/nom-fichier	Test avec le dictionnaire par défaut password.lst
john --wordlist=NomDictionnaire.ext /chemin/nom-fichier	Choix d'un dictionnaire différent
john --wordlist=NomDictionnaire.ext --rules /chemin/nom-fichier	Combinaisons hybrides (exemple : a ↔ @)
john --incremental /chemin/nom-fichier	Force brute
john --show /chemin/nom-fichier	Permet d'afficher les mots de passe récupérés

Remarques :
- Vous devez spécifier le format du hash : **--format=NT**.
- Dézippez le dictionnaire **Rockyou.txt** avec la commande **gunzip**. Celui-ci se trouve dans le dossier **wordlists** : **/usr/share/wordlists/rockyou.txt.gz**.
- **password.lst** peut être modifié (**nano /usr/share/john/password.lst**) par l'ajout de ses propres mots de passe. On peut deviner par exemple qu'un utilisateur aura utilisé le lieu + son nom + un chiffre pour constituer son mot de passe : mspMsa2.

```
  GNU nano 2.8.7                File: password.lst                      Modified

#!comment: This list has been compiled by Solar Designer of Openwall Project
#!comment: in 1996 through 2011.  It is assumed to be in the public domain.
#!comment:
#!comment: This list is based on passwords most commonly seen on a set of Unix
#!comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!comment: (that is, more common passwords are listed first).  It has been
#!comment: revised to also include common website passwords from public lists
#!comment: of "top N passwords" from major community website compromises that
#!comment: occurred in 2006 through 2010.
#!comment:
#!comment: Last update: 2011/11/20 (3546 entries)
#!comment:
#!comment: For more wordlists, see http://www.openwall.com/wordlists/
mspMsa2
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
                          [ Read 3559 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell ^_ Go To Line
```

© DR

Travaux en laboratoire informatique Page 94
Étape 1
1) vboxuser est le premier compte admin
Créer 3 comptes administrateurs
ENEDIS/judo63 MSA/aurillac15 CLIC/Windows10TP17022025
CLIC 1003 ENEDIS 1001 MSA 1002
2) Périphériques → Lecteurs optiques → Choose a Disk File → kali linux
Démarrer la machine windows et spammer f12 et cliquer sur Live system (amd64)

Document 2 3) sda1
4 /media/kali/E418D5AA18D57BCC/Users/vboxuser/Desktop/

Étape 2 Document 3
3)

Informatique quantique : Utiliser des particules physiques et les architecturer en ensemble pour permettre de faire des calculs, accélérer le processus.
Ordinateur quantique : 1 millions de fois plus rapide qu'un ordinateur normal.
Électrons, lumière.
Chiffrer les données avec un ordinateur quantiques. Web service de chiffrement assurés par des ordinateurs quantiques
Chiffrement en 512B vers les MB.

19ème siècle Télégraphe : fils entre des villes, bips courts et longs, morse.
2nd guerre mondiale Chiffrement avec la machine Enigma et diffusion par ondes radio.
Almanac clé de chiffrement chaque jour pour Enigma
Point faible pendant la 2nd guerre mondiale : doctrinement nazie phrases terminée par Hitler.
Captcha test pour empêcher un dictionnaire ou un brute force d'entrer des mots de passes.
victime pour générer des mots de passes personnalisés.
Un Captcha analyse les réponses et la façon dont l'humain répond, vitesse, hésitation.
Test complètement automatisé de Turing pour différencier les signes humains.
Déterminer si l'utilisateur est un humain ou un ordinateur.

Pour se protéger des attaques par force brute/dictionnaire
- Double authentification
- sms SIM swapping
- application mobile
- mail
- app messagerie
- courrier postal
- Limiter le nombre de saisie de mots de passes possibles momentanément ou indéfiniment Attente entre les tentatives
- Utiliser des captcha pour déterminer si celui qui saisit le mot de passe est un être humain ou un ordinateur