Bloc 3 – Cybersécurité – BTS SIO 1

TP 1 commun en laboratoire informatique

Ch 6 – Assurer la sécurité des terminaux

Préambule

Le TP proposé est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains protocoles réseaux afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.

- **Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.**

Pour rappel, **l'article 323-1 du code pénal** stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Audit de la qualité de l'authentification sur les terminaux

Téléchargez la première partie de la maquette VirtualBox de l'entreprise Benoit Myon depuis le NAS de la section : \\172.16.20.5\commun\templates-Vbox\Bloc3-Sem2-InfraMyon-Part1.ova.

L'empreinte SHA-256, appelée aussi somme de contrôle, du fichier Bloc3-Sem2-InfraMyon-Part1.ova est : **a45bdd02d490796a21bbd6330ce206ed131479fab98216d7479de8cc0aa532dc**

Une fois le téléchargement du fichier en question effectué sur votre ordinateur, obtenir son empreinte SHA-256 à l'aide de l'invite de commandes et comparez-la à celle fournie précédemment.

1. Est-ce la même empreinte ? Pourquoi vous demande-t-on de réaliser cette vérification ? À quoi sert la somme de contrôle d'un fichier ?

Suite à une formation sur la sensibilisation à l'utilisation de mots de passe robuste, Mme Carlier souhaite réaliser un audit à propos des identifiants de connexion pour s'assurer que la formation des utilisateurs a été efficace. Pour cela, elle vous demande de réaliser un test d'intrusion physique sur des ordinateurs clients et dans un premier temps celui de la secrétaire.

Pour réaliser cette tâche, vous devrez avoir accès à la machine virtuelle de la secrétaire sous Windows 11 nommée « Bloc3-CyberSIO1-W11 » dans VirtualBox. Puis vous devrez démarrer sur un live DVD bootable Kali Linux au lieu du disque dur de la machine.

Étape 1 Préparation des tests

Plusieurs étapes sont nécessaires en amont de la réalisation des tests :

- Préparer les différents environnements indispensables aux tests d'intrusion.
- Récupérer la base SAM (Security Account Manager, « gestionnaire des comptes de sécurité ») et l'extraire dans un fichier.

2. Dans la peau de quel type d'attaquant allez-vous vous mettre lorsque vous allez réaliser le pentest auprès de l'entreprise Benoît Myon ? À l'aide de recherche sur Internet, définir quel type de pentest sera réalisé ?

À l'aide du document 2, paramétrez votre VM pour être en mesure de la faire démarrer sous Kali Linux et non sous Windows 11.

À l'aide du document 3, configurez l'environnement Kali Linux puis monter la partition Windows sur l'arborescence Linux dans /mnt afin de pouvoir l'exploiter depuis le système attaquant.

Étape 2 Première réalisation des tests

Votre environnement de test d'intrusion est dorénavant opérationnel. Vous allez tenter de réaliser deux type d'attaque sur les couples login – mot de passe Windows (une attaque par force brute et une attaque par dictionnaire) qui vous permettront de trouver ou non les identifiants et les mots de passe utilisés sur la machine Windows 11 concernée.

Exécutez les différents tests proposés par l'outil John the ripper en commençant par ceux à l'aide d'un dictionnaire pour terminer par le test de force brute en isolant les mots de passe qui n'ont pas encore été cassés. Pour cela, appuyez-vous sur les informations fournies par le document 4.

3. Notez les identifiants trouvés et tirez les conclusions qui en découlent.

Étape 3 Deuxième réalisation de test

Se déplacer dans le répertoire stockant la base SAM et le fichier SYSTEM depuis l'émulateur de terminal puis mettre en place un mot de passe vide au compte administrateur qui a servi à la création de compte à l'aide des informations présentes dans le document 5.

Redémarrer sur Windows 11 et vérifier que l’accès au compte administrateur sans mot de passe est bel et bien effectif.

4. Expliquer les différences en termes d’objectifs entre la première et la deuxième réalisation.

Étape 4 Troisième réalisation des tests

Modifiez le mot de passe du compte techads afin de renforcer la sécurité de cette authentification en respectant les bonnes pratiques.

5. Proposez, d’après vos observations, au moins un critère qui permet d’améliorer la sécurité des mots de passe.

6. Enfin, proposez puis appliquez sur la machine virtuelle Windows une contre-mesure empêchant un attaquant de lancer un système Kali Linux dessus.

Annexes

Document 1 L'audit et les tests de pénétration

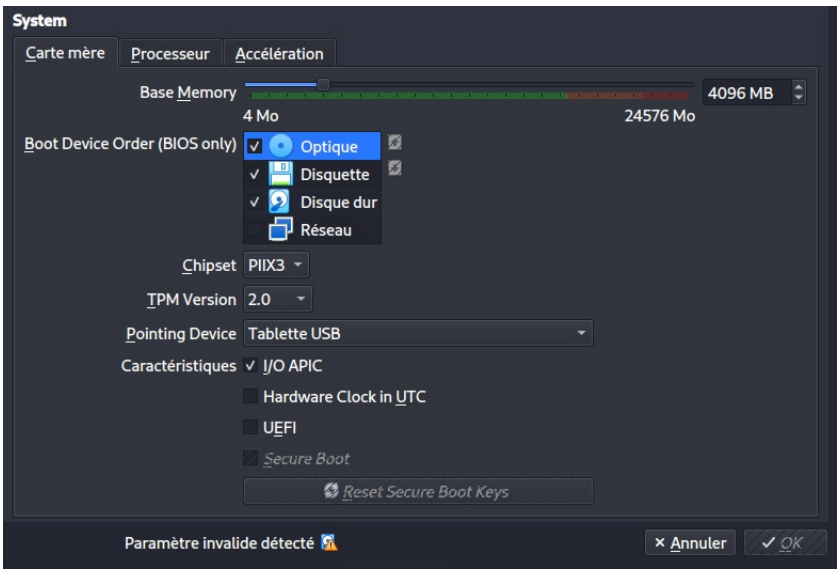
White Hat	Grey Hat	Black Hat
		
Le pentesteur travaille en étroite collaboration avec le DSI et l'équipe technique du SI. Il dispose de l'ensemble des informations.	Le test sera réalisé au départ avec un nombre limité d'information. On se place par exemple dans la situation où l'on est un utilisateur du SI.	Le testeur se met réellement dans la peau d'un attaquant externe et commence son test d'intrusion en ayant le moins d'information possible sur la cible.

Document 2 Le guide de configuration de la machine virtuelle Windows de test

Copier l'image ISO live de Kali Linux présente sur le NAS : \\172.16.20.5\commun\isos\kali-linux-2025.4-live-amd64.iso

Indiquer dans les paramétrages de la VM qu'il faut démarrer sur le live DVD Kali Linux sur le lecteur de CD-ROM virtuel (l'image ISO devra être montée à l'intérieur).

Attention ! Pour pouvoir booter sur le live DVD Kali, vous devez également désactiver l'UEFI dans les paramètres VirtualBox de la machine virtuelle.



Document 3 La préparation de l'environnement Kali Linux

Avant d'utiliser les différents outils proposés par la distribution Kali Linux, il est nécessaire de réaliser plusieurs configurations :

1. Modifier le clavier QWERTY en AZERTY en ouvrant un émulateur de terminal et en tapant la commande **`setxkbmap fr`**
2. Repérer la partition Windows avec la commande **`sudo fdisk -l`**. Généralement, un disque dur SATA se nomme sd suivi d'une lettre (sda pour un premier disque dur sata, sdb pour un second disque dur sata). Les partitions sont représentées par des chiffres à la suite des deux premières valeurs (ex : sdb1, sdb2).
3. Monter la partition Windows identifiée précédemment dans l'arborescence de Kali Linux à l'aide de la commande : **`sudo mount -t ntfs /dev/sdax /mnt` (où x représente le numéro de la partition et /mnt le dossier dans lequel elle sera montée)**.
4. Avant de commencer les tests d'attaque, il convient de récupérer les identifiants et mot de passe des différents utilisateurs stockés dans la base SAM qui contient les identifiants des comptes utilisateurs et leur mot de passe sous forme de haches.

Pour cela, ouvrir un émulateur de terminal puis copier la base SAM et le fichier SYSTEM présents dans le répertoire /mnt/Windows/System32/config sur le bureau ~/Desktop.

```
kali@kali:~$ cp  /mnt/Windows/System32/config/SAM  ~/Desktop
kali@kali:~$ cp  /mnt/Windows/System32/config/SYSTEM  ~/Desktop
kali@kali:~$ cd  ~/Desktop
kali@kali $ impacket-secretsdump -outputfile  w11hash  -sam  SAM  - system  SYSTEM LOCAL
kali@kali:Desktop$ cat  w11hash.sam
```

Document 4 L'outil John the ripper

La première chose à faire lorsque l'on souhaite utiliser une commande que l'on ne connaît pas sous GNU/Linux est d'accéder à son manuel d'utilisation :

```
kali@kali $ man john
```

Attaque par dictionnaire

Il existe un dictionnaire présent par défaut sur Kali Linux et qui se nomme « rockyou ». Au départ, il est présent sous forme d'archive compressée *gz*. Vous allez devoir la décompresser pour récupérer le fichier au format texte (*txt*).

```
kali@kali $ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

Maintenant que le fichier texte est accessible, regardons de combien de lignes est composé le dictionnaire :

```
kali@kali $ wc -l /usr/share/wordlists/rockyou.txt
```

Voici un lien qui vous permettra de comprendre comment utiliser l'outil John the ripper. C'est grâce à lui que vous serez en mesure de casser les hashs présents dans la base SAM.

https://pentesthacker.wordpress.com/2020/12/27/kali-hashcat-and-john-the-ripper-crack-windows-password-hashdump/

Attaque par force brute

Pour réaliser une attaque par force brute avec John the ripper, il suffit de préciser à l'outil que l'on souhaite utiliser ce type d'attaque :

```
kali@kali $ john --incremental --format=NT votrefichieravecleshashs
```

Document 5 Modifier les paramètres de la base SAM d'un système Windows à l'aide de l'utilitaire chntpw

```
kali@kali $ cd /mnt/Windows/System32/config
kali@kali $ chntpw -l SAM
kali@kali $ chntpw -u etudiant SAM
```

Ne mettre aucun mot de passe au compte concerné et sauvegarder les modifications.