Activité : Audit sur la sécurité des identifiants avec Kali (sans VM Windows 10)

Présentation

Le responsable de la Maison de services au public (MSAP) M. Brillat souhaite réaliser un **audit sur la sécurité des identifiants de connexion des utilisateurs**. Il s'agit de s'assurer que les utilisateurs respectent bien les recommandations sur l'utilisation de **mot de passe solide**.

Pour cela, il décide de faire réaliser des tests d'usurpation des éléments de connexion en utilisant les outils de la distribution Kali.

Vous devez disposer pour cette activité :

- d'une machine virtuelle Windows 10,
- du fichier ISO de la distribution Kali Linux (Live Boot Kali 2021)

Etape 1 : Préparation des tests

Préparation de la VM Windows

- **Préparez** la machine virtuelle Windows de test :
 - ouvrez une session avec un compte administrateur,
 - créez le compte local ENEDIS qui ne soit pas un compte Microsoft avec un mot de passe de moins de huit caractères alphabétiques,
 - créez le compte local MSA qui ne soit pas un compte Microsoft avec un mot de passe de plus de huit caractères alphabétiques,
- Dans le paramétrage de la VM Windows, indiquez que lors du lancement de la VM, le **boot sera réalisée à partir du lecteur de** CD-ROM :
 - Associez le fichier ISO de Kali au lecteur de CD-ROM.
 - dans la session Windows accédez à **Paramètres**,
 - Mise à jour et sécurité,
 - Récupération,
 - Cliquez sur le bouton Redémarrer maintenant,

0	 Au redémarrage choisissez l'option Dépannage										
	Windows10edu [En fonction] - Oracle VM VirtualBox										
	Fichier	Mach	ine Écrar	Entrée	Périphériques	Aide					
	Options avancées										
			< \$	Outil de 1 système Corriger les pro le chargement d	redémarrage ^{blèmes qui empêchent Je Windows}		Désinstaller des mises à jour				
			\$	Paramètri Changer le com Windows au dé	ES portement de marrage		Restauration du système Utiliser un point de restauration sur votre PC pour restaurer Windows				
			C:\	Invite de Utiliser l'invite d dépannage avai	commandes le commandes pour un ncé	+	Récupération de l'image système Récupérer Windows à l'aide d'un fichier image système spécifique				

• Cliquez ensuite sur **Redémarrer**

Autre solution pour récupérer la base SAM avec Windows 10 sans utiliser de VM Windows 10

- Téléchargez et utiliser l'utilitaire pwdump8 8.2; Cet utilitaire supporte les hash en AES-128 utilisés par Windows 10.
- Récupérez les informations sur les comptes avec la commande en lançant une invite de commandes **cmd.exe** en tant qu'administrateur et enregistrez les dans un fichier mdp.txt:

pwdump8 > mdp.txt

Lien :

- https://www.openwall.com/passwords/windows-pwdump
- https://syskb.com/telecharger-pwdump/

Les mots de passe obtenus sont hashés et un utilitaire comme John The Ripper va permettre de les connaître

- Créer une VM Live Kali sans disque dur mais en associant le fichier ISO au lecteur de CD-ROM
- Lancez la VM Live Kali et ouvrez uns session avec les identifiants kali mot de passe kali.

Attention : la VM Kali utilise un clavier QWERTY.

Préparation de la VM Kali

- 1. lancer un terminal
- 2. Modifiez le clavier QWERTY en AZERTY avec la commande

\$ setxkbmap fr

3/5



• Repérez la partition Windows avec la commande suivante :

\$ sudo fdisk -l

Généralement, les différentes partitions sont représentées par le mot /**dev/sda** suivi d'un numéro. Il est probable que la **partition la plus volumineuse** soit celle qui est recherchée.

Notez le numéro de la partition, qui sera utile par la suite.

• Montez la partition Windows identifiée précédemment dans Kali : <code shell> \$ sudo mount -t nfts /dev/sdax /mnt </code>

- x représente le numéro de la partition
- mnt représente le dossier de destination



* avec l'outil chntpw lister les comptes utilisateurs présents dans la base SAM et effacer leur mot de passe:

\$ chntpw -l SAM

<pre>[kal1 (% kal1)-[/mnt/Windows/System32/config]</pre>										
└─\$ chntpw -l <u>SAM</u>										
chntpw version 1.00 140201, (c) Petter N Hagen										
Hive <sam> name (from header): <\SystemRoot\System32\Config\SAM></sam>										
ROOT KEY at offset: 0×001020 * Subkey indexing type is: 686c <lh></lh>										
File size 65536 [10000] bytes, containing 8 pages (+ 1 headerpage)										
Used for data: 352/40176 blocks/bytes, unused: 31/16912 blocks/bytes.										
	RID —	Username ————	Admin?	⊢ Lock? —						
ĺ	01f4	Administrateur	ADMIN	dis/lock						
ĺ	01f7	DefaultAccount		dis/lock						
ĺ	03ea	ENEDIS								
l	01f5	Invit�	1	dis/lock						
l	03eb	MSA	ľ	f f						
l	03e9	Sio	ADMIN							
	01f8	WDAGUtilityAccount		dis/lock						

• pour effacer le mot de passe d'un compte en choisissant l'option correspondante :

\$ chntpw -u compte SAM

```
* l'outil samdump2 permet d'obtenir les hash des mots de passe
```

- * se positionner dans le dossier de la base SAM
- * lancer l'outil et sauvegarder les informations dans un fichier

- \$ cd /mnt/windows/system32/config
- \$ samdump2 SYSTEM SAM > /mnt/mdp.txt

La **base SAM** du registre de Windows contient les identifiants des comptes utilisateurs ainsi que leur mot de passe sous forme de hach calculé avec l'**algorithme MD5** :

- Les mots de passe locaux des utilisateurs sont hachés et stockés dans un fichier appelé Security Account Manager (SAM).
- Les hachages sont cryptés avec une clé qui se trouve dans un fichier nommé SYSTEM.

Lien : https://technicalconfessions.com/blogs/2021/using-samdump-for-windows-password-extraction/

Etape 2 : Première réalisation des tests

Vous allez réaliser deux types de tests pour essayer de trouver ou non les identifiants et mots de passe de chaque compte.

Le compte administrateur sera également testé par défaut.

Exécutez les différents tests proposés par l'outil John the ripper pour trouver les identifiants et mots de passe en utilisant :

- le test par force **force brute**,
- et le test par dictionnaire.

Remarques :

- Le dictionnaire **Rockyou.txt** se trouve dans le dossier wordlists : /usr/share/wordlists. Il doit être dézippé (gunzip) pour être utilisé.
- Le dictionnaire **password.lst** se trouve dans le dossier john : /**usr/share/john**. Ce dictionnaire peut être modifié par l'ajout de vos propres mots de passe. Dans le cas où les mots de passe ne sont pas connus, on peut deviner qu'un utilisateur aura pu utiliser par exemple l'organisation + son nom + un chiffre pour constituer son mot de passe. Vous pouvez alors rajouter ces mots de passe possibles dans le fichier **password.lst**.

Tests à l'aide de l'outil John The Ripper

From: / - Les cours du BTS SIO

Permanent link: /doku.php/reseau/kali/password?rev=1643573939

Last update: 2022/01/30 21:18

