Compte rendu TP intrusion : Mots de passe (TEWES Arnaud)

Dans ce TP, nous allons tenter de nous introduire dans une session Windows sans mot de passe et de lire et modifier un fichier que nous avons créé au préalable. Dans un premier temps, nous allons essayer de lire le fichier en mode Live ou Essai sous Ubuntu. Dans un second temps, nous allons supprimer le mot de passe d'une session Windows grâce à certains outils disponibles sur Internet. Ensuite, nous allons expérimenter tout ce que nous avons vu, mais cette fois sous Linux pour vérifier si les mêmes problèmes peuvent nous arriver.

<u>Création d'une machine virtuelle sous Windows, définition d'un mot de passe, création d'un fichier</u> <u>texte et tentative de lecture en mode Live ou Essai sous Ubuntu.</u>

Tout d'abord, j'ai ouvert une machine virtuelle sous Windows 10 qui a un mot de passe, puis j'ai créé un document texte nommé « Mots de passe » avec comme contenu « Mot de passe 1 »

contaile				
Microsofi Edge				
VecentAgentW		Vecam/dgentW		
Normalien Voca				
Moti de pase				
	Affichage des tâches			9-41
P Tapez ici pour effectuer une recherch	e 🔠 💽 🖡		□ ^ @ ■ ♣ 4 ³ 20/1	0/2023

Ensuite, en démarrant à partir d'un ISO Ubuntu qui a un mode « Test », j'ai essayé de lire le fichier et de le modifier en ajoutant « Mot de passe 2 » en dessous.

Activités	💿 Volume de 26 GB			20 oct. 07	:12			fr1	#: 🔹 🗎
\otimes									
	Volume de 2	26 GB / Users	/ CLI-V-01-A	T / Desktop	: Q	E	- E -		×
	D Récents			0100	0100				×
							ZiP		
		RESTORED- VeeamAgen	VeeamAgen tWindows_	desktop.ini	Edge.lnk	Mot de passe.txt	VeeamAgen tWindows_		
	Dossier personnel	twindow	6.0.2.1090				6.0.2.109		
•	Bureau								
	Documents								
$\overline{\mathbf{O}}$	🛋 Images								
	🎵 Musique								
	<u>Téléchargements</u>								
	☐ Vidéos								
A	💼 Corbeille								
	+ Autres emplacements								
								-	itu
									ſ
	Afficher les applications							Dos	sier personnel



Grâce à cette technique, j'ai bien pu ouvrir le fichier que j'avais créé sans utiliser le mot de passe de la session, et même le modifier. Je vais maintenant essayer de le lire en me reconnectant sur ma session avec mon mot de passe habituel.

0		
Corbeille	Mot de passe - Bloc-notes	-
	Fichier Edition Format Affichage Aide	
Microsoft Edge	hot de passe 2	
VeeamAgentW.	и и	
RESTORED-Veca		
nin de jasse		
۹ 🖿	Tapez ici pour effectuer une recherche 🛛 🗮 😧 🥫 😭 🐋 🥥	09:17 □ ^ @ ■ € 4)) 09:17

Tout a fonctionné, nous avons pu ouvrir, lire et modifier un fichier qui avait été créé sous Windows, et tout cela sans connaître le mot de passe de la session.

Question 1 et 2 :

Il est donc bien possible de lire et de modifier un fichier en démarrant simplement à partir d'un ISO Linux, et nous pouvons d'ailleurs accéder à tout le disque dur de la machine.

Maintenant, nous allons essayer, grâce à l'outil Rescatux, de supprimer le mot de passe de ma session Windows.

Tout d'abord, il faut démarrer sur l'iso de Rescatux et ouvrir la console Rescapp. Ensuite, nous avons plusieurs choix, dont celui de supprimer le mot de passe Windows « Reset Windows password ».

		Rescapp 0.56	• - • ×	
	Easy GNU/Linux Boot Fix	Postoro Grub	Lindate Grub Monus	
	Charle bies and and this an ODT	Restore Grub	opuace of up Menus	open source & cloud solut
	Check blos_grub partition on GPT			
*	Filesystem			
	File System Check (Forced Fix)	Easy GNU/Linux Boot Fix		
	Password			
	Change Gnu/Linux Password	Regenerate sudoers file	Reset Windows password	
	Easy Windows Admin			
	Windows			
	Restore Windows MBR	Easy Windows Admin	Reset Windows password	
	Promote Windows user to Admin	Unlock Windows user	Reinstall Microsoft Windows UEFI	
	GPT			73
	Gptsync	Recompute Hybrid GPT/MBR CHS	Check bios_grub partition on GPT	
	Expert Tools			
	Gparted	Photorec	Testdisk	
	About			
	About Descenn			

La console nous demande sur quelle partition se trouve l'utilisateur et de quel utilisateur il faut supprimer le mot de passe. Ensuite, le programme démarre.

Rescap		d the manual below c	Rescapp 0.56 arefully and press th	e «Run ! button when ready.	• × tactic
Rescapp Iv	O Menu	RESET WINDO	NS PASSWORD	Run !	
(Reset Windows (N	r,200x,XP,Vista,So	even,10) password	
	Chat	Share log	CHelp	Status: Finished.	
	DEBUG Getting tr DEBUG Getting tr DEBUG Getting tr DEBUG Getting tr (DEBUG Getting tr Guessed long nan Iong-name-guess (ANSWER) sda (DEBUG) Performin (DEBUG) Performin (DEBUG) Resetting (SUCCESS) Wir	e partitions filesystem Iternate name. (sda3) e-partitions filas. (sd s-prober long name. (s hich Windows parti me Alternate name sed sda3 3 g backup of Windows 9 Windows password. ndows password wa	n type. (sda3) a3) sda3) tion? Select Partii TRUE sda3 Windo registry files. s reset OK! :)	tion Description File system Flags ws_/_Data_/_Other ntfs msftdata No	
Debian (GNU/Linux	10 (buster) i	i386 Build:	2020-03-29 15:26:05	
linux: 4	.19.98-1 li	ive-build: 1:	20190315		
live-boo	ot: 1:20190	0614 live-co	nfig: 5.201	190519 live-tools: 1:2	20171207

_

La console a terminé, nous essayons donc de nous connecter sur notre session Windows.



Le mot de passe a bien été supprimer.

Question 3

La méthode qui se rapproche le plus de la vidéo de Mr Robot est la méthode n°2 qui consiste à démarrer sur un ISO Windows 10, ouvrir une invite de commande et modifier le fichier Utilman.exe en cmd.exe pour ensuite pouvoir modifier ou supprimer le mot de passe d'une session Windows. Voici quelques captures d'écran :

_			
Administrateur:X/windows Microsoft Windows [ver	system32(cmd.exe sion 10.0.19041.2965]		
(c) Microsoft Corporat	ion. Tous droits reserves.		
A. (3001/Ces/			



Il suffit ensuite de redémarrer le PC, les outils d'ergonomie sont désormais une invite de commande. Maintenant, nous pouvons écrire la commande « net user NomDeSession NouveauMotDePasse », en remplaçant NomDeSession par le nom de l'utilisateur, et NouveauMotDePasse par le nouveau mot de passe. Nous pouvons ensuite nous connecter avec le nouveau mot de passe.

Le texte du message asso	cié au numéro 0x2350 es	st introuvable d	ans le fichier	de messages pou	r Application.	
(c) Microsoft Corporation Les ressources mémoire d	on. Tous droits réservés lisponibles sont insuffi	s. Isantes pour tha	iter cette com	mande.		
C:\Windows\System32>net	user					
comptes d'utilisateurs d	le \\					
Administrateur	DefaultAccount	Florian				
Invité Des erreurs ont affecté	WDAGUtilityAccount l'exécution de la comma	ande.				
C:\Windows\System32>net	user Florian MonNouveau	MotDePasse	(

Question 4

En conclusion, un mot de passe Windows ne suffit pas à protéger ses données et son disque dur. Nous avons vu plusieurs méthodes simples qui permettent, soit d'accéder directement au dossier du disque dur, soit de modifier le mot de passe. D'autres méthodes permettent aussi de le contourner sans le modifier et d'accéder à la session. Une personne lambda ne pourra pas y accéder, mais pour une personne qui se renseigne, toutes les sources disponibles sur internet permettent effectivement, sans trop de recherche, de réussir à passer outre ce mot de passe. Un mot de passe Windows n'est donc pas quelque chose de sûr et il faut mettre d'autres choses en place pour assurer la sécurité des données comme un chiffrement du disque dur ou une double authentification.

Question 5

Pour se protéger de ce problème, plusieurs solutions sont possibles comme :

- Activer le chiffrement du disque dur (avec BitLocker par exemple) sera très utile si une intrusion a lieu. Le cryptage intégral garantit que seules les personnes possédant la bonne clé de cryptage pourront décrypter et accéder aux fichiers et informations du disque dur crypté.
- Utilisez un mot de passe fort et complexe pour votre compte utilisateur local. Évitez d'utiliser des mots courants ou des informations personnelles dans votre mot de passe. Un mot de passe fort est essentiel pour protéger votre ordinateur contre les attaques par force brute. Comme nous l'avons vu en cours et selon les recommandations de la CNIL, un mot de passe fort doit être long et complexe, avec une combinaison de lettres majuscules et minuscules, de chiffres et de symboles. Un tel mot de passe peut mettre plusieurs mois voire plusieurs années a se faire demasquer.
- Nous avons la possibilité de mettre un mot de passe sous Windows pour accéder à nos fichiers. Mettre un mot de passe pour accéder à ses fichiers est une méthode courante pour protéger ses données contre les accès non autorisés. Cependant, il est important de noter que cela ne garantit pas une sécurité absolue.
- Si l'on a un ordinateur portable, ne jamais le laisser à portée d'un inconnu (comme sur le siege de sa voiture par exemple) lorsqu'on s'absente, ou sur son bureau au travail lorsqu'on y est pas. Au vu de tous les moyens possible qu'il existe de contourner le mot de passe, ce n'est pas sécurisé de laisser un PC a portée.
- Prévoir une sauvegarde de notre disque dur en suivant la méthode du 3-2-1. Cela permet, en cas de soucis, de vol, ou d'attaque de ransomware, de pouvoir toujours récupérer nos données.

Question 6

Nous allons maintenant reprendre le fil de ce TP pour vérifier si nous rencontrons les mêmes problèmes avec une distribution Linux. Kali Linux ne fonctionnant pas sur mon PC, j'ai fait le test avec une VM sous Ubuntu, et en bootant également sur Ubuntu en version « essai » pour essayer de lire le fichier mot de passe.



Dans un premier temps, j'ai créé un fichier mot de passe sur mon bureau.

J'ai ensuite demarré ma VM sur la version d'essai d'Ubuntu et j'ai essayé de lire le fichier.

Open ~ 🗐	*Mots de passe.txt admin:///media/ubuntu/e6ecbdc0-8c3e-48c4-a56d-41ad984b60e8/home/user/Bureau	Save =		×
1 Mot de passe 1				
Ī				
	Plain Text 🗸 🛛 Tab Width: 8	 Ln 1, Col 16 	i v IN	١S

J'ai ajouté une ligne « Mot de passe 2 » dans le fichier, et j'ai essayer de le lire avec mon Ubuntu installé sur ma VM.



J'ai réussi à lire le fichier texte « Mots de passe » avec les deux lignes inscrites a l'interieur. J'ai donc bien pu lire et modifier le fichier, et ca, sans mot de passe...

Pour résumer, il faut donc d'autres alternatives, que l'on soit sous Linux ou sous Windows pour protéger ses données comme vu plus haut à la question 5...

Pour aller plus loin :

Je vais maintenant essayer de lire le fichier texte « Mots de passe » de ma VM sous Windows 10 en ayant activé BitLocker au préalable et en ayant chiffré mon disque dur.

Fichier Ordinateur	Gérer Ce PC Affichage Outils de lecteur	××
 ← → ∧ ➡ > 0 ★ Accès rapide Bureau ★ Téléchargements # ➡ Documents ➡ Images 	CEPC > > Dossiers (7) Bureau Musique	Créer un mot de passe pour déverrouiller ce lecteur Vous dece cofe une de passe foit constitué de caractères minuscules et majuscules, de nombres, de symboles et d'espaces. Entre voitre mot de passe
Musique Vidéos OneDrive Ce PC Késeau	Videos V Périphériques et lecteurs (2) Disque Iccal (C) 11,4 Go Ibres sur 29,3 Go	Entre a nouveau le mot de passe
		Conseils pour créer un moit de passe fort. Selivent Annuler
9 élément(s) 1 élément	telertionné	8:: 0

J'ai donc activé BitLocker sur ma VM Windows 10.



J'ai ensuite démarré sur Ubuntu version « test » et j'ai essayé d'ouvrir le disque dur ou Windows est installé.

Activities	32 GB Encrypted O	00	t 30 18:21		en: 👗 🌒 🕛
0					
6					
	$\leq f'$	Authenticatio	on Required		
\bigcirc		A passphrase is needed to on "Msft Virtual Disk	access encrypted data (32 GB Hard Disk)".	fer .	
		Password	۱		
Â		Remember Password	1	I and the second	
?		Cancel	Unlock		(
Gr					
4					

Le disque dur est correctement chiffré et il nous est impossible d'y accéder, même en utilisant les techniques mentionnées précédemment.

Conclusion

La méthode de chiffrement du disque dur est une méthode fiable qui permet de sécuriser les données de son disque dur. Il est nécessaire de prendre des précautions lorsqu'on traite des données sensibles et de rester vigilant, car les attaques malveillantes peuvent survenir de n'importe où !