Cybersécurité des services informatiques

PROFESSEURS : MR JOBARD

TP N°2 : Intrusion simple Windows

Objectif : découvrir l'intérêt de sécuriser correctement une machine sous Windows et savoir se protéger en se mettant à la place de l'attaquant.

Introduction :

Microsoft prend la sécurité au sérieux. Les comptes Microsoft, le système d'exploitation Windows et les autres produits Microsoft incluent des mots de passe pour sécuriser nos informations. Cependant dans certaines séries télévisées cela semble à un jeu d'enfant, de contourner ce dispositif. C'est dans l'exemple du série MR Robot S04E03.

Cette procédure de sécurité qui est de mettre un mot de passe à l'allumage de sa machine. Est-ce vraiment efficace et infaillible ?

Pour répondre à ces questions on va se mettre en pratique.

En premier lieu, on va créer une VM avec un Windows 10 Pro dessus. Puis créer un document texte dans le bureau qui s'appelle toto.text

En deuxième lieu on va essayer d'accéder sur le document en supposant de ne pas savoir le mot de passe du compte administrateur.

En troisième lieu on va procéder autrement pour avoir accéder au compte administrateur en changeant son mot de passe.

Et enfin on va faire le même procédé sur un VM Linux.

I. La création du VM

1.1. Les quelques différentes étapes de la création de notre VM

Je choisis d'abord le système opération du VM

~
~
~
~
~
~

Cette étape correspond à la spécification du nombre de processeurs du VM. Je choisis cores 4 pour permettre la machine d'être un peu plus rapide à la suite de notre procédure.

Processors			
Number of processors:	2	\sim	
Number of cores per processor:	2	\sim	
Total processor cores:	4		

Dans cette étape on choisit le nombre de RAM du VM.

New	v Virtual Mach	nine Wizard	\times
	Memory for the How much	ne Virtual Machine memory would you like to use for this virtual machine?	
Spe	ecify the amoun st be a multiple	nt of memory allocated to this virtual machine. The memory size of 4 MB.	
€ 120 € 64 33	8 GB - 4 GB - 2 GB -	Memory for this virtual machine: 2048 State MB	
	6 GB - 8 GB - 4 GB - 2 GB -	 Maximum recommended memory: 9.6 GB 	
512 256	1 GB - 2 MB - 5 MB -	 Recommended memory: 2 GB 	
64 32 16	4 MB - 2 MB - 5 MB - 2	 Guest OS recommended minimum: 2 GB 	
8	3 MB - 1 MB -		
	Help	< Back Next > Cancel	

A ce niveau on sélectionne le type du réseau. J'ai sélectionné le NAT pour que mon VM n'interfère pas au réseau externe.

New Virtual Machine Wizard			\times
Network Type What type of network do you	ı want to add?		
Network connection			
 Use bridged networking Give the guest operating system The guest must have its own IP 	direct access to address on the	an external Ethe external network.	rnet network.
 Use network address translation Give the guest operating system external Ethernet network conne 	(NAT) access to the h action using the	ost computer's dia host's IP address.	al-up or
 Use host-only networking Connect the guest operating syst computer. 	tem to a private	virtual network o	on the host
O Do not use a network connection	i.		
Help	< Back	Next >	Cancel

Et enfin une Récapitulatif de de notre futur VM

Name:	Windows 10 x64
Location:	C:\Users\Mame Gor\Documents\Virtual Machines\Windows
Version:	Workstation 17.x
Operating System:	Windows 10 x64
Hard Disk:	60 GB, Split
Memory:	2048 MB
Network Adapter:	NAT
Other Devices:	4 CPU cores, CD/DVD, USB Controller, Printer, Sound Card
Customize Hardy	vare

Après avoir insérer l'ISO, on démarre le VM pour finaliser la dernière partie. C'est-à-dire :

✓ Choisir :la langue, le format horaire et la langue du clavier.

Installation de Windows	
H_ Winc	lows
Langue à installer : <mark>Français (France)</mark> Eormat horaire et monétaire <mark>: Français (France)</mark> Clavier ou méthode d'entrée : <mark>Français</mark>	· · · · · · · · · · · · · · · · · · ·
Entrez la langue et les préférences de votre cho	ix et cliquez sur Suivant pour continuer.
Microsoft Corporation. Tous droits réservés.	Suivant

✓ Le système d'exploitation. J'ai choisi Windows 10 famille

🚱 橘 Installation de Windows			
and a settlement of the settle day it when the set of settle			
Selectionner le système d'exploitation à inst	Assistant	Data da mad	
Systeme d exploitation	Architecture	Date de mod	
Windows 10 Famille	x64	09/04/2021	
Windows to Famile N	x64	09/04/2021	
Windows 10 Familie Langue unique	x04	09/04/2021	
Windows to Education	x04	09/04/2021	
Windows to Education N	X04	09/04/2021	
		Suis	vant

✓ Crée un mode de passe « compte administrateur »

	Créer un mot Vérifiez que vous choisiss	de passe faci	le à retei endrez sans faute.	nir
		8		
	•••••• 		ି	
				Suivant
(+ L				10



✓ Définir le nom du compte administrateur

✓ Et voila notre VM est prêt

Cont	beille																											
Microso	oft Edg	je																										
																						1						
																				+								
	Q	Та	pezi	ci p	our	effe	ctu	er u	ne r	rech	nerc	he	0		2	-						~	æ	(1))	10:0	9	民	

1.2 La création du document texte

Dans mon VM, je crée dans le bureau un document : toto.text puis j'écris les paroles du chanson Dadju « compliqué » dans le fichier toto. Après j'éteins la machine.



II. Accéder sur le document texte : toto.text

Dans la suite je vais essayer d'accéder sur le fichier toto.text pour lire et modifier le contenu sans oublier que l'utilisateur avais mis un mot de passe qui respecte les normes. En autre terme on va se mettre à la place de l'attaquant.

 Boot normally
 Device Path: PeiRoot (0x0) /Pei (0x11,0x 0) /Pei (0x3,0x0) /Sata (0x1,0x 0) /Pei (0x3,0x0) /Pei (0x1,0x 0) /Pei (0x3,0x0) /Sata (0x1,0x 0) /Pei (0x3,0x0) /Pei (0x1,0x 0) /Pei (0x1,0

Pour ce faire, je vais utiliser l'ISO de UBUNTU et booter dessus.

On démarre en mode live-DVD. Pour l'installation et choisis « Essayer Ubuntu »

Activities	🗅 Files 🔻			Nov 27 10:42				▲ ● ∪ -	
0	â								
	< > Gi Home ◄					Q i ≡	T	- 😐 😣	
	C Recent			$\overline{\overline{v}}$	5		~°	0	
	★ Starred	Desktop	Documents	Downloads	Music	Pictures	Public	Templates	
	습 Home								
	Desktop	Videos							
	Ir Documents								
$\overline{\mathbf{O}}$									
	□ Music								
	Pictures								
	☐ Videos								
	💼 Trash								
?	+ Other Locations								
SSD									
					Le contra de la co				

2.1. Trouvons notre fichier toto.text

Apparemment le fichier toto.text est dans le VM Ubuntu. Dans le chemin d'accès suivant : fils/other locations/users/TP-SLAM /Desktop.

Et maintenant pour répondre à la question est-il possible de lire le fichier. Je vais faire un clic droit /open.



Bien sûr on peut lire le fichier toto.text, je vois le contenu : les paroles de la chanson de Dadju. Vue que on a accès sur le fichier. Est-il possible de le modifier ? Autrement dit est ce que on a les droits administrateurs pour le modifier. Pour répondre à cette question je vais essayer de supprimer les trois premières lignes du texte puis fais une sauvegarde.



Voici les lignes (colores en jaune) qu'on va supprimer.



Lorsque que j'ai ouvert le fichier de nouveau après la sauvegarde, on ne voie plus les trois premières lignes. Donc on a modifié le fichier toto.text



III. Accéder au compte administrateur en changeant son mot de passe.

Dans cette partie, on va réinitialiser le mot de passe Administrateur de Windows 10, en appliquant une méthode parmi les cinq qui sont proposés par le prof

3.1 Méthode n°2b : via l'Environnement de récupération Windows (WinRE)

Cette méthode consiste à remplacer l'exécutable "Utilman.exe" par "Cmd.exe" (Invite de commandes) dans les fichiers système de Windows.

 D'abord je vais Lancez l'invite de commandes. Notre VM est un Windows 10, donc je vais aller dans le bios en appuyant sur F4 (NB : sa peut être différent selon les machines) lors du démarrage. Après on choisit Options de démarrage avancées puis sélectionnez Dépannage ensuite Options avancées et en fin Invite de commandes.



2. Une fois dans le cmd on cherche notre lecteur qui correspond à notre installation. Pour savoir quelle lettre correspondant à notre installation de Windows, on entre une lettre (par exemple C:) puis saisisse la commande « dir » pour lister son contenu. Si on retrouvez les dossiers propres à Windows (Program Files, Users, Windows...), c'est que on y est.



3. Maintenant on est sur le lecteur contenant Windows. J'utilise le commande « cd » pour se déplacer dans le dossier Windows\System32.

Administrateur : X:\windows\SYSTEM32\cmd.exe	
Le lecteur spécifié est introuvable.	^
X:\Sources> dir e: Le chemin d'accès spécifié est introuvable.	
X:\Sources>e: dir	
Le lecteur specifie est introuvable.	
X:\Sources>c:	
C:\>dir Le volume dans le lecteur C n'a pas de nom. Le numéro de série du volume est 2CA3-C797	
Répertoire de C:\	
07/12/2019 10:14 <dir> PerfLogs</dir>	
18/10/2023 09:30 <dir> Program Files</dir>	
09/04/2021 14:59 <dir> Program Files (x86)</dir>	
27/11/2023 13:12 0 Recovery.txt	
18/10/2023 09:25 <dir> Users</dir>	
27/11/2023 10:09 <dir> Windows</dir>	
1 fichier(s) 0 octets	
5 Rép(s) 42 885 619 712 octets libres	
C:\>cd Windows	
C:\Windows>cd System32	
C:\Windows\System32>	~

4. Après on crée une sauvegarde du fichier utilman.exe, en utilisant le ligne de commande suivant : Copy Utilman.exe Utilman.exe.bak

Le chemin d	l'accès s	pécifié est	introuvable.	
V. \ Sourcos	o, din			
Le lecteur	spécifié	est introu	vable.	
X:\Sources	·c:			
C:\>dir				
Le volume	dans le	lecteur C n	a pas de nom.	
Le numéro	de série	e du volume (est 2CA3-C797	
Répertoire	de C:\			
07/12/2019	10:14	<dir></dir>	PerfLogs	
18/10/2023	09:30	<dir></dir>	Program Files	
09/04/2021	14:59	<d1r></d1r>	Program Files (X86)	
2//11/2023	13:12	OTES	0 Recovery.txt	
07/11/2023	10.00	COTRS	Windows	
2771172025	1 fi	chier(s)	0 octets	
	5 Ré	p(s) 42 88	619 712 octets libres	
	10000			
C:\>cd Wind	IOWS			
C:\Windows	cd Syste	em32		
C:\Windows	System32	> copy Util	nan.exe Utilman.exe.bak	
	icnier(s	S) CODIE(S).		

5. Par la suite on remplace les options d'ergonomie utilman.exe par l'invite de commandes : copy cmd.exe Utilman.exe

<:\Sources>c:				
C:\≻dir Le volume dans le ∷ Le numéro de série	lecteur C n' du volume e	'a pas de nom. ≥st 2CA3-C797		
Répertoire de C:\				
97/12/2019 10:14 18/10/2023 09:30 99/04/2021 14:59 77/11/2023 13:12 18/10/2023 09:25 27/11/2023 10:09 1 fi. 5 Réj	<dir> <dir> <dir> <dir> <dir> <dir> chier(s) p(s) 42 885</dir></dir></dir></dir></dir></dir>	PerfLogs Program Files Program Files (x86) 0 Recovery.txt Users Windows 0 octets 5 619 712 octets libres		
C:\>cd Windows				
:\Windows>cd System	m32			
:\Windows\System32 1 fichier(s	> copy Utilm) copié(s).	aan.exe Utilman.exe.bak		
C:\Windows\System32 Remplacer Utilman.e 1 fichier(s	> copy cmd.e xe (Oui/Non/) copié(s).	exe Utilman.exe 'Tous) : oui		
:\Windows\Svstem32	>_			

6. A ce point on va redémarrer notre VM. Et Sur l'écran de connexion de Windows, on appuie sur les touches Win + U pour lancer l'invite de commandes (en lieu et place des options d'ergonomie).



7. Maintenant on peut changer le mot de passe Pour réinitialiser le mot de passe d'un compte utilisateur, on tape la commande suivante : « net

user "nom_compte_utilisateur" nouveau_mot_de_passe » (net user "TP-SLAM" 4321Azerty@)



C'est fait on a changé le mot de passe du compte utilisateur TP-SLAM.

Cette même méthode est utilisée par Elliot dans la série Mr Robot S04E03



Une petite conclusion

D'après ce qu'on vient de découvrir, il est possible de réinitialiser le mot de passe d'un compte utilisateur en exploitant une faille de sécurité de Windows. La méthode que je viens d'utiliser en ai une preuve. En gros il s'agit de renommer le fichier utilman.exe en cmd.exe afin qu'en pressant les touches Windows + U nous puissions avoir l'Invite de commande Windows à la place des options d'ergonomie

3.2 Deux manières de se protéger de ce problème :

On peut utiliser BitLocker pour protéger le lecteur système. En effet il ne sera pas possible de réinitialiser le mot de passe Administrateur avec la méthode employée ci-dessus ! Sauf si la personne connaît le mot de passe de déverrouillage (sur un PC sans puce TPM) ou la clé de récupération pour déverrouiller manuellement le lecteur chiffré.

Ou en utilisant LAPS Legacy ou Windows LAPS. De ce fait Windows ne nous permettra pas de réinitialiser le mot de passe par ce que le compte est contrôlé par une stratégie externe.

Ou encore VeraCrypt.

3.3 Exprimons les dans noter VM

Pour notre cas on va utiliser VeraCrypt pour chiffrer notre lecteure. Ce logiciel est une alternative à BitLocker, le logiciel de chiffrement de Microsoft. Vue que on utilise Windows 10 home on ne peut pas utiliser BitLocker. Par contre VeraCrypt peut être utiliser sur n'importe quelle version (Windows 10, 8, 7, Vista, XP) et n'importe quelle édition de Windows.

On va passer à l'installation de VeraCrypt et le chiffrèrent de notre disque système.

D'abord je vais installer veraCrypt



Je vais ouvrier VeraCrypt puis sélectionner système /chiffrer la pation/le disque système

ि Home ×	$$ Windows 10 x64 \times $$ TP-SLAM1 \times $$ TP-SLAM-1	×
Eichiar Ordinataur	y VeraCrypt	× ee Web
← → × ↑ 💻	Le Déchiffrer la partition/le disque système A: Déchiffrer définitivement la partition/le disque système B: Reprendre un processus interrompu E: Créer un système d'exploitation caché	
 Bureau Téléchargeme Documents Images 	G: Créer un disque de secours H: Vérifier le disque de secours D: Vérifier l'image du disque de secours K: Vérifier l'image du disque de secours	
Musique Vidéos	Image: Monter sans authentification lors du preamorçage Image: Monter sans authentification lors du preamorçage <td>_</td>	_
Ce PC	Cri Propriétés der le cache	
Bureau Bocuments Images 9 élément(s) 1 élér	Volume Parametres VeraCrypt Fichier VeraCrypt Ne jamais enregistrer l'historique Outils pour le volume Périphérique ér Périphérique Outils pour le volume Périphérique	
Taper id	ici pour rechercher O 🛱 💽 📜 😭 ⊻ 🔨	ይ 🖫 ላ») 10:02 11/12/2023 🔻

Je sélectionne normal



Dans Nombre de système d'exploitation, je vais sélectionner Amorçage parce que on a qu'une seule installation sur notre vm





Dans cette partie je choisis le mot de passe

VeraCrypt utilise ces mouvements de souris pour augmenter la force des clés de chiffrement. Une fois la barre de progressio est remplie, je clique sur Suivant.



Pour la suite il faut une clé USB pour Décompresser le fichier ZIP. Malheureusement on n'a pas de clé USB pour continuer les manipulations.

\fbox Home $ imes$ \fbox Windows 10 x64 $ imes$	TP-SLAM1 ×	TP-SLAM-1 ×
🟥 🛃 📑 = Documents	-	
Fichier Accueil Partage Affichage		~ 🕐
← → ヾ ↑ 🛱 > Ce > Do > 🗸 ऎ	Rechercher dans : Documents	
Vidéos ^ Nom ^	Modifié le	Туре
> 🜰 OneDrive 🔋 VeraCrypt Rescue Disk	11/12/2023 10:26	Dossier co
V 🛄 CePC		
> 🛄 Bureau		
> 🗄 Documents		
> 📰 Images		
> 1 Objets 3D		
> 🗸 Téléchargement:		
1 élément		
■ P Taper ici pour rechercher	o 🛱 💽 🐂	へ 空 記 小) FRA 10:40 11/12/2023

Voici le dossier veraCrypt qu'on devait décompresser

IV. Le même procédé sur un VM Linux

Dans cette partie je vais créer un VM Ubuntu dont le compte administrateur contient un mot de passe. Par la suite on va essayer de se connecter sur ce même compte en supposant de ne pas connaitre le mot de passe du compte administrateur. Autrement dit on va faire la même chose qu'on a fait sur Windows.

4.1 La création du VM Ubuntu

D TP-SLAM1 - VMware Workstation	- 🗆 ×
File Edit View VM Tabs Help 📙 🕶 🛱 🚇	
🕼 Home 🛛 🕞 Windows 10 x64 🛛 🕞 TP-SLAM1 🗙	
	Nov 27 16:21 🛃 📢 🕛 👻
	Install
Who are you?	
Y	our name: mame
Your compute	r's name: mame-virtual-machine
Did at the second se	The name it uses when it talks to other computers.
Pickau	
Choose a p	
Conrirm your p	
	Require my password to log in
and the second	Back Continue
and the second	
	• • • • • • •
Click in the virtual screen to send keystrokes VMware Tools enables many features movement, video and performance. Lo operating system and click "Install Too	and improves mouse og in to the guest Install Tools Remind Me Later Never Remind Me Is ⁴ .
To direct input to this VM, click inside or press Ctrl+G.	

Accéder sur le compte admis sans connaître le mot de passe ?

Pour ce faire on va démarrer notre VM en mode rescue.

Le mode rescue est un mode de récupération que l'on peut activer au démarrage du PC. Cela permet d'accéder à des outils de dépannage intégré à la distribution Linux.

Pour ouvrir le mode rescue, j'ai appuyé sur la touche **ESC** au démarrage.

Ensuite on choisit Options avancées pour Ubuntu (Advanced option for Ubuntu).





Après on sélectionne la deuxième option (recovery mode)

Dans le menu de récupération, on sélectionne Root puis appuie sur entrée

Recovery Menu (filesystem st	tate: read-only)
resume	Resume normal boot
clean	Try to make free space
dpkg	Repair broken packages
fsck	Check all file systems
grub	Update grub bootloader
network	Enable networking
root	Drop to root shell prompt
system-summary	System summary
	<ok></ok>

Ainsi on appuie sur la touche entrée du clavier. Puis pour réinitialiser le mot de passe de l'utilisateur, on utilise la commande passwd ex passwd mame et taper le nouveau mot de passe.

☆ Home	×	Windows 10 x64	× 🕞 TP-SI	AM1 ×	TP-SLAM-1	×	
		nesi	Imo	Pacuma nor	amal boot		
		clea	an	Try to mak	ke free space		
		dpk: fsci	Ś	Check all	oken packages file systems		
		grut) Nork	Update gru	ub bootloader		
		root		Drop to ro	ot shell promp	ot	
		sys1	tem-summary	System sur	mmary		
				<0k>			
	Pre	ess Enter for mainte	enance				
	(or	r press Control−D to t@mame_virtual_mark	o continue): nine:~# nasswd	mame			
	Neu	password:		liano			
	кет pas	∶ype new password: swd: password updat	ted successful.	ly			
	roc	∣t@mame-virtual-mack	nine:~# _				

Et en fin il ne reste qu'a saisi exit pour revenir au menu de récupération, sélectionné Résume et ok

Maintenant essayons de se connecter avec le nouveau mot de passe qu'on a créer



Conclusion :

Grâce à ce TP, je suis capable de réinitialiser le mot de passe administrateur d'une machine sous Windows mais aussi comment se protéger à ce problème.