Compte rendu TP intrusion Windows

Première partie

Nous allons voir comment accéder à un fichier sur le bureau d'un utilisateur sans démarrer sa session.

Tout d'abord on crée une VM Windows 10 pro, puis on choisit un mot de passe utilisateur avant de lancer Windows. On crée un fichier Toto en txt avec des paroles de chanson.





Une fois le fichier enregistré on éteint la VM et on ajoute l'iso d'Ubuntu.



Puis on relance la VM en choisissant « essayer Ubuntu »

Maintenant on va essayer d'accéder à notre fichier Toto.



Après avoir redémarré notre VM (en éjectant l'iso au préalable) on peut ouvrir notre fichier toto et voir qu'effectivement les modifications ont été enregistrées.

🕎 VM W10 PRO intrusio	in sur 14-D-2 - Connection à un ordinateur virtuel
Fichier Action Média	Affichage Aide
	IN B. S. P.
	Totolafrica - Bloc-notes
6	Fichier Edition Format Affichage Aide
	Thear the drums achoing tonight
	But she hears only whisteres of some nulet conversation
Minorod Hildge	She's coming in. 12:30 flight
	The moonlit wings reflect the stars that guide me towards salvation
	I stopped an old man along the way
	Hoping to find some old forgotten words or ancient melodies
	He turned to me as if to say
	"Hurry boy, it's waiting there for you"
	It's gonna take a lot to drag me away from you
	There's nothing that a hundred men or more could ever do
	I bless the rains down in Africa
	Gonna take some time to do the things we never had (ooh, ooh)
	Super cool la musique

Par conséquent on peut en déduire qu'en démarrant sur Ubuntu par exemple on peut avoir accès au reste de l'ordinateur sans rencontrer de sécurité.

Deuxième partie

Nous allons voir comment nous connecter à notre session Windows sans avoir à saisir le mot de passe, pour cela il y a énormément d'outils sur internet dont trois que l'on va tester dans ce tp.

1/ Rescatux

Après avoir téléchargé l'iso de rescatux (trouvé sur Google en quelques clics) il suffit de l'ajouter dans notre VM comme précédemment avec Ubuntu.

estionnaire Hyper-V 14-D-2 Nom Ètat Odinateurs virtuels Nom Ètat Odinateur vinteit alpine 5. Désactivé so-2: stomaheld nk Désactiv		arge P
T4:D-2 Ordinateurs virtuels Etat Nom État Ordinateurs virtuels Organiser ▼ Nouveau dossier ISO Multiper Stol PC Désactivé VM win10 pro Stol PC Désactivé VM win10 Stol PC Désactivé Windowsi Dipro nk Désactivé Windowsi Dipro nk Désactivé	v Ø Rechercher dans : Teléch ≣≣ + Taille	arge A
Nom Etat Ordinateriu vm test alpine S Désactivé Organiser ▼ Nouveau dossier Bio-2: atomatvid rik. Désactivé Bio-2: atomatvid rik. Désactivé Uburtu nik. Désactivé VM W10 PRD rituision Désactivé VM W10 PRD rituisit Désactivé VM	Taille	
Bio-C. attornance nr. Descrivé ISO Nom Modifié le Type Bio-C. attornance nr. Déscrivé Microsoft Manage Bipne-extended-3.16.2-x86_54 05/09/2022 15:35 Fichier d'image VM W10 PRO intrusion Déscrivé El Ce PC Progetré Bureau Bureau Windows 10 pro nk Déscrivé El Bureau El Bureau Fichier d'image	Taille	
Butortunk Désactivé Microsoft Manage alpine-extended-3.16.2-x86_64 05/09/2022 15:35 Fichier d'image VM W10 PRD intrusion Désactivé Image rescatux-0.73 18/10/2022 10:30 Fichier d'image VM w10 pro SiOl PC Désactivé Image Image rescatux-0.73 18/10/2022 10:30 Fichier d'image VM w10 pro SiOl PC Errogistrie Image Image Image Fichier d'image VM w10 pro SiOl PC Errogistrie Image Image Image Fichier d'image Image Image Image Image Image Image Image Image Image Image Image Image Image Image		
VM W10 PR0 intrusion Désactivé minitiobilit manage minitiobilit manage distributilité manage VM w10 pro SiO PC Désactivé C e PC istresaturé-0.373 18/10/2022 10:55 Fichier d'Image VM w10 SiO PC Evregativé B Bureau istresaturé-0.374 18/10/2022 00:55 Fichier d'Image	di 729.328.Kb	
M win10 pro SIO1 PC Désactivé Evrogativé Imodessi 10 pro nk Désactivé mage windows 10 pro nk Désactivé mage	di 707.584 Ko	
i windows serv nk Désactivé i Documents	di 3 737 140 Ко	
Points de contrôle Images		
Teléchargement		
Vidéos Windows (C:) Disque local (D:) Data (G:) Lexar (H:) Lexar (H:)		
VM W10 PRO intrusion Nom du fichier: rescatur-0.73	 Fichiers image ISO 	~
Créé(e):	Ouvrir	nnuler
Version de configuration : Génération : Remarques : G.\Vm Canale Pierre \VM W10 Pi	tr r réplication	
OK Annuler Ap	pliquer	





Le mot de passe a maintenant été réinitialisé, il suffit donc d'éteindre la VM et la relancer pour qu'elle démarre sous Windows et on peut s'apercevoir qu'on peut se connecter sans entrer de mot de passe.

4		Rescapp 0.56		- Occurring	
	🗑 Read the manua	al below carefully and press the	Run ! button when ready.		
Menu	RESET WINDOWS PASSWORD		e Run !	e Run !	
	Reset Windows (NT,20	00x,XP,Vista,Seven,10) pass	sword		
Chat	C Share log	CHelp	Status: Finished.		
DEBUG Getting Microso DEBUG Getting System DEBUG Parsing the /etc DEBUG Getting the part DEBUG Getting alternal DEBUG Getting os-prob IEBUG Getting os-prob	If Windows OS partitions. partitions. (issue file. (sda2) titions filesystem type. (sda te name. (sda2) titions flags. (sda2) windows partition? Selec	2) ct Partition Description File	system Flags Guessed long name Alt	ernate name	
hEBUG; Getting System DEBUG; Getting System DEBUG; Getting the par DEBUG; Getting alternal DEBUG; Getting os-prob PLOUESTION] Which 1 NUE sda2 Windows J, (ANSWER] sda2 IEBUG; Paretorming bad IEBUG; Paretorming bad IEBUG; Paretorming bad ISEUG; Paretorming bad	Ift Windows OS partitions. Joantitions. Jissue file. (sda2) titions filesystem type. (sda te name. (sda2) titions filags. (sda2) er long name. (sda2) Windows partition? Select Data/_Other ntfs No-fila kup of Windows registry file ows password. a password was reset OK	2) ct Partition Description File gs No-long-name-guessed s is. (1 :)	system Flags Guessed long name Alt da2	ernate name	

On voit qu'aucun mot de passe n'est demandé, on a donc pu accéder à la session utilisateur sans passer par le mot de passe.



2/ Puppy linux



Comme précédemment on ajoute l'iso désirée dans notre VM, pour cet exemple puppy linux.

Une fois démarré nous pouvons changer la langue pour le français, dans l'onglet qui s'ouvre automatiquement, pour faciliter les étapes suivantes.

On ouvre la console et on tape les commandes suivantes :

« cd /mnt/sda2 » > pour aller dans le répertoire 'sda2'

« cd Windows/System32 » pour aller dans 'System32'

« mv Utilman.exe Utilman.exe.bak » crée 'Utilman.exe.bak' et y place 'Utilman.exe'

« cp cmd.exe Utilman.exe » copie 'cmd.exe' dans Utilman.exe.

Ceci fait on peut redémarrer notre machine et sur l'écran d'accueil appuyer sur 'ctrl + u' qui au lieu d'ouvrir l'utilitaire va ouvrir le cmd. Dans le cmd on va écrire net user « nom_d'utilisateur » (PC) nouveau_mot_de_passe (Azerty123).



Le mot de passe est maintenant changé pour celui qu'on a choisi, il ne nous reste plus qu'à remettre en place l'interface de base en repassant par puppy linux.

/mnt/sda2/Windows/System32	_ 🗆 ×	On ouvre la
root# cd /mnt/sda2 root# cd Windows/System32 root# rm Utilman.exe root# mv Utilman.exe.bak Utilman.exe root# _	I	« cd /mnt/so « cd Window « rm Utilmal 'Utilman.exe « mv Utilma déplace 'Uti 'Utilman.exe

- console et on écrit :
 - da2 »
 - ws/System32 »
 - n.exe » supprime ,'
- In.exe.bak Utilman.exe » Iman.exe.bak' dans è,

3/ Medicat

On remplace l'iso précédente par celle de Medicat puis on lance la VM.



On ouvre l'utilitaire et on écrit « password » pour trouver plus rapidement les outils nécessaires au changement de mot de passe.

J'ai choisis PasswordChanger, on va donc suivre les étapes de ce logiciel.





On coche la première case pour rechercher tous les volumes SAM (Security Accounts Manager).



On sélectionne notre disque.



Puis notre utilisateur.



On coche « Clear this Users's Password » pour réinitialiser le mot de passe.



Avec ce logiciel aussi le mot de passe a pu être modifié.

Dernière partie

Nous avons vu qu'il était possible d'accéder assez facilement à notre session Windows en contournant le mot de passe à l'aide de différents outils, qu'en est-il de linux ?

On crée une VM avec Ubuntu (dans cet exemple Ubuntu 20.04).

Après avoir créé un utilisateur on redémarre la machine et on appuie sur « MAJ » pour entrer dans le menu grub, après avoir sélectionné « boot options » puis « restore mode » on arrive sur cette fenêtre.

enu de récupérat	ion (état du système de fichiers : lecture seule
resume	Reprendre le démarrage normal
clean	Essayer de libérer de l'espace
upkg fock	Keparer les paquels Casses Vénifien tous les sustèmes de fichiens
gruh	Mettre à jour le chargeur d'amorcage GRUB
network	Activer la prise en charge du réseau
root	Passer sur une console administrateur (root)
system-summary	Rapport d'état du système

Ici on choisit « root »



Ensuite on écrit « passwd 'nom_d'utilisateur' » pour changer le mot de passe.



Sous linux également le mot de passe peut donc facilement être contourné.

Conclusion

On a vu au cours de ce TP qu'il était relativement simple de passer outre un mot de passe quelques soit le système en place, cependant il existe des moyens de se protéger des personnes malveillantes qui voudraient s'introduire dans votre pc, dans la vidéo d'exemple (Mr Robot) Eliott utilise la méthode deux en remplaçant le mot de passe grâce au cmd qui a pris la place l'utilitaire.

Pour se prémunir de ses dangers on peut d'abord envisager de chiffrer son ou ses disques durs pour rendre les rendre plus difficile d'accès, mais aussi choisir un mot de passe BIOS pour éviter la modification de séquence de démarrage (clé usb), et pour les attaque qui serait en mesure de contourner cette défense on peut encore désactiver les ports usb de la machine concernée pour empêcher n'importe qui de brancher une clé usb sur la machine.