TP CYBERSÉCURITÉ : Intrusion simple Windows

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

Dans un premier t Je crée une nouve	temps j'ouvre VM Wa elle machine virtuelle	ire, avec le minimum de spécificité.	
J'utilise l'ISO de V	Vindows 7 du lecteur	réseau de MEWO \\10.10.0.5	
	New Virtual Machine Wizard	×	
		Welcome to the New Virtual Machine Wizard	
	17	What type of configuration do you want?	
		Typical (recommended) Create a Workstation 17.x virtual machine in a few easy steps.	
		Custom (advanced) Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.	
	Help	< Back Next > Cancel	
J'installe Windows	s 7		
J'installe Windows Ensuite je rentre u	s 7 un mot de passe		
J'installe Windows Ensuite je rentre u	s 7 un mot de passe		
J'installe Windows Ensuite je rentre u	s 7 un mot de passe configurer Windows Définir un mot de passe pou	r votre compte	
J'installe Windows Ensuite je rentre u	s 7 un mot de passe configurer Windows Définir un mot de passe pou Créer un mot de passe est une bonnr compte d'utilisateur contre les utilisa conservez-le en lieu sûr.	r votre compte e précaution de sécurité qui permet de protéger votre teurs indésirables. N'oubliez pas votre mot de passe ou	
J'installe Windows Ensuite je rentre u	s 7 un mot de passe Configurer Windows Définir un mot de passe pou Créer un mot de passe est une bonne compte d'utilisateur contre les utilisa conservez-le en lieu sûr.	I r votre compte e précaution de sécurité qui permet de protéger votre teurs indésirables. N'oubliez pas votre mot de passe ou lé) :	
J'installe Windows Ensuite je rentre u	s 7 un mot de passe Configurer Windows Définir un mot de passe et une bonne compte d'utilisateur contre les utilisa conservez-le en lieu sûr. Entrez un mot de passe (recommand force en lieu sûr.	Ir votre compte e précaution de sécurité qui permet de protéger votre teurs indésirables. N'oubliez pas votre mot de passe ou lé) :	
J'installe Windows Ensuite je rentre d	s 7 un mot de passe Configurer Windows Définir un mot de passe pou Créer un mot de passe est une bonn compte d'utilisateur contre les utilisa conservez-le en lieu sûr. Entrez un mot de passe (recommand Entrez à nouveau votre mot de passe Entrez à nouveau votre mot de passe	Ir votre compte e précaution de sécurité qui permet de protéger votre teurs indésirables. N'oubliez pas votre mot de passe ou lé) : e (obligatoire) :	
J'installe Windows Ensuite je rentre u	s 7 un mot de passe Configurer Windows Définir un mot de passe est une bonne compte d'utilisateur contre les utilisa conservez-le en lieu sûr. Entrez un mot de passe (recommand Entrez a nouveau votre mot de passe Entrez à nouveau votre mot de passe Entrez a nouveau votre mot de passe Entrez a nouveau votre mot de passe Azerty123 Choisisez un mot ou une expression Si vous oubliez votre mot de passe, V	Ir votre compte e précaution de sécurité qui permet de protéger votre teurs indésirables. N'oubliez pas votre mot de passe ou lé) : 	
J'installe Windows Ensuite je rentre d	s 7 un mot de passe Configurer Windows Définir un mot de passe pou Créer un mot de passe est une bonne compte d'utilisateur contre les utilisa conservez-le en lieu sûr. Entrez un mot de passe (recommand Entrez à nouveau votre mot de passe Entrez à nouveau votre mot de passe Entrez à nouveau votre mot de passe Azerty123 Choisissez un mot ou une expression Si vous oubliez votre mot de passe, V	Ir votre compte e précaution de sécurité qui permet de protéger votre teurs indésirables. N'oubliez pas votre mot de passe ou lé) : 	
J'installe Windows Ensuite je rentre u	s 7 un mot de passe Configurer Windows Définir un mot de passe est une bonne compte d'utilisateur contre les utilisa conservez-le en lieu súr. Entrez un mot de passe (recommand formation de mot de passe formation de mot de passe fazerty123 Choisissez un mot ou une expression Si vous oubliez votre mot de passe, V	r votre compte e précaution de sécurité qui permet de protéger votre teurs indésirables. N'oubliez pas votre mot de passe ou lé): e (obligatoire): qui vous aide à vous souvenir de votre mot de passe. Vindows affiche cette indication. Suivant	
J'installe Windows Ensuite je rentre u	s 7 un mot de passe Configurer Windows Définir un mot de passe est une bonne compte d'utilisateur contre les utilisa conservez-le en lieu sûr. Entrez un mot de passe (recommand formation Entrez à nouveau votre mot de passe formation Tapez une indication de mot de passe Azerty123 Choisissez un mot ou une expression Si vous oubliez votre mot de passe, V	r votre compte a précaution de sécurité qui permet de protéger votre teurs indésirables. N'oubliez pas votre mot de passe ou ié): ie de lobigatoire): iqui vous aide à vous souvenir de votre mot de passe. Vindows affiche cette indication. Suivant	



J'arrête la VM

erbeille	
Mise en route	
Se connecter à un projecteur	
Calculatrice	Thomas
Pense-bête	Documents
Outil Capture	Images Musieure
Paint	Ordinatour
Visionneuse XPS	
Télécopie et numérisation Windows	Périohériques et imprimantes
Connexion Bureau à distance	Programmes par défaut
Loupe	Aide et support
Tous les programmes	
echercher les programmes et fichiers	
	Fermez tous les programmes ouverts, arrêtez Windows et éteignez l'ordina

2) Booter sa VM Windows 7 avec Ubuntu

Pour ce faire, dans les paramètres de VMware j'enlève l'ISO de Windows 7 et je place l'ISO d'Ubuntu

Ensuite je fais clic droit sur la VM, je vais dans Power puis power On to Firmware pour démarrer sur le BIOS.



Sur le BIOS je change l'ordre de BOOT en plaçant le DVD/CD disque en premier





Une fous ubuntu démarré, je vais dans fichier puis dans Volume de 64 GB / User / Thomas et enfin Desktop







3) Expérimentation de la Méthode n°2b : via l'Environnement de récupération Windows

En suivant le tutoriel du site « <u>Réinitialiser le mot de passe d'un compte utilisateur sur Windows –</u> <u>Le Crabe Info</u> »

Je démarre ma VM en mode démarrage avancée en appuyant sur F8 puis je clique sur invite de commande



Dans l'invite de commande je tape

- D : pour aller sur le disque D
- dir pour vérifier que c'est bien le lecteur de windows
- cd Windows\system32 pour me déplacer dans le fichier system32
- copy Utilman.exe Utilman.exe.bak
- copy cmd.exe Utilman.exe

Je redémarre le pc et effectue la combinaison Windows + U pour ouvrir les options d'ergonomie mais grâce à l'intervention ci-dessus c'est cmd qui s'ouvre

FR		
Administrateur : C:\Wind	lows\system32\utilman.exe	
Microsoft Windows [Copyright (c) 2009	version 6.1.7601] Microsoft Corporation. Tous droits réservés.	
C:\Windovs\system32	>_	
	Thomas Mot de passe	
C	🥵 Windows 7 Professionnel N	

J'exécute ensuite la commande net user "nom_compte_utilisateur" nouveau_mot_de_passe



Avec le nouveau mot de passe thomas je peux accéder au bureau



La méthode utilisée dans la vidéo ressemble beaucoup à la Méthode n°2b : via l'Environnement de récupération Windows

Car le personnage lance l'outil Operating system pour ensuite changer cmd avec sethc pour que cmd s'ouvre à la place de celle-ci pour ensuite faire netuser et changer le mot de passe

4) Enfin

- Conclusion et méthode de protection : La plupart des utilisateurs ne se satisfont que d'un mot de passe pour protéger leur pc, mais on la bien vu grâce à ce TP, qu'un mot de passe seul est une méthode de protection trop faible pour sécuriser ses données.
 Il existe plusieurs méthodes pour protéger ses données.
 Crypter les données de son disque dur (cf : image ci-dessous)
 Utiliser une authentification à deux facteurs ou un compte Microsoft connecté
 Ou encore directement protégé son BIOS avec un mot de passe
- Pensez-vous qu'on a le même souci sur Mac ou Linux ?
 Je pense que tout comme Windows, Linux a aussi ses vulnérabilités et pour ce faire je vais tester le tutoriel ci-dessous
- Je crée une VM sur Linux (Ubuntu) je configure un mot de passe Puis je suis le tutoriel de <u>J'ai oublié mon mot de passe ! (ubuntu-fr.org)</u>

Je redémarre Ubuntu en maintenant la touche Maj pour accéder au menu de récupération Je lance root

network Activer la prise en charge du réseau root Passer sur une console administrateur	GRUB
	r (root)
<0k>	

En root je tape la commande passwd thomas Ensuite je tape un nouveau mot de passe

	network <mark>root</mark> system-summary	Activer la prise en charge du réseau Passer sur une console administrateur (root) Rapport d'état du système	
		<0k>	
Appuyez	sur Entrée pour la	la maintenance	
root@th Nouveau MOT DE	omas-virtual-machin mot de passe : PASSE INCORRECT : I	o pour continer) : ine:~# passwd thomas Le mot de passe comporte moins de 8 caractères	
Retapez Les mot Nouveau MOT DE	ie nouveau mot de s de passe ne corri mot de passe : PASSE INCORRECT : I	e passe : respondent pas. Le mot de passe comporte moins de 8 caractères	
Retapez passwd root@th	le nouveau mot de : mot de passe mis omas–virtual–machin	e passe : s à jour avec succès ine:~# _	

Je redémarre Ubuntu et dans la case mot de passe, je mets le nouveau de passe crée précédemment



J'arrive bel et bien à rentrer sur le bureau

