## **TP Intrusion simple Windows-Bloc3**

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

• Mettons-nous en condition ;

\_



 Nous avons bel et bien mis un mot de passe sur notre compte local administrateur et avons créer un fichier << toto.txt>> sur le bureau nous avons inséré les paroles de notre chanson préférée.

📓 🥅 toto - Notepad	—		×
Recy File Edit Format View Help			
Eh, ah, d'accord, ça va Tcho (jheez) tcho, tcho, tcho (let's get it) Quand elle marche, son booty fait "rakatakou" Quand j'ai vu ca, obligé de lui parler (ah) Mauvais djo, toujours une kichta sur moi Devant la cinquième, mon bébé, j'ai tout payé (on y va) Elle a kiffé le mood (elle aime trop parler) Elle a kiffé le mood (elle aime trop parler)			
			>
Ln 1, Col 1 100% Windows (CRLF)	UTF-	-8	
🗄 🔎 Type here to search 🛛 🔯 🎁 🖽 💽 🚍 🗐 之 🥥			ㅅ @ ☜ 맏 ∽» 『

-Eteignons notre VN	1.		
👽 Oracle VM VirtualBox - Gestionnaire de ma	chines	_	$\times$
Fichier Machine Aide			
Outils	Nouvelle Ajouter Configuration Oublier Démarrer		
64 <b>TP</b>	Prévisualisation		
CO 🙂 Éteinte	🦲 Général		
64 Jean Nguema	Nom : WIN10 Système d'exploitation : Windows 10 (64-bit)		
20 😃 Éteinte	System		
win10	Mémoire vive : 2048 Mo Ordre d'amorçage : Disquette, Optique, Disque dur Accélération : Pagination imbriquée, Paravirtualisation Hyper-V		
	Affichage		
	Mémoire vidéo : 128 Mo Contrôleur graphique : VBoxSVGA Serveur de bureau à distance : Désactivé Enregistrement : Désactivé		
	Stockage Contrôleur : SATA Port SATA 0: WIN10.vdi (Normal, 20,00 Gio) Port SATA 1 : [Lecteur optique] Windows.iso (4,48 Gio)		
	Didte hôte : Windows DirectSound Contrôleur : Intel Audio HD		
	Réseau Interface 1: Intel PRO/1000 MT Desktop (NAT)		
	USB     OHCI Filtres de périphérique : 0 (0 actif)		
	Dossiers partagés Aucun		
	Description     Aucune		

Continuons notre expérimentation ;
 Bouttons sur notre VM mais en utilisant une ISO de Ubunto Desktrop cette fois.

outils	Nouvelle Ajouter Configuration Oublier Démarrer							
Outils	Nouvelle Ajouter Configuration Oublier Démarrer							
ТР								
	Prévisualisation							
U de Éteinte	🦲 Général							
Jean Nguema	Nom : WIN10 Système d'exploitation : Windows 10 (64-bit)	Nom : WIN10 Système d'exploitation : Windows 10 (64-bit)						
	System							
WIN10	Mémoire vive : 2048 Mo Ordre d'amorçage : Disquette, Optique, Disque dur Accélération : Pagination imbriquée, Paravirtualisation Hyper-V							
	E Affichage							
	Mémoire vidéo : 128 Mo Contrôleur graphique : VBoxSVGA Serveur de bureau à distance : Désactivé Enregistrement : Désactivé							
	Stockage							
	Contrôleur : SATA Port SATA 0 : WIN10.vdi (Normal, 20,00 Gio) Port SATA 1 : [Lecteur optique] ubuntu-18.04.6-live-server-amd64.iso (969,00 M	B)						
	🕪 Audio							
	Pilote hôte : Windows DirectSound Contrôleur : Intel Audio HD							
	Préseau Réseau							
	Interface 1: Intel PRO/1000 MT Desktop (NAT)							
	🥟 USB							
	Contrôleur USB : OHCI Filtres de périphérique : 0 (0 actif)							
	Dossiers partagés							
	Aucun							
	Description							
	Aucune							







- A l'aide de l'ISO Ubuntu nous avons démarré en mode live DVD (<<Essayer Ubuntu>>) et nous avons pu accéder à notre fichier toto et il est également possible de modifier le fichier.
- Essayons autre chose ;

-A l'aide de ce lien <u>https://lecrabeinfo.net/reinitialiser-mot-de-passe-compte-utilisateur-local-windows.html</u> choisissons l'une des techniques et expérimentons là pour voir si effectivement ce serait aussi simple que cela.

WINDOWS 10 [En 1 Fichier Machine Écran	fonction] - Entrée F	Oracle VM VirtualBox Périphériques Alde			1.7	×
e A	Adva	anced option	IS			ţ.
	<0>	Startup Repair Fix problems that keep Windows from loading	4	System Restore Use a restore point recorded on your PC to restore Windows		
	C:\	Command Prompt Use the Command Prompt for advanced troubleshooting	-	System Image Recovery Recover Windows using a specific system image the		
	¢	Uninstall Updates Remove recently installed quality or feature updates from Windows				
						N

\*A ce niveau nous rentrons dans les commandes avancées afin de pouvoir indiquer des commandes.



-Nous suivons le cheminement en introduisant des commandes.





-A ce niveau nous pouvons alors modifier le mot de passe de l'utililsateur.



\_Chose faite, nous pouvons redémarrer la machine et introduire le nouveau mot de passe.

- Alors après avoir expérimenter la méthode 2b, nous pouvons donc en déduire qu'elle est très similaire à celle de la vidéo évoquée en introduction.
- Enfin ;
  - En vue de la facilité avec laquelle nous avons pu enfreindre Nous la sécurité dans un Windows, de ce fait, on peut en conclure que la sécurité avec un system Windows reste toujours un souci majeur et doit être une des priorités pour ces derniers afin de mieux à point ce souci.
  - Nous pouvons se protéger de ce problème tout d'abord en faisant fréquemment nos mises à jour, puis éviter des virus.
  - Reprenons le fil de ce TP avec une machine linux et voyons ensemble si nous avons la même défaillance.

\*Commençons par créer une machine virtuelle Linux .



\*Puis utilisons le touche MAJ ou Echap au démarrage de la VM, cela ouvre le menu Grub et va nous permettre d'accéder aux options avancées.



## \*Puis rentrer dans le mode de reécupération.

💕 keran [En fonction] - Oracle VM VirtualBox	_		$\times$	
Fichier Machine Écran Entrée Périphériques Aid				
GNU GRUB vers	on 2.04			
₩Ubuntu, with Linux 5.15.0-91-generic Ubuntu, with Linux 5.15.0-91-generic ( Ubuntu, with Linux 5.4.0-42-generic Ubuntu, with Linux 5.4.0-42-generic (r	ecovery mode) covery mode)			
Use the ↑ and ↓ keys to select whic Press enter to boot the selected OS before booting or `c' for a command menu.	∣entry is highl `e' to edit th line. ESC to re	lighted. ne commar eturn pre	nds avious	

\*Puis on arrive on se met en root pour ouvrir la console en administrateur.



\*A ce niveau on va utiliser la commande **passwd** suivi de l'utilisateur pour changer son mot de passe. Et pour finir taper la commande reboot pour redémarrer la machine virtuelle.

esume	Resume normal boo clean dpkg fsck grub network root system-summary	ot normal boot Try to make free space Repair broken packages Check all file systems Update grub bootloader Enable networking <u>Drop to root shell prompt</u> System summary <ok></ok>	
ress Enter for m or press Control oot@keran-Virtua ew password: etype new passwor asswd: password oot@keran-Virtua	aintenance -D to continue):  lBox:~# passwd ker  rd: updated successful  lBox:~#	ran .ly	



- Par conséquent, nous pouvons constater que nous retrouvons le même souci sur un Linux.