Clément Arki BTS SIO 1

### 1) Validation et mise en place réseau

srvatck (1ère machine)

Mise en place des IP (Adresse IP: 192.168.1.50) :

📷 srvatck nouveau [En fonction] - Oracle VM Virtu... 🛛 –

Fichier Machine Écran Entrée Périphériques

l	<u>ь</u> Р	Propriétés de Protocole Internet (TCP/IP)	<u>? × </u>											
	Gé	Général												
Ior	s [	Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.												
	C	O Obtenir une adresse IP automatiquement												
	Γ	Utiliser l'adresse IP suivante :	/s											
		Adresse IP : 192 . 168 . 1 . 50												
		Masque de <u>s</u> ous-réseau : 255 . 255 . 0												
		Passerelle par défaut :         192 . 168 . 1 . 254												
	[	<ul> <li>Obtenir les adresses des serveurs DNS automatiquement</li> <li>Utiliser l'adresse de serveur DNS suivante :</li> </ul>	s											
		Serveur DNS pré <u>f</u> éré :	4											
	Γ	Serveur DNS auxiliaire :												
	Ŀ	<u>A</u> vancé												
	_	OK Annul	er me											

### Routeur accès distant activé :

😹 srvatck nouveau [En fonction] - Oracle VM Virtu... 🛛 —

Fichier	Machine	Écran	Entrée	Périphériques	Ai
Services	Propriétés	de Routage et	accès distant	(Ordinateur local)	<u>? ×</u>
Eichier Action	A Général Nom du Nom affi Descript Chemin C:WIN Iype de Statut di Dén Statut di	Èonnexion       Rét         service :       Remot         ché :       Rou         ion :       Off         d'accès des fichie       DOWS\system32         démarrage :       Aut         u service :       Démarrage         a service :       Démarrage         uvez spécifier les         res de démarrage	eupération Déper eAccess Itage et accès dis e aux entreprises s les environneme rs exécutables : (svochost.exe -k n omatique ré grêter Suis S paramètres qui s'	endances	
			UK	Annuler App	liquer

Enlever le pare feu Windows :

Test de ping sur le CMD :



Cela correspond à l'IP de la machine 1 (il voit aussi s'il est connecté avec la machine 2 avec l'IP de passerelle et aussi avec le masque de sous réseau).

#### arki (2ème machine)

### Mise en place des IP (Adresse IP: 192.168.1.52):



## Routage et accès distant activé :

Fichier M	lachine Écra	n Entrée	Périphériques	Aid
🖏 Services	Propriétés de Rout	age et accès dista	unt (Ordinateur loc	? 🔀
Fichier Action A	Général       Connexion         Nom du service :       F         Nom complet :       Description :         Description :       C:WINDOWS\syst         Type de démarrage       Statut du service :         Statut du service :       Description :         Vous pouvez spécifiservice.       Paramètres de démarrage	Age et acces (1) to         Récupération       Dépe         emoteAccess         Routage et accès dis         Offre aux entreprises         dans les environneme         fichiers exécutables :         em32\svchost.exe -k n         Automatique         émarré         Agrêter       S         er les paramètres qui s'a         rage :	appliquent pour le démarrage o	
		ОК	Annuler Appliq	liner

🛣 arki nouveau [En fonction] - Oracle VM VirtualBox

Enlever le pare feu Windows :

# 🚡 arki nouveau [En fonction] - Oracle VM VirtualBox

Fichier N	Machine Écran Entrée Périphériques Aic
Services	Propriétés de Pare-feu Windows / Partage de connexi ? 🗙
Fichier Action	A       Général       Connexion       Récupération       Dépendances         Nom du service :       SharedAccess         Nom complet :       Pare-feu Windows / Partage de connexion Internet         Description :       Assure la traduction d'adresses de réseau, l'adressage, les services de réseaution de noms         Chemin d'accès des fichiers exécutables :       C:\WINDOWS\system32\svchost.exe -k netsvcs         Lype de démarrage :       Désactivé
	Statut du service : Arrêté         Démarrer       Arrêter       Suspendre       Regrendre         Vous pouvez spécifier les paramètres qui s'appliquent pour le démarrage du service.         Paramètres de démarrage :       OK       Annuler       Appliquer

Test de ping sur le CMD :



Cela correspond à l'IP de la machine 2 (il voit aussi s'il est connecté avec la machine 1 avec l'IP de passerelle et aussi avec le masque de sous réseau).

1) Les 2 machines sont connectées l'une à l'autre. On peut voir si elles sont connectées l'une à l'autre grâce au cmd de Windows, puis en tapant ping "l'adresse IP"

2) Surcharger un serveur pour avoir un déni de service



### Ou :



On peut constater que l'UC (Unité centrale), c'est-à-dire le pourcentage du temps pendant lequel le processeur est utilisé, augmente constamment lorsque le fichier est exécuté (soit une fois ou plusieurs fois).

2) Le constat est prouvé car il y a l'image au-dessus qui montre que quand le fichier est exécuté, on voit sur le gestionnaire des tâches (onglet performance) qu'il y a une

augmentation du processeur dans l'ordinateur (qui est montré sur le graphique avec les pourcentage).

3) L'explication est que le fait d'exécuter plusieurs fois le fichier .bat, on voit que l'UC, c'està-dire le pourcentage du temps pendant lequel le processeur est utilisé, augmente constamment. Le fait d'exécuter plusieurs fois ce fichier peut entraîner à des dénis de services du serveur.

4) Pour parer ce type d'attaque, il faut avoir des bases de précautions lorsque par exemple on reçoit un fichier (.bat par exemple), c'est-à-dire ne pas l'ouvrir et même effacer ce fichier de l'ordinateur. Voici quelques conseils pour ne pas tomber sur une attaque ou prendre les devants (ex: sauvegarde de données) en cas d'attaque:

- Ne pas ouvrir les messages dont la provenance ou la forme est douteuse
- Apprendre à identifier les extensions douteuse des fichiers pour ensuite effacé celle qui ne vont pas
- Mettre à jour les outils et sauvegarder les données
- Utiliser un compte utilisateur plutôt qu'un compte administrateur
- 3) Jeux express

### 1) Mise en place

### Création d'un nom d'utilisateur "testeurfou" dans les Utilisateurs :



Création dossier : jeux express

2003	🚡 srvatck nouveau 2 [En fonction] - Oracle VM VirtualBox 🦳 —											
Fic	hier	Ma	chine	Écran	Entr	ée Pér <mark>i</mark> p	hériques	Aide				
	🚞 C:\Do	cuments	s and Settin	gs\All Us	ers\clemen	t\Documents				_ 8		
	<u>F</u> ichier	<u>E</u> dition	Affic <u>h</u> age	Fa <u>v</u> oris	<u>O</u> utils <u>?</u>							
	🔇 Précé	dente 👻	🕤 - 😥	🔎 Rech	iercher 🛛 🌔 🛛	Dossiers 🛛 📴 👔	7 🗙 🍤 🛛 🖽	]-				
	A <u>d</u> resse	🚞 C:\Do	ocuments and	Settings\/	All Users\cleme	nt\Documents			•	🔁 ок		
[	Nom 🔺				Taille	Туре	Date de r	nodification	Attributs			
	🚞 jeux e	express				Dossier de fichiers	; 09/12/20	22 11:19				

Cocher Contrôle Total (pour Tout le monde) dans le Partage :

-	😹 srvatck nouveau 2 [En fonction] - Oracle VM VirtualBox 🦳 🛛 [											
	Fichier	Machine	Écran	Entrée	Périphériq	ues	Aide					
	C:\Docu Eichier E O Précéde Agresse C Nom A	Propriétés de Autorisat Gé Autorisa Noms	ioux evoress ions pour jeux tions du partage d'utilisateurs ou o out le monde	k express			21x					
ж ц		Autoris Con Mod Lec	ations pour Tout trôle total lífier ture	: le monde		Autoriser	Refuser					

Cocher Contrôle Total (pour Tout le monde) dans Sécurité :



Le dossier à une icône qui signifie que le partage et la sécurité est activé :



Un raccourcie à été créé s'appelant "JEUDECON" et une icône en forme d'arbre a été mise :

📷 srva	😹 srvatck nouveau 2 [En fonction] - Oracle VM VirtualBox —										
Fichier	Machine É	cran Enti	rée Périp	ohériques	Aide						
C:\Documents and Settings\All Users\clement\Documents\jeux express											
Eichier	Edition Affichage Fa	a <u>v</u> oris <u>O</u> utils <u>?</u>									
🔇 Pré	edente 🝷 🕤 👻 🥬 🎾	🔍 Rechercher 🛛 🌔	Dossiers 🛛 📴 🧯	» 🗙 🍤   🔡-							
Adresse	C:\Documents and Se	ttings\All Users\clem	ent\Documents\jeu	ix express		-					
Nom 4		Taille	Туре	Date de mod	lification	Attributs					
SP JEU	DECON	2 Ko	Raccourci	09/12/2022	11:25	А					

Le fichier "attrape\_nigault.bat" (ou on à remplie du code en bat) a été enregistré dans le dossier jeux express :

2003	🚠 srvatck nouveau 2 [En fonction] - Oracle VM VirtualBox 🦳 🗌											
Fie	chier	Machine	Écrar	n Entr	ée Périp	hériques	Aide					
	C:\Documents and Settings\All Users\clement\Documents\jeux express											
	Eichier	Edition Affichage	Fa <u>v</u> oris	<u>O</u> utils <u>?</u>								
	🔇 Précé	dente 👻 🕤 👻 ಶ	🛛 🔎 Rec	hercher 🏾 🌔 🕻	Dossiers 🛛 🕞 🗯	» 🗙 🍤   🗉	-					
	Adresse	🛅 C:\Documents ar	id Settings\	All Users\cleme	ent\Documents\jeu	x express		<b>•</b>	🔁 ок			
	Nom 🔺			Taille	Туре	Date de i	modification	Attributs				
	P JEUDE	ECON		2 Ko	Raccourci	09/12/20	22 11:25	A				
	📑 attrap	pe_nigault.bat		1 Ko	Fichier de comma	ind 09/12/20	22 11:30	А				

Un raccourcie a été créé en liaison avec le fichier "attrape\_nigault.bat". Le raccourci s'appelle maintenant "BEAUNIGAULT".

Une icône en forme de cadena à été miseLe fichier "attrape\_nigault.bat" (ou on à remplie du code en bat) a été enregistré dans le dossier jeux express :

2003	srvat	ck nou	iveau 2	[En	fonctio	n] - (	Oracle	VM Virtu	alBox	_		×
Fie	hier	Ma	chine	Éc	cran	Entr	ée	Périphéri	ques	Aide		
	🚞 C:\Do	ocuments	s and Setti	ngs\/	All Users\c	lemen	t\Docun	nents∖jeux ex	press			_ 8 ×
	<u>F</u> ichier	<u>E</u> dition	Affic <u>h</u> age	Fay	oris <u>O</u> util	s <u>?</u>						<b>1</b>
	🔇 Préc	édente 👻	🕤 ד 😥	1	Rechercher	r 🌔 🛙	Dossiers	📴 🎯 🗙	⊌			
	A <u>d</u> resse	C:\De	ocuments an	d Sett	ings\All Use	rs\cleme	nt\Docum	ients\jeux expr	ess		•	🔁 ок
	Nom 🔺					Taille	Туре		Date de mo	dification	Attributs	
	🔐 JEUD	ECON				2 Ko	Raccour	ci	09/12/2022	2 11:25	А	
1	👅 attra	pe_nigault	t.bat			1 Ko	Fichier d	e command	09/12/2022	2 11:30	A	
1	👌 BEAL	INIGAULT				2 Ko	Raccour	ci	09/12/2022	2 11:32	А	
1												

Un partage à été fait entre Windows XP et Windows 2003.

Le partage provient du dossier "jeux express" qui se trouve dans le serveur Windows 2003 (Et maintenant ce dossier est lié entre les 2 serveurs qui sont Windows 2003 et Windows XP). Il y a aussi les fichiers correspondant à :





### 2) Tester un Trojan

On créé un utilisateur testeurfou sur Windows XP : 🕻 arki nouveau 2 [En fonction] - Oracle VM VirtualBox  $\square$ Fichier Écran Machine Entrée Périphériques Aide 🔞 Outils 🛛 administration Fichier Edition Affichage Favoris Outils ? 🔇 Précédente 🔹 🍙 🕤 🎁 💭 Rechercher 🛛 🔂 Dossiers 🛛 📰 🗸 📕 Gestion de l'ordinateur Adresse 🦏 🕻 🖳 Fichier Action Affichage Fenêtre ? \_ 8 Gestion (  $\rightarrow$ **E** 🕼 🖪 😭 4 🖳 Gestion de l'ordinateur Actualiser 📺 Rend Nom Nom complet Description 🐔 Outils système 😰 Dépla Ė٠ 🕵 admin 🗄 💼 Observateur d'événements 🜆 Administrateur Copi Compte d'utilisateur d'administratio 🔓 HelpAssistant 🛃 Invité 🔕 Publi Compte Assistant de l'aide... Compte d'assistance à distance Compte d'utilisateur invité 🖄 Enve 🔁 Utilisateurs SUPPORT\_38... CN=Microsoft Corporation... Ceci est le compte d'un fournisseur élect 🚞 Groupes 🗙 Supp 🜆 testeurfou testeurfou 🎆 Journaux et alertes de perfo 🚚 Gestionnaire de périphérique 🕍 Stockage

On se connecte dans la session testeurfou dans le serveur Windows XP :



Le partage entre Windows XP (dans la session testeurfou) et le Windows 2003 sont liés (il y a aussi le partage entre Windows 2003 (dans la session Administrateur) et le Windows XP qui sont liés).

5) Quand on clique sur "jeudecon", voici ce qu'il se passe :



5) On constate qu' en cliquant sur "JEUDECON" il y a un arrêt du système.

Même le dossier partagé fait planter le système :



6) L'explication est que quand on clique sur "jeudecon" il se passe qu'on a un message d'arrêt du système sur les 2 machines.

7) Pour parer ce type d'attaque, il faut faire attention au fichier que l'on télécharge et où on clique.

8) On constate que quand on clique sur attrape\_nigault.bat. le fichier jeudecon s'efface :

🛛 🔀 arki nouveau 2 [En fo	onction] - Oracle	VM VirtualBox		— П	×
	é <u> </u>		A : 1		
Fichier Machine E	Ecran Entrée	Périphériques	Aide		
📽 jeux express sur '192.168.1.'	50' (Z:)				
Fichier Edition Affichage Favoris	Outils ?				
Précédente 🔹 🕥 🕤 🧊	🔎 Rechercher 🛛 🎼 🛛	Dossiers			
Adresse 🗝 Z:\					💌 🄁 🗸
Gestion des fichiers       Image: Créer un nouveau dossier         Image: Créer un nouveau dossier       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur le Web       Image: Créer un nouveau dossier         Image: Publier ce dossier sur	attrape Fichier d 1 Ko	nigault le commande MS-DOS	BEAUNIGAULT Raccourci 1 Ko	t	
Pareil sur l'autre machine	<u>}.</u>				
😹 srvatck nouveau	2 [En fonctio	n] - Oracle VM V	Vir —		$\times$
Fichier Machine	Écran	Entrée Périp	ohériques A	\ide	
🚞 C:\Documents and Settings	\All Users\clemen	t\Documents\jeux e	press		_ 8 ×
Eichier Edition Affichage Fa	a <u>v</u> oris <u>O</u> utils <u>?</u>				_
🔇 Précédente 🝷 🕤 👻 🏂 🌙	🔎 Rechercher 🛛 🌔	Dossiers 🛛 📴 🍞 🗙	<b>9</b>		
Auresse 🗀 C:\Documents and Se	ettings\All Users\clem	ent\Documents\jeux expr	ess	•	🔁 ок
Nom 🔺	Taille	Туре	Date de modification	Attributs	
🐻 attrape_nigault.bat	1 Ko	Fichier de command	09/12/2022 11:30	A	

9) L'explication est que le fait d'avoir cliquer sur le fichier attrape\_nigault.bat, une commande a permis d'effacer le fichier "jeudecon", et aussi sur l'autre machine sur le Windows 2003 (car on a cliqué sur la machine Windows XP).

10) Pour parer cette parade, il faut éviter de télécharger des fichiers malveillants et les effacer si on les as téléchargé.

1 Ko Raccourci

09/12/2022 14:11

А

🍰 BEAUNIGAULT