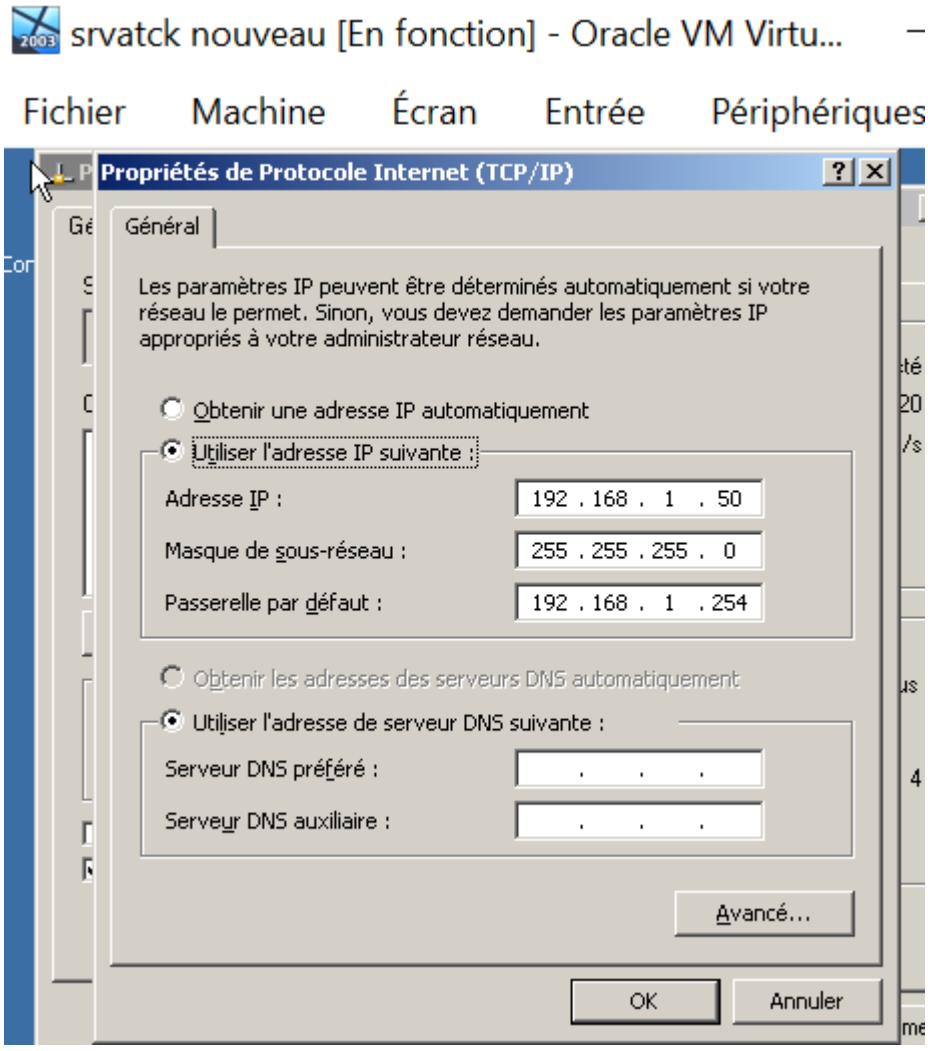
Clément Arki
BTS SIO 1

TP: Attaque défense (cybersécurité chapitre 2a) 27/09/2022

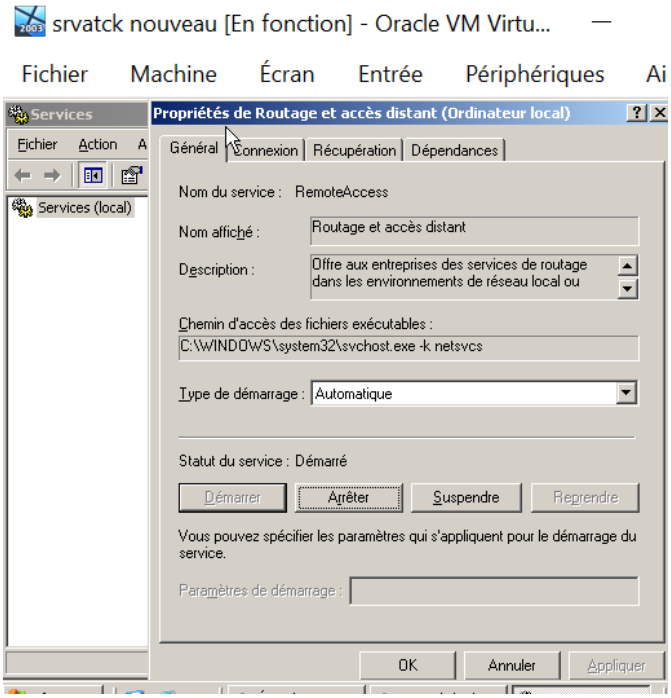
1) Validation et mise en place réseau

srvatck (1ère machine)

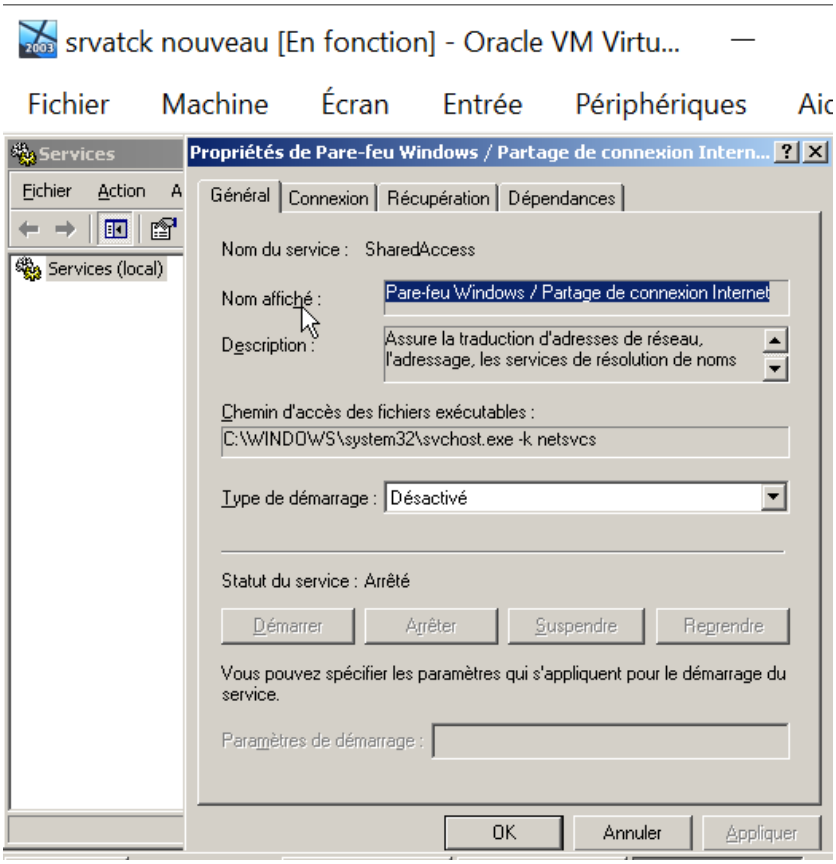
Mise en place des IP (Adresse IP: 192.168.1.50) :



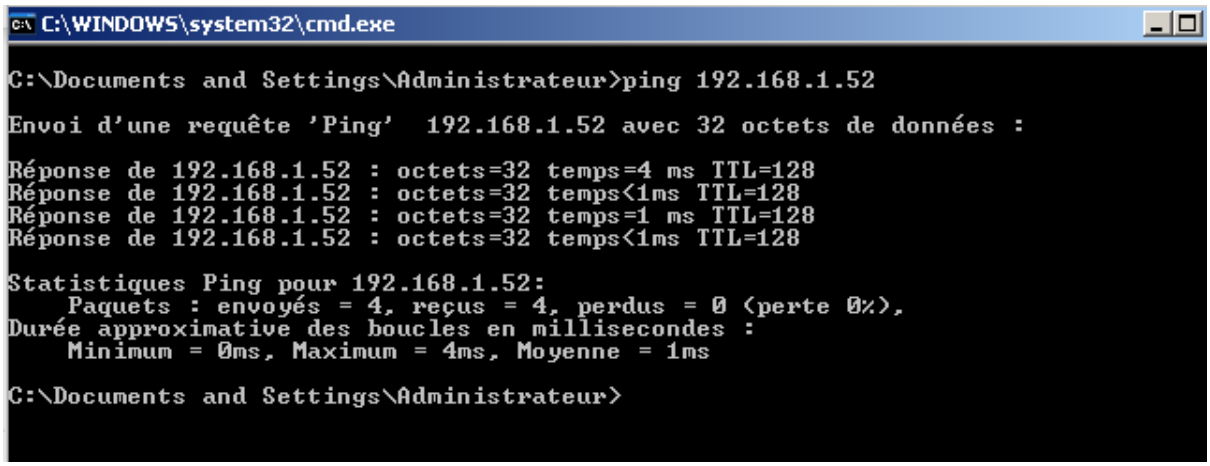
Routeur accès distant activé :



Enlever le pare feu Windows :



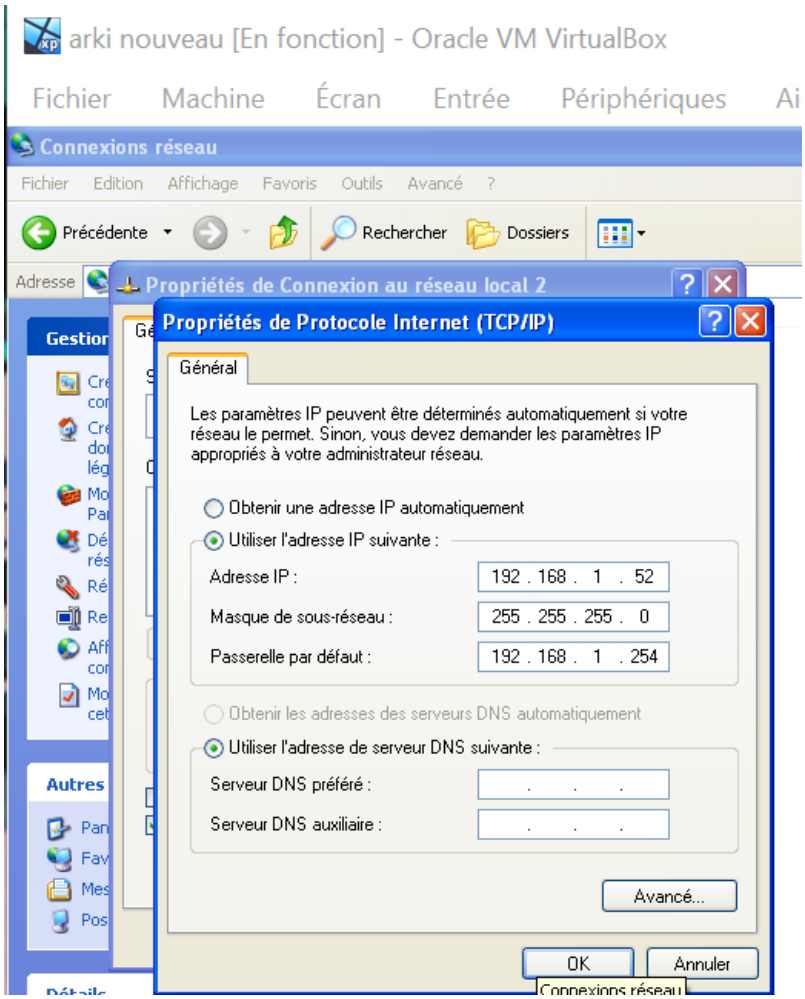
Test de ping sur le CMD :



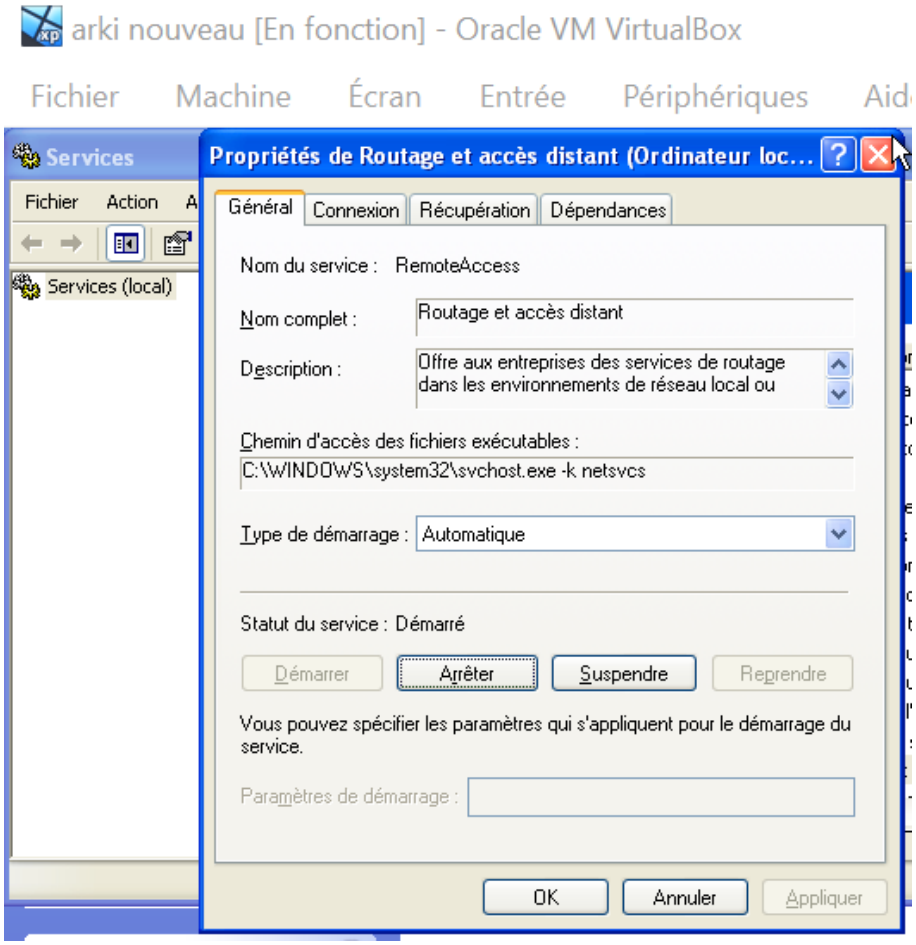
Cela correspond à l'IP de la machine 1 (il voit aussi s'il est connecté avec la machine 2 avec l'IP de passerelle et aussi avec le masque de sous réseau).

arki (2ème machine)

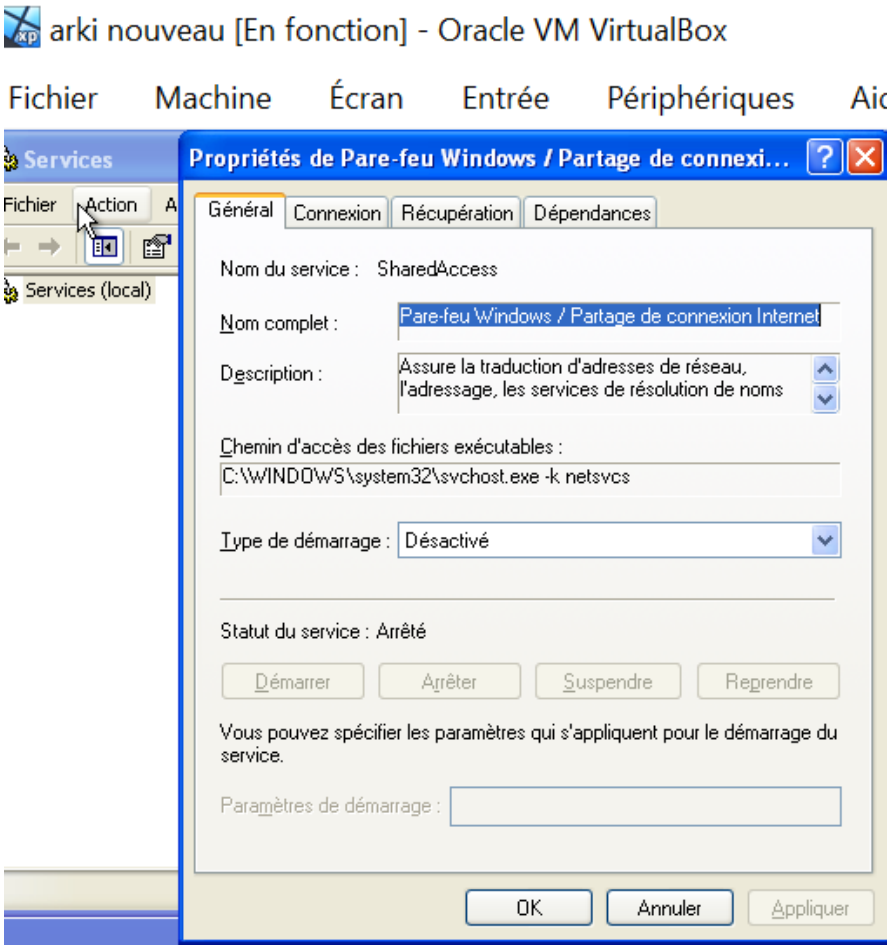
Mise en place des IP (Adresse IP: 192.168.1.52):



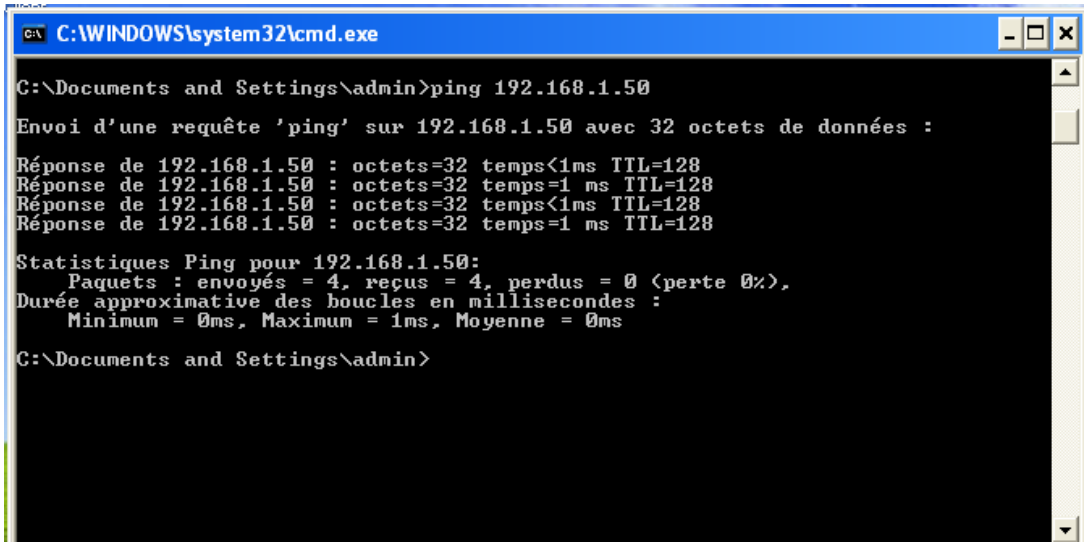
Routage et accès distant activé :



Enlever le pare feu Windows :



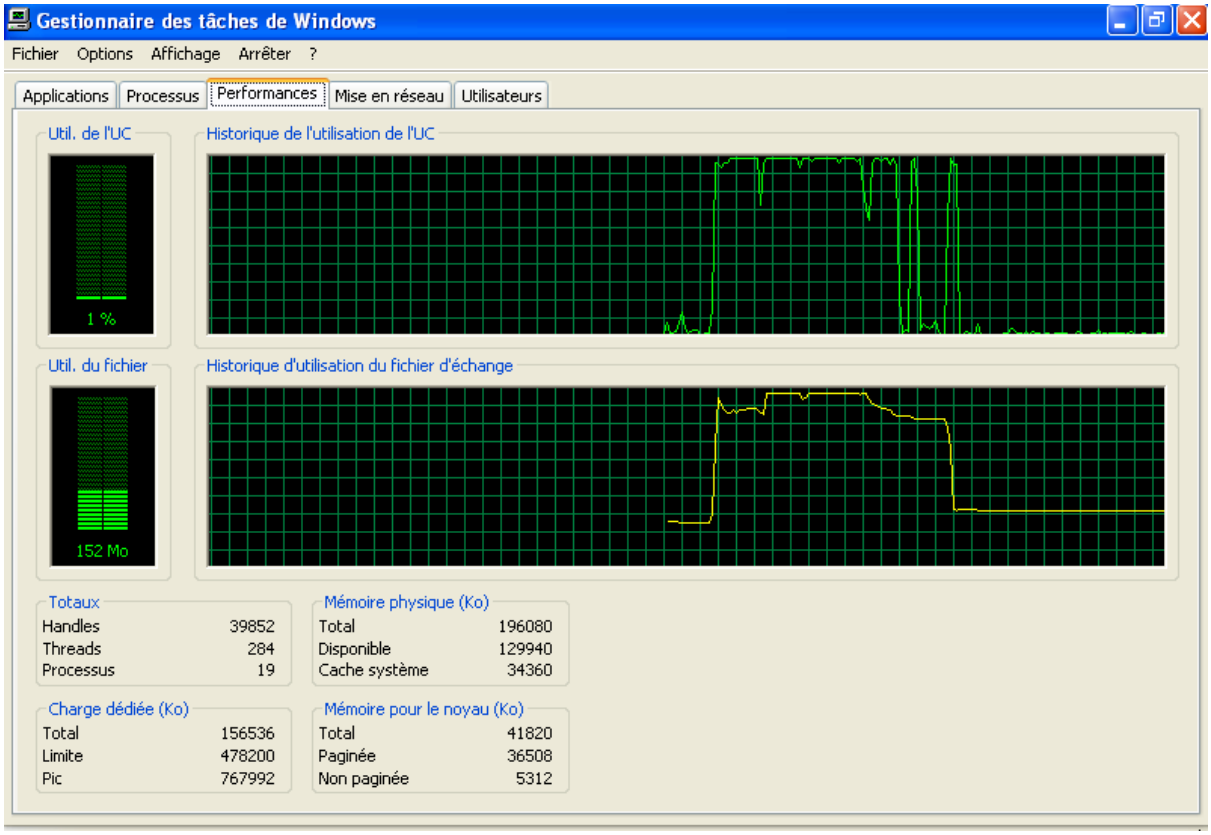
Test de ping sur le CMD :



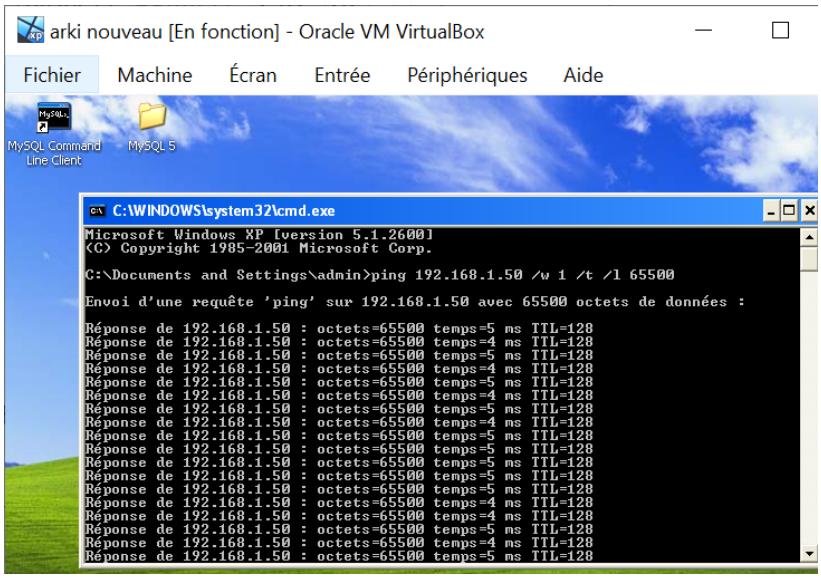
Cela correspond à l'IP de la machine 2 (il voit aussi s'il est connecté avec la machine 1 avec l'IP de passerelle et aussi avec le masque de sous réseau).

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'est-à-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.

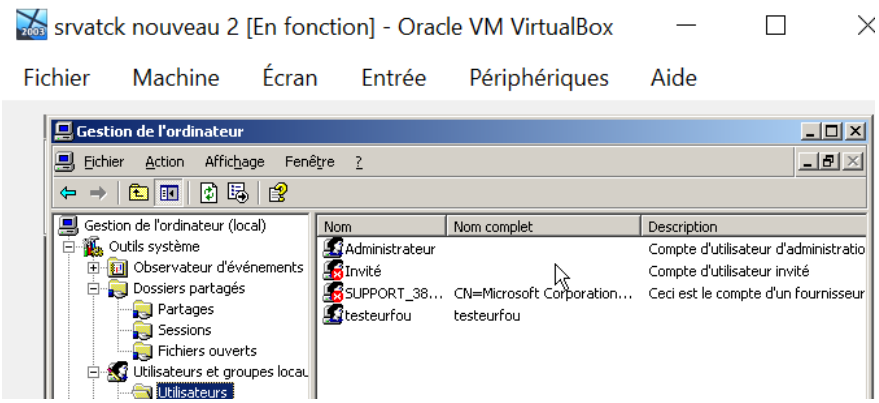
4) Pour parer ce type d'attaque, il faut avoir des bases de précautions lorsque par exemple on reçoit un fichier (.bat par exemple), c'est-à-dire ne pas l'ouvrir et même effacer ce fichier de l'ordinateur. Voici quelques conseils pour ne pas tomber sur une attaque ou prendre les devants (ex: sauvegarde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

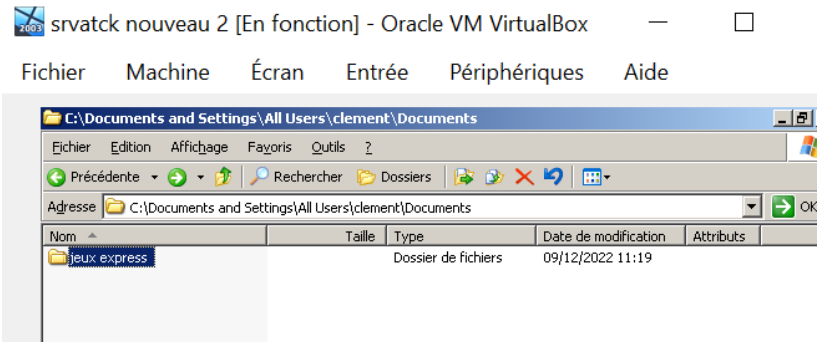
3) Jeux express

1) Mise en place

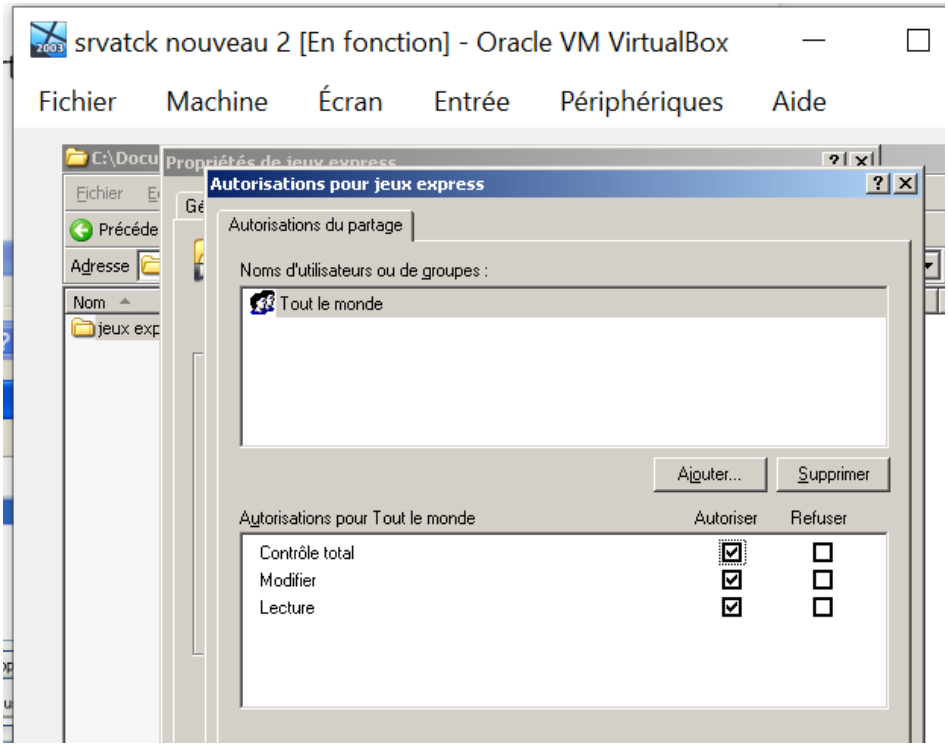
Création d'un nom d'utilisateur "testeurfou" dans les Utilisateurs :



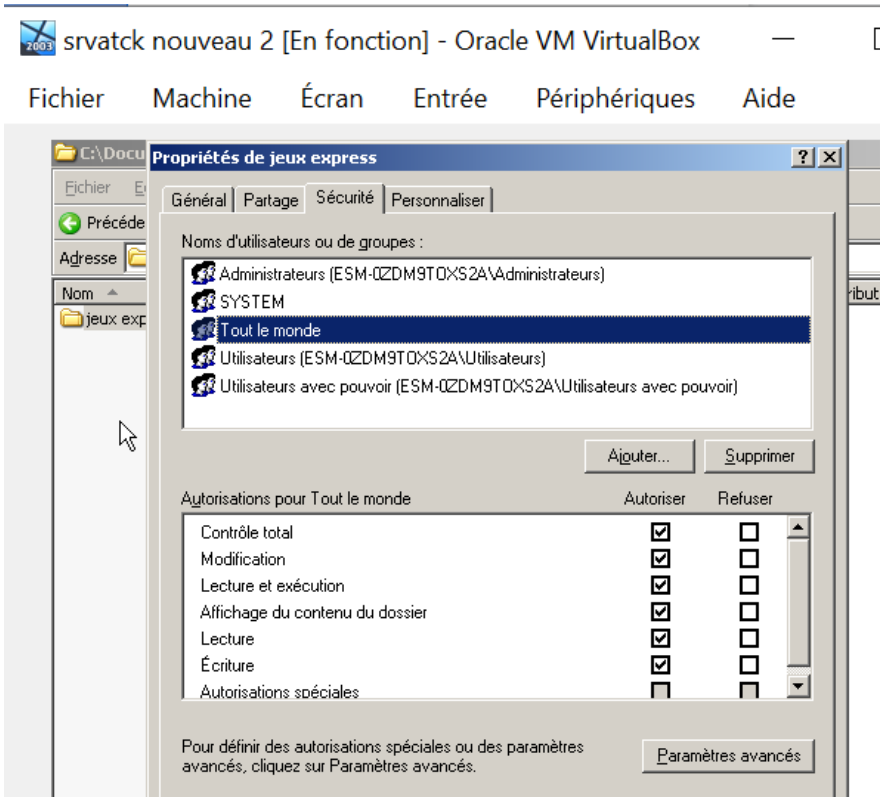
Création dossier : jeux express



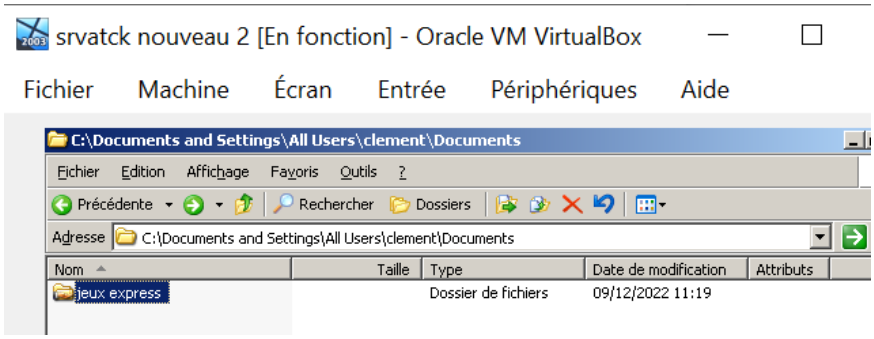
Cocher Contrôle Total (pour Tout le monde) dans le Partage :



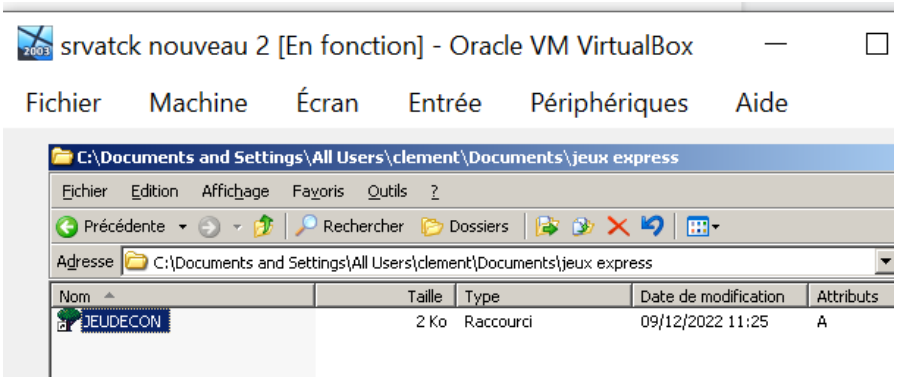
Cocher Contrôle Total (pour Tout le monde) dans Sécurité :



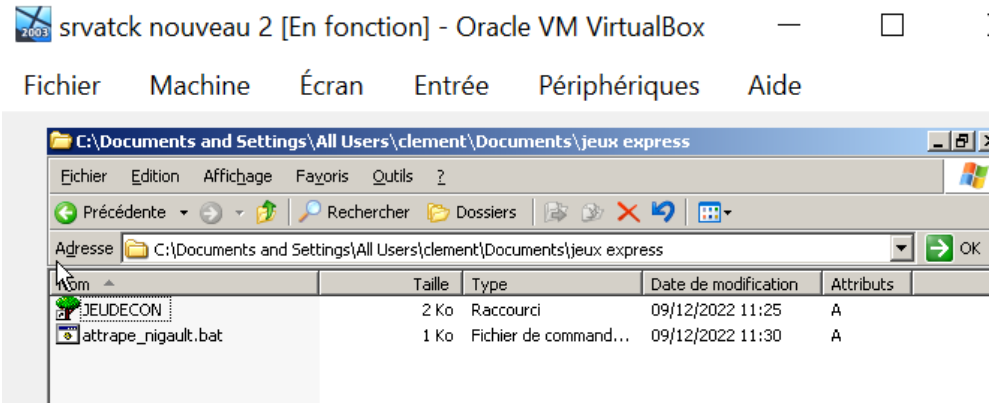
Le dossier à une icône qui signifie que le partage et la sécurité est activé :



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

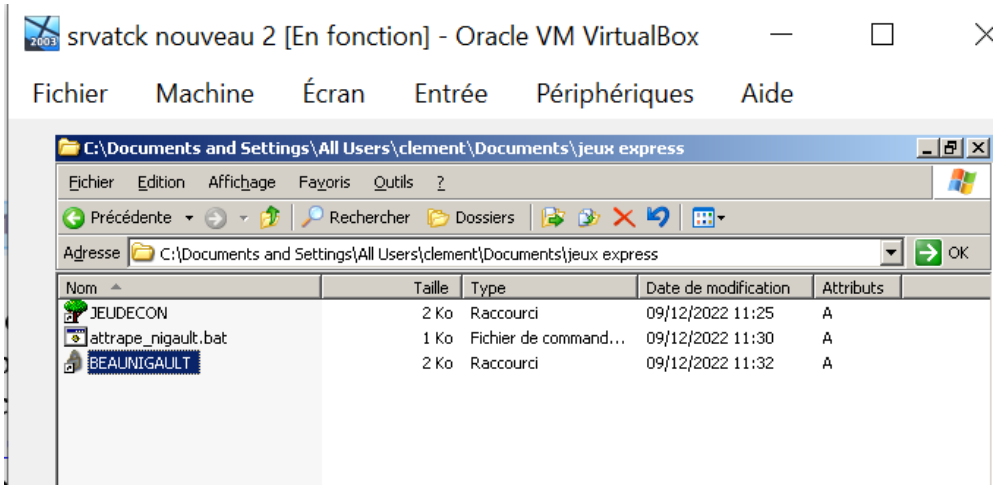


Le fichier “attrape_nigault.bat” (ou on à remplie du code en bat) a été enregistré dans le dossier jeux express :



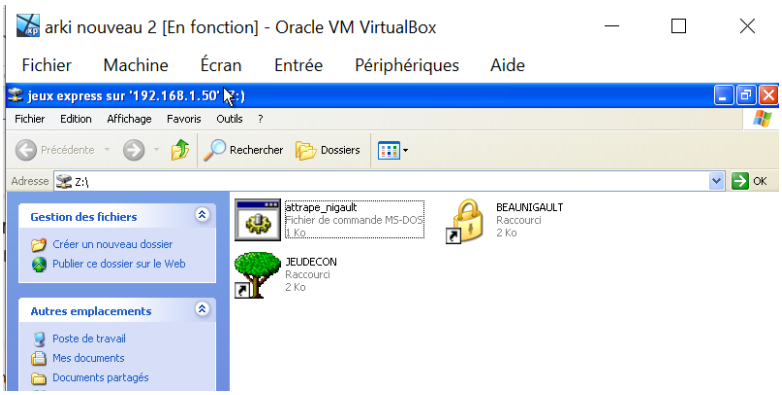
Un raccourcie a été créé en liaison avec le fichier “attrape_nigault.bat”. Le raccourci s'appelle maintenant “BEAUNIGAULT”.

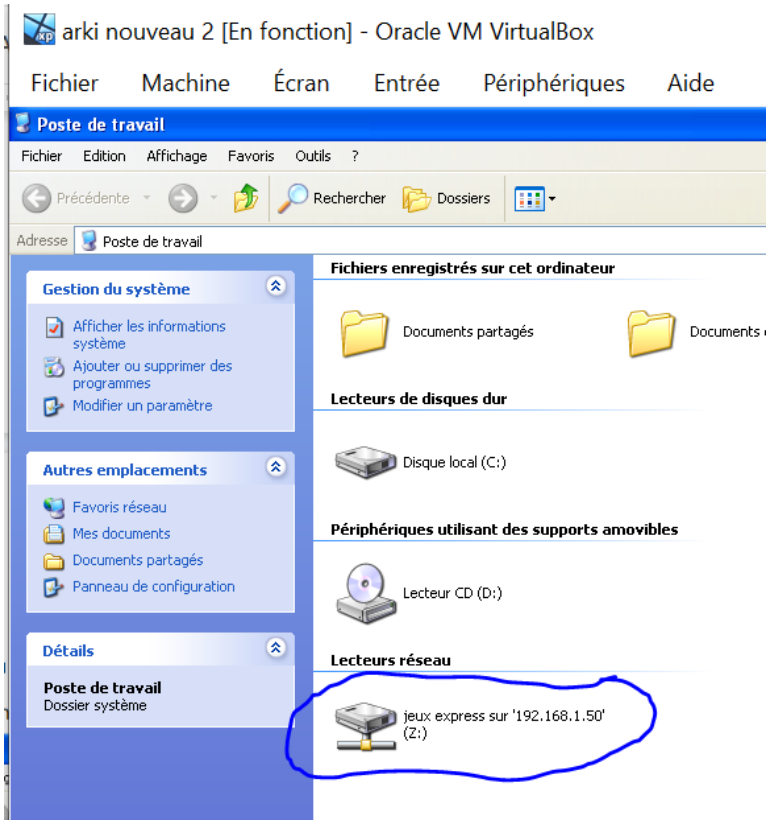
Une icône en forme de cadena à été miseLe fichier “attrape_nigault.bat” (ou on à remplie du code en bat) a été enregistré dans le dossier jeux express :



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

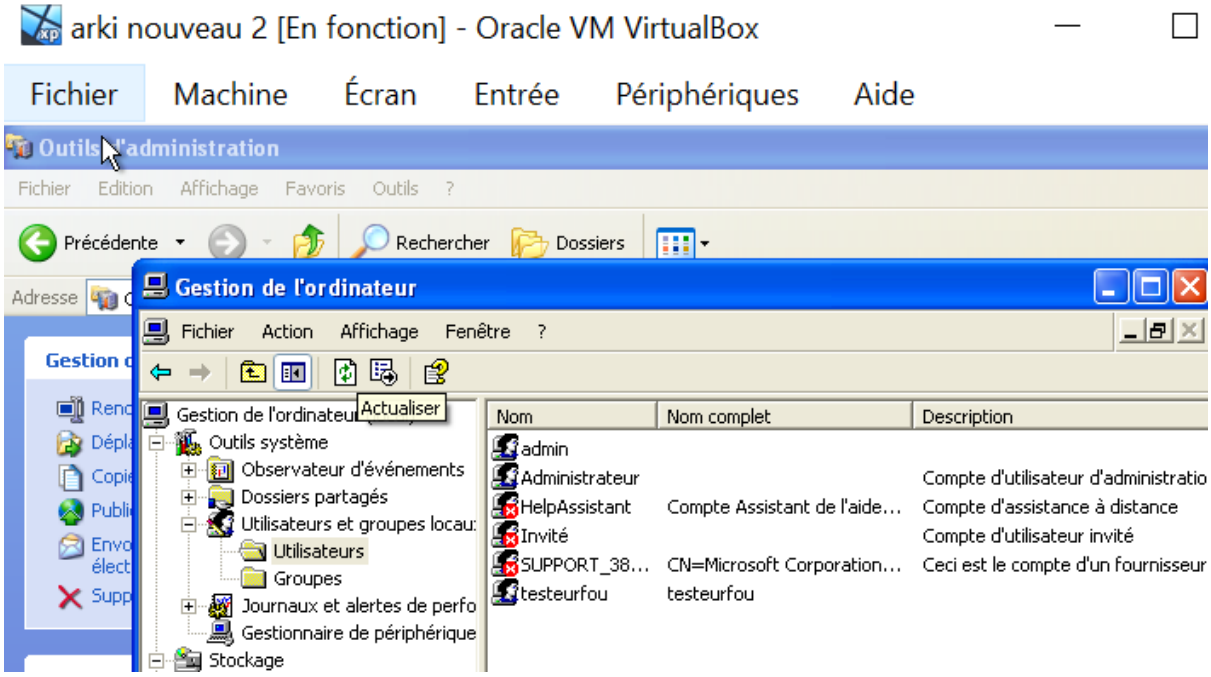
Le partage provient du dossier “jeux express” qui se trouve dans le serveur Windows 2003 (Et maintenant ce dossier est lié entre les 2 serveurs qui sont Windows 2003 et Windows XP). Il y a aussi les fichiers correspondant à :



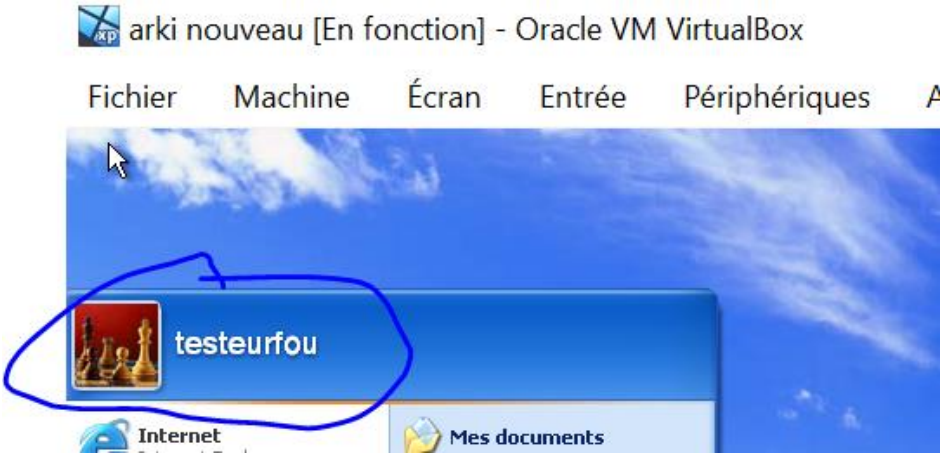


2) Tester un Trojan

On créé un utilisateur testeurfou sur Windows XP :

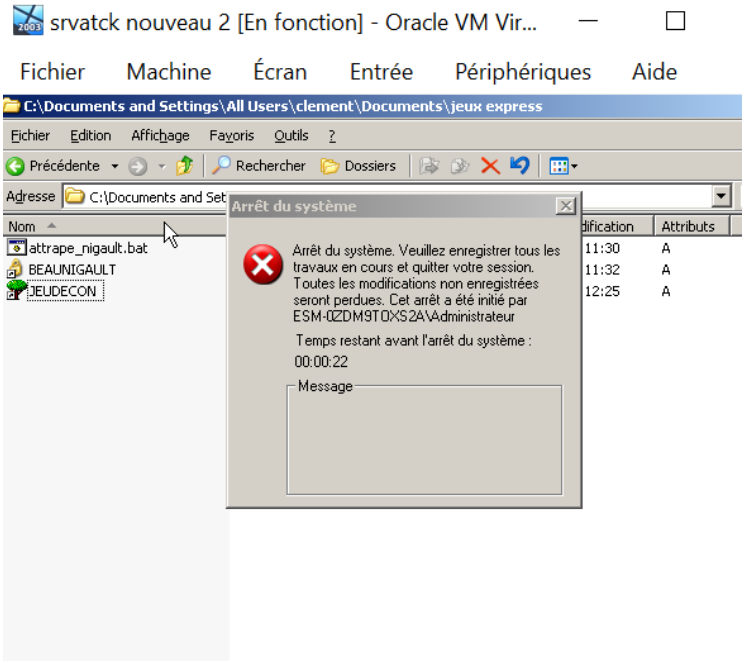


On se connecte dans la session testeurfou dans le serveur Windows XP :



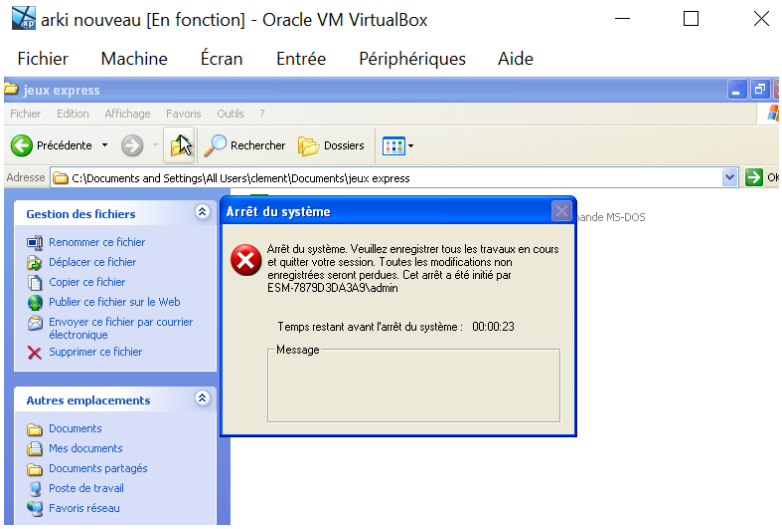
Le partage entre Windows XP (dans la session testeurfou) et le Windows 2003 sont liés (il y a aussi le partage entre Windows 2003 (dans la session Administrateur) et le Windows XP qui sont liés).

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.

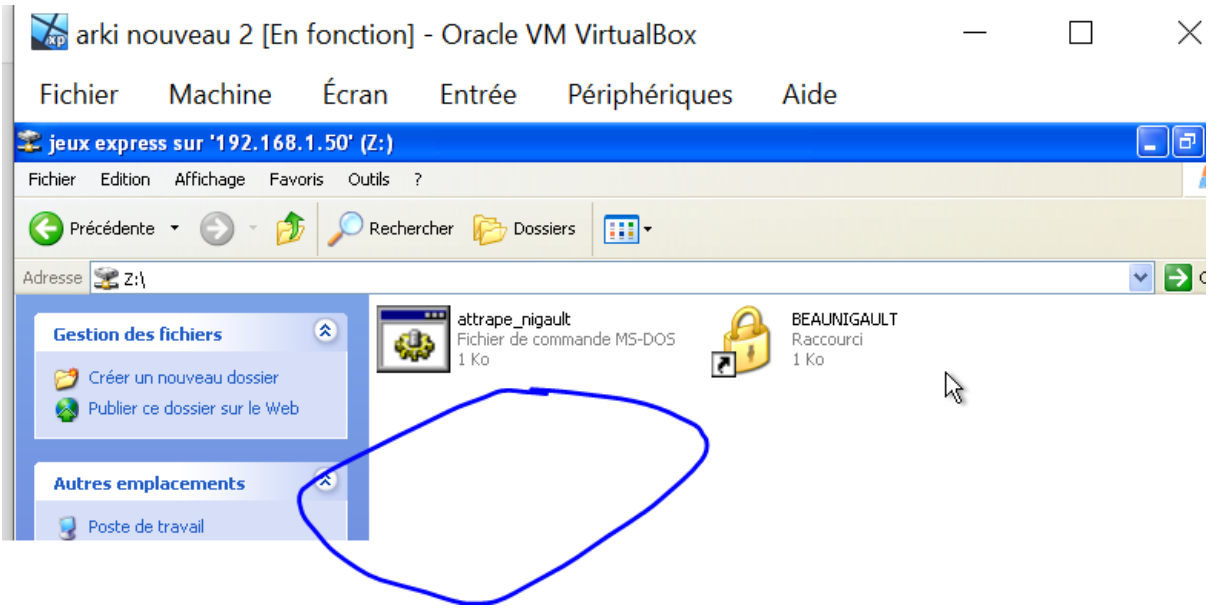
Même le dossier partagé fait planter le système :



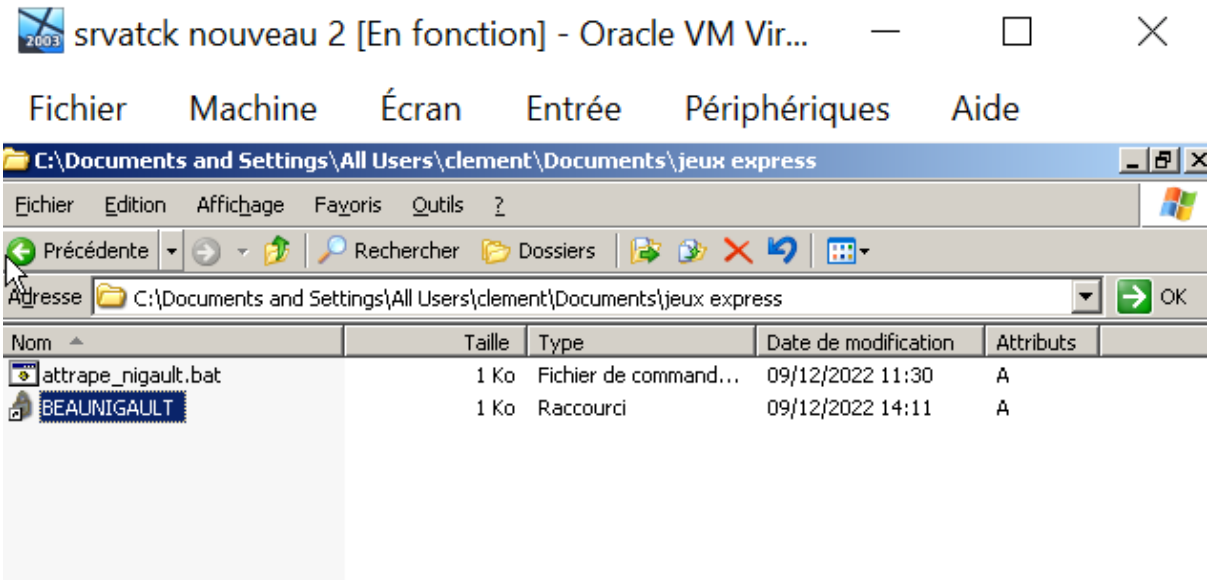
6) L’explication est que quand on clique sur “jeudecon” il se passe qu’on a un message d’arrêt du système sur les 2 machines.

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 :



Pareil sur l'autre machine.



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.