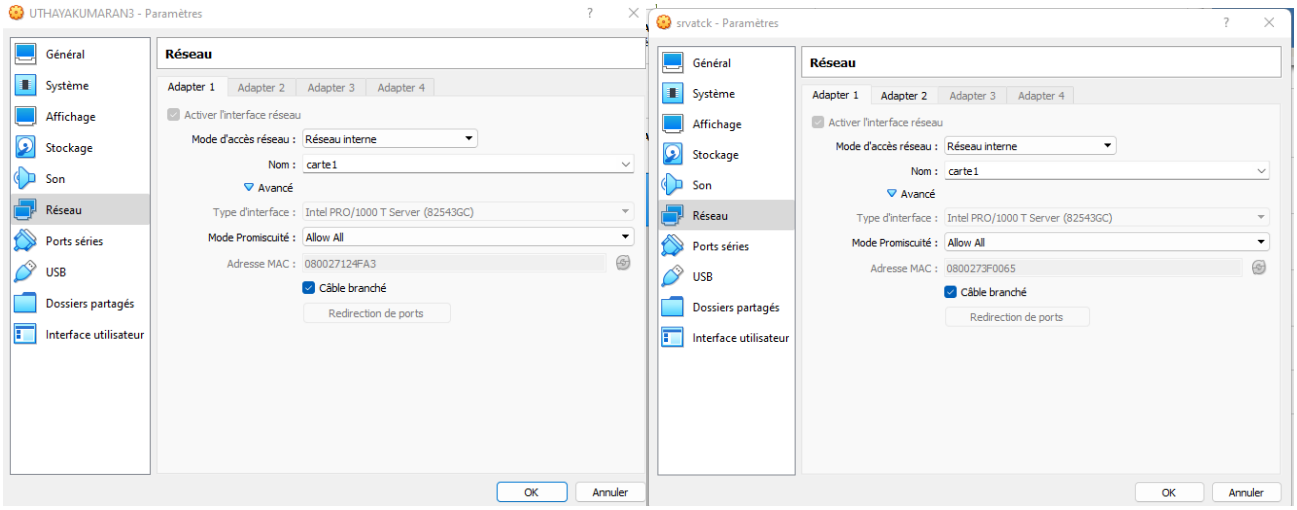
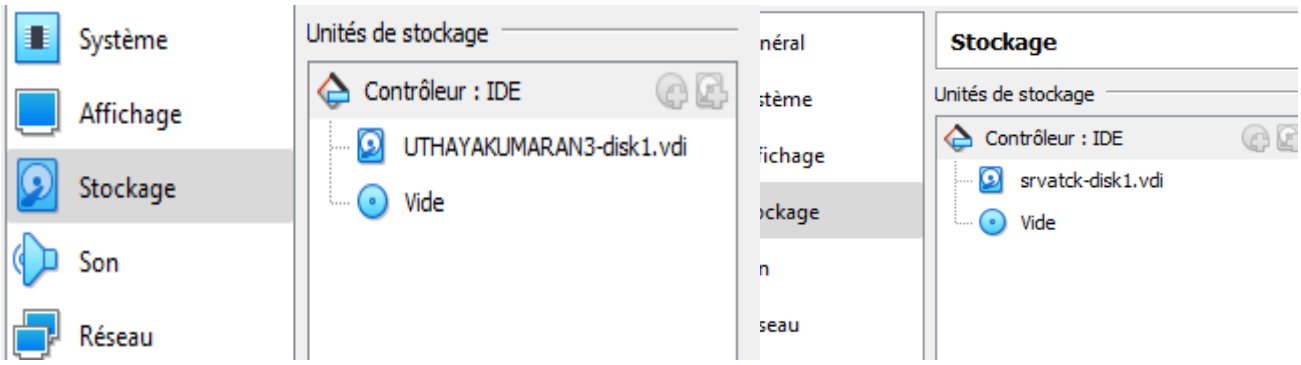
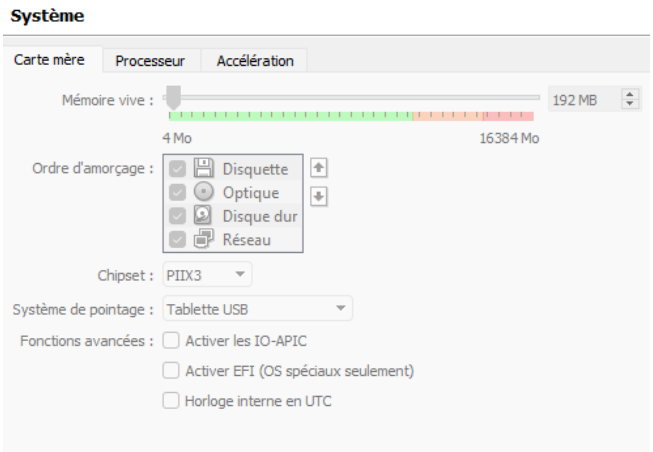
TP : Attaque Défense

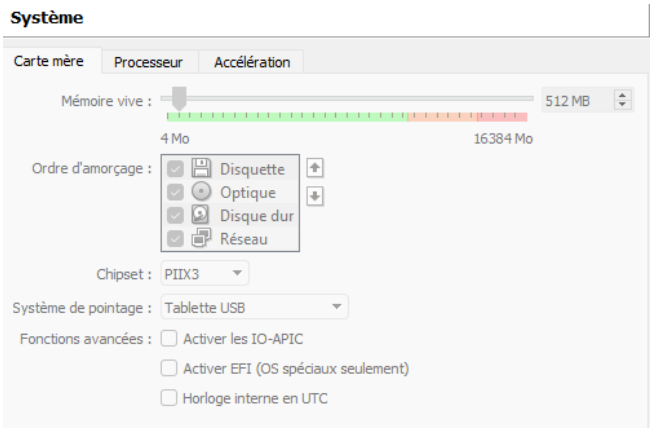
Parametre des machines :

UTHAYAKUMARAN3 / SRVATCK



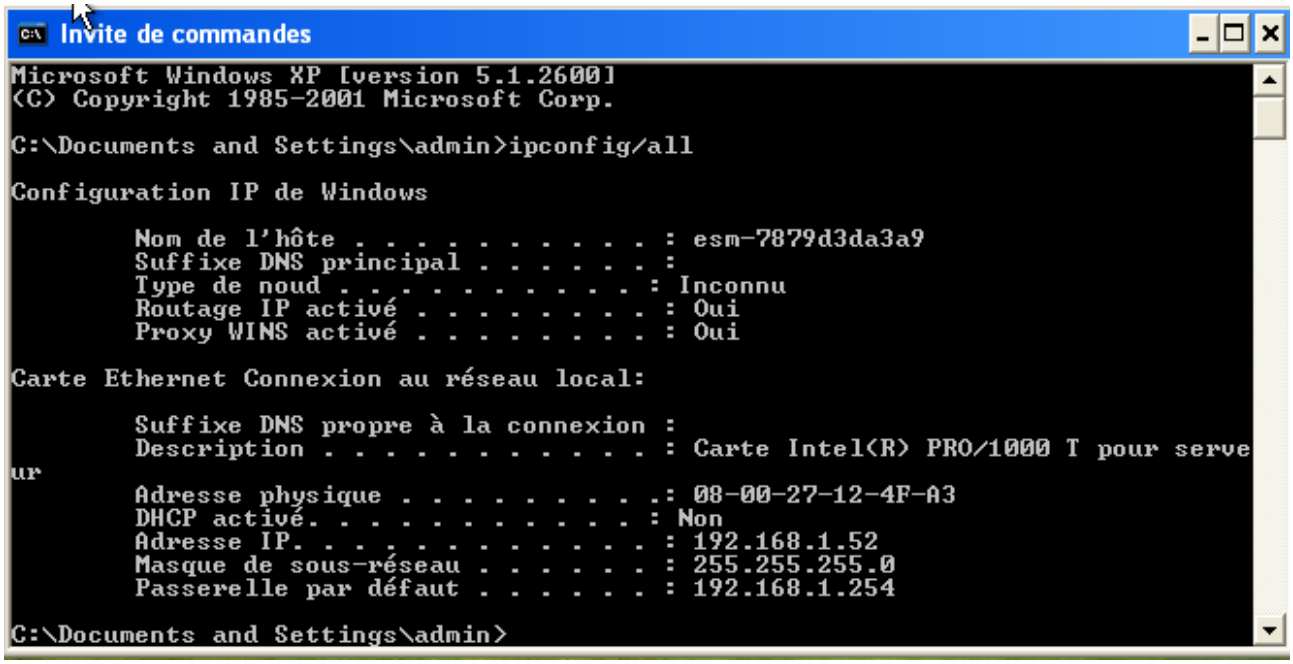


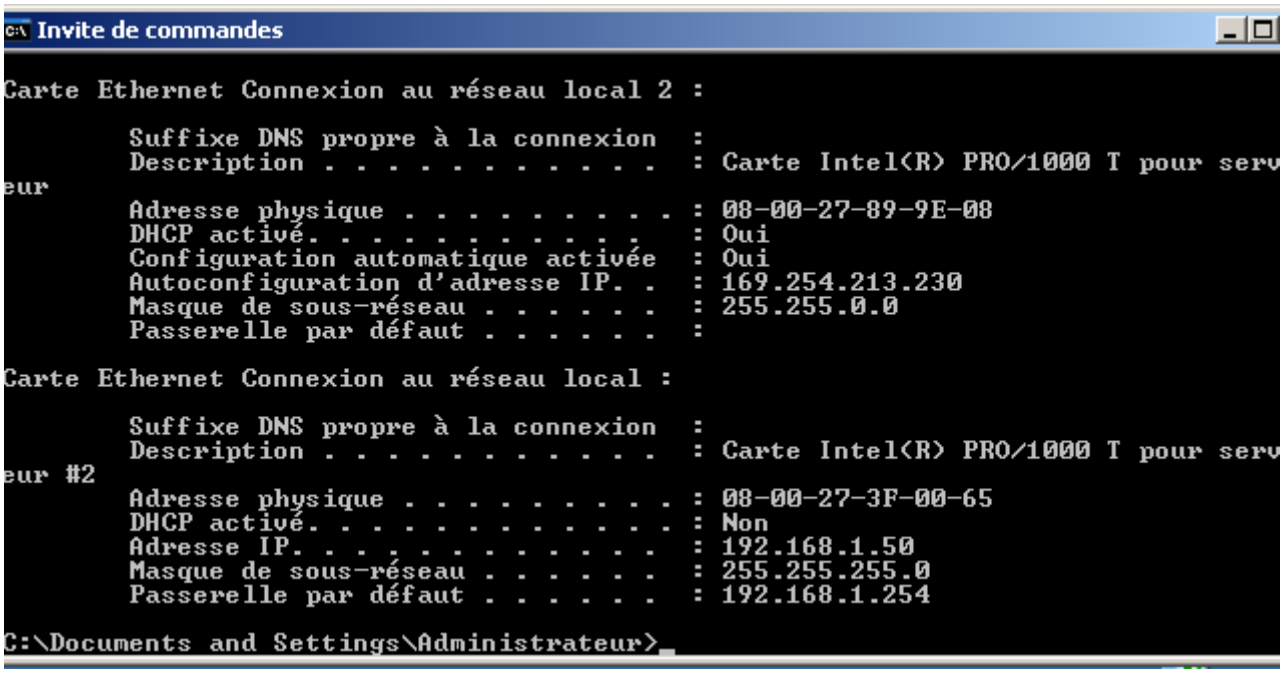


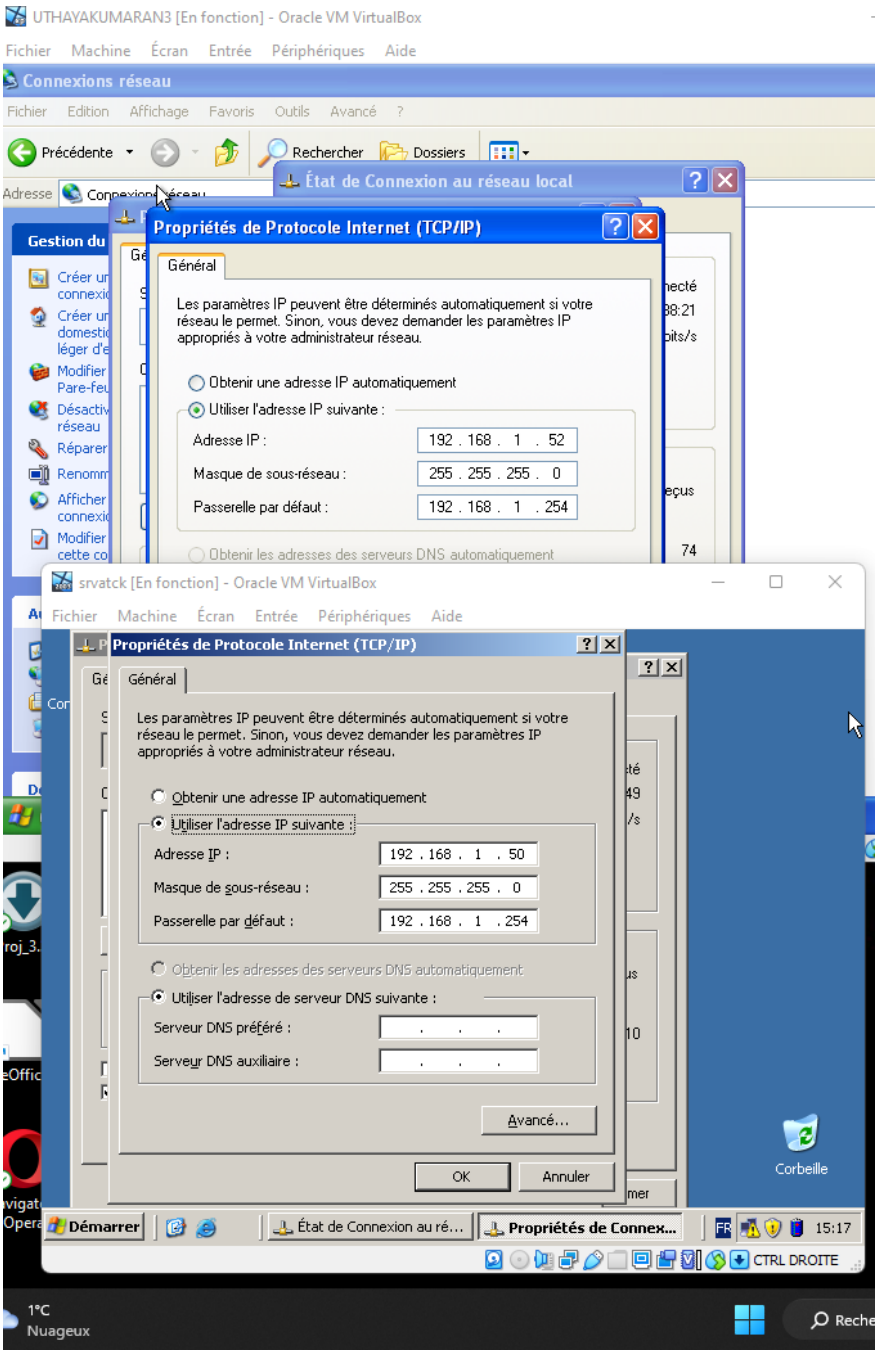


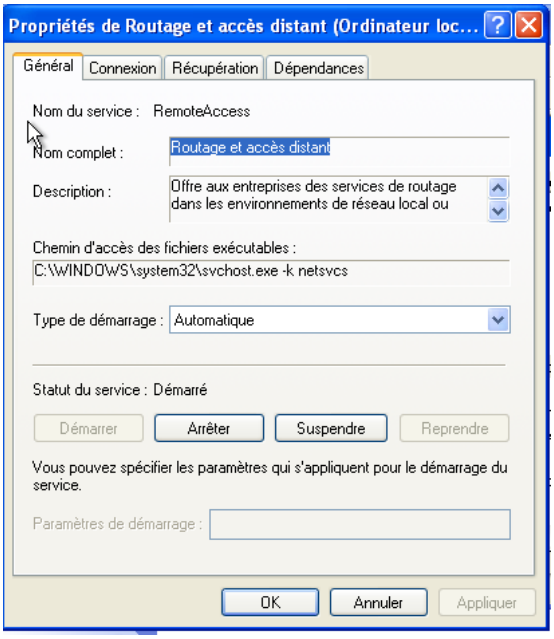
dans cmd :

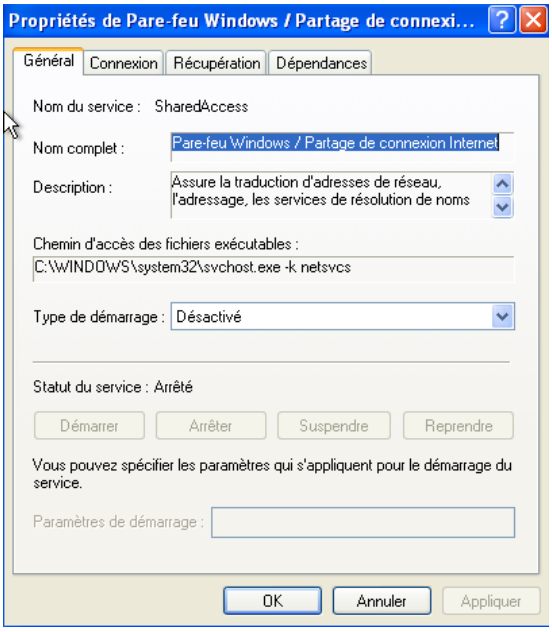
ipconfig/all

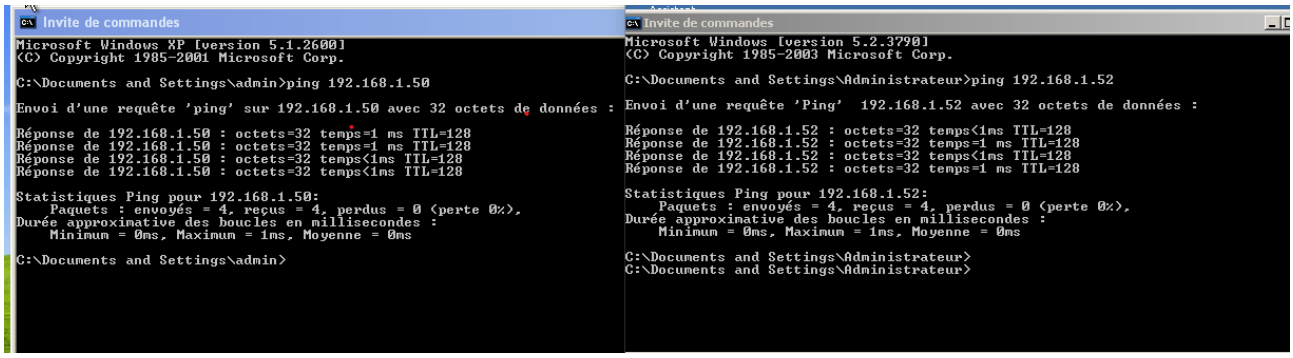

Invite de commandes
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\admin>ipconfig/all
Configuration IP de Windows
Nom de l'hôte . . . . . : esm-7879d3da3a9
Suffixe DNS principal . . . . . :
Type de noud . . . . . : Inconnu
Routage IP activé . . . . . : Oui
Proxy WINS activé . . . . . : Oui
Carte Ethernet Connexion au réseau local:
Suffixe DNS propre à la connexion :
Description . . . . . : Carte Intel(R) PRO/1000 T pour serve
ur
Adresse physique . . . . . : 08-00-27-12-4F-A3
DHCP activé. . . . . : Non
Adresse IP. . . . . : 192.168.1.52
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . : 192.168.1.254
C:\Documents and Settings\admin>


Invite de commandes
Carte Ethernet Connexion au réseau local 2 :
Suffixe DNS propre à la connexion :
Description . . . . . : Carte Intel(R) PRO/1000 T pour serv
eur
Adresse physique . . . . . : 08-00-27-89-9E-08
DHCP activé. . . . . : Oui
Configuration automatique activée : Oui
Autoconfiguration d'adresse IP. . : 169.254.213.230
Masque de sous-réseau . . . . . : 255.255.0.0
Passerelle par défaut . . . . . :
Carte Ethernet Connexion au réseau local :
Suffixe DNS propre à la connexion :
Description . . . . . : Carte Intel(R) PRO/1000 T pour serv
eur #2
Adresse physique . . . . . : 08-00-27-3F-00-65
DHCP activé. . . . . : Non
Adresse IP. . . . . : 192.168.1.50
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . : 192.168.1.254
C:\Documents and Settings\Administrateur>


UTHAYAKUMARAN3 [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Connexions réseau
Fichier Edition Affichage Favoris Outils Avancé ?
Précédente
Rechercher
Dossiers
Adresse
État de Connexion au réseau local
Propriétés de Protocole Internet (TCP/IP)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 1 . 52
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 192 . 168 . 1 . 254
Obtenir les adresses des serveurs DNS automatiquement
srvatck [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Propriétés de Protocole Internet (TCP/IP)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 1 . 50
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 192 . 168 . 1 . 254
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré :
Serveur DNS auxiliaire :
Avancé...
OK
Annuler
Corbeille
Démarrer
État de Connexion au ré...
Propriétés de Connex...
15:17
CTRL DROITE
1°C
Nuageux

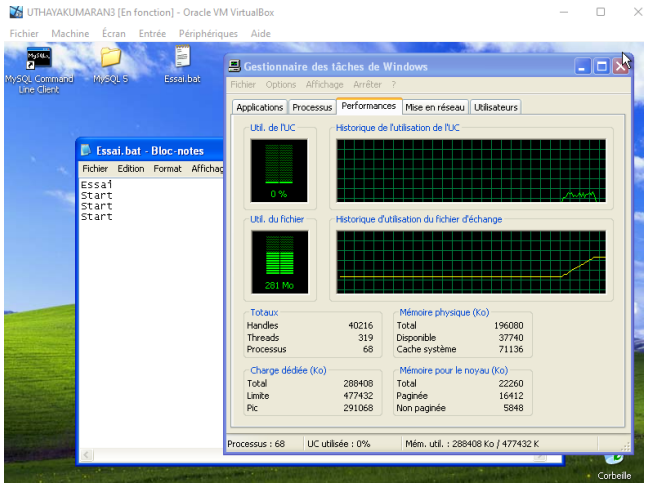


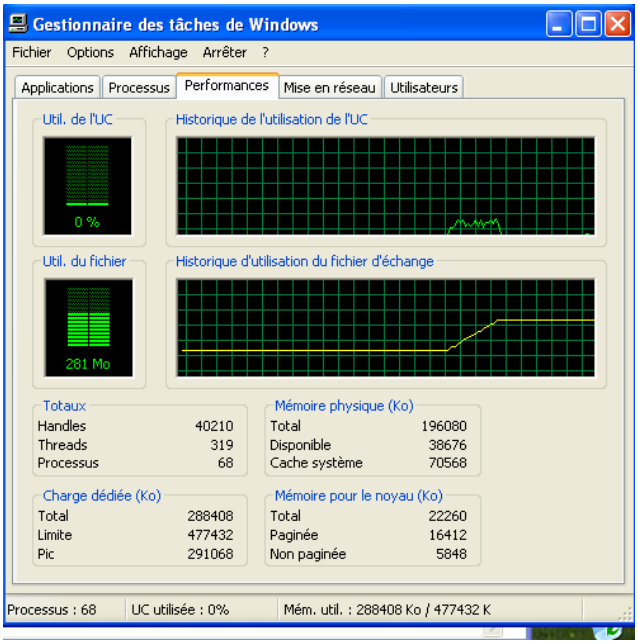




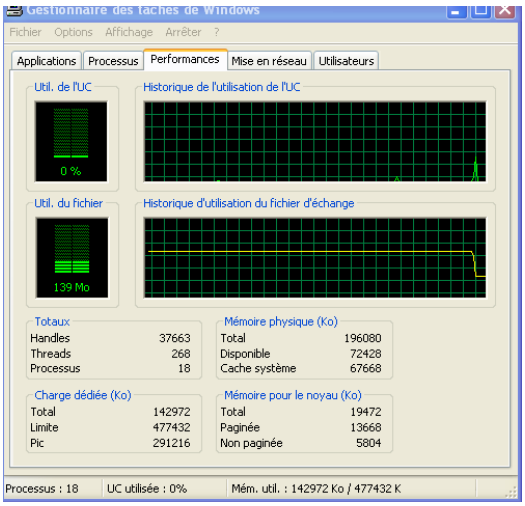
<u>dans le cmd, on a fait :</u> ping 192.168.1.50 ou 192.168.1.52 sur les different machines pour tester la connectivité des 2 machines

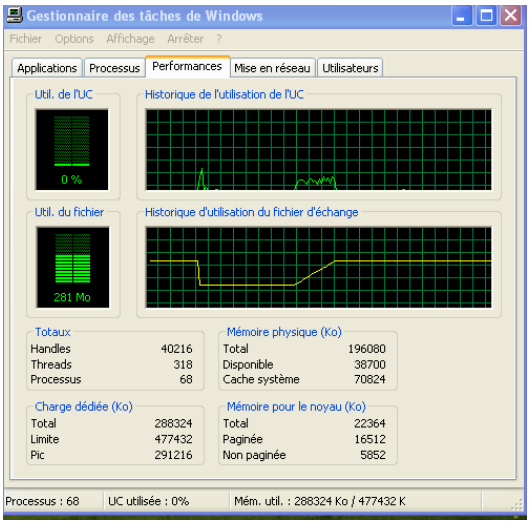
Ctrl + Maj + echap : pour démarrer le gestionnaire des taches





Voici ce que donne la performances dans le gestionnaire de taches après avoir ouvert 50 fois le bloc-note Essai.bat et le bloc note-note pingdos.bat .



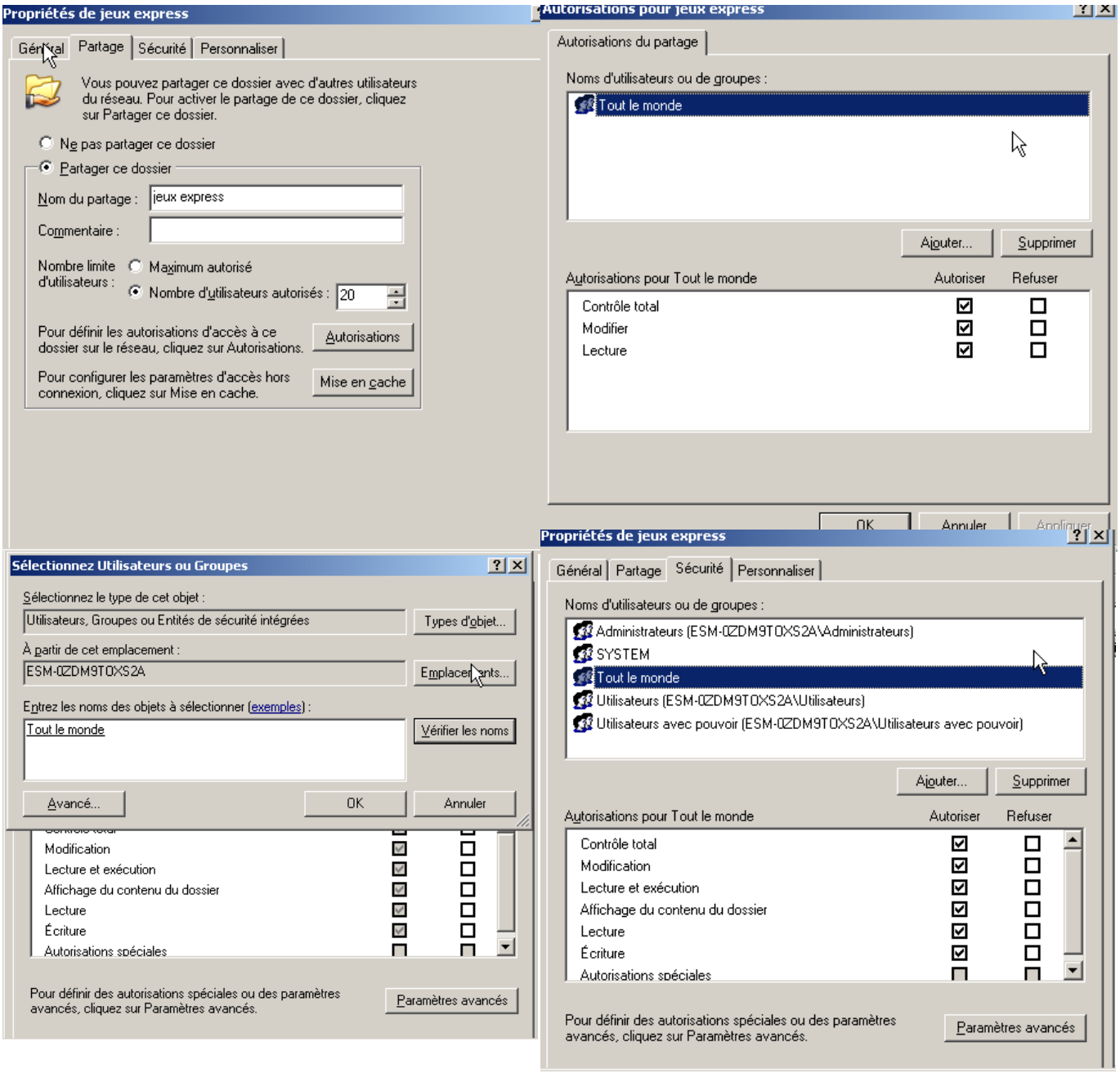


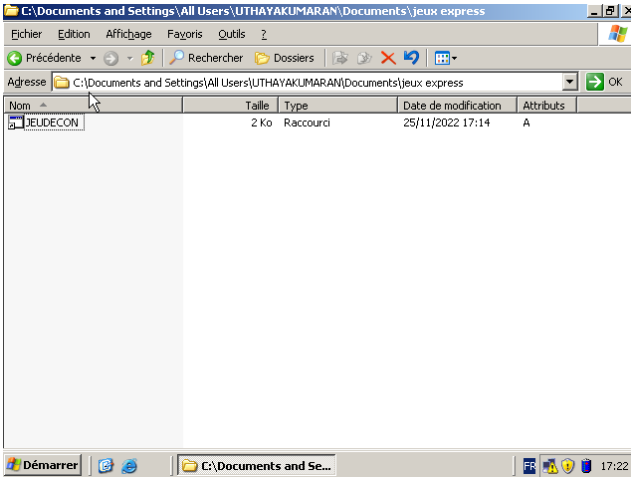
Après avoir fermé les 50 blocs- note.

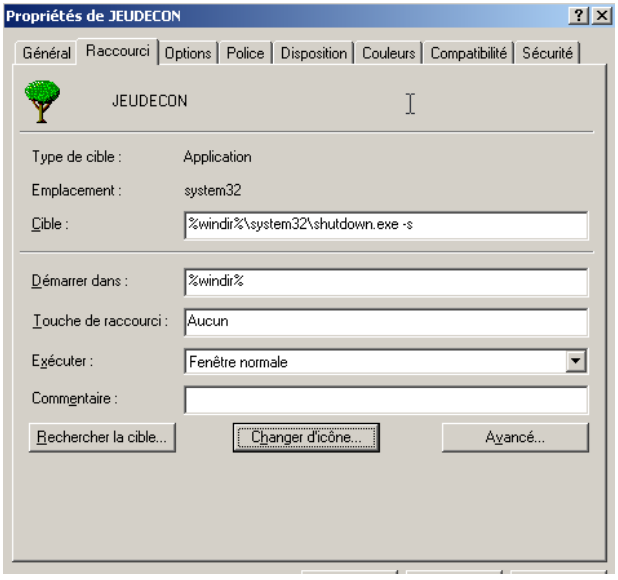
En ouvrant plusieurs fois le même fichier, le processus, la mémoire utilisé, le total de la charges dédié, la disponible de la mémoire physique (Ko) ont tous augmenté en grandes quantité. En fermant simultanément tout les fichiers, tout cela à de nouveau baisser et est revenu à son point de départ.

4.
Les attaques par déni de service non distribuées peuvent être contrées en identifiant l'adresse IP de la machine émettant les attaques et en la bannissant au niveau du pare-feu ou du serveur. Les paquets IP provenant de la machine hostile sont dès lors rejetés sans être traités empêchant que le service du serveur ne soit saturé et ne se retrouve donc hors-ligne.

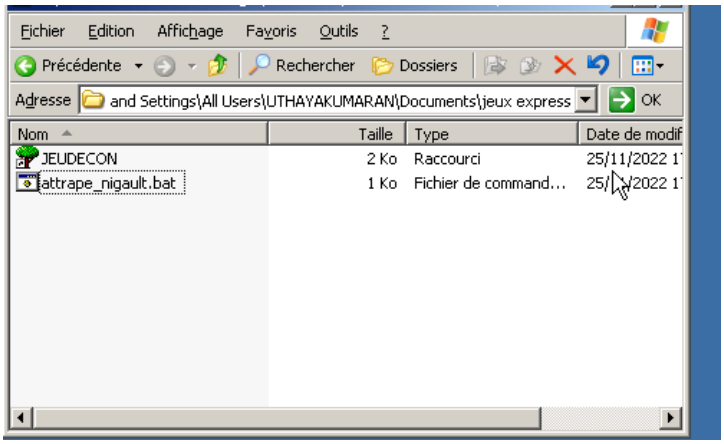
Jeux express


Propriétés de jeux express
Général
Partage
Sécurité
Personnaliser
Vous pouvez partager ce dossier avec d'autres utilisateurs du réseau. Pour activer le partage de ce dossier, cliquez sur Partager ce dossier.
Ne pas partager ce dossier
Partager ce dossier
Nom du partage :
jeux express
Commentaire :
Nombre limite d'utilisateurs :
Maximum autorisé
Nombre d'utilisateurs autorisés :
20
Pour définir les autorisations d'accès à ce dossier sur le réseau, cliquez sur Autorisations.
Autorisations
Pour configurer les paramètres d'accès hors connexion, cliquez sur Mise en cache.
Mise en cache
Autorisations pour jeux express
Autorisations du partage
Noms d'utilisateurs ou de groupes :
Tout le monde
Ajouter...
Supprimer
Autorisations pour Tout le monde
Autoriser
Refuser
Contrôle total
Modifier
Lecture
OK
Annuler
Appliquer
Sélectionnez Utilisateurs ou Groupes
Sélectionnez le type de cet objet :
Utilisateurs, Groupes ou Entités de sécurité intégrées
Types d'objet...
À partir de cet emplacement :
ESM-0ZDM9T0XS2A
Emplacements...
Entrez les noms des objets à sélectionner (exemples) :
Tout le monde
Vérifier les noms
Avancé...
OK
Annuler
Modification
Lecture et exécution
Affichage du contenu du dossier
Lecture
Écriture
Autorisations spéciales
Pour définir des autorisations spéciales ou des paramètres avancés, cliquez sur Paramètres avancés.
Paramètres avancés
Propriétés de jeux express
Général
Partage
Sécurité
Personnaliser
Noms d'utilisateurs ou de groupes :
Administrateurs (ESM-0ZDM9T0XS2A\Administrateurs)
SYSTEM
Tout le monde
Utilisateurs (ESM-0ZDM9T0XS2A\Utilisateurs)
Utilisateurs avec pouvoir (ESM-0ZDM9T0XS2A\Utilisateurs avec pouvoir)
Ajouter...
Supprimer
Autorisations pour Tout le monde
Autoriser
Refuser
Contrôle total
Modification
Lecture et exécution
Affichage du contenu du dossier
Lecture
Écriture
Autorisations spéciales
Pour définir des autorisations spéciales ou des paramètres avancés, cliquez sur Paramètres avancés.
Paramètres avancés

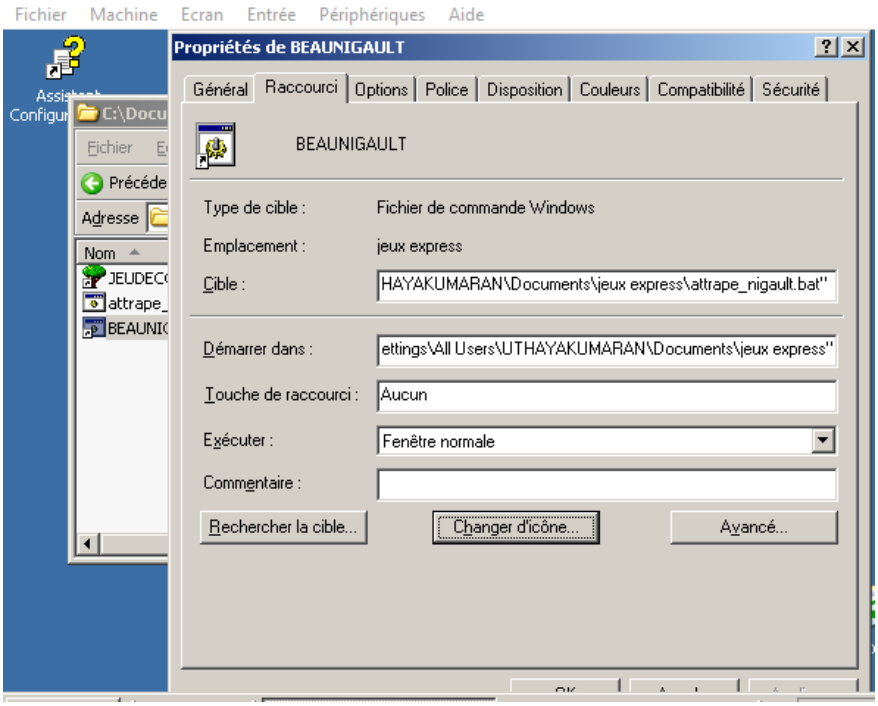




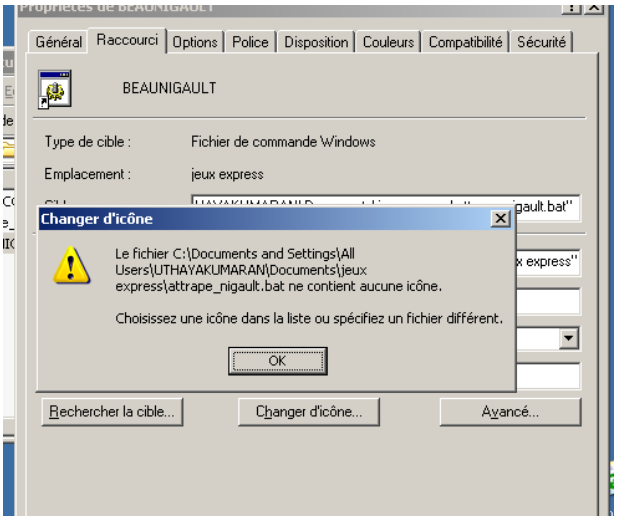
Ou retrouver le fichier attrape_nigault.bat :

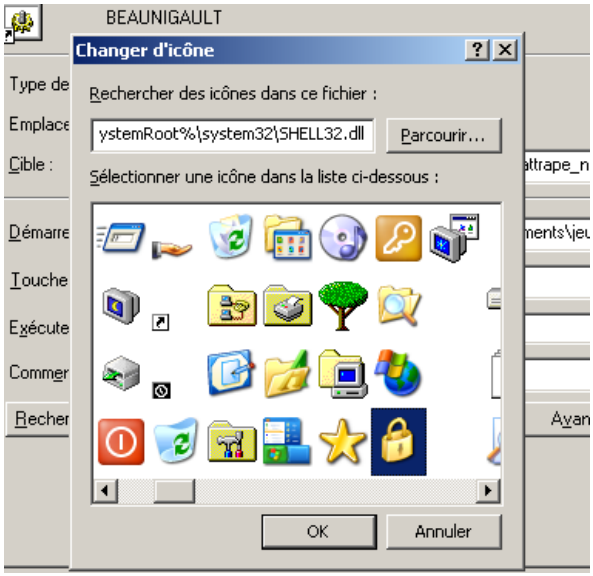


Dans propriétés de BEAUNIGAULT, faire :

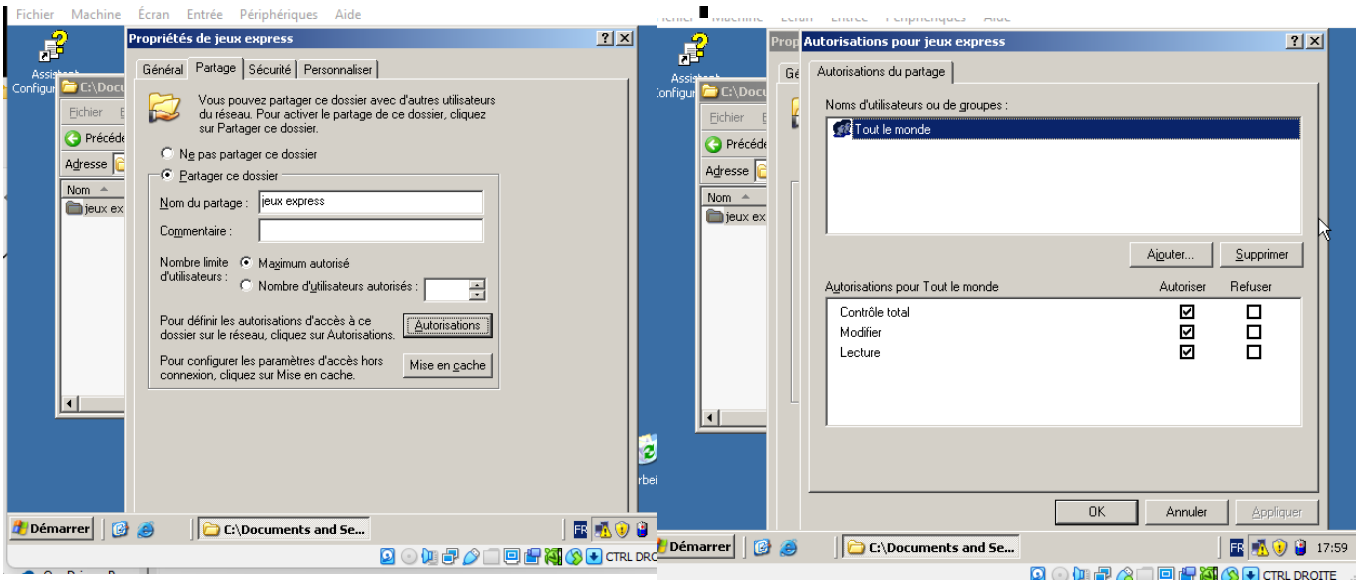


Changer d’icone, puis cliquez ok, et choisir l’icone du cadenas et ne pas oublier de cliquer sur «appliquer» et puis «ok» pour valider l’icone :

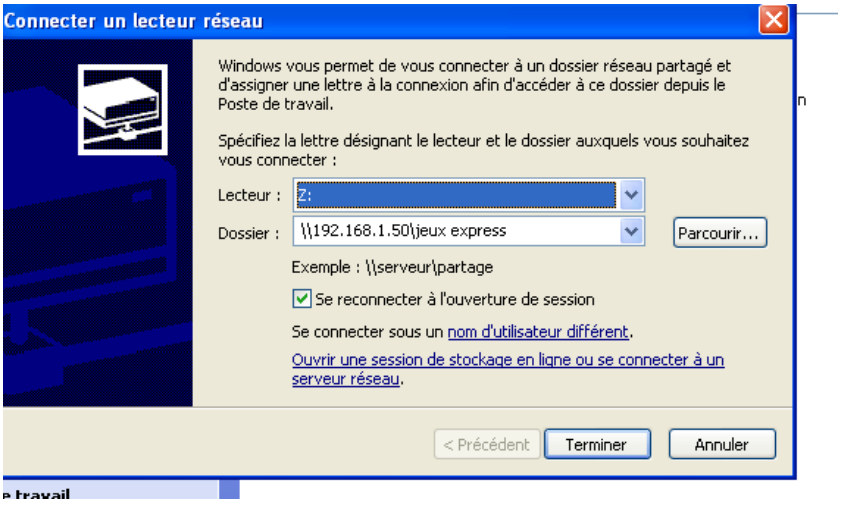




Pour faire la partage du fichier jeux express :

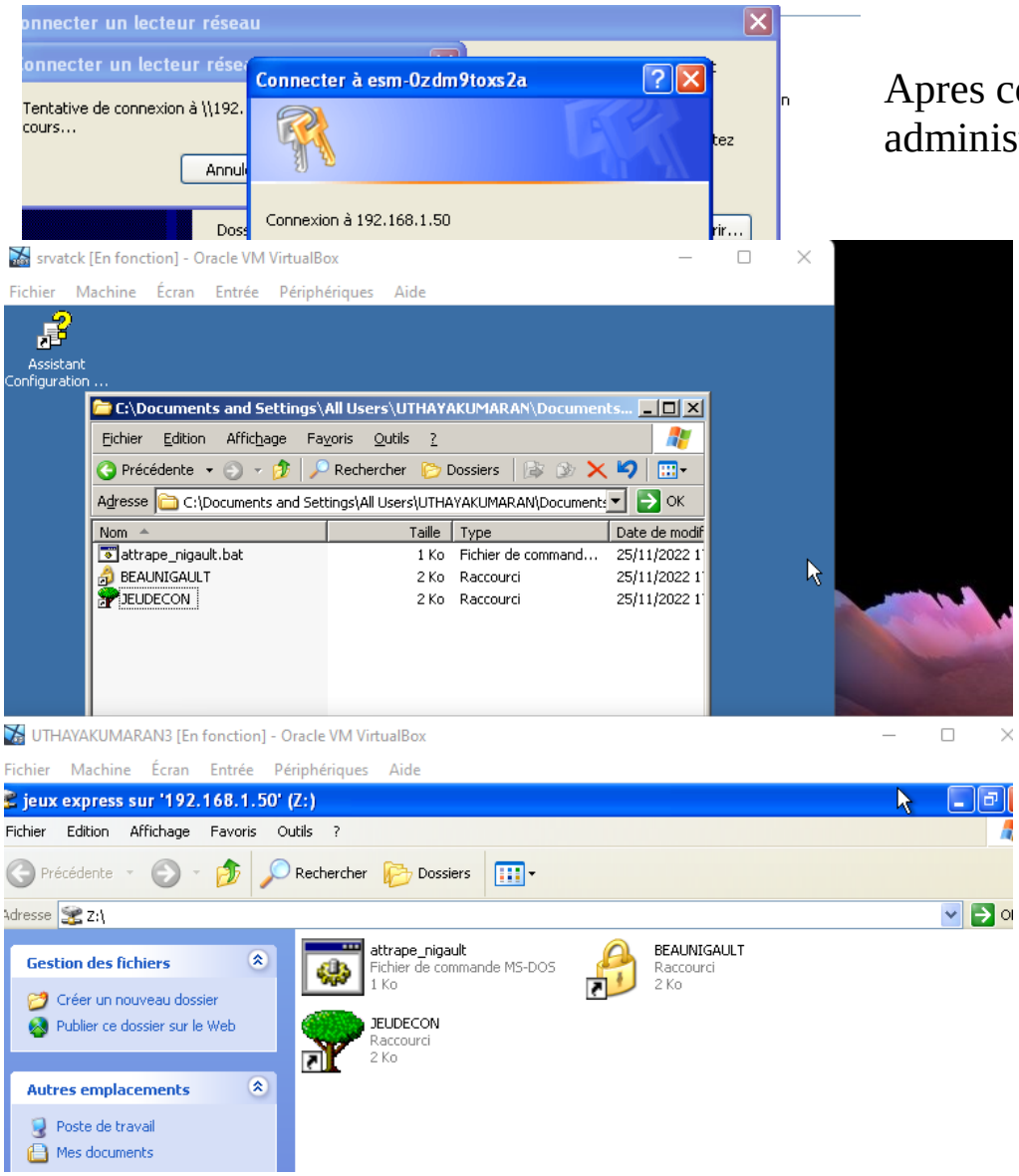


Connecter un lecteur réseau…



Nom d’utilisateur :
Administrateur

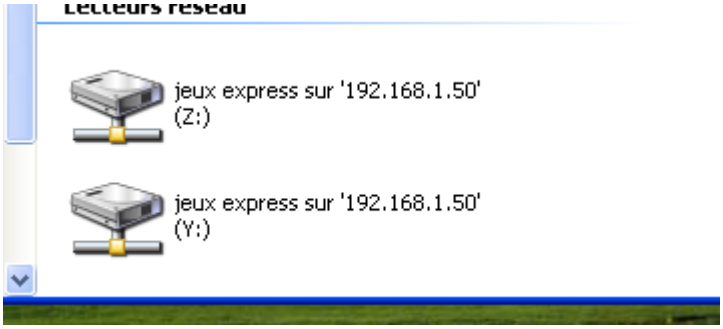
Mot de passe :
Routeur0*



Apres connexion administrateur :

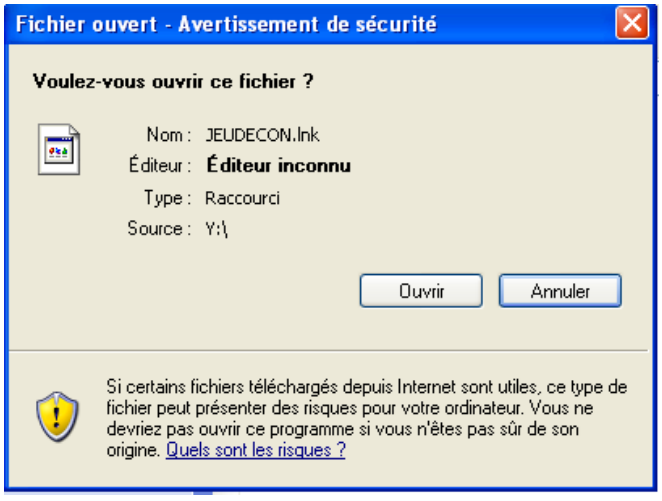
Jeux express est maintenant connecté sur les 2 machines virtuelles.

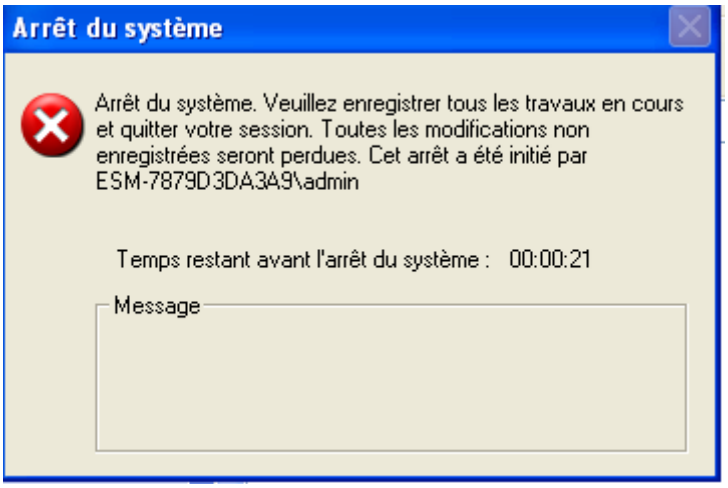
Tester un Trojan :



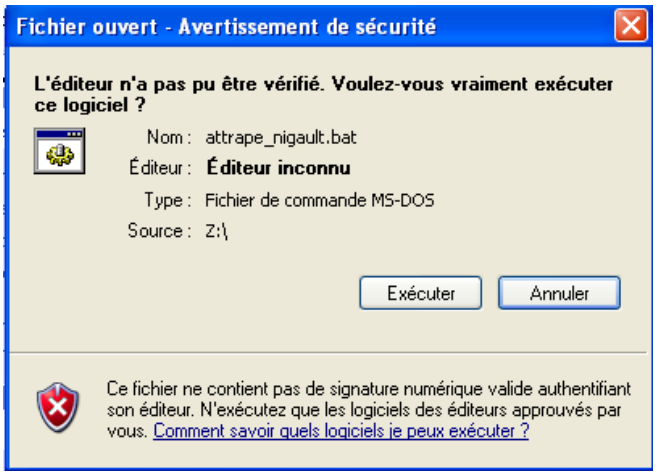
Voici la création d'un lecteur reseau dans le poste de travail.

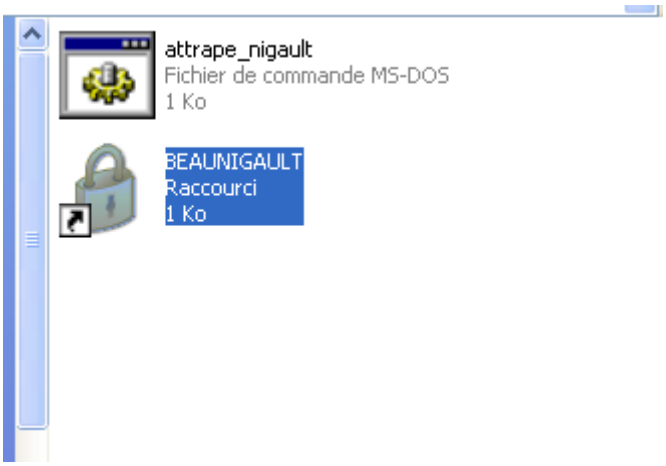
En cliquant sur JEUDECON :





En cliquant sur BEAUNIGAULT :



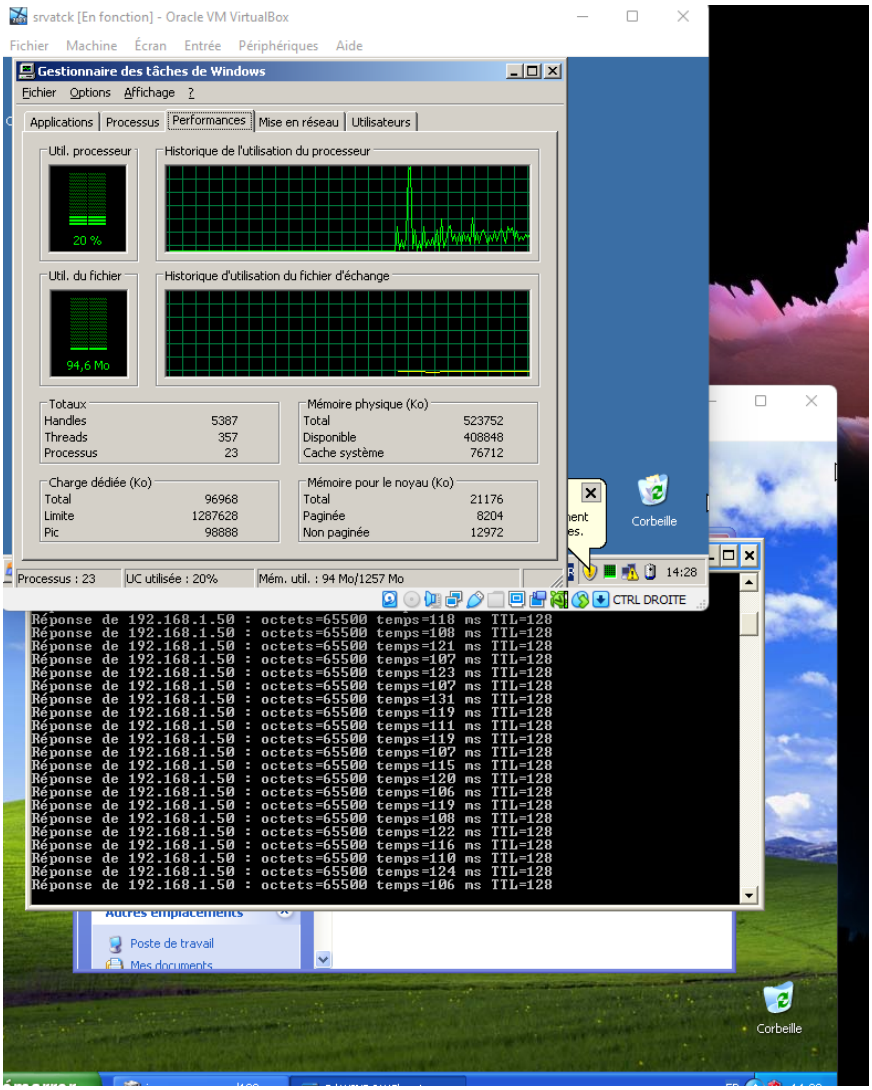


Apres avoir lancer JEUDECON, un minuteur c'est lancé, affichant le temps restant avant que la machine ne s'eteigne.

Apres avoir lancer BEAUNIGAULT, le fichier JEUDECON a été effacer.

JEUDECON est un code attaque qui éteint la machine après l'avoir lancé, tandis que BEAUNIGAULT est un code défense qui supprime la menace d'attaque.

Ceci est un test trojan :


srvatck [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Gestionnaire des tâches de Windows
Fichier Options Affichage ?
Applications Processus Performances Mise en réseau Utilisateurs
Util. processeur
20 %
Historique de l'utilisation du processeur
Util. du fichier
94,6 Mo
Historique d'utilisation du fichier d'échange
Totaux
Handles 5387
Threads 357
Processus 23
Mémoire physique (Ko)
Total 523752
Disponible 408848
Cache système 76712
Charge dédiée (Ko)
Total 96968
Limite 1287628
Pic 98888
Mémoire pour le noyau (Ko)
Total 21176
Paginée 8204
Non paginée 12972
Processus : 23
UC utilisée : 20%
Mém. util. : 94 Mo/1257 Mo
Corbeille
14:28
CTRL DROITE
Réponse de 192.168.1.50 : octets=65500 temps=118 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=108 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=121 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=107 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=123 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=107 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=131 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=119 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=111 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=119 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=107 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=115 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=120 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=106 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=119 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=108 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=122 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=116 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=110 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=124 ms TTL=128
Réponse de 192.168.1.50 : octets=65500 temps=106 ms TTL=128
Autres emplacements
Poste de travail
Mes documents
Corbeille