**TP INSTALLATION D’UN RAID LOGICIEL**

**MISE EN PLACE DE SAUVEGARDE DE DONNEES**

|  |  |
| --- | --- |
| Compétences |  |
| **Objectifs** | **Réaliser une attaque DDOS et un TROJAN pour mieux comprendre les parades à mettre en place** |
| Vocabulaire à connaitre | **Malveillance, Ingénierie sociale,** Le piratage psychologique, L’usurpation d’identité ou hameçonnage, Le vol d’information, **Codes malveillants,** Les virus, Les vers, La bombe logique**, Programmes furtifs, Le cheval de Troie, Logiciel espion, Cookies traceurs, Logiciel de publicité, pop up, Les bots, Spam, Attaque en force, Déni de service** |
| Evaluation | DST  E6 |

**Sommaire**

[**Contexte** 1](#_Toc494986153)

[**Installation Windows Server 2003** 1](#_Toc494986154)

[**Mise en place DE VOTRE RÉSEAU** 1](#_Toc494986155)

[**PARAMETRAGE DE VOTRE RÉSEAU** 2](#_Toc494986156)

[**A faire sur chacune des deux machines serveur** 4](#_Toc494986157)

[**Surcharger un serveur** 5](#_Toc494986158)

[**Jeux express** 5](#_Toc494986159)

[**Mise en place** 5](#_Toc494986160)

[**Tester un trojan** 6](#_Toc494986161)

**Contexte**

Vous travaillez pour la société TUEMOUCHE qui veut tester certaines attaques afin de mieux protéger son système d’information.

**Installation Windows Server 2003**

**Mise en place DE VOTRE RÉSEAU**

Via votre plateforme virtuelle, créer

* un premier Serveur Windows 2003 et nommez le « srvatck »
* un client xp et nommez le votre\_nom\_de\_famille
* Vous devez avoir, pour les écrans spécifiques, les configurations suivantes, pour chacune de vos machines :

Dans virtualbox pour les deux machines :

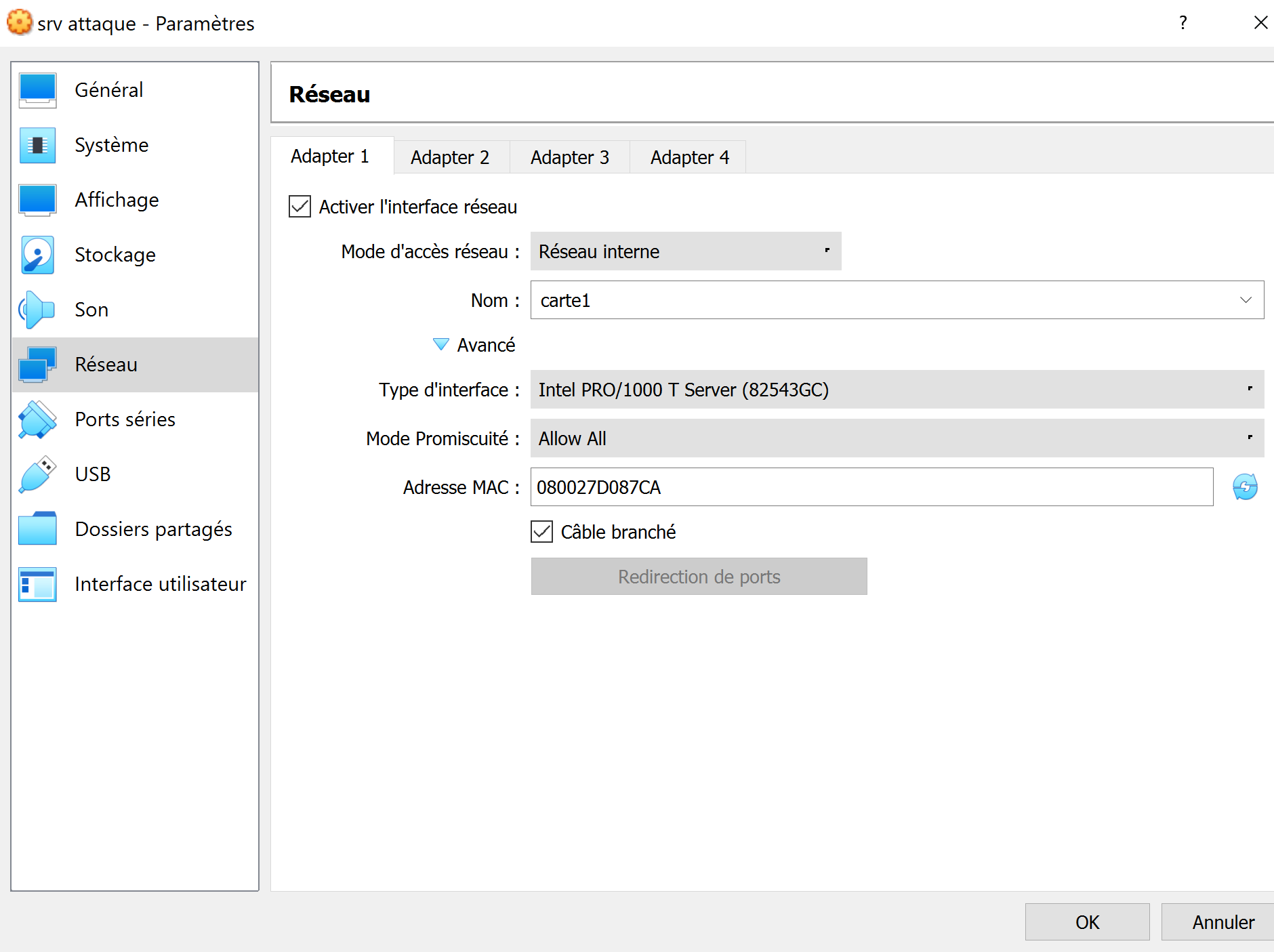
Cliquer sur configuration, puis réseau

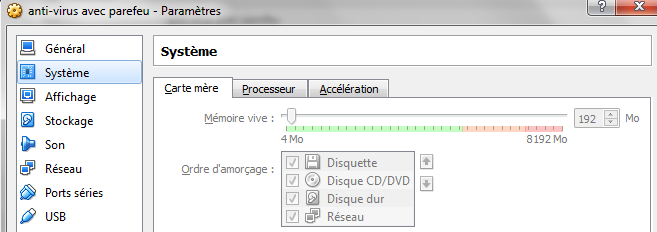
Dans Adapter 1 : Mode d’accès réseau choisir Réseau interne

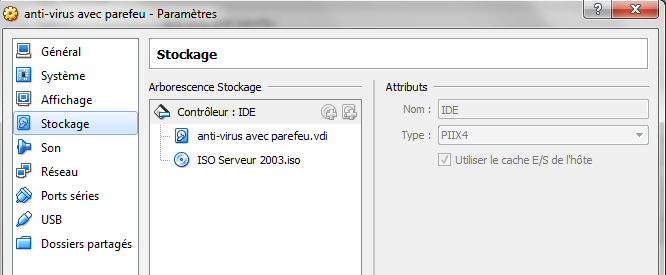
Nom : carte 1

Mode de promiscuité : Allow all

Changer l’adresse mac

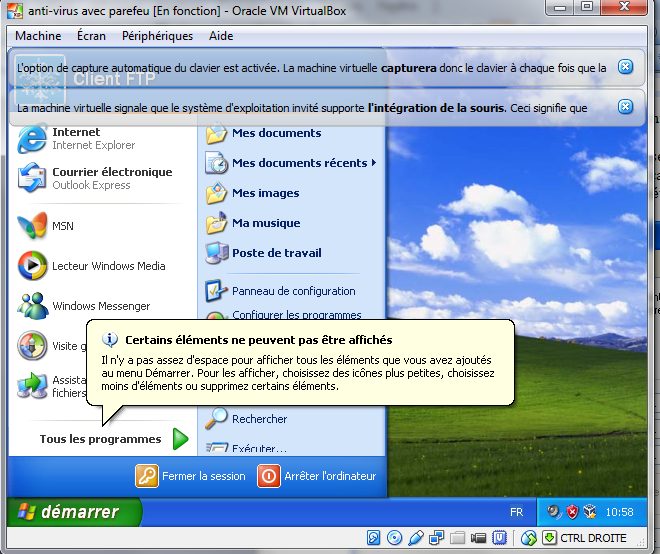


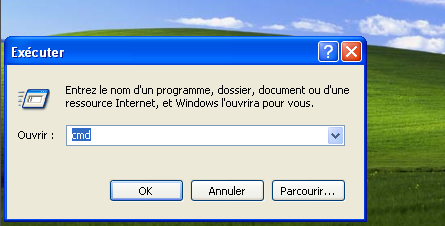




**PARAMETRAGE DE VOTRE RÉSEAU**

Aller dans Démarrer / Exécuter



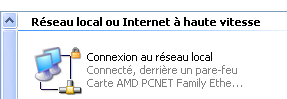


Vérifiez votre paramétrage réseau par le commande **ipconfig /all** en console.

Si vous devez changer votre paramétrage réseau, aller dans :

Panneau de configuration, Connexion réseau

Votre carte réseau apparaît

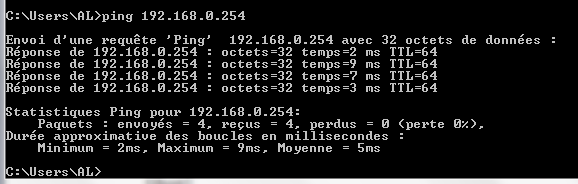


Cliquer dessus, Propriétés, choisissez votre carte réseau puis Propriétés puis Protocole TCP/IP et Propriétés. Effectuez votre paramétrage puis ok, fermer tout.

Revérifiez votre paramétrage réseau par le commande **ipconfig /all** en console.

**A faire sur chacune des machines**

* Démarrer / panneau de configuration / connexion réseau / réseau local / cliquer sur la carte réseau / cliquer sur le protocole TCP/IP / propriétés / fixer l’adressage des cartes comme suit :
* srvatack @ip 192.168.1.50 masque de sous-réseau 255.255.255.0 @passerelle 192.168.1.254
* votre\_nom\_de\_famille @ip 192.168.1.52 masque de sous-réseau 255.255.255.0 @passerelle 192.168.1.254
* Aller dans Démarrer / panneau de configuration / Performance et maintenance/ outils d’administration / services / Routage et accès distant / double clic sur le service / Automatique / appliquer / Démarrer / ok
* Aller dans Démarrer / panneau de configuration / outils d’administration / services / parefeu windows / double clic sur le service / Désactiver / appliquer / Arrêter / ok
* Tester la connectivité entre srvatck et votre\_nom\_de\_famille. Aller dans Démarrer / CMD / entrer / taper la commande ping 192.168.1.52 sur srvatack et taper ping 192.168.1.50 sur votre\_nom\_de\_famille
* Le système doit vous répondre sous cette forme



**Validation**

1. **Prouver la bonne marche de votre connectivité sur toutes les machines**

**Mettre votre résultat dans un document pour synthèse**

**Surcharger un serveur pour avoir un déni de service**

Démarrer le gestionnaire de tâches du serveur srvatack et observer l’onglet mise en réseau.

Démarrer votre poste client Votre\_nom\_de\_famille. Aller dans bloc note et et écrire :

Essai

Start

Start

Start

Enregistrer ce fichier en Essai.bat.

Aller sur le gestionnaire de tâches de votre serveur, outils d’administration, cliquer sur performance.

Lancer l’exécutable que vous avez nommé essai.bat.

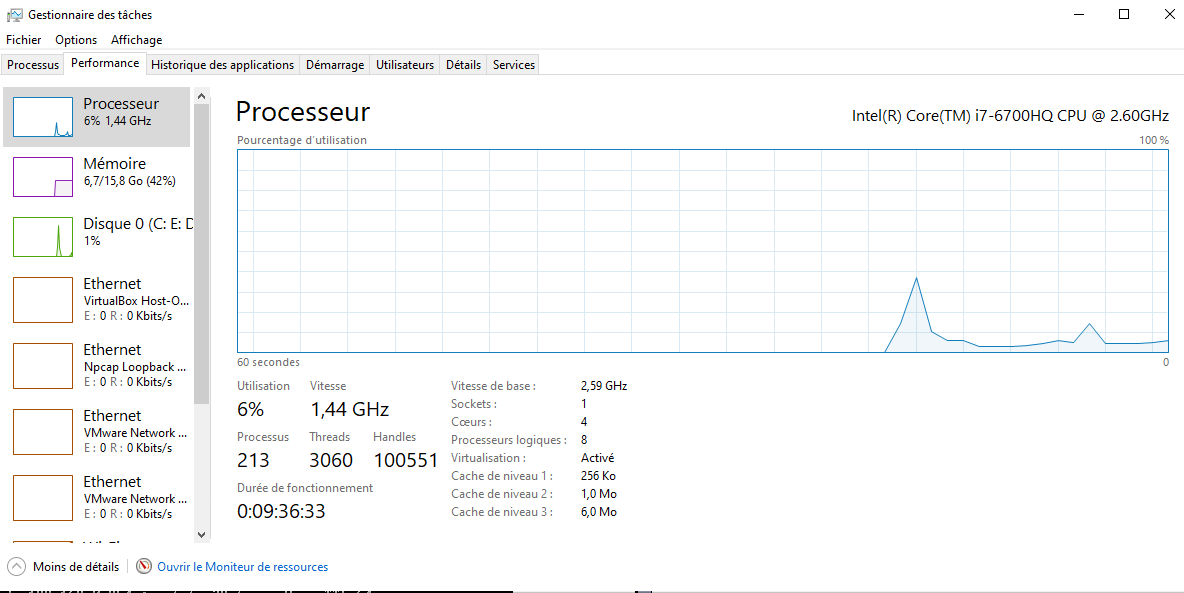
Lorsque le fichier a été lancé une bonne cinquantaine de fois sur le poste client , arrêtez le.

Sur l’onglet Performance, observez l’évolution.

Refaire la même procédure avec le programme pingdos.bat contenant :

ping 192.168.1.50 /w 1 /t /l 65500

ou ping 192.168.1.50 –n 150



Que constatez-vous ? Expliquer.

**Validation**

1. **Prouver le constat**
2. **Donner l’explication**
3. **Chercher sur Internet comment parer ce type d’attaque**

**Mettre votre résultat dans un document pour synthèse**

**Jeux express**

**Mise en place**

Démarrer votre serveur , connectez-vous en tant qu’administrateur.

Dans démarrer / outils d’administration / gestion de l’ordinateur / utilisateurs et groupes locaux / utilisateurs / invité / propriétés / .Ou dans démarrer / poste de travail / clique droit / gérer.

Cliquer sur utilisateurs et groupes locaux / utilisateurs / créer un nouvel invité avec un clic droit dans le champs de droite en blanc / nouvel utilisateur

Dans nom d’utilisateur et nom complet taper **testeurfou.**

**Décocher l’utilisateur doit changer son mot de passe à la première connexion**

**Cocher l’utilisateur ne peut pas changer de mot de passe**

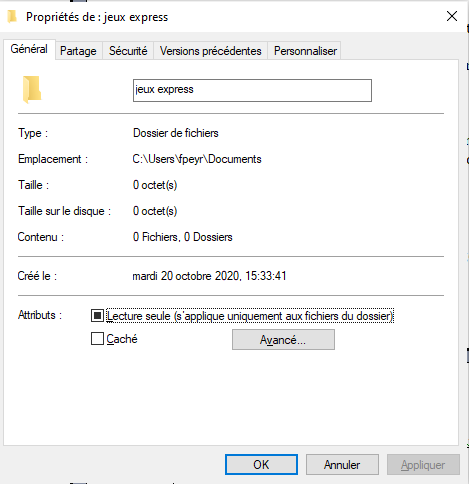
Créer / Fermer

Toujours sur le serveur, en tant qu’administrateur,

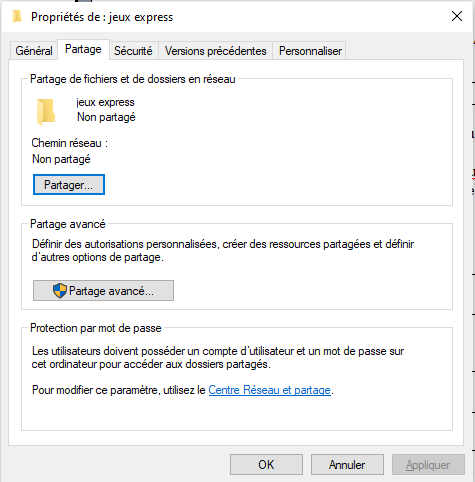
Aller dans c:/Documents and settings /All Users/votre\_nom/Documents

Créer le dossier jeux express

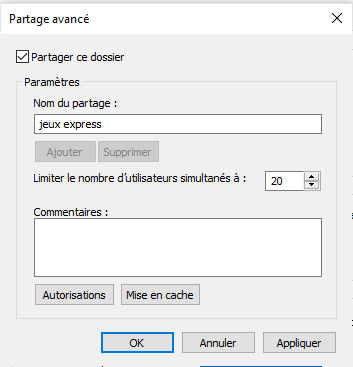
Faire clic droit / propriété sur jeux express



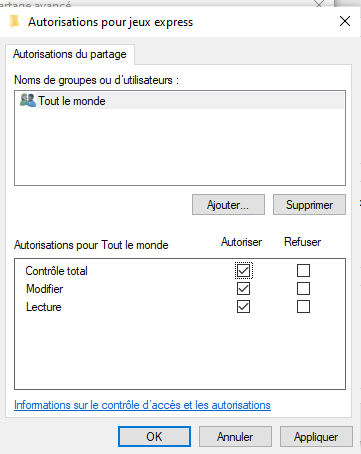
Cliquer sur l’onglet Partage



Cliquer sur Partage Avancé



Cocher Partager ce dossier puis cliquer sur Autorisations

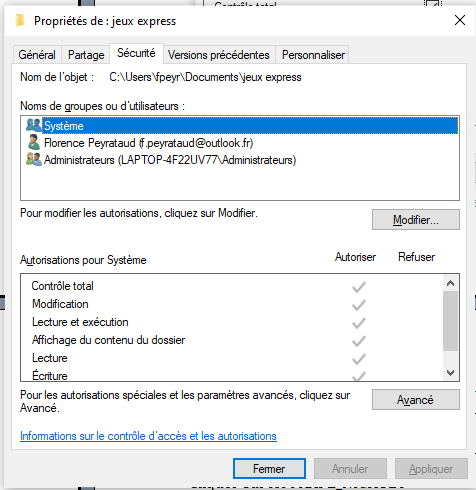


Cocher Contrôle total pour tout le monde

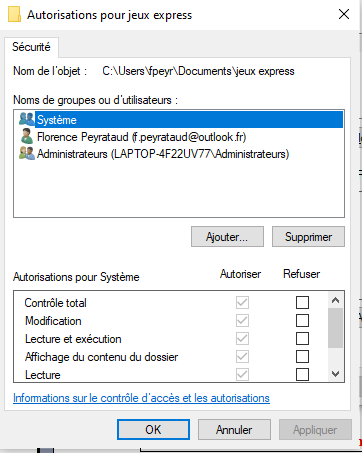
Faire Appliquer / ok

Faire Appliquer sur Partager ce dossier

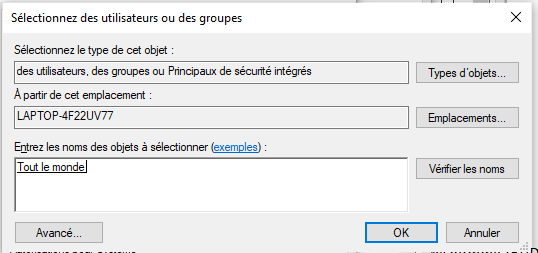
Cliquer sur l’onglet Sécurité



Cliquer sur Modifier



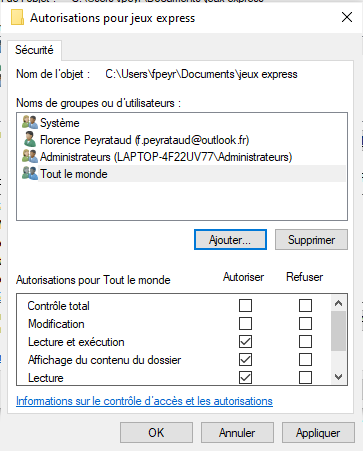
Cliquer sur Ajouter



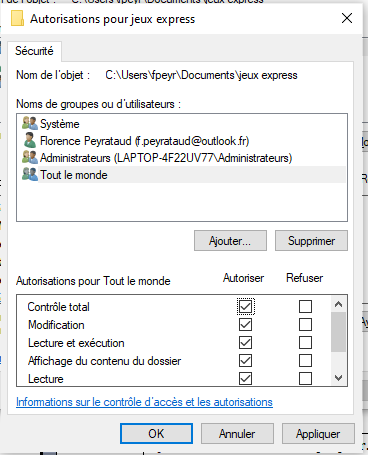
Dans le cadre blanc entrer : Tout (avec une majuscule) puis Vérifier les noms

Tout le monde doit apparaître souligné

Cliquer sur ok



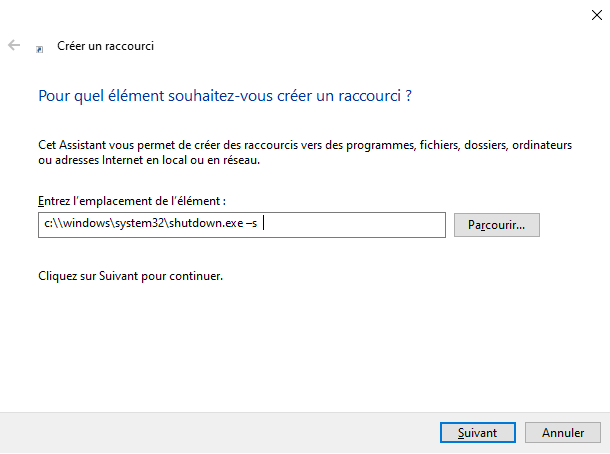
Sélection Tout le monde et cocher Contrôle total



Faire Appliquer / ok / Fermer

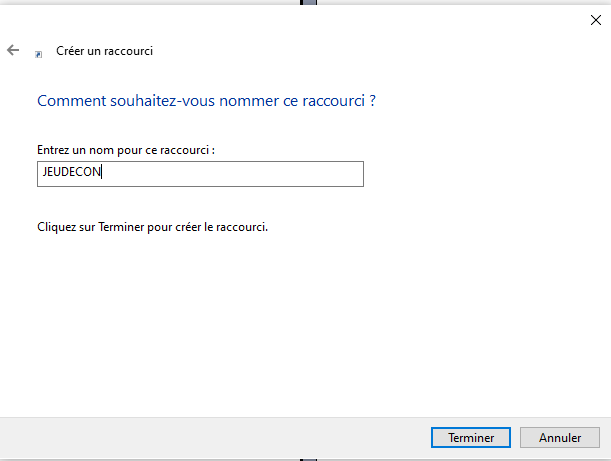
Entrer dans ce nouveau dossier

Faire Clique droit / nouveau raccourci



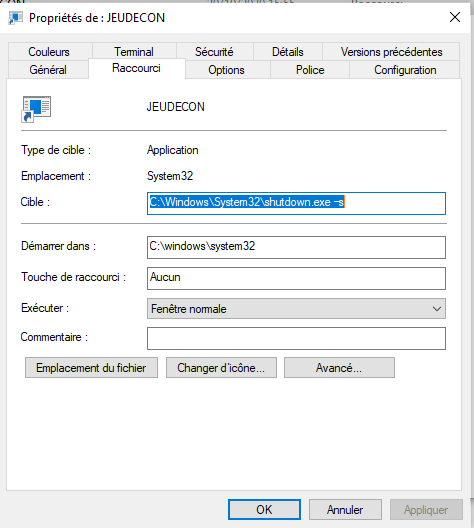
Dans l’emplacement de l’élément taper c:\\windows\system32\shutdown.exe –s

Faire suivant

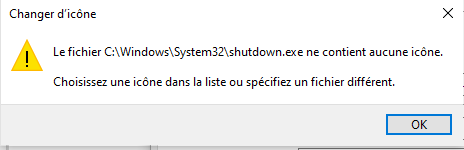


Cliquer sur Terminer

Clique droit / propriété / changer d’icône



Cliquer sur Changer d’icône



Le message suivant apparaît.

Cliquer sur OK

Choisir 

Faire Appliquer / ok

Vous devez obtenir ceci :



Ouvrir Notepad++ ou le bloc note

Saisir les lignes suivantes

echo off

cd

CD C:\Users\Votre\_nom\Documents\jeux express\

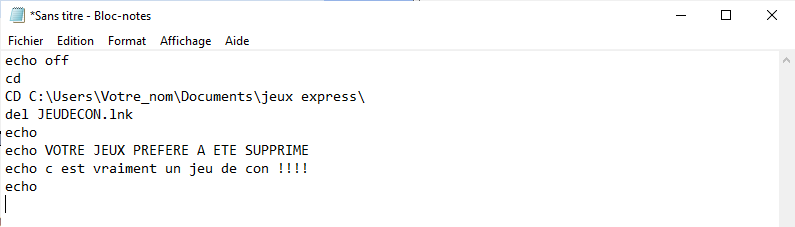
del JEUDECON.lnk

echo

echo VOTRE JEUX PREFERE A ETE SUPPRIME

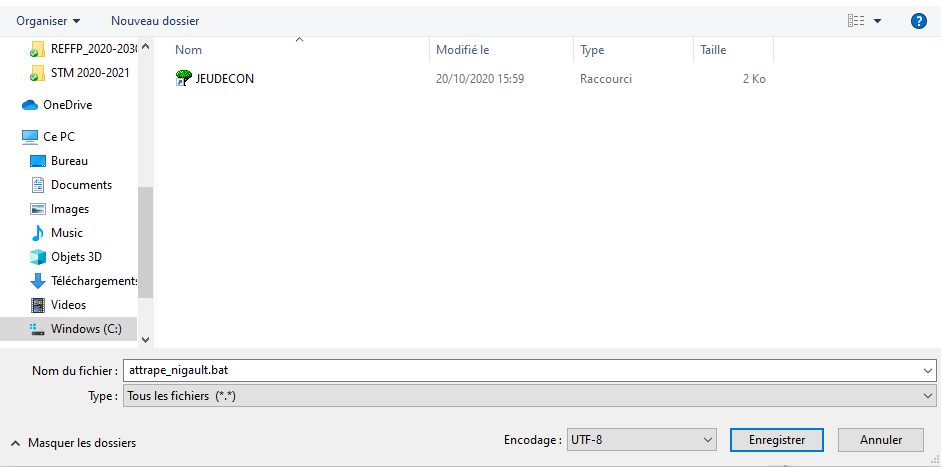
echo c est vraiment un jeu de con !!!!

echo



Faire Fichier / Enregistrer sous

Aller dans CD C:\Users\Votre\_nom\Documents\jeux express\



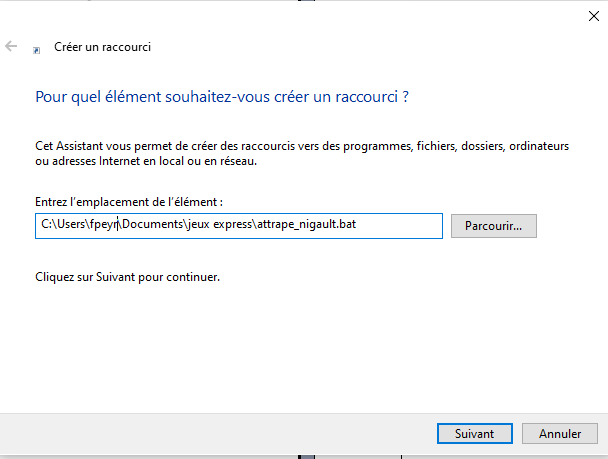
Dans Nom de fichier entrer attrape\_nigault.bat

Dans Type, sélectionner Tous les fichiers (\*.\*)

Laisser l’encodage en UTF-8 et faire Enregistrer

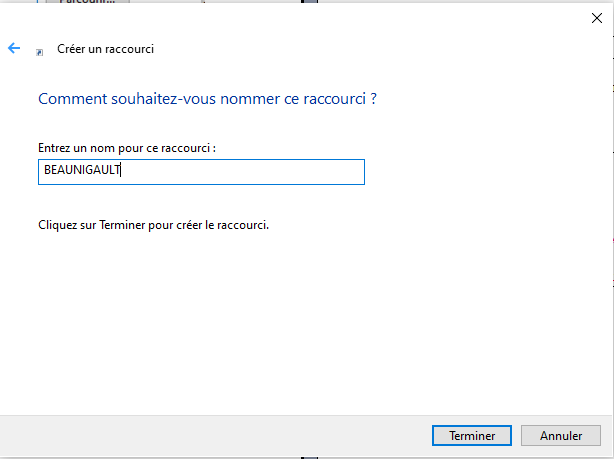
Dans le dossier C:\Users\Votre\_nom\Documents\jeux express\

Créer un nouveau raccourci



Dans l’emplacement de l’élément taper C:\Users\Votre\_nom\Documents\jeux express\attrape\_nigault.bat

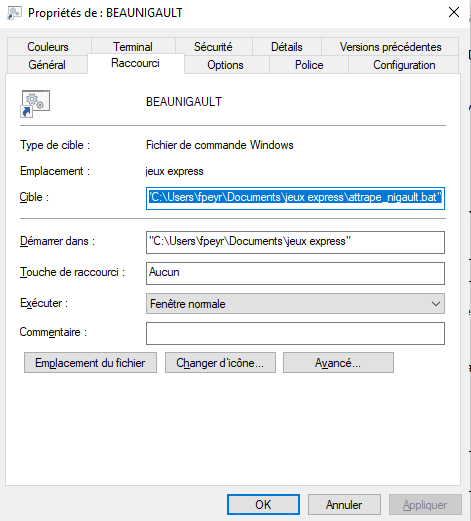
Faire suivant



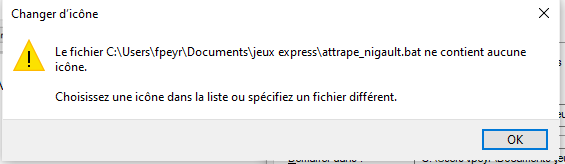
Dans Entrer le nom du raccourci taper BEAUNIGAULT

Faire Terminer

Sur le raccourci BEAUNIGAULT faire Clique droit / Propriétés



Cliquer sur Changer d’icône



Le message suivant apparaît

Faire OK

Choisir cette icône 

Appliquer / ok

Vous devez obtenir ceci



Puis dans jeux express cliquer sur propriété, partage, partager ce dossier.

Dans autorisation, tout le monde, contrôle total, appliquer, ok

Sur xp, dans poste de travail, aller sur outils, connecter un lecteur.

Choisir une lettre, dans dossier taper [\\192.168.1.50\jeu](../../../../../../../../../../../..//192.168.1.50/jeu) express

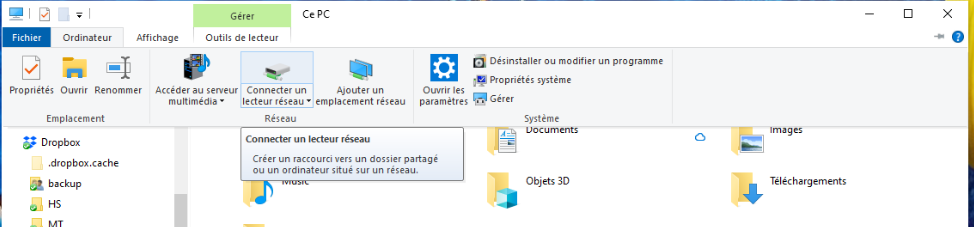
Connecter vous en temps qu’administrateur, avec le mot de passe de l’administrateur

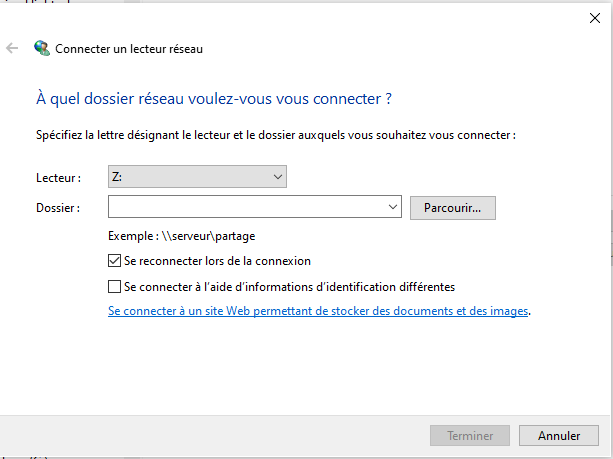
**Tester un trojan**

Fermer la session administrateur et ouvrir une session sur le pc votre\_nom\_de\_famille avec testeurfou.

Aller dans poste de travail, sur c:\

Aller sur Ordinateur outils / Connecter un lecteur réseau / créer un lecteur réseau





Vérifier l’obtention de votre nouveau lecteur réseau dans poste de travail.

Cliquer sur JEUDECON

Que constatez-vous ? Expliquer.

Cliquer sur BEAUNIGAULT

Que constatez-vous ? Expliquer.

**Validation**

1. **Prouver le constat**
2. **Donner l’explication**
3. **Chercher comment parer ce type d’attaque**

**Mettre votre résultat dans un document pour synthèse**

**Mettre en place un système de parade**

Sur votre poste de travail Votre\_nom\_de\_famille2, installer un anti-trojan.

Installer votre trojan et tester la parade.

**Validation**

1. **Prouver le constat**
2. **Donner l’explication**
3. **Chercher comment parer ce type d’attaque**

**Mettre votre résultat dans un document pour synthèse**