

TD ATTAQUE DEFENSE :

Adam Jaballah

test de la commande ipconfig/all

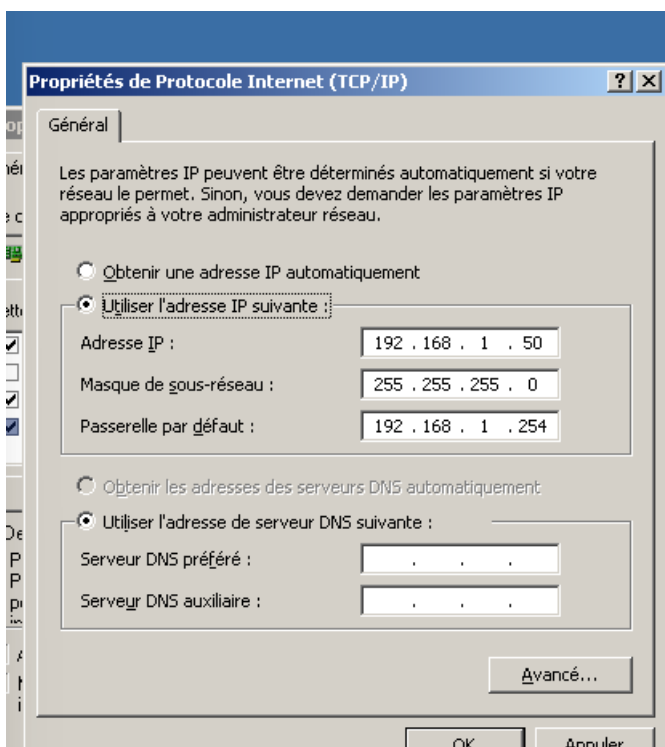
Test sur le serveur srvatack

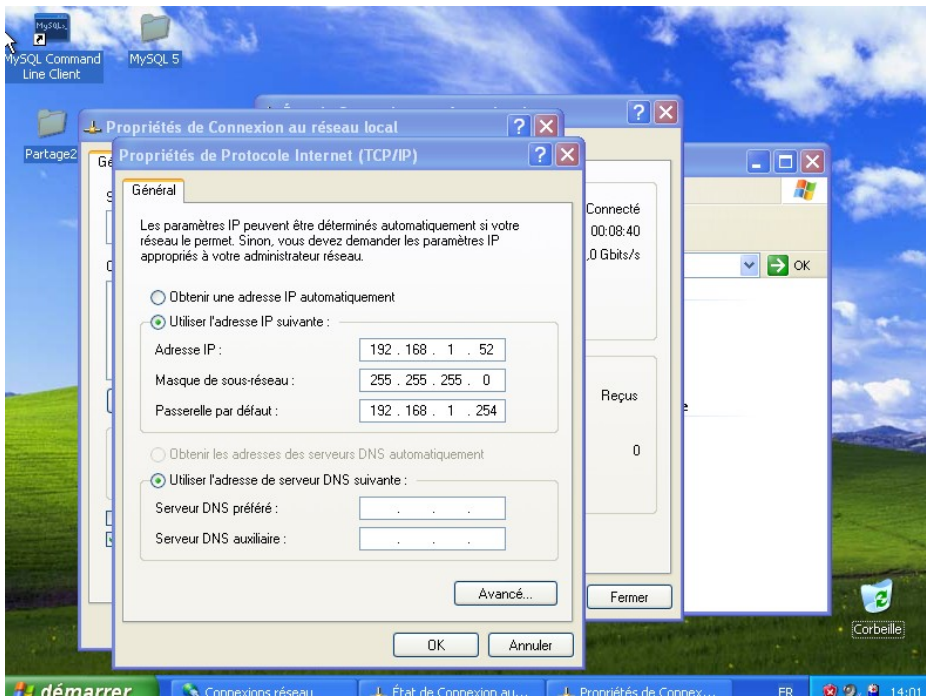
```
C:\WINDOWS\system32\cmd.exe
Carte Ethernet Connexion au réseau local 2 :
Suffixe DNS propre à la connexion :
Description . . . . . : Carte Intel(R) PRO/1000 T pour serv
eur
Adresse physique . . . . . : 08-00-27-AF-3D-7F
DHCP activé . . . . . : Oui
Configuration automatique activée : Oui
Autoconfiguration d'adresse IP . . : 169.254.72.157
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-CD-23-82
DHCP activé . . . . . : Non
Adresse IP . . . . . : 192.168.1.254
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . :

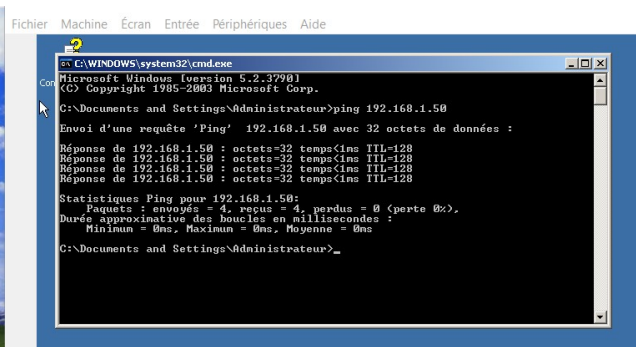
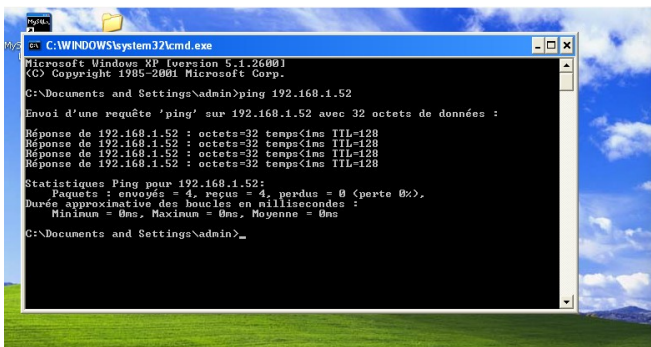
C:\Documents and Settings\Administrateur>
```

Ensuite je met les adresses ip dans le « srvatack » et le « jaballah »



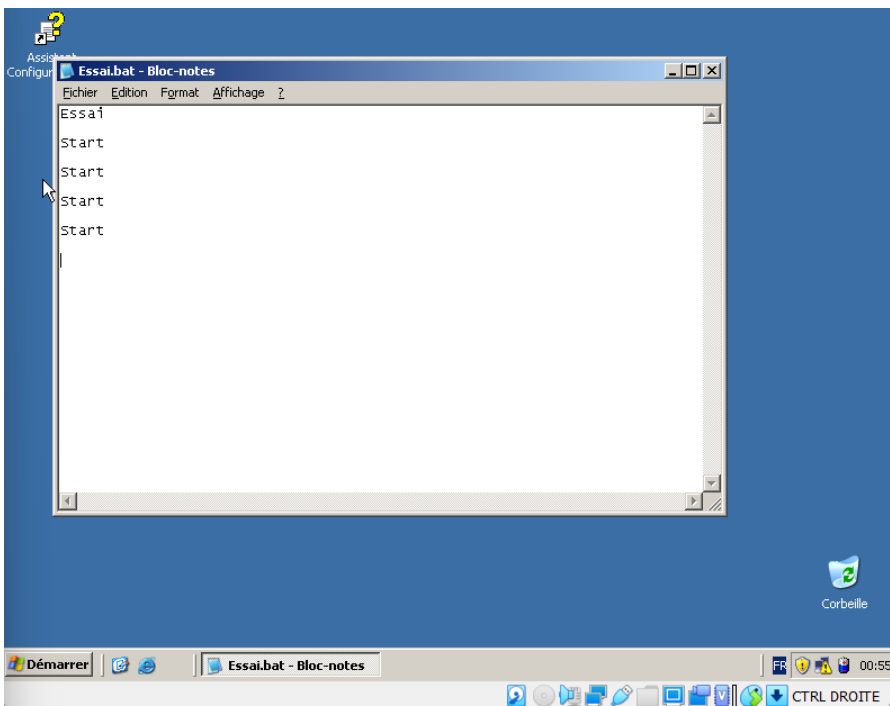


Connexion des deux serveurs :



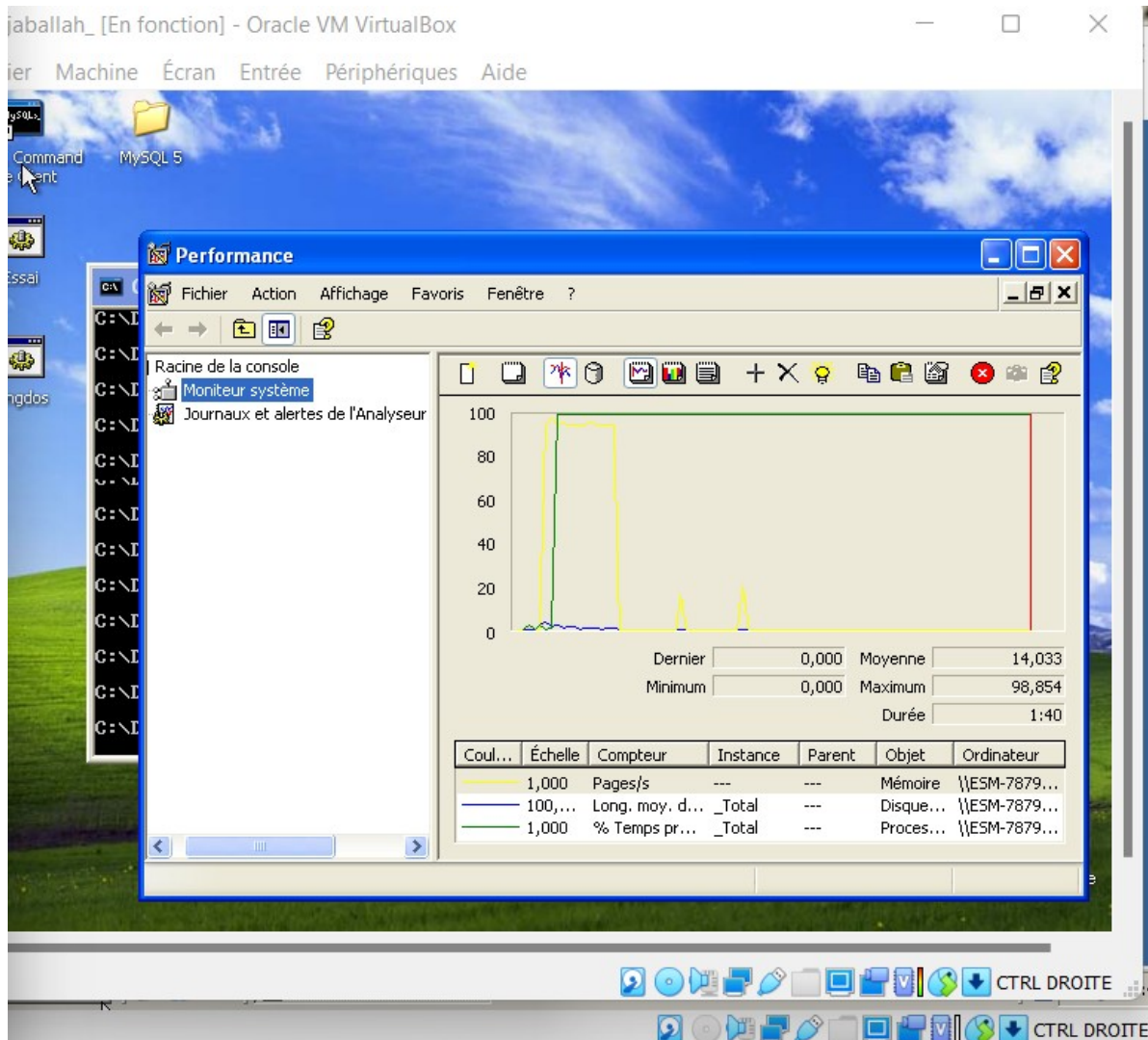
Ici nous voyons que les 2 serveurs ce sont bien reconnu

Test de DDOS dans un serveurur :

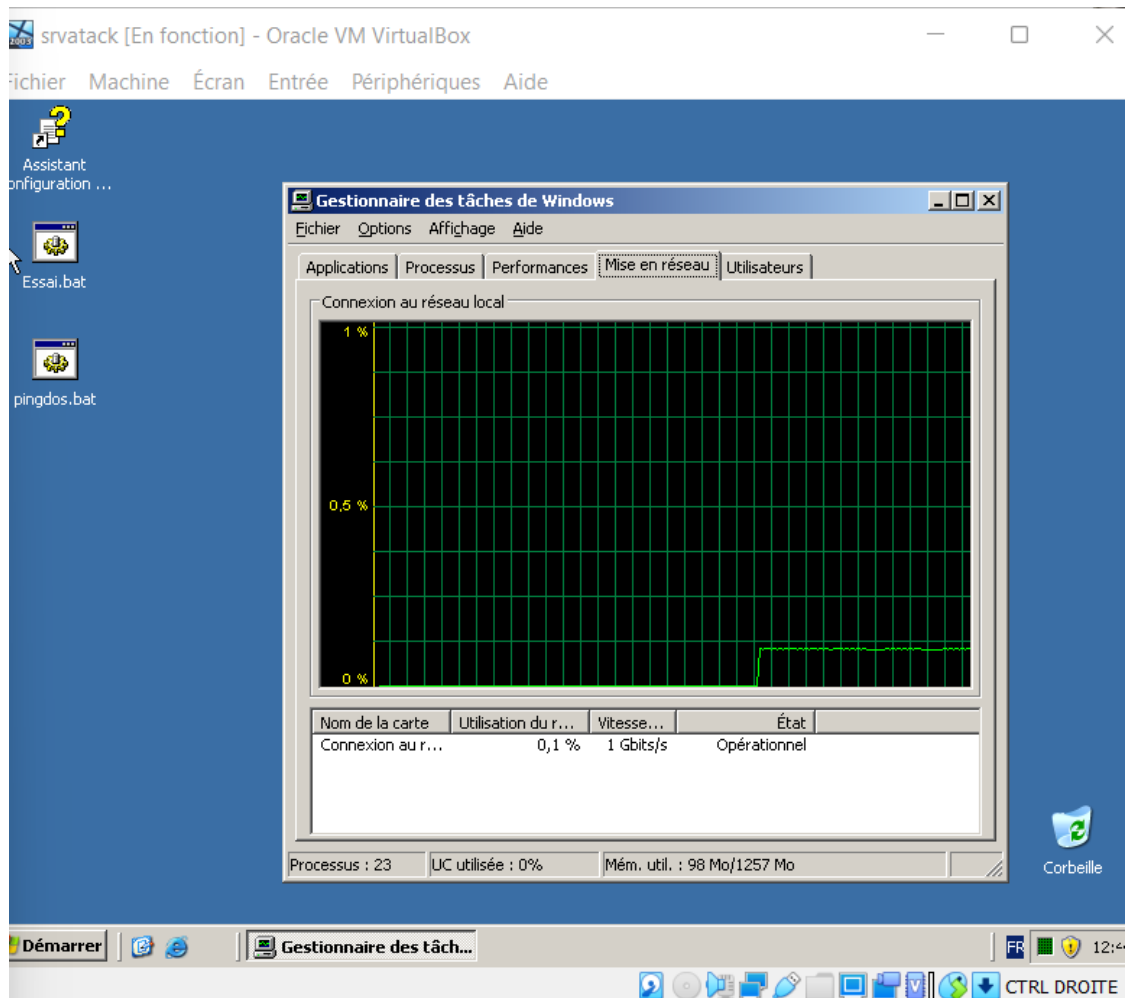


Avant de ddos le serveur je vais commencer par créer le fichier .bat que je vais ouvrir par la suite.

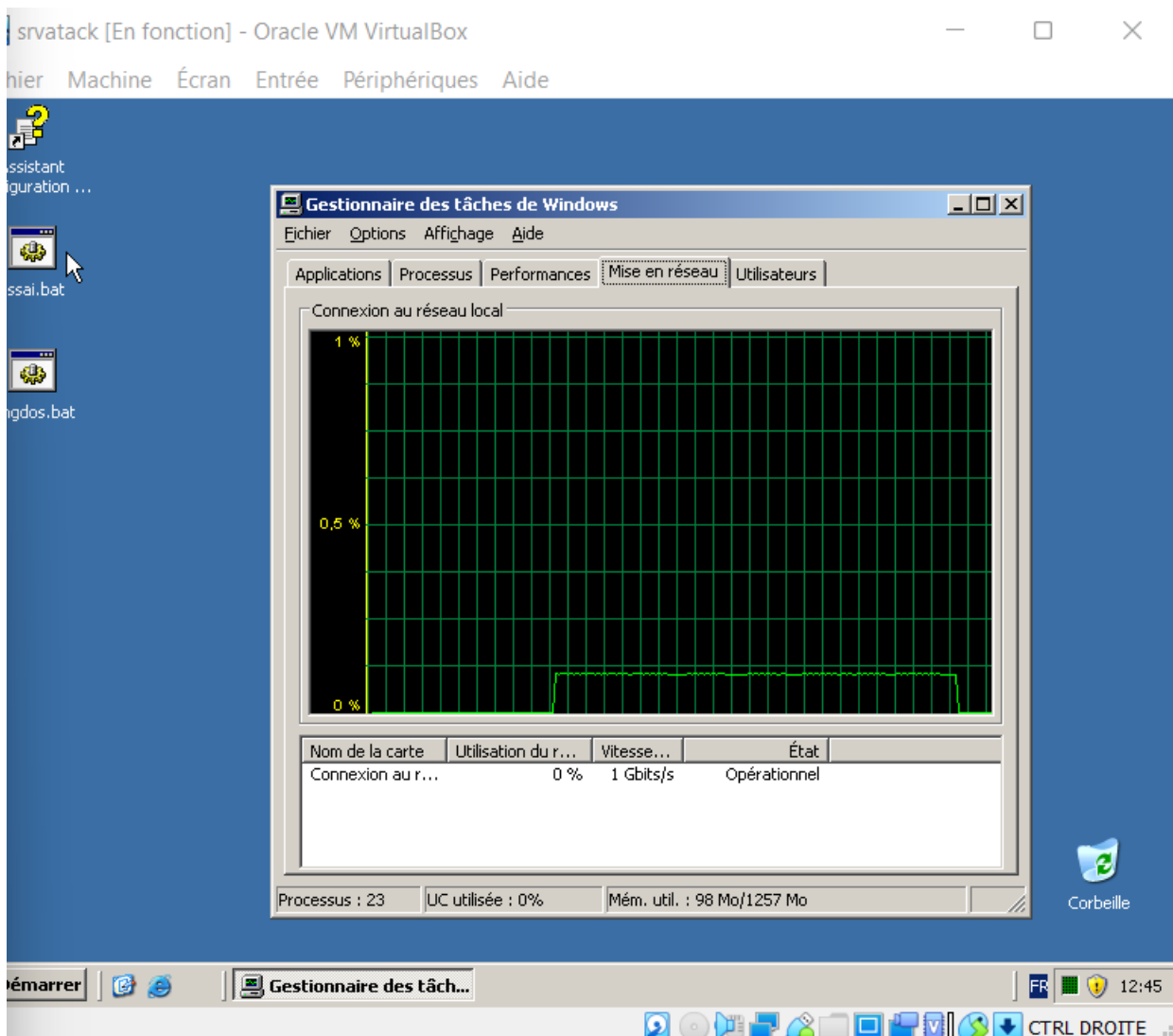
Après l'ouverture du screen je constate que l'utilisation du processeur (la bande passante) est monter à 100 % car j'ai envoyer beaucoup trop de demande au reseau



Après ouverture du pingddos je constate aussi que le réseau commence peu à peu à saturer à cause des nombreuses demande auparavant



Voici le résultat après la fermeture du pingddos, je constate que le réseau commence petit à petit à redevenir stable grâce à la fermeture du pingddos



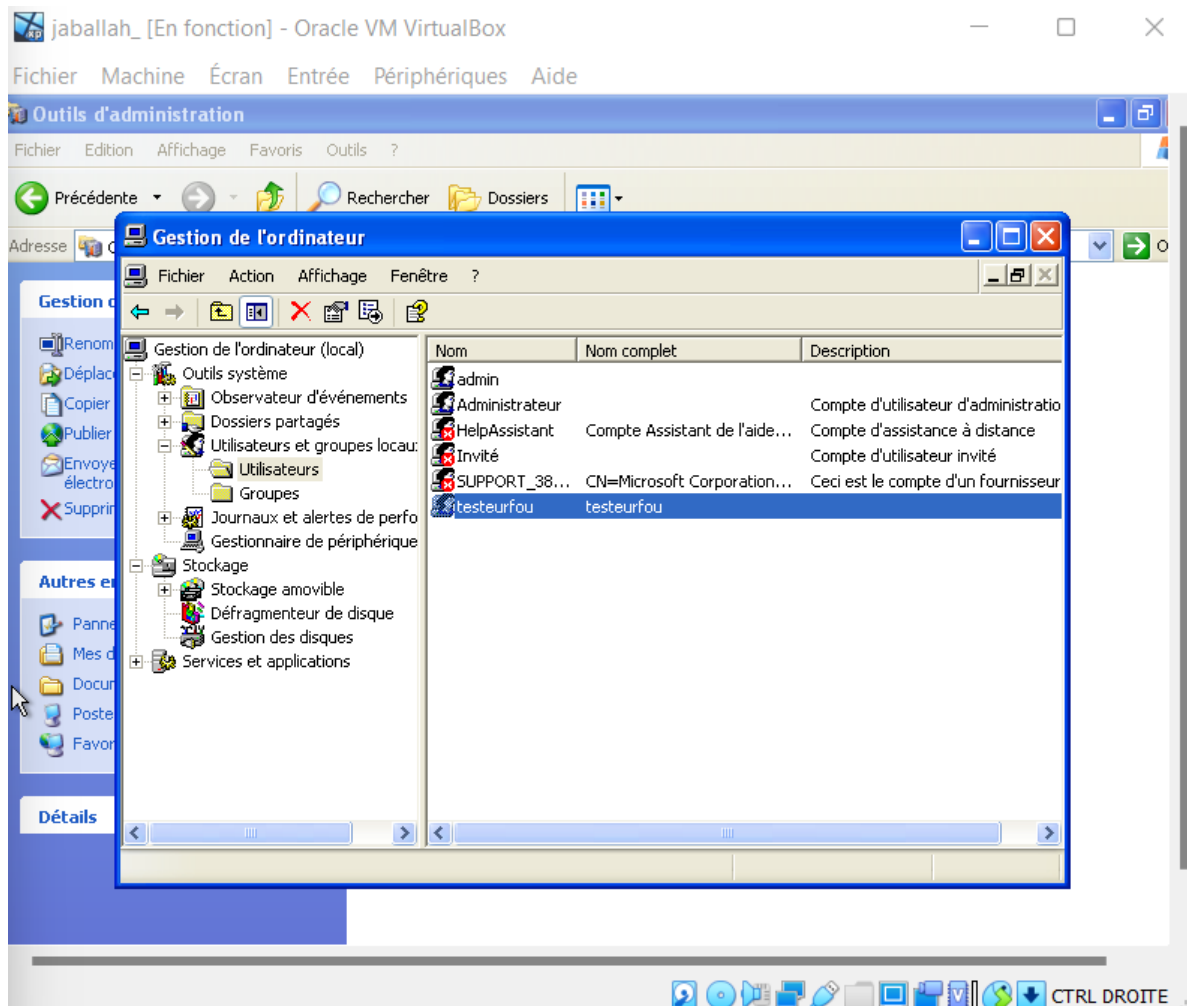
Comment contrer ce genre d'attaque ?

- Avoir une architecture composée de plusieurs serveurs offrant le même service au client afin de répartir les points d'accès aux services et offres. En cas d'attaque, les clients subissent un ralentissement, plus acceptable qu'un arrêt de service.

- Mettre en place un serveur tampon, appelé « cleaning center » pour filtrer et nettoyer le trafic de manière à ce que les menaces n'affectent pas le serveur.

Et bien sur activer ses pare feu, un bon vpn est aussi primordiale

Après avoir créer l'utilisateur testeurfou j'ai changé de systeme pour repartir sur du windows serveur 2019 pour continuer le tp, et voici le « JEUDECON » qui à été créer dans le raccourci de « testeurfou »



Puis j'ai placé l'attrape nigault, beaugault dans le dossier jeux express

jeux express

Fichier Accueil Partage Affichage

< > << Disque local (C:) > Utilisateurs > Public > jeux express > Rechercher dans : jeux express

Nom	Modifié le	Type	Taille
attreape_nigault	03/12/2022 15:02	Fichier de comman...	1 Kc
BEAUNIGAULT	03/12/2022 15:04	Raccourci	2 Kc
JEUDECON	03/12/2022 14:40	Raccourci	2 Kc

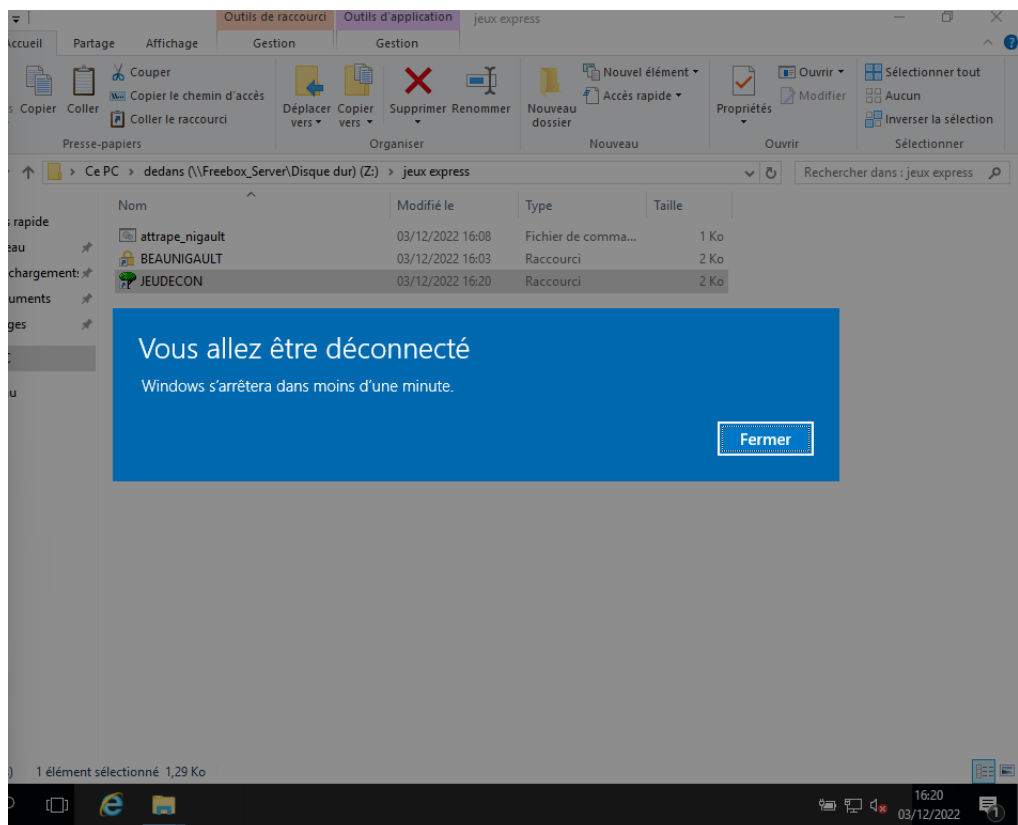
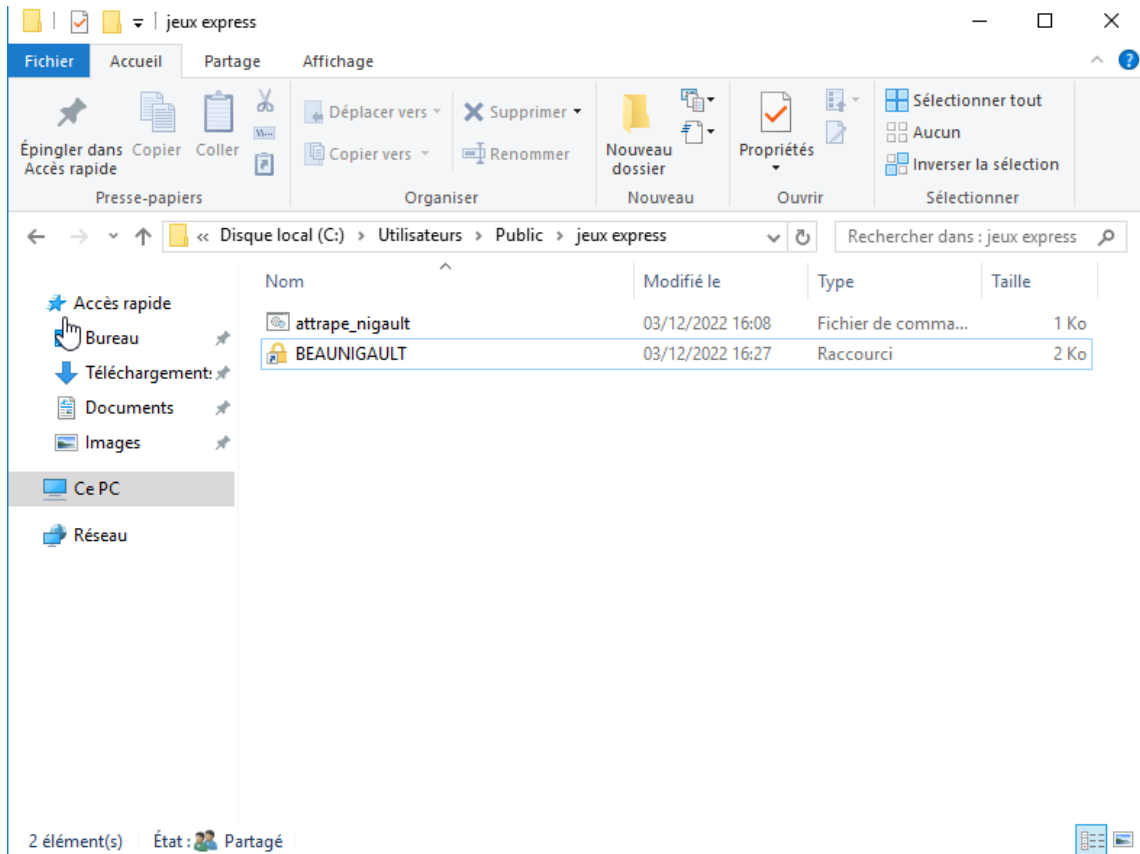
Accès rapide

- Bureau
- Téléchargement
- Documents
- Images
- devoir24012022
- Mon site internet
- nomde

Ce PC

Réseau

3 élément(s) État : Partagé



Comme les images le montrent juste dessus, après avoir lancé le jeu, ma session s'est déconnectée et le jeu a été supprimé car dans le code il y avait des lignes de code qui étaient censées supprimer le jeu après le lancement