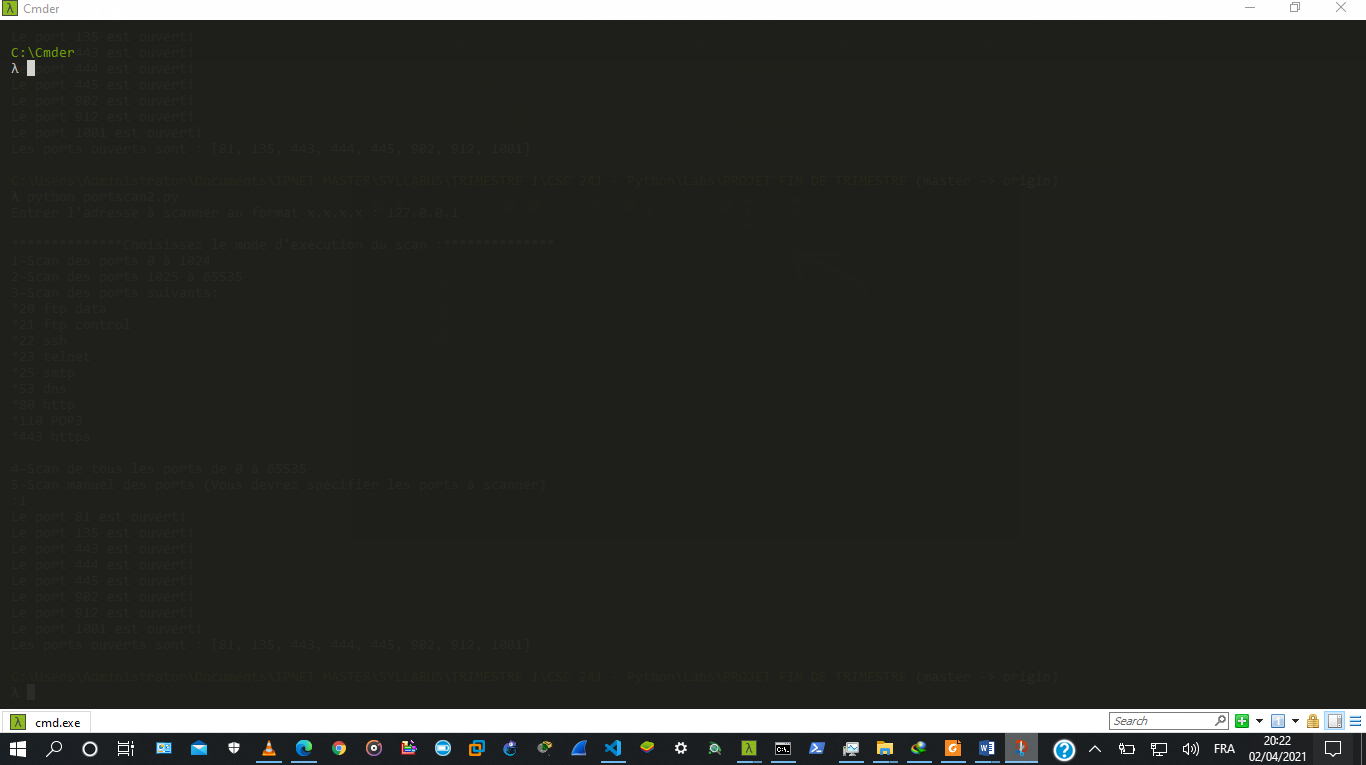
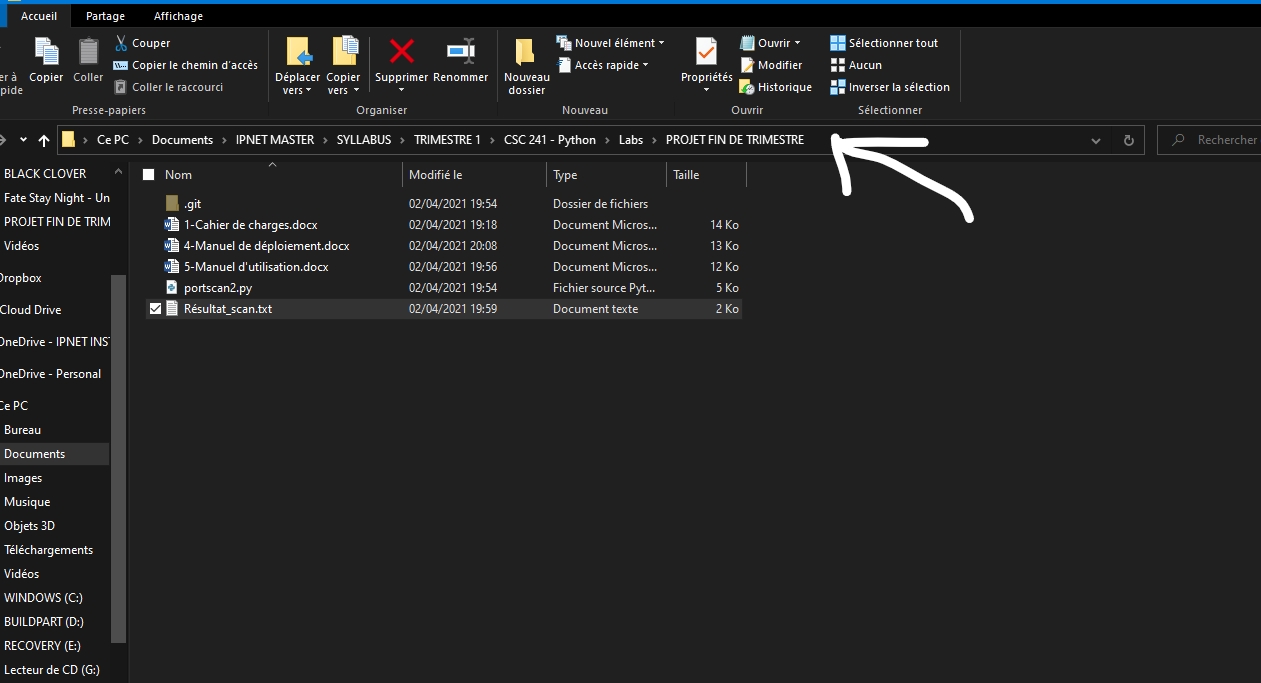
1-Lancer Cmder en fonction de là où vous l’avez installé. Une fenêtre devrait apparaitre comme celle-ci :

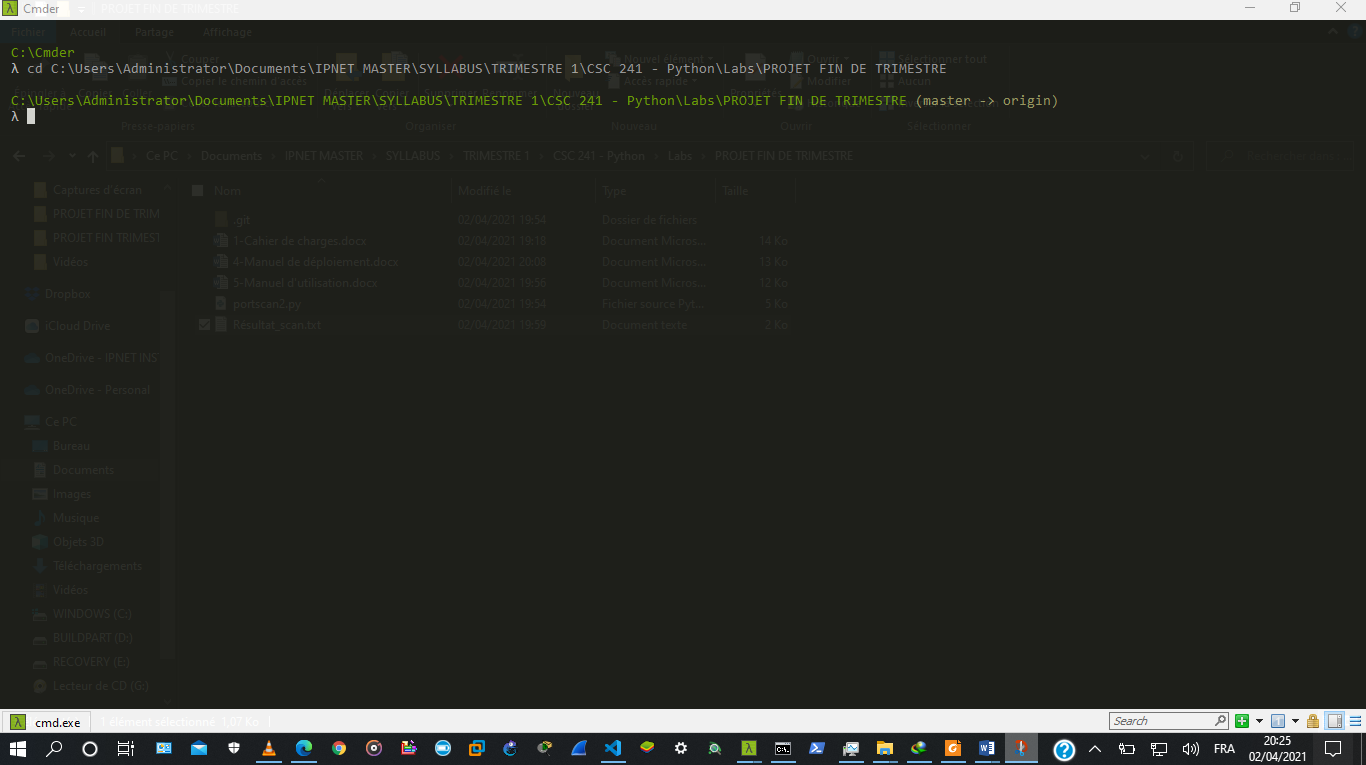


2-Copiez le chemin du répertoire où est stocké le script portscan.py en cliquant dans la barre latérale dans l’explorateur de fichiers



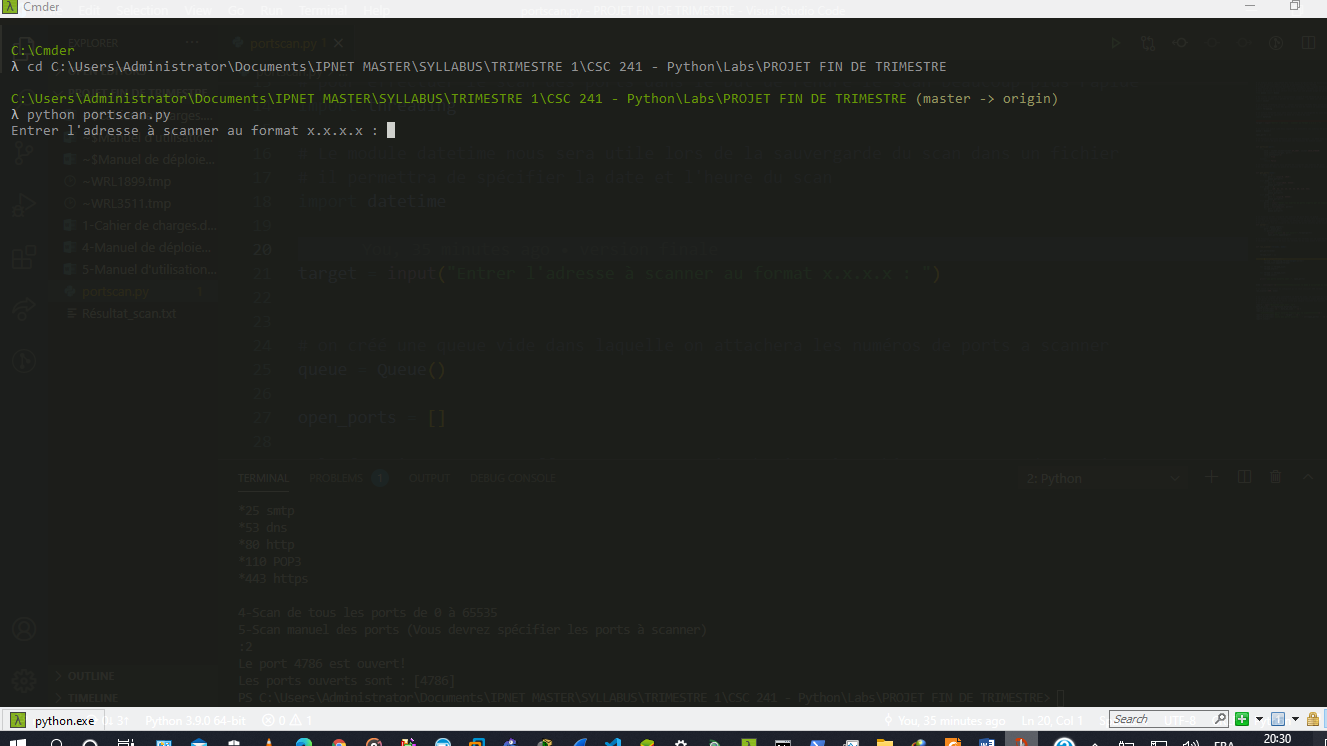
Notez que votre répertoire ne devrait pas avoir un fichier Résultat\_scan.txt au départ. Dans mon cas j’ai effectué des test avant la prise de la capture d’écran donc le script m’a généré ce fichier contenant les résultats de mes scans.

3-Dans la fenêtre de votre programme Cmder, écrivez « cd » puis collez le chemin d’accès que vous avez copié et appuyez sur la touche« Entrer ». Cela devrait donner un résultat semblable au suivant :



Ne vous préoccupez pas de la mention « master -> origin » qui apparait sur la capture.

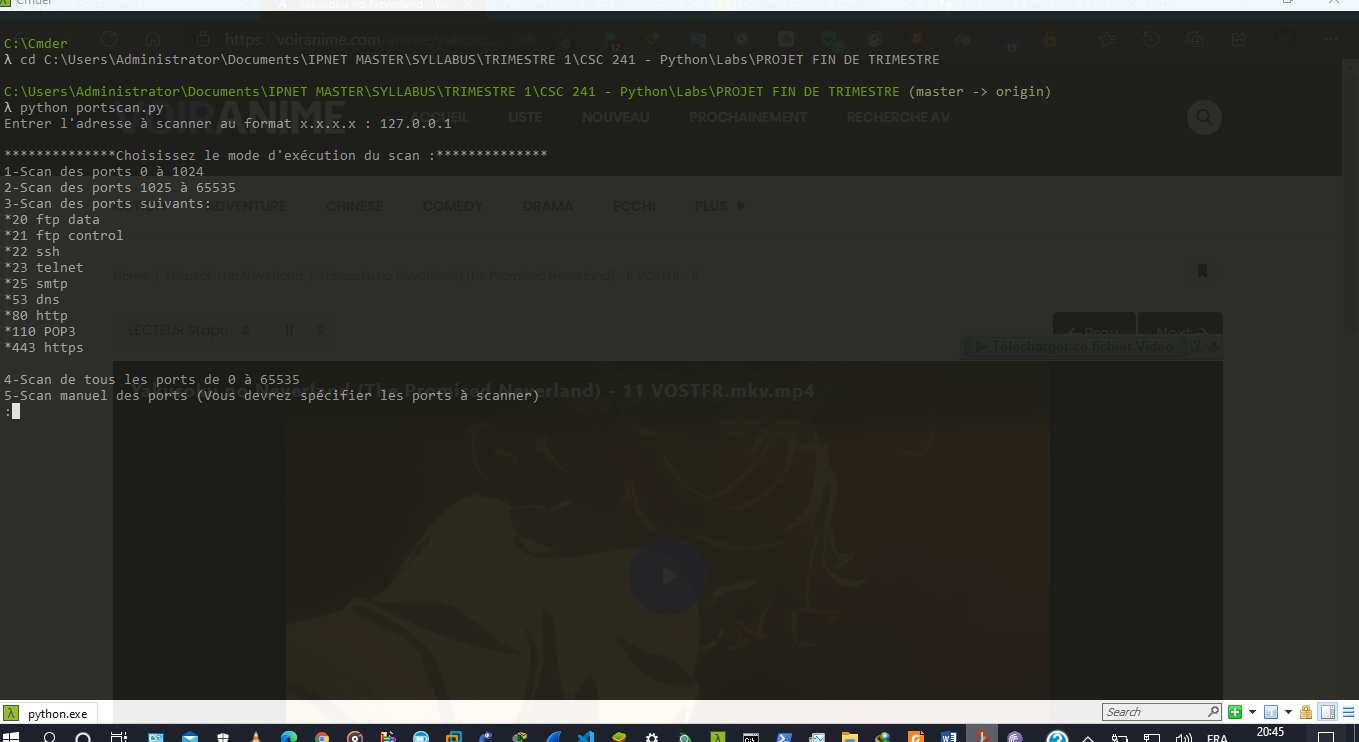
4-Toujours dans Cmder, écrivez « python portscan.py » et appuyer sur la touche « Entrer »



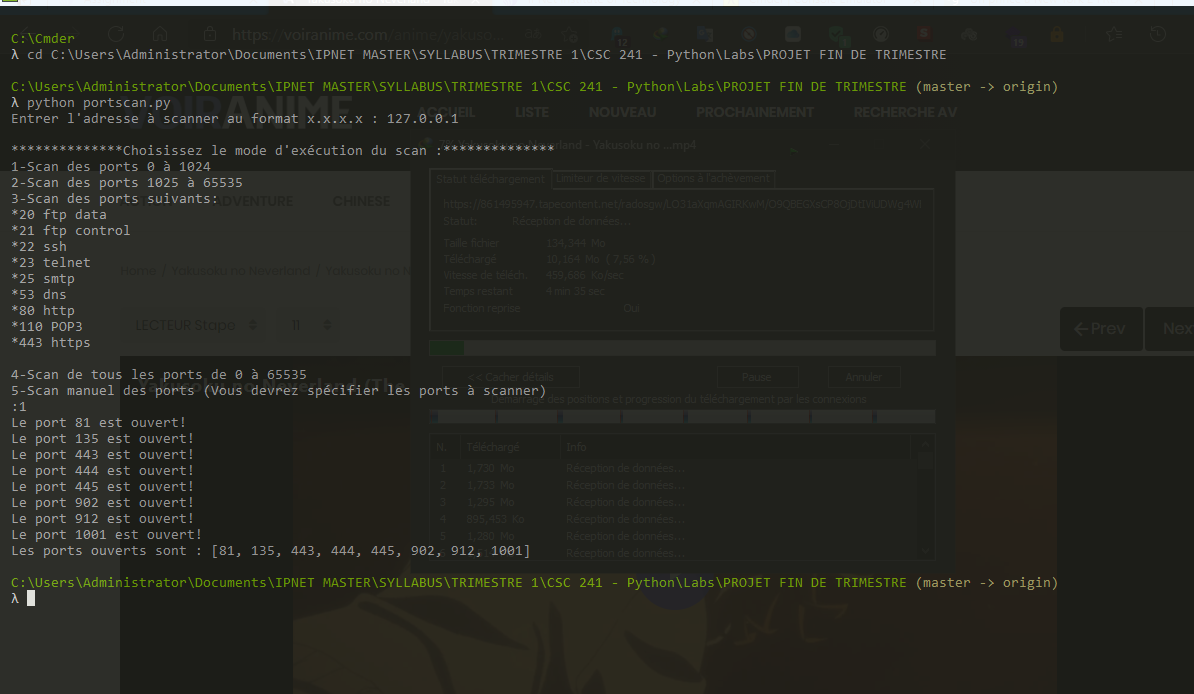
A ce point le script est lancé et vous êtes invité à entrer une adresse ip. Si vous êtes connecté à un réseau et que vous connaissez l’adresse d’une machine vous pouvez l’entrer ou si vous avez accès à internet vous pouvez également entrer le nom d’un site comme (ipnetuniversity.com, facebook.com, youtube.com…).

Dans le cas où vous n’avez aucune connexion, vous pouvez toujours scanner votre propre machine en entrant 127.0.0.1

5-Dans notre cas puisque je ne peux prédire en quelle situation vous exécuterez le scan, supposons que vous n’avez pas de connexion. Entrons donc l’adresse ip de notre machine qui est 127.0.0.1 et appuyer sur « entrer »

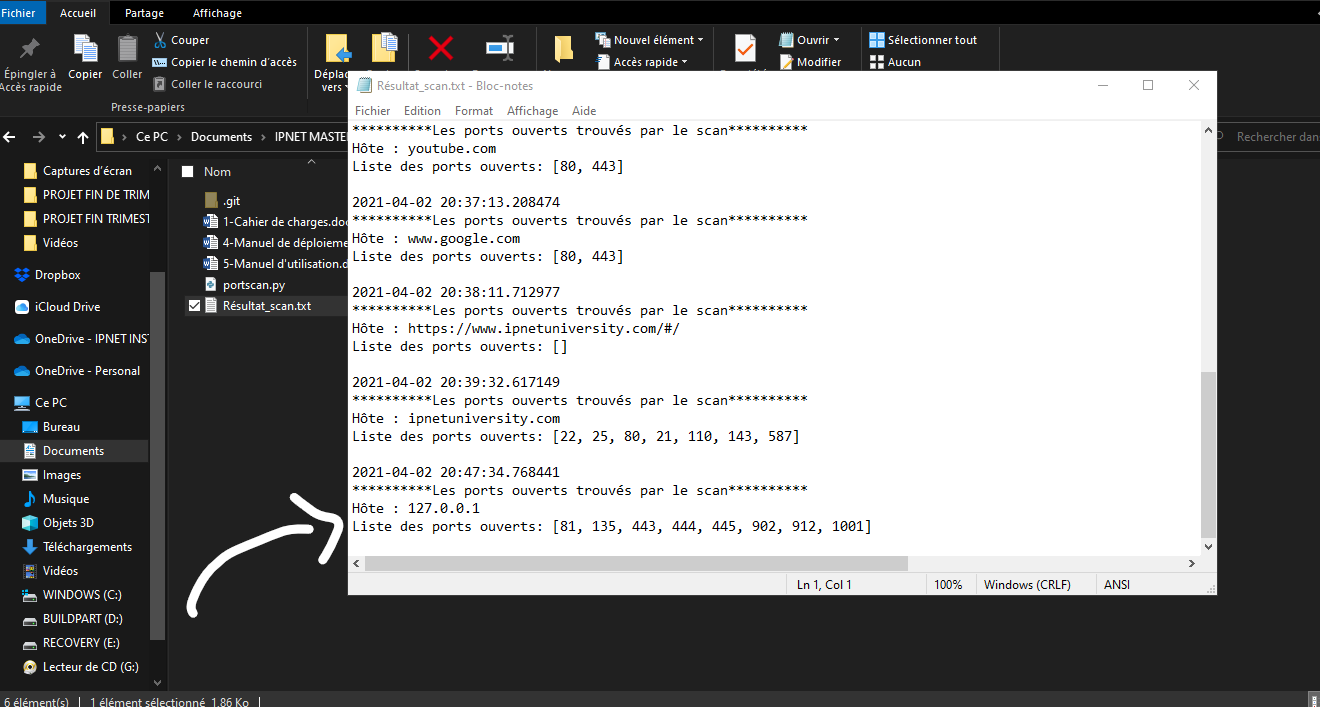


Un menu listant des options s’offre à nous. Essayons l’option 1 :



On peut voir les différents ports ouverts sur ma machine au moment du scan. A chaque fois qu’un port ouvert est découvert, on obtient un affichage à l’écran et à la fin une liste qui résume les ports découverts. Notez que la première occurrence commence part le port 81, cela parce qu’on lorsqu’on port n’est pas ouvert on obtient pas de résultat à l’écran.

6-Retournez a votre répertoire où se trouve le script python, vous devriez maintenant avoir le fichier Résultat\_scan.txt qui contient le résultat de votre premier scan. Ouvrez-le :



On peut effectivement voir notre résultat qui correspond bien aux sorties de notre script. Effectivement j’ai beaucoup plus d’entrées puisque comme je l’ai dit précédemment il m’a fallu effectuer des tests au préalable. Dans votre cas vous ne devriez avoir qu’une seule entrée.

NB :

Notez qu’en raison de la manière dont j’ai implémenté mon script il vous faudra relancer le script pour effectuer un autre test.

Pour ce faire, de votre fenêtre Cmder, appuyez simplement sur la touche directionnelle du haut pour rappeler la commande d’exécution du script et appuyez sur la touche « entrer ».

Pour pallier à ce léger défaut, une fonctionnalité permettant de refaire des tests sans relancer pourra être ajoutée s’il m’en est donné l’occasion.