..:: Scanner des failles VNC avec Dfind ::..

INTRODUCTION :

Ce tutorial est simplement destiné à ceux qui veulent étendre leur savoir. Scanner des adresses IP est strictement interdit, je le rappelle. Je ne pourrais être tenu responsable de vos actes en cas d'utilisation interdite de ces explications.
VNC est un logiciel de contrôle d'ordinateur à distance. Le bureau du PC ou le SERVEUR VNC est actif apparaît alors comme par magie sur VOTRE bureau en entrant tout simplement l'adresse IP du PC concerné ainsi que le mot de passe qui va avec dans le VNC VIEWER.
Mais il existe (^^) des FAILLES VNC, qui sont appelées « NULL SESSION ». Ces failles sont en fait des ordinateurs où un serveur VNC est actif, mais non protégé par un mot de passe…
Il reste donc à trouver ces ordinateurs ouverts librement au public…

1°/ MATERIEL :

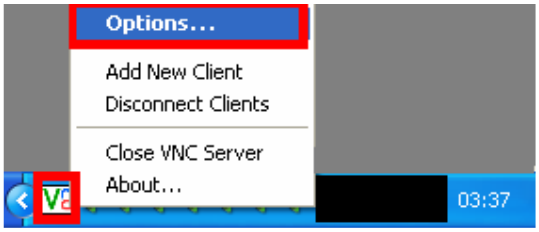
- Un cerveau (primordial) ;
- Le logiciel VNC (version du tuto : VNC Free Edition 4.1.1) ;
- L'application Dfind.exe (considéré comme un virus par la plupart des antivirus) ;
- La liste des IP à ne pas scanner (très important).

2°/ VNC :

Installer VNC (je ne donnerais pas d'explication là-dessus lol).
Une fois VNC installé, je vous conseille vivement de retirer le serveur qui s'est activé automatiquement, ou alors, protéger ce serveur par un mot de passe, afin que vous puissiez accéder à votre bureau depuis un autre PC.
L'icône se trouve en bas à droite, à côté de l'horloge Windows :

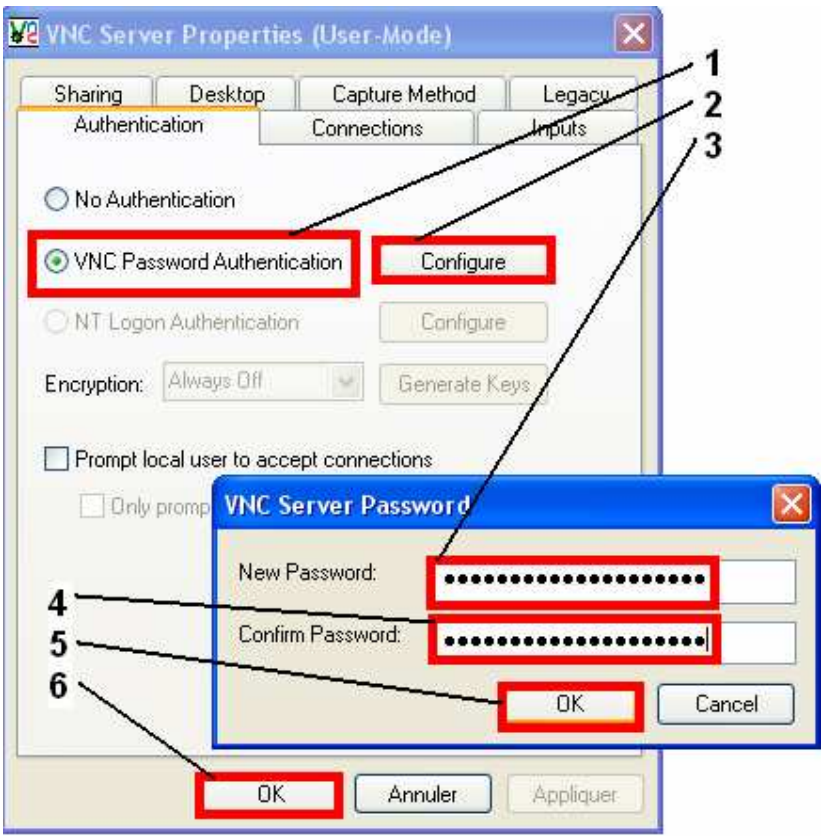
Protection par mot de passe :

Cliquez avec le bouton droit de la souris sur l'icône et allez dans les options…



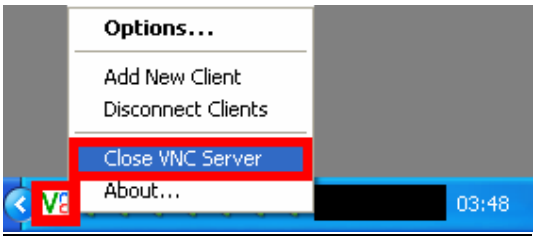
Cochez ensuite la case mot de passe (1), et créez-en un (le taper 2 fois) (2,3, 4 et 5).

Validez (6).



<u>Pour fermer le serveur :</u>

Cliquez droit sur l'icône et fermez.



3°/ SCANNER LES FAILLES VNC AVEC DFIND :

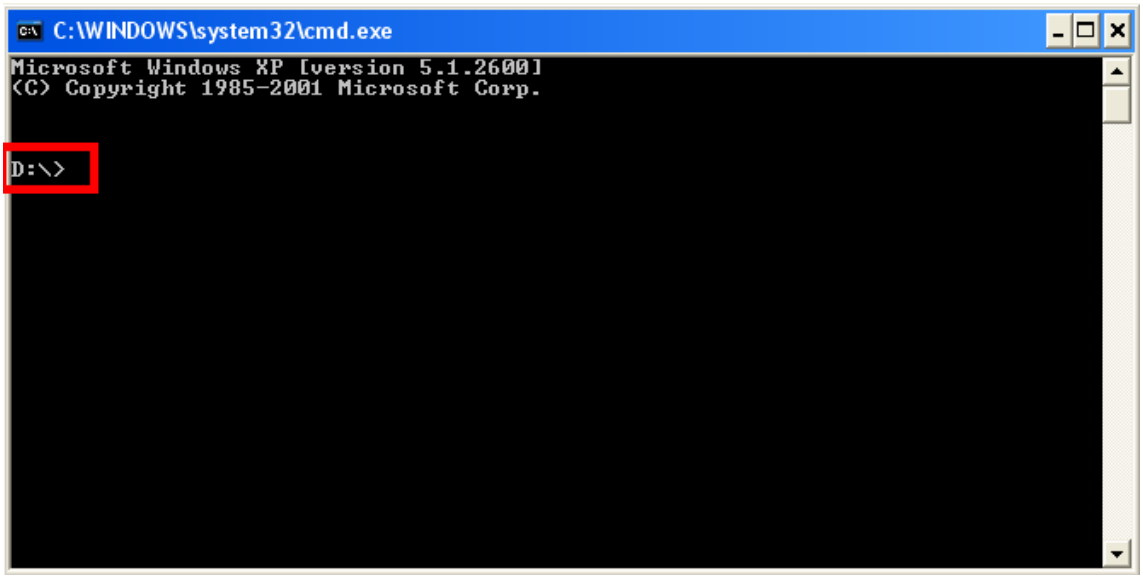
Tout d'abord, il est plus simple de placer Dfind .exe à la racine d'un disque dur, genre c:\ ou d:\, car il va falloir y accéder avec la commande DOS, donc moins il y a de répertoire à parcourir, plus çà sera rapide :

Démarrer la commande MSDOS :
Allez dans Démarrer, Exécuter, et tapez cmd :

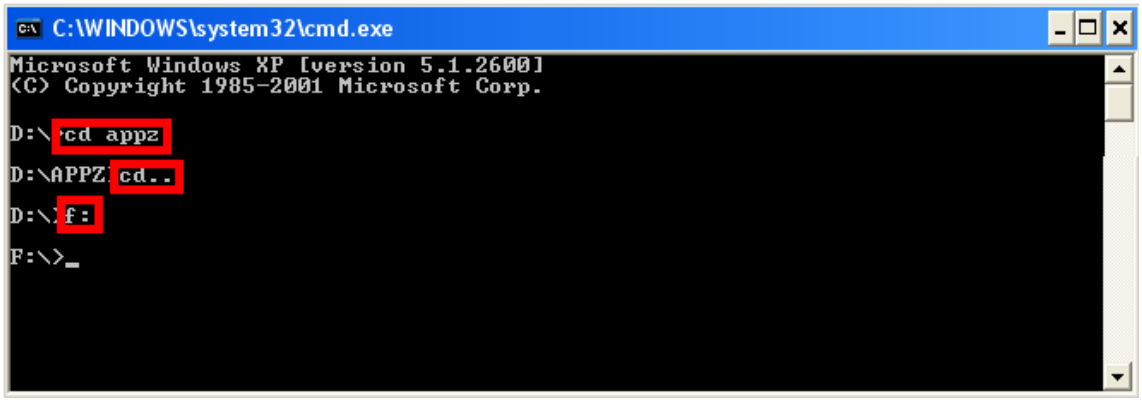
La commande MSDOS s'ouvre alors.

<u>Rappel sur les commandes de changement de dossier :</u>

Exemple : vous vous trouvez dans d:\ :



Pour accéder au dossier nommé « APPZ » qui se trouve dans « d:\ », tapez « cd APPZ » puis la touche ENTREE.
Pour revenir dans le dossier précédent, tapez « cd.. ».
Pour changer de disque dur, tapez la lettre tout simplement (f :).

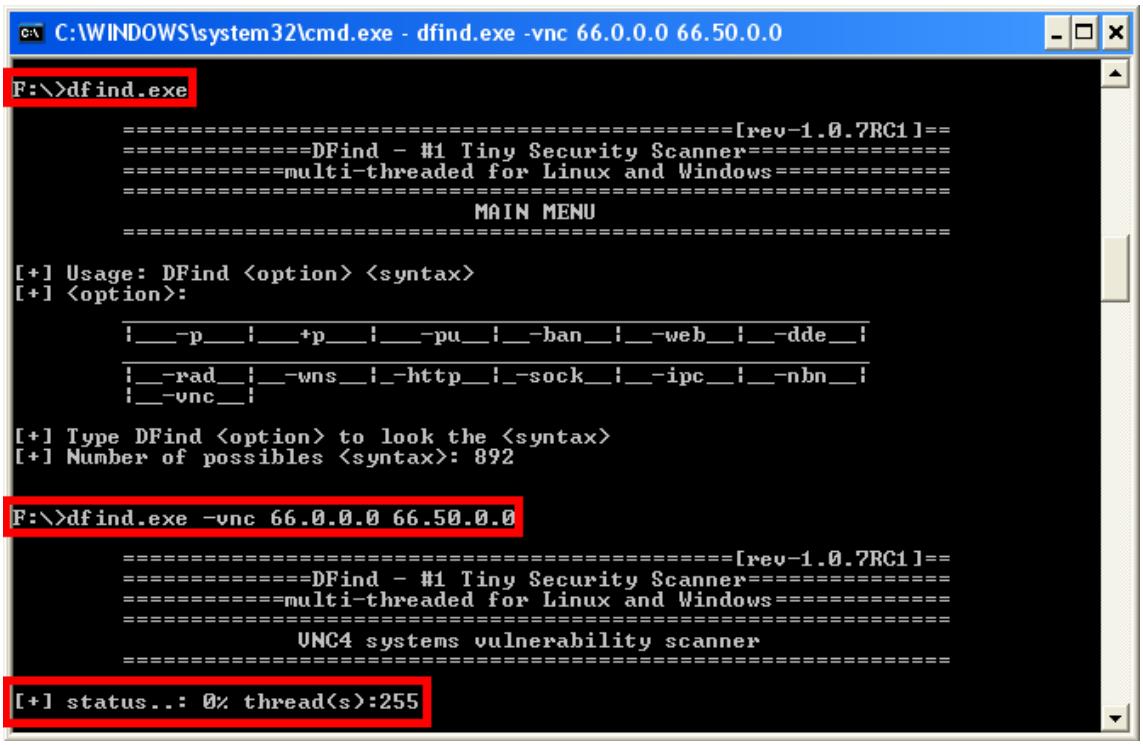


Une fois dans le dossier ou se trouve Dfind.exe, démarrer-le en tapant « dfind.exe ».
Un tableau va apparaître. Tapez alors la commande suivante, en remplaçant XX.XX.XX.XX par l'IP par laquelle vous voulez débuter votre scan et YY.YY.YY.YY par l'IP à laquelle le scan va se terminer.

Voici la commande (un copier/coller marche très bien) :

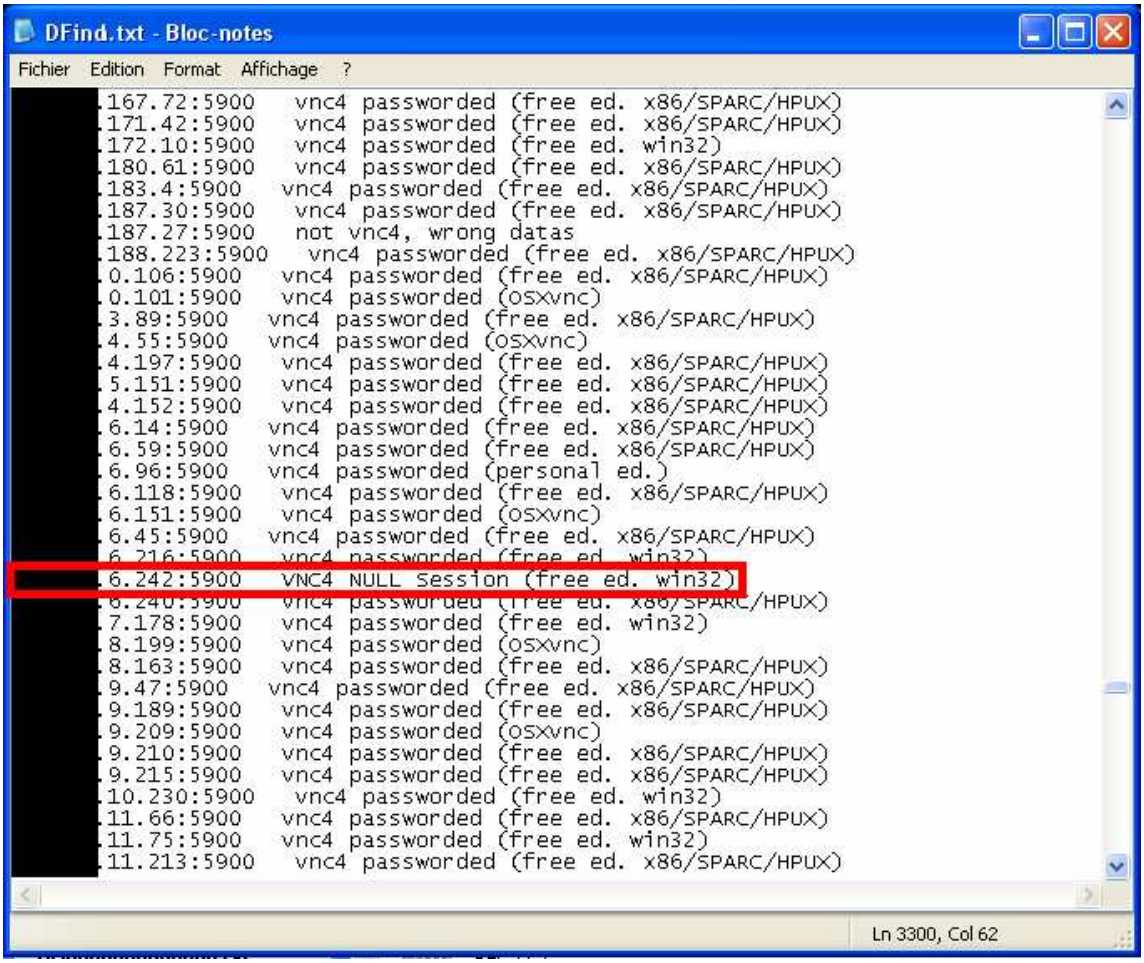
Dfind.exe –vnc XX.XX.XX.XX YY.YY.YY.YY

Vous devriez alors voir la progression du scan comme ceci :
Exemple :



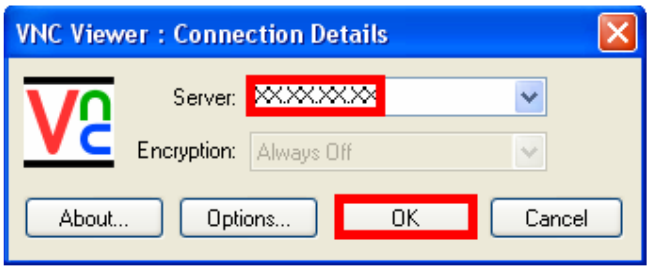
Je conseille de mettre une range d'IP faible, afin de voir le temps que le scan prendra…
Augmentez par la suite, sinon vous risquerez de vous retrouver avec un scan durant 3 jours !!
Une fois terminé (100%), allez dans le dossier ou vous avez mis le Dfind.exe.
Un Dfind.txt doit être apparu.

Les FAILLES VNC sont symbolisées, comme vu dans l'introduction par une NULL SESSION.
Vous devez alors éliminer du fichier teste tout ce qui n'est pas utile, tout ce qui n'est pas null session :



4°/ TESTER LES RESULTATS :

Démarrez alors le VNC VIEWER (vncviewer.exe) et entrer l'IP trouvée…



Les premières fois, vous tomberez sur quelques trucs amusants, pas mal de PC Windows Server 2003 protégés par mots de passe, ou encore les Imac.

Avec de la chance, vous pourrez trouver des bons Windows XP avec une grosse connexion Internet et un beau disque dur tout neuf presque pas entamé et non protégé par quoi que ce soit, et vous pourrez créer un joli Stro :D

Mais gardez à l'esprit que vous ne trouverez pas beaucoup de failles exploitables !

J'espère que ce tuto vous a plu !

TUTO créé par MôûA® (le 28 Août 2006)