Modifier le port 22 utilisé pour les connexions SSH.

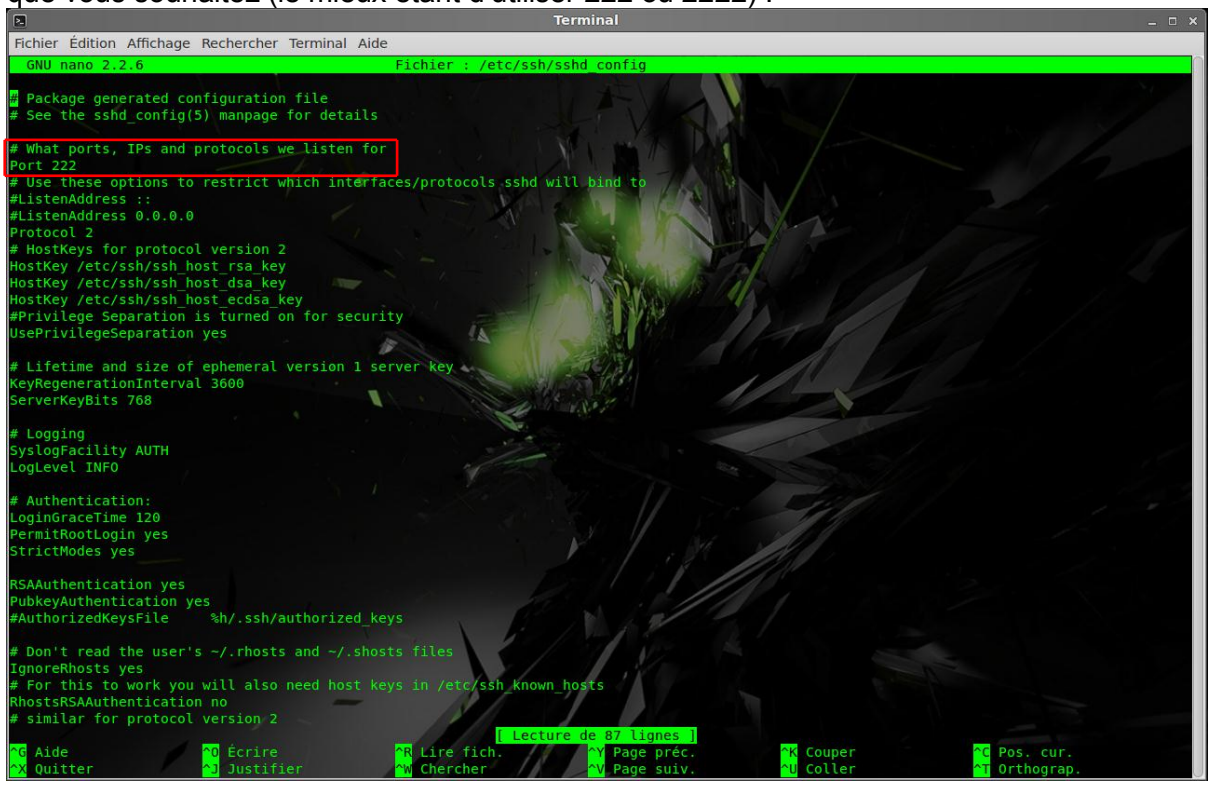
Pré-requis : Logiciel **Putty** présenté précédemment ainsi qu'une machine UNIX.

Présentation du sujet :
Afin de permettre aux clients de se connecter à des serveurs, des numéros de ports logiciels sont utilisés. Les plus connues et les plus importants sont :

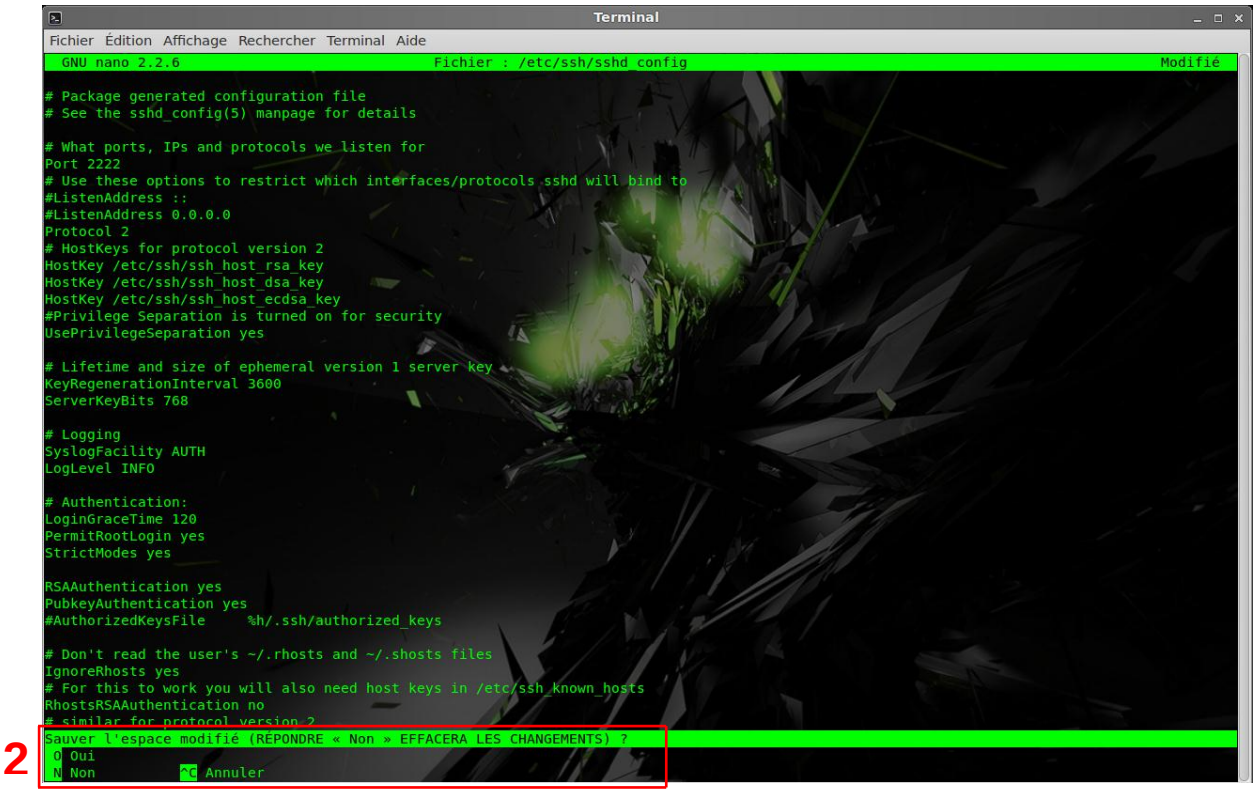
- 80 (**HTTP**)
- 443 (**HTTPs**)
- 22 (**SSH**)
- 20-21 (**Ftp**)
- 23 (**Telnet**)
- 5900 (**VNC Server**)
-

Dans cette procédure, nous allons apprendre à modifier le port 22, utilisé pour des connexions SSH, afin de savoir comment faire pour « sécuriser » ce serveur contre d'éventuelles connexions distantes que nous ne souhaitons pas accepter.

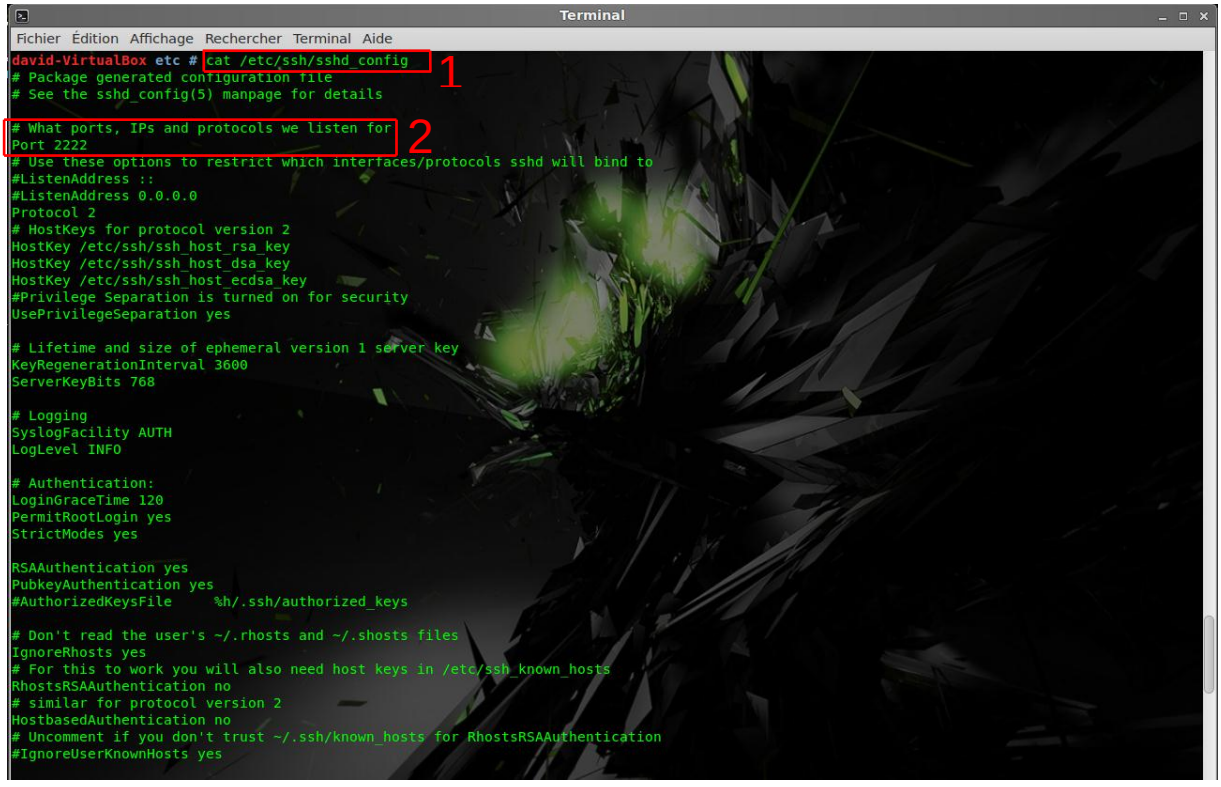
1ère étape : Lancer un terminal, sur votre machine UNIX, puis modifier le ficher sshd_config en tapent : `nano /etc/ssh/sshd_config.`
Une fois que vous êtes dans l'éditeur de texte (nano), changer à la ligne `# What ports, IPs and protocols we listen for` (**1**), le numéro du port par celui que vous souhaitez (le mieux étant d'utiliser 222 ou 2222) :



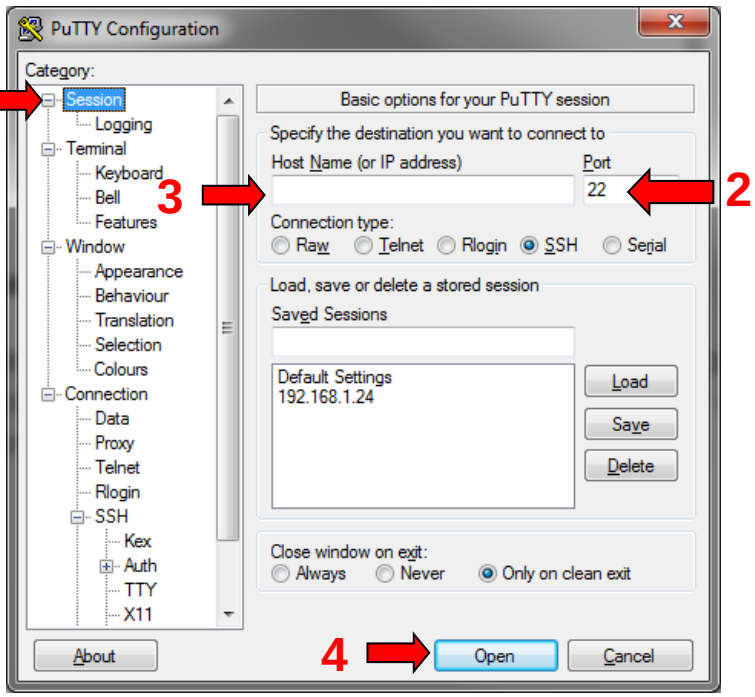
Une fois que vous avez changé le numéro, faite un Ctrl+X puis tapez « Y » ou « O » (**2**) et « Entrer » :



2ème étape : Afin d'être sûr que le port a bien était modifié, tapez : **cat /etc/ssh/sshd_config** (1) puis « Entrer ». Normalement vous devriez voir le port 2222 (2) :



3ème étape : Maintenant que votre port est modifié, il ne vous reste plus qu'à le tester. Ouvrez le logiciel Putty et cliquez sur « Session » (**1**) puis modifier le port par défaut (**2**), en le port que vous venez de changer précédemment. Ensuite entrer l'adresse IP de la machine distante (**3**) puis cliqué sur « Open » (**4**) :



Remarque : Cette procédure peut varier pour les commandes, en fonction des distributions. N'oubliez pas de lancer votre serveur SSH avant de tenter une connexion.