

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 :

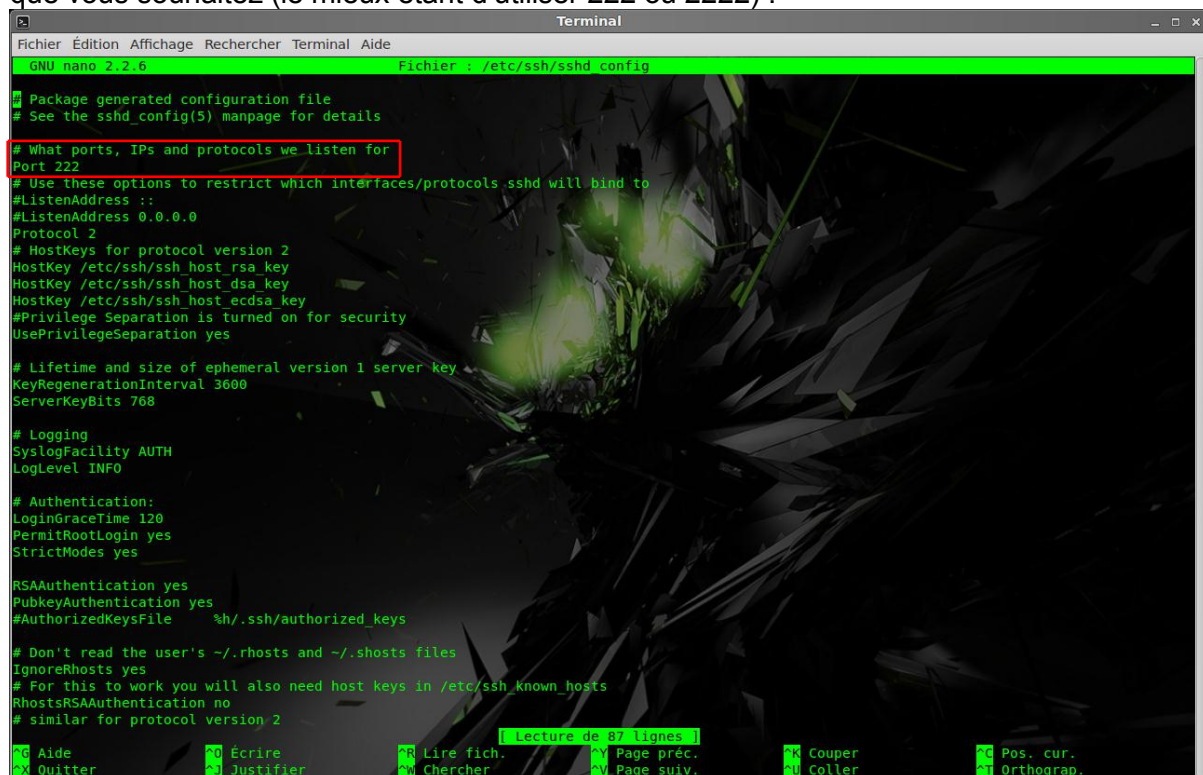
- 80 (**HTTP**)
- 443 (**HTTPS**)
- 22 (**SSH**)
- 20-21 (**Ftp**)
- 23 (**Telnet**)
- 5900 (**VNC Server**)
-

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.

1^{ère} étape : Lancer un terminal, sur votre machine UNIX, puis modifier le fichier `sshd_config` en tapant : `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) :



```
GNU nano 2.2.6 Fichier : /etc/ssh/sshd_config
# Package generated configuration file
# See the sshd_config(5) manpage for details
1 # What ports, IPs and protocols we listen for
  Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile  %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh/known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2

[Ctrl] Aide      [Ctrl] Lire fich.  [Ctrl] Couper      [Ctrl] Pos. cur.
[Ctrl] Quitter  [Ctrl] Justifier   [Ctrl] Chercher    [Ctrl] Page préc.
[Ctrl]          [Ctrl]            [Ctrl]           [Ctrl] Page suiv.
[Ctrl]          [Ctrl]            [Ctrl]           [Ctrl] Coller
[Ctrl]          [Ctrl]            [Ctrl]           [Ctrl] Orthograp.
```

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

```
Terminal
Fichier Edition Affichage Rechercher Terminal Aide
GNU nano 2.2.6 Fichier : /etc/ssh/sshd_config Modifié

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 2222
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# IgnoreUserKnownHosts yes

Sauver l'espace modifié (RÉPONDRE « Non » EFFACERA LES CHANGEMENTS) ?
O Oui
N Non Annuler
```

2

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

```
Terminal
Fichier Edition Affichage Rechercher Terminal Aide
david-VirtualBox etc # cat /etc/ssh/sshd_config 1
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for 2
Port 2222
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

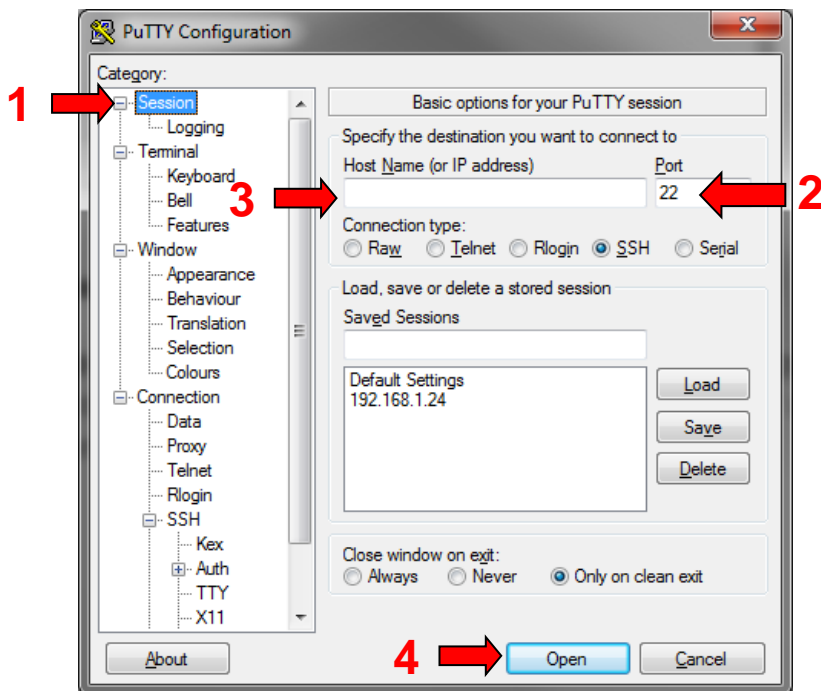
# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# IgnoreUserKnownHosts yes
```

3^{ème} 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.