Les techniques de la télémaintenance

1 . VNC

Virtual Network Computer est un produit gratuit de prise de contrôle à distance;

Sa particularité est de permettre le contrôle de l'interface graphique d'une machine; il est donc plus adapté au contrôle des clients que des serveurs.

Certaines versions compressent les données si bien que le contrôle est possible même avec une connexion internet à 56kbits/s (bas-débit)

Répondre aux questions :

- Quelle est la machine serveur : celle qui contrôle ou celle qui est contrôlée ?
- Quelle est la machine cliente : celle qui contrôle ou celle qui est contrôlée ?
- Quels ports le logiciel VNC utilise-t-il ? _____

Exercice :

- connectez-vous à la machine Linux munie d'une interface graphique et installez le paquets « tightvnc server »
- lancez le serveur avec la commande : vncserver -geometry 800x600
- prenez le contrôle à distance avec un client vnc sur un poste Windows XP
- Quelle règle NAT faut-il créer sur le routeur pour y accéder depuis internet ?

Correction :

2 . OpenSSH

OpenSSH est une implémentation libre du protocole SSH, qui est une version sécurisée de Telnet.

Il permet le contrôle à distance en mode texte.

Il permet aussi de créer des tunnels sécurisés pour des protocoles ciblés (à la différence du VPN)

Installation d'OpenSSH et configuration

Le login : root ou pas root ....

Les systèmes sécurisés refusent la connexion de root; on se connecte donc en « admin » puis on passe un « su »

La charge machine

Pour savoir si un processus s'accapare trop de charge machine (mémoire ou cpu) :
top ou **htop**

note : un processus qui consomme trop est en général un processus qui dysfonctionne (mémoire non-libérée, boucles infinies, ...)

Tuer un processus

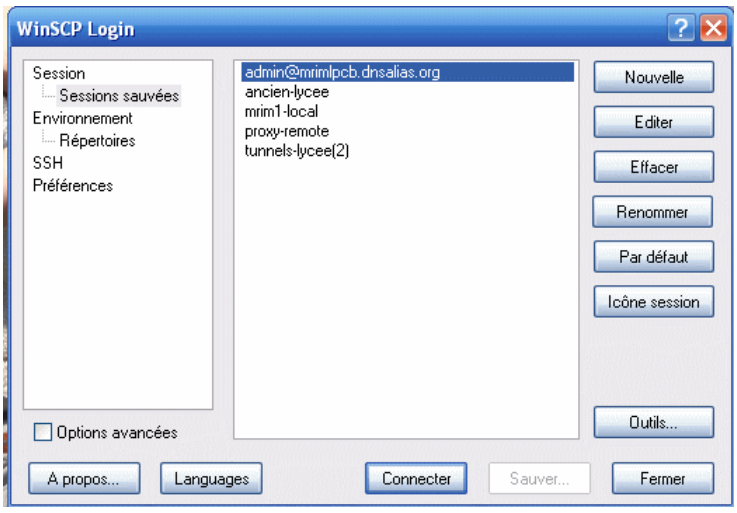
Planté ou bien... :
kill 15674
On refait un *ps ax* pour vérifier qu'il est mort...
S'il est récalcitrant :
kill -9 15674

manipuler les fichiers et répertoires

Exercice : écrire les commandes pour :

Créer un fichier	
Supprimer un fichier	
Changer le propriétaire	
Changer les droits UNIX	

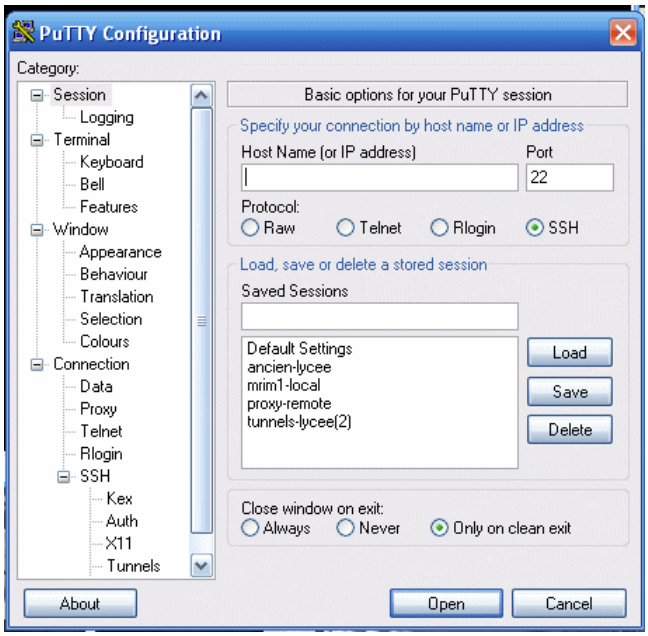
Copie de fichiers depuis ou vers une machine cliente avec Winscp



- ✔ Téléchargez et installez Winscp sur une machine WinXP
- ✔ Créez une « nouvelle » connexion vers le serveur ssh (ex : Scribe)
- ✔ Copier ou télécharger des fichiers vers ce serveur

Conclusion : quel type de service faut-il installer sur le serveur pour y accéder avec Winscp ?

_____



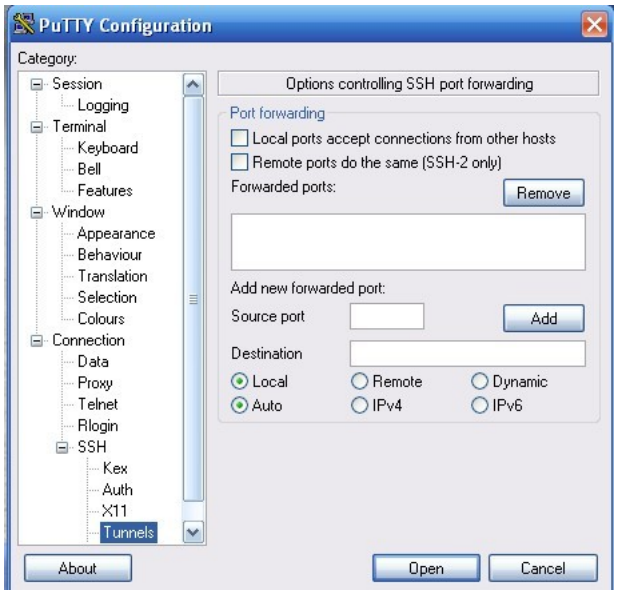
Le tunnel permet d'accéder à l'intérieur du réseau local depuis un accès internet, même si ces machines sont en adressage privé. La fonctionnalité est équivalente à du NAT/PAT, mais ici, tout est crypté et authentifié par défaut.

- ✔ Télécharger et installer Putty sur une machine cliente.
- ✔ Créer une session « test »
- ✔ Host Name : ia2009.dyndns.org
- ✔ Port : 22

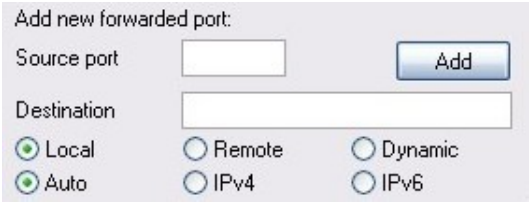
Sauver la session « test »

Exercice : accéder à toutes les ressources du serveur par des tunnels ssh

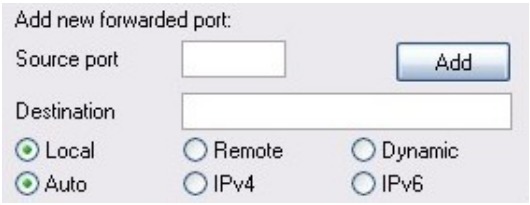
- créer un tunnel vers l'EAD ==========>



- créer un tunnel vers le SSH



- créer un tunnel vers le SPIP-EVA



- sauver la session « test »
- Accéder à ces différentes ressources; expliquez la méthode utilisée :

3. OpenVPN

Vous configurez OpenVPN client sous Windows XP pour vous connecter au serveur VPN;

Voici le fichier de configuration à reproduire :

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
;client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun
ifconfig 192.168.25.2 192.168.25.1

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote mrimlpcb.dnsalias.org 8147
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
#;ca ca.crt
#;cert client.crt
#;key shared.key
secret "c:\\program files\\openvpn\\config\\shared.key"


# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
;ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```