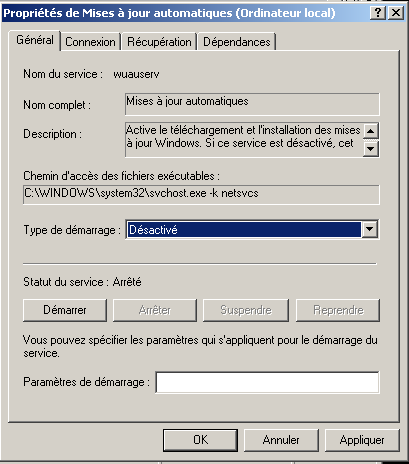
# Paramétrage de Windows XP et configuration de Cuckoo

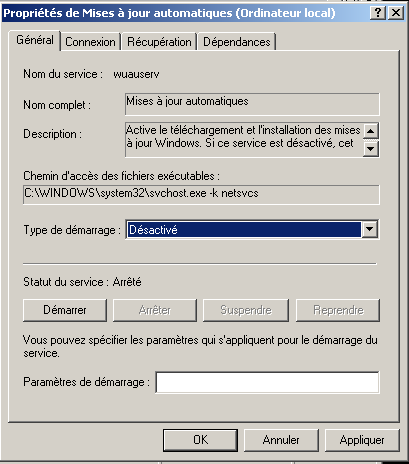
Ajuster windows pour de meilleures performances (désactivation des thèmes graphiques et autres)

Désactivation des infos bulle du centre de sécurité de windows (pas d’antivirus, firewall non configuré).

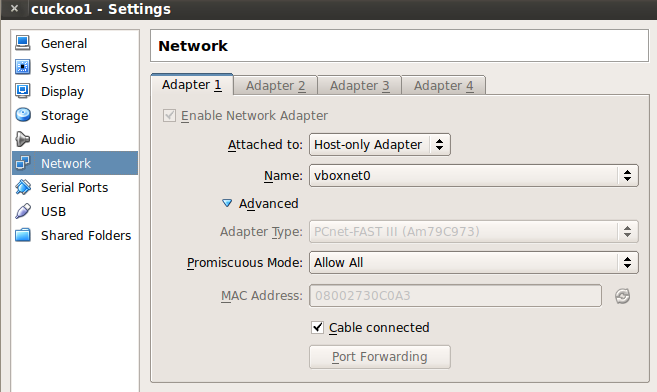
Extinction et désactivation du service windows update pour ne pas sécuriser XP.



Extinction et désactivation du parefeu windows et du partage de connexion internet.



Ajout d’une interface réseau dans Virtualbox « Host-only adapter » nommée par défault vboxnet0 :

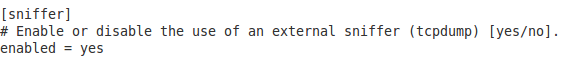


# cuckoo.conf :

Configuration de cuckoo (/opt/cuckoo/cony/cuckoo.conf) pour communiquer avec la VM par cette connexion réseau :

Macintosh HD:Users:Bruno:Desktop:Capture d’écran 2013-03-26 à 15.42.53.png

Ajout d’un sniffer external à la configuration de cuckoo (tcpdump)

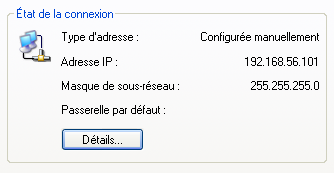


Changement du path de tcpdump de cuckoo par

Macintosh HD:Users:Bruno:Desktop:Capture d’écran 2013-03-26 à 17.51.03.png

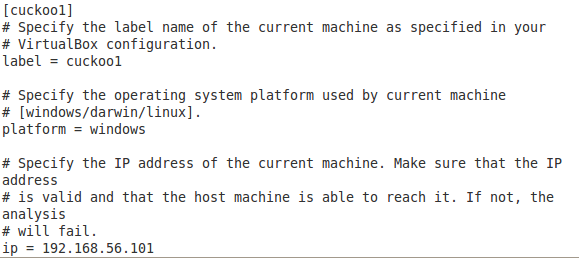
# virtualbox.conf :

Configuration de l’adresse réseau et masque de sous réseau de notre machine XP :



Configuration correspondante de cuckoo (/opt/cuckoo/cony/virtualbox.conf) :

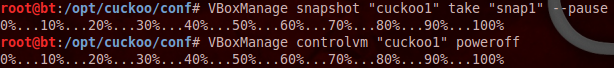
* Nom de la machine virtuelle contenant XP : cuckoo1
* Adresse IP de la machine virtuelle contenant XP : 192.168.56.101



Execution du script agent.py dans la machine XP permettant à Cuckoo de capter les conversations entre la machine guest et la machine hôte.

Maintenant que la machine est prête, nous allons faire une image de restauration de celle-ci à cette instant pour pouvoir que Cukoo puisse la restaurer après avoir fini l’analyse d’un malware.

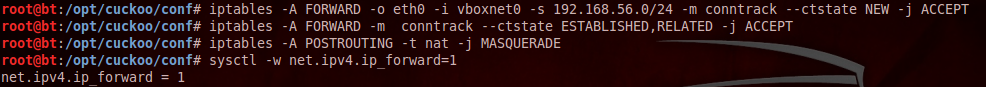
Création d’un snapshot nommé « snap1 » de la machine virtuelle XP pour pouvoir la restaurer après test d’un malware à l’intèrieur :



Test de restauration effectué avec succès :

Macintosh HD:Users:Bruno:Desktop:Capture d’écran 2013-03-26 à 15.41.44.png

Configuration du parefeu iptables dans BT3 :



Paramétrage terminé pour la VM Backtrack R3 ainsi que pour la VM XP contenu dans la VM Backtrack.