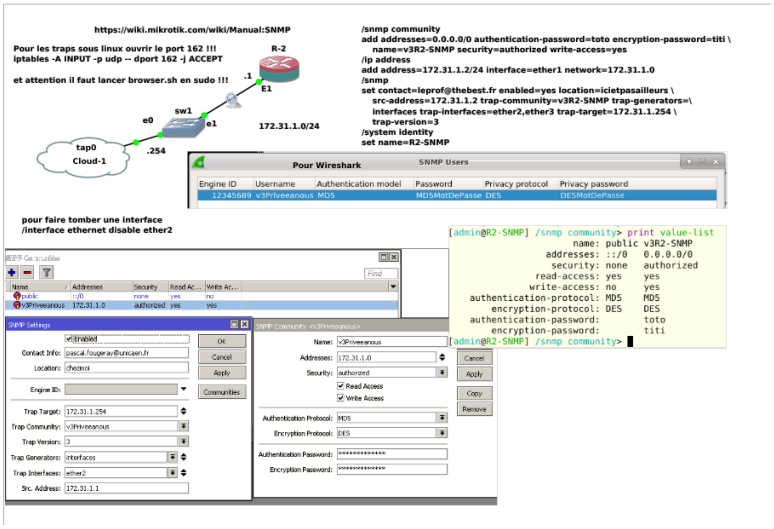
UNIVERSITÉ CAEN NORMANDIE

TP-SNMP

14.03.2023

Pas si simple que cela !☺

Auteur : Pascal Fougeray



1 Introduction

Dans ce TP, je vous propose d'étudier le protocole SNMP aussi bien pour un serveur que pour un routeur.

Remarque : Comme mentionné en CM, il existe plusieurs versions de SNMP !

Je vous impose d'étudier seulement la version v3, la plus compliquée ! mais quand on a compris les principes cela fonctionne.

2 On y va

1. Il faut installer les paquets suivants dans la VM ! ! !

   apt install snmp snmpd snmp snmp-mibs-downloader

   ```
   Paramétrage de snmpd (5.7.3+dfsg-5) ...
   adduser : Attention ! Le répertoire personnel « /var/lib/snmp » n'appartient pas à l'utilisateur que vous êtes en train de créer.
   Created symlink /etc/systemd/system/multi-user.target.wants/snmpd.service → /lib/systemd/system/snmpd.service.
   Traitement des actions différées (« triggers ») pour libc-bin (2.28-10) ...
   Traitement des actions différées (« triggers ») pour systemd (241-7~deb10u1) ...
   Traitement des actions différées (« triggers ») pour man-db (2.8.5-2) ...
   root@debian-10-etu:~#
   ```

   On ne va travailler qu'en V3 et utiliser la version d'essai gratuite 30 jours de ***mibbrowser d'ireasoning***.

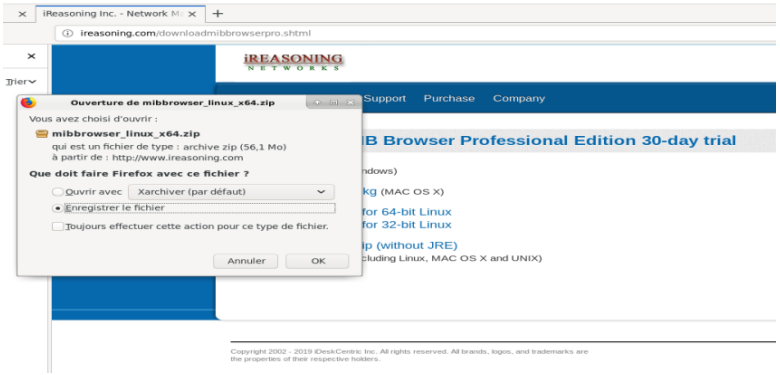
   Facile à installer.

   Attention télécharger la version professionnel pour la V3 ! ! !

   Je rappelle que dans le protocole SNMP tout le monde est serveur et seule l'interface qui interroge les machines est le client. Il fait des requêtes de type SNMP.

2. **Téléchargez** la version 64 bit avec JRE intégrée ! ! !

   http://ireasoning.com/downloadmibbrowserpro.shtml



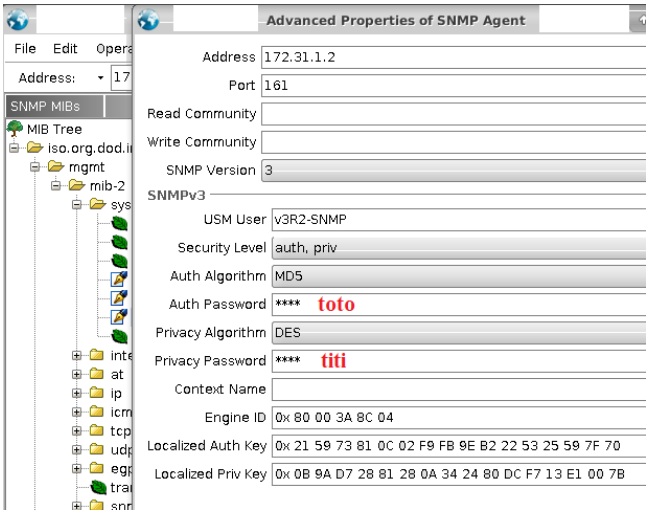
3. **Installez** dans votre répertoire ***home*** !
4. **Lancez** le programme : On verra qu'il faut être root pour les traps ! ! !

```
[2]+  Arrêté                 sudo ./browser.sh
etudiant@ubuntu-gns3:~/ireasoning/mibbrowser$ sudo ./browser.sh
[sudo] Mot de passe de etudiant :
./jre/bin/java
Log file: /home/etudiant/ireasoning/mibbrowser/log/log.txt
1558538680319 [INFO ]  [main] You are using an Evaluation version of iReasoning Product
```

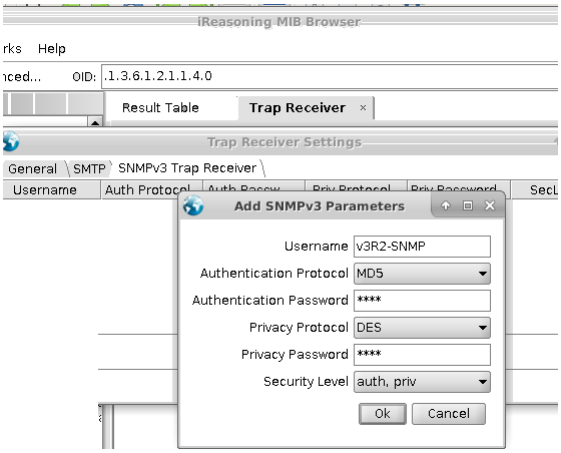
5. **Ouvrez** le projet GNS3 correspondant à SNMP (Voir ecampus !)
6. **Placez** le Cloud permettant de relier le routeur à l'hôte via interface ***tap0*** @IP 172.31.1.254/24 et **testez** la connectivité avec un ping
   Si ce n'est pas fait... Avec les nouvelles versions de GNS3 c'est OK
7. **Lancez** le routeur et **loguez** vous dessus
8. **Vérifiez** qu'il ping la VM : ping 172.31.1.254 je crois ...
9. **Placez** une sonde wireshark entre le routeur et le Cloud et **sélectionnez** le protocole SNMP
10. **Examinez** la conf du router avec la commande ***snmp community print*** et **interprétez la ! ! !**

```
/snmp community
add addresses=0.0.0.0/0 authentication-password=toto encryption-password=titi \
    name=v3R2-SNMP security=authorized write-access=yes
/ip address
add address=172.31.1.2/24 interface=ether1 network=172.31.1.0
/snmp
set contact=leprof@thebest.fr enabled=yes location=icietpasailleurs \
    src-address=172.31.1.2 trap-community=v3R2-SNMP trap-generators=\
    interfaces trap-interfaces=ether2,ether3 trap-target=172.31.1.254 \
    trap-version=3
/system identity
set name=R2-SNMP
[admin@R2-SNMP] >
```

11. **Configurez *mibrowser*** de manière qu'il puisse interroger le routeur. Il faut configurer pour **interroger** et pour les **traps** ! ! !
    (a) **Sélectionnez *Advanced*** et **sélectionnez** v3

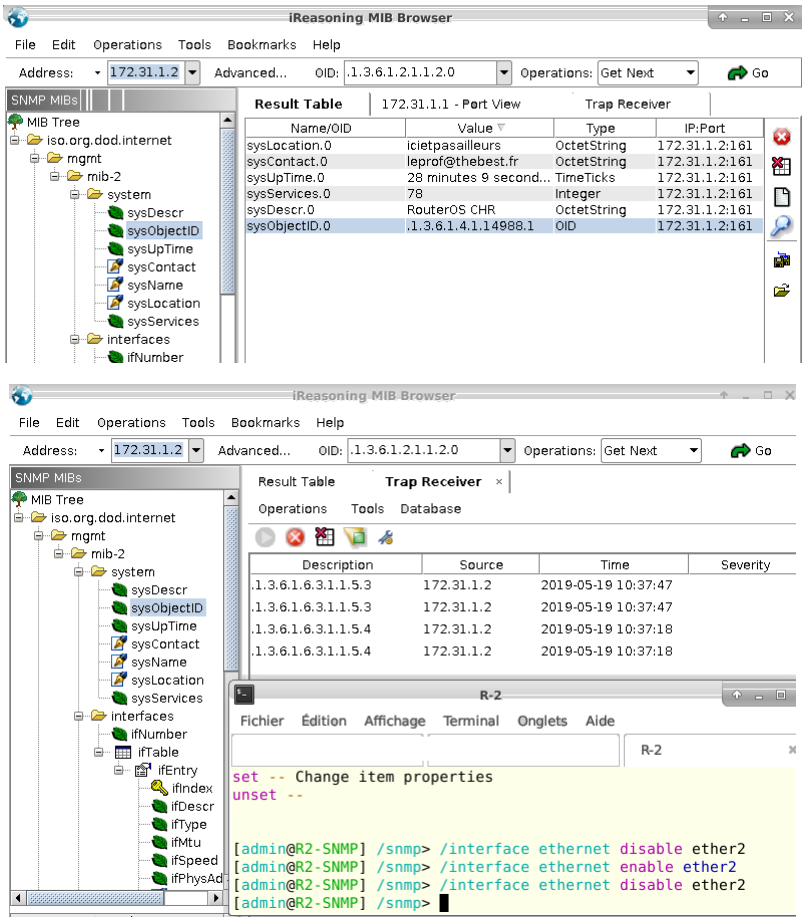


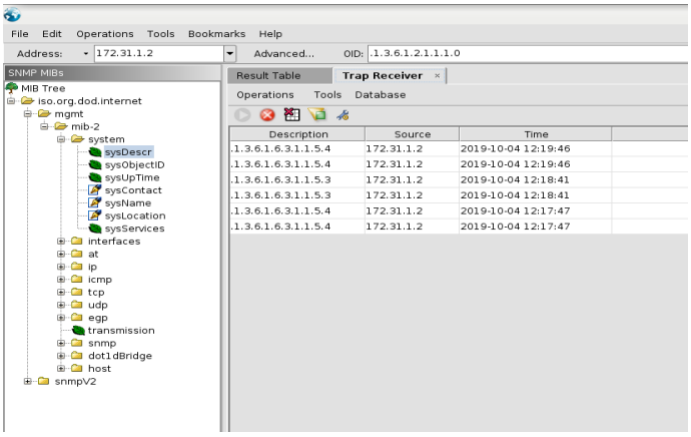
12. Configuration des traps !
    (a) Faire ***tools***, ***trap receiver***, une fenêtre s'ouvre, puis ***tools***, ***option*** et vous obtenez la fenêtre suivante : On configure, **ADD** et **OK**



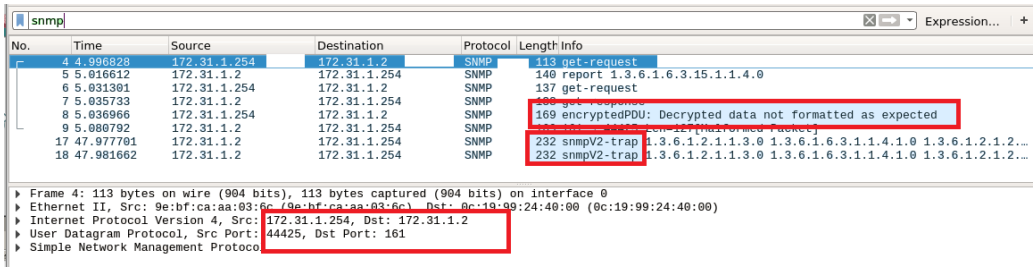
    (b) Et vous devez obtenir l'image suivante

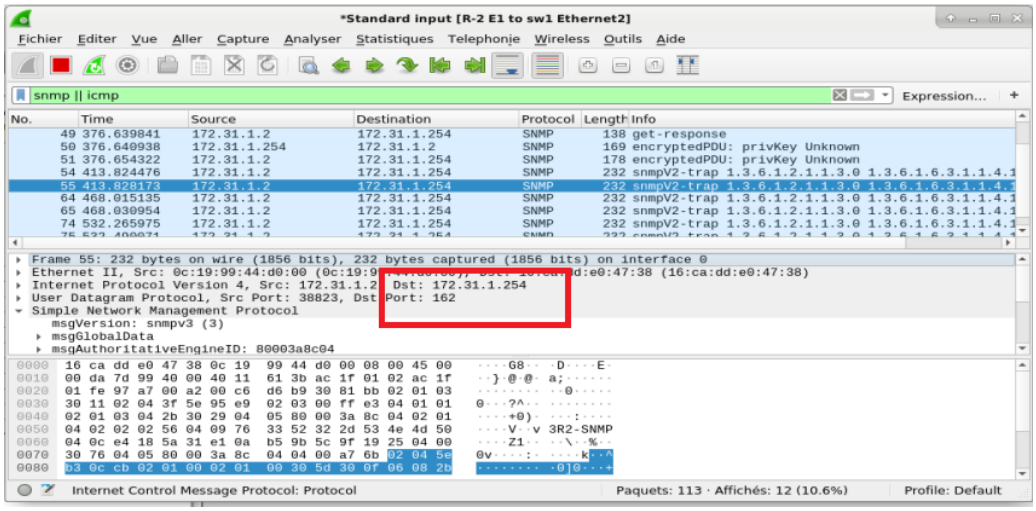
13. **"Jouez"** avec en interrogeant des choses simples comme ci-dessous



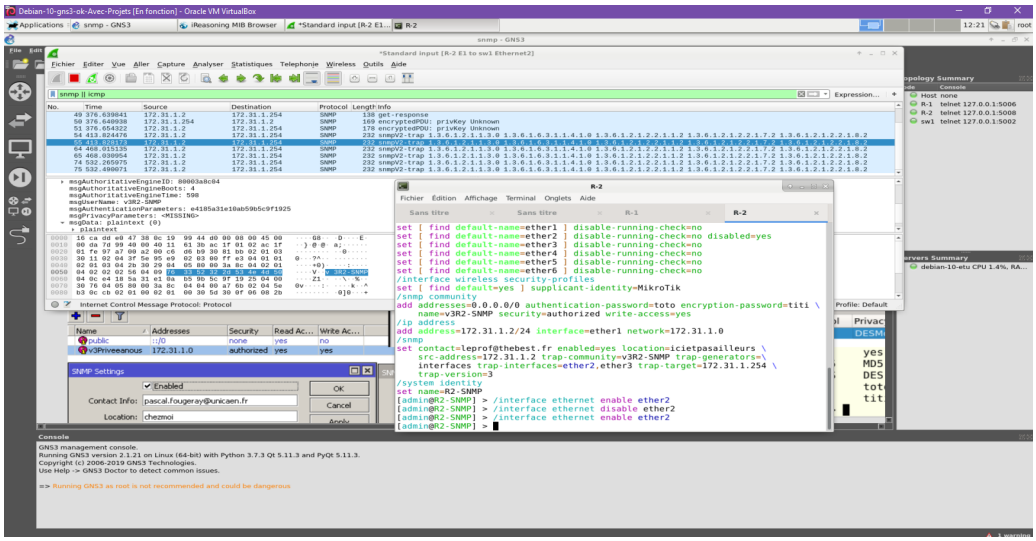


14. **Visualisez** les trames et **examinez** les afin de comprendre le protocole SNMP en v3
    Ici un ***get request*** en v3 et aussi 2 ***traps*** en v3





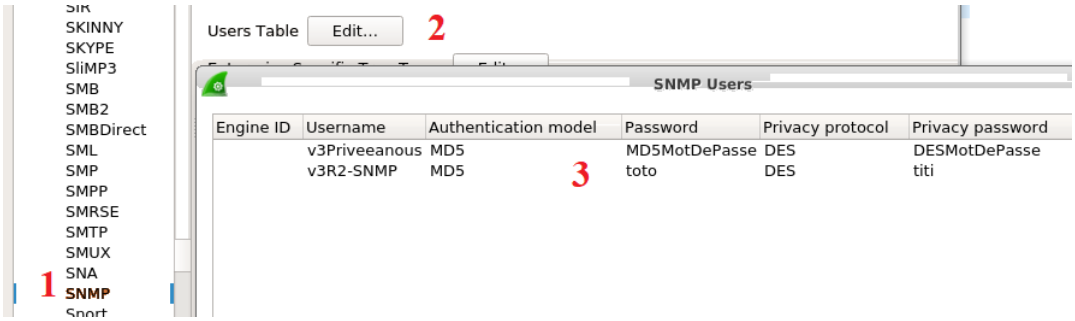
Résultat Final !



15. Si vous avez du temps. Il est possible avec wireshark de déchiffrer les trames chiffrées. (**Man of the Middle**)

    Pour cela on sélectionne une trame chiffrée, ***bouton droit, Protocole Préférence, Users table, Edit, New*** et remplir les champs *User*, DES, *MD5* etc...

    http://robert.penz.name/1215/decoding-snmpv3-encrypted-traffic-in-wireshark/



16. Et vous verrez que les trames sous wireshark sont déchiffrées !
17. **Concluez** sur le protocole SNMP

3 Conclusion

C'est simple SNMP ?
— Qu'est-ce qu'une mib ?
— Pourquoi **snmpd** et **snmp** ?
— Il vaut mieux utiliser la v3 ou la v2 ?