Institut Supérieur de l'Informatique ISI	TP 1: Administration et Sécurité des Réseaux SNMP	A.U.: 2012/2013 Niveau : L3-SIL

I. Rappel:

1. SNMP:

SNMP (Simple Network Management Protocol) est un protocole qui permet aux administrateurs de gérer les équipements et de diagnostiquer les problèmes

Linux implémente un agent SNMP et offre plusieurs commandes Shell pour interagir avec ce dernier.

Les communications SNMP se font via les ports UDP 161 et 162.

L'agent SNMP est géré par deux démons

a. snmpd qui gère les requêtes SNMP sauf les traps (écoute du port 161)
b. snmptrapd qui gère les interruptions SNMP (les traps) (écoute du port 162)

2. OID et MIB:

Un OID (Object Identifier) est une paire clé-valeur unique qui sert à identifier les ressources. C'est un identifiant universel hiérarchique représenté sous la forme d'une suite d'entiers séparés par des points.

Les OID peuvent être longs et compliqués, c'est pour cela qu'une méthodes à été mise au point pour traduire un OID numérique à une forme textuelle, cette traduction est stockée dans un fichier texte appelé MIB (Management Information Base).

3. Authentification:

Un système d'authentification basique existe dans le SNMP; il permet d'envoyer un community name (qui est en fait un mot de passe en clair) pour autoriser la lecture ou l'écriture des OID. La plupart des périphériques utilisent le community name non sécurisé "public".

4. Installation de SNMP:

Installez les packages NET-SNMP et NET-SNMP UTILS qui sont un ensemble d'applications utilisées pour implémenter le protocole SNMP (v1, v2c et v3) .

Il permet aussi l'installation des commandes de base pour interroger l'agent SNMP sous /usr/bin telles que:

- o Rechercher des informations SNMP en employant des demandes simples (snmpget, snmpgetnext), ou des demandes multiples (snmpwalk)
- o Manipuler des informations de configuration sur des périphériques compatibles SNMP (snmpset)
- o Convertir entre les formes numériques et textuelles d'OIDs de MIB et montrer le contenu de MIB et la structure (snmptranslate).

Les outils (snmpget, snmpset, snmpgetnext, snmpwalk, snmptranslate) ont besoin de connaitre:

i. La version de SNMP (-v 1 pour SNMP version 1)
ii. La communauté : qui est en fait un mot de passe en clair
iii. La cible : @IP ou nom de l'agent
iv. La feuille ou le nœud de la MIB à laquelle on s'interese

.

5. **snmpget**
   Elle permet l'envoi d'une requête SNMP GET pour obtenir une information sur un objet de la MIB d'un agent SNMP distant.

   - Récupération par SNMPv1 de la valeur courante de l'objet sysUpTime géré par l'agent SNMP du localhost :

```
# snmpget -v 1 -c public localhost system.sysUpTime.0
```

   - Récupération de la valeur courante de l'objet sysUpTime avec SNMPv2c :

```
# snmpget -v 2c -c public localhost system.sysUpTime.0
```

   - Récupération de la valeur courante des objets sysLocation et sysContact :

```
# snmpget -v 1 -c public localhost system.sysLocation.0
# snmpget -v 1 -c public localhost system.sysContact.0
```

6. **snmpset**
   Elle permet l' envoi d'une requête SNMP SET pour mettre a jour la valeur d'un objet de la MIB d'un agent distant.

   - Affectation d'une nouvelle valeur à sysLocation.0 de la MIB de l'agent avec SNMPv1 :

```
# snmpset -v 1 -c private localhost system.sysLocation.0 s "ISI"
```

   - Affectation d'une nouvelle valeur à sysLocation.0 de la MIB de l'agent avec SNMPv2c :

```
# snmpset -v 2c -c private localhost system.sysLocation.0 s "ISI"
```

7. **snmpgetnext**
   Elle permet l' envoi d'une requête SNMP GETNEXT et donne aussi la valeur de l'objet suivant de la MIB d'un agent SNMP distant si toutefois il en existe un.

8. s**nmpwalk**
   cette commande fonctionne comme snmpgetnext mais permet de balayer complètement une branche de la MIB d'un agent SNMP distant.

   - Parcours de la branche system de la MIB de l'agent SNMP:

```
# snmpwalk -v 1 -c public localhost system
```

9. **snmptranslate**
   Elle permet de convertir un objet d'une MIB représenté sous sa forme décimale OID en sa forme symbolique et réciproquement.
   - Obtention d'une correspondance OID et nom symblique :

```
# snmptranslate 1.3.6.1.2.1.1.3.0
```

- Représentation sous forme graphique de la branche system de la MIB par analyse de l'ensemble des fichiers MIB sous /usr/local/share/snmp/mibs :

```
# snmptranslate -Tp -IR system
```

II. **Manipulation 1 :** Activez l'agent SNMP sous linux en suivant les étapes décrites ci-dessous :

1) Activez ces deux démons en exécutant :
   a. service snmpd start ou /etc/init.d/snmpd start
   b. service snmptrapd start ou /etc/init.d/snmptrapd start
2) Vérifiez que les deux démons sont activés
   a. service snmpd status ou /etc/init.d/snmpd status
   b. service snmptrapd status ou /etc/init.d/snmptrapd status

Information 1:

1) Nous utilisons, dans la manipulation 2 de ce TP, la configuration par défaut déclaré dans /etc/snmp/snmpd.conf. Cette configuration permet uniquement de consulter le groupe system de la MIB.

2) Utilisez le fichier /var/log/snmpd.log pour surveiller les paquets SNMP entrants et sortants.

III. **Manipulation 2 :**

1. Ouvrez un terminal et tapez la commande tail –f /var/log/snmpd.log et consultez ce terminal de temps en temps pour voir les paquets SNMP envoyés et reçus.
2. Où se trouve le fichier snmpd.conf ? et les fichiers des MIBs ?
3. Testez les exemples suivants qui permettent de récupérer le temps depuis lequel l'agent est démarré:
   2) snmpget –v 1 –c public localhost .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0
   3) snmpget –v 1 –c public localhost .1.3.6.1.2.1.1.3.0
   4) snmpget –v 1 –c public localhost system.sysUpTime.0

   Que remarquez vous?

4. La commande snmptranslate permet d'établir la correspondance entre l'OID et le nom du nœud concerné. Quel est l'OID de sysContact ?
5. Affichez l'arbre de la hiérarchie System à l'aide de la commande snmptranslate.
6. Récupérez la description de votre machine à l'aide de snmpget.

Information 2:

Pour pouvoir modifier une valeur d'un objet, il faut que :

- l'objet soit en mode read-write (on peut vérifier à l'aide de la commande "snmptranslate -Td OID")
- Avoir le droit de modifier la MIB: il faut modifier le fichier snmpd.conf et ajouter cette ligne:

  rwcommunity private

  cette commande permet de configurer rapidement et simplement l'accès à l'agent pour les utilisateurs en mode v1 et v2c.

7. A l'aide de la commande snmpset, modifiez le nom de device (sysName)
8. De la même manière, modifiez de la personne chargée « administrativement » de s'occuper de la machine...
9. Modifiez le paramètre sysUpTime de la machine…

Information 3:
On ne peut pas modifier un objet qui a été configuré par le fichier de configuration; c'est le cas de sysContact. Donc, pour modifier cette valeur, on a deux solutions: soit éditer le fichier de configuration et modifié la valeur, soit supprimer l'entrée dans le fichier de configuration.

10. Ecrivez les commandes qui permettent de parcourir le groupe system en utilisant les 2 méthodes : snmpgetnext et snmpwalk.

IV. Manipulation 3 :

1. Testez la commande suivante et expliquer le résultat :
   snmpwalk –v 1 –c public localhost .1.3.6.1.2.1.2.1 (consultation de l'objet ifnumber du groupe interface)

Vous l'avez peut-être remarqué qu'avec la commande snmpwalk précédemment, on n'accède pas par défaut à autre chose qu'au groupe system : cela provient de la configuration de snmpd.
Vous allez donc éditer le fichier de configuration de net-snmp pour autoriser l'accès au sous-arbre .iso.org.dod.internet.mgmt.mib-2.interfaces

2. Modifiez la configuration par défaut en agissant sur /etc/snmp/snmpd.conf. trouvez cette ligne:
   view systemonly included .1.3.6.1.2.1.1
et rajoutez cette ligne juste après:
   view systemonly included .1.3.6.1.2.1.2

   a. Enregistrez le fichier et relancez le démon snmpd
   b. Testez les nouvelles autorisations en consultant des objets
3. De la même manière, trouvez toutes les informations sur l'objet IP (OID: .1.3.6.1.2.1.4)