

# TP 2

## SNMP v1 v2, v3

Rhibi Hamza

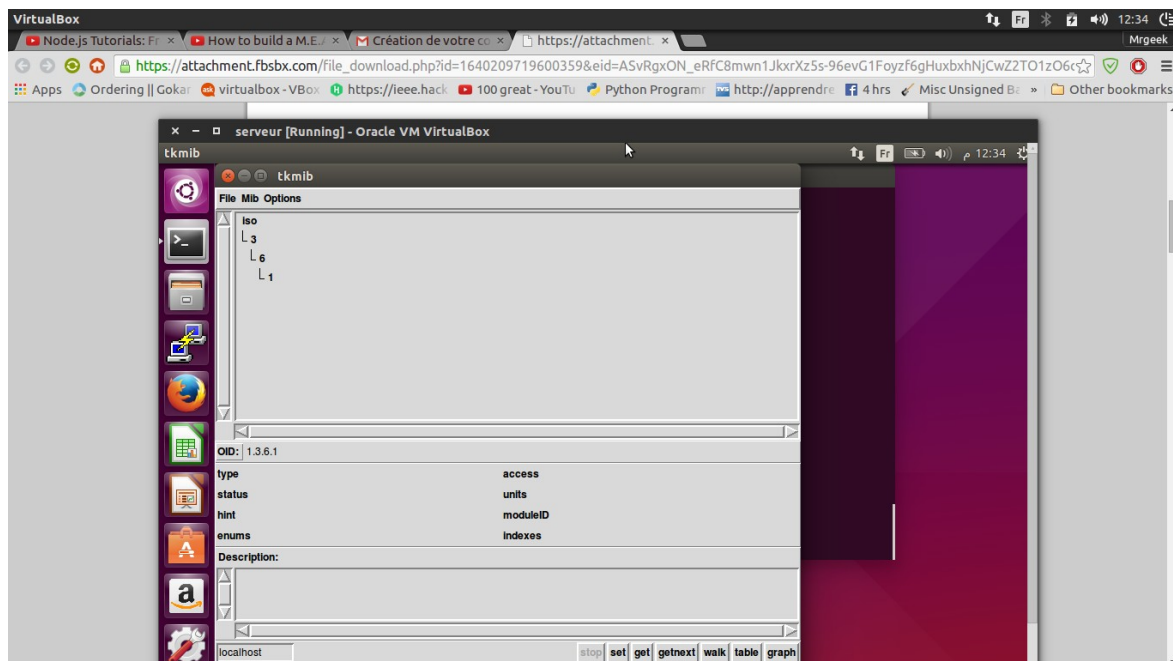
Hammami Firas

Rebhi Adel

### Activité 1 :

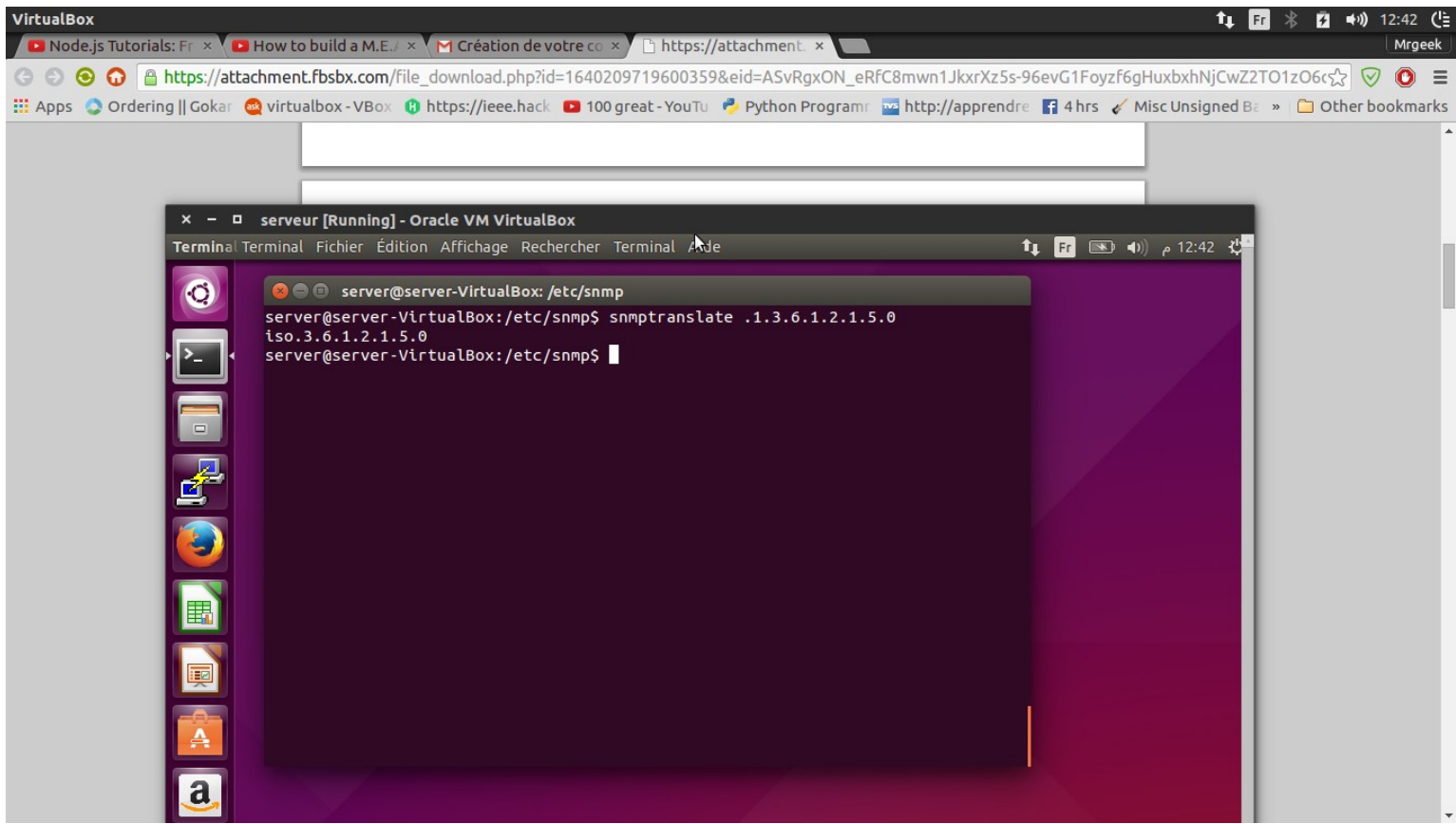
1)

La commande `tkmib` nous permet de voir l'arborescence MIB (Management Information Bases) .



On remarque que les objets sont identifiés par leurs numéros et non pas par leurs nom .

2)



la commande `snmptranslate` donne 1 OID comme resultat

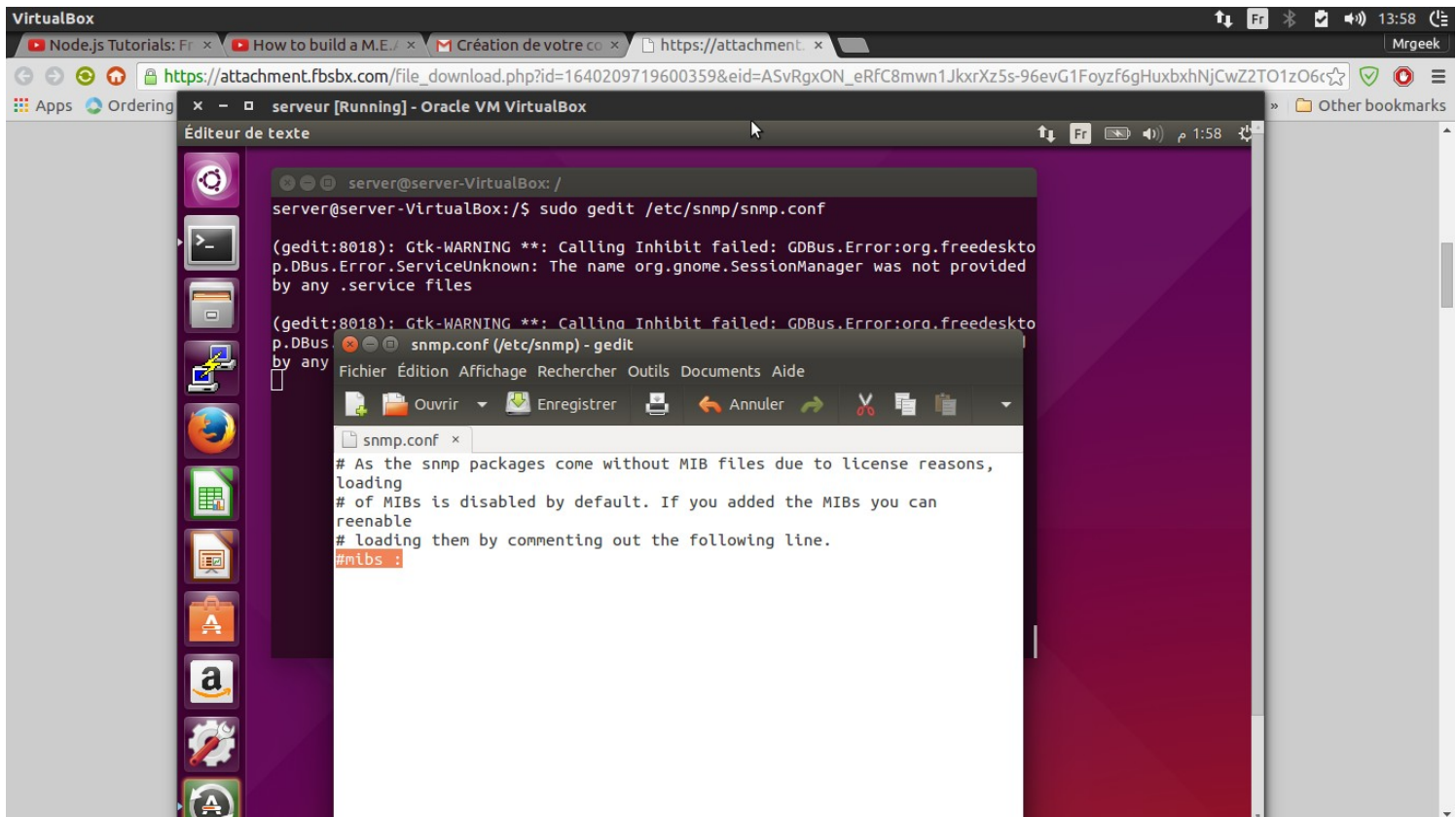
3)

Installation de `snmp-mibs-downloader` résoudre ce problème .

`Apt-get install snmp-mibs-downloader`

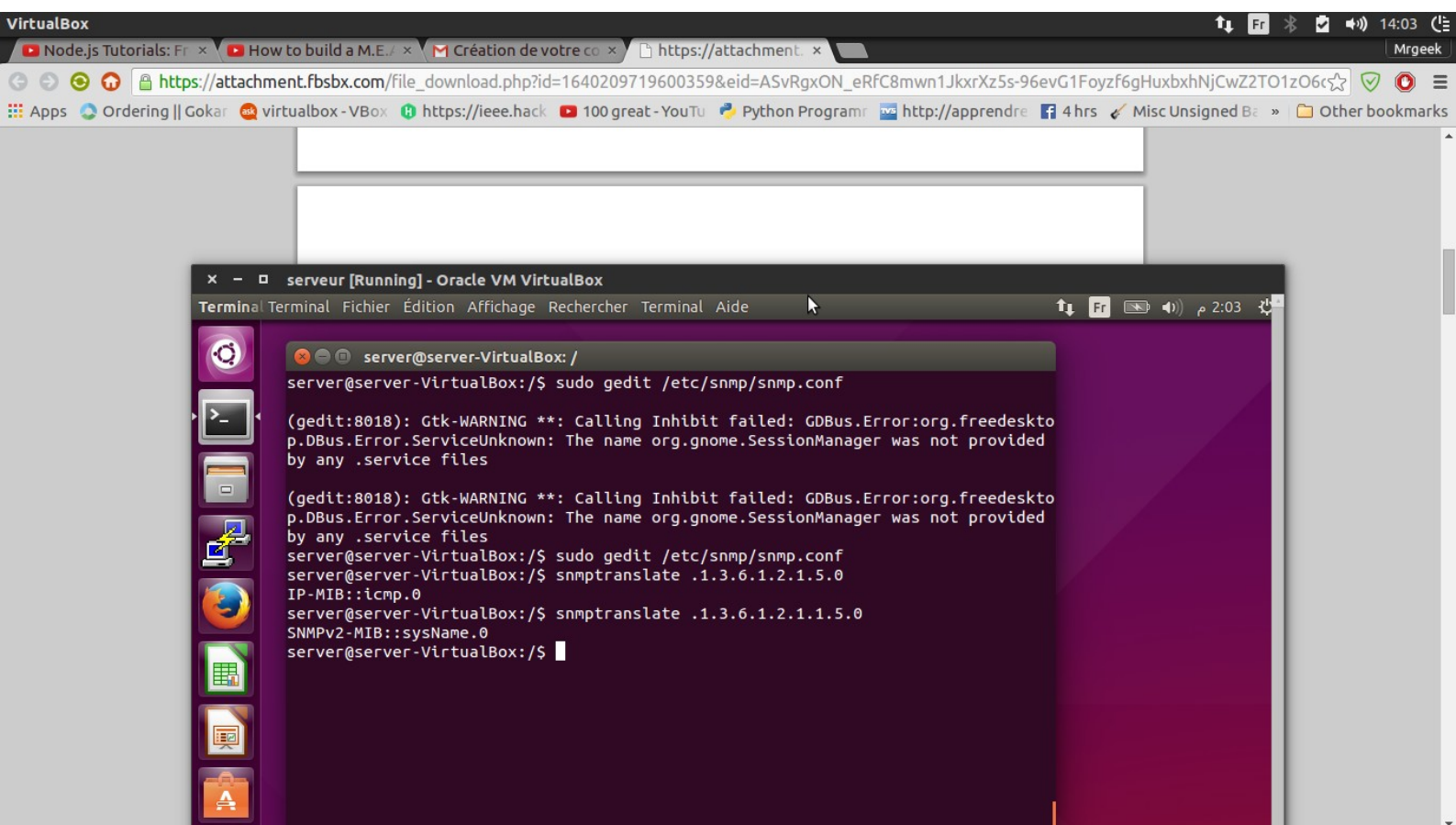
4)

On commente la ligne `mibs` : en ajoutant #



5 )/etc/init.d/snmpd restart

6)



L'OID .1.3.6.1.2.1.1.5.0 correspond au nom du système qui est SNMPv2-MIB

7) l'arborescence de la MIB : tkmib

On remarque que les objets sont maintenant identifiés par leurs nom .

8)



```
serveur [En fonction] - Oracle VM VirtualBox
root@server-VirtualBox: /etc/default

snmp est déjà la plus récente version disponible.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 315 non mis à jour.
root@server-VirtualBox:/etc/default# service snmp start
Failed to start snmp.service: Unit snmp.service failed to load: No such file or directory.
root@server-VirtualBox:/etc/default# /etc/init.d/snmp start
bash: /etc/init.d/snmp: Aucun fichier ou dossier de ce type
root@server-VirtualBox:/etc/default# service snmpd start
root@server-VirtualBox:/etc/default# snmpwalk -c public -v1 127.0.0.1|more
SNMPv2-MIB::sysDescr.0 = STRING: Linux server-VirtualBox 3.19.0-15-generic #15-Ubuntu SMP Thu Apr 16 23:32:01 UTC 2015 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (39171) 0:06:31.71
SNMPv2-MIB::sysContact.0 = STRING: Me <me@example.org>
SNMPv2-MIB::sysName.0 = STRING: server-VirtualBox
SNMPv2-MIB::sysLocation.0 = STRING: Sitting on the Dock of the Bay
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (18) 0:00:00.18
SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.2 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.3 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.9 = STRING: The MIB modules for managing SNMP Notification, plus filtering.
SNMPv2-MIB::sysORDescr.10 = STRING: The MIB module for logging SNMP Notifications.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (14) 0:00:00.14
```

La commande `snmpwalk` permet de sortir sur la console toutes les informations accessibles sur le périphériques.

**-c public** : indique le *community*

**-v1** : indique que l'on utilise le protocole SNMP version 1 (la version du protocole à utiliser dépend du périphérique supervisé).

localhost (127.0.0.1) : indique l'adresse IP du périphérique.

9)

```
root@Geek: ~  
root@Geek:~# snmpget -c public -v1 192.168.1.8 .1.3.6.1.2.1.1.5.0  
Timeout: No Response from 192.168.1.8.  
root@Geek:~#
```

L'application `snmpget` permet d'obtenir l'information concernant un OID précis.

Cette commande nous permet de récupérer le nom de la machine mais on a pas pu le récupérer pour la raison suivante : `Timeout: No response from 192.168.0.107` .

10)

on commenté la ligne `agentAdress udp:127.0.0.1:161` qui permet d'écouter seulement les périphériques dans le système local et on a commenté la ligne `agentAdress udp:161,udp6:[::1]:161` qui nous permet d'écouter les périphériques dans le réseau.

La commande maintenant fonctionne et on a pu récupérer le nom du périphérique qui est `ubuntu` et de type `string`.

```
snmpd.conf (/etc/snmp) - gedit
File Edit View Search Tools Documents Help
+ Open Save Undo
snmpd.conf x
#####
#
# EXAMPLE.conf:
# An example configuration file for configuring the Net-SNMP agent ('snmpd')
# See the 'snmpd.conf(5)' man page for details
#
# Some entries are deliberately commented out, and will need to be explicitly activated
#
#####
# AGENT BEHAVIOUR
#
# Listen for connections from the local system only
#agentAddress udp:127.0.0.1:161
# Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161

#####
#
# SNMPv3 AUTHENTICATION
#
# Note that these particular settings don't actually belong here.
# They should be copied to the file /var/lib/snmp/snmpd.conf
# and the passwords changed before being uncommented in that file *only*

root@Geek:~
root@Geek:~# snmpget -c public -v1 192.168.1.8 .1.3.6.1.2.1.1.5.0
Timeout: No Response from 192.168.1.8.
root@Geek:~# snmpget -c public -v1 192.168.1.8 .1.3.6.1.2.1.1.5.0
SNMPv2-MIB::sysName.0 = STRING: server-VirtualBox
root@Geek:~# snmpget -c public -v1 192.168.1.8 .1.3.6.1.2.1.1.5.0
SNMPv2-MIB::sysName.0 = STRING: server-VirtualBox
root@Geek:~#
```

```
root@Geek: ~
root@Geek:~# snmpset -c public -v1 10.42.0.125 .1.3.6.1.2.1.1.5.0 s "machinehamza"
SNMPv2-MIB::sysName.0 = STRING: machinehamza
root@Geek:~#
```

Capturing from any [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

21:39

Filter: **snmp** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
2001	3.947628000	10.42.0.1	10.42.0.125	SNMP	99	set-request 1.3.6.1.2.1.1.5.0
2002	3.949240000	10.42.0.125	10.42.0.1	SNMP	99	get-response 1.3.6.1.2.1.1.5.0

Frame 2001: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface 0  
Linux cooked capture  
Internet Protocol Version 4, Src: 10.42.0.1 (10.42.0.1), Dst: 10.42.0.125 (10.42.0.125)  
User Datagram Protocol, Src Port: 45734 (45734), Dst Port: 161 (161)  
Simple Network Management Protocol

0000 00 04 00 01 00 06 84 4b f5 61 ec 5b 2a 5d 08 00 .....K .a.[\*]..  
0010 45 00 00 53 fe 78 40 00 40 11 27 50 0a 2a 00 01 E..S.x@. @.'P.\*..  
0020 0a 2a 00 7d b2 a6 00 a1 00 3f 6f 66 30 35 02 01 .\*).....?of05..  
0030 00 04 06 70 75 62 6c 69 63 a3 28 02 04 6e 46 4c ...publi c(..nFL  
0040 15 02 01 00 02 01 00 30 1a 30 18 06 08 2b 06 01 .....0 .0...+..  
0050 02 01 01 05 00 04 0c 6d 61 63 68 69 6e 65 68 61 .....m achineha  
0060 6d 7a 61 mza

any: <live capture in progress> ... Packets: 5173 · Displayed: 2 (0.0%) Profile: Default

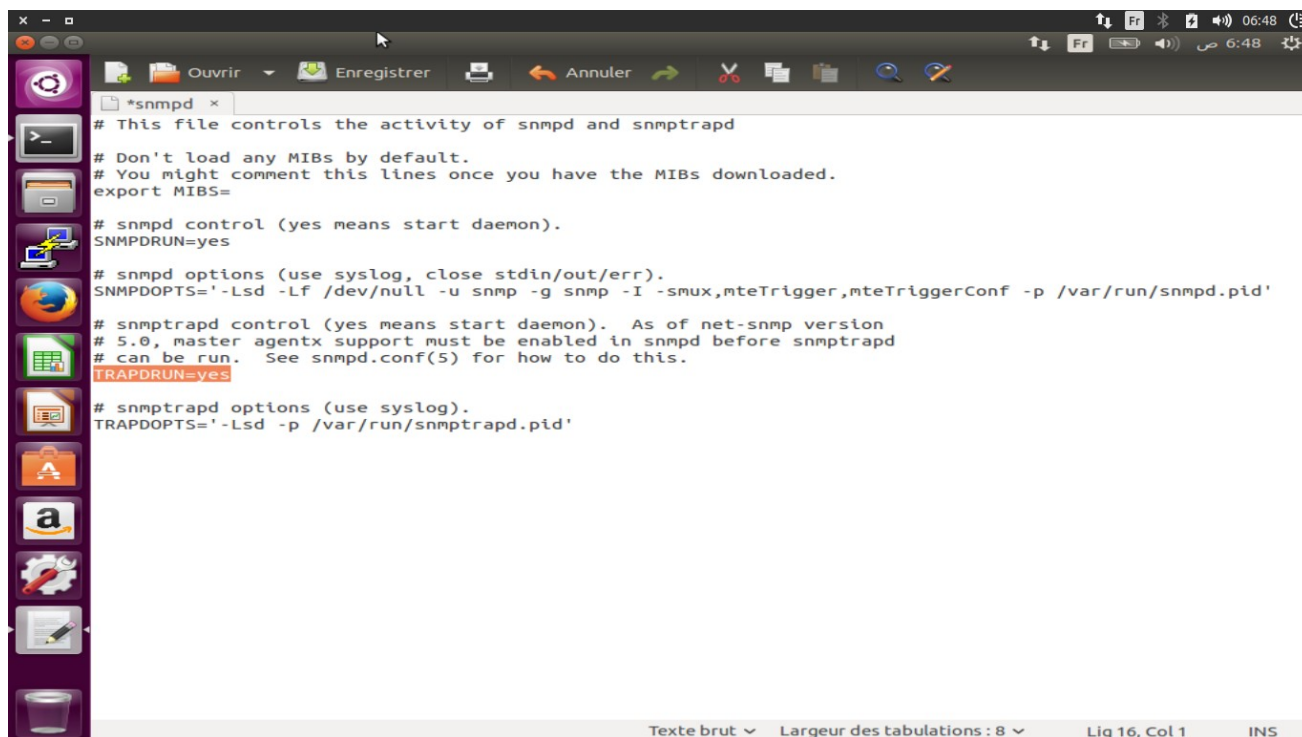
view systemonly included .1.3.6.1.2.1.25.1

```
the local host # Full access from
#rocommunity public localhost # Default access to
basic system info # Full access from
rocommunity public default -V systemonly # Adjust this
an example network # settings,
network address to match your local
change the community string,
```

Matlab ▾ Largeur des tabulations: 8 ▾ Lig 43, Col 1 INS

```
(gedit:3539): GLib-GIO-CRITICAL **: g_dbus_connection_get_unique_name: assertion 'G_IS_DBUS_CONNECTION (co
nnexion)' failed
(gedit:3539): dconf-WARNING **: failed to commit changes to dconf: La connexion est fermée
(gedit:3539): dconf-WARNING **: failed to commit changes to dconf: La connexion est fermée
(gedit:3539): dconf-WARNING **: failed to commit changes to dconf: La connexion est fermée
** (gedit:3539): CRITICAL **: Unable to connect to Zeitgeist's DataSourceRegistry: La connexion est fermée
```





```
# This file controls the activity of snmpd and snmptrapd

# Don't load any MIBs by default.
# You might comment this lines once you have the MIBs downloaded.
export MIBS=

# snmpd control (yes means start daemon).
SNMPDRUN=yes

# snmpd options (use syslog, close stdin/out/err).
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux,mteTrigger,mteTriggerConf -p /var/run/snmpd.pid'

# snmptrapd control (yes means start daemon). As of net-snmp version
# 5.0, master agentx support must be enabled in snmpd before snmptrapd
# can be run. See snmpd.conf(5) for how to do this.
TRAPDRUN=yes

# snmptrapd options (use syslog).
TRAPDOPTS='-Lsd -p /var/run/snmptrapd.pid'
```

2)

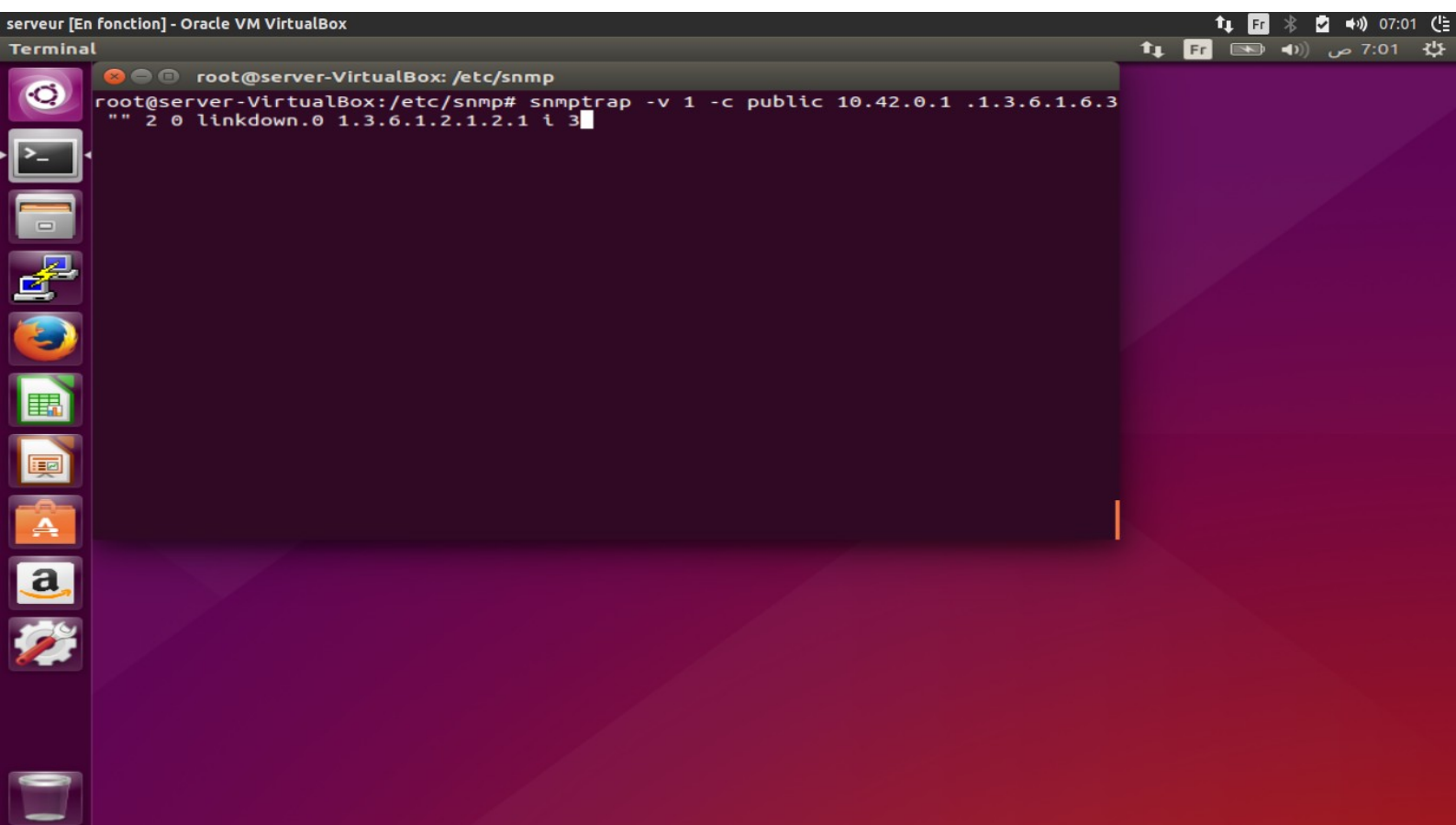


```
snmptrapd.conf x
authCommunity log,execute,net public
```

On ajoute cette ligne dans le fichier /etc/snmp/snmptrapd.conf pour autorisé au service snmpdtrapd d'accepter les trap .

3) Redémarrage du service snmpd avec la commande /etc/init.d/snmpd restart pour que les modifications soient prises en charge .

4) Alerter (trap) le manager que l'interface numéro 3 est désactivé ou dysfonctionné.



5)cat /var/log/syslog|grep snmptrap n a pas affichier de resultat

6)

Capturing from any [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

Filter: **snmp** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
555	402.91475506	10.42.0.125	10.42.0.1	SNMP	97	trap iso.3.6.1.6.3 1.3.6.1.2.1.2.1

▶ Frame 555: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0  
 ▶ Linux cooked capture  
 ▶ Internet Protocol Version 4, Src: 10.42.0.125 (10.42.0.125), Dst: 10.42.0.1 (10.42.0.1)  
 ▶ User Datagram Protocol, Src Port: 40644 (40644), Dst Port: 162 (162)  
 ▶ Simple Network Management Protocol

```

0000  00 00 00 01 00 06 08 00 27 f7 c0 ec 00 00 08 00  ..... '.....
0010  45 00 00 51 80 97 40 00 40 11 a5 33 0a 2a 00 7d  E..Q..@. @..3.*.}
0020  0a 2a 00 01 9e c4 00 a2 00 3d d2 a9 30 33 02 01  .*..... .=..03..
0030  00 04 06 70 75 62 6c 69 63 a4 26 06 05 2b 06 01  ..publi c.&...+..
0040  06 03 40 04 0a 2a 00 7d 02 01 02 02 01 00 43 01  ..@..*.) .....C.
0050  00 30 0e 30 0c 06 07 2b 06 01 02 01 02 01 02 01  .0.0...+ .....
0060  03
  
```

any: <live capture in progress> ... Packets: 564 · Displayed: 1 (0.2%) Profile: Default

## Activité 3 :

1)

```
*snmpd.conf (/etc/snmp) - gedit
File Edit View Search Tools Documents Help

*snmpd.conf x
#
# SNMPv3 AUTHENTICATION
#
# Note that these particular settings don't actually belong here.
# They should be copied to the file /var/lib/snmp/snmpd.conf
# and the passwords changed, before being uncommented in that file *only*.
# Then restart the agent

createUser hamza1
createUser hamza2 MD5 hamza2pass
createUser hamza3 MD5 hamza2pass DES hamza2encryption

# If you also change the usernames (which might be sensible),
# then remember to update the other occurrences in this example config file to match.

#####
#
# ACCESS CONTROL
#

view systemonly included .1.3.6.1.2.1.1 # system + hrSystem groups only
view systemonly included .1.3.6.1.2.1.25.1

rocommunity public localhost # Full access from the local host
rocommunity public default -V systemonly # Default access to basic system info

# Full access from an example network
# Adjust this network address to match your local
# settings, change the community string,
```

2)

```
*snmpd.conf (/etc/snmp) - gedit
File Edit View Search Tools Documents Help

snmpd.conf x
# Note that these particular settings don't actually belong here.
# They should be copied to the file /var/lib/snmp/snmpd.conf
# and the passwords changed, before being uncommented in that file *only*.
# Then restart the agent

createUser hamza1
createUser hamza2 MD5 hamza2pass
createUser hamza3 MD5 hamza2pass DES hamza2encryption
rouser hamza1 noauth 1.3.6.1.2.1.1
rouser hamza2 auth 1.3.6.1.2.1
rouser hamza3 priv 1.3.6.1.2.1

# If you also change the usernames (which might be sensible),
# then remember to update the other occurrences in this example config file to match.

#####
#
# ACCESS CONTROL
#

view systemonly included .1.3.6.1.2.1.1 # system + hrSystem groups only
view systemonly included .1.3.6.1.2.1.25.1

rocommunity public localhost # Full access from the local host
rocommunity public default -V systemonly # Default access to basic system info

# Full access from an example network
```

rouser hamza1 noauth 1.3.6.1.2.1.1 : utilisateur hamza1  
peut seulement lire le nom de la machine , Aucune authentification  
et aucun chiffrement requis.

rouser hamza2 auth 1.3.6.1.2.1 : utilisateur hamza2 peut seulement lire le nom de la machine , Authentification et pas de chiffrement .

rwuser hamza3 priv 1.3.6.1.2.1 : utilisateur hamza3 peut lire et écrire sur l'OID 1.3.6.1.2.1.1 , Authentification et chiffrement des données requis.

3)

```
geekhamza@Geek: /etc/asterisk
geekhamza@Geek:/etc/asterisk$ snmpget -v3 -u hamza1 192.168.1.6 .1.3.6.1.2.1.1.5.0
SNMPV2-MIB::sysName.0 = STRING: machinehanza
geekhamza@Geek:/etc/asterisk$
```

L'utilisateur hamza1 peut récupérer le nom de la machine sans l'authentification .

4)



```
geekhamza@Geek: /etc/asterisk
geekhamza@Geek:/etc/asterisk$ snmpget -v3 -u hamza1 192.168.1.6 .1.3.6.1.2.1.2.1.0
IF-MIB::ifNumber.0 = No Such Object available on this agent at this OID
geekhamza@Geek:/etc/asterisk$
```

L'utilisateur hamza1 n'a pas le droit d'afficher le numéro d'interface à travers l'OID .1.3.6.1.2.1.2.1.0 car il a aucune permission pour ce OID (il peut seulement lire depuis L'OID 1.3.6.1.2.1.1)

5)

```
geekhamza@Geek: /etc/asterisk
geekhamza@Geek:/etc/asterisk$ snmpget -v3 -u hamza2 -l NoauthNoPriv 192.168.1.6 .1.3.6.1.2.1.1.0
Error in packet
Reason: authorizationError (access denied to that object)
geekhamza@Geek:/etc/asterisk$
```

L'utilisateur hamza2 n'a pas le droit d'afficher le numéro d'interface car il doit être authentifié.

Il peut lire depuis L'OID 1.3.6.1.2.1.1.1.0 mais il doit être authentifié .L'argument -l est le paramètre de securityLevel ,on utilisé NoauthNoPriv qui veut dire pas d'authentification et pas de chiffrement .

6)

```
geekhamza@Geek: /etc/asterisk
geekhamza@Geek:/etc/asterisk$ snmpget -v3 -u hamza2 -l authNoPriv -a MD5 -A "hamza2pass" 192.168.1.6 .1.3.6.1.2.1.2.1.0
IF-MIB::ifNumber.0 = INTEGER: 2
geekhamza@Geek:/etc/asterisk$
```

**-v 3** : indique que l'on utilise le protocole SNMP version 3

**-u hamza2** : indique le nom de l'utilisateur

**-l authNoPriv** : le niveau de sécurité utilisé ,il y a 3 types :

noAuthNoPriv : pas d'authentification de l'utilisateur et pas de chiffrement des données.

authNoPriv : authentification de l'utilisateur mais de chiffrement des données (notre cas).

authPriv : authentification de l'utilisateur et chiffrement des données .

**-a MD5** : définir le type d'authentification ,MD5 ou SHA .

**-A "noor2pass"** : pour donner le PASSPHRASE

**192.168.153.139** : indique l'adresse ip du périphérique

**1.3.6.1.2.1.1.1.0** : OID correspondant à le numéro d'interface

