MONITOR YOUR INFRA

Nicolas Vadkerti Quentin Risdorfer

9 décembre 2019

https://github.com/SlaynPool/CR_MONITOR_YOUR_INFRA

1 Utilisation de SNMP comme vecteur de monitoring

1.1 Installez le client SNMP sous Linux

```
apt-get update
apt-get install snmp snmp-mibs-downloader
#Remplacez la ligne dans /etc/snmp/snmp.conf par
mibs +ALL
# Remplacer la mib qui genere une erreur ( dangereux ne pas faire en prod) :
wget http://pastebin.com/raw.php?i=p3QyuXzZ -O /usr/share/snmp/mibs/ietf/SNMPv2-PDU
```

Listing 1 – Installation d'un Client

```
# Pour recuperer Les OID de registry.iutbeziers.fr
snmpwalk  -v  2c -c publicbeziers registry.iutbeziers.fr
SNMPv2-MIB::sysDescr.0 = STRING: Linux registry 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2
    (2018-10-27) x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1320059745) 152 days, 18:49:57.45
SNMPv2-MIB::sysContact.0 = STRING: Moa  <jean-marc.pouchoulon@iutbeziers.fr>
SNMPv2-MIB::sysName.0 = STRING: registry
SNMPv2-MIB::sysLocation.0 = STRING: iutbeziers

# Pour  le switch :
[slaynpool@MiniZbeub]~$ snmpwalk  -v  2c -c publicbeziers 10.255.255.253
SNMPv2-MIB::sysDescr.0 = STRING: HP Comware Platform Software, Software Version 5.20.99
    Release 2220P09
HP A5500-24G EI Switch with 2 Interface Slots
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.25506.11.1.24


# Pour L'ad (Oui c'est la mauvaise communate )

[slaynpool@MiniZbeub]~$ snmpwalk  -v  2c -c public 10.6.0.1
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 4 Stepping 3 AT/AT
    COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (2020700073) 233 days, 21:03:20.73
SNMPv2-MIB::sysContact.0 = STRING: M. Duban
SNMPv2-MIB::sysName.0 = STRING: SERVER-RT
SNMPv2-MIB::sysLocation.0 = STRING: Salle des serveurs
SNMPv2-MIB::sysServices.0 = INTEGER: 78
IF-MIB::ifNumber.0 = INTEGER: 3
```

Listing 2 – Test d'interogation

Pour Autoriser les connections de l'exterieur, il faut :

```
#  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



systemctl restart snmpd
```

Listing 3 – snmpd.conf

2 Utilisez le client SNMP afin de visualiser les informations des machineslistées dans le "terrain de jeux"

2.1 Interrogation via SNMP du serveur ayant pour IP 10.6.0.1.

2.1.1 Dumper l'ensemble des informations du serveur distant via un snmpwalk

```
[slaynpool@MiniZbeub]~$ snmpwalk  -v  2c -c public 10.6.0.1
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 4 Stepping 3 AT/AT
    COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (2020868420) 233 days, 21:31:24.20
SNMPv2-MIB::sysContact.0 = STRING: M. Duban
SNMPv2-MIB::sysName.0 = STRING: SERVER-RT
SNMPv2-MIB::sysLocation.0 = STRING: Salle des serveurs
SNMPv2-MIB::sysServices.0 = INTEGER: 78
IF-MIB::ifNumber.0 = INTEGER: 3
```

Listing 4 – snmpwalk

2.1.2 Retrouver le système d'exploitation de la machine via un snmpget.

```
# snmpget  -v  2c -c public 10.6.0.1 sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 4 Stepping 3 AT/AT
    COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
```

Listing 5 – snmpget

2.1.3 Afficher l'arbre system de la mib à l'aide de la commande

```
[slaynpool@MiniZbeub]~$ snmptranslate -On -Tp SNMPv2-MIB::system
+--system(1)
   |
   +-- -R-- String    sysDescr(1)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -R-- ObjID     sysObjectID(2)
   +-- -R-- TimeTicks sysUpTime(3)
   |  |
   |  +--sysUpTimeInstance(0)
   |
   +-- -RW- String    sysContact(4)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -RW- String    sysName(5)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -RW- String    sysLocation(6)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -R-- INTEGER   sysServices(7)
   |        Range: 0..127
   +-- -R-- TimeTicks sysORLastChange(8)
   |        Textual Convention: TimeStamp
   |
   +--sysORTable(9)
      |
      +--sysOREntry(1)
         |  Index: sysORIndex
         |
         +-- ---- INTEGER   sysORIndex(1)
         |        Range: 1..2147483647
         +-- -R-- ObjID     sysORID(2)
         +-- -R-- String    sysORDescr(3)
         |        Textual Convention: DisplayString
         |        Size: 0..255
         +-- -R-- TimeTicks sysORUpTime(4)
                  Textual Convention: TimeStamp
```

Listing 6 – Arbre de la mib SNMPv2

2.1.4 Traduisez en oid SNMPv2-MIB : :system et réciproquement

```
[slaynpool@MiniZbeub]~$   snmptranslate -Ot .1.3.6.1.2.1.1
SNMPv2-MIB::system
[slaynpool@MiniZbeub]~$  snmptranslate -On -Td SNMPv2-MIB::system
.1.3.6.1.2.1.1
system OBJECT-TYPE
  -- FROM SNMPv2-MIB
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) 1 }
```

Listing 7 – Traduction

2.1.5 Retrouvez à l'aide de snmpnetstat la liste des connections TCP et UDP du serveur distant

```
[slaynpool@MiniZbeub]~$ snmpnetstat  -v  2c -c public 10.6.0.1
Active Internet (udp) Connections
Proto Local Address               Remote Address                PID
udp4  *.*                         *.*                             0
```

Listing 8 – snmpNetstat

2.1.6 quoi sert la commande snmpgetnext ? Utilisez la pour retrouvez SNMPv2-MIB : :sysContact.0

Source : `mansnmpgetnext`

> snmpgetnext is an SNMP application that uses the SNMP GETNEXT request to query for information on a network entity. One or more object identifiers (OIDs) may be given as arguments on the command line. Each variable name is given in the format specified in variables(5). For each one, the variable that is lexicographically "next" in the remote entity's MIB will be returned.

La commande sert donc à afficher des informations à propos du périphérique interrogé.

```
 snmpgetnext 10.6.0.1 -v 2c -c public  SNMPv2-MIB::sysContact.0
SNMPv2-MIB::sysName.0 = STRING: SERVER-RT
```

Listing 9 – snmpgetnext