SNMP analysis

SNMP (**Simple Network Management Protocol**) is an application-layer protocol that is designed to run on the UDP port 161 . Its main function is to monitor all the network devices for conditions that may require administrative attention, such as a power outage or an unreachable destination. The SNMP-enabled network typically consists of network devices, a manager, and an agent.

A manager controls the administrative tasks for the network management and monitoring operations. An agent is a software that runs on the network devices, and these network devices could involve routers, switches, hubs, IP cameras, bridges, and sometimes operating system machines (Linux, Windows). These agent-enabled devices report information about their bandwidth, uptime, running processes, network interfaces, system services, and other crucial data to the manager via SNMP. The information is transferred and saved in the form of variables that describe the system configuration. These variables are organized in systematic hierarchies known as **Management Information Bases** (**MIBs**), where each variable is identified with a unique **Object Identifier** (**OID**). A total of three versions are available for SNMP (v1, v2, v3).

From a security point of view, v1 and v2 were designed to handle community-based security scheme, whereas v3 enhanced this security function to provide better confidentiality, integrity, and authentication. The tools that we present in this section will mainly target v1- and v2c-based SNMP devices.

> **Note**
>
> In order to learn more about SNMP protocol, visit: http://www.tech-faq.com/snmp.html.

SNMP Walk

SNMP Walk is a powerful information-gathering tool. It extracts all the device configuration data, depending on the type of device that is under examination. Such data is very useful and informative in terms of launching further attacks and exploitation attempts against the target. Moreover, the SNMP Walk is capable of retrieving a single group MIB data or specific OID value.

To start SNMP Walk, use the console to execute the following command:

```
# snmpwalk
```

You will see the program usage instructions and options on the screen. The main advantage of using SNMP Walk is its ability to communicate with three different versions of SNMP protocol (v1, v2c, v3). This is quite useful in a situation where the remote device does not support backward compatibility. In our exercise, we formulated the command-line input focusing on v1 and v2c, respectively:

```
# snmpwalk -v 2c -c public -O T -L f snmpwalk.txt 10.20.127.49
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 4 Stepping
1 AT/AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790
Multiprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.2
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1471010940) 170 days,
6:08:29.40
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: CVMBC-UNITY
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 76
IF-MIB::ifNumber.0 = INTEGER: 4
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.65538 = INTEGER: 65538
IF-MIB::ifIndex.65539 = INTEGER: 65539
IF-MIB::ifIndex.65540 = INTEGER: 65540
IF-MIB::ifDescr.1 = STRING: Internal loopback interface for 127.0.0 network
IF-MIB::ifDescr.65538 = STRING: Internal RAS Server interface for dial in
clients
IF-MIB::ifDescr.65539 = STRING: HP NC7782 Gigabit Server Adapter #2
IF-MIB::ifDescr.65540 = STRING: HP NC7782 Gigabit Server Adapter
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
```

```
IF-MIB::ifType.65538 = INTEGER: ppp(23)
IF-MIB::ifType.65539 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.65540 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 32768
IF-MIB::ifMtu.65538 = INTEGER: 0
IF-MIB::ifMtu.65539 = INTEGER: 1500
...
IF-MIB::ifPhysAddress.65539 = STRING: 0:13:21:c8:69:b2
IF-MIB::ifPhysAddress.65540 = STRING: 0:13:21:c8:69:b3
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
...
IP-MIB::ipAdEntAddr.127.0.0.1 = IpAddress: 127.0.0.1
IP-MIB::ipAdEntAddr.192.168.1.3 = IpAddress: 192.168.1.3
IP-MIB::ipAdEntAddr.192.168.1.100 = IpAddress: 192.168.1.100
IP-MIB::ipAdEntAddr.10.20.127.52 = IpAddress: 10.20.127.52
IP-MIB::ipAdEntIfIndex.127.0.0.1 = INTEGER: 1
IP-MIB::ipAdEntIfIndex.192.168.1.3 = INTEGER: 65540
IP-MIB::ipAdEntIfIndex.192.168.1.100 = INTEGER: 65538
IP-MIB::ipAdEntIfIndex.10.20.127.52 = INTEGER: 65539
IP-MIB::ipAdEntNetMask.127.0.0.1 = IpAddress: 255.0.0.0
IP-MIB::ipAdEntNetMask.192.168.1.3 = IpAddress: 255.255.255.0
IP-MIB::ipAdEntNetMask.192.168.1.100 = IpAddress: 255.255.255.255
IP-MIB::ipAdEntNetMask.10.20.127.52 = IpAddress: 255.255.255.248
IP-MIB::ipAdEntBcastAddr.127.0.0.1 = INTEGER: 1
IP-MIB::ipAdEntBcastAddr.192.168.1.3 = INTEGER: 1
IP-MIB::ipAdEntBcastAddr.192.168.1.100 = INTEGER: 1
IP-MIB::ipAdEntBcastAddr.10.20.127.52 = INTEGER: 1
IP-MIB::ipAdEntReasmMaxSize.127.0.0.1 = INTEGER: 65535
IP-MIB::ipAdEntReasmMaxSize.192.168.1.3 = INTEGER: 65535
IP-MIB::ipAdEntReasmMaxSize.192.168.1.100 = INTEGER: 65535
IP-MIB::ipAdEntReasmMaxSize.10.20.127.52 = INTEGER: 65535
RFC1213-MIB::ipRouteDest.0.0.0.0 = IpAddress: 0.0.0.0
RFC1213-MIB::ipRouteDest.127.0.0.0 = IpAddress: 127.0.0.0
RFC1213-MIB::ipRouteDest.127.0.0.1 = IpAddress: 127.0.0.1
RFC1213-MIB::ipRouteDest.192.168.1.0 = IpAddress: 192.168.1.0
RFC1213-MIB::ipRouteDest.192.168.1.3 = IpAddress: 192.168.1.3
RFC1213-MIB::ipRouteDest.192.168.1.100 = IpAddress: 192.168.1.100
RFC1213-MIB::ipRouteDest.192.168.1.255 = IpAddress: 192.168.1.255
RFC1213-MIB::ipRouteDest.10.20.127.48 = IpAddress: 10.20.127.48
RFC1213-MIB::ipRouteDest.10.20.127.52 = IpAddress: 10.20.127.52
RFC1213-MIB::ipRouteDest.10.20.127.255 = IpAddress: 10.20.127.255
...
```

Information extracted from the preceding code provides us with useful insights for the target machine. The command-line switch, `-c`, represents the community string that is to be used to extract MIBs, `-O` is used to print the output in a human-readable text format (`T`), and `-L` is used to log the data into a file (`f snmpwalk.txt`). More information on the various uses of SNMP Walk can be found at http://net-snmp.sourceforge.net/wiki/index.php/TUT:snmpwalk. The more the information is harvested and reviewed, the more it will help the penetration tester understand the target network's infrastructure.