Using SNMP for Security Testing

The Simple Network Management Protocol (SNMP) is a network management protocol. On SNMP-enabled devices, an SNMP agent collects information from the device and stores it within a Management Information Base (MIB) where this data is stored so that it can be accessed whenever the SNMP manager polls the SNMP agent. Linux and Windows also supports other tools such as **`snmpget`** and **`snmpset`**.

```
$ snmpwalk k -v1 -c public 172.16.2.101
SNMPv2-MIB::sysDescr.0 = STRING: APC Web/SNMP Management Card
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.318.1.3.7
SNMPv2-MIB::sysUpTime.0 = Timeticks: (47372422) 5 days, 11:35:24.22
SNMPv2-MIB::sysContact.0 = STRING: Comparitech
SNMPv2-MIB::sysName.0 = STRING: APC-3425
SNMPv2-MIB::sysLocation.0 = sTRING: 3425EDISON
SNMPv2-MIB::sysServices.0 = INTEGER: 72
IF-MIB:: ifNumber.0 = INTEGER: 1
IF-MIB:: ifIndex.1 = INTEGER: 1
IF-MIB:: ifDescr.1 =STRING: veya
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
SNMPv2-MIB:: snmpOutGetResponses.0 =Counter32: 338
SNMPv2-MIB: snmpOutTraps.0 = Counter32: 0
SNMPv2-MIB:: snmpEnableAuthenTraps.0 = INTEGER: 0
$
```

Using **`snmpwalk`** we can specify the version of the SNMP protocol to use using the **`-v`** flag and the community string used for authentication purposes via the **`-c`** flag. Or we can use the Microsoft Windows SNMPWalk utility.

```
C:\> SnmpWalk.exe
SnmpWalk.exe [-q] -r:host [-p:port] [-t:timeout] [-v:version] [-c:community]
         [-ei:engine_id] [-sn:sec_name] [-ap:auth_proto] [-aw:auth_passwd]
         [-pp:priv_proto] [-pw:priv_passwd] [-ce:cont_engine] [-cn:cont_name]
         [-os:start_oid] [-op:stop_oid] [-csv]

   -q                Quiet mode (suppress header; print variable values only).
   -r:host           Name or network address (IPv4/IPv6) of remote host.
   -p:port           SNMP port number on remote host. Default: 161
   -t:timeout        SNMP timeout in seconds (1-600). Default: 5
   -v:version        SNMP version. Supported version: 1, 2c or 3. Default: 1
   -c:community      SNMP community string for SNMP v1/v2c. Default: public
   -ei:engine_id     Engine ID. Format: hexadecimal string. (SNMPv3).
   -sn:sec_name      SNMP security name for SNMPv3.
   -ap:auth_proto    Authentication protocol. Supported: MD5, SHA (SNMPv3).
   -aw:auth_passwd   Authentication password (SNMPv3).
   -pp:priv_proto    Privacy protocol. Supported: DES, IDEA, AES128, AES192,
                     AES256, 3DES (SNMPv3).
   -pw:priv_passwd   Privacy password (SNMPv3).
   -cn:cont_name     Context name. (SNMPv3)
   -ce:cont_engine   Context engine. Format: hexadecimal string. (SNMPv3)
   -os:start_oid     Object ID (OID) of first SNMP variable to walk. Default:.1
   -op:stop_oid      Object ID (OID) of last SNMP variable to walk.
                     Default: walk to the very last variable.
   -csv              Output in CSV (Comma Separated Values) format.
C:\>
```