# Express-Guide
# ~to~
# Basic & Secure Setup of
# SNMP
# with Remote Resource Monitoring

by, **ABK** ~ http://www.twitter.com/**aBionic**

## ::Task Detail::

- Implementing SNMP service on a machine monitoring it's connection on two NICs of a machine.
- Raising a trap sending SNMP message if any of the link goes down.

---

## ::Background::

Links: *http://www.faqs.org/rfcs/rfc2570.html*

- Its a ***UDP-based service for Network Management*** inclusive of an Application Layer Protocol, database schema and set of objects. Typically ***161/udp for Agent and 162/udp for manager.*** Master could either query from slave's Agent or Agent could generate Trap/Inform messages for Master. Master could also set some information on Remote System and change its behavior.

- ***SNMP service is quite famous in vulnerability*** world to reveal loads of secrets about a machine, if not implemented properly. ***Secured SNMPv3*** service available for remote resource monitoring.

- Difference between different implementations:
  - SNMP ***v1 has simple application-wide data types***; has poor security being authorized by Community String
  - SNMP ***v2 has MIB models***, Compliance Statements (describing requirements for agents) and Capability Statements (describing permissions for agents)
  - Improved performance and security; has two versions v2c and v2u due to complexities; Incompatible with SNMPv1
  - SNMP ***v3 primarily added Message Integrity, Authentication and Encryption***

- Possible Attacks
  - SNMP ***v1 and v2c are subjected to Packet Sniffing*** due to clear-text community string being passed in the data packets
  - ***All versions are subjected to Brute Force Attack*** as they don't implement a

Challenge-Response Handshake, so to be secure on users part using Entropy in Community String is suggested.

- ***All of them are vulnerable to IP Spoofing***.

---

## ::Execution Method::

Setting up SNMP Traps Monitor for specific events.

- On **Windows**
  - Installing
    - Insert your Windows Installation Disc or get a folder sharing its files, would be required.
    - Go to 'Control Panel' > 'Add or Remove Programs' > 'Add or Remove Windows Component' > 'Management and Monitoring Tools' > 'Details' >'Simple Network Management Protocol' > 'OK' > 'Next' > follow the instructions ahead

  - Starting Services
    - 'Start Menu' > 'Run' > 'Services.msc'
      {or get it from Control Panel, As You Like It}
    - Double Click 'SNMP Service' entry, select 'Security' in dialog box Opened here remove the default community name if any and add a new name Secure enough, but not your common password. Then add machines that can access it in the list, don't go for 'all' option. Then 'Start' it.
    - If you wanna raise Traps, also start 'SNMP Trap Service' entry.
      Note: you could install Net-SNMP port for Windows to use instead of default Microsoft Implementation. Also, if you don't have access to Windows Installation Disc/Content, this option works.

- On **Linux**
  these commands are tested for a Fedora/CentOS based machine; for other platforms also the net-snmp binaries are available

  - Installing
    - `#yum install net-snmp`
    - `#yum install net-snmp-utils`
    - `#yum install net-snmp-perl`

  - Starting Services
    - `#service snmpd start`
    - `#service snmptrapd start`

  - Setting up SNMPv3
    on Fedora/CentOS location of files is /etc/snmp/ in other versions it may be

/root/.snmp/ or else {thing to check}

    -
      ```
      #cd /etc/snmp
      ```
    - and remove snmp.conf, snmpd.conf, snmptrapd.conf (better to configure from scratch), so
      - ➔
        ```
        #rm snmp*.conf
        ```
    - create a new "snmp.conf" with following content
      - ➔
        ```
        ######start of file: snmp.conf#############
        defversion 3
        defsecuritylevel authPriv
        defauthtype MD5
        defprivtype AES
        #######end of file: snmp.conf###############
        ```
    - create a new "snmpd.conf" with following content
      - ➔
        ```
        ######start of file: snmpd.conf############
        createUser <snmpUserName> MD5 <snmpPassword> AES
        rouser <snmpUserName> priv
        agentuser <AgentName>
        agentgroup <AgentGroupName>
        syscontact <SNMPAdmin's_E-MailID>
        ########end of file: snmpd.conf##############
        ```
    - create a new "snmptrapd.conf" with following content
      - ➔
        ```
        #######start of file: snmptrapd.conf#########
        ignoreauthfailure 0
        ########end of file: snmptrapd.conf###########
        ```
  - Restart Services

    -
      ```
      #service snmpd restart
      ```

    -
      ```
      #service snmptrapd restart
      ```
  - Checking if its implemented correctly

    -
      ```
      #snmpget -v 3 -u <snmp_User> -l authPriv -a MD5 -A -x AES
      -X 127.0.0.1 sysUpTime.0
      ```
      - ➔ if this gives an output like below; its setup correctly
        - ➢ Output:
          ```
          DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8680198) 1 day,
          0:06:41:98
          ```
      - ➔ if output is like following, some Authorization problem; anything changed from CONF to SNMPGET command can create this
        - ➢ Output:
          ```
          "Timeout: No Response from <IPAddress>"
          or
          ```

```
"Error in packet"
or
"Reason: authorizationError (access denied to that
object)"
```

- ➔ for following output, check the MBIOID value provided, like sysUpTime.0 here
  - ➢ Output:

```
"the given OID is not supported"
or
"No Such Instance currently exists at this OID"
or
"Error building ASN.1 representation (Can't build OID
for variable)"
```

- ◆ Configuring **TRAP Daemon on a Linux Box**
  - ○ Open 'snmptrapd.conf' file in an editor, and create from scratch with following content
    - ▪

```
#######start of file: snmptrapd.conf#######
syslocation anyPlace
syscontact Admin'sEmailID
sysservice 72
rocommunity commName
agentSecName internal
rouser internal
linkUpDownNotification yes
authtrapenable 1
trapsink itsSNMPTrapDaemonIPAddress commName 162
ignoreauthfailure 0
#######end of file: snmptrapd.conf#####
```

- ◆ Enabling **TRAPS on a Cisco Firewall**
  - ○ Console Commands

```
CiscoF/W> enable
CiscoF/W# conf t
CiscoF/W(config)# snmp-server host
inside firewallsName.internal communtiy commNam

CiscoF/W(config)# snmp-server location Place
CiscoF/W(config)# snmp-server contact Admin'sMailID
CiscoF/W(config)# snmp-server community commNam
CiscoF/W(config)# snmp-server enable traps snmp
authentication linkup linkdown coldstart

CiscoF/W(config)# exit
CiscoF/W# wr mem
```

## ::Tools/Technology Used::

- Net-SNMP : http://www.net-snmp.org/
- SNMPWalk : http://www.net-snmp.org/docs/man/snmpwalk.html
- SNMP Fuzzer : http://www.hackingciscoexposed.com/?link=tools

---

## ::Inference::

- SNMP is a real strong management protocol which could be used in an intense manner in an IT infrastructure but requires to be kept secured for the same reason of being strong.
- A single loophole can flip open your entire machine state for hacker.

---

## ::Troubleshooting/Updates::

- ***Problem:*** in statements for querying SNMP using snmpget or snmpwalk, keeping ' -v 2' didn't worked for statements where '-v 1' and '-v 3' were working.
  ***Solution:***
  *A*s stated before SNMP v2 is out there in two implementation v2c and v2u, so here I was supposed to mention '-v 2c' instead of plain '2'; though '2u' also didn't worked.

- ***Problem:*** in statements for querying SNMP using snmpget or snmpwalk, same script was working for a machine but raising MIBOID error for other.
  ***Solution:***
  *D*ifferent system architecture may differ in the MIBOIDs and not all MIBs may be accessible too, so you need to do a plain SNMPWalk to check for all accessible MIBs.

---