GIAC CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

SNMP Alert 2002: What is it all about?
Brad Beckenhauer
February 21, 2002

Introduction

On February 12th, 2002, an advisory [1][2] was issued concerning the vulnerabilities of SNMP. But what is SNMP? Hasn't it been around for years and why should we be concerned about SNMP now?

In this paper I will take your through a brief history of SNMP and provide you with some tools and information that can be used to test for SNMP vulnerabilities and increase security on your networking infrastructure.

SNMP History in Review

The Simple Network Management Protocol (hereafter called SNMP) beginnings trace back to 1988 [3] when the Internet Architecture Board (IAB)[4] published RFC 1052 (Request for Consideration)[3] which outlined the need for network management standardization and recommended that SNMP be adopted by the Internet community for network management.

Out of this recommendation, SNMP grew to become a management protocol for network and internet work devices. But SNMP encompassed much more than was originally envisioned by the Internet Architecture Board. Today, the SNMP management protocol has been adopted and implemented on computers, network hubs, switches, routers, bridges and network adapter cards to name but a few.

Ok, so what does SNMP really do? To answer this question we must examine SNMP to determine its capabilities.

SNMP is a management protocol written so that administrators can inspect and/or alter a network device from remote locations. It is through device inspection that network administrators can monitor their networks performance and build baselines [5]. These baselines are used as references to determine networks needs, gather and graph trends and are useful for comparison when the network is not working properly.

In order to manage these devices SNMP was designed with a small but powerful set of operators: *get-request, get-next-request, get-next-request* and *set-request* [6]. The *get* commands can be used to retrieve hundreds of pieces of information from a device such as the TCP/IP address, power supply status or utilization. Armed with this information, vendors and end-users can develop software to read this information and provide trending and status information as well as provide alerts that can be sent to administrative personnel via pagers or

© SANS Institute 2000 - 2005 Author retains full rights.

email. Information trending is a very powerful tool. With trending you can track and graph information like your current Internet line usage and other useful pieces of information like disk space consumption, server CPU utilization, network adapter utilization and the operational status of the power supplies in vital business equipment.

The last SNMP operator is *set-request*. In this command lies the real power of SNMP, because by using this command you can reconfigure such things as your router TCP/IP address, change its default route or mask, reboot a device and even to instruct a device to power itself off. In the capable hands of an authorized administrator, SNMP could be used to manage an endless numbers of devices. If a hacker is able to get control of SNMP, we can only theorize the number of ways they could wreak havoc on your organization.

Another important component of the SNMP command is the SNMP *community string*. The community string is like a password that allows access to the device we want to control. Management programs send devices they wish to control a community string with every SNMP request. The sent community string is then compared to the devices pre-configured community string. If the strings match, the device responds with the requested information. If the community strings do not match, the device discards the request and does not respond.

There are actually four community strings for SNMP-speaking devices:

- The SNMP *Read-only* community string enables a remote device to retrieve "read-only" information from a device.

- The SNMP *Read-Write* community string allows a remote device to read information from a device and to modify settings on that device.

- The SNMP *Read-Write-All* community string allows a remote device to read information on a device and to modify settings on that device using one common string

- The SNMP Trap community string is used when an event, such as a utilization threshold, has exceeded a predetermined value. When this user-defined threshold has been exceeded, a message (trap) is sent to an SNMP monitoring device.

By convention, most equipment ships from the factory with a read-only community string of "public". This industry practice makes it very easy for a hacker to send SNMP information requests to a newly installed device, and retrieve back configuration information, such as the Operating System version. Armed with the Operating System version information, a hacker would be able to “lookup” known exploits about that version and begin attacking the device.

© SANS Institute 2000 - 2005, Author retains full rights.

SNMP – Are your devices using the public community string?

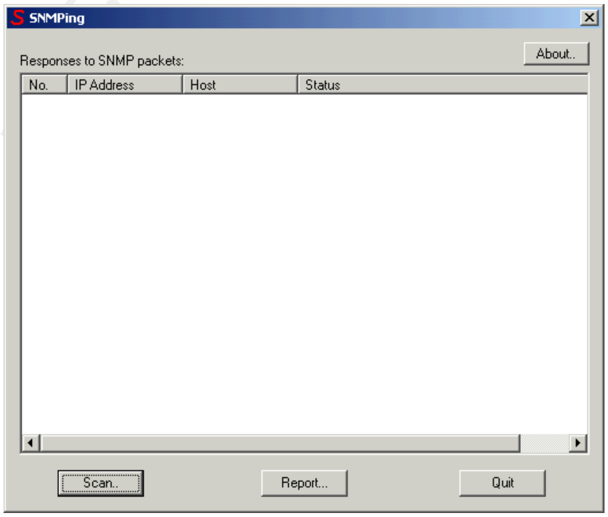
While it is standard practice for network managers to change all the community strings so that outsiders cannot see information about the internal network. If a network manager is not involved during a system configuration, then it is quite possible for systems to be left running with default community strings.

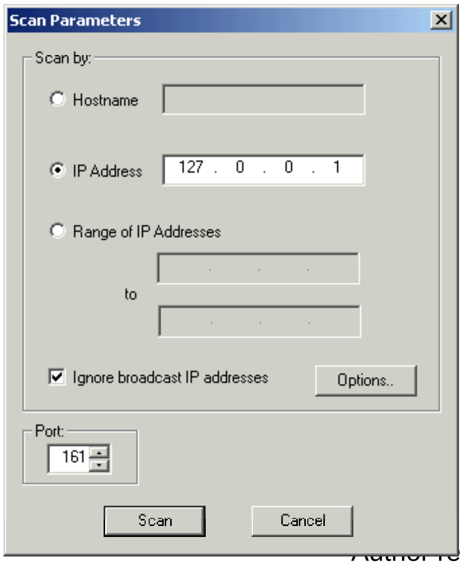
Given the size of some networks, with dozens or hundreds of known devices, it would be impractical to manually review each and every device to determine if it is using a public community string. This is where the SANS Institute [2] comes to your rescue. The SANS Institute has a free SNMP testing tool for Windows NT and 2000 to help you locate SNMP devices on your network. This powerful tool allows you to scan entire subnets very quickly to locate devices using the public SNMP community or another community name you specify.

Take a moment now and visit the SANS Institute [2] website and download the SNMP testing tool. The tool is compressed using WinZip, so you'll need to unzip it first.

Now we're ready to begin testing your workstation using the SNMP testing tool available from the SANS Institute.

Execute the SNMPING.exe tool and select the "SCAN" button at the bottom left of the utility. For our test, we'll scan your own workstations internal address of 127.0.0.1.





○ Hostname

● IP Address 127 . 0 . 0 . 1

○ Range of IP Addresses

to

☑ Ignore broadcast IP addresses

Port: 161

When you press the "scan" button a new creen will pop appear titled the scan arameters screen. On this screen please elect the IP Address button and enter 27.0.0.1. Other selectable items on this creen include the ability to scan by a ostname or a range of IP addresses. You lso have the option to Ignore the broadcast ddresses and what port you want to scan for

s
p
s
1
s
h
a
a

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

the SNMP service in case it's not running at the default port of 161.

The Options button is where you can change the community name and the timeout, which is how long the utility will wait for a response before moving on to the next device. This setting is preset to public so we're all set to scan our own machine. Select the scan button and observe the results screen. This screen will show you four columns of information:

1. No. Column - The scan number
2. IP address column– The IP address scanned
3. Host column - The name of the Host if it can be determined
4. Status column – this is where the results of the scan are displayed

The last item, the status column is where you will focus your attention. There are four possible responses that can be displayed in this column and they are:

> 1) **Unable to resolve hostname** – Hostnames have to be translated into an IP address before the utility can check SNMP. This message indicates that the hostname could not be translated to an IP Address. In this case you should check your spelling or better yet, try using the workstations IP address. Since we scanned using 127.0.0.1, this result should not appear.
>
> 2) **No answer from host** – This is the preferred response. This indicates one of two things, 1) either this machine is ignoring the SNMP request because you have a wrong community string, or 2) there is no machine at this IP Address. Since we are scanning our own internal IP address of 127.0.0.1, we can conclude that this means either SNMP is not enabled or our community string is NOT "public".
>
> 3) **SNMP enabled and available** – This message means that your workstation is configured for SNMP and is using the default community string of public, something we did not want to find.
>
> 4) **SNMP disabled or on another port** – Your workstation responded with a "Connection reset". This mean is inconclusive in that SNMP could be running, but is running on a port other than the default of port 161. If this message appears, be suspicious and plan to investigate.

Now that you have run a scan of your workstation, and concluded that this was a simple exercise, you are probably feeling like you want to check out something bigger, like you work network or somebody else's network and this is where you can get into trouble, possibly BIG trouble.

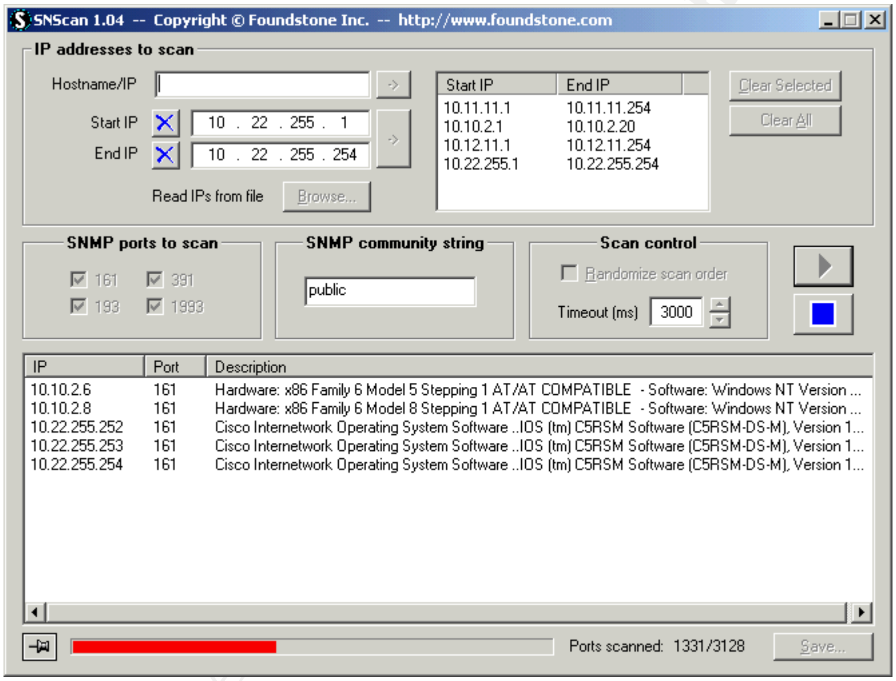
If you do not have permission to run a scan (of any type) on the network, get it now from the Security or Information Technology Manager, Director or Vice

© SANS Institute 2000 - 2005 Author retains full rights.

President and get it in writing. Running any port scanner on a network without permission can be a career-ending move. While you are now equipped with a scanning tool used to find exploits, be forewarned that there are also detection devices that can record these scans and triggers alerts. Triggering one of these devices could result in someone visiting you and asking some very pointed, uncomfortable questions.

Another free SNMP Scanner, SNSCAN, available from Foundstone Inc. [7], allows you to scan the common SNMP ports of 161, 193, 361 and Cisco's port 1993. While SNSCAN is restricted to only these four ports, it does allow you to scan all four ports in a single pass and you can scan multiple IP ranges at a time. The utility also allows you to import the addresses ranges so you can quickly rescan ranges as your needs require.

The slide below illustrates SNSCAN's features and shows five devices that will require follow up action.



SNScan 1.04 -- Copyright © Foundstone Inc. -- http://www.foundstone.com

IP addresses to scan

Hostname/IP:

Start IP: 10 . 22 . 255 . 1

End IP: 10 . 22 . 255 . 254

Read IPs from file

Start IP	End IP
10.11.11.1	10.11.11.254
10.10.2.1	10.10.2.20
10.12.11.1	10.12.11.254
10.22.255.1	10.22.255.254

SNMP ports to scan

☑ 161 ☑ 391
☑ 193 ☑ 1993

SNMP community string

public

Scan control

☐ Randomize scan order

Timeout (ms) 3000

IP	Port	Description
10.10.2.6	161	Hardware: x86 Family 6 Model 5 Stepping 1 AT/AT COMPATIBLE - Software: Windows NT Version ...
10.10.2.8	161	Hardware: x86 Family 6 Model 8 Stepping 1 AT/AT COMPATIBLE - Software: Windows NT Version ...
10.22.255.252	161	Cisco Internetwork Operating System Software ..IOS (tm) C5RSM Software (C5RSM-DS-M), Version 1...
10.22.255.253	161	Cisco Internetwork Operating System Software ..IOS (tm) C5RSM Software (C5RSM-DS-M), Version 1...
10.22.255.254	161	Cisco Internetwork Operating System Software ..IOS (tm) C5RSM Software (C5RSM-DS-M), Version 1...

Ports scanned: 1331/3128

Public Alert, Now what?

After scanning your network infrastructure, you probably have a list of potential devices that are showing SNMP access of some sort, the question now is, what are you going to do?

According to the SANS Institute Top 20 Document [8] section U7.5, there are five things you can do to help defend against SNMP exploits, these five items

© SANS Institute 2000 - 2005, Author retains full rights.

are listed here for your convenience.

1. If you do not absolutely require SNMP, disable it.

2. If you must use SNMP, use the same policy for community names as used for passwords. Make sure they are difficult to guess or crack, and that they are changed periodically.

3. Validate and check community names using snmpwalk. Additional information can be found at: http://www.zend.com/manual/function.snmpwalk.php

4. Filter SNMP (Port 161/UDP) at the border-router or firewall unless it is absolutely necessary to poll or manage devices from outside of the local network.   Port 161 is the port SNMP uses to listen for requests and from which it responds.

5. Where possible make MIBs read only. Additional information can be found at: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315

So what is a MIB? MIB stands for Management Information Base and is a common format used by vendors that breaks down network device features into eleven distinct groups [9]. These groups define management or statistical areas of the device such as system interfaces, address translation, transmission and several protocols like IP, tcp and udp.

Ok, for some people, this sounds like a simple task, but consider how many devices you have to make changes too. Calculate the time, energy and effort required to perform these tasks on a large system of network device and computers. It could well be that you are faced with a very large task. If this is your first venture into network security, consider making these five items your highest priority. If you do not have the expertise to do all of these items, do what you can and consider outsourcing the rest.

Hands On

Do not attempt these procedures on a corporate or company computer unless you have permission from the department in charge of your computer systems. Your internal support staff may have a legitimate business purpose or policy regarding SNMP configuration. It's best to leave computer configurations to those that are ultimately responsible for the computer itself. I am about to empower you with the capability to perform certain actions on SNMP devices, however, if it is not your responsibility to makes these changes

© SANS Institute 2000 - 2005, Author retains full rights.

or you do not have the authority to make these changes, stop now.

Checking a Windows 2000 Professional workstation

Determining if SNMP is installed on a Microsoft Windows 2000 workstation or server.
From the Windows desktop

- Locate the icon titled *My Network Places* and right-click on the icon.
- Select the *Properties* option. A new window will open up titled “Network and Dial-up Connections”.
- Select the word *Advanced* which is located along the top row of options
- Select *Optional Networking Components*
- Select *Management and Monitoring Tools*
- Select the *Details* button

On the *“Management and Monitoring Tools*” screen you will see an option named “*Simple Network Management Protocol*”. Look to the left of this word for a small white box with a check mark in it. A check mark means that the service is installed.

If this is you personal home computer, you can turn off SNMP by unchecking the box and selecting the *OK* button. This will remove the service from your computer. If you have SNMP turned off on your workstation, pat yourself on the back, your workstation is not vulnerable to a SNMP hacker attack.

Determining the SNMP community string on a Windows 2000 workstation or server.
From the Windows desktop

- Locate and select the *Start* icon
- Select the *Settings* option.
- Select the *Control Panel* option
- Select the *Administrative Tools* Option
- Select *Services* option
- Scroll down the list and select the *SNMP Service* option and open it
- Select the *Security* tab

If your computer is using default parameters, you will see a community string of “public” and a setting of “READ ONLY”

Determining if SNMP is installed and running on a Microsoft Windows NT4

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Server.

From the Windows desktop

- Locate and select the *Start* icon
- Select the *Settings* option.
- Select the *Control Panel* option
- Select the *Services* Option
- Scroll down the list and look for the *SNMP* service option. The STATUS column will tell you if the service is running or not. If the service is running and you wish to shut it off, then click on the stop button to the right. This will stop the service until the system is rebooted. To make sure that the system does not restart the service, click on the button and change the startup type to disabled. This will not remove the service from the system, but will keep it from running if the system is rebooted. This will allow you to quickly re-anable the service after applying the vendors recommended patches.

Determining the SNMP community string on a Windows NT4 Server.

- Locate and select the *Start* icon
- Select the *Settings* option.
- Select the *Control Panel* option
- Select the *Network* option
- Select the *Services* Tab
- Locate the *SNMP Service* option
- Select the *Properties* button
- Take a close look at the *Traps* and *Security* tabs. Remember that traps are where the system will send alerts, the Security tab controls the community names and from what stations SNMP commands will be accepted.

Conclusion

While SNMP is not perfect and was designed to be simple from the beginning, vendors have widely accepted this standard for managing IP Devices. While the vendors debate how to secure and improve SNMP, you need to take action to protect network assets for which you are responsible. Much like any other protocol available on the market, it was only a matter of time before an exploit was discovered. And when the exploit was revealed, manufacturers where quick to address the vulnerability and provide options and solutions to their customers. Given the powerful capabilities of SNMP, system administrators should use tools to periodically review their networks, discover any existing

© SANS Institute 2000 - 2005, Author retains full rights.

vulnerabilities and address them.

References

[1] CERT® Coordination Center, CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)
http://www.cert.org/advisories/CA-2002-03.html

[2] SANS Institute Online, A Cooperative Education and Research Organization, http://www.sans.org

[3] IAB Recommendations for the Development of Internet Network Management Standards, Request for Comments: 1052
ftp://ftp.isi.edu/in-notes/rfc1052.txt

[4] Internet Architecture Board, a technical advisory group of the Internet Society
http://www.iab.org

[5] Sybex, CCNA Cisco Certified Network Associate Study Guide, ISBN: 0-7821-2381-3, page 83-84

[6] A Simple Network Management Protocol (SNMP), Request for Comments: 1157
ftp://ftp.isi.edu/in-notes/rfc1157.txt

[7] Foundstone Inc.**,** A company that provides Professional Security Services
http://www.foundstone.com

[8] SANS Institute Online, A Cooperative Education and Research Organization, The Twenty Most Critical Internet Security Vulnerabilities (Updated) v2.502 posted 30 Jan 2002
http://www.sans.org/top20.htm

[9] Digital Press, TCP/IP Explained, Philip Miller, ISBN: 1-55558-166-8, page 367.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.