Global Information Assurance Certification Paper

Much to do About SNMP

Mike A.R. Luessi
October 14, 2002
Version 1.4b

A Paper Submitted in Partial Fulfillment
Of the Requirements for GSEC

SANS Institute

Introduction

It seems amazing that something as simple as SNMPv1 (Simple Network Management Protocol) with only 5 commands could create such a commotion back in the spring of 2002. After the release of the security warnings a flurry of activity followed, including articles, recommendations, and patches to fix the problems with SNMP. I found myself surprised by the response. I had assumed most people that work with networks and management tools understood the benefits and dangers involved with SNMP and had properly protected their environments.

Everyone seems to have his or her opinions on SNMP's place and use in a network. Whether it is called a necessary evil or an indispensable tool, SNMP is here to stay. I could not fathom an environment where it would not have a place. I would imagine it to be similar to flying a plane in the fog without the use of instruments. SNMPv1 is only the first part of the problem, the second part has been its implementation since it inception back in 1987. This paper is a guide to understanding how SNMP works, what PROTOS tested, and how to create a more secure environment for the use of SNMP. With the right implementation SNMP can be a wonderful and secure tool.

Background

Since its development in 1987 SNMP has become the de facto standard for network management. One of the intents of SNMP was to develop a simple protocol, which would give network administrators the ability to manage almost any device in the network. Examples of these devices include routers, switches, PCs, and etc. Network Administrators needed a way to see into and manage their networks, and SNMP provided that functionality. SNMP is now everywhere and has become an industry within itself. Millions of dollars each year are being spent to see into ones network. It has even become popular at Universities around the world to use SNMP to monitor the current soda levels of Coke machines. By knowing the soda levels you don't have to waste time walking out to an empty machine. SNMP can provide valuable information in terms of system performance and health. It can also be used to alert us when something goes wrong. The following chart shows how SNMP works.

Figure 1 is a simplified view of the SNMPv1 structure:

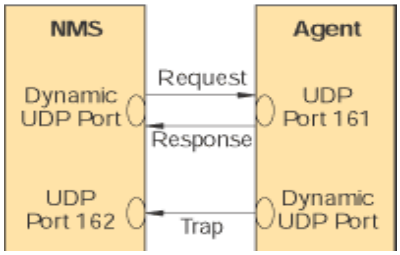
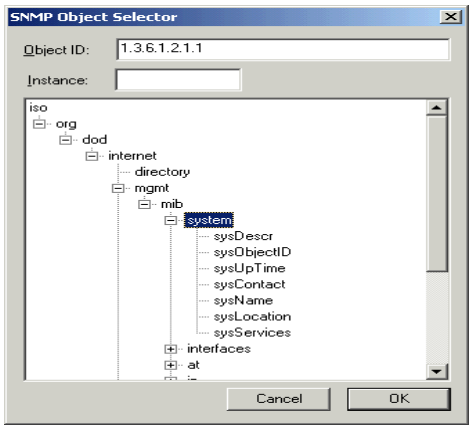


Figure 1. A simplified SNMPv1 architecture. Courtesy of (ISTS), Dartmouth College.

The NMS represents the Network Management Station and the Agent represents the device that will be polled (router, server, etc.) SNMP Protocol Data Unit or a PDU is the acronym to describe the conversation between the NMS and Agent. The NMS sends out a Get_Request that comes across as a UDP packet on port 161. The Agent then responds with a Get_Response. The NMS can also send out a Get_Next_Request, which is replied with another Get_Response. "Despite being unreliable UDP won the battle for the post of the messenger because of its ability to have a very small packet size."(3) UDP as a protocol is attractive because it is small and that makes it quick.

The benefit of the small packets is that most of these NMS are polling at a frequent rate. Tools that I have used have been customizable down to 30 seconds. The rate at which you poll is dependent on the network, but the goal is to find out how the network is doing without introducing a high volume of management traffic from the NMS. SNMP can also run on UDP 162. This port is most likely to be used for traps. A trap can occur for many reasons and is really based off of the SNMP vendor's implementation. When the trap is triggered it is sent from the Agent back to the NMS. Traps are mainly generated for significant events such as an interface going up or down, reboots, or failed login attempts. Network management stations can also send Set_Request. This can be used to change a MIB (Management Information Base) or it can be used to reboot a device.

The MIB is the structure where the Agent stores collected information on the device. This structure is sometimes called a tree. Each part of the tree is represented by what is called a OID(Object Identifier). Below is a screenshot from a program called WSPingPro.



The screenshot gives you idea of the structure. As you "walk" the MIB you will see these numbers (1.3.6.1.2.1.1) change. These numbers are the OID. If you

are troubleshooting an SNMP problem and you need to find the value held at a specific OID, tools like the one above are very effective.

SNMPv2

You might have heard of SNMPv2 (Version 2). SNMPv2 was developed in 1993 to address security concerns. The intention of SNMPv2 was to fix the following security concerns[4]:

1. Privacy
2. Authentication
3. Access Control

Privacy was going to be accomplished by scrambling or encrypting the message. Only the sender could read the message. Authentication would perform a check on who the requestor was to make sure that it was trusted. Finally Access Control would validate that only certain users were able to perform management functions.

For one reason or another SNMPv2 was never widely adopted by the technical community. SNMP Research Intl reported,

> Although SNMPv2 was granted Proposed Standard status by the IETF, it was not accepted by the industry as a de facto standard in that few vendors included SNMPv2 in their products. There were many complaints about the complexity of the design of the security and administrative framework. While these aspects had been shown to be implemental and interoperable, they were often criticized as too complex for the average network administrator to deploy, configure, and use. [5]

The above information points out that SNMPv2's real problem is it strayed away from being simple. SNMP was designed to be simple and the technical community wanted it to stay that way. But there was a need for the added security, and that is where SNMPv3 came into play.

SNMPv3

SNMPv3 was designed to pickup where SNMPv2 failed. Uri Blumental and Bert Wijnen of IBM Watson Research said, "The ultimate question a security system has to answer is: ``Should I permit this operation?' Naturally, in order to be able to do that, several lesser questions have to be answered first." [8] They went on to say that the questions that must be answered first are"

- Is the message specifying an operation unaltered and timely?
- Who requested the operation to be performed?
- What objects are accessed in the operation?

- What are the rights of the requester with regard to the objects of the operation?

The question of whether the operation should be permitted or not, really falls under what I would classify as a security issue. SNMPv2 started to address these issues but failed. The first step in having SNMPv3 accepted is finding out what Network Administrators need. It is the same concept that one would follow if they were going to open a business. Is there a need for this good or service? Depending on what type of business you are in the answer can vary. I could see the greatest need coming from the government, especially defense.

Maybe as time goes on we will also see this need in normal business cases, but right now I don't understand the push. Let me clarify what I mean. If one follows good security practice of locking down SNMP access from the outside world (Internet) and specifically permits access only from the inside or private address space the need should be mitigated. Access list and a separate Management segment should also eliminate security concerns. But in order for SNMPv3 to find it place in the technological world, companies are going to have to start accepting it and implementing it into their hardware and software. Some have started to do this, but the community as a whole has not. Again going back to government, I think there will be a push to include SNMPv3 support in order to sale equipment to the government in the future. The functionality provided in SNMPv3 is useful for anyone sending data across unsecured segments.

The only way to know if SNMPv3 will be accepted is time. Time will show us what we need to be careful of and what threats are going to come our way. Network administrators will adopt SNMPv3 if it proves to offer features that are necessary in the world that is our reality.

Alternatives

The best-known alternative to SNMP is Common Management Information Protocol (CMIP). After researching CMIP it seems that it differs from SNMP in a few ways. CERT has broken down the advantages into the following [8]:

- CMIP variables not only relay information, but also can be used to perform tasks. This is impossible under SNMP.

- CMIP is a safer system as it has built in security that supports authorization, access control, and security logs.

- CMIP provides powerful capabilities that allow management applications to accomplish more with a single request.

- CMIP provides better reporting of unusual network conditions

The disadvantage of CMIP is that it is a resource hog. The overhead of the devices has kept many people away from implementing it in their environments. The other problem is that there are not a lot of developers working on software for CMIP. There is more security built into CMIP, but hopefully with the acceptance of SNMPv3 we can depend on that same level of security.

PROTOS – University of OULU

PROTOS is a research project at the University of OULU in Finland. The University develops testing suites in order to test for unknown vulnerabilities and verify the robustness of different protocols. The suite developed to test SNMPv1 is called c06-snmpv1. (11) The goal of this specific test was to evaluate the implementation level security and robustness. SNMP was chosen with the following criteria in mind:

- Widely adopted management protocol, may be enabled in network devices by default
- SNMP manageable devices maybe critical infrastructure, thus creating a need for protection
- SNMP may be vulnerable to exception handling, make it vulnerable to attacks even with authentication
- Because of the length of time SNMP has been involved in network devices it should give a fair representation of the current state of implementation level robustness

The test presented some alarming findings. First of all if a Network Administrator had setup an environment and was not using SNMP for monitoring they might still have a problem because it had been enabled by default. Imagine if you had a router that faced the Internet and you had locked it down, but did not do anything with SNMP because you were not using it. There could be possibility that an attack could be carried out against the router because the default configuration had set the community string to public and had enabled the service.

It also pointed out the fact that just because there really hadn't been any previous large-scale attacks against SNMP, it didn't mean that it was safe. Some vendors had problems with their agents because of programs that did not look for abnormal request. The technology industry had put SNMP up on the shelf and had forgot about its dangers. The test reminded us of what might be if actions were not taken. The test represented the need to follow well-known security guidelines in protecting critical network infrastructure. It also presented the fact that many vendors needed to patch their SNMP agents and managers to protect against malicious activity.

SNMP Best Practices

Many resources are available for ways of securing SNMP across different networks. Included at the end of this paper is a list of resources for gaining a broader under-standing of SNMP and the techniques for secure implementations. The following list is a good starting point and is intended to be general. It is your responsibility to make sure that the information fits the needs of your network. I don't claim this to be a one-stop shop for SNMP information and recommend you using the resource page for further information. If you still have questions I am sure there is someone at SANS who would be thrilled to help you in your endeavor. After getting that out of the way lets get back to the list. The following list was comprised by CERT [(1)].

1. Apply a patch from your vendor.

2. Disable all nonessential SNMP software.

3. Filter SNMP access to managed devices to ensure the traffic originates from known management systems.

4. Filter SNMP services at your network perimeter (ingress/egress filtering).

5. Change SNMP community strings from their defaults.

6. Segregate network management traffic onto a separate network.

Let us break the list down into meaningful information. First "Apply a patch from your vendor" is very important because in some situations it has been possible to crash devices by buffer overflows. An example of this would be putting in a community string, which is 150 characters long, and the program could only handle 25 characters. In this situation a well-designed community string is not going to protect the device. There was a flurry of patches released after the PROTOS project released their findings. It is a good idea to verify all devices in the network to make sure they are updated with all patches regarding SNMP.

Second, it is recommended to "Disable all nonessential SNMP software." This is just a good and very basic security concept. An example of this concept would be someone's desktop machine running a personal web server without his or her knowledge. In most situations that would mean that the machine is listening on TCP port 80. This could lead to numerous security vulnerabilities for the server. It is important to know how you devices operate and what might be turned on by default.

Third, I would setup devices to only allow SNMP traffic from known partners. NT allows the administrator to create a list of who can poll the server. Again know your devices and what is available in terms of security.

Fourth, protect your network at the firewall. If possible it is a good idea to lock down the perimeter. This can be done with firewall rules and access-list. In most situations there should be no need to have someone from outside the network

polling devices on the inside. Don't forget to include locking down SNMP access to the firewall itself.

Fifth, build strong community strings. Many resources are available for this. A resource I would recommend is SANS. SANS recommends a password that is at least 6 characters long, is a mixture of upper and lower case letters, and includes numbers. I would recommend staying away from words. (10) Many tools are available to quickly crack poorly built passwords. A strong password policy is a good idea to have on all devices in the network. Make sure you stay away from the defaults of public and private.

The final recommendation is to segregate the network management traffic. I would recommend having a segment dedicated to network management devices. This will make it easier to control access and to create rules in the firewalls that best protect your critical devices.

This list is a good starting place for creating a more secure environment. But security is really something that never is completed, rather a work in progress that requires constant attention and nurturing. Please look to the end of this paper for a list of resources that should guide you in the right direction for protecting your critical devices.

Testing

How do you know if your network has been locked down? You might say, "I personally went to all devices and made sure that the passwords are strong, and that only necessary devices have SNMP enabled. I would ask the question, "Have you tested your environment?" If you answered no, then you should. If you answered yes, when was the last time you ran the test? The point I am trying to make is that running test and understanding the results is the only way you know what an intruder might find out. Let us look again at the SNMPv1 model.

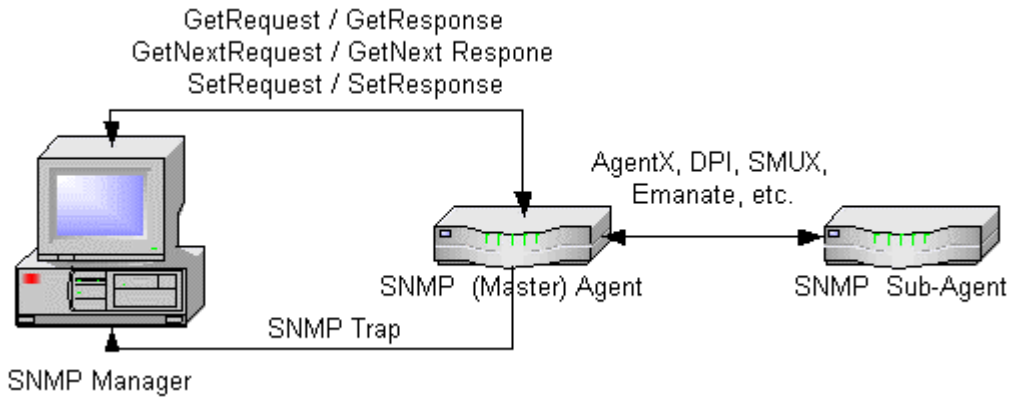


Figure 2. Flow of PDUs between SNMP managers and agents. Courtesy of iDefense [(2)].

A good test will look at the SNMP manager and any of the SNMP agents. We should take the approach that the environment is not secure. A tool should be used that test for vulnerabilities which could lead to a denial of service attack. The test should also test each agent in how it handles buffer overflows and exceptions.

Many tools are available for testing your SNMP implementation. If you look around you should find quite a few free tools for doing this testing. Otherwise, there are plenty of tools available for a price.

Conclusions

The following is an excerpt from an article written by Jim Reavis of Nwfusion.

> The Simple Network Management Protocol (SNMP) is probably the most pervasive tool you could possibly find. All operating systems have this capability in one form or another. Hubs, switches and routers have this capability as well. Of course, the wonderful capability for network administrators to reach out and touch a device across the net is a double-

edged sword - hackers can do the same thing. (9)
After reading this paper I hope that you have gained an understanding of how SNMP works and where to start in locking it down.

The PROTOS group reminded us that there are problems with SNMP and many implementations. Sometimes the only way problems get fixed is when it is brought to the forefront. PROTOS with it test called c06-snmpv1 did that very thing. PROTOS demonstrated that diligence is needed in any implementation. The test also showed us that it is important to gain a full understanding of what we are trying to lock down.

Whether it is SNMPv1 or one of it successors we need to know how it works, and what needs it was designed to fulfill. SNMPv3 will probably find its way into your network sooner or later. If I had to guess it would probably be later. Remember SNMP was designed to be simple and easy to implement. It is hard to say whether SNMPv3 will follow the same design. My research leads me to think that SNMPv3 is quite a bit more labor intensive. But if your network requires authentication and encryption for polling devices then it might be a step in the right direction for you to take.

Although SNMP does have certain vulnerabilities following simple steps such as strong passwords and filtering access can go along way for protection. The quote at the beginning of the Conclusion was written on 10/04/99. The PROTOS testing was done earlier this year. The problems with SNMP, and how they where addressed should be viewed as a lesson in network administration. By following well-known security practices SNMP can be more secure, and still be our beloved tool for looking into what is going on in our environments.

Resources for Understanding and Securing SNMP

I wanted to take a little bit of time to give you the reader an opportunity to have a resource for better securing you environment. I have included links to documents that refer to steps in locking down some of the better known devices and operating systems used in today's networks. I have also attached a few links for developing strong passwords. They are listed below:

2000/NT

http://www.mike-tech.com/article.php?gif=winnt4&article=129

http://www.giac.org/practical/Robert_Hayden.doc
www.giac.org/practical/Stephen_Cicirelli_GSEC.doc
http://www.microsoft.com/windows2000/techinfo/reskit/en/CNET/cneb_snp_kwch.htm

SUN

http://securityresponse.symantec.com/avcenter/security/Content/2005.html
http://www.samag.com/documents/s=1148/sam0107m/0107m.htm
http://web.singnet.com.sg/~chihung/bookmark/solaris.html
http://www.maryville.com/MTSNMPVBrief.pdf

Cisco

www.cisco.com/warp/public/477/ SNMP/snmpsecurity-20370.html
http://www.solarwinds.net/Tools/Security/Security_SNMP.htm

Free Tools

http://silver.he.net/~rrg/snmp_free_tools.htm

References

[1] CERT Coordination Center. "Simple Network Management Protocol (SNMP) Vulnerabilities Frequently Asked Questions (FAQS)". February 13, 2002. URL: http://www.cert.org/tech_tips/snmp_faq.html

[2] iDefense. "SNMP Test Suite Released by Finnish University" February 14,2002. URL: http://www.idefense.com/Intell/CI021402.html

[3] Mukhi, Vijay. "SNMP, The Simple Network Management Protocol". URL:

http://www.vijaymukhi.com/vmis/snmp.htm

[4] Ericsson. "H.8.3 SNMP and SNMPv2". URL: http://www.ericsson.com/about/telecom/part-h/h-8-3.shtml

[5] SNMP Research International, INC. "SNMPv2 Standardization Process". URL: http://www.snmp.com/news/v2-background.html

[6] The Simple Times. "The Simple Times, Volume 5, Number 1, December, 1997". URL: http://www.simple-times.org/pub/simple-times/issues/5-1.html

[7] Carnegie Mellon Software Engineering Institute. "Simple Network Management Protocol".September 22, 2000 URL: http://www.sei.cmu.edu/str/descriptions/snmp_body.html

[8] Carnegie Mellon Software Engineering Institute. "Common Management Information Protocol". September 22, 2000 URL: http://www.sei.cmu.edu/str/descriptions/cmip.html

[9] Reavis, Jim. Network World on Security. "SNMP – simple management tool for hackers?" October 04, 1999 URL: http://www.nwfusion.com/newsletters/sec/1004sec1.html

[10] SANS Institute. "SANS / FBI The Twenty Most Critical Internet Security Vulnerabilities". Version 3.2 October 17,2002 URL: http://www.sans.org/top20/

[11] University of OULU. "PROTOS Test-Suite: c06-snmpv1". February 12, 2002 URL: http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/index.html