



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 permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Securing SNMP in Windows

SNMP overview

Simple Network Management Protocol (SNMP) is used to monitor, configure and send alarms from network-enabled equipment. It consists of two parts: the SNMP manager and the SNMP agent.

The SNMP manager software is typically a GUI interface (though there are command line programs that will do similar things) that shows the “state of the network.” The manager retrieves configuration and performance counters from the agent software by issuing *get* commands. It can also change a network element’s configuration by sending a *set* command (provided the appropriate permissions are set).

The SNMP agent responds to set and get commands issued from a management software with the correct community code. On Windows NT the agent retrieves information from the registry and converts it to the accepted format for SNMP. Agent software also has the ability to send an alarm or trap to the management console (or whatever IP address it’s configured).

SNMP agents use a Management Information Base (MIB) to determine what traps are sent and what performance counters are used. These MIBs are the foundation for reporting and sending traps.¹

If SNMP is installed on Windows NT after the application of service pack 3 or later you **must** reinstall the service pack. Microsoft recommends reinstalling service packs after installing any software, but in this situation it is mandatory as there is a .dll incompatibility that will cause the SNMP service to fail to start. Reapplication of the service pack fixes this problem.

Built in Security

The security implementation in SNMP is very primitive. SNMP run over UDP port 161 (traps are sent over UDP 162). Authentication is accomplished through the use of a community name (or string). The community string is sent along with the SNMP command. The community string is then compared to the list the agent contains; valid permissions are checked for the community and if all is in order the command are executed.

The default community name in Windows NT, and in general, is “public,” as specified in RFC 1157, although some vendors are setting the default community as “private.” These two as well as an empty community string are well known and the first that will be tried.

¹ For more information on MIBs see: RFC 1213 and RFC 1155.

This shared password is transmitted in clear text, as part of the UDP package, so simply sniffing the network will reveal the community.

Default Install

With a default install of Windows NT 4.0 with SNMP the default community is set (public) and the default (and only) settings are Read/Write. This allows any and all to issue a command such as:

```
SNMPUTIL walk hostname public .1.3.6.1.4.1.77.1.2.25
```

The user will receive a listing of all usernames on the machine (or Domain if a DC is targeted). SNMPUTIL is a program that ships with the Windows NT resource Kit. Another potential exploit is:

```
snmpset -v 1 ipaddress public .1.3.6.4.1.311.1.2.5.3.0 a
```

This will erase all entries in the WINS database. SNMPSET is a UNIX command using the CMU SNMP development kit. The potential for harm is easily grasped.

Securing SNMP in Windows NT

The next question is: How does one go about securing SNMP in Windows NT. The solution is fivefold.

Ports

The very first thing that should be done is to block port 161 and 162 UDP on your firewall or gateway. SNMP utilizes port 161 to issue and respond to SNMP queries and commands. Port 162 is used to send trap messages. Port 161 should be set to block both inbound and outbound, thereby preventing someone from sending or receiving information on these ports. Port 162 should be blocked for outbound at the least. If systems were compromised, or a user changes the parameters, traps could be sent out of the network.

If you really need control over where and where not messages are sent these ports could be filtered on the routers of various subnets to contain them on one or a few subnets. For example one could block 161 and 162 on all routers except the server's subnet and the monitoring station's subnet to monitor only the servers and to keep "adventurous" users from sending and receiving SNMP packages.

Community String

Change the community string. By default the community string of "public" is installed and active (with Read/Write access). This is not an oversight, but expected behavior (see RFC 1157) and easily overlooked. Set a new community string and be sure to delete the

“public” community string. Public, private and NULL are the three most common public strings and should never be used.

Install Service Pack 4 or better

The option to set a community to ‘Read Only’ is **not** available on the default install. To change the default community to an option other than Read/Write service pack 4 or later must be installed. Remember, if the SNMP service was installed after a service pack, the service pack **must** be reinstalled or the SNMP service will not operate.

After installing service pack 4 or greater the option to set permissions by community string becomes available under: “Control Panel” -> “Network” -> “Services” -> “SNMP, properties” -> “Security tab”. Different permissions for different communities can be set. The options are Read/Write (default), Read Only, and Read/Create (the default setting for Windows 2000 is Read Only). Try to set these strings to “Read Only” (perfect if you’re just monitoring systems). If you are using SNMP to manage the systems use one community set to “Read/Write” to make changes and another set to “Read Only” for normal monitoring activities. This will cut down on the exposure of the “Read/Write” community string.

Use a packet filter

In the SNMP properties window there is an option to set packet filters. This allows an administrator to determine what IP addresses a machine is allowed to communicate with by community. After selecting a new community name and setting the permissions for the string, one can add valid IP addresses for that community string. As many IP addresses can be added as needed and one IP address can be a member of as many community strings as there are defined.

To set the packet filtering options go to “Control Panel” -> “Network” -> “Services” -> “SNMP, properties” -> “Security tab.” Select the community string, check the “accept packets from these IP’s only, type in the IP address in the box and click add. Repeat as necessary.

This doesn’t prevent IP spoofing but it does prevent the responses from being sent to another machine. Unless the perpetrator has a sniffer on one of the subnets issuing a get will do them no good. They could, however, issue a set command with a spoofed IP that would be accepted if it were sent using a Read/Write community string.

Secure the registry and .dll

The last step is to secure the registry. This is important as a user could edit the registry directly and modify the settings for SNMP and the .dll files associated with the MIBs. The other part of this section is securing the .dll files (the MIBs) directly. These files need to be protected to prevent the introduction of a trojan horse or other mischief.

The registry keys that need to be changed are:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\DHCPMibAgent
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\LANManagerMIB2Agent  
HKEY_LOCAL_MACHINE\Software\Microsoft\RFC1156Agent  
HKEY_LOCAL_MACHINE\Software\Microsoft\SNMP
```

as well as any other keys with MIB pointers. These registry entries will point to the associated files in the (typically) %systemroot%\system32 directory. These files should be set to Read and Execute permissions for the system and administrator, and no access permissions set for everyone and other accounts.

The following registry keys should be fine with the default settings, but you may want to check them:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMPTRAP
```

Summary

The five basic things that need to be done to secure SNMP in Windows NT are:

- Ports: secure ports 161 and 162 on the network and at routers.
- Change community string and set permissions.
- Install the latest service pack (at least service pack 4).
- Activate various packet filters.
- Secure registry keys and .dll files.

Be sure to reinstall any service pack you have if you install the SNMP service after applying the service pack, as there are conflicting files that will cause the service to fail to start.

© SANS Institute 2000 - 2002, Author retains full rights.

References

Taylor, Paul. "Enterprise Integration Using SNMP." Enterprise Integration Using SNMP Feature Article, July 1998 by Paul Taylor. July, 1998. URL:
http://www.ntsistemas.com/db_area/archive/1998/9807/207fe2.shtml (8/22/2000)

Network Associates, Inc. "Windows NT SNMP Security Permissions." COVERT Research Center Windows NT SNMP Security Permissions. November 17, 1998. URL:
<http://www.pgp.com/research/covert/advisories/030.asp> (8/22/2000)

Shiva. "What is SNMP?" Shiva SNMP Reference. URL:
http://www.shiva.com/prod/docs/archive/netmod/11_snmpf.html (8/22/2000)

Rouland, Christopher. "SNMP holes in Windoze NT 4.0."(sic) October 8, 1998. URL:
http://www.insecure.org/spl0its/NT.snmp.domain_users.record_deletion.html (8/22/2000)

NetIQ Corporation. "Troubleshooting tips for Hardware category products" URL:
<http://www.netiq.com/support/hrdwrtips.asp> (8/22/2000)

© SANS Institute 2000 - 2002, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Honolulu SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Orlando SEC401	Orlando, FL	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
Community SANS Chantilly SEC401	Chantilly, VA	Jan 29, 2018 - Feb 03, 2018	Community SANS
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZ	Feb 05, 2018 - Feb 10, 2018	Live Event
Community SANS Madison SEC401	Madison, WI	Feb 05, 2018 - Feb 10, 2018	Community SANS
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
Southern California- Anaheim 2018 - SEC401: Security Essentials Bootcamp Style	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	vLive
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
Community SANS Columbia SEC401	Columbia, MD	Feb 12, 2018 - Feb 17, 2018	Community SANS
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, Japan	Feb 19, 2018 - Mar 03, 2018	Live Event
SANS New York City Winter 2018	New York, NY	Feb 26, 2018 - Mar 03, 2018	Live Event