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
"Securing Windows and PowerShell Automation (Security 505)"
at http://www.giac.org/registration/gcwn

GIAC Securing NT

Practical Assignment for

SNAP/SANS2000 San Jose

Robert Hayden

Version 1

June, 2000

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Microsoft® and Windows NT® are registered trademarks of Microsoft Corporation.
http://www.microsoft.com/

Changes are made periodically to this document. Changes, technical inaccuracies, and typographical errors will be corrected in subsequent editions.

This publication was created using Microsoft Word for Windows 97 SR1 software. The typeface is Times New Roman.

The information in this document is subject to change

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table of Contents

TRADEMARKS i
TABLE OF CONTENTS ii
REVISION HISTORY iii

1 INTRODUCTION 1
1.0 PURPOSE AND SCOPE OF DOCUMENT 1
1.1 SUPPORTING DOCUMENTS / REFERENCES 2
1.2 ACRONYMS AND DEFINITIONS 2
2 VULNERABILITIES 3
2.0 INFORMATION READABLE 3
SHARES 3
USER NAMES 3
STATUS OF RUNNING SERVICES 3
2.1 INFORMATION WRITABLE 4
3 CONTROLS 5
3.0 DEINSTALL SNMP IF IT IS NOT NECCESSARY 5
3.1 PROPER SNMP CONFIGURATION 5
3.2 HOST FILTERING 7
3.3 UPGRADE TO THE LATEST SERVICE PACK, MINIMALLY SP4 8
3.4 UTILIZE COMMUNITY STRING ACCESS LEVELS 8
3.5 RESTRICT REGISTRY KEY ACCESS 10

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Securing the SNMP Service

REVISION HISTORY

Date	Author	Version	File Name	Change Reference
06-02-2000	Robert Hayden	Prelim.	sans1.doc	Document Creation
06-15-2000	Robert Hayden	1.0	RHayden.doc	Final document

REVIEWERS

Name	Position

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1 Introduction

1.0 Purpose and Scope of Document

Due to the size, complexity, and geographic dispersion of computer networks today, a mechanism to remotely monitor and manage network devices is necessary. NT servers are included in the set of devices than may require remote management, along with other OS servers, routers, switches, probes, etc.

SNMP (Simple Network Management Protocol) is a protocol that allows this remote management and monitoring capability. Additionally, SNMP is the protocol recommended by the IETF (Internet Engineering Task Force) for the remote management of nodes on an IP (Internet) network. (Windows NT SNMP – O'Reilly) SNMP is described in the IETF RFC 1157, "A Simple Network Management Protocol".

Microsoft provides the SNMP service so that NT servers may be remotely monitored and managed using any of the vast array of monitoring/managing software tools currently available which are based on the SNMP protocol. This management/monitoring capability may be part of a complete network management/monitoring strategy, or may be focused on the NT server space alone.

Unfortunately, the default installation of the SNMP service on Microsoft Windows NT 4 leaves the NT system vulnerable to malicious actions. This document describes the various vulnerabilities that exist when the SNMP service is installed on NT 4, and actions that can be taken to minimize those vulnerabilities. The purpose of this document is to alert system administrators to the vulnerabilities, and to provide steps to secure NT implementations that choose to use SNMP for management/monitoring.

This material covers an aspect of the Windows NT Security: Step by Step course (Track 6 – SANS 2000 San Jose) that received only brief treatment in the course text under the "SNMP Snooping" heading on page 21.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1.1 Supporting Documents / References

IETF RFC 1157 "A Simple Network Management Protocol"

Internet Security Systems (ISS) – Online help for Internet Scanner v6.01

Microsoft Knowledge Base Articles
- Q135597 - "No prompt to Restart When Adding SNMP Community Names"
- Q228543 – "Policy editor does not read SNMP communities correctly"
- Q200890 – "SNMP Security Extended by service pack 4"
- Q99880 – "SNMP agent responds to any community name"
- Q186473 – "You can delete all records on a WINS server using SNMP"

Windows NT Security: Step by Step by Fossen/Johansson May 11, 2000

Windows NT SNMP – O'Reilly description on www.ora.com

1.2 Acronyms and Definitions

IETF	Internet Engineering Task Force
MIB	Management Information Base
RFC	Request for Comments
SNMP	Simple Network Management Protocol (or, "Security Not My Problem", as it is sometimes less than affectionately known)

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2 Vulnerabilities

The default installation of SNMP service will respond to any "community string", which can be thought of as a password. Additionally, the service will honor requests for both read ('get') and write ('set') functions. Having information readable or writable from a remote location is a serious vulnerability.

2.0 Information Readable

The ability to read critical information from a remote location without any authentication makes NT servers vulnerable to information gathering reconnaissance, one of the first phases in planning an attack from the outside. The following information is all accessible, verified by using an SNMP MIB browser tool operating against a default NT 4 SNMP service installation (SP3).

Shares

Share names often give clues as to their contents, a first step in determining whether a particular server is worthy of the effort required to break in. This process can be thought of as a hacker cost-benefit analysis.

User Names

User names are enumerated, providing a starting point for either a brute-force cracking effort, or they may be used in social engineering attacks or to determine what type of machine is being probed (i.e.: a PDC will have many users).

Status of running services

Services running can be determined. This information, as well as the information described above, is used as the basis for further attacks. For example, knowing that RAS, WINS, DHCP, or Network Monitor are running gives a hacker valuable information upon which to base future actions.

Other information

A wealth of other information is available which can be useful in reconnaissance efforts. For example, computer and domain names, network adapter properties, media type, other IP addresses, etc. can all be used to build a clearer picture of the network, and the place/function that the server being probed plays in the network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

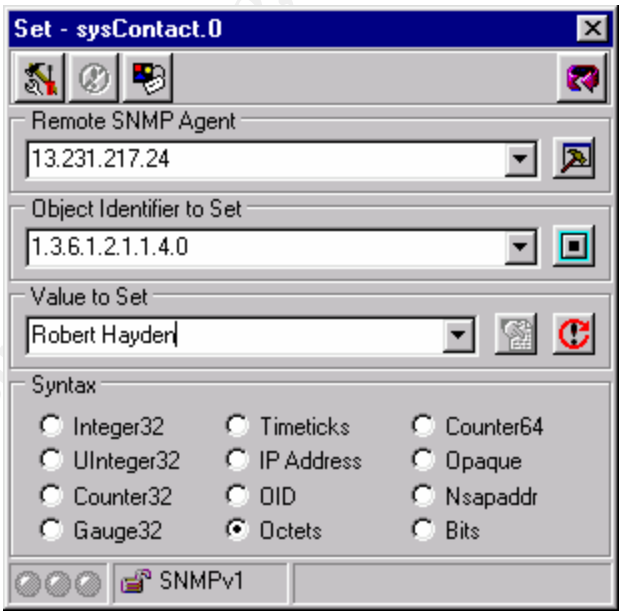
2.1 Information Writable

Having information readable is dangerous enough. Imagine the possibilities that exist when the capability to UPDATE information on the server exists. One example is turning the state of the network interface to OFF.

Microsoft's knowledge base contains a rather ominous sounding article entitled "You Can Delete All Records on a WINS Server Using SNMP" (Q186473). This underscores the damage that can be done with an unprotected SNMP service (known as an SNMP Agent).

ISS Internet Scanner vulnerability assessments at my company frequently find machines that are secure in most ways except that SNMP 'sets' (writes/updates) are allowed.

In the figure below, the contact information for a server is updated to Robert Hayden using the MG-SOFT MIB Browser Professional Edition, from a remote location. The use of this tool is beyond the scope of this document, however it



should be noted that a graphical interface was used to easily locate the contact information field (shown as sysContact.0) in the header bar at the top of the figure. Other information is just as easily located, such as computer name.

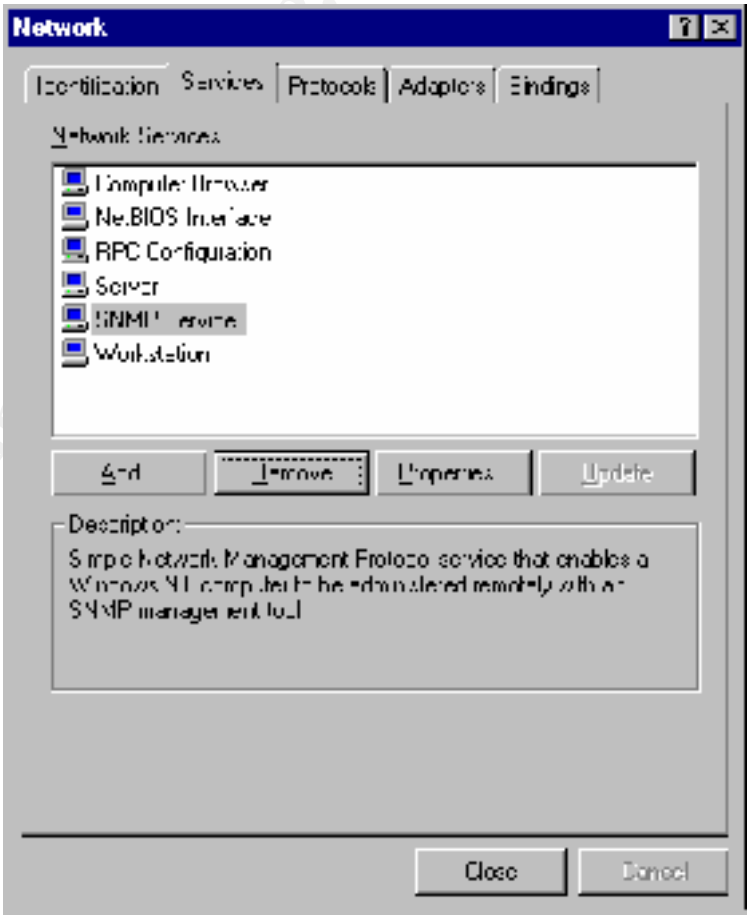
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3 Controls

A step by step procedure for controlling the security exposure of having SNMP service running follows.

3.0 Deinstall SNMP if it is not necessary

A properly secured NT installation will only be running services that are necessary for the intended operation of the machine in question (Windows NT Security: Step by Step, pg. 47). The SNMP service is no exception: if the SNMP service (the agent) is not necessary, remove the service as follows. Open the **Control Panel**, then double-click on **Network**. Click the **Services** tab, select **SNMP**. Click **Remove** (or press enter, as Remove will be pre-selected) as shown in the following figure, and then click **Yes** when presented with the warning dialog asking for confirmation of your action.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

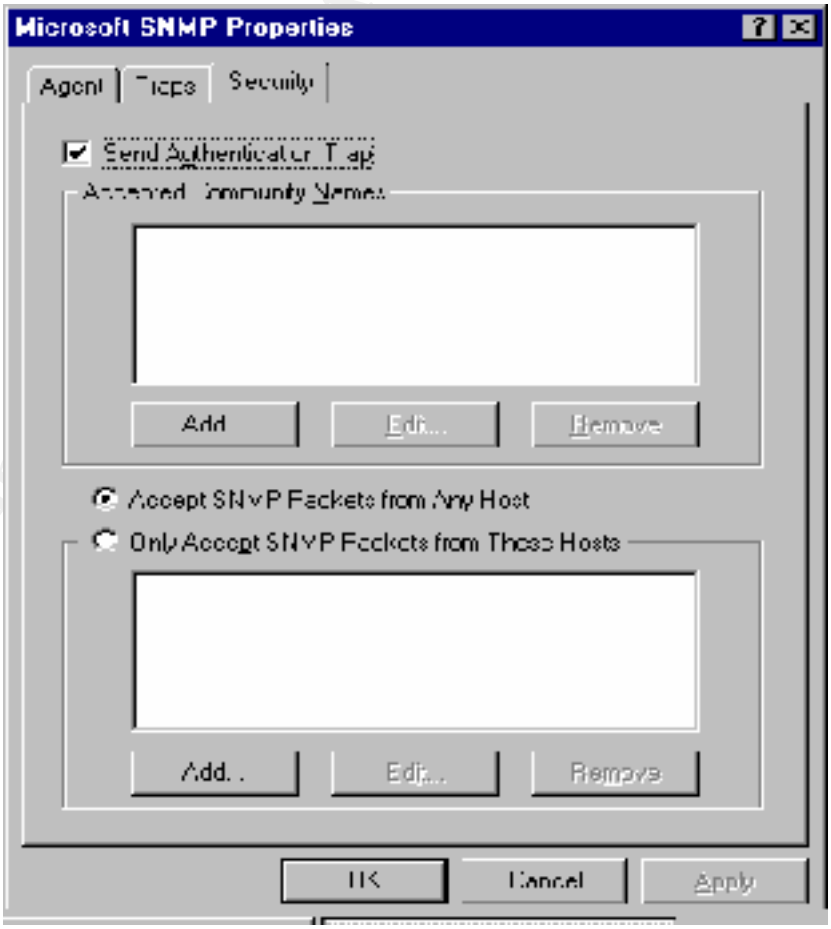
3.1 Proper SNMP Configuration

SNMP was designed as an "open" protocol lacking robust authentication capabilities. Later versions of SNMP (notably SNMPv3) have enhanced security capabilities. However, the Microsoft agent or service does not support SNMPv3. For this reason, proper configuration is essential to ensure the highest level of protection possible given the limitations of the SNMP protocol.

Define at least one community name string

When no community name strings are specified, the SNMP Agent/Service will respond to set/get requests from any provided community string. This is by design. (Reference RFC 1157).

A default installation of SNMP service has no defined community strings, which essentially leaves the machine wide open to SNMP set/get from anyone who can send an SNMP packet the computer, and who selects ANY community string. The following figure illustrates this (empty Accepted Community Names box).



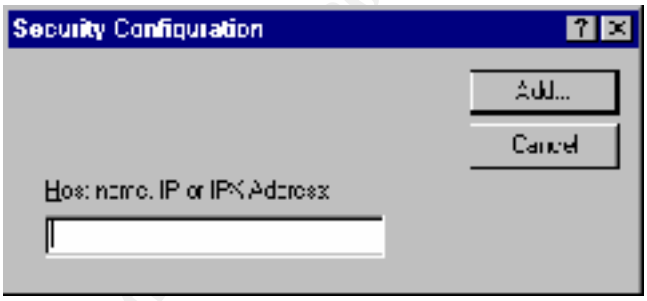
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Choose a community name other than "public"

The community string of "public" is well known and should not be used. This is equivalent to the default passwords that ship with many software packages today. The hackers are aware of them, and will be the first ones tried when attempting to break into a system. Place the community name(s) into "Accepted Community Names" box shown in the previous figure.

3.2 Host Filtering

As shown in the figure on the previous page, by default SNMP packets are accepted from *any* host. However it is possible to prevent the SNMP service from processing packets from hosts other than those specified, by selecting the option "Only accept SNMP Packets from These Hosts", and then clicking the "Add" button. This will bring up a dialog where you may specify hostname, IP address, or IPX address, as shown in the following figure.



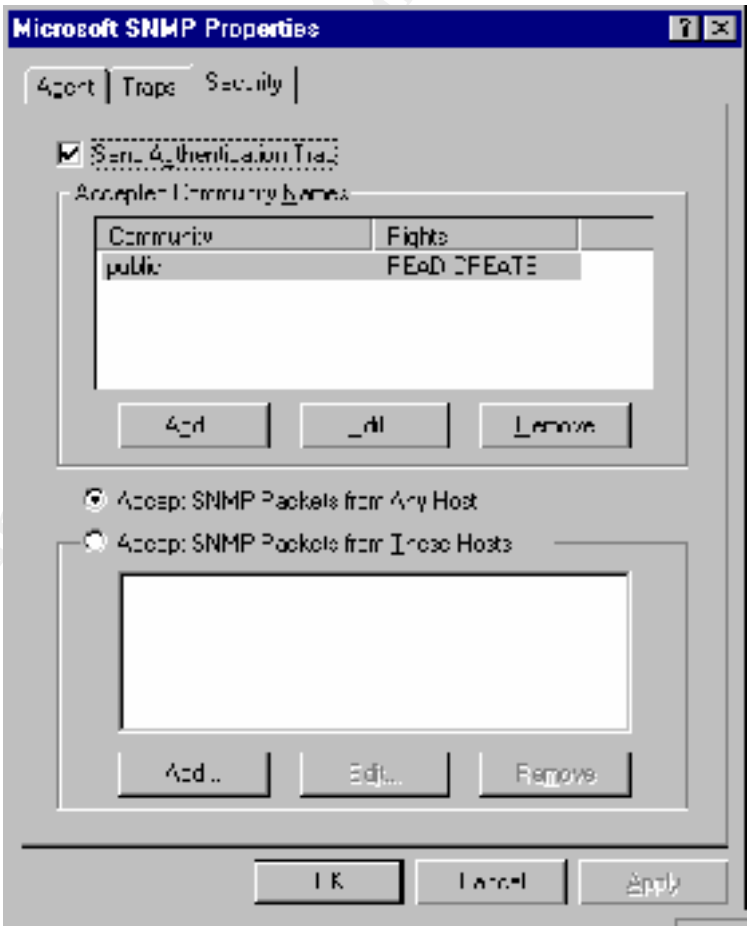
Enter the information, and click "Add". This will return you to the figure on the previous page. However, the host or address just specified will appear in the lower window under "Only Accept SNMP Packets from These Hosts".

It is important to understand however, that because SNMP uses UDP packets, the source IP address is spoofable. This makes it possible to issue SNMP 'set' commands, and a response to the issuer would not be necessary. In order to be successful at such a spoof, however, the IP hosts that are allowed to communicate to the SNMP service would need to be known in the first place. This could be accomplished via a network sniffer, or by accessing the registry where this information is stored. Information on protecting the registry is provided in section 3.6.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.3 Upgrade to the latest service pack, minimally SP4

Prior to SP4, the NT SNMP service gives all community names write access when SNMP 'set' commands are received using those names. For this reason, updating to SP4 is critical if the SNMP service is to be installed. Additionally, interoperability issues have surfaced as third party SNMP management consoles are developed. Some of these issues were based on Microsoft software bugs, and there has been a number of post-SP4 SNMP bugfixes. For this reason, if at all possible the *latest* service pack should be installed. This is good practice in general anyway.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

After upgrading to SP4, the appearance of the SNMP Properties page will change to reflect the addition of community string access levels, as defined in section 3.4 below. Note the addition of a "Rights" column along with the "public" community string now coming along as a default value in the preceding figure. As mentioned earlier, the community string of "public" is well known and should not be used. Verify that the string "public" does not exist as it does in the screen shot.

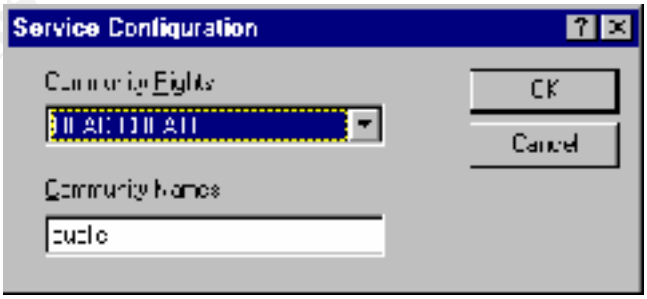
3.4 Utilize community string access levels

SP4 adds new security settings with regard to SNMP. These settings are accessible by going into the **Control Panel**, then double-clicking on **Network**. Click the **Services** tab, select **SNMP**, click **Properties**, and then click on the **Security** tab.

Each community string may have a host defined access level as follows:

- NONE – Cannot read or write any variables
- NOTIFY – An unsolicited message is sent to an SNMP management station
- READ-ONLY – Cannot set any values
- READ-WRITE – Can read or write any values that the MIB definition allows.
- READ-CREATE – Allows the creation of a new row

The access levels assigned to community names, and the community names themselves, are changed by clicking "Edit" button after selecting (highlighting) the row of data to be modified. The following box will appear:



The pulldown values will be as identified in the bullets above.

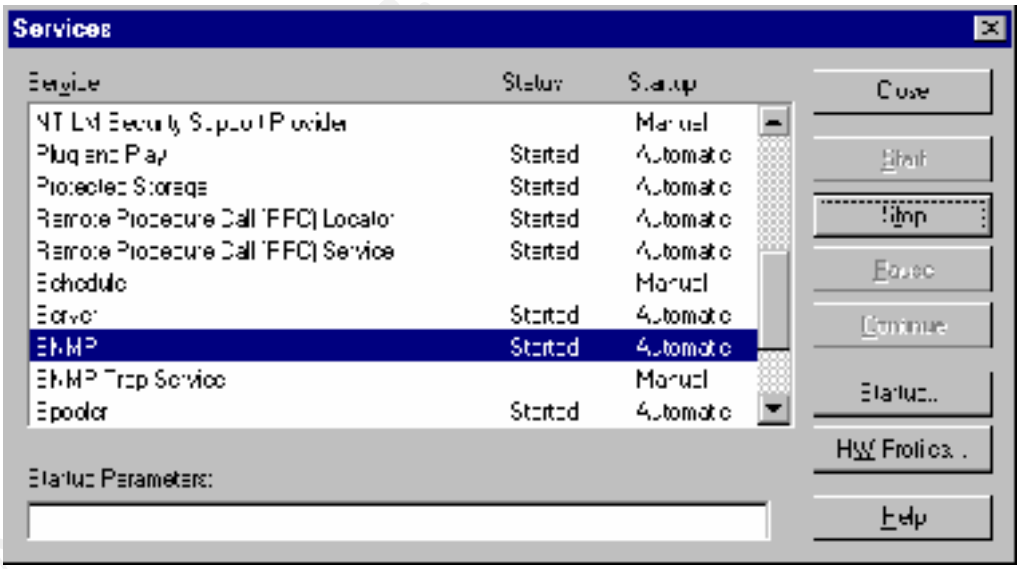
The MIB access variables (items that can be read or written) have their own 'built-in' access levels. The more restrictive of either MIB access variable access levels or host defined access levels are what determine ultimate access.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Host based access levels should be defined in accordance with application requirements. In many cases, READ-ONLY is sufficient for monitoring applications. READ-WRITE and READ-CREATE levels should only be assigned after careful consideration of the application and of the other controls in place surrounding SNMP.

3.5 Reboot if community name strings are added

A bug in the Microsoft software (Q135597) allows the network setting dialog box to be closed without prompting for a system restart, after adding an SNMP community name. This results in SNMP community names added not being recognized until after the system restarts. As a workaround, shutdown and restart Windows NT. Alternatively, you may stop and restart the SNMP service. This is accomplished by opening Control Panel, then double-clicking Services. Scroll down to SNMP and highlight as shown in the following figure. Click "Stop", and then respond to the dialog box that appears asking for confirmation. Once the service stops, you can start it by clicking on the "Start" button as shown.



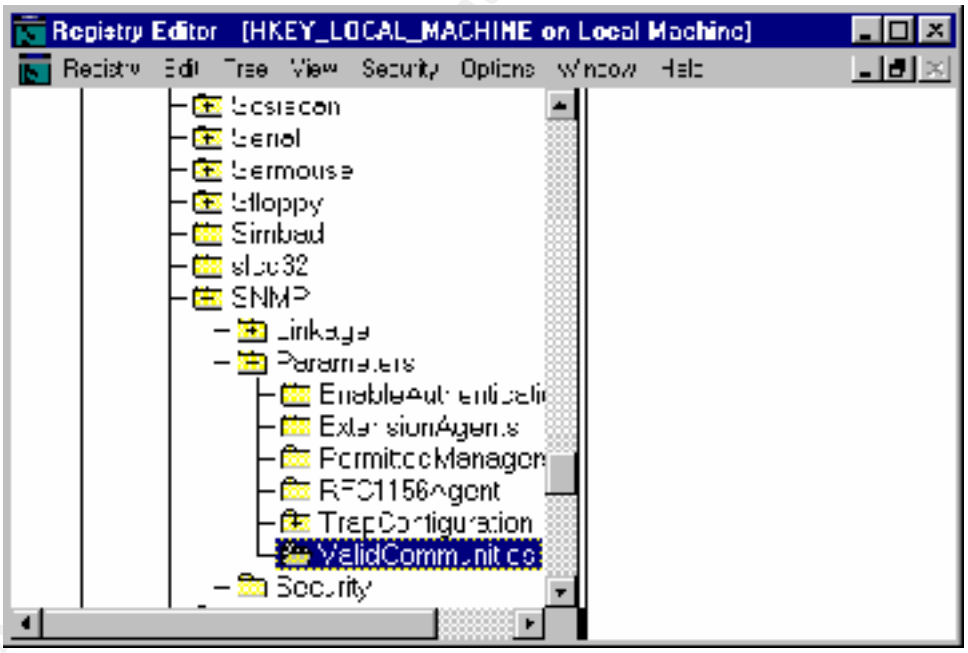
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.6 Restrict Registry Key Access

Additionally, restrict the ability to read the SNMP community string(s) from the server registry by setting registry key permissions to only allow approved users access to the following:

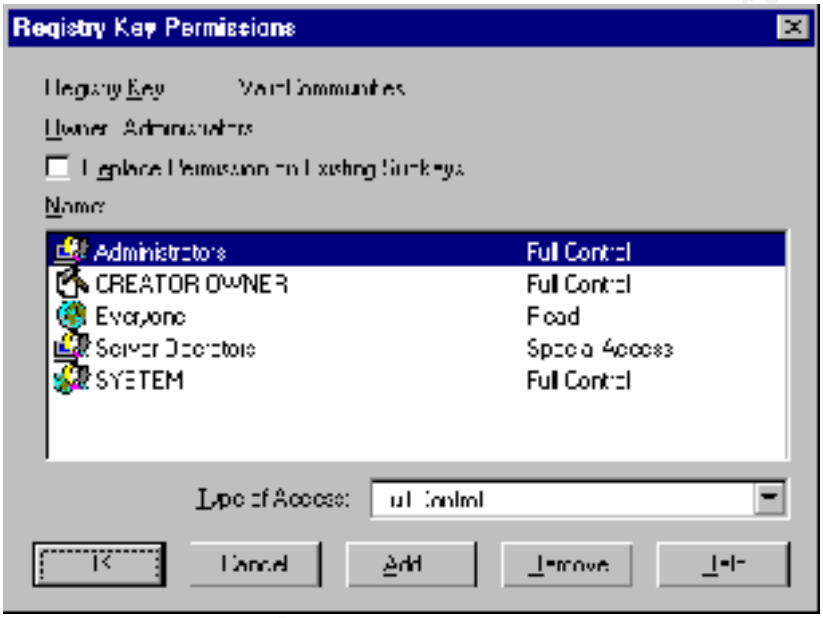
Hive Key	HKEY_LOCAL_MACHINE\System CurrentControlSet\Services\SNMP\Parameters\ValidCommunities

This is accomplished by going into the REGEDT32, selecting the key above (shown selected in the figure below), then using the Security menu to select Permissions, and assigning access only to those requiring access to the community strings.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In the example figure below, the Everyone group should be removed from those who have permission to access the community names via the registry. One alternative to granting read access to the Everyone group is to instead use "Authenticated Users".



One reason for setting the permission on the registry key is because of other NT vulnerabilities that may not have been controlled. For example, remote access to the registry may still be possible, in which case allowing Everyone to have read access is giving it to anyone, authenticated or not.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

SANS Security West 2017	**San Diego, CA**	**May 09, 2017 - May 18, 2017**	**Live Event**
SANS Northern Virginia - Reston 2017	**Reston, VA**	**May 21, 2017 - May 26, 2017**	**Live Event**
SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**