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
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Default SNMP Community Strings Set to “public” and “private”
by James Romanski
GIAC Advanced Incident Handling and Hacker Exploits Practical Assignment Option 2
SANS Security DC 2000
August 12, 2000

Exploit Details

Name

Default Simple Network Management, SNMP, community strings set to “public” and “private”.

Variants

Other variants of this attack consist of other easily guessable or default SNMP community strings such as “all private” and “snmpd”.

Operating System

All system and network devices running SNMP agents.

Protocols/Services

This exploit uses the Simple Network Management Protocol that communicates using UDP port 161.

Brief Description

The Simple Network Management Protocol, SNMP, is a commonly used service that provides network management and monitoring capabilities. SNMP offers the capability to poll networked devices and monitor data such as utilization and errors for various systems on the host. SNMP is also capable changing the configurations on the host, allowing the remote management of the network device. The protocol uses a community string for authentication from the SNMP client to the SNMP agent on the managed device. The default community string that provides the monitoring or read capability is often “public”. The default management or write community string is often “private”. The SNMP exploit takes advantage of these default community strings to allow an attacker to gain information about a device using the read community string “public”, and the attacker can change a systems configuration using the write community string “private”. The opportunity for this exploit is increased because the SNMP agent is often installed on a system by default without the administrator’s knowledge.

Protocol Description

The Simple Network Management Protocol was designed to provide a means of managing and monitoring diverse network devices. SNMP has a client-server architecture and uses unencrypted text known as community strings

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

for authentication. Communication between the client and server is accomplished using a message called a protocol data unit or PDU. There are four commonly used PDUs: a get request, a get next request, a set request, and a trap message.

The get request is used to fetch a specific value that is stored in a table on the server. The table is called the Management Information Base or MIB. The MIB values are referenced using a series of dotted integers. For example a request for the MIB variable "1.3.6.1.2.1.1.1" would return the system description for the network device.

The get next request fetches the next MIB variable subsequent to the last request. This allows the client to walk though all the variables in the MIB table and gain a great deal of information about the network device.

The set request allows the client to set a MIB value. This can be used to change the configuration of the host such as redefining interfaces parameters. This is a very powerful function and requires a community string with write access for authentication.

The trap message is sent from the network device to the client. This trap is event triggered and allows alerts to be sent when certain system states are reached. This PDU is different from the other three PDUs because the communication originates at the server and is pushed to the client.

How the exploit works

SNMP is vulnerable because it is often automatically installed on many network devices with “public” as the read string and “private” as the write string. This would mean that systems might be installed on a network without any knowledge that SNMP is functioning and using these default keys.

This default installation of SNMP provides an attacker with the means to perform reconnaissance on a system, and, an exploit that can be used to create a denial of service. SNMP MIBs provide information such as the system name, location, contacts, and sometimes even phone numbers. This soft intelligence can be very useful in social engineering. An attacker could call an organization and use the system contact and system name to gain a password from an unsuspecting user. The telephone number for the system contact could be used to provide a dialing prefix that the attacker could use for war dialing.

SNMP information also provides a great deal of hard intelligence about the system. One MIB provides the system description that reveals the operating system that the host is using. This can be matched against known exploits that would allow the attacker to gain further access into the SNMP host. SNMP data also provides interface descriptions, types, and other interface configuration information. This interface information can be

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

gathered from more that one system to allow an attacker to piece together a network map of an organization showing how systems are interconnected.

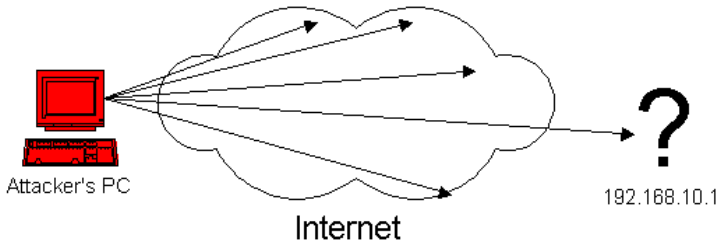
Some MIBs are writeable allowing the attacker to change the system configuration creating a denial of service opportunity. One such MIB is “ifAdminStatus”. “IfAdminStatus” is set to “1” when the interface is operational and to “2” when it is down. An attacker could set “ifAdminStatus” to “2” using the SNMP set PDU which could disconnect the host from the network creating a denial service.

Description of variants

“Public” and “private” are not the only default or easy guessable community stings which are used. Some Solaris systems use “all private” by default. HP SNMP agents have been known to use “snmpd” as their default community strings. A Compaq customer advisory notice stated that, “Insight Manager Console using Compaq Insight Manager Version 3.00” will only use the first three characters of any community string that is used, making this agent very susceptible to a brute force SNMP attack.

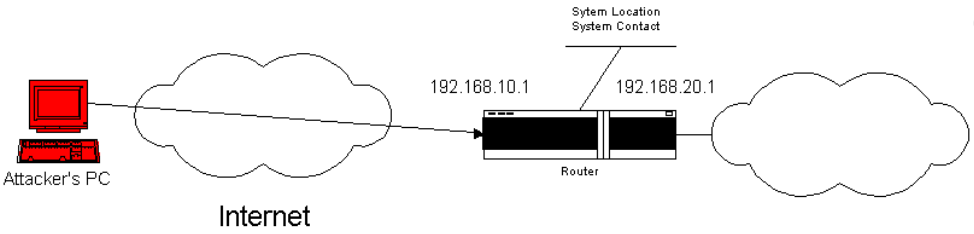
Diagram

In this example the attacker launches an SNMP scan against a range of addresses on the Internet. This scan has resulted in a device at IP address 192.168.10.1 responding to an SNMP request with a community string of “public”.

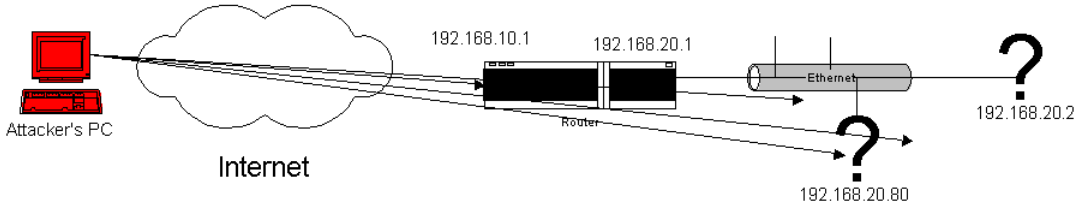


Zeroing in on the device, the attacker further scans 192.168.10.1 to obtain the values of all of its MIBs. Using this information the attacker has determined that this device is a router with a serial and an Ethernet interface. The serial interface has an IP address of 192.168.10.1 and the Ethernet interface has an IP address of 192.168.20.1. He has also determined that the device is located at 1313 Mockingbird Lane and that the system contact is Alfred Newman.

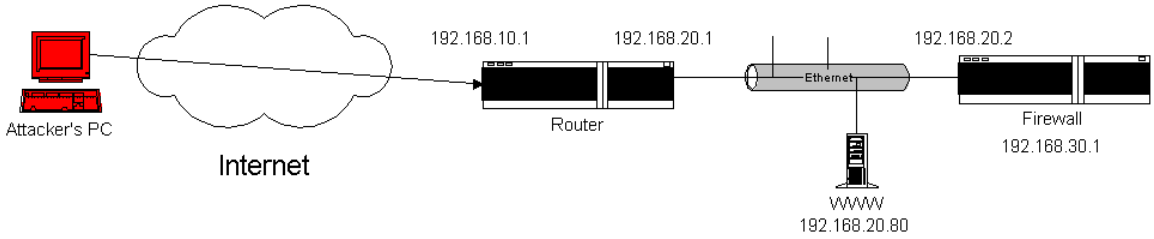
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Next the attacker conducts a SNMP scan with “public” as the community string on the 192.168.20.0 network and discovers two other devices at 192.168.20.80 and 192.168.20.2.



Conducting a more detailed SNMP walk against both IP addresses the attacker determines that the device at 192.168.20.80 is a web server and the device at 192.168.20.2 is firewall with another interface at 192.168.30.1. The attacker attempts to conduct further SNMP scans into the 192.168.30.0 network but these are blocked by the firewall.



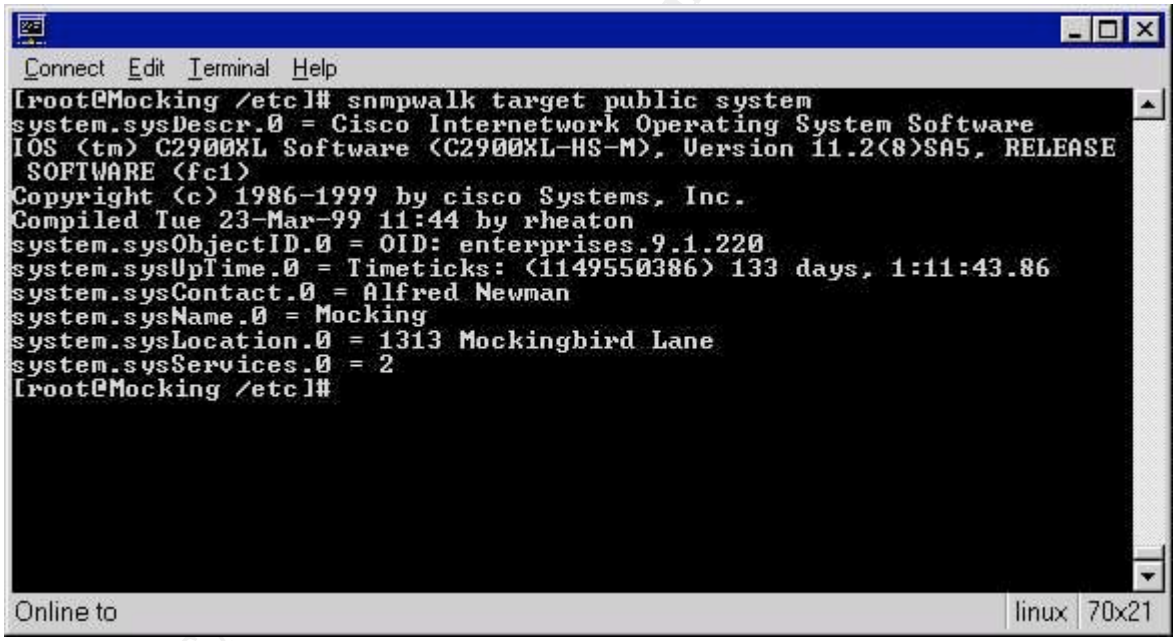
Using the information that attacker has gathered from the SNMP scans he can attempt to change the configuration of the three devices using the write community string “private”. There is a good chance that this may work since the default community string “public” permitted read access of the MIB variables. The attacker could down the router’s interface and prevent all access to the Internet for the organization. He could down the interface of the web server to create a denial of service to the organizations web server. He could also down the firewall’s interfaces and prevent the organization from accessing the Internet. Downing all of the interfaces, firewall, web server, and router would cause a catastrophic incident making the problem difficult to troubleshoot.

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

How to use it?

Snmpwalk and Snmpset

Snmpwalk and snmpset are part of a group of tools originally developed at Carnegie Mellon University. These tools run on various Unix, Linux and Windows platforms. Snmpwalk uses the get-next function of SNMP to walk though the MIBs on an SNMP host. In the below example, the attacker could use the command “snmpwalk target public system”, “Target” is the system name of the server running the SNMP agent. “Public” is the community string and “system” is the group of MIB variables that will be polled. If the MIB variable field were left blank, snmpwalk would output all the SNMP variables for the host. Running the command generates the following.

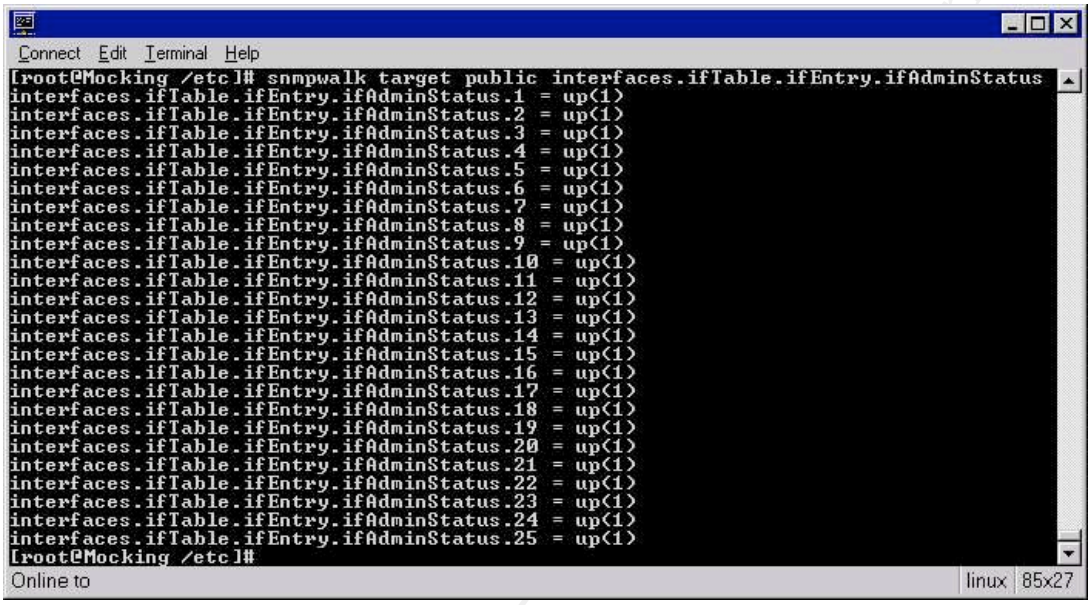


Looking at the above results we can see that this device is a Cisco 2900XL. It is running Version 11.2(8) of the IOS software. The system type and the version of the software could be checked against known exploits to launch further attacks against the device. The system contact is Alfred Newman and it is located at 1313 Mockingbird Lane. Using this information an attacker could call and organization posing as Alfred Newman and try to gain further information or even logins and passwords.

Snmpset invokes the set PDU that is used to change the value of writeable MIB variables. This can be used to create a denial of service by changing the configuration of an interface. For example, we can use

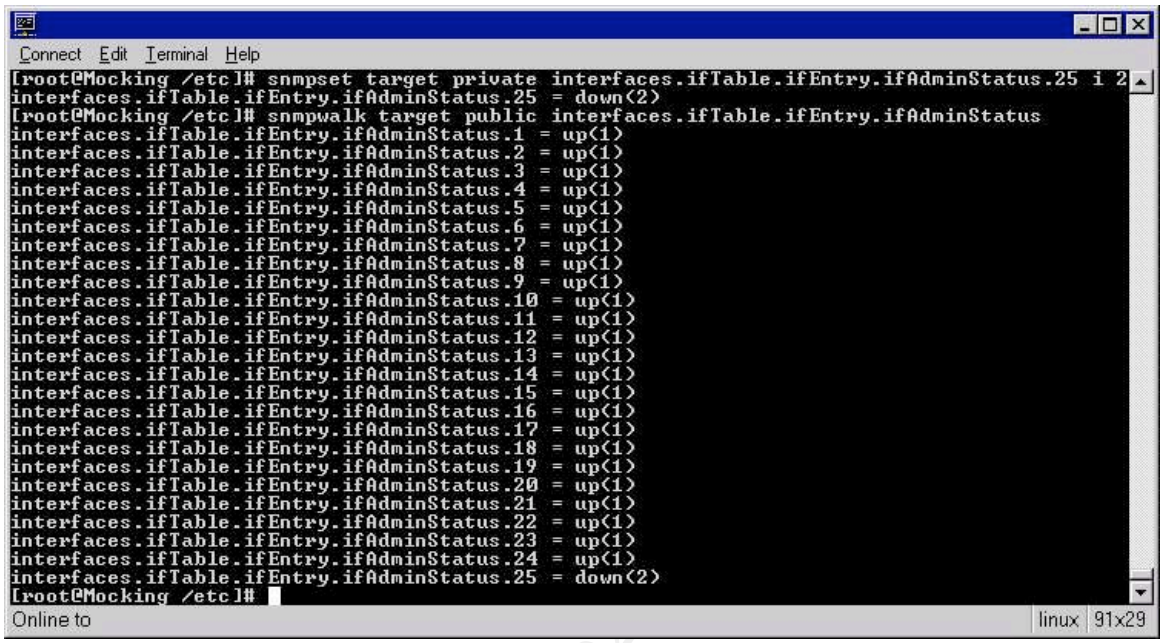
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

snmpwalk to gain interface information about “target” using the command “snmpwalk target public interfaces.ifTable.ifEntry.ifAdminStatus” giving us the following output.



Using this information we could change any of the twenty-five interfaces’ “ifAdminStatus” from 1 (up) to 2 (down). In this example we will use the command, “snmpset target private interfaces.ifTable.ifEntry.ifAdminStatus.25 i 2”, to bring the twenty-fifth interface down.

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

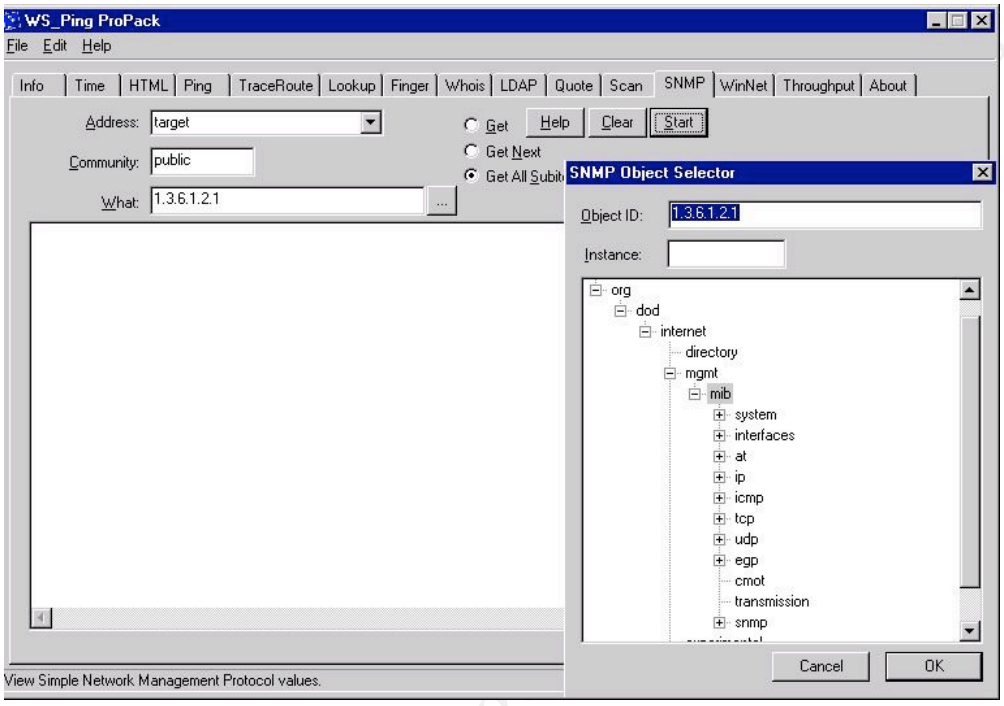


The snmpwalk command run after snmpset confirms that the “ifAdminStatus” of interface twenty-five changed to down. This could disconnect the device from the network causing an outage. Recovering from this attack could be made extremely difficult if all the systems interfaces are taken off the network because it would force the system administrator to be physically in front of the device to resolve the problem.

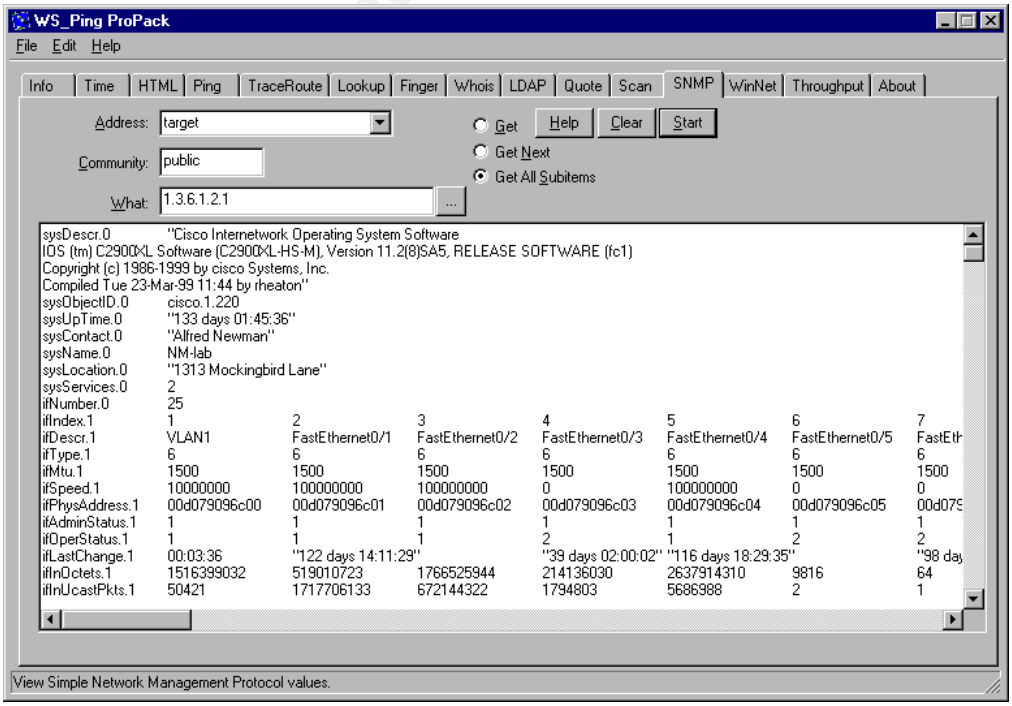
WS Ping Pro Pack

WS Ping Pro Pack provides a finished Windows product with a sharp GUI that makes it very easy to gather SNMP information. Simply open WS Ping Pro, click on the SNMP tab and then enter an address of the SNMP agent and community string. Clicking on the “What” drop down box allows the users to select the specific MIB object or group of objects to scan. Selecting “Get all Subitems” will walk all the MIB objects after the object selected in the “What” box. In this example we will now walk the MIBs of the system “target” using WS Ping Pro.

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

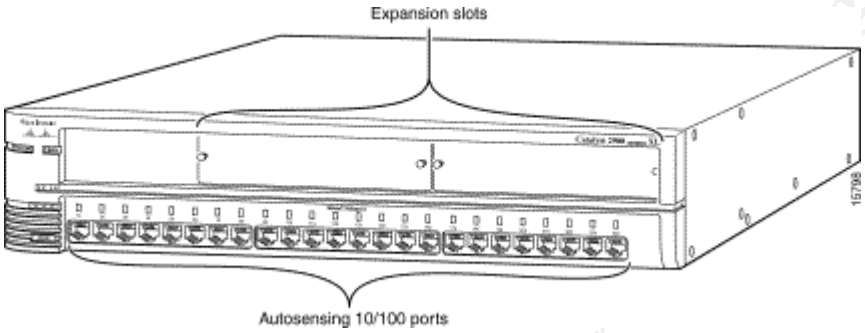


Selecting start from the above window will walk though the MIBs and produce the following output.



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

In this example WS Ping was run against a Cisco 2924XL which is a twenty-four port switch that looks like:



This picture can be compare with the output of the first five ports from WS Ping:

ifIndex.1	1	2	3	4	5
ifDescr.1	VLAN1	FastEthernet0/1	FastEthernet0/2	FastEthernet0/3	FastEthernet0/4
ifType.1	6	6	6	6	6
ifMtu.1	1500	1500	1500	1500	1500
ifSpeed.1	10000000	100000000	100000000	0	100000000
ifPhysAddress.1	00d079096c00	00d079096c01	00d079096c02	00d079096c03	00d079096c04
ifAdminStatus.1	1	1	1	1	1
ifOperStatus.1	1	1	1	2	1

The output of WS Ping almost matches the physical layout of the device which helps to paint a picture in the users mind. Reviewing this output we can see that the first port is a virtual interface and ports 2 through 5 correspond to the first four physical interfaces on the switch. The MIB “ifType.1” has a value of 6 which indicates all of the interfaces are Ethernet. “IfMtu.1” shows the maxim transmission unit for each interface and the “ifSpeed.1” shows that four of the 5 interfaces are configured for 100 Mbs. “IfPhysAddress.1” corresponds to the MAC address for each interface. The “ifAdminStatus” is a writeable MIB that can be configured to bring the interface up (value=1), down (value-2), or in a test mode (value=3). “IfOperStatus.1” is a MIB that is closely related to “ifAdminStatus”. “IfAdminStatus” can be thought of as a desired state where “ifOperStatus” reports the actual status. An “ifOperStatus” value of 1 indicates that the interface is up, 2 indicates that the interface is down, 3 indicates that the interface is in a test mode, 4 indicates in a unknown status and 5 is a dormant value.

Signature of the attack

An attack using the SNMP exploit can by identified by observing unauthorized systems trying to access hosts on your network using the UDP port 161. You can see an attempt in the following log entry from the Linux firewall package Ipchains.

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

```
Aug 10 19:15:59 cm-192-168-20-2 kernel: Packet log: bad-if DENY eth0
PROTO=17 162.168.10.38:1097 192.168.202:161 L=132 S=0x00 I=59140
F=0x0000 T=128 (#10)
```

The field “PROT=17” indicates UDP protocol and “24.29.66.119:161” shows an attempt to connect to port 161. Further examination of this unauthorized traffic would reveal that the unauthorized client trying to use “public” or “private” as community strings.

Authorized SNMP gathering systems are internal network management platforms such as IBM’s Tivoli, Concord’s Nethealth or Network Associates’ Router PM that use SNMP to track availability and utilization of network devices.

How to protect against it?

The principle of least privileges is the best method to avoid the SNMP exploit. SNMP should not be enabled on devices that do not require it. It is more secure to push the information from the managed devices using SNMP traps rather that polling the devices using SNMP agents. SNMP community write strings can be disable if the network management platform only poll devices and does not change the remote devices configuration.

If SNMP is needed the community strings should be set at their maximum length and include a combination of letters, numbers, and special characters to avoid a brute force attack. All network devices should be scanned using an SNMP vulnerability scanner to ensure that they do not use the default community strings.

SNMP access should also be limited to only the devices that require SNMP for monitoring. This can be accomplished by allowing only authorized clients to access UDP port 161. All access to UDP port 161 should be denied from external networks.

Source code/ Pseudo code

All of the exploit tools were found using a search engine. Snmpwalk and WS Ping Pro Pack all use an algorithm similar to the following:

```
while not error
    begin
      getnext MIB
      print MIB MIB-value
    end
```

Snmpwalk and Snmpset

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

Snmpwalk and snmpset can be found at ucd-snmp.ucdavis.edu. Snmpwalk and snmpset are also part of the ucd-snmp-utils-4.1.1-2 rpm.

WS Ping Pro Pack

WS Ping Pro Pack can be found at www.ipswitch.com.

Additional Information

References and Links to additional information:

1. The SNMP FAQ
   www.faqs.org/faqs/by-newsgroup/comp/comp.protocols.snmp.html

2. RFC 1574 Evolution of the Interfaces Group of MIB-II
   www.faqs.org/rfcs/rfc1573.html

3. RFC 1212 Concise MIB Definitions
   www.faqs.org/rfcs/rfc1212.html

4. An Introduction to Network Management
   www.inforamp.net/~kjvallil/t/snmp.html

5. DDRI SNMP Overview
   www.ddri.com/Doc/SNMP_Overview.html

6. Insight Manager 3.00: Default Community String
   www.compaq.com.pl/support/techpubs/customer_advisories/s0627-03.html

7. Cisco 2900XL Overview
   www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35sa6/ig_2900/maoverv.htm

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