Global Information Assurance Certification Paper

Lookman Y. Fazal

The Simple Network Management Protocol(SNMP)is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. 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.

Searching the BugTraq database reveal quite a few SNMP vulnerabilities. Before you panic, the vendors have patched many of the vulnerabilities discussed here. However, we all know how hard it can be to stay current on vendor fixes, especially when they have a tendency to break something else that is working. Also, some of the tech-notes referenced describe best practices vs. a specific vulnerability. Here are some of the favorites:

A. Insecure perimeter

SNMP queries may be inadvertently allowed to firewalls and packet filters. If this condition is true, then remote network scanners could be able to obtain the exact filter rules for your network.

B. Not securing the defaults

The default community name for the SNMP string is PUBLIC. Some products are shipped this way. This is of course the first thing the attacker will look for. The solutions to this and the way to prevent this are that products should force you to enter a community name which of course is hard to guess string. A combination of alpha numeric is the best choice.

C. Worse then PUBLIC

Having no community name at all is worse than having just PUBLIC because now anyone can access the device, learn whatever they can from the device, and possibly alter its configuration.

D. Stop authentication trapping

An advisory was issued about the ability to write to the snmpEnableAuthenTraps object within various systems. Potentially, an attacker could prevent the device from sending traps for failed authentication. Then the attacker could take his time to crack the admin password for the device, all without drawing attention to his activity.

E. Controlling the access

A common problem mentioned is to not control the Read-Write community tightly, giving the wrong people the ability to alter the device. What this could lead to is having an attacker cause problems by bringing down the interface.

F. Hidden SNMP communities

In 1998, HP Openview was found to have a hidden SNMP community string that exists in various versions of HP OpenView. This community may allow unauthorized access to certain SNMP variables. Attackers may use this hidden community to learn about network topology as well as modify MIB variables. It was soon found that this problem extended to other vendors' products such as Sun Solstice and Solaris

G. Windows NT

The problem with NT was that before Service Pack 4, communities could not be set to read-only. So an interface could be brought down, or WINS records be deleted or changes could be made to the routing table, if someone had access to a server with SNMP enabled. To make matters worse, the default community name was still PUBLIC, giving an attacker an open door. Of course, Microsoft being security paranoid, fixed the bug in Service Pack 4, unfortunately Service Pack 4 had other problems such as memory leaks which consumed all of the machines resources. But we all have SP5 now don't we?

H. ICMP echo requests

Some routers for example Cisco can be configured to issue ICMP echo requests through the SNMP agent. If you repeat this numerous times the memory of the router can be filled. This would cause performance problems and an inability to respond to the ICMP echo requests.

I. Remote Packet Capturing

There are tools that do packet-capturing over the network using SNMP. Now this could lead to an attacker who is eavesdropping to obtain information about the network and other critical data. Two such tools come to my mind are Microsoft's NetMon and NAI's Distributed Sniffer.

J. Printer hiccups

HP printers, Series 5 lets malicious people execute DOS attack by sending SNMP gets, specifically the older firmware in the HP Series 5 printers.

Subscribing to mailing list with security advisories and keeping patches current are some of the things which need to be done to keep SNMP security problems away, some others are:

- To keep a migrating path in mind off of Snmp Version 1 as Snmp Version 1 has no security built in. If you had a sniffer, you could easily sniff the entire sequence of packets needed to reboot a device. Snmp Version 2 encrypts this kind of traffic.

- The first question you should ask is if the host really needs SNMP. It isn't worthwhile if you only require SNMP on a host to let the Network Operation Center to be able to see when the host is unavailable.

- Access Control Lists. Make sure you implement ACL filtering to only allow access to your Read-Write community from approved stations or subnets.

- Guessing the community strings should be made difficult.

Task force such as IETF is working on making SNMP harder to hack. SNMPv3 has some really good and promising features. SNMPv3 framework addresses the deficiencies in SNMPv2 relating to security and administration. It incorporates most of the advancements that working groups put forth for the elided SNMPv2, while also addressing various shortcomings of the original SNMP. Some of the features include the "GetBulk" operator, 64-bit counters, an improved "Set" operator and the addition of a unique ID for each SNMP engine. Best of all, SNMPv3 brings a powerful, complex security model to the table.

The latest version also proposes several changes to the SNMP management framework itself, such as adding the ability to update configuration parameters in the SNMP agent via SNMP, thus enabling complete remote management of SNMP devices. Finally, SNMPv3 adds an "snmpEngineID," as well as the ability to address multiple contexts within a managed device. These features help track relationships within a network topology, aid in authentication and address more complex network infrastructure components that have multiple logical contexts within a single managed device. For example, with SNMPv3, each port on a switch can be addressed as a logical bridge inside the switch object.

As the long-awaited next-generation SNMP embarks on the road to standardization, we peer closely at the protocol's early implementations and continue to examine possible implications of the newcomer on secure network management in the enterprise.

Radcliff, Deborah “Cover your SNMP”, 2/7/2000, URL:
http://www.computerworld.com/cwi/story/0,1199,NAV63-1356_STO41144,00.html

Stuart McClure, Joel Scambray and George Kurtz, Network Security Secrets and Solutions,“Hacking Exposed” Mc-Graw Hill,

Reavis,Jim. “SNMP - simple management tool for hackers?”, Network World Fusion Focus on Security, 10/04/99. URL: http://www.nwfusion.com/newsletters/sec/1004sec1.html

Backman,Dan. “Basking in Glory- SNMPv3”. 9/15/99, URL:
http://www.networkcomputing.com/915/915f1.html

Caruso Jeff. “IETF to tighten SNMP security features”, 10/4/99. URL
http://www.nwfusion.com/archive/1999/77058_10-04-1999.html

SecureTeam.com, “Windows NT's SNMP service vulnerability.”, 11/20/1998, URL:
http://www.securiteam.com/exploits/Windows_NT_s_SNMP_service_vulnerability.html