SimpleSleuth™

An SNMP Vulnerability Probe

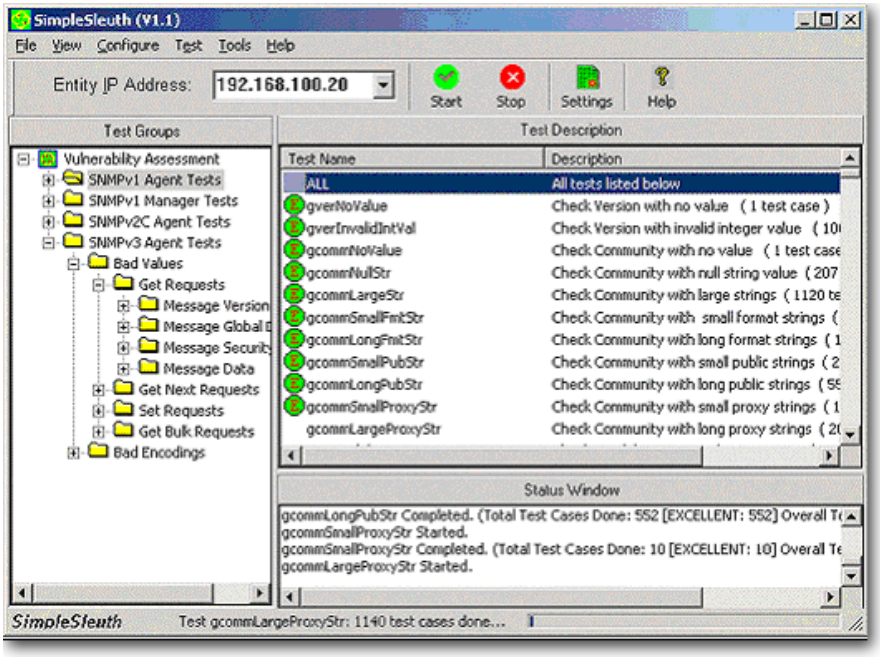

Fig1: Screen shot of the SimpleSleuth running SNMP Agent Tests.

Overview

The Simple Network Management Protocol (SNMP) is used extensively in today's networks to provide configuration and monitoring for a wide variety of networked devices. On 12th February 2002, the CERT advisory announced that products from large number of vendors, when made to process invalid SNMPv1 packets, were susceptible to "denial-of-service" (DoS) attacks.

SimpleSleuth with its associated test modules, extends this approach for all versions of SNMP (v1, v2c, v3) and includes tests for both agent and manager implementations. It dynamically creates close to a million different invalid packets, and then sends them to SNMP implementations under test to check if they are able to handle the packets without failure. Since the SNMP protocol uses the ASN.1 BER (Basic Encoding Rules) to encode SNMP packets, the invalid packets sent by SimpleSleuth typically fall into two categories: badly encoded packets, and bad value packets that are correctly encoded. This allows the different components within an SNMP implementation that decode packets, and then process them, to be checked for vulnerabilities.

SimpleSleuth provides an easy to use interface that simplifies vulnerability testing and enables users to specify the type of test packets to send and then pinpoints the packet that caused the vulnerability. All the test packets are dynamically created allowing the user control over the various values used in the packet. The modular architecture of SimpleSleuth maximizes ROI by allowing users to purchase only the needed test suite modules.

Features

SimpleSleuth is an easy-to-use, Windows-based test tool that probes for vulnerabilities in SNMPv1, SNMPv2c, and SNMPv3 implementations. Using this tool, you can:

- Check ***devices*** and ***managers*** in the network for vulnerability to an SNMP denial-of-service (DoS) attack.
- Verify that a patch actually fixes known vulnerabilities and does not introduce new ones.

Current Modules

- SNMPv1 Agent Test Module (over 189,000 malformed SNMPv1 Get/GetNext/Sets).
- SNMPv2c Agent Test Module (over 272,000 malformed SNMPv2c Get/GetNext/Set/GetBulks)
- SNMPv3 Agent Test Module (over 443,000 malformed SNMPv3 Get/GetNext/Set/GetBulks)
- SNMPv1 Manager Test Module (over 200,000 SNMPv1 Traps/GetResponses)
- SNMPv2c Manager Test Module (over 451,000 SNMPv2c Traps/Get Responses)
- SNMPv3 Manager Test Module (over 500,000 Traps/Informs and 500,000 GetResponses/Reports)

System Requirements

SimpleSleuth requires Microsoft Windows 98/NT/2000/XP.
Supports both IPv4 and IPv6.

SimpleSoft

Simplifying Testing & Simulation

SimpleSoft
257 Castro Street
Suite 220
Mountain View,
CA 94041
650.965.4515
650.965.4505 fax
sales@snmptest.com
www.snmptest.com
www.simplesoftinc.com