Global Information Assurance Certification Paper

GIAC SECURING UNIX PRACTICAL ASSIGNMENT

GCUX Version 3.0

Option 1

Installing HP Openview NNM

Lynda L. Morrison

November 04, 2004

TABLE OF CONTENTS

I. Abstract

This paper explores the implementation of HP Openview Network Node Manger (NNM) on an existing server within GIAC Enterprises, a fictitious company, which has other management tools installed. It addresses the security concerns that exist on a management station as well as new security concerns that are introduced when HP Openview NNM is installed. The implementation of authentication and the need for it is discussed. The use of the X-Windows subsystem, which is required for HP Openview NNM, is reviewed and mitigated with the use of SSH tunneling for securing the X-Windows sessions. There is a review of the history and development of the SNMP protocol and the security issues it brings with it to the management station via Openview's NNM, and suggestions on how to more securely implement SNMP management. The Web implementation is addressed and how to secure it. Finally, auditing, backup and recovery of the HP Openview databases and processes are discussed, and suggestions for further research.

II. Environment

The machine on which the new software will be installed is a Sun Sunfire 280R running Solaris 5.8. It has one 440 MHz CPU with 1024 MB RAM and 2 MB Ecache. Its primary function is to monitor the GIAC Enterprises network. It currently has Big Brother software, a jumpstart system for building new servers, and a variety of other software tools running on it, including Perl, mrtg, open ssh, open ssl, nessus, syslog, Apache web server, tripwire agent and the tripwire console.

It is configured as a stand-alone system, and has the following services running on it, which were verified using Nessus:

ssh (22/tcp)
smtp (25/tcp)
http (80/tcp)
rpcbind (111/tcp) sun rpc portmapper[9]
sunrpc (111/udp) The portmapper, block it[9]
ntp (123/udp) – needs to be updated[9]
snmp (161/udp) - network management protocol
exec (512/tcp) Used by rexec(), no logging, unsafe[9]
shell (514/tcp) – not safe as no logging – used by rpc[9]
submission (587/tcp) sendmail additional acceptance port[9]
bigbrother (1984/tcp)
nfs (2049/tcp) Default NFS port; very dangerous[9]
nfs (2049/udp) Default NFS port; very dangerous[9]
mysql (3306/tcp)
lockd (4045/tcp) NFS lock daemon manager
lockd (4045/udp) NFS lock daemon manager

VeritasNetbackup (13722/tcp)
VeritasNetbackup (13782/tcp)
VeritasNetbackup (13783/tcp)
sometimes-rpc11 (32774/tcp) sometimes an rpc port on a Solaris box
sometimes-rpc13 (32775/tcp) sometimes an rpc port on a Solaris box
sometimes-rpc18 (32777/udp) sometimes an rpc port on a Solaris box walld
sometimes-rpc19 (32778/tcp) sometimes an rpc port on a Solaris box rstatd
sometimes-rpc21 (32779/tcp) sometimes an rpc port on a Solaris box
sometimes-rpc23 (32780/tcp) sometimes an rpc port on a Solaris box
sometimes-rpc24 (32780/udp) sometimes an rpc port on a Solaris box
unknown (32783/tcp)
unknown (32784/udp)
unknown (36417/udp)
unknown (59033/tcp)

Shell, exec, comsat, tftp, walld, fs, bpcd,vnetd,vopied, and bpjava-msvc were all started in the inetd configuration file. Many of these services were started with the Jumpstart server and will be disabled, unless needed. Others were started with the Veritas Netbackup product, and they will be reviewed also for secure implementation.

The system has the latest Solaris recommended patch cluster installed.

This machine has one primary administrator, and two additional users that have sudo access to obtain a root bash shell for administrative purposes.

III. New software to be added

The new software to be added is "**HP OpenView Network Node Manager"** (NNM), version 6.1 with a 500-node license. This software was purchased over a year ago and has been sitting in a drawer waiting for someone to install it.

"HP Openview NNM" is an SNMP (simple network management protocol) based network management system that is very often found in larger organizations being used as the foundation of their enterprise network management. It presents a graphical snapshot of the enterprise network. "HP Openview NNM" adds the discovery and network mapping functionality that is missing from the Big Brother network monitoring software that we currently are using to monitor the GIAC Enterprise network. Openview scans the networking looking for routers and switches and then builds a graphical diagram that displays the router connectivity at the higher level, and provides a means to drill down through the routers and switches to see which systems, devices or workstations are actually connected to the enterprise network. Once the network devices are discovered, the manager can select which machines that the enterprise would actually like to manage or monitor. NNM uses ICMP and SNMP to scan the network, and additionally uses router ARP caches and routing tables. Since we have a 500

user license, and considerably more that 1000 devices, it will be important to selectively choose which machines to manage. After the initial discovery of the network is done, and the devices selected for management, it will also provide a means to detect any new devices that are added to our network.

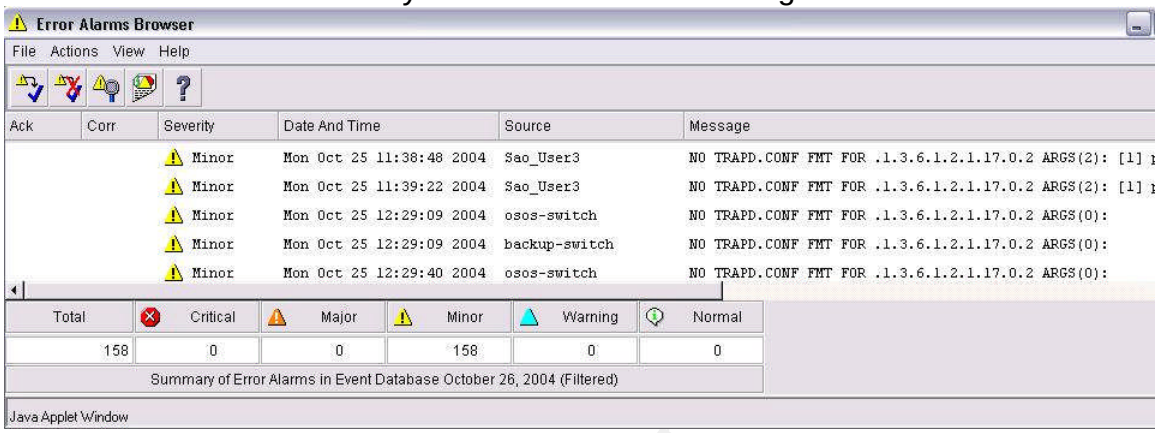
"HP Openview NNM" is a highly extensible piece of software that allows for the integration of many other pieces of network management software under the same umbrella. For example, "CiscoWorks" is a companion piece of software, used for monitoring Cisco equipment, which is often found integrated with HP Openview. "Optivity", a management system from Nortel Networks, which monitors their network equipment, also integrates with "HP Openview", as does the open source product MRTG (MultiRouter Traffic Grapher) developed under the GNU public license. If one does a search on the Internet for "HP OpenView NNM integration", a plethora of products appear touting that they seamlessly work with "HP OpenView". "Tripwire" is another software product that exclaims it's powerful integration functionality with "HP Openview". From their website they state "Tripwire for Network Devices includes a Smart Link Integration (SLI) for HP OpenView Network Node Manager (NNM) that provides network managers the ability to trigger checks for device changes, receive alerts when changes are detected, and launch Tripwire for Network Devices directly from within NNM."[7]

Tripwire and MRTG, two products that assert that they integrate with "HP OpenView NNM", are already running on this machine. "Big Brother", which has some of the same functionality as HP Openview, has the ability to also be integrated in some ways. All of these products together provide a powerful suite of management tools for the enterprise network engineers.

The Big Brother monitoring has its forte in application specific monitoring, as scripts can be written to extend its functionality in those directions. HP Openview has a stronger infrastructure base, lending to a powerful tool for monitoring and managing infrastructure switches, hubs and routers right from the start. It comes pre-packaged with reports that give statistics on router interface availability, exception reports such as threshold violations, inventory & performance reports. It can be configured, like Big Brother, to report on application problems. Some of the same scripts that are used in Big Brother could be ported to HP Openview.

Devices that are selected to be "managed", may be set up to use SNMP monitoring or management from the Openview console. Poling can be set up so that various statistics are gathered and kept in either a proprietary database or it may be integrated with an existing database infrastructure such as Oracle. The statistics that are collected are then used to produce a variety of reports, as described above. Trending can be configured so that a normal view of traffic flow can be baselined. This will provide a way to monitor changes as new products or services are added to the network.

SNMP traps and alerts can also be configured to report to the Openview management stations, and actions can be defined to notify support staff in a variety of ways that there are problems with equipment or software. E-mail notifications can be configured so that Openview sends pages or emails alerts as problems arise; network maps will change colors and give visual indicators of problems; an alarms browser will list information that it receives, from normal to critical and can be selectively reviewed and acknowledged.



Openview functionality is configured for management in an X-Windows environment. This gives the manager a Windows desktop look and feel so that a good deal of the management is set up using a point-and-click methodology. For that reason, a person without a great deal of Unix background can easily manage this product, in its most basic mode. There is also a web-based platform that allows for visual monitoring via a web browser. This monitoring may then be turned over to a help desk or other group for visual monitoring. For a manager knowledgeable in Unix scripting, additional functionality may be added. For web view examples, see Appendix B.

There are some pre-installation steps defined in the “HP Openview Installation Guide”[10]. The Common Desktop Environment (CDE) is required for the installation, as is the Java Plug-in JPI.

For clients that will use the web-based monitoring capabilities, such as a helpdesk, browser pop-up windows and cookies have to be enabled, and the Java runtime environment has to be installed in order to run the web browser connection. Java & Java Script entries have to be enabled on the browser as well. The HP OpenView Launcher is a java application that allows the network maps, alarms and reports to be displayed via web browsers and is intended to be used on a local subnet. This functionality may need considerable testing to resolve.

These are only a few of the functional components of Openview. This is a powerful and all-encompassing tool that may take considerable time to configure to ones needs. The power of its extensibility gives room for continual enhancements as networks grow and needs change.

IV. Security Issues Introduced by the new software

Authentication and management

Since this tool provides a topological view of the network, the need for controlling who or what workstations can use this information becomes very important. The structural and enterprise use of the product needs to be considered and roles need to be evaluated and assigned as needed based on the principle of least privilege.

X-Windows

The X-Windows protocol is an open source protocol that has historically been used in Unix environments. There are also many popular emulation programs that run on Windows or Macintosh machines to allow X-Windows connections to Unix based servers, such as Hummingbird's Exceed and NetSarang's XManager. X-Windows was designed to share resources in a secure environment. Security was not an issue and was not addressed in the original design. Today, there are three security aspects of X-Windows that need to be addressed: Authentication, Authorization, and Privacy.[40]

X-Windows X11R6 provides two different methods of authentication, either host-based or user-based authentication. It does not have a session or connection based mechanism for authentication.

Host-based authentication is done using the xhost command, as recommended in the HP Openview installation guide. It is a simple process to restrict which machines can use an X-Windows session. The command xhost + allows any machine on the Internet/Intranet to connect using an X-Window. The command xhost – enables access control so that only authorized clients can connect. After this, each host that will connect needs to be added to the access control list. This is done using the xhost +remote.host command. If this access control list is disabled, any host can connect to the X-Server.

X11R6 has four methods of securing user-based authentication. They are: MIT-MAGIC-COOKIE-1, a shared plain-text "cookie"; XDM-AUTHORIZATION-1, a DES based private-key; SUN-DES-1 using Sun's secure rpc system; MIT-KERBEROS-5 using Kerberos Ver. 5 user-to user. The most commonly used of these is the MIT-MAGIC-COOKIE.

In the MIT-MAGIC-COOKIE method, the 128 bit "cookie" is either stored in the .Xauthority file in the users home directory, or a pointer to it is stored in the XAUTHORITY environment variable, if it has been relocated. The cookie is transmitted over the network without encryption and the system will trust anyone who has a cookie.

The XDM-AUTHORIZATION also stores its information in the .Xauthority file, which includes a 56 bit DES key plus 64 bits of random data.

The SUN-DES solution uses a secure public key and the principal who started the server – which is also stored in the .Xauthority file. This only works if the system supports secure rpc. The owner of the display can enable or disable authorization using the xhost client.

MIT-KERBEROS is a user-to-user authentication using third party Kerberos keys. A user gets a Kerberos "ticket" from a Kerberos server using the user's secret key. The Xserver has no place to store secret keys so they are shared with the user who logs on. The owner of the display can enable or disable authorization using the xhost client. Unfortunately, not too many people are using a Kerberos ticket server.

The biggest security problem is in the ~/.Xauthority file. Anyone with root on a server can access the .Xauthority file, and therefore can access your desktop and control the desktop, independent of the authentication method[35]. The most serious problem is that they can access keystrokes. Any administrator can already access your desktop, but they cannot access your keystrokes without some kind of intervention of this type. Accessing another person's keystrokes is not part of any administrator's job description, and the potential for it should not be allowed.

Arturo Guillen notes in his paper entitled "X Windows Security: How to Protect your Display"[40], that once a connection is granted there is no mechanism to close the X Windows connection, except perhaps with a reboot! The decision on how to handle X Windows connections should be made when the machine is built.

Since X-Windows is such a huge security risk, it would be better not to use X-windows at all. This application is designed around the use the X-Windows environment. In order to use the product, the use of X-Windows has to be mitigated to provide the most secure environment possible. Choosing a user-base authentication method and tunneling the X-windows request through SSH will eliminate most of the security weaknesses of the X-windows environment.

SSH

SSH is a protocol suite of connectivity tools. It is used to replace such programs as telnet, ftp, and rlogin with a more secure alternative. It encrypts the session so that everything, including the password exchange, is tunneled in a secure shell. Using the option to forward tcp packets or forward X11 packets through SSH introduces other security risks.

SNMP

SNMP (Simple network management protocol) was defined in **RFC 1157**[14] in 1990. In this memo, the Internet Activities Board recommends that all IP and TCP implementations be network manageable. The protocol specification states: "The network management protocol is an application protocol by which the variables of an agent's MIB may be inspected or altered." Messages are used to accomplish the exchange of information between the various protocols, within a single UDP datagram. Each message has a version identifier, an SNMP community name, and a protocol data unit (PDU). The MIB or "Management Information Base" describes "the managed objects contained in the MIB as set forth in **RFC 1156**[13]**."**

Security concerns were introduced with this protocol, but initially they were hardly addressed at all. The SNMP community string was used to establish authentication, access control and proxy characteristics. The community string was used like a password, to verify the authenticity of the request. Most network devices that agreed to comply with this protocol used a default community string for read, write and trap access. Public was the usual read community string, private was the read-write, and read-write-all was secret. But even the default community string sometimes varied according to the manufacturer. In addition, there were some known hidden community strings set by different manufacturers, one of which was HP Openview. All of the manufacturers used some "default" community strings. The community string is defined on the agent and is a primitive way to restrict access to the MIB [9]. The agent may establish multiple community strings in order to distinguish between the various levels of management support. For example, the string public was used to allow read access only while private was to allow read and write access to the device.

The IP address of the manager may also restrict access to the MIB. It can be used to limit to whom the agent may respond.

An agent may also act as a proxy for other agents. This standard was developed because of the number of devices that did not support TCP/IP, like modems, dsu-csu's, bridges, and even some workstations. The proxy acted on behalf of other devices that did not support SNMP.

SNMP is defined in terms of commands. There are 5 commands in SNMPv1. They are Get, GetNext, Set, GetResponse, and Trap. The Get command retrieves information from an agent; the GetNext command uses the structure of the objects in a MIB which are arranged in a tree, so it moves down the tree and returns the next value. This is what allows the command snmpwalk to work. The Set command allows a manager to update values at an agent. The agent, in order to respond to a request from a manager, uses the Getresponse command. The agent uses the trap command to send information to a manager, without waiting for a request.

SNMPv2

SNMPv2 was developed because of several deficiencies that were noticed in the original implementation. Specifically, SNMPv1 lacked support for distributed network management. It also had many security deficiencies.

A Manager-to-Manager MIB in **RFC1451**[16] was added for distributed support among management stations. The Party MIB defined in **RFC1447**[15] was used to control security information and the security protocols that protect the information being transferred.

SNMPv2 was described in **RFC1901**[17] in 1996. SNMPv2 includes all of the commands included in SNMPv1 as well as two new ones. The Inform command allows one management station to talk to another management station, or inform another management station about stations that it is monitoring. This extends the usefulness of the management protocol to share responsibility with other management stations. The GetBulk command allows the management station to retrieve a large amount of data at one time – like sending the entire MIB table. There is one other slight difference in the Get command. In SNMPv2, if the MIB information is incomplete, the command gives partial results. In other words, it reports what it knows. SNMPv1 would return nothing if the information was incomplete.[9]

Prior to SNMPv2, using SNMP to manage equipment was no better or worse than using telnet. Telnet has a clear text password management system, while SNMPv1 passed community strings in clear text format. Both are inherently insecure.

RFC1909[18] defines the administrative infrastructure for SNMPv2. In that RFC, developed in conjunction with the other RFC's from 1901-1909, Authorization, Authentication & Privacy, and Access Control are addressed. **RFC1910**[19] addresses the user-based Security Model. This model exposes the danger of modification of information, identity authorization, message stream modification, and disclosure by eavesdropping. It does not deal with the potential for denial of service or traffic analysis. Out of these RFCs for SNMPv2 has come support for integrity, confidentiality, authentication, and access control. This adds a significantly greater amount of security than using telnet for system management.

Authentication and privacy can be selectively enabled. When it is enabled, the message digest field is computed using an MD5 algorithm to authenticate the originator of the message. Timestamp information is used to help prevent replays. Encryption can selectively be used to encapsulate the majority of the SNMP packet, including the authentication information.[32]

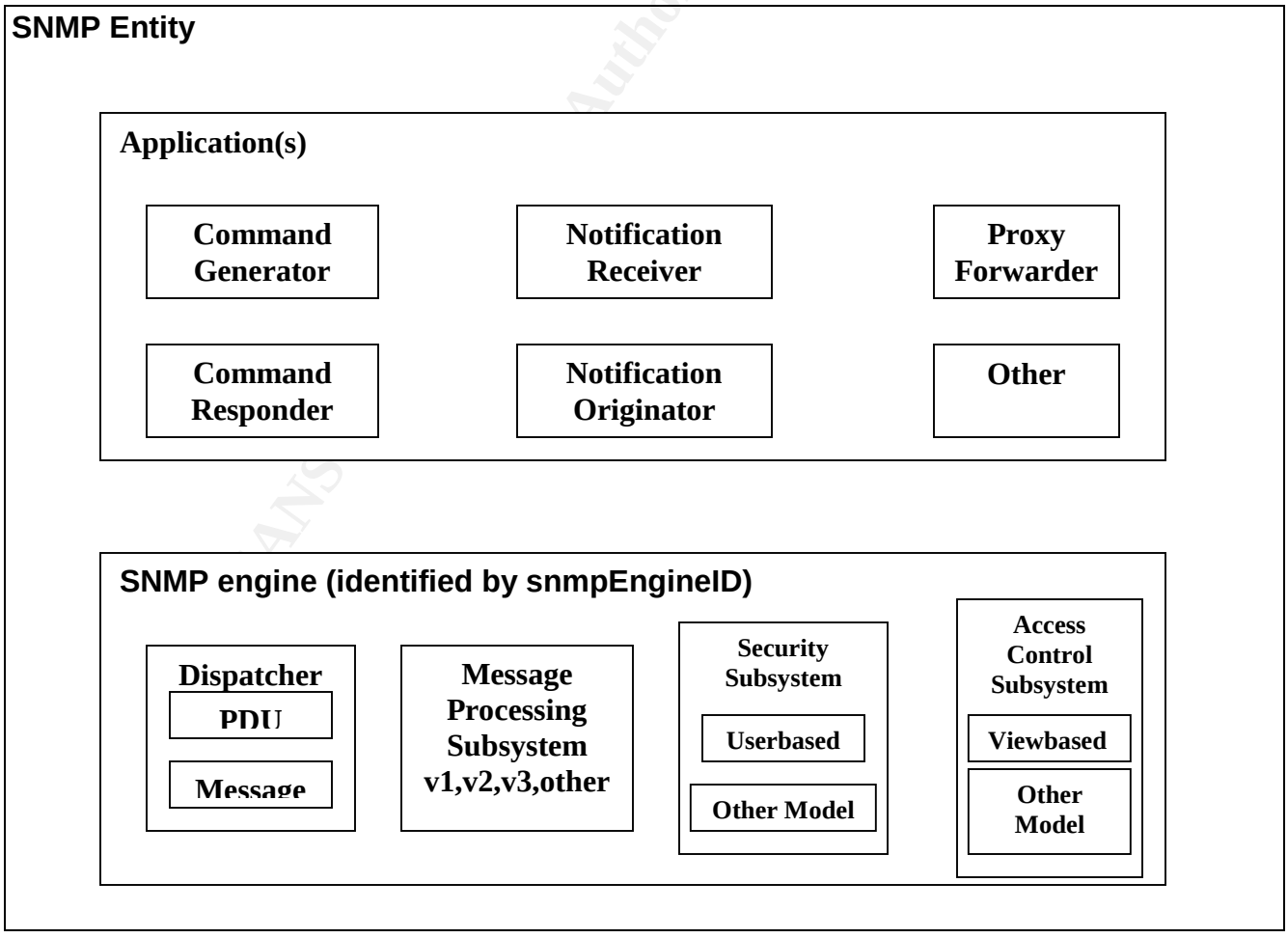
SNMP V3

SNMPv3 architecture is described in **RFC2261**[20]. This RFC gives an historical summary of the SNMP development to this point, as well as other information about transitioning to new models.

Security is specifically addressed and is divided into two subgroups: message level security (referred to as security) and access control for protocol operations. It provides for three levels of security. The highest level is with authentication and privacy. The middle level is with authentication and no privacy and the bottom level is without authentication or privacy. Again, it can be selectively enabled.

RFC2570[21] provides another overview of the three SNMP versions and dubs itself as tutorial in nature. RFC2570-2575[21-26] all provide a framework on how to incorporate the new security features of SNMPv3 into the existing SNMP structure. Existing SNMP PDUs (Protocol Data Units) are used in the new standard.

RFC2261[20] identifies the SNMP engine as follows:



SNMPv3 is a much more complex system than the two previous versions. It involves taking the original SNMP engine and adding the security and access control sub systems.

A number of products recognized in the market as Network Management have implemented a version of SNMPv3. Such companies as Cisco, HP OpenView, Tivoli's NetSight, Aprisma's (aka Cabletron) Spectrum management platforms, and MG-SOFT are including support for SNMPv3. Most of these companies offer all three variations of SNMP, but there have been few deployment reports[4]. Customers are not reporting on their implementations or their security problems.

Web Services

Openview provides a web services interface, a web application that that provides read only access to the network infrastructure map. Web services introduce another level of vulnerability in that ports are open that could be susceptible to buffer overflows and other coding errors. Authentication to the web piece is yet another layer of complexity and security. Web based authentication is done in clear text.

Denial of Service and SNMP Buffer Overflows

SNMP has had a great deal of negative press in the past couple of years. This primarily stems from the weaknesses described in the SNMP protocols. SNMPv1 protocol had vulnerabilities ranging from a denial of service condition to buffer overflow problems that allowed an attacker to gain root access. Many of these conditions have been addressed with vendor patches, but new vulnerabilities are constantly being discovered. These types of vulnerabilities must be addressed with policy that assures security patches will be installed as quickly as possible.

Openview uses a significant amount of ICMP traffic in its implementation. The ICMP protocol is another that is prone to denial of service attacks. Attacks using the ICMP protocol often consume all available bandwidth on the network, effectively shutting down the network. Although this is not unique to Openview, it is a situation that could bring down a very important part of the network infrastructure. Here again, vulnerabilities need to be addressed in a timely fashion by applying security patches as soon as possibly.

V. Solution

INSTALLATION – Following the Installation Manual[12]

Task 1 is to verify that the system meets the minimum hardware and software requirements. The platform, OS and minimum hardware requirements match.

As far as software is concerned, the documentation specifically lists 3 patches, which were also verified to have been installed.

Task2 has some additional pre-installation task, involving third-party OpenView products. There are no other third-party Open View applications installed, so the only software that needs to be tested is for the Openview Installation. Other recommendations include making sure that if DHCP is used then a reservation is added for the management station. It needs to have a static, or reserved, IP address. The installation manual says that a web browser is required to be installed on the system, and the Java plug-in JPI. The CDE (common desktop environment) is required. Since these files are needed for the installation, the CDE packages must be installed.

Semaphores must be enabled. The installation guide gives some specifics to add to the /etc/system file if semaphores are not automatically enabled. The ipcs command will show if any semaphores are currently enabled, but it does not tell if the semaphores will automatically be enabled. The installation program does run some checks before it will install.

Task 3 is the actual installation of Network Node Manager. This installation will be a local installation. The Manual gives instructions on how to install from a different Solaris machine if the machine that it needs to be installed does not have a CD-ROM drive. A management console can also be installed seperately, while another server has the NNM common databases and background processes on it.

It is more secure to do the installation locally, even though it is nice to know that if you do not have a CD drive on the target machine, it can be installed remotely. The installation on the local machine is very straightforward. From the installation guide:

1. Log in as root to the system where you will install NNM.
2. If you are upgrading from a previous version of NNM, make sure no HP OpenView processes are running.
3. Insert your NNM CD into the CD-ROM drive.
4. Mount the CD-ROM disk by typing
   cd /cdrom/cdrom0
5. Type in ls –l to see a listing of the files in cdrom0.
6. Start the installation program by typing
   ./install
7. The installation program appears on the screen and the user follows the instruction to complete the install. Any error messages that come up will have to be fixed before the installation can proceed. (NOTE: This was installed remotely, using an SSH tunnel to export the X-window. The CD was mounted locally.)
8. Remove the CD from the CD-ROM by typing

```
cd /
eject cdrom
```

TASK 4 is to configure the agents for Solaris. This is done after the installation has been successful. There are two agents that need to be configured, the Emanate Master Agent (snmdm) and the Solaris Native Agent (snmpdx).

Since we had previously used the UCD-snmpd, it was verified that this would not be used by NNM. It was determined that the UCD version of snmpd would cause conflicts within Openview. It did not need to be removed, but only to be sure that the agent that was configured and starting was the Solaris agent. It was recommended to start the Solaris Native Agent on an unused port, but it uses 50161 as an example. The Native Adaptor Agent (naaagt) also needed to be configured so that it is listening on the same port number as snmpdx. Typing the following does this:

```
export HP_NAA_PORT=50161
```

This is done using the same port as the example. It is always wise to change defaults to something else – be sure to document how you change it. Make this change permanent by editing the /etc/rc.config.d/SnmpNaa file and add the line

```
HP_NAA_PORT=50161
export HP_NAA_PORT
```

Then start the native agent with /usr/sbin/naaagt

NNM also has a web interface. It will install a web server product during the installation, but the use of another web server product is acceptable. It will use port 8880 by default for communication. The aliases OvCgi, OvDocs and OvBackgrounds need to be set accordingly if another web server is used. In order for the web display to be accessible, there must be a non-web based version of NNM running for each map that will be accessible through a remote web access. This means that either the X-windows display must be running on the console, or an X-windows machine connected to the management station must have an exported X-windows display with the non-web based NNM running. Changes can only be made to the non-web based NNM. Remote users see a read-only version of the maps with a web browser. Since we are not running CDE or X-Windows on this server, the X-Windows display is exported to another machine and it will run the necessary maps to be displayed in the web browser. Even though we are not running the CDE environment, the installation still looks for the files and verifies that they are available.

At this point, it is necessary to complete and send in the license request. There was an additional setup step for the license installation that required help from HP customer support in order to complete the install.

At this point in the installation process, it is time to check the HP Openview site to see if there are any patches for this version of HP Openview NNM. The CD version that we had purchased was Version 6.1. Indeed, there was a patch for 6.1 but there was also an upgrade path to Version 6.2. From a remote machine, checking the HP Openview support site showed the following:

network node manager release 6.1 / Solaris 2.X

attention

Attention:

This intermediate patch (PSOV_03143) is the last patch that HP will be providing for NNM6.1. Please upgrade to NNM6.2 to receive future patches.

Customers who do not have NNM6.2 media may download Network Node Manager 6.2.

Developers who do not have NNM6.2 media may download the Network Node Manager 6.2 Developer's Toolkit.

Making a backup of the previous version of Network Node Manager is recommended for customers upgrading. In addition, some configurations of NNM's Data Warehouse will require manual intervention as part of the migration process. Please see the online NNM6.2 release notes.

After installing Network Node Manager 6.2, NNM6.2 patches may be installed. NNM6.2 patches will NOT work on NNM6.0, NNM6.01 or NNM6.1 installations. Conversely, NNM6.0x and NNM6.1 patches will not run on NNM6.2.

Security Bulletin HPSBUX0307-nnm

Follow this link to the README.TXT file for instructions on how to obtain and install the files that address this bulletin.

It now became important to upgrade this installation to version 6.2. The NNM6.2 release was downloaded to another machine, a workstation running a CYGWIN environment. Then looking at the NNM6.2 release, it also had a security patch release. This patch was also downloaded to this workstation.

network node manager release 6.2 / Solaris 2.X

attention

Security Bulletin HPSBUX0307-291

Follow this link to the README.TXT file for instructions on how to obtain and install the files that address this bulletin.

PSOV_03357 | This patch depends on: PSOV_03184

Description:	Patch for Sept-04
Posted Date:	2004-Sep-30
Symptoms:	Change Request: 8606352462 snmpCollect may core dump when used with -S option. Change Request: 8606375751 snmpCollect reports high CPU usage along with rapid memory growth. Change Request: 8606375144 Version tab is not found on oww.dll, ovutil.dll, ovsnmp.dll and ov.dll. Change Request: 8606356720 snmpCollect exhibits slow startup ***...Symptom text truncated. Please refer to the patch text file for a complete list of symptoms.***

From the workstation, a secure channel was established to the network management machine using ssh. The command looks something like

sftp user@machinename

and the following prompt appears:

sftp>

From here, the commands are very similar to ftp commands. Use a cd to change to the appropriate directory and use a put command to upload the files. Patches are often put in the /tmp directory but they could be put in any directory of your choosing, such as the $HOME/tmp. The patches are in a shar format and need to be "unshar"ed. Use the command sh patchname. There will now be a tar file and it is ready to "un-tar". Use the command tar –xovf patchname.tar to expand the tarball. It will create a new directory called patchname.install with the appropriate directory structure and files under it. It also extracts an install script, called install_patch and a text file, which contains a listing of the files and the changes that the patch will make. It lists known conflicts, which patches it will supersede and finally specific installation instructions. Typing the command

tail –200 patchname.txt

will list the last 200 lines of the file, which is just enough to see the installation instructions. There are also special installation instructions included in this file that need to be read and followed. These are important to note, because if you have done any customizations or configurations, it tells which files may be overwritten and how to keep your existing configuration files.

Once all of the patches are up to date, it is time to proceed with the configuration of the system.

Configuration

There now needs to be some additional configuration that will help secure the application and the connecting devices. This version of HP Openview is running SNMPv2. It will be using a community string for access control. A community string is used like a password. For that reason, the community string needs to be set to a complex password that is at least 8 characters long and is a combination of letters and numbers. Although the encryption scheme is not high, the authentication will use the md5 algorithm to secure the community name. Every machine that is to be managed must have the SNMP community set to match. In addition the trap manager SNMP string must be set. Specify the IP address of the management machine so that the hosts do not respond to SNMP requests from any other server.

On Cisco routers and switches, it is necessary to create an access list and only allow access to the SNMP information from the management station. The access list will look something like the following:

```
access list 5 permit xxx.xxx.xxx.xxx
```

In addition, SNMP setting should be configured similar to the following:

```
snmp-server community complex-name RO 5
snmp-server location location-name
snmp-server enable traps snmp authentication linkdown linkup coldstart
        warmstart
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps rtr
snmp-server host xxx.xxx.xxx.xxx complex-name
```

On Windows 2000 machines, the configuration is done in a GUI. Navigate to the control panel, and select the SNMP service trap service. It should be disabled. Next select the SNMP service. It should be set to start automatically. Double click it and a management screen will come up with several tabs. On the agent tab there are choices as to what to monitor. The choices "**physical**, **application**, **datalink & subnetwork**, **Internet** and **end-to-end"** are available. On the Trap tab, list the complex-community string that was used above, and the trap destination, which is the ip address of the management station. Under the security tab, select "Send authentication traps " and list the accepted community names. There are two other choices on this tab. They are:

```
    Accept snmp packets from any host
☒   Accept snmp packets from these hosts
```

The second choice should be checked and use the "add" button to specify the IP address of the management station.

On Solaris machines, the snmpd configuration file is located, by default, in the /etc/snmp/conf directory. In the snmpd.conf file, include the following:

```
sysdescr                Sun SNMP Agent, System Type
syscontact              System Administrator
sysLocation             Computer Room
system-group-read-community     complex-password
read-community          complex-password
trap                    localhost trap-host
trap-community          complex-password
managers                snmp-management station
```

The trap setting is where to send any traps that are generated. Traps are defined by the application or systems as significant events. Up to 5 hosts can be listed. The managers setting are which stations are allowed to send SNMP queries. In this case, the "managers" keyword must be repeated, but it can be repeated up to 32 times, or for 32 different hosts. Both of these should be limited again using the principle of least privilege.

Role-Based Authentication

User roles are configured on the management station for both the console access and the web access. Console mode is managed by local accounts. Users that need to stop and start the services need to be able to use root permissions. This is best accomplished with sudo. Give users rights to the following commands:

```
sudo  ovstart
sudo ovstop
sudo ovpause
sudo ovresume
```

The ovstart and ovstop will allow the users to stop and start the ov services. Ovpause and ovresume are used for backup purposes. Ovw begins a console session and automatically starts ipmap, xnmevents, and some other applications associated with the network maps. The user does not need root access to run ovw. It is important to note that only the first user to run the ovw process will have a map that can be edited. Any user that additionally runs ovw will have it open in read-only mode.

Web-based authentication

User authentication to the browser is via a username and password, which are passed in clear text format, since the browser version runs in an http window. For this reason, it is recommended that users not use the same user name and password on the console as they would to log onto the web browser. Openview has several predefined roles for various kinds of browser users. For Solaris, there is a Network Admin role for the highest level of network monitoring. There is also a Network Operators role that is intended for Helpdesks or for operators who do routine troubleshooting. Other roles are available or can be created as needed.

On the web portion, a session configuration file allows the manager to set the desired level of security. If security is disabled, there will not be a login screen and anyone will have full access. Although this is read only access, it contains significant information about the network. Many reports can be generated from the web interface, snmpwalks are available to use, and other critical information could be easily gleaned from this application.

To configure security for browser access, the following mechanisms have been put in place. First, user authentication is managed through a password file. Passwords have to be set by a system manager using the ovhtpasswd command. As a manager logged on as root, type

ovhtpasswd ovuser

The manager will be prompted for a password. The username and a hashed version of the password is place into the /etc/opt/OV/share/www/etc/htpasswd file.

Next is the user authorization file. The NNM manager also assigns users to groups or roles. Access to the various urls is restricted according to your user role. To change a user's role, edit the /etc/opt/OV/share/www/etc/htgroup and place the user name in the appropriate role.

The session configuration file controls the applications that are started when a user logs in. These applications are started via the Launcher. It basically controls which screens the user will see when the launcher is initiated. The session is terminated when the user closes the browser. There is a default time out of 9 hours, or when the management station closes its map. This functionality is disabled by default. To enable it, edit the session.conf file which is located in the /etc/opt/OV/share/www/conf directory. Set the following values:

UserLogin: on
LoginLoggin: on
AccessLogging: on
SessionTimeout: 9

The new information will take affect when the user closes his browser and a new Launcher is run.

SSH & X-Windows

Since it is possible to secure an X-Windows channel with SSH, choose to use that approach as opposed to trying to lock down a protocol that does not lend itself to lock down! SSH will provide a secure channel through which the X-Window can be displayed on a remote machine. SSH will assume the role of authentication.

In the background, the SSH daemon has to be configured first. It is preferable to use SSH2 as several vulnerabilities have been found in the SSH1 protocol, including packet insertion attacks and password length determination[1]. The choice to use SSH2 can be set in the configuration files for both client and server.

SSH may be configured with the PAM (Pluggable Authentication Module) module. PAM allows the system administrator to configure user authentication mechanisms on a per application basis. Pam also allows multiple access mechanisms to be used. PAM is designed to enable a single sign on environment.[6]

SSH may also be configured with tcpwrappers. Tcpwrappers is used in the inetd file to redirect the logging of services that are started with the inetd daemon to the syslog. This provides a mechanism for access lists and logging such things as ftp and telnet. With this functionality compiled into SSH, it will log via syslog.

In the hosts.allow file, add the following:

sshdfwd-X11: hostaddress ALLOW

In the hosts.deny file, add the following:

sshdfwd-X11: ALL

The management console display will be exported to a Linux workstation running SSH on a hardened Linux system. The workstation system defaults the xhost not to allow any machines to connect. It is good to check to be sure that the xhost is configured. X-Windows is not running on the management host machine. Disabling the startup of dtlogin keeps this from running. The S99dtlogin has been renamed to s99dtlogin in the /etc/rc2.d directory. A choice to use x-windows would add a serious security weakness to this machine. SSH is the protocol of choice to connect to this machine remotely.

X-Windows can be run securely inside a secure shell. Secure Shell encrypts the entire X-windows session, including the user login and controls the connection. The command to connect to a remote server and export an X-windows display in its most basic format is:

ssh -X –l username hostname

This says to connect to server “hostname” with user account “username” and allow an X-window session to be forwarded to the users display. A secure session is started.

The SSH daemon (sshd) can be configured in three different ways. First, it can be configured during compile time with such options as the location of the configuration files, whether binaries are SUID, and which entropy source (used for generating random numbers) to use. Support for tcpwrappers can be added in when SSH is compiled. If sshd is not already installed, then these are things to consider before installing it. Adding additional security measures at compile

time is preferable to configuration changes using the config files. The daemon would have to be re-compiled to make the changes effective[2].

Recompiling is another option to consider, if one would like to have some of the added security. To add another level of security, after compiling, and the machine is configured with all the programs that are needed, remove the compiler from the machine. It is more difficult for a hacker to make changes to programs if they should ever compromise the root privileges of the machine if a compiler is not readily available. It may just take them a little longer to install a compiler if they want it.

The second level of configuration is the sshd_config file. In the configuration files for both the client and server, **X11Forwarding yes** must be added. Also add the warning banner in /etc/issue. In the configuration file, include:

X11Forwarding yes
Banner /etc/issue

This prevents another potential security problem with NMM. On this server, the best way to control the machines that can connect to this server is in the hosts.allow file.

The third level of configuration is done with the Access Control List. As for using the ACL, it does not work correctly with the Solaris operating system. The only things the ACL will do is either specifically deny access to a user or group of users, or specifically allow a user or group of users. The default is to allow all, so access is essentially controlled by Solaris login information. It is preferable for any user that connects to connect using SSH.

Login by root shall also be restricted. Any user that needs to be root can either su to root or can be set up with sudo access. By using su or sudo, there is an audit trail of who logged in and then changed their login to root access. The use of sudo is the preferred solution, as the root password does not have to be given out to allow sudo. Include the following command:

PermitRootLogin no

Port forwarding is an interesting and powerful tool that is available in the sshd configuration. It is useful to proxy someone through a firewall, for example. For a management stations, it would normally be recommended that it be turned off, along with the option for a Gateway Port. To do that, set the following parameters to NO:

AllowTCPForwarding no
GatewayPorts no

In our case, we have found it useful for gathering information from the DMZ to our management station using port forwarding. This allows a secure connection from the DMZ server to our internal server with specific tcp/ip information. We are able to tunnel bigbrother information in this way back to the management station.

To begin the Openview NNM console, once connected to the server using ssh, run the command

```
ovw &
```

The ovw process begins the Openview NNM desktop and exports the display back to the originating workstation. The ampersand tells the OS to run the process in the background, so that the user can continue to have command line access. In this way, only the ovw process is running with the use of X-Windows.

SSH & X-Windows Authentication

After the choice is made to use SSH as the tunneling protocol for X-Windows, the choices for authentication are now controlled using the sshd protocol. Openssh supports three methods of authentication: the traditional user name and password, public key based authentication, and host based authentication.

Although the user-name /password authentication is encrypted when using ssh, it still does not eliminate the possibility of password misuse. The two-factor or key-based authentication that is part of the openssh protocol helps to improve security by eliminating the potential for impersonators. This protocol uses a public and private key pair, along with a challenge and response. It is based not only on something the user knows, but also something the user has (the private key). The pass phrase is used to decrypt the private key. If the pass phrase is lost, a new key pair has to be generated.

Host based authentication trusts a connection based on its IP address. On a local private LAN this method may be satisfactory, but it is a method that is easily misused or abused in the Internet community. For that reason, the following settings are recommended[2]:

HostbasedAuthentication no
RhostsAuthentication no
IgnoreRhosts yes
PermitEmptyPasswords no
PasswordAuthentication yes
PubkeyAuthentication yes

Also, we will use PAM for authentication, which give us a way to change our authentication preferences as technology changes. To enable PAM authentication add the following line:

UsePAM yes

SNMP

The first consideration on this server is to restrict any SNMP queries to and from the server. SNMP is a powerful tool for finding out information about network devices, for detecting and monitoring problems that occur on a network, and for configuring devices on a network. It is useful for both an administrator and a hacker. For that reason, queries need to be restricted to specific machines that an administrator designates shall have access to query the machines. Because of the power behind the SNMP protocol, the ability to make changes to a machine using SNMP should be restricted to none. Those configurations for Sun machines are done in the /etc/snmp/conf/snmpd.conf file. For the EMANATE SNMP Agent used by HP Openview, the snmpd.conf file is located in the /etc/SnmpAgent.d directory. The only information that should be included in this file is the following:

get-community-name:	**complex-community-name**
contact:	**contact-person**
location:	**location of agent**
max-trap-dest:	**1**
trap-dest:	**localhost**

Since this machine is the one monitoring all the other machines, its manager is simply the localhost. Similarly, all other systems will be answering SNMP queries from this system only. Each of those systems needs to be configured with the same read-community, the same trap-community, and the managers should be set to only this management station's IP address.

The write-community string is not given a value, so that no machine can change this machine remotely. A trap community string is set, and the manager set to localhost so that events that occur on this machine cannot be sent to any other machine. And, on other systems, the trap managers should be set to send to this machine only.

A related service, dmispd, is also running on this machine. Since DMI services are rpc based, and the rpc services are ones that we do not want running, this is another that should be disabled. The best way to keep this service from starting is by renaming the /etc/rc3.d/S77dmi to /etc/rc3.d/s77dmi. In this way, it will not automatically start when the system is rebooted.

After these things have successfully been secured and configured, we can go ahead with the software installation.

VI. Auditing

Auditing of the HP Openview web application is available, but is not managed. Logging is turned on in the session configuration file. There are two log files – one for logins and one for URL access through the Launcher. These log files are not managed, so they need to be included in a cron job or period check to rotate the logs.

System logging of OV processes and access is handled by the syslog daemon. On Solaris machines, it is recommended that everything log to a single file. In the /etc/syslog.conf file, under the line

mail.debug ifdef('LOGHOST', /var/log/syslog, @loghost)

add

*.debug ifdef('LOGHOST', /var/log/syslog, @loghost)

Enable the Solaris Basic Security Model[34] by running the script /etc/security/bsmconv. This script will turn on auditing. There is other configuration that should be done, including adding a nightly cron job that will rotate the logs.

Tripwire

Since Tripwire is installed and running on this server, all changes that are made will be recorded and reflected in the tripwire log. After the configuration is complete and the services are running, a new baseline for tripwire needs to be developed. Tripwire then monitors the system for any changes that occur with the new software installed. A sample output from a tripwire report is included in **Appendix A**.

A management station adds additional handling for the tripwire configuration. Since tripwire reports all changes that are made, and a network management station is constantly monitoring, and therefore constantly updating files, it is necessary to modify the tripwire agent to remove directories in which these files are updated, as well as some of the logs.

BACKUP & RESTORE

NNM has a backup facility that is set up to run on a regular basis. It may be scripted and put in a crontab to run at a regularly scheduled weekly backup window. Before the backup script is run, another process, called

$OV_BIN/ovtopofix, should be run. It will verify the objects in the discovery database for accuracy. The file to run for the backup is $OV_BIN/ovbackup.ovpl. It places a copy of all the database files in the $OV_TMP/ovbackup directory. After the backup completes, it will automatically start all of the NNM services again. A check to be sure the services are running should be added to the backup script, as they do not always come back as expected.

The ovbackup.ovpl causes the Openview processes to change to a pause state while the databases are exported. This may cause the snmpCollect process to go into an unrecoverable state. If the processes do not recover from a paused state, it is necessary to fully stop the services, run the backup and get a clean export of the databases, then restart the services.

The primary reason that HP developed the export backup script is because the Sun backup software does not correctly backup the sparse files that are created by the NNM database. The Unix tar command also does not handle the sparse files correctly. We are running the Veritas Net Backup and have verified that Net Backup can handle the sparse files that are created by the NNM database. Sparse files are RDBM files which are stored on the disk with NULs stripped out. Because of this, some restore programs will try to expand the sparse files. It is not necessary to use the OV backup script, but it would simplify the restore procedure.

The restore process should be tested. All NMM services need to be stopped, using the ovstop command. Copy the databases that need to be restored into the $OV_TMP/ovbackup/ directory. The ovrestore.ovpl script will restore all files found in the ovbackup directory. After verifying that the files have been restored, start the NNM background processes using the ovstart command.

It is also possible to restore portions of the backup. The script allows for selectively choosing to restore only database, log or configuration files.

VII. Summary and Research

SNMP Security Pack

The SNMP Security Pack provides an extension to SNMP manager devices that only support SNMPv1 and/or SNMPv2c (without security), allowing these "vintage" managers to use SNMPv3 with security.[31] HP Openview NNM 7.5 will be fully integrated with the newest version of the Security Pack, according to their press releases. The older versions of HP Openview also say they will integrate with the SNMP Security Pack. By design, it should be backward compatible with any SNMP implementations. The “Deployment Report for RFCs 2571-2575”[5] specifically describes the testing and deployment of the SNMP Security Pack with HP Openveiw 6.01 for Solaris/Sparc, and its use of MD5 authentication. They were also able to verify using a sniffer that the communication was

encrypted. Their main complaint had to do with documentation of the security pack as to how it worked with Openveiw. It seems that they had to do some trial and error work to get it fully configured.

To implement this security and make it compatible with SNMPv3, an additional purchase of the SNMP Security Pack would be necessary. The newest version of HP Openview, version 7.5 is advertising its compatibility with the latest SNMP Security Pack. They have been working hand in hand with the SNMP community to make it fully integrated. An upgrade to 7.5 would be advisable.

INTEGRATION

Integration of existing software packages such as Tripwire and MRTG leave considerable room for extending the NNM platform. There are other SNMP based management pieces that could possibly be integrated into Openview. Our Dell servers have a package called OpenManage. This is another product that boasts a connection piece for HP Openview. We have Avaya systems that will integrate with Openview. HP's Jet Admin integrates.

CONFIGURATION & ADMINISTRATION

Continuing configuration and administration of the Openview platform lends itself to new ideas every day. There is much work to be done in the script development and reporting. There are many ways to utilize the collection of data.

Adding and utilizing various vendor MIBs is another area for development. Evaluating and selecting the elements of the mibs that would be useful to monitor is a very large task. Securing the MIBs is another task to consider.
Adding new software to a system forces the administrator to seriously evaluate the server for space, capacity, processing power and compatibility. The machine may handle the processing, but the business logic and design also needs to be considered. In this case, a machine that is constantly monitoring the network incurs a lot of input/output to the hard drive. Depending on what is being done with the data it collects, it may also impose a load on the processor. Since it is collecting a good deal of information from the network, disk space and log file monitoring is addressed.

VULNERABILITIES

Existing vulnerabilities need to be addressed and mitigated prior to adding new software, due to the potential for the addition of new vulnerabilities. Before the new software is in place, an evaluation of the system needs to be performed to analyze and mitigate any existing vulnerabilities. The new software needs to be evaluated to review additional vulnerabilities that may be incurred.

A network management station contains a great deal of information about the network infrastructure. For this reason, it is important to secure this server perhaps more than other servers. This machine needs additional security for the jumpstart server, X-Windows, ssh, SNMP, web services, root login, auditing, and backups. Additional research and testing needs to be done to determine the best way to secure this server when it is not being used as a jumpstart server. Since jumpstart turns on a number of services and processes that are unsecured, they need to be turned off when the server is not needed for jumpstarting a new machine. A script could be developed to shut these services down. The jumpstart systems itself will turn them back on when they are needed.

Another area to address is whether the web interface to NNM can be secured using ssl. Because of the load on this machine, an encryption card might be the best answer to secure the NNM web sessions.

The Windows 2000/2003 servers need to be evaluated for SNMPv3 support. At this time, SNMPv3 agents are only available using 3rd party vendors. There are a number of them available, including the opensource net-snmp agent. This could possibly be ported to Windows using GNUWin32. It is also available via CYGWIN.

An often-overlooked area is the printers and copy machines located on the network. Printers and copiers come with SNMP installed and usually configured with default community strings or proprietary community strings. Many now have hard drives and memory chips, like RAM, that can be configured using SNMP, or with just a telnet access. This is a prime spot for backdoor Trojans and an easy backdoor into the network. Or, it is a great collection point to sit and gather information. Further research needs to be done to help secure these machines and limit their access. The newer machines already use SNMPv2. We have the ability to configure and secure access to these machines via a strong complex community string. This is much preferable to using Telnet, although it is said that many of the HP printers will respond to any community string. This should be tested. SNMPv3 also needs to be researched and addressed.

Printing from the web application, for reports, needs to be configured. The reports are not printed from the browser windows, but instead are printed from the server. The user must know the name of the printer that has been configured on the server in order to print.

A Nessus scan of the machine after installation reveals the following:

. List of open ports :
  o ssh (22/tcp) (Security notes found)
  o http (80/tcp) (Security warnings found)
  o snmptrap (162/tcp)
  o nessus (1241/tcp) (Security warnings found)

- o bigbrother (1984/tcp)
- o mysql (3306/tcp) (Security warnings found)
- o VeritasNetbackup (13722/tcp) (Security notes found)
- o VeritasNetbackup (13782/tcp)
- o VeritasNetbackup (13783/tcp)
- o general/tcp (Security notes found)
- o snmp (161/udp) (Security hole found)
- o unknown (3306/tcp) (Security hole found)

Vulnerability found on port snmp (161/udp): SNMP Agent responded as expected with community name: snmpd

This vulnerability suggests that this machine is responding to SNMP queries using the community string snmpd. Further research is needed to verify this observation. Since this is not set in any of the configuration files, the question that remains is whether there exists a hidden community string that is responding to snmpd. This is mitigated, since it is set only to respond to localhost.

The entire NESSUS scan report is listed in Appendix C.

What this scan tells us is that many of the original vulnerabilities have been shut down, and there are no additional vulnerabilities that have been added as a result of adding the software HP Openview NNM.

A snoop packet capture, using the command:

snoop –r –v –x 10.10.10.11 port 161

shows the following information about the SNMP packet:

```
ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 1 arrived at 12:22:53.30
ETHER:  Packet size = 79 bytes
ETHER:  Destination = 0:50:d1:xx:xx:x,
ETHER:  Source      = 0:3:ba:xx:xx:xx,
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:   ----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 65 bytes
IP:   Identification = 53171
IP:   Flags = 0x4
IP:         .1.. .... = do not fragment
```

```
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 255 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = 91c8
IP:   Source address = 10.10.10.10, 10.10.10.10
IP:   Destination address = 10.10.10.11, 10.10.10.11
IP:   No options
IP:
UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 38488
UDP:  Destination port = 161
UDP:  Length = 45
UDP:  Checksum = 2539
UDP:


         0: 0050 d1ad c400 0003 ba29 c916 0800 4500    .P.......)....E.
        16: 0041 cfb3 4000 ff11 91c8 0a85 0325 0a85    .A..@........%..
        32: 0201 9658 00a1 002d 2539 3023 0201 0104    ...X...-%90#....
        48: 0444 4554 52a1 1802 0233 1702 0100 0201    .COMM....3......
        64: 0030 0c30 0a06 062b 0601 0201 0105 00      .0.0...+.......
```

Note that the community string is clearly visible, in this case as COMM. Although the protocol is snmpv2, it is not using any encryption. Additional research needs to be done to enable encryption.

Although many of the vulnerabilities of SNMP and HP Openview have been addressed, there is still a good deal of research that could be done to more securely implement this product. HP Openview is a work in progress. It takes continual monitoring and evaluation to be able to get the most from this product.

References

1. "Configuring OpenSSH for the Solaris™ Operating Environment" by Jason Reid, http://www.sun.com/blueprints/0102/configssh.pdf

2. "Consultant's Report from auditing UNIX" by Mark A. Winship, http://www.giac.org/practical/GCUX/Mark_Winship_GCUX.pdf

3. "Crash Course in X-Windows Security", http://bau2.uibk.ac.at/matic/ccxsec.htm

4. "Deployment Report for RFCs 1905-7", http://www.ietf.org/IESG/Implementations/SNMPv2-Implementation

5. "Deployment Report for RFCs 2571-2575, http://www.ietf.org/IESG/Implementations/2571-2575-Deployment.txt

6. "Extending Authentication in the Solaris™ 9 Operating Environment Using Pluggable Authentication Modules (PAM): Part I", Michael Haines, SunTM ONE Directory Server Group, http://www.sun.com/blueprints/0902/816-7669-10.pdf

7. "HP OpenView Network Node Manager Integration", http://www.tripwire.com/products/integrations/openview/node_manager.cfm

8. "LBNL ITSD Backup Services FAQ**",** by Christopher Manders, http://servback.lbl.gov/backups/documentation/documentation.html

9. Network Security Essentials, by William Stallings, Prentice Hall, 2000.

10. "Ports & Services",http://www.spirit.com/Resources/ports.html, by Rik Farrow.

11. "Ports List", http://www.neohapsis.com/neolabs/neo-ports/, Maintained by mjanowski @ neohapsis.com.

12. "Quick Start Installation Guide for HP OpenView Network Node Manager and HP OpenView Customer Views for NNM", Hewlett-Packard Company, 2001.

13. RFC1156, "Management Information Base for Network Management of TCP/IP-based internets", http://rfc.net/rfc1156.html

14. RFC1157, “A Simple Network Management Protocol (SNMP)”, http://rfc.net/rfc1157.html

15. RFC1447, “Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)”, http://rfc.net/rfc1447.html

16. RFC1451, “Manager-to-Manager Management Information Base”, http://rfc.net/rfc1451.html

17. RFC1901, “Introduction to community based SNMPv2”, http://rfc.net/rfc1901.html

18. RFC1909, “An Administrative Infrastructure for SNMPv2”, http://rfc.net/rfc1909.html

19. RFC1910, “User-based Security Model for SNMPv2”, http://rfc.net/rfc1910.html

20. RFC2261, “An architecture for Describing SNMP Management Framework”, http://rfc.net/rfc2261.html

21. RFC2570, “Introduction to Version 3 of the Internet-standard Network Management Framework”, http://rfc.net/rfc2570.html

22. RFC2571, “An Architecture for Describing SNMP Management Framework”, http://rfc.net/rfc2571.html

23. RFC2572, “Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)”, http://rfc.net/rfc2572.html

24. RFC2573, “SNMP Applications”, http://rfc.net/rfc2573.html

25. RFC2574, “User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)”, http://rfc.net/rfc2574.html

26. RFC2575, “View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) ”, http://rfc.net/rfc2575.html

27. “Securing Hewlett Packard OpenView Network Node Manager On HP-UX 11” by Rich Antonick, http://www.giac.org/practical/Rich_Antonick_GCUX.doc

28. “Securing SNMP on Solaris”, by Reg Quinton, SysAdmin, the Journal for Unix and Linux Administrator, http://www.samag.com/documents/s=1148/sam0107m/0107m.htm

29. "Security Reivew: Securing SNMP on Solaris", Information Systems and Technology, University of Waterloo, http://ist.uwaterloo.ca/security/howto/2000-10-04/recommend.html

30. "Simple Network Management Protocol", http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

31. "SNMP Security Pack" http://www.snmp.com/products/snmpsecpack.html

32. "SNMPv2 – Extending the Services of SNMP", http://www.cellsoft.de/telecom/snmpv2.htm

33. "Solaris 8 Advanced Installation Guide", http://docs.sun.com/db/doc/806-0957?q=solaris+advanced+installation+guide

34. "Solaris Security Guide", http://sabernet.home.comcast.net/papers/Solaris.html

35. **"**SSH Users beware: The hazards of X11 forwarding"by Brian Hatch, http://www.hackinglinuxexposed.com/articles/20040705.html

36. "Sun Solaris Security", http://wwws.sun.com/software/whitepapers/wp-security/

37. "VERITAS NetBackup Advanced Reporter™ 5.0", http://ftp.up.ac.za/pub/windows/veritas/264221.pdf

38. "What the Heck is PAM anyhow?" By Kevin Fenzi, http://news.tucows.com/ext2/99/08/security/081999-security1.shtml

39. "X Over SSH2 – A Tutorial", Van Emery, May, 2003, http://www.vanemery.com/Linux/XoverSSH/X-over-SSH2.html

40. "X Windows Security: How to Protect your Display" by Arturo Guillen, http://www.sans.org/rr/papers/63/328.pdf

Appendix A

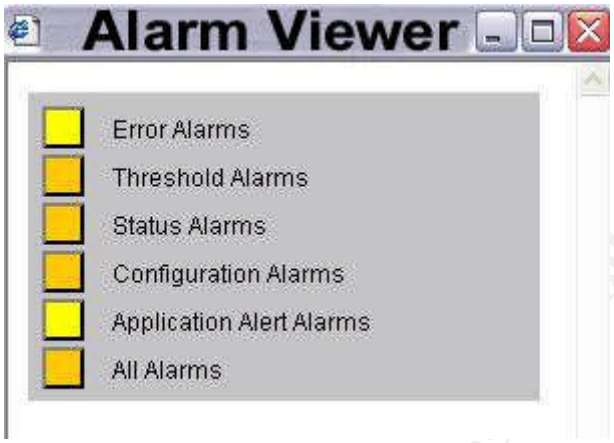
Tripwire Integrity Check Report version 4.0.0
Tripwire(R) for Servers version 4.1.0.210

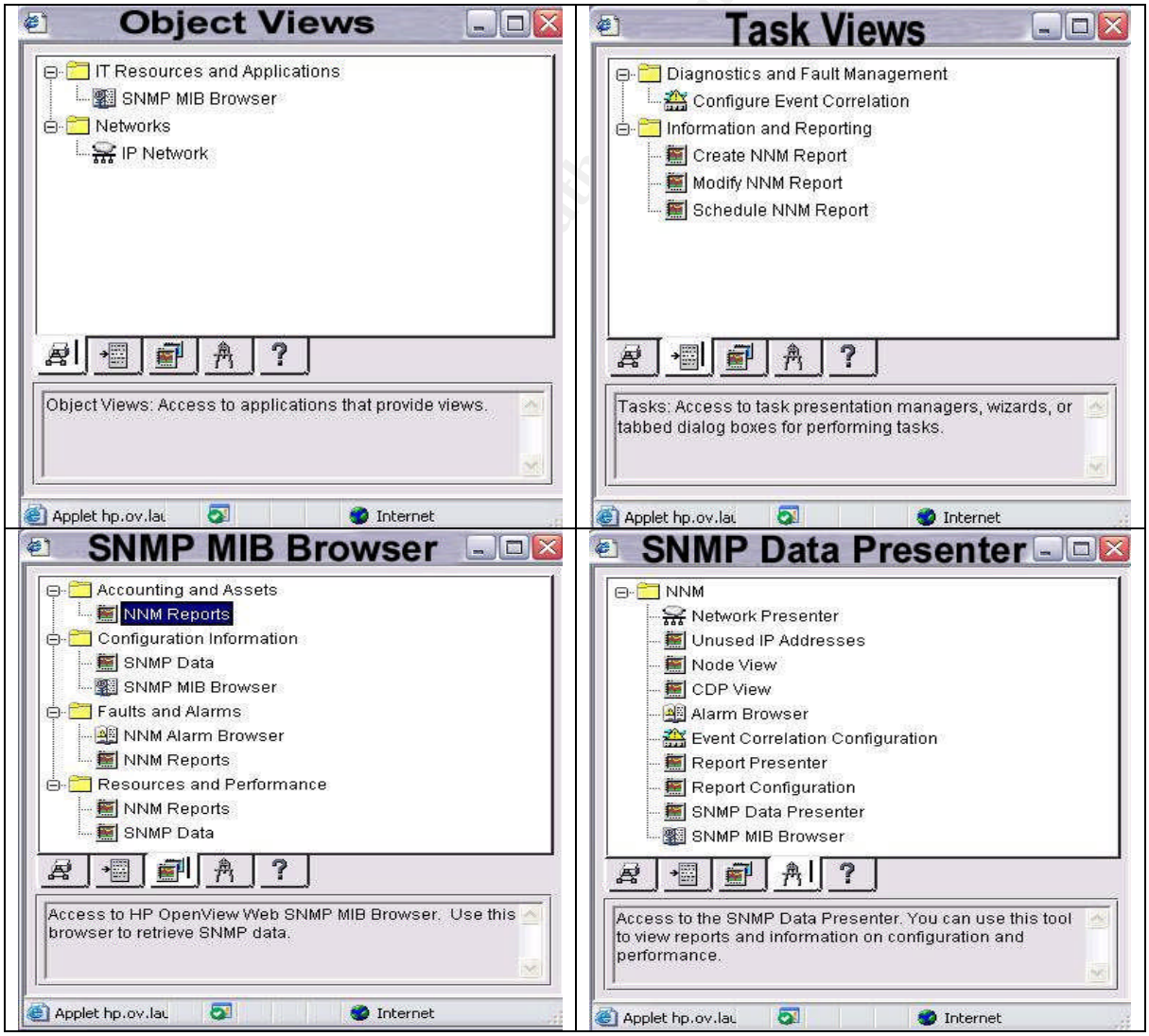
Report generated by: root
Report created on: Tue, 21 Sep 2004 21:30:00 -0700
Database last updated on: Fri, 17 Sep 2004 00:49:06 -0700
==========
Report Summary:
==========
Host name: myhostname
Host IP address: 10.10.10.10
Host ID: 0x8333abcd
Policy file used: /usr/local/tripwire/tfs/policy/tw.pol
Configuration file used: /usr/local/tripwire/tfs/bin/tw.cfg
Database file used: /usr/local/tripwire/tfs/db/database.twd
Command line used: /usr/local/tripwire/tfs/bin/tripwire --check
==========
Rule Summary:
==========
Section: Unix File System

Rule Name	Severity Level	Added	Removed	Modified
Tripwire Data Files	100	0	0	0
System Devices	100	0	0	0
User Home Directories	35	0	0	0
Mounted Filesystems	100	0	0	0
(/mnt)				
Other Filesystems	100	0	0	0
System Processes	100	0	0	0
(/proc)				
Temporary directory	35	0	0	0
(/tmp)				
Variable System Files	35	0	0	0
Tripwire Binaries	100	0	0	0
System Binaries	100	0	0	0
Library Files	35	0	0	0
Include Files	35	0	0	0
Man Pages	35	0	0	0
Administrative Binaries	100	0	0	0
* System configuration files	100	0	0	1
System Directories	100	0	0	0

```
Total objects scanned:  31180
Total violations found:  1
===============================================================
Object Detail:
===============================================================
---------------------------------------------------------------------------
  Section: Unix File System
---------------------------------------------------------------------------
Rule Name: System configuration files (/etc)
Severity Level: 100
---------------------------------------------------------------------------
  ----------------------------------------
  Modified Objects: 1
  ----------------------------------------
Modified object name:  /etc/.pwd.lock
      Modify Time Expected  Fri, 03 Sep 2004 14:45:18 -0700
*             Observed  Fri, 24 Sep 2004 11:11:20 -0700

      Change Time Expected  Fri, 03 Sep 2004 14:45:18 -0700
*             Observed  Fri, 24 Sep 2004 11:11:20 -0700

===============================================================
Error Report:
===============================================================

No Errors

---------------------------------------------------------------------------
*** End of report ***

Report generated by:
Tripwire(R) for Servers version 4.1.0.210 for Solaris (SPARC) Operating
Systems
Tripwire is a registered trademark of Tripwire, Inc. All rights reserved.
```

APPENDIX B





APPENDIX C

Nessus Scan Report

SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 2
- Number of security warnings found : 10
- Number of security notes found : 11

TESTED HOSTS

Host (Security holes found)

DETAILS

+ Host :
. List of open ports :
  o ssh (22/tcp) (Security notes found)
  o http (80/tcp) (Security warnings found)
  o snmptrap (162/tcp)
  o nessus (1241/tcp) (Security warnings found)
  o bigbrother (1984/tcp)
  o mysql (3306/tcp) (Security warnings found)
  o VeritasNetbackup (13722/tcp) (Security notes found)
  o VeritasNetbackup (13782/tcp)
  o VeritasNetbackup (13783/tcp)
  o general/tcp (Security notes found)
  o snmp (161/udp) (Security hole found)
  o unknown (3306/tcp) (Security hole found)

. Information found on port ssh (22/tcp)

  An ssh server is running on this port

. Information found on port ssh (22/tcp)

  Remote SSH version : SSH-2.0-OpenSSH_3.8p1

. Information found on port ssh (22/tcp)

  The remote SSH daemon supports the following versions of the
  SSH protocol :

. 1.99
. 2.0

SSHv2 host key fingerprint : b5:b7:b9:ba:9e:43:bf:61:80:6b:c4:af:98:99:a4:3d

. Warning found on port http (80/tcp)

The remote host is running a version of PHP which is older than 4.3.2

There is a flaw in this version which may allow an attacker who has the ability to inject an arbitrary argument to the function socket_iovec_alloc() to crash the remote service and possibly to execute arbitrary code.

For this attack to work, PHP has to be compiled with the option
--enable-sockets (which is disabled by default), and an attacker needs to be able to pass arbitrary values to socket_iovec_alloc().

Other functions are vulnerable to such flaws : openlog(), socket_recv(), socket_recvfrom() and emalloc()

Solution : Upgrade to PHP 4.3.2
Risk factor : Low
CVE : CAN-2003-0172
BID : 7187, 7197, 7198, 7199, 7210, 7256, 7259

. Warning found on port http (80/tcp)

The remote host is running a version of PHP which is older than 4.3.2

There is a flaw in this version which may allow an attacker who has the ability to inject an arbitrary argument to the function socket_iovec_alloc()to crash the remote service and possibly to execute arbitrary code.

For this attack to work, PHP has to be compiled with the option
--enable-sockets (which is disabled by default), and an attacker needs to be able to pass arbitrary values to socket_iovec_alloc().

Other functions are vulnerable to such flaws : openlog(), socket_recv(), socket_recvfrom() and emalloc()

Solution : Upgrade to PHP 4.3.2
Risk factor : Low
CVE : CAN-2003-0172
BID : 7187, 7197, 7198, 7199, 7210, 7256, 7259

. Warning found on port http (80/tcp)

The remote web server appears to be running a version of Apache that is less that 2.0.49 or 1.3.31.

These versions are vulnerable to a denial of service attack where a remote attacker can block new connections to the server by connecting to a listening socket on a rarely accessed port.

Solution: Upgrade to Apache 2.0.49 or 1.3.31.
CVE : CAN-2004-0174
BID : 9921

. Warning found on port http (80/tcp)

The remote web server appears to be running a version of Apache that is less that 2.0.49 or 1.3.31.

These versions are vulnerable to a denial of service attack where a remote attacker can block new connections to the server by connecting to a listening socket on a rarely accessed port.

Solution: Upgrade to Apache 2.0.49 or 1.3.31.
CVE : CAN-2004-0174
BID : 9921

. Warning found on port http (80/tcp)

The target is running an Apache web server which allows for the injection of arbitrary escape sequences into its error logs. An attacker might use this vulnerability in an attempt to exploit similar vulnerabilities in terminal emulators.

***** Nessus has determined the vulnerability exists only by looking at
***** the Server header returned by the web server running on the target.

Solution : Upgrade to Apache version 1.3.31 or 2.0.49 or newer.
Risk factor : Low
CVE : CAN-2003-0020
BID : 9930
Other references : APPLE-SA:APPLE-SA-2004-05-03, CLSA:CLSA-2004:839, HPSB:HPSBUX01022, RHSA:RHSA-2003:139-07, RHSA:RHSA-2003:243-07, MDKSA:MDKSA-2003:050, OpenPKG-SA:OpenPKG-SA-2004.021-apache, SSA:SSA:2004-133-01, SuSE-SA:SuSE-SA:2004:009, TLSA:TLSA-2004-11, TSLSA:TSLSA-2004-0017

. Warning found on port http (80/tcp)

The target is running an Apache web server which allows for the injection of arbitrary escape sequences into its error logs. An attacker might use this vulnerability in an attempt to exploit similar vulnerabilities in terminal emulators.

```
***** Nessus has determined the vulnerability exists only by looking at
***** the Server header returned by the web server running on the target.

Solution : Upgrade to Apache version 1.3.31 or 2.0.49 or newer.
Risk factor : Low
CVE : CAN-2003-0020
BID : 9930
Other references : APPLE-SA:APPLE-SA-2004-05-03, CLSA:CLSA-2004:839,
HPSB:HPSBUX01022, RHSA:RHSA-2003:139-07, RHSA:RHSA-2003:243-07,
MDKSA:MDKSA-2003:050, OpenPKG-SA:OpenPKG-SA-2004.021-apache,
SSA:SSA:2004-133-01, SuSE-SA:SuSE-SA:2004:009, TLSA:TLSA-2004-11,
TSLSA:TSLSA-2004-0017

. Warning found on port http (80/tcp)

Your webserver supports the TRACE and/or TRACK methods. TRACE and
TRACK are HTTP methods which are used to debug web server connections.
```

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution: Disable these methods.

If you are using Apache, add the following lines for each virtual host in your configuration file:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy.

If you are using Sun ONE Web Server releases 6.0 SP2 and later, add the following to the default object section in obj.conf:

```
<Client method="TRACE">
 AuthTrans fn="set-variable"
```

```
 remove-headers="transfer-encoding"
 set-headers="content-length: -1"
 error="501"
</Client>
```

If you are using Sun ONE Web Server releases 6.0 SP2 or below, compile the NSAPI plugin located at:
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603

See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603
http://www.kb.cert.org/vuls/id/867593

Risk factor : Medium

. Warning found on port http (80/tcp)

Requesting the URI /server-status gives information about the currently running Apache.

Risk factor : Low
Solution :
If you don't use this feature, comment the appropriate section in your httpd.conf file. If you really need it, limit its access to the administrator's machine.

. Information found on port http (80/tcp)

A web server is running on this port

. Information found on port http (80/tcp)

The remote web server type is :

Apache/1.3.26 (Unix) PHP/4.2.3 mod_perl/1.24

Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

. Warning found on port nessus (1241/tcp)

A Nessus Daemon is listening on this port.

. Information found on port nessus (1241/tcp)

A TLSv1 server answered on this port

. Warning found on port mysql (3306/tcp)

You are running a version of MySQL which is older than version 4.0.21.

There are two flaws in the remote version of this database :

- There is an unauthorized database GRANT privilege vulnerability, which may allow an attacker to misuse the GRANT privilege it has been given and to use it against other databases

- A denial of service vulnerability may be triggered by the misuse of the FULLTEXT search functionality.

Solution : Upgrade to MySQL 4.0.21
Risk factor : Medium
BID : 11435, 11432

. Information found on port mysql (3306/tcp)

An unknown service is running on this port.
It is usually reserved for MySQL

. Information found on port mysql (3306/tcp)

Remote MySQL version : 3.23.52

. Information found on port VeritasNetbackup (13722/tcp)

VeritasNetBackup is running on this port:

. Information found on port general/tcp

HTTP NIDS evasion functions are enabled.
You may get some false negative results

. Information found on port general/tcp

10.10.10.10 resolves as Host.

. Vulnerability found on port snmp (161/udp) :

SNMP Agent responded as expected with community name: snmpd
CVE : CAN-1999-0517, CAN-1999-0186, CAN-1999-0254, CAN-1999-0516
BID : 11237, 10576, 177, 2112, 6825, 7081, 7212, 7317, 9681

Other references : IAVA:2001-B-0001

. Vulnerability found on port unknown (3306/tcp) :

The remote host is missing Sun Security Patch number 107299-03
(ntpdate and xntpd patch).

You should install this patch for your system to be up-to-date.

Solution :
http://sunsolve.sun.com/search/document.do?assetkey=1-21-107299-03-1
Risk factor : High
BID : 2540

This file was generated by the Nessus Security Scanner