# Global Information Assurance Certification Paper

# Securing Hewlett Packard OpenView Network Node Manager On HP-UX 11

Rich Antonick
GCUX Practical Assignment
Version 1.8

January 31, 2002

# Table of Contents

# 1 Introduction

This paper describes the steps necessary for a novice system administrator to install the HP-UX 11 operating system and the HP OpenView Network Node Manager application in as secure a manner as possible. Typical vulnerabilities will be described and appropriate configuration measures to mitigate those vulnerabilities will be described in detail.

Ongoing maintenance will be described to maintain the OS and the application at the original level of security.

Methods of verifying the security described will be provided with results of applying those methods.

## *1.1 System Role*

This system will be configured as a network management station running the Hewlett Packard OpenView Network Node Manager product. The steps that follow create a very specific security configuration. Before using this document in a particular environment, the site security policy must be reviewed and the steps modified to conform to the policy.

NNM is a SNMP-based network management tool. It provides network discovery, event management, data collection, graphing, reporting and a graphical representation of the logical topology of the network.

# 2 System Configuration

## *2.1 Hardware Information*

| Type | Description |
|---|---|
| Model | HP 9000/785/C3600 |
| Memory | 512 MB |
| CPU | 552 MHz |
| Disks | 1 SEAGATE ST39204LC at 10/0/15/1.5.0<br>2 SEAGATE ST39204LC at 10/0/15/1.6.0<br>3 SEAGATE ST39175LC at 10/1/5/0.5.0 (external)<br>4 SEAGATE ST39175LC at 10/1/5/0.6.0 (external) |
| Network Cards | LAN 0 10/100BASE-TX card at 10/1/4/0<br>LAN 1 10/100BASE-TX card at 10/0/12/0<br>LAN 2 10/100BASE-TX card at 10/4/3/0 |
| Tape Drive | HP C5683A at 10/1/6/0.3.0 (external) |
| CDROM Drive | MITSUMI CD-ROM FX4830T!B at 10/0/14/0.0.0 |
| Monitor | HP 21 inch color monitor model #D8915 |

## *2.2 Software Information*

| Product | Version |
|---|---|
| HP-UX | 11.0 |

| Product | Version |
|---|---|
| HP OV Network Node Manager | 6.2 |

### 2.2.1 HP-UX CD ROMs

| Name | Date | HP Part Number |
|---|---|---|
| HP-UX 11.0 Additional Core Enhancements (Install/Update/Recovery Core OS) CD ROM | December 2000 | 5011-4484 |
| HP-UX 11.0 Core OS Options | June 2000 | B3782-10495 |
| HP-UX 11.0 Support Plus | December 2000 | 5011-7888 |

### 2.2.2 Applications/Packages

Always install the latest version of an application, whenever possible, to ensure that the latest security enhancements have been included.

The NNM 6.2 package includes the following applications/components:

- Emanate SNMP Agent
- Event Correlation Services (ECS)
- Apache
- Solid DB
- Netscape

## 3 Risk Analysis of the server

Computing systems have inherent security vulnerabilities. Each application brings new and different vulnerabilities peculiar to its operation. Network management systems (NMSs) communicate with many devices in an enterprise. Depending on the size of the management domain, the NMS could manage every device in the network. Since network devices are prime targets for attacks, a great deal of sensitive information is passed over the network during the course of the day. And most of that information is stored on the NMS

Typically, a network management system is configured to monitor the primary networking devices such as routers, switches and hubs. The NMS is thus able to collect a large about of information about the network.

**A note on monitoring versus managing**. The terms "monitor" and "manage" are often used interchangeably. The primary difference is that monitoring is a (relatively) passive function. The systems being monitored are not altered or directed to change state in any way. Managing implies that the managed device can be controlled, for example, instructed to reboot or to disable a network interface.

### *3.1 Information Gathering*

An attacker does not have to eavesdrop on messages passing between the management system and the managed nodes to gather information. If the NMS is comprised, it's entire database is available to the attacker.

### 3.2 Denial Of Service and other disruptions

As a networked node using the TCP/IP protocol suite, the NMS is vulnerable to all the common attacks such as denial of service and other disruptions. Although there are a number of ways to alter the TCP/IP stack to reduce or eliminate these attacks, by its nature, the NMS can't always use these methods. For example, NNM relies on arp cache entries and ICMP echo request broadcasts for network discovery. These very mechanisms are often used for attacks.

### 3.3 Platform For Further Attacks

Again, like other networked nodes using TCP/IP, the NMS can be exploited to be used as a platform for a hacker to launch attacks on other systems. The impact is magnified due to the potentially large number of systems which could be attacked.

### 3.4 Additional Applications Vulnerabilities

NNM relies on additional packages and components for its operation (see the Applications/Packages section below). And each of those components brings their own vulnerabilities. For example, Apache is used for web services. Like many popular networking packages, Apache is often exploited. These applications bring potential liabilities which are magnified by the effort of dealing with different support organizations when an exploit is revealed and a fix is needed.

### 3.5 Remote Control

SNMP is capable of changing the state of managed devices.

1. This requires that the SNMP set community string used by the manager matches the set community string of the agent on the managed device.
2. The agent supports MIB objects which can modify its state.
3. The manager knows what those manageable MIB objects are.

Since SNMP get and set community strings are passed in plain text over the network, it is generally a bad idea to allow sets of any kind. This obviously reduces the management capability of an SNMP-based management system.

## 4 Step-By-Step Guide

### 4.1 OS Installation

This installation assumes that the system has been configured and connected. If the operating systems is pre-installed, it will be overwritten during the installation.

#### 4.1.1 Preparation

| # | Task |
|---|---|
| 1. | Disconnect all network interfaces. This prevents intruders from attacking the system before all hardening mechanisms have been configured. |
| 2. | Turn on the computer. First, power on the monitor. Second, power on each of the 3 peripherals (1 tape drive and 2 disk drives). Third, turn on the system power. |

### 4.1.2 Boot Up HP-UX Installation Program

| # | Task |
|---|---|
| 1. | At the prompt "Processor is starting autoboot process, press any key to stop" press any key to stop the boot process. The boot menu will appear. |
| 2. | Insert the CD ROM labeled HP-UX 11.0 Additional Core Enhancements into the CD ROM drive. |
| 3. | Determine the boot path for the CD ROM by typing search at the "enter command >" prompt. Look for the Device Type FX4830T and note the Path Number (P0) |
| 4. | Issue the boot command using the Path Number, for example,<br>`bo P0` |
| 5. | The system will ask if you would like to interact with IPL. Answer "**NO**" to this prompt. |
| 6. | The Message "booting…" will appear, followed by progress of the boot process, which should take approximately 3 to 5 minutes. |
| 7. | When the keyboard language prompt appears ("Enter the number of the language you want:") enter **26** for USB_PS2_DIN_US_English |
| 8. | A menu will appear with the title "*Welcome to the HP-UX installation process,*" Select **Install HP-UX** from the menu. |

(Installing HP-UX 11, 34 – 41)

### 4.1.3 Select OS Installation Options

| # | Task |
|---|---|
| 1. | A menu will appear with the title "*User Interface and Media Options,*" Check off the following:<br>[ * ] **Media only installation**<br>[ * ] **Advanced Installation** (recommended for disk and file system management) |
| 2. | Select **OK** |

A configuration window will appear with the title "/opt/ignite/bin/itool () ." This is the configuration screen for all operating system parameters required for installation. It is divided into sections. The tables which follow in this section include the specific information for each section and are labeled to match the section. Use the Tab and Shift-Tab keys to navigated through the menus. Keyboard shortcuts are available for any choice with the first letter underlined. See the Help section for additional information on using the configuration interface.

**NOTE: Due to system limitations, only 1 disk was available for this configuration. It is desirable, when possible, to use multiple disks for a NNM installation. This allows installing the OS on the root disk and the application(s) on additional disks. Separate controllers should be used. This provides improved disk performance and increased stability of the root disk. If additional disks are available, see the Appendix section Appendix B: File system layout using 2 disks**

**Basic**

| Parameter | Value |
|---|---|

| Parameter | Value |
|---|---|
| Configurations | 11.00 for Technical Computing (Requires Core-Options + Support Plus (CDs) |
| Environments | 64-Bit CDE HP-UX Environment |
| Root Disk | SEAGATE ST39204LC 10/0/15/1.5.0, 8678M |
| File System | Logical Volume Manager (LVM) with VxFS |
| Root Swap | 1024 |
| Languages | English |
| Keyboards | USB_PS2_DIN_US_English |
| Additional | See Additional table below |

**Additional**

| Parameter | Value |
|---|---|
| Create /export volume | No (NOTE: NFS will be disabled due to security vulnerabilities) |
| Create separate Volumes | Yes |
| Secondary Swap space | 0 |
| # of disks in root VG | 1 |
| Force Ignite-UX autoboot? | YES |
| Disable DHCP? | YES (NOTE: This server must use a static address since managed nodes need a permanent address to send SNMP traps to) |
| Save patches files? | YES |

**Software**

| Category | Value |
|---|---|
| OrderedApps | <NONE> |
| UserLicenses | 2-user HP-UX 2-User License |
| PCI Card Apps | B5509BA 100BT/9000 PCI |
| HPPB Card Apps | <NONE> |
| GSC/HSC Card Apps | <NONE> |
| HPUXAdditions | 64-bitDevLibs Cross Platform Development Kit<br>Integ-Logon Integrated Logon Bundle<br>KernDev HPUX Kernel Developers Kit<br>XSWGR1100 HP-UX General Release Patches, December 2000<br>XSWHWCR1100 HP-UX Hardware Enablement and Critical Patches, June 2000 |
| Uncategorized | <NONE> |

**System**

| Category | Value |
|---|---|
| Final System Parameters | Set parameters now |
| Hostname: | hpovnnm1 |
| IP Address | 10.1.2.20 |
| Subnet Mask: | 255.255.0.0 |
| Time, Day, Month, | <Enter as appropriate> |

| Category | Value |
|---|---|
| Year | |
| Set Time Zone | For example: Atlantic Standard/Daylight PST8PDT |
| Network Services | See Network Services table below |
| Set Root Password | Use a strong password to prevent guessing and easy cracking. See password guidelines section: Appendix C. Password Guidelines |
| Additional Interfaces | Lan0 10/0/12/0 10.1.2.20 255.255.0.0 Primary Interface<br>Lan0 10/1/4/0 <NONE><br>Lan0 10/4/3/0 <NONE> |

**Network Services**

| Category | Value |
|---|---|
| Static Routes | Destination: default<br>Gateway Address: 10.1.254.254<br>Hop Count: 1 |
| DNS | <NONE><br>NOTE: Do not set up DNS now. This server would search for the DNS server for all network services requiring name resolution. The subsequent resolution timeouts and retries would significantly impact boot up time and interfere with CDE.<br>DNS will be configured when the server is connected to a network. |
| NIS | <NONE><br>NIS security is weak. Passwords are passed in plain text and it does not support shadow password files. |
| XNTP | 255.255.0.0 |

**File System**

| Mount Point | Usage | Size | Group |
|---|---|---|---|
| / | VxFS | 500 | vg00 |
| /stand | HFS | 84 | vg00 |
| Primary Swap | swap | 1024 | vg00 |
| /home | VxFS | 500 | vg00 |
| /opt | VxFS | 1000 | vg00 |
| /tmp | VxFS | 300 | vg00 |
| /usr | VxFS | 1500 | vg00 |
| /var | VxFS | 2000 | vg00 |

**Advanced**

| Category | Value |
|---|---|
| Scripts to be Executed | <NONE> |

### 4.1.4 Install With Selected Options

| # | Task |
|---|---|
| 1. | After all configuration screens have been filled out as specified in the tables above, select **Go!** |

| # | Task |
|---|---|
| 2. | A message box will appear with information similar to the following:<br>itool Confirmation<br>All data will be destroyed on the following disks:<br>10/0/15/1/5/0 8678 MB SEAGATE_ST39204L<br><br>Supply the HP-UX Core OS Options media and the HP-UX Support Plus media when prompted during the installation |
| 3. | The install will run for about 10 minutes. Then the system will beep and display the following:<br>USER INTERACTION REQUIRED<br>To complete the installation you must now insert the "HP-UX 11.00 Core OS Options" CD.<br>Once this is done, press the <Return> key to continue.<br>Press **Return** |
| 4. | The install will resume running. After about 5 minutes. The system will beep again and display the following:<br>USER INTERACTION REQUIRED<br>To complete the installation you must now insert the "HP-UX 11.00 Support Plus" CD.<br>Once this is done, press the <Return> key to continue.<br>Press **Return** |

### 4.1.5 Install system patches

| # | Task |
|---|---|
| 1. | Install the General Release Patch Bundle:<br>**swinstall -s hpovnnm1:/SD_CDROM/XSWGR1100 -x patch_match_target=true -x autoreboot=true** |
| 2. | Install the Critical Release Patch Bundle:<br>**swinstall -s hpovnnm1:/SD_CDROM/XSWHWCR1100 -x patch_match_target=true -x autoreboot=true** |

## *4.2 Operating System Configuration*

### 4.2.1 Networking Configuration

#### 4.2.1.1 Network Services

##### *4.2.1.1.1 /etc/inetd.conf*

inetd controls many of the Internet server processes on the system. Most are not required, pose potential security risks, and should be disabled if not explicitly needed. Inetd cannot be completely disabled since there are a number of services required to support X11 and CDE. Comment out or delete the following entries:

**Inetd Services To Disable**

| Service | Description |
|---|---|

| | |
|---|---|
| ftp | File Transfer Protocol. Prevent the installation of evil software or copying of sensitive files (ftpd).<br>**Note**: FTP will be used to transfer software to this system for installation. Don't disable it now. Do it in the post-installation tasks (see Disable FTP) |
| login | Remote login (rlogind) |
| shell | Remote command (remshd) |
| exec | Remote execution (rexecd) |
| ntalk | New talk, conversation (ntalkd) |
| ident | TCP/IP IDENT (authentication) protocol server (identd) |
| printer | Remote print spooling (rlpdaemon) |
| daytime | Inetd internal service |
| time | Inetd internal service |
| echo | Inetd internal service |
| chargen | Inetd internal service |
| discard | Inetd internal service |
| kshell | Kerberized remshd |
| klogin | Kerberized rlogind |

#### *4.2.1.1.2 /etc/rc.config.d*

HP-UX provides a simplified mechanism for disabling the startup of system services. In other UNIX versions, such as Solaris, the links in the rc directories must be altered or removed to prevent a service from starting. HP-UX uses configuration files in /etc/rc.config.d. These files contain environment variables which are sourced in by each startup script. The script determines if the service should be started and how it should behave based on those variables. The following table lists the file name, parameter and value it must be set to for the service to be turned off (not started) or modified to operate more securely. Changes to these parameters will take effect after the next reboot. Disable/modify the following services:

**System Services To Disable/Modify**

| File Name | Parameter | Value | Description |
|---|---|---|---|
| mailservs | SENDMAIL_SERVER | 0 | Sendmail server |
| namesvrs | NAMED<br>NIS_MASTER_SERVER<br>NIS_MASTER_SERVER | 0 (default)<br>0 (default)<br>0 (default) | DNS server<br>Network Information Services<br>(formerly Yellow Pages) |
| netconf | GATED<br>RARP<br>DHCP_ENABLE[0] | 0 (default)<br>0 (default)<br>0 (default) | Routing daemon<br>Reverse ARP<br>DHCP for each interface |
| netdaemons | INETD_ARGS<br>START_RBOOTD<br>MROUTED<br>RWHOD | -l (ell)<br>0<br>0 (default)<br>0 (default) | Enable inetd logging<br>Remote boot daemon<br>Multicasting routing daemon<br>Remote system status daemon |
| nfsconf | NFS_CLIENT<br>NFS_SERVER | 0<br>0 | Network File System Client<br>Network File System Server |
| syslogd | SYSLOGD_OPTS | -DN | The N option disables logging from remote systems |

| File Name | Parameter | Value | Description |
|---|---|---|---|
| Rpcd | START_RPCD | 0 | Disable DCE RPC daemon |

#### 4.2.1.2 TCP/IP Parameters

TCP/IP tuning parameters are dynamic and must be set after each reboot using the ndd (1M) command. HP-UX 11 provides the /etc/rc.config.d/nddconf file for specifying changes to the TCP/IP parameters at boot time. Changes to these parameters will take effect after the next reboot. Entries are in the form:

TRANSPORT_NAME[0]=
NDD_NAME[0]=
NDD_VALUE[0]=

Transport Name is the part of the parameter name up to the first underscore. For example, the Transport Name for ip_forwarding is ip.

NDD_VALUE is in the V column in the table below. Add the entries listed below to the file:

| Parameter Name | V | Description |
|---|---|---|
| ip_forward_directed_broadcasts | 0 | Don't forward directed broadcasts |
| **ip_forward_src_routed** | 0 | Don't forward packets with source route options |
| ip_forwarding | 0 | Disable IP forwarding |
| tcp_conn_request_max | 500 | Increase TCP listen queue maximum (performance) |
| tcp_syn_rcvd_max | 500 | HP SYN flood defense |
| tcp_text_in_resets | 0 | Don't send text messages in TCP RST segments (should be the default) |

(Steves, section 10)

### 4.2.2 System Operation Configuration

#### 4.2.2.1 Update umask

Add the following to /etc/profile

```
#Tighten up default file permissions
umask 022
```

#### 4.2.2.2 Disable Root Login From The Network

To prevent anyone from logging in as root from the network, add the following line to /etc/securetty

```
console root
```

And change the permissions to hide the setting:

```
chmod 400 /etc/securetty
```

This will force all users to log in as themselves, and then su to root, providing an audit trail.

#### 4.2.2.3 Enable Trusted Computing

HP-UX does not support shadow passwords, by default. The encrypted passwords in /etc/passwd are world readable. Shadow password functionality is provided with HP's Trusted Computing facility. Use sam (1M) to enable Trusted Computing.

| Operation | Description |
|---|---|
| Convert to a Trusted System. Make the selections and follow the prompts | Select Auditing and Security<br>Select System Security Policies<br>Yes<br>Yes |
| Password Format Policies. Disable all Options<br>Maximum password length | Uncheck all boxes except User Specifies<br>13 |
| Password Aging | Disabled |
| General User Account Policies<br>Unsuccessful login Tries Allowed<br>Require Login Upon Boot to Single-User State | 3<br><br>Check |
| Terminal Security Policies | No change |

Note: All encrypted password fields in /etc/passwd will now have an asterisk (*) in place of the password. The actual passwords are now store under alphabetical directories in /tcb/files/auth. (Managing Systems and Workgroups 553-554)

#### 4.2.2.4 Syslog

Add and entry to /etc/syslog.conf for daemon logging. This allows tracking when system daemons start. This is useful since system daemons opening ports (such as ftpd) can be a security exposure. Even though most of the system daemons have been disabled in inetd.conf, logging will help catch changes caused by patches or accidental mis-configurations.

#### 4.2.2.5 Cron

Cron is disabled by default for all users except root, adm and uucp. Remove adm and uucp from /usr/lib/cron/cron.allow.

#### 4.2.2.6 User Accounts

User accounts should be kept to a minimum. Use NNM web access as much as possible. System service user accounts should be disabled or removed if possible. All pseudo accounts should not allow login.

"you should change the login shell to some invalid path, for example /, or consider using the **noshell** program from the Titan package"
bin:*:2:2:NO LOGIN:/usr/bin:/
(Steves, section 5, item 9)

### *4.3 Additional System Software*

Additional system software will be installed to provide extra security or supporting functionality not provided by the operating system or the primary applications. This software can be

downloaded from the sites listed in the following table. Installation instructions are in the section following the table.

### 4.3.1.1 Download Software

Download the following software into /tmp:

**Additional System Software Download sites**

| Software | URL |
|---|---|
| **IgniteUX** | **http://software.hp.com** |
| **perl 5** | **http://software.hp.com**<br>Note: Follow the instructions to download perl_11.00.depot. This version of perl is required for the security_patch_check installed in section Run security patch checker. The perl depot does not need to be uncompressed. |
| zlib | http://hpux.cs.utah.edu/hppd/hpux/Misc/zlib-1.1.3/ |
| SSL | http://hpux.cs.utah.edu/hppd/hpux/Languages/openssl-0.9.6/ |
| SSH | http://hpux.cs.utah.edu/hppd/hpux/Networking/Admin/openssh-3.0.2p1/ |
| lsof | http://hpux.cs.utah.edu/hppd/hpux/Sysadmin/lsof-4.55/ |

### 4.3.1.2 Install Software

Swinstall (1M) is the software installation component of HP's Software Distributor product. The commands above will invoke the GUI version of swinstall. For each package, highlight the package name and then select **Actions->Mark for Install** and **Actions->Install** and follow the instructions.

Some of these files will be in compressed format. Use /usr/contrib/bin/gunzip to uncompress each depot with a ".gz" extension

**Package installation:**

| Package | Installation Command Line |
|---|---|
| perl 5 | swinstall –s hpovnnm1:/tmp/perl_11.00.depot |
| zlib | swinstall –s hpovnnm1:/tmp/zlib-1.1.3-sd-11.00.depot |
| SSL | swinstall –s hpovnnm1:/tmp/openssl-0.9.6-sd-11.00.depot |
| SSH | swinstall –s hpovnnm1:/tmp/openssh-3.0.2p1-sd-11.00.depot |
| lsof | swinstall –s hpovnnm1:/tmp/lsof-4.55-sd-11.00.depot |
| sudo | swinstall –s hpovnnm1:/tmp/sudo-1.6.2b1-sd-11.depot |

### 4.3.1.3 Additional software configuration

#### *4.3.1.3.1 SSHD*

SSH is a secure replacement for rlogin and telnet. Create the start/stop and control scripts as shown in Appendix F: SSHD initialization script

#### *4.3.1.3.2 lsof*

"lsof may be the most indispensable system administration and forensics tool that nobody ever uses." (Pomeranz, 155)
It is used here for determining the relationships between processes, ports and files which may be mis-configured, malicious or misguided.

#### *4.3.1.3.3 sudo*

Root access should be limited to the fewest number of people. And root should be used as little as possible. Both to prevent malicious intent and to reduce errors, resulting in improved security. Sudo allows users to run commands as root without knowing the root password or actually switching users to root. Sudo is configured here to allow the *netmgr* user the ability to start and stop the NNM background processes. The commands ovstart and ovstop require root privilege.

Run the command /opt/sudo/sbin/visudo and add the following lines:

```
User_Alias   NNM_ADMINS=netmgr
HOST_ALIAS   NNM_SRVR=10.1.2.20
Cmnd_Alias   NNM = /opt/OV/bin/ovstart, /opt/OV/bin/ovstop
root         ALL = (ALL) ALL
NNM_ADMINS   NNM_SRVR = (root) NNM
```

Copy the temporary file to /etc/sudoers

```
cp /opt/sudo/etc/sudoers/sudoers.tmp /etc/sudo
```

Set the permissions to allow access only to root to hide the information from unauthorized users.

```
Chmod 600 /etc/sudoers
```

Allow sudo to run as root

```
chmod u+x /opt/sudo/bin/sudo
```

#### *4.3.1.3.4 Update PATH and MANPATH Environment Variables*

Several of the packages installed do not update the PATH environment variable. Add the following to /etc/PATH

```
:/opt/lsof/bin:/opt/openssh2/bin:/opt/sudo/bin:/opt/sudo/sbin
```

Command Reference manual (man) pages provide useful information on using the commands installed for securing this system. Several of the packages installed do not update the MANPATH environment variable. Add the following to /etc/MANPATH

```
:/opt/lsof/man:/opt/openssl/man:/opt/openssh2/man:/opt/sudo/man:
/opt/OV/httpd/man
```

### 4.3.2 Make A Bootable Recovery Tape

**Load an 8mm tape with sufficient capacity to hold all the data on the root disk (e.g. DDS2). The following command will write a bootable image of the root disk to the default tape device.**
**make_recovery –A**

## *4.4 Applications Install*

### 4.4.1 Install NNM

**NNM CD-ROM**

| Title | Version | Date | Part No. | Rev. |
|---|---|---|---|---|
| HP OpenView Solutions Network Node Manager HP-UX 10.20, 11.0, 11.11 | 6.0 | April 2001 | J1240-10827 | B.06.20 |

### 4.4.2 Pre-installation Steps

#### 4.4.2.1 DHCP

The NNM server must be assigned a static address. The server should not obtain its address from DHCP unless it can be guaranteed to be the same. Since DHCP configurations change and are administered by multiple administrators, DHCP should be used for the server only when absolutely necessary.

#### 4.4.2.2 Web Browser Installation

A web browser is required for normal NNM operation. Both the Reports and Event Correlation System (ECS) are configured via the web interface. Although a remote browser can be used, a local browser should be included to allow all configuration tasks from the server, unless a particular implementation does not include a graphics monitor. The Java-based graphical interfaces require the Java plug-in (JPI). Since this configuration includes one, Netscape will be installed as part of the NNM installation.

#### 4.4.2.3 Install Netscape Communicator

Download from http://software.hp.com by selecting Internet and Security Solutions and filling out the form. Select Netscape Communicator version 4.79 for HP-UX 11.0. Download the package into /tmp.

#### 4.4.2.4 Install NNM

| # | Task |
|---|---|
| 1. | Log in as root to the system where you will install NNM |
| 2. | Insert your NNM CD into the CD-ROM drive. |
| 3. | Mount the CD-ROM disk by typing<br>`/sbin/mount /dev/dsk/device_name /cdrom`<br>where **device_name** is the specific name of your CD drive. |
| 4. | Change to the /cdrom directory.<br>`cd /cdrom` |
| 5. | Start the installation program by typing<br>`./install` |

**NNM Installation Dialog**

| Prompt/Task | Value |
|---|---|
| Do you want to install the manpages? | y |

| Prompt/Task | Value |
|---|---|
| Do you want Network Node Manager to discover your network automatically after the installation? | n |
| Do you want the Network Node Manager to be displayed after the installation? | n |
| After the successful install message is displayed along with the NNM process status, Would you like to view the Release Notes? | n |
| xhost + hpovnnm1 | |

### 4.4.2.5 Verify NNM installation

After installation the NNM process status list will be displayed and should resemble the following:

```
Name              PID  State          Last Message(s)
OVsPMD           1559  RUNNING        -
ovsessionmgr     1571  RUNNING        Initialization complete.
ovwdb            1572  RUNNING        Initialization complete.
ovuispmd         1635  RUNNING        Initialized. 0 ovw clients registered.
ovtrapd          1631  RUNNING        Initialization complete.
ovactiond        1632  RUNNING        Initialization complete.
ovalarmsrv       1633  RUNNING        Initialization complete.
pmd              1573  RUNNING        Initialization complete.
ovdbcheck        1574  RUNNING        Connected to embedded database.
httpd               -  unknown        (Does not communicate with ovspmd.)
ovtopmd          1630  RUNNING        Connected to database "openview".
netmon           1636  RUNNING        Initialization complete.
snmpCollect      1637  RUNNING        Initialization complete.
ovrequestd       1576  RUNNING        Initialization complete.
```

### 4.4.2.6 Install NNM Patches

#### *4.4.2.6.1 NNM Patches*

HP OpenView provides individual patches to correct specific problems or add functionality between releases. Periodically, the individual patches are packaged into a bundle called a cumulative consolidated patch. HP OpenView recommends that the latest cumulative patches should be installed. Individual patches should be installed when needed.

| Number | Name/Description |
|---|---|
| PHSS_25743 | NNM Cumulative Consolidated Patch, Patch 2 1/7/2002 |
| PHSS_24945 | Emanate SNMP Cumulative Consolidated Agent Patch dated 10/4/2001 |

#### *4.4.2.6.2 Install NNM Consolidated Patch*

Download the PHSS_25743 NNM Cumulative Consolidated Patch (or latest)

**NNM Patch download and installation**

| # | Task |
|---|---|
| 6. | Select the network node manager product |
| 7. | Select Release 6.2 and HP-UX 11.X |
| 8. | Select PHSS_25743 Cumulative Consolidated Patch. This is Patch 2 dated 1/7/2002. Put |

| # | Task |
|---|---|
| | the patch into /tmp |
| 9. | Login as root |
| 10. | Close all ovw sessions and stop all of the NNM processes:<br>`ovstop` |
| 11. | Copy the patch to the /tmp directory and unshar the patch:<br>`cd /tmp`<br>sh PHSS_25743 |
| 12. | 1. Run swinstall to install the patch:<br>`swinstall -x autoreboot=true -x patch_match_target=true -s \ /tmp/PHSS_25743.depot`<br>By default swinstall will archive the original software in /var/adm/sw/save/PHSS_25743. For future reference, the contents of the PHSS_25743.text file is available in the product readme:<br>`swlist -l product -a readme -d @ /tmp/PHSS_25743.depot` |
| 13. | By default swinstall will archive the original software in /var/adm/sw/save/PHSS_25743. For future reference, the contents of the PHSS_25743.text file is available in the product readme:<br>`swlist -l product -a readme -d @ /tmp/PHSS_25743.depot` |
| 14. | Perform the tasks in Appendix E: NNM Cumulative Consolidated Patch Special Instructions to configure each of the patches in the consolidated patch bundle requiring additional installation steps. |

#### *4.4.2.6.3 Install The Emanate SNMP Agent Consolidated Patch*

| # | Task |
|---|---|
| 1. | Download d the latest Emanate PHSS_24945 Cumulative Consolidated Agent Patch from the HP OpenView web site |
| 2. | Select the emanate snmp agent product |
| 3. | select Release 14.2 and HP-UX 11.X |
| 4. | select PHSS_24945 Cumulative Consolidated Agent Patch dated 10/4/2001 |
| 5. | Copy the patch to the /tmp directory |
| 6. | Move to the /tmp directory and unshar the patch:<br>`cd /tmp`<br>`sh PHSS_24945` |
| 7. | 1. Run swinstall to install the patch:<br>`swinstall -x autoreboot=true -x patch_match_target=true -s \ /tmp/PHSS_24945.depot` |
| 8. | By default swinstall will archive the original software in /var/adm/sw/save/PHSS_24945. For future reference, the contents of the PHSS_24945.text file is available in the product readme:<br>swlist -l product -a readme -d @ /tmp/PHSS_24945.depot |

## *4.5 Applications Configuration*

### 4.5.1 Configure NNM

Configuring the NNM application to manage a network is outside of the scope of this paper. The following sections list the minimal configurations required to perform the remaining security tasks involving NNM. For detailed information on NNM resources and references see Welcome To HP OpenView Network Node Manager

#### 4.5.1.1 User Environment

Add to /etc/profile

```
# Set up OpenView environment
if [ -f /opt/OV/bin/ov.envvars.sh ]; then
   . /opt/OV/bin/ov.envvars.sh
   PATH=$PATH:$OV_BIN
   export PATH
   MANPATH=$MANPATH:$OV_MAN
fi
```

### 4.5.2 Configure NNM Server's SNMP Agent

The NNM server system also runs a local SNMP agent. This agent's SNMP community string must be modified to strengthen local SNMP security. SNMP community strings are essentially passwords which get passed between the management system and the SNMP agent on the managed node. On this system, the Get (or read) community string will be modified and the Set community string will be disabled. The procedure follows:

**Emanate SNMP Agent Configuration**

| Operation | Commands |
|---|---|
| Stop the local SNMP agent | `ps -ef \| grep snmpdm`<br>`kill -9 <snmpdm_PID>` |
| Edit the SNMP agent configuration file. Change the Get community name. NOTE: DO NOT use the password listed. Replace it with a strong password. Leave the Set community name commented out, which will disable SNMP sets to this agent. Set the trap destination to the NNM system (the local host) | **vi /etc/snmpd.conf**<br>get-community-name: <A9!s#j5C><br>#set-community:<br>trap-dest: 10.1.2.20 |
| Re-start the SNMP agent. Note that the snmpd script starts the snmpdm daemon. | **/usr/sbin/snmpd** |

### 4.5.3 Secure NNM

#### 4.5.3.1 NNM File And Directory Permissions

The NNM Cumulative Consolidated Patch bundle included patch PHSS_25743 contains a script named ovperms.ovpl. It will change the permissions of existing NNM files and directories "to the values which are considered more appropriate" according to the Special Installation Instructions in PHSS_25743.text, the documentation for the patch. The script is located in $OV_BIN and should be run once after initial NNM installation. See ovperms.ovpl (1m) for

more information. After running the script, verify that the permissions and ownerships have been changed correctly. The procedure follows:

**Update NNM permissions**

| Operation | Commands |
|---|---|
| Switch user to root | `su -` |
| Stop the NNM processes | `ovstop` |
| Run the script with options to save the prior status and the current status | `$OV_BIN/ovperms.ovpl -b /tmp/before -a /tmp/after` |
| Re-start the NNM processes | **ovstart** |

### 4.5.3.2 Securing The NNM Apache Web Server

HP ships the Apache web server with NNM. Apache is installed during the NNM installation process. The Apache server supports NNM web services. Apache security is pre-configured and does not require major changes to be secure.

### 4.5.4 Configure NNM Web Access & Security

**Password file /etc/opt/OV/share/www/etc/htpasswd**

**ovhtpasswd rich**

The NNM web access accounts should follow the same rules for strong passwords as any other authentication mechanism. See the Appendix C. Password Guidelines section for help with choosing strong passwords.

See ovhtpasswd (1M)

Role file
**/etc/opt/OV/share/www/etc/htgroup**
Limit access to roles by removing all "+" from each role. For example:

```
NetworkAdmin: netmgr
NetworkOper:
```

Session configuration file

```
/etc/opt/OV/share/www/conf/session.conf
UserLogin: on
```

**LoginLogging: on**

```
AccessLogging: on
```

**SessionTimeout: 1**

There are two audit log files — one for logging logins and one for logging URL access from the Launcher. See the NNM Web access logs section for the log file locations.

## *4.6 Post-Installation Tasks*

### 4.6.1 Re-locate The System

- Connect the system to the production network
- If the system does not need to be relocated, reboot it to activate all of the system configuration changes.

### 4.6.2 Enable DNS

| Operation | Commands |
|---|---|
| Edit /etc/resolv.conf and add the specified lines | domain domain.company.com<br>nameserver 10.1.1.1<br>nameserver 10.1.1.2 |
| Edit /etc/nsswitch.conf and modify the specified line | Hosts: dns[NOTFOUND=continue UNAVAIL=continue] files |

### 4.6.3 Run The HP-UX Security Patch Checker

HP offers a script which determines which minimal security patches are missing from the system, and will generate a report listing the recommended patches that correspond to the minimal patches missing. The comparison is made against a catalog of the latest security patches which the script downloads from the HP web site. This operation requires Internet access from the NNM server. The script is available as patch B6834AA from the HP software download site: http://software.hp.com
Download the patch into /tmp and install it with the command:
**swinstall –s hpovnnm1:/tmp/B6834AA.depot**

If Internet access is not available, download the security catalog from: ftp://ftp.itrc.hp.com/export/patches/security_catalog and put it into /opt/sec_mgt/spc/security_catalog.

Run the script with the commands:
**cd /opt/sec_mgt/spc/security_catalog**
**/opt/sec_mgmt/spc/bin/security_patch_check –c ./security_catalog**

```
*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by:
/opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root
Analyzed localhost (HP-UX 11.00) from hpovnnm1
Security catalog: ./security_catalog
Security catalog created on: Sat Jan 26 22:48:33 2002
Time of analysis: Sun Jan 27 16:49:39 2002

List of recommended patches for most secure system:

#  Recommended  Bull(s) Spec? Reboot? PDep? Description
-------------------------------------------------------------
```

```
Security patches are up to date with the security patch catalog
used
-------------------------------------------------------------------------
*** END OF REPORT ***
```

For more information see security_patch_check (1M) and /opt/sec_mgmt/spc/README.

### 4.6.4 Disable FTP

The final post-installation task should be to disable FTP after all required software has been transferred to the NNM server. Do this by commenting out the FTP entry in /etc/inetd.conf.

### 4.6.5 Physical Security

Normally, application servers are locked up tight in a secure room such as a data center or machine room. The NNM server, as configured in this paper with a large graphics console, will be accessed physically on a regular basis. In this case, the system unit and all peripherals should be in a locked cabinet adjacent to the monitor. Be sure that the cabinet has adequate ventilation to prevent the system from overheating and crashing. Power should be provided by a UPS.

If possible, locate the system in a secure room such as a network operations center (NOC).

## 5 Ongoing Maintenance

### *5.1 Backups*

The daily NNM backup (ovbackup.ovpl) will provide a current, stable copy of the NNM operational databases. But if a disk fails or the system is destroyed in a disaster like a fire, the data will be lost. The data must be copied and securely stored. All data should be backed up to a separate system or to durable media. The backup storage system should be located at a secure site some geographical distance away. The same applies to media (e.g., tape or writable CD), it should be stored securely off-site.

A comprehensive backup scheme includes both periodic and as-needed backups, both full and incremental

The NNM operational databases use a proprietary format. The mechanism uses hashing which results in sparse files. That is, the data is not stored sequentially, but has gaps between. Records when standard UNIX utilities are used to manipulate these files, the gaps are filled with nulls or zeros. This results in files which are much larger than the amount of data they contain. Sparse file-aware utilities must be used when saving and restoring the databases. HP's fbackup HP OmniBack Plus support sparse files.

A key component of backup security is testing of the backups. This step is time-consuming, but is the only way to verify that backups are valid.

### *5.2 Updates/Patches*

Periodically check for updates to all applications installed. Consider subscribing to automatic announcement services where available. HP offers bulletin digests, custom patch notification and other services. Visit the HP IT Resource Center site at: http://us-support.external.hp.com

HP OpenView also offers an automatic patch release notification service for OpenView patches:

- To subscribe, send a message to "ovpatches@listserv.cnd.hp.com" with the word "subscribe openview_patches_released" in the body.
- To unsubscribe, send a message to "ovpatches@listserv.cnd.hp.com" with the word "unsubscribe openview_patches_released" in the body.

Run the security patch checker script. See the section Run Security patch checker. An entry to run this script should be put into cron to run every day. The output should be emailed to the system administrator

***Whenever new patches have been installed, review all running services since patches could restart them.***

Whenever patches are installed, an updated backup should be made:
System patches  bootable recovery tape (make_tape_recovery)
Periodically (e.g., quarterly) an incremental system backup should be made.

### *5.3 Periodic Scans*

Re-run the scans and system checks specified in the verification section above monthly or at least quarterly.

### *5.4 Logging Or Log Monitoring/Review*

#### 5.4.1 Syslog

Since many system processes log to syslog, unusual events or behavior can often be correlated by the time they are logged in syslog

| Purpose | File Name |
|---|---|
| **System log** | /var/adm/syslog/syslog.log |

#### 5.4.2 Apache Log Files

Apache log files can be very useful in detecting vulnerability scans. See

**Apache Log Files**

| Purpose | File Name |
|---|---|
| **Error log** | /var/opt/OV/log/httpd_error_log |
| **Request log** | /var/opt/OV/log/httpd_access_log |

#### 5.4.3 NNM Web Access Log Files

Each line of the file contains one entry including the following information:

- Host

- User name
- Date
- Session number
- Access permitted; either Allowed or DENIED
- URL accessed (for the access_log file only)

| Purpose | File Name |
|---|---|
| **login log** | `/var/opt/OV/www/logs/launch/login_log` |
| **access log** | `/var/opt/OV/www/logs/launcher/access_log` |

### *5.5 Manage Log Files*

#### 5.5.1 Apache

The files grow without bounds. They must be periodically trimmed or removed. See the Apache Log Files section for log file locations.

#### 5.5.2 NNM Web

The files grow without bounds. They must be periodically trimmed or removed. See the NNM Web access logs section for log file locations.

### *5.6 Update Passwords*

Trusted computing policies will force users to update passwords. The NNM web access passwords are not controlled by this mechanism. The administrator must enforce this separately.

### *5.7 Wish List*

Part of on-going maintenance is to evaluate existing processes and improve and replace them when necessary. As budgets and needs dictate, additional products can be purchased which will improve the security of the NNM server.

#### 5.7.1 SNMP v3

SNMP Security Pack 15.3. The SNMP Security Pack provides an extension to HP Open View Network Node Manager (NNM), allowing NNM (4.1 and later) to use SNMPv3 with security. SNMPv3 provides safe configuration and control operations. Its administration offers logical contexts, view-based access control, and remote configuration. The user-based authentication mechanism is based on MD5, SHA, and a loosely synchronized monotonically increasing time indicator. (SNMP Security Pack)

#### 5.7.2 UPS-triggered Shutdown

A UPS only runs as long as the battery lasts. Even a UPS connected to a generator will fail if the generator runs out of gas before power is restored. At some point in time, the servers will crash. When available, the UPS should signal the NNM server that the power is running out so that the system can shut itself down correctly.

### 5.7.3 Notification

UNIX scripts and programs are often programmed to send email to administrators to alert them to problems. NNM is often integrated with some type of notification services. This can be email or pagers or signboards. There are many homegrown and commercial products which offer varied levels of functionality and support. HP OpenView recommends the Telamon TelAlert product (see the NNM release notes for the Recommended Paging Software).

## 6 Check Your Configuration

### *6.1 Internet services*

Run a port scanner from another system
nmap –O 10.1.2.20

Output should resemble the following

| Port | State | Service |
|---|---|---|
| 22/tcp | open | ssh |
| 111/tcp | open | sunrpc |
| 162 | open | snmptrap |
| 1508 | open | diagmond |
| 6000 | open | X11 |
| 6112 | open | dtspc |

Verify that none of the services in the /etc/inetd.conf table are running.

### *6.2 NNM SNMP Agent*

Verify that SNMP data can't be read from the NNM server's SNMP agent using the default get community string.

```
/opt/OV/bin/snmpwalk -c public hpovnnm1 system
```

Verify that SNMP data can't be written to the NNM server's SNMP agent using the default set community string.

```
/opt/OV/bin/snmpset -c private hpovnnm1
```

### *6.3 NNM Web Access*

Normally, each of the NNM web screens is accessed through the OpenView launcher. When web security is enabled, Verify that the NNM web access security is working. From a web browser, select each of the URL's in the table below. Check that a login screen is presented for each. Enter a valid login to check that the login works as well.

| Window | URL | Login Screen Y/N |
|---|---|---|
| OV Launcher | http://hpovnnm1:8880/OvCgi/ovlaunch.exe | |
| Network Presenter | http://hpovnnm1:8880/OvCgi/ovlaunch.exe | |
| Alarm Browser | http://hpovnnm1:8880/OvCgi/.exe | |
| Grapher | http://hpovnnm1:8880/OvCgi/jovgraph.exe | |

| Window | URL | Login Screen Y/N |
|---|---|---|
| MIB Browser | http://hpovnnm1:8880/OvCgi/snmpviewer.exe | |
| Report Configurator | http://hpovnnm1:8880/OvCgi/nnmRptConfig.exe | |
| Report Presenter | http://hpovnnm1:8880/OvCgi/nnmRptPresenter.exe | |
| ECS Configurator | http://hpovnnm1:8880/OvCgi/ecsmg.ovpl | |

### *6.4 Test the backups*

The primary reason backups are often not fully tested is the cost in time and equipment. A thorough backup test would require clean disks to simulate restoring onto new disks after a disk failure. This would require that the production system be taken out of service for the test and new disks swapped in (and then the old disks swapped back). Or a second, similarly configured server would be needed.
Whichever method time and money allows, the following three sections described the primary backup tests recommended.

#### 6.4.1 Re-install HP-UX from the Ignite recovery tape

| # | Task |
|---|---|
| 1. | Reboot the system. |
| 2. | Interrupt the boot process. Be ready; you only have 10 seconds! |
| 3. | Load the recovery tape into the tape drive. |
| 4. | Load the recovery tape into the tape drive. |
| 5. | Perform a search (SEA) at the boot prompt. |
| 6. | Select the tape device. |
| 7. | Boot from the tape. |

#### 6.4.2 Reinstall The Applications From The Latest Application Backup

Depending on the backup scheme used, the instructions will vary. Assuming a tape backup, mount the tape and restore the applications. Once the restore completes, verify the operation of the application.

#### 6.4.3 Reinstall the latest NNM databases using ovrestore.ovpl

When ovbackup (1M) was executed, the operational and analytical data was copied to the default directory. Ovrestore.ovpl (1M) will restore the data from the same directory, unless directed to look elsewhere. Verify that the backup data was loaded into the correct directory. Keep in mind that the operational databases are sparse files, so use frecover (1M) with the –s option to maintain the sparse files.

Unlike ovbackup.ovpl, ovrestore.ovpl does not pause the NNM operational databases. When doing a restore, all NNM processes must be stopped using the following command:
**sudo ovstop**

### *6.5 Nessus Scan*

Nessus is a publicly available security scanner. It scans for a wide range of vulnerabilities. A scan of the NNM system after all configurations were completed resulted in the following:

2 security holes
7 security warnings

| Level | Description |
|---|---|
| Holes: 2 | 1. snmp (161/udp): SNMP agent responded as expected with community name: <NAME DELETED> CVE: CAN-1999-0517<br>**Analysis:** nessus did not get access with the conventional public & private community names. It did discover a bug or possible backdoor in the HP Emanate agent. 2 lines of data are returned from an snmpwalk of the entire MIB tree using the name nessus used.<br>2. unknown (49152/tcp) The cmsd RPC service is running. This services has a long history of security holes, so you should really know what you are doing if you decide to let it run.<br>* NO SECURITY HOLE REGARDING THIS PROGRAM HAS BEEN TESTED, SO THIS MIGHT BE A FALSE POSITIVE * CVE-1999-0320<br>Risk Factor: High<br>**Analysis:** rpc.cmsd is part of CDE and it is the standard GUI environment for HP graphics consoles. A possible work-around would be to eliminate the graphics console and run X from a remote X-Term. This would also allow the system to be located in a more secure room. |
| Warnings: 7 | 1. X11 (6000/tcp) This X server does *not* accept clients to connect to it however it is recommended that you filter incoming connection to this port as cracker may send garbage data and slow down your X session or even kill the server. CVE-1999-0526<br>Risk Factor: Low<br>**Analysis:** As in hole number 2 above, X is required for the operation of the NMS.<br>2. unknown (8880/tcp) a web server is running on this port<br>**Analysis:** The NNM Apache web server runs on port 8880<br>3. general/tcp Microsoft Windows 5 and 98 clients have the ability to bind multiple TCP/IP stack on the same MAC address…<br>The remote host has several TCP/I stacks with the same IP binded on the same MAC address. As a result, it will reply several times to the same packets, such as by sending multiple ACK to a single SYN, creating noise on your network.<br>Risk Factor: Medium<br>**Analysis:** Since the system is HP-UX and not Microsoft Windows, it is unknown whether this warning is valid.<br>4. unknown (49152/tcp) The tooltalk RPC service is running. An possible implementation fault in the ToolTalk object database server may allow a cracker to execute arbitrary commands as root.<br>** This warning may be a false positive since the presence of the bug was not tested. CVE—1999-003<br>Risk Factor: High<br>**Analysis:** lsof did reveal the process using that port.<br>5. general/icmp The remote host answered to an ICMP_MASKREQ query and us its netmask |

| Level | Description |
|---|---|
| | An attacker can use this information to understand how your network is set up and how the routing is done. This may help him to bypass your filters.<br>Solution: reconfigure the remote host so that it does not answer to those requests. Set up filters that deny ICMP packets of type 17.<br>CAN—1999-0524<br>Risk Factor: Low<br>**Analysis:** The solution should be implemented. |

## 7 Appendix A: References


**7.1.1.1 Coble, Art, Network Management Server Security Assessment For GIAC Enterprises, GCUX Practical Assignment Version 1.6d July 26, 2001**

**7.1.1.2 Installing HP-UX 11.0 and Updating HP-UX 10.x to 11.0, HP 9000 Computers, Edition 2, HP Part Number: B2355-90679 E0300,March 2000 Hewlett-Packard Company**

**7.1.1.3 Release Notes for HP-UX 11.0, HP 9000 Computers Edition 3, HP Part Number: B3782-90716 E1298, December 1998 Hewlett-Packard Company**

**7.1.1.4 Managing Systems and Workgroups: A Guide for HP-UX System Administrators HP 9000 Computers Edition 5; HP Part Number: B2355-90742,**

**7.1.1.5 Garfinkel, Simpson and Spafford, Gene; Practical UNIX and Internet Security; Second Edition, April, 1996; Sebastopol: O'Reilly and Co.;**

**7.1.1.6 Google. http://www.google.com**

**7.1.1.7 HP OpenView Patches. http://support.openview.hp.com/cpe/patches/**

**7.1.1.8 HP-UX 11.x Manuals. http://docs.hp.com/hpux/os/11.0/index.html.**

**7.1.1.9 HP-UX Security Bulletins. http://itrc.hp.com.**

**7.1.1.10HP Software download site: http://software.hp.com**

**7.1.1.11 HP support site: http://us-support.external.hp.com/**

**7.1.1.12 HP-UX patches: http//unix.hp.com/operating**

**7.1.1.13 nessus. http://www.nessus.org.**

**7.1.1.14 PHSS_25743 NNM Cumulative Consolidated Patch, Patch 2. 1/7/2002. http://support.openview.hp.com/cpe/patches/**

**7.1.1.15 PHSS_24945 Cumulative Consolidated Agent Patch. 10/4/2001. http://support.openview.hp.com/cpe/patches/**

**7.1.1.16Pomeranz, Hal. "Unix Security Tools." . 6.2 UNIX Security Tools & Their Uses. SANS Institute, 2001**

**7.1.1.17 Quick Start Installation Guide for HP OpenView Network Node Manager and HP OpenView Customer Views for NNM HP-UX, HP Part Number: J1240-90063, March 2001 Hewlett Packard Company**

**7.1.1.18 Schmidt, Della, Securing UNIX GCUX Practical Assignment Version 1.6b, HP-UX 11.0 Installation Checklist**

**7.1.1.19 SNMP Security Pack. 10/4/2001. http://ovweb3.external.hp.com/solcat/products/display.cfm?id=665**

**7.1.1.20 Steves, Kevin. " Building a Bastion Host Using HP-UX 11." http://people.hp.se/stevesk/bastion.html (26 May 2001).**

**7.1.1.21 "Solaris Security Step by Step Version 2", The SANS Institute. http://www.sans.org**

**7.1.1.22 Thomas, Rob. UNIX IP Stack Tuning Guide v2.7. 03 DEC 2000 . http://www.nsforce.org/docs/UNIX%20IP%20Stack%20Tuning%20Guide%20v2.7.htm**

**7.1.1.23 Managing Your Network with HP OpenView Network Node Manager Windows NT®, Windows® 2000, HP-UX, and Solaris, HP Part Number: J1240-90058, March 2001. Available from http://ovweb.external.hp.com/lpe/doc_serv/**

**7.1.1.24 SSH http://hpux.connect.org.uk/hppd/hpux/Networking/Admin/**

**7.1.1.25 TeraTerm telnet emulator. http://hp.vector.co.jp/authors/VA002416/teraterm.html.**

**7.1.1.26 TeraTerm SSH extension for TeraTerm. http://www.zip.com.au/~roca/ttssh.html**

**7.1.1.27Welcome To HP OpenView Network Node Manager, Windows NT®, Windows® 2000, HP-UX, and Solaris. Hewlett-Packard Company. Part Number: J1240-90052. March 2001**

**7.1.1.28.**

## 8 Appendix B: Filesystem layout using 2 disks

From the File System tab, select the Add/Remove Disks item and add the additional disk. Create a new volume group called vg_OV. Modify the filesystem layout as described in the table below.

File System Layout

| Mount Point | Usage | Size | Group |
|---|---|---|---|
| / | VxFS | 300 | vg00 |
| /stand | HFS | 84 | vg00 |
| Primary Swap | swap | 1024 | vg00 |
| /home | VxFS | 500 | vg00 |
| /opt | VxFS | 1000 | vg00 |
| /tmp | VxFS | 300 | vg00 |
| /usr | VxFS | 1500 | vg00 |
| /var | VxFS | 1000 | vg00 |
| /var/opt/OV | VxFS | 2000 | vg_OV |
| /etc/opt/OV | VxFS | 1000 | vg_OV |
| opt/OV | VxFS | 2000 | vg_OV |

## 9 Appendix C.Password Guidelines

Passwords are the weakest link of security. Note that there are many resources available for suggestions on passwords (just do a Google search on "password guidelines"). Here is a subset of some suggestions from Practical UNIX Security, by Simson Garfinkel and Gene Spafford ( Garfinkel and Spafford, section 3.6.1):

To be secure, a password should not be any of the following:

- Anybody's name.
- The name of the operating system you're using.
- Information in the GECOS field of your passwd file entry.
- The hostname of your computer.
- Your phone number or your license plate number.
- Any part of your social security number.
- Anybody's birth date.
- Other information easily obtained about you (*e.g.,* address, alma mater).
- Words such as wizard, guru, gandalf, and so on.
- Any username on the computer in any form (as is, capitalized, doubled, etc.).
- A word in the English dictionary or in a foreign dictionary.
- Place names or any proper nouns.
- Passwords of all the same letter.
- Simple patterns of letters on the keyboard, like qwerty.
- Any of the above spelled backwards.
- Any of the above followed or pre-pended by a single digit

Good Passwords are passwords that are difficult to guess. In general, good passwords

- Have both uppercase and lowercase letters.
- Have digits and /or punctuation characters as well as letters.
- Are easy to remember, so they do not have to be written down.
- Are seven or eight characters long.
- Can be type quickly, so somebody cannot follow what you type by looking over your shoulder.

## 10 Appendix D: NNM Cumulative Consolidated Patch Special Instructions

NOTE : ovstart is NOT executed after the patch is loaded. You will need to manually run ovstart.

**PHSS_25743**: If the previous consolidated patch for NNM6.2 has not been installed on the system and the script ovperms.ovpl has not been run then do the following:
A script is provided that can be used to change the permissions of existing files and directories to the values which are considered more appropriate. To ensure that these permission changes are implemented, the administrator must run this script once the patch is installed. Please read the manpage on $OV_BIN/ovperms.ovpl for more details.

**PHSS_25731**: On Unix, copy the ovHomePage registration file to the appropriate directory:
cp $OV_NEW_CONF/OVNNM-RUN/registration/C/ovHomePage \
$OV_REGISTRATION/C
cp $OV_NEW_CONF/OVNNMGR-JPN/registration/$LANG/ovHomePage \
$OV_REGISTRATION/$LANG

**PHSS_25698**: Run the following command after patch installation to get the updated on-line help.
cp $OV_NEW_CONF/OVNNM-RUN/nnm.sdl $OV_HELP/C/NNM/nnm.sdl

**PHSS_25694**: Two ovw registration files need to be copied from the $OV_NEW_CONF directory to the $OV_REGISTRATION directory. Please follow the instructions below.
- Stop all ovw sessions.
- For English platforms do:
copy $OV_NEW_CONF/OVNNM-RUN/registration/C/nnmLinkMgmt to
$OV_REGISTRATION/C/
copy $OV_NEW_CONF/OVNNM-RUN/registration/C/ovip/NNM-IP.gph
to $OV_REGISTRATION/C/ovip/

**PHSS_25680**: Because the file
$OV_CONF/ovbackup/checkpoint/operational/nnm_checkpoint.ovpl is customizable by an administrator, the patch installation will not copy this file directly to the $OV_CONF/ovbackup/checkpoint/operational directory. The new file will be placed in the $OV_NEW_CONF/OVMIN/conf/ovbackup/checkpoint/operational directory. If any customizations have been made to this file then the changes will need to be merged and the resulting file placed in $OV_CONF/ovbackup/checkpoint/operational. If no changes have been made to the original file, simply copy:

$OV_NEW_CONF/OVMIN/conf/ovbackup/checkpoint/operational/nnm_checkpoint.ovpl
to:
$OV_CONF/ovbackup/checkpoint/operational/nnm_checkpoint.ovpl

**PHSS_25650**: Multiple Java archive (JAR) files are updated in this patch. Web browsers that employ caching, either internally or through a proxy server, must have their caches cleared in order to access the new functionality provided by this patch. Procedures for clearing caches vary according to the browser you use, so please follow procedures appropriate for your browser.

**PHSS_25516**: To turn on this feature:
1. For Ovw:
- Stop Ovw
- Edit $OV_REGISTRATION/C/CDP
Append "managedNodes=1" to the following entries for actions "CDPViewOneSel" and "CDPView" respectively. <Command "ovweb \"http:/OvCgi/cdpView.ovpl?cdpnode=${OVwSelection1}\"";> and <Command "ovweb \"http:/OvCgi/cdpView.ovpl\"";>
e.g. <Command "ovweb \"http:/OvCgi/cdpView.ovpl?cdpnode=${OVwSelection1}&managedNodes=1\"";> and <Command "ovweb \"http:/OvCgi/cdpView.ovpl?managedNodes=1\"";>
- Restart Ovw
2. For Network Presenter:
- Edit $OV_WWW_REG/jovw/C/CDP
Append "managedNodes=1" to the following entries for actions "CDPviewSel0" and "CDPviewSel11" respectively.
<URL "/OvCgi/cdpView.ovpl";> and <URL "/OvCgi/cdpView.ovpl?cdpnode=$OVwSelection1";>
e.g. <URL "/OvCgi/cdpView.ovpl?managedNodes=1";>
and <URL "/OvCgi/cdpView.ovpl?cdpnode=${OVwSelection1}&managedNodes=1";>
3. For OV Launcher:
- Edit $OV_WWW_REG/launcher/C/CDP
Append "managedNodes=1" to the following entry for action "NNMCDPview".
<URL "/OvCgi/cdpView.ovpl";>
e.g. <URL "/OvCgi/cdpView.ovpl?managedNodes=1";>

**PHSS_24156**: To complete installation of this patch on HP-UX and Solaris systems, manually copy the nodeView and CDPView registration files to the NNM and Network Presenter registration file directories. This is not required on NT or Windows 2000 systems. This should be done after backing up the OpenView directories and installing this patch. As root, execute the following commands:
- cp $OV_NEW_CONF/OVNNM-RUN/registration/C/nodeview $OV_REGISTRATION/C/nodeview
- cp $OV_NEW_CONF/OVNNM-RUN/registration/C/CDP $OV_REGISTRATION/C/CDP
- cp $OV_NEW_CONF/OVWWW-FW/www/registration/jovw/C/nodeview $OV_WWW_REG/jovw/C/nodeview

## 11 Appendix E: SSHD initialization script

### *11.1 Create start/stop links*

```
ln –s /sbin/init.d/sshd /sbin/rc2.d/S130sshd
ln –s /sbin/init.d/sshd /sbin/rc2.d/K130sshd
```

### *11.2SSH control file: /etc/rc.config.d/sshd*

```
#!/sbin/sh
#
# Openssh2 startup configuration (sshd)
#
#
START_SSHD=1
```

### *11.3 SSH start/stop script: /sbin/init.d/sshd*

```
#!/sbin/sh
#
# @(#) $Revision: 82.1 $
#
# NOTE:    This script is not configurable!  Any changes made to this
#          script will be overwritten when you upgrade to the next
#          release of HP-UX.
#
# WARNING: Changing this script in any way may lead to a system that
#          is unbootable.  Do not modify this script.

#
# sshd - start the ssh server
#

# Allowed exit values:
#0 = success; causes "OK" to show up in checklist.
#1 = failure; causes "FAIL" to show up in checklist.
#2 = skip; causes "N/A" to show up in the checklist.
#           Use this value if execution of this script is overridden
#    by the use of a control variable, or if this script is not
#    appropriate to execute for some other reason.
#       3 = reboot; causes the system to be rebooted after execution.
#4 = background; causes "BG" to show up in the checklist.
#           Use this value if this script starts a process in background
mode.

# Input and output:
#stdin is redirected from /dev/null
#
#stdout and stderr are redirected to the /etc/rc.log file
#during checklist mode, or to the console in raw mode.

PATH=/usr/sbin:/usr/bin:/sbin
export PATH

rval=0
```

```
# Check the exit value of a command run by this script.  If non-zero, the
# exit code is echoed to the log file and the return value of this script
# is set to indicate failure.

set_return() {
   x=$?
   if [ $x -ne 0 ]; then
      echo "EXIT CODE: $x"
      rval=1# script FAILed
   fi
}

# Kill the named process(es).
# $1=<search pattern for your process>

killproc() {
pid=`ps -el | awk '( ($NF ~ /'"$1"'/) && ($4 != mypid) && ($5 != mypid)  ){
   print $4 }' mypid=$$ `
   if [ "X$pid" != "X" ]; then
      if kill "$pid"; then
         echo "$1 stopped"
      else
         rval=1
         echo "Unable to stop $1"
      fi
   fi
}


case $1 in
   'start_msg')
   # Emit a _short_ message relating to running this script with
   # the "start" argument; this message appears as part of the checklist.
   echo "Starting the ssh subsystem"
   ;;

'stop_msg')
   # Emit a _short_ message relating to running this script with
   # the "stop" argument; this message appears as part of the checklist.
   echo "Stopping the ssh subsystem"
   ;;

'start')

   # source the system configuration variables
   if [ -f /etc/rc.config ] ; then
      . /etc/rc.config
   else
      echo "ERROR: /etc/rc.config.d defaults file MISSING"
   fi

   # Check to see if this script is allowed to run...
   if [ "$START_SSHD" != 1 ]; then
      rval=2
   else
      /opt/openssh2/sbin/sshd
   fi
```

```
   ;;

'stop')
   # source the system configuration variables
   if [ -f /etc/rc.config ] ; then
      . /etc/rc.config
   else
      echo "ERROR: /etc/rc.config defaults file MISSING"
   fi

   # Check to see if this script is allowed to run...
   if [ "$START_SSHD" != 1 ]; then
      rval=2
   else
      # kill sshd
      killproc sshd
   fi
   ;;

*)
   echo "usage: $0 {start|stop|start_msg|stop_msg}"
   rval=1
   ;;
esac

exit $rval
```

## 12 Appendix F: Sample Apache Attack Log Entry

Here is a typical entry from a nessus scan.:

10.1.3.50 - - [10 Jan/2002:17:33 –0500] GET /cgi-bin/nessus_is_probing_this_host_87002947 HTTP/1.1" 404 251