Global Information Assurance Certification Paper

Network Management Server Security Assessment

For

GIAC Enterprises

Art Coble
GCUX Practical Assignment
Version 1.6d
July 26, 2001

Executive Summary

GIAC Enterprises has engaged Coble Consulting Inc. to perform a security assessment on its Network Management System (NMS) server. The NMS server is used to monitor their co-located e-Business Web servers and network devices.

GIAC is concerned about the security risks imposed by the connectivity of their corporate network to the co-located servers at the Co-Lo-Company data center. This NMS server assessment is seen by GIAC as a first step towards ensuring the security between their corporate network and their co-located environment.

Information for the NMS server security assessment was gathered by:

- Collecting and reviewing all available documentation relevant to the NMS server and the co-located environment.
- Interviewing with key personnel that have an influence of the security posture of the NMS server.
- Server vulnerability testing using security vulnerability tools.
- A manual audit of server.

Twenty six vulnerabilities were found concerning the NMS server and its network environment; 18 high severity, 5 medium and 3 low severity vulnerabilities.
Coble Consulting recommends that the following next steps to secure the NMS server and its environment:

1. Develop comprehensive corporate wide security policies.
2. Harden the NMS server against security vulnerabilities.
   - Install current OS and application patches
   - Configuration changes
     - Disable open ports
     - Strengthen file permissions
     - Set secure network parameters
     - Change insecure SNMP community strings
     - Add access banners
     - Secure RPC services
     - Improve X authentication
     - Improve HPOV security
3. Improve password security.
4. Improve log monitoring .
5. Install a file integrity checker.
6. Install SSH to replace telnet and ftp.
7. Develop administrative policies and procedures.
8. Develop a change control policy.
9. Implement a firewall and network based intrusion detection at the perimeter of the GIAC network and the co-location site.

TABLE OF CONTENTS

Paragraph & Description **Page**

Title Page i
Executive Summary ii
Table of Contents iii

1.0 Introduction 1

2.0 Assessment Scope 2

3.0 Assessment Methodology 2

4.0 Assessment Tools 3

5.0 Network Management Server Security Assessment Findings 3
5.1 Security Policies and Procedures 3
5.1.1 Finding: GIAC Enterprises has no security policies and procedures 4
5.2 System Configuration Vulnerabilities 4
5.2.1 Finding: Many non required services running on server 4
5.2.2 Finding: Open FTP server 4
5.2.3 Finding: Open Telnet Server 4
5.2.4 Finding: RPC not secured 5
5.2.5 Finding: SNMP Read Community String set to default of public 5
5.2.6 Finding: No /etc/ftpusers file 5
5.2.7 Finding: FTP banner displays system information. 5
5.2.8 Finding: Telnet banner displays system information. 5
5.2.9 Finding: X users not using any authentication 5
5.3 Software Revisions and Patches 5
5.3.1 Finding: Recommended Patches not installed on the NMS server 6
5.4 File Permission Vulnerabilities 6
5.4.1 Finding: Multiple files have file permissions of SUID root and eighty-eight files have file permissions of SGID root. 6
5.4.2 Finding: RC directories and files have insecure permissions. 6
5.4.3 Finding: Multiple directories and files have world writable file permissions 6
5.4.4 Finding: Incorrect directory group write privileges 6
5.4.5 Finding: Multiple directories and files should have root as the owner 6
5.5 Password and User Account Security 7
5.5.1 Finding: Weak passwords 7

5.5.2 Finding: No password policy – user guidelines and education 7
5.5.3 Finding: No password expiration and aging 7
5.5.4 Finding: Many disabled login IDs have valid shells 7
5.5.5 Finding: Multiple users using the same user account..... 7
5.6 Logging 8
5.6.1 Finding: Logging set to default..... 8
5.6.2 Finding: No manual or automated log monitoring 8
5.7 Operating System Vulnerabilities..... 8
5.7.1 Finding: No stack protection to prevent buffer overflows..... 8
5.7.2 Finding: Default network parameters running on server 8
5.7.3 Finding: Umask for system daemons not set to 022..... 8
5.8 Application Security 8
5.8.1 Finding: Read / Write SNMP community strings in HPOV settings set to default of public / private. 9
5.9 Operational Procedures 9
5.9.1 Finding: System back up mechanisms are incomplete..... 9
5.9.2 Finding: No disaster recovery plan and procedures. 9
5.9.3 Finding: No change control policy for servers and network devices. 9
5.9.4 Finding: No formal administration procedures or responsible personnel have been defined for the NMS server. 9
5.9.5 Finding: No file integrity checking. 10
5.10 Physical Security 10
5.10.1 Finding: Network Maps and Information displays are visible through the Data Center windows. 10
5.11 Network Security..... 10
5.11.1 Finding: There is no network access control between the co-located environment and the GIAC data center. 10
5.11.2 Finding: There is no network based intrusion detection monitoring traffic originating from the co-located environment. 11

6.0 Security Vulnerabilities..... 12

7.0 Recommendations 13
7.1 Vulnerability – GIAC Enterprises has no formal security policies and procedures 13
7.2 Vulnerability: Server software not up latest patch level 13
7.3 Vulnerability: Many non required open ports running on server..... 14
7.4 Vulnerability: Poor Password Administration..... 14
7.4.1 Recommendation:..... 14
7.4.2 Recommendation:..... 15
7.4.3 Recommendation:..... 15
7.5 Vulnerability: Open Telnet and FTP server on the NMS server 15
7.6 Vulnerability: Insufficient Logging and Log Monitoring..... 16
7.6.1 Recommendation:..... 16
7.6.2 Recommendation:..... 16
7.6.3 Recommendation:..... 16

7.7 Vulnerability: No file integrity checking 16
7.8 Vulnerability: No formal procedures or responsible personnel defined for system administration 16
7.9 Vulnerability: No stack Protection to prevent buffer overflows 17
7.10 Vulnerability: Default network parameters set on server 17
7.11 Vulnerability: Server backup mechanism is incomplete 18
7.12 Vulnerability: No disaster recovery plans and procedures 18
7.13 Vulnerability: No change control policy for servers and network devices 18
7.14 Vulnerability: No network access control and intrusion detection between co-location network and GIAC corporate network 19
7.15 Vulnerability: Multiple files have SUID and SGID permissions 20
7.16 Vulnerability: Insecure directory and file permissions 20
7.16.1 Recommendation: 20
7.16.2 Recommendation: 20
7.16.3 Recommendation: 20
7.16.4 Recommendation: 20
7.17 Vulnerability: RPC not secured 21
7.18 Vulnerability: SNMP community string set to default 21
7.19 Vulnerability: Umask for system daemons not set to 022 21
7.20 Vulnerability: Default SNMP community strings set in HPOV 21
7.21 Vulnerability: Multiple users using the same account 21
7.22 Vulnerabiliy: Disabled logins have valid shells 22
7.23 Vulnerability: Login banners not set to warn against unauthorized access 22
7.23.1 Recommendation 22
7.23.2 Recommendation 22
7.23.3 Recommendation 22
7.24 Vulnerability: No /etc/ftpusers file 22
7.25 Vulnerability: X users not using any authentication 23
7.26 Vulnerability: NMS Monitors visible to non authorized personnel 23

8.0 Estimated Tasks and Timeframes to Fix Vulnerabilities 24
8.1 Develop GIAC Corporate Security Policies 24
8.2 Server Hardening 24
8.3 Server Policies and Procedures 24
8.4 Perimeter Firewall and IDS 25
8.5 Total Project Cost 25

Figure	Description	Page
Figure 1	GIAC Enterprises Co-location Connectivity	1
Figure 2	Recommended Firewall and IDS for Co-location Connectivity	19

Table	Description	Page
Table 1	Open Ports and Services for NMS Server	4
Table 2	Summary of Security Vulnerabilities	12
Table 3	Unnecessary Open Ports and Services	14
Table 4	Recommended Traffic Flows Originating From GIAC Data Ctr.	20
Table 5	Recommended Traffic Flows Originating From Co-Location	20

Appendix	Description	Page
Appendix A	SUID and SGID Files Found	26
Appendix B	Files With World Writable Permissions	29
Appendix C	Directories With Incorrect Group Write Privileges	31
Appendix D	Incorrect File Ownership	32
References		33

1.0 Introduction

GIAC Enterprises (GIAC) has engaged Coble Consulting Inc. to perform a security assessment on its Network Management System (NMS) server. The NMS server is used to monitor their co-located e-Business Web servers and network devices. Currently, GIAC has three Web servers, a DNS server, a router and a switch on a dedicated subnet that is co-located at a Co-Lo-Company Inc. data center in Los Angeles. GIAC accesses the co-located e-Business infrastructure via a dedicated T1 frame relay connection from its Colorado corporate office that terminates at the Co-Lo-Company Inc. data center.

The GIAC NMS server is a SUN Ultra-5 running Solaris 2.7. GIAC is running Hewlett Packard's Open View Network Node Manager version 6.2 (HPOV) application to monitor their co-located Web servers and network equipment. HPOV monitors the co-located equipment using the SNMP and ICMP protocols.

GIAC Web customers access the co-located Web servers via the Internet or via a T1 frame relay connection terminating at the Co-Lo-Company data center. The GIAC Web servers are connected to the Internet and secured via a Co-Lo-Company Inc. maintained firewall.

GIAC is concerned about the security risks imposed by the connectivity of their corporate network to the co-located servers at the Co-Lo-Company data center. This NMS server assessment is seen by GIAC as a first step towards ensuring the security of the connectivity between their corporate network and their co-located environment. GIAC's connectivity to its Co-location environment is detailed in Figure 1.

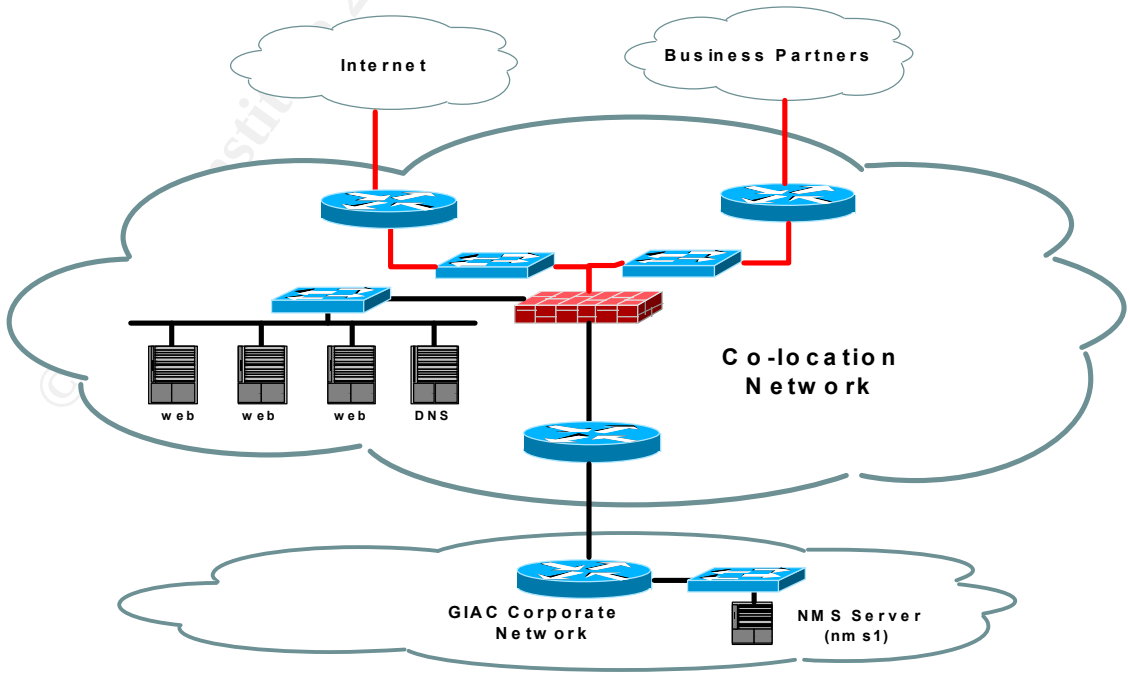

Figure 1 – GIAC Enterprises Co-location Connectivity

2.0 Assessment Scope

The scope of this project is to assess the security posture of the GIAC enterprises network management server. The NMS server security assessment covers, but is not limited to, the following areas:

- GIAC Enterprises security policies and procedures
- NMS server's system configuration vulnerabilities
  - NMS server's software revisions and patches
  - NMS server's file permissions
  - Password and user account security
  - System logging
- Operating system Vulnerabilities
- Application security
- Operational procedures
  - Administrative and operational policies and procedures
  - Server backup and disaster recovery policies and procedures
- Physical security
- Network security

Although the scope of this assessment is limited to the security posture of the GIAC NMS server, it is highly recommended that GIAC have a comprehensive security assessment conducted against all components (policies, procedures, servers, network devices, digital assets, etc.) of its corporate and co-located networks.

3.0 Assessment Methodology

The NMS server assessment was conducted using the following methodology:

- Data Collection - This activity involved collecting all relevant documentation for the NMS server and the co-located Web environment that is being monitored. This included project contacts, network diagrams, existing security policies and procedures, existing system administrative and operational policies and procedures, facility locations, business partner documentation etc.

- Documentation Review – This activity consisted of reviewing existing security policies, system administrative and operational procedures, network topology and other documentation collected.

- Interviews - Key individuals were identified, each representing departments that have direct influence on the NMS server's security posture. Interviews were conducted with personnel from various levels of management and operational staff representing the GIAC Enterprises IT, network and security departments.

- Server vulnerability testing was conducted using a variety of security tools (see Section 4) and a manual security analysis was performed on the NMS server. The server was tested for vulnerabilities using remote testing tools, such as port scanners, UNIX security auditing tools and password guessing programs.

- Physical Review – The facility that houses the NMS server was reviewed by performing an on-site inspection, designed to look for physical vulnerabilities and threats that may affect the security and operational stability of the NMS server.

- Assessment findings and recommendations – Based on the data obtained through documentation, interviews, vulnerability testing and analysis and an on-site physical review, final assessment findings and recommendations were formulated based on industry best practices and recognized standards such as the SANS Institute and the ISO17799 standard.

4.0 Assessment Tools

Vulnerability testing was conducted on the GIAC NMS server using the tools detailed below. In some cases, to assure adequate coverage, multiple tools were used to perform the same type of testing.

- **Tiger v2.2.1p1** - Tiger is an automated UNIX security auditing tool.
- **Crack v5.0 –** Crack is a password guessing program used to find weak user passwords.
- **John the Ripper v1.6 –** Jack the Ripper is a password guessing program used to find weak user passwords.
- **Nmap v2.54** - Nmap is a freeware port scanner that also allows remote operating system identification through TCP/IP stack fingerprinting.
- **Nessus v1.08 -** Nessus is a security scanner that is updated frequently to include the latest security vulnerabilities.
- **Cerberus Internet Scanner v5.0.02** – Cerberus is an application that scans for general known vulnerabilities on various platforms. Very fast and often catches vulnerabilities that some commercial scanners miss.
- **Twwwscan v1.2 -** Twwwscan is a highly effective web scanning tool that uncovers a constantly updated database of known vulnerabilities. It also includes the ability to circumvent some IDS systems.

5.0 Network Management Server Security Assessment Findings

This section details the findings of the GIAC Enterprises network management server security assessment. The assessment was conducted using the methodology detailed in Section 3 and the tools detailed in Section 4.

5.1 Security Policies and Procedures

Comprehensive security policies and procedures are the foundation of an information security program. Information security cannot be managed and enforced without a set of security policies that cover all areas of an organization's information technology's management and operations.

5.1.1 Finding: GIAC Enterprises has no security policies and procedures

When interviewing GIAC personnel about the formal security policies and procedures governing administration of the NMS server and governing the GIAC security program as a whole, it was found that GIAC had no documented security policies and procedures.

5.2 System Configuration Vulnerabilities

The purpose of this section is to detail findings of default Solaris 2.7 configuration settings or user imposed configuration options that pose security risks. This section covers issues such as unnecessary and insecure services, poor authentication, non-encrypted services, and services that give away system information.

5.2.1 Finding: Many non required services running on server

Open ports and their associated services that were detected by the tools nmap and nessus are detailed above in Table 1. Many of the services that are available on the NMS server are not required and can impose a security risk. The overall severity of risk in having these services open is considered to be high.

Table 1 – Open Ports and Services for Server nms1
Tools: nmap, nessus

Port Number	Service	Port Number	Service
7 / tcp	echo	2690 / tcp	ovembeddb
9 / tcp	discard	4045 / tcp	lockd
13 / tcp	daytime	6000 / tcp	X11
19 / tcp	chargen	6112 / tcp	dtspc
21 / tcp	ftp	7100 / tcp	font-service
23 / tcp	telnet	7161 / tcp	unknown
25 / tcp	smtp	7777 / tcp	ovuispmd
37 / tcp	time	8880 / tcp	ovhttp (httpd)
79 / tcp	finger	8886 / tcp	unknown
111 / tcp	sunrpc	8887 / tcp	unknown
162 / tcp	snmptrap	22370 / tcp	hpnpd
512 / tcp	exec	32771 / tcp	rpc5 (sometimes)
513 / tcp	login	32772 / tcp	rpc7 (sometimes)
514 / tcp	shell	32773 / tcp	rpc9 (sometimes)
515 / tcp	printer	32774 / tcp	rpc11 (sometimes)
540 / tcp	uucp	32775 / tcp	rpc13 (sometimes)
2389 / tcp	ovsessionmgr	32776 / tcp	rpc15 (sometimes)
2447 / tcp	ovwdb	32778 / tcp	rpc19 (sometimes)
2532 / tcp	ovtopmd	32780 / tcp	rpc23 (sometimes)

5.2.2 Finding: Open FTP server

An FTP server is accessible from any source IP address. FTP sessions are transmitted in clear text and the data between the client and the server can be sniffed allowing an attacker to capture login names and passwords and gain access to the server. It is also possible for an attacker to brute force a login and password on an FTP server.

5.2.3 Finding: Open Telnet Server

A Telnet server is accessible from any source IP address. Telnet sessions are transmitted in clear text and the data between the client and the server can be sniffed allowing an attacker to capture login names and passwords and gain access to the

server. It is also possible for an attacker to brute force a login and password on a Telnet server.

5.2.4 Finding: RPC not secured

Some applications required by HPOV require SunRPC in order to operate correctly. RPC has a history of security issues, such as, inadequate process registration and buffer overflows.

5.2.5 Finding: SNMP Read Community String set to default of public

The servers SNMP read community string is set to the default of public. The read community string is used as a password for an SNMP-GET or SNMP-GET-NEXT command to read values from the servers Management Information Base (MIB). Reading information from the MIB can give an attacker detailed system information.

5.2.6 Finding: No /etc/ftpusers file

If FTP cannot be replaced by SSH and be disabled, then a file that restricts user access via ftp should be created. Any source IP address can access the ftp service running on the NMS server, this leaves the server open to use by any system user. Since FTP traffic is transmitted in clear text, FTP users are vulnerable to password sniffing.

5.2.7 Finding: FTP banner displays system information.

The current ftp banner identifies the server platform and operating system version the server is running; this information can be used by an attacker.
The FTP banner displayed the following system information:

nms1 FTP server (SunOS 5.7) ready

5.2.8 Finding: Telnet banner displays system information.

The current telnet banner identifies the server platform and operating system version the server is running; this information can be used by an attacker.
The telnet banner displayed the following system information:

SunOS 5.7
Login:

5.2.9 Finding: X users not using any authentication

HPOV requires users to have an X Windows server to support their Open View display ovw client processes. During interviews with GIAC system administrators, it was found that X authentication was disabled by allowing users to run the xhost + command.

5.3 Software Revisions and Patches

The purpose of this section is to detail findings regarding Operating System and application patch levels. Keeping Operating System and application patch levels up to date is crucial to maintaining a secure system. Many times patches are released to fix security vulnerabilities that have been found "in the wild" and are likely to be launched against a server that is potentially vulnerable.

5.3.1 Finding: Recommended Patches not installed on the NMS server

Review of the NMS server's patch level and interviews with GIAC personnel found that no patches have been installed on the NMS server since it originally configured.

5.4 File Permission Vulnerabilities

The purpose of this section is to list potential file permission vulnerabilities that can allow an attacker to gain access to system information or even gain user access that exceeds their designated system access. Weak file permissions can open severe security holes that can be exploited by attackers.

5.4.1 Finding: Multiple files have file permissions of SUID root and eighty-eight files have file permissions of SGID root.

SUID files allow a user to run an executable with a user privilege different from their own. If an executable has a SUID privilege of root, an exploit against the executable can potentially cause the attacker to gain root access. SUID files are frequently the target of buffer overflow attacks. SGID executables run in the same fashion, allowing the user to run an executable with a group privilege different from their own. Listings of forty-eight SUID root and SGID root files found are listed in appendix A.

5.4.2 Finding: RC directories and files have insecure permissions.

The following directories in /etc have permissions of 775 and are part of a group other than root: which will allow other users in the group other than root to write in the system's initialization directories and potentially execute their new file or changes as root - /etc/rc0.d /etc/rc1.d /etc/rc2.d /etc/rc3.d /etc/rcS.d

5.4.3 Finding: Multiple directories and files have world writable file permissions.

World writable files and directories allow any user to read, modify and overwrite them if directory permissions allow. If they run as root, then they can be used to run certain commands with a privilege the user would not normally have. World writable files can also allow any user to read sensitive configuration or data files. A listing of ninety-two world writable directories and files found are listed in Appendix B.

5.4.4 Finding: Incorrect directory group write privileges

The tool Tiger found eleven critical directories that have group write privileges other than root. This can allow users for the improper group to write files into critical directories possibly gaining unauthorized system access or impairing existing files. A listing of directories with incorrect group write privileges are listed in Appendix C.

5.4.5 Finding: Multiple directories and files should have root as the owner

The tool Tiger found seventeen critical directories and files that should have root as the owner. Without root as the owner there is a chance that these critical files and directories can be accessed by users that do not require access. A listing of file that should have root as the owner are listed in Appendix D.

5.5 Password and User Account Security

The purpose of this section is to detail findings associated with password and user account security. Poor password creation and administration is a major cause of unauthorized access to systems and network devices.

5.5.1 Finding: Weak passwords

The password guessing tool Jack the Ripper was able to crack the password for the following user accounts:

- ovuser
- rwitt
- franco

In all cases the passwords cracked contained the user name combined with other characters. The weaker the password the easier it is to guess. Once a password is guessed a system is open to unauthorized access by the cracker using the account which can lead to the cracker using a variety of techniques to gain access to a more privileged access, such as root.

5.5.2 Finding: No password policy – user guidelines and education

During interviews with GIAC personnel it was found that GIAC has no system password policy or user password guidelines and education. Without a password policy, it is difficult to give users proper guidance as to password creation and to enforce their responsibility to create "secure" passwords.

5.5.3 Finding: No password expiration and aging

Password expiration and aging should be enabled to force users to change their passwords on a regular basis. The current values of the /etc/default/passwd file are as follows:

```
MAXWEEKS=
MINWEEKS=
PASSLENGTH=6
```

5.5.4 Finding: Many disabled login IDs have valid shells

The test tool tiger found that many disabled logins have valid shell entries in the /etc/passwd file. The accounts are: adm bin daemon listen lp noaccess nobody4 sys uucp. There is a potential that an intruder could put a password on a system account and use it as a back door account.

5.5.5 Finding: Multiple users using the same user account

During interviews with GIAC personnel it became apparent that level-1 and level-2 Network Operations staff are logging into the NMS server using the same user account – ovuser. With multiple users using the same account it is impossible to accurately audit which user took what actions while logged into the account.

5.6 Logging

The purpose of this section is to detail findings regarding system logging.
Logging and intrusion detection go hand in hand. If logging is not adequately performed than it is probable that all potential information regarding a system intrusion will not be available.

5.6.1 Finding: Logging set to default

The NMS server has its logging capabilities set to the installation default. System logging (syslog) should log at a level of info – which will log at info and all higher levels (notice, warning, err, crit, alert, emerg).

5.6.2 Finding: No manual or automated log monitoring

Critical log files such as /var/adm/messages, /var/log/syslog, /var/log/utmp, /var/adm/wtmp, /var/log/loginlog are not being monitored. Proactive inspection of these log files can be crucial in detecting an intruder in a timely manner.
UNIX servers can produce a large volume of log information that can get discarded or not acknowledged in a timely, semi-proactive manner. A log monitoring tool can take the manual burden of log monitoring off of a system administrator and can be programmed to alert the appropriate parties when an anomaly is noted in the logs.

5.7 Operating System Vulnerabilities

The purpose of this section is to detail findings of default Solaris 2.7 Operating system configuration settings that pose security risks. This section covers settings or lack of settings that can cause or mitigate various OS kernel based attacks.

5.7.1 Finding: No stack protection to prevent buffer overflows

No system parameters are set to deny attempts to execute instructions in the stack.
Many attacks to gain privileged access, such as root are based on buffer overflow attacks on poorly coded executables.

5.7.2 Finding: Default network parameters running on server

During interviews with GIAC operational staff, it was found that no networking parameters were changed on the NMS server after installation. By default, network parameters that help protect against denial of service attacks, spoofing attacks, operating system mapping or other informational gathering techniques are not set. Setting various network parameters on the system can protect the system or other systems on the network from attack.

5.7.3 Finding: Umask for system daemons not set to 022

The default umask for daemon files is not set to 022. Files created by daemons should have appropriate permissions set by running with a umask of 022.

5.8 Application Security

The purpose of this section is to detail findings of security risks imposed by installation of third party software. GIAC has installed Hewlett Packard's Open

View Network Node Manager version 6.2 application as its network management application platform on the NMS server.

5.8.1 Finding: Read / Write SNMP community strings in HPOV settings set to default of public / private.

The HPOV application is accessing all of the GIAC servers and network devices that are being monitored by using the default read and write SNMP community strings of public and private. Leaving SNMP community strings at the common default setting allows an attacker to read system configuration information via SNMP GET and SNMP GET-NEXT commands and to modify system configuration settings via SNMP SET commands.

5.9 Operational Procedures

The purpose of this section is to detail findings that are associated with GIAC's operational procedures in relation to the system administration of the NMS server. Interviews with GIAC staff indicated that system administration is performed on an as-needed basis by various network operations staff members that have various levels of UNIX system administration expertise.

5.9.1 Finding: System back up mechanisms are incomplete.

Backups are conducted on weekly basis via a cron job. Cron executes a shell script that uses the tar command to back up the /etc and HPOV application directories. The back up tape is not archived off-site and the previous week's backup is overwritten.

5.9.2 Finding: No disaster recovery plan and procedures.

There is no disaster recovery plan in place for the NMS server. If the NMS server were to fail, there is no back up server to take over monitoring of the co-location Web servers. There is no formal disaster recovery plan detailing what actions will be taken in a disaster recovery scenario.

5.9.3 Finding: No change control policy for servers and network devices.

A formal change control process for all GIAC production servers and network equipment is recommended. This will ensure that server environments are controlled and manageable. All changes should be reviewed and approved by a change control review board that includes representatives from groups that support the Web and e-Business infrastructure, including representatives from security operations, network operations, development, call centers, QA, and upper management.

5.9.4 Finding: No formal administration procedures or responsible personnel have been defined for the NMS server.

Without a formal set of system administration procedures and a formal schedule of system administration activities, GIAC cannot guarantee that its server is being properly administered this includes activities such as log monitoring, OS patch administration, and system back ups.

5.9.5 Finding: No file integrity checking.

The NMS server does not have a file integrity checker running on it. A file integrity checker should be run on a regular basis to monitor for unplanned file additions, deletions or changes. When a change is found the proper personnel should be alerted. Moreover, a historical archive of reports generated by the file integrity checker should be available for forensics purposes.

5.10 Physical Security

The purpose of this section is to detail findings associated with the physical security of the NMS server. Physical security includes areas such as physical access, environmental conditioning, fire suppression, surveillance and power.

The NMS server is housed in the GIAC corporate data center. Physical access to the data center is controlled by card key access which is logged to a disk and a console at the front lobby desk. FM-200 fire suppression is installed and adequate air conditioning and humidity control is in place. All servers and related equipment (tape drives, disk arrays) are enclosed in locked racks. Three video cameras panning across the data center are in place. Back up power to the data center is supplied by a combination of battery power and a diesel generator. One wall of the data center is made up of windows that border an open hall way.

5.10.1 Finding: Network Maps and Information displays are visible through the Data Center windows.

To make its network topology maps and SNMP trap displays visible to network operations and data center staff, GIAC has installed two 35 inch large screen monitors to display this information. Both displays are freely visible to any person walking down the free access hallway as they pass by the windows bordering the data center. Although the monitors act as a show case to the general people passing by, they also display information regarding the network that can be used by a person to infiltrate the GIAC network and its devices.

5.11 Network Security

The purpose of this section is to detail finding and concerns directly related to the network environment in which the NMS server is housed. This section should not be interpreted as comprehensive security assessment of the entire GIAC network.

The NMS server monitors the GIAC co-located servers via a router in the data center that has a frame relay connection to a GIAC router at the Co-Lo-Company data center. GIAC accesses the co-located Web servers and network devices (switches and routers) at the Co-Lo-Company data center via the frame relay connection for all of its system administration needs.

5.11.1 Finding: There is no network access control between the co-located environment and the GIAC data center.

Although the co-located environment is protected from the Internet by a firewall maintained by the Co-Lo-Company data center, there is no protection from traffic originating to/from the co-location environment from/to the GIAC corporate data

center. If a Web server or other co-located device is compromised an attacker can launch an attack on the GIAC data center network without any obstacles, such as router access lists or a firewall rule-set.

5.11.2 Finding: There is no network based intrusion detection monitoring traffic originating from the co-located environment.

Network based intrusion detection consists of a sensor that examines network traffic and looks for traffic patterns that are indicative of an attack in progress or other suspicious activity. Once the sensor detects an attack it can send an alert via SNMP or other mechanisms to alert the appropriate personnel. Network based intrusion detection is part of a defense-in-depth security strategy and is essential to early detection of an attack in progress.

6.0 Security Vulnerabilities

The purpose of this section is to list and prioritize the security vulnerabilities that are associated with the GIAC network management server security assessment findings detailed in section 5.0.

Table 2 details the security vulnerabilities found during the NMS server assessment. Each vulnerability found has a severity of risk assigned to it. Vulnerability severity of risk is classified as high, medium and low. High risk vulnerabilities are those, which can potentially provide unauthorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those, which provide access to sensitive, yet non-critical, server or network data. It is recommended that all high risk and medium risk vulnerabilities be corrected as soon as possible.

Table 2: Summary of Security Vulnerabilities
Server Assessed: nms1
IP Address: 172.16.X.X
Operating System: Solaris 2.7

Severity	Description
High	GIAC Enterprises has no formal Security Policies and Procedure
High	Server software not up to latest patch level – no patches installed.
High	Many non required services running on the server
High	Poor password administration
High	Open telnet and ftp server - SSH not implemented
High	Insufficient logging and log monitoring
High	No file integrity checking
High	No formal procedures or responsible personnel defined for system administration
High	No stack protection to prevent buffer overflows
High	Default networking parameters set on server
High	Server backup mechanism is incomplete
High	No disaster recovery plans and procedures
High	GIAC Enterprises has no change control policies for servers and network devices
High	No network access control and intrusion detection between co-located environment and GIAC network
High	Multiple SUID and SGID files
High	Insecure directory and file permissions
High	RPC not secured
High	SNMP community string set to default
Medium	Umask for system daemons not set to 022
Medium	Default SNMP community strings set for all devices monitored by HPOV
Medium	Multiple users using the same account
Medium	Disabled logins have valid shells
Medium	Banners not set to warn against unauthorized system access
Low	No /etc/ftpusers file
Low	X users not using any authentication
Low	Network maps and other network information visible through data center windows

7.0 Recommendations

The following section is a list of recommendations that are associated with the vulnerabilities listed and prioritized in section 6.0. In some cases, multiple recommendations will be necessary to correct a vulnerability found.

7.1 Vulnerability – GIAC Enterprises has no formal security policies and procedures

Recommendation:

Coble Consulting recommends that GIAC develop a comprehensive set of security policies that will cover the GIAC co-located network, staff and facilities; and the GIAC Corporate network, staff and facilities. The intent of the security policy is to protect GIAC assets and GIAC customer's assets from unauthorized access by GIAC employees, GIAC customers, the Internet community, business partner/outsource partners and other potential threats.

The GIAC security policy should address, but not be limited to, the following: [1]

- A definition of information security and its objectives and scope
- Management's intent in supporting in supporting information security
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Access control
- System development and maintenance
- Business continuity management
- Compliance to applicable laws and standards

7.2 Vulnerability: Server software not up latest patch level

Recommendation: Sun releases patch clusters that are considered to be the most critical system and security fixes. It is recommended that GIAC take the following actions:

- Install the latest SUN 7 recommended and security patches available from: http://sunsolve.sun.com
- Register to receive the security bulletins from SUN's Security Coordination Team by sending an email to security-alert@sun.com and including subscribe cws [email address] in the subject line.
- Implement an administrative procedure that checks the SUN Web site for new patches at http://sunsolve.sun.com/sunalert_patches.html and updates to the SUN 7 recommended and security patch cluster at http://sunsolve.sun.com.

[1] ISO/IEC 17799-2000(E): *Information technology - Code of practice for information security management (2000-12-01)*

7.3 Vulnerability: Many non required open ports running on server

Recommendation: Table 3 details recommended open ports and their associated services that can be disabled, concerns associated with the service and the procedure to disable the service.

Table 3: Unnecessary Open Ports and Services on NMS server
Tools used for analysis: nmap, nessus

Port Number	Service	Concern	Recommendation
7 / tcp	echo	Not needed for operations. Can be used in denial of service attacks.	Comment out entry in /etc/inetd.conf
9 / tcp	discard	Not needed for operations.	Comment out entry in /etc/inetd.conf
13 / tcp	daytime	Not needed for operations. Can be used for OS guessing in denial of service attacks.	Comment out entry in /etc/inetd.conf
19 / tcp	chargen	Not needed for operations. Can be used for denial of service attacks.	Comment out entry in /etc/inetd.conf
25 / tcp	smtp	Not needed for operations. The remote SMTP server answers to the EXPN and VRFY commands which can allow an attacker to gain user account information.	Move /etc/rc2.d/S88sendmail to a filename that does not start with S or K in /etc/rc2.d
37 / tcp	time	Not needed for operations.	Comment out entry in /etc/inetd.conf
79 / tcp	finger	Not needed for operations. Provides user information to attackers.	Comment out entry in /etc/inetd.conf
512 / tcp	rexec	Not needed for operations. Can allow remote users to execute commands.	Comment out entry in /etc/inetd.conf
513 / tcp	login	Not needed for operations. Can allow remote users to login without username and password.	Comment out entry in /etc/inetd.conf
514 / tcp	shell	Not needed for operations. Can allow remote users to gain a shell without username and password.	Comment out entry in /etc/inetd.conf
515 / tcp	printer	Not needed for operations.	Comment out entry in /etc/inetd.conf
540 / tcp	uucp	Not needed for operations.	Comment out entry in /etc/inetd.conf

7.4 Vulnerability: Poor Password Administration

7.4.1 Recommendation:

It is recommended that GIAC system administrators automatically run a password guessing tool, such as Jack the Ripper or Crack on a regular basis to find user passwords that are weak and can be cracked.

7.4.2 Recommendation:

It is recommended that GIAC institute a password policy that covers issues such as:

- Initial password creation and transference
- Password Standards
  - Length
  - Aging
  - Expiration
  - User's ability to change password
- Password handling guidelines
- Prohibited activities regarding passwords
- Password Policies for non GIAC personnel

7.4.3 Recommendation:

Password expiration should be enabled to force users to change their passwords on a regular basis. The current values of the /etc/default/passwd file are as follows:

MAXWEEKS=
MINWEEKS=
PASSLENGTH=6

It is recommended that the MAXWEEKS variable be set to 4 weeks (1 month), that MINWEEKS be set to a minimum of 2 weeks, so that users cannot immediately change back to an old password, and that the password length be increased to 8 characters as illustrated below:

MAXWEEKS=4
MINWEEKS=2
PASSLENGTH=8

7.5 Vulnerability: Open Telnet and FTP server on the NMS server

Recommendation:

It is recommended that telnet and ftp be disabled and the SSH utility be used in place of telnet and ftp. SSH provides an encrypted data stream with public / private key based authentication. Information on SSH can be obtained from www.openssh.com and www.vandyke.com. If SSH cannot be installed in a timely manner, then it is recommended that TCP wrappers be installed to limit source addresses that have telnet and ftp access to the server, until SSH can be implemented.

7.6 Vulnerability: Insufficient Logging and Log Monitoring

7.6.1 Recommendation:

Configure the system logging daemon (syslogd) to log LOG_AUTH information to a file called /var/log/authlog. Put the following entry into /etc/syslog.conf: [1]

auth.info /var/log/authlog

Create the log file /var/log/authlog:
touch /var/log/authlog
chown root /var/log/authlog
chmod 600 /var/log/authlog

7.6.2 Recommendation:

Configure a log to monitor failed login attempts: [2]

touch /var/adm/loginlog
chmod 600 /var/adm/loginlog
chown root:sys /var/adm/loginlog

7.6.3 Recommendation:

It is recommended that GIAC configure a log monitoring tools such as swatch or logcheck to automatically monitor system log files and send an alert to the appropriate system administration or security personnel.

7.7 Vulnerability: No file integrity checking

Recommendation:

It is recommended that GIAC configure a file integrity checker to detect file system changes and archive reports on a minimum of a daily basis. A best of breed file integrity checker is the tripwire tool.

7.8 Vulnerability: No formal procedures or responsible personnel defined for system administration

Recommendation:

It is recommended that GIAC identify a full time resource to function as the responsible party for system administration. A back-up system administrator should also be identified, if the primary administrator is not available. System administration should follow a set of procedures that ensures, but is not limited to:

- System administration:
  - User account and password management
  - OS and application patches

[1] Hal Pomeranz. Editor. *Solaris Security – Step By Step– Version 2.0 (2001),* The SANS Institute. (Page 14)
[2] Hal Pomeranz. Editor. *Solaris Security – Step By Step– Version 2.0 (2001),* The SANS Institute. (Page 14)

  - System monitoring (disk space, CPU, etc.)
- Adequate log monitoring and archival
- Back up management
- Change control

7.9 Vulnerability: No stack Protection to prevent buffer overflows

Recommendation:

Edit the /etc/system file and insert the following entries to prevent and log buffer overflows: [1]

```
set noexec_user_stack = 1
set noexec_user_stack_log = 1
```

7.10 Vulnerability: Default network parameters set on server

Recommendation:

It is recommended that a start up script be created in /etc/rc2.d that executes after /etc/rc2.d/S69inet that contains the following entries:[2]

```
#!/sbin/sh
# Prevent SYN floods
ndd –set  /dev/tcp tcp_conn_req_max_q0 8192
ndd –set /dev/tcp tcp_ip_abort_cinterval 60000

# Prevent mapping (this system) and smurf attacks
ndd –set /dev/ip ip_respond_to_timestamp 0
ndd –set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd –set /dev/ip ip_respond_to_address_mask_broadcast 0
ndd –set /dev/ip ip_forward_directed_broadcasts 0

# Tune down ARP timeouts
ndd –set /dev/arp arp_cleanup_interval 60000
ndd –set /dev/ip ip_ire_flush_interval 60000

# Disable ICMP redirects
ndd –set /dev/ip ip_ignore_redirect 1
ndd –set /dev/ip ip_send_redirects 0

# Disable source routing
ndd –set /dev/ip ip_forward_src_routed 0

# Disable IP forwarding
ndd –set /dev/ip ip_forwarding 0
ndd –set /dev/ip ip_strict_dst_multihoming 1
```

[1] Hal Pomeranz. Editor. *Solaris Security – Step By Step– Version 2.0 (2001),* The SANS Institute. (Page 11)
[2] Hal Pomeranz. Editor. *Solaris Security – Step By Step– Version 2.0 (2001),* The SANS Institute. (Page 10)

7.11 Vulnerability: Server backup mechanism is incomplete

Recommendation:
It is recommended that GIAC implement a back up procedure that does the following:

- Written back up policy and procedures
- Weekly full back ups of the entire system
- Nightly incremental backups
- Off-site, secure tape storage with a minimum of a three month tape rotation
- Full back ups before and after major changes are implemented
- Regular testing and verification of the back up tapes, so that there are no suprises when a complete or partial restore from a back up has to occur.

7.12 Vulnerability: No disaster recovery plans and procedures

Recommendation:
It is recommended that GIAC document a disaster recovery plan for the NMS server. The disaster recovery plan should cover the following:

- Personnel roles and responsibilities
- Secondary NMS server resource (backup NMS server)
- Restoration and baseline configuration of the NMS server

All steps in the disaster recovery plan should be tested and a simulated disaster recovery should be staged on a quarterly basis.

7.13 Vulnerability: No change control policy for servers and network devices

Recommendation:
It is recommended that GIAC implement a formal change control process for all GIAC production servers and network equipment. This will ensure that server environments are controlled and manageable. All proposed changes should be approved or denied by a change control review board include representatives from groups that support the Web and e-Business infrastructure, including representatives from security operations, network operations, development, call centers, QA, and upper management. An example of a change control process is outlined below:

- The party that needs to implement a change submits a change request via email to the change control review board. Timeframe for the lead-time between submission to the board, formal review of the change by the board, and the actual implementation of the change need to be determined.
- The change request should include:
  - The requestor's contact information
  - A description of the change
  - The potential impact of the change on users, including any potential outages
  - The severity of the change (ranking)

- The proposed date of the change
- The expected time duration of the change
- A detailed back-out plan

- The review board will:
  - Review the change
  - Approve or Deny the change
  - Schedule the change
  - Notify the affected parties
  - Conduct a post-mortem on the change

7.14 Vulnerability: No network access control and intrusion detection between co-location network and GIAC corporate network

Recommendation:

It is recommended that GIAC implement a firewall and network based intrusion detection sensor to protect the perimeter of the GIAC corporate network, where it connects to the co-located network at the Co-Lo-Company data center. Access lists and logging should be implemented on the corporate router that connects to the co-located facility until a stateful or application layer firewall can be implemented. Figure 2 details the network topology with the recommended firewall and IDS sensor in place. Tables 4 and 5 detail recommended traffic flows.

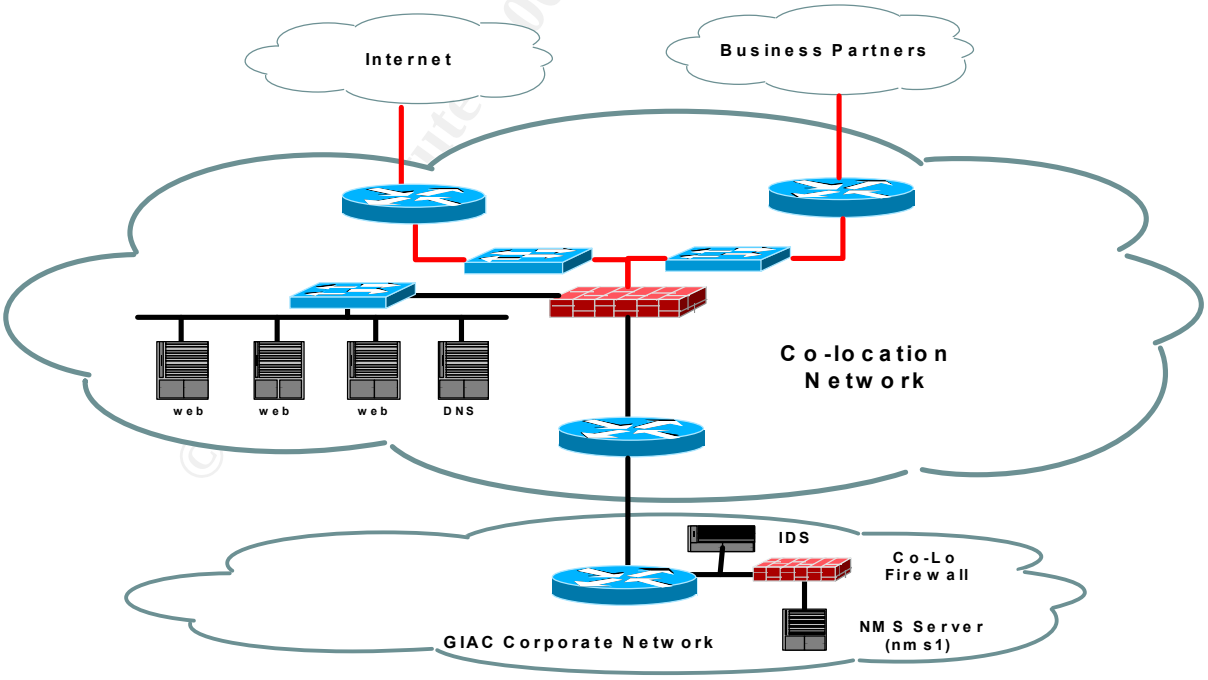

Figure 2: Recommended Firewall and IDS for Co-location Connectivity

Table 4 Recommended Traffic Flows Originating From GIAC To Co-location Data Center		
Source	**Destination**	**Service**
NMS Server	All co-located devices	SNMP (161 udp), ICMP
Network /System Administration	All co-located devices	SSH

Table 5 Recommended Traffic Flows Originating From Co-location Data Center to GIAC		
Source	**Destination**	**Service**
All co-located devices	NMS server	SNMP-Trap (162 udp)

7.15 Vulnerability: Multiple files have SUID and SGID permissions

Recommendation:
In order to reduce the number of SUID and SGID files (see appendix A) it is recommended that GIAC run the tool fix-modes to set file permission modes to a safer setting on executables where changing file permissions will not impair the functionality of the executable.

7.16 Vulnerability: Insecure directory and file permissions

7.16.1 Recommendation:
The following rc directories should have their group changed to root and their permissions changed to 700. Note: At the time of this assessment the owner was root, it the directory owner is not root, then it should be changed.
/etc/rc0.d
/etc/rc1.d
/etc/rc2.d
/etc/rc3.d
/etc/rcS.d

7.16.2 Recommendation:
The world writable files and directories in Appendix B, should be changed so that they are not world writable.

7.16.3 Recommendation:
Appendix C lists critical directories that should not be group writable.

7.16.4 Recommendation:
Appendix D lists critical files and directories that should have their ownership set to root.

7.17 Vulnerability: RPC not secured

Recommendation:
Install Weitse Venema's enhanced versions of rpcbind and portmap which allow filtering based on IP addresses.

7.18 Vulnerability: SNMP community string set to default

Recommendation:
Change NMS server's default read community string in /etc/snmp/conf/snmpd.conf from default of public to a harder to guess string using secure password best practices. The line to change in /etc/snmp/conf/snmpd.conf is: read-community public

7.19 Vulnerability: Umask for system daemons not set to 022

Recommendation:
To ensure that each startup script sets the umask to 022 do the following commands: [1]

```
echo 'mask 022' > /etc/init.d/umask.sh
chmod 744 /etc/init.d/umask.sh
    for dir in /etc/rc?.d
    do
            ln –s ../init.d/umask $dir/S00umask.sh
done
```

7.20 Vulnerability: Default SNMP community strings set in HPOV

Recommendation:
Change the default SNMP read and write community strings on all GIAC servers and network devices in the HPOV configuration. New read and write community strings should created using secure password best practices. The NMS server should be configured to use the new SNMP community strings. This can be configured off of the HPOV main map screen by selecting:

- Options
- SNMP Configuration

7.21 Vulnerability: Multiple users using the same account

Recommendation
It is recommended that each person in the Network Operations staff that requires access to the NMS server have their own user account. This will allow better auditing of individual users actions. It is also recommended that the current shared account, ovuser, be disabled.

[1] Hal Pomeranz. Editor. *Solaris Security – Step By Step– Version 2.0 (2001),* The SANS Institute. (Page 8)

Note: It should be noted, that adding more user accounts can potentially increase the risk of poor user password creation and administration, which could increase the risk of an intrusion based on poor password security. Therefore, it is essential that the recommendations in section 7.4 be followed if more user accounts are added.

7.22 Vulnerabiliy: Disabled logins have valid shells

Recommendation

Set the login shell for disabled accounts to be /dev/null for the accounts listed below: adm bin daemon listen lp noaccess nobody4 sys uucp

7.23 Vulnerability: Login banners not set to warn against unauthorized access

7.23.1 Recommendation

Edit the /etc/default/ftpd file and insert a login banner that gives no system information and says "Warning: restricted to authorized use only".

7.23.2 Recommendation

Edit the /etc/default/telnetd file and insert a login banner that gives no system information and says "Warning: restricted to authorized use only".

7.23.3 Recommendation

Edit the /etc/motd and /etc/issues files to warn users against unauthorized access. An example would be:

```
--------------------------------------------------------------------------------
 WARNING!  ACCESS TO THIS RESOURCE IS RESTRICTED!

 Unauthorized access to this system is a violation
 of United States federal statutes.  Users accessing
 this system are subject to and consent to monitoring.
Unauthorized access or monitored activity deemed to
 Violate company policy, state law or federal law may be
 turned over to local or federal law enforcement officials
 for prosecution.
--------------------------------------------------------------------------------
```

7.24 Vulnerability: No /etc/ftpusers file

Recommendation

If SSH is not enabled, then an /etc/ftpusers file should be created that has entries to restrict root and all other user accounts except those that require the ftp service.

7.25 Vulnerability: X users not using any authentication

Recommendation

It is recommended that .Xauthority files be set up in each X user's home directory and copied to remote systems that need to access the NMS server. It is recommended that the xhost executable be deleted from the server, so that users can use the command to circumvent the .Xauthority file mechanism.

7.26 Vulnerability: NMS Monitors visible to non authorized personnel

Recommendation:

It is recommended that the data center windows bordering the hallway be shaded, so that people looking through the windows cannot see network information displayed on the 35'' monitors. If shading the windows is undesirable, then the 35" monitors should be repositioned, so that they are not visible from the hallway windows.

8.0 Estimated Tasks and Timeframes to Fix Vulnerabilities

8.1 Develop GIAC Corporate Security Policies

1. Information Gathering:	
– Interview GIAC personnel	3 days
– Review current policies	1 day
– Review relevant network and other IT documentation	5 days
2. Comprehensive Security Policy Document Development	20 days
3. Presentation to GIAC management	1 day
Total Time	30 days
Cost (rate $200.00 per hour * 8 hrs = $1,600 per day)	$48,000

8.2 Server Hardening

1. Install Patches	1 day
2. Configuration changes	2 days
– Disable open ports	
– /etc/services	
– file permissions	
– SNMP community strings	
– Banners	
– RPC	
– /etc/ftpusers	
– X authentication	
– HPOV changes	
3. Install / Configure / Test SSH	2 days
4. Install / Configure / Test File Integrity Checker	3 days
5. Password security	1 day
6. Install / Configure / Test Log Monitoring Tool	3 days
7. Install / Configure/ Test Backups	3 days
8. Documentation	3 days
Total Time	18 days
Cost (rate $150.00 per hour * 8 = $1,200 per day)	$21,600

8.3 Server Policies and Procedures

1. Administrative Policy Development	5 days
2. Change Control Policy Development	5 days
Total Time	10 days
Cost (rate $200.00 per hour * 8 = $1,600 per day)	$16,000

8.4 Perimeter Firewall and IDS

1. Develop Requirements and Design Document	5 days
2. Product Selection	2 days
3. Firewall installation / configuration / test	3 days
4. IDS installation / configuration / test / tune	5 days
5. As-Built documentation	3 days
Total Time	18 days
Estimated Equipment	
Firewall	$30,000
IDS	$30,000
Cost (rate $200.00 per hour * 8 = $1,600 per day)	$28,800
Total	$88,800

8.5 Total Project Cost

GIAC Security Policy Development	$48,000
Server Hardening	$21,600
Server Policies and Procedures	$16,000
Perimeter Firewall and IDS	$88,800
Total Estimated Cost	**$ 174,400**

Appendix A: SUID and SGID Files Found on NMS Server: nms1

SUID Files:

```
/usr/lib/lp/bin/netpr
/usr/lib/fs/ufs/quota
/usr/lib/fs/ufs/ufsdump
/usr/lib/fs/ufs/ufsrestore
/usr/lib/pt_chmod
/usr/lib/utmp_update
/usr/lib/acct/accton
/usr/lib/uucp/remote.unknown
/usr/lib/uucp/uucico
/usr/lib/uucp/uusched
/usr/lib/uucp/uuxqt
/usr/lib/sendmail
/usr/bin/sparcv7/ps
/usr/bin/sparcv7/uptime
/usr/bin/sparcv7/w
/usr/bin/at
/usr/bin/atq
/usr/bin/atrm
/usr/bin/crontab
/usr/bin/eject
/usr/bin/fdformat
/usr/bin/login
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/rcp
/usr/bin/rdist
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/su
/usr/bin/tip
/usr/bin/yppasswd
/usr/bin/admintool
/usr/bin/ct
/usr/bin/cu
/usr/bin/uucp
/usr/bin/uuglist
/usr/bin/uuname
/usr/bin/uustat
/usr/bin/uux
/usr/bin/sparcv9/ps
/usr/bin/sparcv9/uptime
/usr/bin/sparcv9/w
/usr/bin/chkey
/usr/bin/nispasswd
/usr/bin/cancel
/usr/bin/lp
/usr/bin/lpset
/usr/bin/lpstat
/usr/bin/volcheck
```

```
/usr/bin/volrmmount
/usr/dt/bin/dtaction
/usr/dt/bin/dtappgather
/usr/dt/bin/sdtcm_convert
/usr/dt/bin/dtprintinfo
/usr/dt/bin/dtsession
/usr/openwin/bin/xlock
/usr/openwin/bin/ff.core
/usr/openwin/bin/kcms_configure
/usr/openwin/bin/kcms_calibrate
/usr/openwin/bin/sys-suspend
/usr/openwin/lib/mkcookie
/usr/sbin/sparcv7/whodo
/usr/sbin/allocate
/usr/sbin/mkdevalloc
/usr/sbin/mkdevmaps
/usr/sbin/ping
/usr/sbin/sacadm
/usr/sbin/traceroute
/usr/sbin/deallocate
/usr/sbin/list_devices
/usr/sbin/afbconfig
/usr/sbin/sparcv9/whodo
/usr/sbin/ffbconfig
/usr/sbin/igsconfig
/usr/sbin/m64config
/usr/sbin/lpmove
/usr/sbin/pmconfig
/usr/sbin/static/rcp
/usr/sbin/pgxconfig
/usr/ucb/sparcv7/ps
/usr/ucb/sparcv9/ps
/usr/vmsys/bin/chkperm
/opt/OV/bin/netcheck
/opt/OV/bin/ovtraceroute
/opt/OV/www/htdocs/classes/nodeView/nodeView.jar
/etc/lp/alerts/printer
/proc/360/object/a.out
/proc/453/object/a.out
```

Appendix A: (Continued) SUID Files

```
/usr/platform/sun4u/sbin/eeprom
/usr/platform/sun4u/sbin/prtdiag
/usr/lib/fs/ufs/ufsdump
/usr/bin/sparcv7/ipcs
/usr/bin/mail
/usr/bin/mailx
/usr/bin/netstat
/usr/bin/passwd
/usr/bin/write
/usr/bin/yppasswd
/usr/bin/sparcv9/ipcs
/usr/bin/nispasswd
/usr/dt/bin/dtaction
/usr/dt/bin/sdtcm_convert
/usr/dt/bin/dtmail
/usr/dt/bin/dtmailpr
/usr/dt/lib/fdl
/usr/dt/lib/fdl/adobe
/usr/dt/lib/fdl/adobe/CMap
/usr/dt/lib/fdl/sparc
/usr/dt/lib/fdl/icons
/usr/openwin/bin/Xprt
/usr/openwin/bin/Xsun
/usr/openwin/bin/ff.core
/usr/openwin/bin/mailtool
/usr/openwin/bin/kcms_configure
/usr/openwin/bin/kcms_calibrate
/usr/sbin/sparcv7/prtconf
/usr/sbin/sparcv7/swap
/usr/sbin/sparcv7/sysdef
/usr/sbin/arp
/usr/sbin/wall
/usr/sbin/sparcv9/prtconf
/usr/sbin/sparcv9/swap
/usr/sbin/sparcv9/sysdef
/usr/vmsys/bin/chkperm
/usr/local/bin/sparcv7/top
/usr/local/bin/sparcv9/top
/var/spool/calendar
/proc/344/object/a.out
```

Appendix B: Files with World Writable Permissions

```
/etc/SnmpAgent.d/
/etc/opt/OV/share/conf/
/etc/opt/OV/share/conf/C/
/etc/opt/OV/share/conf/analysis/requests/
/etc/opt/OV/share/conf/analysis/requests/C/
/etc/opt/OV/share/conf/analysis/sqlScripts/
/etc/opt/OV/share/conf/analysis/templates/
/etc/opt/OV/share/conf/analysis/templates/NNM/
/etc/opt/OV/share/conf/ecs/forms/
/etc/opt/OV/share/conf/ecs/forms/C/
/etc/opt/OV/share/conf/eventFilters/
/etc/opt/OV/share/conf/oid_to_sym_reg/
/etc/opt/OV/share/registration/C/ovmib/
/etc/opt/OV/share/symbols/C/Cards/
/etc/opt/OV/share/symbols/C/Client/
/etc/opt/OV/share/symbols/C/Computer/
/etc/opt/OV/share/symbols/C/Connection/
/etc/opt/OV/share/symbols/C/Connector/
/etc/opt/OV/share/symbols/C/Device/
/etc/opt/OV/share/symbols/C/Domain/
/etc/opt/OV/share/symbols/C/Location/
/etc/opt/OV/share/symbols/C/Logo/
/etc/opt/OV/share/symbols/C/NetDevice/
/etc/opt/OV/share/symbols/C/Network/
/etc/opt/OV/share/symbols/C/SW_Utils/
/etc/opt/OV/share/symbols/C/Server/
/etc/opt/OV/share/symbols/C/Software/
/etc/opt/OV/share/symbols/C/Transceiver/
/etc/rc.config.d/
/opt/local/src/security/netscape/communicator-v477.sparc-sun-solaris2.5.1/
/opt/local/src/security/scans/
/var/crash/
/var/dt/tmp/
/var/mail/
/var/opt/OV/analysis/
/var/opt/OV/analysis/ovrequestd/
/var/opt/OV/analysis/ovrequestd/config/
/var/opt/OV/log/
/var/opt/OV/share/
/var/opt/OV/share/databases/analysis/
/var/opt/OV/share/databases/openview/defmap/
/var/opt/OV/share/databases/openview/mapdb/
/var/opt/OV/share/databases/openview/mapdb/default/
/var/opt/OV/share/databases/openview/mapdb/default/current/
/var/opt/OV/share/databases/openview/ovwdb/
/var/opt/OV/share/databases/openview/ovwdb/current/
/var/opt/OV/share/databases/openview/topo/
/var/opt/OV/share/databases/snmpCollect/
/var/opt/OV/share/databases/snmpCollect/stringData/
/var/opt/OV/share/help/C/ovmib/OVW/
/var/opt/OV/share/help/C/ovmib/OVW/Functions/
/var/opt/OV/share/log/
/var/opt/OV/share/log/ecs/
```

```
/var/opt/OV/share/log/ecs/1/
/var/opt/OV/share/snmp_mibs/
/var/opt/OV/share/snmp_mibs/Vendor/3Com/
/var/opt/OV/share/snmp_mibs/Vendor/ATT/
/var/opt/OV/share/snmp_mibs/Vendor/Banyan/
/var/opt/OV/share/snmp_mibs/Vendor/BayNetworks/
/var/opt/OV/share/snmp_mibs/Vendor/Cabletron/
/var/opt/OV/share/snmp_mibs/Vendor/Cisco/
/var/opt/OV/share/snmp_mibs/Vendor/Compaq/
/var/opt/OV/share/snmp_mibs/Vendor/Crescendo/
/var/opt/OV/share/snmp_mibs/Vendor/Fibronics/
/var/opt/OV/share/snmp_mibs/Vendor/Juniper/
/var/opt/OV/share/snmp_mibs/Vendor/Microsoft/
/var/opt/OV/share/snmp_mibs/Vendor/NorthernTelecom/
/var/opt/OV/share/snmp_mibs/Vendor/Novell/
/var/opt/OV/share/snmp_mibs/Vendor/OTHER-VENDORS/
/var/opt/OV/share/snmp_mibs/Vendor/OpticalDataSys/
/var/opt/OV/share/snmp_mibs/Vendor/Plaintree/
/var/opt/OV/share/snmp_mibs/Vendor/Racal/
/var/opt/OV/share/snmp_mibs/Vendor/Timeplex/
/var/opt/OV/share/snmp_mibs/Vendor/TyLink/
/var/opt/OV/share/snmp_mibs/Vendor/Xyplex/
/var/opt/OV/share/tmp/
/var/opt/OV/sockets/
/var/opt/OV/sockets/ecs/1/
/var/opt/OV/tmp/
/var/opt/OV/www/
/var/opt/OV/www/logs/
/var/opt/OV/www/logs/launcher/
/var/opt/OV/www/tmp/
/var/preserve/
/var/spool/lp/fifos/public/
/var/spool/pkg/
/var/spool/uucppublic/
/var/tmp/
```

Appendix C: Directories with incorrect group write privileges (Source Tiger test tool)

```
--WARN-- [perm019w] /etc should not have group write.
--WARN-- [perm003w] /export should not have group write.
--WARN-- [perm003w] /sbin should not have group write.
--WARN-- [perm003w] /usr should not have group write.
--WARN-- [perm003w] /usr/4lib should not have group write.
--WARN-- [perm003w] /usr/openwin should not have group write.
--WARN-- [perm003w] /usr/demo should not have group write.
--WARN-- [perm003w] /usr/games should not have group write.
--WARN-- [perm003w] /usr/bin should not have group write.
--WARN-- [perm003w] /usr/lib should not have group write.
--WARN-- [perm003w] /usr/ucb should not have group write.
```

Appendix D: Incorrect File Ownership (Source: Tiger Test Tool)

```
--WARN-- [perm001w] The owner of /usr/ucblib should be root (owned by bin).
--WARN-- [perm003w] /dev should not have group write.
--WARN-- [perm003w] /etc/dfs should not have group write.
--WARN-- [perm003w] /etc/vfstab should not have group write.
--WARN-- [perm001w] The owner of /etc/remote should be root (owned by bin).
--WARN-- [perm001w] The owner of /etc/mail/sendmail.cf should be root (owned
         by bin).
--WARN-- [perm001w] The owner of /etc/uucp/Permissions should be root (owned
         by uucp).
--WARN-- [perm001w] The owner of /usr/bin/uulog should be root (owned by
         uucp).
--WARN-- [perm001w] The owner of /usr/bin/uuto should be root (owned by
uucp).
--WARN-- [perm001w] The owner of /usr/bin/uupick should be root (owned by
         uucp).
--WARN-- [perm003w] /usr/bin/tip should not have owner write.
--WARN-- [perm001w] The owner of /usr/bin/write should be root (owned by
bin).
--WARN-- [perm001w] The owner of /usr/sbin/wall should be root (owned by
bin).
--WARN-- [perm001w] The owner of /usr/bin/sh should be root (owned by bin).
--WARN-- [perm001w] The owner of /usr/bin/acctcom should be root (owned by
         bin).
--WARN-- [perm001w] The owner of /sbin/sh should be root (owned by bin).
--ALERT-- [perm024a] /usr/sbin/arp is setgid to `bin'.
--WARN-- [permxxxw] The owner of /var/sadm/install should be root (owned by
         bin).
```

References:

1. ISO/IEC 17799-2000(E): *Information technology - Code of practice for information security management (2000-12-01)*

2. Hal Pomeranz. Editor. *Solaris Security – Step By Step– Version 2.0 (2001),* The SANS Institute.

3. Sidne Feit. *SNMP A Guide to Network Management*. McGraw-Hill Inc, 1995

4. D. Brent Chapman, Elizabeth D. Zwickey. *Building Internet Firewalls*. O'Reilly and Associates, Inc. 1995.

5. AEleen Frisch. *Essential System Administration*. O'Reilly and Associates, Inc. 1995.

6. SANS Institute: *Securing UNIX* courseware. Baltimore MD. May 2001.