Global Information Assurance Certification Paper

FROM: Ted Ying
Student Username: ted.yin001

TO: SANS – GIAC Testing
giactc@sans.org

DATE: 14 August 2000

Enclosed please find the practicum portion of the GIAC Testing procedure.

For the practicum, a server in my local domain was used. As per instructions at the SANS Conference, the system information has been sanitized. For the purposes of the practicum, the name of the server has been changed to **server1.gsfc.nasa.gov**. The IP address has been replaced with **192.168.111.222.**

Table of Contents

I. Executive Summary

server1 is a Sun Sparc 10 running the 4.1.3 U1 Rev B Operating System. The system is pending an operating system upgrade to Solaris 2.7 after certain specific projects are completed. Some operating system patches and security toolkit applications have been installed as time has permitted, however, downtime is very difficult to schedule for any additional patching. The system is a mission-critical server and the windows for operating system patches, upgrades, and reboots are very small. Once the mission-critical projects have completed, a complete overhaul starting with an OS upgrade will be performed. At this point, however, several operating system patches and software patches have been installed as detailed in this review. Additionally, several security applications have been added. In general, however, the security level of this machine is very low.

This server is the primary NIS and NFS server for a cluster of machines supporting one particular project. In addition, the system is one of several key servers supporting an in-house written software program for a specific mission-critical database application.

Section II covers a discussion of the current level of Security on this system. The section will cover the details from the Network down to the Third Party applications. It will also cover Procedures and Policies and finally Backup and Disaster Recovery. Due to restrictions from the site where the server is located, some of the information has been slightly modified for anonymity. In general, a hodge-podge of security patches, fixes, and tools have been installed to combat the more serious problems identified by the support staff. However, the amount is woefully inadequate for long-term security needs, but will have to suffice for the short-term.

To start the security review, a scan from the commercial version of ISS was run on the host in question. As part of our network-based security review, all hosts in the cluster were scanned; but the notes specific to **server1** have been isolated out for this review. Those will be presented in Section III of this document. Section III will discuss additional known security problems that will need to be repaired under the current format.

Section IV will discuss the plans for fixing those problems should appropriate windows for system upgrades become available.

Section V will discuss the long-term security plans including the Operating System upgrade and associated fixes.

II. Current Security Implementation

A. Network-Based Security

Although the system-level security on **server1** is very patchy, some significant network-based security has been implemented to enhance the system-based security. It is understood that network-based security is not a substitute for system-based security, however, it can help in the situation where there is some delay in implementing system-based security.

Due to the proprietary nature of this server, and the limited access that is required to the entire cluster of machines, most outside traffic has been excluded from this machine. The server resides on a private subnet that is controlled by a switched router. Only select TCP/IP traffic is allowed to pass in or out of that router. TCP/IP connections from select portions of the other subnets of the local domain are allowed. Only a limited set of hosts outside the local domain are allowed to have any TCP/IP connections to this subnet and those connections are restricted via the domain gateway and it's access list. ICMP traffic is allowed from within the local domain, but not from nodes external to the local domain. All other traffic is routed and not allowed.

This effectively only allows host-to-host connections of certain types from outside the local domain. The hosts that are allowed are specific hosts at the contractor company site that writes and maintains a third-party vendor software application package written specifically for use by this site. The software is specialized for this site's needs and is proprietary and not used by any another client. The application can be used in its client form from any node in the local domain, but not from outside the local domain. Telnet and FTP access to the cluster hosts are allowed from client nodes within the domain. Several additional ports are allowed from the vendor site for maintenance of the database applications (and those are non-standard port numbers for some additional anonymity). Those connections again are governed by the point-to-point access list by the domain gateway.

B. Operating System

As cited above, **server1** is a Sun Sparc 10 system running SunOS 4.1.3 U1 Rev B. The Sun Jumbo patch has been installed as recommended. Additional patches have been installed as per instructions from the ISS scan run on the system.

The OS Kernel has been modified to comment out all unused options (e.g. HSFS, PCFS, the System V IPC facilities) and recompiled. The vmunix file is smaller and hopefully more secure this way.

C. Configuration

1. File Systems

The system has been configured with separate partitions for each of the following file systems: / (root), /home, /tmp, /usr, /var. Since the system uses NIS, a netgroup has been created for the various hosts within the cluster and all local file systems that are exported are exported read-only to the clusters netgroup. Only one file system is automounted on this server from another server and that server is also governed by the NIS netgroup and exported from that server read-only. It is mounted explicitly read-only on this server. On the various client machines in the cluster, automount is used to mount file systems. The entire cluster of machines has been checked and all file systems are exported read-only where possible. The limited number of file systems that are exported read-write are governed by the export policy. All file systems are exported only to the NIS netgroup that includes all systems in the cluster. All file systems are mounted via the automounter to ensure that if the mount status changes, the file system will be unmounted after the default timeout time.

2. Root

All terminals other than console have been tagged as "unsecure" in /etc/ttytab so that root can only log directly into the console. Only a select number of people (three people, all on-site employees) are in the wheel group and can su into the root account. Additionally, getty has been turned off for all devices except the console. The root account's .cshrc, .login, and .profile files have been modified to remove the "." (dot) from the PATH to set the umask to 022.

3. IP address resolution and sendmail

Since there are only a limited number of hosts that this cluster should be accessing, DNS has not been enabled on this system. A very small, select list of hosts is maintained in the /etc/hosts file on the server and exported via NIS to the cluster. Also, since the only machine in the cluster that will need to receive mail is the mail server, sendmail has been disabled and removed from the startup on all machines in the cluster other than the server. On the server, a newer version of sendmail was ftp'ed from Eric Allman's site and compiled. The sendmail daemon is newer than the operating system version, but still not the latest (circa 8.7, but the sendmail version string was modified to be a local designation version). The sendmail package will be upgraded once again after the Operating System upgrade (see Section V).

4. System services

The inetd.conf file has been modified to comment out many unused services (including comsat, finger and tftp). All services remaining are actually being used to support the project and user community. RPC's and the portmapper cannot be removed as some database applications require RPC's for data transmission. Only three users are entered in the cron.allow file to modify their crontab settings. All other users are restricted.

5. Users and NIS

The NIS server has been configured with a non-trivial domainname. Although there are elements of the project name in it, additional letters, digits, and punctuation have been added to make it more obscure and harder to guess. Additionally, the NIS files have been moved to a

non-standard place (outside of /etc). This includes the NIS passwd file, so only the original system defined accounts exist in /etc/passwd. Although the files can be found by tracing through

Configuration (cont)

5. Users and NIS (cont)
the NIS Makefile, it is slightly more obscure and needs on-line access to find. Remote attacks are less likely to discover any useful information from standard files like /etc/passwd.

Due to project policy, expired accounts are not removed from the passwd file, but the shells have been changed to /bin/false which is not in /etc/shells. Also, all expired users and some current users are in /etc/ftpusers to prevent ftp access to those accounts. Only a limited number of accounts are permitted ftp access to this server.

6. TCP Wrappers
TCP Wrappers have been configured for this system. The hosts.allow file has been used to only allow access by those hosts that are in the domain gateway access list and any host within the local domain. This duplicates the access list granted at the network gateway at the system level. Additionally, the TCP Wrappers pre-login banner is used to give a fairly standard warning about appropriate use. This is a requirement by the appropriate legal council for the institution that owns the server.

D. Third Party Packages

This server uses two major third-party packages on-line. The first is ORACLE for their database support engine. The second is the private third-party application package that is the primary purpose of the project and cluster of systems.

The system is using an old version of ORACLE. The patches received up to a certain point have been installed as per instructions by the vendor. However, newer patches after a certain date for the database engine have not been installed. When the system is upgraded to Solaris 2.7, a newer version of Oracle will be procured for the server and patches will once again be applied as per the vendor instructions on the database engine.

As for the in-house third party package, the key programmer who developed this application still works on the application and maintains it. His computer back at the vendor home site is one of the few machines outside the domain that has access to this cluster for TCP/IP traffic in-bound. The developer can telnet and ftp into this server without restrictions from his local machine.

E. Administrative Practices

There are three system administrators for this project and this cluster. There is one junior level admin who has her office in the computer room facility. She is responsible for day-to-day administration of the system and cluster. She creates new accounts, handles day-to-day problems, handles user requests and problems, and handles the backups. There are two senior level admins. The author is the network operations manager and provides support for this project. The author is the primary security administrator for this group as well as the supervisor to the network support staff for the entire department (much larger than this group). Due to

Administrative Practices (cont)
additional responsibilities for the department, the amount of time available for security support is limited to what is detailed in this report.

The third administrator is the former local administrator for the project. She has moved on to other work and still provides backup for the local junior administrator and some additional support for the third-party application program that is on the server, but she no longer tends to these machines except in special circumstances. The local junior admin is the primary point of contact and the one who tracks all access to the servers for consistency. This makes a single point of contact for control of the systems. Unfortunatelythere is not a more structured policy and procedure outline, but this is what is currently available for this project..

F. Backup/Disaster Recovery

The institution to which this department belongs has some overall policies that govern backups and disaster recovery. Only weekly incremental backups are run on the systems in this department. There are relatively few changes on the cluster as the database and primary application are more of an archival resource than a working, changing repository. The weekly backups are stored in a different building on-site at this institution in the offices of the network support staff. The backup tapes are checked approximately once every 4-6 months to ensure that there are readable tapes in the backup stock. There is very little data loss that is critical outside of the weekly changes. Full level 0 backups are performed monthly.

The primary archive for the database application and the local third-party application program are stored on a large RAID drive. For most purposes, the RAID array is sufficient to prevent data loss, but we have had to restore from backups once when two of the RAID devices failed and hence there was data loss. The backup tapes were available and readable for a successful restoration.

The disaster recovery plan is actually for the department in general. Spare systems are available to replace the servers in the event of a server crash or damage; and as mentioned above, the backups are stored off-site in another building and can be retrieved easily to restore to one of the backup systems. The physical facilities have automatic fire suppression systems and there are rolls of large plastic sheeting that are designed to be pulled and placed over system equipment to protect them from the fire-suppression system.

The building has a generator for backup power should it be needed. Additionally, the servers are all on UPS systems with about 30 minutes of battery storage when not powered. The institution maintains the generators in the buildings on-site and there are semi-annual planned switchovers from city power to the building generators to test that power switch-overs function correctly.

G. Physical Security

The servers are all housed in a large server room with cinder block and concrete walls. There are solid doors that are only key-locked (no electronic locks). There are a limited number of keys to the room, although the limited number is high as there are a significant number of project staff who work in the computer facilities room (approximately 8). The doors are always locked when no staff member is in the room. The facility has a raised floor that is completely internal to the room (the floor under the raised floor is the same level as the floor in the hallways outside the room and the cinder block walls come down to the real floor.

The building has card-key access only for after hours (the card key main doors are open during the business day). These doors fail closed in the event of power loss but there is a release on the inside of the door which will allow the door to be opened from the inside (when this happens the door will no longer lock until someone reengages the release from the inside. The card-key doors are made of thick shatter-resistant glass (or so they are advertised).

III. ISS Scan Results

Network Vulnerability Assessment Report – Sorted by Vulnerability Severity

Report Description

This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilitys and suggests corrective action. Vulnerabilities are classified as high, medium, and low. High risk vulnerabilities are those which provide unauthorized access to the host, and possibly the network.

Session Name:	Security_Scan_XXX	**Session ID:**	11
File Name:	Security Scan XXX_000710	**Template:**	Security Scan Tmp
Comment:	Security Scan XXX	**Termination Status:**	Finished
Scan Summary Information			
Hosts Scanned:	31	**Scan Start:**	2000/07/10 16:09:10
Hosts Active:	15	**Scan End:**	2000/07/10 18:12:02
Hosts Inactive:	16	**Elapsed:**	02:02:52

Vulnerability Name	**Severity**
CDE rpc.ttdbserver daemon allows remote root access	**High**

Description

ToolTalk is a utility that allows applications to exchange messages between each other. A stack overflow in the rpc.ttdbserver could allow a remote attacker to execute arbitrary code with root privileges.

IP Address	DNS Name	Associated Info	Session ID
192.168.111.222	server1.gsfc.nasa.gov		11
[other hosts omitted]			

Vulnerability Name	**Severity**
Guessable NFS filehandles	**High**

Description

The NFS Guess vulnerability was found, which allows an attacker to access the file system, bypassing mountd security by guessing file handle.

IP Address	DNS Name	Associated Info	Session ID
192.168.111.222	server1.gsfc.nasa.gov		11

Vulnerability Name	Severity
NFS portmapper export	**High**

Description

NFS was found to be mountable via portmapper. An attacker can mount the system through the portmapper, gaining access to a restricted host. To the portmapper it seems as if the local host is mounting, since the local host is permitted to mount itself.

IP Address	DNS Name	Associated Info	Session ID
192.168.111.222	server1.gsfc.nasa.gov		11

Vulnerability Name	Severity
NFS writable	**High**

Description

An NFS export was found to be writable by anyone. An attacker could modify any files on this system.

IP Address	DNS Name	Associated Info	Session ID
192.168.111.222	server1.gsfc.nasa.gov	/home/oracle/rdbms/log	11
192.168.111.222	server1.gsfc.nasa.gov	/home/oracle/rdbms/doc	11
192.168.111.222	server1.gsfc.nasa.gov	/home/oracle/rdbms/mesg	11
192.168.111.222	server1.gsfc.nasa.gov	/home/oracle/rdbms/man	11
192.168.111.222	server1.gsfc.nasa.gov	/home/oracle/rdbms	11
[additional similar lines omitted]			

Vulnerability Name	Severity
Open X Display	**High**

Description

Open X Displays allow an attacket to capture keystrokes and to execute commands remotely. Many users have their X Server set to xhost +, permitting access to the X Server by anyone, from anywhere.

IP Address	DNS Name	Associated Info	Session ID
192.168.111.222	server1.gsfc.nasa.gov		11

Vulnerability Name	Severity
RPC statd remote file creation and removal	**High**

Description

A remote rpc.lockd can provide false information to the rpc.statd file, allowing a file to be removed or created. RPC.statd maintains state information in cooperation with RPC.lockd, to provide crash and recovery functionality for file locking across NFS. Because statd does not validate the information it receives from the remote lockd, an attacker can send a remote procedure call, resulting in the creation or removal of any file on the system.

Most machines presently running NFS can allow remote removal of a file, Internet Scanner can only determine if statd is possibly vulnerable to the attack. To conclusively determine a system's vulnerability before patching it, check the system for the file /tmp/statd-vulnerable. If this file exists after a scan, then the machine is vulnerable to attack.

IP Address	DNS Name	Associated Info	Session ID
192.168.111.222	server1.gsfc.nasa.gov		11

Vulnerability Name	Severity
RPC.ypupdated daemon allows remote commands execution as root	**High**

Description

The NIS update daemon rpc.ypupdated contains a vulnerability in how it passes commands to certain function calls, which allows a remote attacker to trick the service into executing arbitrary commands on the system with root privileges. Exploit information for this hole has been made widely available.

IP Address	DNS Name	Associated Info	Session ID
192.168.111.222	server1.gsfc.nasa.gov		11

Vulnerability Name	Severity
Sendmail daemon outdated	**High**

Description

The Sendmail version on the machine is no longer actively supported. All versions of Sendmail prior to 8.7.0 are considered vulnerable. This vulnerability is derived from the version string in the Sendmail banner.

IP Address	DNS Name	Associated Info	Session ID
192.168.111.222	server1.gsfc.nasa.gov		11

Vulnerability Name	Severity
Sendmail remote execution	**High**

Description

The Sendmail program allows commands to be remotely executed. An attacker can gain access through Sendmail and execute commands on the system.

IP Address	DNS Name	Associated Info	Session ID
192.168.111.222	server1.gsfc.nasa.gov		11

Vulnerability Name	Severity
X11 MIT-MAGIC-COOKIE-1 prediction could allow remote access to arbitrary X-Session	**High**

Description

A vulnerability exists in some implementations of X11 that rely on MIT-MAGIC-COOKIE-1 for security, allowing a remote attacker access to arbitrary X sessions. The vulnerability affects sites using xdm for generating keys when xdm has not been compiled to use XDM-AUTHORIZATION-1. The keys produced by xdm will be cryptographically insecure and easily guessable.

IP Address	DNS Name	Associated Info	Session ID
192.168.111.222	server1.gsfc.nasa.gov		11

III. ISS Scan Results

A. Discussion of Scan Results

The ISS scan was run as part of this department's internal Security audit. The listing above includes the output regarding **server1**. The following section discusses those items that were fixed based on the ISS scan results. The next section will discuss those vulnerabilities that have not been fixed (dealing with known security vulnerabilities).

CDE rpc.ttdbserver daemon allows remote root access

As mentioned before, the portmapper and RPC-based services have been culled down to the minimum necessary, but some RPC-based services are still required on this system. Until the system can be scheduled for the full Operating System re-install, these services will have to remain in use as is. This vulnerability is currently covered by the domain gateway as no TCP/IP traffic can be sent to any port on the cluster hosts except from select hosts outside the domain.

CDE rpc.ttdbserver daemon allows remote root access (CONT)
After the upgrade, the system will be using Sun's Secure-RPC and should be less vulnerable to this type of attack.

Guessable NFS filehandles
After the scan, the Sun NFS Jumbo patch was acquired and installed. Using the new fsirand utility was used to help make the system less vulnerable. This recommendation came with the ISS scanner package and was the recommended fix for this vulnerability.

NFS portmapper export
NFS writable
After the scan, the /etc/exports file on all systems in the cluster were reviewed and significantly culled for only those file systems that were absolutely necessary. Most remaining file systems were exported read-only with only a limited number of read-write file systems which were exported to only those client hosts that required them.

Open X Display
The system was reviewed and all xhost commands were changed to *"xhost –"* for all users. Additionally, all users who have standard shell access have been informed not to modify this. Most users of the system log into a captured shell account which does not grant them shell access and cannot change this. There is a script that actively checks for the string *"xhost +"* in any . (dot) file in any home directory.

RPC statd remote file creation and removal
The patch #100988-05 was acquired from Sunsolve as recommended by ISS. This patch was installed as recommended and eliminated the remote file creation problem. Although this error still arises when a scan is run, the target file is no longer created from an ISS scan.

RPC.ypupdated daemon allows remote commands execution as root
Unfortunately, no patch from Sun has been registered at Sunsolve for SunOS. This problem will be handled when the Operating System is upgraded. Sun is no longer issuing solutions for SunOS only Solaris products.

Sendmail daemon outdated
Sendmail remote execution
Sendmail has been disabled and commented out in rc.local on all the client machines. This machine as the server is the only machine that retains sendmail locally. The version of sendmail is one of the 8.7 subversions of sendmail, although the version string was modified to be something for the administration team, it is not identifiable relative to the sendmail versions. A patch to remove the pipe interpretation in sendmail was implemented and this version is no longer susceptible to that bug. At this point, mail can be sent and received locally within the cluster and from those select hosts that are allowed through the domain gateway. When the server is updated to Solaris 2.7, a newer version of sendmail will be acquired.

X11 MIT-MAGIC-COOKIE-1 prediction could allow remote access to arbitrary X-Session
This vulnerability has not been repaired. The recommendation is to upgrade to X11R6.1 or later and this cannot be done due to time restraints. The latest version of X11 will be installed under the new operating system.

ISS Scan Results (CONT)

Discussion of Scan Results (CONT)

The ISS scan helped identify a number of significant security vulnerabilities. Those that could be dealt with were resolved. Many are still outstanding. At this point, the administration team is at least aware of the most serious security vulnerabilities to the system. The administrators keep scanning the system for signs of intrusion. And the system will be monitored seriously until such time as the operating system upgrade can be performed.

B. Known Security Vulnerabilities

ISS has identified the most serious security vulnerabilities. Additional vulnerabilities are apparent from the discussions in various security classes attended by the administration staff (including the SANS Security Conference 2000 in Washington DC). The administration team is aware that the following are significant vulnerabilities to be monitored until such time as the system will be upgraded to a later version of the operating system:

- RPC-based attacks
- Sendmail-based attacks
- Unusual traffic to/from the hosts (monitored by the network support team via the Cisco routers
- NFS based intrusion
- NIS based intrusion

Additionally, there is no encryption based data transfer applications in place for this system (e.g. SSH or related products). All data transfer to the systems are through unencrypted TCP/IP traffic. The administration team is aware of this vulnerability and will address the issue in the future.

IV. Recommended Fixes and Short Term Plan

The administration team supporting this server and cluster are aware of the potential problems. As time allows, the team will continue to implement those patches and security toolkit utilities that can be performed in the maintenance windows allowed. Amongst the plans are plans to acquire a later version of sendmail, acquire additional patches for some of the problems addressed by ISS and to continue to try to lock down the NIS and NFS type vulnerabilities. Crack will be acquired to test the users passwords for guessability.

V. Long Term Plan

As soon as the mission-critical status of the applications permit (due to the on-set of a major deadline late in 2001, this will be required by early 2001 at the latest), the operating system will be upgraded to Solaris 2.7 (already purchased and awaiting upgrade). Several other systems in the cluster were already upgraded and the licenses were purchased before the shipping of Solaris 8. After the operating system upgrade, the installation guide supplied at the SANS Security Conference (*Solaris Security: Step-by-Step*) will be used to provide a configuration guideline. New versions of sendmail, wu-ftpd, TCP-wrappers will all be installed. The system will ultimately be tripwired. Crack will be acquired and run on a routine basis. Passwd+ and npasswd will be evaluated for a potential implementation on this system. The network support team will continue to run the commercial version of ISS on a routine basis to determine the level of vulnerability to the system.

VI. References

The author continually refers to a whole shelf of references in perfomring Sun system administration. Those include (but are not limited to):

1. Unix System Administration Handbook (both versions 1/yellow and 2/red)
   Nemeth, Snyder, Seebass, Hein
2. Essential System Administration (the O'Reilly book)
   Frisch
3. Sendmail (O'Reilly)
   Allman
4. Class materials from LISA '94, '95, '96 (Usenix)
5. Class materials from SANS '00
6. Class materials from additional security classes
   (The author formerly taught Unix System Administration, Unix System Security and Security Toolkit courses for one of the FIRST organizations and still retains a number of the materials he contributed to while in that position—the name of the FIRST organization has been "sanitized" to help maintain anonymity of the author's organization)

These are the primary resources used by the system administration team for maintaining the system/cluster and for producing this report.