Auditing a Sun Solaris 8 Technology Distribution Server: An Auditors Perspective

GSNA Practical Version 2.1

Author: Scott P. Cassidy

Date: 7 November 2003

Table of Contents

Table of Figures

List of Tables

1 Assignment 1 - Research in Audit, Measurement Practice, and Control

1.1 Identify the system to be audited

The focus of this audit will be the technology distribution server (hereafter referred to as the TDS) for Wobulators Inc. Wobulators Inc. is a manufacturer of computer-controlled wobulation systems with a corporate headquarters located in New York City. Wobulators Inc. also has Wobulator manufacturing plants located in Mexico City, Mexico, Berlin, Germany and Tokyo, Japan.

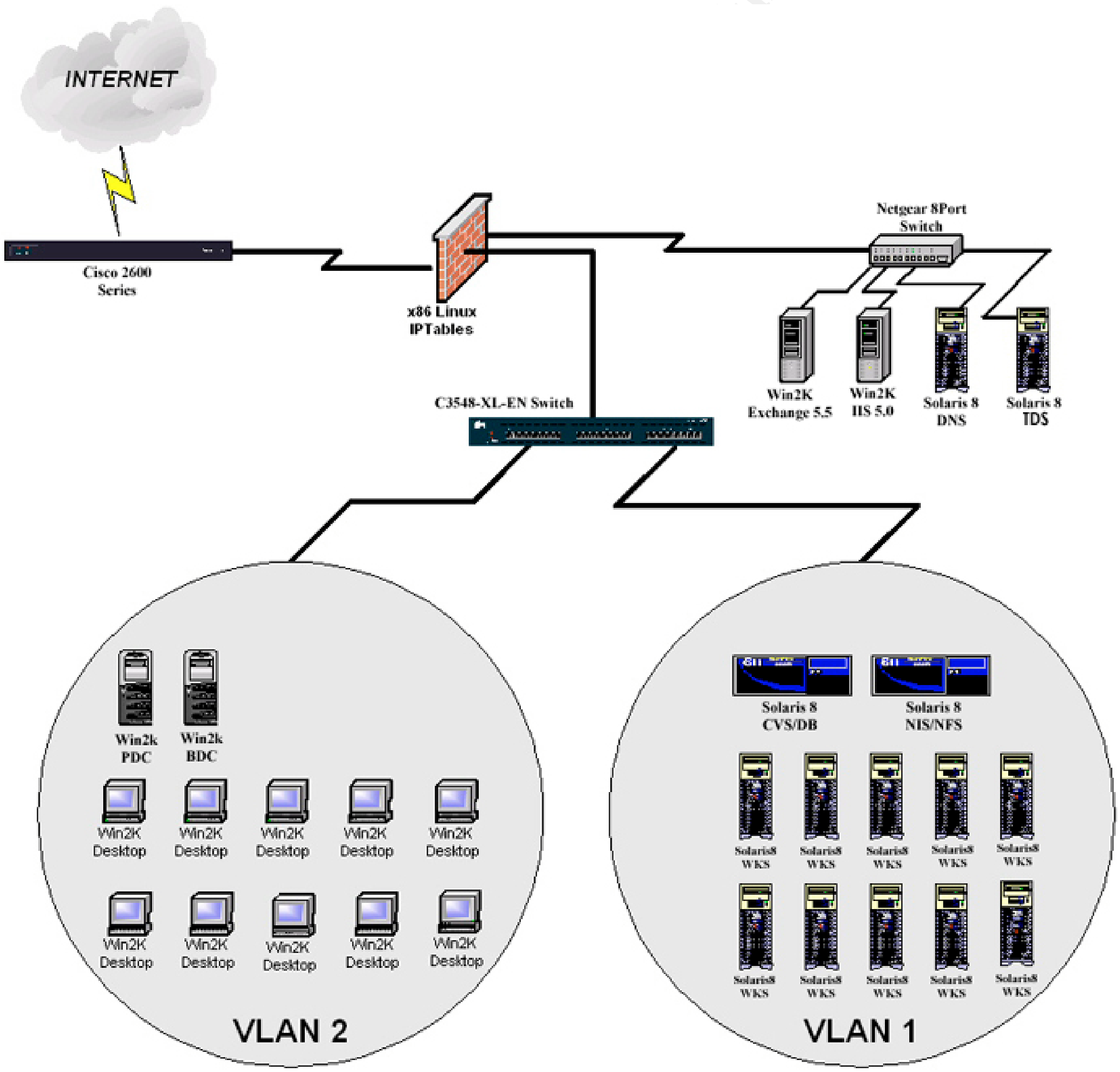
As part of a modernization effort by Wobulators Inc. management, a plan was established to upgrade the distribution of the Wobulator engineering plans and software. The focus of the effort is to improve cost, efficiency, and delivery time of new technical documents and software to the manufacturing plants. Traditionally the Wobulator technical plans and updated revisions of the Wobulator Operating System (WOS) were distributed on CDROM via common carrier to the Wobulator Inc. manufacturing facilities.

The market for Wobulators is very competitive and the crown jewels of any Wobulator manufacturing firm is its design work and software. With this in mind I was hired by Wobulators Inc. to ensure that their new TDS installation conformed to the companies desire for system security and addressed to the greatest degree possible their concerns about protecting their Wobulator engineering documentation and software.

Wobulators Inc. maintains a network for day-to-day business and engineering functions at its New York City offices. The business network is comprised of two Windows 2000 Servers (PDC and BDC) and 10 Windows 2000 Professional Desktops utilized for standard office file and print services, The engineering network consisting of 10 Sun Ultra 10 Workstations running Sun Solaris 8, utilized for engineering and software development, and two Sun Enterprise 250R servers also running Sun Solaris 8 that are utilized for file storage for engineering documents, CVS, a technical support database, and a NIS/NFS infrastructure. The network is connected to the Internet via a Fractional T-1 Frame Relay line provided by BARFCONET. The Fractional T-1 Frame Relay line is terminated at a Cisco 2600 series router that connects to a X86 system running RedHat Linux/IPTables that firewalls the network and segments it into three distinct zones (EXTERNAL-NET, INTERNAL-NET, and DMZ) and provides network address translation for the internal business network.

The Wobulators Inc. administrative personnel recently installed the TDS into the Wobulators Inc. DMZ. Also located in the Wobulators Inc. DMZ is an Exchange 5.5 server providing company email and groupware functions, a Windows 2000 server running IIS 5.0 serving the Wobulators Inc. website and a Sun Ultra 10 running Solaris 8 performing DNS services for the network. All of the systems within the DMZ are connected via 100BaseT 802.3 Ethernet to an unmanaged Netgear 8 port Ethernet switch connected directly to the DMZ leg of the firewall. The systems within the DMZ as well as the router, firewall, and associated UPS units are located in a physically secure, locked room within the Wobulators Inc. offices. Access to the network room is controlled via a steel door equipped with a cipher lock. The combination of the cipher lock is known only to a small handful of individuals within the company.

Figure 1. Wobulators Inc. NYC Office Network



The TDS itself is comprised of a Sun Microsystems Ultra 10 computer running the Solaris 8 operating system. The mechanism selected to perform the data transfers is the standard Solaris file transfer protocol (ftpd) server. The reasons stated for this choice were familiarity of the staff with administration of the Solaris ftp daemon, and the widespread availability of ftp client software for multiple platforms, cost effectiveness (the ftp server comes with the operating system release), and the fact that the Wobulators Inc. firewall was already configured to allow inbound ftp access to the DMZ for the purpose of permitting the Wobulators Inc. website developer to post updates to the Windows 2000 IIS server.

Updates to engineering documents and WOS are published once per month on average. Engineers burn the technical documents and WOS updates to CDROM once the head engineer signs them off for release to the manufacturing plants. The CDROM containing the release then has a control number applied to it, it is cataloged, and the updates are posted to the TDS via "Sneaker-Net". After the updates are posted to the TDS, the previous release is deleted from the system and the CDROM media containing the new release is archived in a safe located in the engineering office. This method was implemented for accountability purposes.

1.2 Evaluate the risk to the system

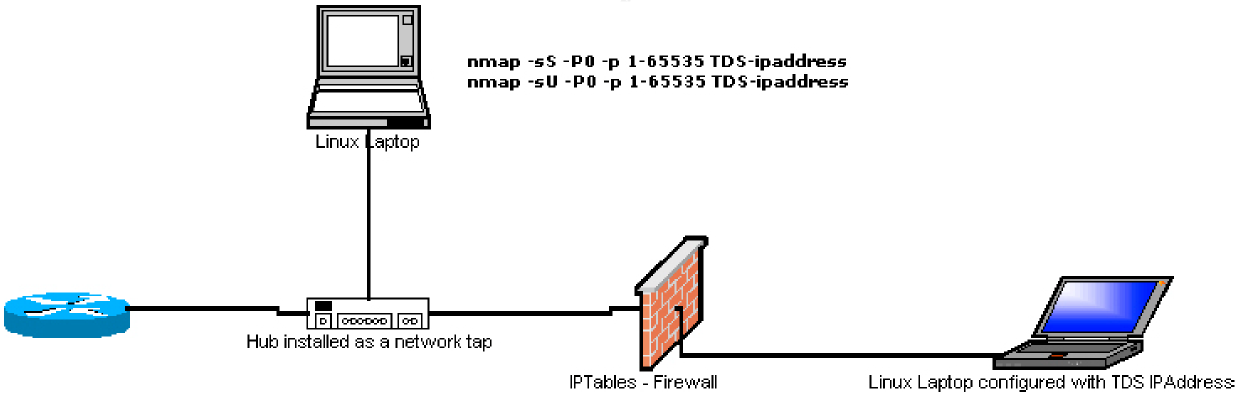
After conducting an initial site visit that consisted of personnel interviews, a network diagram review, and a technical walkthrough, it was apparrent that the Wobulators Inc. staff were security conscious, but were limited by staff technical knowledge, time, and monetary resources. There were no full time network administrators on staff. IT administrative duties were split between one of the Wobulator engineers that handled the Solaris administration for the technical network, and a technically savvy "computer buff" individual from the marketing department that maintained the small Windows 2000 office network. All network engineering and anything outside the scope of day-to-day administrative duties has been farmed out to a long list of technical consultants.

The scope of my audit was limited to the TDS itself, but network environment greatly impacts the security posture of the TDS, so an overview of the Wobulators internet facing network environment was conducted.

The perimeter router was leased from BARFCONET. The router was shipped preconfigured, and its configuration is not modifiable under the usage agreement for Wobulators Inc. It appears that the router is passing all inbound and outbound traffic, and thus is offering little or no protection in the form of network ingress and egress control. Without the benefit of a screening router at the network perimeter, the risks to the internet facing systems on the Wobulators Inc. network are increased. This is because any vulnerabilities on Internet facing systems will have an exposure of those vulnerabilites to publicly routed networks, and an increased potential for exploit. In turn there is an increased probability for attack, denial of service, or loss of any intellectual property / data housed on Wobulators Inc. Internet facing systems and the TDS itself.

A review of the IPTables/Firewall configuration is outside the scope of this audit. However, it is important to gain an understanding of the type network traffic the TDS has exposure to so that risks to the system can be accurately gauged. With this in mind, a Linux laptop was situated between the border router and the firewall and another Linux laptop temporarrily temporary setup within the DMZ configured with the IP Address of the TDS. Figure 2. displays the configuration used to check the TDS network traffic exposure, and Table 1. displays the findings as verified by an nmap scan from the network tap outside the firewall and another laptop temporarily configured with the TDS IP address running tethereal (in a classic catcher-pitcher configuration).

Figure 2. Configuration for Verification of TDS Network Traffic Exposure.



```
nmap -sS -P0 -p 1-65535 TDS-ipaddress
nmap -sU -P0 -p 1-65535 TDS-ipaddress
```

Linux Laptop
Hub installed as a network tap
IPTables - Firewall
Linux Laptop configured with TDS IPAddress

Table 1. Network Traffic Exposure / Resulting Potential Risks Posed to the TDS

Service	TCP/ UDP Port	Notes	Service/Protocol Required for TDS Operation	Existing / Potential / Overall Risks
ftp (Active)	20,21 TCP/ UDP	Used for posting of website updates to www server, and data transfer for TDS	Active ftp is required for TDS operation.	**Existing Risks:** The ftp server running on the TDS has full exposure to the internet. Any security issues found with this server have a high probability of exploit. At any point in the route in-between the ftp client and the TDS there exists the potential for the compromise of account credentials for the remote TDS user, or of company data because credentials and data transfer for the ftp protocol traverse the network in the clear.

Service	TCP/ UDP Port	Notes	Service/Protocol Required for TDS Operation	Existing / Potential / Overall Risks
				Additionally, OS fingerprinting is probable from default ftp daemon banners, providing information that can be utilized for a more targeted attack on the system. **Potential Risks:** Any of these situations can lead to unauthorized access/use of the TDS or other Wobulators Inc. systems if the TDS user credentials are shared with other systems. An exploit would more than likely result in the compromise of company intellectual property. **Overall Risks:** The likelihood of a security incident resulting from this exposure is considered to be relatively high.
Telnet	23 TCP/ UDP	Used for remote administration of DNS server.	Telnet is not required for normal operation of the TDS. (system administration is performed from the system console)	**Existing Risks:** The Telnet server running on the TDS has full exposure to the internet. Any security issues found with this server have a high probability of exploit. At any point in the route in-between the telnet client and the TDS there exists the potential for the compromise of account credentials for the remote TDS user, or of company data because credentials and data transfer for the telnet protocol traverse the network in the clear. Additionally, OS fingerprinting is probable from default telnet daemon banners, providing information that can be utilized for a more targeted attack on the system. **Potential Risks:** Any of these situations can lead to unauthorized access/use of the TDS or other Wobulators Inc. systems if the TDS user credentials are shared with other systems. An exploit would more than likely result in the compromise of company intellectual property. **Overall Risks:** The likelihood of a security incident resulting from this exposure is considered to be relatively high.
SMTP	25 TCP/ UDP	Utilized by Exchange server for mail transfer	SMTP is not required for normal operation of the TDS. The TDS is not used for mail services or mail relay.	**Existing Risks:** The Sendmail server running on the TDS has full exposure to the internet. Any security issues found with this server have a high probability of exploit. At any point in the route in-between an smtp client and the TDS there exists the potential for the compromise of account credentials for the remote TDS user, or of company data because credentials and data transfer for the smtp protocol traverse the network in the clear. Additionally, OS fingerprinting is probable from default smtp daemon banners, providing information that can be utilized for a more targeted attack on the system.

Service	TCP/ UDP Port	Notes	Service/Protocol Required for TDS Operation	Existing / Potential / Overall Risks
				Potential Risks: Any of these situations can lead to unauthorized access/use of the TDS or other Wobulators Inc. systems if the credentials are shared with other systems, or the compromise of company intellectual property. **Overall Risks:** The likelihood of a security incident resulting from this exposure is considered to be relatively high.
DNS	53 TCP/ UDP	Standard Name to IP resolution for wobulators.com domain	Domain Name Services are not required for normal operation of the TDS.	**Existing Risks:** None **Potential Risks:** If a DNS server is running on the TDS it will have full exposure to the internet. Any security issues found with this server has a high probability of exploit unless diligence is maintained in regard to applying security patches. There have been numerous serious remotely exploitable issues with bind on Solaris. This situation could lead to unauthorized access/use of the TDS or other Wobulators Inc. systems, or the compromise of company intellectual property. **Overall Risks:** At the current time, because of the absence of a DNS server on the system the risk is considered to be negligible. The likelihood of a security incident resulting from this exposure would be considered relatively high if a DNS server were implemented in the future on the TDS.
HTTP	80 TCP/ UDP	Used for standard HTTP website traffic	Web Services are not required for normal operation of the TDS.	**Existing Risks:** The HTTP server running on port 80 of the TDS has full exposure to the internet. Any security issues found with this server have a high probability of exploit. If there were an existing or future remotely exploitable issue with apache or any other web server (on port 80) running on the TDS, a situation exists that could lead to unauthorized access/use of the TDS or other Wobulators Inc. systems, or the compromise of company intellectual property. **Potential Risks:** Any security issues with the web server can lead to unauthorized access/use of the TDS or other Wobulators Inc. Systems. An exploit of the TDS web server would more than likely result in the compromise of company intellectual property. **Overall Risks:** The likelihood of a security incident resulting from this exposure is considered to be of medium-high risk.
POP3	110 TCP/ UDP	Utilized by Exchange server for mail transfer	POP3 services are not required for normal operation of the TDS.	**Existing Risks:** None **Potential Risks:** If a POP server were running on port 110 of the TDS it would have full exposure to the

Service	TCP/ UDP Port	Notes	Service/Protocol Required for TDS Operation	Existing / Potential / Overall Risks
				internet. Any security issues found with this server has a high probability of exploit unless diligence is maintained in regard to applying security patches. If there were an existing or future, remotely exploitable security issue with a POP server that were configured to run on the TDS, this situation could lead to unauthorized access/use of the TDS or other Wobulators Inc. systems, or the compromise of company intellectual property. **Overall Risks:** At the current time, because of the absence of a POP3 server on the system the risk is considered to be negligible. The likelihood of a security incident resulting from this exposure is considered to be relatively high if a POP3 server is implemented in the future on the TDS.
MS RPC	135 TCP/ UDP	Utilized by Exchange server for support of Outlook Clients	MSRPC services are not required for the normal operation of the TDS.	**Existing Risks:** None **Potential Risks:** There is not currently s samba server running on the TDS. While samba is not vulnerable to attacks against Microsoft based RPC services, if a remote exploit were found for samba, there exists the potential for unauthorized access/use of the TDS or other Wobulators Inc. systems, or the compromise of company intellectual property. **Overall Risks:** At the current time, because the TDS is a Solaris based system and the absence of a samba server the risk is considered to be negligible.
IMAP	143 TCP/ UDP	Utilized by Exchange server for mail transfer	IMAP services are not required for the normal operation of the TDS.	**Existing Risks:** None **Potential Risks:** If an IMAP server were running on port 143 of the TDS it would have full exposure to the internet. Any security issues found with this server has a high probability of exploit unless diligence is maintained in regard to applying security patches. If there were an existing or future, remotely exploitable security issue with a IMAP server running on the TDS, this situation could lead to unauthorized access/use of the TDS or other Wobulators Inc. systems, or the compromise of company intellectual property. **Overall Risks:** At the current time, because of the absence of an IMAP server on the system, the risk is considered to be negligible. The likelihood of a security incident resulting from this exposure is considered to be none.
LDAP	379,389, 636, 3268 TCP/ UDP	Utilized by Exchange server for support of Outlook Clients	LDAP services are not required for normal operation of the TDS.	**Existing Risks:** None **Potential Risks:** If an LDAP server were running on the TDS it would have full exposure to the internet. Any security issues found with this server would have a high probability of exploit unless diligence is

Service	TCP/ UDP Port	Notes	Service/Protocol Required for TDS Operation	Existing / Potential / Overall Risks
				maintained in regard to applying security patches and directory configurations. At any point in the along the route between the LDAP client and the LDAP server TDS there exists the potential for the compromise of account credentials for the remote TDS user, unless TLS is utilized on the LDAP server. If there were an existing or future remotely exploitable issue with an LDAP server running on the TDS, this situation could lead to unauthorized access/use of the TDS or other Wobulators Inc. systems, or the compromise of company intellectual property. **Overall Risks:** At the current time, because of the absence of an LDAP server on the system, the risk is considered to be negligible. The likelihood of a security incident resulting from this exposure is considered to be none.
HTTPS	443 TCP/ UDP	Utilized by Exchange server for support of Outlook Web Access Clients	HTTPS services are not required for normal operation of the TDS.	**Existing Risks:** None **Potential Risks:** If an HTTPS server were running on port 443 of the TDS it would have full exposure to the internet. Any security issues found with this server would have a high probability of exploit. If there were an existing or future remotely exploitable issue with apache or any other web server running on the TDS, this situation could lead to unauthorized access/use of the TDS or other Wobulators Inc. systems, or the compromise of company intellectual property. **Overall Risks:** At the current time, because of the absence of an HTTPS server on the system, the risk is considered to be negligible. The likelihood of a security incident resulting from this exposure is considered to be none.
SMTP (SSL)	465 TCP/ UDP	Utilized by Exchange server for support of Outlook Web Access Clients	SMTP (SSL) services are not required for normal operation of the TDS.	**Existing Risks:** None **Potential Risks:** If a SMTP (SSL) l server were running on the TDS it would have full exposure to the internet. Any security issues found with this server would have a high probability of exploit. This situation could lead to unauthorized access/use of the TDS or other Wobulators Inc. Systems if the credentials are shared with other systems, or the compromise of company intellectual property. **Overall Risks:** At the current time, because of the absence of an SMTP (SSL) server on the system, the risk is considered to be negligible. The likelihood of a security incident resulting from this exposure is considered to be none.

Service	TCP/ UDP Port	Notes	Service/Protocol Required for TDS Operation	Existing / Potential / Overall Risks
LSA	691 TCP/ UDP	Utilized by Exchange server for support of Outlook/ Outlook Web Access Clients	LSA services are not required for normal operation of the TDS.	**Overall Risks:** No current or future risk is posed to the TDS or to Wobulators Inc. from this exposure. (Windows specific protocol)
IMAP4 (SSL)	993 TCP/ UDP	Utilized by Exchange server for support of Outlook /Outlook Web Access Clients	IMAP (SSL) is not required for normal operation of the TDS.	**Existing Risks:** None **Potential Risks:** If an IMAP server were running on the TDS it would have full exposure to the internet. Any security issues found with this server have a high probability of exploit unless diligence is maintained in regard to applying security patches, and access control precautions such as TCP_Wrappers are configured on the system. This situation could lead to unauthorized access/use of the TDS or other Wobulators Inc. Systems if the credentials are shared with other systems, or the compromise of company intellectual property. **Overall Risks:** At the current time, because of the absence of an IMAP4 (SSL) server on the system, the risk is considered to be negligible. The likelihood of a security incident resulting from this exposure is considered to be none.
POP3 (SSL)	995 TCP/ UDP	Utilized by Exchange server for support of Outlook /Outlook Web Access Clients	POP3 (SSL) is not required for normal operation of the TDS.	**Existing Risks:** None **Potential Risks:** If a POP (SSL) server were running on the TDS it would have full exposure to the internet. Any security issues found with this server have a high probability of exploit unless diligence is maintained in regard to applying security patches, and access control precautions such as TCP_Wrappers are configured on the system. This situation could lead to unauthorized access/use of the TDS or other Wobulators Inc. Systems if the credentials are shared with other systems, or the compromise of company intellectual property. **Overall Risks:** At the current time, because of the absence of a POP3 (SSL) server on the system, the risk is considered to be negligible. The likelihood of a security incident resulting from this exposure is considered to be none.

Service	TCP/ UDP Port	Notes	Service/Protocol Required for TDS Operation	Existing / Potential / Overall Risks
MAPI	5001, 5002, 5003 TCP/ UDP	Utilized by Exchange server for support of Outlook /Outlook Web Access Clients	No current Risk posed to the TDS	**Overall Risks:** No current or future risk is posed to the TDS or to Wobulators Inc. from this exposure. (Windows specific protocol)

Due to the high degree of exposure to exterraneous network traffic traversing the Wobulators Inc. DMZ, there is a greater risk of exploit incurred by the TDS if any unnesessary network services are running on the system. This is especially true if the system is not current on vendor supplied operating system security patches.

The TDS also gains risk exposure from the other systems within the DMZ. If another system within the DMZ becomes compromised, the compromised system can be utilized to collect account credentials by conducting a layer 2 attack against the DMZ switch, and then routing all DMZ traffic through the compromised system allowing the attacker to harvest the cleartext account credentials from legitimate ftp or telnet sessions conducted as part of normal TDS operations. The Exchange, IIS, and Bind servers also located in the DMZ are high risk, high value targets for a potential attacker. If one of these systems became compromised all systems within the DMZ could fall successively. The attacker could reroute http requests, deface the Wobulators Inc. website, obtain sensitive emails, and any intellectual property housed on the TDS. This situation could result in a high profile incident discrediting the company, or worse, a low profile compromise of crown jewel intellectual property. Either way an incident of this nature can be devastating to Wobulators Inc.

If local TDS user account data can be garnered from an SMTP server on the system, or obtained from account names that were shared across systems or not properly protected by users/administrators the system could also be vulnerable to a brute force attack if strong password and account policies are not maintained.

The enforcement of least privilege on the system is also imperative. Off-site employees, salesmen, and manufacturing plant workers with accounts on the TDS must be limited in privilege to the greatest degree possible. If they, or individuals in possession of their account credentials gain access to the system, there must be mechanisms in place to limit the potential for privilege escalation or further compromise of data. Additionally, the network services running on the system must also operate with the least amount of privilege possible, and in a chrooted (jail) environment if supported. This would limit the damage incurred by any successful attacks against these services.

If the system does not support adequate detective security controls by maintaining granular system logging and kernel level auditing, in addition to having the associated logs sufficiently protected and reviewed by the system administrators, a compromise or suspicious activity might not even be detected by the administrators for a considerable length of time, if at all.

As stated earlier, physical access to the system is strictly controlled and it would take a compromise of the physical security measures in place, or a trusted insider, to perform a physical attack against the system itself, or an attack from the system console, such as bringing the system into single user mode and effectively gaining root access to the TDS. The risk of this type of attack against the TDS is considered small, but not absent.

1.3 What is the current state of practice

Sun Solaris is a widely deployed and well-documented operating system. There is a wealth of documentation available about the secure configuration and operation of computer systems running Sun Solaris. Many universities, government agencies, and computer security organizations have formal security guides or guidance on the secure configuration of the Sun Solaris operating system. Additionally, there are a plethora of applicable books, and user websites, in addition to Sun Microsystems own website.

There is almost too much information on Solaris security, in too many places. In the past it has been difficult to collect, collate, and ensure the timeliness of all this information.

Over the past few years the Center for Internet Security (CIS) has done a tremendous job of collecting, organizing, and maintaining security information for Sun Solaris in addition to a number of other operating systems. They publish their Benchmark documents that are comprised of widely accepted best practices with input from vendors, industry, education, government and numbers of computer security organizations on a regular basis. These documents consolidate this information in a well formatted document, and they are published along with scoring tools that provide administrators and auditors with a well designed application to evaluate their Sun Solaris systems against security best practices and industry standard “prudent levels of due care”. These benchmarks are an excellent place to start when evaluating a Sun Solaris system. Particularly if the organization under evaluation does not have a security policy in place, or the system administrators are not well versed in the security aspects of the Sun Solaris operating system, as is the situation with Wobulators Inc. The CIS Benchmark document and scoring tool are available from the Center for Internet Security at http://www.cisecurity.org/.

The CIS Benchmark for Sun Solaris makes an excellent foundation for a security audit or a set of Sun Solaris hardening procedures. However, the Benchmark should be considered a foundation from which an application or server/service specific set of security procedures, or checks should be built upon. It makes no sense to have a secured/hardened operating system installation serving an insecure application to the world, or vice versa. This situation would provide a false sense of security to the system administrators. It might be beneficial for the CIS to compile additional, application specific security Benchmarks for items such as web servers, NFS, or ftp servers to address application specific security best practices in the Sun Solaris environment.

In addition to the CIS and scoring tool there is an excellent paper entitled “Solaris 8 Build Document” written by Gideon Rasmussen of Infostruct LLC. This paper is targeted at individuals wanting to build a hardened Sun Solaris server, but there is a wealth of information in it that is of great value to the system auditor. The paper is available from the SANS reading room http://www.sans.org/rr/.

Sun Microsystems also makes their Solaris Security Tool Kit (jass) freely available. This tool can be used to automatically harden Solaris servers, but can also be used as an effective auditing tool. It addresses a comprehensive list of Sun Solaris operating system security attributes, and is also well documented. The accompanying documentation also provides a wealth of security best practice information, especially the “Network Settings for Security” document which is an extensive guide on tuning Sun Solaris network parameters for security centric operation. The jass application along with a wide assortment of security guidance and papers is available at the Sun Blueprints website located at:

http://www.sun.com/solutions/blueprints/online.html

Another best bet for auditing guidelines for Sun Solaris when there is an absence of organizational security policy is the System Administrators Guild Guide “Building a Solaris Host” web site:

http://sageweb.sage.org/resources/online/solaris/solaris/checklist.html#Install

This site also contains a thorough list of “best practices” for Sun Solaris that should be implemented to the greatest degree possible by all organizations. The site is also a good baseline from which to implement a security policy for Sun Solaris for your own organization.

Additionally, there are four books that have proven to be extremely useful resources for security and configuration information for Sun Solaris, and are highly recommended.

Practical Unix and Internet Security (2nd Edition)(3rd Edition now available) – By Simson Garfinkel and Gene Spafford: Copyright 1996 O’Reilly & Associates, Inc ISBN: 1-56592-148-8

Solaris Security – A concise guide to maintaining secure systems in the Solaris Environment – By Peter H. Gregory: Copyright 2000 Prentice-Hall, Inc – ISBN: 0-13-096053-5

Solaris 8 Essential Reference – (2nd Edition) – By John P. Mulligan: Copyright 2001 New Riders Publishing – ISBN: 0-7357-1007-4

Hack Proofing Sun Solaris 8 – By Wyman Miles, Ed Mitchell, F. William Lynch Technical Editor Randy Cook: Copyright 2001Syngress Publishing, Inc – ISBN: 1-928994-44-X

2 Assignment 2 – Create an Audit Checklist

Due to the fact there was no formal information security policy in place at Wobulators Inc., and the authoring of a security policy was outside the scope of this engagement, the audit of the TDS was comprised of a configuration audit of the TDS based upon sections of the CIS Benchmark for Sun Solaris as well as other “best practices” garnered from various technical sources and system/security administrative experience.

The audit checklist was presented to the Wobulators Inc. CIO and his technical staff. The checklist was reviewed, accepted, and signed off on by Wobulators Inc. representatives. It was also agreed upon that the audit would be conducted by myself, while supervised by the CIO and witnessed by the chief engineer.

The audit would focus on several key technical areas with a number of predetermined audit checks executed for each area, and the results reviewed to come to a determination of system risk. It was agreed upon that the audit checks could be satisfied via three methods in order for a determination to be made. Those three methods are outlined below.

Table 2. Methods of Determination for Audit Checks

Method	Procedure	Determination of Outcome
(**I**) Interview	Auditor conducts verbal interview with concerned administrative or technical personnel.	Response to of interview question(s) utilized by the auditor to arrive at conclusion for audit checks.
(**O**) Observation	Auditor reviews documentation, or observes the actions of personnel or environmental conditions, output of a system command, or resultant state of an action.	Auditor utilizes the action in order to make an observation, the outcome of which is used by the auditor in order to make a conclusion for an audit check.
(**A**) Analysis	Auditor performs an analysis of system behavior, output of scripts, system tests, or analyzes system configuration files.	Auditor performs a comparative or objective analysis in order to arrive at a conclusion for an audit check.

While all of the items contained within the CIS Benchmark for Solaris version 1.2.0 can be checked in an automated fashion with the associated scoring tool, Wobulators Inc. specifically asked that manual procedures be included in the checklist. This will allow them to better understand the overall audit process, allow system administrators to conduct system configuration checks on a item by item basis, and allow for manual auditing in the event there is an condition where the CIS scoring tool cannot be run, or is not permitted to be installed on the system, or is no longer actively maintained, and will not run on future versions of the Solaris operating system. Checklist items compiled from other sources or time tested security best practices will also have manual verification procedures documented.

Table 3. Security Audit Checklist

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	**Expected Result**	**Eval**	**Associated Risk**
AC1: Ensure All Applicable Operating System Security Patches Are Installed **OC:** System must have all current vendor supplied operating system security patches installed. **CP:** (1) Compare the output of a **showrev –p** against the most current patch report section “Solaris 8 Patches Containing Security Fixes” available from www.sunsolv.sun.com. (2) If available run either the patcheck.pl or PatchManager application to perform this comparative automatically. **SC:** Solaris Benchmark V1.2.0 Section 1.1, Hack Proofing Sun Solaris 8 p 13-14	Solaris Installation should have all vendor supplied operating system security patches installed for all packages installed on the system.	**O/A**	Not having all vendor supplied operating system security patches installed leaves the system vulnerable to well known and often widely exploited security vulnerabilities.
AC2: Verify Use and Proper Operation of TCP Wrappers **OC:** Verify that the TCP Wrappers application is installed, properly configured and operational on the system. **CP:** Check for the existence of /etc/hosts.allow and /etc/hosts.deny. Ensure that the /etc/hosts.deny file contains a single ALL:ALL entry notating a deny by default posture. Review the /etc/hosts.allow file and ensure that the file contains only a list of hosts either by IP version 4 address or conical domain name that are explicitly allowed to connect to the host on a service by service bases. Verify the network services started by inetd are wrapped by verifying they are started from tcpd in /etc/inet/inetd.conf For example: ftp stream tcp6 nowait root **/usr/sbin/tcpd** in.ftpd Configure a test system to reside outside the IP address range defined in /etc/hosts.allow and attempt to make a connection to the ftp server running on the TDS. The connection attempt should be refused. **SC:** Solaris Benchmark V1.2.0 Section 1.2, Solaris Security p 168-169, Solaris 8 Build Document p 52	The /etc/hosts.allow and the /etc/hosts.deny file should contain the appropriate entries. All tcp network services controlled by inetd should configure to be called from the TCP Wrappers binary (tcpd).	**O/A**	Without TCP Wrappers restricting access to the network services via IP address or conical name, the TCP based services are vulnerable to attack by unauthorized systems.

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	**Expected Result**	**Eval**	**Associated Risk**
AC3: Determine if Secure Shell (SSH) is Installed and Operational. **OC:** Verify the installation of the secure shell (SSH) **CP:** Execute the following commands as root: # ps –e | grep sshd # pkginfo –l | grep openssh Just in case the ssh daemon was not installed via a Solaris package, we can also check for a startup script and remotely for sshd. # ls /etc/rc2.d | grep ssh If this command returns nothing there is not an ssh startup script in /etc/rc2.d Next conduct a scan from a remote host using nmap to see if the ssh daemon is listening: nmap –p22 XXX.XXX.XXX.XXX (IP Address of target) **SC:** Solaris Benchmark V1.2.0 Section 1.3, Hackproofing Sun Solaris 8 p 189 - 192	Secure Shell (SSH) should be installed and operational on the system	**O/A**	Not utilizing ssh in place of traditional network services such as rexec, rlogin, telnet and ftp can allow for compromise of system credentials or sensitive data because they are passed in the clear over the network. Systems running these older services are also vulnerable to impersonation.
AC4: Verify the Minimization of all Nonessential Network Services **OC:** All but mission essential network services should be disabled by commenting out with a "#" before the applicable line in /etc/inet/inetd.conf, or have their startup scripts renamed/deleted so that they do not execute at system boot time. **CP:** (1) Determine what network services are essential for routine system operation: Conduct an interview with system administrators to determine what protocols/services are utilized for system administration and what protocols/services are utilized by authorized clients for system connectivity. (2) Utilize the results of the interview to formulate a list of network protocols/services that are should be disabled on the system to avoid unnesessary threat exposure. (3) Check the invocation mechanisms for the network protocols/services deemed unnesessary and ensure that they are disabled.	All nonessential network services controlled by inetd should be disabled. All nonessential network services not controlled by inetd should have their runlevel scripts renamed or removed to prevent these services from starting. The nmap scans from the remote host should verify the findings of the prior steps of this audit check.	**I/A/O**	Running nonessential services or services that are inherently insecure or that can be the target of future security exploits greatly decreases the security posture of the system by expanding the possibly and probability of an exploit being successfully conducted against the system.

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	Expected Result	Eval	Associated Risk
(3)(a) Review the /etc/inet/inetd.conf file and verify that all services deemed have been disabled with a comment character “#” before their applicable entry, or had their entries removed from the file. Those services that have not been disabled/removed should be noted in the findings and should be assessed for known vulnerabilities. Services that should be strongly considered for being disabled at a minimum are listed below: time, echo, discard, daytime, chargen, fs, dtsc, exec, comsat, talk, finger, uucp, name, xaudio, telnet, ftp, rlogin, rsh, rcp, tftp, printer (lpd), rquotad, rpc.ttdbserverd, DiskSuite support daemons, and kerbd (3)(b) Review the runlevel directories rcX.d (where X is a value of 2 through 3) and ensure that all services deemed unnesessary have been disabled by renaming or removal of the applicable startup script, so that the network protocol/service does not become invoked what the system is brought to the applicable run level. *Note* The number and type of services to be disabled are situationally dependant.* **Note:** Depending upon the prior system configuration and the packages selected at install time, some of the startup scripts listed above may not be present. A convenient and easily reversible method to disable start scripts without deleting them is to place the characters “NO” at the beginning of the script name so that they are passed over by the boot process. From a remote host utilize the nmap application to verify what network services the system is running. As root execute the following commands: For TCP based services: nmap –sT XXX.XXX.XXX.XXX (IP Address of target) For UDP based services: nmap –sU XXX.XXX.XXX.XXX (IP Address of target) For RPC based services nmap –sR XXX.XXX.XXX.XXX (IP Address of target) **SC:** Solaris Benchmark V1.2.0 Section 2.1 – 2.11, Solaris Security p 124 – 128, Solaris 8 Build Document p 15 - 20			

<table>
<tr><th>Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)</th><th>Expected Result</th><th>Eval</th><th>Associated Risk</th></tr>
<tr><td>**AC5:** Ensure That Security Enhanced Network Settings Have Been Applied on the System
OC: The TCP/IP tunable parameters should match those listed in sections 4.4 and 4.5 of the Solaris Benchmark V1.2.0
CP: Run the shell script ndd.sh (by Andres Kroonma) listed below as root:
#!/bin/ksh
#
ndd.sh
#
PATH=/usr/sbin:$PATH
if [-z "$1"]; then
   echo "Usage: $0 [udp | tcp | ip | icmp | arp | ...]"
   exit
fi
ndd /dev/$1 '?' | nawk -v c="ndd /dev/$1" '
/write/ {
  split($0,a,/[\t(]/);
  n=c t " " a[1];
  printf "echo %s = ",a[1];
  printf "`%s`\n",n;
}' | sh
*The script must be run once for udp, tcp, ip, icmp, and arp settings.
NOTE: The TCP/IP tunable kernel parameters will be restored to their default values once the system is rebooted. In order for them to be configured at boot time a startup script must be configured using ndd to set the desired parameters at boot time.
A review of the startup scripts should reveal a custom startup script configured that will reassign the required TCP/IP parameters at boot time.
SC: Solaris Benchmark V1.2.0 Section 4.4 and 4.5</td><td>The TCP/IP tunable kernel parameters should match those listed below.
ip_forward_src_routed = 0
ip6_forward_src_routed = 0
tcp_rev_src_routes = 0
ip_forward_directed _broadcasts = 0
tcp_conn_req_max_q0 = 4096
tcp_ip_abort_cinterval = 60000
ip_respond_to_timestamp = 0
ip_respond_to_timestamp_ broadcast = 0
ip_respond_to_address_ mask_broadcast = 0
arp_cleanup_interval = 60000
ip_ire_arp_interval = 60000
ip_ignore_redirect = 1
ip6_ignore_redirect = 1
ip_forwarding = 0
ip6_forwarding = 0
ip_strict_dst_multihoming =1
ip6_strict_dst_multihoming = 1
ip_send_redirects = 0
ip6_send_redirects = 0</td><td>**O/A**</td><td>By not having the required TCP/IP tunable parameters in place and a script to assign them at boot time the system can be vulnerable to or an unwilling participant in layer 2 and layer 3 based attacks.</td></tr>
</table>

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	Expected Result	Eval	Associated Risk
AC6: Verify Usage of Strong TCP Sequence Numbers **OC:** Ensure that the system is configured to use strong initial sequence numbers. **CP:** Review the /etc/default /inetinit configuration file for the following line: TCP_STRONG_ISS= Next, conduct a scan from a remote host using nmap to set with the OS detection switch (-O) and the super verbose setting. As root on the remote host with nmap installed execute the following command: nmap –O –v –v XXX.XXX.XXX.XXX (IP Address of target) | grep 'TCP Sequence Prediction' Review the nmap output for verification of TCP sequence number randomness. **SC:** Solaris Benchmark V1.2.0 Section 4.6, Solaris 8 Build Document p 15	The TCP_STRONG_ISS value should be assigned a "1" or preferably a "2". The "TCP Sequence Prediction:" in the nmap output should be either " Class=random positive increments" for TCP_STRONG_ISS=1 or " "Class=truly random" for TCP_STRONG_ISS=2.	**O/A**	Unless TCP sequence numbers are assigned the system will be vulnerable to man in the middle, injection or other TCP sequence prediction based attacks.

AC7: Ensure System Accounting is Being Used
OC: Ensure that system is being used to record and baseline system utilization.
CP: Verify that the following lines have been uncommented from the /etc/init.d/perf configuration file:
if [-z "$_INIT_RUN_LEVEL"]; then
        set -- `/usr/bin/who -r`
       _INIT_RUN_LEVEL="$7"
       _INIT_RUN_NPREV="$8"
       _INIT_PREV_LEVEL="$9"
 fi
 if [$_INIT_RUN_LEVEL -ge 2 -a $_INIT_RUN_LEVEL -le 4 -a \
     $_INIT_RUN_NPREV -eq 0 -a \($_INIT_PREV_LEVEL = 1 -o \
     $_INIT_PREV_LEVEL = S \)]; then
       /usr/bin/su sys -c "/usr/lib/sa/sadc /var/adm/sa/sa`date +%d`"
 fi
SC: Solaris Benchmark V1.2.0 Section 5.5, Solaris 8 Build Document p 10
	The lines notated in the CP portion of this check should be uncommented.	**O/A**	If system accounting is not in use of the system the administrator has a greatly diminished ability to detect when system resource utilization goes beyond the baseline. Without this capability users conducting password brute force attacks or some denial of service attempts may go unnoticed.

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	Expected Result	Eval	Associated Risk
AC8: Verify Kernel Level Auditing is in Use **OC:** Ensure that kernel level system auditing is being used via the Solaris Basic Security Module (BSM). **CP:** Check for the following to verify that the BSM conversion has been performed on the system. /etc/system contains the following lines: set c2audit:audit_load = 1 set abort_enable = 0 Check the /etc/rc2.d directory for the S99audit script. Run the following command # modinfo | grep c2audit The output should be 26 f5934000 c644 186 1 c2audit (C2 system call) To verify of the audit process is currently running, run the following command as root: # auditconfig –getcond The output of the auditconfig –getcond command should be as follows: audit condition = auditing Review the /etc/security/audit_control configuration file and ensure that it's configuration matches the following: dir:/var/audit flags:lo,ad,ex,fm,-fw,-fc,-fd,na naflags:lo,ad,ex,fm,-fw,-fc,-fd,nt minfree:20 **SC:** Solaris Benchmark V1.2.0 Section 5.6, Solaris 8 Build Document p 24-25, Hack Proofing Sun Solaris 8 p 189 - 192	The BSM conversion should have been performed on the system and verified by the steps listed in the CP section of this check.	**O/A**	Without kernel level auditing in place there will be no mechanism for administrators to review kernel space activity on the system such as file attribute modification attempts, and mode changes. Without this capability in place malicious activity that happens in kernel space will be difficult or impossible to detect.

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	Expected Result	Eval	Associated Risk
AC9: Verify /etc/passwd, /etc/shadow and /etc/group File Permissions **OC:** Review the /etc directory and ensure that the passwd, shadow and group configuration files are owned by root with sys and the primary group. File permissions for passwd and group should be no more permissive than 644, and permissions for shadow should be no more permissive than 400. **CP:** Perform a long listing (ls –al) on /etc/passwd, /etc/group and /etc/shadow and ensure that file ownership and permissions are in accordance with the above stated guidelines. As a non-administrative users on the local system attempt to write to the /etc/passwd file, attempt to read the /etc/shadow file and attempt to write to the /etc/group file. None of the above should be possible. **SC:** Solaris Benchmark V1.2.0 Section 6.5	A long listing for the passwd, shadow and group files will show root as the owner and sys as the group with permissions as follows: /etc/passwd: -rw-r--r— /etc/shadow: -r-------- /etc/group: -rw-r--r— The /etc/passwd and the /etc/group file should not allow writing to them from non-administrative users. The /etc/shadow file should not be able to be viewed by any account other than root (UID 0).	**O/A**	When permission that are more liberal than those listed are assigned to passwd. shadow, or group, unauthorized account modification can occur leading to privilege escalation, system compromise, or other unauthorized activity.
AC10: Find Unauthorized World-Writeable Files **OC:** Identify all world writeable files and determine if they are required for operation. **CP:** Use the find command to list all world writeable files on all mounted file systems. As root execute the following command: # find / -type f -perm -0002 -ls Review the listing of files output by this command and ensure that they are either removed or have their permissions made as restrictive as possible. **SC:** Solaris Benchmark V1.2.0 Section 6.7	There should be no world writeable files located on local file systems that are not absolutely required for system operation.	**O**	Data in world-writeable files can be modified and compromised by any user on the system. World writeable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.
AC11: Find unauthorized SUID/SGID system executables **OC:** Identify all unauthorized executables that are set user ID or set group ID, particularly those that are set user ID to root. **CP:** Use the find command to list all files that are SUID/SGID. As root execute the following command: # find / -type f \(-perm -04000 -o -perm -02000 \) -ls Review the listing of files output by this command against the baseline list located at: http://ist.uwaterloo.ca/security/howto/2000-08-17/ or any previously established baseline for your system and ensure that any additional files that are	The files that are SUID/SGID are only those that are a part of the operating system baseline or carefully audited and documented administrator/user created files.	**O**	Files that are SUID/SGID to a particular use can often be used to execute commands on a system at the privilege level of the assigned user. These files are a high value target for attackers and should be minimized and audit for security risks.

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	Expected Result	Eval	Associated Risk
SUID/SGID are either removed or reviewed for security implications. **SC:** Solaris Benchmark V1.2.0 Section 6.8, Hack Proofing Sun Solaris 8 p 139			
AC12: Verify the Use of the fix-modes Utility **OC:** Verify that the fix-modes utility is in use on the system to correct insecure default file system permission settings. **CP:** Review the cron jobs configured on the system and interview the system administrators to verify that the fix-modes utility is being run on the system on a regular basis. This check can also be performed by running the fix-modes utility a precompiled version that has been tested on Solaris 8 Sparc can be downloaded at: ftp.CISecurity.org/pub/pkgs/Solaris/fix-modes.tar.Z **SC:** Solaris Benchmark V1.2.0 Section 6.9, Hack Proofing Sun Solaris 8 p 139, Section 5.6, Solaris 8 Build Document p 52	The fix-modes utility should be in use on the system to correct and maintain secure file permissions	**O/A**	The fix-modes software corrects various ownership and permission issues with files throughout the Solaris file systems. If the fix-modes script is not run on a regular bases on a Solaris system, The system may be susceptible to many well-publicized conditions of loose file permissions associated with a default install of Solaris.
AC13: Verify the Existence, Contents and Permissions of the /etc/ftpusers File **OC:** Ensure that the system contains an /etc/ftpusers file and all accounts that should never access the system via ftp are listed in the file. **CP:** Review the /etc/ftpusers and ensure it contains the following accounts at a minimum: root, daemon, bin, sys, adm, lp, uucp, nuucp, smmsp, listen, nobody, noaccess, nobody4 Perform a long listing (ls –al) on the file and ensure the permissions are 600, and the file is owned by root with a primary group of root. Example: # ls –al /etc/ftpusers -rw------- 1 root root 69 Jan 29 2002 ftpusers As a non-root user, attempt to view and then copy the contents of the /etc/ftpusers file to another directory. **SC:** Solaris Benchmark V1.2.0 Section 7.3, Hack Proofing Sun Solaris 8 p 147	The /etc/ftpusers file will exist, be owned by root with a primary group of root and contain the appropriate list of accounts that should NOT be allowed ftp access to the system.	**O/A**	Only normal users should ever access the system via ftp-there should be no reason for "system" type accounts to be transferring information via this mechanism. Certainly the Root account should *never* be allowed to transfer files directly via ftp. Consider also adding the names of other privileged or shared accounts which may exist on your system such as user oracle and the account which your Web server process runs under.

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	**Expected Result**	**Eval**	**Associated Risk**
AC14: Check the Default Locking Screensaver Timeout Settings **OC:** Ensure that the CDE screensaver lockout is set for 10 minutes or less. **CP:** Review the /usr/dt/config/*/sys.resources config file for the following values: dtsession*saverTimeout: **10** dtsession*lockTimeout: **10** **SC:** Solaris Benchmark V1.2.0 Section 7.7	The sys.resources file should contain a timeout value of 10 minutes for the screensaver lockout.	**O/A**	If the screensaver lockout is not assigned or assigned for a value of greater than 10 minutes the possibility of an insider taking over a session when another user/administrator walks away from their terminal is greatly increased. This situation would allow them to conduct activity at the privilege of the currently logged in user.
AC15: Verify Use of Appropriate Warning Banners **OC:** Ensure that appropriate legal notice/warning banners have been applied to the system. **CP:** Perform the following functions to ensure that appropriate warning banners have been applied to the system: As root execute the following: # eeprom | grep oem-banner The result should be the following: oem-banner=Warning Banner Text oem-banner?=true As root execute the following: #cat /etc/motd /etc/issue /etc/default/telnetd /etc/default/ftpd | more Each of the files should contain the appropriate warning text. Next check the permissions and ownership for each of these banner files: # ls –al /etc/motd /etc/issue /etc/default/telnetd /etc/default/ftpd The output of this command should match the following: -rw-r--r-- 1 root sys /etc/default/ftpd -rw-r--r-- 1 root sys /etc/default/telnetd -rw-r--r-- 1 root root /etc/issue -rw-r--r-- 1 root sys /etc/motd Next we will check the configuration of the CDE warning banners:	An appropriate legal notice / consent to monitoring banner should be displayed before logging in to the system.	**0/A**	Failure to display a legal notice / consent to monitoring warning banner can inhibit the ability to prosecute an individual in the event the system is compromised.

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	Expected Result	Eval	Associated Risk
Review the following CDE configuration files for the appropriate value: usr/dt/config/*/sys.resources or etc/dt/config/*/sys.resources Dtlogin*greeting.labelString: Dtlogin*greeting.persLabelString: An appropriate warning banner should be assigned to these values. **SC:** Solaris Benchmark V1.2.0 Section 7.10, Solaris 8 Build Document p 20, Solaris 8 Essential Reference – (2nd Edition) p 282			
AC16: Check that Root Logins Are Restricted to the System Console. **OC:** Ensure that root login activity is restricted to the system console. **CP:** Review the /etc/default/login file for the following value: CONSOLE=/dev/console Additionally, a long listing of the /etc/default/login file should match the following: -r--r--r-- 1 root sys login **SC:** Solaris Benchmark V1.2.0 Section 7.11, Solaris 8 Build Document p 11, Hack Proofing Sun Solaris 8 p 105	The value /dev/console (the system console) should be applied for the CONSOLE= variable in the /etc/default/login file. The file ownership should also be root:sys and the effective file permissions 444.	**O/A**	Allowing remote unencrypted network connections with the root account can expose the root credentials to compromise or interception. It is much better to utilize ssh, and require any remote user to su to root. While it should be understood that even when su is used over clear text protocols, the credentials are still transmitted in the clear, at least there is a record of who utilized the root account.
AC17: Ensure That the Number of Failed Login Attempts is Limited to Three or Less **OC:** Ensure that the system is protected against brute force attacks by having the number of unsuccessful login attempts limited. **CP:** Review the /etc/default login file and ensure that the RETRIES variable is assigned the value of 3 or less. RETRIES=3 Additionally, a long listing of the /etc/default/login file should match the following: -r--r--r-- 1 root sys login **SC:** Solaris Benchmark V1.2.0 Section 7.12, Solaris 8 Build Document p 12 - 13	The system will be configured to limit the number of successive failed login attempts to three by having the proper value set for RETRIES in /etc/default/login. Additionally the file ownership should be root:sys and the permissions set to 444	**O/A**	Not having the number of successive failed login attempts set to a predefined limit allows for automated brute force utilities or dictionary based brute force attacks to be conducted against system accounts unhindered.

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	**Expected Result**	**Eval**	**Associated Risk**
AC18: Verify That There Are No Accounts with Empty Password Fields **OC:** Ensure that all accounts are configured to require a password for logins. **CP:** As root execute the following: # logins –p The command should return a black output. Any accounts that are listed do not require a password for login and should be immediately addressed. **SC:** Solaris Benchmark V1.2.0 Section 8.2	All accounts will require a valid password for login access.	**O/A**	Allowing accounts to be logged in to without two-factor authentication completely bypasses the identification and authentication mechanisms of the Solaris operating system. Allowing any individual to execute commands at the privilege level of that user.
AC19: Ensure Account Expiration Parameters Are Set On Active Accounts **OC:** Ensure that the default account expiration values are set and that they are applied to all user accounts on the system. **CP:** As root perform the following: # more /etc/default/passwd The values in /etc/default/passwd should meet or exceed the following values: MAXWEEKS=13 MINWEEKS=1 WARNWEEKS=4 PASSLENGTH=6 As root execute the following: # logins -ox |awk -F: '($1 == "root" || $8 == "LK") { next } { $cmd = "passwd" }($11 <= 0 || $11 > 91) { $cmd = $cmd " -x 91" }($10 < 7) { $cmd = $cmd " -n 7" } ($12 < 28) { $cmd = $cmd " -w 28" } ($cmd != "passwd") { print $cmd " " $1 }'> ./no-expire-acnt.txt The expire-acnt.txt file will contain any accounts in violation of the system policy for account expiration. **SC:** Solaris Benchmark V1.2.0 Section 8.3, Solaris Security p 67	The default account parameters in /etc/default/passwd should meet those listed and all user accounts on the system should have password aging applied.	**O/A**	Failure to enforce proper account passwd aging parameters can lead to dormant accounts with known password values or increase the probability of brute force passwd attacks.
AC20: Verify That Least Privilege Has Been Instituted for the Home Directories of the ftp Users. **OC:** All of the home directories for the TDS ftp accounts should be protected from unauthorized file viewing, or modification by other ftp account holders. **CP:** Review the /etc/passwd file and ensure that all	All ftp users on the system should have a unique UID and a unique GID. All ftp user home directories in /export/home should have a permission setting of 750 or more restrictive.	**I/O/A**	Users that can browse or modify data in other users home directories can lead to leakage of sensitive information or compromise of information that can be utilized in privilege escalation.

Audit Check (AC), Objective of Check (OC), Check Procedure (CP), Source of Check (SC)	**Expected Result**	**Eval**	**Associated Risk**
ftp users have their own unique UID and GID. All ftp users home directories should be under /export/home. Perform a long listing of /export/home and ensure that permissions on the ftp user directories are no more permissive than 750. Next login to the system via ftp as at least two different ftp users and attempt to view files in other ftp users home directories **SC:** General Best Practice	Any ftp users should not be able to view of modify files in any other ftp users home directory.		

3 Assignment 3 – Conduct the Audit

The items listed below are the ten audit checks from the audit checklist in section 2 that have the greatest impact on the overall security posture of the Wobulators Inc. Technology Distribution Server (TDS). The audit checks and their associated findings are listed as they appear in the audit checklist and are not ranked by impact or severity. Under different operational conditions or system configuration a somewhat different list of representative audit checks may have been presented for evaluation.

3.1 Audit Check AC1

AC1: Ensure All Applicable Operating System Security Patches Are Installed

Audit Check AC1 Results: Failure

OC: System must have all current vendor supplied operating system security patches installed.

SC: Solaris Benchmark V1.2.0 Section 1.1, Hack Proofing Sun Solaris 8 p 13-14

Notes: The security patch analysis was performed against the "Patches Containing Security Fixes" section of the Solaris 8 Recommended and Security patches report dated June 16 2003. This was the most current revision at the time of test. Sun Microsystems releases the Recommended and Security Patches report twice monthly, and is available from http://sunsolve.sun.com.

This chart was compiled by performing a comparative analysis of the output of a showrev –p command against the current list of patches containing security fixes at the time if test. A similar type analysis can be performed in an automated fashion with tools supplied by Sun Microsystems. The issue with these tools is one requires the installation of perl and the other an additional package to the system. I felt that it was important to illustrate that a proper security patch analysis can be performed utilizing "operating system standard" commands. This can be helpful on a minimalist installation such as a firewall or DNS system, where the smallest possible system install is appropriate.

Table 3. Sun Solaris 8 Security Patch Analysis Report

Solaris Patch	Installed Revision	Current Revision	Solaris Patch Description	Security Findings / Recommendations
108869	18	19	snmpdx/mibiisa/libssasnmp/snmplib patch	Revision 19 of the 108869 patch resolves an issue where snmpdx fails while encoding pdu whose OID is greater than 32bits. The TDS is not running snmpdx or any other SNMP applications. The security impact of the absence of this patch is considered to be minimal. The auditor does however recommend the removal of the SNMP/snmpdx packages in order to prevent any possible future exposure to this or subsequent security issues.
108975	6	8	/usr/bin/rmformat and /usr/sbin/format patch	This patch resolves a function issue with the format command. Absence of this patch has no security impact to this system at this time.
108987	12	13	Patch for patchadd and patchrm	Resolves a number of issues with the patchadd and patchrm commands that can potentially result in an unstable system. Absence of patch has minimal security impact on this system at this time
109091	5	6	/usr/lib/fs/ufs/ufsrestore patch	Corrects a situation where ufsrestore has problems after restoring empty incremental dump. The absence of this patch is considered to have a no security impact upon the system at this time.
109154	9	18	PGX32 Graphics	Resolves a number of issues that can result in screen distortions and displaying some URLs with PGX32 causes Xserver to crash, a locally exploitable buffer overflow, and a number of conditions that can result in a denial of service condition. Absence of patch has a security impact on this system. It is strongly recommended that revision 18 of the 109154 patch for Solaris 8 (sparc) be installed on the TDS.
109354	5	19	dtsession patch	Resolves a security issue where a local user may be able to execute arbitrary code or commands with the privileges of the dtsession(1) CDE Session Manager. The dtsession CDE Session Manager runs with root privileges. The absence of this patch has medium-high security impact upon this system at this time. It is strongly recommended that revision 19 of the 109354 patch for Solaris 8 (sparc) be installed on the TDS.

Solaris Patch	Installed Revision	Current Revision	Solaris Patch Description	Security Findings / Recommendations
109793	14	18	su driver patch	Resolves a number of issues that could result in a denial of service condition. Absence of patch has minimal security impact on this system at this time. However, it is recommended that revision 18 of the 109793patch for Solaris 8 (sparc) be installed on the TDS.
109951	-	1	jserver buffer overflow	Resolves a buffer overflow condition with jserver. Absence of patch has no security impact on this system at this time. The jserver packages are not installed on the TDS.
110386	2	3	RBAC Feature Patch	Resolves a condition with getexecuser than can result system performance degradation. Absence of patch has minimal security impact on this system at this time. However, it is recommended that revision 3 of the 110386 patch for Solaris 8 (sparc) be installed on the TDS.
110387	3	4	ufssnapshots support, ufsdump patch	Resolved a condition in which ufsdump fails to dump a file larger than 2G on Solaris 8 This situation could potentially prevent a system recovery after a failure or security incident. Absence of patch has medium-low impact on this system at this time. It is recommended that revision 4 of the 110387 patch for Solaris 8 (sparc) be installed on the TDS.
110615	5	9	Sendmail patch	A local or remote unprivileged user may be able to gain unauthorized root access or cause a denial of service due to a buffer overflow in the sendmail daemon. The absence of this patch has high security impact upon this system at this time. It is recommended that revision 9 of the 110615 patch for Solaris 8 (sparc) be installed on the TDS.
110668	2	4	/usr/sbin/in.telnetd patch	Resolves a potential remotely executable buffer overflow that can result in a remote user obtaining root privileges on the system. The TDS is currently running a telnet daemon therefore the absence of this patch has a very high security impact on this system at this time. It is strongly recommended that revision 4 of the 110668 patch for Solaris 8 (sparc) be installed on the TDS.

Solaris Patch	Installed Revision	Current Revision	Solaris Patch Description	Security Findings / Recommendations
110934	8	13	pkgtrans, pkgadd, pkgchk and libpkg.a patch	Resolves a number of issues relating to patch management that can result in an unstable system, or the inability to properly install security patches. Absence of patch currently has a minimal security impact on this system at this time. However, it is recommended that revision 13 of the 110934 patch for Solaris 8 (sparc) be installed on the TDS.
111606	-	3	/usr/sbin/in.ftpd patch	This patch resolves a condition where a local or remote unprivileged user may be able to disrupt ftp services on Solaris systems which act as ftp servers using the Sun supplied version of in.ftpd. This system is running a susceptible version if in.ftpd, and therefore the security impact to the system is considered to be medium-high. It is strongly recommended that revision 3 of the 111606 patch for Solaris 8 (sparc) be installed on the TDS.
114673	-	1	/usr/sbin/wall patch	Resolves a condition wherein the wall application could be utilized in an impersonation of the root account resulting in potential information leakage/social engineering. The security impact of the absence of patch is dependant upon the systems function and class of users. The TDS does not provide shell accounts for non-administrative users; therefore impact is deemed to be minimal. However, it is recommended that revision 1 of the 114673 patch for Solaris 8 (sparc) be installed on the TDS.

Audit Check Result Notes: There are a number a very serious security issues with the TDS that are the result of not keeping current with all applicable vendor supplied operating system security patches. The results of this analysis also show that patches are being applied individually in place of installing applicable patch clusters. Unless extreme diligence is applied to maintaining operating system patches individually, it is strongly recommended that the applicable patch cluster be applied at least monthly, in order to help ensure no patches are missed. It should be noted that all operating system patches should be thoroughly tested on a development or backup system prior to deployment on a production server. Installation of operating system patches without proper testing can result in a self-induced denial of service condition, by inadvertently disrupting system functionality.

3.2 Audit Check AC2

AC2: Verify Use and Proper Operation of TCP Wrappers

Audit Check AC2 Results: Failure

OC: TCP Wrappers installed, properly configured and operational on the system

CP: Check for the existence of /etc/hosts.allow and /etc/hosts.deny. Ensure that the /etc/hosts.deny file contains a single ALL:ALL entry notating a deny by default posture. Review the /etc/hosts.allow file and ensure that the file contains only a list of hosts either by IP version 4 address or conical domain name that are explicitly allowed to connect to the host on a service by service bases.

Verify the network services started by inetd are wrapped by verifying they are started from tcpd in /etc/inet/inetd.conf.

For example:

```
ftp    stream  tcp6    nowait  root    /usr/sbin/tcpd      in.ftpd
```

Configure a test system to reside outside the IP address range defined in /etc/hosts.allow and attempt to make a connection to the ftp server running on the TDS. The connection attempt should be refused.

SC: Solaris Benchmark V1.2.0 Section 1.2, Solaris Security p 168-169, Solaris 8 Build Document p 52

The following screen output was captured utilizing the “script” command while executing the steps in Audit Check AC2. When applicable, notes have been added to the output for clarification purposes.

As root enter the /etc directory and check for the existence and review the contents of the hosts.allow and hosts.deny configuration files:

```
# cd /etc

# more hosts.allow

hosts.allow: No such file or directory

# more hosts.deny

hosts.deny: No such file or directory
```

Switch to the /etc/inet.d and check the inetd.conf entry for an known operational TCP based network service and check that it is being started from tcpd and not directly from the service binary:

```
# cd /etc/inet

# more inetd.conf | grep in.ftpd

ftp     stream  tcp6    nowait  root    /usr/sbin/in.ftpd       in.ftpd
```

Audit Check Result Notes: The actions of this audit check listed above revealed that the TCP Wrappers application is not installed on the TDS and the system does not have the ability to control connection attempts to TCP based services via IP version 4 address or conical domain names. The need for remote verification of the function of TCP Wrappers has been negated by the absence of the application.

3.3 Audit Check AC3

AC3: Determine if Secure Shell (SSH) is installed and operational.

Audit Check AC3 Results: Failure

OC: Verify the installation of the secure shell (SSH)

CP: Execute the following commands as root:

```
# ps –e | grep sshd
```

```
# pkginfo –l  | grep openssh
```

Just in case the ssh daemon was not installed via a Solaris package, we can also check for a startup script and remotely for sshd.

```
# ls /etc/rc2.d | grep ssh
```

If this command returns nothing there is not an ssh startup script in /etc/rc2.d

Next conduct a scan using nmap to see if the ssh daemon is listening:

```
nmap –p22 XXX.XXX.XXX.XXX (IP Address of target)
```

SC: Solaris Benchmark V1.2.0 Section 1.3, Hackproofing Sun Solaris 8 p 189 - 192

The following screen output was captured utilizing the “script” command while executing the steps in Audit Check AC3. When applicable, notes have been added to the output for clarification purposes.

Check for the existence of a ssh daemon:

```
bash-2.03# ps -e | grep sshd
bash-2.03#
```

Next check to see if ssh has been installed via a Solaris package:

```
bash-2.03# pkginfo -l | grep OpenSSH
bash-2.03#
```

Verify that there is no startup script for the ssh daemon:

```
bash-2.03# ls /etc/rc2.d | grep ssh
bash-2.03#
```

Finally a remote scan for ssh will be conducted from a remote host on the same network segment running Linux:

```
[kromar@hector ssh]$ nmap -p 22 XX.XX.XX.XXX (TDS IP Address)

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
The 1 scanned port on  (XX.XX.XX.XXX) is: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
```

Audit Check Result Notes: From the above actions we can tell that ssh is neither active nor installed on the TDS. The ssh suite of applications provides equivalent functionality as many of the standard UNIX protocols such as rsh, rexec, rlogin, telnet, and ftp in a much more secure manner. Not utilizing ssh to the greatest extent possible greatly reduces the overall security posture of the TDS by increasing the probability of interception of system credentials in transit, susceptibility to impersonation, and man in the middle attacks, network sniffing, and other means of compromise for sensitive company data. In short, move off of telnet and ftp for day-to-day operations and replace all of the traditional r-services with the ssh equivalent. At this point in time there are not many valid reasons for substituting less secure services with ssh.

3.4 Audit Check AC4

AC4: Verify the Minimization of All Nonessential Network Services

Audit Check AC4 Results: Failure

OC: All but mission essential network services should be disabled by commenting out with a "#" before the applicable line in /etc/inet/inetd.conf, or by having their startup scripts renamed/deleted so that they do not execute at system boot time.

CP:

(1) Determine what network services are essential for routine system operation:

Conduct an interview with system administrators to determine what protocols/services are utilized for system administration and what protocols/services are utilized by authorized clients for system connectivity.

(2) Utilize the results of the interview to formulate a list of network protocols/services that are should be disabled on the system to avoid unnesessary threat exposure.

(3) Check the invocation mechanisms for the network protocols/services deemed unnesessary and ensure that they are disabled.

(3)(a) Review the /etc/inet/inetd.conf file and verify that all services deemed unnesessary have been disabled with a comment character "#" before their applicable entry, or had their entries removed from the file. Those services that have not been disabled/removed should be noted in the findings and should be assessed for known vulnerabilities.

Services that should be strongly considered for being disabled at a minimum are listed below:

time, echo, discard, daytime, chargen, fs, dtsc, exec, comsat, talk, finger, uucp, name, xaudio, telnet, ftp, rlogin, rsh, rcp, tftp, printer(lpd), rquotad, rpc.ttdbserverd, DiskSuite support daemons, and kerbd

(3)(b) Review the runlevel directories rcX.d (where X is a value of 2 through 3) and ensure that all network services deemed have been disabled by renaming or removal of the applicable startup script, so that the network protocol/service does not become invoked what the system is brought to the applicable run level.

Note: Depending upon the prior system configuration and the packages selected at install time, some of the startup scripts listed above may not be present. A convenient and easily reversible method to disable start scripts without deleting them is to place the characters “NO” at the beginning of the script name so that they are passed over by the boot process.

From a remote host utilize the nmap application to verify what network services the system is running. As root execute the following commands:

For TCP based services:

```
nmap –sT XXX.XXX.XXX.XXX (IP Address of target)
```

For UDP based services:

```
nmap –sU XXX.XXX.XXX.XXX (IP Address of target)
```

For RPC based services

```
nmap -sR XX.XX.XX.XXX (IP Address of target)
```

SC: Solaris Benchmark V1.2.0 Section 2.1 – 2.11, Solaris Security p 124 – 128, Solaris 8 Build Document p 15 – 20

After interviewing the TDS system administrators and carefully reviewing the functional requirements of the TDS it was determined that the only network services that was essential for the TDS operation was an FTP server and an X11 server for the use of CDE on the system console. The TDS itself provided no other services to remote or local clients other than file transfer. Most, if not all of the system administration is performed from the system console. The administrators did express a desire for an SSH implementation so that system maintenance and troubleshooting could be performed from their desktops or a remote location in a secure manner.

The /etc/inet/inetd.conf configuration file was then reviewed and the following services were found to not have their entries commented (with a “#”) out, preventing them from being started via the superserver.

Table 4. Uncommented Services in /etc/inet/inetd.conf

Uncommented Entry in inetd.conf	Comments
ftp stream tcp6 nowait root /usr/sbin/in.ftpd in.ftpd	FTP server is not having access controlled by TCP_Wrappers.
telnet stream tcp6 nowait root /usr/sbin/in.telnetd in.telnetd	Telnet server is not having access controlled by TCP_Wrappers.
100232/10 tli rpc/udp wait root /usr/sbin/sadmindsadmind	The sadmin server is not required and should have been commented out.
100235/1 tli rpc/ticotsord wait root /usr/lib/fs/cachefs/cachefsd cachefsd	The cachefsd server in not required (no NFS) and should have been commented out.

.

/etc/inetd.conf Review Notes: While the majority of nonessential services were commented out of the inetd.conf configuration file, the sadmind and cachefsd daemons were not commented and are not required for fulfillment of the TDS operational mission. Additionally the FTP and TELNET daemons were not having there access controlled via TCP wrappers (services not started via tcpd). While not the primary objective of this check, it is nonetheless a significant factor in the overall risk posture of the TDS, and indicates a failure for audit check AC2

The following screen output was captured utilizing the “script” command while executing the steps in Audit Check AC4. When applicable, notes have been added to the output for clarification purposes.

```
Script started on Sun 22 Jun 2003 11:59:29 AM EDT
```

Perform a listing of the contents of the /etc/rc2.d directory to see if the startup script for nonessential network services have been renamed/removed preventing the service from starting. Scripts that should have been disabled or renamed have been highlighted:

```
# cd /etc/rc2.d

# ls

K06mipagent        S40llc2            S74autofs          S88utmpd
K07dmi             S69inet            S74syslog          S89bdconfig
K07snmpdx          S70uucp            S74xntpd           S90wbem
K16apache          S71ldap.client     S75cron            S88sendmail
S93cacheos.finish  K28nfs.server      S71rpc             S75savecore
S94ncalogd         S71sysid.sys       S76nscd            S95ncad
S01MOUNTFSYS       S72autoinstall     S80lp              S99audit
S05RMTMPFILES      S72inetsvc         S80PRESERVE        S99dtlogin
S20sysetup         S72slpd            S80spc S21perf
S73cachefs.daemon  S85power           S30sysid.net       S73nfs.client
```

Next, perform a listing of the contents of the /etc/rc3.d directory to see if the startup script for nonessential network services have been renamed/removed preventing the service from starting. Scripts that should have been disabled or renamed have been highlighted:

```
bash-2.03# cd rc3.d/

bash-2.03# ls

README          S50apache      S77dmi

S15nfs.server   S76snmpdx      S80mipagent
```

Next verify the findings listed above from a Linux host on the same network segment by using the nmap scanner to see what is available on the TDS network interface. All network services deemed nonessential as part of the audit are highlighted and should be disabled.

```
[root@hector rpcinfo]# nmap -sT XX.XX.XX.XXX (TDS IP Address)

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (XX.XX.XX.XXX):
(The 1590 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
587/tcp    open        submission
898/tcp    open        unknown
4045/tcp   open        lockd
6000/tcp   open        X11
32771/tcp  open        sometimes-rpc5
32786/tcp  open        sometimes-rpc25

Nmap run completed -- 1 IP address (1 host up) scanned in 50 seconds
```

All of the above listed TCP ports with the exception of ftp and the X11 server are not required for normal TDS operation and should be disabled.

```
[root@hector rpcinfo]# nmap -sU XX.XX.XX.XXX (TDS IP Address)

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (XX.XX.XX.XXX):
(The 1454 ports scanned but not shown below are in state: closed)
Port       State       Service
111/udp    open        sunrpc
161/udp    open        snmp
177/udp    open        xdmcp
514/udp    open        syslog
520/udp    open        route
4045/udp   open        lockd
32771/udp  open        sometimes-rpc6
32772/udp  open        sometimes-rpc8
32773/udp  open        sometimes-rpc10
32775/udp  open        sometimes-rpc14
32776/udp  open        sometimes-rpc16
32777/udp  open        sometimes-rpc18
32780/udp  open        sometimes-rpc24
```

```
32786/udp  open        sometimes-rpc26

Nmap run completed -- 1 IP address (1 host up) scanned in 190 seconds
```

All of the above listed UDP ports are not required for normal TDS operation and should be disabled.

```
[root@hector rpcinfo]# nmap -sR XX.XX.XX.XXX (TDS IP Address)

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (XX.XX.XX.XXX):
(The 1590 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc (rpcbind V2-4)
587/tcp    open        submission
898/tcp    open        unknown
4045/tcp   open        lockd (nlockmgr V1-4)
6000/tcp   open        X11
32771/tcp  open        sometimes-rpc5 (status V1)
32786/tcp  open        sometimes-rpc25 (snmpXdmid V1)

Nmap run completed -- 1 IP address (1 host up) scanned in 56 seconds
```

All of the above listed ports found via the RPC scan with the exception of ftp and X11 are not required for normal TDS operation and should be disabled. There is some repetition here between what was found with the TCP and UDP scans, but it is best to try all three port scan methods in order to ensure maximum accuracy.

```
Script done on Sun Jun 22 12:33:59 2003
```

The findings collected from the Linux laptop verify the findings of the configuration review More network services than are needed are indeed alive and well on the TDS.

Audit Check Result Notes: While it is very important to minimize ALL non-essential network services in order to minimize threat exposure, the telnet, rpcbind server, and the Sendmail smtp server are particularly high value targets. They run at a high privilege level, and have been the subject of numerous serious security exploits in the past (and future no doubt).

3.5 Audit Check AC6

AC6: Verify Usage of Strong TCP Sequence Numbers

Audit Check AC3 Results: Pass

OC: Ensure that the system is configured to use strong initial sequence numbers.

CP: Review the /etc/default /inetinit configuration file for the following line:

TCP_STRONG_ISS=

Next conduct a scan from a remote host using nmap to set with the OS detection switch (-O) and the super verbose setting. As root on the remote host with nmap installed execute the following command:

nmap –O –v –v XXX.XXX.XXX.XXX (IP Address of target) | grep 'TCP Sequence Prediction'

Review the nmap output for verification of TCP sequence number randomness.

SC: Solaris Benchmark V1.2.0 Section 4.6 , Solaris 8 Build Document p 15

The following screen output was captured utilizing the "script" command while executing the steps in Audit Check AC6. When applicable, notes have been added to the output for clarification purposes.

On the TDS review the /etc/default/inetinit file for the appropriate TCP_STRONG_ISS setting:

```
bash-2.03# more /etc/default/inetinit | grep TCP_STRONG_ISS

# TCP_STRONG_ISS sets the TCP initial sequence number generation
parameters.
# Set TCP_STRONG_ISS to be:

TCP_STRONG_ISS=2
```

Finally a remote scan with nmap will be conducted from a remote host on the same network segment in order to verify the TCP Sequence number setting

```
[root@xactoid sol_tcp_sqn]# nmap -O -v -v xx.xx.xx.xxx | grep 'TCP
Sequence Prediction'

No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use
-sP if you really don't want to portscan (and just want to see what
hosts are up).

TCP Sequence Prediction: Class=truly random
```

Audit Check Result Notes: The local configuration check and the remote TCP sequence number verification performed with nmap revealed that the system is configuring to use nonrandom TCP sequence numbers. This situation makes it markedly more difficult for an attacker to conduct injection or man in the middle attacks against the TDS.

3.6 Audit Check AC8

AC8: Verify Kernel Level Auditing is in Use and Properly Configured

Audit Check AC8 Results: Pass (Conditional See Notes for AC8)

OC: Ensure that kernel level system auditing is being used via the Solaris Basic Security Module (BSM).

CP: Check for the following to verify that the BSM conversion has been performed on the system.

/etc/system contains the following lines:

```
set c2audit:audit_load = 1
set abort_enable = 0
```

check the /etc/rc2.d directory for the S99audit script.

Run the following command

```
# modinfo | grep c2audit
```

The output should be

```
26 f5934000 c644 186 1 c2audit (C2 system call)
```

To verify of the audit process is currently running, run the following command as root:

```
# auditconfig –getcond
```

The output of the auditconfig –getcond command should be as follows:

```
audit condition = auditing
```

Review the /etc/security/audit_control configuration file and ensure that it's configuration matches the following:

```
dir:/var/audit
flags:lo,ad,ex,fm,-fw,-fc,-fd,na
naflags:lo,ad,ex,fm,-fw,-fc,-fd,nt
minfree:20
```

SC: Solaris Benchmark V1.2.0 Section 5.6, Solaris 8 Build Document p 24-25, Hack Proofing Sun Solaris 8 p 189 - 192

The following screen output was captured utilizing the "script" command while executing the steps in Audit Check AC8. When applicable, notes have been added to the output for clarification purposes.

```
Script started on Sun Jun 22 15:40:15 2003
```

Check the /etc/system file for verification that the BSMconv script has been run on the system.

```
# more /etc/system | grep set

set c2audit:audit_load = 1
set abort_enable = 0
```

Next verify that the startup script for the audit daemon is in rc2.d.

```
# cd /etc/rc2.d

# ls

K06mipagent        S40llc2            S74autofs          S88utmpd
K07dmi             S69inet            S74syslog          S89bdconfig
K07snmpdx          S70uucp            S74xntpd           S90wbem
K16apache          S71ldap.client     S75cron
S93cacheos.finish  K28nfs.server      S71rpc             S75savecore
S94ncalogd         S71sysid.sys       S76nscd            S95ncad
S01MOUNTFSYS       S72autoinstall     S80PRESERVE        S99audit
S05RMTMPFILES      S72inetsvc         S80lp              S99dtlogin
S20sysetup         S72slpd            S80spc S21perf     S88sendmail
73cachefs.daemon   S85power           S30sysid.net       S73nfs.client
```

Ensure that the c2audit kernel module is loaded.

```
# modinfo | grep c2audit
```

30 f5bc0802   edec 186   1 c2audit (C2 system call)

```
Make sure that auditing is currently enabled

# auditconfig –getconf
```

audit condition = auditing

Now that we have determined that the auditd process in installed and functioning, the audit configuration file will be reviewed.

```
# more /etc/security/audit_control

# Copyright (c) 1988 by Sun Microsystems, Inc.
#
#ident  @(#)audit_control.txt  1.3     97/06/20 SMI
#
dir:/var/audit
flags:lo,ad,-fa,-fd,nt,na,pc,fc,fm:
minfree:20
naflags:lo
#
script done on Tue Jun 22 15:41:26 2003
```

Audit Check Result Notes: While the system does not completely meet the requirements outlined in AC8, auditing is enabled and most of the required audit flags are configured with the exception of ex (execution), –fw (file write failures), and no (no class). Several audit flags were missed in the non-attributable section; ad (administrative), ex (execution), fm (file modification), -fw (file write failure), -fs (file create failure), -fd (file delete failure), nt (network events) were all absent from the operational configuration.

C2 or kernel level auditing is often a very subjective situation. Each system should be baselined, and a determination made as to what level of granularity is sufficient in order to introduce an appropriate level of detective control in to the system configuration. C2 or BSM auditing is very processor and disk (both activity and storage) intensive. If the administrator is too aggressive with the audit configuration, there can be a serious performance hit on the system or even the potential for a denial of service condition if there is a large deviation from baseline system activity. In short, BSM auditing is more of an art than a science. While the TDS configuration did not meet the standard set in the Solaris Benchmark V1.2.0, it was deemed appropriate for this hardware under this operational situation.

3.7 Audit Check AC13

AC13: Verify the Existence, Contents and Permissions of the /etc/ftpusers File

Audit Check AC13 Results: Pass

OC: Ensure that the system contains an /etc/ftpusers file and all accounts that should never access the system via ftp are listed in the file.

CP: Review the /etc/ftpusers and ensure it contains the following accounts at a minimum:

root, daemon, bin, sys, adm, lp, uucp, nuucp, smmsp, listen, nobody, noaccess, nobody4

Perform a long listing (ls –al) on the file and ensure the permissions are 600, and the file is owned by root with a primary group of root.

Example:

```
# ls –al /etc/ftpusers

-rw-------   1 root     root          69 Jan 29  2002 ftpusers
```

As a non-root user, attempt to view and then copy the contents of the /etc/ftpusers file to another directory.

SC: Solaris Benchmark V1.2.0 Section 7.3, Hack Proofing Sun Solaris 8 p 147

Note: On many systems this check may not be considered of primary importance, but due to the fact the that TDS is in essence an FTP Server, this check is considered of high value.

The following screen output was captured utilizing the “script” command while executing the steps in Audit Check AC13. When applicable, notes have been added to the output for clarification purposes.

Check the existence of, and review the contents of the /etc/ftpusers file:

```
# more /etc/ftpusers
root
daemon
bin
sys
adm
lp
uucp
nuucp
listen
nobody
noaccess
nobody4
```

Compare the contents against the /etc/password file and see if all appropriate users are listed within the /etc/ftpusers file.

```
# more /etc/passwd
root:x:0:1:Super-User:/:/usr/bin/bash
daemon:x:1:1::/:/dev/null
bin:x:2:2::/usr/bin:/dev/null
sys:x:3:3::/:/dev/null
adm:x:4:4:Admin:/var/adm:/dev/null
lp:x:71:8:Line Printer Admin:/usr/spool/lp:/dev/null
uucp:x:5:5:uucp Admin:/usr/lib/uucp:/dev/null
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/dev/null
listen:x:37:4:Network Admin:/usr/net/nls:/dev/null
nobody:x:60001:60001:Nobody:/:/dev/null
noaccess:x:60002:60002:No Access User:/:/dev/null
nobody4:x:65534:65534:SunOS 4.x Nobody:/:/dev/null
bizmark:x:1007:6007:/export/home/bizmark:/usr/bin/bash
sherwin:x:1008:6008:/export/home/sherwin:/bin/sh
mexicocity1:x:1003:6003:/export/home/mexicocity1:/bin/sh
berlin7:x:1004:6004:/export/home/berlin7:/bin/sh
tokyo4:x:1005:6005:/export/home/tokyo4:/bin/sh
newyork3:x:1006:6006:/export/home/newyork3:/bin/sh
```

Finally check and verify the /etc/ftpusers file ownership and permissions:

```
# ls -al /etc/ftpusers

-rw-------   1 root     root          69 Jan 29  2002 /etc/ftpusers
```

As a non-root user, attempt to view and then copy the contents of the /etc/ftpusers file to another directory:

```
bash-2.03$ more /etc/ftpusers

/etc/ftpusers: Permission denied

bash-2.03$ cp /etc/ftpusers /export/home/kromar

cp: cannot open /etc/ftpusers: Permission denied
```

Audit Check Result Notes: Particularly because the TDS is in essence a File Transfer Protocol server, is it important to prevent users from logging in to the server with system level accounts. The results of this check show that the /etc/ftpusers file is properly configured and has the correct effective permission settings.

3.8 Audit Check AC15

AC15: Verify Use of Appropriate Warning Banners

Audit Check AC15 Results: Pass

OC: Ensure that appropriate legal notice/warning banners have been applied to the system.

CP: Perform the following functions to ensure that appropriate warning banners have been applied to the system:

As root execute the following:

```
# eeprom | grep oem-banner
```

The result should be the following:

```
oem-banner=Warning Banner Text
oem-banner?=true
```

As root execute the following:

```
cat /etc/motd /etc/issue /etc/default/telnetd /etc/default/ftpd | more
```

Each of the files should contain the appropriate warning text.

Next check the permissions and ownership for each of these banner files:

```
# ls –al /etc/motd /etc/issue /etc/default/telnetd /etc/default/ftpd
```

The output of this command should match the following:

```
-rw-r--r--   1 root     sys  /etc/default/ftpd
-rw-r--r--   1 root     sys /etc/default/telnetd
-rw-r--r--   1 root     root /etc/issue
-rw-r--r--   1 root     sys  /etc/motd
```

Next we will check the configuration of the CDE warning banners:

Review the following CDE configuration files for the appropriate value:

```
 usr/dt/config/*/sys.resources
```

or

```
etc/dt/config/*/sys.resources
```

Dtlogin*greeting.labelString:
Dtlogin*greeting.persLabelString:

An appropriate warning banner should be assigned to these values.

SC: Solaris Benchmark V1.2.0 Section 7.10, Solaris 8 Build Document p 20, Solaris 8 Essential Reference – (2nd Edition) p 282

The following screen output was captured utilizing the “script” command while executing the steps in Audit Check AC15. When applicable, notes have been added to the output for clarification purposes.

```
Script started on Sun Jun 22 12:32:00 2003
```

Check to see if a banner has been applied to the eeprom, and if it contains appropriate text:

```
sh-2.03# eeprom | grep oem-banner

oem-banner= TDS Authorized users only
oem-banner?=true
```

Review the contents of the motd, issue, telnet banner, and ftp banner files:

```
sh-2.03# cat /etc/motd /etc/issue /etc/default/telnetd
/etc/default/ftpd | more

TDS Authorized users only
TDS Authorized users only
BANNER="TDS Authorized users only"
'BANNER="TDS Authorized users only"'
```

Check the permissions of the above listed files:

```
sh-2.03# ls -al /etc/motd /etc/issue /etc/default/telnetd
/etc/default/ftpd

-rw-r--r--   1 root     sys           30 Mar  7 15:09 /etc/default/ftpd

-rw-r--r--   1 root     sys         30 Mar  7 15:08 etc/default/telnetd

-rw-r--r--   1 root     root          19 Mar  7 15:01 /etc/issue

-rw-r--r--   1 root     sys           19 Mar  7 15:01 /etc/motd
```

Review the sys.resources file for the proper banner entries for the CDE login screen:

```
sh-2.03# more /usr/dt/config/*/sys.resources |grep Dtlogin*

Dtlogin*greeting.labelString: Wobulators Inc. TDS Authorized users
only. All activity is monitored." \

Dtlogin*greeting.persLabelString: Wobulators Inc. TDS Authorized users
only. All activity is monitored."\
```

Audit Check Result Notes: While this audit check may not appear high on some individuals priority list, it has been included because not only is having warning banners proven to be a deterrent for many would be intruders, they allow help to prove due diligence, and greatly enhance the prosecutability of security incidents. I myself have been involved in investigations where this was one of the deciding factors in whether to pursue legal action one the security incident was identified, documented, investigated and the perpetrator identified.

3.9 Audit Check AC19

AC19: Ensure Account Expiration Parameters Are Set On Active Accounts

Audit Check AC19 Results: Failure

OC: Ensure that the default account expiration values are set and that they are applied to all user accounts on the system.

CP: As root perform the following:

```
# more /etc/default/passwd
```

The values in /etc/default/passwd should meet or exceed the following values:

```
MAXWEEKS=13
MINWEEKS=1
WARNWEEKS=4
PASSLENGTH=6
```

As root execute the following:

```
# logins -ox |awk -F: '($1 == "root" || $8 == "LK") { next } { $cmd = "passwd" }($11
<= 0 || $11 > 91) { $cmd = $cmd " -x 91" }($10 < 7) { $cmd = $cmd " -n 7" } ($12
< 28) { $cmd = $cmd " -w 28" } ($cmd != "passwd") { print $cmd " " $1 }'> ./no-
expire-acnt.txt
```

The expire-acnt.txt file will contain any accounts in violation of the system policy for account expiration.

SC: Solaris Benchmark V1.2.0 Section 8.3

The following screen output was captured utilizing the “script” command while executing the steps in Audit Check AC19. When applicable, notes have been added to the output for clarification purposes.

Review the /etc/default/password settings:

```
bash-2.03# more /etc/default/passwd
#ident  "@(#)passwd.dfl 1.3     92/07/14 SMI"
MAXWEEKS=13
MINWEEKS=1
WARNWEEKS=4
PASSLENGTH=6
```

Run the following command against the system user list to find any user accounts that are in violation of the password policy:

```
bash-2.03# logins -ox |awk -F: '($1 == "root" || $8 == "LK") { next } {
$cmd = "passwd" }($11 <= 0 || $11 > 91) { $cmd = $cmd " -x 91" }($10 <
7) { $cmd = $cmd " -n 7" } ($12 < 28) { $cmd = $cmd " -w 28" } ($cmd !=
"passwd") { print $cmd " " $1 }
'> ./no-expire-acnt.txt
bash-2.03#
```

Review the output of the command listed above to find any accounts in violation:

```
bash-2.03# more no-expire-acnt.txt
passwd -x 91 -n 7 -w 28 bizmark
passwd -x 91 -n 7 -w 28 sherwin
bash-2.03#
```

Audit Check Result Notes: Dormant accounts or accounts with ancient passwords are often the successful targets of brute force attacks but are also an avenue of action for former or disgruntled employees. The information technology staff and system administrators should work with the human resources department of you organization to include an “account cleansing” procedure as part of the official outprocessing procedure for departing employees.

3.10 Audit Check AC20

AC20: Verify That Least Privilege Has Been Instituted for the Home Directories of the ftp Users.

Audit Check AC20 Results: Pass

OC: All of the home directories for the TDS ftp user accounts should be protected from unauthorized viewing, or modification by other ftp account holders.

CP: Review the /etc/passwd file and ensure that all ftp users have their own unique UID and GID.

All ftp users home directories should be under /export/home. As root perform a long listing of /export/home and ensure that permissions on the ftp user directories are no more permissive than 750.

Next, login to the system via ftp as at least two different ftp users and attempt to view files in other ftp users home directories.

SC: General Best Practice

The following screen output was captured utilizing the “script” command while executing the steps in Audit Check AC20. When applicable, notes have been added to the output for clarification purposes.

Review the /etc/passwd file and ensure that all ftp users have their own unique UID and GID.

```
# more /etc/passwd
root:x:0:1:Super-User:/:/usr/bin/bash
daemon:x:1:1::/:/dev/null
bin:x:2:2::/usr/bin:/dev/null
sys:x:3:3::/:/dev/null
adm:x:4:4:Admin:/var/adm:/dev/null
lp:x:71:8:Line Printer Admin:/usr/spool/lp:/dev/null
uucp:x:5:5:uucp Admin:/usr/lib/uucp:/dev/null
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/dev/null
listen:x:37:4:Network Admin:/usr/net/nls:/dev/null
nobody:x:60001:60001:Nobody:/:/dev/null
noaccess:x:60002:60002:No Access User:/:/dev/null
nobody4:x:65534:65534:SunOS 4.x Nobody:/:/dev/null
bizmark:x:1007:6007:/export/home/bizmark:/usr/bin/bash
sherwin:x:1008:6008:/export/home/sherwin:/bin/sh
mexico1:x:1003:6003:/export/home/mexicocity1:/bin/sh
berlin7:x:1004:6004:/export/home/berlin7:/bin/sh
tokyo4:x:1005:6005:/export/home/tokyo4:/bin/sh
newyork3:x:1006:6006:/export/home/newyork3:/bin/sh
```

All ftp users home directories should be under /export/home. As root perform a long listing of /export/home and ensure that permissions on the ftp user directories are no more permissive than 750.

```
bash-2.03# cd /export/home

bash-2.03# ls -al
total 42
drwxr-xr-x  13 root     root         512 Aug 15 10:39 .
drwxr-xr-x   3 root     sys          512 Oct 14  2002 ..
dr-x------   2 berlin7  berlin7      512 Aug 15 10:38 berlin7
dr-x------   2 bizmark  bizmark      512 Mar  3  2003 bizmark
dr-x------   4 sherwin  sherwin      512 Mar  3  2003 sherwin
dr-x------   2 root     root        8192 Jan 29  2002 lost+found
dr-x------   2 newyork3 newyork3     512 Aug 15 11:16 newyork3
dr-x------   2 tokyo4   tokyo4       512 Aug 15 10:39 tokyo4
```

From the long listings above we can see that all ftpusers have an individual home directory and that these directories have an effective permission setting of 500. This will allow them to read data from their home directories, but they cannot post data to them, or view the contents of other users home directories.

Next we will verify the effective permission settings for these directories. We will login to the system via ftp as at least two different ftp users and attempt to view files in other ftp users home directories.

Connected to the TDS via ftp and login as an ftp user:

```
bash-2.03# ftp localhost
Connected to localhost.
220 TDS FTP server (TDS Authorized users only) ready.
Name (localhost:sherwin): berlin7
331 Password required for berlin7.
Password:
230 User berlin7 logged in.
```

Next switch to the /export/home directory and attempt to view other ftp users home directory contents:

```
ftp> cd ..
250 CWD command successful.
ftp> pwd
257 "/export/home" is current directory.

ftp> cd mexico1
550 mexico1: Permission denied.
ftp> cd newyork3
550 newyork3: Permission denied.
```

Finally to verify the "500" permissions on the home directory, let's attempt to copy a file to our own home directory:

```
ftp> cd /export/home/berlin7
250 CWD command successful.
ftp> pwd
257 "/export/home/berlin7" is current directory.
ftp> put testfile.txt
200 PORT command successful.
553 testfile.txt: Permission denied.
ftp> bye
221 Goodbye.
```

Connected to the TDS via ftp and login as a second ftp user:

```
bash-2.03# ftp localhost
Connected to localhost.
220 TDS ftp server (TDS Authorized users only) ready.
Name (localhost:sherwin): mexico1
331 Password required for mexico1.
Password:
230 User mexico1 logged in.
```

Next switch to the /export/home directory and attempt to view other ftp users home directory contents:

```
ftp> cd ..
250 CWD command successful.
ftp> pwd
257 "/export/home" is current directory.

ftp> cd newyork3
550 newyork3: Permission denied.
ftp> cd tokyo4
550 tokyo4: Permission denied.
```

Finally to verify the "500" permissions on the home directory, let's attempt to copy a file to our own home directory:

```
ftp> cd /export/home/mexico1
250 CWD command successful.
ftp> pwd
257 "/export/home/mexico1" is current directory.
ftp> put testfile.txt
200 PORT command successful.
553 testfile.txt: Permission denied.
ftp> bye
221 Goodbye.
```

Audit Check Result Notes: From the results of the audit check procedures we can determine that the principal of least privilege has been implemented on the TDS for the ftp users to a very high degree. A normal ftp user can not view other ftp user files and they can not post any data to their home directories. This will help to prevent information leakage and the misuse of the TDS for unauthorized file transfers. It should be noted that ftp users on the TDS will still be able to view the local file system because the standard Solaris ftp server does not run in (and does not support) a "chroot" or "jail" environment.

Measure Residual Risk

3.11 Qualitative Assessment of Individual Findings

Table 5. summarizes the individual audit checks addressed in section 3 of this document, the results of the audit check in a pass or failure format, a brief summary of any mitigating factors or controls, and finally the associated residual risk associated with the findings of that particular audit check.

Table 5. Summary of Audit Check Results

Audit Check	Result	Mitigation/Controls	Residual Risk
AC1: Operating System Security Patches	Failure	Limiting the number of operational and thus exposed network services, and providing protection from remote attackers via a stateful inspection firewall helps to mitigate this finding to a minimal degree. However, the Wobulators Inc. firewall has a very liberal rule set for the DMZ that exposes the TDS to much more potentially hostile traffic than should be permitted. There also is no logical segmentation within the DMZ other than an unmanaged switch, and any host within it that becomes compromised is a serious threat to the TDS. There is not a large base of system users on the TDS, but those non-admin accounts are accessed from off site machines that the system administrators have no control over. The two main network services on the TDS (telnetd, and ftpd) are exposed to the public net without restriction and both are vulnerable to serious remote exploits. Additionally, TCP_Wrappers is not deployed on the TDS expanding the potential points of origin for attack on the TDS to all systems connected to the internet. The presence of kernel level auditing and the diligent review of system audit logs helps mitigate this issue by providing the system administrators with the ability to detect malicious activity.	High
AC2: Verify Use and Proper Operation of TCP Wrappers	Failure	Limiting the number of operational TCP network services and thus exposure to potential attack, and providing protection from remote attackers via a stateful inspection firewall helps to mitigate the absence of the TCP Wrappers to a certain degree. As stated in the Mitigation/Controls section for Operating System Security Patches, the Wobulators Inc. firewall has a very liberal rule set for the DMZ that exposes the TDS to much more potentially hostile traffic than should be permitted. Once again, the two main network services on the TDS (telnetd, and ftpd) are exposed to the public net without restriction and both are vulnerable to serious remote exploits. The absence of TCP Wrappers opens up the	High

Audit Check	**Result**	**Mitigation/Controls**	**Residual Risk**
		opportunity for exploit of these conditions from any host with a route to the TDS. The presence of kernel level auditing and the diligent review of system audit logs helps mitigate this issue by providing the system administrators with the ability to detect malicious activity.	
AC3: Secure Shell (SSH) Installed and Operational	Failure	The absence of a Secure Shell installation on the TDS is a great concern. All of the core responsibilities of the TDS could be fulfilled by SSH, thus eliminating much of the operational risk now associated with the TDS at a minimal price point. At this time there are no significant mitigators for the absence of an ssh implementation. The presence of kernel level auditing and the diligent review of system audit logs helps mitigate the issue by providing the system administrators with the ability to detect malicious activity.	High
AC4: Verify the Minimization of All Nonessential Network Services	Failure	While there has been some service minimization performed on the TDS, there still are many unnesessary and potentially dangerous services being launched by inetd. Additionally there are other vulnerable services on the system that are started from run level directories. These factors combined with an entirely too liberal firewall policy, and the absence of operating system security patches, make for a dangerous situation. The presence of kernel level auditing and the diligent review of system audit logs helps mitigate the issue by providing the system administrators with the ability to detect malicious activity.	High
AC6: Verify Usage of Strong TCP Sequence Numbers	Pass	The proper implementation of Strong (random) TCP sequence number will help protect the TDS and attached clients from spoofing, TCP injection and man in the middle attacks.	None
AC8: Verify Kernel Level Auditing is in Use	Pass	Sun Solaris BSM or C2/kernel level auditing has been implemented on the TDS in an acceptable fashion. The current configuration provides a good balance between resource utilization and thoroughness of audit.	None
AC13: Verify the Existence, Contents and Permissions of an /etc/ftpusers file	Pass	The ftpusers file on the TDS in properly configured and provides protection against system account activity being conducted via ftp.	None
AC15: Verify Use of Appropriate Warning Banners	Pass	The TDS contained appropriate warning banners.	None

Audit Check	Result	Mitigation/Controls	Residual Risk
AC19: Ensure account expiration parameters are set on active accounts	Failure	While the default password aging parameters were properly applied to the system, there were two accounts on the system that did not adhere to the policy. The fact that all users on the TDS are trusted insiders, and thorough auditing and logging is operational recording security relevant activity, and the logs are regularly reviewed, mitigates this issue to a great degree.	Low
AC20: Verify That Least Privilege Has Been Instituted for the Home Directories of the ftp Users.	Pass	The system was configured to restrict ftp users from writing to or viewing the contents of other ftp users home directories. Additionally, the ability of users to write data to their home directories has been disabled, further limiting the opportunity of authorized or unauthorized users from misusing the system for illicit purposes.	None

3.12 Overall Qualitative Residual Risk Assessment of the TDS

Given the significance of the operational functionality of the TDS in acting as the primary intellectual property distribution point for Wobulators Inc, and the severity and number of serious threat conditions that exists on the system in its current state, the overall risk level to the TDS, and in turn Wobulators Inc. is considered to be very high.

When the operational environment is taken in to consideration, with the firewall not providing proper preventive security controls, by allowing malicious network traffic to reach the systems most critical flaws (the remote root exploits present in the Telnet, FTP, and SMTP servers) the risk condition, and threat to the system and its key assets, is considered to be exceptionally severe.

While the audit shows that the operational and environmental risks to the TDS are unacceptable, these conditions can be quickly and inexpensively rectified.

By applying operating system security patches, all of the most severe risk conditions can be eliminated. Shifting the data distribution mechanism from the File Transfer Protocol, to Secure Shell, and adding an additional interface card to the firewall, modifying the IPTables configuration to place the TDS on its own network segment with SSH being the only network protocol permitted to flow either inbound or outbound to the TDS will essentially eliminate all of the existing risks now associated with the TDS. All of this can be accomplished with minimal cost and user training. Once these recommendations are implemented, the TDS, and in turn the most important company assets will be operating in an exponentially more secure fashion.

3.13 Evaluation of the Audit

While the contract limited the audit in scope to the TDS itself, I felt that the audit would not have been complete without addressing the network infrastructure and operational environment and how these factors contribute to the overall risk posture. The extra time spent on evaluating the TDS network traffic exposure and the effects of the DMZ environment upon the risk posture of the TDS was in turn time well spent, and provided great value to the customer because it uncovered the fact that the firewall and DMZ configuration/structure did not provide (or provided a false sense of protection) adequate protection/mitigation for the security issues uncovered with the TDS during the course of the audit. The overall goal of the audit was to determine the existing risks to the TDS, the potential of these risks for exploit, and in turn the effectiveness of the controls placed on the intellectual property of the company. The audit was able to achieve all of these.

The audit itself was conducted over the course of a Sunday, thus providing minimal distraction for the staff during normal business hours. Executing the audit during non business hours provided the system administrators with the ability to "ride shotgun" and use the audit as a learning experience and as the guidepost for future self-assessment. With the limited scope (one system) the audit itself was easily completed and the goals of the endeavor accomplished within the timeframe allotted.

The customer expressed satisfaction with how the audit was conducted, the scope of the audit, and the how the audit addressed their primary concerns and objectives:

- *What are the operational risks to the system?*

  In its current configuration, and operating environment the TDS was found to have several serious security vulnerabilities, including remotely exploitable root-level vulnerabilities that place the companies "crown jewel" intellectual property in a very high-risk situation. Additionally, it was determined that the ftp protocol does not offer sufficient protection from client or server impersonation (potentially leading to data/account compromise), nor sufficient protection from interception or manipulation of sensitive company data/system credentials in transit across the Internet. One of the primary objectives of the audit was to determine what risks the TDS and in turn the companies intellectual property was exposed to, and this was accomplished to their satisfaction.

- *What factors do we have in place to mitigate these risks?*

  As a result of the audit, it was determined that the current perimeter security configuration for the Wobulators Inc. network does not provide adequate protection for the TDS. None of the most serious threat exposures existing on the TDS were mitigated by the firewalls current configuration. The absence of a properly configured and operational installation of TCP Wrappers on the TDS compounded this issue by expanding the threat exposure of these vulnerabilities to effectively every routable IP address on the Internet.

The audit was able to identify that the current risk exposure of the TDS was not without some mitigating factors. An effective implementation of least privilege for TDS users enforced by restrictive file permissions limited the potential for extensive compromise of intellectual property by compartmentalizing sensitive data, and limiting the potential for privilege escalation on the system. It was also uncovered by the audit that detective security controls in the form of kernel level auditing and system logging in place on the TDS provides administrators with the ability to detect and determine the scope of malicious or suspect activity on the system in a timely and accurate manner.

- *What can be done to address the risks to our system, and what are the costs?*

  As a result of the analysis of the findings of the audit, and a review of the capabilities of the existing TDS hardware/software, along with the Wobulators Inc network infrastructure, a roadmap for the rectification of the risks uncovered in the audit was formulated. The costs incurred to Wobulators Inc. to perform this rectification were minimized by the auditor advising management and the system administrators how to better utilize the capabilities of their existing equipment, modify the network architecture to minimize threat exposure, fully utilize the capabilities of freely available open source software, and instituting security best practices. The end result would be an exponential increase in the overall system security posture on a small investment of hardware and system administrative man-hours.

- *Can we use the audit as a leaning experience to help develop practices and procedures that we can utilize to perform future self-assessments?*

  Wobulators Inc. system administrators and management staff witnessed the entire audit, actively asked questions, and took detailed notes on the procedures. In addition they were furnished with the audit checklist, the audit results, and a list of technical references upon completion of the engagement. They verbally expressed satisfaction with the level of detail of the audit, and the desire to implement the “lessons learned” from the engagement on their remaining Sun Solaris systems. The Wobulators Inc. staff also indicated the desire to institute a program of periodic self-assessment based upon my audit.

- *Did the audit provide a good overall level of value to the organization?*

  In terms of the return on investment, the Wobulators Inc. management expressed great satisfaction with the way the audit was conducted in both time and scope (although not with the results). It was also requested that I return on a regular basis for comparable follow-up assessments on their remaining systems.

4 Assignment 4 – Audit Report

4.1 Executive summary

The primary objective of the audit was to provide a system risk evaluation and security configuration assessment, for one system, the Wobulators Inc. Sun Solaris based Technology Distribution Server (TDS). This system houses, and controls the dissemination of the key intellectual property assets of Wobulators Inc. Any risks to this system, or the data that it contains should be of great concern to the company.

During the course of the audit a number of serious system security concerns were uncovered. Three of the security concerns (associated with the ftp, telnet and smtp servers on the system) involved remotely executable root-level exploits to the system, that could allow a remote attacker to gain complete control of the system from almost any system on the internet., none of which were mitigated by the Wobulators Inc. firewall. The existence of these exploits, in conjunction with the poorly configured network perimeter firewall create a very high risk situation for the TDS and in turn Wobulators Inc.

It is strongly recommended that immediate action be taken to rectify both the system configuration issues and the resultant security risks found with theTDS, and the current DMZ configuration that facilitates a very high potential for exploit of the these security risks.

Once the immediate security risks to the system are addressed by the application of required operating system security patches, the disabling of unnesessary network services, and the reconfiguration of the Wobulators Inc. firewall so that the threat exposure to the TDS is minimized, a more secure data transmission mechanism should be implemented. The current data transmission mechanism, the file transfer protocol (ftp), has a number of security issues associated with it that should be of concern to the Wobulators Inc. organization. The file transfer protocol does not provide protection against client or server impersonation, and it transmits account credentials and proprietary data unprotected by encryption across the Internet where they are vulnerable to interception, or manipulation in transit. It is strongly recommended that as soon as practical the current data transmission mechanism (ftp) be replaced by Secure Shell (ssh). Secure Shell will protect the TDS and its clients against impersonation attacks, and provide appropriate protection for account credentials and proprietary data by the use of strong end-to-end encryption between the TDS and remote clients. Secure shell can also be used in place of telnet for system administration tasks, providing the same strong level of protection for administrative accounts and activities.

4.2 Technology Distribution Server Audit Findings

Table 6 lists the results of the individual Audit Checks conducted as part of the security audit of the TDS, the results of those checks in a Pass or Failure format, any existing mitigating factors or compensatory controls, the resulting residual risks to the TDS associated with the Pass or Failure in conjunction with any mitigating/compensatory factors, and finally any remedial actions required to address the risks associated with that particular finding as well as an estimated cost for remediation.

Table 6 Audit Findings

Audit Check	Result	Mitigation/Compensating Controls	Residual Risk	Remediation Steps/Cost
AC1: Ensure All Applicable Operating System Security Patches Are Installed	Failure	Limiting the number of operational and thus exposed network services, and providing protection from remote attackers via a stateful inspection firewall helps to mitigate this finding to a minimal degree. However, the Wobulators Inc. firewall has a very liberal rule set for the DMZ that exposes the TDS to much more potentially hostile traffic than should be permitted. There also is no logical segmentation within the DMZ other than an unmanaged switch, and any host within it that becomes compromised is a serious threat to the TDS. There is not a large base of system users on the TDS, but those non-admin accounts are accessed from off site machines that the system administrators have no control over. The two main network services on the TDS (telnetd, and ftpd) are exposed to the public net without restriction and both are vulnerable to serious remote exploits. Additionally, TCP_Wrappers is not deployed on the TDS expanding the potential points of origin for attack on the TDS to all systems connected to the internet.	High	**Remediation Steps:** A minimum of monthly, apply the Recommended Patch Cluster, or at least those patches from the cluster that contain security fixes. The patch cluster is available from Sun Microsystems at: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access It is apparent that the existing operating system patch methodology (applying individual patches) is not maintaining a sound and secure system configuration, and in turn leaving the TDS unnecessarily vulnerable to several widely known and exploited security vulnerabilities. It should be noted that three of the most significant findings of the audit could have been prevented by keeping the system current with vendor supplied security patches. Install TCP_Wrappers on the TDS and configure /etc/hosts.deny for to ALL:ALL. Enter IP Address of only explicitly permitted hosts in to /etc/hosts.allow. This step will limit exposure of the TDS to this vulnerability until further measures can be taken. A TCP_Wrappers package is available for Solaris 8 from http://www.sunfreeware.com **Cost:** Minimal Bandwidth to download patch cluster (approximately 90MB) or individual patches containing security fixes, and time for administrator to install the patch cluster or patches.

Audit Check	Result	Mitigation/Compensating Controls	Residual Risk	Remediation Steps/Cost
		The presence of kernel level auditing and the diligent review of system audit logs helps mitigate the issue by providing the system administrators with the ability to detect malicious activity.		
AC2: Verify Use and Proper Operation of TCP Wrappers	Failure	The absence of the TCP Wrappers application in conjunction with the remotely executable root exploits found on the system, and the fact that the firewall is offering negligible protection against these threats makes for a very dangerous situation. This is particularly true when the fact that the TDS is responsible for protecting key intellectual property assets of Wobulators Inc. In the systems current configuration, the presence of kernel level auditing and the diligent review of system audit logs combined with the small system user base, and tightly implemented "least privilege" for these users, does help mitigate the threats to the system to a degree.	High	**Remediation Steps:** Download and install the TCP_Wrappers package for Solaris 8. Configure /etc/hosts.deny for to ALL:ALL. Enter IP Address of only explicitly permitted hosts in to /etc/hosts.allow. This step will limit exposure of the serious vulnerabilities found on the TDS until further measures can be taken. A TCP_Wrappers package is available for Solaris 8 from http://www.sunfreeware.com **Cost:** Approximately two hours of system administrators time and bandwidth to download the TCP Wrappers package**.**

Audit Check	Result	Mitigation/Compensating Controls	Residual Risk	Remediation Steps/Cost
AC3: Determine if Secure Shell (SSH) is installed and operational.	Failure	The absence of a Secure Shell installation on the TDS is a great concern. All of the core responsibilities of the TDS could be fulfilled by SSH, thus eliminating much of the operational risk now associated with the TDS at a minimal price point. At this time there are no significant mitigators for the absence of an ssh implementation. The presence of kernel level auditing and the diligent review of system audit logs helps mitigate the issue by providing the system administrators with the ability to detect malicious activity.	High	**Remediation Steps:** Download and install OpenSSH packages. All required packages and detailed documentation is available from: http://www.sunfreeware.com/openssh8.html Install TCP_Wrappers on the TDS and configure /etc/hosts.deny for to ALL:ALL. Enter IP Address of only explicitly permitted hosts in to /etc/hosts.allow. This step will limit exposure of the TDS to this vulnerability until further measures can be taken. A TCP_Wrappers package is available for Solaris 8 from http://www.sunfreeware.com **Cost:** Approximately five hours of system administrator's time and bandwidth to download OpenSSH packages or source and install and configure.
AC4: Verify the Minimization of All Nonessential Network Services	Failure	While there has been some service minimization performed on the TDS, there still are many unnesessary and dangerous services being launched by inetd in addition to the other vulnerable services on the system that are started from run level directories. As shown by the security patch analysis, the TDS is vulnerable to a number of remotely executable root exploits. This condition poses a great threat to the TDS, and the intellectual property of Wobulators Inc. These factors combined with an entirely too liberal firewall policy, make for a dangerous situation. There currently are no significant mitigating factors in place that counteract the severity of this condition. The presence of kernel level auditing and the diligent review of system audit logs helps mitigate the issue by providing the system administrators with the ability to detect malicious activity.	High	**Remediation Steps:** **Interim:** Remove all but essential services (telnet, ftpd, and X11) from the inetd configuration file or run level directories. Install TCP_Wrappers on the TDS and configure /etc/hosts.deny for to ALL:ALL. Enter IP Address of only explicitly permitted hosts in to /etc/hosts.allow. This step will limit exposure of the vulnerabilities on the TDS until further remediation measures can be taken. A TCP_Wrappers package is available for Solaris 8 from http://www.sunfreeware.com **Final:** Remove all services from inetd configuration file (create blank file) install SSH and utilize sftp in place of traditional ftp, and ssh in place of telnet. If remote X session will be used on the TDS, port forwarding for X11 should be enabled for ssh and all X sessions tunneled to the remote clients via ssh. Ensure that the system is monitored closely for malicious activity, and be sure to maintain currency with the vendor supplied operating system security patches. **Cost:** Approximately five to eight hours of system administrator's time and bandwidth to download OpenSSH package or source and install and configure.

Audit Check	Result	Mitigation/Compensating Controls	Residual Risk	Remediation Steps/Cost
AC6: Verify Usage of Strong TCP Sequence Numbers	Pass	The /etc/default /inetinit configuration file TCP_STRONG_ISS variable is defined with a 2. This configures the operating system to use strong random TCP sequence numbers and will help the TDS and its clients from becoming susceptible to TCP injection attacks, spoofing or man in the middle attacks.	None	**Remediation Steps:** None required **Cost:** None
AC8: Verify Kernel Level Auditing is in Use and Properly Configured	Pass	Sun Solaris BSM or C2/kernel level auditing has been implemented on the TDS in an acceptable fashion. The current configuration provides a good balance between resource utilization and thoroughness of audit.	None	**Remediation Steps:** None required **Cost:** None
AC13: Verify the Existence, Contents and Permissions of the /etc/ftpusers File	Pass	The ftpusers file on the TDS in properly configured and provides protection against system account activity being conducted via ftp.	None	**Remediation Steps:** None Required **Cost:** None
AC15: Verify Use of Appropriate Warning Banners	Pass	The TDS contained appropriate warning banners.	None	**Remediation Steps:** None Required **Cost:** None
AC19: Ensure Account Expiration Parameters Are Set On Active Accounts	Failure	While the default password aging parameters were properly applied to the system, there were two accounts on the system that did not adhere to the policy. The fact that all users on the TDS are trusted insiders, and thorough auditing and logging is operational recording security relevant activity, and the logs are regularly reviewed, mitigates this issue to a great degree.	Low	**Remediation Steps:** Edit the /etc/shadow file and apply the proper password aging to the following accounts: bizmark sherwin **Cost:** Approximately 30 minutes of system administrator's time.

Audit Check	Result	Mitigation/Compensating Controls	Residual Risk	Remediation Steps/Cost
AC20: Verify That Least Privilege Has Been Instituted for the Home Directories of the ftp Users.	Pass	The system was configured with restrictive permission settings for all remote user account home directories. The permission setting of 500 will prevent other system users from viewing, reading data from, or writing data to other user home directories. Additionally users could not write data to their home directories, preventing the TDS from being utilized for unauthorized file transfer or storage. These permission settings will have a positive impact on the overall security posture of the TDS.	None	**Remediation Steps:** None Required **Cost:** None

4.3 Network Traffic Exposure Risks Posed to the TDS

The Wobulators Inc. firewall permitted undue exposure of the systems most severe risk factors to the essentially the entire internet. By configuring the firewall ruleset as a DMZ wide policy in place of a system by system policy for systems within the DMZ, the TDS is placed in a position of great risk for compromise. The Wobulators Inc firewall essentially is providing a false sense of security to the system administrators in regards to the overall security of the TDS and the key information assets that reside on the system.

Table 7. Network Traffic Exposure Findings

Service	TCP/UDP Port	Threat Exposure for TDS
ftp (Active)	20,21 TCP/UDP	**HIGH**: TDS has vulnerabilities to globbing attack and potential denial of service conditions exposed by this port being open to inbound and outbound traffic. Consult http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=111606 for further details.
Telnet	23 TCP/UDP	**HIGH**: TDS has vulnerabilities to a remotely executable buffer overflow and to a denial of service condition. Consult http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=110668 for further details.
SMTP	25 TCP/UDP	**HIGH**: TDS is vulnerable to a number of serious security issues. Consult http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=110615 for further details.
DNS	53 TCP/UDP	None
HTTP	80 TCP/UDP	Moderate
POP3	110 TCP/UDP	None
MS RPC	135 TCP/UDP	None
IMAP	143 TCP/UDP	None
LDAP	379,389, 636, 3268 TCP/UDP	None
HTTPS	443 TCP/UDP	None
SMTP (SSL)	465 TCP/UDP	None
LSA	691 TCP/UDP	None
IMAP4 (SSL)	993 TCP/UDP	None
POP3 (SSL)	995 TCP/UDP	None
MAPI	5001,5002,5003 TCP/UDP	None

Remediation Steps:

Initially the firewall should be reconfigured to block all but active ftp access to the TDS. This can be accomplished by applying the following configuration changes to the IPTables configuration on the firewall:

```
$IPTABLES -A FORWARD  -i eth1 -p tcp  --source-port 20  -d xx.xx.xx.xx  --destination-port 1024:65535  -m state --state NEW  -j
eth1_In_RULE_0

$IPTABLES -A FORWARD  -i eth1 -p tcp  -d xx.xx.xx.xx  --destination-port 21  -m state --state NEW  -j eth1_In_RULE_0

$IPTABLES -A eth1_In_RULE_0   -j LOG  --log-level info --log-prefix "RULE 0 -- ACCEPT "
$IPTABLES -A eth1_In_RULE_0   -j ACCEPT
$IPTABLES -N eth1_Out_RULE_0
$IPTABLES -A OUTPUT  -o eth1 -p tcp  --source-port 20  -d xx.xx.xx.xx  --destination-port 1024:65535  -m state --state NEW  -j
eth1_Out_RULE_0

$IPTABLES -A OUTPUT  -o eth1 -p tcp  -d xx.xx.xx.xx  --destination-port 21  -m state --state NEW  -j eth1_Out_RULE_0

$IPTABLES -A FORWARD  -o eth1 -p tcp  --source-port 20  -d xx.xx.xx.xx  --destination-port 1024:65535  -m state --state NEW  -j
eth1_Out_RULE_0

$IPTABLES -A FORWARD  -o eth1 -p tcp  -d xx.xx.xx.xx  --destination-port 21  -m state --state NEW  -j eth1_Out_RULE_0

$IPTABLES -A eth1_Out_RULE_0   -j LOG  --log-level info --log-prefix "RULE 0 -- ACCEPT "
$IPTABLES -A eth1_Out_RULE_0   -j ACCEPT
```

Where the IP Address of the TDS is substituted for the xx.xx.xx.xx. Once this is applied be sure to restart the firewall and make sure that all remote clients are making their connections with clients configured for active ftp sessions.

As soon as time permits, add an additional network card to firewall to create a segment specifically for the TDS. At the firewall Allow ONLY inbound and outbound SSH connections to this segment, and in turn the TDS. An additional rule set that explicitly allows connections only from the machines located at the manufacturing facilities (or their ISP if they receive their address from DHCP) can be added to provide an additional layer of access control to the system.

Cost: 10/100 PCI Based Ethernet Card: $80.00 and approximately 3-5 hours of system administrator's time.

4.4 Overall System Risk Level Summary

Overall the risk level associated with the Technology Distribution Server (TDS) in its current configuration and network environment is considered to be **very high.**

The TDS is a public facing system with multiple serious remotely executable vulnerabilities on three different system network daemons (ftpd TCP 21, telnetd TCP 23 and SMTP (Sendmail) TCP 25). None of witch is filtered/protected properly by the firewall.

The probability of a successful attack occurring against any one of these three vulnerabilities, leading to a root level compromise of the system is extremely likely. In fact, it surprising that this has not happened already. However, it should be noted that the audit revealed no indications of a compromise (although a complete forensic analysis was outside the scope of this engagement).

It is strongly recommended that the system administrators take immediate action to rectify the security issues uncovered by the audit of the TDS. The results of the audit show that there is an unacceptable level of risk associated with the operation of the TDS in its current configuration and level of network traffic exposure.

Initially the firewall should be reconfigured to block all but active ftp access to the TDS. Immediately after this, all system patches should be applied (after proper testing on another system), and the telnet, SMTP and RPC servers disabled and /or removed from the system as well as all other unnesessary network services. As soon as practical the secure shell suite of applications should be installed on the TDS, and all user activity moved to sftp and the ftp server subsequently disabled (but kept installed on the system for contingency purposes). Next, an additional network interface should be installed in the firewall and the TDS moved to its own DMZ leg that only allows ssh traffic both inbound and outbound. This will not only provide granular network traffic control over the system, but it will also protect the TDS in the event another system within the DMZ is compromised. If for any reason all of these recommendations cannot be immediately implemented, at a minimum it is recommended that the latest Sun Solaris 8 patch cluster (or at the very least those patches containing security fixes) be installed on the TDS to address the most severe of the existing security issues. Followed by the firewall modification, the remaining network service minimization, installation of the ssh packages, and finally the movement of the TDS to its own independent DMZ segment.

The total costs for Wobulators Inc. to correct most of the risk factors addressed in this audit report are minimal when the existing threats to the system are considered. Approximately two working days of system administrator time and some bandwidth to download the required operating system patches and other required packages or source code.

It would require only a small additional investment to isolate the TDS on its own DMZ leg and upgrade all of the system functionality from ftp and Telnet to the more secure ssh equivalents.

The cost to Wobulators Inc. of a security incident involving the compromise of the TDS could be catastrophic. The compromise of company intellectual property and the negative publicity associated with a security incident would undoubtedly prove detrimental to the economic performance of the company against future prospects. The cost to rectify the existing security issues is literally a few hundred dollars and a few man-days. There is no investment in expensive hardware, new software applications, or extensive administrator training required to greatly enhance the overall security posture of TDS and in turn Wobulators Inc. When this is weighed against the costs of a high visibility security incident, or the dissemination of intellectual property to competitors or foreign nationals, the choice of whether to address the security risks uncovered by this audit in a timely manner should be apparent.

5 List of References

5.1 Publications

Solaris Benchmark v1.2.0 February 19, 2003
Copyright 2001-2003, The Center for Internet Security (CIS)
http://www.cisecurity.org/

Practical Unix and Internet Security (2nd Edition)(3rd Edition now available) – By Simson Garfinkel and Gene Spafford: Copyright 1996 O'Reilly & Associates, Inc ISBN: 1-56592-148-8

Solaris Security – A concise guide to maintaining secure systems in the Solaris Environment – By Peter H. Gregory: Copyright 2000 Prentice-Hall, Inc – ISBN: 0-12-096053-5

Solaris 8 Essential Reference – (2nd Edition) – By John P. Mulligan Copyright 2001 New Riders Publishing – ISBN: 0-7357-1007-4

Hack Proofing Sun Solaris 8 – By Wyman Miles, Ed Mitchell, F. William Lynch Technical Editor Randy Cook: Copyright 2001Syngress Publishing, Inc – ISBN: 1-928994-44-X

Solaris 8 Build Document: By Gideon Rasmussen, CISSP Information Security Manager for Infosctruct LLC. Available from:
http://www.sun.com/bigadmin/content/submitted/Solaris_build_document.pdf

5.2 Internet Websites

Center for Internet Security
http://www.cisecurity.org/

SANS Reading Room
http://www.sans.org/rr/

Sun Microsystems BluePrints Online
http://www.sun.com/solutions/blueprints/online.html

Solaris Security Toolkit (JASS)
http://www.sun.com/software/security/jass/

Sun Microsystems SunSolve Online
http://www.sunsolv.sun.com/

System Administrators Guild “Building a Solaris Host”
http://sageweb.sage.org/resources/online/solaris/solaris/checklist.html#Install

Nmap stealth port scanner
http://www.insecure.org/

Information Systems and Technology University of Waterloo
http://ist.uwaterloo.ca/security/howto/2000-08-17/

Sun Microsystems Recommended and Security Patch Clusters
http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access

Sun Solaris Fix-Modes Application (Made available by the Center for Internet Security)
ftp.CISecurity.org/pub/pkgs/Solaris/fix-modes.tar.Z

Solaris 2.x - Tuning Your TCP/IP Stack and More
http://www.sean.de/Solaris/soltune.html

Sun Freeware (Prebuilt Solaris Packages) SSH and TCP_Wrappers or Solaris 8
http://www.sunfreeware.com