Global Information Assurance Certification Paper

Audit of a Distributed Solaris ™ Jumpstart Infrastructure: An Auditor's Perspective

Michael Meacle
GSNA Practical Assignment Version 2.1
Option 1

Abstract

The impossible dream; scalable, secure, flexible and reproducible server building with unquestioned integrity.

As soon as your organisation starts managing more than a handful of servers the bean counters are looking for economies of scale. But we all know how hard it is to build and maintain a server that is fast, secure and easy to maintain.

Enter Solaris™ Jumpstart, a tool by Sun that allows easy building of servers and coupled with another tool JASS (JumpStart Architecture and Security Scripts now known as Solaris™ Security Toolkit [3]) can build a new server efficiently and reasonably secure. But we have one problem, Jumpstart relies on swag of notoriously insecure protocols. In addition we are all taught to always verify your media's integrity yet Jumpstart makes it all available via nfs derived from ufs file system; hardly as immutable as a vendor supplied and verified cd -rom.

So have convenience, flexibility and scalability come at a cost to integrity upon which all your new servers are built from.

In this audit I review a Distributed, Lights-Out implementation[1] of Solaris™ Jumpstart to determine if it is in fact an 'Impossible Dream' of a System administrator.

Table of Contents

Table Of Checklists

Table Of Audits

Table of Stimulus / Response

Table of Residual Risks

.

1. Assignment 1: Research in Audit, Measurement Practice, and Control

1.1. Identify the system to be audited

The purpose of this audit is to review ACME Corp new Distributed Solaris ™ Jumpstart infrastructure. The primarily reasons why both the Information Technology Manager and Chief Security Officer of ACME Corp have requested and support ed the audit are:

- Over the next two years it is expected in excess of 2000 servers will have been built from it.
- Jumpstart methodology is also used as part of ACME Corp business continuity plan to minimise downtime.

So who is ACME Corp, it is a large geo graphically distributed company renamed for the purposes of this audit due to restrictions placed on me by ACME Corp Chief Security Officer who contracted the organisation where I work for this audit.

The distributed Jumpstart infrastructure is housed in three geographically separated data centres. All centres' Jumpstart infrastructure is the same consisting of:

1 * Jumpstart Server
- Sunfire V100
- Solaris™ 8
- JASS 0.3
- openSSH

1 * Cisco terminal server (16 rs232 ports)
- Cisco 2511rj

1 * Cisco core router
- Cisco 2600

N * Sun Sparc servers

All Jumpstart servers are the same with one exception, one of them, the one at Server Hosting Site A. This one is deemed as being the 'Master' and is labelled as such in the following diagram. All configuration and management of the whole jumpstart directory tree is done on this server, then through the use of scripts synchronised both on demand and via overnight scheduled synchronisation operations. The others will be collectively referred to as 'Slaves', one slave is also depictured in the following diagram. The master and thus slaves also contain all current vendor patches for OS and applications in use within ACME Corp.

Jumpstart framework requires three distinct parts: [2] (page 3)

- Boot : Server provides a fail -safe OS to a client
- Configuration : Server provides a profile to the client
- Install : Server repository of OS and required software

You can install all components on one server or across multiple servers the only restriction is you need at least one 'Boot Server' per seg ment. ACME Corp decided to install all three components on all Jumpstart servers thus allowing smaller WAN links.

ACME Corp have decided to put two LAN segments per data centre. This has been done purely to increase each data centre LAN capacity. To minim ise the number of Jumpstart servers required each has been equipped with two fast Ethernet NIC's with one connected per segment.

As ACME Corp does not have staff nominally located at any of the Data Centres they have installed one terminal server per data centre to allow remote virtual console access from their workstations.

To facilitate hardening of new hosts and of the Jumpstart servers themselves, JASS[3] a hardening package from Sun has been integrated into the Jumpstart infrastructure.

There is basic http only connectivity of users to the Internet via individually authenticated proxy. All traffic is scanned for virus, Trojans and certain objects are disabled e.g. Java. In addition there is no incoming connections allowed from the Internet except email , which goes via a scanning relay. Additionally a multi stage multi vendor firewall is used. None of this is shown on the diagram both for simplicity and confidentiality.

My brief was to provide an audit of the Jumpstart servers and associated infrastructure.

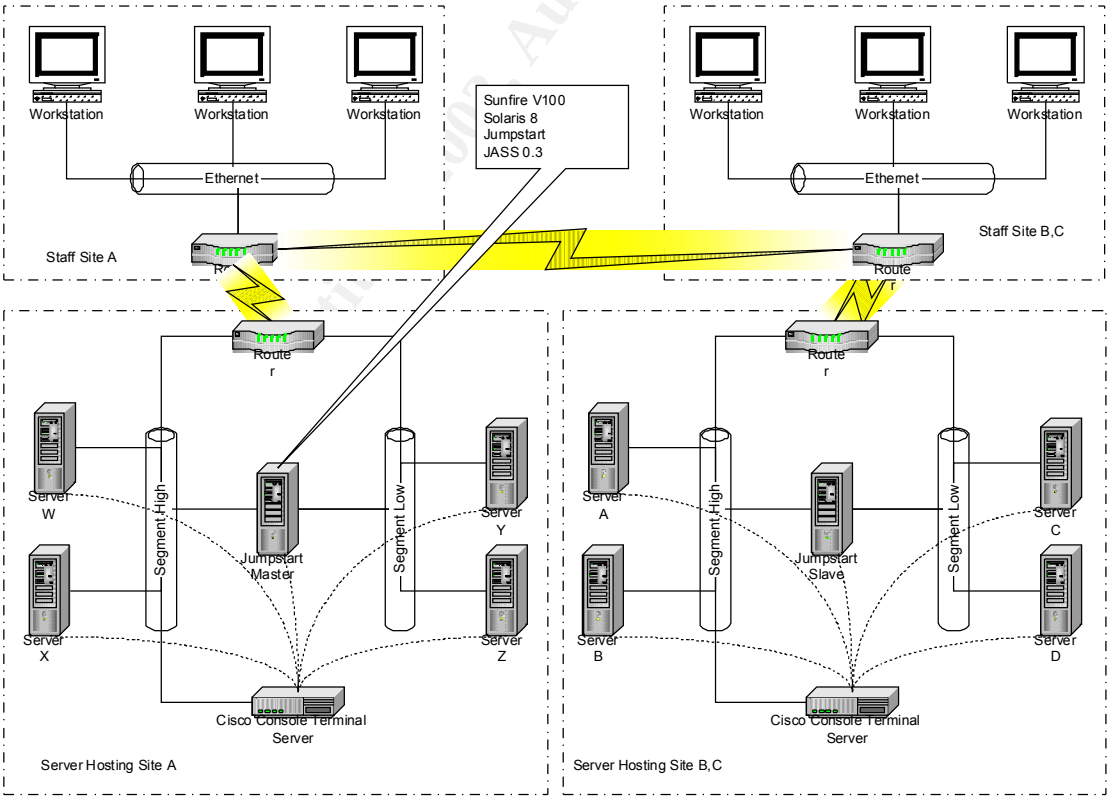


Diagram 1: ACME Corp Network Diagram

1.2. Evaluate the risk to the system

There are three primary areas of concern:

- Jumpstart server themselves
- Console servers
- Services required by Jumpstart being available to unknown cli ents

Following is a tabulated form of identified potential risks, the likelihood of them occurring, the consequences of it happening along with an indicative effective risk.

Risk Item	Probability	Consequences	Effective Risk
Not patching Jumpstart servers in a timely manner.	Medium	Known security vulnerabilities, which could be avoided by timely patching, remain on active servers longer than optimum.	Medium / High
Sniffing confidential console traffic.	Medium	Someone internal to ACME Corp could sniff a root password.	High
Services required for Jumpstart are left enabled when not in use.	High	Someone internal to ACME Corp would be able to completely analyse /jumpstart nfs share.	High
Ineffective or no change management resulting in all new clients being added to the Jumpstart server differently.	Medium	No consistent or efficient procedures used to add new clients resulting in everyone doing it 'their-way'	Medium
Changes go unnoticed.	Medium	An undetected intruder could substitute a program with a Trojan version.	High
Builds based on OS minimisation.	High	The less minimisation up front requires more ongoing maintenance effort to attain equivalent effective security.	High

Ineffective management of users obtaining access to Jumpstart infrastructure.	Medium	Individual's other than those who should have access gain access to core infrastructure.	High
Slave servers don't remain fully synchronised with the master.	Medium	New Servers built from a Slave server won't be built correctly.	Medium
Synchronisation between Master and Slaves is compromised because encryption is not used.	Medium	The synchronisation account and password may be sniffed. An adversary could then use these credentials to compromise the integrity of any Slave.	High

The focus of this audit will be on the Jumpstart servers and only where necessary on the Terminal server and Cisco WAN router. I have intentionally not done a thorough audit on either the Cisco router and the Cisco terminal server as there is already a large amount of information available. [4] and [5] What's more the audit would become too large and unfocused. Thus it will be assumed for the purpose of this audit best practice is currently being performed on both Cisco devices.

1.3. What is the current state of practice

The central component to this audit is a number of Solaris ™ Jumpstart servers. The approach I took in identifying the current state of practice was:

- Identify what practices are used within ACME Corp
- Identify what could be found on the internet
- Read vendor documentation
- Read book on the Jumpstart

Considering the penetration of Sun hardware and it associated Solaris Operating Environment worldwide and the fact that Jumpstart technology was released by Sun in 1995 I could find very little documentation, which specifically addressed auditing any Jumpstart infrastructure. In addition I found absolutely nothing about auditing a Distributed Lights-out variation.

So what did I find ?

- How Jumpstart really works.
  - Jumpstart Technology, Effective use in the Solaris Operating Environment [2]
  - Solaris Jumpstart Basics [6]
  - Enterprise Rollouts with Jumpstart [7]

- How to harden any Solaris server.
  - How Hackers Do it: Tricks, Tools, and Techniques [8]
  - Solaris™ Operating Environment Network Settings for Securit y [9]
  - CIS Solaris Benchmark v1.2.0 [10]
  - Solaris™ Operating Environment Security [11]

- How to build and secure Jumpstart server.
  - Building and Securing a Solaris 8 Jumpstart Server [12]

- How to install and use JASS
  - Hardening Solaris with JASS [13]
  - The Solaris™ Security Toolkit – Installation, Configuration and Usage Guide [14]

Problem is, all documents associated with Security continually told you how to disable Jumpstart core protocols e.g. NFS, tftp, bootp, boot.paramd and inetd super server. As a rule they were generally unhelpful when, as in the case of Jumpstart, you need to leave these protocols enabled.

While the documentation about Jumpstart was good at telling you how to get it to work they contained very little about how to do it when you are concerned about security.

So what proved most useful ?

- the book [2] had three pages about general security issues with Jumpstart,
- the article 'Hardening Solaris with JASS' [13]
- the article [12] found on the GIAC posted practical site.

Although no (distributed) Jumpstart auditing checklist(s) could be found using the above resources, my personal experience and knowledge of how Jumpstart works enabled me to construct a checklist suited to ACM E Corp environment.

2. Assignment 2: Create an Audit Checklist

2.1. Checklist Item 1 – No long links out of /jumpstart

Checklist Item 1 : No long links out of /jumpstart	
Reference	Hardening Solaris with JASS [13] (page 9) Solaris Benchmark v1.2.0 [10] (page 34) Personal experience
Control Objective	The partition /jumpstart has to be exported using nfs. To make matter worse it has to be exported where anonymous user is mapped to root. [2](page 15) We want to ensure the /jumpstart partition is mounted read -only and exported read -only.
Risk	Since /jumpstart is shared via nfs we want to take a defence in depth stance and assume that either of the following will happen one day, 1: a new vulnerability be released on how to get read -write access to nfs share shared read -only 2: someone accidentally or otherwise shares it read -write
Compliance	1: /jumpstart is a separate dedicated partition 2: procedure exists to ensure it is mounted read -only before it is shared
Testing	1: ask sysadmin representative to demonstrate that it is a separate partition. df –k; cat /etc/vfstab 2: verify that it is shared read -only cat /etc/dfs/dfstab 3: review procedure
Objective/Subjective	Objective : It is a separate partition Objective : It is shared read -only Subjective: Procedure exists and is sufficient

2.2. Checklist Item 2 – /tftpboot read only and no suid

Checklist Item 2 : /tftpboot read only and no suid	
Reference	UNIX Security Checklist v2.0 [15] Personal experience
Control Objective	tftp is an anonymous protocol we want to minimise what any anonymous user can do remotely to this shared resource. We can minimise our exposure by the following means 1: mounting the /tftpboot file system read only prior to enabling tftp daemon, 2: ensuring no suid files in partition 3: no group or world writable files
Risk	A creative hacker may be able to substitute a miniroot image with a Trojan version.
Compliance	1: A written procedure exists on mounting /tftpboot read only prior to starting the tftp daemon; note this requires a reboot 2: check no suid files in /tftpboot 3: no writable files in /tftpboot 4: dedicated partition /tftpboot
Testing	1: review procedure on mounting /tftpboot partition 2: get the sysadmin representative to demonstrate no suid files find /tftpboot –xdev –type f \ \(-perm –04000 –o –perm –02000 \) -print 3: no writable file find /tftpboot/ -xdev -type f \ \(-perm -00020 -o -perm -00002 \) -print 4: dedicated partition df –k; cat /etc/vfstab
Objective/Subjective	Subjective : Procedure exists and is sufficient Objective : Additional checks

2.3. Checklist Item 3 – Review version of JASS

Checklist Item 3 : Review version of Jass	
Reference	Personal experience
Control Objective	Ensure the current version of JASS is being used
Risk	Enhancements and bug fixes provided by latest released cannot be used if latest version is not installed.
Compliance	The installed version will be what is available from the official sun site.
Testing	Identify official version from of ficial sun site http://www.sun.com/solutions/blueprints/tools/license.html [16] Identify version currently in use: grep "JASS_VERSION=" /jumpstart/Drivers/driver.init
Objective/Subjective	Objective

2.4. Checklist Item 4 – Standard JASS scripts unmodified

Checklist Item 4 : Standard JASS scripts unmodified	
Reference	Jass Quick Start reference [16] Hardening Solaris with JASS [13]
Control Objective	JASS documentation clearly states that JASS scripts should not be modif ied rather copied then modified.
Risk	Difficult to upgrade to latest version of JASS without losing local customisations. Thus there may be reluctance to upgrade or probably worse uncontrolled upgrade losing local customisations.
Compliance	The standard scripts installed by JASS are not modified. A documented procedure exists on the process to be used in creating additional scripts and / or permutations of standard scripts.

Testing	Get the sysadmin representative to demonstrate that none of the standard scripts have been modified. /jumpstart/MANIFEST will be used as reference. Use script: JASS Standard scripts modified detector Review the procedure.
Objective/Subjective	Objective : No files have been modified Subjective : Procedure exists and is sufficient

2.5. Checklist Item 5 – JASS reapplied as required

Checklist Item 5 : JASS reapplied as required	
Reference	Jass Config Installation Documentation [14]
Control Objective	JASS documentation states the followi ng., 'Standalone mode is particularly useful when re -hardening a system after patches have been applied'. Thus we need to verify if JASS is being reapplied.
Risk	Patches from SUN may restore a file's permission to its default thus undoing any previous h ardening. Thus the risk is your box becomes increasingly less hardened as more patches are applied.
Compliance	There is policy and a procedure on how to and evidence of reapplying JASS after patching.
Testing	Review policy Review procedure(s) Get the sysadmin representative to demonstrate that JASS has been periodically applied especially after OS patching. For example identify when patching has been done: ls –latr /var/sadm/patches/ List the various dates JASS applied jass-execute –H
Objective/Subjective	Subjective : Policy exists and is sufficient

	Subjective : Procedure(s) exists and is/are sufficient Objective : Evidence JASS being reapplied

2.6. Checklist Item 6 – No changes bypassing JASS

Checklist Item 6 : No changes bypassing JASS	
Reference	Personal Experience
Control Objective	To detect any changes made to the box which undoes what JASS has done.
Risk	Individuals may make changes without considering all security issues. Thus the risk is the box becomes increasingly less hardened as more changes are ma de.
Compliance	Any variations can be explained and are documented where necessary.
Testing	Identify any files which were changed by JASS which have subsequently been changed /jumpstart/jass -check-sum Verify that hardening is still consistent with docu mented profile /jumpstart/jass -execute –v secure.driver | grep '\[FAIL\]'
Objective/Subjective	Objective : All check -sum variations are documented Objective : All FAIL's variations are documented

2.7. Checklist Item 7 – enable/disable tftp, nfs, rpc, boot p

Checklist Item 7 : Enable/disable tftp,nfs, rpc, bootp	
Reference	Jumpstart Technology [2] page 145
Control Objective	Known risk services, which are required for jumpstart to work, should only be enabled as required.
Risk	The services tftp , nfs, rpc, bootp that are used by jumpstart have all had their fare share of security issues.

	Every additional service on a box increases your risk. To minimise this risk these services should only be enabled when required. The longer they are enabled the greater the window of opportunity for someone to exploit a vulnerability.
Compliance	A documented procedure exists on the process to be used to enable and disable services when not in use. Automated monitoring should be in place to detect services left activated.
Testing	Review the procedure. Get the sysadmin representative to activate nfs on one of the Jumpstart servers without following the documented procedure. Wait up to 10 minutes and observe if a system alert is generated into an event management console.
Objective/Subjective	Subjective : Procedure exists and is sufficient Objective : Alert is generated

2.8. Checklist Item 8 – Access control to Jumpstart Services

Checklist Item 8 : Access control to Jumpstart Services	
Reference	Jumpstart Technology [2] page 148 Solaris™ Operating Environment Security [11] (page 45) Personal Experience
Control Objective	Known risky services, which are required for jumpstart to work, are only available to nominated hosts.
Risk	The services tftp, nfs, rpc, bootp that are used by jumpstart have all had their fare share of security issues. Every additional service on a box increases your risk. To minimise this risk these services should only be accessible from no minated hosts. Because /jumpstart is shared globally to anyone, any user on ACME Corp could mount this share (read only) and look for information which could subsequently be used to attack

	this host or hosts jumpstarted from it.
Compliance	Host based firewall (e.g SunScreen 3.2 [17]) exists on each Jumpstart server. Access lists exists on routers to prevent access to these services from another segment. Procedure exist to ensure that /jumpstart is not shared to every host, rather the specific host being jumpstarted or at the very most its directly connected network. For example : # Single host line from /etc/dfs/dfstab share –F nfs –o ro,anon=0,hosta jumpstart # directly connected network, less preferable share –F nfs –o ro=192.168.1.0/25:192.168.2.0/2 5,anon=0 /jumpstart
Testing	Get the sysadmin representative to demonstrate that a host based firewall policy exists and is active. Get the router representative to highlight the access -lists on the routers, which prevents nfs, tftp, and rpc services of the jumpstart servers being remotely accessible. Review the procedure to share the /jumpstart directory and determine if any host restrictions are in use.
Objective/Subjective	Objective : Host based firewall policies exists and are sufficient Objective : Router access lists exists and are sufficient and activated Objective : Host restrictions are documented in procedure and in use

2.9. Checklist Item 9 – Console access encrypted

Checklist Item 9 : Console Access encrypted	
Reference	Personal Experience
Control Objective	Ensure that all traffic is encrypted between management

	stations and console servers.
Risk	At various stages sensitive commands will need to be put in via the console. Each console is extended via Cisco terminal servers to allow remote access into the server farms. As a result there is a risk someone will be able to capture critical data. To minimise this risk data has to be encrypted between workstations and terminal servers.
Compliance	The Cisco Terminal servers only allow encrypted access. (Unfortunately it is only ssh v1 … we await Cisco to take security seriously and implement v2)
Testing	Get the sysadmin representative to demonstrate that they can access via ssh and not via telnet ssh 192.168.1.2 2001 telnet 192.168.1.2 2001
Objective/Subjective	Objective : You can only access via ssh

2.10. Checklist Item 10 – Console access is restricted

Checklist Item 10 : Console access is restricted	
Reference	Personal Experience
Control Objective	Remote console access allows an individual to effectively have physically access to the server yet still be remote from the equipment. Need to ensure all requests for console access are approved.
Risk	Someone who wouldn't be allowed physical access to equipment because his/her job doesn't require it might accidentally or otherwise achieve it logically via a console server.
Compliance	A standard procedure exists for all account creation and periodic review.

	Each Cisco terminal server is configured to use central authentication and authorisation.
Testing	Review the procedure. Get the sysadmin representative to demonstrate that central authentication / authorisation is in use.
Objective/Subjective	Subjective : Procedure exists and is sufficient Objective : Console access is restricted

2.11. Checklist Item 11 – Console Access Monitored

Checklist Item 11 : Console Access Monitored	
Reference	Personal Experience
Control Objective	Ensure that no session is left logged in via console.
Risk	Console access should not be required often, but when it is the root account maybe required. Unfortunately when a user logs out of the terminal server the active user is not logged out of the console. What this means is the console could accidentally be left logged in for an extended period of time using the root account. For anyone to take advantag e of this all they need is access to the console server.
Compliance	A procedure / tool exists to periodically scan for console ports still logged in. A security incident should be generated whenever one is found.
Testing	Examine procedure / tool fo r completeness.
Objective/Subjective	Objective : Procedure / tool exists and is effective.

2.12. Checklist Item 12 – File Integrity Checker in use

Checklist Item 12 : File Integrity Checker in use	
Reference	Hardening Solaris with JASS [13] Building and Securing a Solaris 8 Jumpstart Server [12]
Control Objective	Ensure any changes to the Jumpstart server are detected in a timely manner.
Risk	The biggest risk is that someone installs a Trojan version of a program in the /jumpstart tree. If this is undetected then it is probable that it will be installed on all boxes subsequently built. Thus all new boxes will be compromised from day one.
Compliance	A notable file integrity program is in use, e.g Tripwire.
Testing	Review which file Integrity is in use.
Objective/Subjective	Objective : Exists and is sufficient

2.13. Checklist Item 13 – Sync of boxes is encrypted

Checklist Item 13 : Sync of boxes is encrypted	
Reference	Personal Knowledge
Control Objective	Ensure all sync traffi c between Jumpstart Primary and all Remotes is encrypted.
Risk	If a non-encrypted mechanism is used someone may be able to sniff the traffic and obtain information which could subsequently be used against you. For example they may learn the user i.d and password used to do the synchronisation, they could then use it to load a Trojan up onto to remotes.
Compliance	Syncing is done via an encrypted means.
Testing	Review with the sysadmin representative how syncing is done.
Objective/Subjective	Objective : It is either encrypted or not

2.14. Checklist Item 14 – Vendor OS patches are up to date

Checklist Item 14 :	Vendor OS patches are up to date
Reference Control Objective	Solaris Patch Management: Recommended Strategies [18] A Patch Management Strategy for the Solaris ™ OE [19] Determine if patches are being applied in a timely manner.
Risk	New vulnerabilities are being released regularly. Vendors address these 'known' vulnerabilities by releasing patches. The onus is on you as a customer to apply the patches to your systems in a timely manner.
Compliance	If the boxes are fully up to date with vendor patches then it will be compliant.
Testing	Get the sysadmin representative to demonstrate that the system is fully patched. The output from one of the following is suffi cient 1: patchcheck [20] 2: Solaris™ Patch Manager [21]
Objective/Subjective	Objective : it is either patched or it is not

2.15. Checklist Item 15 – NESSUS vulnerability scan

Checklist Item 15 :	NESSUS vulnerability scan
Reference	Audit Networks with NMAP and other Tools [22]
Control Objective Risk	To identify any known vulnerabilities using a well -known tool. A vulnerability combined with an exploit will result in a compromise. Friends and foe will use vulnerability scanners to identify weakness in your armour. We can minimise our risk by addressing known

	vulnerabilities in a controlled manner.
Compliance	All vulnerabilities identified by the scan must be individually and collectively considered to determine our exposure. The system is only compliant when a document exists addressing all detected vulnerabilities as either [23] 1: accept the risk 2: mitigate the risk 3: transfer the risk
Testing	Perform an approved (in writing) scan using the latest stable version of NESSUS [24]. Verify that all identified vulnerabilities are documented.
Objective/Subjective	Objective : They are either documented or they are not

2.16. Checklist Item 16 – Individual MAC addresses

Checklist Item 16 :	Individual MAC addresses
Reference	Personal Experience Hardening Solaris with JASS [13] Building and Securing a Solaris 8 Jumpstart Server [12]
Control Objective	Individual MAC addresses should be used on all Dual NIC'd servers.
Risk	Difficult to do analysis of traffic, and impossible to analyse the ARP table of Cisco routers which have a dual NIC'd Sparc server connected to two Fast Ethernet interfaces on the same router.
Compliance	The eeprom is set to use individual MAC addresses.
Testing	Get the sysadmin representative to demonstrate that the eeprom variable local-mac-address is set to true. eeprom | grep 'local-mac-address'
Objective/Subjective	Objective : It will be either true or false

2.17. Checklist Item 17 – SSH current Version

Checklist Item 17 : SSH current Version	
Reference	Personal Experience Configuring th e Secure Shell Software [25]
Control Objective	Ensure that the latest version of software is installed.
Risk	As all remote access onto these boxes, apart from console access, will be SSH it is imperative that the latest version is always in use. If latest version is not maintained, and since the service has to be running all the time we will be vulnerable to any new ssh vulnerabilities.
Compliance	The latest version is installed and active.
Testing	Determine the latest stable version available from th e official site. http://www.openssh.com Get the sysadmin representative to demonstrate that the latest version is installed. ssh –V sshd -V
Objective/Subjective	Objective : It either is or it is not current

2.18. Checklist Item 18 – OS Minimisation

Checklist Item 18 : OS Minimisation	
Reference	Operating Environment Minimisation for Security [26] Armouring Solaris [27]
Control Objective	Only the absolute minimal OS environment required to support Jumpstart clients be installed on the Jumpstar t servers.
Risk	The more packages installed the more ongoing maintenance required to ensure patches are up to date. The more work the greater chance of falling behind or one being missed.
Compliance	All unnecessary software has been removed.

Testing	Review the Jumpstart server build procedure to determine if initial build is based on minimal cluster (Core – SUNWCreq) then packages added to as needed. And put in the following command: cat /var/sadm/system/admin/CLUSTER Get the sysadmin representativ e to demonstrate that only minimal packages still remain installed. pkginfo
Objective/Subjective	Objective : Build procedure is based on SUNWCreq Subjective : All unnecessary packages removed

2.19. Checklist Item 19 – JASS default password overridden

Checklist Item 19 : JASS default password overridden	
Reference Control Objective	Jass Quick Start reference [16] The Art of Deception [28] page 299 No default password must be allowed anywhere anytime.
Risk	A busy sysadmin staff member delays changin g the root password on a newly jumpstarted box for an extended period of time. Since it is a known default password it makes it easier for a hacker to utilise.
Compliance	The default root password of 't00lk1t' is overridden in /jumpstart/Drivers/user.i nit
Testing	Get the sysadmin representative to demonstrate that /jumpstart/Drivers/user.init have been modified. grep 'JASS_ROOT_PASSWORD' \ /jumpstart/Drivers/user.init Expect something like JASS_ROOT_PASSWORD="JdqZ5HrSDYM.o" export JASS_ROOT_PASSWORD
Objective/Subjective	Objective : It is either overridden or it is not

2.20. Checklist Item 20 – CIS Solaris Benchmark

Checklist Item 20 : CIS Solaris Benchmark	
Reference	CIS Solaris Benchmark [10]
Control Objective	Audit to ensure , wherever possible, all host -hardening suggestions by a reputable organisation have been met or exceeded.
Risk	Any recommendation that is not met or exceeded probably will lower our overall host security. It is for this reason all variations need to b e individually and collectively analysed taking into consideration limitations of technology and business requirements.
Compliance	The system is only compliant when a document exists addressing all identified issues as either [23] 1: accept the risk 2: mitigate the risk 3: transfer the risk The CIS Benchmark document is most helpful in addressing each 'Negative'.
Testing	Download and install the latest version of the tool [10]. Install the tool uncompress cis*.Z tar –xvf cis*tar pkgadd –d CISscan all Perform audit. /opt/CIS/cis-scan Verify that all identified issues are documented in the host baseline document. vi /opt/CIS/cis -most-recent-log
Objective/Subjective	Objective : Either there ar e documented or there not

3. Assignment 3: Audit Evidence

3.1. Conduct the audit

The audit was conducted on the master site and on one slave site. The audit was carried out on both sites except in cases where it was only relevant on one, e.g Checklist Item 13 – Sync of boxes is encrypted . For the purpose of this section the testing and output will be shown once only when the result is exactly the same.

To help you the sysadmin representative and myself have agreed on the following prompts.

- [root@master] : a root shell on the master Jumpstart server
- [root@slave] : a root shell on one slave Jumpstart server
- [root@both] : to indicate that the result was the same on both servers
- [root@client] : root shell on normal unix client on separat e segment
- [user@client] : user shell on normal unix client on separate segment

All checklist item were done on both servers, however below are the 10 items which are most important in developing a report for the Information Technology Manager and Chief Security Officer of ACME Corp. Please refer to ' Assignment 4: Audit Report ' for further details.

I have also used the following to assist the reader:

- comments are normal highlight, e.g like this
- commands are bold, e.g **like this**
- observed output is indented normal highlight

3.1.1 Audit Item 1 – No long links out of /jumpstart – Pass (comments)

Auditlist Item 1 -	No long links out of /jumpstart
Checklist Reference	Checklist Item 1 – No long links out of /jumpstart
Reference	Hardening Solaris with JASS [13] (page 9) Solaris Benchmark v1.2.0 [10] (page 34) Personal experience
Control Objective	The partition /jumpstart has to be exported using nfs. To make matter worse i t has to be exported where anonymous user is mapped to root. [2](page 15) We want to ensure the /jumpstart partition is mounted read -only and exported read -only.
Risk	Since /jumpstart is shared via nfs we want to take a defe nce in depth stance and assume that either of the following will happen one day, 1: a new vulnerability be released on how to get read -write access to nfs share shared read -only 2: someone accidentally or otherwise shares it read -write
Compliance	1: /jumpstart is a separate dedicated partition 2: procedure exists to ensure it is mounted read -only before it is shared
Testing	1: ask sysadmin representative to demonstrate that it is a separate partition. df –k; cat /etc/vfstab 2: verify that it is shar ed read-only cat /etc/dfs/dfstab

	3: review procedure
Objective/Subjective	Objective : It is a separate partition Objective : It is shared read -only Subjective: Procedure exists and is sufficient
Perform Testing	**[root@both]df -k** Filesystem kbytes used avail capacity Mounted on /dev/md/dsk/d101 1985487 897000 1028923 47% / /proc 0 0 0 0% /proc fd 0 0 0 0% /dev/fd mnttab 0 0 0 0% /etc/mnttab swap 944160 16 944144 1% /var/run swap 524288 132856 391432 26% /tmp /dev/md/dsk/d104 71889970 38121031 33050040 54% /jumpstart /dev/md/dsk/d105 1985 487 1534303 391620 80% /export/home **[root@both] cat /etc/vfstab** [root@both]cat /etc/vfstab #device device mount FS fsck mount mount #to mount to fsck point type pass at boot options # #/dev/dsk/c1d0s2 /dev/rdsk/c1d0s2 /usr ufs 1 yes - fd - /dev/fd fd - no - /proc - /proc proc - no - /dev/md/dsk/d100 - - swap - no - /dev/md/dsk/d 101 /dev/md/rdsk/d101 / ufs 1 no - /dev/md/dsk/d105 /dev/md/rdsk/d105 /export/home ufs 2 yes - /dev/md/dsk/d104 /dev/md/rdsk/d104 /jumpstart ufs 2 yes -

	swap - /tmp tmpfs - yes size=512m **[root@both]cat /etc/dfs/dfstab** # Place share(1M) commands here for automatic execution # on entering init state 3. # # Issue the command '/etc/init.d/nfs.server start' to run the NFS # daemon processes a nd the share commands, after adding the very # first entry to this file. # # share [-F fstype] [-o options] [-d "<text>"] <pathname> [resource] # .e.g, # share -F nfs -o rw=engineering -d "home dirs" /export/home2 share -F nfs -o ro,anon=0 /jumpstart
Result & Comments	1: Pass as it is a separate partition 2: Pass as partition is shared read -only 3: Fail as there is no procedure to ensure it is mounted read -only prior to sharing Pass – overall but a procedure should be creat ed so as to have greater defence -in-depth

3.1.2 Audit Item 2 – Review version of JASS – Fail

Auditlist Item 2 -	Review version of Jass
Checklist Reference	Checklist Item 3 – Review version of JASS

Reference	Personal experience
Control Objective	Ensure the current version of JASS is being used
Risk	Enhancements and bug fixes provided by latest released can't be used if latest version is not installed.
Compliance	The installed version will be what is available from the official sun site.
Testing	Identify official version from official sun site http://www.sun.com/solutions/blueprints/tools/license.html[16] Identify version currently in use: grep "JASS_VERSION=" /jumpstart/Drivers/driver.init
Objective/Subjective	Objective
Perform Testing	Sun's current version: 0.3.11 Jumpstart current version: **[root@both] grep "JASS_VERSION=" /jumpstart/Drivers/driver.init** 0.3.10
Result & Comments	Fail

3.1.3 Audit Item 3 – Standard JASS scripts unmodified – Pass

Auditlist Item 3 -	Standard JASS scr ipts unmodified
Checklist Reference	Checklist Item 4 – Standard JASS scripts unmodified
Reference	Jass Quick Start reference [16]

	Hardening Solaris with JASS [13]
Control Objective	JASS documentation clearly states that JASS scripts should not be modified rather copied then modified.
Risk	Difficult to upgrade to latest version of JASS without losing local customisations. Thus there may be reluctance to upgrade or proba bly worse uncontrolled upgrade losing local customisations.
Compliance	The standard scripts installed by JASS are not modified. A documented procedure exists on the process to be used in creating additional scripts and / or permutations of standard scripts.
Testing	Get the sysadmin representative to demonstrate that none of the standard scripts have been modified. /jumpstart/MANIFEST will be used as reference. Use script: JASS Standard scripts modified detector Review the procedure.
Objective/Subjective	Objective : No files have been modified Subjective : Procedure exists and is sufficient
Perform Testing	**[root@both]./manifest.sh /jumpstart/MANIFEST** Welcome to manifest Checker Creating current signatures And now for the d ifferences ####### BEGIN DIFF ######## ####### END DIFF ########
Stimulus /	**Stimulus / Response 1 -** Modify a JASS script and recheck

Response	Modify any script, remember which one and how, then retest **[root@both]./manifest.sh /jumpstart/MANIFEST** Welcome to manifest Checker Creating current signatures And now for the differences ####### BEGIN DIFF ######## ./README ####### END DIFF ########
Result & Comments	Pass

3.1.4 Audit Item 4 – JASS reapplied as required – Fail

Auditlist Item 4 -	JASS reapplied as required
Checklist Reference	Checklist Item 5 – JASS reapplied as required
Reference	Jass Config Installation Documentation [14]
Control Objective	JASS documentation states the following., 'Standalone mode is particularly useful when re -hardening a system after patches have been applied'. Thus we need to verify if JASS is being reapplied.
Risk	Patches from SUN may restore a file's permission to its default thus undoing any previous hardening. Thus the risk is your box becomes increasin gly less hardened as more patches are applied.
Compliance	There is policy and a procedure on how to and evidence of reapplying JASS after patching.
Testing	Review policy

	Review procedure(s) Get the sysadmin representative to demonstrate that JASS has been periodically applied especially after OS patching. For example identify when patching has been done: ls –latr /var/sadm/patches/ List the various dates JASS applied jass-execute –H
Objective/Subjective Perform Testing	Subjective : Policy exists and is sufficient Subjective : Procedure(s) exists and is/are sufficient Objective : Evidence JASS being reapplied **[root@both] ls –latr /var/sadm/patches/ | tail** drwxr-xr-- 2 root other 512 Jun 24 2002 108827 -25 drwxr-xr-- 2 root other 512 Jun 24 2002 108993 -09 drwxr-xr-- 2 root other 512 Jun 24 2002 110723 -05 drwxr-xr-- 2 root other 512 Jun 24 2002 110460 -18 drwxr-xr-- 2 root other 512 Jun 24 2002 108727 -15 drwxr-xr-- 2 root other 512 Jun 24 2002 108725 -09 drwxr-xr-- 2 root other 512 Jun 24 2002 108975 -06 drwxr-xr-- 2 root other 512 Jun 24 2002 109007 -07 drwxr-xr-x 11 root sys 512 Jun 24 2002 .. drwxr-xr-x 54 root root 1536 Jun 24 2002 . The last patch applied was on Jun 24 2002, on long time ago more about this soon.

	[root@both] /jumpstart/jass -execute –H Note: This information is only applicable for applications of the Solaris Security Toolkit starting w ith version 0.3. The following is a listing of the applications of the Solaris Security Toolkit on this system. This list is provided in reverse chronological order: 1. June 24, 2002 at 23:48:20 (20020624234820) As you can see it has only been applie d once; when the box was built
Stimulus / Response	**Stimulus / Response 2 -** Reapply in verify mode only to check consistency. Freshen to latest cluster patch – taken from ACME Corp procedure **[root@both] cd /jumpstart/Patches** **[root@both] rm –rf 8_Recommended/*** **[root@both] unzip 8_Recommended.zip** Perform re-verification **[root@both] /jumpstart/jass -execute –v secure.driver > /tmp/jass.log** **root@both]grep FAIL /tmp/jass.log** # JASS_LOG_FAILURE [FAIL] Patch ID 110934-13 or higher is not installed. [FAIL] Patch ID 110662-11 or higher is not installed. [FAIL] Patch ID 108987-13 or higher is not installed. .... [FAIL] The MD5 software is not installed in /opt/md5. [FAIL] Verify Check Total : 1 Error(s) [FAIL] The Fix Modes software does not exist in /opt/FixModes/fix -modes.

	[FAIL] The Fix Modes has not been used on this system. [FAIL] Verify Check Total : 2 Error(s) [FAIL] Driver Script Total : 71 Error(s) [FAIL] Grand Total : 154 Error(s)
Result & Comments	Fail, it has not been periodically applied nor have patches. Additionally a lot of the errors were because patches were not applied, many were avoidable.

3.1.5 Audit Item 5 – Enable/disable tftp, nfs, rpc, bootp – Fail

Auditlist Item 5 -	Enable/disable tftp,nfs, rpc, bootp
Checklist Reference	Checklist Item 7 – enable/disable tftp, nfs, rpc, boo tp
Reference	Jumpstart Technology [2]page 145
Control Objective	Known risky services, which are required for jumpstart to work, should only be enabled as required.
Risk	The services tftp, nfs, rpc, bootp th at are used by jumpstart have all had their fare share of security issues. Every additional service on a box increases your risk. To minimise this risk these services should only be enabled when required. The longer they are enabled the greater the window of opportunity for someone to exploit a vulnerability.
Compliance	A documented procedure exists on the process to be used to enable and disable services when not in use. Automated monitoring should be in place to detect services left activated.
Testing	Review the procedure. Get the sysadmin representative to activate nfs on one of the Jumpstart servers without following the

	documented procedure. Wait up to 10 minutes and observe if a system alert is generated into an event management console.
Objective/Subjective	Subjective : Procedure exists and is sufficient Objective : alert is generated
Perform Testing	**[root@both] /etc/init.d/rpc start** **[root@both] /etc/init.d/nfs.server start** No alert was generated, in fact no monitoring has been esta blished to monitor unwelcome services on these servers.
Stimulus / Response	**Stimulus / Response 3 -** Check active ports Before stopping nfs, tftp etc **[root@both] netstat –na | grep –v 'ESTABLISHED'** UDP: IPv4 Local Address Remote Address State ---------- ---------- ------- *.69 Idle *.123 Idle 127.0.0.1.123 Idle 192.168.1.1.123 Idle 192.168.2.1.123 Idle *.1691 Idle *.32768 Idle *.32769 Idle *.57283 Idle

```
      *.4045                 Idle
      *.111                  Idle
      *.38634                Idle
      *.38635                Idle
      *.2049                 Idle
      *.36665                Idle

UDP: IPv6
  Local Address               Remote Address              State      If
----------------------------- --------------------------- ---------- -----
      *.69                                                Idle

TCP: IPv4
  Local Address      Remote Address    Swind Send  -Q Rwind Recv-Q  State
------------------- ------------------- ----- ------ ----- ------ -------
      *.22             *.*               0     0 24576     0 LISTEN
      *.62822           *.*              0     0 24576     0 LISTEN
      *.4045            *.*              0     0 24576     0 LISTEN
      *.111             *.*              0     0 24576     0 LISTEN
      *.44336           *.*              0     0 2457 6    0 LISTEN
      *.2049            *.*              0     0 24576     0 LISTEN
      *.44752           *.*              0     0 24576     0 LISTEN
      *.768             *.*              0     0 24576     0 BOUND

TCP: IPv6
  Local Address               Remote Address              Swind Send  -Q Rwind Recv-Q   State      If
----------------------------- --------------------------- ----- ------ ----- ------ ---------- -----

Active UNIX domain sockets
Address  Type         Vnode     Conn  Local Addr      Remote Addr
30000a1bb08 stream-ord 30000a236d0 00000000 /var/spool/prngd/pool
```

Stop daemons:

[root@both] /etc/inet.d/nfs.server stop
[root@both] /usr/bin/pkill –x –u 0 inetd
[root@both]netstat -na

```
UDP: IPv4
   Local Address        Remote Address     State
-------------------- -------------------- -------
      *.123                                Idle
127.0.0.1.123                               Idle
192.168.1.1.123                             Idle
192.168.2.1.123                             Idle
      *.1691                               Idle
      *.32768                               Idle
      *.32769                               Idle
      *.111                                Idle
      *.38634                               Idle

TCP: IPv4
   Local Address        Remote Address    Swind Send  -Q Rwind Recv-Q  State
-------------------- -------------------- ----- ------ ----- ------ -------
      *.22                 *.*              0      0 24576       0 LISTEN
      *.111                *.*              0      0 24576      0 LISTEN
      *.768                *.*              0      0 24576      0 BOUND

TCP: IPv6
   Local Address                 Remote Address                Swind Send  -Q Rwind  Recv-Q   State      If
------------------------------ ------------------------------ ----- ------ ----- ------ ---------- -----
```

	Active UNIX domain sockets Address Type Vnode Conn Local Addr Remote Addr 30000a1bb08 stream-ord 30000a236d0 00000000 /var/spool/prngd/pool
Result & Comments	Fail : Procedure exists, however it was noted the services did not start automatically at boot. That is they had to be manually be started prior to use, this was documented. However nothing was mentioned about stopping them when not in use. Fail : no alert generated Fail : overall

3.1.6 Audit Item 6 – Access control to Jumpstart Services – Fail

Auditlist Item 6 -	Access control to Jumpstart Services
Checklist Reference	Checklist Item 8 – Access control to Jumpstart Services
Reference	Jumpstart Technology [2] page 148 Solaris™ Operating Environment Security [11] (page 45) Personal Experience
Control Objective	Known risky services, which are required for jumpstart to work, are only available to nominated hosts.
Risk	The services tftp, nfs, rpc, bootp that are used by jumpstart have all had their fare share of security issues. Every additional service on a box increases your risk. To minimise this risk these services should only be accessible from nominated hosts. Because /jumpstart is shared globally to anyone, any user on ACME Corp could mount this share (read only) and look for information which could subsequently be used to attack this host or hosts jumpstarted from it.

Compliance	Host based firewall (e.g SunScreen 3.2 [17]) exists on each Jumpstart server. Access lists exists on routers to prevent access to these services from an other segment. Procedure exist to ensure that /jumpstart is not shared to every host, rather the specific host being jumpstarted or at the very most its directly connected network. For example : # Single host line from /etc/dfs/dfstab share –F nfs –o ro,anon=0,hosta jumpstart # directly connected network, less preferable share –F nfs –o ro=192.168.1.0/25:192.168.2.0/25,anon=0 /jumpstart
Testing	Get the sysadmin representative to demonstrate that a host based firewall policy exists and is active. Get the router representative to highlight the access -lists on the routers, which prevents nfs, tftp, and rpc services of the jumpstart servers being remotely accessible. Review the procedure to share the /jumpstart directory and determine if any host restrict ions are in use.
Objective/Subjective	Objective : Host based firewall policies exists and are sufficient Objective : Router access lists exists and are sufficient and activated Objective : Host restrictions are documented in procedure and in use
Perform Testing	Host based firewall doesn't exist. Router access lists doesn't exist.

	Procedure does not exist to do restrictive sharing based on either host or segment. In addition a check of the current share file indicates global sharing is enabled. **[root@both]cat /etc/dfs/dfstab** # Place share(1M) commands here for automatic execution # on entering init state 3. # # Issue the command '/etc/init.d/nfs.server start' to run the NFS # daemon processes and the share commands, after addi ng the very # first entry to this file. # # share [-F fstype] [-o options] [-d "<text>"] <pathname> [resource] # .e.g, # share -F nfs -o rw=engineering -d "home dirs" /export/home2 share -F nfs -o ro,anon=0 /jumpstart
Stimulus / Response	**Stimulus / Response 4 -** Mount jumpstart share on a different segment Mount the nfs share on a client pc **[root@client] mkdir /mnt/nfs** **[root@client] mount –F nfs 192.168.1.1:/jumpstart /mnt/nfs** Test access to file **[user@client] cat /mnt/nfs/sysidcfg** # # Copyright (c) 2000-2002 by Sun Microsystems, Inc. # All rights reserved. # #ident "@(#)sysidcfg 3.1 02/08/14 SMI" #

	system_locale=en_US timezone=US/Eastern terminal=vt100 name_service=NONE timeserver=localhost
Result & Comments	Fail : neither host-based nor network based attempts are used to restrict who can accesses these services.

3.1.7 Audit Item 7 – Console Access encrypted – Fail

Auditlist Item 7 -	Console Access encrypted
Checklist Reference	Checklist Item 9 – Console access encrypted
Reference	Personal Experience
Control Objective	Ensure that all traffic is encrypted between management stations and console servers.
Risk	At various stages sensitive commands will need to be put in via the console. Unfortunately each console is extend ed via Cisco terminal servers to allow remote access into the server farms. As a result there is a risk someone will be able to capture critical data. To minimise this risk data has to be encrypted between workstations and terminal servers.
Compliance	The Cisco Terminal servers only allow encrypted access.

	(Unfortunately it is only ssh v1 … we await Cisco to take security seriously and implement v2)
Testing	Get the sysadmin representative to demonstrate that they can access via ssh and not via tel net ssh 192.168.1.2 2001 telnet 192.168.1.2 2001
Objective/Subjective	Objective : You can only access via ssh
Perform Testing	First try ssh: [user@client] ssh 192.168.1.2 2001 Now try telnet **[[root@both]telnet console.acmecorp.com 2001** Trying 192.168.1.2... Connected to console1.acmecorp.com. Escape character is '^]'. ********** * Access to this computer system is limited to authorised users only. * * Unauthorised users may be subject to prosecution under the Crimes * * Act or State legislation * * * * Please note, ALL DETAILS are confidential and must * * not be disclosed. * ********** User Access Verification Username: testuser Password:

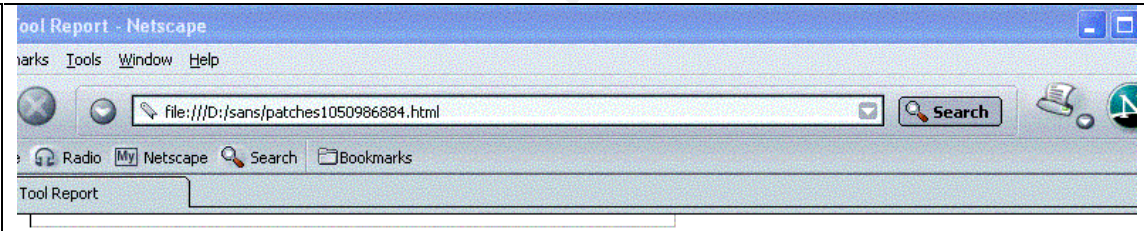
	Password OK
Result & Comments	Fail

3.1.8 Audit Item 8 – File Integrity Checker in use – Fail

Auditlist Item 8 -	File Integrity Checker in use
Checklist Reference Reference	Checklist Item 12 – File Integrity Checker in use Hardening Solaris with JASS [13] Building and Securing a Solaris 8 Jumpstart Server [12]
Control Objective	Ensure any changes to the Jumpstart server are detected in a timely manner.
Risk	The biggest risk is that someone installs a Trojan version of a progra m in the /jumpstart tree. If this is undetected then it is probable that it will be installed on all boxes subsequently built. Thus all new boxes will be compromised from day one.
Compliance	A notable file integrity program is in use, e.g Tripwire.
Testing	Review which file Integrity is in use.
Objective/Subjective	Objective : Exists and is sufficient
Perform Testing	No file integrity checker is in use.
Result & Comments	Fail : this will make intrusions hard to detect and extremely hard to imp ossible to remove.

3.1.9 Audit Item 9 – Vendor OS patches are up to date – Fail

Auditlist Item 9 -	Vendor OS patches are up to date
Checklist Reference	Checklist Item 14 – Vendor OS patches are up to date
Reference	Solaris Patch Management: Recommen ded Strategies [18] A Patch Management Strategy for the Solaris ™ OE [19]
Control Objective	Determine if patches are being applied in a timely manner.
Risk	New vulnerabilities are being released regularly. Vendors address these 'known' vulnerabilities by releasing patches. The onus is on you as a customer to apply the patches to your systems in a timely manner.
Compliance	If the boxes are fully up to date with vendor patches then it will b e compliant.
Testing	Get the sysadmin representative to demonstrate that the system is fully patched. The output from one of the following is sufficient 1: patchcheck [20] 2: Solaris™ Patch Manager [21]
Objective/Subjective	Objective : It is either patched or it is not
Perform Testing	**[root@both] perl patchk.pl –b –l** then save the html file, open in a browser for easy viewing



Sun Patch Check Report
Apr/22/03
Patch Check Version: 1.1

Hostname: [redacted] **SunOS Vers:** 5.8

System Type: sparc **Patch XREF File Date:** Apr/18/03

Report Note: Recommended patches are considered the most important and highly recommended patches that avoid the most critical system, user, or security related bugs which have been reported and fixed to date. A patch not listed on the recommended list does not imply that it should not be used if needed. Some patches listed in this report may have certain platform specific or application specific dependencies and thus may not be applicable to your system. It is important to carefully review the README file of each patch to fully determine the applicability of any patch with your system.

Installed Patches | Uninstalled Recommended Patches
Uninstalled Security Patches | Uninstalled Y2K Patches | Other Related Uninstalled Patches

Patchsuite Generation

Installed Patches

Patch ID	Current Revision	Latest Revision	Synopsis
108434	07	11	32-Bit Shared library patch for C++
108435	07	11	64-Bit Shared library patch for C++
108528	15	20	SunOS 5.8: kernel update patch
108569	06	08	X11 6.4.1: platform support for new hardware
108606	18	30	SunOS 5.8: M64 Graphics Patch
108652	53	66	X11 6.4.1: Xsun patch
108693	06	15	Solstice DiskSuite 4.2.1: Product patch
108714	05	08	CDE 1.4: libDtWidget patch

we then did, (modified output)
[root@both] perl patchk.pl

```
============================== WARNING ==============================
The date of the cross-reference (patchdiag.xref) file is Apr/18/03,
while the date reported by your system is Apr/25/03. Processing
of this program will continue, but you may have an out-of-date
cross-reference file. If you are not sure that you have the most
up-to-date cross-reference file, please visit
  http://sunsolve.Sun.COM/private-cgi/patchDownload.pl?target=patchdiag.xref&method=H
or
  ftp://sunsolve.sun.com/pub/patches/patchdiag.xref
to retrieve it, and run this program again.
=====================================================================

processing...
=============================================================================
System Name: master       SunOS Vers: 5.8       Arch: sparc
Cross Reference File Date: Apr/18/03
Patch Check Version: 1.1
=============================================================================
Report Note:

Recommended patches are considered the most important and highly
recommended patches that avoid the most critical system, user, or
security related bugs which have been reported and fixed to date.
A patch not listed on the recommended list does not imply that it
should not be used if needed.  Some patches listed in this report
may have certain platform specific or application specific dependencies
and thus may not be applicable to your system.  It is important to
carefully review the README file of each patch to fully determine
the applicability of any patch with your system.
=============================================================================
```

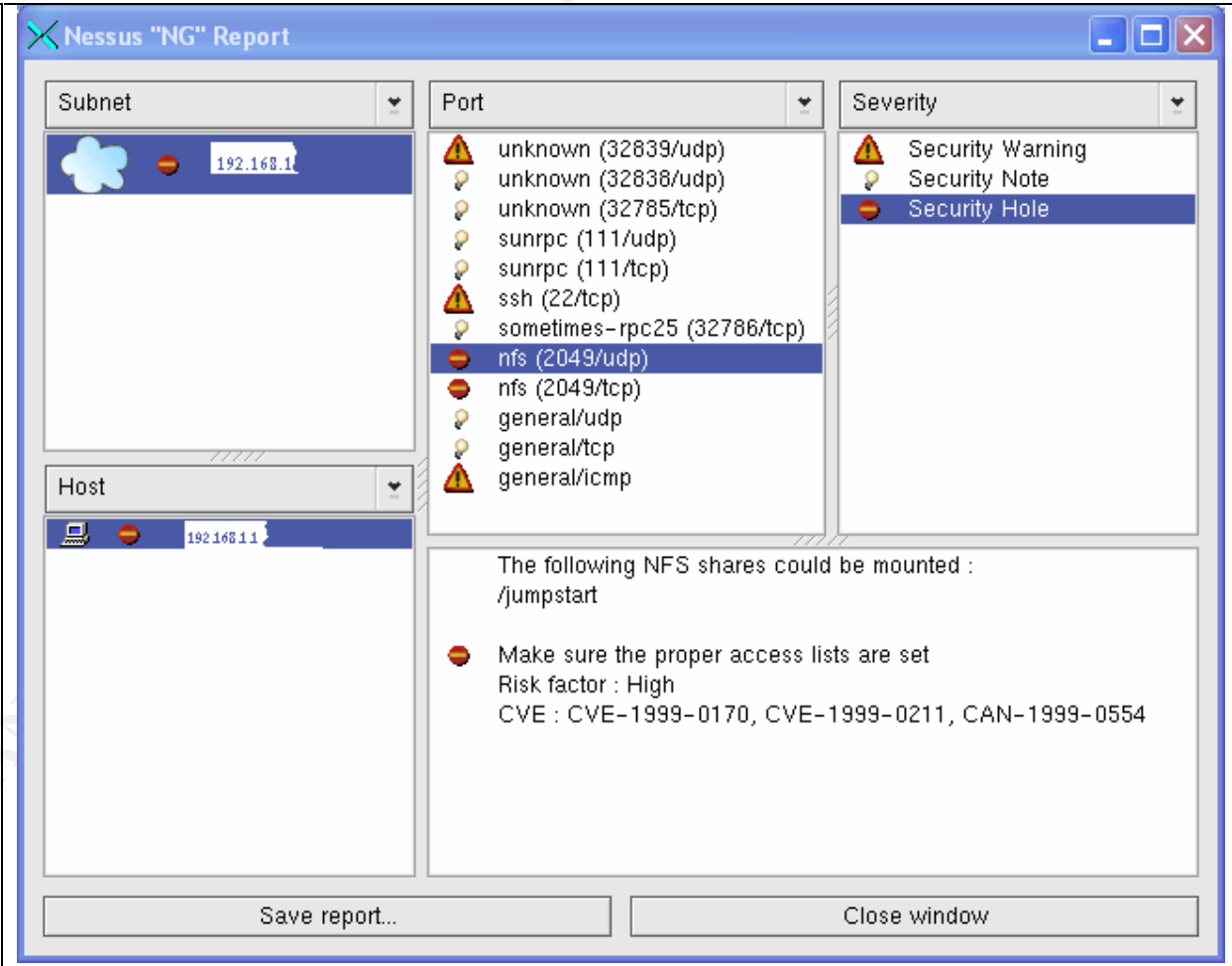
```
INSTALLED PATCHES
Patch  Installed Latest   Synopsis
 ID   Revision  Revision
------ -------- ------- ------------------------------------ ----------------
108434   07       11    32-Bit Shared library patch for C++
...
108723   01     CURRENT  SunOS 5.8: /kernel/fs/lofs and /kernel/fs/sparcv9/lofs patch
...
112796   01     CURRENT  SunOS 5.8: /usr/sbin/in.talkd patch
================== ============================================================

UNINSTALLED RECOMMENDED PATCHES

Patch  Ins Lat Age  Require    Incomp  Synopsis
 ID   Rev Rev       ID         ID
------ --- ------- -------- -------- ---------------------------- --------
108991 N/A  18 534 108528-07 109079-01 (or newer) Obsoleted by: 108827-15 SunOS 5.8: /usr/lib/libc.so.1
patch
             108989-01
....
114152 N/A  01 136                  SunOS 5.8: Japanese SunOS 4.x Binary Compatibility(BCP) patch
================================================================================

UNINSTALLED SECURITY PATCHES

NOTE: This list includes the Security patches that are also Recommended

Patch  Ins Lat Age  Require    Incomp  Synopsis
 ID   Rev Rev       ID         ID
------ --- --- --- -------- -------- ------------------------------------
108979 N/A  10 891 108528-03          Obsoleted by: 108528-04 SunOS 5.8: platform nexus, I2C, Netra ct a
```

	... 111570 N/A 02 226 SunOS 5 .8: uucp patch ... 114673 N/A 01 9 SunOS 5.8: /usr/sbin/wall patch ========== UNINSTALLED Y2K PATCHES NOTE: This list includes the Y2K patches that are als o Recommended Patch Ins Lat Age Require Incomp Synopsis ID Rev Rev ID ID ------ --- --- --- -------- -------- ---------- All Y2K patches installed!
Result & Comments	Fail : as you can see there a re a lot of unapplied patches. Of interest all patches needed are already on each server as they are there to allow easy patching of all other server.

3.1.10 Audit Item 10 – NESSUS vulnerability – Fail

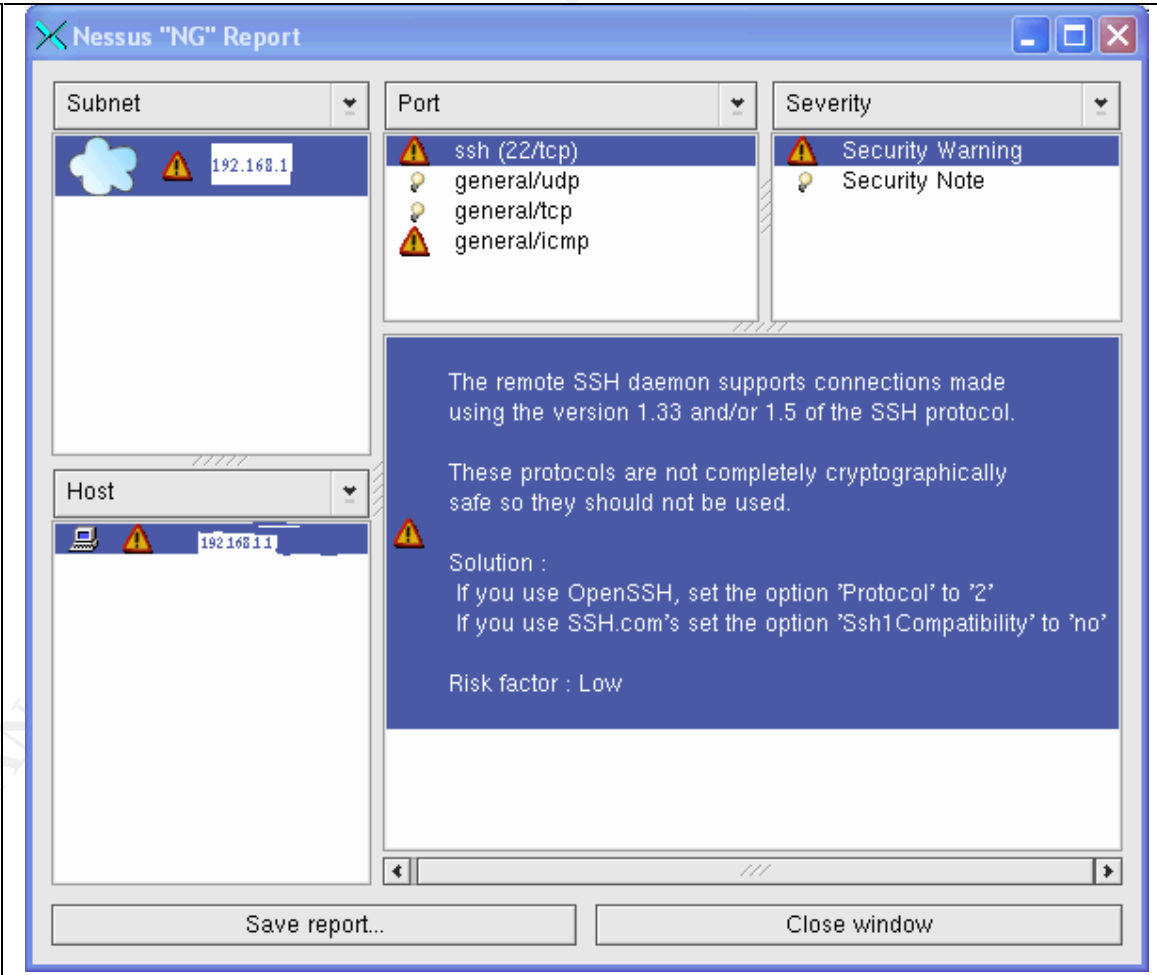
Auditlist Item 10 - NESSUS vulnerability scan	
Checklist Reference Reference	Checklist Item 15 – NESSUS vulnerability scan Audit Networks with NMAP and other Tools [22]
Control Objective	To identify any known vulnerabilities using a well -known tool.
Risk	A vulnerability c ombined with an exploit will result in a compromise.

	Friends and foe will use vulnerability scanners to identify weakness in your armour. We can minimise our risk by addressing known vulnerabilities in a controlled manner.
Compliance	All vulnerabilities identified by the scan must be individually and collectively considered to determine our exposure. The system is only compliant when a document exists addressing all detected vulnerabilities as either [23] 1: accept the risk 2: mitigate the risk 3: transfer the risk
Testing	Perform an approved (in writing) scan using the latest stable version of NESSUS. Verify that all identified vulnerabilities are documented.
Objective/Subjective	Objective : They are either documen ted or they are not
Perform Testing	Obtained written permission Performed scan.



The Nessus scan was easy to perform, it found a number of issues all which were expected due to that fact that unfavourable services are enabled. Of greatest concern is t hat it lists nfs as a security hole not just a

	warning.
Stimulus / Response	**Stimulus / Response 5 -** Stop Jumpstart services and retest **[root@both] /etc/inet.d/nfs.server stop** **[root@both] /usr/bin/pkill –x –u 0 inetd** **[root@both]netstat -na**



Unfortunately even when this t est was performed there was still one warning. The warning was highlighting the fact that the ssh daemon should be reconfigured to only allow ssh version 2 connections.

	A review of ACME Corp requirements indicates that only version 2 is required.
Result & Comments	Fail : document does not exist Fail : ssh daemon needs to be configured correctly

3.2. Measure Residual Risk

Lets first look at zero risk. Zero risk is near on impossible to achieve especially if you want your servers to still do something. U nless you have an unlimited budget it is financial suicide, to make matters worse in some cases you won't be protected from day zero vulnerabilities.

So how does ACME Corp Distributed Solaris ™ Jumpstart rate, lower than expected. But there are some good positives to come out of the audit as well, for example most issues can be addressed for minimal capital cost and minimal labour.

Below is a brief summary of the issues as detected in this audit.

Residual Risk 1. Timely applying Patching	
Description	Patches provided by vendors are a vendor's way of addressing stability and security issues in their products. The sooner you apply a patch the sooner you as a customer reap the full benefits of selecting Vendor X product over Vendor Y.
Threat	An un-patched system will have publicly known vulnerabilities giving the advantage to your adversaries.
Recommendation(s)	Develop, distribute, educate, assist and monitor all relevant parties on the new patching policy. Develop, distribute, educate, assist and monitor all relevant parties on the derived procedures. Develop a patch management strategy. [18] and [19] Establish some KPI's (Key Performance Indicators) measures, plot these indicators over time and use them to assist in efficient resource allocations.
Potential Cost	Policy - $1 000 labour Procedures - $5 000 labour Patch management strategy - $5 000 KPI's - $2 000 labour
Mitigating Options	Unfortunately there isn't a lot you can do however the following can assist: 1: Ensure that all boxes are built with 'OS Minimisation' in mind.

	2: Ensure that only essential services are enabled. 3: A network or host based IDS may assist in identifying some abnormal traffic.

Residual Risk 2. Policy of Encryption wherever possible	
Description	Encryption minimises the opportunity for an adversity to sniff important traffic.
Threat Recommendation(s)	An adversity may be able to sniff important or confidential traffic e.g. a root password. Have a policy that mandates the use of encry pted traffic wherever possible. The policy should also make it mandatory that an O.T.P mechanism be used wherever encryption cannot be used to protect an asset that could be used against ACME Corp if compromised. All servers already use the latest vers ion of Openssh [25] however the console servers pose real and present danger as they presently only support telnet. ACME Corp should seriously consider changing console servers to attain SSH version 2 protocol support.
Potential Cost	Policy - $1 000 labour Console servers - $2 000 labour, $10 000 new IOS images and additional memory.
Mitigating Options	Centralised One-Time passwords for everything. This will provide confidence for passwords but wont assist in confidentially of financial or sensitive documents.

Residual Risk 3. Policy Access Control on internal traffic	
Description	Services which have to be made available for day to day operations e.g. nfs and tftp for Jumpstart should only be available to individual hosts that need ac cess to them.
Threat	The more services available and the wider there availability the more likely one will be used against you.
Recommendation(s)	Develop, distribute, educate, assist and monitor all relevant parties on the new 'access control' policy.

	The policy must consider both host based and network based access control. Develop, distribute, educate, assist and monitor all relevant parties on the derived procedures.
Potential Cost	Policy - $1 000 labour Routers - Procedures - $5 000 labour Solaris SunScreen [17] - Procedure - $10 000 labour Procedure to restrictively share /jumpstart - $2 000 labour
Mitigating Options	Effective patching will assist and rigorous logfile analysis. A network or host based IDS may assist in identifying some abnormal traffic.

Residual Risk 4.	Policy File Integrity all servers
Description	File integrity alert(s) can sometimes be the first sign that you have experienced a security incident. Without doubt they are invaluable in determining this siz e of your breach and consequentially minimise your downtime.
Threat	If you don't use any file integrity checking mechanism then it is extremely hard to identify how much damage you have incurred if in fact any.
Recommendation(s)	Develop, distribute, e ducate, assist and monitor all relevant parties on the new 'file integrity' policy. All servers need a reputable file integrity checker installed and regularly checked. Develop, distribute, educate, assist and monitor all relevant parties on the derived procedures.
Potential Cost	Policy - $1 000 labour File integrity Program $10 000 tripwire $20 000 rollout $50 000 / year for • labour to monitor, • increased time to do any work on any server , e.g.

	apply patches
Mitigating Options	Accept the risk of : • not detecting a breach in a timely manner • increased recovery time

Residual Risk 5.	Policy to start / stop services as required
Description	As jumpstart is not required everyday, to reduce ACME Corp exposure window it is suggested services essential to Jumpstart be disab led when not required.
Threat	A service which is otherwise unneeded, and could have been disabled until needed, has been left enabled thus giving a hacker more paths into ACME Corp's infrastructure.
Recommendation(s)	Develop, distribute, educate, assi st and monitor all relevant parties on the new policy that makes it mandatory to disable temporary services. This would also include base lining all active services on ALL servers within ACME Corp and regular rescanning to verify that it is still consiste nt. Develop, distribute, educate, assist and monitor all relevant parties on the derived procedures.
Potential Cost	Policy - $1 000 labour Establish Base lining - $10 000 labour, $5 000 per year Modify existing Procedures $2 000
Mitigating Options	Effective patching will assist and rigorous logfile analysis. A network or host based IDS may assist in identifying some abnormal traffic.

As a result of the outstanding risks listed above I believe that at present ACME Corp Distributed Solaris™ Jumpstart infrastructure currently is overly exposed.

3.3. Is the system Auditable

The task of auditing the Distributed Solaris ™ Jumpstart can be broken down into two distinct parts:

- Policy and Procedures

- Technology specified issues

Lets first examine policy and pr ocedures. All but the very highest policy were non existent or insufficient. Where they did not exist industry examples were referred to. e.g. SANS Security Policy Project [29]. There were some very detailed procedures yet some important ones didn't exist e.g . file integrity.

Technology specific issues were easier to audit for two reasons:

- either they had been addressed or they hadn't.
- they are generally very objective.

While there was a wide range of technology to audit e.g. Solaris, Jumpstart, JASS, router and console servers they were all auditable.

So overall I suggest that the system was not auditable as there were too many missing or insufficient policy and procedures. That aside there is one big positive, all issues except one can be resolved for very minimal cost. Once they have been resolved the whole system could be easily auditable.

4. Assignment 4: Audit Report

4.1. Executive Summary

This purpose of this audit is to review ACME Corp new Distributed Solaris ™ Jumpstart infrastructure. The primarily reaso ns why both the Information Technology Manager and Chief Security Officer of ACME Corp have requested and supported the audit are:

- Over the next two years it is expected in excess of 2000 servers will have been built from it.
- Jumpstart methodology is also used as part of ACME Corp business continuity plan to minimise downtime.

The distributed Jumpstart infrastructure is housed in three geographically separated data centres and was audited during April and May 2003.

While the planned usage and deployment of the Jumpstart infrastructure along with some procedures shows good potential, missing or insufficient policy documents made it all but impossible to audit against ACME Corp policies. It was however possible to audit the Jumpstart infrastructure against a checklist developed during the audit planning phase based on technology used and industry best practice for those technologies. The resulting audit checklist consisted of 20 items considered most important to audit in the case of ACME Corp Distributed J umpstart infrastructure.

There were some 8 adverse findings which individually and collectively demonstrate room for improvement. Fortunately, all but one are relatively easy and inexpensive to rectify. In most case only needing policies to be written and procedures to developed and documented to support those policies.

4.2. Audit findings

Audit Finding 1. JASS not latest version.

Assignment 3 cross reference : Audit Item 2 – Review version of JASS – Fail

None of the servers had the latest version of the JASS software available from the official SUN web site.

Audit Finding 2. JASS not being periodically reapplied.

Assignment 3 cross reference : Audit Item 4 – JASS reapplied as required – Fail

There was no evidence that JASS is being routinely re -applied to any of the servers. Unfortun ately for JASS to be effective it needs to be reapplied whenever maintenance is performed on all the servers.

Audit Finding 3. Jumpstart services not disabled when not required.

Assignment 3 cross reference : Audit Item 5 – Enable/disable tftp, nfs, rpc, bootp – Fail

Jumpstart requires a number of notoriously insecure services it is best practice to disable any service whenever it is not required. Unfortunately during the audit no procedure was identified to ensure services are disabled when not required, howeve r it was noted that by default the services did not start on reboot.

Audit Finding 4. Non-existence of firewalls to restrict access to Jumpstart.
Assignment 3 cross reference : Audit Item 6 – Access control to Jumpstart Services – Fail

Jumpstart requires a numbe r of notoriously insecure services it is best practice to restrict access to these services to only those servers / users who explicitly require access. Unfortunately during the audit no access control was present on neither the Jumpstart servers themselve s nor connecting routers.

Audit Finding 5. Plain text access to all Console Servers
Assignment 3 cross reference : Audit Item 7 – Console Access encrypted – Fail

At present all console access to any servers maintained by ACME Corp within each data-hosting centre is clear text and thus is susceptible to sniffing.

Audit Finding 6. No File Integrity in use on Jumpstart servers.
Assignment 3 cross reference : Audit Item 8 – File Integrity Checker in use – Fail

File integrity checkers such as Tripwire ™ are invaluable in de tecting and fixing host intrusions. Unfortunately none of the Jumpstart servers audited had any form of file base integrity checking in use.

Audit Finding 7. Vendor OS patches not up to date.
Assignment 3 cross reference : Audit Item 9 – Vendor OS patches are up to date – Fail

An effectively patched server is one of the most effective ways to minimise the number of vulnerabilities you are exposed too. Unfortunately during the audit it was discovered that none of the Jumpstart servers had there OS fully patched.

Audit Finding 8. Openssh daemon not configured correctly.
Assignment 3 cross reference : Audit Item 10 – NESSUS vulnerability – Fail

As with good wine software generally improves with each new revision; enter ssh protocol version 1 which has a major man -in-the-middle attack vulnerability [30]. As a consequence it is commonly recognised that support for anything less than version 2.x should be avoided wherever possible. Unfortunately during the audit it was discovered that all of the Jumpstart servers allowed ssh connections for ver sions less than 2.x of the ssh protocol.

4.3. Audit Recommendations

Audit Recommendation 1. Timely Applying of patches
Relevant Audit Finding(s):

Audit Finding 1 - JASS not latest version.
Audit Finding 2 - JASS not being periodically reapplied.
Audit Finding 7 - Vendor OS patches not up to date.

Background / Risk:
Patches provided by vendors are a vendor's way of addressing st ability and security issues in their products. The sooner you apply a patch the sooner you as a customer reap the benefits of selecting Vendor X product over Vendor Y.

The real risk here is ACME Corp Jumpstart servers are left exposed to a known vulnerability for which the vendor has provided a patch and since the vulnerability is publicly known about they may even be exploit code available.

Recommendation(s):
It is for this reason I recommend that an effective patching methodology be implemented on all Jumpstart servers as soon as possible.

To do this effectively I believe that the following will be needed as a minimum:

- Establish a policy on applying patches in a timely manner
- Establish procedures required to support such a policy
- Monitor the effective ness of patching

Cost:

- Policy development and rollout - $1 000 labour
- Procedures development and rollout - $5 000 labour
- Develop a patch management strategy - $5 000 labour
- Establish a method with KPI's to monitor patching - $2 000 labour

Mitigating Op tions:
Just as death is a sure thing there is very little you can do to avoid the need to apply patches in a timely manner, however each of the following may assist:

- Ensure all boxes are built with 'OS Minimisation' in mind, the less packages installed the less to maintain.
- Ensure only essential services are enabled.
- A network or host based IDS may assist in identifying some abnormal traffic.

Audit Recommendation 2. Policy of Encryption wherever possible.
Relevant Audit Finding(s):
Audit Finding 5 - Plain text access to all Console Servers
Audit Finding 8 - Openssh daemon not configured correctly.

Background / Risk:
Encryption is a means of preventing the loss of confidentia lly. Although encryption cannot prevent other risks it can all but prevent someone sniffing confidential traffic. Additionally it is not good enough to use any kind of encryption but a industry recognised one, it is also suggested that whenever ssh is used protocol version 2 must be used wherever possible.

The greatest risk here is someone is able to sniff the root password to a server being entered in via a terminal server console access.

Recommendation(s):
As a result I suggest that each console server IOS be upgraded and their configurations be change to only allow ssh access. Unfortunately at this point Cisco only support SSH protocol Version 1 consequentially ACME Corp should seriously consider a different vendor for their terminal servers.

Additionally wherever SSH protocol version 2 can be used it 'must' be used.

Cost:

- Policy development and rollout - $1 000 labour
- Console servers
  - Procedures development and rollout - $2 000 labour
  - New IOS images and additional Memory - $10 000
- Jumpstart servers
  - Procedures to restrict to SSH version2 - $2 000 labour

Mitigating Options:
Centralised one-time password will prevent someone being able to sniff a password for latter reuse but wont prevent any additional confidentially breaches.

Audit Recommendation 3. Policy Access Control on internal traffic.
Relevant Audit Finding(s):
Audit Finding 4 - Non-existence of firewalls to restrict access to Jumpstart.

Background / Risk:
Services which have to be made available for day to day operations e.g. nfs and tftp for Jumpstart should only be available to individual hosts that needs access to them. Additionally only provide access to a resource to individuals when they require it e.g Principle of least privilege.

The biggest risk here is that someone other than intended staff member could mount the share and look for useful material for a subsequent attack on either of the Jumpstart servers or any new server built from one of them.

Recommendation(s):
It is suggested the access control lists be configured as soon as possible on the connecting routers to prevent anyone outside the data centres being able to access Jumpstart services.

It is also suggested that SunScreen 3.2 [17], which is a firewall packaged free of charge for Solaris 8 or 9, be installed and configured to also restrict access to these services.

It is also recommended that the Jumpstart procedure be modified to include sharing the /jumpstart share read only to either the individual host being built or the segment it is on.

Having both router and host based firewall complement each other will provide defense-in-depth.

Cost:

- Policy development and rollout - $1 000 labour
- ACL's Routers
  - Procedures development and rollout - $5 000 labour
- Solaris SunScreen 3.2 [17]
  - Procedures development and rollout - $10 000 labour
- Restrictively share /jumpstart to individual host or Network
  - Update procedures and rollout - $2 000 labour

Mitigating Options:

- Effective patching
- Ensure all boxes are built with 'OS Minimisation' in mind, the less packages installed the less to maintain.
- Ensure only essential services are enabled.
- A network or host based IDS may assist in identifying some abnormal traffic.

Audit Recommendation 4. Policy of File Integrity all servers.

Relevant Audit Finding(s):

Audit Finding 6 - No File Integrity in use on Jumpstart servers.

Background / Risk:

File integrity violations alert(s) can sometimes be the first sign that you have experienced a security incident. Without doubt an up to date file integrity utility will prove invaluable in minimising any downtime due to a breach.

The biggest risk here is a breach is the Jumpstart servers is undetected and all servers built or patched from the compromised Jumpstart infrastructure could be subsequently compromised.

Recommendation(s):

Establish a policy as to which servers require a File based Integrity checking.
Develop procedures in rolling out and maintaining file based integrity checkers.

Cost:

- Policy development and rollout - $1 000 labour
- File integrity Program
  - Software (assume tripwire with existing central console) $10 000
  - Rollout $20 000 - labour
  - Ongoing charges
    - Labour to monitor
    - Increased time to do any work on any server, e.g. apply patches

Mitigating Options:

Accept the risk of :

- Not detecting a breach in a timely manner
- Increased recovery time

Audit Recommendation 5. Policy to start / stop services as required.

Relevant Audit Finding(s):

Audit Finding 3 - Jumpstart services not disabled when not required.

Background / Risk:

Jumpstart requires a number of notoriously insecure protocols, the more available the more likely a known vulnerability will be taken advantage of in compromising one or more of ACME Corp Jumpstart servers.

Recommendation(s):

As Jumpstart is not required every day, to reduce ACME Corp exposure window it is suggested services essential to Jumpstart be disabled when not required.

To ensure that services are disabled when not in use a a utomatic scanning process should be put in place to detect services left running.

Cost:

- Policy development and rollout - $1 000 labour
- Establish Base lining and detecting services left on
  - Labour - $10 000
  - ongoing monitoring costs - $5 000 per year
- Modifying existing procedure to ensure services are disabled when not in use

Mitigating Options:

- Effective patching.
- A network or host based IDS may assist in identifying some abnormal traffic.

5. Appendices

5.1. JASS Standard scripts modified detector

```
#! /bin/sh
# Version 0.1 - 1 May 2003
Purpose="
This script is used to detect whether files shipped in a tar.Z which
also comes with a MANIFEST file containing full path and md5 signatures
 - still exists where they were originally installed
 - have not been modified
Usage:
        $0 <path_to_MANIFEST>
"
#
# WARNING:
# it does not care whether there are more files,
# it simple checks the shipped ones
#
# There must be a unix utility which does this but no friend or foe
# knew of one.
#
# Revision Details:
# 01/05/2003 mtm orig inal
#
usage () {
        echo "${Purpose}"
}

echo "Welcome to manifest Checker"
#
# Check we have one and only one arg
#
if [ $# -ne 1 ]
then
        usage
        exit 1
fi

#
# Check to see if the Manifest file exists
#
if [ ! -f $1 ]
then
        echo MANIFEST file not found
        usage
fi

#
```

```
# Determine the base path of installed files and change to it
#
base=`dirname $1`
cd $base

rm -f /tmp/md5NowUnsorted
echo "Creating current signatures"

#
# for each file in manifest create its signature
#
filelist=`cat $1 | cut  -f2 -d'(' | cut -f1 -d')' `
for i in $filelist
do
        /usr/local/bin/md5 $i >> /tmp/md5NowUnsorted
done

#
# sort to make comparisons more accurate
#
cat /tmp/md5NowUnsorted | sort > /tmp/md5NowSorted
cat $1 | sort > /tmp/md5OrigSorted

echo "And now for the differences"
echo "####### BEGIN DIFF ########"
diff /tmp/md5OrigSorted /tmp/md5NowSorted | grep MD5   \
    | cut -f2 -d'(' | cut -f1 -d')' | sort | uniq
echo "#######  END DIFF  ########"

#
# clean up mess
#
rm -f /tmp/md5NowUnsorted /tmp/md5NowSorted /tmp/md5OrigSort  ed
```

6. References

[1] Sun Microsystems.
NETRA 20 Frequently Asked Questions,
http://www.sun.com/products -n-solutions/hw/networking/netrat/netra20/faq.html (1 March 2003)

[2] Howard, John S and Noordergraaf, Alex.
Jumpstart Technology, Effective Use in the Solaris™ Operating Environment, ISBN 0130621544

[3] Solaris Security Toolkit ('jass').
http://www.sun.com/solutions/blueprints/tools/
(select link 'Solaris Security Toolkit ('jass')), February 2003, (02 March 2003)

[4] Dana Graesser.
Cisco Router Hardening Step -by-Step, 25 July 2001,
http://www.sans.org/rr/firewall/router2.php (1 May 2003)

[5] SANS institute.
http://www.sans.org/rr/firewall/

[6] Pomeranz, Hal.
Solaris Jumpstart Basics, Deer Run Associates,
http://www.deer -run.com/~hal/jumpstart/Jumpstart.pdf (02 April 2003)

[7] Heiss, Jason.
Enterprise Rollouts with Jumpstart, Collective Technologies,
http://xi.nu/~jheiss/js/lisa99/paper.html (23 March 2003)

[8] Noordergraaf, Alex.
How Hackers Do It: T ricks, Tools, and Techniques,
Enterprise Server Products, Online – May 2002,
http://www.sun.com/blueprints/0502/816 -4816-10.pdf (1 February 2003)

[9] Noordergraaf, Alex and Watson, Keith.
Solaris™ Operating Environment, Network Settings for Security: updated for Solaris 8, Online – December 2000,
http://www.sun.com/blueprints/1200/network -updt1.pdf (1 February 2003)

[10] The Centre for Internet Security.
Solaris™ Benchmark v1.2.0, 19 February 2003,
http://www.cisecurity.org/ , (1 April 2003)

[11] Noordergraaf, Alex and Watson, Keith.
Solaris™ Operating Environment Security, U pdated for Solaris 9 Operating Environment, Sun Blueprints ™ Online – December 2002

http://www.sun.com/blueprints/1202/816 -5452.pdf (1 March 2003)

[12] Huffner, Michael J.
Building and Securing a Solaris™ 8 Jumpstart Server, December 2001,
http://www.giac.com/practical/Michael_Huffner_GCUX.doc (27 April 2003)

[13] Boran, Sean.
Hardening Solaris with JASS,
http://www.boran.com/security/sp/Solaris_hardening4.html , (23 March 2003)

[14] Noordergraaf, Alex and Brunette, Glen.
The Solaris™Security Toolkit – Installation, Configuration and Usage Guide, Update d for Toolkit version 0.3,
http://www.sun.com/blueprints/0601/jass_conf_install_-v03.pdf, (05 March 2003)

[15] UNIX Security Checklist V2.0,
http://www.cert.org/tech_tips/usc20_full.html , (02 April 2003)

[16] Noordergraaf, Alex and Brunette, Glen.
The Solaris™ Security Toolkit – Quick Start, Updated for Toolkit Version 0.3,
http://www.sun.com/blueprints/0601/jass_quick_start_-v03.pdf, (05 March 2003)

[17] Sun™ Microsystems.
Docs.sun.com – Sun Product Documentation,
http://docs.sun.com/db/doc/806 -6347/6jfa0g862?q=sunscreen&a=view (1 May 2003)

[18] A White Paper.
Solaris Patch Management: Recommended Strategies,
http://www.sun.com/services/su pport/sw_only/pmstrategies10.02.pdf (28 April 2003)

[19] Radhakrishnan, Ramesh.
A Patch Management Strategy for the Solaris ™ Operating Environment,
Sun Blueprints online – January 2003,
http://www.sun.com/bluep rintts/0103/817-1115.pdf (1 April 2003)

[20] Sun™ Microsystems.
Sun™ Patch Check, Version 1.2,
http://sunsolve.sun.com/pub -cgi/show.pl?target=patchk (28 April 2003)

[21] Sun™ Microsystems.
Solaris™ Patch Manager 1.0,
http://www.sun.com/service/support/sw_only/patchmanager.html (28 April 2003)

[22] SANS Institute.
7.4 Auditing Networks with Nmap and Other Tools, (S ydney 2003)

[23] SANS Institute.

1.1 SANS Security Essential 1: Information Security, The Big Picture, (Sydney 2002)

[24] NESSUS Security scanner V2.0.5.
http://www.nessus.org/nessus_2_0.html (1 May 2003)

[25] Reid, Jason.
Configuring the Secure Shell Software, Sun Blueprints online April 2003,
http://www.sun.com/solutions/blueprints/0403/817_-2485.pdf (28 April 2003)

[26] Bailey, Jeffrey.
Operating Environment Minimisation for Security,
http://www.sans.org/rr/sun/op_environment.php , (17 April 2003)

[27] Spitzer, Lance.
Armouring Solaris,
http://www.spitzner.net/armoring.html (15 January 2003)

[28] Mitnick, Kevin D and Simon, William L.
The Art of Deception,
ISBN 0471237124

[29] SANS Institute.
The SANS Security Policy Project,
http://www.sans.org/resources/policies/ (01 March 2003)

[30] Silverman, Richard E.
dsniff and SSH,
Reports of My Demise are Greatly Exaggerated,
http://sysadmin.oreilly.com/cgi-bin/print.article (1 May 2003)

Last Updated: May 28th, 2017

Upcoming Training

SANS Secure Europe 2017	**Amsterdam, Netherlands**	**Jun 12, 2017 - Jun 20, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**