



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Abstract / Summary

The following practical is for the GCNA certification. The Purpose of the paper is to develop and conduct an audit of a networking component or computer system. For this audit I have chosen the Cisco Secure IDS 4235. I chose the first option which is to perform an audit from the perspective of an independent auditor.

© SANS Institute 2003, Author retains full rights.

**Auditing a Cisco Secure IDS System:
An Auditors Perspective**

Colby DeRodeff, GCIA

November 22, 2003
GSNA Assignment Version 2.1

© SANS Institute 2003, Author retains full rights.

SECTION 1 RESEARCH, MEASUREMENT, CONTROL **5**

INTRODUCTION:	5
NETWORK DIAGRAM:	5
1.1 SYSTEM TO BE AUDITED:	5
SYSTEM DETAILS:	6
1.2 RISK EVALUATION	6
1.3 CURRENT STATE OF PRACTICE	9

SECTION 2.0 CISCO SECURE IDS AUDIT CHECKLIST **10**

2.1 OPERATING SYSTEM CHECKS	10
2.1.1 SECURE AUTHENTICATION AND SYSTEM ACCESS	10
2.1.2 VERIFY THAT ROOT ACCESS IS DISABLED VIA SSH	11
2.1.3 VERIFY TELNET IS DISABLED	11
2.1.4 VERIFY MINIMAL SYSTEM SERVICES ARE RUNNING	11
2.1.5 VERIFY PASSIVE INTERFACE IS SECURE	12
2.1.6 VERIFY OPEN NETWORK PORTS	13
2.1.7 VERIFY PHYSICAL SECURITY: SINGLE USER MODE	13
2.1.8 FILE INTEGRITY: TRIPWIRE	14
2.1.9 VERIFY SYSTEM SECURITY USING A VULNERABILITY SCANNER: NESSUS	14
2.2 CISCO IDS APPLICATION CHECKS	15
2.2.1 VERIFY THE IDS IS RUNNING THE LATEST VERSION OF THE CISCO APPLICATION	15
2.2.2 VERIFY THE LATEST SIGNATURES ARE BEING USED BY THE IDS	15
2.2.3 VERIFY THAT AUTO UPDATE IS BEING USED	16
2.2.4 VERIFY SCP IS BEING USED FOR AUTO UPDATE	17
2.2.5 VERIFY THE REMOTE SCP SERVER IS INCLUDED IN RSA KNOWN HOSTS	17
2.2.6 VERIFY ACL'S ON THE IDS	18
2.2.7 VERIFY TIMESTAMPS ARE ACCURATE: NTP	19
2.2.8 VERIFY USER PRIVILEGES	19
2.2.9 VIEWER ACCOUNTS ON THE IDS HAVE NO SHELL ACCESS	20
2.2.10 AUTO UPDATE PASSWORDS ARE NOT STORED IN CLEAR TEXT	21
2.2.11 VERIFY THAT AUTO BLOCKING IS DISABLED	21

SECTION 3 AUDIT EVIDENCE **22**

SECTION 3.1 CONDUCT THE AUDIT	22
3.1.1 SECURE AUTHENTICATION AND SYSTEM ACCESS	22
3.1.2 VERIFY THAT ROOT ACCESS IS DISABLED VIA SSH	23
3.1.3 ENSURE TELNET IS DISABLED ON THE IDS	23
3.1.4 ENSURE ARP IS DISABLED ON THE SNIFFING INTERFACE	24
3.1.5 VERIFY OPEN NETWORK PORTS ARE LIMITED TO NECESSARY SERVICES	25
3.1.6 VERIFY SYSTEM SECURITY USING A VULNERABILITY SCANNER: NESSUS	26
3.1.7 VERIFY THE IDS IS RUNNING THE LATEST VERSION OF THE CISCO APPLICATION	28
3.1.8 VERIFY ACL'S ON THE IDS	29
3.1.9 VIEWER ACCOUNTS ON THE IDS HAVE NO SHELL ACCESS	30

3.1.10 ENSURE AUTO UPDATE PASSWORDS ARE NOT STORED IN CLEAR TEXT	30
SECTION 3.2 RESIDUAL RISK	32
SECTION 3.3 IS THE SYSTEM AUDITABLE	33
 SECTION 4 AUDIT REPORT	 33
 4.1 EXECUTIVE SUMMARY	 33
SECTION 4.2 AUDIT FINDINGS	34
OPERATING SYSTEM SUMMARY	34
CISCO IDS APPLICATION SECURITY	38
SECTION 4.3 BACKGROUND / RISK	41
SECTION 4.4 AUDIT RECOMMENDATIONS	42
SECTION 4.5 COSTS	43
SECTION 4.6 COMPENSATING CONTROLS	43
 CONCLUSION	 44
 REFERENCES	 45

© SANS Institute 2003, Author retains full rights.

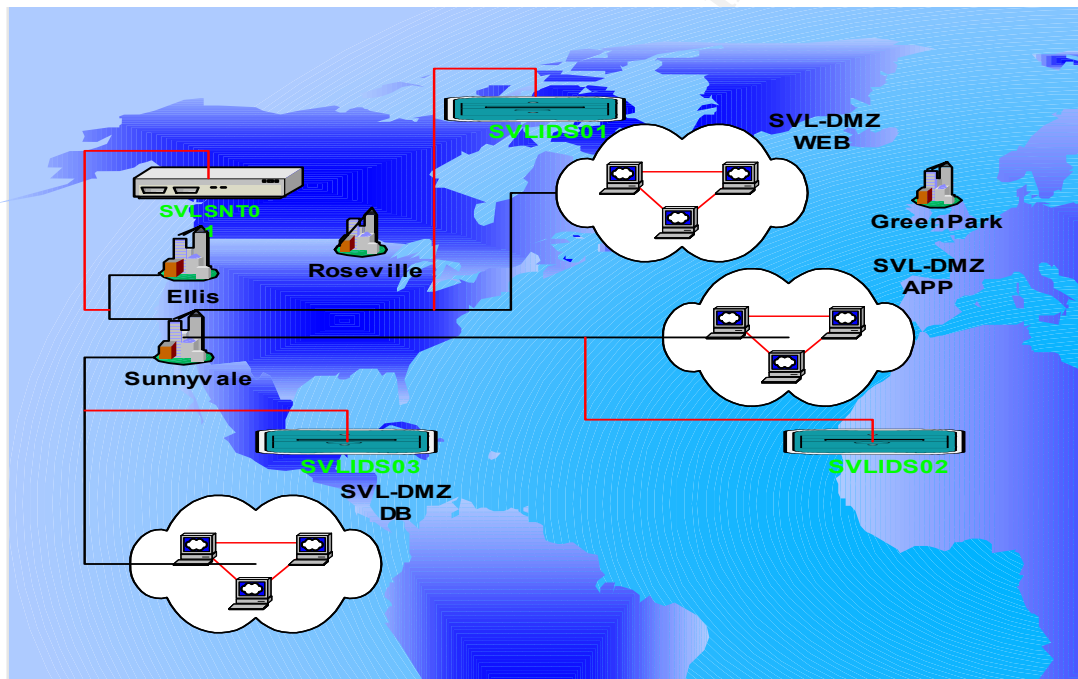
Section 1 Research, Measurement, Control

Introduction:

This audit is being conducted at a large software company and will focus on their IDS infrastructure. The company has recently deployed Cisco Secure IDS Systems globally and they are in need of an audit to ensure that the intrusion detection systems are secure and running with the best known configuration. They are currently using the IDS' to monitor their DMZ systems and WAN links between major metropolitan cities. The audit is being conducted in their Silicon Valley location. This paper is written from the perspective of a consultant who has been hired to design and perform the audit.

Network Diagram:

The following diagram is a topology of the network on which the target IDS resides.



1.1 System to Be Audited:

The focus of this audit is a Cisco Secure IDS 4235 running version 4.1 with the latest signature packs. The target system is an appliance, being used to monitor the Web Server DMZ. The IDS sniffing interface (eth0) is connected to port on the switch that is spanning the web DMZ vlan. The management interface (eth1) resides on a security vlan which is protected using ACL's on the switch. The purpose of the security vlan is to

separate security focused devices such as the IDS and scanning systems from regularly accessible systems within the corporate environment.

System Details:

Manufacturer	Dell / Cisco Systems Inc.
System	Cisco IDS-4235
Processor	Intel Pentium III CPU 1266MHz
Memory	1 gb
eth0	Intel PRO/1000
eth1	Intel PRO/1000
Operating System	Linux version 2.4.18-5smp
IDS Software Version	4.1(2)
Signature Pack Version	S58

1.2 Risk Evaluation

Risk Evaluation is intended to outline the possible scenarios that need to be addressed by the audit. Once the risks are determined then it is possible to develop an audit plan that takes these risks into account as well as providing the steps necessary based on best practices to avoid these pitfalls. When determining the risks of the IDS systems I have considered the specific risk, the probability that the risk will be exploited, as well as the consequences if an attacker were to exploit one of the named vulnerabilities.

1)

Risk	Attacker gains root access to the system.
Probability	Low. The IDS is on a private vlan and as long as best practices are used as far as authentication and patch management this shouldn't be much of a concern.
Severity	High. The system would be compromised.
Consequences	With a root shell an attacker could manipulate the signatures, disable the IDS entirely, or numerous other malicious activities.

2)

Risk	Timestamps are inaccurate because NTP is not utilized.
Probability	High. Most systems I've seen the administrators have overlooked small details like the system time.
Severity	Medium. This is based on the importance of time stamps when trying to correlate IDS events with events from other security devices such as firewalls.
Consequences	If the time stamps are inaccurate it will not provide analysts with accurate information when analyzing the events from the IDS which may cause an attack to be overlooked.

3)

Risk	Signatures are out of date.
Probability	High. Administrators need to keep the signatures up to date and this may be easily overlooked.
Severity	High. Attacks may not be detected.
Consequences	If the signatures are not up to date the IDS will not detect an attack which is intended to exploit a recently discovered vulnerability. There are new viruses and worms released all the time and with these new exploits signatures are written and released to detect them.

4)

Risk	Clear text passwords are being passed on the network.
Probability	Low. By default telnet is disabled on the IDS system and ssh is running.
Severity	High. Clear text passwords can be sniffed on the network and utilized to gain access to the system.
Consequences	Based on the privileges of the compromised account many malicious activities can be performed. If it is the root account then the system would be compromised.

5)

Risk	Open network ports on the IDS
Probability	Medium. There are several services running by default, and other less secure services may be enabled.
Severity	High. Depending on the ports that are open and the services listening on those ports the system may be vulnerable to an exploit.
Consequences	Depending on the vulnerability a wide variety of results are possible such as a denial of service or a buffer overflow.

6)

Risk	IDS is accessible from any 10.0.0.0 address.
Probability	High. By default access is enabled from any 10.0.0.0 address.
Severity	Medium. By having weak ACL's on the system it is easier to access the IDS from another possibly compromised host or by using a spoofed address.
Consequences	Consequences vary depending on the intent of the attacker but at the very least the events being generated could be viewed informing the attacker of the signatures that are being used. An attacker could then try different attack methods on systems until they find one that is not detected.

7)

Risk	User changes the configuration due to improper privilege assignment.
Probability	Low. It would take an administrator to change the privilege level.
Severity	High. The user could disable the sensing interface or change a crucial configuration.
Consequences	IDS may not be generating events or might not detect attacks based on the configuration change that was made.

8)

Risk	Access is gained to remote SCP server being used for auto updates.
Probability	Low. If an attacker gains access to the system with either a root shell or a Cisco IOS shell they can obtain the password used for auto update via SCP as the username and password are stored in clear text. With an IOS shell the show configuration command can be issued and the password is not obfuscated. If an attacker gains a bash shell they can view the file /usr/cids/idsRoot/etc/curHostConfig.xml , which contains both the username and password for the system setup as a remote scp server.
Severity	High. Providing a username and password to another system is extremely dangerous
Consequences	If an attacker gains access to the remote scp server the system is compromised and they may have access to other systems depending on the account being used for the auto update.

9)

Risk	Legitimate traffic is blocked.
Probability	Medium. If auto blocking is enabled and not configured correctly legitimate traffic may be blocked.
Severity	High. This could cause business transactions to be blocked.
Consequences	This could cause customers to be denied service or block critical infrastructure services.

10)

Risk	IDS floods event correlation engine.
Probability	High. By default all signatures are enabled.
Severity	Medium. An event flood may cause inaccurate results when overall security is analyzed.
Consequences	An analyst may miss critical events or events that are important to particular systems due to a flood of false positives.

11)

Risk	Attacker gains access to the system via the sniffing interface.
Probability	Low. If ARP is enabled an attacker could send out a spoofed ARP request and receive a response from the passive interface containing the physical address of the interface. The physical address could also be gained from the ARP tables on either a router or another system. Many Cisco routers running an older IOS can give up configuration information via an HTTPS request.
Severity	High. The attacker may launch a DOS on the IDS or possibly gain access to the system.
Consequences	Depending on the attacker's intentions, the system may be compromised or a DOS could be directed at the physical address causing the IDS to slow down and miss attacks on other systems.

1.3 Current State of practice

After researching the Cisco IDS system and extensively searching for auditing techniques regarding these systems, I was slightly surprised that I was unable to find any audit checklists or even pointers as to best security practices when using these systems. Since I was hired to deploy these systems as well as audit them once configured, I have generated my own audit checklist based on the work I have done with the IDS'. There are configuration guidelines as well as documentation for the IDS available from the Cisco TAC, www.cisco.com/tac Unfortunately as far as this paper is concerned you must have a CCO account to access these documents.

The Cisco documentation basically covers the different options as far as configuration goes but does not cover best security practices. In fact I was a little disappointed at the seemingly lack of focus on security when it came to the device in general. Since I was unable to find a sufficient audit checklist to base my audit plan on, I am generating my checklist based on the configuration I wrote as part of my deployment process. While building these systems I discovered what I found to be the most secure and efficient ways to configure and protect the IDS not only from malicious activity but user error and configuration management as well. I took into account the update process to ensure the IDS was always running the latest signature packs, I also took into account the integrity of the data being generated by the IDS, and the overall security of the system itself down to the basics of the operating system.

Since the IDS runs on a slightly modified version of Red Hat Linux I was able to pull basic auditing techniques from the "Auditing Linux" checklist written by Krishini Naidu. http://www.sans.org/score/checklists/Auditing_Linux.doc

I was also able to reference a practical written by Brent Zimmerman.

"Auditing a Snort Intrusion Detection System: An Auditors Perspective"

http://www.giac.org/practical/GSNA/Brent_Zimmerman_GSNA.pdf

Using these documents and personal knowledge and experience, I derived the initial section of my audit plan which focuses on the overall system security.

Section 2.0 Cisco Secure IDS Audit Checklist

The audit being outlined in this checklist is intended to check the overall security of the Cisco 4235 Secure IDS. The audit will begin with the operating system security then move to the Cisco application and configuration security. This audit should be conducted with an administrator who has root access to the IDS as well as a working knowledge of the target environment.

To perform the audit the following tools will be needed.

NMAP available from www.insecure.org

Nessus Vulnerability Scanner available from www.nessus.org

2.1 Operating System Checks

2.1.1 Secure Authentication and System Access

References	<ol style="list-style-type: none">1. Naidu, Krishni. "Auditing Linux" http://www.sans.org/score/checklists/AuditingLinux.doc2. Personal Knowledge and Experience3. Zimmerman, Brent. "Auditing a Snort Intrusion Detection System: An Auditors Perspective" http://www.giac.org/practical/GSNA/Brent_Zimmerman_GSNA.pdf	
Control Objective	Ensure SSHd is running and listening on port 22.	
Risk	SSH is a secure protocol and by using SSH rather than telnet one avoids passing clear text passwords and commands on the network. Clear text passwords may be sniffed and used in a malicious manner.	
Test Type	Both tests are objective	
#	Test	Compliance
1	From a bash shell on the IDS, as root, run the chkconfig command and look for sshd. [root@sensor]# chkconfig --list grep sshd	The following line should be displayed: sshd 0:off 1:off 2:on 3:on 4:on 5:on 6:off
2	From a remote system use NMAP to scan the system and verify the output shows SSHd running on port 22. [root@lab20]# nmap -sS -vv -n -p 22 "ipAddress" the -sS option specifies a SYN scan where a SYN packet is sent to the specified port. The -vv option specifies to be very verbose in the output, -n specifies to not resolve the hostname, while -p 22 specifies scan only port 22.	The output from NMAP should look like this: PORT STATE SERVICE 22/tcp open ssh
3	From a bash prompt enter the following	The netstat command should return that

commands: [root@sensor]# netstat -an grep 22 [root@sensor]# ps -ef grep ssh	port 22 is in a listening state and the ps –ef command should return /usr/sbin/sshd is running.
---	---

2.1.2 Verify that root access is disabled via SSH

References	1. Personal Knowledge and Experience	
Control Objective	Ensure that the root user is not allowed to login to the IDS via SSH.	
Risk	If the root account is allowed to login via ssh then a weak password or a brute force attack could allow the attacker root access to the IDS.	
Test Type	Objective	
#	Test	Compliance
1	Enter the following command: [root@sensor]# cat /etc/ssh/sshd_config grep PermitRootLogin	The result should be the following line in the sshd_config file: PermitRootLogin no
2	Try to ssh to the IDS system as root. ssh root@sensor	The result of this attempt should be a failed login.

2.1.3 Verify Telnet is disabled

References	1. Personal Knowledge and Experience	
Control Objective	Verify that telnet is disabled.	
Risk	If telnet is enabled then an attacker can sniff the network traffic and gather usernames, passwords, and configuration commands. Using this information the attacker can log onto the IDS and compromise the system.	
Test Type	Objective	
#	Test	Compliance
1	From the Cisco IOS shell enter the show configuration command: sensor# show configuration	In the configuration the following line will be displayed: telnetOption disabled
2	Try to telnet to the IDS and verify that telnet is not accepting connections. telnet sensor where sensor is the hostname or IP address of the IDS.	The result of this test should be a connection time out.

2.1.4 Verify minimal system services are running

References	1. Naidu, Krishni. "Auditing Linux" http://www.sans.org/score/checklists/AuditingLinux.doc 2. Personal Knowledge and Experience 3. Company Best Known Configuration Practices
-------------------	---

Control Objective	Verify that only minimal system services are running on the IDS.	
Risk	In the case of a dedicated IDS, since no other function is preformed besides packet analysis and event reporting it is not recommended to have unnecessary services running because it can affect performance and create additional vulnerabilities, which may allow an attacker to exploit a vulnerability that otherwise wouldn't be present.	
Test Type	Objective.	
#	Test	Compliance
1	From a console as root run the setup command and select system services . View the services that are enabled.	Based on the security policy and their best practices as far as the Cisco IDS the only services that should be enabled are: Anacron, cids, crond, keytable, network, random, rawdevices, sshd, syslog, xinetd
2	From a bash shell as root use the chkconfig command to find all the enabled services. [root@sensor]# chkconfig -list grep on	The services that are returned as on should be: Anacron, cids, crond, keytable, network, random, rawdevices, sshd, syslog, xinetd

2.1.5 Verify Passive Interface is Secure

References	<ol style="list-style-type: none"> 1. Personal Knowledge and Experience 2. Stephen Northcutt at SANS Intrusion Analyst Training in San Francisco December 2001 	
Control Objective	Ensure that ARP is disabled on the sniffing interface (eth0)	
Risk	If ARP (Address Resolution Protocol) is enabled then an attacker could possibly send out a crafted ARP request and receive a response from the passive interface. The response will contain the Ethernet address or the physical address of the interface. The attacker could also gain access to either a router or another system's ARP table. Using the physical address an attacker could launch a DOS on the IDS causing a disruption in traffic analysis or possibly gain access to the system since the passive interface on a semi public network segment as opposed to the management interface which resides on a private vlan.	
Test Type	Objective	
#	Test	Compliance
1	As root issue the ifconfig command and examine the output for the ARP configuration. [root@sensor]# ifconfig -a	The expected result should contain the NOARP entry for eth0 and look like this: [root@sensor]# ifconfig -a eth0 Link encap:Ethernet HWaddr 00:03:47:90:99:67 UP BROADCAST NOARP MULTICAST MTU:1500 Metric:1 RX packets:0 errors:0 dropped:0

	overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:100 RX bytes:0 (0.0 b) TX bytes:0 (0.0 b) Interrupt:11 Base address:0xf000
--	---

2.1.6 Verify Open Network Ports

References	1. Personal Knowledge and Experience 2. Company Best Known Configuration Practices	
Control Objective	Verify that the only open ports are 22 (sshd) and 443 (https) the Cisco IDS web server runs on port 443 and only accepts secure HTTP connections.	
Risk	If there are open ports other than the ones specified, there will be increased chances of a vulnerability that can be exploited by a malicious attacker.	
Test Type	Objective.	
#	Test	Compliance
1	From a bash prompt as root enter the following command: [root@sensor]# netstat -an	The result should be that only ports 22 and 443 are in a listening state.
2	Using NMAP scan the IDS to check for open ports. Try different types of scans by using different options to ensure the results are accurate. [root@lab20 root]# nmap -sS -vv -n -p 1-65535 10.17.17.10 [root@lab20 root]# nmap -sT -vv -n -p 1-65535 10.17.17.10 [root@lab20 root]# nmap -sF -vv -n -p 1-65535 10.17.17.10 [root@lab20 root]# nmap -sX -vv -n -p 1-65535 10.17.17.10	The result of all four of these scans should be the same and identical to the following output: (The 65533 ports scanned but not shown below are in state: closed) PORT STATE SERVICE 22/tcp open ssh 443/tcp open https

2.1.7 Verify Physical Security: Single User Mode

References	1. Naidu, Krishni. "Auditing Linux" http://www.sans.org/score/checklists/AuditingLinux.doc 2. Personal Knowledge and Experience 3. Zimmerman, Brent. "Auditing a Snort Intrusion Detection System: An Auditors Perspective" http://www.giac.org/practical/GSNA/Brent_Zimmerman_GSNA.pdf
Control	Verify that the system requires a password when booted into single user

Objective	mode.	
Risk	If a password is not required for single user mode anyone with physical console access to the system could reboot it and enter single user mode without the use of a password. Once they get a shell they could change the root password add accounts and the system would be considered compromised.	
Test Type	Objective	
#	Test	Compliance
1	From a bash prompt on the IDS view the lilo.conf file: [root@sensor root] cat /etc/lilo.conf	The lilo.conf file should contain the following line: password=<password>
2	Reboot the ids and enter linux single at the lilo or boot prompt.	Verify that the system asks for a password before booting into single user mode.

2.1.8 File Integrity: Tripwire

References	<ol style="list-style-type: none"> 1. Naidu, Krishni. "Auditing Linux" http://www.sans.org/score/checklists/AuditingLinux.doc 2. Personal Knowledge and Experience 3. Company Best Known Configuration Practices 	
Control Objective	Ensure Tripwire is running on the IDS	
Risk	If tripwire is not running then an attacker could modify the IDS configuration and the administrator may be unaware of changes made such as the active signatures or system configuration files.	
Test Type	Objective	
#	Test	Compliance
1	From a bash prompt as root enter the following command: [root@sensor root]# rpm -qa grep trip	The following rpm must be installed: X_tripwire_agent_linux-3.0.1-1.i386.rpm This is a custom RPM built by the tripwire administrator at this particular company. Results at other companies will not have this particular RPM installed.

2.1.9 Verify system security using a vulnerability scanner: Nessus

References	<ol style="list-style-type: none"> 1. Personal Knowledge and Experience 2. Company Best Known Configuration Practices 3. http://www.nessus.org 	
Control Objective	Check System Vulnerabilities using a vulnerability scanner. Verify that there are no medium or high severity vulnerabilities due to services that are necessary for sensor operation.	
Risk	If there are vulnerabilities which exist on the system due to essential	

	services that are running then an attacker could exploit these vulnerabilities to disable the IDS to attack other systems without being detected or to gain access to the IDS.	
Test Type		Objective
#	Test	Compliance
1	Run a full Nessus scan with all plugins enabled. Run the scan from a host that does not have access to the IDS based on the ACL's on the system.	There should not be any High or medium severity vulnerabilities reported. There should not be any vulnerabilities reported that can be exploited to gain system access or cause a DOS. If a low severity vulnerability such as an information leak is reported the device is still considered to be in compliance with the company's security policy.

2.2 Cisco IDS Application Checks

2.2.1 Verify the IDS is running the latest version of the Cisco application

References	<ol style="list-style-type: none"> 1. Personal Knowledge and Experience 2. Cisco Secure IDS Configuration Guide www.cisco.com/tac 	
Control Objective	Ensure the CSIDS (Cisco Secure IDS) application is running the latest version.	
Risk	Updates for the IDS application contain security fixes for many different things so far there have been two major updates one of them contained a fix for a vulnerable version of ssh. Since the IDS runs a modified version of ssh the updates must come from Cisco otherwise the support contract on the system is void. To ensure the security and most reliable operation of the IDS it is crucial to have the latest updates.	
Test Type		Objective
#	Test	Compliance
1	From a Cisco IOS prompt issue the show version command at check the version of the main application. sensor# show version	At the time this paper was written the latest application update was Version 4.1(2). The following line must be displayed as a result of the show version command: Cisco Systems Intrusion Detection Sensor, Version 4.1(2)S58

2.2.2 Verify the latest signatures are being used by the IDS

References	<ol style="list-style-type: none"> 1. Personal Knowledge and Experience 2. Cisco Secure IDS Configuration Guide www.cisco.com/tac 	
Control Objective	Ensure the IDS is using the latest signatures.	

Risk	Every time a new vulnerability or virus is released the signature writing team at Cisco tries to get out a new signature pack to include a signature to detect the new attack. If the IDS is running with an out of date signature pack then the system will not detect attempts to exploit a new vulnerability or any new virus / Trojan activity.	
Test Type	Objective	
#	Test	Compliance
1	From a Cisco IOS prompt issue the show version command: Sensor# configure terminal sensor(config)# show version	When this audit checklist was created the latest signature pack was S59. Verify that you see the following line: Upgrade History: IDS-sig-4.1-1-S59.rpm.pkg 16:57:03 UTC Thu Oct 23 2003

2.2.3 Verify that auto update is being used

References	<ol style="list-style-type: none"> 1. Personal Knowledge and Experience 2. Cisco Secure IDS Configuration Guide www.cisco.com/tac 	
Control Objective	Verify that auto update is being used to update the IDS signatures as well as to update the application.	
Risk	If auto update is not being used it is an administrator's responsibility to apply the updates and if the administrator is responsible for managing a large number of these systems it becomes a tedious process and mistakes can be made and updates can be overlooked. As previously stated when the latest updates are not running on the system attacks may be undetected and the system may be vulnerable.	
Test Type	Objective	
#	Test	Compliance
1	From a Cisco IOS prompt run the show configuration command and examine the output. sensor# configure terminal sensor(config)# service host sensor (config host)# show config	Verify the following lines exist: optionalAutoUpgrade active-selection autoUpgradeParams autoUpgradeParams schedule active-selection calendarUpgrade calendarUpgrade timesOfDay time 02:00:00 daysOfWeek day tue
2	From a Cisco IOS host configuration prompt enter the following commands to ensure that the Auto Update is configured to copy the updates from the correct server and location on that server: sensor# configure terminal sensor(config)# service host	Verify the following lines are present: ipAddress 10.17.17.227 directory /home/service/cisco/ids/updates username service password PaSsWoRd **PASSWORD IN PLAIN TEXT**

	sensor (config host)# show config	
3	On the remote server used for auto update you must make sure the directory exists and that the specified user has access to it. [root@sensor root]# ssh user@Server [user@server user] ls /home/service/cisco/ids/updates	The user must be able to access the system so the login attempt must be successful and the directory list must be in existence and should contain Cisco update files with the correct naming convention i.e. IDS-*

2.2.4 Verify SCP is being used for auto update

References	1. Personal Knowledge and Experience 2. Cisco Secure IDS Configuration Guide www.cisco.com/tac	
Control Objective	Verify that the auto update feature is using SCP not FTP.	
Risk	SCP must be used rather than FTP because FTP uses clear text authentication and therefore passes usernames and passwords on the network in clear text. This could allow an attacker to sniff the traffic and gain access to the remote update server.	
Test Type	Objective	
#	Test	Compliance
1	From a Cisco IOS host configuration prompt enter the following commands to ensure that the Auto Update is configured to use SCP rather than FTP: sensor# configure terminal sensor(config)# service host sensor (config host)# show config	Verify the existence of the following line: fileCopyProtocol scp

2.2.5 Verify the remote SCP server is included in RSA known hosts

References	1. Personal Knowledge and Experience 2. Cisco Secure IDS Configuration Guide www.cisco.com/tac	
Control Objective	Ensure that the remote SCP server is added to RSA Known Hosts.	
Risk	If the remote server is not added to the known hosts then SCP will not work and this will cause the signature versions as well as the application version to be out of date.	
Test Type	Objective	
#	Test	Compliance

1	<p>From a Cisco IOS host configuration prompt enter the following commands to ensure that the remote SCP server is contained in RSA known hosts:</p> <pre> sensor# configure terminal sensor(config)# service host sensor (config host)# show config </pre>	<p>Verify that the IP address of the remote server is listed and its public key is displayed. It will be similar to the following entry:</p> <pre> service SshKnownHosts rsa1Keys id x.x.x.x (where x.x.x.x is the IP address of the remote scp server) exponent 35 length 1024 modulus 11960129149732229033877422032741529825 4034792168640480766165460917765661 96673897845365568813248390453874613644 26312455443716818643513476054791070821 7190 54600394709560641938866196206576824040 13004154482136038670385733851253588789 2037 77026231260755785567105228547879699627 90489403992752128609996547640399639926 9 </pre>
---	--	--

2.2.6 Verify ACL's on the IDS

References		1. Personal Knowledge and Experience 2. Cisco Secure IDS Configuration Guide www.cisco.com/tac
Control Objective		Ensure that only hosts that need access to the system are allowed to access the IDS.
Risk		The IDS has ACL's and they must be restricted to only allow specified hosts as defined by the administrator or owner of the system. By default access is allowed from 10.0.0.0 netmask 255.0.0.0 This entry must be removed and replaced with entries limiting access to only the systems that are gathering events from the IDS and systems that are used to manage the IDS.
Test Type		Objective.
#	Test	Compliance
1	<p>From a Cisco IOS prompt enter the following commands:</p> <pre> Sensor# configure terminal sensor(config)# service host sensor (config host)# network parameters sensor (config host net)# show accessList </pre>	<p>The following entries may vary based on the systems that require access to the IDS, you want to ensure that there are hosts permitted to access the system as well as verify that the blanket entry for 10.0.0.0 does not exist:</p> <pre> accessList ipAddress 10.17.12.138 netmask 255.255.255.255 accessList ipAddress 10.17.17.227 netmask 255.255.255.255 accessList ipAddress 10.17.17.223 </pre>

		netmask 255.255.255.255
2	From a host not named in the access list table from test 1 try to ssh to the IDS and verify that the connection is denied. [user@NotAllowed] ssh user@sensor	The connection should not be accepted and the result should be the following: ssh: connect to host sensor port 22: Connection refused
3	From a host that is named in the access list table from test 1 try to ssh to the IDS and verify that the connection is accepted. [user@Allowed] ssh user@sensor	The ssh attempt should return a prompt for a password and allow access to the IDS.

2.2.7 Verify timestamps are accurate: NTP

References	1. Personal Knowledge and Experience 2. Cisco Secure IDS Configuration Guide www.cisco.com/tac	
Control Objective	Verify that NTP is enabled and is configured using authenticated NTP with the correct Key Value pair.	
Risk	With out the use of NTP the timestamps of events will not be accurate when compared to the events generated from other systems. When analyzing and correlating IDS events with events from other systems such as firewalls and host based IDS' the timestamps are critical in ordering the events as well as analyzing if particular events correlate to each other.	
Test Type	Objective	
#	Test	Compliance
1	From a Cisco IOS prompt enter the following commands: sensor# configure terminal sensor(config)# service host sensor (config host)# time parameters sensor (config host tim)# show settings	The following entries must present and the key ID and value need to be compared with the results of test 2: ntpServers ipAddress 10.17.1.45 keyId 100 keyValue 1000
2	On the NTP server verify the correct key ID and Value pair are being used: cat /etc/ntp/keys	Verify that the values match the entries from test 1: # 1000 M akey 100 M pass

2.2.8 Verify user privileges

References	1. Personal Knowledge and Experience 2. Cisco Secure IDS Configuration Guide www.cisco.com/tac
-------------------	--

Control Objective	Verify the privilege level of the Users on the IDS System. The user's privilege level should be set in accordance with their role on the IDS.	
Risk	If a particular user does not have the correct privileges within the Cisco application they may not be able to perform their job functions as well as they may be able to change configuration settings if they are granted too many privileges.	
Test Type	Objective.	
#	Test	Compliance
1	Login to the sensor via the web interface and select the configuration tab and click on users. https://sensor	There should be at least 3 entries here maybe more depending on the number of users who are allowed to access the IDS to view events. Ensure the following accounts are present: Cisco Privilege Level – Administrator Service Privilege Level – Service Viewer Privilege Level – Viewer User1 Privilege Level - Viewer
2	Login to the IDS as an account with Viewer Privileges and issue the following commands: sensor# configure terminal sensor(config)# service host sensor (config host)# network parameters sensor (config host net)# ipAddress	The result of the ipAddress command should be the following: sensor (config host net)# Command Not Found Since the IP Address command is used to configure the IP address of the IDS accounts with the viewer privilege should not be able to execute that command.

2.2.9 Viewer accounts on the IDS have no shell access

References	<ol style="list-style-type: none"> 1. Personal Knowledge and Experience 2. Cisco Secure IDS Configuration Guide www.cisco.com/tac 	
Control Objective	Ensure All viewer accounts on the IDS are configured with no login.	
Risk	If the view only accounts are configured with login access to the system at a shell level, default, then they may su to root or cisco and possibly change the configuration of the system. If an attacker cracks one of these accounts he will be granted a shell on the IDS and may use that for malicious activities.	
Test Type	Objective	
#	Test	Compliance
1	As root on the IDS system cat the password file and verify that all viewer accounts are configured for /sbin/nologin. This will not affect the ability to login via https and access the event viewer.	For the accounts that are designated as viewer accounts ensure they are configured as the following one: viewer:x:5004:5000::/home/viewer:/sbin/nologin

	<code>[root@sensor root] cat /etc/passwd</code>	
2	As a user with view only privileges try to ssh to the IDS and see if the account is allowed to login. <code>[root@lab20 root] ssh viewer@sensor</code>	The login attempt should fail: <code>[root@lab20 root] ssh viewer@sensor</code> viewer@sensor's password: Permission denied, please try again.

2.2.10 Auto Update passwords are not stored in clear text

References		1. Personal Knowledge and Experience
Control Objective		Ensure passwords for auto update are not stored in clear text on the system.
Risk		If an attacker gains access to the IDS and there are configuration files with the auto update passwords stored in clear text on the system then the attacker would be able to compromise the remote SCP server that is being used for auto updates.
Test Type		Objective
#	Test	Compliance
1	As root on the IDS view the configuration file and look at the output: <code>[root@sensor root] cat /usr/cids/idsRoot/etc/curHostConfig.xml</code>	The following line should not display the username and password in clear text: <code><var name="username" protected="false">service</var></code> <code><var name="password" protected="false">PaSsWoRd</var></code>
2	From a Cisco IOS Prompt run the show configuration command and look at the output: <code>sensor# configure terminal</code> <code>sensor(config)# show configuration</code>	You should not see the username and password for auto update displayed in clear text.

2.2.11 Verify that auto blocking is disabled

References		1. Personal Knowledge and Experience 2. Cisco Secure IDS Configuration Guide www.cisco.com/tac
Control Objective		Verify that auto blocking is not enabled.
Risk		Auto blocking is used a protection against malicious traffic. It works by sending border routers and firewalls configuration commands that will block the traffic suspected as malicious. The second option is that the system can send TCP reset packets to the initiator of the traffic deemed malicious. Many IDS signatures have false positives that will result in disrupting of non-malicious connections.
Test Type		Objective.
#	Test	Compliance

1	Login to the IDS via https and click on the configuration tab and select auto blocking. https://sensor	The auto blocking checkbox should be unchecked.
---	--	---

Section 3 Audit Evidence

The following section will cover the ten audit checks deemed most critical, the calculated residual risk, and the overall ability to conduct an audit of a Cisco Secure IDS. The full audit was conducted for the final audit report but as stated only the ten most critical checks will be looked at in detail. Each detailed check will include whether or not the system was in compliance as well as the test results for each test performed.

Section 3.1 Conduct the Audit

3.1.1 Secure Authentication and System Access

Check List Item 2.1.1 PASS

Objective: Ensure SSHd is running and listening on port 22.

Test 1:

From a bash shell on the IDS, as root, run the chkconfig command and look for sshd.

```
[root@sensor]# chkconfig --list | grep sshd
sshd          0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

Test 2: From a remote system use NMAP to scan the system and verify the output shows sshd running on port 22.

```
[root@lab20]# nmap -sS -vv -n -p 22 sensor

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-11 14:58
Host 10.17.17.10 appears to be up ... good.
Initiating SYN Stealth Scan against 10.17.17.10 at 14:58
Adding open port 22/tcp
The SYN Stealth Scan took 1 seconds to scan 1 port.
Interesting ports on 10.17.17.10:
PORT      STATE SERVICE
22/tcp    open  ssh
Nmap run completed -- 1 IP address (1 host up) scanned in 1.461 seconds
```

Test 3: From a bash prompt enter the following commands:


```
[root@sensor]# netstat -an |grep 22
TCP      0.0.0.0:22      0.0.0.0:0      LISTENING

[root@sensor]# ps -ef | grep ssh
root      0      232      ?    12:19:26 /usr/sbin/sshd
```

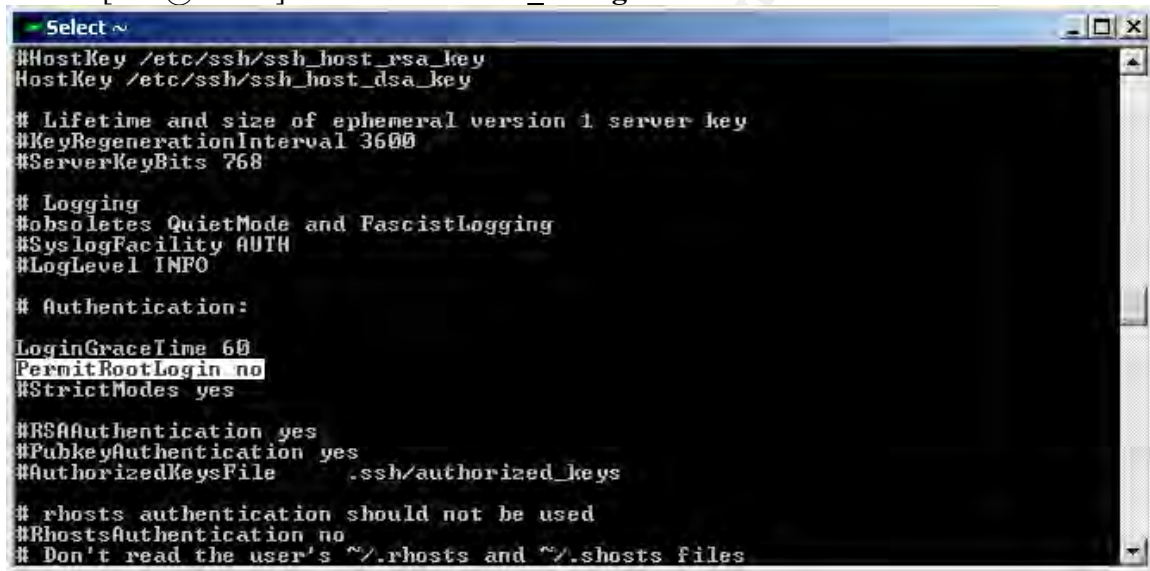
3.1.2 Verify that root access is disabled via SSH

[Check List Item 2.1.2](#) PASS

Objective: Ensure that the root user is not allowed to login to the IDS via SSH.

Test 1: Examine the ssh configuration file to ensure root login is not permitted.

```
[root@sensor]# cat /etc/ssh/sshd_config
```



```
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 3600
#ServerKeyBits 768

# Logging
#obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

LoginGraceTime 60
PermitRootLogin no
#StrictModes yes

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile .ssh/authorized_keys

# rhosts authentication should not be used
#RhostsAuthentication no
# Don't read the user's ~/.rhosts and ~/.shosts files
```

Test 2: Try to ssh to the IDS system as root.

```
[root@lab20 root] ssh root@sensor
root@sensor's password:
Permission denied, please try again.
```

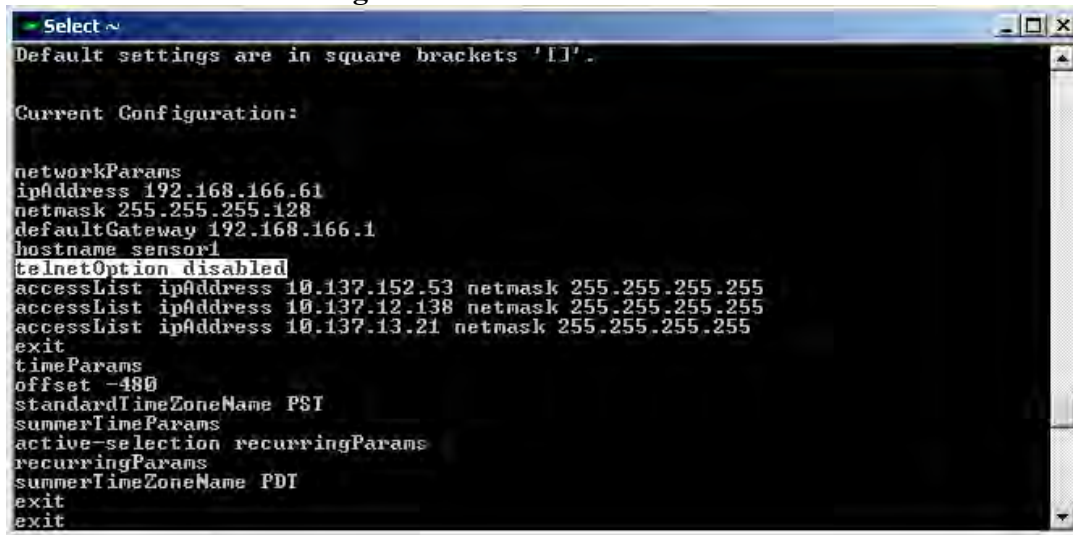
3.1.3 Ensure Telnet is disabled on the IDS

[Check List Item 2.1.3](#) PASS

Objective: Verify that telnet is disabled.

Test 1: From the Cisco IOS shell enter the show configuration command:

sensor# show configuration



```
Select ~
Default settings are in square brackets '[]'.

Current Configuration:

networkParams
ipAddress 192.168.166.61
netmask 255.255.255.128
defaultGateway 192.168.166.1
hostname sensor1
telnetOption disabled
accessList ipAddress 10.137.152.53 netmask 255.255.255.255
accessList ipAddress 10.137.12.138 netmask 255.255.255.255
accessList ipAddress 10.137.13.21 netmask 255.255.255.255
exit
timeParams
offset -480
standardTimeZoneName PST
summerTimeParams
active-selection recurringParams
recurringParams
summerTimeZoneName PDT
exit
exit
```

Test 2: Try to telnet to the IDS and verify that telnet is not accepting connections.

```
[root@lab20 root] telnet sensor
Connecting To sensor...Could not open connection
to the host, on port 23.
No connection could be made because the target
machine actively refused it.
```

3.1.4 Ensure ARP is disabled on the Sniffing interface

[Checklist Item 2.1.5](#) PASS

Objective: Ensure that ARP is disabled on the sniffing interface (eth0)

Test 1: As root issue the ifconfig command and examine the output for the ARP configuration.

```
[root@sensor]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:03:47:90:99:67
          UP BROADCAST NOARP MULTICAST  MTU:1500
          Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:11 Base address:0xf000
```

3.1.5 Verify open network ports are limited to necessary services

[Checklist Item 2.1.6](#) PASS

Objective: Verify that the only open ports are 22 (sshd) and 443 (https) the Cisco IDS web server runs on port 443 and only accepts secure HTTP connections.

Test 1: From a bash prompt as root enter the netstat command and examine the output.

```
[root@sensor]# netstat -an
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING

Test 2: Using NMAP scan the IDS to check for open ports. Try different types of scans by using different options to ensure the results are accurate.

```
[root@lab20 root]# nmap -sS -vv -n -p 1-65535 10.17.17.10
```

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at
2003-11-11 14:58 PST
Host 10.17.17.10 appears to be up ... good.
Initiating SYN Stealth Scan against 10.17.17.10 at 14:58
Adding open port 443/tcp
Adding open port 22/tcp
The SYN Stealth Scan took 3 seconds to scan 65535 ports.
Interesting ports on 10.17.17.10:
(The 65533 ports scanned but not shown below are in state:
closed)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp    open  https

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

```
[root@lab20 root]# nmap -sT -vv -n -p 1-65535 10.17.17.10
```

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at
2003-11-11 14:58 PST
Host 10.17.17.10 appears to be up ... good.
Initiating Connect() Scan against 10.17.17.10 at 14:58
Adding open port 22/tcp
Adding open port 443/tcp
The Connect() Scan took 3 seconds to scan 65535 ports.
Interesting ports on 10.17.17.10:
(The 65533 ports scanned but not shown below are in state:
closed)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp    open  https
```

Nmap run completed -- 1 IP address (1 host up) scanned in 3.468 seconds

```
[root@lab20 root]# nmap -sF -vv -n -p 1-65535 10.17.17.10
```

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at
2003-11-11 14:58 PST
Host 10.17.17.10 appears to be up ... good.
Initiating FIN scan against 10.17.17.10 at 14:59
The FIN Scan took 4 seconds to scan 65535 ports.
Adding open port 443/tcp
Adding open port 22/tcp
Interesting ports on 10.17.17.10:
(The 65533 ports scanned but not shown below are in state:
closed)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp    open  https

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

```
[root@lab20 root]# nmap -sX -vv -n -p 1-65535 10.17.17.10
```

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at
2003-11-11 14:59 PST
Host 10.17.17.10 appears to be up ... good.
Initiating XMAS scan against 10.17.17.10 at 14:59
The XMAS Scan took 4 seconds to scan 65535 ports.
Adding open port 22/tcp
Adding open port 443/tcp
Interesting ports on 10.17.17.10:
(The 65533 ports scanned but not shown below are in state:
closed)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp    open  https
```

Nmap run completed -- 1 IP address (1 host up) scanned in 4.936 second

3.1.6 Verify system security using a vulnerability scanner: Nessus

[Checklist Item 2.1.9](#) PASS

Objective: Check System Vulnerabilities using a vulnerability scanner. Verify that there are no medium or high severity vulnerabilities due to services that are necessary for sensor operation.

Test 1: Run a full Nessus scan with all plugins enabled. Run the scan from a host that does not have access to the IDS based on the ACL's on the system.

Network Vulnerability Assessment Report

10.11.2003

Sorted by host names

Session name: Cisco IDS	Start Time: 10.11.2003 15:17:11
	Finish Time: 10.11.2003 15:18:38
	Elapsed: 0 day(s) 00:01:27
Total records generated: 8 high severity: 0 low severity: 6 informational: 2	

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
10.17.17.10	0	6	2	Finished

10.17.17.10

Service	Severity	Description
https (443/tcp)	Info	Port is open
ssh (22/tcp)	Info	Port is open
General/tcp	Low	Remote OS guess : Linux Kernel 2.4.0 - 2.5.20 CVE : CAN-1999-0454
General/udp	Low	For your information, here is the traceroute to 10.17.17.10 : 10.17.16.4 10.17.40.15 10.17.17.10
general/icmp	Low	<p>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.</p> <p>This may help him to defeat all your time based authentication protocols.</p> <p>Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</p> <p>Risk factor : Low</p>

		CVE : CAN-1999-0524
General/tcp	Low	<p>The remote host does not discard TCP SYN packets which have the FIN flag set.</p> <p>Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.</p> <p>See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113</p> <p>Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487</p>
ssh (22/tcp)	Low	<p>An unknown service is running on this port. It is usually reserved for SSH</p>
https (443/tcp)	Low	<p>The service closed the connection after 0 seconds without sending any data It might be protected by some TCP wrapper</p>

3.1.7 Verify the IDS is running the latest version of the Cisco application

[Checklist Item 2.1.6](#) PASS

Objective: Ensure the CSIDS (Cisco Secure IDS) application is running the latest version.

Test 1: From a Cisco IOS prompt issue the show version command at check the version of the main application.

```

sensor# show version
Application Partition:

Cisco Systems Intrusion Detection Sensor, Version 4.1(2)S58

OS Version 2.4.18-5smpbigphys
Platform: IDS-4235
Sensor up-time is 4 min.
Using 314425344 out of 921522176 bytes of available memory
(34% usage)
Using 598M out of 15G bytes of available disk space (5%
usage)

```

MainApp	2003_Oct_10_11.16	(Release)	2003-
10-10T11:01:13-0500	Running		
AnalysisEngine	2003_Oct_10_11.16	(Release)	2003-
10-10T11:01:13-0500	Running		
Authentication	2003_Oct_10_11.16	(Release)	2003-
10-10T11:01:13-0500	Running		
Logger	2003_Oct_10_11.16	(Release)	2003-
10-10T11:01:13-0500	Running		
NetworkAccess	2003_Oct_10_11.16	(Release)	2003-
10-10T11:01:13-0500	Running		
TransactionSource	2003_Oct_10_11.16	(Release)	2003-
10-10T11:01:13-0500	Running		
WebServer	2003_Oct_10_11.16	(Release)	2003-
10-10T11:01:13-0500	Running		
CLI	2003_Oct_10_11.16	(Release)	2003-
10-10T11:01:13-0500			

Upgrade History:

```
* IDS-K9-min-4.1-1-S47          12:00:00 UTC Thu Jun 30
2005
  IDS-K9-sp-4.1-2-S58.rpm.pkg  05:41:09 UTC Wed Nov 12
2003
```

Recovery Partition Version 1.2 - 4.1(1)S47

3.1.8 Verify ACL's on the IDS

[Checklist Item 2.2.6](#) PASS

Objective: Ensure that only hosts that need access to the system are allowed to access the IDS.

Test 1: From a Cisco IOS prompt enter the following commands:

```
Sensor# configure terminal
sensor(config)# service host
sensor (config host)# network parameters
sensor (config host net)# show settings

ipAddress 10.1.1.151
netmask 255.255.248.0
defaultGateway 10.1.1.1
hostname sensor
accessList ipAddress 10.13.12.138 netmask 255.255.255.255
accessList ipAddress 10.13.17.227 netmask 255.255.255.255
accessList ipAddress 10.13.17.223 netmask 255.255.255.255
accessList ipAddress 10.13.18.9 netmask 255.255.255.255
accessList ipAddress 10.13.152.53 netmask 255.255.255.255
accessList ipAddress 10.13.13.21 netmask 255.255.255.255
accessList ipAddress 10.67226.0 netmask 255.255.255.0
accessList ipAddress 10.13.152.0 netmask 255.255.255.0
accessList ipAddress 10.25.9.0 netmask 255.255.255.0
accessList ipAddress 10.182.216.0 netmask 255.255.255.0
accessList ipAddress 10.14.184.0 netmask 255.255.255.0
```

```
accessList ipAddress 10.137.152.154 netmask 255.255.255.255
accessList ipAddress 10.82.8.174 netmask 255.255.255.255
accessList ipAddress 10.65.136.100 netmask 255.255.255.255
exit
```

Test 2: From a host not named in the access list table from test 1 try to ssh to the IDS and verify that the connection is denied.

```
[user@NotAllowed] ssh user@sensor
ssh: connect to host sensor port 22: Connection refused
```

Test 3: From a host that is named in the access list table from test 1 try to ssh to the IDS and verify that the connection is accepted.

```
[user@Allowed] ssh user@sensor
user@sensor's password:
```

3.1.9 Viewer accounts on the IDS have no shell access

[Checklist Item 2.2.9](#) PASS

Objective: Ensure All viewer accounts on the IDS are configured with no login.

Test 1: As root on the IDS system cat the password file and verify that all viewer accounts are configured for /sbin/nologin. This will not affect the ability to login via https and access the event viewer.

```
[root@sensor root] cat /etc/passwd

viewer:x:5004:5000::/home/viewer:/sbin/nologin
viewer1:x:5004:5000::/home/viewer1:/sbin/nologin
viewer2:x:5004:5000::/home/viewer2:/sbin/nologin
viewer3:x:5004:5000::/home/viewer3:/sbin/nologin
```

Test 2: As a user with view only privileges try to ssh to the IDS and see if the account is allowed to login.

```
[root@lab20 root] ssh viewer@sensor

viewer@sensor's password:
Permission denied, please try again.
```

3.1.10 Ensure auto update passwords are not stored in clear text

[Check List Item 2.2.10](#) FAIL

Objective: Ensure passwords for auto update are not stored in clear text on the system.

Test 1: As root on the IDS view the configuration file and look at the output:

```
[root@sensor root] cat /usr/cids/idsRoot/etc/curHostConfig.xml
```

```
~
~
<item type="OptionalAutoUpgrade" descr="Optional
AutoUpgrade configuration" required="false">
  <union name="optionalAutoUpgrade">
    <struct name="autoUpgradeParams">
      <union name="schedule">
        <struct name="calendarUpgrade">
          <array name="timesOfDay">
            <entry dontDelete="false">
              <var name="time"
protected="false">02:00:00</var>
            </entry>
          </array>
          <array name="daysOfWeek">
            <entry dontDelete="false">
              <var name="day"
protected="false">tue</var>
            </entry>
          </array>
        </struct>
      </union>
      <var name="ipAddress"
protected="false">10.137.17.227</var>
      <var name="directory"
protected="false">/home/service/cisco/ids/updates</va
r>
      <var name="username"
protected="false">service</var>
      <var name="password"
protected="false">pASswOrd</var>
      <var name="fileCopyProtocol"
protected="false">scp</var>
    </struct>
  </union>
</item>
~
~
```

Test 2: From a Cisco IOS Prompt run the show configuration command and look at the output:

```
sensor# configure terminal
sensor(config)# show configuration
```

```
~
~
optionalAutoUpgrade
active-selection autoUpgradeParams
autoUpgradeParams
schedule
active-selection calendarUpgrade
calendarUpgrade
timesOfDay time 02:00:00
daysOfWeek day tue
exit
exit
```



```
ipAddress 10.137.17.227
directory /home/service/cisco/ids/updates
username service
password pAsswOrd
FileCopyProtocol scp
~
~
```

Section 3.2 Residual Risk

In all aspects of information system technology there are risks that a system may be exposed. To determine if a particular risk is acceptable to a company they must rate the importance of the asset to its role in the business, and how if compromised the target asset could affect other assets of the company. As stated by SANS, “residual risk = exposure – controls.” The exposure is described as the result of a system being compromised, how detrimental is it to the business if the particular asset is exposed. The controls are steps that can be taken to try to prevent the system from being exposed but they will not eliminate all risk from the system. For example telnet is a very insecure protocol so as a control SSH should be used instead. Now by using SSH rather than telnet you avoid passing passwords in the clear as well as configuration commands, but you now may have a vulnerability related with SSH. This is an example of a control being used to mitigate a risk, but it does not remove all risks.

The importance to the business, the implementation of controls and the acceptance of the risks should be determined by the security policy of the company. Suggestions can be made as to which controls should be put into place and what risks are more severe as far as consequences and ease of exploitation, but the final decision needs to come from within the company. As an auditor understanding what an IDS is used for and general knowledge as to its role, I suggest that the IDS is an important device in the business infrastructure and should be considered a critical asset. The company in this particular case deems the IDS to be of high importance to the business.

Exposure can be explained as the consequences that are a result of the system being compromised. In this audit we are dealing with an IDS so we have to look at its role in the company. The IDS is used primarily to alert security analysts of possible malicious activity on the network that it is monitoring. The first consequence of the system being compromised is that the attacker could disable or shutdown the IDS application causing additional attacks to not be reported. This could result in attacks on other systems going unnoticed. Furthermore if an attacker gains access to the IDS they could gain access to other systems based on passwords that are stored in clear text as part of the IDS application. I am suggesting that there is a great deal of possible exposure if this asset were to become compromised, so necessary controls should be put into place to mitigate some of the risks.

Since the IDS that was audited passed all but 1 of the control objectives the residual risk is fairly low. The one objective that the audit found to be non compliant was that of

storing passwords in clear text on the IDS. The password that is stored is for an account on a remote server used for auto update. The account is used to SCP the update packages from the remote location. If proper precautions are used to secure the remote server such as locking down the privileges of the account and denying access to any directory other than the update directory, the risk is even less. There is no control other than disabling auto update that can be put in place to mitigate this risk. However in this case auto update is required by the company. I have discussed this further in the audit summary as far as actions that can be taken with the manufacturer to try to get this issue resolved from a product stand point.

Section 3.3 Is the System Auditable

While I was conducting the audit of the Cisco Secure IDS I found the system to be extremely easy to audit. I set forth several objectives that the audit was to encompass including the overall security of the operating system as well as the security of the Cisco application. Since the underlying operating system is Red Hat Linux it was fairly easy to develop audit objectives for this piece of the IDS appliance. I referred to pre existing auditing checklists for Linux and was able to come up with around ten checks that if passed ensure the security of the OS. These 10 controls were easy to audit by both checking configuration settings as well as using stimulus and response techniques.

The most difficult part of this audit was developing a list of controls to ensure the security of the Cisco IDS software. Since I was unable to find any relevant audit checklists I had to use personal knowledge of the Cisco IDS and of security practices in general to come up with controls which mitigated the risks of the application. Most of these controls were enabling or disabling configuration options. These controls were easy to audit using stimulus and response methods as well as checking configuration settings within the Cisco application.

Overall I found the Cisco Secure IDS can be audited. If appropriate consideration is given to the way the application is configured the audit becomes that much better. Again since the operating system is a standard Linux build it can and should be included in any audit of the Cisco IDS.

Section 4 Audit Report

4.1 Executive Summary

The auditing of the Cisco Secure IDS determined that the system is as secure as it can be while still maintaining its functionality. Overall the operating system security is up to standards set by experts in the information security field. As far as the Cisco application is concerned the configuration is secure based on the requirements set forth in the security policy.

All of the control objectives described have been checked and all were passed except for the storing of passwords in clear text. The audit covered aspects of operating system security such as the methods to access the server, IP addresses that were allowed to access the server, services that were running on the IDS, and the configuration of the intrusion detection software.

As far as system access the audit ensured that users were not allowed to telnet to the IDS due to security issues related to telnet. Rather than using telnet, a control was put in place that forced system access to be via SSH (Secure Shell). SSH is an encrypted protocol that allows users command line access and the ability to copy files from or to the system. Also checks were made as to the configuration of SSH such as verifying that the root user can not SSH directly to the system. The IP addresses that are allowed to access the system are only those of users who require access to the Cisco Event viewer, mainly security analysts and the administrators of the system. The user accounts all have the appropriate privileges set as described by the administrator. User privileges are an important aspect because it ensures that users do not change configurations that may disable the IDS entirely or cause an insecure configuration to be in use. The audit also covered the checking of services that are running on the IDS. Since it's a security device and is dedicated to analyzing network traffic and reporting events to the analysts, it's important that unnecessary services are not running that may make the system vulnerable to an attacker.

The only concern that I found with the Cisco application was that the password for the account used to copy the updates automatically from a remote server via SCP (secure copy protocol) is stored in clear text. This raises an issue of the server that is being used to store the updates and what other functions this server may have. Let's assume that this is a general purpose file server and not dedicated for the auto update process of several IDS'. The account used to SCP the updates has access to this system. It's important to look at the server and lock down the account so that if the password was discovered an attacker couldn't do further damage. This will be disused further in the background and risk section of this audit report.

Section 4.2 Audit Findings

After conducting the audit I found that the IDS passed all but one of the control objectives that were outlined in the audit checklist. To summarize the audit findings I will start with the checks concerning the operating system level and then summarize the IDS application checks.

Operating System Summary

The control objectives for the operating system included checks to ensure that the system is secure as far as user access, network access, checking for known vulnerabilities, and that the passive or sniffing interface is secure. To ensure that users access the system in a secure manner, [check 2.1.1](#) used Nmap, a network port scanner, to scan the system to

ensure that SSH is listening on port 22. The following output from Nmap shows that the system is listening on port 22 (SSH).

```
[root@lab20]# nmap -ss -vv -n -p 22 sensor

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at
2003-11-11 14:58 PST
Host 10.17.17.10 appears to be up ... good.
Initiating SYN Stealth Scan against 10.17.17.10 at 14:58
Adding open port 22/tcp
The SYN Stealth Scan took 1 seconds to scan 1 port.
Interesting ports on 10.17.17.10:
PORT      STATE SERVICE
22/tcp    open  ssh

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

From the output you can see that port 22 is reported as open and running SSH. Another important factor in determining the security of the IDS is to ensure that ARP is disabled on the sniffing interface. ARP is address resolution protocol and is used to resolve IP addresses to physical or layer 2 addresses. Since the Sniffing interface is configured with no IP address or passive, an attacker can not attack the system by targeting the IP address. Since the interface does have a physical address an attacker could send out a broadcast ARP request and the interface would see it on the network and may respond with its physical address. By ensuring that ARP is disabled it prevents this from happening. You can see from [check 2.1.5](#) results that ARP is disabled. The following output is from the ifconfig command which is used in Linux to show the settings of the selected interface. You can see that NOARP is present meaning that ARP is turned off on the interface.

```
eth0    Link encap:Ethernet HWaddr 00:03:47:90:99:67
        UP BROADCAST NOARP MULTICAST MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
        Interrupt:11 Base address:0xf000
```

Along with SSH running on the IDS we want to verify that the Web Server used to view events and configure the IDS is using HTTPS and listening on port 443. [Check 2.1.6](#) uses Nmap again to verify all open ports on the system. The following output is from Nmap using the -S option for a syn packet scan, -vv for very verbose, -n to not resolve names and -p to check ports 1-65536.

```
[root@lab20 root]# nmap -ss -vv -n -p 1-65535 10.17.17.10

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at
2003-11-11 14:58 PST
Host 10.17.17.10 appears to be up ... good.
Initiating SYN Stealth Scan against 10.17.17.10 at 14:58
Adding open port 443/tcp
Adding open port 22/tcp
The SYN Stealth Scan took 3 seconds to scan 65535 ports.
Interesting ports on 10.17.17.10:
```

(The 65533 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
22/tcp	open	ssh
443/tcp	open	https

Nmap run completed -- 1 IP address (1 host up) scanned in 3.461 seconds

You can see in bold that the IDS passed this control objective as the only open ports are 22, and 443. The final results for operating system security are those from [check 2.1.9](#). The control objective for this check is to ensure that there are no High or Medium severity vulnerabilities on the IDS. This is tested by using a network vulnerability scanner. For this audit I used Nessus. Nessus is available at www.nessus.org. The following report was generated by Nessus.

Network Vulnerability Assessment Report

10.11.2003

Sorted by host names

Session name: Cisco IDS	Start Time: 10.11.2003 15:17:11
	Finish Time: 10.11.2003 15:18:38
	Elapsed: 0 day(s) 00:01:27
Total records generated: 8	
high severity: 0	
low severity: 6	
informational: 2	

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
10.17.17.10	0	6	2	Finished

10.17.17.10

Service	Severity	Description
https (443/tcp)	Info	Port is open
ssh (22/tcp)	Info	Port is open
General/tcp	Low	Remote OS guess : Linux Kernel 2.4.0 - 2.5.20

		CVE : CAN-1999-0454
General/udp	Low	For your information, here is the traceroute to 10.17.17.10 : 10.1.16.4 10.17.40.15 10.17.17.10
General/icmp	Low	<p>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.</p> <p>This may help him to defeat all your time based authentication protocols.</p> <p>Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</p> <p>Risk factor : Low CVE : CAN-1999-0524</p>
general/tcp	Low	<p>The remote host does not discard TCP SYN packets which have the FIN flag set.</p> <p>Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.</p> <p>See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113</p> <p>Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487</p>
ssh (22/tcp)	Low	An unknown service is running on this port. It is usually reserved for SSH
https (443/tcp)	Low	<p>The service closed the connection after 0 seconds without sending any data</p> <p>It might be protected by some TCP wrapper</p>

Based on this report you can see that there are no High Severity warnings. The warnings that were found are Low severity and are allowed by the security policy. Most of these warnings are the result of no firewall between network segments. The ICMP warnings

and the general TCP warning regarding packets with the SYN and FIN flags are not really issues because the perimeter firewall will not allow this traffic. These results of these tests confirm that the Operating System is secure above and beyond the standards set forth in the company security policy.

Cisco IDS Application Security

After conducting the audit I found the Cisco IDS application to be secure for the most part. The application has different configuration options some of which, if enabled make the system less secure. The control objectives described in Section 2.2.0 are meant to ensure that the application is configured in the most secure way while still able to maintain functionality. The control objectives include version and signature release checks, ACLs (access control lists) being in use, user privileges, and Auto Update passwords.

The results of checks [2.2.1](#) and [2.2.2](#) show that the application and signature packs are running at the latest released version as of the date of the audit.

```
sensor# show version
Application Partition:

Cisco Systems Intrusion Detection Sensor, Version 4.1(2)S58

OS Version 2.4.18-5smpbigphys
Platform: IDS-4235
Sensor up-time is 4 min.
~
~
Upgrade History:

* IDS-K9-min-4.1-1-S47          12:00:00 UTC Thu Jun 30
2005
  IDS-K9-sp-4.1-2-S58.rpm.pkg  05:41:09 UTC Wed Nov 12
2003
```

The next important checks as far as overall application security verify that ACLs are in use to limit the IP addresses that are allowed to access the IDS. ACLs are used to restrict access to the system to addresses that are used to connect to the IDS Event Viewer or to administer the system. Check [2.2.6](#) looks at the configuration settings and ensures that specific addresses are stated and that there is not a blanket entry covering the 10.0.0.0 network. Test 2 in this check is to try to connect to the system from an address that is not allowed to connect as stated by the ACL table. The results show that the IDS passed all of these tests.

```
Sensor# configure terminal
sensor(config)# service host
sensor (config host)# network parameters
sensor (config host net)# show settings

ipAddress 10.1.1.151
netmask 255.255.248.0
```

```

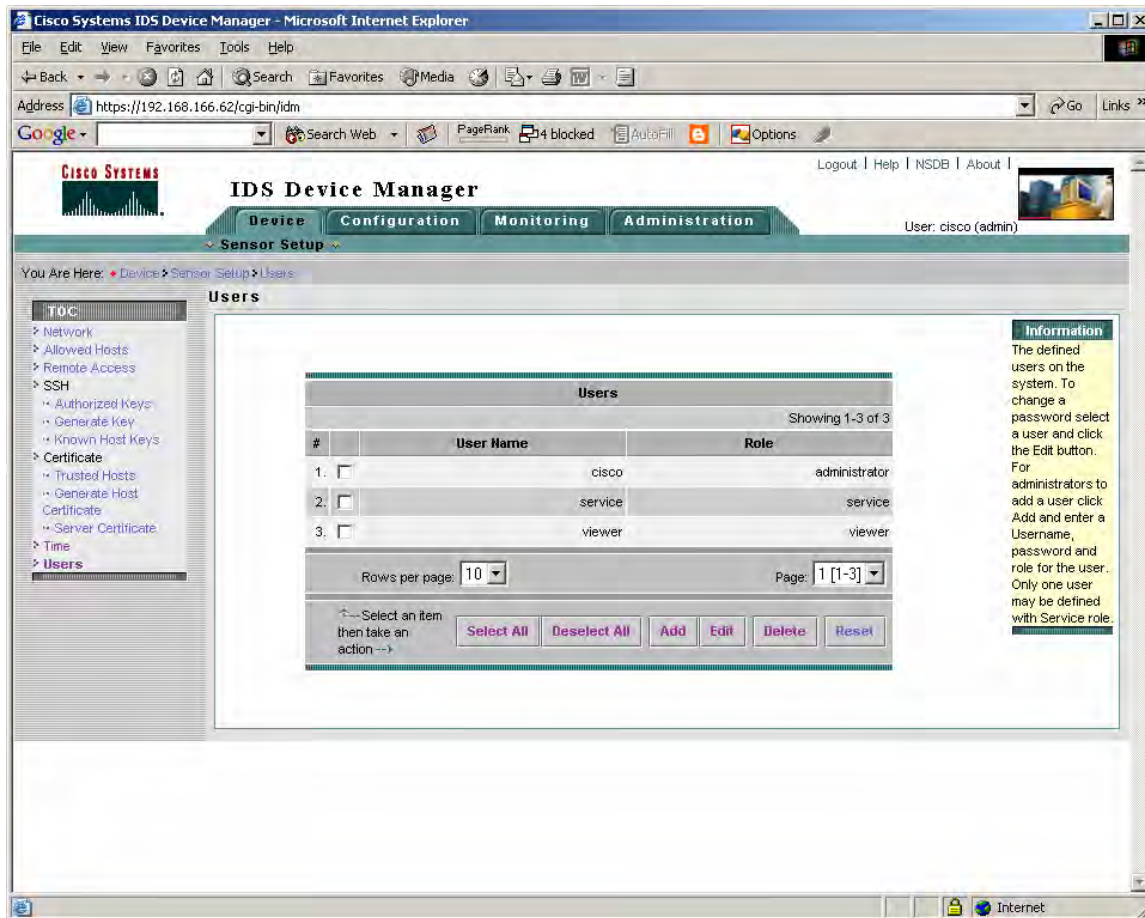
defaultGateway 10.1.1.1
hostname sensor
accessList ipAddress 10.13.12.138 netmask 255.255.255.255
accessList ipAddress 10.13.17.227 netmask 255.255.255.255
accessList ipAddress 10.13.17.223 netmask 255.255.255.255
accessList ipAddress 10.13.18.9 netmask 255.255.255.255
accessList ipAddress 10.13.152.53 netmask 255.255.255.255
accessList ipAddress 10.13.13.21 netmask 255.255.255.255
accessList ipAddress 10.67226.0 netmask 255.255.255.0
accessList ipAddress 10.13.152.0 netmask 255.255.255.0
accessList ipAddress 10.25.9.0 netmask 255.255.255.0
accessList ipAddress 10.182.216.0 netmask 255.255.255.0
accessList ipAddress 10.14.184.0 netmask 255.255.255.0
accessList ipAddress 10.137.152.154 netmask 255.255.255.255
accessList ipAddress 10.82.8.174 netmask 255.255.255.255
accessList ipAddress 10.65.136.100 netmask 255.255.255.255
exit

```

Test 2: From a host not named in the access list table from test 1 try to SSH to the IDS and verify that the connection is denied.

```
[user@NotAllowed] ssh user@sensor
ssh: connect to host sensor port 22: Connection refused
```

The IDS has the ability to define user privileges based on the user's role as it pertains to the IDS. The levels that can be assigned are viewer, which is used to view some configuration settings and view events. Service is used to make base operating system changes and when logging in as service you are not placed in a Cisco IOS shell, rather you get a bash prompt and can change to the systems root user. There is also an administrative account for application administration. Check [2.2.8](#) ensures that there is only 1 service and administrative account. All others should be at the viewer level. These results show that the IDS passed this control objective.



The final check that will be covered in this audit summary is check [2.2.10](#). The control objective here is to make sure that the password used to copy the update packages from a remote server is not stored in clear text. The IDS failed this test. The following two test results show that the password is stored in clear text in a configuration file and is also shown when the show configuration command is run.

```
[root@sensor root] cat /usr/cids/idsRoot/etc/curHostConfig.xml
```

```
<item type="OptionalAutoUpgrade" descr="Optional
AutoUpgrade configuration" required="false">
  <union name="optionalAutoUpgrade">
    <struct name="autoUpgradeParams">
      <union name="schedule">
        <struct name="calendarUpgrade">
          <array name="timesOfDay">
            <entry dontDelete="false">
              <var name="time"
protected="false">02:00:00</var>
            </entry>
          </array>
          <array name="daysOfWeek">
            <entry dontDelete="false">
```

```

        <var name="day" protected="false">tue</var>
      </entry>
    </array>
  </struct>
</union>
<var name="ipAddress"
protected="false">10.137.17.227</var>
<var name="directory"
protected="false">/home/service/cisco/ids/updates</var>
<var name="username" protected="false">service</var>
<var name="password" protected="false">pASswOrd</var>
<var name="fileCopyProtocol"
protected="false">scp</var>
~
~

```

Test 2: From a Cisco IOS Prompt run the show configuration command and look at the output:

```

sensor# configure terminal
sensor(config)# show configuration

```

```

~
~
optionalAutoUpgrade
active-selection autoUpgradeParams
autoUpgradeParams
schedule
active-selection calendarUpgrade
calendarUpgrade
timesOfDay time 02:00:00
daysOfWeek day tue
exit
exit
ipAddress 10.137.17.227
directory /home/service/cisco/ids/updates
username service
password pASswOrd
FileCopyProtocol scp
~
~

```

Section 4.3 Background / Risk

This section is used to describe the risks involved when a particular audit check is non compliant. During the course of this audit I found only one control objective that was not met. This was Checklist item [2.2.10](#). The control objective is to ensure that auto update passwords are not stored in clear text. First let me describe the auto update process as it relates to the Cisco IDS. Every time a bug is found in the IDS application or there is a new vulnerability released an application update or a signature pack update is released by Cisco. The system administrator will be notified via email of a new update. The administrator can then download the update from www.cisco.com/tac as a Linux package. If the administrator only has one IDS to update it is feasible to do the update manually from the Cisco IOS shell. In this case the Cisco sensors are deployed worldwide and it would take a considerable amount of time to update all of them and mistakes can be made.

Since we are dealing with a large deployment auto update is a requirement. The auto update package once downloaded by the administrator is placed on a remote server that is running SSH. There is a pre determined directory that the update will be copied into on the remote server and the IDS is configured to check in this directory for the update. If there is a newer update than the IDS is running it will SCP (Secure Copy) the update to the local system and run the update process automatically.

In order to SCP the package from the remote server the Cisco IDS application must have a valid username and password on the remote server. This is where we run into trouble. Rather than storing the password in an encrypted format, the username and password are both stored in clear text and also they are shown when the show configuration command is run. By it's self the auto update process is copying the files and accessing the remote server in a secure way since it's done via SSH, but it's the way that the username and password are stored by the application that creates the major concern. If an attacker were to breach the security of the IDS they could obtain the username and password allowing them access to the remote server. Depending on the privilege level of this user an attacker could use this account to gain access to sensitive configuration files on the server. Once the attacker gains access to the remote server he then has access to other servers that it may have shares on, or depending on other functions that the server may be used for the attacker could disable critical network services. They may be able to access user data and company information if this is a general purpose file server. The SCP server could also be used as a launch pad for other attacks since it may have access to different places on the network that the IDS does not.

Section 4.4 Audit Recommendations

Based on the audit findings the control objective that was not met was the storing of passwords in clear text. Although the username and password that are stored in clear text are not for the IDS its self, they are for a remote server that stores the auto updates. Based on this finding there are several recommendations that I as an auditor would like to see put in place to ensure a more secure setup.

- As a preventative control the account on the remote server should be locked down only allowing access to the directory that contains the specified updates. This ensures that if the account is compromised an attacker that tries to access the SCP server only has access to the upgrade directory.
- A ticket should be opened with Cisco's TAC (Technical Assistance Center) regarding the password and username being stored in clear text. The issue will most likely need to be dealt with by the sales representative who is responsible for the account. The TAC will say that it's not a bug but that's how it was designed and product requests need to be made to the account representative. I would recommend that no more Cisco IDS are purchased until this issue is resolved with a new release of the software.

- To further secure the auto update process I would suggest that the server used to store the update packages is a dedicated server and is not used for other network or business functions. This would help ensure that additional systems are not compromised and that user data is not accessed by a successful attack on the update server.
- As a corrective control, the system administrators of the IDS should be subscribed to Cisco's update notification service. Since the updates come out fairly frequently, it is important that they get copied to the update server as soon as they are available.
http://www.cisco.com/warp/public/779/largeent/it/ids_news/subscribe.html

Section 4.5 Costs

The costs in implementing the suggestions made in the previous section will not be substantial as the main objective will need to be delivered as an application update from Cisco. For the specific costs, each individual recommendation will be examined. The first suggestion of locking down the permissions of the account used to access the auto update server should take about 2 man hours at the most. I wouldn't think that anymore time would need to be spent and this should not be an ongoing process. I would allow one hour for research and one hour for implementation and testing.

Secondly making a request to the Cisco TAC or to the sales representative may take several man hours in dealing with the request being followed through with. Usually if the feature request is valid and the account is important to Cisco it shouldn't be a problem to get the problem fixed in the next release of the application. Once the new software is released it will require testing for compliance and this may take up to an hour.

The most costly suggestion that was made is to use a dedicated server to store the updates. This does not need to be a high end system and could be a desktop PC running Linux and Open SSH. Open SSH and Linux are free and a desktop PC can be purchased for under a thousand dollars. I would allow for 5 man hours to build and test the system.

The final suggestion is of no cost and requires little effort on the part of the administrator. With a valid TAC account, the administrator of the IDS system should to subscribe to the update notification service at the link provided. There is a form to fill out that should take no more than five minutes. This service will provide an email notification every time there is an update available.

Section 4.6 Compensating Controls

Since most of the recommendations made were of little cost to the company I don't see why they wouldn't be implemented. If for some reason the resources are not available then I can make a few recommendations that could be used until the resources become available. Compensating controls can be put in place or may already be in place to help

lessen the risks that are present on the IDS. First off if an attacker cannot gain access to the IDS then they will not be able to view the username and password that's stored in clear text. As far as controls to prevent an attacker gaining access to the IDS there are several in place such as the use of SSH rather than telnet and the use of HTTPS versus HTTP. Another control that is already in place is accounts that don't need shell access to the system, accounts other than cisco and service, be configured with no login in the /etc/passwd file.

Additionally if a dedicated server can't be provided for the update process I would recommend that critical network services if run on that system be moved to a less exposed system and that the server is monitored with a host based IDS. I would further suggest that the host IDS have a rule that alerted administrators if there was a login by the update account other then at the times scheduled for updates. I would also consider running a file integrity checker such as tripwire on the update server. This would help ensure the overall security of the update process and the integrity of the server being used to store the updates.

Finally I can't stress enough the importance of contacting Cisco and explaining the disregard for security standards by storing a password in clear text. The system is called the Cisco "Secure" IDS and as a security device the highest attention to little details should be paid.

Conclusion

After conducting the Audit of the Cisco Secure IDS, I would have to say that the overall security of the system is up to standards. Except for the control objective that was not in compliance, the system passed nineteen of twenty checks and the system meets all the requirements of a production IDS. If the recommendations that were made in the previous section are put into place it will definitely strengthen the overall security of the IDS and finally I would like to see a request made to Cisco to fix the outstanding issue regarding the clear text passwords. All things considered this is a reasonably secure system and I believe that it is auditable by following the steps I have outlined in this report.

References

- Nmap Online documentation.
http://www.insecure.org/nmap/nmap_documentation.html
- Nessus Online documentation.
<http://www.nessus.org/documentation.html>
- Naidu, Krishini. "Auditing Linux" .
<http://www.sans.org/score/checklists/Auditing Linux.doc>
- Zimmerman, Brent. "Auditing a Snort Intrusion Detection System: An Auditors Perspective"
http://www.giac.org/practical/GSNA/Brent_Zimmerman_GSNA.pdf
- Cisco Online Documentation for the Cisco Secure IDS
<http://www.cisco.com/tac>
- Cisco Product Documentation CD for the Cisco Secure IDS
- "Linux Security Quick Reference Guide"
<http://www.linuxsecurity.com/docs/QuickRefCard.pdf>
- Northcutt, Stephen. "Network Intrusion Detection: An Analysts Handbook"
New Riders Publishing, 1999.

© SANS Institute 2003. All rights reserved. Author retains full rights.