GIAC
CERTIFICATIONS

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 permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at http://www.giac.org/registration/gsna

Using RAT (Router Audit Tool) from CIS (Center for Internet Security) to Perform a Security Audit of the Configuration File of a Cisco Router at the Level-1 Benchmark

Auditing Networks, Perimeters, and Systems
GSNA Practical Assignment
Version 3.2 (July 1, 2004)
Option 1

Author: Robert BECK
Date: 10 February 2005

© SANS Institute 2005, Author retains full rights.

Summary

This report was written to satisfy the practical assignment portion of SANS Institute's GIAC Systems and Network Auditor (GSNA) certification program. This assignment demonstrated my ability to perform a technical audit and basic risk analysis of a CISCO router. The audit was scoped to match the assessment limitations of the Router Audit Tool (RAT) from the Center for Internet Security (CIS)..

Part one of this report contains a risk assessment of a CISCO router. It describes the role of the router that was audited. This risk assessment evaluated the threats to routers. It also determined the vulnerabilities that might allow those threats to cause harm. In addition, the assets that would be adversely by an exploit to the router were examined. A list of references is given at the end of part one. These references are recommendations of up-to-date reading material on both secure configurations and auditing techniques for Cisco routers.

Part two of this report contains the instructions that an auditor would follow to perform their own audit of a Cisco router. All of the checklist items require that the auditor first run RAT on the router's configuration file, and then examine the output for exceptions. With that in mind, part two begins with a description of how to install and run RAT from a Windows PC. Since RAT is not capable of testing for all of the vulnerabilities listed in part one, part two of the report shows where the scope of the audit was adjusted to match RAT's capabilities.

Part three of this report contains the actual testing of the Cisco router. It shows the steps that were followed to run RAT, as well as the ten most important exceptions. Screenshots of the testing are included, as well as descriptions of the checklist items that are associated with the exceptions.

Part four contains an Executive Summary, as well as further details concerning the ten findings, offering recommendations that would decrease the router's vulnerability to threats.

© SANS Institute 2005, Author retains full rights.

Table of Contents

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

1. Research in Audit, Measurement Practice, and Control

Objective

The overall objective of this audit is to use the Router Audit Tool (RAT) from the Center for Internet Security (CIS) to perform a security audit of the CISCO router in the test network. In order to consider this audit a success, three objectives must be met:

1. Determine what a secure configuration of a router is,
2. Scope the audit to fit RAT's ability to test whether the router meets that configuration, and
3. Use RAT to determine whether the router is securely configured.

1.a. Identify the System to be audited

1.a.1. Description of the Cisco Router being audited

The router is of the Cisco 2600 series. Its model number is 2651, and the operating system is called the Internetworking Operating System (IOS), version 12.2 (5d). The major release is 12.0 and the maintenance version is 5d. This router has six Ethernet connections. The router has a module installed, model "ETHERNET 4E", containing four of the Ethernet connections. The router itself contains the other two Ethernet connections.

1.a.2. Role of this Cisco Router

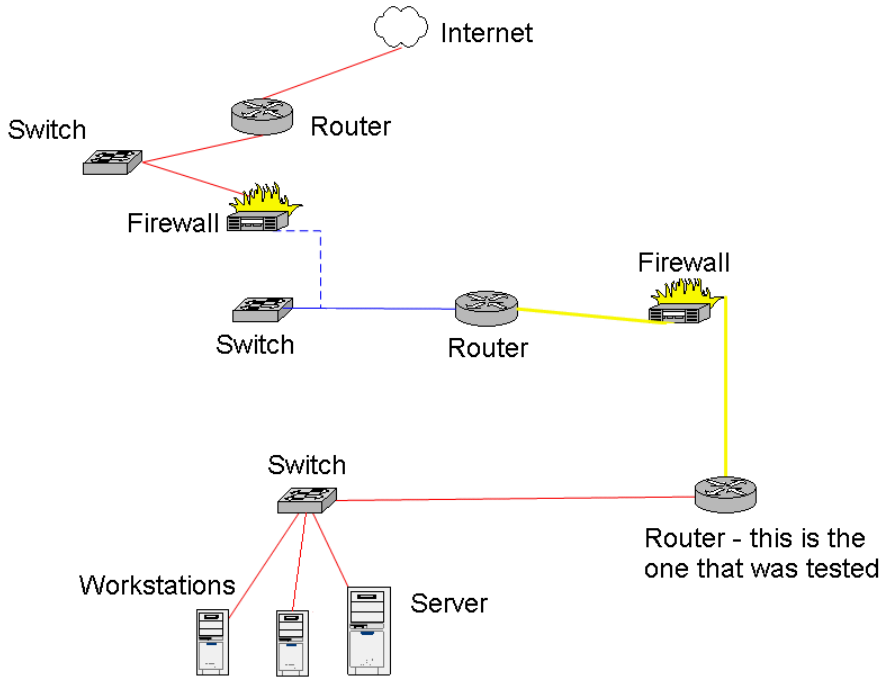
This router is being used in a test network for both:

1. Testing configurations before installing them on the production network and
2. Training network administrators about security (running scans, etc.).

The test network that contains this router is not connected to the production network. It is not connected to a secured or trusted network. The router that was tested goes between a switch for an internal network and a firewall. It connects the network used in the test network to other network devices, and ultimately, the Internet. The types and roles of the other network devices

© SANS Institute 2005, Author retains full rights.

change as required by the testing and training for which they are being used. The following shows a representative diagram of the test network that was obtained from the network administrator:



The above network can be configured however desired by the network's administrators. The above configuration is the one that was in place at the time of the testing. The network administrator showed how they could connect the routers to the firewalls through either one of the following two methods: 1. The router connects to the firewall through a switch, or 2. The router connects to the firewall through a Crossover Cable. He said that the Crossover cable connects the receive line to the transmit leave on each device, allowing them to be connected directly together without going through a switch. Using a switch instead of a crossover cable allows the testers to connect packet sniffers between routers and firewalls.

1.a.3. How would other models, etc. be audited differently than this one?

External routers are under greater threat due to their proximity to the Internet,

© SANS Institute 2005

Author retains full rights.

which increases the likelihood of their being seen. In addition, if this router was located in a more sensitive location, then the cost of cleaning up after a successful hack would likely be greater due to the importance of the assets that would be affected.

Items that increase the importance of the router:
The router acts as a Gateway that connects your network to the Internet,
The router is part of a firewall,
The router performs packet filtering. (Akin page 5)

Items that increase Assets/Costs:
The router is connected to a trusted or secure network. (Akin page 5)

Routers other that those made by Cisco, could not be audited by the RAT program. During a webcast, George Jones said that his RAT program would not work on any systems other than those made by Cisco (Jones). It would appear that the general ideas behind the audit would apply to any router, though. Sometimes other devices can act as routers, such as Linux machines, or a firewall or similar device. Obviously, the RAT program would not work on these.

1.b. RISK. Evaluate the most significant Risks to the System

According to Akin, a simple risk analysis formula would be the following:

Risk = vulnerability x threat x cost

Where:

- **Vulnerability** is the likeliness that an attack will succeed,
- **Threat** is the likelihood of an attack, and
- **Cost** is the how much the threat would cost if it succeeded. (Akin page 4)

For example, if you lived in a house without protection from burglars (such as a house with poor locks and no alarm system), then your house has a vulnerability to burglars. The level of threat, though, determines the amount of risk you are taking. Just because you live in a vulnerable house does not mean you are at a high risk of being burglarized. Those of you who lived in an area whose demographics showed a high level of crime would have a high threat of your home being burglarized, and therefore your vulnerable home has a great deal of risk. If your home is in a low crime area, though, your home may have the same

© SANS Institute 2005 Author retains full rights.

level of vulnerability, but have a lower risk since your threat of burglary is much lower.

Looking at our router is a similar fashion; we could say that if our network contained a router that was not protected against hackers (such as being poorly configured), then we could say that this modem has a vulnerability to hackers. If other routers throughout your network are configured in a similar way, then they would have pretty much the same vulnerabilities, therefore the level of risk for each router would be determined by it's threats. This shows that having a vulnerable router does not necessarily mean that the level of risk is high. A router located in the exterior part of the network has a higher threat of it being hacked; therefore, its level of risk is higher. A router located internally has less chance of being hacked by an outsider, and has a lower level of risk. In addition, the level of threat increases when the cost of the assets increases. A router located in a sensitive network protects assets of greater value than those in a test network, and therefore have a greater level of risk.

1.b.1. THREAT. Describe at least two threats and their capacity to inflict damage

Types of Threats	Description of the Threat
Physical Threats	Fire, floods, water damage, earthquakes, weather-related, landslides, avalanches, electrical spikes, lightning.
Human Threats	Vandalism, thievery, hacking, cracking, criminal activity, terrorism, espionage, employee discontentment, employee incompetence.

EVALUATING THE DAMAGE THAT CAN OCCUR IF THE ABOVE THREATS ARE INFLICTED ON ROUTERS	
Damage that can be inflicted by a Threat	**Cost**
DAMAGE INFLICTED BY BOTH PHYSICAL AND HUMAN THREATS	
Both can destroy the router therefore disabling the network.	Loss of Sensitive Data and Reputation. Loss of training facilities. Network could become unavailable for a long time and be difficult to fix. (Akin page 3)
DAMAGE INFLICTED SPECIFICALLY BY HUMAN THREATS	

© SANS Institute 2005

Author retains full rights.

Routers are taken over and then used to attack systems on the internal network. (Akin page 3) Intruders could: Bypass intrusion detection systems, Gain access to sensitive networks, Confuse efforts to monitor or log the attackers actions, Obtain information for future attacks, and Disable the network	Loss of Sensitive Data and Reputation.
Routers are taken over and then used to attack external sites. (Akin page 4)	Extremely difficult and costly to investigate who is performing the attack. Loss of reputation.
Rerouting Attack (also known as Route Injection Attack) Packets entering and leaving the network are rerouted to an unauthorized location In effect, hackers take full control of all the data that enters and leaves your network. (Akin page 4) (NSA page 29)	Sensitive data becomes available to criminals. Loss of reputation.
Session Replay Attack Attackers record web sessions, and replay them, maybe with some changes. This causes unexpected actions to occur, or unauthorized access for the attacker. (NSA page 29)	Sensitive data becomes available to criminals. Loss of reputation.
Masquerading IP addressed on packets are changed. Allows attacker to place their data into the network, or to gain access to your network. (NSA page 29)	Sensitive data becomes available to criminals. Loss of reputation.
Denial of Service (DoS) So much traffic is sent to a site that it overloads and becomes inoperable. (NSA page 29)	Network becomes unavailable. Loss of reputation.

1.b.2. ASSET. Describe the major information asset that is directly affected by the role of this Router

Losses due to compromise are most important when they affect 1. Sensitive Data and 2. Reputation. These are the most important assets of most networks. Systems can generally be restored rather quickly, resources are usually readily available, but your sensitive data, and your reputation, once lost are much, much harder to recover.

The major information asset that is affected in this instance is the test network. Its loss would not, one would think, result in the loss of any sensitive data. Nor would it greatly affect the entities reputation. Overall, the testing lab may seem like an insignificant resource, although it could possibly serve as a tool for helping an intruder to attack the production network. Often, test networks are overlooked when it comes to security. The test network might contain sensitive information (such as administrative passwords) that if made available to intruders, could possibly be used to facilitate an attack on the production network. Therefore, policy must require adequate protection for the test network.

1.b.3. VULNERABILITY. Describe the major vulnerabilities of the Cisco Router

MAJOR Vulnerabilities	**Degree of Exposure in the event of successful exploitation**	**Potential impact on the organization in the event of successful exploitation**
V1 - Vulnerabilities in the Cisco router operating system (IOS)		

© SANS Institute 2005, Author retains full rights.

V1a - Vulnerabilities in the Cisco router operating system (IOS) (Akin chapter 2) See Cisco's website for list of latest IOS vulnerabilities: <http://www.cisco.com/go/psirt> In addition the ICAT Metabase lists up-to-date IOS vulnerabilities: <http://icat.nist.gov/icat.cfm> The X-Force Home Page at Internet Security Systems also allows you to search for up-to-date vulnerabilities: <http://xforce.iss.net/> The SecurityFocus website lists vulnerabilities also: <http://www.securityfocus.com/> The Common Vulnerabilities and Exposures (CVE) Website lists all IT related vulnerabilities and assigns each on a standardized name: <http://cve.mitre.org/>.	Denial of Service attacks can disable Routers. Information concerning the router available to unauthorized individuals. The router's configuration is changed. (Akin page 6)	Loss of reputation. Loss of sensitive data. Loss of training facilities. Network could become unavailable for a long time and be difficult to fix. Intruder gains access to the test network. (Akin page 3) Intruders could: • Bypass intrusion detection systems, • Gain access to sensitive networks, and • Mess up efforts to monitor or log the attackers actions.
V2 – Authenticating Users and Restricting Access		
V2a – Lack of Accountability for Router Users. (Jones page 9)	Unable to determine who made changes to the router's configuration.	Removes accountability.

V2b – Passwords are not being used to control access to the Console port, Auxiliary port (AUX) and Virtual TTY (VTY). (Jones page 5) (Akin page 13)	No passwords are necessary. The Router can be administered by anyone with access to the router.	Loss of reputation. Intruders could gain access to sensitive networks.
V2c – Access Control Lists are not being used to control access to the router through the VTY lines. (Jones page 11) (Akin page 25)	Reduced security of VTY access. Anyone can attempt to connect to the router through the Internet.	Loss of reputation. Intruders could gain access to sensitive networks.
V2d – Router is not being timed-out when inactive. (Jones page 15) (Akin page 26)	Easier to access router through Internet through VTY.	Loss of reputation. Intruders could gain access to sensitive networks.
V3 - Password Security		
V3a – Weak Password Encryption. MD5 encryption is not being used. (Jones page 8) (Akin page 34)	Router can be administered by anyone who can read the packets going to the router and run a password cracking software	Loss of reputation. Intruders could gain access to sensitive networks.
V3b - Passwords are being sent in clear test for: telnet, SNMP, http and in configurations. (Jones page 6) (Akin page 35)	Router can be administered by anyone who can read the packets going to the router.	Loss of reputation. Intruders could gain access to sensitive networks.
V3c - Passwords are easy to guess. (Jones page 7) (Akin page 35)	Router can be administered by anyone with access to the router.	Loss of reputation. Intruders could gain access to sensitive networks.
V3d - Router Configuration Files are not being stored in a secure fashion. (Jones page 17) (Akin pages 36 and 37)	Attacker could read the IOS configuration of the network and get sensitive information such as: passwords, SNMP community strings, shared secrets, shared addresses, shared net blocks	Loss of reputation. Intruders could gain access to sensitive networks.

© SANS Institute 2005

Author retains full rights.

V3e – Uploads of router configuration files and images are not done using SCP or SSH. (Jones page 18) (Akin pages 36 and 37)	Attacker could read the IOS configuration of the network and get sensitive information such as: passwords, SNMP community strings, shared secrets, shared addresses, shared net blocks	Loss of reputation. Intruders could gain access to sensitive networks.
V4 - AAA Security (authentication, authorization, accounting)		
V4a – The AAA Security method is not being used. (AAA = authentication, authorization, and accounting) (Jones page 9) (Akin page 43)	Reduced accountability of users.	Unauthorized use of the router.
V5 - Warning Banners		
V5a – The Warning Banners do not provide legal protection. (Akin pages 52 and 53)	Intruder is not warned about monitoring or recording of system use.	Makes it more difficult to investigate incidents.
V5b – The Warning Banners contain system information. (Akin pages 52 and 53)	Warning banner leaks information that is useful to intruders	Intruders could gain access to sensitive networks.
V6 - Unnecessary Protocols and Services		
V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol. (Jones page 10) (Akin chapter 7)	Unnecessary services can allow intruders to: determine user names, disable or crash devices, create DoS attacks, etc.	Intruders could gain access to sensitive networks. Network could become unavailable.
V6b - ICMP-Directed Broadcasts are enabled. (Jones page 12) (Akin page 60)	Routers are taken over and then used to attack external sites. Smurf attack.	Extremely difficult and costly to investigate who is performing the attack.
V7 - SNMP Security		

V7a - SNMP Security is enabled. (Akin chapter 8)	Attackers use SNMP to map out your network, find out MACs and IP address binding, and determine hardware and software on the network.	Intruders could gain access to sensitive networks.
V8 - Routing Protocol		
V8a - Routing Protocol is enabled. (Akin chapter 9, page 83)	Attacker can insert false routing information into the router causing DoS. In addition, attacker could relay your traffic through another system and bypass your firewall and intrusion detection system.	Denial of Service. Intruders could gain access to sensitive networks.
V9 - Anti-spoofing filters		
V9a - Anti-spoofing filters are not enabled. (Akin chapter 9, page 83)	External users are not prevented from sending forged packets that look as though they came from your internal network, therefore bypassing security controls that allow or deny access based on a packet's source IP address.	Intruders could gain access to sensitive networks.
V10 - NTP Security (Network Time Protocol)		
V10a - NTP (Network Time Protocol) Security is not being used to synchronize time between routers. (Akin chapter 10, page 96)	Removes ability to accurately correlate information between devices. Removes ability to compare logs between routers and servers.	Make it more difficult to develop a reliable picture of an incident and use it to prosecute an intruder.
V11 - Inadequate Logging		
V11a – Inadequate Logging (Jones page 13) (Akin chapter 11)	No advance warning that outages are about to occur. No warning that an intruder is analyzing your network for vulnerabilities. No audit trail for determining what went wrong or what an intruder did to your network.	Difficult to prosecute attackers. Loss of reputation.

V12 - Physical Security		
V12a – Inadequate Physical Security. (Akin Appendix B, page 133)	Attackers can disable, reconfigure, replace and steal systems.	Loss of hardware. Loss of reputation. Loss of sensitive information.
V13 - Incidence Response		
V13a – Poor Incidence Response capability. (Akin Appendix C)	Since intruders are not detected, they are not blocked and can continue attacking.	Difficult to prosecute attackers. Loss of reputation.

1.c. The Current State of Practice

1.c.1. Resources containing Secure Configurations

List of Resources Containing Secure Configurations for Cisco Routers	Explain Why This Resource is Important
Akin, Thomas. Hardening Cisco Routers. Sebastopol CA: O'Reilly Media, Inc., 2002.	Purchased used through Amazon. Best book that was found for this project. Focuses on securing Cisco routers. Has checklists. Gives threats and vulnerabilities. Most pages contain examples of secure configurations for Cisco routers. Each of these configurations is explained, as well as associated with an item on a security checklist.
CIS - Center for Internet Security. Gold Standard Benchmark for Cisco IOS, Level 1 and 2 Benchmarks, Version 2.1. 2003. <http://www.cisecurity.org/bench_cisco.html>.	Benchmark for securing Cisco routers. RAT is based on these benchmarks. This audit used them to develop the Checklist Items in Part 2, and in Part 4 to provide recommendations. This document was used to provide Checklist Compliance material for Part 2 and Recommendations for router commands in Part 4 of this audit.

© SANS Institute 2005

Author retains full rights.

Cisco Systems, Inc. Improving Security on Cisco Routers. 12 Oct 2004 <http://www.cisco.com/warp/public/707/21.pdf >	Interactive guide to securing Cisco Routers.
Cisco Systems, Inc. Cisco IOS Interface Configuration Guide, Release 12.2. 2001. <http://www.cisco.com/application/pdf/en/us/guest/products/ps4032/c2001/ccmigration_09186a008011dfec.pdf>	Guide from Cisco. This resource is what router administrators use to learn how to configure their routers. It is freely available through the Internet. This audit used the CIS for determining checklist items.
Cisco Systems, Inc. Cisco ISP Essentials, Essential IOS Features Every ISP Should Consider, Lessons from people who have been operating backbones since the early days of the Net, Version 2.9. 5 June 2001 <http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip>	Contains 182 pages. Pages 49 through 96 deal with Securing Routers.
Cisco Systems, Inc., Cisco Security Advisories and Notices Web Page. 2005. <http://www.cisco.com/en/US/products/products_security_advisories_listing.html>	Up to date listing of vulnerabilities of all Cisco products. For routers would be used to search for IOS vulnerabilities.
Cobb, Chey. Network Security for Dummies. New York: Wiley Publishing, Inc., 2003.	Chapter 3 gives an overview of performing a risk assessment, listing various threats along with their associated vulnerabilities. This chapter also has helpful discussions on how to determine likelihood and cost of threats. The book says very little concerning vulnerabilities of routers. Page 120 mentions that router operating systems often have security problems, therefore check for security patches from the manufacturer, it also says to watch out for default password values that have not been changed.
Common Vulnerabilities and Exposures (CVE) Homepage. 2005. The MITRE Corporation. 20 January 2005 <http://cve.mitre.org/>.	They maintain a list of vulnerabilities. Each vulnerability is assigned a unique standardized name. This way, when a specific vulnerability is being addressed by a number of different parties, they can be certain that they are all talking about the same one.

Eder, John. Router Security. 2005. Information Systems Audit and Control Association. Orange County Chapter. PowerPoint presentation located at <http://www.isaca-oc.org/Archives/Router%20Security.ppt>	Instructs the auditor to be aware of False Positives when running RAT.
Gentry, Josh. Cisco Router Configuration Tutorial, 1999, <http://www.swcp.com/~jgentry/topo/cisco.htm>	Read this to get an overview on how to configure a Cisco Router. Quite short, but a good place to start for the inexperienced.
Huegen, Craig. The Latest in Denial of Service Attacks: "Smurfing" Description and Information to Minimize Effects. 2000. <http://www.pentics.net/denial-of-service/white-papers/smurf.cgi>	Information on how to protect your Cisco router from smurf and fraggle DoS attacks.
Internet Security Services advICE website. 2005. Internet Security Services. <http://www.iss.net/security_center/advice/Services/Routing/Cisco/default.htm>	Contains a section they call advICE, which includes information on hardening Cisco routers. ISS's advICE section is a database of information security and anti-hacker information. It has a section on Setting up secure services, and within that section is a section on Routing.
Internet Security Systems X-Force Home Page. 2005. Internet Security Systems. <http://xforce.iss.net/>	Their front page, under X-FORCE SECURITY ALERTS, had a link to "Multiple Vulnerabilities in Cisco IOS", January 27, 2005. IOS version 12.2 is affected by this vulnerability. This vulnerability could cause a denial of service attacks. This is the first place I learned about this vulnerability (SANS NewsBites Vol.7 Num.5 February 2, 2005 was the second)
McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed, Fourth Edition. Berkeley: McGraw-Hill/Osborne, 2003.	Gives what they call Countermeasures against Attacks. Some of the Countermeasures they give contain configuration changes for securing Cisco routers.
ICAT Metabase Home Page. 2005. Computer Security Division. National Institute for Standards and Technology. 12 September 2003 <http://icat.nist.gov/icat.cfm>.	A CVE Vulnerability search engine. Easy to use. Listed one vulnerability for Cisco IOS version 12.2.

SANS NewsBites Vol. 7 Num. 5. SANS Institute, 2005.	Showed the latest IOS vulnerabilities that can be used to perform denial-of-service attacks.
SecurityFocus Home Page. 2005. SecurityFocus. <http://www.securityfocus.com/>	Their vulnerability database listed the latest Cisco IOS vulnerabilities. Vulnerabilities can be searched: vendor, title, keyword, bugtraq id, or date.
Tripod, Mark. Cisco Router Configuration & Troubleshooting, Second Edition. Indianapolis: New Riders, 2000.	Purchased used through Amazon. Gives overall information on using Cisco routers. Contains a configuration file, but does not explain how it works. Recommends that you consult Cisco for explanation of the commands.
United States. National Security Agency. Router Security Configuration Guide, Version 1.1b. 2003. <http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/routers/cis_securityguides.zip>	Very thorough, but not much fun to read. Basis for the CIS benchmarks and RAT's testing.
Velte, Toby J. and Anthony T. Velte. Cisco, A Beginner's Guide, Second Edition. Berkeley: Osborne/McGraw-Hill, 2001.	Purchased used through Amazon. Good for familiarizing yourself with a wide variety of Cisco networking products.

1.c.2. Resources containing Auditing Methods

List of Resources Containing Methods for Auditing Cisco Routers	Explain Why This Resource is Important
Akin, Thomas. Hardening Cisco Routers. Sebastopol CA: O'Reilly Media, Inc., 2002.	This book provided an excellent resource for obtaining secure router configurations. Appendix A tells how to use checklists as a basis for auditing the security of routers.
Jones, George. SANS Institute presents: Improving Router Security with RAT: The Top 10 List. SANS Wednesday Webcast, 5 November 2003. <https://www.sans.org/webcasts/show.php?webcastid=90421>	Excellent overall discussion of the RAT Router Audit Tool. Gave list of Top 10 vulnerabilities. In addition, the audio helped explain the impact on an organization if these vulnerabilities are exploited.

McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed, Network Security Secrets & Solutions, Fourth Edition. Berkeley: McGraw Hill/Osborne, 2003.	Discussed denial of service attacks, encryption, passwords, and spoofing. Also problems caused by enabling Finger.
SANS Institute. Track 7 – Auditing Networks, Perimeters & Systems. Volume 7.1. 2004.	Discusses threats and baselines.
SANS Institute. Track 7 – Auditing Networks, Perimeters & Systems. Volume 7.2. 2004.	Part 4 discusses securing routers.
SANS Institute. Track 7 – Auditing Networks, Perimeters & Systems. Hands-On Exercises. SANS Press. 2004.	Section 1 covers using RAT to audit routers.
Stewart, Brian. Router Audit Tool: Securing Cisco Routers Made Easy! SANS Institute 2002. <http://www.sans.org/rr/whitepapers/networkdevs/238.php>	This paper is somewhat out of date and although it is good for giving you background information on RAT, its information on configuring RAT does not cover the latest versions of RAT.
United States. Government Accounting Office. Accounting and Information Management Division. Federal Information Systems Controls Audit Manual. 1999. <http://www.gao.gov/special.pubs/ai12.19.6.pdf>	Contains methods for auditing security controls of information systems. Becoming somewhat dated, but still widely used, it tends to concentrate on the world of mainframes, and does not work as well with networks.
United States. National Institute of Standards and Technology. Risk Management Guide for Information Technology Systems, Special Publication 800-30. 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>	Used to determine types of threats. Readable. Teaches you tons about Risk Management. You should read this document before beginning a security audit to know what is meant by threat, vulnerability, likelihood, cost and risk.
United States. National Security Agency. Router Security Configuration Guide, Version 1.1b. 2003. <http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/routers/cis_securityguides.zip>	Chapter 6, Testing and Security Validation contained auditing methods.

2. Create an Audit Checklist

Through the development of the checklist, this audit determined that the following vulnerabilities can be tested by RAT: V2, V2a, V2c, V2d, V3a, V3b, V3c, V3e, V4a, V6a, V6b, V7a, and V10a, and V11a. The other vulnerabilities are considered to be outside of the scope of this audit and will therefore not be given a checklist item since they cannot be tested by a Level One RAT router security assessment.

2.1. Guide to Using RAT to Perform Your Audit

This audit concentrates on using RAT to perform a security audit on a Cisco router. RAT will inspect the router configuration file, looking for default material and configuration issues. All of the checklist items listed below require the auditor to first run RAT.

2.1.1. Obtain the RAT program

First obtain the RAT program from the website for the Center for Internet Security (CIS). Their homepage is located at <http://www.cisecurity.org>. It lists all of the different types of Benchmarks and Security Tools that CIS has available for downloading. In order to obtain the RAT software, look under the heading “Network Device” and click on the line beginning “Cisco IOS Router”. This will take you to their “Benchmarks/Tools” webpage. You will have to answer a few questions about your affiliation. Select the download for the Benchmark Package titled “Cisco IOS Router/PIX (Level-1/Level-2)” and click on the Select button at the bottom of the page. On the next page, click on Download the Windows Cisco Router Tools Installer. Save the file to a folder of your choice, the default should work fine for you (the default is C:\CIS\RAT). Since this is a DOS program, try to avoid using spaces or special characters in the folder’s name. You might also want to download some of the Benchmark documents for your reference. For RAT version 2.2 the name of the downloaded file is RAT_2.2.win32-native-installer.exe, later versions might have a different filename.

2.1.2. Install the RAT program on your PC

The RAT program is easy to install. All you have to do is:

1. To run the Windows Cisco Router Tools Installer, use Windows Explorer to go to the folder that you downloaded and double-clicked on “RAT_2.2.win32-native-

© SANS Institute 2005 Author retains full rights.

installer.exe". This will run the InstallShield Wizard, which will copy all the files you need to run RAT onto your hard drive. The wizard will ask you to choose the Destination Folder. Use the name that you chose above. When asked for the Setup Type, choose Basic. When the wizard asks you if you are Ready to Install RAT files, if everything looks OK, click the Install button. Then follow the rest of the wizard's instructions to exit the installer. RAT is now installed on your PC.

2.1.3. Configure RAT to test your router configuration file

This is where you are going to have to interview the router administrators in order to determine how their router is configured. You might want to have them there by your side as you run the configuration program to localize RAT to match the router that you are auditing. It is easy to run the configuration program through Windows by going to the Start menu and choosing Programs and CIS, then running "Shell for Rat". This will take you right to the correct DOS directory for running the RAT program. Type bin\ncat_config and hit the enter key to run the RAT configuration program. You will be asked many questions (about 31) concerning how the router is configured. You can get by just hitting return for them all and taking the defaults (or hit an exclamation mark "!" and return to take the defaults for all of them), but the test would not then be customized for your router. This might be OK for the audit if you realize that the results might not always apply to the router that you are auditing.

2.1.4. Run RAT

Although RAT is touted as a program for Windows, it's only *sort of* a Windows program, because you actually run it from the DOS command prompt. The directory that your are in when you run RAT will also be the same directory that RAT will write its reports to. Therefore, it is recommended that you copy your router configuration file to a directory such as "C:\cis\rat\reports" and then run RAT from that same directory. The following example of how to run RAT assumes that your router configuration file is named router and exists in the folder named "c:\cis\rat\reports":

1. Go to the command prompt:
    a. With version 2.2P of RAT you can go right to the correct dos directory from Windows by going to Start > Programs > CIS > RAT > Shell for RAT and then go to the subdirectory containing your router configuration file (in this example the command to go to the correct subdirectory would be cd reports),

© SANS Institute 2005

Author retains full rights.

   b. Otherwise go to the command prompt however you are accustomed to and go to the directory “c:\cis\rat\reports” by typing in a command such as cd\cis\rat\reports;
2. Add c:\cis\rat to your path statement through a DOS command such as “path c:\cis\rat\reports; %path%”
3. Type in “rat reports”.

RAT now runs its reports on the router configuration file and places its results in the subdirectory (or you can call it folder) of “c:\cis\rat\reports”. This audit will use the report named all.hmtl to obtain the results for the testing.

Note: There is a SANS White Paper about using RAT (Stewart), but it’s somewhat out of date and although it is good for giving you background information on RAT, its information on configuring RAT does not cover the latest versions of RAT.

2.2. Audit Checklist

2.2.1. Description of the Layout for Checklist Items

Checklist subtitle	Description
Checklist Item #	Numbered from 1 to 50
Checklist Item Title	Short description of the test.
Reference	Books, websites, PDF files, etc. that were used to come up with this test.
RISK, Importance of this item:	Ranked from Low to High based on the 1-10 scale as assigned by the CIS consensus process. (CIS OIS Benchmark page iv). This checklist associates the numbers from 1 to 3 as Low, 5 as Medium, and from 7 to 10 as High.
RISK, Vulnerabilities being checked	Based on the Table of Vulnerabilities in Part 1.
RISK, Assets affected by a successful exploit.	Assets affected by a successful exploit.

© SANS Institute 2005 Author retains full rights.

RISK, Likelihood that a threat could exploit the vulnerabilities: Does the threat source have the capability to take advantage of the vulnerability? How capable is the threat source of exploiting the vulnerability?	Likelihood = how likely it is for a threat source is to have the motivation, resources and capability to take advantage of a vulnerability. (NIST 800-30 page14)
Testing Procedure / Compliance Criteria:	All of the tests listed are based on RAT. The RAT output will show whether this particular test failed or failed.
Test Nature	Objective or Subjective.
Evidence	From Part 3.
Findings	From Part 3.

2.2.2. Authenticating Users and Restricting Access

Checklist Item #1	**Checklist Item Title:** Protocols other than Telnet can be used to access the router.
Reference: (CIS 3.1.17, CIS 3.2.9) Action 3.1.17 and Supporting Documentation 3.2.9 from Center for Internet Security. Gold Standard Benchmark for Cisco IOS, Level 1 and 2 Benchmarks, Version 2.1. 2003. <http://www.cisecurity.org/bench_cisco.html>. (NSA pages 64 and 214) from United States. National Security Agency. Router Security Configuration Guide, Version 1.1b. 2003. <SNAC.Guides@nsa.gov>. (Akin pages 22 to 24) from Akin, Thomas. Hardening Cisco Routers. Sebastopol CA: O'Reilly Media, Inc., 2002.	
RISK	
Importance of this item: Medium. Checks to make sure that Telnet is the only protocol that can be used to access the router through VTY. Want to keep protocols other than Telnet, such as rlogin or through the web, from accessing the router through VTY. Since Telnet sends passwords in the clear (non-encrypted), try to use SSH if the router supports it.	**Vulnerabilities checked:** V2 – Basic Access Control

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Medium. Although Web access would make it easier to access the router, unless the router is not protected by access controls, it would still be difficult to connect to.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions given at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "IOS – VTY transport telnet". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: "transport input telnet" (CIS 3.2.9)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Medium level of Importance.	

2.2.3. Shared Accounts

Checklist Item #2	**Checklist Item Title:** Check that local authentication being used to provide accountability. NOTE: This test is also reflected under V4a – The AAA Security method is not being used. (AAA = authentication, authorization, and accounting), Checklist Item #14
References: (CIS 3.1.3, 3.2.1) (Jones page 9) from Jones, George. SANS Institute presents: Improving Router Security with RAT: The Top 10 List. SANS Wednesday Webcast, 2003. (Akin page 44, Chapter 5)	
RISK	
Importance of this item: High. The router has not been changed from its default value, it is not configured to require authentication of users. Router administrator needs to establish a new authorization model that requires local login.	**Vulnerabilities checked:** V2a – Lack of Accountability for Router Users.

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Without accountability, there is nothing to prevent disgruntled employees from attacking the router without being accountable for their actions.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "IOS – Use local authentication". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: aaa new-model aaa authentication login $(AAA_LIST_NAME) local aaa authentication enable \S+ (CIS 3.2.1)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: Local user authentication is being not used. Due to its High level of Importance, this exception will be added to the report as a Finding.	

Checklist Item #3	**Checklist Item Title:** Check that local users have been defined.
Reference: (CIS 3.1.4, 3.2.2) (Jones page 9) (Akin page 15)	
RISK	
Importance of this item: High. Users are not given names. They just login with a common password, without being asked who they are. Therefore, there is no accountability as to who has made changes to the router's configuration.	**Vulnerabilities checked:** V2a – Lack of Accountability for Router Users.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Internal threat. Disgruntled employee could make changes to router configurations without accountability.

Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "IOS – Create local users". Look under the column Pass/Fail to determine if your router configuration file failed this test.
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: username \S+ password \d \S+ (CIS 3.2.2)
Test Nature: Objective
Evidence: The Router Audit Tool report showed FAIL for this test.
Findings: User authentication is not required. Due to its High level of Importance, this exception will be added to the report as a Finding.

2.2.4. Missing Passwords

Checklist Item #4	**Checklist Item Title:** Check that passwords are required in order to access the router through the Console, Auxiliary port, or Virtual TTY.
Reference: (CIS 3.1.24, 3.2.14) (NSA page 58) (Jones page 5) (Akin page13)	
RISK	
Importance of this item: High. Make sure that a password is required to access the router is case other stronger access controls are not configured correctly.	**Vulnerabilities checked:** V2b – Passwords are not being used to control access to the Console port, Auxiliary port (AUX) and Virtual TTY (VTY).
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities**: High. Lack of passwords makes it easy to access the router.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "IOS – require line passwords". Look under the column Pass/Fail to determine if your router configuration file failed this test.	

Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: password [^\n\s]+ (CIS 3.2.14)
Test Nature: Objective or Subjective? Objective
Evidence: The Router Audit Tool report showed FAIL for this test.
Findings: Passwords are not required to access the router. Due to its High level of Importance, this exception will be added to the report as a Finding.

2.2.5. Missing or Bad VTY (Virtual Teletype) ACLs (access control lists)

Checklist Item #5	**Checklist Item Title:** Check that Access Control Lists (ACLs) are applied.
Reference: (CIS 3.1.28, 3.2.18) (NSA page 64) (Akin page 25)	
RISK	
Importance of this item: High. Access to the VTY port is not limited to specific IP addresses, therefore anyone from anywhere on the Internet can keep guessing passwords to your router until they find the right one.	**Vulnerabilities checked:** V2c – Access Control Lists are not being used to control access to the router through the VTY lines.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Attackers can try to access the router from anywhere on the Internet.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "apply VTY ACL". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: access-class $(VTY_ACL_NUMBER) in (CIS 3.2.18)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	

Findings: Access Control Lists have not been applied to the VTY lines. Due to its High level of Importance, this exception will be added to the report as a Finding.

Checklist Item # 6	**Checklist Item Title:** Check that Access Control Lists have been defined for the VTY lines.
Reference: (CIS 3.1.30, 3.2.19) (NSA page 64)	
RISK	
Importance of this item: High. This allows you to control access to your router by creating access control lists containing the IP addresses of who is allowing to login.	**Vulnerabilities checked:** V2c – Access Control Lists are not being used to control access to the router through the VTY lines.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Hackers can enter router from any IP address on the Internet
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "Define VTY ACL". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: access-list $(VTY ACL NUMBER) permit tcp $(VTY ACL BLOCK WITH MASK) any access-list $(VTY ACL NUMBER) permit tcp host $(VTY ACL HOST) any access-list $(VTY ACL NUMBER) deny ip any any log (CIS 3.2.19)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: Access Control Lists have not been defined for the VTY lines. Due to its High level of Importance, this exception will be added to the report as a Finding.	

2.2.6. Inactive Sessions

Checklist Item # 7	**Checklist Item Title:** Check that inactive router sessions are being timed out.

Reference: (CIS 3.1.18, 3.2.10) (NSA page 58)	
RISK	
Importance of this item: High. Want to make sure that inactive router sessions are timed out after 10 minutes or so (to match local policies and needs). This prevents an intruder from administering the router if an administrator walks away from the router's terminal screen and forgets to log off.	**Vulnerabilities checked:** V2d – Router is not being timed-out when inactive.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. If the administrator walks leaves their workstation without logging off the router, anyone with physical access to the administrator's terminal can enter commands to modify the configuration of the router.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "exec-timeout". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: No benchmark given by CIS	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed pass for this test.	
Findings: None.	

Checklist Item # 8	**Checklist Item Title:** Check that the tcp keepalive service is disabled.
Reference: (CIS 3.1.69, 3.2.45)	
RISK	
Importance of this item: Medium. TCP connections that are not in use should not be kept alive because they could be taken over by intruders and used to attack the router.	**Vulnerabilities checked:** V2d – Router is not being timed-out when inactive.

© SANS Institute 2005

Author retains full rights.

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Medium. Intruder could take over the TCP connection.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "tcp keepalive service". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ^service tcp-keepalives-in (CIS 3.2.45)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Medium level of Importance.	

2.2.7. Weak Password Encryption

Checklist Item # 9	**Checklist Item Title:** Check that MD5 encryption is used to encrypt the privilege-level password.
Reference: (CIS 3.1.25, 3.2.15) (NSA page 61) (Akin pages 34 and 35)	
RISK	
Importance of this item: High. Weak password encryption ciphers are easy to crack. MD5 encryption is a strong form of encryption.	**Vulnerabilities checked:** V3a – Weak Password Encryption. MD5 encryption is not being used.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Wide-availability of password crackers and motivation to obtain privileged access to the router increases likelihood of exploitation.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "enable secret". Look under the column Pass/Fail to determine if your router configuration file failed this test.	

© SANS Institute 2005

Author retains full rights.

Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: enable secret \d \S+ (CIS 3.2.15)
Test Nature: Objective
Evidence: The Router Audit Tool report showed pass for this item.
Findings: None.

2.2.8. Clear text passwords

Checklist Item # 10	**Checklist Item Title:** Check that the privileged password in the router configuration file is not stored in readable text
Reference: (CIS 3.1.39, 3.2.25) (NSA page 62) (Akin page 34)	
RISK	
Importance of this item: High. This requires passwords to be encrypted in the configuration file to prevent unauthorized users from learning the passwords by reading the configuration.	**Vulnerabilities checked:** V3b - Passwords are being sent in clear test for: telnet, SNMP, http and in configurations.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Anyone able to read the router configuration can read the privileged password. Promise of having privileged access increases the intruder's motivation.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "encrypt passwords". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ^service password-encryption (CIS 3.2.25)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: Due to its High level of Importance, this exception will be added to the report as a Finding.	

© SANS Institute 2005

Author retains full rights.

2.2.9. Poor Passwords

Checklist Item #11	**Checklist Item Title:** Check that poor quality line passwords are not being used.
Reference: (CIS 3.1.26, 3.2.16) (NSA page 62) (Akin pages 34 and 35)	
RISK	
Importance of this item: Medium. The router configuration file should use complex passwords that are difficult to guess.	**Vulnerabilities checked:** V3c - Passwords are easy to guess.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Medium. Although the passwords are not complex, the attacker has to spend time trying different passwords using brute force.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "line password quality". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: password 7 \S+ (CIS 3.2.16)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Medium level of Importance.	

Checklist Item # 12	**Checklist Item Title:** Check that poor quality user passwords are not being used.
Reference: (CIS 3.1.27, 3.2.17) (NSA page 62) (Akin page 33)	
RISK	

© SANS Institute 2005

Author retains full rights.

Importance of this item: Medium. Should use complex passwords that are difficult to guess.	**Vulnerabilities checked:** V3c - Passwords are easy to guess.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Medium. Although the passwords are not complex, the attacker has to spend time trying different passwords using brute force.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "user password quality". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: user.*password 7 \S+ (CIS 3.2.17)	
Test Nature: Objective	
Evidence: The Router Audit Tool report did not perform this test for this particular configuration.	
F**indings:** None.	

2.2.10. Password Security - Insecure Uploads

Checklist Item # 13	**Checklist Item Title:** Check that the loading of router configuration files from remote locations has been disabled.
Reference: (CIS 3.1.68 and 3.2.44) (NSA page 73)	
RISK	
Importance of this item: High. Allows loading of the router configuration file from a remote location, therefore placing sensitive information about your network to pass though the Internet unencrypted. CIS 3.2.44 says that an "… attacker could read the IOS configuration of the network and get sensitive information such as: passwords, SNMP community strings, shared secrets, shared addresses, shared net blocks"	**Vulnerabilities checked:** V3e – Uploads of router configuration files and images are not done using SCP or SSH.

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Anyone monitoring Internet traffic to the router could read the sensitive information contained in the router's configuration file and use it in an attack against the network.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no service config". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: service config (CIS 3.2.44)	
Test Nature: Objective or Subjective? Objective	
Evidence: The Router Audit Tool report showed pass for this item.	
Findings: None.	

2.2.11. Authentication, Authorization, Accounting - AAA Security

Checklist Item #14	**Checklist Item Title:** Check that local authentication is being used to provide accountability. NOTE: This test is also reflected under V2a – Lack of Accountability for Router Users, Checklist Item #2
Reference: (CIS 3.1.3, 3.2.1) (Jones page 9) (Akin page 44)	
RISK	
Importance of this item: High. As it comes out of the box, the Cisco router operating system is not configured to require authentication of users. Router administrator needs to establish a new authorization model that requires local login	**Vulnerabilities checked:** V4a – The AAA Security method is not being used. (AAA = authentication, authorization, and accounting)
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Without accountability, there is nothing to prevent disgruntled employees from attacking the router without being accountable for their actions.

Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "IOS – Use local authentication". Look under the column Pass/Fail to determine if your router configuration file failed this test.
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: aaa new-model aaa authentication login $(AAA_LIST_NAME) local AAA authentication enable \S+ (CIS 3.2.1)
Test Nature: Objective
Evidence: The Router Audit Tool report showed FAIL for this test.
Findings: Local user authentication is being not used. Due to its High level of Importance, this exception will be added to the report as a Finding.

Checklist Item # 15	**Checklist Item Title:** Check that a valid ID and password is not required for login.
Reference: (CIS 3.1.21, 3.2.12) (NSA page 58 and 68)	
RISK	
Importance of this item: High. Checks to see if the router has been changed from the default AAA security setup that requires users to login with a valid ID and password.	**Vulnerabilities checked:** V4a – The AAA Security method is not being used. (AAA = authentication, authorization, and accounting).
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Very tempting for an intruder when they are allowing to login to a router without using an ID or password
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "login default". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: login [^\n\s]+ (CIS 3.2.12)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed pass for this test.	

Findings: None.

Checklist Item # 16	**Checklist Item Title:** Check that access through VTY lines is controlled by an AAA authentication list.
Reference: CIS 3.1.22, 3.2.13 NSA page 58 and NSA page 168	
RISK	
Importance of this item: High. Access to the VTY lines should be limited to the users specified in an AAA authorization list.	**Vulnerabilities checked:** V4a – The AAA Security method is not being used. (AAA = authentication, authorization, and accounting).
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. This vulnerability simplifies intruder's access to the router through a VTY line.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "login named list". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: Confirm use of Least Privilege. RAT checks the Router Configuration File for a rule that matches the following Benchmark: login authentication $(AAA LIST NAME)	
Test Nature: Objective	
Evidence: The Router Audit Tool report did not perform this test for this particular configuration.	
Findings: None.	

2.2.12. Unnecessary Protocols and Services – Such as small services

Checklist Item #17	**Checklist Item Title:** Check that access to the router through a modem connected to an unused AUX port is prevented.
Reference: (CIS 3.1.20, 3.2.11) (NSA page 58) (Akin page 23)	

RISK	
Importance of this item: Low. Keeping an unused AUX port open and connected to a modem allows access to the router from a phone line.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Low. There would have to be a modem connected to the router. In addition, the intruder would also have to determine the router's phone number.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "IOS – disable aux". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: no exec$ (CIS 3.2.11)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Low level of Importance.	

Checklist Item # 18	**Checklist Item Title:** Check that the finger service has been disabled. (IOS version 11)
Reference: (CIS 3.1.34, 3.2.20) (NSA page 71)	
RISK	
Importance of this item: Medium. Disable finger service if not needed to both: 1. Keep hackers from learning about your network, and 2. Help prevent Denial of Service attacks.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Intruders often look for services (such as finger) to exploit when attacking routers.

© SANS Institute 2005

Author retains full rights.

Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no finger service". Look under the column Pass/Fail to determine if your router configuration file failed this test.
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: no (service|ip) finger (CIS 3.2.20)
Test Nature: Objective
Evidence: The Router Audit Tool report does not perform this test for this version of the IOS.
Findings: None.

Checklist Item # 19	**Checklist Item Title:** Check that the identd service has been disabled (Version 11 of the IOS only).
Reference: (CIS 3.1.35, 3.2.21)	
RISK	
Importance of this item: High. Services that are not needed should be turned off because they present potential avenues of attack and may provide information that could be useful for gaining unauthorized access.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. An intruder could use information gained through the identd service to help plan an attack.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no identd service". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ip identd (CIS 3.2.21)	
Test Nature: Objective	
Evidence: The Router Audit Tool report did not perform this test for this particular configuration.	

Findings: None.

Checklist Item # 20	**Checklist Item Title:** Check that the finger service has been disabled. (IOS version 12.1, 2, 3 only)
Reference: (CIS 3.1.36, 3.2.22) (NSA page 71)	
RISK	
Importance of this item: Medium. Disable finger service if not needed to both: 1. Keep hackers from learning about your network, and 2. Help prevent Denial of Service attacks.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Intruders often look for services (such as finger) to exploit when attacking routers.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no finger service". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ^ip finger (CIS 3.2.22)	
Test Nature: Objective or Subjective? Objective	
Evidence: The Router Audit Tool report showed pass for this test.	
Findings: None.	

Checklist Item # 21	**Checklist Item Title:** Check that the finger service has been disabled. (IOS version 12.0 only)
Reference: (CIS 3.1.37, 3.2.23) (NSA page 71) (Pages 78 and 89 from McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed, Network Security Secrets & Solutions, Fourth Edition. Berkeley: McGraw Hill/Osborne, 2003.)	
RISK	

Importance of this item: Medium. Disable finger service if not needed to both: 1. Keep hackers from learning about your network, and 2. Help prevent Denial of Service attacks.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Intruders often look for services (such as finger) to exploit when attacking routers.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no finger service". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ^This will always fail (CIS 3.2.23)	
Test Nature: Objective	
Evidence: The Router Audit Tool report did not perform this test for this particular configuration.	
Findings: None.	

Checklist Item # 22	**Checklist Item Title**: Check that the http server has been disabled.
Reference: (CIS 3.1.38, 3.2.24) (NSA page 72)	
RISK	
Importance of this item: High. Although http allows remoter management of the router, it should be turned off because it sends passwords in the clear.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. There is a high temptation for intruder to read clear text passwords going over the Internet and use them to attack the router.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no ip http server". Look under the column Pass/Fail to determine if your router configuration file failed this test.	

Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ^ip http server (CIS 3.2.24)
Test Nature: Objective
Evidence: The Router Audit Tool report showed pass for this test.
Findings: None.

Checklist Item # 23	**Checklist Item Title:** Check that the TCP small services have been disabled. (IOS version 11 only)
Reference: (CIS 3.1.62, 3.2.38) (NSA page 71) (Akin page 64)	
RISK	
Importance of this item: High. Unused services should be disabled to prevent them from being used by intruders to gather information about the router and attack the network. For example, the echo service has been used in denial of service attacks.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Intruders often exploit small-unprotected services.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no tcp-small-servers". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: no service tcp-small-servers (CIS 3.2.38)	
Test Nature: Objective or Subjective? Objective	
Evidence: The Router Audit Tool report does not perform this test for this version of the IOS.	
Findings: None.	

Checklist Item # 24	**Checklist Item Title:** Check that the UDP small services have been disabled. (IOS version 11 only)
Reference: (CIS 3.1.63, 3.2.39) (NSA page 71)	
RISK	
Importance of this item: High. Unused services should be disabled to prevent them from being used by intruders to gather information about the router and attack the network. For example, the echo service has been used in denial of service attacks.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Intruders often exploit small-unprotected services.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no udp-small-servers". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: no service udp-small-servers (CIS 3.2.29)	
Test Nature: Objective or Subjective? Objective	
Evidence: The Router Audit Tool report does not perform this test for this version of the IOS.	
Findings: None.	

Checklist Item # 25	**Checklist Item Title:** Check that the TCP small services have been disabled. (IOS version 12 only)
Reference: (CIS 3.1.64, 3.2.40) (NSA page 71)	
RISK	

Importance of this item: High. Unused services should be disabled to prevent them from being used by intruders to gather information about the router and attack the network. For example, the echo service has been used in denial of service attacks.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Intruders often exploit small-unprotected services.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no tcp-small-servers". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ^service tcp-small-servers (CIS 3.2.40)	
Test Nature: Objective or Subjective? Objective	
Evidence: The Router Audit Tool report showed pass for this test.	
Findings: None.	

Checklist Item # 26	**Checklist Item Title:** Check that the UDP small services have been disabled. (IOS version 12 only)
Reference: (CIS 3.1.65, 3.2.41) (NSA page 71)	
RISK	
Importance of this item: High. Unused services should be disabled to prevent them from being used by intruders to gather information about the router and attack the network. For example, the echo service has been used in denial of service attacks.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Intruders often exploit small-unprotected services.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no udp-small-servers". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ˆservice udp-small-servers (CIS 3.2.41)	
Test Nature: Objective or Subjective? Objective	
Evidence: The Router Audit Tool report showed pass for this test.	
Findings: None.	

Checklist Item # 27	**Checklist Item Title:** Check that the ip bootp server has been disabled.
Reference: (CIS 3.1.66, 3.2.42) (NSA page 73)	
RISK	
Importance of this item: Medium. Minor services such as ip bootp should be turned-off, if not used, to prevent possible exploitation through information gathering and denial-of-service attacks.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. **I**ntruders often look for minor services to exploit when attacking routers.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no ip bootp server". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ˆno ip bootp server (CIS 3.1.66, 3.2.42)	

Test Nature: Objective or Subjective? Objective
Evidence: The Router Audit Tool report showed pass for this test.
Findings: None.

Checklist Item # 28	**Checklist Item Title:** Check that the Cisco Discovery Protocol has been disabled.
Reference: (CIS 3.1.67, 3.2.43) (NSA page 71) (Akin page 65)	
RISK	
Importance of this item: High. Attackers could draw a diagram of your network from all the information given by CDP. In addition, there are known denial of service attacks that exploit this protocol.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Attackers often exploit small services such as CDP.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no cdp run". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: no cdp run (CIS 3.2.43)	
Test Nature: Objective or Subjective? Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: The Cisco Discovery Protocol (CDP) is not disabled. Due to its High level of Importance, this exception will be added to the report as a Finding.	

Checklist Item # 29	**Checklist Item Title:** Check that the tftp-server has been disabled.

Reference: (CIS 3.1.70, 3.2.46) (Akin page 19)	
RISK	
Importance of this item: High. Attackers can use tftp to download the router's configuration file.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Simplified access to router configuration file increases motivation for this vulnerability to be exploited by an attacker.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no tftp-server". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: tftp-server (CIS 3.2.46)	
Test Nature: Objective	
Evidence: The Router Audit Tool report did not perform this test for this particular configuration.	
Findings: None.	

Checklist Item # 30	**Checklist Item Title**: Check that IP Source Routing has been disabled.
Reference: (CIS 3.1.75, 3.2.49) (NSA page 74) (Akin page 63)	
RISK	
Importance of this item: High. Attackers exploit IP Source Routing to bypass firewalls and intrusion detection systems.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Many well-known exploits take advantage of IP Source Routing.

Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no ip source-route". Look under the column Pass/Fail to determine if your router configuration file failed this test.
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: no ip source-route (CIS 3.2.49)
Test Nature: Objective
Evidence: The Router Audit Tool report showed pass for this test.
Findings: None.

2.2.13. ICMP-Directed Broadcasts are enabled

Checklist Item # 31	**Checklist Item Title:** Check that ICMP-directed broadcasts are disabled (IOS Version 11 only)
Reference: (CIS 3.1.73, 3.2.47) (NSA page 75) (Akins page 60) (Huegen, Craig. The Latest in Denial of Service Attacks: "Smurfing" Description and Information to Minimize Effects, 2000. http://www.pentics.net/denial-of-service/white-papers/smurf.cgi)	
RISK	
Importance of this item: High. Attackers use ICMP-directed broadcasts for smurf attacks.	**Vulnerabilities checked:** V6b - ICMP-Directed Broadcasts are enabled.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Smurf attacks using ICMP-directed broadcasts are well known.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no directed broadcast". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: no ip directed-broadcast (CIS 3.2.47)	
Test Nature: Objective	

Evidence: The Router Audit Tool report does not perform this test for this version of the IOS.
Findings: None.

Checklist Item # 32	**Checklist Item Title:** Check that ICMP-directed broadcasts are disabled (IOS Version 12 only)
Reference: (CIS 3.1.74, 3.2.48) (NSA page 75) (Akins page 60) (Huegen)	
RISK	
Importance of this item: High. Attackers use ICMP-directed broadcasts for smurf attacks.	**Vulnerabilities checked:** V6b - ICMP-Directed Broadcasts are enabled.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Smurf attacks using ICMP-directed broadcasts are well known.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no directed broadcast". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ˆ ip directed-broadcast (CIS 3.2.48)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed pass for this test.	
Findings: None.	

2.2.14. SNMP Security

Checklist Item # 33	**Checklist Item Title:** Check that SNMP is disabled.
Reference: (CIS 3.1.7, 3.2.3) (NSA page 76) (Akin page 68. Also chapter 8, SNMP Security.)	
RISK	

Importance of this item: High. Intruders can use SNMP to learn about your network layout, hardware, and software. They can use this information to find and attack vulnerable systems on your network.	**Vulnerabilities checked:** V7a - SNMP Security is enabled.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. It would be highly tempting for an attacker can use the information gathered through SNMP to find out which hardware or software on your network has vulnerabilities that they can easily exploit.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no snmp-server". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ˆsnmp-server (CIS 3.2.3)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: SNMP is enabled. Due to its High level of Importance, this exception will be added to the report as the finding.	

Checklist Item #34	**Checklist Item Title:** Check that SNMP read-write is disabled.
Reference: (CIS 3.1.8, 3.2.4) (NSA page 138) (Akin page 73)	
RISK	
Importance of this item: High. Allows SNMP to be managed remotely. Intruder can completely take over the router through the Internet.	**Vulnerabilities checked:** V7a - SNMP Security is enabled.

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. This vulnerability allows remote management of SNMP, which hackers could be tempted to take advantage of.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "forbid SNMP read-write". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: snmp-server community.*RW (CIS 3.2.4)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: Due to its High level of Importance, this exception will be added to the report as a Finding.	

Checklist Item # 35	**Checklist Item Title:** Check if "public" is used as the SNMP community string for read-only access.
Reference: (CIS 3.1.9, 3.2.5) (NSA page 138) (Akin page 71)	
RISK	
Importance of this item: High. Public is the default community string for SNMP read-only access. Many hackers know about it. They can use it to find out how your router and network is configured.	**Vulnerabilities checked:** V7a - SNMP Security is enabled.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Access to SNMP through the default community string is a popular exploit.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "forbid SNMP community public". Look under the column Pass/Fail to determine if your router configuration file failed this test.	

Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: snmp-server community public (CIS 3.2.5)
Test Nature: Objective
Evidence: The Router Audit Tool report showed FAIL for this test.
Findings: The SNMP read-only community string has not been changed from its default value. Due to its High level of Importance, this exception will be added to the report as a Finding.

Checklist Item # 36	**Checklist Item Title:** Check if "private" is used as the SNMP community string for read/write access.
Reference: (CIS 3.1.10, 3.2.6) (NSA page 138) (Akin page 71)	
RISK	
Importance of this item: High. Private is the default community string for SNMP read/write access. Many hackers know about it. Change it.	**Vulnerabilities checked:** V7a - SNMP Security is enabled.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Access to SNMP through the default community string is a popular exploit.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "forbid SNMP community private". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: snmp-server community private (CIS 3.2.6)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: The SNMP read/write community string has not been changed from its default value. Due to its High level of Importance, this exception will be added to the report as a Finding.	

Checklist Item # 37	**Checklist Item Title:** forbid SNMP without ACLs
Reference: (CIS 3.1.11, 3.2.7) (NSA page 85)	
RISK	
Importance of this item: High. If ACLs are not applied, then anyone with a valid SNMP community string may monitor and manage the router. An ACL should be defined and applied for all SNMP community strings to limit access to a small number of authorized management stations.	**Vulnerabilities checked:** V7a - SNMP Security is enabled.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:**
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "forbid SNMP without ACLs". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: snmp-server community.*(RW|RO)$ (CIS 3.2.7)	
Test Nature: Objective	
Evidence: The Router Audit Tool report did not perform this test for this particular configuration.	
Findings: None.	

Checklist Item # 38	**Checklist Item Title:** Check if access to SNMP is restricted through Access Control Lists
Reference: (CIS 3.1.13, 3.2.8) (NSA page 85) (Akin page 73)	
RISK	
Importance of this item: High. Access control lists limit remote access to SNMP to specific IP addresses.	**Vulnerabilities checked:** V7a - SNMP Security is enabled.

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Intruders can remotely manage your network through SNMP.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "Define SNMP ACL". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: access-list $(SNMP ACL NUMBER) permit $(SNMP ACL BLOCK WITH MASK) access-list $(SNMP ACL NUMBER) deny any log (CIS 3.2.8)	
Test Nature: Objective	
Evidence: The Router Audit Tool report did not perform this test for this particular configuration.	
Findings: None.	

2.2.15. NTP Security (Network Time Protocol)

Checklist Item # 39	**Checklist Item Title:** Check if Network Time Protocol (NTP) is used to set the router's time against a timeserver.
Reference: (CIS 3.1.42, 3.2.26) (NSA page 136) (Akin chapter 10)	
RISK	
Importance of this item: Medium. Synchronizes the router's time setting with the time settings of the other devices on the network. This way when an intrusion has been detected the time of the event is logged correctly and can be compared with other devices. Helpful when prosecuting an attacker.	**Vulnerabilities checked:** V10a - NTP (Network Time Protocol) Security is not being used to synchronize time between routers.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Medium. If an attacker may realizes your router is not properly logging time, they might be more tempted to exploit vulnerabilities on the router.

© SANS Institute 2005

Author retains full rights.

Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "ntp server". Look under the column Pass/Fail to determine if your router configuration file failed this test.
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ntp server $(NTP HOST) (CIS 3.2.26)
Test Nature: Objective
Evidence: The Router Audit Tool report showed FAIL for this test.
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Medium level of Importance.

Checklist Item # 40	**Checklist Item Title:** Check if Network Time Protocol (NTP) is used to set the router's time against a second timeserver.
Reference: (CIS 3.1.44, 3.2.27) (NSA page 136)	
RISK	
Importance of this item: Medium. It is important to be able to access a second timeserver in case the first one is not available.	**Vulnerabilities checked:** V10a - NTP (Network Time Protocol) Security is not being used to synchronize time between routers.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Low. Not really something an intruder would be tempted to exploit.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "ntp server 2". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ntp server $(NTP HOST 2) (CIS 3.2.27)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Medium level of Importance.	

© SANS Institute 2005

Author retains full rights.

Checklist Item # 41	**Checklist Item Title:** Check if Network Time Protocol (NTP) is used to set the router's time against a third timeserver.
Reference: (NSA page 136)	
RISK	
Importance of this item: Medium. It is important to be able to access a third timeserver in case the first two are not available.	**Vulnerabilities checked:** V10a - NTP (Network Time Protocol) Security is not being used to synchronize time between routers.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Low. Not really something an intruder would be tempted to exploit.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "ntp server 3". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ntp server $(NTP HOST 3) (CIS 3.2.28)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Medium level of Importance.	

2.2.16. Inadequate Logging

Checklist Item # 42	**Checklist Item Title: Check if the router is set to Greenwich Mean Time**
Reference: (CIS 3.1.50, 3.2.29) (NSA page 134) (Akin page 102)	
RISK	
Importance of this item: Low. Important if the network has routers in different time zones.	**Vulnerabilities checked:** V11a – Inadequate Logging.

© SANS Institute 2005

Author retains full rights.

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Low. Probably not the kind of thing an attacker would be interested in.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "clock timezone - GMT". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: clock timezone GMT 0 (CIS 3.2.29)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Low level of Importance.	

Checklist Item # 43	**Checklist Item Title:** Check if daylight saving time is disabled.
Reference: (CIS 3.1.51, 3.2.30) (Akin page 102)	
RISK	
Importance of this item: Medium. Important to keep all your routers set to the same time. Important to use straight Universal Coordinated Time without local or seasonal variances.	**Vulnerabilities checked:** V11a – Inadequate Logging.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Medium. Attacker may be tempted to take advantage of time variances in order to hide their tracks.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "forbid clock summer-time - GMT". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: clock summer-time (CIS 3.2.30)	

© SANS Institute 2005

Author retains full rights.

Test Nature: Objective.
Evidence: The Router Audit Tool report showed pass for this test.
Findings: None.

Checklist Item # 44	**Checklist Item Title:** Check that all log entries are time stamped
Reference: (NSA page 129) (Akin page 110)	
RISK	
Importance of this item: Medium. Important to timestamp logged events, in order determine when an incident took place.	**Vulnerabilities checked:** V11a – Inadequate Logging.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Low. However, if the hacker knew that log entries were logged but not time stamped, it might tempt them to attack since it would be difficult to associate their activity with a particular incident.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "service timestamps logging". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: service timestamps log datetime(msec)? show-timezone (CIS 3.2.31)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Medium level of Importance.	

Checklist Item # 45	**Checklist Item Title:** Check that debug messages in the log include timestamps.

Reference: (CIS 3.1.53, 3.2.32) (NSA page 129)	
RISK	
Importance of this item: Medium. Important to timestamp debug messages. It helps with the investigation of intrusion events.	**Vulnerabilities checked:** V11a – Inadequate Logging.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Low. However, if the hacker knew that debug messages were not time stamped, it might tempt them to attack since this makes it more difficult to track their activity.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "service timestamps debug". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: service timestamps debug datetime(msec)? show-timezone (CIS 3.2.32)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Medium level of Importance.	

Checklist Item # 46	**Checklist Item Title:** Check if logging is enabled
Reference: (CIS 3.1.54, 3.2.33) (NSA page 129)	
RISK	
Importance of this item: Medium. Important to log events otherwise difficult to investigate intrusions.	**Vulnerabilities checked:** V11a – Inadequate Logging.

© SANS Institute 2005

Author retains full rights.

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Low. An attacker aware that logging was not enabled would be more likely to attack since the router would not log their actions.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "enable logging". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: no logging on (CIS 3.2.33)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed pass for this test.	
Findings: None.	

Checklist Item # 47	**Checklist Item Title:** Check if a syslog server is used.
Reference: (CIS 3.1.55, 3.2.34) (NSA page 130) (Akin page 113)	
RISK	
Importance of this item: Medium. Routers can only store a limited number of logs in their RAM. In addition, the logs are lost if the router reboots. syslog logging writes router logs to a file on a Unix server.	**Vulnerabilities checked:** V11a – Inadequate Logging.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Low. Attacker could try to fill up router memory in order to hide their activities.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "set syslog server". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: logging $(SYSLOG HOST) (CIS 3.2.34)	
Test Nature: Objective	

© SANS Institute 2005

Author retains full rights.

Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Medium level of Importance.	

Checklist Item # 48	**Checklist Item Title:** Check if the router is keeping log messages in RAM
Reference: (CIS 3.1.57, 3.2.35) (NSA page 129) (Akin pages 111 and 112)	
RISK	
Importance of this item: Medium. Allows logs to be temporary stored on the router itself.	**Vulnerabilities checked:** V11a – Inadequate Logging.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Medium. Intruder could attack without logging of their activities
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "logging buffered". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: logging buffered \d+ (CIS 3.2.35)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Medium level of Importance.	

Checklist Item # 49	**Checklist Item Title:** Check if router displays critical logging messages to its console monitor screen
Reference: (CIS 3.1.59, 3.2.36) (NSA page 129) (Akin pages 109 to 111)	
RISK	

Importance of this item: Low. The router displays important logging messages that are marked as critical or higher, on its console monitor as soon as they occur.	**Vulnerabilities checked:** V11a – Inadequate Logging.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Low. Intruder might be more tempted to attack router if they knew that their activities would not be displayed on the console monitor screen.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "logging console critical". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: logging console critical (CIS 3.2.36)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: This audit exception will not be added to the list of 10 findings to be reported to management due to it only having a Low level of Importance.	

Checklist Item # 50	**Checklist Item Title:** Check if logging trap is set at information or higher
Reference: (CIS 3.1.60, 3.2.37) (NSA page 132) (Akin page 114)	
RISK	
Importance of this item: Low. Want to make sure that the severity level that produces log messages is set at informational or higher.	**Vulnerabilities checked:** V11a – Inadequate Logging.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** Low. If only the most severe events are logged increases possibly that hacker could go unnoticed.

Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "logging trap info or higher". Look under the column Pass/Fail to determine if your router configuration file failed this test.
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: logging trap ((alerts)|(critical)|(emergencies)|(errors)|(warnings)|(notifications)|([0-5])) (CIS 3.2.37)
Test Nature: Objective
Evidence: The Router Audit Tool report showed pass for this test.
Findings: None.

3. Conduct the Audit Testing, Evidence and Findings.

3.1. Ran RAT

3.1.1. Obtained the router configuration file

The following router configuration file was obtained from the Router Administrator. The router configuration file, router_config.txt, contained the following text. To hide the client's IP addresses, they have all been changed to 5.5.5.5.

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ABCDEFGH
!
logging buffered 4096 debugging
enable secret 5 LASJDFOIASDFJASLKFJLKSA
enable password welcome
!
ip subnet-zero
no ip source-route
!
!
ip host STLROT02 5.5.5.5
ip host STLROT03 5.5.5.5
!
no ip bootp server
```

© SANS Institute 2005, Author retains full rights.

```
!
!
!
interface FastEthernet0/0
 ip address 5.5.5.5 5.5.5.5
 speed 10
 half-duplex
!
interface FastEthernet0/1
 ip address 5.5.5.5 5.5.5.5
 speed 100
 full-duplex
!
interface Ethernet1/0
 ip address 5.5.5.5 5.5.5.5
 no ip mroute-cache
 full-duplex
!
interface Ethernet1/1
 ip address 5.5.5.5 5.5.5.5
 full-duplex
!
interface Ethernet1/2
 no ip address
 no ip mroute-cache
 shutdown
 half-duplex
 no cdp enable
!
interface Ethernet1/3
 ip address 5.5.5.5 5.5.5.5
 no ip mroute-cache
 full-duplex
 no cdp enable
!
router rip
 version 2
 network 10.0.0.0
!
no ip classless
ip route profile
ip route 5.5.5.5 5.5.5.5 5.5.5.5
ip route 5.5.5.5 5.5.5.5 5.5.5.5
ip route 5.5.5.5 5.5.5.5 5.5.5.5
ip route 5.5.5.5 5.5.5.5 5.5.5.5
ip route 5.5.5.5 5.5.5.5 5.5.5.5
ip route 5.5.5.5 5.5.5.5 5.5.5.5
ip route 5.5.5.5 5.5.5.5 5.5.5.5
no ip http server
ip pim bidir-enable
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
snmp-server community public RO
snmp-server community private RW
!
line con 0
 password welcome
```

© SANS Institute 2005, Author retains full rights.

```
 login
line aux 0
line vty 0 4
 password welcome
 login
!
end
```

3.1.2. Configured RAT

The RAT configuration program was run by typing bin\ncat_config from C:\CIS\RAT. The router administrator was present during this phase to provide their input. The following shows the screen dump from running the RAT configuration:

```
bin\ncat_config: Select configuration type [cisco-ios] ?
bin\ncat_config: Applying rules from:
bin\ncat_config:   C:\CIS\RAT/etc/configs/cisco-ios/common.conf
bin\ncat_config:   C:\CIS\RAT/etc/configs/cisco-ios/cis-level-1.conf
bin\ncat_config:   C:\CIS\RAT/etc/configs/cisco-ios/cis-level-2.conf
bin\ncat_config:   C:\CIS\RAT/etc/configs/cisco-ios/local.conf
bin\ncat_config: Apply some or all of the rules that are selectable
[Yes] !
bin\ncat_config:   Apply some or all of CIS level 1 rules [yes] ?
bin\ncat_config:     Check rules and data related to system
management [Yes] !
bin\ncat_config:       Use local authentication [yes] ?
bin\ncat_config:         Create new AAA model using local usernames
and passwords [yes] !
bin\ncat_config:         Create local usernames [yes] !
bin\ncat_config:           Username of user for local authentication
[username1] ? bin\ncat_config:       Apply standard SNMP checks [Yes]
!
bin\ncat_config:         Disable SNMP server [yes] ? bin\ncat_config:
Forbid SNMP read-write [yes] ? bin\ncat_config:         Forbid SNMP
community string 'public' [yes] !
bin\ncat_config:         Forbid SNMP community string 'private' [yes]
!
Info: skipping IOS - forbid SNMP without ACLs because it conflicts
with IOS - no snmp-server which is already selected
Info: skipping IOS - Define SNMP ACL because it conflicts with IOS -
no snmp-server which is already selected
bin\ncat_config:       Apply standard checks to control access to the
router [yes] ? bin\ncat_config:         Allow Telnet access for
remote administration? [yes] ? bin\ncat_config:           Allow only
telnet access for remote login [yes] !
bin\ncat_config:         Specify maximum allowed exec timeout [yes] !
bin\ncat_config:           Exec timeout value [10 0] ?
bin\ncat_config:         Disable the aux port [yes] ?
bin\ncat_config:         Use default AAA login authentication on each
line [yes] ? Info: skipping IOS - login named list because it
conflicts with IOS - login default which is already selected
bin\ncat_config:         require line passwords [yes] ?
```

© SANS Institute 2005 Author retains full rights.

```
bin\ncat_config:         Require an enable secret [yes] !
bin\ncat_config:         Check line password quality [yes] ?
bin\ncat_config:         Check user password quality [yes] ?
bin\ncat_config:         Require VTY  ACL to be applied [yes] !
bin\ncat_config:           Specify ACL number to be used for telnet
or ssh [182] ? bin\ncat_config:         Define simple (one netblock +
one host) VTY ACL [yes] ? bin\ncat_config:           Address block
and mask for administrative hosts [5.5.5.5 5.5.5.5] ?
bin\ncat_config:           Address for administrative host [5.5.5.5]
? bin\ncat_config:       Disable unneeded management services [yes] ?
bin\ncat_config:         Forbid finger service (on IOS 11) [yes] !
bin\ncat_config:         Forbid identd service (on IOS 11) [yes] !
bin\ncat_config:         Forbid finger service (on IOS 12) [yes] !
bin\ncat_config:         Forbid finger service (on IOS 12) [yes] !
bin\ncat_config:         Forbid http service [yes] !
bin\ncat_config:         Encrypt passwords in the configuration [yes]
!
bin\ncat_config:     Check rules and data related to system control
[Yes] !
bin\ncat_config:       Synchronize router time via NTP [yes] ?
bin\ncat_config:         Designate an NTP time server [yes] !
bin\ncat_config:           Address of first NTP server [1.2.3.4] ?
bin\ncat_config:         Designate a second NTP time server [yes] ?
bin\ncat_config:           Address of second NTP server [5.6.7.8] ?
bin\ncat_config:         Designate a third NTP time server [yes] ?
bin\ncat_config:           Address of third NTP server [9.10.11.12] ?
bin\ncat_config:       Apply standard logging rules [yes] ?
bin\ncat_config:         Use GMT for logging instead of localtime
[yes] ? bin\ncat_config:         Check timezone and offset [yes] !
bin\ncat_config:           Forbid summertime clock changes [yes] !
bin\ncat_config:         Timestamp log messages [yes] !
bin\ncat_config:         Timestamp debug messages [yes] !
bin\ncat_config:         enable logging [yes] !
bin\ncat_config:         Designate syslog server [yes] !
bin\ncat_config:           Address of syslog server [13.14.15.16] ?
bin\ncat_config:         Designate local logging buffer size [yes] !
bin\ncat_config:           Local log buffer size [16000] ?
bin\ncat_config:         Require console logging of critical messages
[yes] !
bin\ncat_config:         Require remote logging of level info or
higher [yes] !
bin\ncat_config:       Disable unneeded control services [yes] ?
bin\ncat_config:         Forbid small TCP services (on IOS 11) [yes]
!
bin\ncat_config:         Forbid small UDP services (on IOS 11) [yes]
!
bin\ncat_config:         Forbid small TCP services (on IOS 12) [yes]
!
bin\ncat_config:         Forbid small UDP services (on IOS 12) [yes]
!
bin\ncat_config:         Forbid bootp service [yes] !
bin\ncat_config:         Disable CDP service [yes] ? bin\ncat_config:
Forbid config service [yes] ? bin\ncat_config:         Use tcp-
keepalive-in service to kill stale connections [yes] !
bin\ncat_config:         Forbid tftp service [yes] ? bin\ncat_config:
Check rules and data related to data flow [Yes] !
bin\ncat_config:       Apply standard routing protections [yes] ?
bin\ncat_config:         Forbid directed broadcasts (on IOS 11) [yes]
```

© SANS Institute 2005

Author retains full rights.

```
!
bin\ncat_config:          Forbid directed broadcasts (on IOS 12) [yes]
!
bin\ncat_config:          Forbid IP source routing [yes] !
bin\ncat_config:    Apply some or all of CIS Level 2 rules [no] ?
```

Then I created a directory named c:\cis\rat\routers and copied the router's configuration file (router_config.txt) to it

Then c:\cis\rat\bin was added to the path statement by typing in the command path c:\cis\rat\bin;%path%.

3.1.3. Ran RAT against the router configuration file

Then RAT was run against the router configuration file by typing rat router_config.txt from the c:\cis\rat\reports directory. This way all the reports produced by RAT will end up in the c:\cis\rat\reports directory. The following is a screendump from running RAT, it shows all the files that RAT uses as well as the reports that are copied into the c:\cis\rat\reports directory:

3.2. Evaluate the results from RAT

3.2.1. Display the "all.html" report

The following shows the report, all.html that was generated by RAT. It gives the results of the testing and will be used along with the checklist to look for audit

© SANS Institute 2005

Author retains full rights.

exceptions →

Router Audit Tool report for
all
Audit Date: Sun Jan 16 22:15:23 2005 GMT
Sort Order: importance,passfail,rule,device,instance,line

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.
10	pass	IOS - no ip http server	router_config.txt		
10	pass	IOS - login default	router_config.txt		
10	pass	IOS - enable secret	router_config.txt		
10	FAIL	IOS - require line passwords	router_config.txt	aux 0	82
10	FAIL	IOS - no snmp-server	router_config.txt	snmp-server community private RW	2
10	FAIL	IOS - no snmp-server	router_config.txt	snmp-server community public RO	2
10	FAIL	IOS - forbid SNMP read-write	router_config.txt	private	77
10	FAIL	IOS - forbid SNMP community public	router_config.txt	n/a	76
10	FAIL	IOS - forbid SNMP community private	router_config.txt	n/a	77
10	FAIL	IOS - apply VTY ACL	router_config.txt	vty 0 4	83
10	FAIL	IOS - Use local authentication	router_config.txt	n/a	2
10	FAIL	IOS - Define VTY ACL	router_config.txt	n/a	2
10	FAIL	IOS - Create local users	router_config.txt	n/a	2
7	pass	IOS 12 - no udp-small-servers	router_config.txt		
7	pass	IOS 12 - no tcp-small-servers	router_config.txt		

7	pass	IOS 12 - no directed broadcast	router_config.txt		
7	pass	IOS - no service config	router_config.txt		
7	pass	IOS - no ip source-route	router_config.txt		
7	pass	IOS - exec-timeout	router_config.txt		
7	FAIL	IOS - no cdp run	router_config.txt	n/a	2
7	FAIL	IOS - encrypt passwords	router_config.txt	n/a	2
5	pass	IOS 12.1,2,3 - no finger service	router_config.txt		
5	pass	IOS - no ip bootp server	router_config.txt		
5	pass	IOS - forbid clock summer-time - GMT	router_config.txt		
5	pass	IOS - enable logging	router_config.txt		
5	FAIL	IOS - tcp keepalive service	router_config.txt	n/a	2
5	FAIL	IOS - set syslog server	router_config.txt	n/a	2
5	FAIL	IOS - service timestamps logging	router_config.txt	n/a	2
5	FAIL	IOS - service timestamps debug	router_config.txt	n/a	2
5	FAIL	IOS - ntp server 3	router_config.txt	n/a	2
5	FAIL	IOS - ntp server 2	router_config.txt	n/a	2
5	FAIL	IOS - ntp server	router_config.txt	n/a	2
5	FAIL	IOS - logging buffered	router_config.txt	n/a	11
5	FAIL	IOS - line password quality	router_config.txt	vty 0 4	83
5	FAIL	IOS - line password quality	router_config.txt	con 0	79
5	FAIL	IOS - line password quality	router_config.txt	aux 0	82
5	FAIL	IOS - VTY transport telnet	router_config.txt	vty 0 4	83
3	pass	IOS - logging trap info or higher	router_config.txt		

3	FAIL	IOS - logging console critical	router_config.txt	n/a	2
3	FAIL	IOS - disable aux	router_config.txt	aux 0	82
3	FAIL	IOS - clock timezone - GMT	router_config.txt	n/a	2

Summary for all

#Checks	#Passed	#Failed	%Passed
41	14	27	34

Perfect Weighted Score	Actual Weighted Score	%Weighted Score
278	95	34

Ovarall Score (0-10)
3.4

Note: PerfectWeightedScore is the sum of the importance value of all rules. ActualWeightedScore is the sum of the importance value of all rules passed, minus the sum of the importance each instance of a rule failed.

end of the report all.html

3.2.2. Examining the "all.html" report for exceptions

This audit examined the RAT report named "all.html" for any Fails and checked them against the Checklist from Part 2. The following shows the results of using all.html and having matched all the rules that failed to the items on the checklist, and having an Importance of at least High. This audit chose the first 10 of the 11 items of High Importance to be used as a demonstration of using RAT with Windows to perform a Technical Audit. These items are going to be considered as the findings of this audit:

3.3.3. Summary of the Ten Findings to be reported to Management

List of Findings to Be Reported to Management				
Finding	**Description**	**Checklist Item**	**Vulnerability**	**CIS Gold Standard Benchmark**

1	Passwords are not required to access the router.	4	V2b	3.1.24, 3.2.14
2	SNMP is enabled.	33	V7a	3.1.7, 3.2.3
3	SNMP read/write is allowed.	34	V7a	3.1.8, 3.2.4
4	The SNMP read-only community string has not been changed from its default value.	35	V7a	3.1.9, 3.2.5
5	The SNMP read/write community string has not been changed from its default value.	36	V7a	3.1.10, 3.2.6
6	Access Control Lists have not been applied to the VTY lines.	5	V2c	3.1.28, 3.2.18
7	Local user authentication is being not used.	2	V2a	3.1.3, 3.2.1
8	Access Control Lists have not been defined for the VTY lines.	6	V2c	3.1.30, 3.2.19
9	User authentication is not required.	3	V2a	3.1.4, 3.2.2
10	The Cisco Discovery Protocol (CDP) is not disabled.	28	V6a	3.1.67, 3.2.43

SANS Institute 2005

3.3.4. Details on the ten findings from their associated checklist items

This section shows the Checklist Items that are associated with the exceptions from RAT. These exceptions will be written up as findings in the audit report.

Finding #1, Passwords are not required to access the router, is associated with Checklist Item #4:

Checklist Item #4	**Checklist Item Title:** Check that passwords are required in order to access the router through the Console, Auxiliary port, or Virtual TTY.
Reference: (CIS 3.1.24, 3.2.14) (NSA page 58) (Jones page 5) (Akin page13)	
RISK	

Importance of this item: High. Make sure that a password is required to access the router is case other stronger access controls are not configured correctly.	**Vulnerabilities checked:** V2b – Passwords are not being used to control access to the Console port, Auxiliary port (AUX) and Virtual TTY (VTY).
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities**: High. Lack of passwords makes it easy to access the router.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "IOS – require line passwords". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: password [^\n\s]+ (CIS 3.2.14)	
Test Nature: Objective or Subjective? Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: Passwords are not required to access the router. Due to its High level of Importance, this exception will be added to the report as a Finding.	

Finding #2, SNMP is enabled, is associated with Checklist Item #33:

Checklist Item # 33	**Checklist Item Title:** Check that SNMP is disabled.
Reference: (CIS 3.1.7, 3.2.3) (NSA page 76) (Akin page 68. Also chapter 8, SNMP Security.)	
RISK	
Importance of this item: High. Intruders can use SNMP to learn about your network layout, hardware, and software. They can use this information to find and attack vulnerable systems on your network.	**Vulnerabilities checked:** V7a - SNMP Security is enabled.

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. It would be highly tempting for an attacker can use the information gathered through SNMP to find out which hardware or software on your network has vulnerabilities that they can easily exploit.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no snmp-server". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: ^snmp-server (CIS 3.2.3)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: SNMP is enabled. Due to its High level of Importance, this exception will be added to the report as the finding.	

Finding #3, SNMP read/write is allowed, is associated with Checklist Item #34:

Checklist Item #34	**Checklist Item Title:** Check that SNMP read-write is disabled.
Reference: (CIS 3.1.8, 3.2.4) (NSA page 138) (Akin page 73)	
RISK	
Importance of this item: High. Allows SNMP to be managed remotely. Intruder can completely take over the router through the Internet.	**Vulnerabilities checked:** V7a - SNMP Security is enabled.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. This vulnerability allows remote management of SNMP, which hackers could be tempted to take advantage of.

© SANS Institute 2005

Author retains full rights.

Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "forbid SNMP read-write". Look under the column Pass/Fail to determine if your router configuration file failed this test.
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: snmp-server community.*RW (CIS 3.2.4)
Test Nature: Objective
Evidence: The Router Audit Tool report showed FAIL for this test.
Findings: Due to its High level of Importance, this exception will be added to the report as a Finding.

Finding #4, The SNMP read-only community string has not been changed from its default value, is associated with Checklist Item #35:

Checklist Item # 35	**Checklist Item Title:** Check if "public" is used as the SNMP community string for read-only access.
Reference: (CIS 3.1.9, 3.2.5) (NSA page 138) (Akin page 71)	
RISK	
Importance of this item: High. Public is the default community string for SNMP read-only access. Many hackers know about it. They can use it to find out how your router and network is configured.	**Vulnerabilities checked:** V7a - SNMP Security is enabled.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Access to SNMP through the default community string is a popular exploit.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "forbid SNMP community public". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: snmp-server community public (CIS 3.2.5)	

Test Nature: Objective
Evidence: The Router Audit Tool report showed FAIL for this test.
Findings: The SNMP read-only community string has not been changed from its default value. Due to its High level of Importance, this exception will be added to the report as a Finding.

Finding #5, The SNMP read/write community string has not been changed from its default value, is associated with Checklist Item #36:

Checklist Item # 36	**Checklist Item Title:** Check if "private" is used as the SNMP community string for read/write access.
Reference: (CIS 3.1.10, 3.2.6) (NSA page 138) (Akin page 71)	
RISK	
Importance of this item: High. Private is the default community string for SNMP read/write access. Many hackers know about it. Change it.	**Vulnerabilities checked:** V7a - SNMP Security is enabled.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Access to SNMP through the default community string is a popular exploit.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "forbid SNMP community private". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: snmp-server community private (CIS 3.2.6)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: The SNMP read/write community string has not been changed from its default value. Due to its High level of Importance, this exception will be added to the report as a Finding.	

Finding #6, Access Control Lists have not been applied to the VTY lines, is associated with Checklist Item #5:

Checklist Item #5	**Checklist Item Title:** Check that Access Control Lists (ACLs) are applied.
Reference: (CIS 3.1.28, 3.2.18) (NSA page 64) (Akin page 25)	
RISK	
Importance of this item: High. Access to the VTY port is not limited to specific IP addresses, therefore anyone from anywhere on the Internet can keep guessing passwords to your router until they find the right one.	**Vulnerabilities checked:** V2c – Access Control Lists are not being used to control access to the router through the VTY lines.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Attackers can try to access the router from anywhere on the Internet.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "apply VTY ACL". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: access-class $(VTY_ACL_NUMBER) in (CIS 3.2.18)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: Access Control Lists have not been applied to the VTY lines. Due to its High level of Importance, this exception will be added to the report as a Finding.	

Finding #7, Local user authentication is being not used, is associated with Checklist Item #2:

Checklist Item #2	**Checklist Item Title:** Check that local authentication being used to provide accountability. NOTE: This test is also reflected under V4a – The AAA Security method is not being used. (AAA = authentication, authorization, and accounting), Checklist Item #14

References: (CIS 3.1.3, 3.2.1) (Jones page 9) from Jones, George. SANS Institute presents: Improving Router Security with RAT: The Top 10 List., SANS Wednesday Webcast, 2003. (Akin page 44, Chapter 5)	
RISK	
Importance of this item: High. The router has not been changed from its default value, it is not configured to require authentication of users. Router administrator needs to establish a new authorization model that requires local login.	**Vulnerabilities checked:** V2a – Lack of Accountability for Router Users.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Without accountability, there is nothing to prevent disgruntled employees from attacking the router without being accountable for their actions.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "IOS – Use local authentication". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: aaa new-model aaa authentication login $(AAA_LIST_NAME) local aaa authentication enable \S+ (CIS 3.2.1)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: Local user authentication is being not used. Due to its High level of Importance, this exception will be added to the report as a Finding.	

Finding #8, Access Control Lists have not been defined for the VTY lines, is associated with Checklist Item #6:

Checklist Item # 6	**Checklist Item Title:** Check that Access Control Lists have been defined for the VTY lines.

Reference: (CIS 3.1.30, 3.2.19) (NSA page 64)	
RISK	
Importance of this item: High. This allows you to control access to your router by creating access control lists containing the IP addresses of who is allowing to login.	**Vulnerabilities checked:** V2c – Access Control Lists are not being used to control access to the router through the VTY lines.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Hackers can enter router from any IP address on the Internet
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "Define VTY ACL". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: access-list $(VTY ACL NUMBER) permit tcp $(VTY ACL BLOCK WITH MASK) any access-list $(VTY ACL NUMBER) permit tcp host $(VTY ACL HOST) any access-list $(VTY ACL NUMBER) deny ip any any log (CIS 3.2.19)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: Access Control Lists have not been defined for the VTY lines. Due to its High level of Importance, this exception will be added to the report as a Finding.	

Finding #9, User authentication is not required, is associated with Checklist Item #3:

Checklist Item #3	**Checklist Item Title:** Check that local users have been defined.
Reference: (CIS 3.1.4, 3.2.2) (Jones page 9) (Akin page 15)	
RISK	

Importance of this item: High. Users are not given names. They just login with a common password, without being asked who they are. Therefore, there is no accountability as to who has made changes to the router's configuration.	**Vulnerabilities checked:** V2a – Lack of Accountability for Router Users.
Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Internal threat. Disgruntled employee could make changes to router configurations without accountability.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "IOS – Create local users". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark: username \S+ password \d \S+ (CIS 3.2.2)	
Test Nature: Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: User authentication is not required. Due to its High level of Importance, this exception will be added to the report as a Finding.	

Finding #10, The Cisco Discovery Protocol (CDP) is not disabled, is associated with Checklist Item #28:

Checklist Item # 28	**Checklist Item Title:** Check that the Cisco Discovery Protocol has been disabled.
Reference: (CIS 3.1.67, 3.2.43) (NSA page 71) (Akin page 65)	
RISK	
Importance of this item: High. Attackers could draw a diagram of your network from all the information given by CDP. In addition, there are known denial of service attacks that exploit this protocol.	**Vulnerabilities checked:** V6a – There are unnecessary protocols and services - such as the small services or the Cisco discovery protocol.

Assets affected by a successful exploit: Sensitive data. Reputation.	**Likelihood that a threat could exploit the vulnerabilities:** High. Attackers often exploit small services such as CDP.
Testing Procedure: Obtain the router configuration file and run RAT against it, following the instructions at the beginning of Part 2. Examine the file named "all.html" for a line with the Rule Name of "no cdp run". Look under the column Pass/Fail to determine if your router configuration file failed this test.	
Compliance Criteria: RAT checks the Router Configuration File for a rule that matches the following Benchmark:no cdp run (CIS 3.2.43)	
Test Nature: Objective or Subjective? Objective	
Evidence: The Router Audit Tool report showed FAIL for this test.	
Findings: The Cisco Discovery Protocol (CDP) is not disabled. Due to its High level of Importance, this exception will be added to the report as a Finding.	

4. Audit Report

4.a. Executive Summary

4.a.1. Background

Routers are the backbone for the Internet. Their main job is to connect together different types of networks. This job must be done quickly, and securely. In addition, routers can be used to block intrusive packets, packets that might be attempting to exploit vulnerabilities on your network. When hardening your systems, it is easy for security administrators to overlook the importance of routers, but routers can be used in many types of computer-based attacks.

The router that was audited is part of your test network, and security personnel need to be careful not overlook the importance of securing the routers that are present in test networks, also. Attacks on this router could undermine your testing process. In addition, employees may not think that network devices used for testing and training have to be as stringently secured as those in a production environment, although a router in such a network could still be taken over by an intruder through an outside connection (such as the Internet). This would allow the intruder to obtain sensitive information from the test network, information that could be used to attack your production network. For example,

© SANS Institute 2005, Author retains full rights.

what if an intruder finds an administrator's password on an unsecured test network, and then discovers that it also works on the production network?

4.a.2. Objective

This audit met its overall objective of using RAT to perform a security audit of the Cisco router in the test network. This audit can be considered a success, because the following three objectives were met:

1. This audit determined a secure configuration for your router,
2. This audit was able to scope the audit to fit RAT's ability to test whether your router meets that configuration, and
3. This audit successfully utilized RAT to determine whether your router is securely configured.

4.a.3. Audit Recommendations

This audit recommends that improvements be made to important network devices in the test network. In particular, this audit examined a router, which is a device essential to running a network, to make sure that it was configured in a secure manner. Routers often serve as an entrance to your network, therefore, when they are compromised, it makes it easier for intruders to obtain unauthorized access to the rest of your network.

The areas that could be improved, with little cost to the business, are to the router's configuration file. This report will offer some suggestions for improvement.

We suggest going over your network security policies with your network administrators, assuring them of the importance of maintaining a secure configuration of the routers. We suggest that management consider assuring that its policy for securing the network covers items such as router configuration files. In addition, we suggest that management assure that the router configuration files are audited at regular intervals, using a program such as the Router Auditing Tool from the Center for Internet Security (RAT). The RAT program greatly simplifies the auditing of routers, allowing you to quickly determine their level of security. In addition, RAT provides recommendations that your network administrators can use to modify the configuration files of your routers, and make them as secure as possible.

The greatest opportunities for improvement are found in the following areas:

Management needs to assure that access controls for the router are adequate.

© SANS Institute 2005 Author retains full rights.

© SANS Institute 2005 Author retains full rights.

At its present configuration, we found that passwords are not being used to control access the router. Passwords should be the first line of defense in securing a router. In addition, access to the router is not being limited to specific users. The present router configuration could allow intruders to access the router from any location on the Internet.

In addition, management needs to consider limiting the use of unnecessary services and protocols on the router, especially those that can be used by intruders to obtain information concerning the configuration of your test network. At present, your router allows anyone from anywhere on the Internet to learn about the type of hardware and software in the test network, and effectively draw a picture of the network. We recommend that unneeded services be removed from your router. If management determines they are needed, then they must be configured in a secure manner.

A more detailed discussion of the audit findings and recommendations follows in the next section.

© SANS Institute 2005, Author retains full rights.

4.b. Audit Findings and Recommendations

4.b.1. Summary of Audit Findings

This audit used the Router Auditing Tool from the Center for Internet Security (RAT) to perform a security audit of a router in use at the test network. This audit found that there were some weaknesses in the configuration of the router. These weaknesses are summarized in the following chart:

List of Findings				
Finding	**Description**	**Checklist Item**	**Vulnerability**	**CIS Gold Standard Benchmark**
1	Passwords are not needed to access the router through the Console, Auxiliary port, or Virtual TTY.	4	V2b	3.1.24, 3.2.14
2	SNMP is enabled.	33	V7a	3.1.7, 3.2.3
3	SNMP read/write is allowed.	34	V7a	3.1.8, 3.2.4
4	The SNMP read-only community string has not been changed from its default value.	35	V7a	3.1.9, 3.2.5
5	The SNMP read/write community string has not been changed from its default value.	36	V7a	3.1.10, 3.2.6
6	Access Control Lists have not been applied to the VTY lines.	5	V2c	3.1.28, 3.2.18
7	Local user authentication is being not used.	2	V2a	3.1.3, 3.2.1
8	Access Control Lists have not been defined for the VTY lines.	6	V2c	3.1.30, 3.2.19
9	User authentication is not required.	3	V2a	3.1.4, 3.2.2
10	The Cisco Discovery Protocol (CDP) is not disabled.	28	V6a	3.1.67, 3.2.43

All of these findings can be associated directly with Gold Standard Benchmarks

© SANS Institute 2005

Author retains full rights.

for Cisco IOS (from CIS). These Benchmarks are a reflection of those found in NSA's Router Security Configuration Guide. By running RAT on the router configuration file that was received from the network administrator for the test network, ten findings were identified. What follows is a brief analysis of those findings, along with our recommendations for improvement.

4.b.2. Detailed Findings and Recommendations

Audit Finding #1 - Passwords are not required to access the router through the Console, Auxiliary port, or Virtual TTY.

Checklist Item #4 – Check that passwords are required in order to access the router through the Console, Auxiliary port, or Virtual TTY.

Evidence > The router configuration file failed RAT's test for Checklist Item #4, require line passwords. The following shows the line from the all.html report that reported this weakness:

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	FAIL	IOS - require line passwords	router_config.txt	aux 0	82

Cause > Router was not configured to require passwords for access through the Console, Auxiliary port, or Virtual TTY.

Justification for this finding. What risks are the direct results of this finding? > An intruder could gain access to the router without using a password. Intruders could gain access to sensitive networks.

© SANS Institute

Recommendation > Applying passwords should be the first thing you do when securing your router. Management needs to enforce formal policies and procedures that define best security practices for passwords. Best Practices recommend implementing the following configuration settings:

Use the following as an example for setting the password on the console line:

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password PASSWORD-FOR-THE-CONSOLE-LINE
```

Use the following as an example for how to set a password on all five of the default VTY lines at the same time:

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password PASSWORD-FOR-THE-VTY-LINES
```

Use the following as an example for how to set a password on the AUX line:

```
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password PASSWORD-FOR-THE-AUX-LINE
```

(Akin page 14)

Costs > The only resources required for this fix is a small amount of time from the router administrator.

Compensating Controls > When level-one local passwords are used, or TACACS level-two authentication is used, then local passwords are not needed for authentication, but they do help to protect against unauthorized access in case these other options are configured incorrectly.

Finding #2 SNMP is enabled.

Checklist Item #33 Check that SNMP is disabled.

Evidence > The router configuration file failed RAT's test for Checklist Item #33. The following shows the line from the all.html report that reported this weakness:

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number

10	FAIL	IOS - no snmp-server	router_config.txt	snmp-server community private RW	2
10	FAIL	IOS - no snmp-server	router_config.txt	snmp-server community public RO	2

Cause > The router was not configured to disable SNMP.

Justification for this finding. What risks are the direct results of this finding? > Intruders can use SNMP to learn about your network's layout. They will be able to determine types and versions of your hardware and software. They can use this information to find and attack vulnerable systems on your network.

Recommendation > Management needs to make sure that they need to use SNMP in the management of this router, otherwise best practices recommend implementing the following configuration setting:

Router(config)# no snmp-server

(CIS 3.1.7)

Costs > The only resources required for this fix is a small amount of time from the router administrator.

Compensating Controls > Use a strong password your SNMP community string. Make sure it is not the same as the other passwords on your router. Or use SNMP version 3.

Finding #3 SNMP read/write is allowed.

Checklist Item #34 Check that SNMP read-write is disabled.

Evidence > The router configuration file failed RAT's test for Checklist Item #34. The following shows the line from the all.html report that reported this weakness:

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	FAIL	IOS - forbid SNMP read-write	router_config.txt	private	77

Cause > The router was configured to allow SNMP read/write.

Justification for this finding. What risks are the direct results of this finding? > Allows SNMP to be managed remotely. Intruder can completely take over the router through the Internet.

Recommendation > If management determines that SNMP must be implemented, they will need enforce formal policies and procedures that define best security practices for use of SNMP Read/Write. Best practices recommend implementing the following configuration setting:

Router(config)# no snmp-server community RW_Community_String RW

(Akin page 73)

Costs > The only resources required for this fix is a small amount of time from the router administrator.

Compensating Controls > None.

Finding #4 The SNMP read-only community string has not been changed from its default value.

Checklist Item #35 Check if "public" is used as the SNMP community string for read-only access.

Evidence > The router configuration file failed RAT's test for Checklist Item #35. The following shows the line from the all.html report that reported this weakness:

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	FAIL	IOS - forbid SNMP community public	router_config.txt	n/a	76

Cause > The router was not configured to change the SNMP read-only community string from its default value.

Justification for this finding. What risks are the direct results of this finding? > Public is the default community string for SNMP read-only access. Many hackers know about it. They can use it to find out how your router and network is configured.

Recommendation > If management determines that SNMP must be implemented, they will need enforce formal policies and procedures that define best security practices for use of SNMP Community Strings. Best practices recommend implementing the following configuration setting:

Router(config)# no snmp-server community public

(CIS 3.1.9)

Costs > The only resources required for this fix is a small amount of time from the router administrator.

Compensating Controls > Use a strong password your SNMP community string. Make sure it is not the same as the other passwords on your router. Alternatively, use SNMP version 3.

Finding #5 The SNMP read/write community string has not been changed from its default value.

Checklist Item #36 Check if "private" is used as the SNMP community string for read/write access.

Evidence > The router configuration file failed RAT's test for Checklist Item #36. The following shows the line from the all.html report that reported this weakness:

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	FAIL	IOS - forbid SNMP community private	router_config.txt	n/a	77

Cause > The router was not configured to change the SNMP read/write community string from its default value.

Justification for this finding. What risks are the direct results of this finding? > "Private" is the default community string for SNMP read/write access. Many hackers know about it. This allows for SNMP to be managed remotely. An intruder can use it to completely take over the router through the Internet.

Audit Recommendation > If management determines that SNMP must be implemented, they will need enforce formal policies and procedures that define best security practices for use of SNMP Community Strings. Best practices recommend implementing the following configuration setting:

Router(config)# no snmp-server community private

(CIS 3.1.10)

Costs > The only resources required for this fix is a small amount of time from the router administrator.

Compensating Controls > Install SNMP version 3.

Finding #6 Access Control Lists have not been applied to the VTY lines.

Checklist Item #5 Access Control Lists are not applied.

Evidence > The router configuration file failed RAT's test for Checklist Item #5. The following shows the line from the all.html report that reported this weakness:

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	FAIL	IOS - apply VTY ACL	router_config.txt	vty 0 4	83

Cause > An access control list has not been defined to limit access to the VTY lines to specific IP addresses.
Justification for this finding. What risks are the direct results of this finding? > Access to the VTY port is not limited to specific IP addresses, therefore anyone from anywhere on the Internet can keep guessing passwords to your router until they find one that works.
Recommendation > Management needs to enforce formal policies and procedures that define best security practices for controlling access to the router. Best practices recommend implementing the following configuration settings: Need to first create an access control list: Router(config)#access-list 10 permit 5.5.5.5 Router(config)#access-list 10 permit 5.5.5.4 Router(config)#access-list 10 deny any Then apply this access control list to the VTY lines with the following two commands: Router(config)#line vty 0 4 Router(config-line)#access-class 10 in (Akin page 25)
Costs > The only resources required for this fix is a small amount of time from the router administrator.
Compensating Controls > Disable VTY lines altogether.

Finding #7 Local user authentication is being not used.					
Checklist Item #2 Check that local authentication being used to provide accountability.					
Evidence > The router configuration file failed RAT's test for Checklist Item #2. The following shows the line from the all.html report that reported this weakness:					
Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	FAIL	IOS - Use local authentication	router_config.txt	n/a	2
Cause > The router has not been changed from its default value, it is not configured to require authentication of users. Router administrator needs to establish a new authorization model that requires local login.					
Justification for this finding. What risks are the direct results of this finding? > Users can use the router without authentication.					

Recommendation > Management needs to enforce formal policies and procedures that define best security practices for authorization to use the router. Best practice recommends establishing a new authentication model that requires local login. We recommend implementing the following configuration settings; (Make sure that local users are created and an enable secret is set before applying the following rules) Router(config)# aaa new-model Router(config)# aaa authentication login $(AAA_LIST_NAME) local Router(config)# aaa authentication enable default enable (CIS 3.1.3)
Costs > The only resources required for this fix is a small amount of time from the router administrator.
Compensating Controls > Use of line passwords.

Finding #8 Access Control Lists have not been defined for the VTY lines.					
Checklist Item #6 Check that Access Control Lists have been defined for the VTY lines.					
Evidence > The router configuration file failed RAT's test for Checklist Item #6. The following shows the line from the all.html report that reported this weakness:					
Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	FAIL	IOS - Define VTY ACL	router_config.txt	n/a	2
Cause > No one has assured that access control lists were defined for the router.					
Justification for this finding. What risks are the direct results of this finding? > Access control lists are not being used to control who logs into the router. [CIS 3.2.19]					

© SANS Institute 2005

Author retains full rights.

Recommendation > Management needs to enforce formal policies and procedures that define best security practices for controlling access to the router. Best practices recommend implementing the following configuration settings:

Router(config)# no access-list $(VTY_ACL_NUMBER)
Router(config)# access-list $(VTY_ACL_NUMBER) permit tcp $(VTY_ACL_BLOCK_WITH_MASK) any
Router(config)# access-list $(VTY_ACL_NUMBER) permit tcp host $(VTY_ACL_HOST) any
Router(config)# access-list $(VTY_ACL_NUMBER) deny ip any any log

(CIS 3.1.30)

Costs > The only resources required for this fix is a small amount of time from the router administrator.

Compensating Controls > Disable all VTY lines.

Finding #9 User authentication is not required.

Checklist Item #3 Check that local users have been defined.

Evidence > The router configuration file failed RAT's test for Checklist Item #3. The following shows the line from the all.html report that reported this weakness:

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	FAIL	IOS - Create local users	router_config.txt	n/a	2

Cause > Management did not develop policies and procedures for addressing best practice security settings for their network router implementation, nor could they implement such settings.

Justification for this finding. What risks are the direct results of this finding? > Users are not given names. They just login with a common password, without being asked who they are. Therefore, there is no accountability as to who has made changes to the router's configuration.

© SANS Institute 2005

Author retains full rights.

Recommendation > Management should establish and enforce formal policies and procedures that define best security practices for controlling access to the router. Local authentication solves the accountability issue by letting users be defined on each router and having each point of access configured to use locally defined usernames and passwords. To use local authentication, first configure user accounts on each router and then configure each line to use these usernames for authentication. To create users, use the username command:

Router(config)# username USER password PASSWORD

Then use the login local command to tell each line to use local authentication:

Router(config)# aaa new-model
Router)config)# aaa authentication login default local

Note: Make sure that enable secret is enabled before applying the above lines. (Akin page 15)

Costs > The only resources required for this fix is a small amount of time from the router administrator.

Compensating Controls > Use of line passwords.

Finding #10 The Cisco Discovery Protocol (CDP) is not disabled.

Checklist Item #28 Check that the Cisco Discovery Protocol has been disabled.

Evidence > The router configuration file failed RAT's test for Checklist Item #28. The following shows the line from the all.html report that reported this weakness:

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
7	FAIL	IOS - encrypt passwords	router_config.txt	n/a	2

Cause > The Cisco Discovery Protocol has been disabled.

Justification for this finding. What risks are the direct results of this finding? > Attackers could draw a diagram of your network from all the information given by CDP. In addition, there are known denial of service attacks that exploit this protocol.

Recommendation > Management needs to enforce formal policies and procedures that define best security practices for the use of the Cisco Discovery Protocol. If this protocol is not needed, best practice recommends implementing the following configuration setting to disable CDP:

Router(config)# no cdp run

(Akin page 65)

Costs > The only resources required for this fix is a small amount of time from the router administrator.
Compensating Controls > None.

© SANS Institute 2005, Author retains full rights.

References

Akin, Thomas. Hardening Cisco Routers. Sebastopol CA: O'Reilly Media, Inc., 2002.

CIS - Center for Internet Security. Gold Standard Benchmark for Cisco IOS, Level 1 and 2 Benchm
Version 2.1. 2003. <http://www.cisecurity.org/bench_cisco.html>.

Cisco Systems, Inc. Improving Security on Cisco Routers. 12 Oct 2004
<http://www.cisco.com/warp/public/707/21.pdf >.

Cisco Systems, Inc. Cisco IOS Interface Configuration Guide, Release 12.2. 2001.
<http://www.cisco.com/application/pdf/en/us/guest/products/ps4032/c2001/ccmigration_09186a0
f>

Cisco Systems, Inc. Cisco ISP Essentials, Essential IOS Features Every ISP Should Consider, Le
people who have been operating backbones since the early days of the Net, Version 2.9. 5 June 2
<http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip>

Cisco Systems, Inc., Cisco Security Advisories and Notices Web Page. 2005.
<http://www.cisco.com/en/US/products/products_security_advisories_listing.html>

Cobb, Chey. Network Security for Dummies. New York: Wiley Publishing, Inc., 2003.

Common Vulnerabilities and Exposures (CVE) Homepage. 2005. The MITRE Corporation. 20 Ja
<http://cve.mitre.org/>.

Eder, John. Router Security. 2005. Information Systems Audit and Control Association. Orange C
Chapter. PowerPoint presentation located at <http://www.isaca-oc.org/Archives/Router%20Securi

Gentry, Josh. Cisco Router Configuration Tutorial. 1999. <http://www.swcp.com/~jgentry/topo/cisc

Huegen, Craig. The Latest in Denial of Service Attacks: "Smurfing" Description and Information to
Effects. 2000. <http://www.pentics.net/denial-of-service/white-papers/smurf.cgi>

Internet Security Services advICE website. 2005. Internet Security Services.
<http://www.iss.net/security_center/advice/Services/Routing/Cisco/default.htm>

Internet Security Systems X-Force Home Page. 2005. Internet Security Systems. <http://xforce.is

ICAT Metabase Home Page. 2005. Computer Security Division. National Institute for Standards
Technology. 12 September 2003 <http://icat.nist.gov/icat.cfm>.

Jones, George. SANS Institute presents: Improving Router Security with RAT: The Top 10 List., SA
Wednesday Webcast, 5 November 2003. <https://www.sans.org/webcasts/show.php?webcastid=

McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed, Network Security Secrets
Fourth Edition. Berkeley: McGraw Hill/Osborne, 2003.

SANS Institute. Track 7 – Auditing Networks, Perimeters & Systems. Volume 7.1. 2004.

SANS Institute. Track 7 – Auditing Networks, Perimeters & Systems. Volume 7.2. 2004.

SANS Institute. Track 7 – Auditing Networks, Perimeters & Systems. Hands-On Exercises. SANS

SANS NewsBites Vol. 7 Num. 5. SANS Institute, 2005.

SecurityFocus Home Page. 2005. SecurityFocus. <http://www.securityfocus.com/>

Stewart, Brian. Router Audit Tool: Securing Cisco Routers Made Easy! SANS Institute 2002.
<http://www.sans.org/rr/whitepapers/networkdevs/238.php>

Tripod, Mark. Cisco Router Configuration & Troubleshooting, Second Edition. Indianapolis: New R

United States. Government Accounting Office. Accounting and Information Management Division
Information Systems Controls Audit Manual. 1999. <http://www.gao.gov/special.pubs/ai12.19.6.pd

© SANS Institute 2005

Author retains full rights.

United States. National Institute of Standards and Technology. Risk Management Guide for Inform Technology Systems, Special Publication 800-30. 2002. <http://csrc.nist.gov/publications/nistpubs 30/sp800-30.pdf>

United States. National Security Agency. Router Security Configuration Guide, Version 1.1b. 200 <http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/routers/cis_securityguides.zip>

Velte, Toby J. and Anthony T. Velte. Cisco, A Beginner's Guide, Second Edition. Berkeley: Osbor Hill, 2001.

© SANS Institute 2005, Author retains full rights.