Audit of Juniper Router: An Auditor's Perspective

Research in Audit, Measurement Practice and Control

Mary H. Foote

GSNA Practical Assignment Version 2.1, Option 1

January 31, 2003

Table of Contents

Summary

This paper outlines the audit of a Juniper router that is going to replace outdated unsupported routers on a Federal network. The Juniper router is located in a lab environment. The point of view of this paper is that of an auditor. The auditor did not have pre-existing knowledge of Juniper routers. During the audit, the auditor was given a user password without privileged access to the system. The auditor worked primarily with a system administrator and a network administrator. First the auditor did research on the router and auditing best practices. Second the auditor created an audit checklist. Third the auditor performed the audit by completing the steps and recording the results. Lastly, the auditor generated an audit report for management.

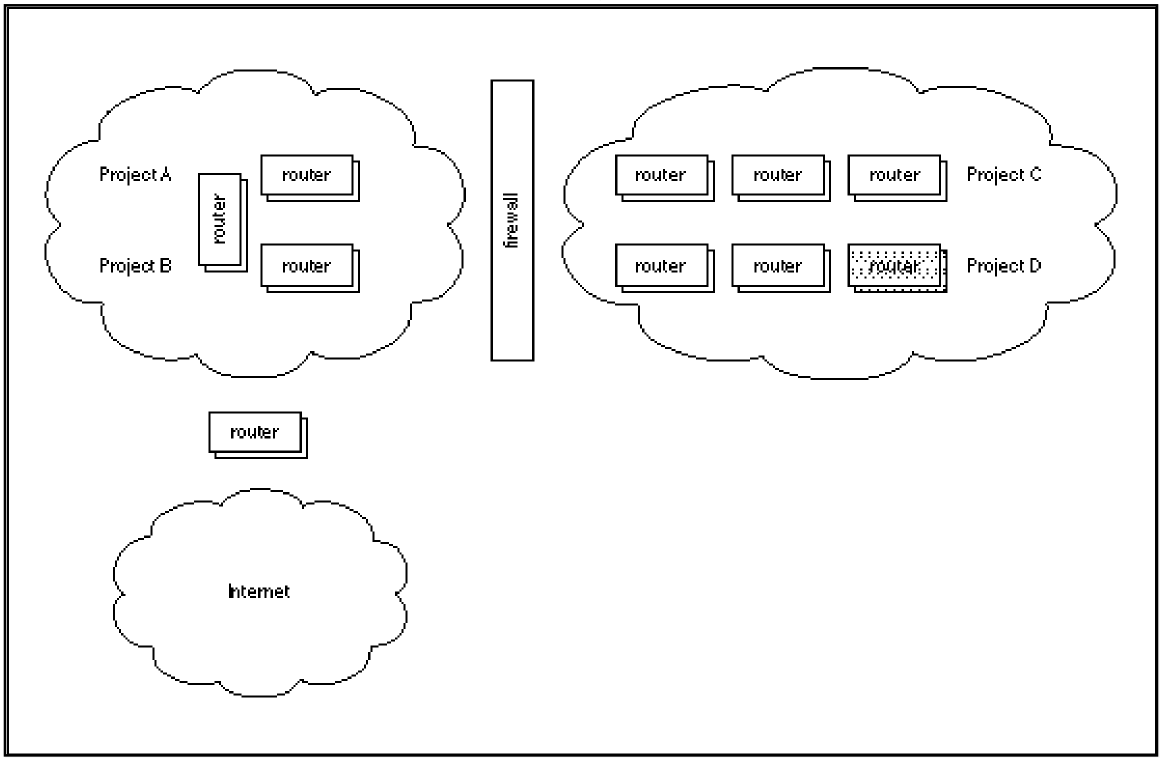
The result of the audit was that there are residual risks for the Network Security Officer to assume and conditions that need to be corrected. In spite of that, the Juniper router has passed the security steps taken and is ready to go operational on the Federal network involved. Future audits of Juniper routers should be more efficient due to the checklist created for this paper.

Assignment 1 – Research in Audit, Measurement Practice and Control

System to be audited

The system to be audited is a Juniper M5 Internet Router. The approach taken will be that of an auditor. A Juniper M5 router will be used in testing and is located in a lab on a federally owned and operated network. The routers that will go operational in the federal network after testing are Juniper M10s. The only difference between the lab router and the operational routers is the number of slots. The slots provide high-speed interfaces for networks. The router's maximum throughput is 6.4 Gbps in full duplex. The operating system is UNIX-based JUNOS Release. The Packet Forwarding Engine performs control operations in the router, which consists of hardware designed by Juniper Networks. The architecture separates control operations from packet forwarding operations. This design eliminates processing and traffic bottlenecks, which permits the router to achieve high performance rates.

The role of the router is an intermediate router in a large Federal Agency network that runs operationally 24x7. There is a firewall installed so the router does not supply the entire end-point defense. There are multiple projects within the Federal Agency using the router so it must accommodate multiple traffic flows. This router will be a border router for one project's flow into the rest of the operational network. The router tested will be implemented as part of a backbone network. Its future position in the network is shaded on the diagram below. Projects connect to that network and use its transport services. There are protections at the borders. The network has no connected workstations other than a management station in a physically controlled room.



The intended scope of this audit is to determine if the Juniper routers are safe enough to replace selected outdated Cisco and 3COM routers in the network. The audience for the audit report is the Network Security Officer (NSO) and his Deputy for the Federal Agency network involved.

Risks to the system

A threat is an event that has the potential to cause harm to a computer, network facility, or computer/communication system. Threats are generally categorized as either human threats or environmental threats. Human threats can be intentional (e.g. deliberate malicious acts) or unintentional (e.g., errors due to lack of training). Environmental threats can be natural or fabricated, (i.e., man- or machine-caused events or mechanical/structural defects). A threat cannot harm anything that has no vulnerabilities. Threat plus vulnerability generates risk.

The purpose of this audit is to find out how likely threats are to access the vulnerabilities that would generate risk. Some of the potential vulnerabilities are poor passwords, poor router configuration, changeable routing tables, weak router access control. Nessus and Internet Security Systems scanner (ISS) will be used to identify specific vulnerabilities in this router.

The control objectives are the umbrella that surround risk analysis and aid in reducing vulnerabilities. The control objectives are important since they discuss best practices. For example one of the control objectives is managing quality. As a person strives to attain the control objectives, the vulnerabilities are discovered and eliminated. There is nothing that can be done about threats. Threats are a constant presence. It is the vulnerabilities that need to be reduced to the lowest possible denominator so that risk can be reduced. Control objectives aid in the reduction of vulnerabilities that in turn reduce risk.

An overview of the security control objectives for a router are some of the high-level control objectives found in CobiT Control Objectives for Information and related Technology (COBIT®), found at http://www.isaca.org/cobit.htm. The applicable controls are found in the following table that maps the control objectives to threats and to consequences with an educated guess as to how often these would occur.

Control Objective	**Threat**	**Consequences**	**Likelihood of Occurrence**
Defining a strategic IT plan	Poor planning	Reduce the overall security of a router, lack of quality, lack of integrity, lack of efficiency	High
Defining the information architecture	Hardware failure	Lack of available information.	Medium

Control Objective	**Threat**	**Consequences**	**Likelihood of Occurrence**
Developing and maintaining procedures	Human error	Unauthorized access, exposure of sensitive data. Information theft	Medium
Managing changes	Human error	Improper function of system, information theft	Medium
Managing performance and capacity	Reduced performance	Denial of Service (DOS), session hijacking, rerouting, masquerading	Medium
Educating and training users	Human error	Unauthorized access, exposure of sensitive data. Information theft	Medium
Managing the configuration	Poor router configuration	Reduce the overall security of a router, expose internal network components to undesired traffic, make it easier for hackers to avoid detection	High
Managing problems and incidents	Hacking, Intentional harm	Make it easier for hackers to avoid detection, information theft, masquerading, DOS, exposure of sensitive data, rerouting, unauthorized access	High
Managing data	Hacking	Information theft, denial of service, rerouting	High
Auditing	Lack of auditing	Human intentional error, information theft, reduce the overall security of the router, expose internal network components to undesired traffic, make it easier for hackers to avoid detection	Medium
Managing facilities	Environmental changes	Lack of available data	Low

There will always be some residual risk. The NSO must determine if the risks that are left are acceptable. During the report phase of the audit, the consequences and likeliness of the residual risks will be presented. Since this network practices defense in depth, network security does not depend solely on the strength of this router. Some other defenses in this network are a firewall, other routers, auditing, configuration management, an Intrusion Detection System (IDS), a network manager, 24x7 personnel on watch, and specialized custom-made tools.

Current State of Practice

No current state of practice for Juniper routers was encountered. The auditor searched the web and reviewed the class work for Track 7: Auditing Networks, Perimeters, and Systems. The auditor found material about evaluating routers, evaluating systems and auditing checklists. The intent of this audit is to compare the Juniper M5 to the Cisco router information and to use UNIX and Cisco information to aid in the audit of the Juniper M5. The auditor also intends to apply best practice checklists for routers and systems to evaluate this router.

Some sources explored were:

1. The Juniper Web site http://www.juniper.net/products/
2. NSA/SNAC Router Configuration Guide, http://www.nsa.gov/snac/cisco/download.htm
3. Improving Security on Cisco Routers, http://www.cisco.com/warp/public/707/21.html
4. The SANS Router Security Policy, http://www.sans.org/newlook/resources/policies/Router_Security_Policy.pdf
5. The 'SANS 'Solaris Security: Step-by-Step' and 'Securing Linux Step-By-Step'.
6. NASA, NASA Procedures and Guidelines, NPG 2810.1, 26 August 1999,

   URL: http://nodis.gsfc.nasa.gov/library/npg_sort.cfm
6. Krishni Naidu, Cisco Checklist, SANS, URL: http://www.sans.org/SCORE/checklists/CiscoChecklist.doc
7. Cisco Systems, Cisco IOS Software Command Summary Release 11.1, San Jose, CA., Cisco Systems, Inc.

At the Juniper Web site the auditor did not find any resources to audit Juniper routers. However the web site did contain operational information about the Juniper routers. There were two references that proved to be useful.

1. Juniper Networks, Inc., JUNOS Internet Software Configuration Guide, Getting Started, Release 5, Sunnyvale, CA, Juniper Networks, Inc. 2002. URL: http://www.juniper.net/techpubs/software/junos51/swconfig51-getting-started/frameset.htm
2. Juniper Networks, Inc., JUNOS Internet Software Configuration Guide, Routing and Routing Protocols Release 5.1, Sunnyvale, CA, Juniper Networks, Inc. 2002, URL: http://www.juniper.net/techpubs/software/junos51/swconfig51-routing/frameset.htm

The National Security Agency (NSA) material was referenced in the SANS class and contained some valuable information. The NSA material had a checklist that could be used as a guide for auditing. The security information from Cisco also presented ideas that could be transformed into steps in a checklist. The SANS security policy also contained information valuable for the checklist. The information about UNIX operating systems from SANS was very helpful as the Juniper router's operating system is a hardened version of UNIX.

While reviewing the material, the auditor documented potential tests for the checklist that was compiled in Assignment 2.

Assignment 2 – Create an Audit Checklist

The NSO requested an audit of the Juniper routers in the lab to verify that they are secure enough to go operational. The purpose of the Juniper routers is to replace certain specified outdated Cisco and 3COM routers. The Juniper routers are currently in a lab environment to verify performance and compatibility with the operational network. The router is in a non-operational configuration some of the time, so some of the tests results will not mirror operations exactly. However, enough tests will be conducted to address the NSO's concerns.

Checklist

Each step in the checklist includes a reference, a control objective, the risk the step addresses, the criteria for compliance, the tests to be conducted, and a statement on the objectivity or subjectivity of the test. The Control objective is one of the objectives found in CobiT Control Objectives for Information and related Technology (COBIT®). The references are detailed in the reference section at the end of this paper.

Step 1	**Verify Router Security Plan**
Reference	NSA/SNAC Router Configuration Guide, NASA Procedures and Guidelines, NPG 2810.1.
Control Objective	Defining a strategic Information Technology (IT) plan. The purpose of this step is to verify that there is a security plan in the IT plan and that the router is following the plan.
Risk	The risk is the project won't accomplish what it wants to accomplish with the router. The router may not meet the needs of the network. Poor planning leads to poor configuration of router. There could be lack of quality, lack of integrity, lack of efficiency. If the IT plan or security plan is poorly written, the risks are good that there will be confusion about how the routers should be safely and effectively implemented.
Compliance	There is a range of conditions for this item. This is a binary step in that the system is compliant if the security plan exists. This step is also conditional in that the system is compliant if the security plan conforms to the standards for a security plan found in NPG 2810.1.
Testing	1. Locate the IT plan. 2. Review the plan and compare the plan to NPG 2810.1 Section 5 and Appendix A. 3. Document the results.
Objective/ Subjective	This test is objective in that the auditor will determine if there is a security plan. This test is subjective because the 2810.1 requirements are open to auditor interpretation as is compliance of

Step 1	**Verify Router Security Plan**
	requirements are open to auditor interpretation as is compliance of the router security plan with the requirements.

Step 2	**Verify that Simple Network Management Protocol (SNMP) has been disabled or the password has been changed.**
Reference	NSA/SNAC Router Configuration Guide, NPG 2810.1, Improving Security on Cisco Routers, The SANS Router Security Policy, Cisco Checklist.
Control Objective	Ensuring system security to safeguard information against unauthorized use, disclosure or modification, damage or loss. This step is designed to verify that SNMP, which can convey information, is not able to convey that information to unauthorized parties.
Risk	Unauthorized access by an outside party such as a hacker, exposure of sensitive data, information theft. This step is important because information about the network is very sensitive. The network strength depends on the strength of the routers in it.
Compliance	This is a binary step. The system is compliant if SNMP has been disabled or if a password checker cannot guess the password.
Testing	1. At router type in command, 'show SNMP statistics'. 2. Verify that SNMP is running on the router. 3. Run ISS against router with policy that checks for everything. 4. Generate report for services and vulnerabilities for the router. 5. Review the report. Report will state whether SNMP is present or not and if scanner guessed the SNMP password.
Objective/ Subjective	Objective

Step 3	**Verify router passwords are encrypted and hard to guess.**
Reference	NSA/SNAC Router Configuration Guide, NPG 2810.1, Improving Security on Cisco Routers, The SANS Router Security Policy, Cisco Checklist.

Step 3	**Verify router passwords are encrypted and hard to guess.**
Control Objective	Ensuring system ability to safeguard information against unauthorized use, disclosure or modification, damage or loss. This step is designed to verify that passwords cannot be guessed to help a hacker get access to the router. Poor passwords are one of the easiest ways to attack a device.
Risk	Unauthorized access by an outside party such as a hacker, exposure of sensitive data, makes it easier for hackers to avoid detection, information theft. This step is important because secure passwords in operational routers will reduce the chance of unauthorized access.
Compliance	This is a binary step. The system is compliant if the passwords are encrypted and the password cracker cannot crack the password.
Testing	1. Type in command 'show configuration' at router prompt. 2. Verify whether the passwords are encrypted or are in plain text. 3. Copy the passwords into a separate file. 4. Run crack against the password file. 'Crack -nice 10 <file name>' 5. Verify whether crack could identify the passwords. ' Reporter |more' 6. If the passwords can be cracked, ask the network administrator to change the passwords immediately.
Objective/ Subjective	Objective

Step 4	**Verify access restrictions are imposed on console, auxiliary and Virtual Terminals (VTYs)**
Reference	NSA/SNAC Router Configuration Guide, Improving Security on Cisco Routers, Cisco Checklist.

Step 4	**Verify access restrictions are imposed on console, auxiliary and VTYs**
Control Objective	Ensuring system ability to safeguard information against unauthorized use, disclosure or modification, damage or loss. This step is designed to verify that someone would not be able to gain access to

Step 4	**Verify access restrictions are imposed on console, auxiliary and VTYs**
	designed to verify that someone would not be able to gain access to the equipment.
Risk	Unauthorized access by an outside party such as a hacker. This step is very important, as the routers are placed in international locations so whether an unauthorized person can access the routers is critical to network defense.
Compliance	This is a binary step. The system is compliant if there is no access via modems, VTYs and console.
Testing	1. Determine if console and auxiliary are or can be physically attached to the router. 2. At login prompt, type in command 'show configuration'. 3. Verify that console can only be accessed by login and password. 4. Verify that it is impossible to use the auxiliary. 5. Verify how the VTYs are set up. 6. Attempt to login without using a password or use the wrong password.
Objective/ Subjective	Objective

Step 5	**Verify telnet, Secure Shell (SSH) based network protocols are present instead of rlogin.**
Reference	Improving Security on Cisco Routers, Cisco Checklist.
Control Objective	Identifying automated solutions to ensure an effective and efficient approach to satisfy the user requirements. This step is designed to verify that insecure IP protocols are not present and the protocols that are used will help protect the router, not endanger it.
Risk	Unauthorized access, exposure of sensitive data, and improper function of system, information theft. This step is important because IP-based network protocols impose more risk on system as a hacker could take advantage of telnet and rlogin, whereas it will be harder to attack if SSH is being used. As the routers are placed internationally, use of these protocols to manage the routers is mandatory. However adding IP protocols to the router adds additional IP risk.

Step 5	**Verify telnet, Secure Shell (SSH) based network protocols are present instead of rlogin.**
Compliance	This is a binary test. The system is compliant if rlogin is not present and if telnet and SSH are present.
Testing	1. At a UNIX console in the lab, telnet and SSH into the router. 2. Verify whether successful or unsuccessful. 3. At the router try to rlogin out of the router. 4. Verify whether successful or unsuccessful. 5. At command prompt, type 'show configuration' to verify which services are allowed
Objective/ Subjective	Objective

Step 6	**Verify physical security.**
Reference	NPG 2810.1, Improving Security on Cisco Routers
Control Objective	Managing facilities to provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards. This step is to verify that the physical controls prevent unauthorized personnel from getting access to the device.
Risk	Router may be physically taken over or damaged. Some routers are in international locations so exact location must be protected and locked up so that personnel cannot inadvertently or purposely harm the equipment.
Compliance	There is a range of conditions for this item. There may be various types of locks, and routers may be isolated or put with certain other equipment. The step is compliant if there are controlled keycards and/or locks on doors to the rooms where routers are kept. The step is compliant if these controlled locks and keys are distributed to less than 10 people.
Testing	Follow steps in physical audit checklist provided as Appendix A.
Objective/ Subjective	Subjective: There are a variety of situations and the situations are open to interpretation whether the physical location is satisfactory.

Step 7	**Verify warning banner on router (telnet, ftp)**
Reference	NPG 2810.1, Improving Security on Cisco Routers, SANS ‘Solaris Security: Step-by-Step', Cisco Checklist.
Control Objective	Communicating management aims and direction to ensure user awareness and understanding of those aims; ensuring compliance with external requirements to meet legal regulatory and contractual obligations; and educating and training users to ensure that users are aware of the risks and responsibilities involved. This step is to verify that a warning banner is there so that if the device is hacked, it is possible to prosecute the violator.
Risk	Federal Agency cannot prosecute hacker without a warning banner therefore a warning banner must be on every Federal IT device.
Compliance	This is a binary step. The system is compliant if the warning banner is present.
Testing	1. Log on to router – Is the banner present? If no console, 2. Telnet into router – Is the banner present? 3. Ftp into router – Is the banner present? 4. At router prompt, type in command ‘show configuration’ and verify that banner will be displayed when router is brought up.
Objective/ Subjective	Objective

Step 8	**Verify information is being logged.**
Reference	NPG 2810.1, Improving Security on Cisco Routers, SANS ‘Solaris Security: Step-by-Step’, NSA/SNAC Router Configuration Guide, Cisco Checklist.
Control Objective	Managing data and managing operations. This step is designed to verify that if a hacker attacks this device, personnel will be able to retrace the hacker’s steps by reading the logs. Hopefully this will help investigators find and remedy the vulnerability used to get in and may help prosecute the attacker.

Step 8	**Verify information is being logged.**
Risk	Lack of information in case of unauthorized access. If there were no logging, there would be no record to help an auditor figure out what happened or when it happened.
Compliance	The system is compliant if the router is collecting logs. The system is compliant if the journals contain access failures to systems, files objects and resources. The system is compliant if system privilege use (root access) is logged.
Testing	1. Log into router and type command 'show configuration'. 2. Verify syslog is running. 3. Type command, 'show log' to verify log files are accumulating. 4. Review ISS and Nessus report to verify that syslog is running. 5. Type command, "show log <filename>", to view logs files.
Objective/ Subjective	Objective.

Step 9	**Verify that logs are checked regularly.**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide, and Cisco Checklist.
Control Objective	Managing data and managing operations. This step is designed to verify that if a hacker attacks this device, personnel are reading the log files and will find out and attempt to stop the intrusion. Hopefully this will help find and remedy the vulnerability used to get in and may help prosecute the attacker.
Risk	Operational personnel won't know what is happening to the router if logs are not checked regularly.
Compliance	This is a binary step. The system is compliant if the logs are reviewed daily.
Testing	1. Interview network administrator. Verify how logs are checked. 2. Interview system administrator. Verify how logs are checked.
Objective/ Subjective	Subjective. Determination of whether the logs are reviewed daily depends on interviews with other people.

Step 10	**Ensure that router's time of day is set accurately and connected to Network Time Protocol (ntp).**
Reference	Improving Security on Cisco Routers, SANS 'Solaris Security: Step-by-Step', NSA/SNAC Router Configuration Guide, Cisco Checklist.
Control Objective	Managing data. If the time is different on different routers, it will be difficult to retrace a hacker's steps from device to device in the log files. Inaccurate times between devices will also make persecution in court difficult or impossible.
Risk	If the times on the routers are not correct, there is a risk that an auditor cannot follow the times of an incident and figure out what happened. The times on the routers need to be synchronized with each other so the logs are synchronized.
Compliance	This is a binary step. The system is compliant if the time is synchronized with ntp.
Testing	1. At login prompt, type command 'show configuration'. 2. Verify command for ntp in configuration file. 3. At login prompt, type command 'show ntp status'. 4. At login prompt, type command 'show ntp associations'. 5. Run ISS and Nessus to verify that ntp is running.
Objective/ Subjective	Objective

Step 11	**Verify anti-spoofing has been applied with access lists**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide, and Cisco Checklist.
Control Objective	Managing quality, Ensuring systems security. This step is designed to prevent an attacker from being able to fool the router and send information from an outside host that the router thinks is an inside host.
Risk	If the router can be spoofed, information could be given out or access could be given to an unauthorized user.

Step 11	**Verify anti-spoofing has been applied with access lists**
Compliance	This is a binary step. The system is compliant if anti-spoofing commands are added or present by default.
Testing	1. Log on to the router. 2. At the prompt, type command, 'show configuration.' 3. Verify that the internal IP address range is prohibited to come in from outside the router.
Objective/ Subjective	Objective

Step 12	**Verify controlled directed broadcasts.**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide
Control Objective	Managing quality, Ensuring systems security. This step is designed to help the router resist a DOS attack, which could shut down or disable the router.
Risk	Directed broadcasts can take down a router.
Compliance	This is a binary step. The system is compliant if there are no IP directed broadcasts permitted by command or by default.
Testing	1. Set up lab test with host and Juniper router. 2. Ping the broadcast address of the Juniper router subnet. (Pings for the entire Juniper subnet should hit the router.) 3. Verify that router handles the pings either by not forwarding pings or not responding. 4. Set up lab with host, Juniper router, and Cisco router. 5. Ping the broadcast address of the Cisco router subnet. (Pings for the entire Cisco subnet should hit the router.)
Objective/ Subjective	Objective

Step 13	**Determine which services are running. Verify all unneeded services are disabled.**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide, SANS 'Solaris Security: Step-by-Step', Cisco Checklist.
Control Objective	Managing quality, Ensuring systems security. This step is to verify that needed services are in fact running and to verify that extra services are not running. Extra services make it easier for an attack as there are unnecessary services running and extra ports open.
Risk	Information theft, DOS, exposure of sensitive data. Unneeded services open ports to compromise by hackers. This is an extremely important step.
Compliance	This is a conditional step. The part of the step that determines which services are running is binary. Finding out which services are needed includes conversations with the network manager and NSO and may be conditional.

Step 13	**Determine which services are running. Verify all unneeded services are disabled.**
Testing	1. Run (Network Mapper) nmap against router. Enter command 'nmap -O -v <router IP address>'. Display output. 2. Run ISS against router and display services running. 3. Interview network administrator to explain why questionable services are running on router.
Objective/ Subjective	Objective and Subjective. Finding the enabled services is objective. Determining what are unneeded services depends on the traffic needed. Discussions with network administrators may be subject to interpretation.

Step 14	**Discover vulnerabilities present on router.**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide, SANS 'Solaris Security: Step-by-Step', Cisco Checklist.
Control	Managing quality, Ensuring systems security. This step is to verify

Step 14	**Discover vulnerabilities present on router.**
Objective	that known vulnerabilities are closed and not accessible to hackers to exploit.
Risk	Information theft, DOS, exposure of sensitive data. Uncovered vulnerabilities make it easier for hackers to compromise the router.
Compliance	This is a binary step to find the vulnerabilities that are present. This is also a conditional step because certain vulnerabilities may be justified. The system is compliant if there are no vulnerabilities present or if the vulnerabilities are justified by the needs of the network.
Testing	1. Ping the router from the lab. 2. Bring up ISS and select a session key and hit the next button. 3. Select a policy and hit the next button. 4. Put in the information to configure the session. 5. Specify the hosts by accepting the default to ping the hosts in the session key. 6. Pull down the scan menu and start the scan. 7. At the end of the scan generate reports for services and vulnerabilities. 8. Type in command at the UNIX host 'nessus' 9. Log in to Nessus and click on log in button. 10. At the Nessus set-up screen select 'Enable all but the dangerous plug-ins'. 11. Select the scan options screen and change port range to 65,535. 12. Select the target selection tab and put in Juniper IP address. 13. Select the 'Start the Scan' button. 14. Run the scan and generate the report. 15. Compare Nessus and ISS report. 16. Interview network administrator about vulnerabilities found.
Objective/ Subjective	Objective and Subjective. Finding the vulnerabilities is objective. Exactly eliminating all vulnerabilities depends on the traffic needed and discussions with network administrators and the NSO. Discussions with network administrators may be subject to interpretation.

Step 15	**Verify patches are up to date.**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide, SANS ‘Solaris Security: Step-by-Step', Cisco Checklist.
Control Objective	Acquiring and maintaining technology infrastructure. This step is to verify that known vulnerabilities are closed and not accessible to hackers to exploit.
Risk	Information theft, DOS, exposure of sensitive data. Unpatched routers create opportunities for unauthorized access.
Compliance	This is a binary step. The system is compliant if the auditor goes to CERT, obtains any advisories that are present, and then verifies that the patches addressing the advisories have been installed on the router.
Testing	1. Go to CERT and Juniper Networks web sites and read advisories for Juniper routers. 2. Log onto router and type command ‘show version’ and verify patches have been installed. 3. If a patch has not been installed, verify that operational personnel did an evaluation of patch, and discuss why the patch was not installed.
Objective/ Subjective	Objective and Subjective. If a patch has been installed, this is an objective test. If it has not been installed, an evaluation of why it wasn’t installed is necessary. Interviews may be required.

Step 16	**Verify that no local user accounts are present on router.**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide,
Control Objective	Managing quality, Ensuring systems security. This step is to verify that there are no unnecessary accounts on the router. Local accounts cannot be taken over by someone experimenting or trying to harm the router if they do not exist.
Risk	Local user accounts create logon opportunities for unauthorized access.

Step 16	**Verify that no local user accounts are present on router.**
Compliance	This is a binary step. The system is compliant if there are no local user accounts.
Testing	1. At the prompt, type in command 'show configuration'. 2. Examine accounts to verify no local user accounts.
Objective/ Subjective	Objective

Step 17	**Verify web server, Domain Name Service (DNS), Network File Service (NFS), sendmail software are removed.**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide
Control Objective	Managing quality, Ensuring systems security. This step is to verify that there are no unnecessary applications on the router.
Risk	Information theft, exposure of sensitive data. These applications are not used in routing and present unneeded chances to attack the router.
Compliance	This is a binary step. The system is compliant if DNS, NFS, web servers and sendmail are not present. (Auditor's note: Sometimes routers are managed through web servers, but not on this network.)
Testing	1. Run nmap and verify ports are not open. Enter command 'nmap -O -v <router IP address>. 2. Run ISS and Nessus (see step 14) and verify DNS, NFS, or sendmail are not present on router.
Objective/ Subjective	Objective

Step 18	**Verify unused interfaces are disabled.**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide.

Control Objective	Managing quality, Ensuring systems security. This step is to verify that there are no unnecessary interfaces on the router.
Risk	Information theft, exposure of sensitive data. If an interface is not being used there is no need for it to be enabled. Unused interfaces open interfaces open opportunities for unauthorized access.
Compliance	This is a binary step. The system is compliant if unused interfaces are disabled.
Testing	1. At prompt, type command 'show interfaces'. 2. Verify unused interfaces are disabled. 3. Set up test with host, Juniper router and Cisco router. 4. Send command, 'ping <interface IP address> with interface enabled. The router should respond. 5. Disable interface at router. 6. Send command 'ping <interface IP address>' with interface disabled. The router should not respond.
Objective/ Subjective	Objective

Step 19	**Verify the ICMP traffic is blocked at the router.**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide, and Cisco Checklist.
Control Objective	Managing data, Managing operations. This step is designed to verify that a hacker is not given tools with which to explore the network. Pings, time exceeded and unreachable messages all help a hacker determine which hosts are up and how the hosts are configured on a network.
Risk	The risk is loss of sensitive information and that the hacker will understand the network configuration.
Compliance	This is binary. The system is compliant if incoming and outgoing echo requests, time exceeded, unreachable messages, ICMO redirects are blocked at the router.
Testing	1. At prompt, type in 'show configuration.' 2. Verify ICMP is being blocked at router.

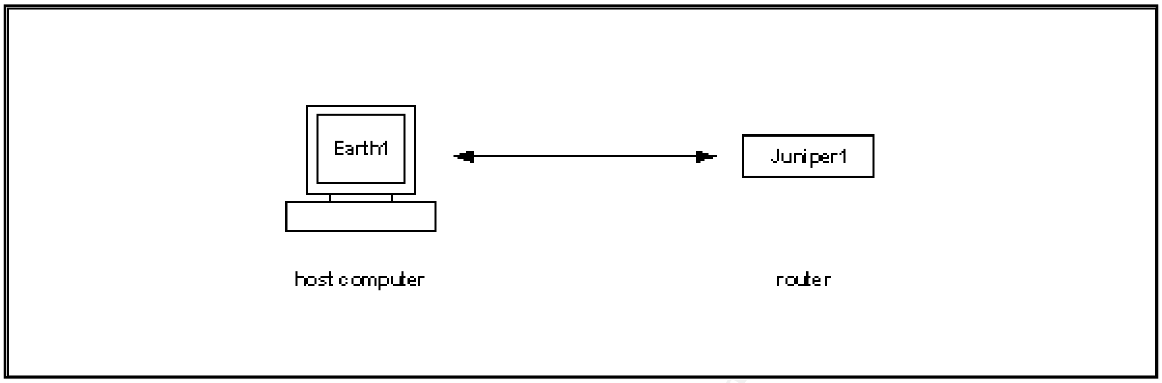
	3. Run test with host, Juniper router and Cisco router. 4. Send command, ‘ping < router IP address>’ with no access list. 5. Verify that pings are successful 6. Apply access list. 7. Send command, ‘ping <Cisco router IP address>’ with access list applied. 8. Verify that pings are not successful.
Objective/ Subjective	Objective

Step 20	**Verify the access lists block reserved and inappropriate addresses.**
Reference	Improving Security on Cisco Routers, NSA/SNAC Router Configuration Guide, and Cisco Checklist.
Control Objective	Managing data, Managing operations. There are private addresses that should not be routed on the network, such as the 192.168.0.0 and 10.0.0.0 networks. This step verifies that these addresses are being blocked. If they are blocked, they will not leak into the network and confuse the data paths.
Risk	Unroutable and inappropriate data will not be routed into the network.
Compliance	This is binary. The system is compliant if reserved and inappropriate addresses are blocked at the router by command or by default.
Testing	1. At prompt, type is ‘show configuration’. 2. Verify that reserved and inappropriate addresses are blocked. 3. Run test with host, Juniper router and Cisco router. 4. Send command, ‘ping host’ with no access list. 5. Verify that pings are successful. 6. Apply access list with inappropriate address. 7. Send command, ‘ping host’ with access list applied. 8. Verify that pings are not successful.
Objective/ Subjective	Objective

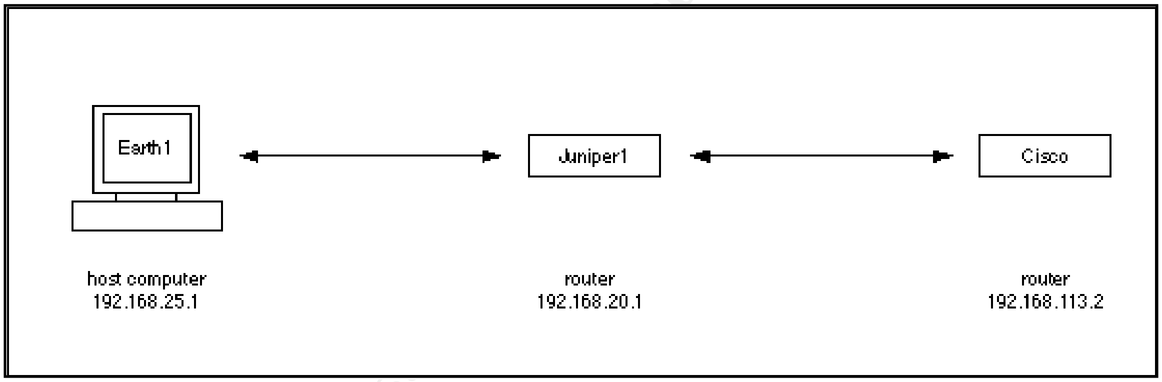
Subjective	

Assignment 3 – Audit Evidence

This section contains evidence discovered while conducting the checklist steps outlined in Assignment 2. The items discussed below represent the most important steps in the audit. They were considered to be the most important steps because they contained the potential for the most serious vulnerabilities. The tests were set up so that Earth1, a Solaris host, was used to connect with the Juniper router.



However there were a few tests (i.e.18-20) where the test scenario is depicted below. A host (Earth1) was connected to the Juniper that was connected to a Cisco router.



The results will be demonstrated as far as possible, given the sensitivity of the actual systems and the proprietary nature of the results.

Step #1 – Verify Router security plan.

After examining NPG 2810.1 and the Federal accepted security plan template, the federal network security plan did not conform to NPG 2810.1 or to the Federal Agency accepted security plan template. The routers were only mentioned briefly and there were no router policies in the plan. (Auditor's note: a checklist was used but it was not solely the auditor's work so was not included in this document.)

The non-conformities are as follows:

1. The system identification is weak and too general to be useful.
2. There is a weak general description or purpose for the specific elements.
3. Network access and connectivity are not discussed or depicted.

4. System software and versions and application software running on the system are not discussed.
5. Critical processing periods are not discussed.
6. Information contacts are out of date.
7. Discussion of impact of loss of system and/or data description is weak.
8. The security plan does not indicate the possible effects the risks could have.
9. The plan does a poor job of documenting any baseline requirements that are not being met and does not indicate very well why the requirement is not being met.
10. The plan does not describe how security incidents will be reported through the management chain and to the local IT Security Manager.

Step #2 - Verify that SNMP has been disabled or the password has been changed.

At the router, typed in the command, 'show snmp statistics' with the following results.

```
SNMP statistics:
  Input:
    Packets: 213544, Bad versions: 0, Bad community names: 213524,
    Bad community uses: 0, ASN parse errors: 20,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 0, Total set varbinds: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops 0
  Output:
    Packets: 143166, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 143166
```

These results verified that SNMP was active.

The ISS commercial scanner (see step #14) demonstrated which services were running on the router. SNMP was one of the services found. (See Appendix B.)

ISS also verified which vulnerabilities were encountered. ISS did not identify SNMP as a vulnerability and ISS did not guess the SNMP password. Identifying SNMP as a vulnerability and trying to guess the SNMP password is one of the checks that ISS performs. This lack of evidence provides the result that the SNMP password was changed to a strong password.

Step #3 - Verify router passwords are encrypted and hard to guess.

After entering the command ' show configuration' the following appeared as part of that command.

```
ports {
  console type vt100;
}
root-authentication {
  encrypted-password "$1$8V4sZ$R9leUqhRHk3IryOF9x56R/"; # SECRET-DATA
```

```
}
login {
  message message
"####################################################################
#\nWARNING! This is a US Government computer.  This system\nis for
the use of authorized users only.  By accessing and\nusing the
computer system you are consenting to system monitoring\nincluding
the monitoring of keystrokes.\nUnauthorized use of, or access to,
this computer system\nmay subject you to disciplinary action and
criminal
prosecution.\n########################################################
##############";

  class john {
      permissions all;
  }
  class engr {
      idle-timeout 10;
      permissions all;
  }
  class ops {
      permissions [ interface network routing trace view firewall ];
  }
  class superuser-local;
  user mcc {
      uid 2001;
      class ops;
      authentication {
          encrypted-password "$1$uHZ2.$8LSO8GF18fbNL9XYxo08K."; #
SECRET-DATA
      }
  }
  user john {
      uid 2003;
      class john;
      authentication {
          encrypted-password "$1$QkMsZ$BB37Su.6hlGUvAx6CWXab1"; #
SESRET-DATA
      }
  }
  user karen {
      full-name "KAREN P";
      uid 2002;
      class superuser;
      authentication {
          encrypted-password "$1$IGl.6$S6M9wSSqzuGjgktzu5kEu."; #
SECRET-DATA
     }
  }
  user engr{
      uid 2000;
      class -engr
```

```
       authentication {
           encrypted-password "$1$UoU2.$EVDdo3a6PPM7J2JfafIlB/"; #
 SECRET-DATA
    }
  }
}”
```

This command verified that the passwords were kept in an encrypted form. Next the passwords were copied into a separate file and a system administrator ran ‘crack’ to attempt to guess the passwords. Mila was the name of the file.

```
 cat mila
 rout1:$1$8V4sZ$R9leUqhRHk3IryOF9x56R/:101:10:router pass 1:/:/bin/csh
 rout2:$1$uHZ2.$8LSO8GF18fbNL9XYxo08K.:102:10:router pass 2:/:/bin/csh
 rout3:$1$QkMsZ$BB37Su.6hlGUvAx6CWXab1:103:10:router pass 3:/:/bin/csh
 rout4:$1$IGl.6$S6M9wSSqzuGjgktzu5kEu.:104:10:router pass 4:/:/bin/csh
 rout5:$1$UoU2.$EVDdo3a6PPM7J2JfafIlB/:105:10:router pass 5:/:/bin/csh
 # cd run
 # rm D* E* K*
```

‘Crack’ was then started.

```
 Crack -nice 10 mila
 Crack 5.0a: The Password Cracker.
 (c) Alec Muffett, 1991, 1992, 1993, 1994, 1995, 1996
 System: SunOS earth1 5.6 Generic_105181-33 sun4u sparc SUNW,Ultra-
 5_10
 Home: /home/mcnally/c50a
 Invoked: Crack -nice 10 mila
 Option: -nice enabled
 Stamp: sunos-5-sparc

 Crack: making utilities in run/bin/sunos-5-sparc
 find . -name "*~" -print | xargs -n50 rm -f
 ( cd src; for dir in * ; do ( cd $dir ; make clean ) ; done )
 rm -f dawglib.o debug.o rules.o stringlib.o *~
 /bin/rm -f *.o tags core rpw destest des speed libdes.a .nfs* *.old \
 *.bak destest rpw des speed
 rm -f *.o *~
 `../../run/bin/sunos-5-sparc/libc5.a' is up to date.
 all made in util
 Crack: The dictionaries seem up to date...
 Crack: Sorting out and merging feedback, please be patient...
 Crack: Merging password files...
 cat: cannot open run/F-merged
 Crack: Creating gecos-derived dictionaries
 mkgecosd: making non-permuted words dictionary
 mkgecosd: making permuted words dictionary
 Crack: launching: cracker -kill run/Kearth1.6589  -nice 10
   Done
```

‘Crack’ was confirmed to be running.

```
 ps -ef |grep crack
```

```
mcnally  6660   1  0 11:25:00 pts/2    0:00 cracker -kill
run/Kearth1.6589 -nice 10
```

When ‘crack’ was finished, the auditor printed out the report to verify that the passwords were not guessed.

```
Reporter |more
---- passwords cracked as of Mon Nov 25 15:57:13 EST 2002 ----

---- errors and warnings ----

E:1038241500:StoreDataHook: invalid ciphertext: rout1
$1$8V4sZ$R9leUqhRHk3IryOF9x56R/
E:1038241500:StoreDataHook: invalid ciphertext: rout2
$1$uHZ2.$8LSO8GF18fbNL9XYxo08K.
E:1038241500:StoreDataHook: invalid ciphertext: rout3
$1$QkMsZ$BB37Su.6hlGUvAx6CWXab1
E:1038241500:StoreDataHook: invalid ciphertext: rout4
$1$IGl.6$S6M9wSSqzuGjgktzu5kEu.
E:1038241500:StoreDataHook: invalid ciphertext: rout5
$1$UoU2.$EVDdo3a6PPM7J2JfafIlB/
E:1038241500:StoreDataHook: wg='rout1 router pass 1' un='rout1'
cm='router pass
1 [mila /bin/csh]' ct='$1$8V4sZ$R9leUqhRHk3IryOF9x56R/' sk='$1'
E:1038241500:StoreDataHook: wg='rout2 router pass 2' un='rout2'
cm='router pass
2 [mila /bin/csh ]' ct='$1$uHZ2.$8LSO8GF18fbNL9XYxo08K.' sk='$1'
E:1038241500:StoreDataHook: wg='rout3 router pass 3' un='rout3'
cm='router pass
3 [mila /bin/csh]' ct='$1$QkMsZ$BB37Su.6hlGUvAx6CWXab1' sk='$1'
E:1038241500:StoreDataHook: wg='rout4 router pass 4' un='rout4'
cm='router pass
4 [mila /bin/csh]' ct='$1$IGl.6$S6M9wSSqzuGjgktzu5kEu.' sk='$1'
E:1038241500:StoreDataHook: wg='rout5 router pass 5' un='rout5'
cm='router pass
5 [mila /bin/csh]' ct='$1$UoU2.$EVDdo3a6PPM7J2JfafIlB/' sk='$1'

---- done ----
```

Verified that ‘crack’ was not still running and the auditor had the final results.

```
earth1% ps -ef |grep crack
earth1%
```

Running ‘crack’ verified that the passwords could not be guessed. The Juniper router has two authentication methods that the user can use to access the router. The user can use SSH or an MD5 password. If the user enters a plain-text password, the Juniper software encrypts the password using MD5-style encryption before entering it into the password database.

Step #4 - Verify access restrictions are imposed on console, auxiliary, VTYs.

Physical examination encountered the fact that there was no console or auxiliary attached to the router however, there was a physical capability to attach a console and an auxiliary.

Upon entering the command, 'show configuration' the console was verified to be controlled by a password. Juniper's software does not identify the console type by default so the console was configured to be vt100. By default the Juniper router's auxiliary port is disabled. It had never been configured on this router so it did not exist in the router or the router's configuration.

```
"system {
    host-name lab-door2;
    time-zone America/Detroit;
    ports {
        console type vt100;
    }
    root-authentication {
        encrypted-password "$1$8V4sZ$R9leUqhRHk3IryOF9x56R/"; #
SECRET-DATA
    }"
```

The Juniper is a UNIX box. As such, it does not have VTYs in the same way as the Cisco router. Each user has to authenticate with a user password. There are user definitions and classes on the router. Each class defines what the user can have access to. There are identifiers that are associated with the user account name. The system administrator either assigns the identifier or the system automatically assigns one. The identifiers must be in the range between 100 through 64000 and must be unique within the router. There essentially is no limit to the users on a Juniper router.

There are 4 classes set up on the router.

```
        class john {
                permissions all;
            }
            class engr {
                idle-timeout 10;
                permissions all;
            }
            class ops{
                permissions [ interface network routing trace view
firewall ];
            }
            class superuser-local;
```

The network manager set up the class 'john' to allow himself the capability to completely test the router. The rest of the classes, including the superuser class, were set up for additional testing of the future operational configuration.

The auditor attempted to login without using a password, by entering a user name without a password and with a wrong password.

```
login: karen
```

```
Password:
Login incorrect
login: john
Password:
Login incorrect
login: karen
Password:
Login incorrect
login: Karen
Password:
```

Step #5 - Verify telnet, SSH based network protocols are present instead of rlogin.

The auditor attempted to telnet to the router from the lab with the following results.

```
earth1% telnet Juniper1
Trying 192.168.20.1...
Connected to juniper1.
Escape character is '^]'.
#####################################################################
WARNING! This is a US Government computer.  This system
is for the use of authorized users only.  By accessing and
using the computer system you are consenting to system monitoring
including the monitoring of keystrokes.
Unauthorized use of, or access to, this computer system
may subject you to disciplinary action and criminal prosecution.
#####################################################################
lab-door2 (ttyp0)

login: karen
Password:
Last login: Sun Nov 24 13:25:55 from 192.168.20.34

--- JUNOS 5.1R2.4 built 2001-12-11 02:11:09 UTC
 karen@lab-door2>
```

This verified that is was possible to telnet to the router.

The auditor attempted to rlogin to the router with the following results.

```
earth1% rlogin Juniper1
juniper1: Connection refused
```

This verified that rlogin was not allowed on the router.

The auditor attempted to rlogin from the router.

```
karen@lab-door2> rlogin
                ^
unknown command.
```

This verified that the router did not allow rlogin.

When the auditor entered the command ‘show configuration’ the following appeared as part of that command.

```
services {
        ssh;
        telnet;
    }
```

This verified that only SSH and telnet are allowed to the router.

The auditor used SSH to connect to router, verifying the SSH service on the router.

```
ssh 192.168.20.1
karen@192.168.20.1's password:
Last login: Sun Dec  1 13:44:00 2002 from 192.168.20.34
--- JUNOS 5.1R2.4 built 2001-12-11 02:11:09 UTC
```

Step #6 - Verify physical security.

Completed the physical audit checklist with the following results.

Physical Audit Checklist

Item	Comments
Are there guards?	There are guards at the gate and guards randomly patrolling the facility.
Are there key card readers?	Key card readers to access the building and access the room
Are there cipher locks?	No
Are there key locks?	No
If key locks, do the keys work on more than one door?	
Are there drop ceilings?	Yes
Are there raised floors?	Yes, but room is in basement so there is cement under the raised floors.
Does the room have windows?	No
Does the door to room have a window?	No
Is there any type of sensor detectors?	No
Is networking hubs, switches, routers, etc., locked in a closet?	No, however the test lab where they are located has a keycard.
Are network cables labeled?	Yes
Is the wiring protected or exposed?	Wiring is protected.

Item	Comments
Are there other projects equipment in the same closet?	No all the lab equipment belongs to the same project.
How many other projects have access to closet?	
Is the facility manned 24x7?	No
If not, what hours is it manned?	8-5
Do they require non-badged people to be escorted?	Yes
Are there dial-in modem interfaces?	No
Do they use Uninterrupted Power Supplies (UPS)?	Yes

Step #8 - Verify information is being logged.

The auditor verified that the syslog was set up in the configuration file on the router by entering the command 'show configuration.' The following appeared as part of that command.

```
.syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
            archive size 100m files 10;
        }
    }
```

The auditor entered the command, 'show log' with the following results, verifying that logs are being collected regularly.

```
karen@lab-door2> show log
total 345344
-rw-r--r--  1 root  bin       41028 Dec 12  2001 access.aprobed
-rw-r--r--  1 root  bin      211471 Dec 12  2001 access.dcd
-rw-r--r--  1 root  bin      183241 Dec 12  2001 access.sampled
-rw-r--r--  1 root  bin           0 Jun 20  2001 aprobed
-rw-r--r--  1 root  bin       20090 Nov 18 15:06 apsd
-rw-r--r--  1 root  bin     1439808 Oct 11 11:00 chassisd
-rw-r--r--  1 root  bin         210 Nov 18 15:51 commits
-rw-r--r--  1 root  bin        5663 Nov 18 15:06 cosd
-rw-r--r--  1 root  bin       26152 Nov 18 15:06 dcd
```

```
-rw-r--r--  1 root  bin        3384 Oct 10 09:39 ilmid
-rw-r--r--  1 root  bin        1058 Dec 12  2001 install
-rw-rw-r--  1 bin   bin     2573136 Nov 24 16:10 lastlog
-rw-rw-r--  1 bin   bin           0 May 29  2001 lpd-errs
-rw-rw-r--  1 bin   bin           0 May 29  2001 maillog
-rw-r--r--  1 root  bin        2255 Nov  8  2001 mastership
-rw-r-----  1 root  wheel  76989633 Nov 24 16:10 messages
-rw-r-----  1 root  wheel      6100 Dec 10  2001 messages.0.gz
-rw-r-----  1 root  wheel     12169 Dec 10  2001 messages.1.gz
-rw-r-----  1 root  wheel      4169 Sep 10  2001 messages.2.gz
-rw-r-----  1 root  wheel      3633 Sep  9  2001 messages.3.gz
-rw-r-----  1 root  wheel      3658 Sep  8  2001 messages.4.gz
-rw-r-----  1 root  wheel      8633 Sep  8  2001 messages.5.gz
-rw-r--r--  1 root  bin        8156 Nov 18 15:06 mib2d
-rw-r-----  1 root  bin       35488 Dec 12  2001 ospf-trace
-rw-r--r--  1 root  bin           0 Dec 12  2001 pccardd.debug
-rw-------  1 bin   bin           0 May 29  2001 ppp.log
-rw-r--r--  1 root  bin        3701 Nov 18 15:06 rmopd
-rw-r-----  1 root  bin       48802 Nov 18 15:06 sampled
-rw-r--r--  1 root  bin           0 May 29  2001 sendmail.st
-rw-------  1 bin   bin           0 May 29  2001 slip.log
-rw-r--r--  1 root  bin        1475 Jun 20  2001 snapshot
-rw-r--r--  1 root  bin        6650 Nov 18 15:06 snmpd
-rw-r-----  1 root  bin      387550 Nov 24 16:10 trace-fednet-bgp
-rw-r-----  1 root  bin    10485828 Nov 24 12:26 trace-fednet-bgp.0
-rw-r-----  1 root  bin    10485882 Nov 20 07:22 trace-fednet-bgp.1
-rw-r-----  1 root  bin    10485825 Nov 16 02:05 trace-fednet-bgp.2
-rw-r-----  1 root  bin    10485844 Nov 11 20:49 trace-fednet-bgp.3
-rw-r-----  1 root  bin    10485746 Nov  7 15:32 trace-fednet-bgp.4
-rw-r-----  1 root  bin    10485780 Nov  3 10:16 trace-fednet-bgp.5
-rw-r-----  1 root  bin    10485854 Oct 30 05:00 trace-fednet-bgp.6
-rw-r-----  1 root  bin    10485821 Oct 26 00:44 trace-fednet-bgp.7
-rw-r-----  1 root  bin    10485873 Oct 21 19:27 trace-fednet-bgp.8
-rw-r-----  1 root  bin       81769 Nov  8  2001 trace-ospf
-rw-r-----  1 root  bin      131179 Nov  8  2001 trace-ospf.0
-rw-r-----  1 root  bin      131181 Nov  8  2001 trace-ospf.1
-rw-r-----  1 root  bin      131178 Nov  8  2001 trace-ospf.2
-rw-r-----  1 root  bin      131178 Nov  8  2001 trace-ospf.3
-rw-r--r--  1 root  bin           0 Dec 12  2001 utmp
-rw-r--r--  1 root  bin        8568 Nov 18 15:06 vrrpd
-rw-rw-r--  1 bin   bin     2003344 Nov 24 16:10 wtmp
```

The commercial scanner ISS confirmed that syslog was running. (See Appendix B.)

The auditor entered the command ‘show log <filename>’ to view the log file. In this case, ‘show log messages’ to view the message log file.

```
Dec  5 12:00:00 lab-door2 newsyslog[3768]: logfile turned over
Dec  5 12:00:29 lab-door2 snmpd[588]: SNMPD_AUTH_FAILURE:
192.168.20.1: not authorized to use community karenmon
Dec  5 12:00:29 lab-door2 snmpd[588]: SNMP_TRAP_AUTH_FAILURE: SNMP
trap: authentication failure
```

```
Dec  5 12:00:29 lab-door2 snmpd[588]: SNMPD_DEBUG: 192.168.20.1:
incoming packet to 192.168.20.1 failed input processing (code 1)
Dec  5 12:00:29 lab-door2 snmpd[588]: SNMPD_AUTH_FAILURE:
192.168.20.1: not authorized to use community karenmon
Dec  5 12:00:29 lab-door2 snmpd[588]: SNMPD_DEBUG: 192.168.20.1:
incoming packet to 192.168.20.1 failed input processing (code 1)
Dec  5 12:00:30 lab-door2 snmpd[588]: SNMPD_AUTH_FAILURE:
192.168.20.1: not authorized to use community karenmon
Dec  5 12:00:30 lab-door2 snmpd[588]: SNMPD_DEBUG: 192.168.20.1:
incoming packet to 192.168.20.1 failed input processing (code 1)
Dec  5 12:00:30 lab-door2 snmpd[588]: SNMPD_AUTH_FAILURE:
192.168.20.1: not authorized to use community karenmon
Dec  5 12:00:30 lab-door2 snmpd[588]: SNMPD_DEBUG: 192.168.20.1:
incoming packet to 192.168.20.1 failed input processing (code 1)
```

Step #13 - Determine which services are running. Verify all unneeded services are disabled.

The auditor ran nmap to determine which services are running.

```
nmap -O -v 192.168.20.1
 Starting nmap V. 2.54BETA36 ( www.insecure.org/nmap/ )
No tcp,udp, or ICMP scantype specified, assuming vanilla tcp
connect() scan. Use -sP if you really don't want to portscan (and
just want to see what hosts are up).
Host juniper1 (192.168.20.1) appears to be up ... good.
Initiating Connect() Scan against juniper1 (192.168.20.1)
Adding open port 22/tcp
Adding open port 179/tcp
Adding open port 23/tcp
The Connect() Scan took 3 seconds to scan 2558 ports.
For OSScan assuming that port 22 is open and port 1 is closed and
neither are firewalled
Interesting ports on juniper1 (192.168.20.1):
(The 2555 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
23/tcp     open        telnet
179/tcp    open        bgp
Remote operating system guess: Juniper Networks JUNOS 5.3 on an Olive
router
Uptime 43.329 days (since Thu Oct 10 09:46:03 2002)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=58370 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 35 seconds
```

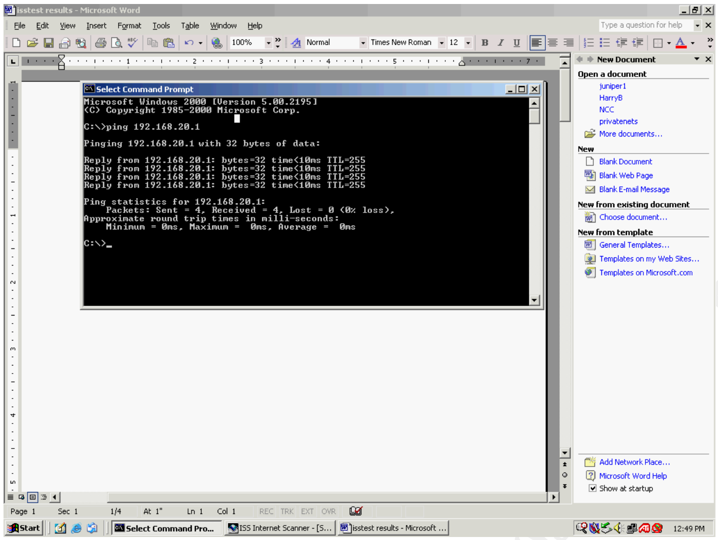
The auditor verified that SSH and telnet ports are open along with bgp (the router routing protocol). These 3 services were the only services nmap found running on the router and all other ports are closed.

The auditor ran the commercial scanner ISS. (See step #14.) ISS found the services Border Gateway Protocol (bgp), ntp, telnet, SSH, SNMP, and syslog. These results are displayed in Appendix B.

There were no unnecessary services encountered so interviews with network and system administrators were unnecessary.

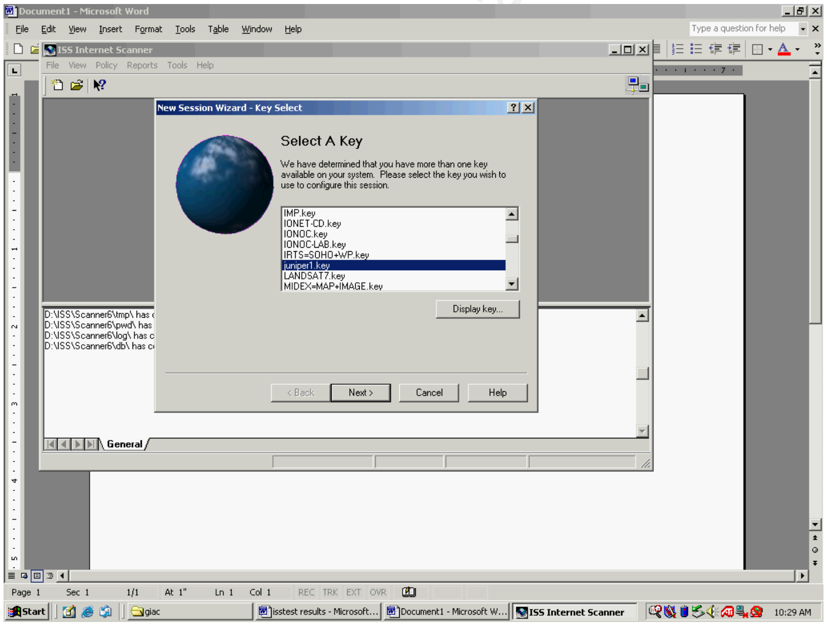
Step #14 - Discover vulnerabilities present on router

The auditor ran the commercial product ISS against the Juniper router. First the router was pinged from inside the lab. (The router has a private address so it is impossible to ping it from outside the lab.)



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time<10ms TTL=255
Reply from 192.168.20.1: bytes=32 time<10ms TTL=255
Reply from 192.168.20.1: bytes=32 time<10ms TTL=255
Reply from 192.168.20.1: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>_
```

The auditor brought up ISS and selected a key. The next button was clicked.



New Session Wizard - Key Select

Select A Key

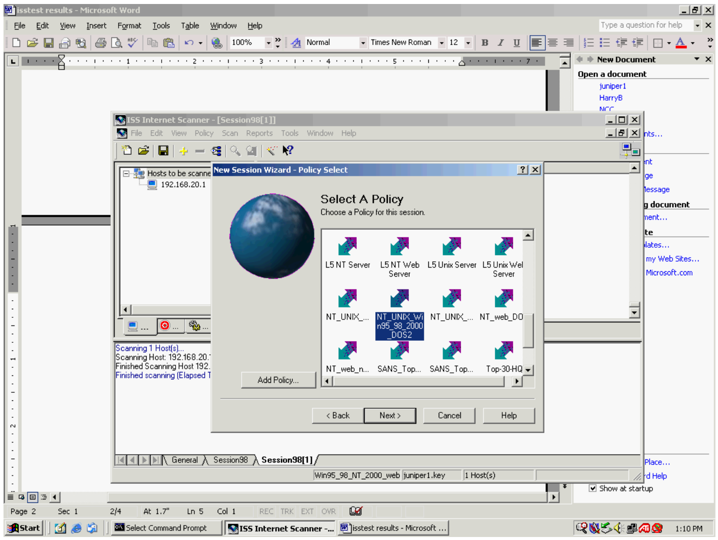
We have determined that you have more than one key available on your system. Please select the key you wish to use to configure this session.

IMP.key
IONET-CD.key
IONOC.key
IONOC-LAB.key
IRTS=SOHO+WP.key
juniper1.key
LANDSAT7.key
MIDEX=MAP+IMAGE.key

```
D:\ISS\Scanner6\tmp\ has c
D:\ISS\Scanner6\pwd\ has
D:\ISS\Scanner6\log\ has c
D:\ISS\Scanner6\db\ has c
```

Document1 - Microsoft Word
ISS Internet Scanner
File View Policy Reports Tools Help
Display key...
< Back
Next >
Cancel
Help
General
Start
giac
isstest results - Microsoft...
Document1 - Microsoft W...
ISS Internet Scanner
10:29 AM

A policy was selected by clicking on the policy that tests everything and then clicking next.



New Session Wizard - Policy Select

Select A Policy

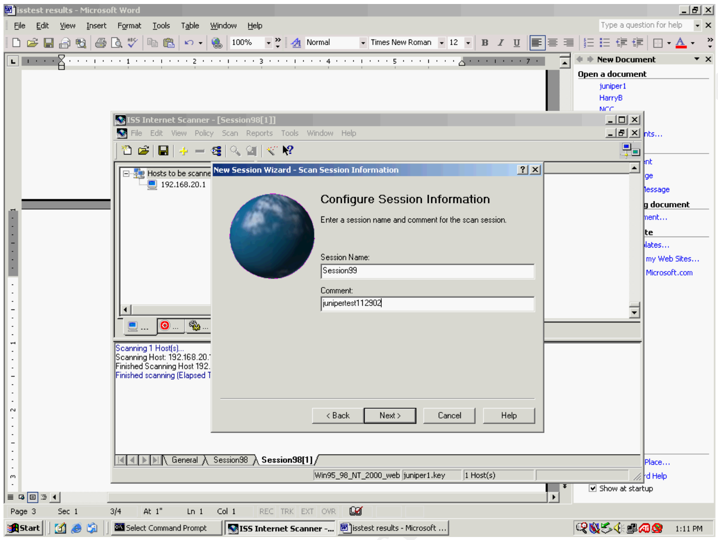
Choose a Policy for this session.

```
Scanning 1 Host(s)...
Scanning Host: 192.168.20.1
Finished Scanning Host 192.
Finished scanning (Elapsed T
```

Hosts to be scanned: 192.168.20.1

Win95_98_NT_2000_web | juniper1.key | 1 Host(s)

The session was configured by entering identifying information and then clicking next.



New Session Wizard - Scan Session Information

Configure Session Information

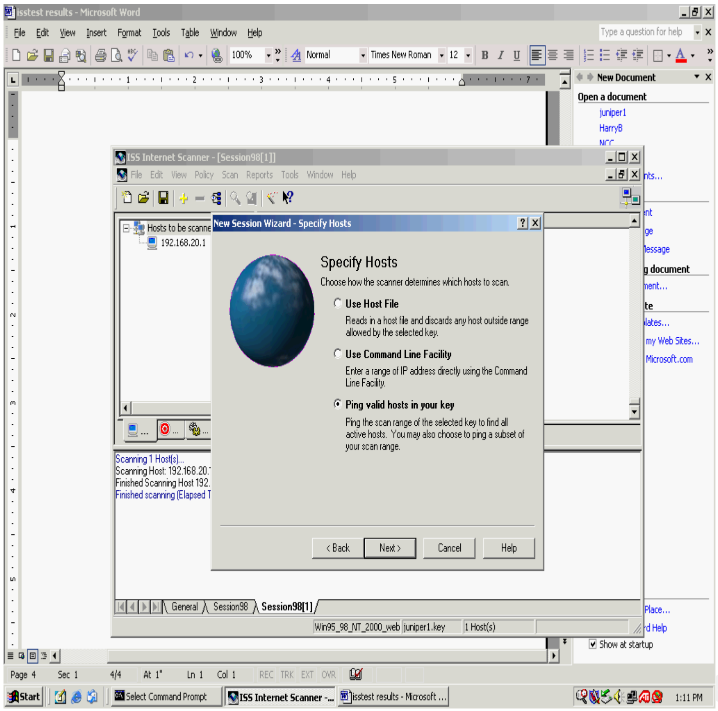
Enter a session name and comment for the scan session.

Session Name: Session99

Comment: junipertest112902

Win95_98_NT_2000_web | juniper1.key | 1 Host(s)

The auditor specified the hosts by having ISS ping the valid hosts within the key. (Juniper1)


isstest results - Microsoft Word
ISS Internet Scanner - [Session98[1]]
File Edit View Policy Scan Reports Tools Window Help
Hosts to be scanne
192.168.20.1
< Back
Next >
Cancel
Help
General
Session98
Session98[1]

New Session Wizard - Specify Hosts

Specify Hosts

Choose how the scanner determines which hosts to scan.

○ Use Host File

Reads in a host file and discards any host outside range allowed by the selected key.

○ Use Command Line Facility

Enter a range of IP address directly using the Command Line Facility.

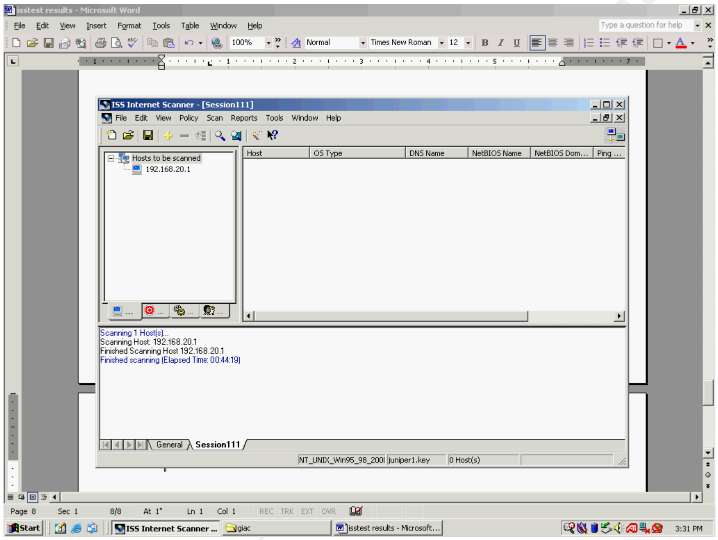
● Ping valid hosts in your key

Ping the scan range of the selected key to find all active hosts. You may also choose to ping a subset of your scan range.

```
Scanning 1 Host(s)...
Scanning Host: 192.168.20.1
Finished Scanning Host 192.
Finished scanning (Elapsed T
```

Win95_98_NT_2000_web | juniper1.key | 1 Host(s)

The auditor pulled down the scan menu and selected start the scan. The scan ran automatically.


isstest results - Microsoft Word
ISS Internet Scanner - [Session111]
File Edit View Policy Scan Reports Tools Window Help
Hosts to be scanned
192.168.20.1
Host
OS Type
DNS Name
NetBIOS Name
NetBIOS Dom...
Ping ...
General
Session111

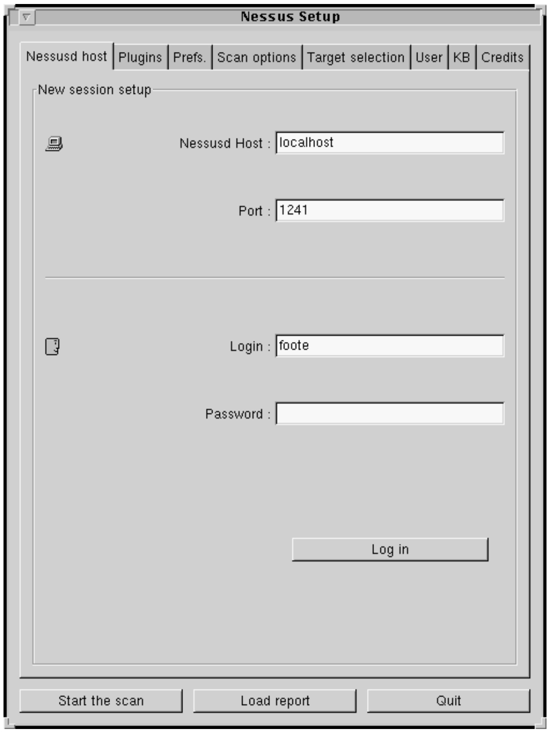
```
Scanning 1 Host(s)...
Scanning Host: 192.168.20.1
Finished Scanning Host 192.168.20.1
Finished scanning (Elapsed Time: 00:44:19)
```

NT_UNIX_Win95_98_200(| juniper1.key | 0 Host(s)

At the end of the scan, the auditor pulled down the report menu and generated reports for services and vulnerabilities for the router. They are attached in Appendix B.

The policy selected for the scan selected all vulnerabilities to be tested, including all operating systems. This policy checks in excess of 700 vulnerabilities. The commercial scanner was last updated in 11/02 for the most current checks. The commercial scanner identified the Juniper router as a UNIX box. The vulnerabilities encountered by the commercial scanner were Internet Control Message Protocol (ICMP) and traceroute and services found were bgp, SNMP, SSH, syslog, and telnet.

The auditor started Nessus by typing ‘nessus’ at the command prompt. The setup graphic appeared. The auditor logged into Nessus setup screen and clicked on the ‘Log in’ button.



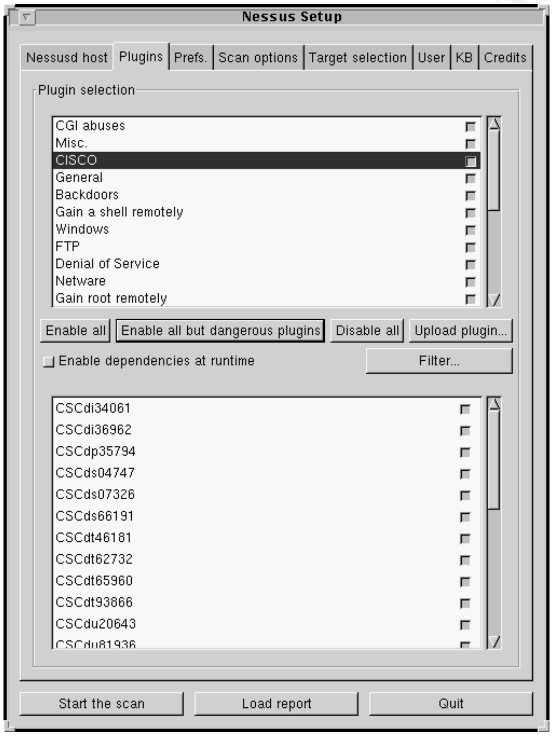
Nessusd Host : localhost

Port : 1241

Login : foote

Password :

The next Nessus Setup screen displayed. The ‘Enable all by dangerous plugins’ button was clicked.

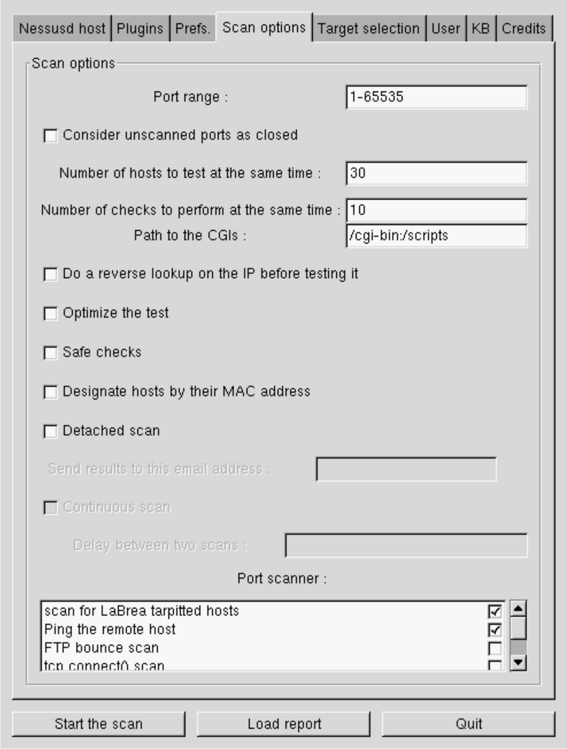


CGI abuses
Misc.
CISCO
General
Backdoors
Gain a shell remotely
Windows
FTP
Denial of Service
Netware
Gain root remotely

□ Enable dependencies at runtime

CSCdi34061
CSCdi36962
CSCdp35794
CSCds04747
CSCds07326
CSCds66191
CSCdt46181
CSCdt62732
CSCdt65960
CSCdt93866
CSCdu20643
CSCdu81936

The scan options screen was selected. The port range was changed to 65,535.



Scan options

Port range : 1-65535

□ Consider unscanned ports as closed

Number of hosts to test at the same time : 30

Number of checks to perform at the same time : 10

Path to the CGIs : /cgi-bin:/scripts

□ Do a reverse lookup on the IP before testing it

□ Optimize the test

□ Safe checks

□ Designate hosts by their MAC address

□ Detached scan

Send results to this email address :

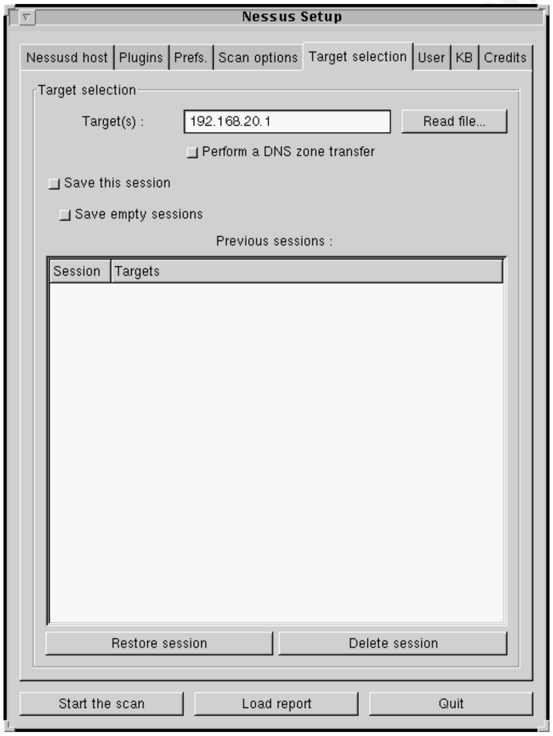
□ Continuous scan

Delay between two scans :

Port scanner :

scan for LaBrea tarpitted hosts	☑
Ping the remote host	☑
FTP bounce scan	□
tcp connect() scan	□

Selected the 'Target selection' tab. The next Nessus Setup screen displayed.



Target selection

Target(s) : 192.168.20.1

□ Perform a DNS zone transfer

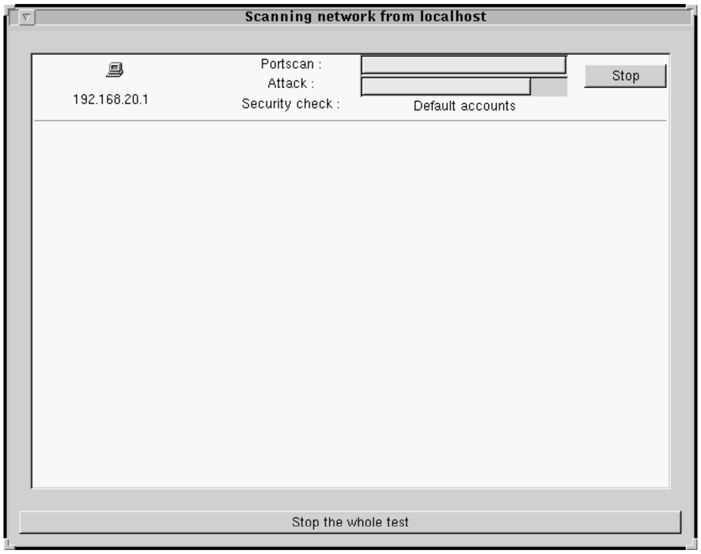
□ Save this session

□ Save empty sessions

Previous sessions :

Session	Targets

The auditor entered the host's IP address and clicked on the 'Start the scan' button and the scan started. While the scan was running the next screen displayed.



Scanning network from localhost

192.168.20.1

Portscan :
Attack :
Security check : Default accounts

At the end of the test, the auditor selected the report by text button. The Nessus report was generated. It is included in Appendix C of this document. The report contained 4 security holes, 4 security warnings and 7 security notes. It listed the open ports. Nessus agreed with the commercial scanner in that it found ports 22, 23, 123, and 179 open. ISS also found 161, and 514 open. Nessus found a vulnerability on port 22 that ISS did not find. It found a lot of problems with SSH, most of which do not apply to the router. The router does not support Kerberos, UseLogin, a Red Hat host, and AFS. Only patched versions of SSH are used in the network. The report also found the use of telnet that has been discussed previously. Nessus stated about telnet, 'This service (telnet) is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.' Nessus found that 'ICMP timestamp' was running on the router. 'The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on your machine. This may help him to defeat all your time based authentication protocols.' Nessus found the ntp service on the router.

Step #15 - Verify patches are up to date

The auditor looked under CERT advisories for Juniper router vulnerabilities and encountered Juniper Network Information for VU#7388331, which is below.

Juniper Networks Information for VU#7383317

Date Notified 08/15/2002

Date Modified 11/13/2002 01:59:20 PM

Status Summary Vulnerable

Vendor Statement

Juniper Networks has determined that its JUNOS Internet Software, used on the M- and T-series of router products, is susceptible to this vulnerability in versions 5.2R1.4, 5.2R2.3, 5.2R3.4, 5.2R4.4, 5.3R1.2, 5.3R2.4, 5.3R3.3, and 5.4R1.4. Customers should contact Juniper or their Juniper reseller to obtain an updated version of JUNOS software.

Juniper Networks has determined that the operating software used on the ERX router products is not susceptible to this vulnerability. No software upgrade is required. However, the SDX-300 Service Deployment system may be susceptible if it is installed on a susceptible host platform. Users of SDX-300 should contact their host operating system vendor regarding this advisory.

The Juniper Networks G10 CMTS product is not susceptible to this vulnerability. No upgrade is required.

CERT/CC Addendum

The CERT/CC has no additional comments at this time.

If you have feedback, comments, or additional information about this vulnerability, please send us email.

Vulnerability Note VU#738331

Domain Name System (DNS) resolver libraries vulnerable to read buffer overflow

Overview

DNS stub resolvers from multiple vendors contain a buffer overflow vulnerability. The impact of this vulnerability appears to be limited to denial of service.

I. Description

A read buffer overflow vulnerability exists in BIND 4 and BIND 8.2.x stub resolver libraries. Other resolver libraries derived from BIND 4 are also affected, including BSD libc, GNU/Linux glibc, and System 5 UNIX libresolv. This vulnerability is similar in scope to VU#803539 and VU#542971, which are referenced by CERT Advisory CA-2002-19.

The name server itself, named, is not affected. The vulnerability exists in DNS stub resolver libraries that are used by network applications to obtain host or network information, typically host names and IP addresses. For example, when a web browser attempts to access http://www.cert.org/, it calls functions in a DNS stub resolver library in order to determine an IP address for www.cert.org.

Within the DNS resolver library, a buffer size value that is smaller than the maximum size of a potential DNS response is passed to the functions that perform DNS resolution. If a response is encountered that is larger than the allocated buffer, the response is truncated and returned to the calling function, along with the amount of buffer space that would be required to handle the entire response. The calling function may use this value for the size of the buffer and read beyond the end of the actual DNS response. In some cases, unmapped memory may be read, which typically causes the calling application to crash. In other cases, mapped memory may be read, and the contents included in the DNS response, which the calling application typically handles as a malformed response.

Applications that call DNS resolution functions directly may also be vulnerable, depending on how those applications handle the returned buffer size value. MIT Kerberos 5, KTH Heimdal Kerberos, nss_ldap, and fetchmail are known to be affected.

Quoting from the ISC advisory:

When looking up address (gethostbyname(), gethostbyaddr() etc.) a less than maximum sized buffer is passed to res_search() / res_query(). If the answer is too large to fit in the buffer the size of buffer required is returned along with the part of the message that will fit. This value is not checked and is passed to getanswer which then may read past the end of the buffer depending up the contents in the answer section.

II. Impact

An attacker who is able to send DNS responses to a vulnerable system could cause a denial of service, crashing the application that made calls to a vulnerable resolver library. It does not appear that this vulnerability can be leveraged to execute arbitrary code. There may be some risk of information disclosure if a vulnerable system returns the contents of memory adjacent to a DNS response.

III. Solution

Patch or Upgrade

Apply a patch or upgrade as specified by your vendor. In the case of statically linked binaries, it is necessary to recompile using the patched version of the DNS stub resolver libraries. ISC has provided the following guidance for applications that call DNS resolution functions directly:

The auditor then logged onto Juniper router. After a successful login, this message was received.

```
 --- JUNOS 5.1R2.4 built 2001-12-11 02:11:09 UTC
```

This message verified that this router was not patched with the latest possible patch. The version 5.2R2.4 is one of the versions cited in the alert and the date is previous to the vulnerability identified and the fix.

Step #16 - Verify that no local user accounts are present on the router.

After entering the command ' show configuration' the following appeared, verifying there were local user accounts present on the router in addition to the operational accounts.

```
root-authentication {
    encrypted-password "$1$8V4sZ$R9leUqhRHk3IryOF9x56R/"; #
SECRET-DATA
  }
class john {
      permissions all;
    }
    class engr {
      idle-timeout 10;
      permissions all;
    }
    class ops {
      permissions [ interface network routing trace view
firewall ];
    }
    class superuser-local;
    user mcc {
      uid 2001;
      class ops;
      authentication {
        encrypted-password "$1$uHZ2.$8LSO8GF18fbNL9XYxo08K.";
# SECRET-DATA
      }
    }
   user john {
      uid 2003;
      class john;
      authentication {
        encrypted-password "$1$QkMsZ$BB37Su.6hlGUvAx6CWXab1";
# SECRET-DATA
      }
    }
    user karen {
      full-name "KAREN P";
      uid 2002;
      class superuser;
      authentication {
        encrypted-password "$1$IGl.6$S6M9wSSqzuGjgktzu5kEu.";
# SECRET-DATA
      }
    }
    user engr {
      uid 2000;
      class engr;
      authentication {
        encrypted-password "$1$UoU2.$EVDdo3a6PPM7J2JfafIlB/";
# SECRET-DATA
```

```
            }
```

The router is currently in a lab setting and any extra accounts need to be deleted before the router goes operational on the federal network.

Step #18 - Verify unused interfaces are disabled.

After entering the command ' show configuration' the following appeared, verifying the devices were not disabled unless the physical link was down for the unused interfaces. The command for disabling an interface was tested by running a ping test on an interface while it was enabled and again while it was disabled.

A test scenario with a Sun box connected to a Juniper router and then connected to a Cisco router was created. The auditor ran a test with the Fast Ethernet Interface configuration up:

```
Physical interface: fe-0/1/3, Enabled, Physical link is Up
 Interface index: 13, SNMP ifIndex: 17
  Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: 
Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Current address: 00:90:69:b3:80:22, Hardware address: 
00:90:69:b3:80:22
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None
  Active defects : None

  Logical interface fe-0/1/3.0 (Index 9) (SNMP ifIndex 35)
    Flags: SNMP-Traps Encapsulation: ENET2
    Protocol inet, MTU: 1500, Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 192.168.10/24, Local: 192.168.20.1,
        Broadcast: 192.168.10.255
```

The auditor ran a ping test to confirm that the interface was up.

```
earth1% ping 192.168.20.1
192.168.20.1 is alive
```

The network manager disabled the Fast Ethernet in the Juniper configuration. The auditor used the command 'show configuration' which displayed:

```
fe-0/1/3 {
        unit 0 {
            disable;
            family inet {
                address 192.168.20.1/24;
            }
        }
    }
```

Entered the command ‘show interfaces’ to verify that the interface was disabled.

```
Physical interface: fe-0/1/3, Enabled, Physical link is Up
  Interface index: 13, SNMP ifIndex: 17
  Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback:
Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Current address: 00:90:69:b3:80:22, Hardware address:
00:90:69:b3:80:22
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None
  Active defects : None

  Logical interface fe-0/1/3.0 (Index 9) (SNMP ifIndex 35)
    Flags: Down SNMP-Traps Encapsulation: ENET2
    Protocol inet, MTU: 1500, Flags: None
      Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
        Destination: 192.168.10/24, Local: 192.168.20.1, Broadcast:
192.168.10.255
```

The auditor ran a ping test with interface disabled:

```
earth1% ping 192.168.20.1
no answer from 192.168.20.1
```

The Fast Ethernet interface was enabled again:

```
fe-0/1/3 {
        unit 0 {
            enable;
            family inet {
                address 192.168.20.1/24;
            }
        }
    }
```

The auditor ran command ‘show interfaces’ to verify the configuration.

```
Physical interface: fe-0/1/3, Enabled, Physical link is Up
  Interface index: 13, SNMP ifIndex: 17
  Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback:
Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Current address: 00:90:69:b3:80:22, Hardware address:
00:90:69:b3:80:22
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None
  Active defects : None

 Logical interface fe-0/1/3.0 (Index 9) (SNMP ifIndex 35)
    Flags: SNMP-Traps Encapsulation: ENET2
    Protocol inet, MTU: 1500, Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 192.168.10/24, Local: 192.168.20.1, Broadcast:
192.168.10.255
```

The auditor ran the ping test to verify that interface was again up.

```
earth1% ping 192.168.20.1
192.168.20.1 is alive
```

Step #19 - Verify the ICMP traffic is blocked at the router

After entering the command ‘ show configuration’ the following was displayed.

```
term BLOCK-ICMP {
            from {
                protocol icmp;
            }
            then discard;
        }
```

The auditor set up test configuration on Juniper interface with no access list to control ping.

```
fe-0/1/3 {
        unit 0 {
            family inet {
                address 192.168.20.1/24;
            }
        }
    }
```

The auditor attempted to ping the Juniper and the Cisco router with ICMP permitted (that is, not blocked by an access list).

```
earth1% ping 192.168.20.1  (Juniper)
192.168.20.1 is alive
earth1% ping 192.168.113.2  (Cisco)
192.168.113.2 is alive
```

A filter blocking ICMP (ping) was configured on the Juniper.

```
filter BLOCK-PING {
        term block-ping {
            from {
                address {
                    192.168.20.1/32;  (Juniper1)
                }
                protocol icmp;
            }
            then {
                reject;
            }
        }
    }
}
```

The auditor ran a ping test with access list applied that blocked ping verifying that ping was blocked at the router for this interface.

```
earth1% ping 192.168.113.2
ICMP 13 Unreachable from Juniper1 (192.168.20.1)
 for icmp from Juniper1 (192.168.20.1) to 192.168.113.2

earth1% ping 192.168.20.1
ICMP 13 Unreachable from gateway Juniper1 (192.168.20.1)
 for icmp from Juniper1  (192.168.20.1) to 192.168.20.1
```

Step #20 - Verify the access lists block reserved and inappropriate addresses.

After entering the command ' show configuration' the following was displayed.

```
term BLOCK-SOURCES {
            from {
                source-address {
                    0.0.0.0/8;
                    10.0.0.0/8;
                    172.16.0.0/12;
                    192.168.0.0/16;
                    223.255.255.0/24;
                    224.0.0.0/4;
                    240.0.0.0/5;
                    248.0.0.0/5;
                    255.255.255.255/32;
                   }
            }
            then discard;
        }
```

This step verified that reserved and inappropriate addresses were being blocked at the router.

A test was run with a host, Juniper router and a Cisco router tied together in one network.   A Juniper router access list allowing a host was applied to interface.   The 'show configuration' command showed this as part of the output.

```
fe-0/1/3 {
        unit 0 {
            enable;
            family inet {
                address 192.168.20.1/24;
            }
        }
    }
```

There was a successful ping from Cisco router to the host

```
ping 192.168.25.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

An access list was applied to the Juniper router to block a host

```
filter BASIC-TEST {
        term block_from_host {
            from {
                address {
                    192.168.113.2/32;
                }
            }
            then {
                reject;
            }
        }
    }
```

The Cisco router was unable to ping the host due to the access list, verifying that the router can block any address selected on the access list.

```
ping 192.168.25.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

Summary

The following is a summary of the steps, control objectives, compliance and the recommendations.

Step	Control objective	Compliant	Stimulus-Response	Recommendations
1-Verify router security plan	Define a strategic IT plan	No	No	Rewrite plan to meet objectives and requirements.
2-Verify that SNMP has been disabled or the password has been changed	Ensuring system security to safeguard information against unauthorized use, disclosure or modification, damage or loss.	Yes	Yes	None
3-Verify router passwords are encrypted, and hard to guess.	Ensuring system security to safeguard information against unauthorized use, disclosure or modification, damage or loss.	Yes	Yes	None
4-Verify access restrictions are imposed on console, aux, VTYs	Ensuring system security to safeguard information against unauthorized use, disclosure or modification, damage or loss.	Yes	Yes	Unlimited user IDs are a residual risk on the network.
5- Verify telnet, SSH based network protocols are	Identifying automated solutions to ensure an effective and	Yes	Yes	Telnet is a residual risk on the network

Step	Control objective	Compliant	Stimulus-Response	Recommendations
present instead of rlogin.	efficient approach to satisfy the user requirements			
6-Verify physical security	Managing facilities to provide a suitable physical surrounding that protects the IT equipment and people against man-made and natural hazards.	Yes	No	None
7- Verify warning banner on router	Communicating management aims and direction to ensure user awareness and understanding of those aims. Ensuring compliance with external requirements to meet legal regulatory and contractual obligation. Educating and training users to ensure that users are aware of the risks and responsibilities involved.	Yes	Yes	None
8- Verify information is being logged	Managing data. Managing operations.	Yes	Yes	None

Step	Control objective	Compliant	Stimulus-Response	Recommendations
9- Verify that logs are checked regularly.	Managing data. Managing operations	Yes	No	None
10-Ensure that router's time of day is set accurately and connected to ntp.	Managing data. Managing operations	Yes	Yes	None
11-Verify anti-spoofing has bee applied with access lists	Managing quality. Ensuring systems security	Yes	Yes	None
12- Verify controlled directed broadcasts.	Managing quality. Ensuring systems security	Yes	Yes	None
13-Determine which services are running. Verify all unneeded services are disabled.	Managing quality. Ensuring systems security	Yes	No	None
14- Discover vulnerabilities present on router.	Managing quality. Ensuring systems security	Yes	No	SSH on the router needs to be updated.
15- Verify patches are up to date	Acquiring and maintaining technology infrastructure	Yes	Yes	Most recent patch examined and new operating system is not applied. DNS is not used on the router

Step	Control objective	Compliant	Stimulus-Response	Recommendations
				so no risk due to DNS.
16-Verify that no local user accounts are present on router.	Managing quality. Ensuring systems security	No	Yes	Test user accounts exist because router is in a lab. Local user accounts need to be removed before router goes operational.
17- Verify web server, DNS, NFS, sendmail software are removed	Managing quality. Ensuring systems security.	Yes	Yes	None
18- Verify unused interfaces are disabled.	Managing quality. Ensuring systems security	No	Yes	The unused interfaces need to be disabled when not in use.
19- Verify the ICMP traffic is blocked at the router.	Managing quality. Ensuring systems security	Yes	Yes	None
20- Verify the access lists block reserved and inappropriate addresses.	Managing data. Managing operations	Yes	Yes	None

Measure Residual Risk

Minimal residual risk exists. The vulnerabilities that were found that cannot be fixed are telnet and unlimited users. In order to get rid of the unlimited users, a new device would have to be picked and the benefit of the router's performance outweighs this vulnerability. In order to eliminate telnet, a study would have to be performed. Right now there are no personnel who can perform that study and the Federal Agency cannot afford to eliminate that risk.

The following control objectives were not met but can be remedied:

1. Step 1 – Define a strategic IT plan. Manpower can revise and rewrite the IT security plan. The security plan was not compliant with the required procedures for the Federal agency involved.
2. Step 14 - Managing quality. Ensuring systems security. SSH needs to be updated at some future date to ensure safety of secure communications.
3. Step 16 - Managing quality. Ensuring systems security. Test user accounts to verify the router need to be deleted before the router goes operational on the network.
4. Step 18 – Managing quality. Ensuring systems security. Unused interfaces need to be disabled in the operational state.

Control objectives that were met are:

1. Ensuring system security to safeguard information against unauthorized use, disclosure, modification, damage or loss.
2. Identifying automated solutions to ensure an effective and efficient approach to satisfy the user requirements.
3. Managing facilities to provide a suitable physical surrounding that protects the IT equipment and people against manmade and natural hazards.
4. Communicating management aims and direction to ensure user awareness and understanding of those aims, ensuring compliance with external requirements to meet legal regulatory and contractual obligation, educating and training users to ensure that users are aware of the risks and responsibilities involved.
5. Managing Data
6. Managing Operations
7. Managing Quality
8. Acquiring and maintaining technology infrastructure

Residual risks that still exists that cannot be eliminated:

1. Basically unlimited user IDs can be logged on to the router in unlimited amounts. Since this is a UNIX box, there is no limit on logins. The auditor considers this a low risk, as many people should not be logged onto a router at the same time. The passwords could not be guessed by 'crack' even though this was a UNIX box.
2. Telnet is a risk as the password is passed in the clear and a hacker could conceivably capture the password and take over the router. The auditor

considers this a medium risk as the network practices defense in depth and has other protections, including other routers and firewalls. Telnet will only be done from the outside of the firewall to the outside of the firewall and from the inside to the inside.

Some of the compensating controls that are in place to mitigate the risks of having telnet and too many users on the routers are as follows:

1. There is a network firewall in place. The firewall blocks many messages and message types such as ICMP. Therefore, it will be difficult for someone outside the firewall to see a telnet session, or determine an IP address of the router in order to make a telnet attempt to the router.
2. ICMP is blocked at all the routers at all the borders of the network.
3. There is an IDS being put in place. The IDS will find anyone trying to scan the network and be able to pick up unauthorized or inappropriate traffic.
4. No workstations are allowed on the backbone of the network, where additional protections are applied to the network
5. All router ports are disabled so a workstation cannot be directly connected to the router without authorization.
6. There is a network management device on the network.
7. Network auditing occurs for every project being connected to the network and auditing is repeated every three years.
8. All projects must conduct a risk analysis of their project.
9. The network has rules of behavior that all users sign, accepting responsibility for their actions.
10. There are home-grown tools that help with automating auditing the logs and the routers.
11. Configuration Management is used throughout the network
12. There are security awareness programs, lunchtime seminars and other training measures.
13. Anti-virus software is run and updated regularly.
14. All network architecture has to be certified by the Network Security Officer's office.
15. Host and network defenses are implemented, including personal and project firewalls.
16. Network and host based vulnerability assessment tools are run on a regular basis, and vulnerabilities are corrected wherever possible.
17. Incident handling processes are in place.

Evaluate the Audit

The audit worked out pretty well. The plan was to audit a Juniper router. It took very little time to establish that security on Juniper routers has not been evaluated. The main concept was to examine the Cisco literature from NSA, Cisco, and SANS, to learn enough about what the important aspects of auditing routers were. NSA, Cisco, and SANS for the most part agreed on the best practices. Information from the SANS Track

7 was extremely helpful, as it had an entire section on securing routers and addressing Cisco in particular. The next step was to take that knowledge and examine the Juniper router. This activity went well. It was necessary to read documentation that was intended for Cisco routers and translate that into Juniper configuration controls. The major difference found was that the Juniper has a UNIX-based operating system and the Cisco has its own operating system, Cisco IOS. The best thing the auditor found was that the Juniper router acts in many ways like the Cisco router. When a command is entered at the command prompt, a question mark can be entered at the end of the command and help will be given. For example, if the word 'show' is entered and a question mark is added, all the various show commands will be displayed.

Because of the preparatory work that was done to perform this audit, it took a great deal of time. However, in the future others can read these audit steps to determine how to evaluate a Juniper router without the need to do all the background investigation needed to perform this audit. The steps provided are, for the most part, best practices for routers that the auditor extracted from extensive Cisco, NSA, and SANS documentation.

The auditor's primary goal was to determine if the router could safely replace the outdated Cisco and 3COM routers in the network that are no longer supported by the vendors. The reason the network manager wanted to experiment with these routers was speed. The Juniper routers are very fast and efficient and could improve network performance.

The audit emphasized the difference between objective and subjective steps. This auditor has had previous experience auditing and has found that many tests are subjective. Pointing out the difference was a good experience. Every time there is a subjective test step, that step needed to be carefully evaluated to see how to make it as objective as possible. For example, more checklists, like the one written for step 6 appear to be a good idea. A checklist standardizes the subjectivity more than just conducting interviews, which may vary widely from one person to the next.

Introducing the auditor to CobiT was very useful. The CobiT control objectives are the same control objectives in use by the Federal Agency involved. Knowing that the Federal Agency is aligned with business best practices was very comforting. It was possible to establish the control objectives one for one with the steps.

Assignment 4 – Audit Report

Executive Summary

The primary purpose of this audit was to verify that the Juniper router is safe enough to replace outdated Cisco and 3COM routers on the Federal Agency network. The results show that the audit objective has been met; the Juniper router can replace the outdated and unsupported routers on the operational network without introducing unacceptable risks.

The results are as follows:

1. Out of 20 tests performed, the router was compliant for 17 tests, and not compliant for 3 tests.

   A. In step 14, SSH was found to be older than the most current release. This was not a problem because all of the possible SSH vulnerabilities described in the Nessus report did not apply to the router. Even though this was not a serious problem, the newest version of SSH should be incorporated in the next release to the router.

   B. In step 16, there proved to be extra user logons due to the test scenarios that have been performed with the router by the auditor and the network administrators. This is not a serious problem but those accounts need to be removed before the router goes operational.

   C. In step 15, the patches were not completely up to date and the patch that was missing required upgrading the operating system. This turned out to not be a problem. The patch was evaluated and the network administrators made a decision not to install the patch. The vulnerability involved being vulnerable to a DNS problem. DNS is not installed or used on the router as verified by other tests. This evaluation verified the process whereby patches are evaluated prior to installation, to ensure no adverse effects.

   D. In step 18, the unused interfaces were not disabled in the lab. This is not a serious problem. Operationally when the routers are set up, the unused interfaces are disabled as well as unused ports. The network administrators have a procedure that describes how that happens. Having an unused interface on the router opens up the possibility that information could be flowing over that interface without anyone knowing. However, the lab should also keep tighter control over the unused interfaces.

   E. In step 1, the most serious problem was uncovered. The security plan is not meeting NPG 2810.1 requirements and the plan did not prove to be strategic. The reason this is the most important discovery is that if the management does not have clear objectives that are clearly conveyed to personnel, the implementation of the router may not meet the needs of management. Clear objectives mean clear implementations. The security plan needs to be rewritten.

2. Out of 20 tests, 18 tests had no residual risks that have to be accepted. Two steps uncovered residual risks, as there is no way to fix the vulnerabilities. In step 4, there is residual risk in that the Juniper router allows unlimited user IDs. In fact, that router will allow thousands to be logged on at the same time. This is more risky than the Cisco router which only allows 5 VTYs to be logged on at a time, thereby limiting the logons to 5. There is nothing that anyone can do about that, as that is how the router is designed. Network management personnel will have to be vigilant and limit the IDs to essential personnel.

   A. In step 5, there is a residual risk of allowing telnet to the router. However, since this network is international and there are encryption laws to be faced, there is nothing that can be done about having telnet on the routers at this time. The problem with telnet is that someone could put a workstation with a sniffer on the network. The password to the router is transmitted in the clear with telnet so that someone watching would learn the password and could use it. There is reduced risk with this problem because there are no workstations on the backbone of the network. Router ports are disabled when not being used. All these routers are in secured areas, so it would be hard to get to a place to install a sniffer, as well. Therefore the chance of someone sniffing the password is not that great, but a certain amount of risk does remain.

In conclusion, the preponderance of tests confirm that the router is compliant and acceptable for operational use.

Audit Findings

There were three types of stimulus-response findings as well as subjective findings. The first type of finding was a step-response type. The second type of finding was running a tool – either COTS or freeware, against the router to receive information. The third type of finding was setting up a small network in the lab to reproduce an operational scenario. Commands were then run through the Juniper router to verify that the configuration that was set up was functioning properly. The subjective finding was by gleaning information by evaluating documentation, physical scrutiny, interviews and discussions with operational personnel.

The purpose of step 1 was to verify that the written policies were strategic and applicable to the needs of the routers in the network. The security plan did not meet requirements and was not strategic. The plan was written in such general terms that it really did not satisfy the requirements. It did not follow the outline required by NPG 2810.1.

The purpose of step 2 was to verify that SNMP was present on the router (as it is used operationally) but presented a minimal risk to the network. SNMP is needed to constantly get information from the router to a Network Manager in the Mission Control Center. ISS and Nessus were run against the router, and ISS found the service SNMP running on the router. However ISS was unable to guess the SNMP password confirming that a strong password had been chosen.

The purpose of Step 3 was to verify that the router passwords were encrypted and hard to guess. This step also included the demonstration that the passwords were encrypted ("$1$8V4sZ$R9leUqhRHk3IryOF9x56R/"). Then the encrypted passwords were copied into a file on a UNIX workstation and the freeware utility ‘crack’ was run against the passwords. The Juniper does not use the encryption scheme that ‘crack’ expected so, after 4 or 5 hours, ‘crack’ just gave up. Crack’s unsuccessful attempt to guess even one password verified that they were hard to guess.

The purpose of step 4 was to verify access restrictions on the console, auxiliary and VTYs. No one wants it to be easy to access the router physically. A physical examination confirmed that there was no console or auxiliary hooked to the Juniper. However there was the physical capability for a console and an auxiliary. The ‘show configuration’ command demonstrated that the console was enabled, but not the auxiliary. The paperwork research confirmed that the router does not configure the auxiliary by default. Since there is no need for the auxiliary, it had never been configured. There is occasional need for a console so it had been configured on the router

The VTYs were different. VTYs are used on Cisco routers and they are not on Juniper routers. Each user and operational login was configured with an encrypted password. There is no limit to user logins however. According to the Juniper documentation, there are identifiers that are associated with the user account name. The system administrator either assigns the identifier or the system automatically assigns one. The identifiers must be in the range between 100 through 64000 and must be unique within the router. This poses a residual risk to the system. Choosing this router means that the network is running that risk.

The purpose of step 5 was to verify telnet and SSH based protocols were present and rlogin was not. The commands demonstrated that SSH and telnet were present and rlogin was not. From inside the lab, it was possible to telnet to the router. It was also possible to SSH to the router. It was impossible to rlogin to the router or use rlogin on the router. Telnet is necessary in this network as it is worldwide and there are encryption laws preventing the use of SSH overseas.

The purpose of step 6 was to verify the physical security. In this case a form was used to standardize this evaluation. Standard physical security for the facility was identified during the examination of the facility. The standard for this network is that everything be locked up and this router was locked up.

The purpose of step 7 was to verify that the Federal warning banner was displayed on the router. Without the banner, the Inspector General (IG) cannot take anyone to court if they illegally access the router. The warning banner was displayed.

The purpose of step 8 was to verify the information was being logged. The command to log was verified and the log files that were created were verified. ISS was run against the router that verified that syslog was generating logs.

The purpose of step 9 was to verify that logs were being checked regularly. Through interviews with network management personnel and an examination of some of their administration tools that show the logs, regular (in fact practically real-time) log checking was verified.

The purpose of step 10 was to ensure that the router's time of day was set accurately and connected to ntp as all the routers in the network are. The purpose of this is to verify that if anything happened to the router, log backups would be synchronized with other router log backups so the f would be able to take the logs to court and create a story of how the routers had been compromised. The router was set to use ntp.

The purpose of step 11 was to verify that anti-spoofing had been applied with access lists. The purpose of this is to make sure that no one can pretend to be part of the network and gain access that way to the network. Anti-spoofing had been applied.

The purpose of step 12 was to verify that no one could take down the network by causing directed broadcasts to the network. This would cause a denial of service attack against the router. The network was set up to control directed broadcasts.

The purpose of step 13 was to determine which services were running. For this purpose nmap, Nessus and ISS were run against the router. The services that were found were: telnet, SSH, SNMP, bgp, ntp, and syslog. These are the only services that are needed on the network. Bgp is the router networking protocol. SNMP is necessary to get information from all the routers in the network. Ntp is the time protocol to synchronize the routers. Syslog is necessary to run logs and backups. Telnet is necessary to manage the routers.

The purpose of step 14 was to discover the vulnerabilities present on the router. The freeware tool Nessus, and the COTS product ISS were run against the router. With ISS, the only vulnerabilities encountered were ICMP timestamp and traceroute. The fix for ICMP timestamp is to block ICMP at the router, which the Juniper does, as verified in another test. (See step 19). Traceroute is allowed on the router to be able to locate connections to sites on the network. Traceroute is also used to find out where information is blocked when communication has been interrupted. ISS and Nessus found telnet, and considered it to be a problem. Nessus recommends that telnet be disabled which is not possible on this network. Telnet is needed to manage the routers since many of them are international routers and there are stringent encryption laws. Nessus encountered the fact that the SSH utility is out of date on the router. The vulnerabilities cited by Nessus were not applicable to the Juniper router, but SSH should be updated at a future time.

The purpose of step 15 was to verify that the patches were up to date. This step found a problem in that the patches were not completely up to date. However a discussion with a network administrator confirmed that the recommended new operating system had been evaluated, and network management personnel had determined that they did not need to change the whole operating system, as the network was not vulnerable to the DNS vulnerability. What was good about this step was that there was a process in place for evaluating patches and that procedure was being followed.

The purpose of step 16 was to verify that there were no local user accounts on the router. There were local user accounts but these were test accounts that could be explained through interviews. At this time, the auditor, and network management personnel are all testing this router at the same time, so there is a temporary need for all these extra accounts. Interviews confirmed that the network manager, at final acceptance of the router, would remove the extra accounts.

The purpose of step 17 was to verify that web servers, DNS, NFS, sendmail software were removed. This was an importance test as the router is a UNIX box and the capability for all these extra services exist in UNIX. However, tests confirmed that none of these software packages were present.

The purpose of step 18 was to verify that unused interfaces were disabled. In the test lab these interfaces were enabled. Tests confirmed that they could be disabled. Interviews with a network administrator confirmed that once the router was put in place, unused operational interfaces are downed as part of an operational acceptance procedure.

The purpose of step 19 was to verify that ICMP traffic was blocked at the router at each interface. Tests confirmed that ICMP was blocked and could be blocked at the router.

The purpose of step 20 was to verify that access lists block reserved and inappropriate addresses. Tests confirmed that these addresses are able to be blocked and were blocked.

Background/Risk

The following requirements were not met, but noncompliance can be remedied:

1. Step 1 – The IT security plan did not meet the standards of NPG 2810.1. A good security plan defines 'what' must be done to protect information transmitted on the federal network so that the 'how' can be implemented effectively. A security plan states who is responsible for what. Since this is not a good security plan, things are not clear. If personnel are not sure 'what' they should be doing, they will not know 'how' to do it. There are not sufficient guidelines in the plan in order to develop procedures.
2. Step 14 – The SSH application being used on the router is not the most current version. Even though the risk is small SSH should be updated in the next release. The system and network administrators use SSH to update and reconfigure the routers. The router configuration information should not be in the hands of anyone who does not have a need to know.
3. Step 16 - Test user accounts to verify the security and functionality of the router are present on the router. These extra accounts/passwords need to be deleted before the router goes operational on the network. Extra logon accounts provide extra opportunity for someone to logon to the router. Test logons typically allow super-user powers. This would enable an outside user to take control of the routers and access the network.
4. Step 18 – Unused interfaces need to be disabled in an operational state. Tests confirmed that these interfaces could be disabled. However, the unused interfaces are not disabled in the test lab. This will be remedied when the router goes operational. Procedures in place verify that when the router is put on the operational network, unused interfaces will be disabled. Unused interface might enable an outside user to use that interface to gain access to the network.

Some residual risks still exists that cannot be eliminated are:

1. Basically unlimited user IDs can be logged on in unlimited amounts. Since this is a UNIX box, there is no limit on logons. The auditor considers this a low risk, as many people should not be logged onto a router at the same time. The passwords could not be guessed by 'crack' even though this is a UNIX box. Unlimited users might enable an outside user to gain logon capabilities.
2. Telnet is a risk as the password is passed in the clear and a hacker could conceivably capture the password and take over the router. If an outside took over the router, he could gain access to the network. The auditor considers this a medium risk as the network practices defense in depth and has other protections, including other routers and firewalls. The network contains no workstations, only routers. So it would be difficult to put a sniffer on this network that the network operational personnel did not discover. The network is manned 24x7 and special tools monitor the routers every few minutes. There is also an experimental IDS on this network soon to become operational.

Audit Recommendations

The audit results lead to the recommendation that the Juniper router be allowed to go online when operational testing has been successfully completed. This router is secure enough to be a router on the Federal operational network.

Further Recommendations:

The network security plan is not sufficient for operational use, which leads to a few recommendations. The easiest recommendation is to update the network security plan to meet requirements and provide strategic guidance to the router network administrators. However, finding this situation lead to the conclusion that not enough money is spent on training. If people were better trained, they would realize that strategic plans are a necessity, not a luxury. The second part of this issue is that not enough manpower is dedicated to developing operational policies and then developing the procedures from the strategic policies. In other words, lack of training and lack of manpower is the real reason the security plan is deficient. If management does not document where they want to go, there is a possibility that the workforce will not get them there. How the routers should be secured is not discussed in the plan at all. Fortunately the network administration team has a very dedicated individual who has looked up and researched secure configurations and put them on the routers to the best of his ability. These actions must be documented to ensure these best practices continue in the absence of that individual.

The next recommendation involves the network not dedicating enough time to research and development. The majority of tools that are used on the network are freeware or homegrown tools. Therefore, the SSH utility that was provided on the router when it was purchased is the utility that is being used. Engineering staff time should be dedicated to explore new tools and investigate new releases of some COTS products. It is recommended that network engineers study the encryption algorithms to see if they can find an encryption tool that is safer to use than telnet, legal to use in the international network, and can replace the outdated SSH and telnet on the router. This would reduce the biggest vulnerability there is right now. Telnet is actually dangerous on this network as someone could conceivably sniff the operational password, log onto the router and change the configuration of the routers remotely. There is a possibility that this could endanger or stop the information being transmitted on this network.

There needs to be a new process in use in the lab environment. The lab environment should more closely conform to the operational conditions. For example, lab engineers should automatically disable the interfaces that they are not using to safe-guard the lab environment as well as the operational environment. Test accounts should be limited as much as possible to not have extra accounts that could be taken advantage of by accident or design.

More personnel need to be trained and utilized in auditing the systems and projects on the network. The staff is in short supply and cannot audit everything as thoroughly as the Juniper router was audited.

Costs

The cost to fix the problems involves increased personnel vs. money for equipment. The following costs should be implemented:

1. At least one network engineer should be trained in security knowledge at some professional training conference such as, SANS Essentials, and then given the job to revise the network security plan according to the requirements in NPG 2810.1.
2. At least two people should be dedicated to investigating research into new security technologies for the network. For example one person could investigate encryption on the network. The federal laws regarding encryption are changing and it is not clear that anyone involved in the network is keeping up with those changes. As an example, if there is a way to improve the encryption, that way should be investigated and developed.
3. The staff in the lab should be increased by at least one person, who can oversee security in the lab among all the equipment. Right now the lab system administrator is also responsible for the security of the lab. That means that the security time is limited to what is left over after the system administration work is accomplished.
4. Additional auditing staff should be hired to assist in auditing the many projects and systems on the federal network.
5. As there is a lab in existence, there is not a need at this time for any further equipment.

Compensating Controls

Like all federal budgets, this budget is being decreased, not increased, so it is impossible to eliminate all the risks. There are some compensating controls that are in use.

Some of the compensating controls are as follows:

1. There is a network firewall in place. The firewall blocks many messages and message types such as ICMP. Therefore, it will be difficult for someone outside the firewall to see a telnet session, or determine an IP address of the router in order to make a telnet attempt to the router.
2. ICMP is blocked at all the routers at all the borders of the network.
3. There is an IDS being put in place. The IDS will find anyone trying to scan the network and be able to pick up unauthorized or inappropriate traffic.
4. No workstations are allowed on the backbone of the network, where additional protections are applied.
5. All router ports are disabled so a workstation cannot be directly connected to the router without authorization.
6. There is a network management device on the network.

7. Network auditing occurs for every project being connected to the network and auditing is repeated every three years.
8. All projects must conduct a risk analysis of their project.
9. The network has rules of behavior that all users sign, accepting responsibility for their actions.
10. There are home-grown tools that help with automating auditing the logs and the routers.
11. Configuration management is used throughout the network
12. There are security awareness programs, lunchtime seminars, and other training measures.
13. Anti-virus software is run and updated regularly.
14. All network architecture has to be certified by the Network Security Officer's office.
15. Host and network defenses are implemented, including personal and project firewalls.
16. Network and host based vulnerability assessment tools are run on a regular basis, and vulnerabilities are corrected wherever possible.
17. Incident handling processes are in place.

These compensating controls mitigate the costs sited in the previous section by practicing defense in depth. They provide layers of defense so risk is reduced.

Future compensating controls that could be installed to improve the network:

1. A VPN server should be installed to regulate and protect traffic. Firewalls could installed on the remote VPN appliances.
2. An authentication server should be installed to regulate and protect traffic
3. Finish the planned implementation of the IDS.
4. Transition to Voice over IP in remote locations in order to fully utilize and dynamically allocate bandwidth.

Appendix A

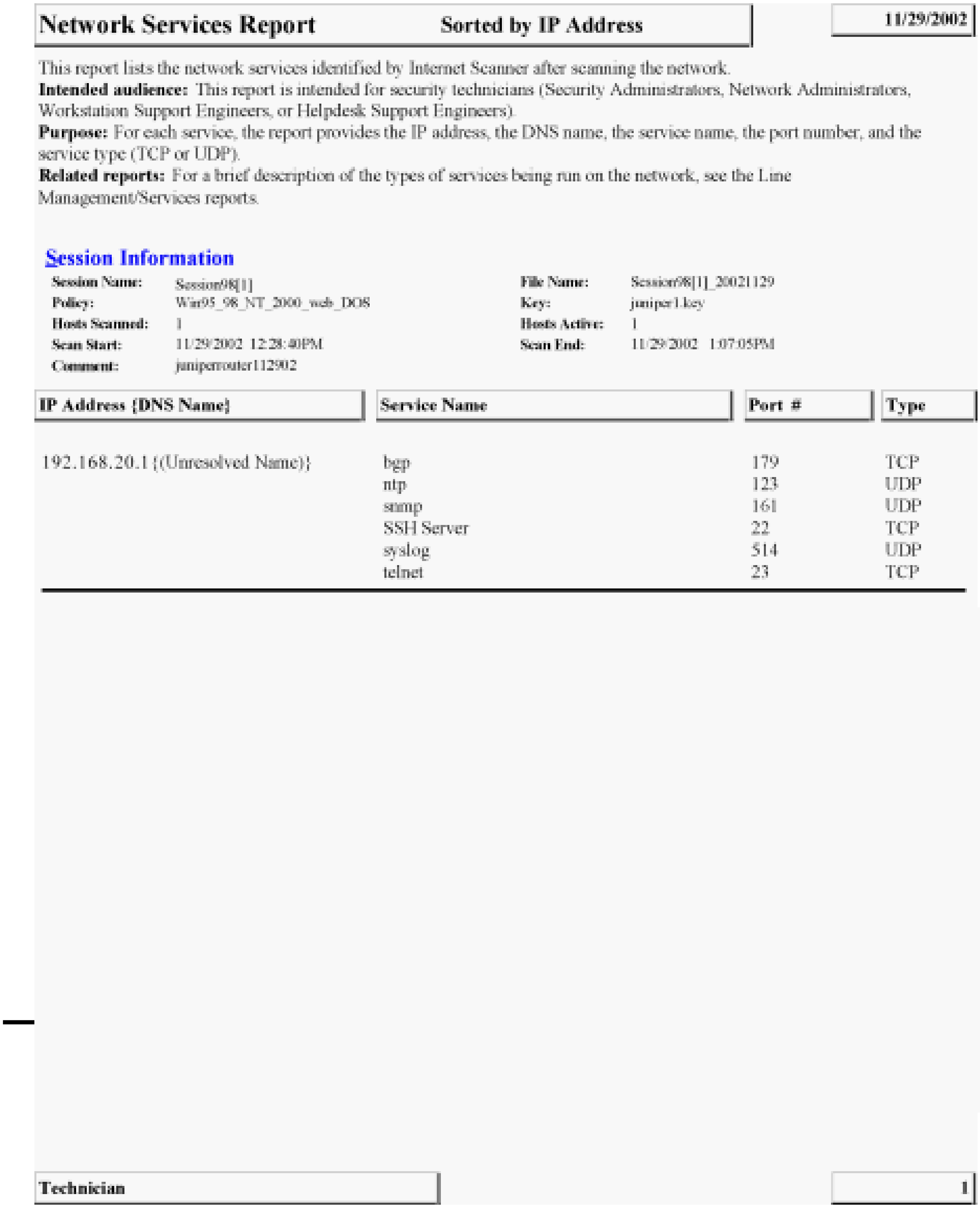
Physical Audit Checklist

Item	Comments
Are there guards?	
Are there key card readers?	
Are there cipher locks?	
Are there key locks?	
If key locks, do the keys work on more than one door?	
Are there drop ceilings?	
Are there raised floors?	
Does the room have windows?	
Does the door to room have a window?	
Are there any type of sensor detectors?	
Is networking hubs, switches, routers, etc., locked in a closet?	
Are network cables labeled?	
Is the wiring protected or exposed?	
Are there other projects equipment in the same closet?	
How many other projects have access to closet?	
Is the facility manned 24x7?	
If not, what hours is it manned?	
Do they require non-badged people to be escorted?	
Are there dial-in modem interfaces?	

Item	Comments
Do they use Uninterrupted Power Supplies (UPS)?	

Appendix B

11/29/2002



Network Services Report **Sorted by IP Address** 11/29/2002

This report lists the network services identified by Internet Scanner after scanning the network.
Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators, Workstation Support Engineers, or Helpdesk Support Engineers).
Purpose: For each service, the report provides the IP address, the DNS name, the service name, the port number, and the service type (TCP or UDP).
Related reports: For a brief description of the types of services being run on the network, see the Line Management/Services reports.

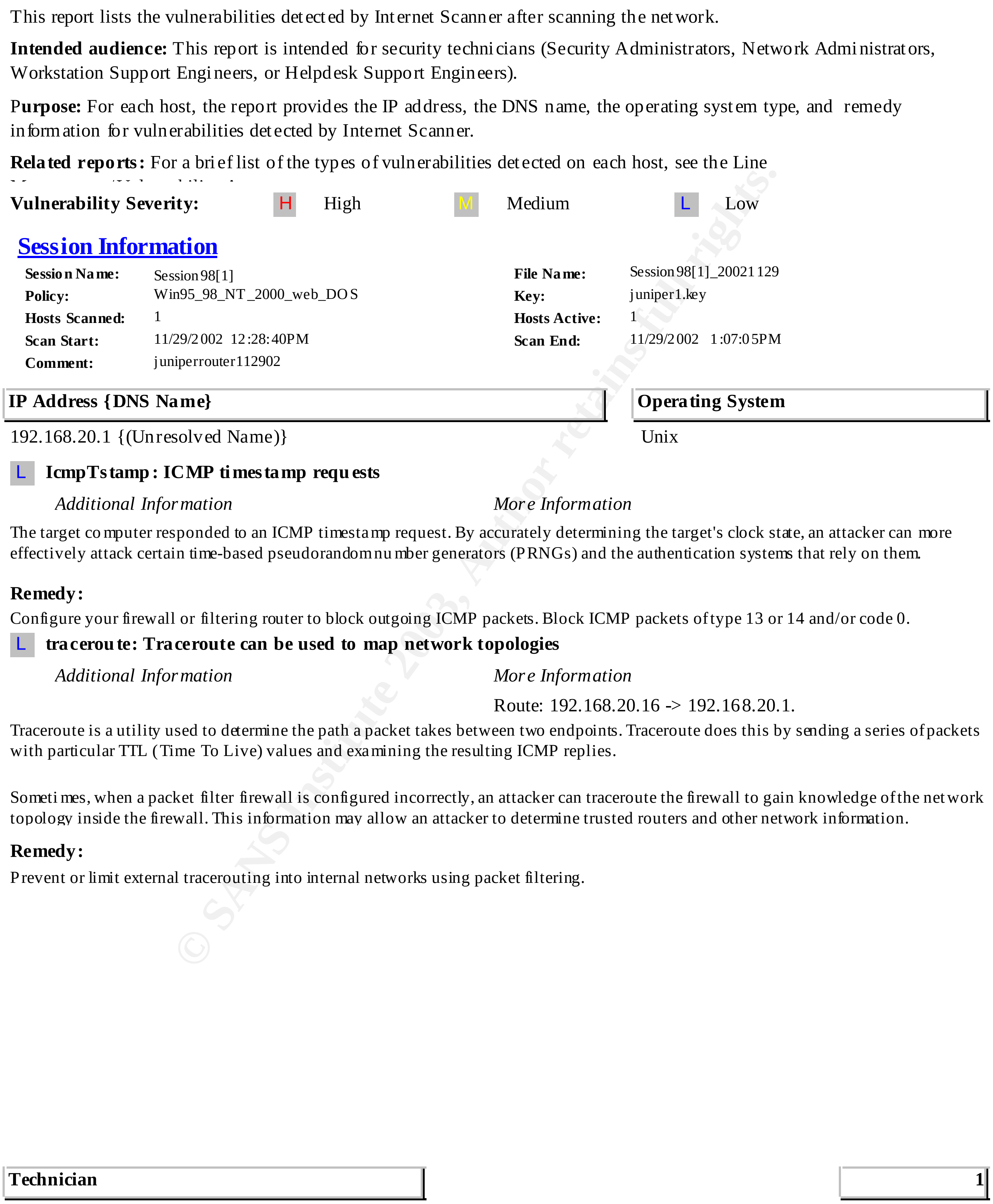
Session Information

Session Name:	Session98[1]	**File Name:**	Session98[1]_20021129
Policy:	Win95_98_NT_2000_web_DOS	**Key:**	juniper1.key
Hosts Scanned:	1	**Hosts Active:**	1
Scan Start:	11/29/2002 12:28:40PM	**Scan End:**	11/29/2002 1:07:05PM
Comment:	juniperrouter112902		

IP Address {DNS Name}	Service Name	Port #	Type
192.168.20.1 {(Unresolved Name)}	bgp	179	TCP
	ntp	123	UDP
	snmp	161	UDP
	SSH Server	22	TCP
	syslog	514	UDP
	telnet	23	TCP

Technician 1

Network Vulnerability Assessment Report **Sorted by IP Address**



This report lists the vulnerabilities detected by Internet Scanner after scanning the network.

Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators, Workstation Support Engineers, or Helpdesk Support Engineers).

Purpose: For each host, the report provides the IP address, the DNS name, the operating system type, and remedy information for vulnerabilities detected by Internet Scanner.

Related reports: For a brief list of the types of vulnerabilities detected on each host, see the Line

Vulnerability Severity: H High M Medium L Low

Session Information

Session Name:	Session98[1]	**File Name:**	Session98[1]_20021129
Policy:	Win95_98_NT_2000_web_DOS	**Key:**	juniper1.key
Hosts Scanned:	1	**Hosts Active:**	1
Scan Start:	11/29/2002 12:28:40PM	**Scan End:**	11/29/2002 1:07:05PM
Comment:	juniperrouter112902		

IP Address {DNS Name}	Operating System
192.168.20.1 {(Unresolved Name)}	Unix

L **IcmpTstamp: ICMP timestamp requests**

Additional Information *More Information*

The target computer responded to an ICMP timestamp request. By accurately determining the target's clock state, an attacker can more effectively attack certain time-based pseudorandom number generators (PRNGs) and the authentication systems that rely on them.

Remedy:

Configure your firewall or filtering router to block outgoing ICMP packets. Block ICMP packets of type 13 or 14 and/or code 0.

L **traceroute: Traceroute can be used to map network topologies**

Additional Information *More Information*

Route: 192.168.20.16 -> 192.168.20.1.

Traceroute is a utility used to determine the path a packet takes between two endpoints. Traceroute does this by sending a series of packets with particular TTL (Time To Live) values and examining the resulting ICMP replies.

Sometimes, when a packet filter firewall is configured incorrectly, an attacker can traceroute the firewall to gain knowledge of the network topology inside the firewall. This information may allow an attacker to determine trusted routers and other network information.

Remedy:

Prevent or limit external tracerouting into internal networks using packet filtering.

Technician 1

Appendix C

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 4
 - Number of security warnings found : 4
 - Number of security notes found : 7



TESTED HOSTS

 192.168.20.1 (Security holes found)



DETAILS

+ 192.168.20.1 :
 . List of open ports :
   o unknown (22/tcp) (Security hole found)
   o telnet (23/tcp) (Security warnings found)
   o unknown (179/tcp)
   o general/tcp (Security notes found)
   o general/icmp (Security warnings found)
   o ntp (123/udp) (Security warnings found)
   o general/udp (Security notes found)

 . Vulnerability found on port unknown (22/tcp) :
    You are running a version of OpenSSH which is older than 3.0.1.

    Versions older than 3.0.1 are vulnerable to a flaw in which
    an attacker may authenticate, provided that Kerberos V support
    has been enabled (which is not the case by default).
    It is also vulnerable as an excessive memory clearing bug,
    believed to be unexploitable.

    *** You may ignore this warning if this host is not using
    *** Kerberos V

    Solution : Upgrade to OpenSSH 3.0.1
    Risk factor : Low (if you are not using Kerberos) or High (if kerberos is
     enabled)

. Vulnerability found on port unknown (22/tcp) :



    You are running a version of OpenSSH which is older than 3.4

    There is a flaw in this version that can be exploited remotely to
    give an attacker a shell on this host.

    Note that several distribution patched this hole without changing
    the version number of OpenSSH. Since Nessus solely relied on the
    banner of the remote SSH server to perform this check, this might
    be a false positive.

    If you are running a RedHat host, make sure that the command :
              rpm -q openssh-server

    Returns :
     openssh-server-3.1p1-6



    Solution : Upgrade to OpenSSH 3.4 or contact your vendor for a patch
    Risk factor : High
```

```
   CVE : CAN-2002-0639

. Vulnerability found on port unknown (22/tcp) :



   You are running a version of OpenSSH older than OpenSSH 3.2.1

   A buffer overflow exists in the daemon if AFS is enabled on
   your system, or if the options KerberosTgtPassing or
   AFSTokenPassing are enabled.  Even in this scenario, the
   vulnerability may be avoided by enabling UsePrivilegeSeparation.

   Versions prior to 2.9.9 are vulnerable to a remote root
   exploit. Versions prior to 3.2.1 are vulnerable to a local
   root exploit.

   Solution :
   Upgrade to the latest version of OpenSSH

   Risk factor : High
   CVE : CAN-2002-0575

. Vulnerability found on port unknown (22/tcp) :



   You are running a version of OpenSSH which is older than 3.0.2.

   Versions prior than 3.0.2 are vulnerable to an environment
   variables export that can allow a local user to execute
   command with root privileges.
   This problem affect only versions prior than 3.0.2, and when
   the UseLogin feature is enabled (usually disabled by default)

   Solution : Upgrade to OpenSSH 3.0.2 or apply the patch for prior
   versions. (Available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH)

   Risk factor : High (If UseLogin is enabled, and locally)
   CVE : CVE-2001-0872

. Warning found on port unknown (22/tcp)



   The remote SSH daemon supports connections made
   using the version 1.33 and/or 1.5 of the SSH protocol.

   These protocols are not completely cryptographically
   safe so they should not be used.

   Solution :
    If you use OpenSSH, set the option 'Protocol' to '2'
    If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

   Risk factor : Low

. Information found on port unknown (22/tcp)


   An ssh server is running on this port

. Information found on port unknown (22/tcp)


   Remote SSH version : SSH-1.99-OpenSSH_2.3.0

. Information found on port unknown (22/tcp)


   The remote SSH daemon supports the following versions of the
   SSH protocol :

     . 1.33
     . 1.5
     . 1.99
     . 2.0
. Warning found on port telnet (23/tcp)



   The Telnet service is running.
   This service is dangerous in the sense that
   it is not ciphered - that is, everyone can sniff
   the data that passes between the telnet client
   and the telnet server. This includes logins
   and passwords.

   You should disable this service and use OpenSSH instead.
   (www.openssh.com)

   Solution : Comment out the 'telnet' line in /etc/inetd.conf.

   Risk factor : Low
   CVE : CAN-1999-0619

. Information found on port telnet (23/tcp)


   A telnet server seems to be running on this port

. Information found on port general/tcp


   Nmap found that this host is running Juniper Networks JUNOS 5.3 on an Olive
    router

. Warning found on port general/icmp




   The remote host answers to an ICMP timestamp
   request. This allows an attacker to know the
   date which is set on your machine.

   This may help him to defeat all your
   time based authentication protocols.
   Solution : filter out the ICMP timestamp
   requests (13), and the outgoing ICMP
   timestamp replies (14).

   Risk factor : Low
   CVE : CAN-1999-0524

. Warning found on port ntp (123/udp)



   An NTP server is running on the remote host. Make sure that
   you are running the latest version of your NTP server,
   has some versions have been found out to be vulnerable to
   buffer overflows.

   *** Nessus reports this vulnerability using only
   *** information that was gathered. Use caution
   *** when testing without safe checks enabled.

   If you happen to be vulnerable : upgrade
   Solution : Upgrade
   Risk factor : High
   CVE : CVE-2001-0414

. Information found on port ntp (123/udp)



   It is possible to determine a lot of information about the remote host
   by querying the NTP variables - these include OS descriptor, and
   time settings.

   Theoretically one could work out the NTP peer relationships and track back
   network settings from this.

   Quickfix: Set NTP to restrict default access to ignore all info packets:
    restrict default ignore
    Risk factor : Low

 . Information found on port general/udp



    For your information, here is the traceroute to 192.168.20.1 :
    192.168.20.1





------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

References

James Bayne, **An Overview of Threat and Risk Assessment,** http://rr.sans.org/audit/overview.php**,** SANS Information Reading Room**,** January 22, 2002.

CERT, http://www.cert.org/.

CERT, http://search.cert.org/query.html?rq=0&ht=0&qp=&qs=&qc=&pw=100%25&ws=1&la=&qm=0&st=1&nh=25&lk=1&rf=2&oq=&rq=0&si=1&col=allcert&col=trandedu&col=vulnotes&col=techtips&col=research&col=certadv&col=incnotes&col=secimp&qt=juniper+router+bulletins&x=16&y=11.

CIAC, http://www.ciac.org/cgi-bin/index/bulletins.

Cisco, Improving Security on Cisco Routers, http://www.cisco.com/warp/public/707/21.html, 11/2/2002.

Cisco Systems, Cisco IOS Software Command Summary, Release 11.1, San Jose, CA., Cisco Systems, Inc.

CobiT, Control Objectives for Information and related Technology (COBIT®), http://www.isaca.org/ct_dwnld.htm. 2000.

Mark Hill, 'Audit and Control Checklist for the Elron Internet Manager (IM) Firewall: An Auditor's Perspective', www.giac.org/practical/Mark_Hill_GSNA.doc, GSNA Practical version 2.0, February 2002.

Juniper Networks, Inc., Juniper System Overview, http://www.juniper.net/techpubs/hardware/m5-m10/m5-m10-hwguide/download/overview-system.pdf. 10/09/02.

Juniper Networks, Inc., JUNOS Internet Software Configuration Guide, Getting Started, Release 5., Sunnyvale, CA, Juniper Networks, Inc. 2002. URL: http://www.juniper.net/techpubs/software/junos51/swconfig51-getting-started/frameset.htm.

Juniper Networks, Inc., JUNOS Internet Software Configuration Guide, Routing and Routing Protocols Release 5.1, Sunnyvale, CA, Juniper Networks, Inc. 2002, URL: http://www.juniper.net/techpubs/software/junos51/swconfig51-routing/frameset.htm.

NASA, Information Technology Security Plan Format, http://code297.gsfc.nasa.gov/docs/doc-templates.htm#sec-plans, June 2001.

NASA, IP Operational Network (IONet) Security Plan, October 2000.

NASA, NASA Procedures and Guidelines, NPG 2810.1, URL: http://nodis.gsfc.nasa.gov/library/npg_sort.cfm, 26 August 1999.

NSA/SNAC Router Configuration Guide, http://www.nsa.gov/snac/cisco/download.htm, July 9, 2002.

SANS Institute, Router Security Policy, http://www.sans.org/newlook/resources/policies/Router_Security_Policy.pdf.

SANS Institute, Track 1 – LevelOne SANS Security Essentials, The SANS Institute, May 2001.

SANS Institute, Track 7 – Auditing Networks, Perimeters and Systems, The SANS Institute, 2002.

Darrin Wassom, 'Auditing a Distributed Intrusion Detection System: An Auditors Perspective', www.giac.org/practical/Darrin_Wassom_GSNA.doc, GSNA Practical version 2.0, July, 2002.