



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

Auditing a Cisco A Cisco 1721 Router: An Auditor's Perspective

Ray Welshman
February 18, 2004
GSNA Practical Assignment 3.0

Abstract/Summary

This paper deals with a comprehensive audit of a typical small office/home office environment that purchased their internet connection from an ISP. The company in this instance is a small law firm (fictitious name of XYZ Law). The service purchased from the ISP is a 1721 Router connected to the internet via DSL connection. The configuration and management of the router is outsourced to the ISP. This audit deals with the router only and its associated risks, not the IT infrastructure behind it. Research has been conducted on the recommended security of Cisco routers in general and has been applied in this case.

The audit contains the following as pertaining to the Cisco 1721 Router:

- System Identification
- Risks to the router
- Research References
- A checklist to identify possible weaknesses and exposures
- Audit results and recommendations

Although this paper is concerned with a 1721 device it can be used as a basis to help conduct an audit on similar routers with Cisco IOS in similar scenarios

Table of Content

ASSIGNMENT 1: RESEARCH IN AUDIT, MEASUREMENT, PRACTICE AND CONTROL.....	4
INTRODUCTION	4
1.1 SYSTEM TO BE AUDITED	5
1.2 RISK ASSESSMENT/EVALUATION	7
1.2.1 <i>Company Practices</i>	8
1.2.2 <i>Technical Risk Assessment/Evaluation</i>	10
1.2.3 <i>Current State of Practice</i>	12
2. CREATE AN AUDIT CHECKLIST	14
2.1 GENERAL CHECKLIST	15
2.2 CISCO SPECIFIC CHECKLIST	44
3. CONDUCT THE AUDIT.....	61
3.1 AUDIT – GENERAL CHECKLIST	62
2.2 CISCO SPECIFIC CHECKLIST	109
PART 4 – AUDIT REPORT.....	126
EXECUTIVE SUMMARY	126
4.1 AUDIT FINDINGS.....	126
4.2 AUDIT RECOMMENDATIONS	130
4.2.2 <i>General Recommendations</i>	130
4.2.3 <i>Exception Specific Recommendations</i>	131
4.2.4 <i>Summary</i>	134
5. REFERENCES	134
APPENDIXES	135
APPENDIX A – NESSUS SCAN RESULTS	135
APPENDIX B – ROUTER AUDITING TOOL (RAT) RESULTS	139
APPENDIX C – SHOW TECH-SUPPORT RESULT	144

Tables

Table 1 - Cisco 1721 Router Specifications	6
--	---

Table of Figures

Figure 1: Office Network.....	5
Figure 2 - Cisco 1721 (copied from Cisco Website)	6
Figure 3: Rear View of Cisco 1721 (copied from Cisco)	7

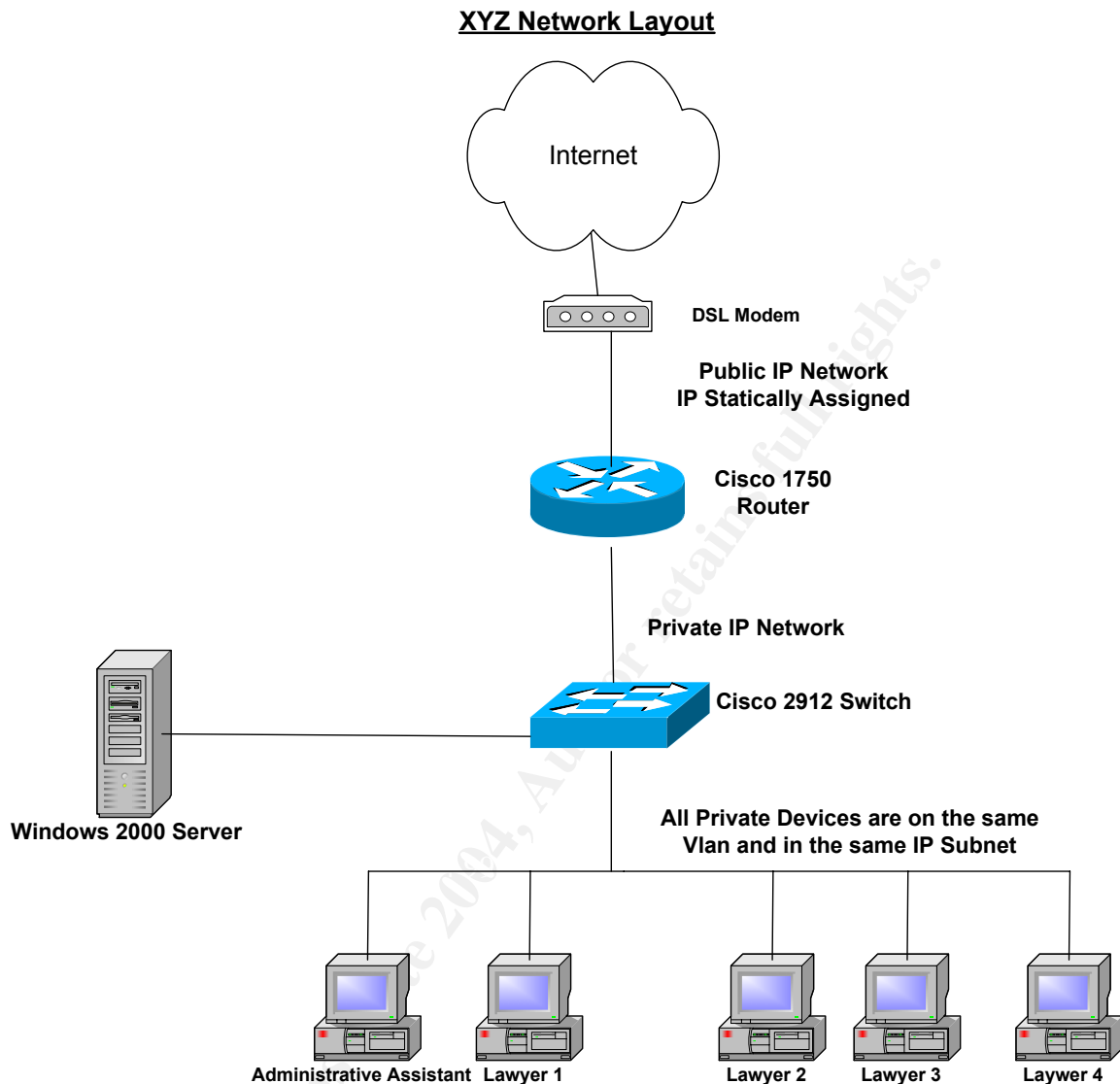
Assignment 1: Research in Audit, Measurement, Practice and Control

Introduction

Company XYZ(fictitious name) is a law firm. The firm consists of four lawyers with one administrative assistant. Each lawyer has a private office and the administrative assistant is in the reception area. There is one Windows 2000 server that provides file and print capabilities. The firm utilizes a Cisco 1721 router as its primary perimeter defense device. The primary and only connection to the internet is a DSL connection. The IT infrastructure of this law firm is outsourced to a consultant firm, including the configuration and management of the 1721 router. XYZ Law has requested an independent audit of the Cisco 1721 to ensure that the perimeter of their IT infrastructure is protected.

© SANS Institute 2004, Author retains full rights.

Figure 1: Office Network



1.1 System to Be Audited

I am auditing a Cisco 1721 Router that is running Cisco IOS 12.2 The Router is the primary perimeter defence to protect XYZ Law's server, PC's, and the sensitive client files from possible internet intrusion. The Router is meant to perform traffic/packet filtering and as a gateway to the public internet.

XYZ Law has no security policy written or verbal so the 1721 Router will be audited against industry best practices.

This audit is to investigate the Cisco 1721 only. The assessment will cover the following:

- physical security
- Configuration review
- Penetration Tests
- Change management/System Administrator procedures

Table 1 - Cisco 1721 Router Specifications

Manufacturer	Cisco
Name of Device	Cisco 1721 Series Router
Intended Market	Small/Medium Business
Software	<p>Software on this router IOS Version 12.2(15)T9, System Bootstrap, Version 12.2(7r)</p> <p>Software Features supported Supports IP, IPX, AppleTalk, IBM, Open Shortest Path First (OSPF), NetWare Link Services Protocol (NLSP), Resource Reservation Protocol (RSVP), encryption, network address translation, and the Cisco IOS Router Feature Set.</p>
Processor	MCP860P
Memory	64MB Ram , 16 MB Flash
Interfaces	1 Ethernet/IEEE 802.3 interface(s) 1 FastEthernet/IEEE 802.3 interface(s)

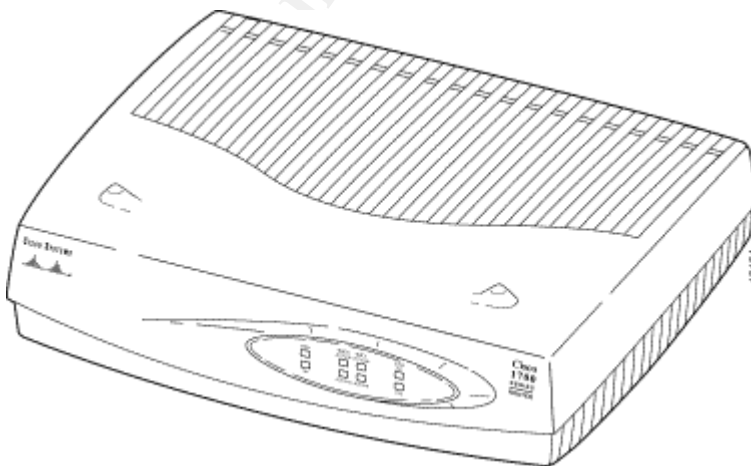
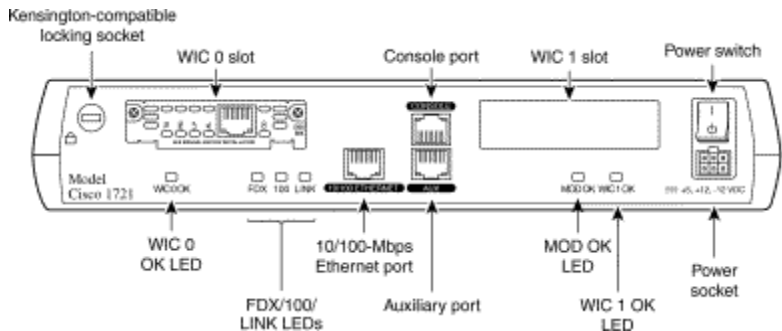
Figure 2 - Cisco 1721 (copied from Cisco Website)

Figure 3: Rear View of Cisco 1721 (copied from Cisco)



For further information on the Cisco 1721 Router products please refer to the following website:

http://www.cisco.com/en/US/products/hw/routers/ps221/products_installation_guide_book09186a008007e585.html

1.2 Risk Assessment/Evaluation

A risk assessment is to determine the **threat** to the system being audited.

The following definition of a threat was taken from the course material of SANS course ILOT Track VII – Auditing Networks file: audit_day4_0403.pdf Slide 2-9

“A threat is a circumstance, condition, or event with the potential to cause harm to personnel and/or network resources in the form of destruction, disclosure, and modification of data, denial of service, and/or fraud, waste, and abuse”

Karen Olsen, NIST Special Publication 800-7 July 1914

In this particular scenario I will be looking at the risks associated to the Cisco 1721 router. If the router is compromised in any way it could lead to serious consequences to XYZ Law. The files and information the router is protecting are very sensitive and hold important information about clients and law cases from the past and current ongoing projects.

The risk assessment will be divided into two categories:

Company Practices – this is described as how the company utilizes the router and how it is managed

Technical – this is described as the technical use of the device and how it is deployed.

Each risk will be evaluated by utilizing the following criteria:

- Type of Risk (Control)
- Possibility of Event Occurring
- Risk Level
 - i. Low – Will affect operations but not put the company out of business
 - ii. Medium – Will affect day to day operations but the company will continue to operate but at a less efficient rate.
 - iii. High – This will affect the company in a very severe way i.e. loss of business or significant loss efficiency.
- Result (Possible result of the perceived risk)

1.2.1 Company Practices

This is described as the daily work operations of the company whose activities may affect the Router operation.

1. Physical Location – Where and how the device is stored and how it is accessed	
Risk	Location of the device will determine physical security in the sense on how easy it is to access the device(s) Temperature and Humidity control will determine working conditions for the device(s)
Possibility	Medium – The office environment is generally kept to comfort zones which the router can operate. The router is a small device and can be easily secured.
Risk Level	High
Result	If device is stolen all relevant configuration information such as IP addresses (private and public) information flow can be obtained. Cost of replacing the device which would also include professional service cost to configure and install the device

2. System Administration – Personnel that manages/configure the Router	
Risk	Router configuration/management is outsourced to a local consultant company. Personnel in XYZ Law have put total trust in this company. XYZ Law has little or no knowledge of Router operations
Possibility	Low – Consultant Firms generally have trained and

	trustworthy employees
Risk Level	High
Result	<p>The sys admin is not a member of XYZ Law and he/she has the ability to open a door to all sensitive client information stored on local PC's and file server.</p> <p>If the sensitive files of XYZ Law are compromised it may lead to legal action against the firm.</p> <p>This may also result in loss of Client trust which may lead to significant loss of business.</p>

3. Internal Personnel – The end users in XYZ Law	
Risk	<p>Administrative Assistant and the Law Partners have very little knowledge of IT operations and may unknowingly while surfing the internet download malicious software which may result in the corruption or loss of sensitive data.</p> <p>Malicious software may also damage PC's and servers which may put XYZ Law out of commission.</p>
Possibility	Medium – Although the use of PC software is generally well known individuals constantly through unknown acts infect their PC's
Risk Level	Medium
Result	<p>Destruction or loss of sensitive files may lead to loss of client trust which may lead to significant loss of business.</p> <p>Time and effort to replace or reacquire this information may be costly and time consuming which may result in XYZ Law missing required deadlines which in turn may lead to significant loss of business.</p>

4. Disgruntled Employee(s) – Administrative Assistant and Partner Lawyers	
Risk	Employee(s) may be disgruntled and purposely damage the router or allow individuals with malicious intent access to the router
Possibility	Low – XYZ Law is a small company with a small amount of employees that generally work well together
Risk Level	High
Result	<p>This could lead to a compromise of the internal network resulting in compromise of sensitive client files which in turn would result of possible legal action and/or loss of customer confidence. This</p>

	will damage the Firm's reputation and result in loss of business. If the router device is damaged there is a cost of replacing and also professional services cost to install and configure the device.
--	--

5. Lack of Security Policy to control Router Activities	
Risk	Lack of direction for company internet activities may lead to mis-configuration of the router which in turn may compromise the intended intent of the router
Possibility	Medium – The default configuration of the Cisco 1721 has known openings. The consultant who manages this router should be competent enough to adequately configure the Router.
Risk Level	High
Result	Possible compromise of the perimeter defence may result in exposing sensitive client files which may result in legal action or loss of customer confidence which in turn may result in loss of business.

1.2.2 Technical Risk Assessment/Evaluation

This is described as the risk to the Router device from a technical outlook. This will look at hardware/software configuration of the 1721 router.

1. Router May be open to Internet Scans (i.e. port scans, ping sweeps etc)	
Risk	Through these scans hackers (professionals and scrip kiddies) may discover the XYZ Law Network.
Possibility	High – The Hacker community is constantly scanning the public internet looking for responses
Risk Level	High
Result	If the router is discovered any inquisitive individual will or may try to test the defences of the router and exploit it. If the attack is successful then XYZ Law and their sensitive client documentation may be compromised. Once past the Router the hacker may destroy information or make the PC's/servers unusable resulting in a shutdown of all operations

2. Denial of Service Attack	
Risk	Hackers through malicious activity may attack the router and through common known tools and techniques may bring down the router and make it unusable
Possibility	High – Denial of Service can come in many forms viruses, worms, or direct attacks such as ping or tcp attacks.
Risk Level	Medium – although the router is out of commission XYZ Law would still be able to function without internet activity
Result	There may be a cost to bring the router back online through professional services.

3. Configuration Errors	
Risk	System Admin may mis-configure the router resulting in allowing individuals with malicious intent to bypass the router security.
Possibility	Low – The router is outsourced to a competent consultant firm
Risk Level	High – If the router has an opening it may allow access to sensitive client information
Result	Possible compromise or the perimeter defence may result in exposing sensitive client files which may result in legal action or loss of customer confidence which in turn may result in loss of business.

4. Router Upgrades – Software or hardware upgrade (i.e. patches/bugs etc)	
Risk	Router is upgraded without proper testing in a safe environment
Possibility	High – May upgrade procedures are not fully tested when released by the vendor and may have adverse results on a production device
Risk level	High – an untested upgrade procedure may either damage the router or leave substantial security flaws in the router
Result	Possible compromise or the perimeter defence may result in exposing sensitive client files which may result in legal action or loss of customer confidence which in turn may result in loss of business.

	There may be a cost to bring the Router back online through professional services.
--	--

5. Hardware Failure	
Risk	Device Fails
Possibility	Low – Cisco routers are very reliable
Risk Level	Low – XYZ Law can continue to operate without internet access
Result	Router will have to be replaced or repaired. If under warranty this will be replaced. If the device is supplied by the consultant firm then it should be replaced as well. There may be a replacement cost if XYZ Law actually owns the device.

1.2.3 Current State of Practice

The Cisco router product line has been available for some time and is a popular choice among Service Providers, Enterprise Networks, and small office/home office users. The following is a list of resources used to perform research on this audit and to compile a checklist:

- www.cisco.com
- www.cisecurity.com
- <http://www.isecom.org/projects/osstmm.shtml>
- <http://nsa2.www.conxion.com/cisco/download.htm>
- www.sans.org
- ILOT TRACK VII Course Material
- <https://cassandra.cerias.purdue.edu/main/index.html>
- “Auditing a Cisco Pix Firewall: An Auditor Perspective” Rick W Yuen April 2003 GSNA Assignment Version 2.1
http://www.giac.org/practical/GSNA/Rick_Yuen_GSNA.pdf
- SANS ILOT Track VII Course Material
- “Firewall Checklist” by Krishni Naidu
<http://www.sans.org/score/checklists/RouterChecklist.doc>
- <http://www.spitzner.net/audit.html> - Lance Spitzner online white paper
- www.nessus.org
- <http://www.insecure.org>
- <http://www.hping.org/>

Cisco systems have a very intuitive website with a wealth of information about their products. They will provide white papers, product information, upgrade procedures, software, technical support, known bugs, and suggested sample configurations. To access some of this information an online account is required. Through my search on the Cisco Website I was unable to discover if a vulnerability/security checklist was available for the Cisco 1721 Router. For an up to date list of security advisories please check here:

http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html

The Center for Internet Security offer methods and tools to test several devices against a benchmark. These benchmarks are very thorough and in the interests of this document CIS offers a benchmark for Cisco routers. The tool provided is the Router Auditing Tool or RAT. This is an automated tool that can be used to determine a routers current security level. The router in this particular audit was tested to match CIS Router Benchmark 1. The benchmark document "Center for Internet Security Benchmark for Cisco IOS – Level 1 and 2 Benchmarks Version 2.0" provides a very detailed audit checklist for Cisco IOS routers.

The Institute for Security and Open Methodologies provide an excellent document "OSSTMM 2.1" Open-Source Security Testing Methodology Manual created by Pete Herzog. This is a very comprehensive manual that can be used as a guideline to conduct a security audit. It has checklists, procedures, and sample reports.

The National Security Agency has excellent reference material for securing Cisco Routers.

The SANS site and its list of top 20 vulnerabilities is valuable tool for security audits. It is also a central point for a vast amount of information in the form of white papers and online seminars.

The course material is the backbone and guideline for preparing this paper.

The Cassandra site is used to look for updated vendor/system vulnerabilities. A logon account is required and you can set up a profile on certain products if you like.

Mr. Yeun's GSNA paper is very helpful to get started with regarding to getting started on an IOS checklist and points of his paper may be adapted to many perimeter scenarios.

Mr. Naidu's paper as stated in Mr.Yeun's GSNA practical is a neutral checklist that can be applied to any perimeter scenario.

The final websites mentioned are examples of tools used to carry out the technical portion of the checklist. Nessus is an industry recognized vulnerability scanner, Nmap is a tool used to map out networks, and Hping is another tool used to run icmp scans on a host.

2. Create an Audit Checklist

The following checklist is designed to audit the Cisco 1721 at XYZ Law. This checklist can apply to other similar scenarios. The checklist will correlate with the risks laid out in Section 1.2 in this document. XYZ Law has no Security Policy so the checklist will outline Industry Best Practices and vulnerabilities common to all Routers.

Any penetration tests in this audit require the written permission of XYZ Law. It is recommended that the checklist be reviewed with the System Administrator responsible for the Cisco 1721 Router. The local ISP will be contacted to inform them that I will be conducting an audit on one of their customer's router.

The checklist will be divided into two categories:

General – this is a checklist designed to test general deployment of routers.

Cisco Specific – this checklist is based on Cisco published security advisories of the 1700 series routers and their IOS.

GSNA Practical 3.0

2.1 General Checklist

Checklist Item 1	
Reference	OSSTMM 2.1 Manual Page 87-92 Personal Experience, “Auditing a Pix Firewall: An Auditor’s Perspective” Rick W Yuen 2003 GSNA Assignment Version 2.1
Objective	Physical Security
Risk	Physical Location Section 1.2.1
Test	This is test is in the form of an office inspection conducted by the Auditor with the permission of XYZ Law <ol style="list-style-type: none"> 1. Is the router Locked in a Secure Area 2. Is the access controlled to the location of the router 3. Is there an authorized list of persons who can access the router 4. In the location of the router, does it meet safe environmental conditions i.e temperature and humidity 5. Does the area have an intrusion alarm system
Objective/Subjective	Subjective

Checklist Item 2	
Reference	Personal Experience
Objective	Determine Process and Ability of Outsourced System Admin
Risk	2. System Administration Section 1.2.1 Section 1.2.2 5 Hardware/Software upgrades
Test	This test is conducted in the form of an interview with the System Administrator

GSNA Practical 3.0

	<ol style="list-style-type: none"> 1. What is your experience with the Cisco IOS Software? 2. Is there proactive management of the router 3. Are configuration changes done remotely or on site 4. Are configuration changes confirmed with XYZ Law 5. Are configuration changes, hardware/software changes tested in a safe environment first before going to Production
Objective/Subjective	Subjective

Checklist Item 3	
Reference	Personal Experience, OSSTM Manual P.41 (Note in this manual the purpose of the test it try and get information from trusted employees, I feel that is not necessary here in that just the router is being audited so I've taken the idea and modified the direction determine how the employee can adversely affect the router)
Objective	Determine possible affects employees will have on router Operation
Risk	Section 1.2.1 (3) and (4)
Test	<p>This test will be conducted in the form of a personal interview with XYZ law's Employees</p> <ol style="list-style-type: none"> 1. How long have you been with the company? 2. What is your position 3. What is your general use of the internet (i.e. downloads, email, chats, etc) 4. Do you know what the router is and what it is used for? 5. What is your general overall feeling about the company?
Objective/Subjective	Subjective

GSNA Practical 3.0

Checklist Item 4	
Reference	OSSTMM 2.1 Manual P.47/55 Section 8 www.cisco.com – 1700 Series Router quick installation guide and configuration guides Own experience
Objective	Verify the router type and Software Version
Risk	No Risk associated – Information Gathering and confirmation
Test	<ol style="list-style-type: none"> 1. Connect the RJ-45 end of the console cable to the CONSOLE port on the back panel of the router, 2. Connect the DB-9 end of the console cable to the console port (also called the <i>serial port</i>) on your PC. If this adapter does not fit your PC console port, you must provide an adapter that fits. 3. Open a HyperTerminal Session to the router. Ensure the following settings are set: <ol style="list-style-type: none"> i. connect using com ports usually Com1 ii. terminal keys is checked iii. Ctrl-H is checked iv. Emulation is Auto detect v. Terminal ID is ANSI vi. Port settings are: 9600,databits 8, parity none, stop bits 1, flow control none 4. Login to the router (note this may be done with the system administrator). To accomplish this: <ol style="list-style-type: none"> i. Hit enter once session starts the following prompt appears: ii. Router> iii. You then type enable you will then be prompted for a password, enter the password. The following is how it will look on a Cisco router

GSNA Practical 3.0

	<p>Press RETURN to get started.</p> <p>xxxxx Internet IISP You must agree to the following before using this system</p> <p>Use of this system is restricted to authorized employees of xxxxx Inc. and authorized contractors. Only authorized work using company-supplied programs may be done on this system. Use of this system is an agreement to monitoring.</p> <p>User Access Verification</p> <p>Password: xxxxxxxxxxxx xyzlaw>en Password: xxxxxxxxxxxx xyzlaw#</p> <p>iv. Type show version this will supply the software and firmware version</p> <p>An example of this layout is:</p> <p>xyzlaw#show version Cisco Internetwork Operating System Software IOS (tm) C1700 Software (C1700-BK8NO3R2SY7-M), Version 12.2(15)T9, RELEASE SOFTWARE (fc2) TAC Support: http://www.cisco.com/tac Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Sat 01-Nov-03 06:24 by ccai</p>
--	--

GSNA Practical 3.0

	<p>Image text-base: 0x80008120, data-base: 0x81207F5C</p> <p>ROM: System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1) ROM: C1700 Software (C1700-BK8NO3R2SY7-M), Version 12.2(15)T9, RELEASE SOFTWARE (fc2)</p> <p>xyzlaw uptime is 1 day, 43 minutes System returned to ROM by power-on System image file is "flash:c1700-bk8no3r2sy7-mz.122-15.T9.bin"</p> <p>cisco 1721 (MPC860P) processor (revision 0x100) with 58002K/7534K bytes of memory. Processor board ID FOC07010MUR (2301023196), with hardware revision 0000 MPC860P processor: part number 5, mask 2 Bridging software. X.25 software, Version 3.0.0. 1 Ethernet/IEEE 802.3 interface(s) 1 FastEthernet/IEEE 802.3 interface(s) 32K bytes of non-volatile configuration memory. 16384K bytes of processor board System flash (Read/Write)</p> <p>Configuration register is 0x2142</p> <p>xyzlaw# v. Type show running- config this will display the current running configuration on the device.</p> <p>An example of this layout is:</p>
--	--

GSNA Practical 3.0

	<pre>xyzlaw#show running-config Building configuration... Current configuration : 1481 bytes !version 12.2 service timestamps debug datetime localtime service timestamps log datetime localtime service password-encryption hostname xxxx logging queue-limit 100 logging buffered 4096 debugging enable password 7 xxxxxxxxxxxx ip subnet-zero no ip domain lookup ip audit notify log ip audit po max-events 100 interface Ethernet0 description Customer LAN Segment ip address xxx.xxx.xxx.xxx 255.255.255.248 shutdown half-duplex no cdp enable interface FastEthernet0 description Connection to ISP ip address xxx.xxx.xxx.xxx 255.255.255.252 shutdown speed auto no cdp enable ip classless ip route 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx no ip http server</pre>
--	--

GSNA Practical 3.0

```

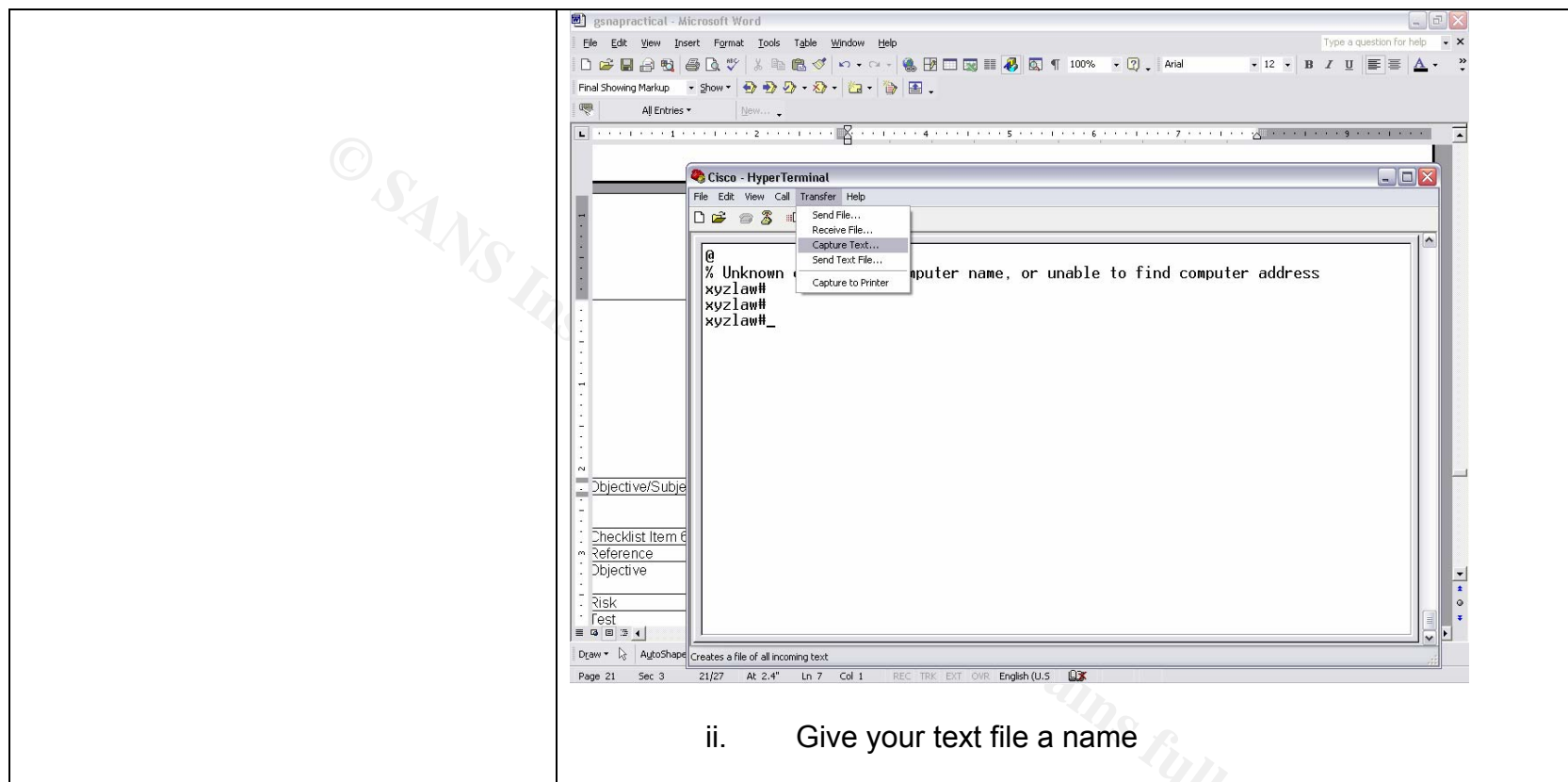
no ip http secure-server
access-list 10 permit xxx.xxx.xxx.xxx
no cdp run
snmp-server location xxxxxxxxxxxxxxxxx
snmp-server contact xxxxxxxxxxxxxxxxxxxsnmp-server enable traps tty
banner motd ^C
        xxxxx Internet IISP
        You must agree to the following before using this system

        Use of this system is restricted to authorized employees of
        xxxxx Inc. and authorized contractors.Only authorized work using
        company-supplied programs may be done on this system.Use of this
        system is an agreement to monitoring.
line con 0
exec-timeout 0 0
password 7 xxxxxxxxxxxxxxxxxxxxxxxx
login
line aux 0
line vty 0 4
access-class 10 in
exec-timeout 30 0
password 7 xxxxxxxxxxxxxxxxxxxxxxxx
login
no scheduler allocate
end
xyzlaw#

5. Save information gathered in a text file.
    i. Go to the transfer option on top of the session page
        chose "capture text"

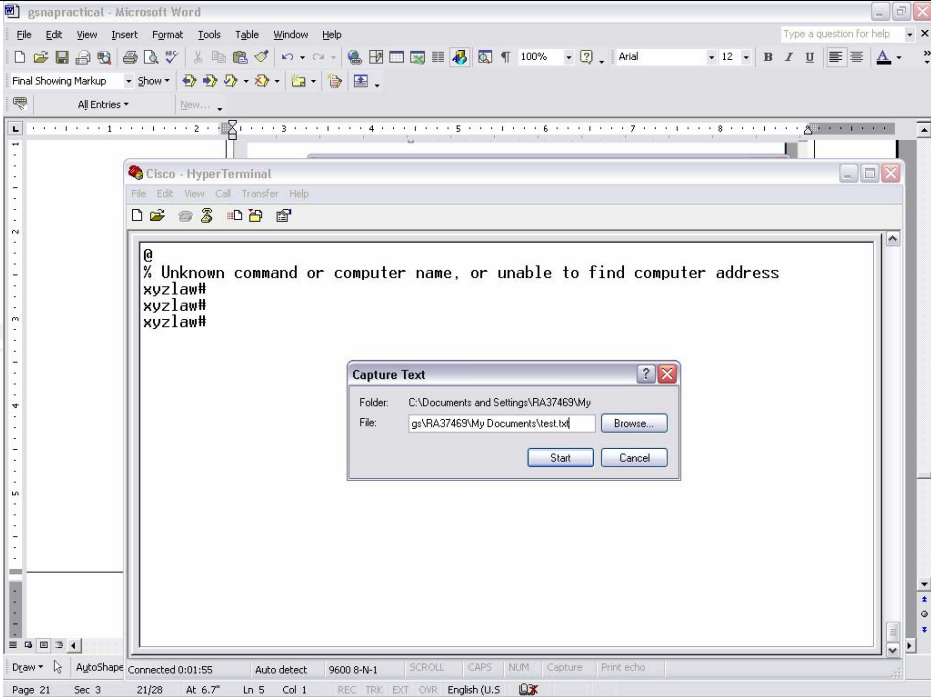
```

GSNA Practical 3.0



ii. Give your text file a name

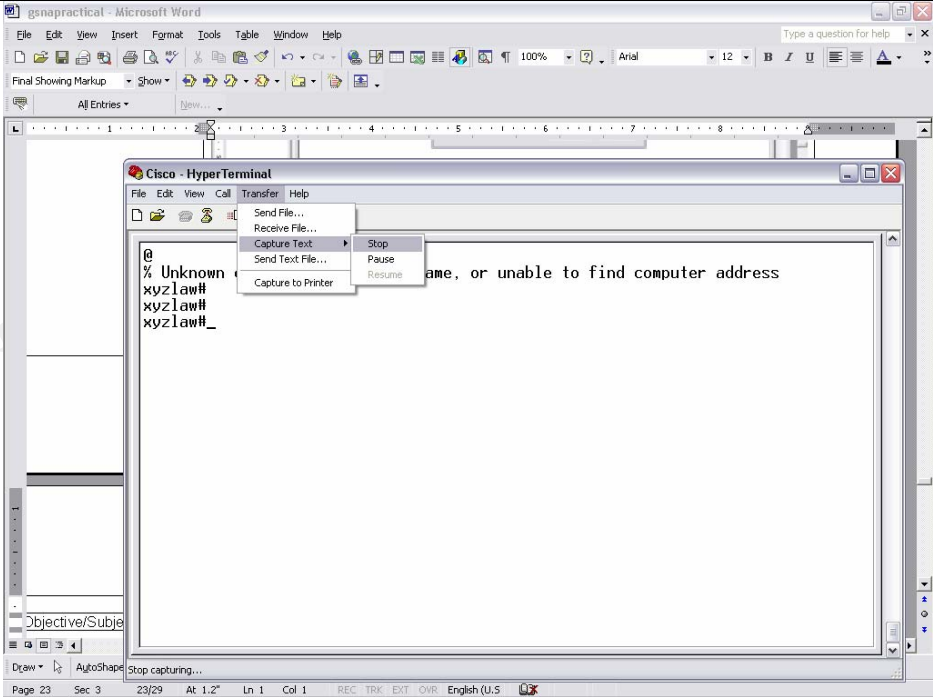
GSNA Practical 3.0



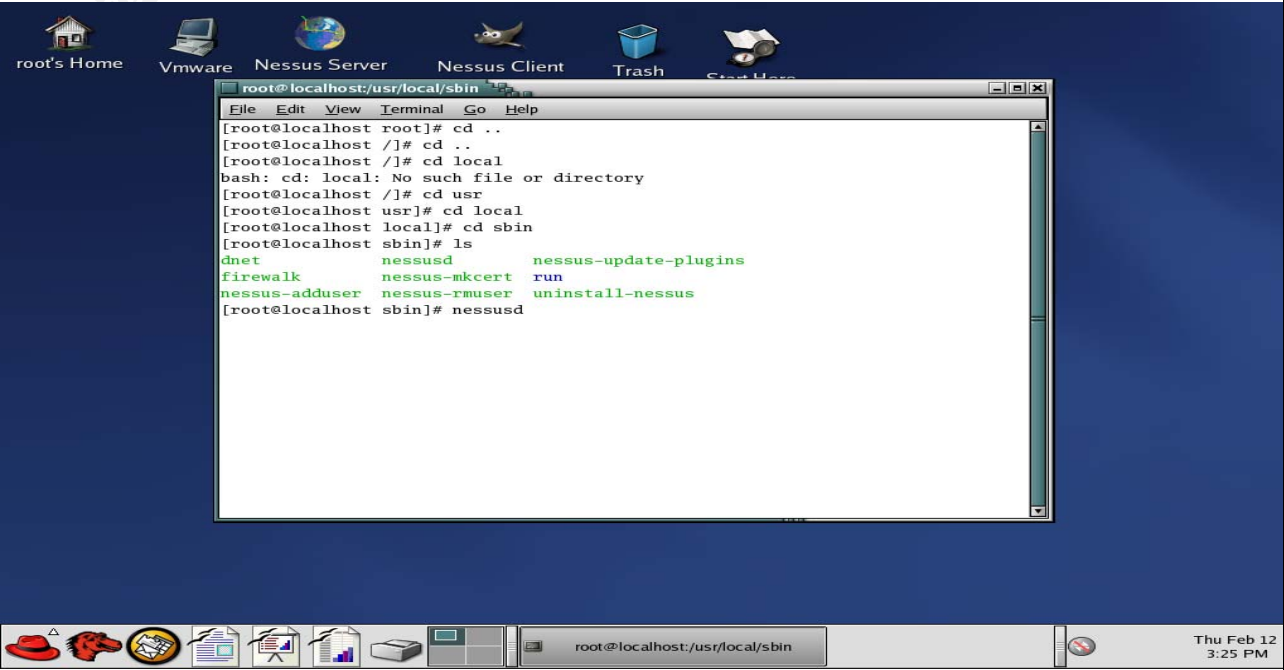
iii. perform the above mentioned show commands

iv. Go to transfer again, choose capture text and then choose “stop” at the dropdown menu.

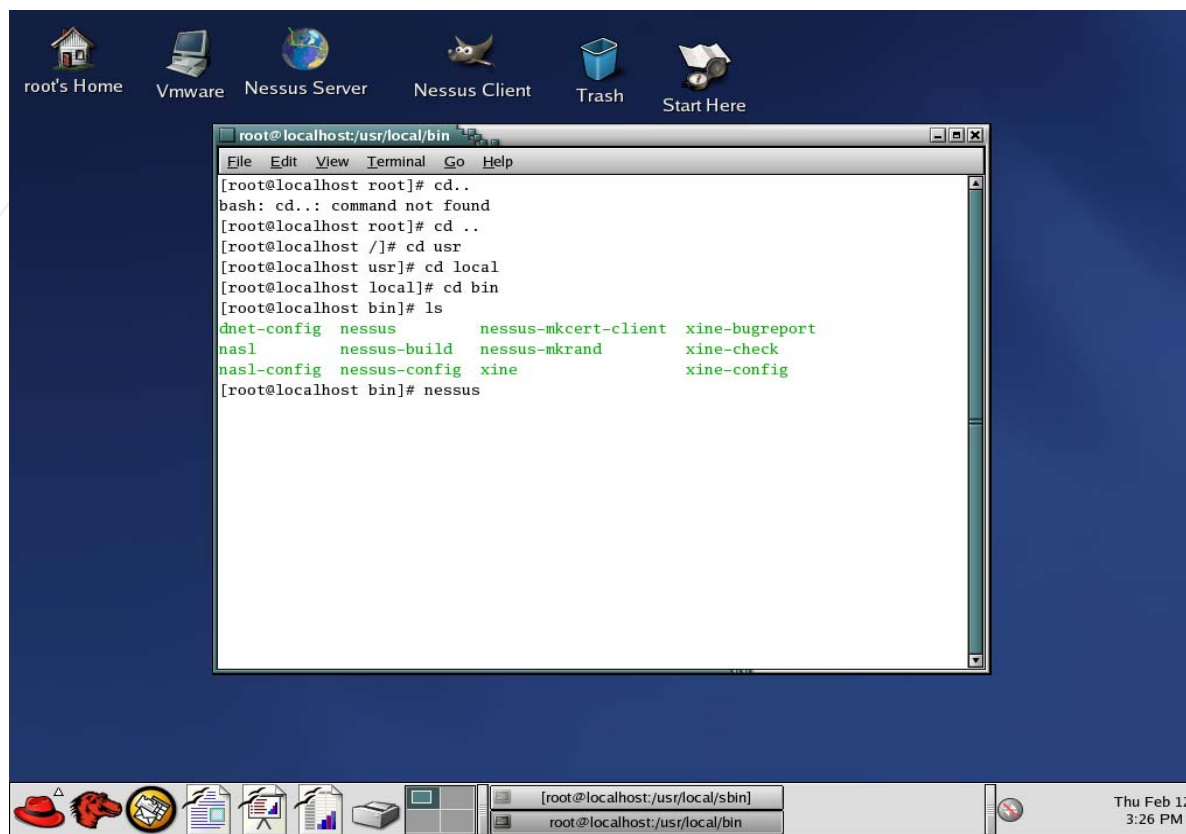
GSNA Practical 3.0

	<div data-bbox="766 240 1692 933"></div> <div data-bbox="814 971 1745 1044"><p>6. For a full comprehensive view of the router configuration at the router prompt type:</p></div> <div data-bbox="863 1081 1239 1117"><p>Router#show tech-support</p></div> <div data-bbox="863 1154 1780 1263"><p>This is quite a large file and passwords are left out by default. An example of the print out of the results of this are in Appendix C of this document.</p></div> <div data-bbox="174 1300 478 1339"><p>Objective/Subjective</p></div> <div data-bbox="766 1300 900 1339"><p>Objective</p></div>
--	---

GSNA Practical 3.0

Checklist Item 5	
Reference	OSSTMM 2.1 Manual P.47 Section 3
Objective	Utilize Nessus Vulnerability Scanner to determine vulnerabilities from the internet.
Risk	Section 1.2 (1) router may be open to internet scans
Test	<p>To be performed by the Nessus Port Scanner. This assumes that Nessus is already installed. If it is not please refer to www.nessus.org for installation instructions</p> <p>1. Start Nessus Server daemon command is nessusd</p> <div data-bbox="646 573 1923 1239"></div> <p>2. Start the nessus client software command is nessus or just click nessus icon on the gnome or KDE desktop</p>

GSNA Practical 3.0



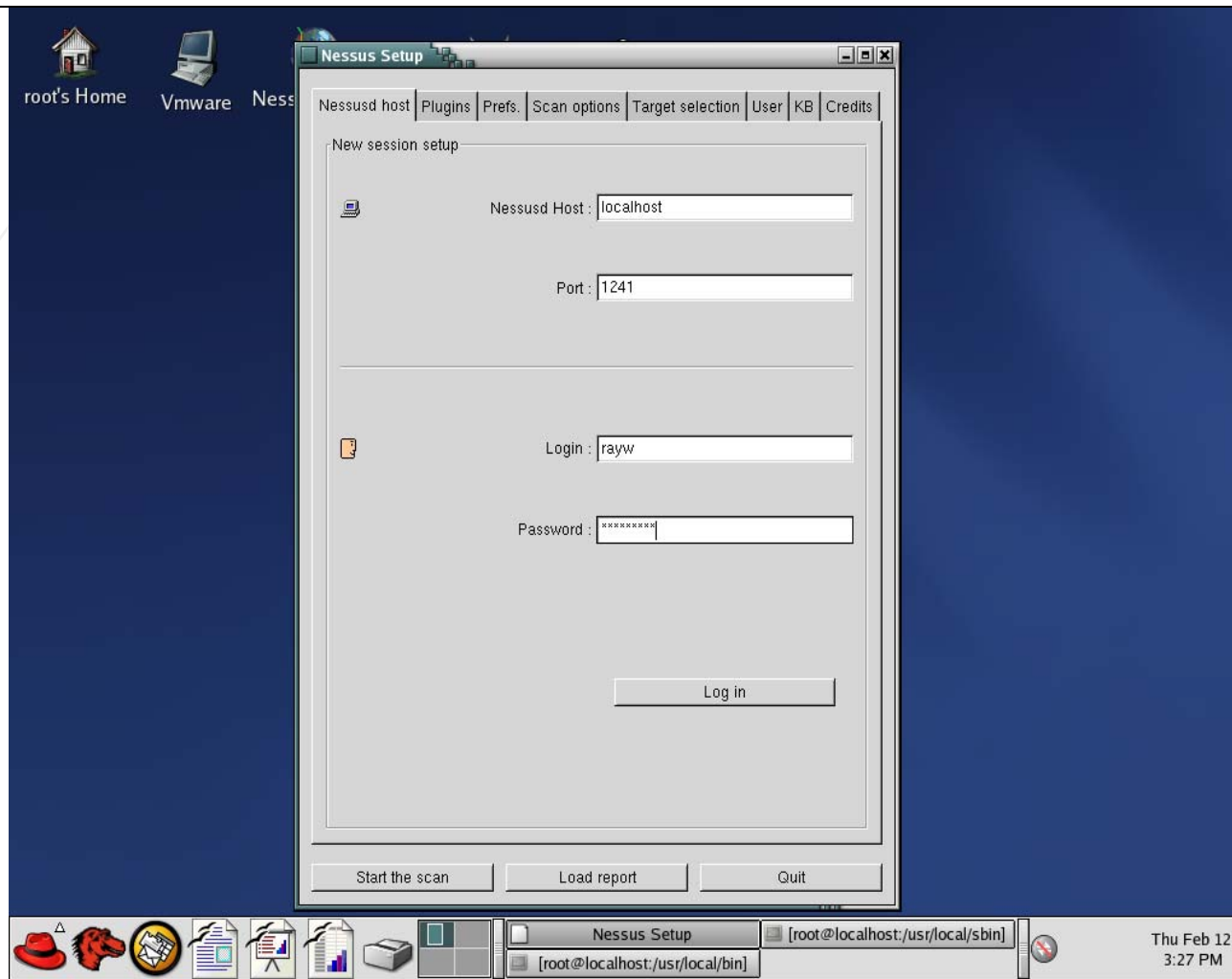
The screenshot shows a Linux desktop with a dark blue background. At the top, there are icons for 'root's Home', 'Vmware', 'Nessus Server', 'Nessus Client', 'Trash', and 'Start Here'. A terminal window is open, displaying the following commands and output:

```
root@localhost:/usr/local/bin
File Edit View Terminal Go Help
[root@localhost root]# cd..
bash: cd..: command not found
[root@localhost root]# cd ..
[root@localhost /]# cd usr
[root@localhost usr]# cd local
[root@localhost local]# cd bin
[root@localhost bin]# ls
dnet-config  nessus          nessus-mkcert-client  xine-bugreport
nasl         nessus-build    nessus-mkrand         xine-check
nasl-config  nessus-config  xine                  xine-config
[root@localhost bin]# nessus
```

The terminal window has a menu bar with 'File', 'Edit', 'View', 'Terminal', 'Go', and 'Help'. The desktop also features a taskbar at the bottom with various application icons and a system tray showing the date and time: 'Thu Feb 12 3:26 PM'.

3. Login in to the Nessus Server

GSNA Practical 3.0



4. In the Target option apply IP or IP address range to be scanned

GSNA Practical 3.0

	<ol style="list-style-type: none"> 5. Enable all Plugins 6. In the preferences section- nmap options check “syn scan,ping the remote host,identify the remote host, fragment ip packets, and get ident info 7. Bottem left hand corner click “start scan” 8. Run a network sniffer (I use ethereal but tcpdump or windump are other examples). For instructions on how to use any of the sniffers mentioned check the following urls http://www.ethereal.com/ http://www.tcpdump.org/ 9. Follow the same order and scan the internal IP's to determine if the router will allow traffic to the internal network 10. On the private side of the router set up ethereal sniffer to capture any data that may be allowed through (see beginning of section for description of ethereal sniffer) 11. On the router use a console connection to determine if the router will log anything also from the router prompt Router#show log 12. Scan the internal IP's as well in the same manner as mentioned above with the exception do not enable all plugins
Objective/Subjective	Objective

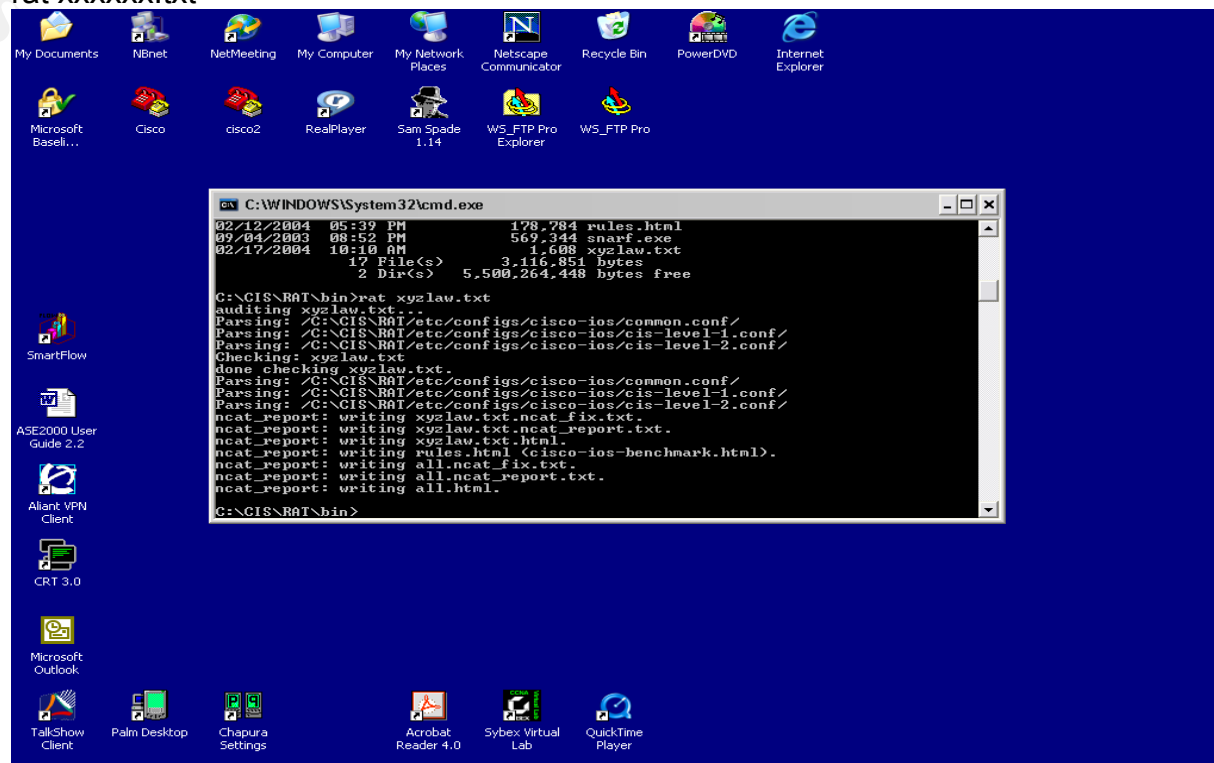
Checklist Item 6	
Reference	Center for Internet Security www.cisecurity.org
Objective	Run Router Auditing Tool (RAT) Benchmark 1 to get a snapshot of the router's overall security
Risk	Section 1.2 (1) router may be open to internet scans

GSNA Practical 3.0

Test

1. Assumption is RAT has been downloaded and installed, if not refer to the www.cisecurity.org for information in doing so.
2. Save the router configuration as laid out in General Checklist Item 4
3. Copy the file to the RAT directory default for a Windows install is c:\cis\rat\bin
4. run RAT – to do so simply run the rat.exe against the text file

rat xxxxxx.txt



5. View HTML file that was created xxxx.txt
6. Inspect for discrepancies

GSNA Practical 3.0

Objective/Subjective	Objective
----------------------	-----------

Checklist Item 7	
Reference	OSSTMM 2.1 Manual P.55 Section 6
Objective	Determine if Router is configured to provide Network Address Translation (NAT)
Risk	Section 1.2 (1) router may be open to internet scans
Test	<p>NAT or Network Address Translator (RFC 1631) is basically the router's ability to translate internal IP addresses to outside public addresses and vice versa. NAT can be used to ensure the inside network is not broadcasted.</p> <p>1.Login to the router as described in General Checklist Item 4 2. router#show ip nat translations</p> <p>or</p> <p>router#show ip nat statistics</p> <p>This will show if there are any NAT activity on the router</p> <p>3. Ping from inside the network to a host outside and redo the above to determine if the count goes up</p> <p>4. router#show run</p> <p>This will show if there are any NAT configurations on the router</p>
Objective/Subjective	Objective

GSNA Practical 3.0

Checklist Item 8	
Reference	OSSTMM 2.1 Manual P.55, Center For Internet Security Gold Standard Benchmark for Cisco IOS
Objective	Test the ACL against the written security policy or against the “Deny All” rule
Risk	Section 1.2.1 Company Practices Section 1.2.2.1 Router Open to internet scans Section 1.2.2.2 Router Open to Denial of Service Attacks
Test	<ol style="list-style-type: none"> 1. Login into the router as described in Checklist Item 4 2. router#show access-list 3. Review company security policy and determine if the configured router ACL is enforcing the security policy
Objective/Subjective	Objective

Checklist Item 9	
Reference	OSSTMM 2.1 Manual P.55
Objective	Verify the router is egress filtering local network traffic and the outbound capabilities of the router
Risk	Section 1.2.1 3 Internal Use of the network Section 1.2.1.4 Disgruntled Employees Section 1.2.1.5 lack of Security Policy to control router activities
Test	<p>This test is to determine if any traffic is being filtered from the inside network to the outside network.</p> <ol style="list-style-type: none"> 1. Using the configuration file obtained in checklist Item 4 and information gathered from Checklist Item 7 determine if there are any access lists on the outgoing public interface. <p>Result – there are no access lists applied to the LAN or WAN ports so as a result there is no filtering from the internal network to the external</p>

GSNA Practical 3.0

	network. 2. From a PC within the organization conduct the following tests <ul style="list-style-type: none"> i. Ping an outside internet address ii. Ping one of the internal PC's address from the test laptop on the internet iii. From an internal PC determine what access is allowed to the public internet
Objective/Subjective	Objective

Checklist Item 10	
Reference	OSSTMM 2.1 Manual P.55
Objective	Verify that the router is performing address spoof detection
Risk	Section 1.2.2.2 Router is Open to internet scans
Test	Using Hping attempt to spoof a trusted address to the router to determine if the router responds 1. hping2 -a xxx.xxx.xxx.xxx (source IP Spoofed) xxx.xxx.xxx.xxx (destination IP)
Objective/Subjective	Objective

Checklist Item 11	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS page 1 , Page 23 Section 3.1.4 Section 3.1.22 P.15 Section 3.1.23 P.15 Section 3.1.24 P.15 Own expérience
Objective	Check Local authentication of Username and passwords
Risk	Section 1.2.1.2 System Administration – Personnel that manages and

GSNA Practical 3.0

	configures the router Section 1.2.1.5 Lack of Security Policy to control Router Activities Section 1.2.1.3 XYZ Law may unknowingly damage the router
Test	1. From the configuration gathered in General Checklist Item 4 determine if there are any user account created on the router and if passwords are assigned. The information to look for is as follows: <ul style="list-style-type: none"> - user-id privilege 15 password 7 (encrypted) - enable password and encrypted 2. Telnet to the router, to do this from a dos or Unix prompt C:\telnet xxx.xxx.xxx.xxx (ip address) 3. Try cisco common username and passwords Username : enter as in enter key Password : enter as in enter key Username: cisco Username : cisco
Objective/Subjective	Objective

Checklist Item 12	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS

GSNA Practical 3.0

	Level 1 Benchmark Version 2.0 Sections 2.1 Page 8 Level 1 Benchmark Version 2.0 Section 3.1 Starting Page 13
Objective	Check to see if SNMP is enabled
Risk	Section 1.2.2 .1 Router may be Open to Internet Scans
Test	<ol style="list-style-type: none"> 1. Connect to the router as described in Checklist Item 4 2. from the prompt <ol style="list-style-type: none"> i. show config ii. Look for the following: snmp-server community (password) RW 12 snmp-server community (password) RO 12 snmp-server location (server location) snmp-server contact (contact information) snmp-server host 2. Run
Objective/Subjective	Objective

Checklist Item 13	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 Benchmark Version 2.0 Sections 2.1 Page 8 Level 1 Benchmark Version 2.0 Section 3.1 Starting Page 13
Objective	Check to determine if Telnet is enabled
Risk	Section 1.2.2.1 Router may be open to internet scans
Test	<ol style="list-style-type: none"> 1. From an outside device (internet connected test PC) attempt to telnet to the router. 2. from the prompt (DOS or Unix) c:\telnet xxx.xxx.xxx.xxx (destination IP)

GSNA Practical 3.0

	3. Once connected you will be presented a login prompt 4. If the connection is refused you will get a “connection refused by host” error message
Objective/Subjective	Objective

Checklist Item 14	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 Benchmark Version 2.0 Sections 2.1 Page 8
Objective	Determine if the exec timeout is enabled and actual configured time. This prevents unauthorized users from taking advantage of unused sessions.
Risk	Section 1.2.2.1 Router may be open to internet scans
Test	1. Determine exec timeout is configured on the router. Use the configuration obtained from Checklist Item 4 or connect directly to the router as outlined in Checklist Item 4 and type: Show config Result – line con 0 exec-timeout 0 0 There is no timeout on the direct connection. line vty 0 4 access-class 10 in exec-timeout 30 0

GSNA Practical 3.0

	<p>On the telnet connection there is an timeout of 30 minutes</p> <p>2. Connect to the router with telnet and conduct no activity, time to see how long the router times you out and compare with configuration information above.</p>
Objective/Subjective	Objective

Checklist Item 15	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 Benchmark Version 2.0 Sections 2.1 Page 8
Objective	Determine if the AUX port is enabled and if any modems are attached
Risk	<p>Section 1.2.1.3 Disgruntled Employees</p> <p>Section 1.2.2.1 Router open to outside scans</p>
Test	<p>1. Physical inspection of the router to determine if there are any modems attached</p> <p>2. Login to the router as laid out in Checklist Item 4 and perform the following commands from the router prompt</p> <p>i. router#show line aux 0</p> <p>The following should show up</p> <pre> router#sho line aux 0 Tty Typ Tx/Rx A Modem Roty AccO Accl Uses Noise Overruns Int 5 AUX 9600/9600 - - - - - 0 0 0/0 - </pre> <p>Line 5, Location: "", Type: ""</p> <p>Length: 24 lines, Width: 80 columns</p>

GSNA Practical 3.0

	<p> Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits Status: Ready Capabilities: none Modem state: Ready Modem hardware state: noCTS noDSR DTR RTS Special Chars: Escape Hold Stop Start Disconnect Activation ^^x none - - none Timeouts: Idle EXEC Idle Session Modem Answer Session Dispatch 00:10:00 never none not set Idle Session Disconnect Warning never Login-sequence User Response 00:00:30 Autoselect Initial Wait not set Modem type is unknown. Session limit is not set. Time since activation: never Editing is enabled. History is enabled, history size is 20. DNS resolution in show commands is enabled Full user help is disabled Allowed input transports are none. Allowed output transports are pad telnet rlogin ssh. Preferred transport is telnet. No output characters are padded No special data dispatching characters </p> <p>ii. This is a view of when the aux port has been disabled, refer to bold type below this is an indication of a disabled aux port.</p>
--	---

GSNA Practical 3.0

```
router#sho line aux 0
```

```
  Tty Typ  Tx/Rx  A Modem  Roty AccO Accl  Uses  Noise
Overruns Int
   5 AUX  9600/9600 -  -  -  -  -  0    0  0/0  -
```

```
Line 5, Location: "", Type: ""
```

```
Length: 24 lines, Width: 80 columns
```

```
Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits
```

```
Status: Ready
```

```
Capabilities: EXEC Suppressed
```

```
Modem state: Ready
```

```
Modem hardware state: noCTS noDSR DTR RTS
```

```
Special Chars: Escape Hold Stop Start Disconnect Activation
```

```
    ^^x  none  -  -  none
```

```
Timeouts:  Idle EXEC  Idle Session  Modem Answer  Session
Dispatch
```

```
    00:10:00      never              none  not set
```

```
    Idle Session Disconnect Warning
```

```
    never
```

```
    Login-sequence User Response
```

```
    00:00:30
```

```
    Autoselect Initial Wait
```

```
    not set
```

```
Modem type is unknown.
```

```
Session limit is not set.
```

```
Time since activation: never
```

```
Editing is enabled.
```

```
History is enabled, history size is 20.
```

```
DNS resolution in show commands is enabled
```

GSNA Practical 3.0

	Full user help is disabled Allowed input transports are none. Allowed output transports are pad telnet rlogin ssh. Preferred transport is telnet. No output characters are padded No special data dispatching characters
Objective/Subjective	Objective

Checklist Item 16	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS
Objective	Determine Configuration of the TTY Lines (passwords and ACLs)
Risk	Section 1.2.2.1 Router May be open to internet scans which may result in attempts to breach router defences to infiltrate XYZ Law's internal network
Test	<ol style="list-style-type: none"> 1. Login into the router as laid out in Checklist Item 4 or view the configuration file. If choosing to login in once connected type the following at the router prompt: <ol style="list-style-type: none"> I. router#show config II. Once the config is shown look for the following: line vty 0 4 (actual connection line) access-class 10 in (access list attached to interface) exec-timeout 30 0 (timeout for unused session 30minutes) password 7 xxxxxxxxxxxxxxxxxxxxxx (password assigned to interface) this is near the end of the configuration file 2. Look at Access List assigned to interface

GSNA Practical 3.0

	Router#show access-list (access list number) 3. Once the information is gathered above prove it's worth by doing the following: <ol style="list-style-type: none"> i. attempt to telnet to the router ii. if connect attempt to login iii. on the router do a "show access-list" to see if there are numbers increasing to determine hits on the access list
Objective/Subjective	Objective
Checklist Item 17	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 Benchmark Version 2.0 Sections 2.1 Page 9 Level 1 Benchmark Version 2.0 Sections 3.1.59/60 Page 20
Objective	Determine if unused Services are enabled HTTP Finger Service CDP BOOTp Config Server TFTP Small TCP Services Small UDP Services
Risk	Section 1.2.2.1 Router may be open to internet scans Section 1.2.2.2 Denial of Service Attacks
Test	1. HTTP – Connect to the router as described in Checklist Item 4, once logged in type : i. Router#show run

GSNA Practical 3.0

	<p>Look for the following in the configuration: no ip http server If this is not in the config HTTP server is enabled this the default setting for Cisco routers</p> <p>ii. From a web browser attempt to connect to the router by putting the IP address in the browser if HTTP is enabled the browser will connect you to the router. If HTTP is disabled then the connection will be refused.</p> <p>iii. And/or inspect results from General Checklist Item 6</p> <p>2. Finger Service – To determine if this service is running login in the router as in Check List Item 4. Perform a “show run” if the finger service is running you will see in the global config</p> <p>Ip finger service</p> <p>If this is not there then finger service is disabled.</p> <p>And/or inspect results from General Checklist Item 6</p> <p>3. CDP – Cisco Discovery Protocol. This protocol is meant for cisco devices to discover each other for troubleshooting purposes. If this is not utilized then it should be disabled. There are known denial of service attacks that utilize CDP.</p> <p>CDP is enabled by default to determine if CDP is enabled login to the router as laid out in Checklist Item 4 and perform the “show run” command. In the global config if you see the following :</p> <p>no cdp run</p>
--	--

GSNA Practical 3.0

	<p>I. This insures that CDP is disabled. CDP is enabled by default and will have to be manually disabled.</p> <p>II. Also in the configuration file on the individual interfaces that are used the following should be there to ensure CDP is disabled</p> <p style="padding-left: 40px;">no cdp enable</p> <p style="padding-left: 40px;">This ensures CDP is disabled on the interface.</p> <p>III. and/or inspect results from Checklist Item 6</p> <p>4. Bootp – There are known DOS attacks utilizing bootp on cisco routers and is enabled by default. Login to the router as laid out in check list Item 4 and type a “show run” at the router prompt. In the Global config if Bootp is disabled you should see the following:</p> <p style="padding-left: 40px;">i. no ip bootp server</p> <p style="padding-left: 40px;">If this is not there then bootp services are enabled.</p> <p style="padding-left: 40px;">ii. Inspect results from General Checklist Item 6</p> <p>5. Config Server – this allows a router to load its startup configuration from remote devices.</p> <p>6. TFTP Server – enabled by default an access list has to be utilized to restrict TFTP.</p> <p>7. tcp-keepalives – Inspect results from General Checklist Item 6</p>
--	--

GSNA Practical 3.0

	8. Small TCP Service – Inspect results from General Checklist item 6 9. Small UDP Service – Inspect results from General Checklist Item 6
Objective/Subjective	Objective

Checklist Item 18	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Benchmark for Cisco IOS page 10 Section 3.1.69 Page 22
Objective	Determine if Directed Broadcast is enabled
Risk	Section 1.2.2.2 Denial of Service Attacks Router Interfaces that allow directed broadcasts can be open to “smurf” attacks
Test	<ol style="list-style-type: none"> 1. Login to the router as describe in Checklist Item 4. 2. Do the “show run” command from the router prompt 3. Inspect each interface for the following: ip directed-broadcast If this is there directed-broadcast is enabled if not it is disabled 4. Inspect Results of RAT from General Checklist Item 6 Pass – Directed Broadcast disabled Fail – Directed Broadcast enabled
Objective/Subjective	Objective

Checklist Item 19	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS
Objective	Determine if IP source routing enabled
Risk	Section 1.2.2.1 Router is open to internet scans Section 1.2.2.2 Denial of Service Attacks
Test	<ol style="list-style-type: none"> 1. Run Router Auditing Tool and determine from the results Pass – IP Source Routing is disabled

GSNA Practical 3.0

	Fail - IP Source Routing in enabled
Objective/Subjective	Objective
Checklist Item 20	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 and 2 Benchmarks page 24
Objective	Determine IP Proxy Arp Enabled Proxy Arp breaks the LAN security perimeter effectively extending a LAN at layer 2 across multiple segments
Risk	Section 1.2.2.1 Router Open to internet Scans Section 1.2.2.2 Denial of Service Attacks
Test	<ol style="list-style-type: none"> 1. Login to the router as laid out in General Checklist Item 4 2. Do a "show run" to bring up the configuration 3. inspect the interfaces and determine if this is included 4. no ip proxy-arp 5. Proxy arp is enabled by default if this line is not there then proxy arp is enabled
Objective/Subjective	Objective

2.2 Cisco Specific Checklist

This checklist is specific to security warnings released by Cisco. It is based on information provided on Cisco's Website located at:

http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html

GSNA Practical 3.0

Checklist Item 1	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Cisco Security Advisory Check Security Advisory: Cisco IOS Software Multiple SNMP Community String Vulnerabilities The following is a description of the impact from Cisco's website</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13b5.shtml#software</p> <p>The following information is from the url above obtained from Cisco's website</p> <p>Knowledge of read-only community strings allows read access to information stored on an affected device, leading to a failure of confidentiality. Knowledge of read-write community strings allows remote configuration of affected devices without authorization, possibly without the awareness of the administrators of the device and resulting in a failure of integrity and a possible failure of availability.</p> <p>These vulnerabilities could be exploited separately or in combination to gain access to or modify the configuration and operation of any affected devices without authorization. Customers are urged to upgrade affected systems to fixed releases of software, or to apply measures to protect such systems against unauthorized use by restricting access to SNMP services until such time as the devices can be upgraded.</p> <ul style="list-style-type: none">• IOS software Major Release version 12.0 and IOS releases based on 11.x or earlier are not affected by the vulnerabilities described in this notice. All other releases of 12.0, such as 12.0DA, 12.0S or 12.0T, may be affected.• CSCdr59314 is only present in certain 12.1(3) releases and does not affect any other IOS releases.• Fixes for all six defects have been integrated into 12.2 prior to its initial availability, and therefore all releases based on 12.2 and all later versions are not vulnerable to the defects

GSNA Practical 3.0

	described in this advisory.
Risk	Section 1.2.2.1 Router may be open to internet scans and weaknesses exploited Section 1.2.2.5 Hardware/Software upgrades – if the version of code is deficient then a possible upgrade may be required.
Test	<p>Determine if software version of router is affected</p> <ol style="list-style-type: none"> 1. Login to the router as described in Checklist Item 4 and at the router prompt type <p>Router#show version</p> <p>Cisco Internetwork Operating System Software IOS (tm) C1700 Software (C1700-BK8NO3R2SY7-M), Version 12.2(15)T9, RELEASE SOFTWARE (fc2) TAC Support: http://www.cisco.com/tac Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Sat 01-Nov-03 06:24 by ccai Image text-base: 0x80008120, data-base: 0x81207F5C</p> <p>ROM: System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1) ROM: C1700 Software (C1700-BK8NO3R2SY7-M), Version 12.2(15)T9, RELEASE SOFTWARE (fc2)</p> <p>xyzlaw uptime is 2 days, 19 hours, 47 minutes System returned to ROM by power-on System image file is "flash:c1700-bk8no3r2sy7-mz.122-15.T9.bin"</p> <p>This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply</p>

GSNA Practical 3.0

	<p>third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.</p> <p>A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html</p> <p>If you require further assistance please contact us by sending email to export@cisco.com.</p> <p>cisco 1721 (MPC860P) processor (revision 0x100) with 58002K/7534K bytes of memory. Processor board ID FOC07010MUR (2301023196), with hardware revision 0000 MPC860P processor: part number 5, mask 2 Bridging software. X.25 software, Version 3.0.0. 1 Ethernet/IEEE 802.3 interface(s) 1 FastEthernet/IEEE 802.3 interface(s) 32K bytes of non-volatile configuration memory. 16384K bytes of processor board System flash (Read/Write)</p> <p>Configuration register is 0x142</p> <p>2. From this information determine the IOS version.</p>
Objective/Subjective	Objective

Checklist Item 2	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html

GSNA Practical 3.0

Objective	<p>Cisco Security Advisory Check Cisco Security Advisory: Cisco IOS ARP Table Overwrite Vulnerability</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b113c.shtml</p> <p>The following information is from the url above obtained form Cisco's website</p> <p>It is possible to send an Address Resolution Protocol (ARP) packet on a local broadcast interface (for example, Ethernet, cable, Token Ring, FDDI) which could cause a router or switch running specific versions of Cisco IOS® Software Release to stop sending and receiving ARP packets on the local router interface. This will in a short time cause the router and local hosts to be unable to send packets to each other. ARP packets received by the router for the router's own interface address but a different Media Access Control (MAC) address will overwrite the router's MAC address in the ARP table with the one from the received ARP packet. This was demonstrated to attendees of the Black Hat conference and should be considered to be public knowledge. This attack is only successful against devices on the segment local to the attacker or attacking host.</p> <p>Impact This issue can cause a Cisco Router to be vulnerable to a Denial-of-Service attack, once the ARP table entries time out. This defect does not result in a failure of confidentiality of information stored on the unit, nor does this defect allow hostile code to be loaded onto a Cisco device. This defect may cause a Denial-of-Service on the management functions of a Cisco Layer 2 Switch, but does not affect traffic through the device</p>
Risk	Section 1.2.2.2 Denial of Service Attack
Test	<p>determine if the router is running an affected IOS,</p> <p>1) log in to the device as laid out in checklist item 4</p>

GSNA Practical 3.0

	<p>2) And issue the command show version command at the router prompt. Inspect the configuration for the following:</p> <p style="text-align: center;">Internetwork Operating System Software" or "IOS (tm</p> <p>3) If this found compare the software version number with the table on this website from Cisco</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b113c.shtml</p> <p>This will provide upgrade information if required</p>
Objective/Subjective	Objective

Checklist Item 3	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the router is affected by the following advisory</p> <p>Security Advisory: Cisco IOS Syslog Crash</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13a7.shtml</p> <p>The following information is from the url above obtained form Cisco's website</p> <p>Certain versions of Cisco IOS software may crash or hang when they receive invalid user datagram protocol (UDP) packets sent to their "syslog" ports (port 514). At least one commonly-used Internet scanning tool generates packets which can cause such crashes and hangs. This fact has been announced on public Internet mailing lists which are widely read both by security professionals and by security "crackers", and should be considered public</p>

GSNA Practical 3.0

	<p>information.</p> <p>This vulnerability affects devices running Cisco IOS software version 11.3AA, version 11.3DB, or any 12.0-based version (including 12.0 mainline, 12.0S, 12.0T, and any other regular released version whose number starts with "12.0"). The vulnerability has been corrected in certain special releases, and will be corrected in maintenance and interim releases which will be issued in the future; see the section on "Software Versions and Fixes" for details on which versions are affected, and on which versions are, or will be, fixed. Cisco intends to provide fixes for all affected IOS variants.</p>
Risk	Section 1.2.2.2 Denial of Service Attack
Test	<ol style="list-style-type: none"> 1. Login to the router as described in Checklist Item 4 2. Do a "show version" as described in the previous Cisco Checklist 3. Go to table on the above webpage at Cisco to determine if the current IOS is affected.
Objective/Subjective	Objective

Checklist Item 4	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the router is affected by the following Security Advisory</p> <p>Cisco Security Notice: MS SQL Worm Mitigation Recommendations</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a0080133399.shtml</p> <p>The following information is from the url above obtained from Cisco's website</p>

GSNA Practical 3.0

	<p>Cisco customers are currently experiencing attacks due to a new worm that has hit the Internet. The signature of this worm appears as high volumes of UDP traffic to port 1434. Affected customers have been experiencing high volumes of traffic from both internal and external systems. Symptoms on Cisco devices include, but are not limited to high CPU and traffic drops on the input interfaces.</p> <p>The worm has been referenced by several names, including "Slammer", "Sapphire" as well as "MS SQL worm".</p> <p>Cisco has a companion document detailing Cisco products which are affected directly by this worm:</p> <p>http://www.cisco.com/warp/public/707/cisco-sa-20030126-ms02-061.shtml</p> <p>The current recommended fix for IOS is to apply an ACL to block traffic on port 1443</p>
Risk	Section 1.2.2.2 Denial of Service Attacks
Test	<ol style="list-style-type: none"> 1. Login to the router as described in General Checklist Item 4. 2. At the prompt do a "show run" 3. Inspect the configuration and determine if the following access list has been applied <pre>access-list 115 deny udp any any eq 1434 access-list 115 permit ip any any</pre> 4. Determine if the access list has been applied to the public interface <pre>int <interface> ip access-group 115 in</pre>

GSNA Practical 3.0

	ip access-group 115 out
Objective/Subjective	Objective

Checklist Item 5	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the router is affected by the following Security Advisory</p> <p>Cisco IOS HTTP Server Query Vulnerability</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13b6.shtml</p> <p>The following information is from the url above obtained from Cisco's website</p> <p>defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to "http://router-ip/anytext?/" is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.</p> <p>The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.</p> <p>The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.</p>

GSNA Practical 3.0

	This vulnerability can only be exploited if the enable password is known or not set.
Risk	Section 1.2.2.2 Denial of Service Attacks
Test	<ol style="list-style-type: none"> 1. Login to the router as laid out in General Checklist Item 4 2. at the router prompt do a "show version" 3. Inspect the information for the IOS version 4. Go to the table on the cisco website (Link above) and determine if the current version of IOS is affected
Objective/Subjective	Objective

Checklist Item 6	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the router is affected by the following Security Advisory</p> <p>Security Advisory: Cisco IOS Remote Router Crash</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b139d.shtml</p> <p>The following information is from the url above obtained form Cisco's website</p> <p>An error in Cisco IOS software makes it possible for untrusted, unauthenticated users who can gain access to the login prompt of a router or other Cisco IOS device, via any means, to cause that device to crash and reload.</p> <p>This applies only to devices running classic Cisco IOS software, including most, but not all, Cisco router products. The easiest way to determine whether your device is running classic Cisco IOS software is to use</p>

GSNA Practical 3.0

	<p>the show version command to determine who is affected.</p> <p>If attackers know the details of the Cisco IOS software error they will be able to cause the router to crash and reload <i>without having to log in to the router</i>. Because this problem involves damage to an internal data struture, it is possible that other, more subtle or targeted effects on system operation could also be induced by proper exploitation. Such exploitation, if it is possible at all, would require significant engineering skill and a thorough knowledge of the internal operation of Cisco IOS software, including Cisco trade secret information</p> <p>Affected IOS Versions</p> <ul style="list-style-type: none"> • 11.3(1), 11.3(1)ED, 11.3(1)T • 11.2(10), 11.2(9)P, 11.2(9)XA, 11.2(10)BC, 11.2(8)SA3 • 11.1(15)CA, 11.1(16), 11.1(16)IA, 11.1(16)AA, 11.1(17)CC, 11.1(17)CT • 11.0(20.3)
Risk	Section 1.2.2.2 Denial of Service
Test	<ol style="list-style-type: none"> 1. Login to the router as described in General Checklist Item 4 2. At the router prompt do a “show version” and determine the IOS Version on the current router. <p>Utilize the results from show version in Cisco checklist item 1</p> <ol style="list-style-type: none"> 3. Determine if the IOS version matches with the list mentioned above.

GSNA Practical 3.0

Objective/Subjective	Objective
Checklist Item 7	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the Router is vulnerable to the following Cisco Advisory</p> <p>Security Advisory: Cisco IOS Software Input Access List Leakage with NAT</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13a8.shtml</p> <p>The following information is from the url above obtained form Cisco's website</p> <p>A group of related software bugs (bug IDs given under "Software Versions and Fixes") create an undesired interaction between network address translation (NAT) and input access list processing in certain Cisco routers running 12.0-based versions of Cisco IOS software (including 12.0, 12.0S, and 12.0T, in all versions up to, but not including, 12.0(4), 12(4)S, and 12.0(4)T, as well as other 12.0 releases). Non-12.0 releases are not affected.</p> <p>This may cause input access list filters to "leak" packets in certain NAT configurations, creating a security exposure. Configurations without NAT are not affected.</p> <p>The failure does not happen at all times, and is less likely under laboratory conditions than in installed networks. This may cause administrators to believe that filtering is working when it is not.</p>
Risk	Section 1.2.2.2 Denial of Service
Test	<ol style="list-style-type: none"> 1. Login to the router as described in General Checklist Item 4 2. At the router prompt do a "show version" and determine the IOS Version on the current

GSNA Practical 3.0

	<p>router.</p> <p>3. Utilize the results from show version in Cisco checklist item 1</p> <p>IOS version is 12.2(15)T9</p> <p>4. Determine if the IOS version matches those found on the table on the Cisco Website mentioned above.</p>
Objective/Subjective	Objective

Checklist Item 8	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the Router is vulnerable to the following Cisco Advisory</p> <p>Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packets</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00801a34c2.shtml</p> <p>The following information is from the url above obtained form Cisco's website</p> <p>routers and switches running Cisco IOS[®] software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. Multiple IPv4 packets with specific protocol fields sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. Traffic passing through the device cannot block the input queue. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. Multiple valid workarounds are available in the form of best practices for situations where software upgrades are not currently feasible.</p>

GSNA Practical 3.0

	<p>If the software version is not on the router the current ACL workaround should be applied</p> <pre> access-list 101 permit tcp any any access-list 101 permit udp any any access-list 101 deny 53 any any access-list 101 deny 55 any any access-list 101 deny 77 any any access-list 101 deny 103 any any !--- insert any other previously applied ACL entries here !--- you must permit other protocols through to allow normal !--- traffic -- previously defined permit lists will work !--- or you may use the permit ip any any shown here access-list 101 permit ip any any </pre>
Risk	Section 1.2.2.2 Denial of Service
Test	<ol style="list-style-type: none"> 1. Login to the router as described in General Checklist Item 4 2. At the router prompt do a “show version” and determine the IOS Version on the current router. 3. Utilize the results from show version in Cisco checklist item 1 4. Determine if the IOS version matches those found on the table on the Cisco Website mentioned above. 5. If the IOS version does not match do a “show run” and determine if the above mentioned access list is configured and applied to the public interface.

GSNA Practical 3.0

Objective/Subjective	Objective
Checklist Item 9	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the Router is vulnerable to the following Cisco Advisory</p> <p>Security Advisory: Cisco IOS Command History Release at Login Prompt</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13aa.shtml</p> <p>The following information is from the url above obtained from Cisco's website</p> <p>An error in Cisco IOS® software makes it possible for untrusted, unauthenticated users who can gain access to the login prompt of a router or other Cisco IOS device, via any means, to obtain fragments of text entered by prior interactive users of the device. This text may contain sensitive information, possibly including passwords. This vulnerability exposes only text entered at prompts issued by the IOS device itself; the contents of data packets forwarded by IOS devices are not exposed, nor are data entered as part of outgoing interactive connections, such as TELNET connections, from the IOS device to other network nodes.</p>
Risk	Section 1.2.2.1 Router may be open to internet scans
Test	<ol style="list-style-type: none"> 1. Login to the router as described in General Checklist Item 4 2. At the router prompt do a "show version" and determine the IOS Version on the current router. 3. Utilize the results from show version in Cisco checklist item 1 4. Determine if the IOS version matches those found on the table on the Cisco Website

GSNA Practical 3.0

	mentioned above.
Objective/Subjective	Objective

Checklist Item 10	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the Router is vulnerable to the following Cisco Advisory</p> <p>Cisco Security Advisory: Cisco IOS Software TCP Initial Sequence Number Randomization Improvements</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b1396.shtml</p> <p>Cisco IOS® Software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.</p> <p>The following information is from the url above obtained from Cisco's website</p> <p>This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.</p> <p>To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.</p> <p>Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual</p>

GSNA Practical 3.0

	devices.
Risk	Section 1.2.2.1 Router may be open to internet scans
Test	<ol style="list-style-type: none">1. Login to the router as described in General Checklist Item 42. At the router prompt do a “show version” and determine the IOS Version on the current router.3. Utilize the results from show version in Cisco checklist item 14. Determine if the IOS version matches those found on the table on the Cisco Website mentioned above.
Objective/Subjective	Objective

3. Conduct the Audit

This audit was conducted with the written permission of XYZ Law. Coordination was completed with the system admin and the local ISP. External penetration testing was accomplished with a Toshiba Satellite Pro Laptop and a Compaq EVO N600C. Specifications of the laptops and tools used are as follows:

Toshiba Satellite Pro

- Linux Redhat 9.0
- Pentium III 733
- 20 Gigabit Hard Drive
- 512 Megs Ram
- Nessus Vulnerability Scanner 2.0.10
- Hping 2

Compaq EVO N600c

- Windows XP
- Pentium III 1.2
- 20 Gig Hard Drive
- 512 Megs Ram
- Ethereal Network Analyzer 3.13.0
- CRT 3.0 (used to connect to the router)

The audit is divided as before into two sections:

General – this is a common checklist

Cisco Specific – Based on latest Cisco Security advisories

The audit of the router can be accomplished two ways and each will be explored in this document. I have decided to complete both methods to ensure that false positives did not provide incorrect information for the audit. The two methods are:

Manual Checks – This is accomplished by manually connecting to the router and logging in. Cisco “show” commands are used to determine the outcome of the checklist.

Automatic Checks – This is accomplished by automatic tools such as Nessus, Hping2, and CIS’s Router Audit Tool (RAT)

GSNA Practical 3.0

3.1 Audit – General Checklist

Checklist Item 1	
Reference	OSSTMM 2.1 Manual Page 87-92 Personal Experience,
Objective	Physical Security
Risk	Physical Location Section 1.2.1
Test	<p>This is test is in the form of an office inspection conducted by the Auditor with the permission of XYZ Law</p> <p>1. Is the router locked in a secure area: Answer – Yes, the router is locked in a wiring closet within the confines of XYZ Law Office. The router is also securely tethered with the cable mechanism supplied by Cisco.</p> <p>2. Is the access controlled to the location of the router: Answer – Yes, all access to XYZ Law Office is controlled by the Administrative Assistant. The office is locked after hours and a security guard is employed to monitor the building.</p> <p>3. Is there an authorized list of persons who can access the router? Answer – Yes, although there is not a formal list the administrative assistant controls all access to the wiring closet and she controls the key.</p> <p>4. In the location of the router does it meet environmental conditions i.e. temperature and humidity? Answer – Yes, the room temperature is controlled and the wiring closet does not reach high temperatures.</p> <p>5. Does the area have an intrusion alarm system? Answer – Yes, as mentioned there is also a security guard employed to monitor the building.</p>

GSNA Practical 3.0

	Result – the router is secured sufficiently
Objective/Subjective	Subjective

Checklist Item 2	
Reference	Personal Experience
Objective	Determine Process and Ability of Outsourced System Admin
Risk	2. System Administration Section 1.2.1 Section 1.2.2 5 Hardware/Software upgrades
Test	<p>This test is conducted in the form of an interview with the System Administrator</p> <ol style="list-style-type: none"> 1. What is your experience with the Cisco IOS Software? Answer – 3 years configuring routers and providing support 2. Is there proactive management of the router Answer – No 3. Are configuration changes done remotely or on site Answer - Both 4. Are configuration changes confirmed with XYZ Law Answer – No, XYZ is just informed of the change with little detail 5. Are configuration changes, hardware/software changes tested in a safe environment first before going to Production Answer – Yes it is completed by the Engineering department and passed on to support. <p>Result – the support and knowledge of the sys admin is up to the task of supporting this router for XYZ Law.</p>
Objective/Subjective	Subjective

GSNA Practical 3.0

Checklist Item 3	
Reference	Personal Experience, OSSTM Manual P.41 (Note in this manual the purpose of the test it try and get information from trusted employees, I feel that is not necessary here in that just the router is being audited so I've taken the idea and modified the direction determine how the employee can adversely affect the router)
Objective	Determine possible affects employees will have on router Operation
Risk	Section 1.2.1 (3) and (4)
Test	<p>This test will be conducted in the form of a personal interview with XYZ law's Employees</p> <p>First Employee Interview - Administrative Assistant</p> <ol style="list-style-type: none"> 1. How long have you been with the company? Answer – Since the firm started 10 years 2. What is your position Answer – Administrative Assistant and book keeper 3. What is your general use of the internet (i.e. downloads, email, chats, etc) Answer – Just email and general surfing of sites for information such as world news and such 4. Do you know what the router is and what it is used for? Answer – Not really just that its used for the internet 5. What is your general overall feeling about the company? Answer – Generally overall very good <p>Note: The Lawyers of the firm were founding members and declined the offer for an interview Result – the members and employees have no ill will towards XYZ Law and</p>

GSNA Practical 3.0

	wish the best for the firm.
Objective/Subjective	Subjective

Checklist Item 4	
Reference	OSSTMM 2.1 Manual P.47/55 Section 8 www.cisco.com – 1700 Series Router quick installation guide and configuration guides
Objective	Verify the router type and Software Version
Risk	No Risk associated – Information Gathering and confirmation
Test	<ol style="list-style-type: none"> 1. Connect the RJ-45 end of the console cable to the CONSOLE port on the back panel of the router, Completed 2. Connect the DB-9 end of the console cable to the console port (also called the <i>serial port</i>) on your PC. If this adapter does not fit your PC console port, you must provide an adapter that fits. Completed 3. Open a HyperTerminal Session to the router. Ensure the following settings are set: <ol style="list-style-type: none"> vii. connect using com ports usually Com1 viii. terminal keys is checked ix. Ctrl-H is checked x. Emulation is Auto detect xi. Terminal ID is ANSI xii. Port settings are: 9600,databits 8, parity none, stop bits 1, flow control none Completed

GSNA Practical 3.0

	<p>4. Login to the router (note this may be done with the system administrator). To accomplish this:</p> <ul style="list-style-type: none">vi. Hit enter once session starts the following prompt appears:vii. xyzlawviii. You then type enable you will then be prompted for a password, enter the password. The following is how it will look on a Cisco router <p>Press RETURN to get started.</p> <p>xxxxx Internet IISP</p> <p>You must agree to the following before using this system</p> <p>Use of this system is restricted to authorized employees of xxxxx Inc. and authorized contractors. Only authorized work using company-supplied programs may be done on this system. Use of this system is an agreement to monitoring.</p> <p>User Access Verification</p> <p>Password: xxxxxxxxxxxx xyzlaw>en Password: xxxxxxxxxxxx xyzlaw#</p> <p>ix. Type show version this will supply the software and firmware version</p> <p>An example of this layout is:</p>
--	--

GSNA Practical 3.0

	<pre>xyzlaw#show version xyzlaw#sho version Cisco Internetwork Operating System Software IOS (tm) C1700 Software (C1700-BK8NO3R2SY7-M), Version 12.2(15)T9, RELEASE SOFTWARE (fc2) TAC Support: http://www.cisco.com/tac Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Sat 01-Nov-03 06:24 by ccai Image text-base: 0x80008120, data-base: 0x81207F5C ROM: System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1) ROM: C1700 Software (C1700-BK8NO3R2SY7-M), Version 12.2(15)T9, RELEASE SOFTWARE (fc2) xyzlaw uptime is 6 minutes System returned to ROM by power-on System image file is "flash:c1700-bk8no3r2sy7-mz.122-15.T9.bin" This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you</pre>
--	---

GSNA Practical 3.0

	<p>agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.</p> <p>A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html</p> <p>If you require further assistance please contact us by sending email to export@cisco.com.</p> <p>cisco 1721 (MPC860P) processor (revision 0x100) with 58002K/7534K bytes of memory. Processor board ID FOC07010MUR (2301023196), with hardware revision 0000 MPC860P processor: part number 5, mask 2 Bridging software. X.25 software, Version 3.0.0. 1 Ethernet/IEEE 802.3 interface(s) 1 FastEthernet/IEEE 802.3 interface(s) 32K bytes of non-volatile configuration memory. 16384K bytes of processor board System flash (Read/Write)</p> <p>Configuration register is 0x142</p> <p>xyzlaw#</p> <p>NOTE: This router is running cryptographic IOS</p> <p>x. Type show running- config this will display the current running configuration on the device.</p>
--	--

GSNA Practical 3.0

An example of this layout is:

xyzlaw#**show running-config**

xyzlaw#**show running-config**
Building configuration...

Current configuration : 1395 bytes

!
version 12.2
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname xyzlaw
!
logging queue-limit 100
logging buffered 4096 debugging
enable password 7 14141B180F0B
!
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
!

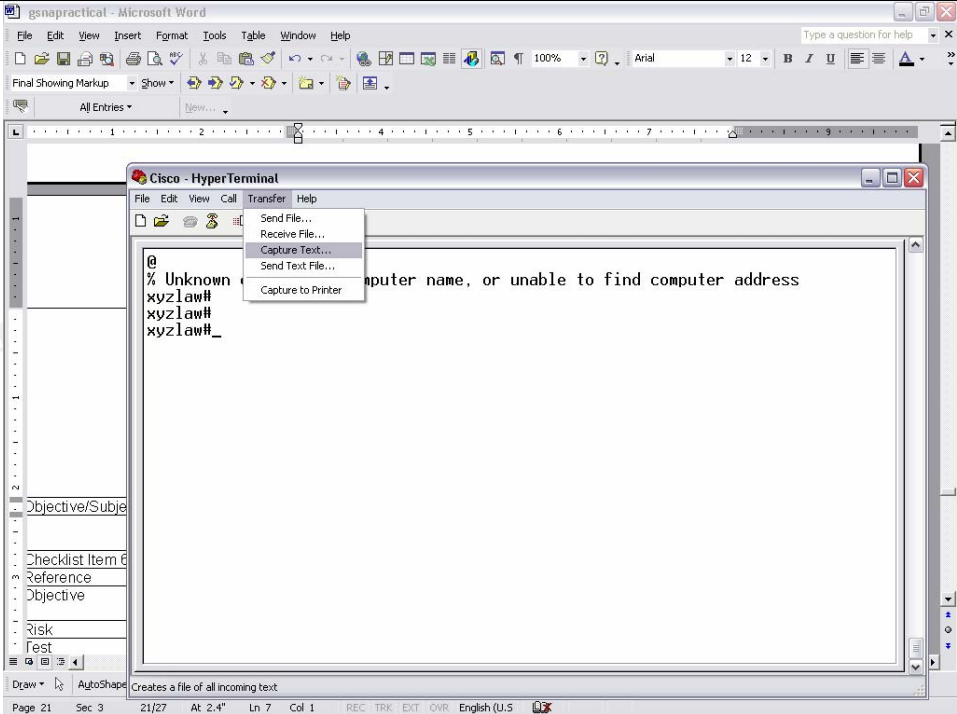
GSNA Practical 3.0

```
!  
!  
!  
!  
!  
interface Ethernet0  
  description Customer LAN Segment  
  ip address xxx.xxx.xxx.xxx 255.255.255.248  
  half-duplex  
  no cdp enable  
!  
interface FastEthernet0  
  description Connection to ISP  
  ip address xxx.xxx.xxx.xxx 255.255.255.252  
  speed auto  
  no cdp enable  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx  
no ip http server  
no ip http secure-server  
!  
!  
!  
access-list 10 permit xxx.xxx.xxx.xxx  
!  
snmp-server location xxxxxxxxxxxxxxxxxxxxxxxx  
snmp-server contact xxxxxxxxxxxxxxxxxxxxxxxx  
snmp-server enable traps tty  
banner motd ^C  
          xxxxx Internet IISP
```

GSNA Practical 3.0

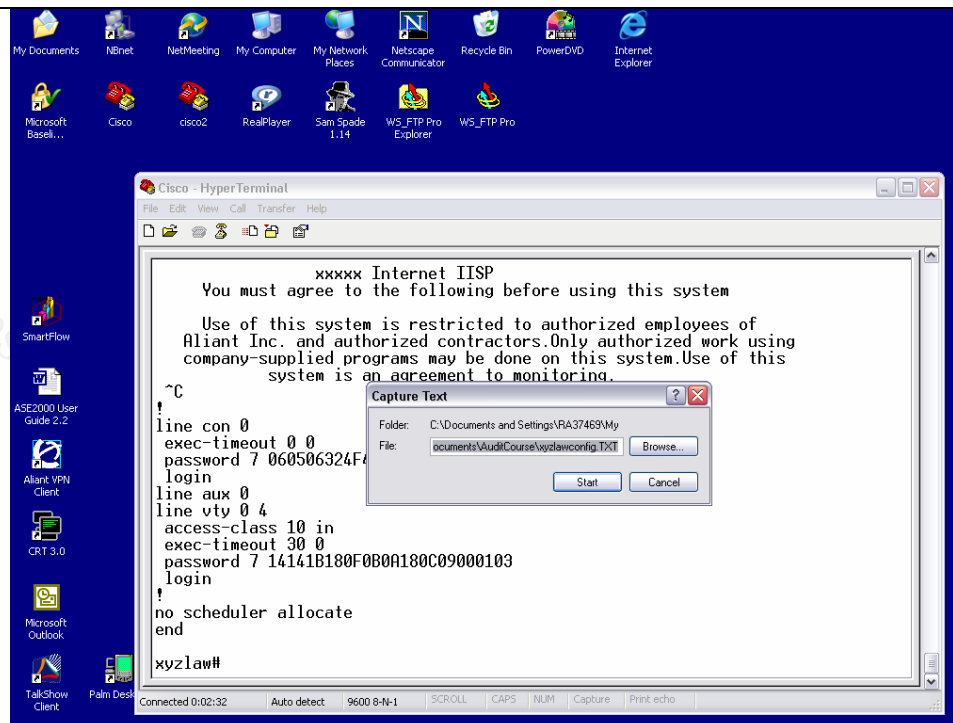
	<p>You must agree to the following before using this system</p> <p>Use of this system is restricted to authorized employees of Xxxxxx ISP and authorized contractors.Only authorized work using company-supplied programs may be done on this system.Use of this system is an agreement to monitoring.</p> <pre>^C ! line con 0 exec-timeout 0 0 password 7 xxxxxxxxxxxxxxxxxxxxxx login line aux 0 line vty 0 4 access-class 10 in exec-timeout 30 0 password 7 xxxxxxxxxxxxxxxxxxxxxx login ! no scheduler allocate end xyzlaw#</pre> <p>5. Save information gathered in a text file.</p> <ol style="list-style-type: none">Go to the transfer option on top of the session page chose “capture text”
--	---

GSNA Practical 3.0



ii. Give your text file a name – **xyzlaw.txt**

GSNA Practical 3.0



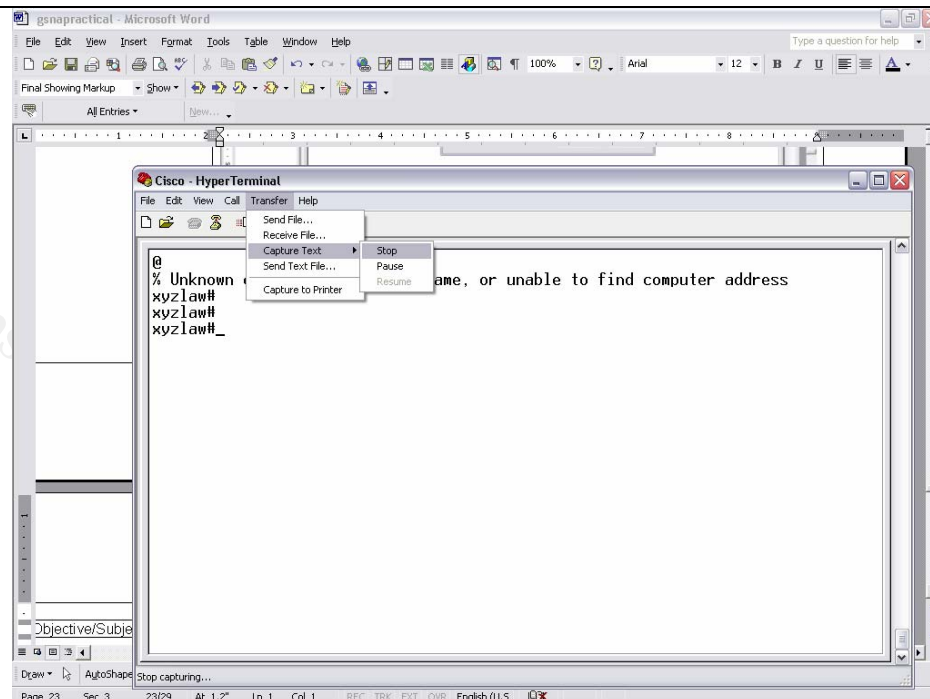
iii. perform the above mentioned show commands

Completed

iv. Go to transfer again, choose capture text and then choose "stop" at the dropdown menu.

Completed

GSNA Practical 3.0

**Completed**

Result – Necessary Information regarding the router has been captured

7. For a full comprehensive view of the router configuration at the router prompt type:

Router#show tech-support

This is quite a large file and passwords are left out by default. An example of the print out of the results of this are in Appendix C of

GSNA Practical 3.0

	this document.
Objective/Subjective	Objective

Checklist Item 5	
Reference	OSSTMM 2.1 Manual P.47 Section 3
Objective	Utilize Nessus Vulnerability Scanner to determine vulnerabilities from the internet.
Risk	Section 1.2 (1) router may be open to internet scans
Test	<p>To be performed by the Nessus Port Scanner. This assumes that Nessus is already installed. If it is not please refer to www.nessus.org for installation instructions</p> <ol style="list-style-type: none"> 1. Start Nessus Server daemon command is nessusd 2. Start the nessus client software command is nessus or just click nessus icon on the gnome or KDE desktop 3. In the Target option apply IP or IP address range to be scanned 4. In the preferences section- nmap options check syn 5. Enable all Plugins 6. In the preferences section- nmap options check “syn scan,ping the remote host,identify the remote host, fragment ip packets, and get ident info 7. Bottem left hand corner click “start scan” 8. run a network sniffer (I use ethereal but tcpdump or windump are other examples). For instructions on how to use any of the sniffers mentioned check the following urls <p>http://www.ethereal.com/ http://www.tcpdump.org/</p>

GSNA Practical 3.0

9. Follow the same order and scan the internal IP's to determine if the router will allow traffic to the internal network
10. On the private side of the router set up ethereal sniffer to capture any data that may be allowed through (see beginning of section for description of ethereal sniffer)

For the scan on the router the sniffer did not pick anything up the reason being Nessus was only set to scan the IP on the public Ethernet only not the full IP range. As stated below a separate scan was conducted to check XYZ's inside IP's

11. On the router use a console connection to determine if the router will log anything also from the router prompt

Router#show log

Result –

xyzlaw#sho log

Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes, 0 overruns, xml disabled)

Console logging: level debugging, 113 messages logged, xml disabled

Monitor logging: level debugging, 0 messages logged, xml disabled

Buffer logging: level debugging, 100 messages logged, xml disabled

Logging Exception size (4096 bytes)

Count and timestamp logging messages: disabled

Trap logging: level informational, 118 message lines logged

Log Buffer (4096 bytes):

Mar 3 19:02:42: %SYS-5-CONFIG_I: Configured from console by console

***Mar 3 19:03:15: %SYS-5-CONFIG_I: Configured from console by console**

GSNA Practical 3.0

	<p>*Mar 3 19:04:17: %SYS-5-CONFIG_I: Configured from console by console</p> <p>*Mar 3 19:07:18: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 19:07:18: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 19:15:44: %SYS-5-CONFIG_I: Configured from console by console</p> <p>*Mar 3 19:16:14: %SYS-5-CONFIG_I: Configured from console by console</p> <p>*Mar 3 19:17:56: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 19:17:56: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 19:19:31: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 19:19:34: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 19:43:34: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 19:43:34: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 19:44:46: %CRYPTO-6-IKMP_UNK_EXCHANGE: IKE peer at xxx.xxx.xxx.xxx sent a message with unknown exchange 1</p> <p>*Mar 3 20:54:20: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 20:54:20: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 20:54:24: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 20:54:24: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 20:56:00: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p>
--	--

GSNA Practical 3.0

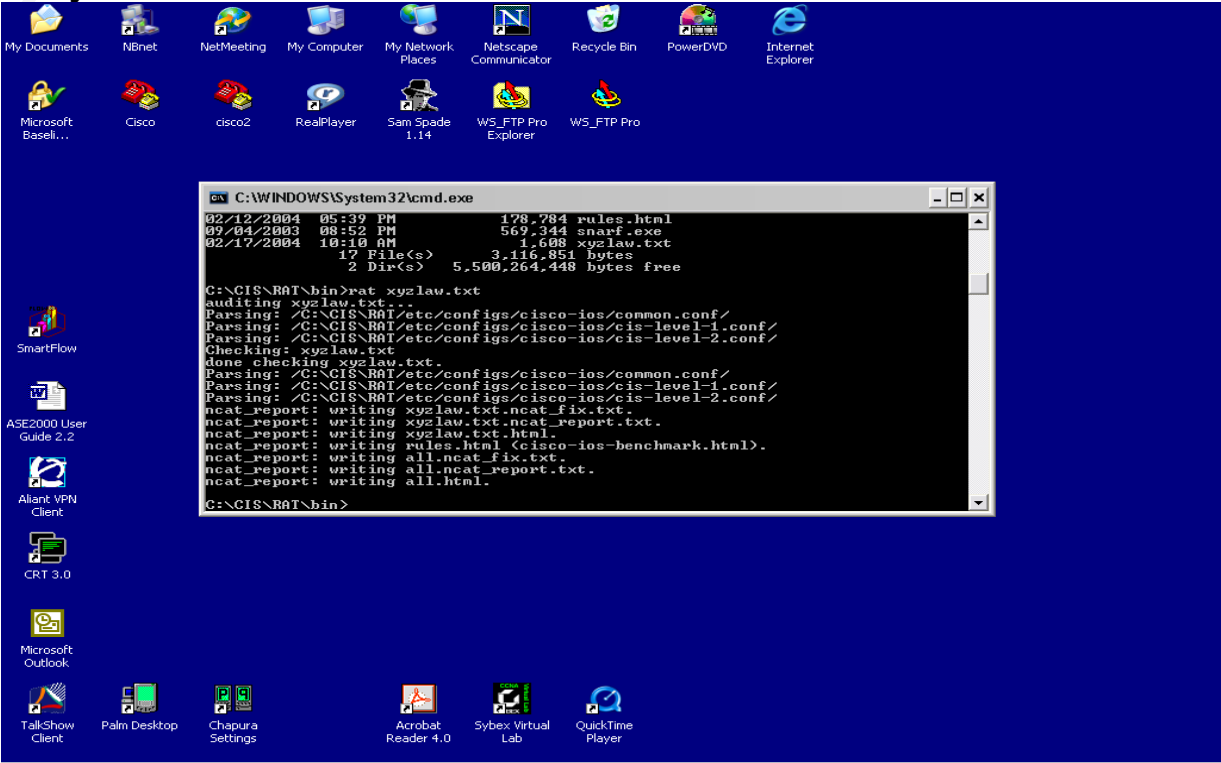
	<p>*Mar 3 20:56:03: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 21:20:05: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 21:20:05: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 3 21:21:18: %CRYPTO-6-IKMP_UNK_EXCHANGE: IKE peer at xxx.xxx.xxx.xxx sent a message with unknown exchange 1</p> <p>*Mar 4 04:38:56: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 04:38:56: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 04:39:02: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 04:39:02: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 04:39:09: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 04:39:09: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 04:40:43: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 04:40:46: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 05:04:45: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 05:04:45: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 05:08:25: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx</p> <p>*Mar 4 05:08:25: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to</p>
--	---

GSNA Practical 3.0

	<p> RSHELL from xxx.xxx.xxx.xxx *Mar 4 05:43:56: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx *Mar 4 05:43:56: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx *Mar 4 05:45:31: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx *Mar 4 05:45:34: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx *Mar 4 06:09:37: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx *Mar 4 06:09:37: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from xxx.xxx.xxx.xxx *Mar 4 06:10:53: %CRYPTO-6-IKMP_UNK_EXCHANGE: IKE peer at xxx.xxx.xxx.xxx sent a message with unknown exchange 1 </p> <p>Scan the internal IP's as well in the same manner as mentioned above with the exception do not enable all plugins</p> <p>Result Nessus was able to detect PC's behind the router and determine OS.</p> <p>Result telnet and icmp ports were open Nessus was able to detect type of router and version of IOS For full report see appendix A of the final report</p>
Objective/Subjective	Objective

Checklist Item 6	
Reference	Center for Internet Security www.cisecurity.org
Objective	Run Router Auditing Tool (RAT) Benchmark 1 to get a snapshot of the router's overall security

GSNA Practical 3.0

Risk	Section 1.2 (1) router may be open to internet scans
Test	<div><div><div><div>1. Assumption is RAT has been downloaded and installed, if not refer to the www.cisecurity.org for information in doing so.</div><div>2. Save the router configuration as laid out in General Checklist Item 4</div><div>3. Copy the file to the RAT directory default for a Windows install is c:\cis\rat\bin</div><div>4. run RAT – to do so simply run the rat.exe against the text file</div></div><div>rat xyzlaw.txt</div><div><pre>C:\WINDOWS\System32\cmd.exe 02/12/2004 05:39 PM 178,284 rules.html 09/04/2003 08:52 PM 569,344 snarf.exe 02/17/2004 10:10 AM 1,608 xyzlaw.txt 17 File(s) 3,116,851 bytes 2 Dir(s) 5,500,264,448 bytes free C:\CIS\RAT\bin>rat xyzlaw.txt auditing xyzlaw.txt... Parsing: /C:\CIS\RAT\etc/configs/cisco-ios/common.conf/ Parsing: /C:\CIS\RAT\etc/configs/cisco-ios/cis-level-1.conf/ Parsing: /C:\CIS\RAT\etc/configs/cisco-ios/cis-level-2.conf/ Checking: xyzlaw.txt done checking xyzlaw.txt. Parsing: /C:\CIS\RAT\etc/configs/cisco-ios/common.conf/ Parsing: /C:\CIS\RAT\etc/configs/cisco-ios/cis-level-1.conf/ Parsing: /C:\CIS\RAT\etc/configs/cisco-ios/cis-level-2.conf/ ncat_report: writing xyzlaw.txt.ncat_fix.txt. ncat_report: writing xyzlaw.txt.html. ncat_report: writing rules.html (cisco-ios-benchmark.html). ncat_report: writing all.ncat_fix.txt. ncat_report: writing all.ncat_report.txt. ncat_report: writing all.html. C:\CIS\RAT\bin></pre></div><div>5. View HTML file that was created xyzlaw.txt</div></div></div>

GSNA Practical 3.0

	6. Inspect for discrepancies Result – Router came back as a fail with a score of 14 out of 40. To see the output see appendix in final report section 3
Objective/Subjective	Objective

Checklist Item 7	
Reference	OSSTMM 2.1 Manual P.55 Section 6
Objective	Determine if Router is configured to provide Network Address Translation (NAT)
Risk	Section 1.2 (1) router may be open to internet scans
Test	<p>NAT or Network Address Translator (RFC 1631) is basically the router's ability to translate internal IP addresses to outside public addresses and vice versa. NAT can be used to ensure the inside network is not broadcasted.</p> <p>1.Login to the router as described in Checklist Item 5.4 2. xyzlaw#show ip nat trans xyzlaw#show ip nat translations xyzlaw# xyzlaw# xyzlaw# xyzlaw# xyzlaw#sho ip nat statistics xyzlaw# 3. I've viewed the config copy from checklist item 4 and also determined there is no NAT configured on this router</p> <p>Result – There is no NAT configured on this router and all IP's are</p>

GSNA Practical 3.0

	publicly routed. This potentially opens the internal network of XYZ Law open.
Objective/Subjective	Objective

Checklist Item 8	
Reference	OSSTMM 2.1 Manual P.55, Center For Internet Security Gold Standard Benchmark for Cisco IOS
Objective	Test the ACL against the written security policy or against the “Deny All” rule
Risk	Section 1.2.1 Company Practices Section 1.2.2.1 Router May be Open to internet Scans Section 1.2.2.2 Denial of Service Attack
Test	<ol style="list-style-type: none"> 1. Login into the router as described in Checklist Item 4 <pre>xyzlaw#show access-list xyzlaw#sho access-list Standard IP access list 10 10 permit xxx.xxx.xxx.xxx</pre> <p>Result – the only IP that has access to this router is stated above. The implicit deny rule is enforced automatically in a Cisco ACL.</p> 2. Review company security policy and determine if the configured router ACL is enforcing the security policy <p>XYZ Law has no current security policy</p> 3. Determine which interface the Access List is applied

GSNA Practical 3.0

	<p>line vty 0 4 access-class 10 in</p> <p>Result - There are no other access lists and none are applied to any other interface</p>
Objective/Subjective	Objective
Checklist Item 9	
Reference	OSSTMM 2.1 Manual P.55
Objective	Verify the router is egress filtering local network traffic and the outbound capabilities of the router
Risk	<p>Section 1.2.1 3 Internal Use of the network</p> <p>Section 1.2.1.4 Disgruntled Employees</p> <p>Section 1.2.1.5 lack of Security Policy to control router activities</p>
Test	<p>This test is to determine if any traffic is being filtered from the inside network to the outside network.</p> <ol style="list-style-type: none"> Using the configuration file obtained in checklist Item 4 and information gathered from Checklist Item 7 determine if there are any access lists on the outgoing public interface. Result – there are no access lists applied to the LAN or WAN ports so as a result there is no filtering from the internal network to the external network. From a PC within the organization conduct the following tests <p>Ping an outside internet address</p> <p>Result – was successful in pinging the router gateway and the</p>

GSNA Practical 3.0

	<p>next hop router on the internet.</p> <p>Ping one of the internal PC's address from the test laptop on the internet</p> <p>Result – this was successful from a device on the internet (in this case my Toshiba laptop I was able to ping the public IP's assigned to the internal PC's. This proves that the internal PC's will respond to requests and the router is not filtering outbound</p> <p>From an internal PC determine what access is allowed to the public internet</p> <p>Result – The users from XYZ has full access to all services on the internet, POP Mail, IRC/MSN chats rooms, ftp, HTML, etc.</p>
Objective/Subjective	Objective

Checklist Item 10	
Reference	OSSTMM 2.1 Manual P.55
Objective	Verify that the router is performing address spoof detection
Risk	Section 1.2.2.1 Router may be open to internet scans Section 1.2.2.2 Denial of Service Attacks
Test	<ol style="list-style-type: none"> 1. From a PC on the internet use Hping to spoof the IP 2. Run a sniffer to determine if the host responds to the pings <p>Result – the router is open to normal pings and the ethereal sniffer captured this Hping2 was used with the –a option and as a result the router did not detect that the ip was being spoofed</p>

GSNA Practical 3.0

First ping with no spoofing

```
root@localhost root]# ping xxx.xxx.xxx.xxx
PING xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx) 56(84) bytes of data.
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=1 ttl=255 time=1.09 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=2 ttl=255 time=0.793 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=3 ttl=255 time=0.803 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=4 ttl=255 time=1.08 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=5 ttl=255 time=0.846 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=6 ttl=255 time=0.771 ms
```

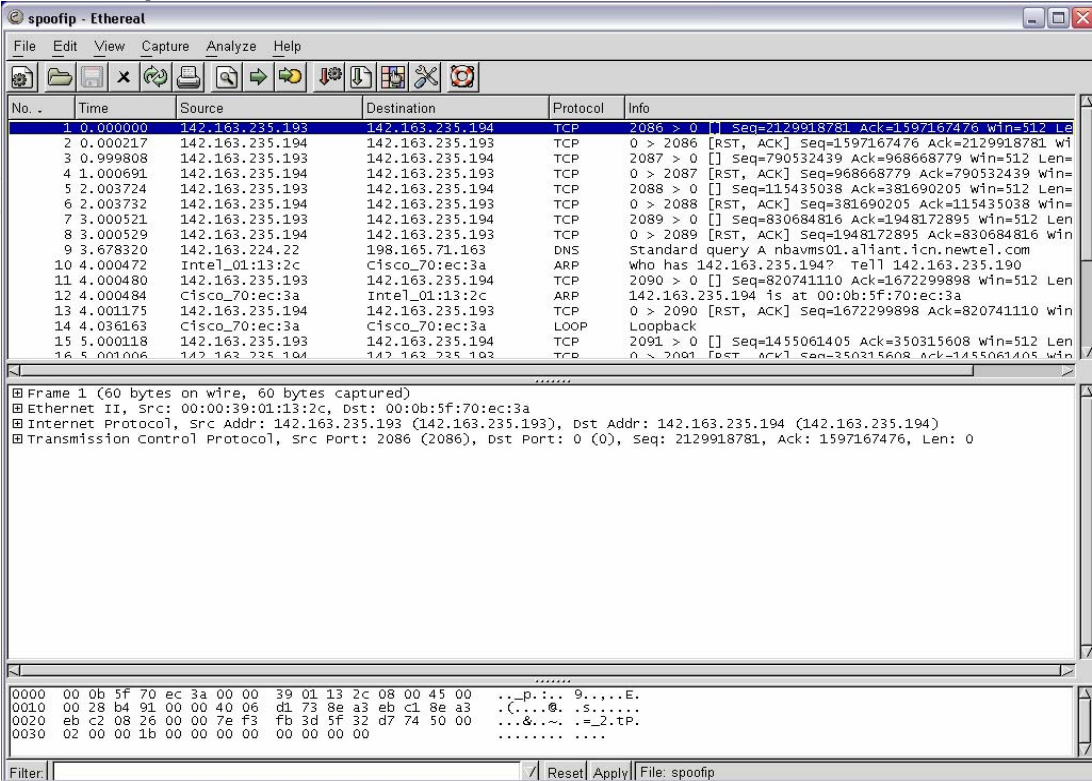
Second ping with IP Spoofed

```
[root@localhost root]# hping -a xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
HPING xxx.xxx.xxx.xxx (eth0 xxx.xxx.xxx.xxx): NO FLAGS are set, 40
headers + 0 data bytes
len=46 ip=xxx.xxx.xxx.xxx ttl=255 id=20405 sport=0 flags=RA seq=0
win=0 rtt=1.0
ms
len=46 ip=xxx.xxx.xxx.xxx ttl=255 id=20406 sport=0 flags=RA seq=1
win=0 rtt=0.9
ms
len=46 ip=xxx.xxx.xxx.xxx ttl=255 id=20407 sport=0 flags=RA seq=2
win=0 rtt=0.9
ms
len=46 ip=xxx.xxx.xxx.xxx ttl=255 id=20408 sport=0 flags=RA seq=3
win=0 rtt=1.0
ms
len=46 ip=xxx.xxx.xxx.xxx ttl=255 id=20409 sport=0 flags=RA seq=4
win=0 rtt=0.9
```

GSNA Practical 3.0

ethereal results show that the host responded to the spoofed IP's

Here is a paste of the trace



Objective/Subjective

Objective

GSNA Practical 3.0

Checklist Item 11	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS page 1 , Page 23 Section 3.1.4 Section 3.1.22 P.15 Section 3.1.23 P.15 Section 3.1.24 P.15 Own experience
Objective	Check Local authentication of Username and passwords
Risk	Section 1.2.1 .2 System Administration Section 1.2.1. 5 Lack of Security Policy to control Router Activities Section 1.2.2.3 Configuration Errors
Test	<p>1. From the configuration gathered in Checklist Item 4 Determine if there are any users accounts created on the router and if passwords are enabled. The information you are looking for is as follows:</p> <ul style="list-style-type: none"> - user-ID privilege 15 password 7 encrypted - enable password <p>Result – from the information in the configuration file there are no usernames configured however the enable password has been configured</p> <p>enable password 7 14141B180F0B</p> <p>Passwords has also been applied to aux and tty ports</p> <pre> line con 0 exec-timeout 0 0 password 7 xxxxxxxxxxxxxxxxxxxxxx login line aux 0 line vty 0 4 access-class 10 in exec-timeout 30 0 </pre>

GSNA Practical 3.0

password 7 xxxxxxxxxxxxxxxxxxxx

2. Telnet to the router, to do this from a dos or unix prompt

C:\telnet xxx.xxx.xxx.xxx (ip address)

3. Try cisco common username and passwords

Username : enter as in enter key
Password : enter as in enter key

Username: cisco
Username : cisco

Each password was tried consecutively; there are no usernames so just the passwords were tried. Each connection was refused

```
root@localhost root]# telnet xxx.xxx.xxx.xxx
Trying xxx.xxx.xxx.xxx...
Connected to xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx).
Escape character is '^]'.
```

```
xxxxxx Internet IISP
You must agree to the following before using this system
```

```
Use of this system is restricted to authorized employees of
Aliant Inc. and authorized contractors.Only authorized work using
company-supplied programs may be done on this system.Use of this
system is an agreement to monitoring.
```

```
User Access Verification
```

GSNA Practical 3.0

	<pre>Password: Password: Password: % Bad passwords Connection closed by foreign host. [root@localhost root]# [root@localhost root]# [root@localhost root]# telnet xxx.xxx.xxx.xxx Trying xxx.xxx.xxx.xxx... Connected to xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx) . Escape character is '^]'. xxxxx Internet IISP You must agree to the following before using this system Use of this system is restricted to authorized employees of Aliant Inc. and authorized contractors.Only authorized work using company-supplied programs may be done on this system.Use of this system is an agreement to monitoring. User Access Verification Password: Password: Password: % Bad passwords Connection closed by foreign host.</pre>
Objective/Subjective	Objective

Checklist Item 12

GSNA Practical 3.0

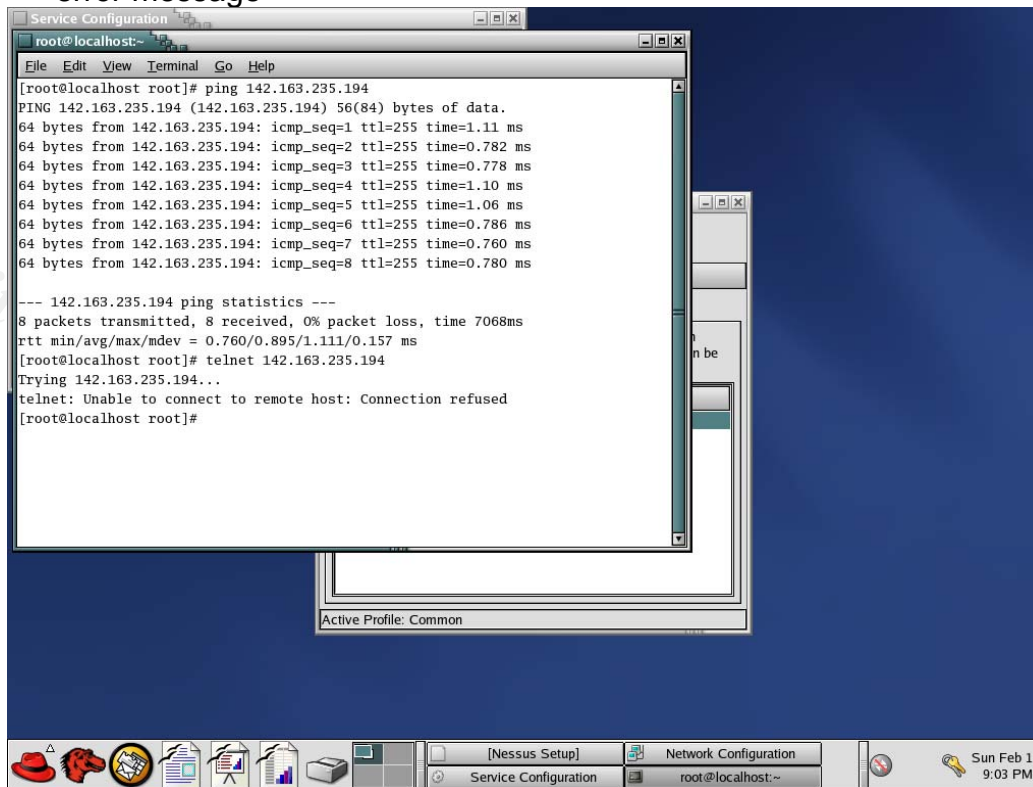
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 Benchmark Version 2.0 Sections 2.1 Page 8 Level 1 Benchmark Version 2.0 Section 3.1 Starting Page 13
Objective	Check to see if SNMP is enabled
Risk	Section 1.2.2 .1 Router may be Open to Internet Scans
Test	<p>3. Connect to the router as described in Checklist Item 4</p> <p>4. from the prompt</p> <p>iii. show config</p> <p>iv. Look for the following:</p> <p>snmp-server community (password) RW 12</p> <p>snmp-server community (password) RO 12</p> <p>snmp-server location (server location)</p> <p>snmp-server contact (contact information)</p> <p>snmp-server host</p> <p>Result –</p> <p>snmp-server location XXXXXXXXXXXXXXXXXXXX</p> <p>snmp-server contact Blair XXXXXXXXXXXXXXXX</p> <p>snmp-server enable traps tty</p> <p>The router has SNMP enables but only enable traps through the TTY port. The TTY port has an ACL on it that only allows the following IP xxx.xxx.xxxx.xxxx</p> <p>The acl is as follows:</p> <p>access-list 10 permit xxx.xxx.xxx.xxx</p> <p>The acl does not specify anything else on the port and it does not have an explicit deny any any so everything is open on the vty port for IP xxx.xxx.xxx.xxx</p>

GSNA Practical 3.0

Objective/Subjective	Objective
Checklist Item 13	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 Benchmark Version 2.0 Sections 2.1 Page 8 Level 1 Benchmark Version 2.0 Section 3.1 Starting Page 13
Objective	Check to determine if Telnet is enabled
Risk	Section 1.2.2.1 Router may be open to internet scans
Test	<ol style="list-style-type: none"> 1. From an outside device (internet connected test PC) attempt to telnet to the router. 2. from the prompt (DOS or Unix) 3. c:\telnet xxx.xxx.xxx.xxx (destination IP) <p>xxxxxx Internet IISP You must agree to the following before using this system</p> <p>Use of this system is restricted to authorized employees of xxxxxxxx. and authorized contractors.Only authorized work using company-supplied programs may be done on this system.Use of this system is an agreement to monitoring.</p> <p>User Access Verification</p> <p>Password:</p> <ol style="list-style-type: none"> 4. Once connected you will be presented a login prompt

GSNA Practical 3.0

5. If the connection is refused you will get a “connection refused by host” error message



The screenshot shows a terminal window titled 'root@localhost:~' with a menu bar (File, Edit, View, Terminal, Go, Help). The terminal output shows a successful ping to 142.163.235.194 with 8 packets received and 0% loss. Following the ping, a telnet attempt to the same IP is shown, resulting in the error message: 'telnet: Unable to connect to remote host: Connection refused'. The terminal window is overlaid on a desktop environment with a taskbar at the bottom showing icons for a red hat, a horse, a globe, and several application windows including 'Nessus Setup', 'Service Configuration', and 'Network Configuration'. The system clock in the bottom right corner indicates 'Sun Feb 15 9:03 PM'.

```
root@localhost root]# ping 142.163.235.194
PING 142.163.235.194 (142.163.235.194) 56(84) bytes of data:
64 bytes from 142.163.235.194: icmp_seq=1 ttl=255 time=1.11 ms
64 bytes from 142.163.235.194: icmp_seq=2 ttl=255 time=0.782 ms
64 bytes from 142.163.235.194: icmp_seq=3 ttl=255 time=0.778 ms
64 bytes from 142.163.235.194: icmp_seq=4 ttl=255 time=1.10 ms
64 bytes from 142.163.235.194: icmp_seq=5 ttl=255 time=1.06 ms
64 bytes from 142.163.235.194: icmp_seq=6 ttl=255 time=0.786 ms
64 bytes from 142.163.235.194: icmp_seq=7 ttl=255 time=0.760 ms
64 bytes from 142.163.235.194: icmp_seq=8 ttl=255 time=0.780 ms

--- 142.163.235.194 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7068ms
rtt min/avg/max/mdev = 0.760/0.895/1.111/0.157 ms
root@localhost root]# telnet 142.163.235.194
Trying 142.163.235.194...
telnet: Unable to connect to remote host: Connection refused
root@localhost root]#
```

**Result – if using the IP as laid out in the acl telnet was successful
If using any other IP connection was refused**

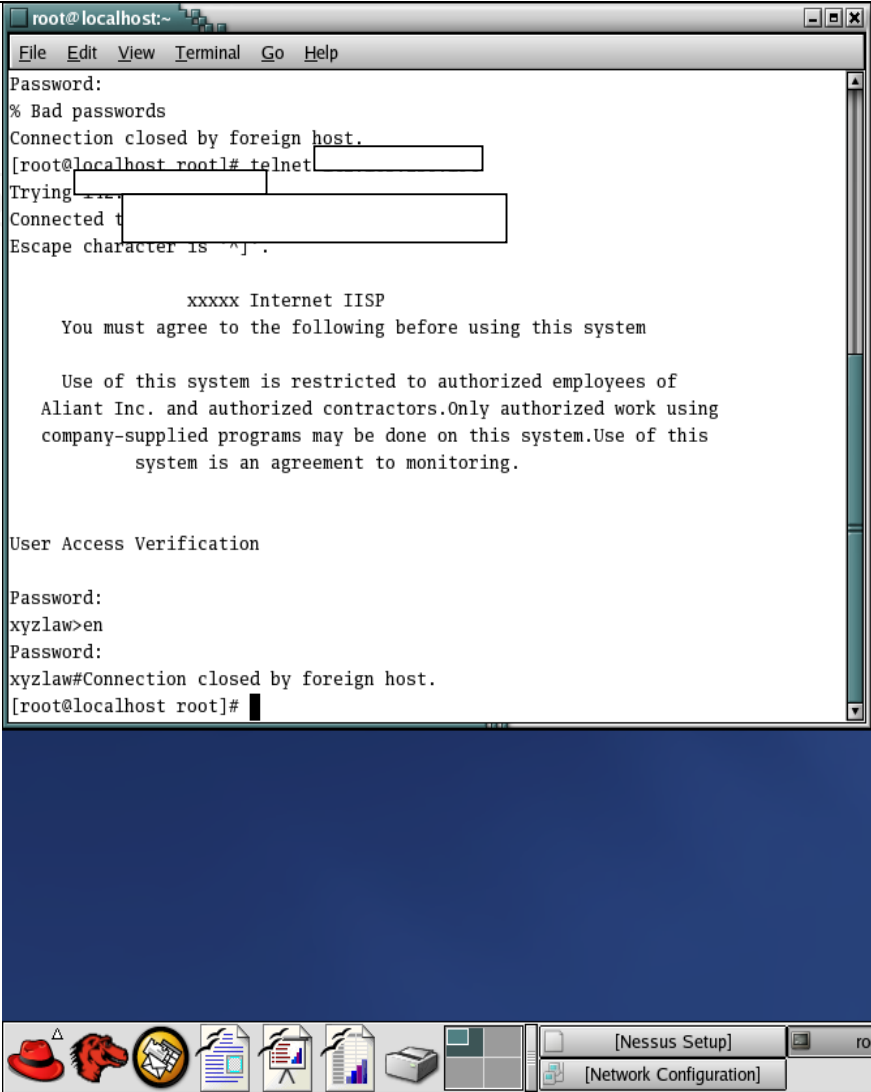
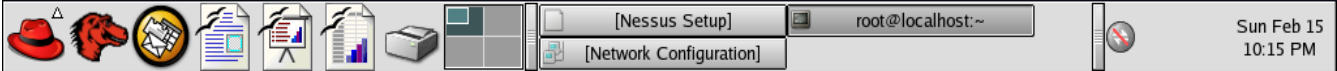
**If the IP is spoofed then telnet will be available to anyone attempting
connection to XYZ 's Router**

GSNA Practical 3.0

	See Results of Nessus Scan which also confirms telnet is open
Objective/Subjective	Objective

Checklist Item 14	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 Benchmark Version 2.0 Sections 2.1 Page 8
Objective	Determine if the exec timeout is enabled and actual configured time. This prevents unauthorized users from taking advantage of unused sessions.
Risk	Section 1.2.2.1 Router may be open to internet scans
Test	<p>2. Determine exec timeout is configured on the router. Use the configuration obtained from Checklist Item 4 or connect directly to the router as outlined in Checklist Item 4 and type:</p> <p>Show config</p> <p>Result –</p> <p>line con 0 exec-timeout 0 0</p> <p>There is no timeout on the direct connection.</p> <p>line vty 0 4 access-class 10 in exec-timeout 30 0</p> <p>On the telnet connection there is an timeout of 30 seconds</p> <p>3. Connect to the router with telnet and conduct no activity, time to see how long the router times you out and compare with configuration information above.</p>

GSNA Practical 3.0

	<div data-bbox="590 238 1455 1325"><pre>root@localhost:~ File Edit View Terminal Go Help Password: % Bad passwords Connection closed by foreign host. [root@localhost root]# telnet [redacted] Trying [redacted] Connected to [redacted] Escape character is '^]'. xxxxx Internet IISP You must agree to the following before using this system Use of this system is restricted to authorized employees of Aliant Inc. and authorized contractors.Only authorized work using company-supplied programs may be done on this system.Use of this system is an agreement to monitoring. User Access Verification Password: xyzlaw>en Password: xyzlaw#Connection closed by foreign host. [root@localhost root]#</pre></div> <div data-bbox="590 1255 1919 1325"><p>[Nessus Setup] [Network Configuration] root@localhost:~ Sun Feb 15 10:15 PM</p></div>
Objective/Subjective	Objective

GSNA Practical 3.0

Checklist Item 15	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 Benchmark Version 2.0 Sections 2.1 Page 8
Objective	Determine if the AUX port is enabled and if any modems are attached
Risk	
Test	<ol style="list-style-type: none"> 1. Physical inspection of the router to determine if there are any modems attached 2. Login to the router as laid out in Checklist Item 4 and perform the following commands from the router prompt <p>iii. router#show line aux 0</p> <p>The following should show up</p> <pre> router#sho line aux 0 Tty Typ Tx/Rx A Modem Roty AccO Accl Uses Noise Overruns Int 5 AUX 9600/9600 - - - - - 0 0 0/0 - Line 5, Location: "", Type: "" Length: 24 lines, Width: 80 columns Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits Status: Ready Capabilities: none Modem state: Ready Modem hardware state: noCTS noDSR DTR RTS Special Chars: Escape Hold Stop Start Disconnect Activation ^^x none - - none Timeouts: Idle EXEC Idle Session Modem Answer Session Dispatch </pre>

GSNA Practical 3.0

	<pre> 00:10:00 never none not set Idle Session Disconnect Warning never Login-sequence User Response 00:00:30 Autoselect Initial Wait not set Modem type is unknown. Session limit is not set. Time since activation: never Editing is enabled. History is enabled, history size is 20. DNS resolution in show commands is enabled Full user help is disabled Allowed input transports are none. Allowed output transports are pad telnet rlogin ssh. Preferred transport is telnet. No output characters are padded No special data dispatching characters iv. This is a view of when the aux port has been disabled, refer to bold type below this is an indication of a disabled aux port. router#sho line aux 0 Tty Typ Tx/Rx A Modem Roty AccO Accl Uses Noise Overruns Int 5 AUX 9600/9600 - - - - - 0 0 0/0 - Line 5, Location: "", Type: "" Length: 24 lines, Width: 80 columns </pre>
--	---

GSNA Practical 3.0

	<p>Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits Status: Ready Capabilities: EXEC Suppressed Modem state: Ready Modem hardware state: noCTS noDSR DTR RTS Special Chars: Escape Hold Stop Start Disconnect Activation ^^x none - - none Timeouts: Idle EXEC Idle Session Modem Answer Session Dispatch 00:10:00 never none not set Idle Session Disconnect Warning never Login-sequence User Response 00:00:30 Autoselect Initial Wait not set</p> <p>Modem type is unknown. Session limit is not set. Time since activation: never Editing is enabled. History is enabled, history size is 20. DNS resolution in show commands is enabled Full user help is disabled Allowed input transports are none. Allowed output transports are pad telnet rlogin ssh. Preferred transport is telnet. No output characters are padded No special data dispatching characters</p> <p>Result – the aux port on this router is enabled but there are no modems attached. The following is a result of the cli show command:</p>
--	--

GSNA Practical 3.0

```
YZLaw#sho line aux 0
```

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	Accl	Uses	Noise	Overruns	Int
5	AUX	9600/9600	-	-	-	-	0	0	0/0	-	

```
Line 5, Location: "", Type: ""
```

```
Length: 24 lines, Width: 80 columns
```

```
Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits
```

```
Status: Ready
```

```
Capabilities: none
```

```
Modem state: Ready
```

```
Modem hardware state: noCTS noDSR DTR RTS
```

```
Special Chars: Escape Hold Stop Start Disconnect Activation
```

```
^x none - - none
```

```
Timeouts: Idle EXEC Idle Session Modem Answer Session Dispatch
```

```
00:10:00 never none not set
```

```
Idle Session Disconnect Warning
```

```
never
```

```
Login-sequence User Response
```

```
00:00:30
```

```
Autoselect Initial Wait
```

```
not set
```

```
Modem type is unknown.
```

```
Session limit is not set.
```

```
Time since activation: never
```

```
Editing is enabled.
```

```
History is enabled, history size is 20.
```

```
DNS resolution in show commands is enabled
```

```
Full user help is disabled
```

```
Allowed input transports are none.
```

```
Allowed output transports are pad telnet rlogin ssh.
```

GSNA Practical 3.0

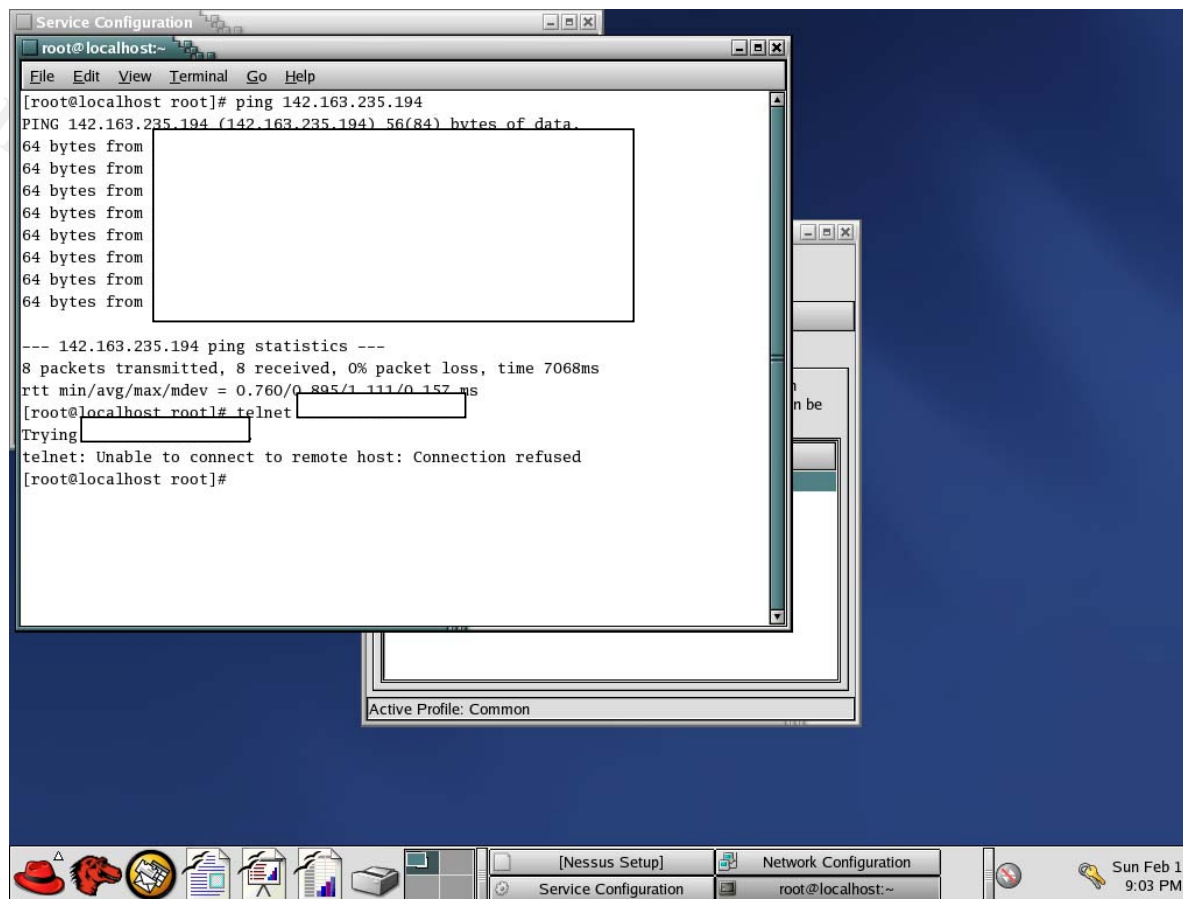
	Preferred transport is telnet. No output characters are padded No special data dispatching characters
Objective/Subjective	Objective

Checklist Item 16	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS
Objective	Determine Configuration of the TTY Lines (passwords and ACLs)
Risk	Section 1.2.2.1 Router May be open to internet scans which may result in attempts to breach router defences to infiltrate XYZ Law's internal network
Test	<ol style="list-style-type: none"> 1. Login into the router as laid out in Checklist Item 4 or view the configuration file. If choosing to login in once connected type the following at the router prompt: <ol style="list-style-type: none"> i. router#show config ii. Once the config is shown look for the following <p>line vty 0 4 (actual connection line) access-class 10 in (access list attached to interface) exec-timeout 30 0 (timeout for unused session 30minutes) password 7 xxxxxxxxxxxxxxxxxxxx (password assigned to interface)</p> <p>this is near the end of the configuration file</p> 2. Look at Access List assigned to interface Router#show access-list (access list number) <p>how access-list 10 Standard IP access list 10 10 permit xxx.xxx.xxx.xxx</p>

GSNA Practical 3.0

3. Once the information is gathered above prove it's worth by doing the following:
- iv. attempt to telnet to the router

Connection refused which proves the access list is working



The screenshot shows a terminal window titled 'Service Configuration' with a root prompt. The user enters 'ping 142.163.235.194'. The output shows 8 successful pings from 142.163.235.194 with 0% packet loss and a time of 7068ms. The user then enters 'telnet'. The output shows 'Trying [redacted]' followed by 'telnet: Unable to connect to remote host: Connection refused'. The terminal window is overlaid on a desktop background with a taskbar at the bottom showing icons for a red hat, a horse, a document, a folder, a printer, and a network icon. The taskbar also shows '[Nessus Setup]', 'Service Configuration', 'Network Configuration', and 'root@localhost:~'. The system clock shows 'Sun Feb 15 9:03 PM'.

```
root@localhost:~  
[root@localhost root]# ping 142.163.235.194  
PING 142.163.235.194 (142.163.235.194) 56(84) bytes of data:  
64 bytes from [redacted]: icmp_seq=1 ttl=64 time=0.760 ms  
64 bytes from [redacted]: icmp_seq=2 ttl=64 time=0.895 ms  
64 bytes from [redacted]: icmp_seq=3 ttl=64 time=0.760 ms  
64 bytes from [redacted]: icmp_seq=4 ttl=64 time=0.760 ms  
64 bytes from [redacted]: icmp_seq=5 ttl=64 time=0.760 ms  
64 bytes from [redacted]: icmp_seq=6 ttl=64 time=0.760 ms  
64 bytes from [redacted]: icmp_seq=7 ttl=64 time=0.760 ms  
64 bytes from [redacted]: icmp_seq=8 ttl=64 time=0.760 ms  
--- 142.163.235.194 ping statistics ---  
8 packets transmitted, 8 received, 0% packet loss, time 7068ms  
rtt min/avg/max/mdev = 0.760/0.895/1.111/0.157 ms  
[root@localhost root]# telnet [redacted]  
Trying [redacted]  
telnet: Unable to connect to remote host: Connection refused  
[root@localhost root]#
```

- v. if connect attempt to login

GSNA Practical 3.0

	<p>I had to use the only IP that the access list allowed once connected a login prompt came up which proves a password is required.</p> <p>vi. on the router do a “show access-list” to see if there are numbers increasing to determine hits on the access list</p> <p>how access-list 10 Standard IP access list 10 10 permit xxx.xxx.xxx.xxx (12 matches)</p>
Objective/Subjective	Objective

Checklist Item 17	
Reference	<p>Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 Benchmark Version 2.0 Sections 2.1 Page 9 Level 1 Benchmark Version 2.0 Sections 3.1.59/60 Page 20</p>
Objective	<p>Determine if unused Services are enabled</p> <p>HTTP Finger Service CDP BOOTp Config Server TFTP Small UDP Service Small TCP Services</p>
Risk	<p>Section 1.2.2.1 Router may be open to internet scans Section 1.2.2.2 Denial of Service Attacks</p>
Test	<p>1. HTTP – Connect to the router as described in Checklist Item 4, once logged in type :</p>

GSNA Practical 3.0

	<p>Router#show run</p> <p>Look for the following in the configuration:</p> <p>no ip http server</p> <p>If this is not in the config HTTP server is enabled this the default setting for Cisco routers</p> <p>Result – this statement is found on the configuration. HTTP Server is disabled</p> <p>From a web browser attempt to connect to the router by putting the IP address in the browser if HTTP is enabled the browser will connect you to the router. If HTTP is disabled then the connection will be refused.</p> <p>Result – I was unable to connect with a browser. I used Mozilla and received a “connection refused”</p> <p>RAT Scan report</p> <p>10 pass IOS - no ip http server xyzlaw.txt</p> <p>2. Finger Service – To determine if this service is running login in the router as in Check List Item 4. Perform a “show run” if the finger service is running you will see in the global config</p> <p>Ip finger service</p> <p>If this is not there then finger service is disabled.</p> <p>Result – Finger service did not show up in the “show run” command so therefore it is not enabled. Refer to the configuration</p>
--	---

	<p>file in Checklist Item 4 for confirmation.</p> <p>RAT Scan Report</p> <p>5 pass IOS 12.1,2,3 - no finger service xyzlaw.txt</p> <p>3. CDP – Cisco Discovery Protocol. This protocol is meant for cisco devices to discover each other for troubleshooting purposes. If this is not utilized then it should be disabled. There are known denial of service attacks that utilize CDP.</p> <p>CDP is enabled by default to determine if CDP is enabled login to the router as laid out in Checklist Item 4 and perform the “show run” command. In the global config if you see the following :</p> <p style="padding-left: 40px;">no cdp run</p> <p>This insures that CDP is disabled. CDP is enabled by default and will have to manually disabled.</p> <p>Also in the configuration file on the individual interfaces that are used the following should be there to ensure CDP is disabled</p> <p style="padding-left: 40px;">no cdp enable</p> <p>this ensures CDP is disabled on the interface.</p> <p>Result - no cdp run CDP is disabled Globally</p>
--	--

GSNA Practical 3.0

	<pre> interface Ethernet0 description Customer LAN Segment ip address xxx.xxx.xxx.xxx 255.255.255.248 half-duplex no cdp enable ! interface FastEthernet0 description Connection to ISP ip address xxx.xxx.xxx.xxx 255.255.255.252 speed auto no cdp enable CDP is disabled on the interface RAT Scan Report 7 pass IOS - no cdp run xyzlaw.txt 4. Bootp – There are known DOS attacks utilizing bootp on cisco routers and is enabled by default. Login to the router as laid out in check list Item 4 and type a “show run” at the router prompt. In the Global config if Bootp is disabled you should see the following: no ip bootp server If this is not there then bootp services are enabled. Result – bootp is not found in the config so therefore bootp is enabled. If this service is not used then it should be disabled. For confirmation please refer to the config file in checklist item 4. </pre>
--	--

GSNA Practical 3.0

	<div><div>RAT Scan Report</div><div>5 FAIL IOS - no ip bootp server xyzlaw.txt n/a 2</div><div>5. TFTP – No ACL Restricting TFTP</div><div>6. Config Server – this allows a router to load its startup configuration from remote devices.</div><div>Result from RAT Scan confirms config server is disabled</div><div>7 pass IOS - no service config xyzlaw.txt</div><div>7. tcp-keepalives – stale connections use resources and could potentially be used to gain access.</div><div>Result from RAT Scan Report confirms TCP Keep alives are enabled</div><div>5 FAIL IOS - tcp keepalive service xyzlaw.txt n/a 2</div><div>8. Small TCP Service</div><div>Results from RAT Scan report small tcp services are disabled</div><div>7 pass IOS 12 - no udp-small-servers xyzlaw.txt</div><div>9. Small UDP Services</div><div>Results from RAT Scan report Small UDP services are disabled</div></div>
--	---

GSNA Practical 3.0

	7 pass IOS 12 - no tcp-small-servers xyzlaw.txt
Objective/Subjective	Objective

Checklist Item 18	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Benchmark for Cisco IOS page 10 Section 3.1.69 Page 22
Objective	Determine if Directed Broadcast is enabled
Risk	Section 1.2.2.2 Denial of Service Attacks Router Interfaces that allow directed broadcasts can be open to “smurf” attacks
Test	<ol style="list-style-type: none"> 1. Login to the router as describe in Checklist Item 4. Completed 2. Do the “show run” command from the router prompt Completed 3. Inspect each interface for the following: <div style="margin-left: 40px;">ip directed-broadcast</div> <div> interface Ethernet0 description Customer LAN Segment ip address xxx.xxx.xxx.xxx 255.255.255.248 half-duplex no cdp enable ! </div> <div> interface FastEthernet0 description Connection to ISP ip address xxx.xxx.xxx.xxx 255.255.255.252 </div>

GSNA Practical 3.0

<p>Objective/Subjective</p>	<p> speed auto no cdp enable 4. If this is there directed-broadcast is enabled if not it is disabled Result directed broadcast is not enabled Result from RAT Scan confirms 7 pass IOS 12 - no directed broadcast xyzlaw.txt </p>
<p>Objective/Subjective</p>	<p>Objective</p>

Checklist Item 19	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS
Objective	Is IP source routing enabled
Risk	Section 1.2.2.2 Denial of Service Attacks Source routing is a feature of IP whereby individual packets can specify routes. This feature is used in several kinds of attacks. Cisco routers normally accept and process source routes. Unless required this feature should be turned off.
Test	<p>Run Router Auditing Tool as described in General Checklist Item 6 and determine from the results</p> <p>Pass – IP Source Routing is disabled</p> <p>Fail - IP Source Routing in enabled</p> <p>Result from RAT Scans</p> <p>7 FAIL IOS - no ip source-route xyzlaw.txt n/a 2</p> <p>IP Source Routing is enabled</p>
Objective/Subjective	Objective

GSNA Practical 3.0

Checklist Item 20	
Reference	Center For Internet Security Gold Standard Benchmark for Cisco IOS Level 1 and 2 Benchmarks page 24
Objective	Determine IP Proxy Arp Enabled Proxy Arp breaks the LAN security perimeter effectively extending a LAN at layer 2 across multiple segments
Risk	Section 1.2.2.1 Router Open to internet Scans Section 1.2.2.2 Denial of Service Attacks
Test	<p>a. Login to the router as laid out in General Checklist Item 4</p> <p>b. Do a “show run” to bring up the configuration</p> <p>c. inspect the interfaces and determine if this is included</p> <p>no ip proxy-arp</p> <p>4. Proxy arp is enabled by default if this line is not there then proxy arp is enabled</p> <p>Result</p> <pre> interface Ethernet0 description Customer LAN Segment ip address xxx.xxx.xxx.xxx 255.255.255.248 half-duplex no cdp enable ! interface FastEthernet0 description Connection to ISP ip address xxx.xxx.xxx.xxx 255.255.255.252 speed auto </pre>

GSNA Practical 3.0

	no cdp enable Proxy arp is enabled on both interfaces
Objective/Subjective	Objective

2.2 Cisco Specific Checklist

This checklist is specific to security warnings released by Cisco. It is based on information provided on Cisco's Website located at:

http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html

Checklist Item 1	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Cisco Security Advisory Check Security Advisory: Cisco IOS Software Multiple SNMP Community String Vulnerabilities The following is a description of the impact from Cisco's website</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13b5.shtml#software</p> <p>The following information is from the url above obtained from Cisco's website</p> <p>Knowledge of read-only community strings allows read access to information stored on an affected device, leading to a failure of confidentiality. Knowledge of read-write community strings allows remote configuration of affected devices without authorization, possibly without the awareness of</p>

GSNA Practical 3.0

	<p>the administrators of the device and resulting in a failure of integrity and a possible failure of availability.</p> <p>These vulnerabilities could be exploited separately or in combination to gain access to or modify the configuration and operation of any affected devices without authorization. Customers are urged to upgrade affected systems to fixed releases of software, or to apply measures to protect such systems against unauthorized use by restricting access to SNMP services until such time as the devices can be upgraded.</p> <ul style="list-style-type: none"> • IOS software Major Release version 12.0 and IOS releases based on 11.x or earlier are not affected by the vulnerabilities described in this notice. All other releases of 12.0, such as 12.0DA, 12.0S or 12.0T, may be affected. • CSCdr59314 is only present in certain 12.1(3) releases and does not affect any other IOS releases. • Fixes for all six defects have been integrated into 12.2 prior to its initial availability, and therefore all releases based on 12.2 and all later versions are not vulnerable to the defects described in this advisory.
Risk	<p>Section 1.2.2.1 Router may be open to internet scans and weaknesses exploited</p> <p>Section 1.2.2.5 Hardware/Software upgrades – if the version of code is deficient then a possible upgrade may be required.</p>
Test	<p>Determine if software version of router is affected</p> <p>3. Login to the router as described in Checklist Item 4 and at the router prompt type</p> <p>Router#show version</p> <p>Cisco Internetwork Operating System Software IOS (tm) C1700 Software (C1700-BK8NO3R2SY7-M), Version 12.2(15)T9, RELEASE SOFTWARE (fc2)</p>

GSNA Practical 3.0

TAC Support: <http://www.cisco.com/tac>
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Sat 01-Nov-03 06:24 by ccai
Image text-base: 0x80008120, data-base: 0x81207F5C

ROM: System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1)
ROM: C1700 Software (C1700-BK8NO3R2SY7-M), Version 12.2(15)T9, RELEASE SOFTWARE (fc2)

xyzlaw uptime is 2 days, 19 hours, 47 minutes
System returned to ROM by power-on
System image file is "flash:c1700-bk8no3r2sy7-mz.122-15.T9.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco 1721 (MPC860P) processor (revision 0x100) with 58002K/7534K bytes of memory.
Processor board ID FOC07010MUR (2301023196), with hardware revision 0000

GSNA Practical 3.0

	<p>MPC860P processor: part number 5, mask 2</p> <p>Bridging software.</p> <p>X.25 software, Version 3.0.0.</p> <p>1 Ethernet/IEEE 802.3 interface(s)</p> <p>1 FastEthernet/IEEE 802.3 interface(s)</p> <p>32K bytes of non-volatile configuration memory.</p> <p>16384K bytes of processor board System flash (Read/Write)</p> <p>Configuration register is 0x142</p> <p>4. From this information determine the IOS version.</p> <p>Result – IOS Version 12.2(15)T9 is not affected by this security advisory</p>
Objective/Subjective	Objective

Checklist Item 2	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Cisco Security Advisory Check</p> <p>Cisco Security Advisory: Cisco IOS ARP Table Overwrite Vulnerability</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b113c.shtml</p> <p>The following information is from the url above obtained from Cisco's website</p> <p>It is possible to send an Address Resolution Protocol (ARP) packet on a local broadcast interface (for example, Ethernet, cable, Token Ring, FDDI) which could cause a router or switch running specific versions of Cisco IOS® Software Release to stop sending and receiving ARP packets on</p>

GSNA Practical 3.0

	<p>the local router interface. This will in a short time cause the router and local hosts to be unable to send packets to each other. ARP packets received by the router for the router's own interface address but a different Media Access Control (MAC) address will overwrite the router's MAC address in the ARP table with the one from the received ARP packet. This was demonstrated to attendees of the Black Hat conference and should be considered to be public knowledge. This attack is only successful against devices on the segment local to the attacker or attacking host.</p> <p>Impact This issue can cause a Cisco Router to be vulnerable to a Denial-of-Service attack, once the ARP table entries time out. This defect does not result in a failure of confidentiality of information stored on the unit, nor does this defect allow hostile code to be loaded onto a Cisco device. This defect may cause a Denial-of-Service on the management functions of a Cisco Layer 2 Switch, but does not affect traffic through the device</p>
Risk	Section 1.2.2.2 Denial of Service Attack
Test	<p>determine if the router is running an affected IOS,</p> <ol style="list-style-type: none"> 4) log in to the device as laid out in checklist item 4 5) and issue the command show version command at the router prompt. Inspect the configuration for the following: <p style="text-align: center;">Internetwork Operating System Software" or "IOS (tm</p> 6) If this found compare the software version number with the table on this website from Cisco http://www.cisco.com/en/US/products/products_security_advisory09186a00800b113c.shtml 7) This will provide upgrade information if required <p>Result – Based on the show version information found in the previous checklist I was able to determine</p>

GSNA Practical 3.0

	that the current version of code is not affected by this advisory.
Objective/Subjective	Objective

Checklist Item 3	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the router is affected by the following advisory</p> <p>Security Advisory: Cisco IOS Syslog Crash</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13a7.shtml</p> <p>The following information is from the url above obtained form Cisco's website</p> <p>Certain versions of Cisco IOS software may crash or hang when they receive invalid user datagram protocol (UDP) packets sent to their "syslog" ports (port 514). At least one commonly-used Internet scanning tool generates packets which can cause such crashes and hangs. This fact has been announced on public Internet mailing lists which are widely read both by security professionals and by security "crackers", and should be considered public information.</p> <p>This vulnerability affects devices running Cisco IOS software version 11.3AA, version 11.3DB, or any 12.0-based version (including 12.0 mainline, 12.0S, 12.0T, and any other regular released version whose number starts with "12.0"). The vulnerability has been corrected in certain special releases, and will be corrected in maintenance and interim releases which will be issued in the future; see the section on "Software Versions and Fixes" for details on which versions are affected, and on which versions are, or will be, fixed. Cisco intends to provide fixes for all affected IOS variants.</p>
Risk	Section 1.2.2.2 Denial of Service Attack

GSNA Practical 3.0

Test	<p>4. Login to the router as described in Checklist Item 4</p> <p>5. Do a "show version" as described in the previous Cisco Checklist</p> <p>6. Go to table on the above webpage at Cisco to determine if the current IOS is affected.</p> <p>Result – IOS Version 12.2(15)T9 is not affected by this security advisory</p>
Objective/Subjective	Objective

Checklist Item 4	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the router is affected by the following Security Advisory</p> <p>Cisco Security Notice: MS SQL Worm Mitigation Recommendations</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a0080133399.shtml</p> <p>The following information is from the url above obtained from Cisco's website</p> <p>Cisco customers are currently experiencing attacks due to a new worm that has hit the Internet. The signature of this worm appears as high volumes of UDP traffic to port 1434. Affected customers have been experiencing high volumes of traffic from both internal and external systems. Symptoms on Cisco devices include, but are not limited to high CPU and traffic drops on the input interfaces.</p> <p>The worm has been referenced by several names, including "Slammer", "Sapphire" as well as</p>

GSNA Practical 3.0

	<p>"MS SQL worm".</p> <p>Cisco has a companion document detailing Cisco products which are affected directly by this worm:</p> <p>http://www.cisco.com/warp/public/707/cisco-sa-20030126-ms02-061.shtml</p> <p>The current recommended fix for IOS is to apply an ACL to block traffic on port 1443</p>
Risk	Section 1.2.2.2 Denial of Service Attacks
Test	<ol style="list-style-type: none"> 1. login to the router as described in General Checklist Item 4. 2. At the prompt do a "show run" 3. Inspect the configuration and determine if the following access list has been applied 4. <code>access-list 115 deny udp any any eq 1434</code> <code>access-list 115 permit ip any any</code> 5. Determine if the access list has been applied to the public interface <p><code>int <interface></code> <code>ip access-group 115 in</code> <code>ip access-group 115 out</code></p> <p>Result – This has not been applied to XYZ Router</p>
Objective/Subjective	Objective
Checklist Item 5	

GSNA Practical 3.0

Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the router is affected by the following Security Advisory</p> <p>Cisco IOS HTTP Server Query Vulnerability</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13b6.shtml</p> <p>The following information is from the url above obtained from Cisco's website</p> <p>defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to "http://router-ip/anytext?/" is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.</p> <p>The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.</p> <p>The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.</p> <p>This vulnerability can only be exploited if the enable password is known or not set.</p>
Risk	Section 1.2.2.2 Denial of Service Attacks
Test	<ol style="list-style-type: none"> 5. Login to the router as laid out in General Checklist Item 4 6. at the router prompt do a "show version" 7. Inspect the information for the IOS version

GSNA Practical 3.0

	<p>8. Go to the table on the cisco website (Link above) and determine if the current version of IOS is affected</p> <p>Result – IOS Version 12.2(15)T9 is not affected by this security advisory</p>
Objective/Subjective	Objective

Checklist Item 6	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the router is affected by the following Security Advisory</p> <p>Security Advisory: Cisco IOS Remote Router Crash</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b139d.shtml</p> <p>The following information is from the url above obtained form Cisco's website</p> <p>An error in Cisco IOS software makes it possible for untrusted, unauthenticated users who can gain access to the login prompt of a router or other Cisco IOS device, via any means, to cause that device to crash and reload.</p> <p>This applies only to devices running classic Cisco IOS software, including most, but not all, Cisco router products. The easiest way to determine whether your device is running classic Cisco IOS software is to use the show version command to determine who is affected.</p> <p>If attackers know the details of the Cisco IOS software error they will be able to cause the router to crash and reload <i>without having to log in to the router</i>. Because this problem involves damage to an internal data struture, it is possible that other, more subtle or targeted effects on system operation could also be induced by proper exploitation. Such exploitation, if it is possible at all, would require significant engineering skill and a thorough knowledge of the internal operation of Cisco IOS software, including Cisco trade secret</p>

GSNA Practical 3.0

	<p>information</p> <p>Affected IOS Versions</p> <ul style="list-style-type: none"> • 11.3(1), 11.3(1)ED, 11.3(1)T • 11.2(10), 11.2(9)P, 11.2(9)XA, 11.2(10)BC, 11.2(8)SA3 • 11.1(15)CA, 11.1(16), 11.1(16)IA, 11.1(16)AA, 11.1(17)CC, 11.1(17)CT • 11.0(20.3)
Risk	Section 1.2.2.2 Denial of Service
Test	<p>4. Login to the router as described in General Checklist Item 4</p> <p>5. At the router prompt do a “show version” and determine the IOS Version on the current router.</p> <p>Utilize the results from show version in Cisco checklist item 1</p> <p>IOS version is 12.2(15)T9</p> <p>6. Determine if the IOS version matches with the list mentioned above.</p> <p>Result – IOS Version 12.2(15)T9 is not affected by this security advisory</p>
Objective/Subjective	Objective

Checklist Item 7	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	Determine if the Router is vulnerable to the following Cisco Advisory

GSNA Practical 3.0

	<p>Security Advisory: Cisco IOS Software Input Access List Leakage with NAT</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13a8.shtml</p> <p>The following information is from the url above obtained from Cisco's website</p> <p>A group of related software bugs (bug IDs given under "Software Versions and Fixes") create an undesired interaction between network address translation (NAT) and input access list processing in certain Cisco routers running 12.0-based versions of Cisco IOS software (including 12.0, 12.0S, and 12.0T, in all versions up to, but not including, 12.0(4), 12(4)S, and 12.0(4)T, as well as other 12.0 releases). Non-12.0 releases are not affected.</p> <p>This may cause input access list filters to "leak" packets in certain NAT configurations, creating a security exposure. Configurations without NAT are not affected.</p> <p>The failure does not happen at all times, and is less likely under laboratory conditions than in installed networks. This may cause administrators to believe that filtering is working when it is not.</p>
Risk	Section 1.2.2.2 Denial of Service
Test	<p>5. Login to the router as described in General Checklist Item 4</p> <p>6. At the router prompt do a "show version" and determine the IOS Version on the current router.</p> <p>7. Utilize the results from show version in Cisco checklist item 1</p> <p>IOS version is 12.2(15)T9</p> <p>8. Determine if the IOS version matches those found on the table on the Cisco Website</p>

GSNA Practical 3.0

	mentioned above. Result – IOS Version 12.2(15)T9 is not affected by this security advisory
Objective/Subjective	Objective

Checklist Item 8	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the Router is vulnerable to the following Cisco Advisory</p> <p>Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packets</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00801a34c2.shtml</p> <p>The following information is from the url above obtained from Cisco's website</p> <p>routers and switches running Cisco IOS® software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. Multiple IPv4 packets with specific protocol fields sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. Traffic passing through the device cannot block the input queue. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. Multiple valid workarounds are available in the form of best practices for situations where software upgrades are not currently feasible.</p> <p>If the software version is not on the router the current ACL workaround should be applied</p> <pre>access-list 101 permit tcp any any access-list 101 permit udp any any access-list 101 deny 53 any any access-list 101 deny 55 any any</pre>

GSNA Practical 3.0

	<pre> access-list 101 deny 77 any any access-list 101 deny 103 any any !--- insert any other previously applied ACL entries here !--- you must permit other protocols through to allow normal !--- traffic -- previously defined permit lists will work !--- or you may use the permit ip any any shown here access-list 101 permit ip any any </pre>
Risk	Section 1.2.2.2 Denial of Service
Test	<p>6. Login to the router as described in General Checklist Item 4</p> <p>7. At the router prompt do a “show version” and determine the IOS Version on the current router.</p> <p>8. Utilize the results from show version in Cisco checklist item 1</p> <p>IOS version is 12.2(15)T9</p> <p>9. Determine if the IOS version matches those found on the table on the Cisco Website mentioned above.</p> <p>This version of code is susceptible to this attack</p> <p>10. If the IOS version does not match do a “show run” and determine if the above mentioned access list is configured and applied to the public interface.</p> <p>Using the information gathered in General Checklist Item 1 it was determined that the required access list is not configured and that this router is open to this attack</p>
Objective/Subjective	Objective

GSNA Practical 3.0

Checklist Item 9	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the Router is vulnerable to the following Cisco Advisory</p> <p>Security Advisory: Cisco IOS Command History Release at Login Prompt</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13aa.shtml</p> <p>The following information is from the url above obtained form Cisco's website</p> <p>An error in Cisco IOS® software makes it possible for untrusted, unauthenticated users who can gain access to the login prompt of a router or other Cisco IOS device, via any means, to obtain fragments of text entered by prior interactive users of the device. This text may contain sensitive information, possibly including passwords. This vulnerability exposes only text entered at prompts issued by the IOS device itself; the contents of data packets forwarded by IOS devices are not exposed, nor are data entered as part of outgoing interactive connections, such as TELNET connections, from the IOS device to other network nodes.</p>
Risk	Section 1.2.2.1 Router may be open to internet scans
Test	<ol style="list-style-type: none">5. Login to the router as described in General Checklist Item 46. At the router prompt do a "show version" and determine the IOS Version on the current router.7. Utilize the results from show version in Cisco checklist item 1 <p>IOS version is 12.2(15)T9</p> <ol style="list-style-type: none">8. Determine if the IOS version matches those found on the table on the Cisco Website mentioned above.

GSNA Practical 3.0

	Result – IOS Version 12.2(15)T9 is not affected by this security advisory
Objective/Subjective	Objective

Checklist Item 10	
Reference	http://www.cisco.com/en/US/products/hw/routers/ps221/prod_security_advisories_list.html
Objective	<p>Determine if the Router is vulnerable to the following Cisco Advisory</p> <p>Cisco Security Advisory: Cisco IOS Software TCP Initial Sequence Number Randomization Improvements</p> <p>http://www.cisco.com/en/US/products/products_security_advisory09186a00800b1396.shtml</p> <p>Cisco IOS® Software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.</p> <p>The following information is from the url above obtained form Cisco's website</p> <p>This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.</p> <p>To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.</p> <p>Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.</p>

GSNA Practical 3.0

Risk	Section 1.2.2.1 Router may be open to internet scans
Test	<p>5. Login to the router as described in General Checklist Item 4</p> <p>6. At the router prompt do a “show version” and determine the IOS Version on the current router.</p> <p>7. Utilize the results from show version in Cisco checklist item 1</p> <p>IOS version is 12.2(15)T9</p> <p>8. Determine if the IOS version matches those found on the table on the Cisco Website mentioned above.</p> <p>Result – IOS Version 12.2(15)T9 is not affected by this security advisory</p>
Objective/Subjective	Objective

Part 4 – Audit Report

Executive Summary

The goal of the audit has been achieved. The Cisco 1721 router has been analyzed to determine its vulnerabilities and strengths in association to XYZ Law. XYZ Law has requested an independent audit of their primary perimeter device and all objectives were met.

This audit has determined that the Cisco 1721 router is doing little to protect the information assets of XYZ Law from internet penetration and possible loss. There were a total of 12 exceptions found in the audit. The advantages each are fairly easy to fix and would require coordination with XYZ's IT partner.

4.1 Audit Findings

The audit findings will correlate the checklist item that found the exception, the risk associated prioritized by level and severity. The detailed findings of each item can be found in Section 3 of this document. The risk levels are as follows:

High – May affect the company in a very severe way i.e. loss of business or significant loss of efficiency.

Medium – May affect day to day operations. The company will continue to operate but at a less efficient rate.

Low – May affect operations in a small way.

1. General Check List Item 5 Section 3 Page 75 – Nessus Vulnerability Scan For Nessus Results see Appendix A	
Risk	XYZ Router is open to Internet scans and possible exploitation of vulnerabilities
Risk Level	High
Exception	<ul style="list-style-type: none"> - Nessus was able to discover open ports such as telnet (port 23) - Nessus Determined that the router is open to ICMP Ping discovery - Nessus was able to determine IOS and type of router. This can be used to determine exploits against the router - By scanning the internal IP space which is public routable IPS Nessus was able to determine OS and port openings of

	the internal XYZ PC's
Summary	The XYZ Law router is dangerously open to any type of internet discovery scans and as a result sensitive information on XYZ Law's personal computers is at risk.

2. General Checklist Item 8 Section 3 Page 82 - Test the ACL against the written security policy or against the "Deny All" rule Section 3 page	
Risk	XYZ Law is open to internet scans, possible perimeter penetration, and denial of service attacks
Risk Level	High
Exception	There are no access list of any kind on the primary interfaces. There is an access list on the tty o4 port allowing everything from one IP address
Summary	Access Lists on a router are the primary protection against internet scans and denial of service attacks. Access lists are used to filter any unwanted traffic that passes through the router. By not applying access lists the primary interface on the router XYZ is open to attack from the internet which in turn may compromise sensitive information such as client data or affect operations through denial of service attacks

3. General Checklist Item 9 Section 3 Page - Verify the router is egress filtering local network traffic and the outbound capabilities of the router	
Risk	The internal network has full access to the outside internet. There are no egress filters in place.
Risk Level	High
Exception	There are no access list on the egress Ethernet interface. The internal network PC's has full access to the public internet.
Summary	<p>Egress filters can be used to for two reasons:</p> <ul style="list-style-type: none"> - Protect the internal network from being used as malicious tools against other networks. It is responsible to keep the internal network from being broadcast out and not allow it to be used in a malicious way. It can damage the reputation of XYZ Law if its network was used as a weapon against other networks. - Protect the internal network from themselves. By restricting certain functionality it can prevent damaging viruses, denial of service attacks caused by Trojans and worms from ever entering the private network. This could cause exposure and damage to XYZ's sensitive information and operations.

4. General Checklist Item 7 Section 3 page 82 - Determine if Router is configured to provide Network Address Translation (NAT)	
Risk	Router may be open to internet scans
Risk Level	High
Exception	NAT is not enabled
Summary	NAT or Network Address Translator (RFC 1631) is basically the router's ability to translate internal IP addresses to outside public addresses and vice versa. NAT can be used to ensure the inside network is not broadcasted. This ties into exception number 3 by enabling NAT the internal network IP's will not be broadcasted to the public internet. Scans cannot penetrate through NAT to discover the network behind it.

5. General Checklist Item 10 Section 3 page 85 - Determine if Router is able to do IP Address Spoof detection	
Risk	Router may be open to internet scans
Risk Level	High
Exception	Router unable to detect IP Address Spoof Detection
Summary	Routers generally don't do IP address spoof detection in its default configuration. Although the tty 04 port has an access list applied that only allows one IP, that IP can be spoofed (the attacker can make their IP address look like the trusted IP) so that the access list and the router sees it as a trusted device. This can be used to penetrate the XYZ network and either damage or compromise sensitive information.

6. General Checklist Item 11 Section 3 Page 88 also see RAT Output Appendix B - Check Local authentication of Username and passwords	
Risk	System Administration Lack of Security Policy to control Router Activities Configuration Errors
Risk Level	High
Exception	No usernames on the router All ports does have passwords applied
Summary	Username are a level of Security to authenticate anybody to connect to the router. The primary connection ports only require a password to connect. The username not only provides another level of security (i.e. username and password must match) but will also keep a record on who is supposed to have access to the router.

7. Cisco Checklist Item 4 Section 3 Page 113 - Cisco Security Notice: MS SQL Worm Mitigation Recommendations	
--	--

Risk	Router open to Denial of Service Attack
Risk Level	High
Exception	Required fix of applying the Cisco Recommended access list is not in place or code upgrade
Summary	Cisco Advisories are meant to warn their customers of potential risks to Cisco products. This particular advisory warns of a vulnerability that can cause a denial of service attack. The recommended fix is an access list of code upgrade. Neither has been applied to XYZ law's router. This can cause the router to be compromised and rendered useless. This access list can also stop the internal PC's from being affected by the same attack.

8. Cisco Checklist Item 8 Section 3 Page 119 - Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packets	
Risk	Router open to Denial of Service Attack
Risk Level	High
Exception	Required fix of applying the Cisco Recommended access list is not in place or code upgrade
Summary	Cisco Advisories are meant to warn their customers of potential risks to Cisco products. This particular advisory warns of a vulnerability that can cause a denial of service attack. The recommended fix is an access list of code upgrade. Neither has been applied to XYZ law's router. This can cause the router to be compromised and rendered useless. This access list can also stop the internal PC's from being affected by the same attack.

9. General Checklist Item 19 Section 3 Page 105 – Determine if IP Source Routing is enabled	
Risk	Router open to Denial of Service Attack and possible compromise
Risk Level	High
Exception	IP Source routing is enabled
Summary	Cisco routers accept source route requests by default. A popular form of attack would be to use this in conjunction with a spoofed IP. The attacker will spoof an IP and send a source route to the router; the router will then see the attackers host as trusted and forward all packets to the attacker's host. The information gathered can then be used to compromise the router and use it for Denial of Service or as a stepping stone into XYZ Law's internal network.

10. General Checklist Item 20 Section 3 Page 105 – Determine if Proxy Arp is enabled	
Risk	Router open to internet scans Router open to Denial of Service Attack and possible compromise
Risk Level	High
Exception	IP Proxy Arp is enabled
Summary	The following is a excerpt from CIS Level 1 Benchmark 2.1 page 24

	<p>Section 3.2.47</p> <p>“Network hosts use the Address Resolution Protocol (arp) to translate network addresses into media addresses. Normally, ARP transactions are confined to a particular LAN segment. A Cisco Router can act as an intermediary for ARP, responding to ARP queries on selected interfaces and thus enabling transparent access between multiple LAN segments. Because it breaks the LAN security perimeter, effectively extending a LAN at layer 2 across multiple segments, proxy arp should only be used between two LAN segments at the same trust level, and only when absolutely necessary to support legacy network architectures. Cisco routers perform proxy arp by default on all IP interfaces.”</p> <p>This can open XYZ Law open to internet scans and possible denial of service attacks that utilize arp as a weapon.</p>
--	---

11. General Checklist Item 17 Section 3 Page 98 – Determine if bootp is enabled	
Risk	Router open to Denial of Service Attack and possible compromise
Risk Level	Medium
Exception	Bootp is enabled
Summary	Cisco recommends that if bootp is not being used then should be disabled and if enabled can result in a denial of service attack.

12. General Checklist Item 15 Section 3 Page 98 – Determine if the aux port is enabled	
Risk	Router open to Denial of Service Attack and possible compromise
Risk Level	Medium
Exception	Aux port is enabled
Summary	In order for the aux port to be accessed it requires a physical connection such as a modem. The router is secured with limited access.

4.2 Audit Recommendations

The recommendations are based on the specific findings of the audit and the overall outlook of XYZ Law firm. The recommendations will be divided into specific exceptions and more general which are both intended to make XYZ Law's network and internet activities more secure. Each recommendation will be accompanied an estimated cost to implement.

4.2.2 General Recommendations

The following are general recommendations that should help XYZ Law secure their network and operations

1. Security Policy – It is a misconceived belief that only large organizations require a security policy. This is not so. XYZ Law should implement a formal Security Policy aimed at protecting their sensitive assets. This can be accomplished by coordinating with their ISP/Consultant Company to give and take direction. The policy can be simple to easier design and implement. Sample security policies can be found at www.sans.org
 - i. Time to design and implement – 5 business days Approximate
 - ii. Cost to design and implement – this will be based on individual time of XYZ Law personnel but if outsourced average professional services cost is \$125 US an hour or \$1050 US a day. Outsource cost would be \$5250 US
2. Arrange a review with the Consultant firm – The consultant firm who is responsible for the Cisco Router at XYZ Law should be consulted as the results of this audit. The router is not secure and XYZ Law should consult with the firm to determine why.
 - i. Time - One day discussion
 - ii. Cost - should be no cost associated
3. Enable software features on the existing router – Upon investigation of the router it was determined the version of code has the Cisco IOS Feature IOS Firewall. XYZ Law can enable this feature to better protect their perimeter. Some of the enhance features that may be enabled are Context-Based Access Control (the firewall), Authentication Proxy, and limited intrusion detection.
 - i. Time to Design and implement – 1 day
 - ii. Cost to design and implement – One day professional services \$1050

4.2.3 Exception Specific Recommendations

The following are recommendations to fix the existing exceptions that have been reported in this audit. If any or all of the recommendations in the previous section are implemented it may take care of some of the individual exceptions listed here. The time and cost will be associated with each exception.

1. General Check List Item 5 Section 3 Page 75 – Nessus Vulnerability Scan

For Nessus Results see Appendix	
Recommendation	fulfill recommendation 3 in section 4.2.2
Time	1 Business Day
Cost	\$1050 US

2. General Checklist Item 8 Section 3 Page 82 - Test the ACL against the written security policy or against the "Deny All" rule Section 3 page	
Recommendation	Have Access List to filter unwanted traffic applied to interfaces
Time	This will take approximately one day to design against requirements and implement
Cost	\$1050 US

3. General Checklist Item 9 Section 3 Page - Verify the router is egress filtering local network traffic and the outbound capabilities of the router	
Recommendation	Have Access List to filter unwanted traffic applied to egress interface
Time	This will take approximately one day to design against requirements and implement
Cost	\$1050 US

3. General Checklist Item 9 Section 3 Page - Verify the router is egress filtering local network traffic and the outbound capabilities of the router	
Recommendation	Have Access List to filter unwanted traffic applied to egress interface
Time	This will take approximately one day to design against requirements and implement
Cost	\$1050 US

4. General Checklist Item 7 Section 3 page 82 - Determine if Router is configured to provide Network Address Translation (NAT)	
Recommendation	Apply Network address translation to ensure the private network is not broadcasted to the internet
Time	One hour to implement
Cost	\$125 US

5. General Checklist Item 10 Section 3 page 85 - Determine if Router is able to do IP Address Spoof detection	
---	--

Recommendation	fulfill recommendation 3 in section 4.2.2
Time	1 Business day
Cost	\$1050 US
6. General Checklist Item 11 Section 3 Page 88 also see RAT Output Appendix B - Check Local authentication of Username and passwords	
Recommendation	Have usernames and passwords implemented. Determine a list of system admins and have each user ID correlate with each system admin. Each system admin each should have a different password.
Time	1 hour
Cost	\$125 US

7. Cisco Checklist Item 4 Section 3 Page 113 - Cisco Security Notice: MS SQL Worm Mitigation Recommendations	
Recommendation	Implement the Cisco Recommended Access List
Time	1 hour
Cost	\$125 US

8. Cisco Checklist Item 8 Section 3 Page 119 - Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packets	
Recommendation	Implement the Cisco Recommended Access List
Time	1 hour
Cost	\$125 US

9. General Checklist Item 19 Section 3 Page 105 – Determine if IP Source Routing is enabled	
Recommendation	Disable IP Source Routing
Time	5 minutes
Cost	\$125 US (Note charge may still be for an hour or there may be a configuration charge)

10. General Checklist Item 20 Section 3 Page 105 – Determine if Proxy Arp is enabled	
Recommendation	Disable IP proxy Arp
Time	5 minutes
Cost	\$125 US (Note charge may still be for an hour or there may be a configuration charge)

11. General Checklist Item 17 Section 3 Page 98 – Determine if bootp is enabled	
Recommendation	Disable bootp
Time	5 minutes
Cost	\$125 US (Note charge may still be for an hour or there may be a configuration charge)

12. General Checklist Item 15 Section 3 Page 98 – Determine if the aux port is enabled	
Recommendation	Disable the AUX port
Time	5 minutes
Cost	\$125 US (Note charge may still be for an hour or there may be a configuration charge)

4.2.4 Summary

In its current state XYZ Law and its perimeter router is very open to the public internet. The current router can easily be safer guarded with a few configuration additions. The implementation of a security policy will also put in important guidelines to further enhance XYZ Law's network security

5. References

See Section 1.2.3

Appendixes

Appendix A – Nessus Scan Results

Nessus Scan Report	
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.	

Scan Details	
Hosts which were alive and responding during test	1
Number of security holes found	0
Number of security warnings found	4

Host List	
Host(s)	Possible Issue
xxx.xxx.xxx.xxx	Security warning(s) found
[return to top]	

Analysis of Host		
Address of Host	Port/Service	Issue regarding Port
xxx.xxx.xxx.xxx	general/tcp	Security warning(s) found
xxx.xxx.xxx.xxx	telnet (23/tcp)	Security warning(s) found
xxx.xxx.xxx.xxx	telnet (23/udp)	No Information
xxx.xxx.xxx.xxx	general/icmp	Security warning(s) found
xxx.xxx.xxx.xxx	general/udp	Security notes found

Security Issues and Fixes: xxx.xxx.xxx.xxx		
Type	Port	Issue and Fix
Warning	general/tcp	<p>The remote host does not discard TCP SYN packets which have the FIN flag set.</p> <p>Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.</p> <p>See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113</p> <p>Solution : Contact your vendor for a patch</p>

GSNA Practical 3.0

Warning	general/tcp	<p>Risk factor : Medium BID : 7487 Nessus ID : 11618</p> <p>The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.</p> <p>An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are:</p> <ol style="list-style-type: none"> 1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network. 2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines. 3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.
Informational	general/tcp	<p>Solution : Contact your vendor for a patch Risk factor : Low Nessus ID : 10201</p> <p>The remote host is up Nessus ID : 10180</p>
Informational	general/tcp	<p>Nmap found that this host is running Cisco 801/1720 running 12.2.8 Nessus ID : 10336</p>
Informational	general/tcp	<p>The remote host is running CISCO IOS 12.0 Nessus ID : 11936</p>
Warning	telnet (23/tcp)	<p>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.</p> <p>Solution: If you are running a Unix-type system, OpenSSH can be used instead of telnet. For Unix systems, you can comment out the 'telnet' line in /etc/inetd.conf. For Unix systems which use xinetd, you will need to modify the telnet services file in the /etc/xinetd.d folder. After making any changes to xinetd or inetd configuration files, you must restart the service in order</p>

GSNA Practical 3.0

		<p>for the changes to take affect.</p> <p>In addition, many different router and switch manufacturers support SSH as a telnet replacement. You should contact your vendor for a solution which uses an encrypted session.</p> <p>Risk factor : Low CVE : CAN-1999-0619 Nessus ID : 10280</p>
Informational	telnet (23/tcp)	<p>Remote telnet banner :</p> <p>xxxxx Internet IISP You must agree to the following before using this system</p> <p>Use of this system is restricted to authorized employees of Aliant Inc. and authorized contractors.Only authorized work using company-supplied programs may be done on this system.Use of this system is an agreement to monitoring.</p> <p>User Access Verification</p> <p>Password: Nessus ID : 10281</p>
Informational	telnet (23/tcp)	<p>Remote telnet banner :</p> <p>xxxxx Internet IISP You must agree to the following before using this system</p> <p>Use of this system is restricted to authorized employees of Aliant Inc. and authorized contractors.Only authorized work using company-supplied programs may be done on this system.Use of this system is an agreement to monitoring.</p> <p>User Access Verification</p> <p>Password: Nessus ID : 10281</p>
Warning	general/icmp	<p>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.</p> <p>This may help him to defeat all your time based authentication protocols.</p> <p>Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</p> <p>Risk factor : Low CVE : CAN-1999-0524 Nessus ID : 10114</p>
Informational	general/udp	<p>For your information, here is the traceroute to xxx.xxx.xxx.xxx : xxx.xxx.xxx.xxx</p>

GSNA Practical 3.0

?
xxx.xxx.xxx.xxx
Nessus ID : 10287

This file was generated by [Nessus](#), the open-sourced security scanner.

Nessus Scan Report
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which were alive and responding during test	1
Number of security holes found	0
Number of security warnings found	0

Host List	
Host(s)	Possible Issue
142.163.224.22	Security note(s) found
[return to top]	

Analysis of Host		
Address of Host	Port/Service	Issue regarding Port
142.163.224.22	general/tcp	Security notes found
142.163.224.22	finger (79/tcp)	No Information
142.163.224.22	netbios-ssn (139/tcp)	No Information
142.163.224.22	unknown (2702/tcp)	No Information
142.163.224.22	unknown (2701/tcp)	No Information

Security Issues and Fixes: xxx.xxx.xxx.xxx		
Type	Port	Issue and Fix
Informational	general/tcp	The remote host is up Nessus ID : 10180
Informational	general/tcp	Nmap found that this host is running Turtle Beach AudioTron Firmware 3.0, Windows NT4 or 95/98/98SE Nessus ID : 10336

This file was generated by [Nessus](#), the open-sourced security scanner.

Appendix B – Router Auditing Tool (RAT) Results

Router Audit Tool report for
xyzlaw.txt

Audit Date: Tue Feb 17 13:41:05 2004 GMT

Sort Order: importance,passfail,rule,device,instance,line

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.
10	pass	IOS - no ip http server	xyzlaw.txt		
10	pass	IOS - login default	xyzlaw.txt		
10	pass	IOS - forbid SNMP community public	xyzlaw.txt		
10	pass	IOS - forbid SNMP community private	xyzlaw.txt		
10	FAIL	IOS - require line passwords	xyzlaw.txt	aux 0	68
10	FAIL	IOS - no snmp-server	xyzlaw.txt	snmp-server location Con 2 Bay Hwy, Bay Roberts, Newfoundland	
10	FAIL	IOS - no snmp-server	xyzlaw.txt	snmp-server enable traps tty	2
10	FAIL	IOS - no snmp-server	xyzlaw.txt	snmp-server contact Blair 2 Morgan 709-786-9720	
10	FAIL	IOS - enable secret	xyzlaw.txt	tn/a	2
10	FAIL	IOS - apply VTY ACL	xyzlaw.txt	vtty 0 4	69
10	FAIL	IOS - Use local authentication	xyzlaw.txt	tn/a	2
10	FAIL	IOS - Define VTY ACL	xyzlaw.txt	tn/a	2
10	FAIL	IOS - Create local users	xyzlaw.txt	tn/a	2
7	pass	IOS 12 - no udp-small-servers	xyzlaw.txt		
7	pass	IOS 12 - no tcp-small-servers	xyzlaw.txt		
7	pass	IOS 12 - no	xyzlaw.txt		

GSNA Practical 3.0

		<u>directed broadcast</u>		
7	pass	<u>IOS - no service</u>	xyzlaw.txt	
		<u>config</u>		
7	pass	<u>IOS - no cdp run</u>	xyzlaw.txt	
7	pass	<u>IOS - encrypt</u>	xyzlaw.txt	
		<u>passwords</u>		
7	FAIL	<u>IOS - no ip source-</u>	xyzlaw.txt/a	2
		<u>route</u>		
7	FAIL	<u>IOS - exec-timeout</u>	xyzlaw.txtvtty 0 4	0
5	pass	<u>IOS 12.1,2,3 - no</u>	xyzlaw.txt	
		<u>finger service</u>		
5	pass	<u>IOS - forbid clock</u>	xyzlaw.txt	
		<u>summer-time -</u>		
		<u>GMT</u>		
5	pass	<u>IOS - enable</u>	xyzlaw.txt	
		<u>logging</u>		
5	FAIL	<u>IOS - tcp keepalive</u>	xyzlaw.txt/a	2
		<u>service</u>		
5	FAIL	<u>IOS - set syslog</u>	xyzlaw.txt/a	2
		<u>server</u>		
5	FAIL	<u>IOS - service</u>	xyzlaw.txt/a	2
		<u>timestamps logging</u>		
5	FAIL	<u>IOS - service</u>	xyzlaw.txt/a	2
		<u>timestamps debug</u>		
5	FAIL	<u>IOS - ntp server 3</u>	xyzlaw.txt/a	2
5	FAIL	<u>IOS - ntp server 2</u>	xyzlaw.txt/a	2
5	FAIL	<u>IOS - ntp server</u>	xyzlaw.txt/a	2
5	FAIL	<u>IOS - no ip bootp</u>	xyzlaw.txt/a	2
		<u>server</u>		
5	FAIL	<u>IOS - logging</u>	xyzlaw.txt/a	12
		<u>buffered</u>		
5	FAIL	<u>IOS - line password</u>	xyzlaw.txtcon 0	66
		<u>quality</u>		
5	FAIL	<u>IOS - line password</u>	xyzlaw.txtaux 0	68
		<u>quality</u>		
5	FAIL	<u>IOS - VTY</u>	xyzlaw.txtvtty 0 4	69
		<u>transport telnet</u>		
3	pass	<u>IOS - logging trap</u>	xyzlaw.txt	
		<u>info or higher</u>		
3	FAIL	<u>IOS - logging</u>	xyzlaw.txt/a	2
		<u>console critical</u>		
3	FAIL	<u>IOS - disable aux</u>	xyzlaw.txtaux 0	68
3	FAIL	<u>IOS - clock</u>	xyzlaw.txt/a	2
		<u>timezone - GMT</u>		

Summary for xyzlaw.txt

#Checks	#Passed	#Failed	%Passed
40	14	26	35
Perfect Weighted Score	Actual Weighted Score	%Weighted Score	
273	100	36	

Overall Score (0-10)

3.6

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

Fix Script for xyzlaw.txt

```
! The following commands may be entered into the router to fix
! problems found. They must be entered in config mode (IOS). Fixes
! which require specific information (such as uplink interface device
! name) are listed but commented out. Examine them, edit and uncomment.
!
! THESE CHANGES ARE ONLY RECOMMENDATIONS.
!
! CHECK THESE COMMANDS BY HAND BEFORE EXECUTING. THEY MAY BE WRONG.
! THEY MAY BREAK YOUR ROUTER. YOU ASSUME FULL RESPONSIBILITY FOR THE
! APPLICATION OF THESE CHANGES.

! enter configuration mode
configure terminal

! RULE: IOS - require line passwords
!
! This fix is commented out because you have to supply a sensitive
value.
! To apply this rule, uncomment (remove the leading "!" on the commands
below)
! and replace "LINE_PASSWORD" with the value you have chosen.
! Do not use "LINE_PASSWORD".
!
!line aux 0
!password LINE_PASSWORD
!exit

! RULE: IOS - no snmp-server
no snmp-server

! RULE: IOS - no snmp-server
no snmp-server

! RULE: IOS - no snmp-server
no snmp-server

! RULE: IOS - enable secret
```

GSNA Practical 3.0

```
!  
! This fix is commented out because you have to supply a sensitive  
value.  
! To apply this rule, uncomment (remove the leading "!" on the commands  
below)  
! and replace "ENABLE_SECRET" with the value you have chosen.  
! Do not use "ENABLE_SECRET".  
!  
!enable secret ENABLE_SECRET  
  
! RULE: IOS - apply VTY ACL  
line vty 0 4  
access-class 182 in  
exit  
  
! RULE: IOS - Use local authentication  
aaa new-model  
aaa authentication login default local  
aaa authentication enable default enable  
  
! RULE: IOS - Define VTY ACL  
no access-list 182  
access-list 182 permit tcp 192.168.1.0 0.0.0.255 any  
access-list 182 permit tcp host 192.168.1.254 any  
access-list 182 deny ip any any log  
  
! RULE: IOS - Create local users  
!  
! This fix is commented out because you have to supply a sensitive  
value.  
! To apply this rule, uncomment (remove the leading "!" on the commands  
below)  
! and replace "LOCAL_PASSWORD" with the value you have chosen.  
! Do not use "LOCAL_PASSWORD".  
!  
!username username1 password LOCAL_PASSWORD  
  
! RULE: IOS - no ip source-route  
no ip source-route  
  
! RULE: IOS - exec-timeout  
line vty 0 4  
exec-timeout 10 0  
exit  
  
! RULE: IOS - tcp keepalive service  
service tcp-keepalives-in  
  
! RULE: IOS - set syslog server
```

GSNA Practical 3.0

```
logging 13.14.15.16

! RULE: IOS - service timestamps logging
service timestamps log datetime show-timezone msec

! RULE: IOS - service timestamps debug
service timestamps debug datetime show-timezone msec

! RULE: IOS - ntp server 3
ntp server 9.10.11.12

! RULE: IOS - ntp server 2
ntp server 5.6.7.8

! RULE: IOS - ntp server
ntp server 1.2.3.4

! RULE: IOS - no ip bootp server
no ip bootp server

! RULE: IOS - logging buffered
logging buffered 16000

! RULE: IOS - line password quality
!
! This fix is commented out because you have to supply a sensitive
value.
! To apply this rule, uncomment (remove the leading "!" on the commands
below)
! and replace "LINE_PASSWORD" with the value you have chosen.
! Do not use "LINE_PASSWORD". Instead, choose a value that is longer
! than seven characters, and contains upper- and lower-case letters,
! digits, and punctuation.
!
!line con 0
!password LINE_PASSWORD
!exit

! RULE: IOS - line password quality
!
! This fix is commented out because you have to supply a sensitive
value.
! To apply this rule, uncomment (remove the leading "!" on the commands
below)
! and replace "LINE_PASSWORD" with the value you have chosen.
! Do not use "LINE_PASSWORD". Instead, choose a value that is longer
! than seven characters, and contains upper- and lower-case letters,
! digits, and punctuation.
!
!line aux 0
!password LINE_PASSWORD
!exit

! RULE: IOS - VTY transport telnet
line vty 0 4
```

GSNA Practical 3.0

```
!transport input telnet
exit
```

```
! RULE: IOS - logging console critical
logging console critical
```

```
! RULE: IOS - disable aux
line aux 0
no exec
transport input none
exit
```

```
! RULE: IOS - clock timezone - GMT
clock timezone GMT 0
```

```
! Save running configuration so that it will be used each time
! the router is reset/powercycled. Only do this after you are
! SURE everything is correct
!
! copy running-config startup-config
```

Appendix C – Show Tech-support result

```
sho tech
xyzlaw#sho tech-support
```

```
----- show version -----
```

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-BK8NO3R2SY7-M), Version 12.2(15)T9, RELEASE
SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Sat 01-Nov-03 06:24 by ccai
Image text-base: 0x80008120, data-base: 0x81207F5C
```

```
ROM: System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1)
ROM: C1700 Software (C1700-BK8NO3R2SY7-M), Version 12.2(15)T9, RELEASE
SOFTWARE (fc2)
```

```
xyzlaw uptime is 5 days, 16 hours, 55 minutes
System returned to ROM by power-on
System image file is "flash:c1700-bk8no3r2sy7-mz.122-15.T9.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco 1721 (MPC860P) processor (revision 0x100) with 58002K/7534K bytes of memory.

Processor board ID FOC07010MUR (2301023196), with hardware revision 0000
MPC860P processor: part number 5, mask 2

Bridging software.

X.25 software, Version 3.0.0.

1 Ethernet/IEEE 802.3 interface(s)

1 FastEthernet/IEEE 802.3 interface(s)

32K bytes of non-volatile configuration memory.

16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x142

----- show running-config -----

Building configuration...

Current configuration : 1475 bytes

!

version 12.2

service timestamps debug datetime localtime

service timestamps log datetime localtime

service password-encryption

!

hostname xyzlaw

!

logging queue-limit 100

logging buffered 4096 debugging

enable password 7 <removed>

```

!
ip subnet-zero
!
!
ip tftp source-interface Ethernet0
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
!
!
!
!
!
!
interface Ethernet0
description Customer LAN Segment
ip address xxx.xxx.xxx.xxx 255.255.255.248
half-duplex
no cdp enable
!
interface FastEthernet0
description Connection to ISP
ip address xxx.xxx.xxx.xxx 255.255.255.252
speed auto
no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx
no ip http server
no ip http secure-server
!
!
!
access-list 10 permit xxx.xxx.xxx.xxx
no cdp run
!
snmp-server location aaaa,bbbb,bbbb
snmp-server contact xxxxx,xxxx,xxxx,xxxx,xxxxx
snmp-server enable traps tty
banner motd ^C
        xxxxx Internet IISP
        You must agree to the following before using this system

```

Use of this system is restricted to authorized employees of

Aliant Inc. and authorized contractors. Only authorized work using company-supplied programs may be done on this system. Use of this system is an agreement to monitoring.

```
^C
!
line con 0
exec-timeout 0 0
password 7 <removed>
login
line aux 0
line vty 0 4
access-class 10 in
exec-timeout 30 0
password 7 <removed>
login
!
no scheduler allocate
end
```

----- show stacks -----

Minimum process stacks:

```
Free/Size  Name
9252/12000  Init
5448/6000   PostOfficeNet
5444/6000   RADIUS INITCONFIG
9720/12000  Exec
5492/6000   CDP Protocol
10616/12000 Virtual Exec
```

Interrupt level stacks:

```
Level  Called Unused/Size  Name
3      0    9000/9000  PA Management Int Handler
4      1766205 7360/9000  Network interfaces
5      0    9000/9000  Timebase Reference Interrupt
6      25424  8880/9000  16552 Con/Aux Interrupt
7      123237223 8920/9000  MPC860P TIMER INTERRUPT
```

----- show interfaces -----

```
Ethernet0 is up, line protocol is down
Hardware is PQUICC Ethernet, address is 0004.dd0d.280c (bia 0004.dd0d.280c)
Description: Customer LAN Segment
```

Internet address is xxx.xxx.xxx.xxx/29
 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
 reliability 128/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Half-duplex, 10BaseT
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 11:34:31, output 00:00:09, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 112245 packets input, 7222854 bytes, 0 no buffer
 Received 5318 broadcasts, 0 runts, 0 giants, 0 throttles
 4160 input errors, 0 CRC, 0 frame, 0 overrun, 4160 ignored
 0 input packets with dribble condition detected
 136322 packets output, 8168373 bytes, 0 underruns
 4160 output errors, 13960 collisions, 1 interface resets
 0 babbles, 0 late collision, 215 deferred
 4160 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out
 FastEthernet0 is up, line protocol is up
 Hardware is PQUICC_FEC, address is 000b.5f70.ec3a (bia 000b.5f70.ec3a)
 Description: Connection to ISP
 Internet address is xxx.xxx.xxx.xxx/30
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Auto-duplex, 10Mb/s, 100BaseTX/FX
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:07:31, output 00:00:05, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/1588/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 540532 packets input, 39547654 bytes
 Received 1294 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 watchdog
 0 input packets with dribble condition detected
 600315 packets output, 41764749 bytes, 0 underruns

4 output errors, 8250 collisions, 1 interface resets
 0 babbles, 0 late collision, 3220 deferred
 4 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out
 Virtual-Access1 is up, line protocol is up
 Hardware is Virtual Access interface
 MTU 1492 bytes, BW 100000 Kbit, DLY 100000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Base PPPoE vaccess, loopback not set
 DTR is pulsed for 5 seconds on reset
 Last input never, output never, output hang never
 Last clearing of "show interface" counters 5d16h
 Input queue: 0/4096/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runs, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 output buffer failures, 0 output buffers swapped out
 0 carrier transitions

----- show controllers -----

PQUICC Ethernet unit 0 using SCC2, Microcode ver 0
 Current station address 0004.dd0d.280c, default address 8167.0758.81cf
 idb at 0x81DB4CCC, driver data structure at 0x81D9AC68
 SCC Registers:
 General [GSMR]=0x0:0x1088003C, Protocol-specific [PSMR]=0x80A
 Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x0002
 Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0xD555
 Interrupt Registers:
 Config [CICR]=0x00365F80, Pending [CIPR]=0x00000C00
 Mask [CIMR]=0x20200000, In-srv [CISR]=0x00000000
 Command register [CR]=0x640
 Port A [PADIR]=0x0000, [PAPAR]=0x060C
 [PAODR]=0x0000, [PADAT]=0xFDFE
 Port B [PBDIR]=0x0000200F, [PBPAR]=0x0000200E
 [PBODR]=0x00000000, [PBDAT]=0x0003DFFC
 Port C [PCDIR]=0x0000, [PCPAR]=0x0000
 [PCSO]=0x00C0, [PCDAT]=0x0F3E, [PCINT]=0x0000
 wic_enet_regs_ptr->ctrl_reg is 0xBD

SCC GENERAL PARAMETER RAM (at 0xFF003D00)

Rx BD Base [RBASE]=0x2530, Fn Code [RFCR]=0x18

Tx BD Base [TBASE]=0x25B0, Fn Code [TFCR]=0x18

Max Rx Buff Len [MRBLR]=1520

Rx State [RSTATE]=0x18000000, BD Ptr [RBPTR]=0x2558

Tx State [TSTATE]=0x18000AE3, BD Ptr [TBPTR]=0x25C0

SCC ETHERNET PARAMETER RAM (at 0xFF003D30)

CRC Preset [C_PRES]=0xFFFFFFFF, Mask [C_MASK]=0xDEBB20E3

Errors: CRC [CRCEC]=0, Alignment [ALEC]=0, Discards [DISFC]=0

PAD Char [PADS]=0x0

Retry Limit [RET_LIM]=15, Count [RET_CNT]=15

Frame Lengths: [MAXFLR]=1518, [MINFLR]=64

Max DMA Lengths: [MAXD1]=1518, [MAXD2]=1518

Group Address Filter [GADDRn]=0000:0000:0000:0000

Indiv Address Filter [IADDRn]=0000:0000:0000:0000

Physical Address [PADDR1]=0C28.0DDD.0400

Last Address Set in Filter [TADDR]=0000.0000.0000

Persistence [P_Per]=0, Backoff Cnt [BOFF_CNT]=65535

BD Pointers:

First Rx [RFBD]=0x0, First Tx [TFBD]=0x25C0, Last Tx [TLBD]=0x25B8

Software MAC address filter(hash:length/addr/mask/hits):

Receive Ring

rmd(FF002530): status 9000 length 42 address 39E7B44
rmd(FF002538): status 9000 length 42 address 39E67C4
rmd(FF002540): status 9000 length 42 address 39ED644
rmd(FF002548): status 9000 length 42 address 39ECFC4
rmd(FF002550): status 9000 length 42 address 39EC2C4
rmd(FF002558): status 9000 length 72 address 39EE344
rmd(FF002560): status 9000 length F7 address 39EDCC4
rmd(FF002568): status 9000 length 72 address 39E2D44
rmd(FF002570): status 9000 length 72 address 39E74C4
rmd(FF002578): status 9000 length 72 address 39E81C4
rmd(FF002580): status 9000 length 72 address 39E9BC4
rmd(FF002588): status 9000 length 72 address 39E5AC4
rmd(FF002590): status 9000 length 72 address 39E4744
rmd(FF002598): status 9000 length 72 address 39EC944
rmd(FF0025A0): status 9000 length 72 address 39EA244
rmd(FF0025A8): status B000 length 72 address 39EBC44

Transmit Ring

tmd(FF0025B0): status 5C01 length 3C address 39EFD4A
tmd(FF0025B8): status 5C01 length 3C address 39F0ECA
tmd(FF0025C0): status 5C01 length 3C address 39F100A
tmd(FF0025C8): status 5C01 length 3C address 39F038A
tmd(FF0025D0): status 5C01 length 3C address 39F060A

tmd(FF0025D8): status 5C01 length 3C address 39EF70A
 tmd(FF0025E0): status 5C01 length 3C address 38A644A
 tmd(FF0025E8): status 5C01 length 3C address 38A5B8A
 tmd(FF0025F0): status 5C01 length 3C address 38A52CA
 tmd(FF0025F8): status 5C01 length 3C address 38A48CA
 tmd(FF002600): status 5C01 length 3C address 38A61CA
 tmd(FF002608): status 5C01 length 3C address 39F0B0A
 tmd(FF002610): status 5C01 length 3C address 39F128A
 tmd(FF002618): status 5C01 length 3C address 39EFFCA
 tmd(FF002620): status 5C01 length 3C address 38A518A
 tmd(FF002628): status 7C01 length 3C address 39EFACA

4160 missed datagrams, 0 overruns
 0 transmitter underruns, 0 excessive collisions
 5549 single collisions, 8411 multiple collisions
 0 dma memory errors, 0 CRC errors

0 alignment errors, 0 runts, 0 giants
 QUICC SCC specific errors:
 4160 buffer errors, 0 overflow errors
 0 input aborts on late collisions
 0 throttles, 0 enables

Interface FastEthernet0

Hardware is PQUICC MPC860P ADDR: 81CBDBEC, FASTSEND: 8001209C

DIST ROUTE ENABLED: 0

Route Cache Flag: 1

ADDR_LOW =0x000B5F70, ADDR_HIGH =0x0000EC3A, HASH_HIGH
 =0x00000000, HASH_LOW =0x00000000

R_DES_ST =0x039BBF20, X_DES_ST =0x039BC060, R_BUFF_SIZ=0x00000600,
 ECNTRL =0xF0000006

IEVENT =0x00000000, IMASK =0x0A000000, IVEC =0xC0000000,

R_DES_ACT=0x01000000

X_DES_ACT=0x00000000, MII_DATA =0x504A0062, MII_SPEED =0x00000014,
 R_BOUND =0x00000600

R_FSTART =0x00000500, X_FSTART =0x00000440, FUN_CODE =0x7F000000,
 R_CNTRL =0x00000006

R_HASH =0x320005F2

X_CNTRL =0x00000000

HW filtering information:

Promiscuous Mode Disabled

Software MAC address filter(hash:length/addr/mask/hits):

pquicc_fec_instance=0x81CC0024

rx ring entries=32, tx ring entries=32

rxring=0x39BBF20, rxr shadow=0x81CC0230, rx_head=0, rx_tail=0

txring=0x39BC060, txr shadow=0x81CC02DC, tx_head=28, tx_tail=28, tx_count=0

RX_RING_ENTRIES

status 8000, len 500, buf_ptr 39D4060
 status 8000, len 500, buf_ptr 39C0E60
 status 8000, len 500, buf_ptr 39C5AE0
 status 8000, len 500, buf_ptr 39DC640
 status 8000, len 500, buf_ptr 39CBA80
 status 8000, len 500, buf_ptr 39D1A20
 status 8000, len 500, buf_ptr 39C01A0
 status 8000, len 500, buf_ptr 39CB420
 status 8000, len 500, buf_ptr 39C8120
 status 8000, len 40, buf_ptr 39D8CE0
 status 8000, len 55, buf_ptr 39D46C0
 status 8000, len 55, buf_ptr 39C9AA0
 status 8000, len 5D, buf_ptr 39C4E20
 status 8000, len 5D, buf_ptr 39DA660
 status 8000, len 40, buf_ptr 39DCCA0
 status 8000, len 55, buf_ptr 39D00A0
 status 8000, len 40, buf_ptr 39D6D00
 status 8000, len 55, buf_ptr 39D3A00
 status 8000, len 5D, buf_ptr 39DDFC0
 status 8000, len 5D, buf_ptr 39BE1C0
 status 8000, len 40, buf_ptr 39CE720
 status 8000, len 55, buf_ptr 39CD400
 status 8000, len 40, buf_ptr 39BDB60
 status 8000, len 55, buf_ptr 39D2D40
 status 8000, len 5D, buf_ptr 39C67A0
 status 8000, len 5D, buf_ptr 39D66A0
 status 8000, len 40, buf_ptr 39DBFE0
 status 8000, len 55, buf_ptr 39C47C0
 status 8000, len 40, buf_ptr 39BFB40
 status 8000, len 55, buf_ptr 39CED80
 status 8000, len 5D, buf_ptr 39DD300
 status A000, len 5D, buf_ptr 39CADC0

TX_RING_ENTRIES

status 0, len 3C, buf_ptr 38A4F0A
 status 0, len 3C, buf_ptr 38A5E0A
 status 0, len 3C, buf_ptr 39F13CA
 status 0, len 3C, buf_ptr 38A540A
 status 0, len 3C, buf_ptr 39F088A
 status 0, len 3C, buf_ptr 39F04CA
 status 0, len 3C, buf_ptr 39F074A
 status 0, len 3C, buf_ptr 38A4DCA
 status 0, len 3C, buf_ptr 39F024A

```

status 0, len 3C, buf_ptr 38A57CA
status 0, len 3C, buf_ptr 38A5CCA
status 0, len 3C, buf_ptr 39F150A
status 0, len 3C, buf_ptr 38A590A
status 0, len 3C, buf_ptr 39EFC0A
status 0, len 3C, buf_ptr 39EF84A
status 0, len 3C, buf_ptr 38A504A
status 0, len 3C, buf_ptr 39F09CA
status 0, len 3C, buf_ptr 39EF98A
status 0, len 3C, buf_ptr 38A66CA
status 0, len 3C, buf_ptr 39F114A
status 0, len 3C, buf_ptr 38A4B4A
status 0, len 3C, buf_ptr 39F0D8A
status 0, len 3C, buf_ptr 38A658A
status 0, len 3C, buf_ptr 39EFE8A
status 0, len 3C, buf_ptr 38A5F4A
status 0, len 3C, buf_ptr 38A4F0A
status 0, len 3C, buf_ptr 38A5E0A

```

*Mar 6 16:55:59: %PQUICC_ETHER-1-LOSTCARR: Unit 0, lost carrier. Transceiver problem? status 0, len 3C, buf_ptr 39F13CA

```

status 0, len 3C, buf_ptr 39F0D8A
status 0, len 3C, buf_ptr 38A658A
status 0, len 3C, buf_ptr 39EFE8A
status 2000, len 3C, buf_ptr 38A5F4A
throttled=0, enabled=0, disabled=0
rx_framing_err=0, rx_overflow_err=0, rx_buffer_err=0
rx_no_enp=0, rx_discard=0
tx_one_col_err=1954, tx_more_col_err=6296, tx_no_enp=0, tx_deferred_err=3220
tx_underrun_err=0, tx_late_collision_err=0, tx_loss_carrier_err=4
tx_exc_collision_err=0, tx_buff_err=0, fatal_tx_err=0

```

PHY registers:

```

Register 00 1000
Register 01 782D
Register 02 0013
Register 03 78E2
Register 04 01E1
Register 05 0021
Register 06 0004
Register 16 0084
Register 17 0580
Register 18 0062
Register 19 0000
Register 20 4732

```

----- show file systems -----

File Systems:

Size(b)	Free(b)	Type	Flags	Prefixes
29688	26071	nvr	rw	nvr
-	-	opaque	rw	system:
-	-	opaque	rw	null:
-	-	opaque	ro	xmodem:
-	-	opaque	ro	ymodem:
-	-	network	rw	tftp:
* 16515072	6087484	flash	rw	flash:
-	-	network	rw	rcp:
-	-	network	rw	ftp:
-	-	network	rw	scp:

----- dir nvr: -----

Directory of nvr:/

27	-rw-	1471	<no date>	startup-config
28	----	46	<no date>	private-config
1	-rw-	0	<no date>	ifIndex-table
2	----	12	<no date>	persistent-data

29688 bytes total (26071 bytes free)

----- show flash: all -----

Partition	Size	Used	Free	Bank-Size	State	Copy Mode
1	16128K	10183K	5944K	8192K	Read/Write	Direct

System flash directory:

File Length Name/status

addr fcksum ccksum

1	10427524	c1700-bk8no3r2sy7-mz.122-15.T9.bin
	0x40	0x423A 0x423A

[10427588 bytes used, 6087484 available, 16515072 total]

16384K bytes of processor board System flash (Read/Write)

Chip	Bank	Code	Size	Name
------	------	------	------	------

GSNA Practical 3.0

```

1 1 8917 8192KB INTEL 28F640J3
1 2 8917 8192KB INTEL 28F640J3

```

----- show memory statistics -----

```

          Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 81CB14BC 30111812 5165744 24946068 24751860 24201180
I/O 38A4800 7714816 1516532 6198284 6091732 6198236

```

----- show process memory -----

Total: 37826628, Used: 6682184, Free: 31144444

PID	TTY	Allocated	Freed	Holding	Getbufs	Retbufs	Process
0	0	152244	10892	5630680	0	0	*Init*
0	0	504	3914156	504	0	0	*Sched*
0	0	14684920	8830568	65412	163260	0	*Dead*
1	0	0	0	6884	0	0	Chunk Manager
2	0	188	188	3884	0	0	Load Meter
3	0	9523080	9517352	22932	0	0	Exec
4	0	292876	0	13736	0	0	IP SNMP
5	0	0	0	6884	0	0	Check heaps
6	0	599048	123264	25880	470900	589760	Pool Manager
7	0	0	0	6884	0	0	AAA_SERVER_DEADT
8	0	188	188	6884	0	0	Timers
9	0	188	188	6884	0	0	Serial Backgroun
10	0	188	188	6884	0	0	AAA high-capacit
11	0	1228	16936	7236	0	0	ARP Input
12	0	188	188	6884	0	0	DDR Timers
13	0	0	0	6884	0	0	HC Counter Timer
14	0	5812	1016	11680	0	0	Entity MIB API
15	0	188	188	6884	0	0	ATM Idle Timer
16	0	0	0	6884	0	0	SERIAL A'detect
17	0	188	188	6884	0	0	GraphIt
18	0	188	188	12884	0	0	Dialer event
19	0	0	0	6884	0	0	Critical Bkgnd
20	0	20916	0	13148	0	0	Net Background
21	0	188	188	12884	0	0	Logger
22	0	39308	324	7020	0	0	TTY Background
23	0	0	0	9884	0	0	Per-Second Jobs
24	0	0	0	3884	0	0	IPM_C1700_CLOCK
25	0	0	0	6884	0	0	Net Input
26	0	188	188	6884	0	0	Compute load avg
27	0	0	0	6884	0	0	Per-minute Jobs
28	0	188	188	6884	0	0	AAA Server

GSNA Practical 3.0

29	0	0	0	6884	0	0 AAA ACCT Proc
30	0	0	0	6884	0	0 ACCT Periodic Pr
31	0	188	188	6944	0	0 AAA Dictionary R
32	0	803312	245820	13480	181800	54720 IP Input
33	0	0	0	6884	0	0 ICMP event handl
35	0	0	0	12884	0	0 SSS Manager
36	0	0	0	12884	0	0 SSS Test Client
37	0	376	376	12884	0	0 PPP Hooks
38	0	5044	0	11928	0	0 X.25 Encaps Mana
39	0	0	0	12884	0	0 VPDN call manage
40	0	17200	188	23896	0	0 PPPOE discovery
41	0	0	0	6884	0	0 PPPOE background
42	0	188	188	12884	0	0 KRB5 AAA
43	0	188	188	12884	0	0 PPP IP Route
44	0	188	188	12884	0	0 PPP IPCP
45	0	924	1016	10020	0	0 IP Background
46	0	176	0	10060	0	0 IP RIB Update
47	0	0	32076	12884	0	0 TCP Timer
48	0	4307336	135432	12884	0	0 TCP Protocols
49	0	0	0	6884	0	0 RARP Input
50	0	0	0	6884	0	0 Socket Timers
51	0	42784	40920	11748	0	0 HTTP CORE
52	0	32708	2900	22924	0	0 DHCPD Receive
53	0	0	95120	6884	0	0 IP Cache Ager
54	0	0	0	6884	0	0 PAD InCall
55	0	188	188	12884	0	0 X.25 Background
56	0	188	188	6884	0	0 PPP SSS
57	0	188	188	6884	0	0 Adj Manager
58	0	188	188	6944	0	0 PPP Bind
59	0	0	0	6884	0	0 Inspect Timer
60	0	2052	188	8748	0	0 URL filter proc
61	0	0	0	6884	0	0 Authentication P
62	0	0	0	6884	0	0 IDS Timer
63	0	0	0	24884	0	0 COPS
64	0	188	188	6884	0	0 Dialer Forwarder
65	0	0	0	6884	0	0 SNMP Timers
66	0	0	0	6884	0	0 XSM_EVENT_ENGINE
67	0	0	0	12884	0	0 XSM_ENQUEUER
68	0	0	0	12884	0	0 XSM Historian
69	0	188	188	6884	0	0 LOCAL AAA
70	0	188	188	6884	0	0 ENABLE AAA
71	0	188	188	6884	0	0 LINE AAA
72	0	188	188	6884	0	0 TPLUS
73	0	188	188	6884	0	0 CRM_CALL_UPDATE_
74	0	508916	0	12884	0	0 PDU DISPATCHER
75	0	188	188	6884	0	0 Crypto Support

GSNA Practical 3.0

```

76 0      0      0 12884      0      0 Encrypt Proc
77 0      0      0 8884      0      0 Key Proc
78 0 15284    724 23444      0      0 Crypto CA
79 0      0      0 8884      0      0 Crypto SSL
80 0 2936    272 27820      0      0 Crypto ACL
81 0 12432      0 25316      0      0 Crypto Delete Ma
82 0 71468 57804 19664      0      0 Crypto IKMP
83 0 146324 147464 12284      0      0 IPSEC key engine
84 0      0      0 6884      0      0 IPSEC manual key
85 0      0      0 6884      0      0 CRYPTO QoS proce
86 0 188     188 6884      0      0 AAA SEND STOP EV
87 0      0      0 6884      0      0 Syslog Traps
88 0 376     188 7072      0      0 IpSecMibTopN
89 0 1864      0 8748      0      0 SAA Event Proces
90 0      0      0 6884      0      0 VPDN Scal
91 0      0      0 6884      0      0 DHCPD Timer
92 0 188      0 7072      0      0 DHCPD Database
93 0 10520 801416 22928      0      0 SNMP ENGINE
94 0      0      0 12884      0      0 SNMP ConfCopyPro
95 0      0      0 12884      0      0 SNMP Traps
96 0      0      0 6884      0      0 CRYPTO IKMP IPC
    6681264 Total

```

----- show process cpu -----

CPU utilization for five seconds: 0%/0%; one minute: 1%; five minutes: 0%

PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
1	0	1	0	0.00%	0.00%	0.00%	0	Chunk Manager
2	16	98591	0	0.00%	0.00%	0.00%	0	Load Meter
3	26896	4845	5551	0.57%	1.64%	0.71%	0	Exec
4	532	1757	302	0.00%	0.00%	0.00%	0	IP SNMP
5	267012	50624	5274	0.00%	0.04%	0.05%	0	Check heaps
6	76	51	1490	0.00%	0.00%	0.00%	0	Pool Manager
7	0	1	0	0.00%	0.00%	0.00%	0	AAA_SERVER_DEADT
8	0	2	0	0.00%	0.00%	0.00%	0	Timers
9	0	2	0	0.00%	0.00%	0.00%	0	Serial Backgroun
10	0	2	0	0.00%	0.00%	0.00%	0	AAA high-capacit
11	2260	12987	174	0.00%	0.00%	0.00%	0	ARP Input
12	4	2	2000	0.00%	0.00%	0.00%	0	DDR Timers
13	12	24643	0	0.00%	0.00%	0.00%	0	HC Counter Timer
14	0	2	0	0.00%	0.00%	0.00%	0	Entity MIB API
15	0	2	0	0.00%	0.00%	0.00%	0	ATM Idle Timer
16	0	1	0	0.00%	0.00%	0.00%	0	SERIAL A'detect
17	56	492734	0	0.00%	0.00%	0.00%	0	GraphIt
18	0	2	0	0.00%	0.00%	0.00%	0	Dialer event

GSNA Practical 3.0

19	0	1	0	0.00%	0.00%	0.00%	0 Critical Bkgnd
20	7820	76831	101	0.00%	0.00%	0.00%	0 Net Background
21	12	1545	7	0.00%	0.00%	0.00%	0 Logger
22	104	492731	0	0.00%	0.00%	0.00%	0 TTY Background
23	1256	492744	2	0.00%	0.00%	0.00%	0 Per-Second Jobs
24	0	1644	0	0.00%	0.00%	0.00%	0 IPM_C1700_CLOCK
25	0	1	0	0.00%	0.00%	0.00%	0 Net Input
26	12	98592	0	0.00%	0.00%	0.00%	0 Compute load avg
27	229952	8241	27903	0.00%	0.04%	0.00%	0 Per-minute Jobs
28	0	2	0	0.00%	0.00%	0.00%	0 AAA Server
29	0	1	0	0.00%	0.00%	0.00%	0 AAA ACCT Proc
30	0	1	0	0.00%	0.00%	0.00%	0 ACCT Periodic Pr
31	0	2	0	0.00%	0.00%	0.00%	0 AAA Dictionary R
32	276472	235501	1173	0.00%	0.00%	0.00%	0 IP Input
33	0	1	0	0.00%	0.00%	0.00%	0 ICMP event handl
35	0	1	0	0.00%	0.00%	0.00%	0 SSS Manager
36	16	65713	0	0.00%	0.00%	0.00%	0 SSS Test Client
37	4	3	1333	0.00%	0.00%	0.00%	0 PPP Hooks
38	0	1	0	0.00%	0.00%	0.00%	0 X.25 Encaps Mana
39	0	1	0	0.00%	0.00%	0.00%	0 VPDN call manage
40	4	3	1333	0.00%	0.00%	0.00%	0 PPPOE discovery
41	3108	30791837	0	0.00%	0.00%	0.00%	0 PPPOE background
42	0	2	0	0.00%	0.00%	0.00%	0 KRB5 AAA
43	4	2	2000	0.00%	0.00%	0.00%	0 PPP IP Route
44	0	2	0	0.00%	0.00%	0.00%	0 PPP IPCP
45	14016	8241	1700	0.00%	0.00%	0.00%	0 IP Background
46	32	8208	3	0.00%	0.00%	0.00%	0 IP RIB Update
47	28	638	43	0.00%	0.00%	0.00%	0 TCP Timer
48	884	618	1430	0.00%	0.00%	0.00%	0 TCP Protocols
49	0	1	0	0.00%	0.00%	0.00%	0 RARP Input
50	0	1	0	0.00%	0.00%	0.00%	0 Socket Timers
51	44	37	1189	0.00%	0.00%	0.00%	0 HTTP CORE
52	8	16	500	0.00%	0.00%	0.00%	0 DHCPD Receive
53	528	8213	64	0.00%	0.00%	0.00%	0 IP Cache Ager
54	0	1	0	0.00%	0.00%	0.00%	0 PAD InCall
55	0	2	0	0.00%	0.00%	0.00%	0 X.25 Background
56	0	2	0	0.00%	0.00%	0.00%	0 PPP SSS
57	1056	8216	128	0.00%	0.00%	0.00%	0 Adj Manager
58	0	2	0	0.00%	0.00%	0.00%	0 PPP Bind
59	0	1	0	0.00%	0.00%	0.00%	0 Inspect Timer
60	0	2	0	0.00%	0.00%	0.00%	0 URL filter proc
61	0	1644	0	0.00%	0.00%	0.00%	0 Authentication P
62	0	1	0	0.00%	0.00%	0.00%	0 IDS Timer
63	0	1	0	0.00%	0.00%	0.00%	0 COPS
64	0	2	0	0.00%	0.00%	0.00%	0 Dialer Forwarder
65	0	1	0	0.00%	0.00%	0.00%	0 SNMP Timers

GSNA Practical 3.0

```

66      0      1      0 0.00% 0.00% 0.00% 0 XSM_EVENT_ENGINE
67     12    49274      0 0.00% 0.00% 0.00% 0 XSM_ENQUEUER
68     32    49274      0 0.00% 0.00% 0.00% 0 XSM_Historian
69      0      2      0 0.00% 0.00% 0.00% 0 LOCAL AAA
70      0      2      0 0.00% 0.00% 0.00% 0 ENABLE AAA
71      0      2      0 0.00% 0.00% 0.00% 0 LINE AAA
72      0      2      0 0.00% 0.00% 0.00% 0 TPLUS
73      0   16434      0 0.00% 0.00% 0.00% 0 CRM_CALL_UPDATE_
74     660   1757    375 0.00% 0.00% 0.00% 0 PDU_DISPATCHER
75      0      2      0 0.00% 0.00% 0.00% 0 Crypto Support
76      0      1      0 0.00% 0.00% 0.00% 0 Encrypt Proc
77      4      1   4000 0.00% 0.00% 0.00% 0 Key Proc
78      0      4      0 0.00% 0.00% 0.00% 0 Crypto CA
79      0      1      0 0.00% 0.00% 0.00% 0 Crypto SSL
80      0      3      0 0.00% 0.00% 0.00% 0 Crypto ACL
81      0     16      0 0.00% 0.00% 0.00% 0 Crypto Delete Ma
82     220   33162      6 0.00% 0.00% 0.00% 0 Crypto IKMP
83    1172   24649     47 0.00% 0.00% 0.00% 0 IPSEC key engine
84      0      1      0 0.00% 0.00% 0.00% 0 IPSEC manual key
85      0      1      0 0.00% 0.00% 0.00% 0 CRYPTO QoS proce
86      0      2      0 0.00% 0.00% 0.00% 0 AAA SEND STOP EV
87      0      1      0 0.00% 0.00% 0.00% 0 Syslog Traps
88      4      2   2000 0.00% 0.00% 0.00% 0 IpSecMibTopN
89    1976 123101467      0 0.00% 0.00% 0.00% 0 SAA Event Proces
90      0      1      0 0.00% 0.00% 0.00% 0 VPDN Scal
91      0   4108      0 0.00% 0.00% 0.00% 0 DHCPD Timer
92    2568  139606     18 0.00% 0.00% 0.00% 0 DHCPD Database
93     744   1757    423 0.00% 0.00% 0.00% 0 SNMP ENGINE
94      0      1      0 0.00% 0.00% 0.00% 0 SNMP ConfCopyPro
95      0      1      0 0.00% 0.00% 0.00% 0 SNMP Traps
96      0     43      0 0.00% 0.00% 0.00% 0 CRYPTO IKMP IPC

```

----- show process cpu history -----

```

          11111
1111111  66666  111111111122222
100
90
80
70
60
50
40
30
20

```

GSNA Practical 3.0

```

10      *****      *****
0....5....1....1....2....2....3....3....4....4....5....5....
      0  5  0  5  0  5  0  5  0  5  0  5
      CPU% per second (last 60 seconds)
  
```

```

1 1
161                                1
100
90
80
70
60
50
40
30
20
10 ***
0....5....1....1....2....2....3....3....4....4....5....5....
      0  5  0  5  0  5  0  5  0  5  0  5
      CPU% per minute (last 60 minutes)
      * = maximum CPU%  # = average CPU%
  
```

```

                                2    2    599    5999
111 1  111911 1 1 118111 11 1 111  1 85 11 99121 1 187  13387
100                                **    **
90                                **    ***
80                                **    ***
70                                **    ***
60                                **    ***
50                                ***    *****
40                                ***    *****
30                                *    ***    *****
20                                *    *    ***    *****
10                                *    *    **    *    *    *    *    *
0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
      0  5  0  5  0  5  0  5  0  5  0  5  0  5  0  5  0
      CPU% per hour (last 72 hours)
      * = maximum CPU%  # = average CPU%
  
```

----- show context -----

No valid exception information to display.

----- show diag -----

Slot 0:

C1721 1FE Mainboard Port adapter, 2 ports

Port adapter is analyzed

Port adapter insertion time unknown

EEPROM contents at hardware discovery:

Hardware Revision : 1.0

PCB Serial Number : FOC07010MUR

Part Number : 73-7546-01

Board Revision : A0

Fab Version : 04

Product Number : CISCO1721

EEPROM format version 4

EEPROM contents (hex):

0x00: 04 FF 40 03 5A 41 01 00 C1 8B 46 4F 43 30 37 30

0x10: 31 30 4D 55 52 82 49 1D 7A 01 42 41 30 02 04 FF

0x20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

WIC Slot 1:

Ethernet 10bT WAN daughter card-Version 4 TLV Cookie Format

Hardware Revision : 3.0

Part Number : 73-5797-03

Board Revision : A0

Deviation Number : 0-0

Fab Version : 02

PCB Serial Number : FOC06520B0E

RMA Test History : 00

RMA Number : 0-0-0-0

RMA History : 00

Top Assy. Part Number : 800-09311-03

Connector Type : 01

Chassis MAC Address : 0004.dd0d.280c

MAC Address block size : 1

Product Number : WIC-1ENET=

----- show c1700 -----

C1700 Platform Information:

Interrupts:

Assigned Handlers...

Vect Handler # of Ints Name

01 80214ED4 07589A24 MPC860P TIMER INTERRUPT
 02 802844A0 00006BD4 16552 Con/Aux Interrupt
 03 80281B9C 00000000 Timebase Reference Interrupt
 04 8028FC18 00000005 WIC Network IO Int & pquicc fec speed/dup INT handler
 05 8028FC60 000ACE47 MPC860P CPM INTERRUPT
 13 800138E4 001024FA pquicc fec interrupt

IOS Priority Masks...

Level 00 = [7C040000]
 Level 01 = [7C040000]
 Level 02 = [7C040000]
 Level 03 = [7C040000]
 Level 04 = [70000000]
 Level 05 = [60000000]
 Level 06 = [40000000]
 Level 07 = [00000000]

SIU_IRQ_MASK = FFFFFFFF SIEN = 7C04xxxx Current Level = 00

Spurious IRQs = 00000000 SIPEND = 0000xxxx

Interrupt Throttling:

Throttle Count = 00000000 Timer Count = 00000000
 Netint usec = 00000000 Netint Mask usec = 000003E8
 Active = 0 Configured = 0
 Longest IRQ = 00000000

IDMA Status:

Requests = 00462777 Drops = 00001588
 Complete = 00461189 Post Coalesce Frames = 00461189
 Giant = 00000000
 Available Blocks = 256/256

----- show controllers t1 -----

----- show controllers e1 -----

----- show controllers j1 -----

----- show region -----

Region Manager:

Start	End	Size(b)	Class	Media	Name
0x038A4800	0x03FFFFFF	7714816	Iomem	R/W	iomem
0x60000000	0x60FFFFFF	16777216	Flash	R/O	flash
0x80000000	0x838A47FF	59394048	Local	R/W	main
0x80008120	0x81207F5B	18873916	IText	R/O	main:text
0x81207F5C	0x81A17873	8452376	IData	R/W	main:data
0x8166B2A8	0x81697547	180896	Local	R/W	data:ADSL firmware
0x8197F328	0x81A17587	623200	Local	R/W	data:firmware
0x81A17874	0x81CB14BB	2726984	IBss	R/W	main:bss
0x81CB14BC	0x838A47FF	29307716	Local	R/W	main:heap

----- show buffers -----

Buffer elements:

500 in free list (500 max allowed)
1098834 hits, 0 misses, 0 created

Public buffer pools:

Small buffers, 104 bytes (total 50, permanent 50, peak 98 @ 3d00h):

50 in free list (20 min, 150 max allowed)
970535 hits, 89 misses, 133 trims, 133 created
0 failures (0 no memory)

Middle buffers, 600 bytes (total 25, permanent 25):

25 in free list (10 min, 150 max allowed)
4806 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

Big buffers, 1536 bytes (total 50, permanent 50):

50 in free list (5 min, 150 max allowed)
5897 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

VeryBig buffers, 4520 bytes (total 10, permanent 10):

10 in free list (0 min, 100 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

Large buffers, 5024 bytes (total 0, permanent 0):

- 0 in free list (0 min, 10 max allowed)
- 0 hits, 0 misses, 0 trims, 0 created
- 0 failures (0 no memory)

Huge buffers, 18024 bytes (total 1, permanent 0, peak 6 @ 2d23h):

- 1 in free list (0 min, 4 max allowed)
- 26125 hits, 5 misses, 33 trims, 34 created
- 0 failures (0 no memory)

Header pools:

Header buffers, 0 bytes (total 137, permanent 128, peak 137 @ 5d16h):

- 9 in free list (10 min, 512 max allowed)
- 125 hits, 3 misses, 0 trims, 9 created
- 0 failures (0 no memory)
- 128 max cache size, 128 in cache
- 494 hits in cache, 0 misses in cache

Particle Clones:

- 1024 clones, 0 hits, 0 misses

Public particle pools:

F/S buffers, 256 bytes (total 384, permanent 384):

- 128 in free list (128 min, 1024 max allowed)
- 256 hits, 0 misses, 0 trims, 0 created
- 0 failures (0 no memory)
- 256 max cache size, 256 in cache
- 0 hits in cache, 0 misses in cache

Normal buffers, 1548 bytes (total 512, permanent 512):

- 384 in free list (128 min, 1024 max allowed)
- 370 hits, 0 misses, 0 trims, 0 created
- 0 failures (0 no memory)
- 128 max cache size, 128 in cache
- 0 hits in cache, 0 misses in cache

Private particle pools:

FastEthernet0 buffers, 1536 bytes (total 96, permanent 96):

- 0 in free list (0 min, 96 max allowed)
- 96 hits, 0 fallbacks
- 96 max cache size, 64 in cache
- 542120 hits in cache, 0 misses in cache

Ethernet0 buffers, 1548 bytes (total 32, permanent 32):

- 0 in free list (0 min, 32 max allowed)
- 32 hits, 0 fallbacks
- 32 max cache size, 16 in cache
- 112051 hits in cache, 194 misses in cache

----- show crypto ipsec client ezvpn -----

Easy VPN Remote Phase: 2

----- show ip nat statistics -----

----- show ip nat translations -----

----- show crypto map -----

No crypto maps found.

----- show access-list -----

Standard IP access list 10

10 permit xxx.xxx.xxx.xxx (715 matches)

----- show crypto isakmp policy -----

Default protection suite

encryption algorithm: DES - Data Encryption Standard (56 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Rivest-Shamir-Adleman Signature

Diffie-Hellman group: #1 (768 bit)

lifetime: 86400 seconds, no volume limit

----- show crypto ipsec transform -----

----- show crypto ipsec profile -----

----- show crypto isakmp sa -----

dst	src	state	conn-id	slot
-----	-----	-------	---------	------

----- show crypto engine connection active -----

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
----	-----------	------------	-------	-----------	---------	---------

----- show crypto ipsec sa -----

No SAs found

xyzlaw#