Global Information Assurance Certification Paper

Are You Ready For A Network Audit?
GIAC Security Essentials (GSEC)
Practical Assignment, Version 1.4b, Option 1
April 3, 2003
George Llano

Abstract

There's much to be said about the saying "penny wise, pound foolish". Planning now for the day when an Auditor calls for an appointment will allow you to provide much needed facts in a timely manner and avoid the suspicion of the delayed response. Organizing all of the material and properly reviewing the content for errors give you a firm sense of where you are and perhaps where you should be. The objective of this document is to bring out some flaws in the methodology we use to respond to the audit process. This document will also suggest what to review and what to document for the inevitable audit. Some suggestions on what not to do and what can cause some unnecessary tension to the audit progression. While this document does not imply that the network should be run to pass an audit, taking all the suggested steps described in the document can place you in ready state should the audit event take place. This document will focus on Firewalls, Routers, Switches, Change control, Call Management and Remote Connectivity.

Understanding what is being audited

A network audit will target various parts of the network, some of these areas are the network routers, core switches, the firewalls, network services like DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name Service), Relay Hosts, remote connectivity, network and host based IDS(intrusion detection systems). It's also not uncommon to have trouble tickets, change control, patches and service packs reviewed as well. The document will not cover all the areas of an audit but will cover firewalls, routers, switches, change control, remote connectivity and trouble ticketing system. Not all audits are consistent and the auditor may want to understand process rather than drilling through documentation. The auditor doesn't know your network so he or she must make some assessment based on the material you provide. The auditor may interview your staff for roles and responsibility or ask for job descriptions and org charts. The auditor may want to install software on a server to collect data or may even want to do some penetration test. Regardless of what's asked you need to understand what you're providing and how this will impact the audit. Providing the auditor with incorrect information can lead the audit towards an incorrect assessment. Here are some suggestions that can help in the exchange of information between you the support person and the auditor.

- Create a folder in email that stores all emails surrounding the audit.
- At the close of each business day review all emails to make sure all requests for information have been properly answered.

- Create a task list of all deliverables and when the deliverable was handled over to the auditor.
- Make sure all documentation has proper identification (title page, revision number and date) so if the need to clarify something over the phone becomes a requirement you are both reading off the correct document.
- Make sure that you provide what is asked. Nothing causes more tension than having an auditor review a log for a firewall that is not even active.
- When providing network diagrams make sure the content is up to date. Another tension point is spending time talking about a segment or physical location that no longer exists.
- Properly executed contracts may be requested, make sure you always have a copy handy.
- Copies of Customer Alerts for network outages may also be requested. Email is a great place to store some previously sent email alerts.
- Most important, make sure you have a good technical backup in case you're out sick or need to be out on vacation. This technical backup is someone who "clearly" understands what needs to be handed over to the auditor.

Understanding Your Infrastructure

Before moving in any direction it's important to understand where you currently are with your environment. Almost everyone in a support role feels their network is in great shape. Some IT support engineers may feel strongly that the network is fine and does not require any changes. Some IT support engineers may also feel that network uptime is where the focus should be. Keeping the users logged in; keeping internet access available, making sure email is moving is enough for most IT support engineers. It's not uncommon to hear IT support engineers say" hey we haven't been hacked yet we must be doing something right". It should be relatively easy to look at the network and say "what could break that would cause a major outage?", "what in my network has no backup?" Auditors obviously want to understand process but want to make sure the network is available. They want to know what safeguards are in place to keep the company using its valuable information resources.

The next sections will document some areas of concern for you to focus on. Documenting and understanding these concerns will also help you develop a remediation process. It can also increase efficiency in troubleshooting the network. When addressing your staff about the network evaluation, it's important to make them aware of what the goals are in the initial self assessment. Employees want to be in involved in the collection and remediation process. Once you have an initial plan you can delegate tasks accordingly.

Ticketing System

One of the areas most likely to be problematic is the way you address your trouble tickets. Some key questions you need to ask yourself.

- When opening a ticket is the proper identification of the problem, the user calling, the business unit involved, time and date properly filled in?
- If you went back to the ticket would you clearly understand the problem that prompted this ticket to be opened in the first place?
- What about closure of an open ticket?
- If you went back to the ticket would you clearly understand the steps taken to properly bring closure to the trouble ticket?
- Can changes to the network be directly matched to a closed ticket?
- Are you monitoring aging reports for tickets not closed in the designated SLA period?
- Are you making additional entries in the trouble ticket showing progress for tickets exceeding the SLA period?
- Does everyone in your staff open and close tickets reasonably the same?
- What reports do you get daily, weekly and monthly on problem tickets?
- Are you archiving those reports in case you need to provide them in a reasonable period of time?

There are many non audit related benefits of having an accurate ticketing system. The trouble ticket database can be used for future problem resolution. The trouble ticketing system can even be used to justify capital or operating expenses. The trouble ticketing system can provide the auditor with great reports on the progress you've made in reducing repeat incidents, increasing efficiency and access to the network. Do not overlook this important area of your network.

Change Control

Communication is another area we as support individuals tend to do poorly. There isn't anything that causes more problems than a planned outage that no one knows anything about. I've seen many IT Supported engineers severely reprimanded for bringing down the network without endorsement from application development and /or the user community. Worse yet, having the only person who knows anything about the outage take the next day off may add unnecessary delay to the resolution of the problem. If you don't have any documented change control try to develop a form as quickly as possible. Here are some suggestions:

- First document what does and doesn't need change control. Changing a user port duplex setting has less impact that an uplink on a core switch.
- Make sure that the change control document clearly states what is being changed and why.
- Make sure there is ample notice to the technology populous first prior to sending an email out to the user community. You need the

endorsement of all those working on critical technical projects if the network is going to be unavailable.

- Make sure you have a good template for sending out network outage notification to the user populous. You don't want to say a network outage will occur yesterday.
- Make sure you also forward any network outage notification to external groups that rely on access to your network but are not on your email system.
- Make sure you have the proper staff ready to implement the back out plan should things not go as planned.
- Make sure there is a trouble ticket opened with the proposed changes
- Make sure that the trouble ticket shows properly documented closure should the project go as planned or backed out of.
- Is there a backup person ready to step in should the primary become ill or call in sick?
- Try to document a brief post mortem on the changes and its successful implementation.

Combining the number of planned outages into one big outage is a risky move. Sometimes combining too many changes can be difficult to back out of or troubleshoot. Doing the changes on a Saturday, Sunday or holiday can have skewed results. Many IT support engineers conclude that the network changes completed over the weekend were a success without testing the changes under normal conditions. When Monday morning arrives and the user population logs in, the IT engineer is faced with the reality; the proposed changes were a failure. Backing out of the changes at that point can have significant impact to the user community. This area must be given proper attention for its high visibility in the audit process. In appendix A there is a sample Change Control document I developed and is used with success at the company I work for. With Microsoft Exchange you can create a form from this document and save the completed form in a public folder on the Exchange server. Bring this form up each time the need for a change is required. Since the change control forms are now being stored on a public folder, an auditor can be given access to review any of the change control forms.

Firewalls

One of the most common areas to get audited is the Firewall Infrastructure inclusive of the firewall rule base and / or the firewall logs. Most auditors will say that the only thing worse than not having a firewall is having one poorly configured. It's critical to maintain a stable and optimal Firewall infrastructure regardless of an audit. Below are some considerations when assessing how well your firewalls are being managed.

- A properly documented rule base will have comments for every rule created. Properly documented comments allow you to know why the rule is there to begin with should troubleshooting the rule base be required.

- Make sure you're not using a generic out of the box rule base.
- A properly created rule will also have a change control reference.
- A properly created rule if requested by a trouble ticket will also make reference to the trouble ticket number in the comments field.
- When removing a rule having proper documentation in the comments field will help you identify what business will be impacted by this change.
- Make sure the Firewall has the latest working patches.
- If you're not using an appliance type Firewall like a Nokia, make sure the server operating system is properly patched as well.
- Make sure you've run some port scanning utility like NMAP to identify any ports open that shouldn't be.
- It's in your best interest to block any P2P ports outbound and blocking access to the websites that are known to sponsor P2P as well.
- Make sure there is a limited access to the firewall console. This limits the number of support engineers who can make a rule change.
- Make sure the Firewall logs are being archived as well.

The last bullet is a very important one. You need to be able to go back to the rule base should an investigation or incident require it. You should also have the ability to show the auditor that the firewall logs are being reviewed at the very least weekly. Unless you have a network and host based IDS infrastructure, not reviewing the firewall logs leave you in a vulnerable position. Create an ongoing periodic rule base review date, perhaps quarterly and make sure that it's properly documented. The Auditor may ask you to review the rule base with them. You should be able to talk about each rule and its purpose. Here are some additional suggestions:

- When the auditor sends their suggested modifications to the exisiting rule base make sure the copy of the revised rule base you're sending back does in fact have the changes.
- When sending back a revised rule base with new additional rules be ready to answer questions surrounding these new entries to the rule base.
- Make sure you have the proper trouble tickets and / or change control associated with the new additional rules.
- It's always best to inform the auditor of the new rules, instead of the auditor finding out on his or her own.

Routers

Routers are always an important consideration for an audit. Routers are the backbone of connectivity and any liability to the core routers could affect the day-to-day operations of any company. This section assumes you have a Cisco environment but many of the suggestions could easily be used in non Cisco environment. Some of the following suggestions might sound obvious but you'd be surprise how many support persons don't adhere to simple maintenance procedures.

- Don't fall behind on the IOS; if you are significantly behind current operating IOS suggested by the manufacturer the auditors may question proper maintenance on the device.
- Test the proposed IOS upgrade as extensively as possible with q documented test criteria. When asked you can at least show the companies requirements are being met with the new code.
- You should have a TFTP server that holds the most current running config in the event of a router failure that requires a total replacement of the router.
- Make sure there are a limited number of support persons with privileged access.
- Make sure that your router config is free from running unnecessary services. Many support persons take a generic router config and tailor it to their needs but seldom remove any superfluous entries.
- Make sure the routers have protected physical access.
- Use SSH over Telnet.
- Use TACACS+ authentication services as an added layer of access security.
- Forward logging to a NETSYS server for weekly review.
- If possible implement CISCO 2000; CISCO 2000 is a great network management tool.
- Make sure any unused ports are shutdown
- Make sure there are proper change control entries for any changes to the running config.
- Make sure there is proper customer notification for any planned outages.
- Limit the use of Cisco Discovery Protocol.
- Treat your SNMP community strings like router passwords
- It would be in your best interest to have a router standard. These router standards could be as follows:
    - Regional Router with no local support person, associated security, model type, memory, services, required slot cards and location of latest standard "Regional" config.
    - Core Router, associated security, model type, memory, services, required slot cards and location of latest standard "Core" config
    - Internet router, associated security, model type, memory, services, required slot cards and location of latest standard "internet" config.

Cisco 2000 is an excellent tool that not only has the potential to reduce the administrative overhead involved in maintaining the routers, it also has a lengthy number of reports that can provide any auditor with an abundance of required information. Having these canned reports saves a great deal of time. A support engineer could easily spend hour's maybe days accessing all the network devices for the appropriate information.

Some auditors may want to review the router config; you must be able to properly justify all the lines in the running config. The auditors may offer some

suggested changes; you should send back the config with the proper changes along with the original and the highlighted changes.

Switches

Switches are not a common point of interest in many network audits. Since a support engineer never knows what's going to be asked for in a network audit it pays to make sure all areas and levels of your network have proper controls and standards. It's important to focus on key areas that are likely to be part of the audit process. Any kind of logging is always of great importance to any auditor. Although Syslog is Cisco's proprietary logging feature, it's the first step in identifying the problem and its first occurrence. Configuring NTP with a proper time source will ensure that time stamps are concise and in synch with other devices on the network. Once NTP is properly implemented it takes less time to correlate an event when reviewing multiple logs.

Cisco Discovery Protocol (CDP) is a setting auditors look for in any Cisco environment. CDP is exceptionally informative at determining network topology and physical configuration. Having CDP enabled can be a security risk.

Additional settings that are commonly looked at are the auto-negotiation on Fast Ethernet ports and the spanning tree switch configurations. Auto negotiation settings are rather simple, you either have auto-negotiating enabled or have a fixed speed and duplex setting. In many cases poor performance has been linked to improper setting synchronization between the switched port and the customer Ethernet card. Proper spanning tree settings allow you to maintain a loop-free switched environment when using redundant switches and bridged networks.

It's not unusual to have all ports configured and patched on a corporate switch even if the port is not in use. This obviously reduces the number of trouble tickets for moves, adds and changes. It's also not uncommon to see support individuals with their own little mini switch under their desk. Although all of these tasks or procedures lend themselves to ease of use or reduce trouble tickets, they can pose a security risk. Providing support individuals with additional network ports can alleviate this situation.

The following suggestions are geared to correct those often overlooked areas that auditors look at in a switched environment:

- Auto-negotiation actually works well between Cisco devices, the auto-negotiate problems occur mostly with desktop network cards. Hardcode the port settings on the switch as a standard and the desktop technicians will never have to guess what the switch is set at thus minimizing any configuration related performance issues with the customer.
- CDP comes enabled by default on any new Cisco device. To disable CDP use the set cdp disable command.

- All Cisco switches have spanning tree enabled. Remember this default setting is there to protect the network from layer 2 loops.
- Don't fall behind on the IOS, falling too far behind may cause the auditors to question proper maintenance on the device.
- Test the proposed upgrade IOS code as extensively as possible with documented test criteria.
- You should have a TFTP server that holds the most current config in the event of a switch failure that requires a total replacement.
- Limit the number of support personnel that have access to the network switched.
- Implement a syslog server, this will provide a central depository for all your Cisco event logs. In the event a switch does not recover a reboot you can review the last events of the failure and potentially avoid reconfiguring the switch the same way.
- Make sure you have a UPS attached to the switch. For Cisco switches with dual power supplies have one power cord in the UPS the other connected to the outlet. If the UPS has a hardware failure the second power connection keeps the switch functioning.
- Use SSH over Telnet.
- Make sure you can justify every line item on the switch config.

Again, some auditors may want to review the switch config, you must be able to properly justify all the lines in the config. If the auditors offer some suggested changes, you should send back the config with the proper changes along with the original and the highlighted changes.

Remote Connectivity

Ubiquitous computing, that's the buzzword for the new millennium. Employees want access to their files and corporate applications wherever they are. More and more employees are shifting away from the traditional dialup connection to the high speed broadband service. As this transition continues overlooking parts of your remote connectivity infrastructure could be flagged by an audit. Some large organizations have a support team that addresses only remote connectivity and all their associated issues. Here are some questions to consider whether you're transitioning to a broadband VPN infrastructure or staying on the traditional dialup.

- Is there someone reviewing the logs of your remote connectivity device(s)?
- Is there two factor authentications for dialup or VPN users?
- Is this remote connectivity infrastructure also used as a disaster recovery solution? If so is there a backup plan should the infrastructure not be available?
- Do you have process for deleting the ID's that are no longer in use for remote connectivity?
- Is there a limited number of administrators able to access your remote access node?

- Is there a scheduled daily, weekly, monthly test of the remote connectivity infrastructure and its efficiency?
- Is the server / service used for two factor authentication physically secure?
- Is the server / service used for two factor authentication properly patched?
- Do vendors have access to the company network via remote connectivity? If so is there a process that protects the company from this privilege?
- Is there a validation process for resetting password lockouts?
- Is there inactivity timeout.

Conclusion

It's important to document any out of compliance issues up front. You should list any applications with special port requirements. The auditor should also be made aware of the business decision and acceptable risks surrounding the ports in use for the application. The auditor may disagree with the decision but they wouldn't think you didn't understand what you were doing. It's always good to document management's awareness of the risks being taken as well.

Using the guidelines described can certainly put you in a better position for the audit. As you go along you will identify more areas that require maintenance and adjust accordingly. Let's review what has been discussed in the document.

You may not be given an opportunity to know ahead of time as to what is going to be audited. Even if you were, you could not realistically correct any issues prior to the audit. You as a support individual need to ask yourself the following:

"What have I been putting off for weeks or months that I should have done already?" "Is that maintenance, upgrade or patch critical to the company?"

"Would there be significant impact if it were disclosed that the maintenance upgrades or patches have not been completed?"

Even worse does your boss think or convey to his management that the maintenance upgrades or patches have been completed?

Each day that goes by is one day less you have to fix an issue. If it's a network audit rest assured the firewall, router and remote connectivity will be targeted. Remember to review all the material you are providing to the auditor. No sense in providing outdated material unless you have no other material. Make sure there is always a backup for yourself or the employee you've delegated to liaise with the auditor. Make sure all the material has proper heading and dates.

Some companies gauge their support teams by the ticket closure counts. Some outsourced companies get penalized for tickets open past their SLA

mark. It only takes an extra minute or two to properly enter a ticket. If you get the problem ticket improperly filled out edit the document if possible and make the proper corrections, call the person who originally opened the ticket for clarification if necessary. If you don't edit the ticket right there and then more than likely the ticket will not get properly closed out. Make sure that any changes are reflected with a problem ticket. Even if you abandon the changes, close out the ticket with detail. Make sure you are viewing the aging reports for open problem tickets, auditors are definitely going to question why problem tickets are open for so long or way past the SLA especially for outsourced vendors. Make your staff consistent in the way they open and close their problem tickets.

Change Control is a highly overlooked area in most companies. Support engineers have a tendency to be spontaneous when it comes to network changes. The network outage should not be as a result of an engineer tweaking a network device. Use the attached form in the appendix or create your own either way make it a point to have a form of some kind. Proper notification to your support peers goes along way. Internal application development may have consultants working on a project or a critical process may be occurring. If the support engineer is the only person aware of the planned outage loss of valuable company information could be as risk. Make an effort to properly archive the change controls in the event they are requested by the auditor.

One of the quickest things to do is to print out the Firewall rule base and review it. At the very least filling in the comments field so that each rule can have some identity can be a great troubleshooting tool. Explaining the rule base to an auditor also becomes easier as well. Many companies have a limited window for downtime and may not have a lab to test a firewall. One suggestion might be to place another firewall parallel to the existing production firewall. The test firewall will have all the new code upgrades and patches. Forward all traffic out through the new firewall. Now you can test appropriately, if issues come up with connectivity, in a few minutes you can switch back to the original firewall.

Make sure you have archived your firewall logs and have reviewed them. If there is any suspect activity you can address it quickly or document the investigation in progress. It's also important to make sure ports that provide P2P access is denied, below is a list of ports for the most common P2P applications.

1214	Kazaa, Morpheus
5025	Aimster
6667	Gnotella
6699	Winmx, Napster (old)
8080	Gnutella
8875	Napster
8876	Napster
8888	Napster
9000	Audio Galaxy
6345 thru 6349	Bearshare, Xolox, Limewire, Knutella

4661, 4662 and 4665	EDonkey

Cisco has a great security manual called SAFE. CiscoSafe
The Cisco document is a best practice in security for a Cisco environment. Sean Convery (CCIE #4232) and Bernie Trudel (CCIE #1884) are the authors of this White Paper. The document has a great statement "If you're going to log it, read it". The Cisco document is very in-depth providing helpful solutions to all your Cisco configurations. Stay current with the Cisco IOS and make sure you have a current diagram depicting your layer 3 environment.

Routers are usually considered in the audit review. Make sure you follow good support habits here as well. Disable any unneeded services. Use Secure Shell to access the routers, use TACACS+ for authentication, and review the logs frequently. If possible use a product like NETSYS, NETSYS Baseliner can even validate your network configurations. NETSYS can monitor any network configuration changes and alert designated data network engineers that a change has occurred.

Remote connectivity is a common area for an audit. Make sure you have a sound process for disabling the ID's of former employees. Make sure that there is a good password policy in effect. Make sure that you log as much as possible in any session be it dialup or VPN. Remote connectivity is a required service companies provide employees. The company's remote connectivity can provide a hacker an access point. If possible use two factor authentication like secureID for your VPN or dialup solutions.

APPENDIX A

SAMPLE CUSTOMER NOTIFICATION EMAIL ALERT

The Acme Shipping IS&T Networking Team will be performing network infrastructure maintenance tonight, Friday December 7th from 10:05 PM EST to 12:05 AM EST. This 2 hour maintenance window will be in response to some of the recent networking issues we have experienced over the past two weeks. The changes that will be implemented tonight were requested from our vendor who supplies all of the hardware for Acme Shipping's network infrastructure, CISCO systems. These changes will affect most of the Acme Shipping offices in one way or another.

Please read this email carefully to see how it will affect your location.

Acme NY Building A:

You will be able to do the following:

- Logon to the network.
- Access your files on the Novell File Servers at Acme NY Building A (home and shared drives).
- Print to a network printer.
- Access email on the Exchange Servers at Acme NY Building A.
- Access the Internet.

You will not be able to do the following:

- Send email outside of the Acme NY building A location.
- Access custom applications housed at the Data Center.
- Access the AS/400 or RS/6000 boxes housed at the Data Center.

Acme NY Building B and other NYC offices:

You will be able to do the following:

- Logon to the network.
- Access your files on the Novell File Servers at Acme NY Building B (or Novell File Servers located within your building) - home and shared drives.
- Print to a network printer.
- Access email on the Exchange Servers if your email server is housed at Acme NY Building B.

You will not be able to do the following:

- Access email on the Exchange Servers at Acme NY Building A.
- Send email outside of the Acme NY Building B.
- Access the Internet.
- Access custom applications housed at the Data Center.

- Access the AS/400 or RS/6000 boxes housed at the Data Center.

West Coast Offices:

You will be able to do the following:

- Logon to the network.
- Access your files on the Novell File Servers (home and shared drives).
- Print to a network printer.
- Access email on the Exchange Servers.
- Access the Internet.

You will not be able to do the following:

- Send mail to any location outside of the West Coast.
- Access custom applications housed at the Data Center.
- Access the AS/400 or RS/6000 boxes housed at the Data Center.

Regional Offices:

You will be able to do the following:

- Logon to the network.
- Access your files on the Novell File Servers (home and shared drives).
- Print to a network printer.
- Access email on the Exchange Servers.
- Access the Internet.

You will not be able to do the following:

- Send mail to any location outside of your regional office.
- Access custom applications housed at the Data Center.
- Access the AS/400 or RS/6000 boxes housed at the Data Center.

If you have any questions regarding the above, please call your local PC Support Help Desk. **Please do not reply to this message **.

Thank you for your cooperation!

Acme Shipping IS&T PC Support Help Desk

APPENDIX B

Change Control Notification

From: Wyle E. Coyote
Date: 5/30/2003
Re: Connecting 20 Clover Street to 80 Oxenford Street

Overview

Production Change
Using the form below, enter a general description of all changes being performed to production equipment.
Install Pre-configured Router and Switch at 10 Dover Street
Install 2620 Router and 3624 Switch in place of ACME SHIPPING Router and hub on new Colt 2 MB G.703 circuit to Oxford Street.
Configure VWIC S2/1:0 on London router to connect to ACME SHIPPING-Intl

Reason for change:
ACME SHIPPING-Intl Currently connects to ACME SHIPPING via 64K International Frame circuit to the U.S which apart from being extremely costly does not offer them the connectivity speed or resources they require.

Equipment Affected:

London Router, All ACME SHIPPING-Intl Network

Users Affected:
ACME SHIPPING-Intl

Date of Change:
18th March 2001

Change Procedure
Provide a detailed procedure for executing each of the changes above. This description should contain all steps required to complete the change. The numbering in this form should match the numbering in the overview section.
Install new router and Switch

Detailed Procedure:

WAN address 10.10.34.42 on S0/0:0
Loopback address 10.10.1.172
Static route to 10.10.34.41
OSPF network 10.10.58.96 0.0.0.31 area 5
Router Ethernet address 10.10.58.97 255.255.255.224 (def. gateway)
Switch Ethernet address 10.10.58.100 255.255.255.224
Check IP connectivity to 10.10.34.41
check input and crc errors.
save running config.

Configure VWIC controller for point to point circuit to ACME SHIPPING Dover Street.

Detailed Procedure:

Add controller E1 – channel-group 0 timeslots 31.
Add description for controller E1.
Add description to Serial 2/1:0
Add WAN address to S2/1:0 – 10.10.34.41
Add Dialer list 1 protocol ip permit.
Attach Ethernet cable to VWIC card and BNC ends to circuit.
Check IP connectivity to 10.10.34.42
check input and crc errors.
save running config.

Contingency Plan

Contingency Plan Procedure:

Provide a detailed contingency plan for reversing each of the changes above. The numbering in the form below should match the numbering in the above sections.
Failure to connect ACME SHIPPING-Intl to Oxford Street Network

Criteria for executing Contingency Plan:

No connectivity

Detailed Procedure:

Workstations remain as is on the current 64K frame link.
Request assistance from Viacom Operations.

I. Appendix - References

1. Cisco Systems. "Improving Security on Cisco Routers." Dec 29, 2002. URL: http://www.cisco.com/warp/public/707/21.html Document ID: 13608, (February 14th, 2003)

2. Canaudit, Inc. "Network Audit." 2003 URL: http://www.canaudit.com/Audits/audit_outlines/Network_Audit.htm (February 19th, 2003)

3. C & A Security Risk Analysis Group. "COBRA Knowledge Bases." March, 2003 URL: http://www.security-risk-analysis.com/cobkbs.htm (March 3rd, 2003)

4. AuditNet.org. "The Internal Audit Process: How It Works!" URL: http://www.auditnet.org/process.htm (March 4th, 2003)

5. PhoneBoy. "PhoneBoys Firewall-1 FAQ's." August 2002, URL: http://www.phoneboy.com/fom-serve/cache/7.html (March 8th, 2003)

6. Centreline 2000 "A Backgrounder to Securing Your Internet Connection" 1st September 2000 URL: Securing the internet link (March 23rd, 2003)

7. Cisco Systems. "Troubleshooting 10/100 Half/Full/ Auto-Negotiation" Updated: Nov 08, 2002 Document ID: 10561 URL: Configuring and Troubleshooting Ethernet 10/100Mb Half/Full Duplex Auto-Negotiation (March 11th, 2003)

8. Hurley, Edward. SearchSecurity "Auditor: There's nothing to fear" April 8, 2002. URL: Auditor: There's nothing to fear (March 19, 2003)

9. Cisco Systems. "Troubleshooting Cisco Switches to NIC Compatibility Issues" Updated: 2003 URL: Troubleshooting Cisco Catalyst Switches to Network Interface Card (NIC) Compatibility Issues (March 23rd, 2003)

10. Hall, Eric. "Firewalls & VPN's.", October 16, 2002 URL: Firewall Essentials (March 23rd, 2003)

11. Antoine, Vanessa, Bongiorni, Raymond, Borza, Anthony, Bosmajian, Patricia, Duesterhaus, Daniel, Dransfield, Michael, Eppinger, Brian, Gallicchio, Kevin, Houser, James, Kim, Andrew, Lee, Phyllis, Miller, Tom, Opitz, David, Richburg, Wiacek, Michael , Wilson, Mark, Ziring, Neal. "Router Security Configuration Guide" September 27, 2002. URL: http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf , Sections 3.4.2 - 3.4.4 (March 30th, 2003)

Last Updated: September 21st, 2017

Upcoming Training

SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event