Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)

Practical Assignment

Version 1.4b

Option 1 – Research on Topics in Information Security

Author: Natalia Belaya

Network Auditing on a Tight Budget

1. Introduction

Working as the sole network engineer in a medium-sized startup company with multiple large financial organizations as its clients and being audited three times in the last few months has made me think about creating and maintaining a set of best practices for auditing an entire network. Although our auditors have yet to find anything egregiously insecure or inadequate in our networks, they have reminded me of the importance of network security as well as how hard it is to keep up to date with the staggering number of possible attack vectors and publicly known vulnerabilities that a modern intruder has at his or her disposal. Even more importantly, they have reminded me of how much trust and reliance our customers and their customers in turn place on our ability to keep their data safe and confidential.

Like any company of our size in the current U.S. economy, we have a fairly tight budget with which to accomplish our mandatory (sometimes by law) goals. Given the enormity of the overall task, it is easy to become discouraged and feel like one simply does not have the time or resources with which to keep all the myriad dangers at bay. However, a little research into the subject will reveal that many high-quality industry standard tools are available for free (often with source code included). Security by its very nature is a process that benefits from peer review, and there is arguably nothing that receives as much peer review in this day and age as open source software. The time spent on due diligence in securing and maintaining a network may be the best investment you can make, and audits are one of the best tools for keeping up to date on vulnerabilities. It is always better to know your weaknesses and work on eliminating them step by step than to be surprised by outside auditors or, even worse, malicious intruders. In this paper, we will survey and discuss a wide range of options from which you may create a set of policies and procedures for performing self-audits.

2. Where to Start?

It is important that your management is aware of and has given approval for your plan of action. Although it may seem far-fetched, lack of documented managerial support can potentially lead to unpleasant legal consequences if anything goes wrong. Once you have the necessary approval, it is important to gather detailed documented information about your network and your company's security policy. You can't fix what you don't know about. Make sure you get a feel for how your network supports your organization, what it is used for and by whom, what the data flows are and how they interact, etc. Note that you may not have to reinvent the wheel at this point. Here are some of the techniques Kevin Day suggests in his book *Inside the Security Mind*:

1. Read press about the organization. The media has a knack for focusing on areas that are important to an organization.
2. Talk to the local IT staff. Learn about the different types of systems, and how they operate, as well as where the largest percentage of resources are allocated.
3. Hold conversations with different department managers. Ask about their operations, what they do, their priorities, and what they see as the most important function of their environment. (Be sure they know that you are not doing an audit or assessment of their positions.)
4. Make a list of objects you are going to audit. You will need to understand of how each major object functions within your environment. Once again go out interview various staff members about each object.
5. Discover the risk factors. Use the gathered information and previous interviews to determine the risk factors. Document your findings.

3. Do not be discouraged; be practical

Now that you have a view of the "big picture" for of your network, the next step is to break it down into components to audit. Taken as a whole, the network is a daunting monolithic system. Understanding it in smaller pieces will make executing your plan much easier. It is very important to understand that, while few technical practices can match the dynamic and challenging demands of security, it is achievable and does not have to come at an exorbitant cost to your organization. Simply by evaluating and entertaining the idea of auditing and tightening security, have started down the right path.

- Keep it manageable. Don't start with the most thorough audit possible that yields thousands of pages of results and dives into the minute details of every system, physical area, and corporate relationship imaginable. It can be more costly than practical and leave you with complicated results that are hard to analyze and even harder to use as a basis for an action plan.
- Be practical. Make the audit affordable not only in terms of monetary expense, but also in terms of your time and effort.

- Focus on quality, not quantity. Concentrate on real vulnerabilities and threats, prioritizing based on likelihood of exploitation and leaving the smaller "nitpicking" details for later cleanup.
- Make sure that the results of the audit are going to be comprehensible to an audience beyond that of network security professionals.
- Conform the audit to your security policies. The audit should be a reflection of your policies, not the other way around.

4. Audit Preparation

The tasks that need to be completed in the process of audit preparation are:

- Make a plan. Outline the specific steps you are going to take, in order, and the systems or devices that you will target.
- Acquire auditing tools. I will be going over the auditing tools you might consider for use in the following section.
- Schedule your activities. Make a project plan of the general sets of activities you are going to perform and when. Milestones help in tracking progress.
- Warn. Then warn again. Then warn some more. Make sure that the administrators and managers involved are aware of the technical activities being performed. There is always a possibility of breaking something while performing network scans, penetration testing, and hands-on analysis.

5. Auditing Tools

There are plenty of tools currently available that can help you in completing your audit. Most of them are mature, well-tested open source products. I recommend that you acquire at least a handful of them for your security-related activities. They can handle a lot of time-consuming details automatically, leaving you more time to focus on the audit itself.

Vulnerability scanners:

- Nmap <http://www.insecure.org/nmap/> - A very powerful portscanner.
- Nessus <http://www.nessus.org/> - Renaud Deraison's automatic remote vulnerability probing and reporting program (with a GUI interface and the ability to create HTML output with pie charts and graphs).
- Sara <http://www-arc.com/sara/> - A host-based security scanner.
- Saint <http://www.saintcorporation.com/products/saint_engine.html> - Another remote vulnerability scanner.
- Vlad the Scanner <http://razor.bindview.com/tools/>

In addition to the wonderful open source offerings listed above, there are many popular commercial scanners available:

- ISS Internet Security Scanner <http://www.iss.net/> - A GUI-based tool with configurable levels of scan intensity.
- ISS System Security Scanner http://www.iss.net/ - The host-based counterpart to ISS Internet Security Scanner, also with configurable scan levels and "suggested fix" capabilities.
- Retina Scanner <http://www.eeye.com/html/>
- QualysGuard <http://www.qualys.com/> - A subscription-based remote scanning service.
- SecureScan <http://www.vigilante.com/> another subscription-based scanning service.

Cracker tools are often nice to use as a supplement to the vulnerability-scanning products. Needless to say, most of the above mentioned tools could be used not only for audits but for attacking the networks as well. Some important tools include password crackers like L0phtCrack <http://www.atstake.com/research/lc/> for Windows "LanMan" passwords and John the Ripper <http://www.openwall.com/john/>, Solar Designer's fast modern Unix password cracker.

There are also automated system hardening programs available such as Dumpsec <http://www.somarsoft.com/> for Windows and Titan http://www.fish.com/titan for Solaris. The list is very long and is constantly changing. I suggest frequent research on the classes of tools that you are interested in and updating or patching them to keep in sync with the latest available code and information.

6. Basic Auditing Steps

Now you have a plan and a set of tools. Depending on the scale of your audit, you can elect to use all of them or just a subset.

Discovery Scan

One of the most popular first audit steps is object discovery or enumeration. Even if you think that you have every system documented and every object accounted for, there is always a chance that you can find something no one even knows about. Start off by creating a current list of all objects that are going to be audited by doing a "discovery scan" on the network address ranges you over which you have jurisdiction. You can combine the discovery scan with collecting information about each device such as its name, operating system, and hardware. Any of the remote security scanners mentioned above are capable of doing enumeration. You can perform the discovery scan both externally (outside any relevant firewalls) and internally. Various techniques exist for differentiating

between responsive and non-responsive hosts, as the possibility exists for live but unresponsive hosts.

I frequently use nmap by "Fyodor" (his preferred pseudonym) for my internal and external discovery scans. There is a very good article by Mark Wolfgang entitled "Host Discovery with Nmap" at http://moonpie.org/writings/discovery.pdf plus lots of useful documentation on the nmap website at http://www.insecure.org/nmap/nmap_documentation.html
Compare the results with your list of the devices. Have you found something new? If so, investigate. If not, you can move forward on to the next step.

Vulnerability Scan

Now that we have an exhaustive list of devices to audit, we can start vulnerability scans using an appropriate scanning tool. This scan can also be done both internally and externally. I suggest that you start with the external scan, which will help you to understand:

- What can be seen from the outside world – this task is similar to the external discovery scan because you are scanning the entire address range and not just the objects you know about. You want to know all the ports on your various systems that are visible to the Internet. During this task you can check you security devices to see if they are properly reporting your probes or intrusion attempts. Check (N)IDS messages, firewall logs, etc.
- What to look for in your logs and other detection tools – what the attacker sees is probably what he or she will target first, given an modestly intelligent attacker or, failing that, a modestly well-written attack tool.

After you are done with external vulnerability scan you can perform the internal scan and compare the results. Comparing these two scans will help you understand how good or bad your perimeter security is.

Different scanners have different options, but most include probing policies based on the type of the object being scanned. You do not have to scan a Unix server for Windows vulnerabilities or scan a router for vulnerabilities associated with a server. Paring down your selected scan types can save quite a bit of time. Vulnerability scanners are very helpful and powerful tools, but you must be very careful because they can be extremely distracting or even harmful when used improperly. Once again, make sure that you have the necessary documented permission to perform a scan of the objects even if they are under your management. Schedule scans in advance and during times when no other changes to the network or systems are going to be made. You can also use a scan including all available options, but it will take more time. Most of the scanners have DoS features. Make sure that you turn those off or schedule a maintenance window if you are planning on using them. I use Nessus for performing vulnerability scans on my networks. It is easily upgradeable with the

latest exploits and you can automate it for future use once you are familiar with it. Nessus has a plug-in architecture so you can easily add you own tests without having to read the source code of the Nessus engine. Nessus will not only tell you what's wrong on your network, but will, most of the time, tell you how to prevent crackers from exploiting the security holes found and will give you the risk level of each problem found. It has lots of other great features and can produce several different types of reports depending on who the intended audience is and what level of detail you are looking for.

7. Hands-On Audit

This part of the Network Audit can help you to further verify the compliance of your security policies with the existing situation. This part of the audit can take a lot of time and resources, so you need to decide on how thorough and detailed you want to be here. Of course, the best-case scenario here is to perform a hands-on verification of every major object. That may be impossible in some cases, however, due to limited resources. Depending on how much time and resources you have and the number of objects being targeted, you can do:

- Hands-on audit of every object
- Hands-on audit of critical objects
- Hands-on audit of high risk objects
- Hands-on audit for a few objects per department
- Hands-on audit of just a few random objects

You will be working on verifying that the objects are configured and performing in accordance with established security policy requirements. Some of the tasks you can perform during this part of the audit could be similar to:

- Is there a modem attached to the device?
- What are the login policies?
- Is there any unauthorized software installed?

Some parts of the hands-on audit can be automated. Depending on what platform most of your objects are, there are different packages available. For example, for Windows you can use Absolute Software <http://www.microsoft.com/resources/sam/sit/catalog/59.asp>, which will track license management, alerts for over-installation, unauthorized software reporting, license compliance, alerts and/or warnings, automatic updates to inventory databases when new software is installed or removed, unauthorized software report and software upgrade readiness. For Unix-based platforms you can use Chkrootkit from http://www.chkrootkit.org.

You can also automate modem searches by downloading or purchasing a war-dialer to call all numbers belonging to your company and check for responsive modems.

8. Physical Audit

During the physical audit, you will be inspecting the actual areas where the objects you are auditing are located and making sure that they are being kept in accordance with the physical portion of your security policy. Some of the things you might want to inspect during the physical audit are:

- Environmental conditions – check for the proper temperature, humidity level, and other environmental conditions that can cause a failure of the device.
- Power – Is the device attached to a UPS or surge suppressor? Is there enough power to restart all the devices in case of failure? Do you have a generator?
- Physical access controls – How easy would it be to walk out with an object? How easy would it be for someone not authorized to physically access it? How is the access monitored? Do you have cameras and/or guards?

9. Wireless Audit

Wireless is here to stay, like it or not. Check your security policy and see if it addresses wireless networks. If it doesn't then you might want to update it – you will need it at some point. If you want to remove any access points found during the audit, you had better be prepared to answer the questions about why you want to remove them. If wireless networks are prohibited by your security policy, you might need as little as just a laptop with a tri-band wireless card (or a couple of different wireless cards for 802.11a and 802.11g) to find the access points and remove them.

If you have a documented wireless network and need to audit it, that will be a whole different task in and of itself. Here is the list of devices you will need for a wireless audit as suggested by Merritt Maxim and David Pollino in their book *Wireless Security*:

- Laptop
- Wireless card
- Global Positioning System (GPS) (optional)
- Building plan
- Batteries
- Sniffing software
- Antennae and cables (optional)
- Amplifiers (optional)
- DC inverter (optional)

Some other useful tools include Airsnort from <http://airsnort.shmoo.com/>,

Kismet from <http://www.kismetwireless.net/>, and LinkFerret Wireless Packet Sniffer from <http://www.linkferret.ws/wireless/wireless.htm>.

Wireless assessment is not as complex as it seems, just different assessment of more traditional media. It is very similar to the basic audit discussed earlier in this paper. The important part is that you have the security requirements for wireless networking specified in your security policy. The wireless network audit consists of three main parts:

1. Information gathering – where you look for wireless devices and get the samples of wireless traffic.
2. Data analysis - where you analyze the information you gathered. For example, checking if the wireless traffic is encrypted in accordance with your security policy.
3. Follow up – action on the findings. This part can be included in the reporting and review of you main audit if the wireless audit is a part of a network audit.

10. Social Engineering Audit

This type of audit is very often (and wrongly) overlooked, to the great satisfaction of intruders.

"A company may have purchased the best security technologies that money can buy, trained their people so well they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally vulnerable…Cracking the human firewall is often easy, requires no investment beyond the cost of a phone call, and involves minimal risk" says Kevin Mitnick in his book *The Art of Deception: Controlling the Human Element*. The book gives some wonderful examples of social engineering attacks. You will not regret reading it even if you are not directly working in the field of security.

A social engineering attack is an attempt to convince a legitimate employee of the target organization to perform an unauthorized (by the organization's security policy) activity.

Depending on the scope of your audit, social engineering attacks can be used as penetration tests. This sort of test will help determine how vulnerable your employees are to adept or charismatic individuals who can convince them that they are help desk personnel, technical support, system or network administrators, etc.

11. Dumpster Diving

"That's right: garbage. It's been a number of years since the hacking underground brought the term dumpster diving into vogue, but it's apparently enjoying a renaissance of sorts. Dumpster diving is an apt, if a bit fanciful, description of the process of sifting through the garbage of large companies

searching for information on how to access corporate networks or fodder for social engineering attacks, which are the online equivalent of a con man running a scam. The Wall Street Journal story instructs about the potential harm to a company and its network and of the ease with which such attacks can be carried out." Dumpster diving can also include searching through the organization's web sites, product information and all kinds of accessible literature. Online dumpster diving is referred to as "scavenging."

Dumpster diving can be used as a penetration test as well. You will discover just how much of your company's information is easily available or left lying around instead of being shredded or destroyed.

12. Review and Report

Now that you are done with all the tasks you planned, you can start reviewing the results. You can use the scores for individual objects and compare these scores to statistical averages or, if it is not your first audit, to the previous audit's results. Although the actual format of the reports can vary from organization to organization, the reports you produce should be clear, concise, and understandable by the people who are going to review them. They should address the purpose of the audit, the scope of the audit, and the results discovered or revealed by the audit. You can include recommendations for improvement along with the audit results.

Owners of devices should be sent copies of the reports for their individual objects. Reports should be reviewed with managers and heads of different departments as well as with their IT staff. The corrective actions suggested by your report should be discussed and scheduled depending on the severity of the vulnerabilities in question. It is important to get engineers and managers to read and understand the report so that they understand the necessity of the corrective actions.

13. Make it a Process

Make auditing a part of your security routine. Perform it regularly. Depending on your organizational needs and ability to automate, the time required can vary. The frequency of the audit reports should be based on the assets and level of risk involved. The more valuable the asset and the higher the risk, the more often the audit should be completed. Some of parts of the audit can be performed more often than others if necessary.

14. Conclusion

Do not think of network auditing as a very expensive or hard to accomplish task. You can do it with a relatively small investment of your time. Do not overwhelm yourself. Make a plan that is realistic and doable. Even if it is not everything you would like to do, it is still far better than doing nothing at all.

Auditing is sometimes thought of as a one-off task that is separate and distinct from day-to-day network management tasks. I consider auditing to be both an integral part of a network administrator's job and a continuous work in progress.

References

1. Day, Kevin. *Inside the Security Mind*. Pearson Education, Inc, 2003. 2-7, 191-193.

2. Maxim, Merritt and Pollino, David. *Wireless Security*. McGraw-Hill/Osborne, 2002. 282-283.

3. Tiffel, Ed, et al. *Certified Information System Security Professional Study Guide*, San Francisco: Sybex, 2003. 476.

4. Mitnick, Kevin and Simon, William. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, 2002.

5. Stevens, W. Richard. *TCP/IP Illustrated, Volume 1*. Reading: Addison Wesley Longman, Inc, 1994. 70 – 71.

6. Smith E. Gordon. *Network Auditing: A Control Assessment Approach.* WilleyEurope, 1999.

7. Skoudis Ed. " Tips for Dealing with Insider Security Threats" September 28, 2001 <http://www.informit.com/isapi/product_id~%7B269E316A-A677-4D24-90BC-8F0DD16709EC%7D/session_id~%7BABF9C8B8-6CB4-4CDF-9F14-C149469173DA%7D/content/index.asp>

8. Skoudis Ed. "Vulnerability-Scanning Tools" September 28, 2001 <http://www.informit.com/isapi/product_id~%7B2F6505CB-C02F-4F82-AC34-E30236CDE676%7D/session_id~%7BABF9C8B8-6CB4-4CDF-9F14-C149469173DA%7D/content/index.asp>

9. Fellinge Jeff. "Surviving IT Audits: Facing your tears" May 2003 http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=38431&pg=1&show=599

10. Latest Security News and Tools on May 2003 <http://www.makesecure.com/main.php>

11. Lincoln Adam, CFO Europe. "Tools of the trade: Auditing Audit Software" February 01, 2003 <http://www.cfo.com/article/1,5309,7080%7C%7CS%7C%7C564,00.html>

12. Rude Tomas " Knockin' At Your Backdoor" A Guide to Penetration Testing. October 2000. http://www.crazytrain.com/penetration.html