Global Information Assurance Certification Paper

Lessons in Learning Network Security

Coleen Wood

July 5, 2003

GSEC Practical Assignment v1.4b, Option 1

Abstract

Advancements in technology including the power of the Internet greatly enhance many aspects of modern life, but with those benefits come risks. In today's environment any person using a computer connected to a network needs to have some knowledge of security. The type, frequency and criticality of that usage will dictate the level of security expertise needed. The volume of information available on network security is overwhelming. New technologies, vulnerabilities, tools, and exploits are created every hour of every day, and communication and distribution of this information happens at blinding speeds via the Internet. Keeping up with new information is a challenge, but the first major hurdle is to gain a solid understanding of security basics.

One approach to developing proficiency in this complex and ever evolving subject is to cultivate processes and tools to enable knowledge and information to be obtained when needed. Reading and studying network security will help to gain insight, but hands-on experience will reinforce and enhance the learning experience. A test environment with one or two computers can provide opportunities for learning and exploring that is limited only by the amount of time devoted to the task. Building and using a test environment will require a lot of information from a variety of sources, so it's beneficial to develop good methods to locate, organize and track information for later reference. The opportunities and possibilities for learning about network security are endless, so keeping information organized and being able to find and utilize tools effectively when needed will help gain proficiency in this area.

Seeking Knowledge on Network Security

Taking classes, attending conferences and seminars, talking with vendors, reading books, white papers and articles is will help to learn network security. Quickly it becomes apparent that there is far more information available than can be absorbed. To alleviate this problem, create a system of indexing and organizing information will facilitate finding information when it is needed. There are many sources of information, and some will be more appropriate for specific environments and levels of experience. Keeping track of good sources of information, taking good notes, and storing copies of documents in a way that can be indexed and searched will make the task of retrieving information much more effective.

In the time it takes to learn existing security concerns and issues, new ones are being discovered. To get current information on security issues, subscribe to Newsletters and Digests available at http://www.sans.org/newsletters/ and BugTraq. BugTraq is a moderated mail list dedicated to computer security vulnerabilities and exploits that is hosted by Security Focus. Both SANS Newsletters and BugTraq keep archives of information online for searching as needed. Many hardware and software vendor web sites and user groups have information and mail lists on patches and vulnerabilities too. Since it may not be possible to read all of this information as it comes out, one option is to scan each item that is published just to get familiar with the topic. Then the archives and web sites can be searched at a later time if specific information on a topic is needed.

An obvious source of information is the Internet. There are a great may web sites with valuable content so organizing Favorites to make it easy to locate information when needed is essential. Separate folders into categories that are logical and relevant so they may be recalled as needed. For example, security procedures, tools by type of function, operating system specific information, networking, conferences and newsgroups, security vendors and hacker sites are examples of some categories that may be used. There is a balance between too many folders of Favorites and not having enough. Organize and reorganize Favorites as needed to maintain a structure that will make information retrieval as efficient as possible.

When selecting a web site to use for reference or as a source of tools to download, consider the quality of the content. Virtually anyone can put anything on the Internet. The content on web sites is not always kept up to date so pay attention to the dates on material to insure it is appropriate and relevant. Also look for ways to validate information found on the Internet. Web sites created by individuals don't typically have any type of quality control or verification process. Newsgroups, mail lists and other public forums may be moderated to oversee content, and others may not. Use caution and good judgment to question the validity of anything found on the Internet, and be wary of downloaded files!

When a web site is found with interesting content, it may be advisable to copy the web pages to a local hard drive so it may be accessed offline or in a test environment. This might also be done as a precaution in case the web page is removed or changed, particularly for hacker web sites or for older tools and technology. For example, vendors remove information on older versions of software at some point after newer versions are released, even though many copies of the old version may still be in use.

A particularly good reason to save a copy of a web site locally is to use it for experimenting with various security tools to analyze and exploit vulnerabilities in a test environment (McClure, Scambray and Kurtz, 815). A free tool that will retrieve and copy web page files is Wget. Offline Explorer is another tool that

copies web sites but both versions require a license to be purchased, although each may be downloaded for trial purposes.

An excellent tool for searching the Internet is Google (http://www.google.com). This wildly popular and extremely powerful search engine indexes more than 3 billion web pages (Calishain and Dornfest, 259) which can be both good and bad. With that much information available, queries can return enormous numbers of results that can take time and patience to sort through. To become more proficient at using Google, and to find many other possible uses for this tool, the book "Google Hacks, 100 Industrial-Strength Tips & Tools" is a handy reference. Using Google Help Central (http://www.google.com/help/index.html) is another way to get information on finding most anything on the Internet.

Get Familiar with the Basics

The next step to learning network security is a good basic understanding of networks and operating systems. This typically requires knowledge of Windows and Unix operating systems, and the TCP/IP networking protocol suite. Networking is the logical place to start because this is the means for communication between computers, which makes networking the key component in launching, identifying and defending against security threats. The type of network access and protocols used will help determine the level of security risk to a particular network. For example, connection to the Internet through an analog dial up phone line to an Internet Service Provider (ISP) has a lower security risk than a broadband IP connection through a cable modem or DSL. Closed networks are not as likely to be compromised by a virus, worm or other type of attack as one that is connected to the Internet. A computer that is not connected to any network has the least risk for a security breach, but a computer that doesn't communicate with any other is also quite limited in its usefulness.

To develop a good understanding of networking, good training and reference information is essential. Many good articles, papers, books and classes are available. One good article is by Karen Kent Fredrick titled "Studying Normal Network Traffic" and has three parts that can be found on the SecurityFocus web site. This article covers basics of interpreting packets using TCPDump / WinDump to capture packets, and explains and illustrates the generation of normal network traffic and examining the results. This type of exercise is very helpful in understanding and recognizing specific types of network traffic, which also helps in recognizing and understanding abnormal network traffic. Another very good article is "Interpreting Network Traffic: A Network Intrusion Detector's Look at Suspicious Events" by Richard Bejtlich. This article also goes through step by step illustrations using data in a TCPDump format to clearly explain networking in the context of both normal and malicious network activity.

A comprehensive reference book on networking is "TCP/IP Illustrated, Volume 1, The Protocols" by W. Richard Stevens. This book describes networking concepts clearly with great illustrations and therefore is substantial in size. It's not a book that would likely be read cover to cover, but it is a great reference when a particular exercise or event requires a more comprehensive understanding of IP networking.

One key to identifying network traffic is understanding the usage of ports. Ports 0 through 1023 are defined as Well Known Ports and are intended for use by system and privileged user processes (such a root). Ports 1024 through 49151 are Registered Ports for applications and processes used by ordinary system users. The remaining ports, 49152 through 65535 are Dynamic or Private Ports that may be used by any user or application as needed. The web site that serves as reference on assigned ports is the Internet Assigned Numbers Authority (IANA) at http://www.iana.org/assignments/port-numbers. The IANA is the organization that registers port numbers for the Internet, and their web site also contains a lot of other information and many useful links to other sites.

While the IANA documents ports that are used for good purposes, other web sites provide lists of port number used by Trojan horse programs. One such web page is http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html maintained by Joakim von Braun. The majority of ports on this list are in the Well Known or Registered port number range, with less than 10 percent of the ports in the Dynamic range. This reference may help to identify the type of malicious activity.

Once the basics of networking are understood, and a solid basis of reference information is established, the next step is to have a good working knowledge of the operating systems. To be able to sufficiently research and understand basic concepts and tools, familiarity of Windows and Red Hat Linux will be helpful.

For information on Windows operating systems, Microsoft Press publishes a series of "Inside Out" books that have a wealth of information. One of the series, "Microsoft Windows Security Inside Out for Windows XP and Windows 2000" by Ed Bott & Carl Siechert has very good information in a clear and readable format. Of course the Microsoft web site is another excellent source of information and downloads. Microsoft Technet in particular has expansive technical information on Windows (http://www.microsoft.com/technet).

For Linux, the book "Red Hat Linux 7.3 Bible" by Christopher Negus covers from installation and basics of using the operating system through setting up servers and networks. This book also has a chapter devoted to getting the user familiar with the operating system for those just starting to work with Linux. Free online technical support and additional information can be obtained from the Red Hat web site at http://www.redhat.com/. For security information pertinent to Linux,

"Hacking Linux Exposed, Second Edition" by Brian Hatch & James Lee is a good reference.

Books can be expensive, but many come with CD's with either the electronic version of the book for easy access or supplemental tools and information that adds value. Some may prefer the hard copy format for reading and referring to rather than soft copy material, even when highlighting and note taking capabilities are available with the soft copy. As with web content, check the date the material was published to insure it is appropriate and relevant.

Armed with this knowledge, or at least the means to acquire the knowledge when needed, the next step is to create a test laboratory where the lessons can be put into practice.

An Environment to Play and Learn

After reading, studying are organizing reference material, hands on experience will expand comprehension and bring concepts into a practical context. To get hands on experience, a safe test environment is needed where tools can be used and vulnerabilities explored on computers that don't contain any important or confidential data. Test computers will be exposed to potential threats so these machines may require frequent reloading of the operating system in addition to the risk of losing data if the machine is compromised.

A good basic test environment can be accomplished with a couple of dedicated computers. The test computers don't have to be the latest technology, but they need to be able to run Windows 2000 Professional and Red Hat Linux 7.3. A computer with a 350 MHz processor, 128 MB of RAM and a 6 GB hard drive is sufficient to support a dual boot of Windows 2000 Professional and Red Hat 7.3, although bigger and faster is always better. A laptop has advantages of being mobile and compact if workspace is limited, plus purchasing an additional hard drive may be an option to use one machine for two purposes (although not simultaneously). Keyboard, mouse and monitor can be shared across multiple computers by using a KVM switch to help save space and cost, especially if more than two computers in the lab.

There are low cost options for acquiring test computers. Upgrading a home computer may free up a machine, or perhaps needing a test machine may be justification to upgrade to a new home machine. Employers may be willing to provide hardware and software for a period of time, assuming the knowledge gained will benefit the company. Large organizations may have computers that are no longer needed that may be available to borrow or to purchase. Refurbished and used equipment is another option for finding low cost test machines. A lot of companies lease computers and that produces used machines that are available for purchase after the leasing period ends.

The first exercise in the "GSEC Security Essentials Toolkit" is to install and configuring a dual boot test machine. The software to set up a dual boot machine is included with Windows and Red Hat Linux. Most Pentium compatible computers come with a version of Windows included however if the goal is to learn to work with security in a professional environment, the higher priced Windows 2000 Professional or Windows XP Professional licenses will be needed. The Windows license can be an expense close to the cost of the hardware and even more for the server licenses. A borrowed machine from an employer could be a benefit here because these are typically purchased with the Professional versions of Windows. Used and refurbished machines can be found with the Windows Professional licenses included for prices substantially less than buying the hardware and software separately.

Red Hat Linux and other open source software can be downloaded for free, but there is a charge for documentation and support that is not unreasonable. If one test machine is all that is available, that will suffice to run the majority of tools and provide a good basic learning environment. Adding a second machine will expand capabilities to probe and compromise a machine without risk. Exploration of some tools and exploits will require multiple computers but the test lab can expand over time as the knowledge and experience level grows.

When the lab grows to more than one computer, the Internet connection can be shared among the test computers with an inexpensive hub. A router, particularly one with a firewall is a great asset for a home network used for personal and business because it will help to protect the network by blocking questionable network traffic. For the purposes of capturing and analyzing network traffic to better understand security, using a hub will provide less router chatter and will also provide the opportunity to collect inbound network traffic probing for likely victims. Probing into network security will undoubtedly encourage the purchase of a router / firewall for the primary home network if one isn't already part of the configuration. Then the Internet connection can be switched between the test and the home network as needed to isolate the home network from any potential invasion or compromise during testing.

A couple of additional components are helpful for working with the test network. Access to a printer and an external storage device is critical. If there isn't a printer on the test network, material to be printed can be written to a CD, Zip disk or USB drive to print from another computer on the home or work network. A CD or DVD writer is good for saving data because of the capacity and also the ability to easily transport the media to other machines. A lot of software can be purchased online and downloaded but there is typically an extra charge to get a copy of the software on CD. Backing up these downloaded program files could be more cost effective. Many options exist for external storage with a variety of prices that continue to drop as new technology with higher capacity evolves.

When the basics of creating the test lab are completed, the interesting work can begin. Here is both good news and bad news. There are large quantities of various types of security related software available on the Internet for free. This is great for the professional trying to learn as much as possible at a reasonable expense, but the availability of these tools to those with less that honorable intentions is a major reason why proficiency in network security in necessary.

Fyodor, the author of Nmap recently conducted a survey to find the favorite security tools of those who subscribe to the Nmap mail list. The list of "Top 75 Security Tools" can be found at http://www.nmap.org/tools.html, with descriptions of the tools, the platforms supported and if the software requires a license to be purchased or if it's available for free. Some tools have basic versions that are free, and full feature versions for purchase. Of the tools that do require a license to be purchased, virtually all of them allow a free trail of the software for evaluation of the tool before buying. Many of these tools have license fees for home users that are not terribly expensive however with so many good tools available, the cost could quickly add up. Try tools before buying, and also try similar tools to see if another one, possibly for free, could fit the need.

Warnings to Consider Before Testing Begins

It is generally not a good idea to use the network of an employer to gather and explore security tools. This type of activity could be cause for dismissal and even possibly criminal charges. Many companies block access to web sites that contain tools and information used by hackers anyway. It may be safer and easier to have the test environment at home and use an Internet Service Provider (ISP) account to access the Internet. Be cautious about using tools over the Internet too. ISP's will suspend or terminate an account for inappropriate usage and possibly notify law enforcement agencies. Dshield.org gathers log files and analyzes them to identify the top ports and sources of attacks. They have a program called Fight Back that reports hacking activity to ISP's. Making their top ten list of attackers might not bring the kind of visibility that would be life enhancing.

State and federal governments are creating legislation regarding some types of computer usage. An example of a current issue between a computer security tool and the law concerns the tool LeBrea, which is a tarpit or honeypot tool. Tom Liston, creator of LeBrea has removed downloads of this tool from his web site because of fears over the interpretation of an Illinois law which went into effect January 1, 2003. The Illinois law wasn't intended to prohibit the use of honeypot tools, but the broad language of the law could be construed as applicable. The Electronic Frontier Foundation has information by state on similar legislation at http://www.eff.org/IP/DMCA/states/. Be very aware that exploring external computers and networks could have very negative ramifications. It's best not to probe or attempt to compromise a network or computer unless written permission to do so has been granted in advance, and

even then good legal council would be recommended. The safest approach is to keep the testing activity confined to a controlled environment to minimize risk of loss of data, confidential information, employment and personal freedom.

To be Productive, Be Prepared!

To help make the time and effort spent in this endeavor the most productive, consider incorporating good methods and procedures into your processes for creating, maintaining and using your test lab. Be advised that it takes time to build and maintain a lab, which takes away from time spent using the lab for the intended purpose. Rebuilding of test machines is to be expected from time to time, so creating backups or images of machines at various stages could make the rebuilding faster and more predictable. Windows XP has the feature of Recovery Points that may be helpful. Many tools exist to backup and restore data, and tools for data recovery that can restore deleted files may also be useful. Magazines and even user reviews on Amazon.com can help provide information to help select tools. Having a proven plan for backing up and restoring data on all computers will save a lot of time and effort. Storing back ups on removal media or an external drive will insure it can be secured safely offline, and brought back when needed to restore, even if restoring to another machine because of a hardware failure.

Once the test machine is configured and backed up, the actual testing will involve visiting many web sites and downloading many files. There is obviously risk associated with these activities. Downloading a file that turns out to be something unexpected can be a good learning experience. To avoid mishaps with downloaded files, it's a good idea to scan files before opening or executing them. One type of scan is using an anti-virus program, however not all malware such as Trojan horse programs are recognized by an anti-virus program. Or a downloaded program could be named incorrectly and therefore not have the contents expected, although it may not be malicious. One way to help insure the integrity of a file downloaded from the Internet is to scan it using PestPatrol. PestPatrol works in a similar way to an anti-virus program when installed on a computer, except it provides protection for things other than viruses. PestPatrol looks for spyware and malware, and even has the ability to eliminate cookies that track web activity. One of the nice features of this product is File Analysis. File Analysis provides information on what is in that file before it is opened or executed. The program also has the ability to get more information on a file by performing a lookup on the PestPatrol web site of the file being scanned by the MD5 signature. There is a free version that will scan a computer and identify pests, but removal of pests must be done manually. The purchased version includes the full features including removal of pests and one year of updates from the vendor. No protection is the complete answer, but verifying downloaded files before using them can save some time and frustration.

The nature of downloading files and tools and exploring vulnerabilities and compromising machines will bring about changes to the test machines. The goal of testing is to understand and monitor those changes to gain a clearer understanding. The best way to do this is to capture baseline information on the open ports, services and processes running, event / system logs, etc. so there is a documented reference to compare to. Hunting around to see what may be "new" on the computer is much easier if there is a record of what was there before. The "GSEC Security Essentials Toolkit" has an exercise for auditing a Windows system that will go through the basic steps and tools involved. For Linux, Tripwire is available in an open source version for free download. Tripwire will monitor system files on a computer that should not change in the course of normal use. It is a reactive tool rather than proactive but it will take the guess work out of finding what files have been affected by an uninvited intruder. The GSEC Toolkit book also has an exercise for installing and using Tripwire.

Let the Games Begin!

Once you have lab machine(s) set up and configured, the endless journey and exploration begins. Each tool you experiment with presents opportunities to learn and explore further. One of the first hurdles is understanding the normal network traffic in your environment. The number of vendors whose products report back to the vendor during their useful life is growing. Installing a personal firewall on a computer will begin to raise awareness of the amount of incoming and outgoing packets, and it can take time to sort out what all of these things are and if it the communication is desirable or necessary. Restricting some network traffic will cause some applications to fail, so the tuning takes some time and effort. In addition to tuning and testing firewall rules, this traffic will show up in packet captures and the list of connections to ports on a machine. The volume of traffic and connections may be surprising. Prepare to spend time using the various reference material and research tools to understand what is going on in the test environment under normal circumstances before introducing anything creative.

As previously mentioned, the "GSEC Security Essentials Toolkit" has a lot of great exercises to start with. Performing an exercise is just the first step. Following each exercise is suggestions for Additional Reading. The information gathering discussed earlier should also provide additional resources to help further understanding of the tools and concepts of each exercise. A number of other books and web sites provide additional inspiration for exercises should more input be needed. The possibilities are virtually endless. Document test processes and results as part of the library of information created earlier. With so many tools, and many of them performing similar functions, it can be difficult to remember exactly what has been done on which machine so good notes can save a lot of time and confusion. A plain old notebook can make a good test log. Logging the beginning state of the test environment, the tests that have been

performed, the steps and tools used, and the result and possible next action can help to make testing time more productive and more valuable.

For a more serious environment, a notebook with bound pages is recommended for logging notes. Pages can be removed from spiral notebooks without leaving a trace, but not so with composition type notebooks. Some are available with number pages to help insure nothing is removed. These types of notebooks are especially useful for logging any important information that might be called up as part of an investigation at a later time. The opportunity for this is situation to occur is quite possible in the area of security, but this begins to address aspects of security not within the scope of this paper such as legal considerations for incident response and rules of evidence. Be aware there is much more to learn about security beyond just the technical bits and bytes.

In Summary

To borrow a quote from Carl Siechert in dedication of the book he co-authored on Windows Security "To my mom. She didn't teach me everything I know (heck, she has trouble with e-mail), but she showed me how to learn". It isn't possible to be taught everything on the topic of network security because there is too much information changing too fast to keep up. To become effective and proficient in the field, it's important to develop good techniques and methods for learning. Organization and effective use of tools will save time and effort and help make the time spent learning and the ability to recall that knowledge when needed more productive.

References

Bejtlich, Richard. "Interpreting Network Traffic: A Network Intrusion Detector's Look at Suspicious Events." 16 Oct 2002.
URL: http://secinf.net/info/ids/intv2-8.htm (17 May 2003).

Bott, Eric, Carl Siechert. Microsoft Windows Security Inside Out for Windows XP and Windows 2000. Redmond: Microsoft Pres, 2003.

BugTraq. Security Focus. URL:
http://www.securityfocus.com/popups/forums/bugtraq/intro.shtml. (21 June 2003).

Calishain, Tara, Rael Dornfest. Google Hacks, 100 Industrial-Strength Tips & Tools. Sebastopol, CA: O'Reilly & Associates, Inc., 2003.

Cole, Eric, Mathew Newfield, John M. Millican. GSEC Security Essentials Toolkit. Indianapolis: Que, 2002.

Computer Security Newsletters and Digests. SANS Institute. URL:
http://www.sans.org/newsletters/ (22 June 2003).

Dshield.org. FightBack. URL: http://www.dshield.org/fightback.php (10 July 2003).

Electronic Frontier Foundation. State-Level "Super DMCA" Initiatives Archive.
URL: http://www.eff.org/IP/DMCA/states/ (10 July 2003).

Fredrick, Karen Kent. Studying Normal Network Traffic, Part One, Part Two & Part Three. http://www.securityfocus.com/infocus/1221. (4 July 2003).

Fyodor. Top 75 Security Tools. http://www.insecure.org/tools.html (12 May 2003).

Hatch, Brian, James Lee. Hacking Linux Exposed, Second Edition. Berkeley: McGraw-Hill/Osborne, 2003.

Internet Assigned Numbers Authority. Port Numbers. URL:
http://www.iana.org/assignments/port-numbers. (20 April 2003).

Liston, Tom. LaBrea vs. The Super DMCA in the State of Illinois. URL:
http://www.hackbusters.net/whatsnew.html (10 July 2003).

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

Microsoft Technet. URL: http://www.microsoft.com/technet/. (21 June 2003).

Negus, Christopher. Red Hat Linux 7.3 Bible. New York: Wiley Publishing, 2002.

Red Hat Technical Support. URL: http://www.redhat.com/apps/support/resources/. (21 June 2003).

Stevens, W. Richard. TCP/IP Illustrated, Volume 1. Boston: Addison-Wesley, 2000.

Von Braun Consultants and Sinovits Consulting. Ports Used By Trojans. URL: http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html. (20 April 2003).

Links to Tools

Dumpel. Microsoft.
URL:
http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/dumpel-o.asp. (17 May 2003).

Ethereal. URL: http://www.ethereal.com/. (17 May 2003).

Nmap. URL: http://www.insecure.org/. (12 May 2003).

Offline Explorer. Meta Products.
URL: http://www.metaproducts.com/mp/mpProducts_Detail.asp?id=1. (17 May 2003).

PestPatrol. Vers. 4.2.0.33. PestPatrol, Inc.
URL: http://pestpatrol.com/. (17 May 2003).

TCPDump. URL: http://www.tcpdump.org/. (21 June 2003).

Tripwire. URL: http://www.tripwire.org/. (22 June 2003).

VisualRoute. Vers. 7.1d. Visualware.
URL: http://www.visualware.com/visualroute/index.html. (17 May 2003).

Wget. URL: http://www.gnu.org/software/wget/wget.html. (17 May 2003).

Windump. URL: http://windump.polito.it/. (21 June 2003).