# Global Information Assurance Certification Paper

# SECURITY ESSENTIALS PRACTICAL ASSIGNMENT:
# *An Inexpensive Personal Security Training Laboratory*

John Trewolla

ABSTRACT:

Formal training in Internet security practices and technology is greatly enhanced by informal "hands on" experience with the technology. However, gaining such practical experience within the corporate environment may be difficult. One alternative is to set up your own inexpensive security technology training laboratory at home. This paper outlines the minimum requirements for such a training laboratory and offers some suggestions about how to set up such a lab with a minimal budget.

---

**INTRODUCTION:**

Many businesses are becoming more aware of their needs for better Internet security. As a result, many people are looking for ways to learn more about the technical aspects of Internet security. The recent popularity of Internet security seminars, conferences and training courses confirms this trend.

While such lecture-style presentations are a good start, most people master new knowledge and skills best by doing – not just listening or reading. Most people have found that the effectiveness of their "book learning" or "lecture hall" experience is greatly enhanced by gaining some "hands-on" practical laboratory experience.

Yet, most corporate environments provide few opportunities to experiment and practice with Internet security tools and techniques. Common barriers include the time, the equipment and the space required to set up an Internet security training laboratory. If the corporation has already secured its internal systems behind a firewall, an even greater barrier may be gaining the non-secured connectivity needed for a realistic and effective training/testing laboratory.

To overcome these obstacles, the aspiring security professional may consider setting up a low-budget personal security training laboratory at home. This paper proposes some suggestions for doing this.

**STEP ONE: ACQUIRE INTERNET CONNECTIVITY**

The first requirement for setting up and using a functional Internet security training laboratory is to obtain Internet connectivity that provides a static IP address.

There are two reasons for this. First, many security tools like "smart" routers and proxy firewalls are configured with rules that presume a fixed "untrusted" IP address. Second, most real-world "hack attacks" occur in phases that often presume a fixed IP address for the target system. For example, an attacker commonly starts with a reconnaissance phase to locate systems, ports and services that are likely to be vulnerable. These are initially identified only by IP address. Attackers then usually return to the IP address to conduct a "profile" or "investigation" phase before actually launching an attack. [1]

There are two easy ways to obtain Internet connectivity with a static IP address. The first is to obtain a DSL (Digital Service Line) from your local telephone company. The second is to have your local cable company install a cable modem for you. Both of these "broadband" connectivity options provide the additional benefit of high-speed Internet access.

However, DSL access is restricted to areas that are physically close to a telephone company's central office and not all cable companies currently offer cable-based modems. Further, not all homes are wired for cable.

While broadband connections are quite convenient (especially for downloading large software applications), high data transfer speeds are NOT a requirement for setting up and experimenting with Internet security tools. This means that even those who do not have ready access to DSL or cable-based "broadband" Internet connectivity can use a dial-up connection for their lab. A dial-up connection is much slower than a broadband connection but can do the job under certain conditions.

If you are going to use a dial-up line for your lab, it is a good idea to obtain a "dedicated" phone line – unless you are willing to tie up your regular phone line for many hours on end. When you order the line, tell the telephone company that you will use the line for a computer because you may find that a "computer line" costs less than a regular phone line. Be sure to have them check the line for "noise" (hissing and clicks) so that you get good quality connections.

The first way to use a dial-up line is to establish a connection into your ISP and then simply leave the connection in service indefinitely. Although your ISP will assign your connection a new IP address each time you dial in, this may be moot if your connection can stay up for days at a time.

However, this approach will work only (1) if your telephone circuit is highly reliable (that is, it doesn't get frequently reset by your local telco diagnostic routines) and (2) your ISP does not routinely disconnect dial-in sessions after a period of inactivity.

The second way to use a dial-up line is to make special arrangements with your local ISP to obtain access to a "direct" or "private" number. For a fee, most ISP's will set aside a "private" dial-in line exclusively for your use. These connections are not usually subject to time-outs due to inactivity. In addition, many ISP's can configure their systems to assign the same IP address each time the connection is established through a specific modem.

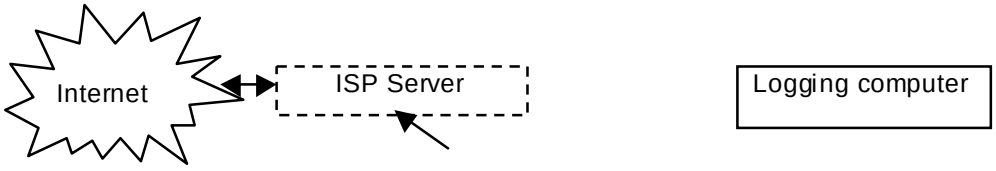
**STEP TWO: ACQUIRE THE EQUIPMENT YOU NEED**

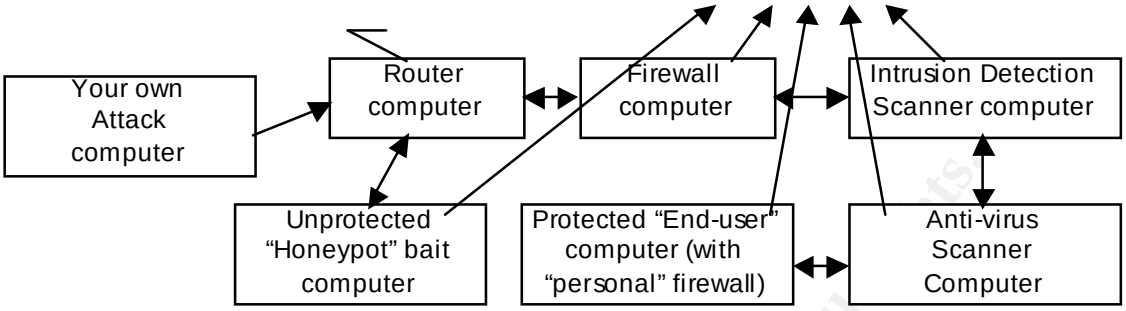
If cost is an issue when selecting the equipment for your Internet security laboratory, remember that high throughput speed is NOT required. In fact, many of your equipment needs may be met by "retired" equipment already in your own (or your neighbor's) basement or attic!

Fortunately, the operating system environments used most frequently for security applications (Windows NT, Linux and Unix) will run on Intel 80486-based (or later) computers. If you do not already have a '486-based machine gathering dust in your basement or attic, used machines are readily available and quite affordable at used computer stores, garage sales and computer clubs. Your company may also have excess/surplus '486 equipment that you can obtain at minimal cost.

Unfortunately, such '486-based systems run these OS's rather slowly. You can usually enhance execution speed substantially by installing at least 32Mb of RAM (64Mb is better!) in the machine. However, be aware that the cost of buying additional SIMM memory may be disproportionate to the value of the machine. One solution is to check with mail-order houses and local computer specialty shops to find RAM at affordable prices. Another solution is to salvage the RAM chips out of one or more (identical) machines to expand the RAM in your test machine. You may discover that you can buy entire '486 machines for less than the cost of buying the RAM alone! Be careful, though. You may need an experienced technician to assist you because RAM chips often do not "mix and match" very well.

One option for compensating for the lower speed and "horsepower" of '486 and older Pentium machines is to use several machines, each for a specific security function. For example, you might configure one machine as an "attacker", another as a router, a third as a firewall, fourth as a logger, a fifth as an intrusion detection network sensor, a sixth as a DMZ request server and so on. (See the diagram below for one possible configuration.) One advantage of this approach is that each device is equipped with its own screen and keyboard that may be helpful in monitoring and "tuning" the operation of the application running on that device.






**STEP THREE: ACQUIRE THE SOFTWARE YOU NEED**

If you are interested in generally exploring Internet security technology, a variety of applications are available over the Internet as downloads. Many are "shareware" which you can install and use for a limited time without payment. If you decide to continue to use the application, the cost of an unrestricted single-user license is usually quite low.

For the Microsoft Windows environments, an excellent source for obtaining these applications is http://www.zdnet.com/downloads. This site lists hundreds (literally!) of security applications. These include many varieties of routers, firewalls, intrusion detection applications, anti-virus scanners, trojan horse detectors, logging utility applications and much more.

Although Microsoft does not distribute its OS systems for free, almost any old computer you acquire is equipped with some version of Windows 9x. On any older '486 equipment, you will probably want to upgrade the OS with upgrades available at no cost from http://www.microsoft.com. If you are working with Windows NT, you will probably have to buy workstation and server licenses if you wish to experiment with these.

Linux has become very popular as an OS for security applications. If you are interested in using this "open source" OS, get a copy of Red Hat Linux from http://www.redhat.com/download. Linux security applications are readily available from several sites:

- http://www.tucows.com offers thirty firewalls, two routers, three IDS applications, twenty logging tools and two virus scanners for Linux, all as shareware.
- http://www.oingo.com offers an excellent software search engine and a nearly overwhelming page of Linux applications links.
- http://www.ganggang.com.au offers dozens of Internet tools and utility applications for Linux and Unix. They also offer hundreds of security-related applications for Windows 95/98 and NT. Each has been user-rated.

If you are interested in working with a specific commercial security application, you will probably have to buy an appropriate license. Most

commercial security software can be purchased directly from the vendor's web site, often as a download. Single-user licenses are not usually very expensive. Some security software vendors offer crippled or short-life evaluation copies at little or no cost.

**STEP FOUR: ACQUIRE THE EXPERIENCE YOU NEED**

Once you have set up your laboratory configuration, start by using your system for your own Internet access and e-mail. It will not be long before your system is scanned to detect open ports and vulnerable applications.

*Set up a "Honeypot" as a lure?*

You may wish to encourage attacks by setting up an unprotected but silently monitored computer behind your router as a "honeypot" lure. Although not without risk, this can be an excellent technique to learn what the "real world" threats are doing. Lance Spitzner offers a guide[2] for setting up a Linux honeypot at http://rootprompt.org/article.php3?article=210. Although this article deals specifically with Linux, the basic steps described in this article apply to honeypots running any OS.

It is essential to know what attacks are likely to be launched against your system. Lance Spitzner has also written a series of three "Know your Enemy" articles[3][4][5] that are an excellent primer on the tools used by many "script kiddies". (See http://rootprompt.org/article.php3?article=159)

In just a few hours or days, your logs will begin to demonstrate the action taken against your honeypot. By comparing your honeypot logs to the logs of your secured system, you can evaluate the effectiveness of the security measures you have implemented on your secure system. One source of attack detection tools is available from Fred Cohen & Associates at http://www.all.net/dtk/ [6].

As you adjust the configurations associated with your security applications, you will be able to evaluate the relative impact of each change you make[7]. If this kind of research excites you, you might consider participating in the forensic challenges offered by the HoneyNet Project at http://project.honeynet.org.

*Set up an "attack" computer:*

Instead of passively waiting to see what attacks are launched against your system, you may wish to set up your own "attack" computer. Doing this allows you to launch attacks of various kinds under your own control. You will quickly gain a much more thorough understanding of various security threats and the effectiveness of various defense strategies and technologies. You can find a (nearly endless!) variety of "script kiddie" and "packet monkey" hacking tools, "how to hack" instructions, "think like a hacker" articles and other offensive tools at http://www.AntiOnline.com and at

www.happyhacker.org.[8][9] Any number of less visible sites offer other and more sophisticated hacking tools and advice. Middle school/junior high school students and local computer clubs are usually ready sources of access to these darker sites.

There is at least one unique advantage to using older, slower equipment in your Internet security technology laboratory. As you evaluate different applications and configurations, the performance impacts of each application and the configuration changes you make will be quite obvious. Such impacts might easily be overlooked on the powerful processors used in commercial production systems. They become important only under heavy traffic loads – which is rarely a good time to be "tweaking" the configuration of a production system! Thus this "poor man's laboratory" may reveal important performance impacts at small scale, long before a full-scale commercial implementation begins to bog down under heavy load.

By the way – if your job is in any way related to the Internet or Internet security, check with your tax advisor about setting up your lab. You may be pleasantly surprised that some or all of your expenditures associated with setting up your security technology training laboratory may qualify as a tax-deductible "employee education/training expense." There's nothing like a tax deduction to "sweeten the pot"!



Notes:

1. Radcliff, Deborah. "Info WAR Games." Computerworld. January 22, 2001.
2. Spitzner, Lance. "Building a Honeypot". March 20, 2000. http://rootprompt.org/article.php3?article=210 (January 22, 2001)
3. Spitzner, Lance. "Know Your Enemy I". March 4, 2000 http://rootprompt.org/article.php3?article=159. (January 22, 2001)
4. Spitzner, Lance. "Know Your Enemy II". March 8, 2000. http://rootprompt.org/article.php3?article=167 (January 22, 2001)
5. Spitzner, Lance. "Know Your Enemy III". March 13, 2000. http://rootprompt.org/article.php3?article=186 (January 22, 2001)
6. Johnson, Rick. "The World of Honeypots". January 9, 2001. LINUX SECURITY NEWSLETTER, ITworld.com. http://www.itworld.com/newsletters. January 24, 2001.
7. Warfield, Michael H. "Honey pots and traps". January 10, 2001. http://www.linuxworld.com/linuxworld/lw-1999-07/lw-07-ramparts-4.html (January 22, 2001)

8. Cramer, Meino Christian. "Guide to (mostly) Harmless Hacking, Vol. 5". January, 1992. http://www.happyhacker.org (January 22, 2001)
9. McClure, Stewart and Scambray, Joel. "Use a honey pot to catch hackers". INFOWORLD NEWSLETTER. August 08, 2000. http://www2.itworld.com/cma/ett_content_article/0,2849,1958_1957,00.html (January 22, 2001)