Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Cyberspace Guardians: A Brief Guide to the Recruitment and Training of Security Personnel

This paper is an overview of the recruitment and training of entry- and intermediate-level information technology (IT) security staff members (referenced here as "security analysts.") Sources for this paper included security texts, news articles, and the experiences of the training team at a Silicon Valley-based network security monitoring company.

Copyright SANS Institute
Author Retains Full Rights

AD

Cyberspace Guardians: A Brief Guide to the Recruitment and Training of Security Personnel

Amina Khattak Claassen

Introduction

Thomas Hobbes, in his landmark treatise Leviathan, noted that if there were no common power, law, or law enforcement to restrain individuals, the life of man would be "solitary, poore, nasty, brutish, and short."[1] The Internet, in its current, mostly unregulated state, is somewhat akin to a lawless land where certain private individuals attempt roam and infiltrate the private domains of peaceable entities. The importance of maintaining a security team to defend networks against such unruly cyberspace denizens is thus of paramount interest to companies conducting business via the Internet.

This paper is an overview of the recruitment and training of entry- and intermediate-level information technology (IT) security staff members (referenced here as "security analysts.") Sources for this paper included security texts, news articles, and the experiences of the training team at a Silicon Valley-based network security monitoring company.

Demand Outstrips Supply

A quick glance at the daily headlines brings home an unfortunate imbalance in the security industry: as the frequency of security events (e.g., hacks, worms, etc.) increase, the shortage of skilled IT security personnel becomes even more severe and troublesome. According to the April 19, 2001 Internetweek.com article, "Security Workers in Short Supply," "For all the millions of dollars being pumped into security, many e-business ventures are woefully insecure. That's because there's a critical lack of quality IT security people…[Industry groups] expect the deficit to exceed one million workers in the next few years."[2]

Given this conundrum, what is a company seeking IT security personnel to do? Security expert Tom Wadlow, in his book The Process of Network Security, suggests that,

> "…your best bet is to find good, smart people and train them. An aggressive training program, the practice of cross-training multiple people for different specialties, and enough people to compensate for absences due to training can produce a formidable security force."[3]

Recruiting Talent

Employers should begin by finding "good, smart people." Where and how might an employer embark upon the personnel hunt?

- **In-house talent.** In a poll of 35 security officers reported in the January 1, 2001 Computerworld article, "Pick Your Security Officer's Brain," an executive noted "that

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

security officers will need to become more creative in their staffing efforts, finding most of their employees inside the organization and then mentoring and training them."[4]

- **Certified professionals.** The well-known Certified Information Systems Security Practitioner (CISSP) credential, offered by the Framingham, Massachusetts-based International Information Systems Security Certifications Consortium Inc., is one of the most coveted in the current security field. The aforementioned Computerworld article also notes the rise in favor of "more diverse and specialized security training through organizations like the SANS Institute in Bethesda, Md."[5] SANS offers rigorous training and certification programs, including intrusion-detection, firewall and incident-analysis certifications.

  Be aware that some certifications may not offer adequate security training. For example, the August 13, 2001 Computerworld article, "Microsoft MCSE Training Faulted," reported that "IT professionals and trainers are blaming insufficient security training offered under the nationwide Microsoft Certified Systems Engineer program for contributing to the spread of Code Red and other damaging viruses." The article goes on to report that many MCSE trainers and students "noted that while basic security is covered as part of the Microsoft Official Curriculum for MSCE certification, in-depth security training is optional and not a core requirement."[6]

- **Experienced defenders.** Wadlow observes that the ideal security employee is one with "enough cleverness to outthink an attacker…someone strong on consistency and measurement…you are looking for good defenders, not good attackers."[7] Wadlow's observation is not a new one when referring to the qualities of defenders. Indeed, circa 375 BC, Greek philosopher Plato noted in The Republic, "We must choose from among our Guardians those who appear to us on observation to be most likely to devote their lives to doing what they judge to be in the interest of the community, and who are never prepared to act against it."[8]

  Traditional sources of security personnel include the military, Department of Defense, programmers, and networking professionals. One unique source of "good defenders" has emerged recently—ex-"New Economy," or dot-com employees. The security manager author of the August 6, 2001 Computerworld article, "Dot-com Brain Drain Helps Corporate Security," observes that the "smaller, newer companies…dedicate more time and effort to securing their systems…This results in staff members who have successfully deployed and managed leading-edge technologies, albeit in small-scale ways."[9]

- **IT security program graduates.** Programs and endowments are being established to meet the needs of the computer security industry. For example, in May 2001, the National Science Foundation announced the establishment of scholarships to six schools-- Carnegie Mellon, Iowa State, Purdue, Universities of Idaho, University of Tulsa, and the Naval Postgraduate School--to educate and develop computer security and information assurance professionals.[10] Graduates of these federally funded "Cypercorps," are expected to work in public service and government positions upon graduation and thus may not be recruited into industry for some time; however, lesser known schools, such Allentown, PA-based East Stroudsburg University (ESU) are developing similar programs. A March 24, 2000 Chronicle of Higher Education article, "Colleges Struggle to Train Experts in Protecting Computer Systems,"

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

reports that ESU students are paired with employees of local companies to learn how to protect networks and website from intruders.[11]

Training Program

Once you have recruited and assembled a security team, your focus will turn to how to train them. High quality training programs address learning styles and needs in a variety of fashions. Components to consider when developing and delivering a security training program include:

- Coursework
- Drills and war games
- Conferences
- Product-specific training
- Research and self-study

Coursework

Coursework will encompass a wide range of topics, and should be on-going as much as feasibly possible. Many companies retain an internal training department to develop and deliver proprietary training (e.g., use of an in-house developed monitoring system). Training departments often work with subject matter experts (SMEs) to translate their knowledge and disseminate it to the security team. One approach used by many companies involves hosting "brown bag lectures" or weekly seminars delivered by SMEs or visiting guests. At the aforementioned network security monitoring company, for example, recent seminars have included:

- Introductory hacking methodology (taught by a former white-hat with extensive penetration testing experience)
- Lectures given by authors/editors of security texts (e.g., *Building Internet Firewalls*)
- Demonstrations of Snort, Firewall-1, and other security software/tools

Studies show that individuals with a "technical bent" retain training that employs their kinesthetic senses. Therefore, successful IT security coursework will include interludes between lecture pieces to allow for lab work, exercises, and other interactive techniques.

Training today augments instructor-led training with on-line and web-based technologies. These alternate forms of delivery can be very helpful in reaching remote users and allowing users to pursue training at their own pace. A word of warning, however, to companies delivering training remotely using some of the popular, publicly available web technologies such as Webex (http://www.webex.com): These sites and the content you post on them are absolutely not secure. Recently, a security engineer reported that he took a web seminar on Webex offered by a vendor of a highly specialized intrusion detection system (IDS). The next day, he received a solicitory e-mail from a direct competitor of this vendor. Coincidence? Or a crafty script?

Drills and war games

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Wadlow, in The Process of Network Security, comments, "Drills give you a way to become familiar with established procedures and to see how they work in action."[12] Drills can range from the highly realistic (e.g., analysts handling simulated attacks in a test environment) to conceptual (such as taking a team out into a parking lot with masking tape and having them "build" a virtual network, and then identify the networks' potential vulnerabilities. An excellent source for this approach could be gleaned from the "Top 14 Security Vulnerabilities" appendix of Hacking Exposed.)[13] It is a good idea to plan drills to start from fundamental concepts, such as common exploit types, and then move to more complex applications that build on the basic knowledge (e.g., a port scan followed by a syn flood.) The design of drills may also be informed by an analysis of the actual events a company experiences itself or has observed in the field. Has the company seen any exploits involving, say, a Linux rpc.statd buffer overflow? Have forensics been gathered that could be converted to a drill or case study? What incident handling techniques are called for in each drill?

Another note about the distinction between realistic and conceptual war games: It is often too easy to get caught up in acquiring technological necessities to stage "realistic" war games (e.g., we lack the training funds to buy the latest and greatest Cisco router, etc.) A conceptual approach often yields very sophisticated results in a timely and cost-effective fashion. One novel approach is that of "attack trees," described by cryptographer Bruce Schneier in his book Secrets and Lies:

> "Attack trees provide a methodical way of describing threats against, and countermeasures protecting, a system. By extension, attack trees provide a methodical way of representing the security of systems. They allow you to make calculations about security, compare the security of different systems…you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes."[14]

Distinctions aside, the benefits of war games have been tracked in academic environments. University of Nottingham Professor Helen Ashman observes in her paper, "War Games: Teaching Web Security Hands-On" that war games yield the benefits listed below.

- Increase students' knowledge in the area
- Motivate students to self-directed study
- Teach students to work successfully in groups with others of varying abilities
- Instill a sense of personal responsibility for the success of the work
- Reinforce understanding of the "wrongness" of security attacks[15]

Conferences

Information security conferences such as USENIX provide a good opportunity to expose security staff to new trends in the field as well as network with peers. Some companies prefer to have their entry-level staff complete a requisite minimum amount of time on the job before sponsoring them for some of the longer and more expensive conferences (e.g., the annual DEF CON in Las Vegas). The opportunity to attend a conference is thus a motivation for an employee to stay with a company for a longer period of time as well as a learning opportunity. Other companies

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

require that conference attendees prepare and deliver training sessions or seminars upon their return to share their new-found wisdom and observations with other team members.

Product-specific training

Vendor-hosted classes and certification tracks, such as those offered by Cisco or Checkpoint, often provide employees with the opportunity to sample newer products and understand the security concepts behind them. Managers should use some caution, however, because the quality of instructors and facilities varies widely from location to location. It is always a good idea to send one or two staff members to assess the quality of the training before committing to training an entire team.

Research and self-study

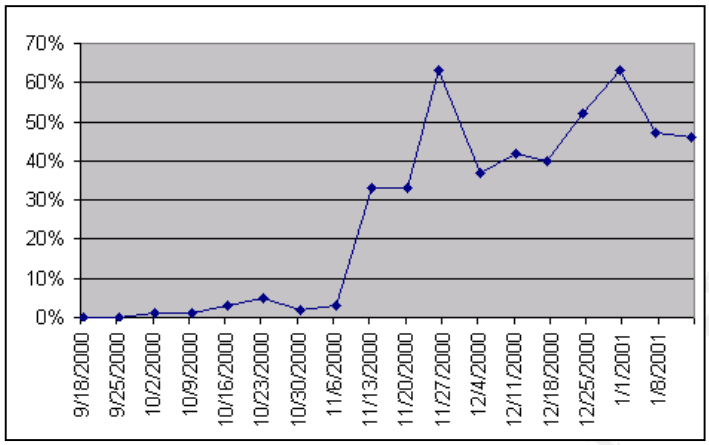
To help employees obtain data to tune devices, stay abreast of current exploits, and otherwise update their general security knowledge, encourage them to conduct research and study security resources such as newsgroups, websites, and security periodicals. The links page of the Hacking Exposed companion website (http://www.hackingexposed.com/links/links.htm) provides a well-organized list. Additionally, subscriptions to security alert/news services, such as the "iALERT Current Intelligence Report" offered by iDEFENCE, Inc., provide timely updates and analyses of security events in an easy-to-read e-mail format.

Companies would do well to budget for a contained, hands-on test lab to encourage security analysts to pursue self-study projects and investigations. The Microsoft website contains documents detailing the general principles behind building test labs, in addition to providing Windows-specific guidance. In particular, the "Building a Windows 2000 Test Lab" chapter of the Windows 2000 Server Deployment Planning Guide (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/reskit/deploy/part1/chapt-4.asp) provides a useful general overview of the test lab development process.[16]

Tracking Training Effectiveness

Once your company has invested the time, money, and energy in developing and maintaining a training program, take the next step by tracking the effectiveness of the training. This goes beyond the trainee questionnaires—sometimes called "smiley sheets"-- that many training departments use to assess and/or justify their efforts. While it is important to gauge the learner opinion of training, training departments would do well to design mechanisms that track trainees' retention and application of the instruction. For example, at one network security monitoring company, training was conducted to increase security analyst compliance with a particular incident handling procedure. A data element indicating the level of compliance with the procedure on the company's proprietary information system, was tracked before and after the training (which occurred in early November 2000) as shown below.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.



In this case, the training proved to be very effective: compliance rates jumped from less than 5% to a more respectable 50% and above. This increase also yielded noticeable improvements in reports and other services related to the particular procedure.

Conclusion

The recruiting and training procedures a company implements will set the foundation for a strong security team. In addition to expending resources to build and maintain these functions, companies will also have to be willing to acknowledge and write off the significant amount of work time necessary for security analysts to learn and research the field. The aforementioned Internetweek.com article, "Security Workers in Short Supply," reports that "a person trying to discover what was damaged or stolen from a compromised system typically spends between 30 and 40 hours examining logs and audit reports, looking for evidence of an attack and what the attacker did."[17] Add even more time on top of this for a security staffer to document the incident, harden against the exploit, and pursue other actions necessary for a post-mortem analysis.

Security is hard; finding and training good people to defend your networks is hard. Careful thought and commitment to the care and feeding of security employees will help companies develop a flourishing and dynamic team.

---

[1] Hobbes, Thomas. Leviathan. London: Penguin Classics, 1651 (first printing), 1985 (reprinted). 65.
[2] Robinson, Teri. "Security Workers in Short Supply." Internetweek.com. 19 April 2001. URL: http://www.internetweek.com/security/secure041901.htm (14 August 2001).
[3] Wadlow, Thomas. The Process of Network Security. Reading: Addison Wesley, 2000. 63.
[4] Radcliff, Deborah. "Pick Your Security Officer's Brain." Computerworld. 01 January 2001. http://www.computerworld.com/cwi/story/0,1199,NAV65-663_STO54802,00.html. (28 August 2001).
[5] Ibid.
[6] Verton, Dan. "Microsoft MCSE Training Faulted." Computerworld. 13 August 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63028,00.html. (16 August 2001).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[7] Wadlow, 59.
[8] Plato. The Republic. Trans. H.D. P. Lee. London: Penguin Classics, 1974 (trans.). 119.
[9] Tuesday, Vince. "Dot-com Brain Drain Helps Corporate Security." Computerworld. 6 August 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO62779,00.html. (16 August 2001).
[10] National Science Foundation press release. "NSF Scholarship for Service Awards Announced at Information Security Colloquium." 22 May 2001. http://www.nsf.gov/od/lpa/news/press/01/pr0145.htm. (19 August 2001).
[11] McCollum, Kelly. "Colleges Struggle to Train Experts in Protecting Computer Systems." The Chronicle of Higher Education. 24 March 2000. http://chronicle.com/free/v46/i29/29a04501.htm. (19 August 2001).
[12] Wadlow, 63.
[13] Scambray, Joel, et al. Hacking Exposed (2nd ed.) Berkeley: Osborne/McGraw-Hill, 2001. 662.
[14] Schneier, Bruce. Secrets & Lies. New York: John Wiley & Sons, Inc., 2000. 318-319.
[15] Ashman, Helen. "War Games: Teaching Web Security Hands-On." 2000. http://www.ausweb.scu.edu.au/aw2k/papers/ashman/paper.html. (23 August 2001).
[16] Microsoft Corporation. "Building a Windows 2000 Test Lab." 2001. http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/reskit/deploy/part1/chapt-4.asp) (23 August 2001).
[17] Robinson.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: November 29th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cape Town 2015	**Cape Town, ZA**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
SANS San Francisco 2015	**San Francisco, CAUS**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
HIMSS	**Boston, MAUS**	**Dec 01, 2015 - Dec 02, 2015**	**Live Event**
Security Leadership Summit & Training	**Dallas, TXUS**	**Dec 03, 2015 - Dec 10, 2015**	**Live Event**
SANS Cyber Defense Initiative 2015	**Washington, DCUS**	**Dec 12, 2015 - Dec 19, 2015**	**Live Event**
SANS Las Vegas 2016	**Las Vegas, NVUS**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Dubai 2016	**Dubai, AE**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Cyber Defence Delhi 2016	**Delhi, IN**	**Jan 11, 2016 - Jan 22, 2016**	**Live Event**
SANS Brussels Winter 2016	**Brussels, BE**	**Jan 18, 2016 - Jan 23, 2016**	**Live Event**
SANS Security East 2016	**New Orleans, LAUS**	**Jan 25, 2016 - Jan 30, 2016**	**Live Event**
Cyber Threat Intelligence Summit & Training	**Alexandria, VAUS**	**Feb 03, 2016 - Feb 10, 2016**	**Live Event**
SANS Scottsdale 2016	**Scottsdale, AZUS**	**Feb 08, 2016 - Feb 13, 2016**	**Live Event**
SANS Secure Japan 2016	**Tokyo, JP**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS Munich Winter 2016	**Munich, DE**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS McLean 2016	**McLean, VAUS**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
ICS Security Summit & Training	**Orlando, FLUS**	**Feb 16, 2016 - Feb 23, 2016**	**Live Event**
SANS Secure India 2016	**Bangalore, IN**	**Feb 22, 2016 - Mar 05, 2016**	**Live Event**
SANS Anaheim 2016	**Anaheim, CAUS**	**Feb 22, 2016 - Feb 27, 2016**	**Live Event**
RSA Conference 2016	**San Francisco, CAUS**	**Feb 28, 2016 - Feb 29, 2016**	**Live Event**
ICS410 London 2015	**OnlineGB**	**Nov 30, 2015 - Dec 04, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**