Training Ethical Hackers: Training the Enemy? by Tim Greene on 03/07/04 ←back

Preface

Training information security professionals carries the risk of training ethical and malicious hackers side-by-side. This paper defines ethical hacking, differentiates it from malicious hacking, presents some of the ways that ethical hacking is taught, identifies some of the risks associated with this training, and concludes with suggestions on how to minimize these risks.

Introduction

Events that occurred on September 11, 2001 along with the ongoing war in Iraq have caused a heightened interest in the field of Information Security. Visiting a computer section in a store such as Barnes and Nobles reveals an increase in the number of books about Information Security. The National Security Agency [1] is looking to increase the number of new hires by 1,500 per year for the next five years. Searching Internet job databases reveals new security positions that require professional security certifications. An Internet search using Google.com [2] revealed 22 such certifications.

There has never been a time when it was easier to learn about hackers and their methods of operation. Many colleges now offer Information Security courses and degrees. It is clear that information security and hacking are "buzz" words at present. The intent of information security training is to improve information security and to educate information security professionals, e.g. ethical hackers. However, providing this "knowledge" in readily available and encapsulated formats presents the hazard of educating not only ethical security professionals but also malicious hackers.

Definitions

To begin the discussion on training information security specialists, more specifically ethical hackers, a working definition of both hackers and ethics is needed. Webster's [3] defines ethics as, "The rules or standards governing the conduct of a person or the members of a profession." From this definition an ethical hacker should have a code of conduct and abide by its principles. For the more elusive term hacker, Webster's [3] offers three definitions of which I'll discuss the first two: "1. One who is proficient at using or programming a computer and 2. One who uses programming skills to gain illegal access to a computer network or file." These definitions differ in the "hacker's" intent. The first definition sounds like a person that is proficient with computers that your company might like to hire. However, the second definition is not as positive with its use of the word illegal: the hacker is up to no good. By combining what we've learned from Webster's definitions of ethics and hacker, an ethical hacker is someone proficient with computers and adheres to the code of behavior for their profession. C.C. Palmer in the IBM Systems Journal offers this description, "ethical hackers…employ the same tools and techniques as the intruders, but they…neither damage the target systems nor steal information. Instead, they…evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them." [4] Jeff Moss, founder of computer security service DefCon and BlackHat, agrees that, "Hacking and cyber-ethics need not be in conflict. You can be a hacker and be ethical at the same time." [5]

There is a long running debate about the proper definition of the word hacker and its many derivatives. The details of this debate are beyond the scope of this paper but it is mentioned to forewarn the reader that in general conversation the term hacker can have varying, even opposite, meanings. Ed Skoudis, in his book Counter Hack, provides the following suggestion, "Hackers, crackers, and hats of all colors—let's just use "attackers"…to refer to someone who attacks computers…The attacker may be a hacker, cracker, white hat, black hat, gray hat, super elite, security researcher, or even a penetration tester. Whatever their skill level, motivation, and the nomenclature you prefer, they are attacking computers." [6] Ethical hackers and malicious hackers both attack computers, only their intent differs.

How and What Ethical Hackers Are Taught

There is no universal method or skill set for training an ethical hacker. Much like the difficulty in defining a hacker, some security professionals don't agree with what ethical hackers should be taught. Palmer states that, "The idea of testing the security of a system by trying to break into it is not new. Whether an automobile company is crash-testing cars, or an individual is testing his or her skill at martial arts by

sparring with a partner, evaluation by testing under attack from a real adversary is widely accepted as prudent." [4] Whereas, Ira Winkler feels that, "The process of breaking into systems has minimal use in the security profession. It is infinitely more difficult to secure computers than it is to break into them. You have to know the proper procedures for fixing the problems. The students should then be trained in what NOT to do. This includes warnings about attacks that can cause denial of service, and how attacks can backfire. There must then be discussion about how to recover if a disaster does happen, and the what to do when you detect a real attack…students should then be educated in the legal and political aspects of ethical hacking." [7]

Now that a little is known about what an ethical hacker should be and do, how and where someone gets their ethical hacker skill set is important to explore. Information Security and hacking books, professional and academic courses, various Internet services like websites and Internet Relay Chat (IRC), friends, and family members all help train ethical hackers. Michael Roberts, President of Mile2, gives some idea of what his company teaches, "In a nutshell, we are teaching them to think like the bad guys by looking from the outside back into their own enterprise and…all the nasty tools that the bad guys use and how to use them so that they can effectively do penetration testing on their own network…all the methods of hacking whether it is active hacking or Trojan type viruses…just about anything that's a threat to a network. But we also cover the soft aspects of hacking such as social engineering, the art of deception and the way hackers try to identify personal information that might lead to potential passwords to escalate their privileges once they get into the network." [8] The Mile2 courses aren't free and can take several days to complete. However, there are free and portable resources on the Internet as well. Websites such as IronGeek.com [9] provide free videos that lead the viewer through step-by-step attacks. Almost anyone who can watch a video can perform these attacks with the added convenience of rewinding and viewing them over and over if needed or even downloading them. This format also allows for easy distribution of this knowledge even if the viewer speaks a different language, a simple monkey-see, monkey-do situation.

Don't Overlook the Risks

Two important questions to ask when teaching these potentially harmful skills are, whether or not they should be taught, and how to teach them safely. It is possible that the very act of describing an information system vulnerability or attack method could lead a student with a malicious bent to attack systems. Also, a channel of communication with other malicious hackers, e.g. a malicious hackers group website, could be initiated simply by providing a web address or URL. An important lesson was learned on September 11 when the passenger jets crashed into the World Trade Center. Suddenly flight simulation software became a tool used to train murderers. Prior to this event most American citizens didn't see the nefarious use for this software which helped the pilots learn the cockpit controls and how to fly their weapon. The dangers present in teaching information security concepts can be as destructive in the wrong hands and don't require loss of the attacker's life.

Roberts of Mile2 says the following about his company's most "expert" hacking class, "if we were to teach it to people that weren't supposed to be doing that class – I was told by one of our friends here in the States that we'd get into almost as much trouble as exporting Stinger missiles because it is electronic warfare." [8] He goes on to say that, "We have hackers always trying to get into our web server" What happens if one of these hackers breaches Mile2's defenses and distributes these "munitions" freely around the Internet?

Minimizing the Risks of Generating Malicious Hackers

Ethical behavior is easier to model than to teach. Brian Harvey of the University of California at Berkeley compares ethical hacking training to teaching someone karate, both of which when improperly used can cause serious problems for both the attacker and target, and offers four suggestions: provide a "serious" model, provide access to real power, provide challenging problems and access to expertise (i.e. apprenticeship), provide a safe arena for moral experimentation. [10] Applying Harvey's advice directly to ethical hacking courses would mean to be a good example for students, i.e. the security trainers should be a near ideal example of a security professional, the student's goal. Trainers should be a plum line against which students can measure their own conduct. Students should use real tools in class. Training students to use crippled or bogus tools discounts the students their experience and may lead them to have a limited view of a real malicious attacker's power. The instructor should realize that they are responsible for the moral development of students not only their technical skill and should steer them in the direction of challenges appropriate to each one's progress providing personal expertise to help the learner. Students should have a safe place to perform attacks of any degree to see their effect. This should not be limited to

technical experiments but also “soft” attacks like social engineering, and malware, e.g. e-mail that carries a worm or virus.

In the event that every possible effort has been made to instill values into students but still fail, safeguards must be in place to account for such occasions. As Joseph Malee suggests, “Ethics do not replace good policies…More and more these days, companies are confronted with employees engaged in unethical behavior in the workplace…Promoting ethical principles can instill positive behavior… but policies … provide clear and mandatory guidelines for acceptable conduct…Even with the greatest efforts of a trainer to instill an ethical mindset into students, simply trusting that students will behave in an ethic manner isn’t enough. Acceptable Use Policies must be enforced to ensure proper conduct.” [11] A policy should be in place to dissuade students with weak ethics. Information security policies should clearly present the improper forms of hacking as illegal or unethical. All activities should be represented as strictly right or wrong so as not to be too "ethically neutral". Exposing students to the ease with which hackers are caught and the laws that they are subject to can help reduce their potential to do wrong. Fear, or rather respect, is a useful tool in this battle. The CISSP (Certified Information Systems Security Professional) exam, one of the 20+ certification exams mentioned earlier, identifies three reasons that contribute to deterrence of crime: the fear of penalty, the probability of being caught, and the probability of the penalty being administered. Schwartau, a self professed hacker and hacking book author says, “The fear of being caught can be a powerful deterrent to malicious behavior. My son somehow discovered that hacking is a people issue, and that is how he gathered up the neighbor's passwords, by 'shoulder surfing'-- looking over their shoulders as they typed in their passwords, a classic social engineering trick. [I] pretended to call the FBI when [I] found out what [my] son was doing and [he] was terrified. So I said 'Well, I guess I could help you fix it if you promise never to do this again.' I made him go to the neighbors, tell them what he had done and also what they needed to do to make themselves more secure.” [5]

It is imperative that all trainers teach the countermeasures to each attack strategy. New laws are continually being written and old ones are being brought up to date to deal with people that have weak morals. After completing a hacking course, a student should be aware of how difficult it is to successfully remain invisible online in post September 11 America. Unfortunately, policies are often where we drop the ball. Policies that aren’t up-to-date often miss the threat that new technologies, like USB flash drives, present. Leon Erlanger states that, “Most organizations have no policy in place for detecting USB drives or regulating their use…most of them [USB drives] are tiny, [and] very easy to hide.” [12] Some of these “memory sticks” even look like an ink pen which lessens the ability of visually detecting who has them. After completing “hacker” training, a student may have the mind set and abilities to use a device like this to readily steal information or execute security tools in order to attack a resource, possibly undetected. Every effort should be made to properly draft and police good security policies. If a student’s conscience fails, fear often will provide guidance.

Conclusion

The benefits of training ethical hackers far out weigh the risks associated with it. Skoudis explains why he wrote a book on hacking: “Let’s face it – the malicious attackers have all the information they need to do all kinds of nasty things. If they don’t have the information now, they can get it easily enough on the Internet though a variety of Web sites, mailing lists, and newsgroups devoted to hacking. Experienced hackers often selectively share information with new attackers to get them started. Indeed, the communication channels in the computer underground among attackers are often far better than the communication among computer professionals. This book is one way to help make things more even.” [6]

As quickly as the field of Information Security is changing, the “good guys” need all the information and help that they can get. “Keeping up with the ever-changing world of computer and network security requires continuous education and review. Just as in sports or warfare, knowledge of the skills and techniques of your opponent is vital to your success. In the computer security realm, the ethical hacker's task is the harder one. With traditional crime anyone can become a shoplifter, graffiti artist, or a mugger.” [4] Proper security training should instill students with a strong ethical sense of what they should and shouldn’t do as security professionals. Policies should help guide students for sections of the training which are ineffective. Properly enforced Laws should be in place to reinforce a student’s healthy fear of getting caught performing unethical attacks.

To conclude and answer the question of whether Ethical Hacker training is actually training the enemy, the bad guys are way ahead of the good guys in the information security arms race. Any and every tool and useful piece of knowledge should be taught to budding security professionals. Safeguards should be in place to help deter students but by no means should ethical hacker training be crippled or halted. Long live

the ethical hackers.

References and Citations

Websites, Books, and Journals

[1] National Security Agency/Central Security Service (NSA/CSS), http://www.nsa.gov/programs/employ/news.cfm

[2] Google.com, http://www.google.com

[3] Dictionary.com, http://www.dictionary.com

[4] Palmer, C. C.; “ETHICAL HACKING”; IBM Systems Journal, 0018-8670, June 1, 2001, Vol. 40, Issue 3

[5] Delio, Michelle; “Wired News: Teaching Kids About Hacking” April 2001; URL: http://www.wired.com/news/culture/0,1284,42923,00.html

[6] Skoudis, Ed. Counter Hack. A step-by-step guide to Computer Attacks and Effective Defenses. Prentice-Hall, Inc. 2002

[7] Winkler, Ira; “Teaching Ethical Hacking?”, The ISSA Journal, March 2004

[8] ABC Radio National: The Buzz 3 April 2004; ”Training for Ethical Hackers”, URL: http://www.abc.net.au/rn/science/buzz/stories/s1079993.htm

[9] IronGeek.com, http://www.irongeek.com

[10] Harvey, Brian, “Computer Hacking and Ethics”; University of California, Berkeley

[11] Malee, Joseph; “Ethics do not replace good policies”, The ISSA Journal, February 2004

[12] Leon Erlanger; “Hacked in a Flash”, PC Magazine, March 16, 2004, http://www.pcmag.com

[13] Principles of Information Security. Dr. Michael E. Whitman, CISSP. Course Technology, Inc. 2003